# WAS Web Application Report

## Results(240)

### Vulnerability (181)

150162 Use of JavaScript Library with Known Vulnerability

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/

| | | | |
|---|---|---|---|
| **Finding #** | 14849392 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | dc3d9672-eb50-44a8-ae0c-7531a8420923 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-937 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A9 Using Components with Known Vulnerabilities | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | - | **Times Detected** | 2 |

**CVSS V3 Base** 6.5 **CVSS V3 Temporal** 5.6 **CVSS V3 Attack Vector** Network

#### Details

**Threat**

The web application is using a JavaScript library that is known to contain at least one vulnerability.

**Impact**

Attackers could potentially exploit the vulnerability in the JavaScript library. The impact of a successful exploit depends on the nature of the vulnerability and how the web application makes use of the library.

**Solution**

Please refer to the information provided in the response section. Also check the vendor's security advisories related to the vulnerable version of the library.

#### Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |

#### Payloads

**#1 Request**

GET https://www.parisssd.org/

Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

**#1 Response**

Vulnerable javascript library: Mustache
version: 0.5.0-dev

Details:
Mustache JS version before 2.2.1 do not escape user input correctly and this could lead to potential XSS (https://github.com/janl/mustache.js/pull/530, https://github.com/janl/mustache.js/releases/tag/ v2.2.1).

Solution: Mustache JS version 2.2.1 has been released to address the issue. Please refer to vendor documentation (https://github.com/janl/mustache.js/blob/master/CHANGELOG.md) for latest the security updates.

Found on the following pages (only first 10 pages are reported):
https://www.parisssd.org/ https://www.parisssd.org/Domain/4
https://www.parisssd.org/Page/1
https://www.parisssd.org/domain/156
https://www.parisssd.org/domain/11
https://www.parisssd.org/domain/268
https://www.parisssd.org/domain/157
https://www.parisssd.org/domain/159
https://www.parisssd.org/domain/158
https://www.parisssd.org/domain/161

## 150162 Use of JavaScript Library with Known Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/

| | | | |
|---|---|---|---|
| **Finding #** | 14849446 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 57013e72-ccfd-41d0-b9f4-520a1beebae8 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-937 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A9 Using Components with Known Vulnerabilities | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | - | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 6.5 | **CVSS V3 Temporal** | 5.6 | **CVSS V3 Attack Vector** | Network |

### Details

**Threat**
The web application is using a JavaScript library that is known to contain at least one vulnerability.

**Impact**
Attackers could potentially exploit the vulnerability in the JavaScript library. The impact of a successful exploit depends on the nature of the vulnerability and how the web application makes use of the library.

**Solution**
Please refer to the information provided in the response section. Also check the vendor's security advisories related to the vulnerable version of the library.

### Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |

### Payloads

**#1 Request**

GET https://www.parisssd.org/

Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

# WAS Web Application Report

## #1 Response

Vulnerable javascript library: jQuery version: 3.0.0 script uri:
https://www.parisssd.org/Static/GlobalAssets/Scripts/min/jquery-3.0.0.min.js

Details:
CVE-2019-11358: jQuery versions below 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. An unsanitized source object containing an enumerable __proto__ property could extend the native Object.prototype. Please refer following resources for more details: https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/, https://nvd.nist.gov/vuln/detail/CVE-2019-11358, https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b, https://nvd.nist.gov/vuln/detail/CVE-2019-11358.

---

jQuery versions below 3.5.0 used a regex in its jQuery.htmlPrefilter method. This regex which is used to ensure that all tags are XHTML-compliant could introduce a vulnerability to Cross-site Scripting(XSS) attack. Please refer to vendor documentation (https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ and https://jquery.com/upgrade-guide/3.5/) for the security fix details.

---

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. Please refer https://github.com/jquery/jquery/security/advisories/GHSA-gxr4-xjj5-5px2 and https://nvd.nist.gov/vuln/detail/CVE-2020-11022 for details.

Found on the following pages (only first 10 pages are reported):
https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=4&IgnoreRedirect=true
https://www.parisssd.org/Domain/4 https://www.parisssd.org/Page/1
https://www.parisssd.org/domain/156 https://www.parisssd.org/domain/11
https://www.parisssd.org/domain/268 https://www.parisssd.org/domain/157
https://www.parisssd.org/domain/159 https://www.parisssd.org/domain/158

## 150122 Cookie Does Not Contain The "secure" Attribute

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/

| | | | |
|---|---|---|---|
| **Finding #** | 14849374 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 80c88895-ecac-47cc-844f-dec468088482 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-614 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A3 Sensitive Data Exposure | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION | **Times Detected** | 2 |
| **CVSS V3 Base** | 4.3 | **CVSS V3 Temporal** | 4.1 |
| **CVSS V3 Attack Vector** | | | |

### Details

Network

**Threat**
The cookie does not contain the "secure" attribute.

**Impact**
Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

**Solution**
If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

### Detection Information

**Cookie Name(s)** **SWScreenWidth, SWClientWidth, SWPageNavState**

**Authentication** In order to detect this vulnerability, no authentication has been required.

## Payloads

### #1 Request

GET https://www.parisssd.org/

Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

SWScreenWidth=240; path=/; domain=www.parisssd.org
Cookies set via JavaScript do not have an associated HTTP response header.

SWClientWidth=1024; path=/; domain=www.parisssd.org
Cookies set via JavaScript do not have an associated HTTP response header.

SWPageNavState=; path=/; domain=www.parisssd.org
Cookies set via JavaScript do not have an associated HTTP response header.

## 150123 Cookie Does Not Contain The "HTTPOnly" Attribute

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/

| | | | |
|---|---|---|---|
| **Finding #** | 14849372 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | f90f72dc-5993-495b-a562-274dc1e84c7a | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-1004 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A3 Sensitive Data Exposure | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION | **Times Detected** | 2 |

**CVSS V3 Base** 4.3 **CVSS V3 Temporal** 4.1 **CVSS V3 Attack Vector**

## Details

Network

### Threat
The cookie does not contain the "HTTPOnly" attribute.

### Impact
Cookies without the "HTTPOnly" attribute are permitted to be accessed via JavaScript. Cross-site scripting attacks can steal cookies which could lead to user impersonation or compromise of the application account.

### Solution
If the associated risk of a compromised account is high, apply the "HTTPOnly" attribute to cookies.

## Detection Information

**Cookie Name(s)** **RedirectTo, SWClientWidth, SWPageNavState, SWScreenWidth**

**Authentication** In order to detect this vulnerability, no authentication has been required.

## Payloads

### #1 Request

GET https://www.parisssd.org/

Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

RedirectTo=
200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 229493
Connection: keep-alive
Date: Sat, 15 Jan 2022 03:03:51 GMT
Cache-Control: no-cache, no-store
Pragma: no-cache
Expires: -1
Server: Microsoft-IIS/8.5
Strict-Transport-Security: max-age=31536000; includeSubDomains;
X-XSS-Protection: 1; mode=block
X-AspNet-Version: 4.0.30319
Set-Cookie: PSN=LjAVScvfF4t8u12OcOc08A==; path=/; secure; HttpOnly
PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; path=/; secure; HttpOnly
CSAN=8/YyjPiDJwJtBZxSxX5+iA==; path=/; secure; HttpOnly
AccountID=Xogon24LhVEF1Gfd40nUZQ==; path=/; secure; HttpOnly
APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8; path=/; secure; HttpOnly
SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; path=/; secure; HttpOnly
RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fdefault.aspx%3FPageID%3D1; path=/; secure
CancelRedirectTo=; expires=Fri, 14-Jan-2022 19:03:51 GMT; path=/; secure
X-Powered-By: ASP.NET
Content-Security-Policy: frame-ancestors 'self' https://*.ally.ac;
X-Frame-Options: SAMEORIGIN
X-Cache: Miss from cloudfront
Via: 1.1 b014854bd0108b7ed0058504b69ccb5a.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: SFO53-C1
X-Amz-Cf-Id: FiyGKLF5N2NWM1Z8ZNxXmZrBCX9bhRURxvJLOzh0G23iN6fEPLGZxg==

SWClientWidth=1024; path=/; domain=www.parisssd.org
Cookies set via JavaScript do not have an associated HTTP response header.

SWPageNavState=; path=/; domain=www.parisssd.org
Cookies set via JavaScript do not have an associated HTTP response header.

SWScreenWidth=240; path=/; domain=www.parisssd.org
Cookies set via JavaScript do not have an associated HTTP response header.

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150246 Path-relative stylesheet import (PRSSI) vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/

| | | | |
|---|---|---|---|
| **Finding #** | 14849376 | **Severity** | Confirmed Vulnerability - Level 1 |
| **Unique #** | 1002a399-2339-4541-a791-04eafebfd333 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |

# WAS Web Application Report

| | | | |
|---|---|---|---|
| **CWE** | CWE-23 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | - | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 3.1 | **CVSS V3 Temporal** | 2.9 | **CVSS V3 Attack Vector** | Network |

## Details

### Threat

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to pathrelative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

### Impact

An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

### Solution

It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/
- Set response header X-Frame-Options: deny
- Set response header X-Content-Type-Options: nosniff.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |

## Payloads

### #1 Request

GET https://www.parisssd.org/

Referer: https://www.parisssd.org/
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

Relative Path CSS Links found:
<link rel="Stylesheet" type="text/css" href="../Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd-theme-default.css">

# WAS Web Application Report

## 150123 Cookie Does Not Contain The "HTTPOnly" Attribute

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org//cms/Module/SelectSurvey/TakeSurveyAction.aspx?DisplayHeader=

| | | | |
|---|---|---|---|
| **Finding #** | 14849386 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 05b4d1c3-dc51-44aa-97ed-61e90339afa9 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-1004 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A3 Sensitive Data Exposure | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION | **Times Detected** | 2 |

**CVSS V3 Base** 4.3 **CVSS V3 Temporal** 4.1 **CVSS V3 Attack Vector**

## Details

Network

### Threat
The cookie does not contain the "HTTPOnly" attribute.

### Impact
Cookies without the "HTTPOnly" attribute are permitted to be accessed via JavaScript. Cross-site scripting attacks can steal cookies which could lead to user impersonation or compromise of the application account.

### Solution
If the associated risk of a compromised account is high, apply the "HTTPOnly" attribute to cookies.

## Detection Information

**Cookie Name(s)** **SelectSurveyNetASPAdvancedCookie**

**Authentication** In order to detect this vulnerability, no authentication has been required.

**Access Path** Here is the path followed by the scanner to reach the exploitable URL:

https://www.parisssd.org/ https://www.parisssd.org/domain/299
https://www.parisssd.org/cms/module/selectsurvey/TakeSurvey.aspx?SurveyID=108

## Payloads

### #1 Request

GET https://www.parisssd.org//cms/Module/SelectSurvey/TakeSurveyAction.aspx?DisplayH eader=

Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

SelectSurveyNetASPAdvancedCookie=
200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 26708

Connection: keep-alive
Date: Sat, 15 Jan 2022 03:34:24 GMT
Cache-Control: private
Server: Microsoft-IIS/8.5
Strict-Transport-Security: max-age=31536000; includeSubDomains;
X-XSS-Protection: 1; mode=block
X-AspNet-Version: 4.0.30319
Set-Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; expires=Tue, 25-Jan-2022 03:34:24 GMT; path=/; secure
X-Powered-By: ASP.NET
Content-Security-Policy: frame-ancestors 'self' https://*.ally.ac;
X-Frame-Options: SAMEORIGIN
X-Cache: Miss from cloudfront
Via: 1.1 9d47bedfe2d83b5ed14a7d02ea9ca902.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: SFO53-C1
X-Amz-Cf-Id: BFe9CqFz2mUZ--mwgtODbXnsvNnQOw_AXnECq99ZTrlmTHir7FgXcw==

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150012 Blind SQL Injection

*https://www.parisssd.org* New

**URL:** https://www.parisssd.org//cms/Module/SelectSurvey/TakeSurveyAction.aspx?DisplayHeader=

| | | | |
|---|---|---|---|
| **Finding #** | 15428012 | **Severity** | Confirmed Vulnerability - Level 5 |
| **Unique #** | a47f93f9-d9ce-468a-8890-5888c1313695 | | |
| **Group** | - | **First Time Detected** | 15 Jan 2022 03:01 GMT |
| **CWE** | CWE-89 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A1 Injection | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-19 SQL INJECTION | **Times Detected** | 1 |
| **CVSS V3 Base** | 9.8 | **CVSS V3 Temporal** | 8 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

### Threat

Blind SQL injection is a specialized type of SQL injection that enables an attacker to modify the syntax of a SQL query in order to retrieve, corrupt, or delete data. A successful exploit manipulates the query's logic. Queries created by concatenating strings with SQL syntax and user-supplied data are prone to this vulnerability. When any part of the string concatenation can be modified, an attacker has the ability to change the meaning of the query.

Typical detection techniques for SQL injection vulnerabilities use a payload that attempts to produce an SQL error from the web application. Detection based on blind SQL injection uses inference based on the differences among the application's responses to various payloads. Blind SQL does not rely on error messages, which is beneficial when testing web applications that trap errors.

The WAS scanning engine uses a well-known technique called True / False inference to determine if there is a blind SQL injection vulnerability. Basically, it uses two payloads: one with a True condition and another with a False condition. If there is a blind SQL injection vulnerability, the query with the True condition payload will cause the web application to return a different response than the False condition payload.

A good example of a True condition payload is ' AND 1=1 (since 1 always equals 1, the condition is true). An example of a False condition payload is ' AND 1=2 (since 1 does not equal 2, the condition is false).

Say there is a web application with an input that searches customer first names and displays the results inside a table. Assume that if someone searches for John there is one result only. When scanning for blind SQL injection, the scanning engine sends two payloads:
- True condition payload: John' AND 1=1
This condition is true, so one record is returned and the output is John, which is the same as if the payload was the name John by itself.
- False condition payload: John' AND 1=2

The condition is false, so no records are returned and the output is nothing or a message such as No Results Found.

Seeing the difference in results, the scanning engine draws the conclusion that there is a blind SQL injection vulnerability.

### Impact
The scope of a SQL injection exploit varies greatly. If any SQL statement can be injected into the query, then the attacker has the equivalent access of a database administrator. This access could lead to theft of data, malicious corruption of data, or deletion of data.

### Solution
SQL injection vulnerabilities can be addressed in three areas: input validation, query creation, and database security.

All input received from the client side should be validated for correct content. If a value's type or content range is known beforehand, then stricter filters should be applied. For example, an email address should be in a specific format and only contain characters that make it a valid address; or numeric fields like a USA zip code should be limited to five digit values.

Prepared statements (also referred to as parameterized queries) provide strong protection from SQL injection. Prepared statements are precompiled SQL queries whose parameters can be modified when the query is executed. Prepared statements enforce the logic of the query and will fail if the query cannot be compiled correctly. Programming languages that support prepared statements provide specific functions for creating queries. These functions are more secure than string concatenation for assigning user-supplied data to a query.

Stored procedures are precompiled queries that reside in the database. Like prepared statements, they also enforce separation of query data and logic. SQL statements that call stored procedures should not be created via string concatenation, otherwise their security benefits are negated.

SQL injection exploits can be mitigated by the use of Access Control Lists or role-based access within the database. For example, a read-only account would prevent an attacker from modifying data, but would not prevent the user from viewing unauthorized data. Table and row-based access controls potentially minimize the scope of a compromise, but they do not prevent exploits.

For more information, see the OWASP SQL Injection Prevention Cheat Sheet.

## Detection Information

**Parameter** It has been detected by exploiting the parameter **ResponseStartDate** of the form located in URL **https://www.parisssd.org/cms/module/selectsurvey/ TakeSurvey.aspx?SurveyID=108**
The payloads section will display a list of tests that show how the param could have been exploited to collect the information

**Authentication** In order to detect this vulnerability, no authentication has been required.

**Access Path** Here is the path followed by the scanner to reach the exploitable URL:
https://www.parisssd.org/ https://www.parisssd.org/domain/299
https://www.parisssd.org/cms/module/selectsurvey/TakeSurvey.aspx?SurveyID=108

## Payloads

### #1 Request

POST https://www.parisssd.org//cms/Module/SelectSurvey/TakeSurveyAction.aspx?DisplayH eader=

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FPageID%3D4276; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289ab2a-9d2425fd36b8; Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*
Content-Length: 690
Content-Type: application/x-www-form-urlencoded

# WAS Web Application Report

cookieexists=true&AdminOrOwnerEditResponse=No&AdminOrOwnerResponseID=0&SurveyID=92KHm97&EmailAddressID=0&EmailMessageID=0&EID=&ResponseTy
%3D108&FirstPageQueryString=SurveyID%3D108&DisplayPageNumber=1&ResponseStartDate=1%2F14%2F2022%2010%3A34%3A14%20PM
%27%2C0%2C0%29%3BWAITFOR%20DELAY%2700:00:29%27--
%20&ActualPageNumber=1&hdnUpdatingSurvey=false&ResponseID=0&QuestionNumber=4&prevQN=1&buttonclicked=0&save=&savePage=&SP=
%2C&QID109=1%2F14%2F2022&QID111||OTHERCHECKBOX=1&QID110=1&QID111||CHECKBOX||107=1&QID111||CHECKBOX||108=1&QID111OTHERTEXT=1&QID111||
CHECKBOX||109=1&QID111||CHECKBOX||110=1&QID111||CHECKBOX||111=1

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment: (Times are expressed in milliseconds.)
Expected response delay: 28000
Observed response delay: 29139
Mean response time: 499
Standard deviation: 638
Number of stddev from mean: 44.823086

This vulnerability was identified using time-based inference that compared the average response time of a page to its response time with an injected payload. This vulnerability is confirmed based on timing rather than the content of the response.

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Domain/14?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848468 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 80f1de82-6516-4c09-9b65-c9ae552eb14a | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

# WAS Web Application Report

## Detection Information

**Parameter** No param has been required for detecting the information.

**Authentication** In order to detect this vulnerability, no authentication has been required.

**Access Path** Here is the path followed by the scanner to reach the exploitable URL:

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=4&SectionMax=15&DirectoryType=6

## Payloads

### #1 Request

GET https://www.parisssd.org/Domain/14?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Domain/14

```
hite-space: pre-wrap; word-wrap: break-word; }
}
 @media screen and (max-width: 479px) {
 pre { width: 280px; }
 }
 </style>
</head>

 <body bgcolor="white">

 <span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

 <h2> <i>Runtime Error</i> </h2></span>

 <font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 <b> Description: </b>An exception o
```

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Domain/156?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848336 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 3e7bafef-0de3-47de-9807-1df0d1073690 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

# WAS Web Application Report

| CVSS V3 Base | 5.3 | CVSS V3 Temporal | 4.7 | CVSS V3 Attack Vector |
|---|---|---|---|---|

## Details

Network

### Threat
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=4&SectionMax=15&DirectoryType=6

## Payloads

### #1 Request

GET https://www.parisssd.org/Domain/156?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Domain/156

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Domain/157?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848464 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 16a42249-d005-47e9-9043-c1ddee52de4e | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 4.7 **CVSS V3 Attack Vector**

Details

Network

### Threat
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

# WAS Web Application Report

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=4&SectionMax=15&DirectoryType=6

## Payloads

### #1 Request

GET https://www.parisssd.org/Domain/157?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Domain/157

```
hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>Runtime Error</i> </h2></span>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

<b> Description: </b>An exception o
```

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Domain/159?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848522 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | fe35c5fa-2e93-4d1a-9077-a3643de774d6 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

# WAS Web Application Report

| CVSS V3 Base | 5.3 | CVSS V3 Temporal | 4.7 | CVSS V3 Attack Vector |
|---|---|---|---|---|

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=4&SectionMax=15&DirectoryType=6

## Payloads

### #1 Request

GET https://www.parisssd.org/Domain/159?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Domain/159

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Domain/161?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848530 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 6fc0ea1c-44b9-4a72-8b43-298e44b9816b | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 4.7 **CVSS V3 Attack Vector**

Details

Network

### Threat
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

# WAS Web Application Report

## Detection Information

**Parameter** No param has been required for detecting the information.

**Authentication** In order to detect this vulnerability, no authentication has been required.

**Access Path** Here is the path followed by the scanner to reach the exploitable URL:

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=4&SectionMax=15&DirectoryType=6

## Payloads

### #1 Request

GET https://www.parisssd.org/Domain/161?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Domain/161

```
hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>Runtime Error</i> </h2></span>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

<b> Description: </b>An exception o
```

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Domain/209?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848414 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | eaa995cb-434e-46bb-b84b-50242443c311 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

# WAS Web Application Report

| CVSS V3 Base | 5.3 | CVSS V3 Temporal | 4.7 | CVSS V3 Attack Vector |
|---|---|---|---|---|

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=4&SectionMax=15&DirectoryType=6

## Payloads

### #1 Request

GET https://www.parisssd.org/Domain/209?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Domain/209

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Domain/232?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848444 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 2f5b04b7-d042-4431-8a3b-b51bdefc53c0 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 4.7 **CVSS V3 Attack Vector**

Details

Network

### Threat
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

# WAS Web Application Report

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=4&SectionMax=15&DirectoryType=6

## Payloads

### #1 Request

GET https://www.parisssd.org/Domain/232?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Domain/232

```
hite-space: pre-wrap; word-wrap: break-word; }
}
 @media screen and (max-width: 479px) {
 pre { width: 280px; }
 }
 </style>
</head>

 <body bgcolor="white">

 <span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

 <h2> <i>Runtime Error</i> </h2></span>

 <font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 <b> Description: </b>An exception o
```

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Domain/337?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848462 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 4585e4cc-b49f-4f27-935a-2b6bc50bb719 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

# WAS Web Application Report

| CVSS V3 Base | 5.3 | CVSS V3 Temporal | 4.7 | CVSS V3 Attack Vector |
|---|---|---|---|---|

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=4&SectionMax=15&DirectoryType=6

## Payloads

### #1 Request

GET https://www.parisssd.org/Domain/337?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Domain/337

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Domain/392?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848352 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | dfdd5410-bb47-4902-90e0-659c10206792 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 4.7 **CVSS V3 Attack Vector**

Details

Network

### Threat
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

# WAS Web Application Report

## Detection Information

**Parameter** No param has been required for detecting the information.

**Authentication** In order to detect this vulnerability, no authentication has been required.

**Access Path** Here is the path followed by the scanner to reach the exploitable URL:

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=4&SectionMax=15&DirectoryType=6

## Payloads

### #1 Request

GET https://www.parisssd.org/Domain/392?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Domain/392

```
hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>Runtime Error</i> </h2></span>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

<b> Description: </b>An exception o
```

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Domain/398?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848506 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 16eaefad-5458-4356-9611-3e1814a82eff | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

# WAS Web Application Report

| CVSS V3 Base | 5.3 | CVSS V3 Temporal | 4.7 | CVSS V3 Attack Vector |
|---|---|---|---|---|

## Details

Network

### Threat
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=4&SectionMax=15&DirectoryType=6

## Payloads

### #1 Request

GET https://www.parisssd.org/Domain/398?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Domain/398

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150246 Path-relative stylesheet import (PRSSI) vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Domain/4

| | | | |
|---|---|---|---|
| **Finding #** | 14848364 | **Severity** | Confirmed Vulnerability - Level 1 |
| **Unique #** | ca17bf0a-e62a-4b1c-845e-244ed7d19836 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-23 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | - | **Times Detected** | 2 |

**CVSS V3 Base** 3.1 **CVSS V3 Temporal** 2.9 **CVSS V3 Attack Vector** Network

### Details

**Threat**

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to pathrelative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

**Impact**

An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

**Solution**

It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/

- Set response header X-Frame-Options: deny
- Set response header X-Content-Type-Options: nosniff.

## Detection Information

**Parameter** No param has been required for detecting the information.

**Authentication** In order to detect this vulnerability, no authentication has been required.

**Access Path** Here is the path followed by the scanner to reach the exploitable URL:

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/Domain/4

Referer: https://www.parisssd.org/
Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fdefault.aspx%3FPageID%3D1; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

Relative Path CSS Links found:
<link rel="Stylesheet" type="text/css" href="../Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd-theme-default.css">

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Domain/6?"%26gt;%26lt;script%26gt;_q_q='('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848394 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | e6e6446a-df82-4eae-9a99-bc19593e7d80 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=4&SectionMax=15&DirectoryType=6

## Payloads

# WAS Web Application Report

## #1 Request

GET https://www.parisssd.org/Domain/6?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Domain/6

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/APIs/

| | | | |
|---|---|---|---|
| **Finding #** | 14849418 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 5f908c8d-900f-4e3e-ba51-f3d716e534f9 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 |
| **CVSS V3 Attack Vector** | Network | | |

### Details

**Threat**

A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

# WAS Web Application Report

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/APIs/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FPageID%3D4276; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289ab2a-9d2425fd36b8; Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/BUGS

| | | | |
|---|---|---|---|
| **Finding #** | 14848552 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 8e607975-6444-4918-bb17-370835a4510b | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

# WAS Web Application Report

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/BUGS

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/CHANGELOG

| | | | |
|---|---|---|---|
| **Finding #** | 14849384 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 87ce8cd4-2a40-4234-8cc2-8724c01754bc | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |

# WAS Web Application Report

| | | | |
|---|---|---|---|
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 |
| **CVSS V3 Attack Vector** | Network | | |

## Details

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/CHANGELOG

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

150004 Path-Based Vulnerability — *https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/ChangeLog

# WAS Web Application Report

| | | | |
|---|---|---|---|
| **Finding #** | 14848344 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | b6726007-e29e-4c62-ba72-7347a7b2ad3c | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/ChangeLog

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

# WAS Web Application Report

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/ChangeLog.txt

| | | | |
|---|---|---|---|
| **Finding #** | 14848484 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | feeea03d-9e83-4599-a14f-5e6ad3417017 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 |
| **CVSS V3 Attack Vector** | | | |

### Details

Network

### Threat

A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact

The contents of this file or directory may disclose sensitive information.

### Solution

Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

### Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

### Payloads

# WAS Web Application Report

## #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/ChangeLog.txt

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

### 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/INSTALL

| | | | |
|---|---|---|---|
| **Finding #** | 14848466 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | aae8f61c-ac04-425e-8d67-dbfa5e145130 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

Details

Network

### Threat

A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact

The contents of this file or directory may disclose sensitive information.

### Solution

Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/INSTALL

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/SERVICE/

| | | | |
|---|---|---|---|
| **Finding #** | 14849396 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | a3afebe0-135d-4ec0-9395-697bc5bd7495 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

### Network

**Threat**
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/SERVICE/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FPageID%3D4276; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289ab2a-9d2425fd36b8; Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/Service/

| | | | |
|---|---|---|---|
| **Finding #** | 14848490 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 22a8b678-4373-4016-9f5d-c47f9999c8da | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

# WAS Web Application Report

Details

Network

## Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

## Impact
The contents of this file or directory may disclose sensitive information.

## Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

### Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

### Payloads

#### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/Service/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FPageID%3D4276; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289ab2a-9d2425fd36b8; Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

#### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

150004 Path-Based Vulnerability https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/WS/

# WAS Web Application Report

| | | | |
|---|---|---|---|
| **Finding #** | 14848430 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 774612ed-439b-4961-a1fc-98182713d987 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/WS/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FPageID%3D4276; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289ab2a-9d2425fd36b8; Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

# WAS Web Application Report

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/WSDL/

| | | | |
|---|---|---|---|
| **Finding #** | 14849420 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | ad069859-9969-4303-9b2b-bc296499beac | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 5 **CVSS V3 Attack Vector**

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

# WAS Web Application Report

## #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/WSDL/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FPageID%3D4276; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289ab2a-9d2425fd36b8; Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/ core/

| | | | |
|---|---|---|---|
| **Finding #** | 14849414 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 36e5c259-9494-4b70-b70d-efbec01ffd62 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION WASC-16 DIRECTORY INDEXING WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Detection Information

# WAS Web Application Report

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/_core/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/adm/

| | | | |
|---|---|---|---|
| **Finding #** | 14849428 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 9ae89c1a-60ce-4117-bfc6-0eecdb69ecfb | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 |
| **CVSS V3 Attack Vector** | Network | | |

## Details

### Threat

A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact

The contents of this file or directory may disclose sensitive information.

### Solution

Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/adm/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/admin.jsp

| | | | |
|---|---|---|---|
| **Finding #** | 14848502 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 0e0fc05d-2d42-4407-9754-6fee0a292dbb | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

# WAS Web Application Report

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/admin.jsp

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/admin.php

| | | | |
|---|---|---|---|
| **Finding #** | 14849438 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 93c0b6ba-0232-4a27-a669-d3018db4b42c | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |

# WAS Web Application Report

| | | | |
|---|---|---|---|
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/admin.php

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

# WAS Web Application Report

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/admin/

| | | | |
|---|---|---|---|
| **Finding #** | 14849478 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 4413a006-72c1-4533-b32e-69da457065eb | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat

A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact

The contents of this file or directory may disclose sensitive information.

### Solution

Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20211215/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/admin/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.108, 15.158.0.118108=151; SelectSurveyASPAnonymousUserID=AnonymousUserID=1698; SWSessionID=46cdda55-b9f9-4dab-b3a3-3949ba195486; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==;

# WAS Web Application Report

PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==;
ASP.NET_SessionId=bgdwdkaztlufjmix5scpx3uf; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept:
*/*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/administration/

| | | | |
|---|---|---|---|
| **Finding #** | 14849430 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 2f5ac242-ad90-49e3-a18a-0beb1f116a00 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

# WAS Web Application Report

https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/administration/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/backup/

| | | | |
|---|---|---|---|
| **Finding #** | 14848390 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 9f18a649-607c-4fbb-bf6b-868d5a1e716f | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat

A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact

The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/backup/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/bin/

| | | | |
|---|---|---|---|
| **Finding #** | 14849410 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | fd0d18d9-de2c-41a8-97af-6b9159823931 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

### Network

# WAS Web Application Report

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/bin/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/classes/

| | | | |
|---|---|---|---|
| **Finding #** | 14849452 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 179bc673-f6cf-4c0c-b64f-c285b653fcf7 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |

# WAS Web Application Report

| | | | |
|---|---|---|---|
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/classes/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:

# WAS Web Application Report

Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/common/

| | | | |
|---|---|---|---|
| **Finding #** | 14849476 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | a2e3f923-ec2e-4bf8-8538-4110339655b0 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION WASC-16 DIRECTORY INDEXING WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 5 **CVSS V3 Attack Vector**

Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20211215/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/common/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.108, 15.158.0.118108=151; SelectSurveyASPAnonymousUserID=AnonymousUserID=1698;

SWSessionID=46cdda55-b9f9-4dab-b3a3-3949ba195486; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=bgdwdkaztlufjmix5scpx3uf; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/config/

| | | | |
|---|---|---|---|
| **Finding #** | 14849382 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 11f67e62-6824-4b1c-a187-cb4692fc5c15 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 |
| **CVSS V3 Attack Vector** | Network | | |

## Details

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

# WAS Web Application Report

## #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/config/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/core/

| | | | |
|---|---|---|---|
| **Finding #** | 14849458 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 75082345-af96-4c91-be5e-1c9d113ac29b | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

### Details

Network

### Threat

A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact

The contents of this file or directory may disclose sensitive information.

### Solution

Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

### Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/core/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/css/

| | | | |
|---|---|---|---|
| **Finding #** | 14849474 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 0e9595a9-fc38-4c1b-b5d5-0c8646482f81 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

### Network

**Threat**
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

# WAS Web Application Report

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20211215/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/css/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.108, 15.158.0.118108=151; SelectSurveyASPAnonymousUserID=AnonymousUserID=1698; SWSessionID=46cdda55-b9f9-4dab-b3a3-3949ba195486; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=bgdwdkaztlufjmix5scpx3uf; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/data/

| | | | |
|---|---|---|---|
| **Finding #** | 14849436 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 5eb82562-0140-4211-94f3-2106fc27c124 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

# WAS Web Application Report

Details

Network

**Threat**
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

**Impact**
The contents of this file or directory may disclose sensitive information.

**Solution**
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/data/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

150004 Path-Based Vulnerability — *https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/db/

# WAS Web Application Report

| | | | |
|---|---|---|---|
| **Finding #** | 14849450 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | f385754a-a63b-4d77-91f0-6f2a4479c1d0 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/db/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;

# WAS Web Application Report

Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/docs/

| | | | |
|---|---|---|---|
| **Finding #** | 14849422 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 8dac7597-1945-46da-a02e-e892b2c1294a | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/docs/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/documents/

| | | | |
|---|---|---|---|
| **Finding #** | 14849378 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 31686af8-193d-4072-93c1-b37062faaff1 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

# WAS Web Application Report

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/documents/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/download/

| | | | |
|---|---|---|---|
| **Finding #** | 14849466 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | a279c51b-a65e-4038-8435-5b328d6ae2b3 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

**Threat**
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

# WAS Web Application Report

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/download/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/errors/

| | | | |
|---|---|---|---|
| **Finding #** | 14849390 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 73490bc2-09e6-4e19-93f4-54cc30b98244 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION WASC-16 DIRECTORY INDEXING WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

# WAS Web Application Report

Details

Network

**Threat**
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

**Impact**
The contents of this file or directory may disclose sensitive information.

**Solution**
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/errors/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

# WAS Web Application Report

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/export/

| | | | |
|---|---|---|---|
| **Finding #** | 14849388 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | e3be152e-87a3-4be8-8002-a9424d89d740 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 |
| **CVSS V3 Attack Vector** | Network | | |

## Details

### Threat

A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact

The contents of this file or directory may disclose sensitive information.

### Solution

Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/export/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

# WAS Web Application Report

## #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

### 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/external/

| | | | |
|---|---|---|---|
| **Finding #** | 14849454 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 719c5008-c155-40fd-b572-d03ea6b4f0ee | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/external/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

### 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/extranet/

| | | | |
|---|---|---|---|
| **Finding #** | 14849368 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | b0442d78-3dca-495f-a102-39806082193d | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |

# WAS Web Application Report

**Access Path** Here is the path followed by the scanner to reach the exploitable URL:

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/extranet/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/files/

| | | | |
|---|---|---|---|
| **Finding #** | 14849460 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 8b47f7ea-2257-4c36-995f-fec97083b1c6 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

### Network

**Threat**
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

# WAS Web Application Report

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/files/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/functions/

| | | | |
|---|---|---|---|
| **Finding #** | 14849462 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | c22f9c43-fccd-410b-9a34-903174bebf24 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

### Network

# WAS Web Application Report

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/functions/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/history/

| | | | |
|---|---|---|---|
| **Finding #** | 14849468 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 1f3c922c-1ce9-4ead-aef9-d0d22fe65c75 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |

# WAS Web Application Report

| | | | |
|---|---|---|---|
| CWE | CWE-22 | Last Time Detected | 15 Jan 2022 03:01 GMT |
| OWASP | A5 Broken Access Control | Last Time Tested | 15 Jan 2022 03:01 GMT |
| WASC | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | Times Detected | 2 |

| | | | | | |
|---|---|---|---|---|---|
| CVSS V3 Base | 5.3 | CVSS V3 Temporal | 5 | CVSS V3 Attack Vector | |

## Details

Network

### Threat

A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact

The contents of this file or directory may disclose sensitive information.

### Solution

Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/history/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

# WAS Web Application Report

## #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

### 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/image/

| | | | |
|---|---|---|---|
| **Finding #** | 14849400 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | be570f8a-e228-4793-9906-0d17b682b489 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/image/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

### 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/images/

| | | | |
|---|---|---|---|
| **Finding #** | 14848340 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | f2459e76-945c-4033-9ae3-df529cc0f06d | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |

# WAS Web Application Report

**Access Path** Here is the path followed by the scanner to reach the exploitable URL:

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/images/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/imports/

| | | | |
|---|---|---|---|
| **Finding #** | 14849366 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | fc8ae8d8-ce27-4158-a88b-2c404ac1a656 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION WASC-16 DIRECTORY INDEXING WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

### Network

**Threat**
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/imports/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/include/

| | | | |
|---|---|---|---|
| **Finding #** | 14848376 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 04188e3d-503b-4df8-9cc9-e778fa6d2f79 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 |
| **CVSS V3 Attack Vector** | Network | | |

## Details

### Threat

# WAS Web Application Report

A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/include/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/install/

| | | | |
|---|---|---|---|
| **Finding #** | 14848498 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | b82fe1d7-538c-417c-9ff6-cdb170ff17f3 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

# WAS Web Application Report

| CVSS V3 Base | 5.3 | CVSS V3 Temporal | 5 | CVSS V3 Attack Vector | |
|---|---|---|---|---|---|

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/install/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

# WAS Web Application Report

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/internet/

| | | | |
|---|---|---|---|
| **Finding #** | 14849402 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 0a11d208-d020-456c-b5c0-d531abf81e9f | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/internet/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;

# WAS Web Application Report

Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **New**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/java/

| | | | |
|---|---|---|---|
| **Finding #** | 15428014 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 66021569-d4d5-493f-9976-7d73bcce72d5 | | |
| **Group** | - | **First Time Detected** | 15 Jan 2022 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 1 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/java/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/js/

| | | | |
|---|---|---|---|
| **Finding #** | 14849404 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | c48307f6-78fb-4b66-84ed-eaa96214ae86 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

### Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

# WAS Web Application Report

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/js/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/jsp/

| | | | |
|---|---|---|---|
| **Finding #** | 14848418 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | c3f11099-bc66-42c0-aa34-9009f13dd924 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

# WAS Web Application Report

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/jsp/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/lib/

| | | | |
|---|---|---|---|
| **Finding #** | 14849440 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 2422f47f-ec10-4e7c-97a4-403d7a5dcac1 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |

# WAS Web Application Report

| | | | |
|---|---|---|---|
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/lib/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:

# WAS Web Application Report

Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* New

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/logs/

| | | | |
|---|---|---|---|
| **Finding #** | 15428008 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 24084a74-1067-4381-b442-ffd7f524efec | | |
| **Group** | - | **First Time Detected** | 15 Jan 2022 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 1 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/logs/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org

%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==;
PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==;
ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept:
*/*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* New

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/manager/

| | | | |
|---|---|---|---|
| **Finding #** | 15428010 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | aa43a13b-1b8b-43b1-8a5b-ae76b2e0bc17 | | |
| **Group** | - | **First Time Detected** | 15 Jan 2022 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION WASC-16 DIRECTORY INDEXING WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 1 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

### Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

# WAS Web Application Report

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/manager/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/service/

| | | | |
|---|---|---|---|
| **Finding #** | 14849442 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 63ca27ad-0d0f-467a-8d50-21e23c2ff2bc | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 |
| **CVSS V3 Attack Vector** | Network | | |

## Details

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

# WAS Web Application Report

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/service/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FPageID%3D4276; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289ab2a-9d2425fd36b8; Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/test.jsp

| | | | |
|---|---|---|---|
| **Finding #** | 14849432 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 538e3660-a10c-4182-8402-692be738dace | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

### Network

**Threat**
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

# WAS Web Application Report

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/test.jsp

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/test.php

| | | | |
|---|---|---|---|
| **Finding #** | 14849406 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 0dbacf4f-0c42-44c2-b1c7-dba30c84dfbc | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

# WAS Web Application Report

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/test.php

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

# WAS Web Application Report

## 150004 Path-Based Vulnerability

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/upload/

| | | | |
|---|---|---|---|
| **Finding #** | 14848528 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 64a0982a-085a-4f6d-9990-58cdf573b542 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat

A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact

The contents of this file or directory may disclose sensitive information.

### Solution

Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/upload/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;

# WAS Web Application Report

Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

### 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/ws/

| | | | |
|---|---|---|---|
| **Finding #** | 14849408 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 2a82b591-e5f8-4c9b-91ed-d38e139b6b01 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

### Impact
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

# WAS Web Application Report

https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/ws/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FPageID%3D4276; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289ab2a-9d2425fd36b8; Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150004 Path-Based Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Generator/TokenGenerator.ashx/wsdl/

| | | | |
|---|---|---|---|
| **Finding #** | 14848424 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 235a8906-76b1-403c-b458-26531aa3b23a | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-22 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A5 Broken Access Control | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION<br>WASC-16 DIRECTORY INDEXING<br>WASC-17 IMPROPER FILESYSTEM PERMISSIONS | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 5 | **CVSS V3 Attack Vector** | |

## Details

### Network

**Threat**
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

**Impact**
The contents of this file or directory may disclose sensitive information.

### Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/Page/2#calendar1/20220115/month

## Payloads

### #1 Request

GET https://www.parisssd.org/Generator/TokenGenerator.ashx/wsdl/

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FPageID%3D4276; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289ab2a-9d2425fd36b8; Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment:
Original URL is: https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest

HTTP/1.1 200 OK

## 150246 Path-relative stylesheet import (PRSSI) vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/1

| | | | |
|---|---|---|---|
| **Finding #** | 14849434 | **Severity** | Confirmed Vulnerability - Level 1 |
| **Unique # Group** | 39be7ea0-3a39-43aa-a933-24f108067d94<br>- | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-23 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | - | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 3.1 | **CVSS V3 Temporal** | 2.9 | **CVSS V3 Attack Vector** | Network |

## Details

### Threat

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to pathrelative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

### Impact
An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

### Solution
It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/
- Set response header X-Frame-Options: deny
- Set response header X-Content-Type-Options: nosniff.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/1

Referer: https://www.parisssd.org/
Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fdefault.aspx%3FPageID%3D1; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

Relative Path CSS Links found:
<link rel="Stylesheet" type="text/css" href="../Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd-theme-default.css">

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/1096?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848374 | **Severity** | Confirmed Vulnerability - Level 3 |

# WAS Web Application Report

| | | | |
|---|---|---|---|
| **Unique #** | eb126d6d-9607-4ff8-9bbe-8417dc8fc069 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 **CVSS V3 Temporal** 4.7 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/209

## Payloads

# WAS Web Application Report

## #1 Request

GET https://www.parisssd.org/Page/1096?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/1096

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/10?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848398 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | cdef4759-ed8a-424d-b8c9-d08c00a934b9 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=9

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/10?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/10

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

# WAS Web Application Report

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/Page/12?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848554 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | eb0b493c-9162-4c52-a979-a8a40106f67f | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 4.7 **CVSS V3 Attack Vector**

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/12?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/12

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/1737?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848452 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 6e60aefa-8bc2-449d-b29c-a780992fff5b | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.

- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/158

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/1737?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/1737

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150122 Cookie Does Not Contain The "secure" Attribute

https://www.parisssd.org New

**URL:** https://www.parisssd.org/Page/1940#sw-maincontent

| | | | |
|---|---|---|---|
| **Finding #** | 15428018 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | e889f641-4867-4792-a77d-1d940a42dd7a | | |
| **Group** | - | **First Time Detected** | 15 Jan 2022 03:01 GMT |
| **CWE** | CWE-614 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A3 Sensitive Data Exposure | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION | **Times Detected** | 1 |
| **CVSS V3 Base** | 4.3 | **CVSS V3 Temporal** | 4.1 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat
The cookie does not contain the "secure" attribute.

### Impact
Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

### Solution
If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

## Detection Information

**Cookie Name(s)** **_gat_BBTracker**

**Authentication** In order to detect this vulnerability, no authentication has been required.

**Access Path** Here is the path followed by the scanner to reach the exploitable URL:

https://www.parisssd.org/
https://www.parisssd.org/domain/268
https://www.parisssd.org/Page/1940

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/1940#sw-maincontent

Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

# WAS Web Application Report

## #1 Response

_gat_BBTracker=1; expires=Sat Jan 15 03:38:57 2022; path=/; domain=parisssd.org
Cookies set via JavaScript do not have an associated HTTP response header.

### 150123 Cookie Does Not Contain The "HTTPOnly" Attribute

*https://www.parisssd.org* **New**

**URL:** https://www.parisssd.org/Page/1940#sw-maincontent

| | | | |
|---|---|---|---|
| **Finding #** | 15428016 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 17e31f8d-5119-4e89-bcdd-8b13e0464476 | | |
| **Group** | - | **First Time Detected** | 15 Jan 2022 03:01 GMT |
| **CWE** | CWE-1004 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A3 Sensitive Data Exposure | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION | **Times Detected** | 1 |

**CVSS V3 Base** 4.3 **CVSS V3 Temporal** 4.1 **CVSS V3 Attack Vector**

## Details

Network

### Threat
The cookie does not contain the "HTTPOnly" attribute.

### Impact
Cookies without the "HTTPOnly" attribute are permitted to be accessed via JavaScript. Cross-site scripting attacks can steal cookies which could lead to user impersonation or compromise of the application account.

### Solution
If the associated risk of a compromised account is high, apply the "HTTPOnly" attribute to cookies.

## Detection Information

**Cookie Name(s)** **_gat_BBTracker**

**Authentication** In order to detect this vulnerability, no authentication has been required.

**Access Path** Here is the path followed by the scanner to reach the exploitable URL:

https://www.parisssd.org/
https://www.parisssd.org/domain/268
https://www.parisssd.org/Page/1940

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/1940#sw-maincontent

Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

# WAS Web Application Report

## #1 Response

_gat_BBTracker=1; expires=Sat Jan 15 03:38:57 2022; path=/; domain=parisssd.org
Cookies set via JavaScript do not have an associated HTTP response header.

### 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/2162?"%26gt;%26lt;script%26gt;_q_q='){'%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848526 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 438af0e0-c68f-41d9-bd5c-14739091862d | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 4.7 **CVSS V3 Attack Vector**

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/235

## Payloads

# WAS Web Application Report

## #1 Request

GET https://www.parisssd.org/Page/2162?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/2162

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/2510?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848360 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 27b41e11-e10c-4162-bcf6-f1a4df19770d | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 4.7 **CVSS V3 Attack Vector**

Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/276

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/2510?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/2510

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

# WAS Web Application Report

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/2587?"%26gt;%26lt;script%26gt;_q_q='('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848346 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 7324ef7d-7f0c-47ac-8d76-6f6a07187c34 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 4.7 **CVSS V3 Attack Vector**

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/276

## Payloads

**#1 Request**

GET https://www.parisssd.org/Page/2587?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/2587

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/2751?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848558 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 63dcab62-cacd-4cf7-b4ed-a735c9857e5a | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/235

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/2751?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/2751

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

# WAS Web Application Report

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/Page/2963?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848422 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 12dca0fe-b0d8-489c-bb9d-6f11050467df | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 4.7 **CVSS V3 Attack Vector**

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/240

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/2963?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/2963

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **New**

**URL:** https://www.parisssd.org/Page/318?"%26gt;%26lt;script%26gt;_q_q='('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 15428002 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 52fe7438-4623-4451-a8f1-5d8e317d4c72 | | |
| **Group** | - | **First Time Detected** | 15 Jan 2022 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 1 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.

- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11
https://www.parisssd.org/domain/96

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/318?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/318

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **New**

**URL:** https://www.parisssd.org/Page/319?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 15428004 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 8d4929b7-5e55-43f4-8a46-6a7886cbc6d7 | | |
| **Group** | - | **First Time Detected** | 15 Jan 2022 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 1 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11
https://www.parisssd.org/domain/96

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/319?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/319

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **New**

**URL:** https://www.parisssd.org/Page/320?"%26gt;%26lt;script%26gt;_q_q='('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 15428006 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 382d803c-a86a-4a42-aff3-ea89828c6708 | | |
| **Group** | - | **First Time Detected** | 15 Jan 2022 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 1 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.

- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11
https://www.parisssd.org/domain/96

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/320?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/320

```
hite-space: pre-wrap; word-wrap: break-word; }
}
 @media screen and (max-width: 479px) {
 pre { width: 280px; }
 }
 </style>
</head>

 <body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

 <h2> <i>Runtime Error</i> </h2></span>

 <font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 <b> Description: </b>An exception o
```

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/Page/3860?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848504 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 6e26fc13-b6f6-4111-8113-7e9ce5863f02 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/276

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/3860?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/

Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/3860

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/3929?"%26gt;%26lt;script%26gt;_q_q='('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848518 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 9ab2d105-3972-4862-b804-c14b504da52e | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.

- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/362

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/3929?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/3929

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/Page/3932?"%26gt;%26lt;script%26gt;_q_q='('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848356 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 00a5db6b-908a-49f5-9461-ba70e12c6720 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/362

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/3932?"><script>_q_q='('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

# WAS Web Application Report

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/3932

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/3936?"%26gt;%26lt;script%26gt;_q_q='){'%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848564 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | dc81fbb2-04f0-455a-a074-bf8637e87c40 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/362

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/3936?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/3936

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/Page/4648?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848388 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 722338b4-f228-422f-8dbd-2da687eff318 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 **CVSS V3 Temporal** 4.7 | **CVSS V3 Attack Vector** | |

## Details

### Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/363

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/4648?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/4648

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/4706?"%26gt;%26lt;script%26gt;_q_q='){'%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848428 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | b7eed7e3-b6b7-4087-af33-00d6aaae875e | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/337

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/4706?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/4706

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/Page/4715?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848368 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 0d448bf0-904e-45b9-a048-8c0cc170fc6b | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 **CVSS V3 Temporal** 4.7 | **CVSS V3 Attack Vector** | |

Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/400

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/4715?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/4715

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/4738?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848510 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 6dec346b-898b-4b57-824d-513782e380d4 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/400

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/4738?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/4738

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/4745?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848420 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 4288244e-d9fa-43c1-bd3b-cf0bc743db80 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/400

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/4745?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/4745

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/4769?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848472 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | f016459d-26cc-4aee-a21b-fd99e15a7048 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/401

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/4769?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/4769

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/Page/5348?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848482 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 078c963d-a6e4-496c-b9ce-100e04c065a0 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/413

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/5348?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/5348

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/5350?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848410 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 478faaca-e1ea-47e8-ab25-d7fd8e0d9950 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/413

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/5350?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/5350

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/758?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848358 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 335868ec-ba62-4c12-b696-840bc49e394e | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/157

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/758?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/758

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/Page/760?"%26gt;%26lt;script%26gt;_q_q='('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848540 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 9232e0e4-8109-44d6-9aa6-f5232ebefb68 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/domain/159

## Payloads

### #1 Request

GET https://www.parisssd.org/Page/760?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/Page/760

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150051 Open Redirect

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/SignInSecure.aspx?SecurePage=https://www.qualys.com?SecurePage=https://www.parisssd.org/SignIn.aspx

| | | | |
|---|---|---|---|
| **Finding #** | 14849448 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | faa5cee2-cafb-4384-915c-d0c5039960c5 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-601 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-38 URL REDIRECTOR ABUSE | **Times Detected** | 2 |
| **CVSS V3 Base** | 6.5 | **CVSS V3 Temporal** | 6.5 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

The web application creates a redirect based on a parameter from a querystring or form field. The redirect destination can be changed by modifying the parameter's value. Redirects are used to automatically force the web browser to request a resource from a new destination. An open redirect occurs when the redirect destination may be any host unrelated to the original web application.

### Impact

Open redirects or otherwise unvalidated redirects are often used as part of a social engineering or phishing attack because the initial malicious link sent to a victim can use a trusted, legitimate web site's URL to redirect to a link on a malicious web server.

### Solution

Verify that the redirect behavior is acceptable according to your application's security or privacy policy. This determines whether redirecting to a host unrelated to the web application is permissible. Consider moving redirect logic to server-side code that verifies the redirect destination is allowed.

## Detection Information

**Parameter** It has been detected by exploiting the parameter **SecurePage**
The payloads section will display a list of tests that show how the param could have been exploited to collect the information

**Authentication** In order to detect this vulnerability, no authentication has been required.

**Access Path** Here is the path followed by the scanner to reach the exploitable URL:

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=4&IgnoreRedirect=true
https://www.parisssd.org/myview/

## Payloads

### #1 Request

GET https://www.parisssd.org/SignInSecure.aspx?SecurePage=https://www.qualys.com?Sec urePage=https://www.parisssd.org/SignIn.aspx

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

Open redirection detected by changing parameter "SecurePage" in request's query/body.

## 150123 Cookie Does Not Contain The "HTTPOnly" Attribute

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/cms/module/selectsurvey/TakeSurvey.aspx?SurveyID=108

| | | | |
|---|---|---|---|
| **Finding #** | 14848514 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | 21b59181-fdfe-4e9a-abdc-09f43004bbad | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-1004 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A3 Sensitive Data Exposure | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION | **Times Detected** | 2 |

**CVSS V3 Base** 4.3 **CVSS V3 Temporal** 4.1 **CVSS V3 Attack Vector**

## Details

Network

### Threat

The cookie does not contain the "HTTPOnly" attribute.

### Impact

Cookies without the "HTTPOnly" attribute are permitted to be accessed via JavaScript. Cross-site scripting attacks can steal cookies which could lead to user impersonation or compromise of the application account.

### Solution

If the associated risk of a compromised account is high, apply the "HTTPOnly" attribute to cookies.

## Detection Information

**Cookie Name(s)** **SelectSurveyASPAnonymousUserID**

**Authentication** In order to detect this vulnerability, no authentication has been required.

**Access Path** Here is the path followed by the scanner to reach the exploitable URL:

https://www.parisssd.org/
https://www.parisssd.org/domain/299

## Payloads

### #1 Request

GET https://www.parisssd.org/cms/module/selectsurvey/TakeSurvey.aspx?SurveyID=108

Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

```
SelectSurveyASPAnonymousUserID=
200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 48756
Connection: keep-alive
Date: Sat, 15 Jan 2022 03:34:14 GMT
Cache-Control: private
Pragma: No-Cache
Expires: Sat, 15 Jan 2022 03:34:13 GMT
Server: Microsoft-IIS/8.5
Strict-Transport-Security: max-age=31536000; includeSubDomains;
X-XSS-Protection: 1; mode=block
X-AspNet-Version: 4.0.30319
Set-Cookie: ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; path=/; secure; HttpOnly; SameSite=Lax
SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; expires=Sat, 05-Feb-2022 03:34:13 GMT; path=/; secure X-Powered-
By: ASP.NET
Content-Security-Policy: frame-ancestors 'self' https://*.ally.ac;
X-Frame-Options: SAMEORIGIN
X-Cache: Miss from cloudfront
Via: 1.1 b014854bd0108b7ed0058504b69ccb5a.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: SFO53-C1
X-Amz-Cf-Id: mVY4rHtDm4jv_GRazR40NmDUVIBbztPJ_t6bSn2X1jzOwFUP13etEg==
```

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150246 Path-relative stylesheet import (PRSSI) vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/11

| | | | |
|---|---|---|---|
| **Finding #** | 14849444 | **Severity** | Confirmed Vulnerability - Level 1 |
| **Unique #** | 42f92809-7f14-45ae-b82f-274f724ad8c1 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-23 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | - | **Times Detected** | 2 |
| **CVSS V3 Base** | 3.1 | **CVSS V3 Temporal** 2.9 | **CVSS V3 Attack Vector** Network |

### Details

**Threat**

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to pathrelative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

**Impact**

An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

### Solution

It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/
- Set response header X-Frame-Options: deny
- Set response header X-Content-Type-Options: nosniff.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/11

Referer: https://www.parisssd.org/
Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FPageID%3D1; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

Relative Path CSS Links found:
<link rel="Stylesheet" type="text/css" href="../Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd-theme-default.css">

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/110?"%26gt;%26lt;script%26gt;_q_q=')("%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848480 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | f82a243b-cc2b-4120-a932-f613ff1fb8ff | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=9

## Payloads

# WAS Web Application Report

## #1 Request

GET https://www.parisssd.org/domain/110?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/110

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/112?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848342 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 7c49b683-433e-4047-90e9-e664e70b4550 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=9

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/112?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/112

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

# WAS Web Application Report

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/131?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848436 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | d333017d-ad00-48ad-ba4d-6feaf27d8892 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=9

## Payloads

**#1 Request**

GET https://www.parisssd.org/domain/131?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/131

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/138?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848378 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 74fa5f4e-645a-4863-ae56-2b23d610b634 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=9

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/138?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/138

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

# WAS Web Application Report

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

150246 Path-relative stylesheet import (PRSSI) vulnerability

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/156

| | | | |
|---|---|---|---|
| **Finding #** | 14849470 | **Severity** | Confirmed Vulnerability - Level 1 |
| **Unique #** | cc6dba47-20f2-4646-8fdd-86e6d56047a2 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-23 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | - | **Times Detected** | 2 |

**CVSS V3 Base** 3.1 **CVSS V3 Temporal** 2.9 **CVSS V3 Attack Vector** Network

## Details

### Threat

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to pathrelative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

### Impact

An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

### Solution

It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/
- Set response header X-Frame-Options: deny
- Set response header X-Content-Type-Options: nosniff.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

# WAS Web Application Report

## #1 Request

GET https://www.parisssd.org/domain/156

Referer: https://www.parisssd.org/
Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FPageID%3D1; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

Relative Path CSS Links found:
<link rel="Stylesheet" type="text/css" href="../Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd-theme-default.css">

### 150246 Path-relative stylesheet import (PRSSI) vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/157

| | | | |
|---|---|---|---|
| **Finding #** | 14849464 | **Severity** | Confirmed Vulnerability - Level 1 |
| **Unique # Group** | 57c51efb-e069-4912-8a68-d9c932d63e9f<br>- | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-23 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | - | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 3.1 | **CVSS V3 Temporal** | 2.9 | **CVSS V3 Attack Vector** | Network |

### Details

**Threat**

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to pathrelative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

**Impact**

An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

**Solution**

It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/
- Set response header X-Frame-Options: deny

- Set response header X-Content-Type-Options: nosniff.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/157

Referer: https://www.parisssd.org/
Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FDomainID%3D268; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

Relative Path CSS Links found:
<link rel="Stylesheet" type="text/css" href="../Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd-theme-default.css">

150022 Server Error Message — *https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/157?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848392 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 4d63e3a0-34ba-45f0-92c8-3a682c489983 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/157?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/157

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

# WAS Web Application Report

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

150246 Path-relative stylesheet import (PRSSI) vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/158

| | | | |
|---|---|---|---|
| **Finding #** | 14849472 | **Severity** | Confirmed Vulnerability - Level 1 |
| **Unique #** | 8db87fa8-c094-463d-8ef9-2153f905c52d | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-23 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | - | **Times Detected** | 2 |
| **CVSS V3 Base** | 3.1 | **CVSS V3 Temporal** | 2.9 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to pathrelative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

### Impact

An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

### Solution

It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/
- Set response header X-Frame-Options: deny
- Set response header X-Content-Type-Options: nosniff.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/158

Referer: https://www.parisssd.org/
Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FDomainID%3D268; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

Relative Path CSS Links found:
<link rel="Stylesheet" type="text/css" href="../Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd-theme-default.css">
Please check there may be more pages with relative path CSS links.

## 150246 Path-relative stylesheet import (PRSSI) vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/159

| | | | |
|---|---|---|---|
| **Finding #** | 14849456 | **Severity** | Confirmed Vulnerability - Level 1 |
| **Unique # Group** | bb06b3c5-f99a-476d-9611-28e71e35c525<br>- | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-23 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | - | **Times Detected** | 2 |
| **CVSS V3 Base** | 3.1 | **CVSS V3 Temporal** | 2.9 |
| **CVSS V3 Attack Vector** | Network | | |

## Details

### Threat

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to pathrelative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

### Impact

An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

### Solution

It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/
- Set response header X-Frame-Options: deny
- Set response header X-Content-Type-Options: nosniff.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/159

Referer: https://www.parisssd.org/
Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FDomainID%3D268; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

Relative Path CSS Links found:
<link rel="Stylesheet" type="text/css" href="../Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd-theme-default.css">

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/161?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848560 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 476b36fd-d6c1-4c23-8766-784d7de626c2 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

# WAS Web Application Report

### Threat
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/161?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/161

```
hite-space: pre-wrap; word-wrap: break-word; }
}
 @media screen and (max-width: 479px) {
 pre { width: 280px; }
 }
 </style>
</head>

 <body bgcolor="white">

 <span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>
```

# WAS Web Application Report

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150146 Passive Mixed Content Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/171

| | | | |
|---|---|---|---|
| **Finding #** | 14849426 | **Severity** | Confirmed Vulnerability - Level 1 |
| **Unique #** | 2e0c9818-e5bb-415c-9bd6-a4e91a39b02e | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-319 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A3 Sensitive Data Exposure | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION | **Times Detected** | 2 |

**CVSS V3 Base** 3.1 **CVSS V3 Temporal** 3 **CVSS V3 Attack Vector**

## Details

Network

### Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

### Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

### Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/171

# WAS Web Application Report

Referer: https://www.parisssd.org/
Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FDomainID%3D178; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

The page at https://www.parisssd.org/domain/171 was loaded over HTTPS, but following requested an insecure resource.
Image http://t1.gstatic.com/images?q=tbn:ANd9GcRaFfO-rao8Y1yW8Uiz_ShinTYBnQefOrIbf321I3G_qEbrL0OY4Q:content.mycutegraphics.com/graphics/reading/kids-reading.png

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/184?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848500 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 5731944f-4cf6-4f3f-94ad-d8a79b4ffe73 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

Detection Information

**Parameter** No param has been required for detecting the information.

| | |
|---|---|
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

# WAS Web Application Report

## #1 Request

GET https://www.parisssd.org/domain/184?"><script>_q_q='('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/184

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/194?"%26gt;%26lt;script%26gt;_q_q='('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848470 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | bf4c836e-d5cc-4dbc-a47d-18c66c8bd5b8 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/194?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/194

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

# WAS Web Application Report

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/196?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848448 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 69fcf476-0491-4a15-81ee-01f15ef3889e | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/196?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/196

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/203?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848512 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | dbb677b6-2cfd-4e16-be79-1f1b06ee7954 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.

- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/203?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/203

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150146 Passive Mixed Content Vulnerability

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/204

| | | | |
|---|---|---|---|
| **Finding #** | 14849370 | **Severity** | Confirmed Vulnerability - Level 1 |
| **Unique #** | 199affc9-512b-4dfa-af20-e81d903f9c1a | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-319 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A3 Sensitive Data Exposure | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION | **Times Detected** | 2 |
| **CVSS V3 Base** | 3.1 | **CVSS V3 Temporal** | 3 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

### Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

### Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=9

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/204

Referer: https://www.parisssd.org/
Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FDomainID%3D210; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

The page at https://www.parisssd.org/domain/204 was loaded over HTTPS, but following requested an insecure resource.
Image
http://www.warrencountyschools.org/userfiles/3125/LoveMyFirstGrade%255B1%255D.jpg

### 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/211?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848402 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 735a926e-1ee4-4707-9094-ea5ad90880ed | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=9

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/211?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/211

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/215?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848382 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 1ced8f27-8992-4d3f-a537-0c4100ad28ae | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

**Threat**

# WAS Web Application Report

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/215?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/215

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

# WAS Web Application Report

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/216?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848400 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 25978e85-b7ea-490a-80e1-c892a34b89a6 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 4.7 **CVSS V3 Attack Vector**

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/216?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/216

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150145 Active Mixed Content Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/227

| | | | |
|---|---|---|---|
| **Finding #** | 14849412 | **Severity** | Confirmed Vulnerability - Level 2 |
| **Unique #** | c2c55a79-b7a5-4158-b116-d872a4edeaf7 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-319 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A3 Sensitive Data Exposure | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 3.1 | **CVSS V3 Temporal** | 3 | **CVSS V3 Attack Vector** | |

Details

Network

**Threat**

# WAS Web Application Report

An active mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Active mixed content with reference to Mozilla Firefox browser behavior. Active mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. script, link, iframe, XMLHttpRequest requests, object, applet

### Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

### Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/227

Referer: https://www.parisssd.org/
Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FDomainID%3D281; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

The page at https://www.parisssd.org/domain/227 was loaded over HTTPS, but following requested an insecure resource.
Script
http://toolbar.avg.com/si.js?p=HxBY1OKREiFBP0edC0DcqhXUKEW00xo1vyzoHrCcFpLDpc8dWAHeQiZAuy1r0TKdepNA93irYkSpKZaTp4%2BUfXuzg%2FDqT4xjlmn1683UtRMLWqoMPm%2Bul59grAA7JSj3sSN2JnYPJPcVsgwjCjomgdZy921pqfT1Afz%2BtQjwFXV%2BjKQHOmDQYNW9eMidF3BwEq06Kd8xW2gKSfytijnbwrsifVZJNIogK6TIiCEGmwA%3D

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/235?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848450 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 4151f321-89ce-40f2-83d3-c6f9d10af910 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

# WAS Web Application Report

| CVSS V3 Base | 5.3 | CVSS V3 Temporal | 4.7 | CVSS V3 Attack Vector | |
|---|---|---|---|---|---|

## Details

Network

### Threat
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/235?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500

# WAS Web Application Report

Original URL is: https://www.parisssd.org/domain/235

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/248?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848534 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | da6210dd-e2e5-4d04-bcfb-4641731dfc4b | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 4.7 **CVSS V3 Attack Vector**

Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=9

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/248?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/248

```
hite-space: pre-wrap; word-wrap: break-word; }
}
 @media screen and (max-width: 479px) {
 pre { width: 280px; }
 }
 </style>
</head>

 <body bgcolor="white">

 <span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

 <h2> <i>Runtime Error</i> </h2></span>

 <font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 <b> Description: </b>An exception o
```

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/249?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848334 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 84ab55ed-8851-40bc-8724-3dccd24ad781 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 4.7 **CVSS V3 Attack Vector**

# WAS Web Application Report

Details

Network

## Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

## Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

## Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/249?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/249

# WAS Web Application Report


hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o


* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/256?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848426 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 5ede90a6-59c1-4879-9328-de556e59996f | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

**Parameter** No param has been required for detecting the information.

# WAS Web Application Report

| | |
|---|---|
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/256?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/256

```
hite-space: pre-wrap; word-wrap: break-word; }
}
 @media screen and (max-width: 479px) {
 pre { width: 280px; }
 }
 </style>
</head>

 <body bgcolor="white">

 <span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

 <h2> <i>Runtime Error</i> </h2></span>

 <font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 <b> Description: </b>An exception o
```

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/263?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848380 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | dc98f195-5f13-42a6-b59d-047ce61ce2be | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

# WAS Web Application Report

Network

## Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

## Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

## Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/263?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/263

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {

# WAS Web Application Report

```
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>Runtime Error</i> </h2></span>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

<b> Description: </b>An exception o
```

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/265?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848348 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 5af6767a-aa85-4d14-b1a5-d5839a9bf6f3 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | Network | | |

## Details

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

# WAS Web Application Report

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/265?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/265

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150246 Path-relative stylesheet import (PRSSI) vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/268

| | | | |
|---|---|---|---|
| **Finding #** | 14849480 | **Severity** | Confirmed Vulnerability - Level 1 |
| **Unique #** | 808ed9fb-1960-4401-86e5-32d9860f1327 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-23 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | - | **Times Detected** | 2 |

**CVSS V3 Base** 3.1 **CVSS V3 Temporal** 2.9 **CVSS V3 Attack Vector** Network

# WAS Web Application Report

## Details

### Threat

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to pathrelative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

### Impact

An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

### Solution

It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/
- Set response header X-Frame-Options: deny
- Set response header X-Content-Type-Options: nosniff.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/268

Referer: https://www.parisssd.org/
Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FPageID%3D1; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

Relative Path CSS Links found:
<link rel="Stylesheet" type="text/css" href="../Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd-theme-default.css">

# WAS Web Application Report

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/268?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848516 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 7130412c-3baf-4f57-b620-1f753e6fa677 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

# WAS Web Application Report

## #1 Request

GET https://www.parisssd.org/domain/268?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/268

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/271?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848456 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 95f26ec8-334e-4102-b733-ea8eed52cfe8 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/271?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/271

```
hite-space: pre-wrap; word-wrap: break-word; }
}
 @media screen and (max-width: 479px) {
 pre { width: 280px; }
 }
 </style>
</head>

 <body bgcolor="white">

 <span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

 <h2> <i>Runtime Error</i> </h2></span>
```

# WAS Web Application Report

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/276?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848370 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | ce273af0-fdd7-45d1-bb68-9f7045a0ef6a | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/276?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/276

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/281?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848524 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 66ebb910-3dac-42df-bd70-f71a14e6108c | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.

- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/281?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/281

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/284?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848532 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 876212c6-d5b8-4047-95d8-5caddce55c6a | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/284?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

# WAS Web Application Report

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/284

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/285?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848486 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | cf9e2ac0-1be8-43d3-b9cf-b09453296965 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/285?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/285

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/299?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848354 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 735192b8-3bd8-43bd-ac78-492522f12d4e | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 **CVSS V3 Temporal** 4.7 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/299?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/299

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/305?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848438 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 23612499-429a-4b13-bef1-75d11f49ff05 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/305?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/305

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/310?"%26gt;%26lt;script%26gt;_q_q='('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848478 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 404ee886-e190-4fc8-9082-93f5da848749 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=9

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/310?"><script>_q_q='('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/310

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/327?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848492 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 171d86f1-5ef9-4f23-9173-59bcd5e8bb44 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/327?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/327

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/339?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848550 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 35ae5426-7999-4070-b1e0-a62b07956ea1 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 **CVSS V3 Temporal** 4.7 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=9

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/339?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/339

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/342?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848460 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 885e58cd-fa0d-4768-89f4-4d8cb17cf702 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=9

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/342?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/342

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/344?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848386 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 6537e4e3-a153-4b2f-8892-9cd0ad6169c5 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 **CVSS V3 Temporal** 4.7 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/344?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

# WAS Web Application Report

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/344

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/348?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848546 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | b5088c59-a937-4d9b-8b8f-8c084392084d | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/348?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/348

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/366?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848442 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 59979d07-9c52-4d19-bb19-e70c7a38d157 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/366?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/366

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/370?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848406 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 63adf236-cd33-42af-bb78-a1aaf02294fd | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=9

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/370?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/370

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/371?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848508 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | e6346463-38e1-4f7e-86f1-caa0c97fb56a | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 **CVSS V3 Temporal** 4.7 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/371?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

# WAS Web Application Report

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/371

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/376?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848496 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | a6006363-8f02-4743-9a7a-da78e95bc84e | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/376?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/376

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/379?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848384 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | a178c5ae-88e1-48f9-b74c-e2cb2f1f710d | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 **CVSS V3 Temporal** 4.7 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/379?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

# WAS Web Application Report

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/379

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/381?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848548 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | c2aeaef9-d774-45ba-a480-e192f8e15132 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 **CVSS V3 Temporal** 4.7 | **CVSS V3 Attack Vector** | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/381?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/381

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/382?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848416 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 4ff11ed5-bb43-4e5c-9b96-2850ff9edbbe | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 **CVSS V3 Temporal** 4.7 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/382?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/382

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/384?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848338 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | d08d5b74-5834-4d55-93e6-4f7decfe4ea5 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/384?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/384

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/386?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848434 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 5f84d736-dcca-44fc-afa9-87d82f9b6a3c | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/386?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

# WAS Web Application Report

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/386

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/387?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848536 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | aa3e84a6-00c6-49df-92ae-1620d7e86f81 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/387?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/387

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/388?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848332 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 4ee22c7d-c77e-49ae-8662-fb4813afafec | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 **CVSS V3 Temporal** 4.7 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=9

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/388?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/388

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/393?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848538 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 49dd0c34-d1e5-411c-9ca7-cb769a4aa795 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/393?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/393

```
hite-space: pre-wrap; word-wrap: break-word; }
}
 @media screen and (max-width: 479px) {
 pre { width: 280px; }
 }
 </style>
</head>

 <body bgcolor="white">

 <span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

 <h2> <i>Runtime Error</i> </h2></span>

 <font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 <b> Description: </b>An exception o
```

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/394?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848476 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 6e822733-a9c0-4e8b-b33c-87240d2348da | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 **CVSS V3 Temporal** 4.7 | **CVSS V3 Attack Vector** | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/394?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/394

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/399?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848372 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 2c93910d-6a2d-4b2d-a238-ea401b492e42 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/399?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/399

```
hite-space: pre-wrap; word-wrap: break-word; }
}
 @media screen and (max-width: 479px) {
 pre { width: 280px; }
 }
 </style>
</head>

 <body bgcolor="white">

 <span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

 <h2> <i>Runtime Error</i> </h2></span>

 <font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 <b> Description: </b>An exception o
```

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/401?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848432 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 623c86f7-4409-4e4f-832e-6562046d888a | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/401?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/401

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150146 Passive Mixed Content Vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/404

| | | | |
|---|---|---|---|
| **Finding #** | 14849398 | **Severity** | Confirmed Vulnerability - Level 1 |
| **Unique #** | c4afae15-d9a9-413e-967e-0bff32949015 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-319 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A3 Sensitive Data Exposure | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION | **Times Detected** | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **CVSS V3 Base** | 3.1 | **CVSS V3 Temporal** | 3 | **CVSS V3 Attack Vector** | |

Details

Network

### Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

### Impact
The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

### Solution
The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/404

Referer: https://www.parisssd.org/
Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FDomainID%3D372; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

The page at https://www.parisssd.org/domain/404 was loaded over HTTPS, but following requested an insecure resource.
Image http://www.steelworks.us/wp-content/uploads/2019/04/science-clip-art-graphic-1.jpg

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/413?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848440 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 864fc96e-9df4-46bc-9fe5-c19f1a9dcdd2 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

# WAS Web Application Report

### Threat
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/413?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/413

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

# WAS Web Application Report

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/420?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848556 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 0949e1cb-1161-48fb-8f8d-691ab8583ac2 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 4.7 **CVSS V3 Attack Vector**

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=9

## Payloads

**#1 Request**

GET https://www.parisssd.org/domain/420?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/420

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/424?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848366 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | a00b2547-0557-4712-a1c5-72f0dddc6e68 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | Network | | |

## Details

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/424?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/424

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

# WAS Web Application Report

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/427?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848396 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 2ae558e3-5ca5-48ce-8a4c-6e32d55bc52f | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 4.7 **CVSS V3 Attack Vector**

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/427?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/427

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/430?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848446 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 1c5111bd-171f-4359-80ee-ffca2d2abd60 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.

- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/430?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/430

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/431?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848474 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | df386679-25ab-41d1-a886-df305fa11444 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/431?"><script>_q_q='(</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/431

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/433?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848488 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 284e80c8-7e2b-49e1-906e-74ee8deeb619 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/433?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/433

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/55?"%26gt;%26lt;script%26gt;_q_q='')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848350 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 1039b7f6-5307-432b-94af-4151c83d308e | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/55?"><script>_q_q='')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788;

# WAS Web Application Report

SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org %2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/55

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/56?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848408 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | adbe4edc-1116-4ea1-9c9d-50a56035e0c5 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/56?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/56

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

# WAS Web Application Report

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150146 Passive Mixed Content Vulnerability

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/60

| | | | |
|---|---|---|---|
| **Finding #** | 14849416 | **Severity** | Confirmed Vulnerability - Level 1 |
| **Unique #** | 8b14aa1a-9e37-4b3e-b3d1-beccd3a4a9e1 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-319 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A3 Sensitive Data Exposure | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION | **Times Detected** | 2 |
| **CVSS V3 Base** | 3.1 | **CVSS V3 Temporal** | 3 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

### Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

### Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/60

Referer: https://www.parisssd.org/
Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FDomainID%3D384; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

The page at https://www.parisssd.org/domain/60 was loaded over HTTPS, but following requested an insecure resource.
Image http://blog.writeathome.com/wp-content/uploads/2012/09/dog-reading.jpg

### 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/62?"%26gt;%26lt;script%26gt;_q_q='(%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848520 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 6530b5b6-d45c-4760-ae43-b58865764e06 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/62?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/62

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/68?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848412 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | a261ae51-37b1-44ce-8b85-422cb3849fad | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

**Threat**

# WAS Web Application Report

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/68?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/68

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

# WAS Web Application Report

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/domain/75?"%26gt;%26lt;script%26gt; q q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848454 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | c4743984-425f-4f5d-a0e7-da68d3e19b58 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |

**CVSS V3 Base** 5.3 **CVSS V3 Temporal** 4.7 **CVSS V3 Attack Vector**

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

# WAS Web Application Report

## #1 Request

GET https://www.parisssd.org/domain/75?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/75

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/93?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848362 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 865000c3-bd18-4467-99e4-ec8b3d09d34b | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022
- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact
Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution
Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/93?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/93

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

# WAS Web Application Report

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/domain/96?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848494 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | f2933468-af54-43e8-b53f-6e7d10ea7456 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

## Details

Network

### Threat

This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/domain/96?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/domain/96

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150022 Server Error Message

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/mcleese?"%26gt;%26lt;script%26gt;_q_q=')('%26lt;/script%26gt;

| | | | |
|---|---|---|---|
| **Finding #** | 14848562 | **Severity** | Confirmed Vulnerability - Level 3 |
| **Unique #** | 43e5ef7e-553a-4e01-be71-b64e44b124b8 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-209 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | **Times Detected** | 2 |
| **CVSS V3 Base** | 5.3 | **CVSS V3 Temporal** | 4.7 |
| **CVSS V3 Attack Vector** | | | |

Details

Network

**Threat**
This finding will be reported when run time errors, verbose server errors, and potential stack trace are detected

The following are two examples of 150022

- WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads, in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding.
- Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.

### Impact

Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure, allowing them to target it more effectively.

### Solution

Implement strong error and exception handling to ensure that the web application displays only generic error messages. Avoid returning stack traces, debugging information, or other technical details to the client side. The application should also implement rigorous input data validation. Restrict user-supplied data to consist of a minimal set of characters necessary for the input field and validate the data to ensure it conforms to the expected format.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=13

## Payloads

### #1 Request

GET https://www.parisssd.org/mcleese?"><script>_q_q=')('</script>

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3Fpagetype%3D15%26SiteID%3Dhttps%3A%2F%2Fwww.qualys.com%3FSiteID%3D; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Response status: 500
Original URL is: https://www.parisssd.org/mcleese

hite-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> Runtime Error </h2>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

# WAS Web Application Report

 Description: An exception o

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150146 Passive Mixed Content Vulnerability

https://www.parisssd.org **Active**

**URL:** https://www.parisssd.org/site/Default.aspx?PageID=1120

| | | | |
|---|---|---|---|
| **Finding #** | 14849394 | **Severity** | Confirmed Vulnerability - Level 1 |
| **Unique #** | 569456f4-950f-4e58-8916-a1fc3a6a8974 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-319 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A3 Sensitive Data Exposure | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION | **Times Detected** | 2 |

**CVSS V3 Base** 3.1 **CVSS V3 Temporal** 3 **CVSS V3 Attack Vector**

## Details

Network

### Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

### Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

### Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=9

## Payloads

### #1 Request

GET https://www.parisssd.org/site/Default.aspx?PageID=1120

Referer: https://www.parisssd.org/
Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FDomainID%3D138; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==;

# WAS Web Application Report

APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

## #1 Response

The page at https://www.parisssd.org/site/Default.aspx?PageID=1120 was loaded over HTTPS, but following requested an insecure resource.
Image
http://www.roomrecess.com/Pictures/SSDoubleClick.png
http://www.roomrecess.com/Pictures/SSSpiderSwatter.png
http://www.roomrecess.com/Pictures/mobilePics/SSMeegleMath.png
http://www.storylineonline.net/wp-content/themes/storylineonline/assets/images/logo.png

## 150246 Path-relative stylesheet import (PRSSI) vulnerability

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/site/Default.aspx?PageType=7%26SiteID=4%26IgnoreRedirect=true

| | | | |
|---|---|---|---|
| **Finding #** | 14849424 | **Severity** | Confirmed Vulnerability - Level 1 |
| **Unique # Group** | 655f9d24-3d5d-4a3d-83c7-262ca19b7313<br>- | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-23 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | - | **Times Detected** | 2 |
| **CVSS V3 Base** | 3.1 | **CVSS V3 Temporal** | 2.9 |
| **CVSS V3 Attack Vector** | Network | | |

## Details

### Threat

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to pathrelative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

### Impact

An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

### Solution

It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/
- Set response header X-Frame-Options: deny
- Set response header X-Content-Type-Options: nosniff.

# WAS Web Application Report

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/

## Payloads

### #1 Request

GET https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=4&IgnoreRed irect=true

Referer: https://www.parisssd.org/
Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fdefault.aspx%3FPageID%3D1; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8;
Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

Relative Path CSS Links found:
<link rel="Stylesheet" type="text/css" href="../Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd-theme-default.css">

## 150084 Unencoded characters

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/site/UserControls/TermsOfUse/TermsOfUse.aspx?RedirectPath=%3C%0a%0dscript%20a%3D4%3EqssfU7sHk7K%3D7%3C%0a%0d%2Fscript%3E%26IgnoreRedirect=true

| | | | |
|---|---|---|---|
| **Finding #** | 14848542 | **Severity** | Potential Vulnerability - Level 1 |
| **Unique #** | e5b37022-9d9a-41ec-9224-bf971128a354 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-79 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A7 Cross-Site Scripting (XSS) | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-22 IMPROPER OUTPUT HANDLING | **Times Detected** | 2 |
| **CVSS V3 Base** | - | **CVSS V3 Temporal** - | **CVSS V3 Attack Vector** |

## Details

-

### Threat

The web application reflects potentially dangerous characters such as single quotes, double quotes, and angle brackets. These characters are commonly used for HTML injection attacks such as cross-site scripting (XSS).

### Impact

No exploit was determined for these reflected characters. The input parameter should be manually analyzed to verify that no other characters can be injected that would lead to an HTML injection (XSS) vulnerability.

### Solution

Review the reflected characters to ensure that they are properly handled as defined by the web application's coding practice. Typical solutions are to apply HTML encoding or percent encoding to the characters depending on where they are placed in the HTML. For example, a double quote might be encoded as " when displayed in a text node, but as %22 when placed in the value of an href attribute.

## Detection Information

| | |
|---|---|
| **Parameter** | It has been detected by exploiting the parameter **RedirectPath**<br>The payloads section will display a list of tests that show how the param could have been exploited to collect the information |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=4&IgnoreRedirect=true
https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=4&IgnoreRedirect=true#

## Payloads

### #1 Request

GET https://www.parisssd.org/site/UserControls/TermsOfUse/TermsOfUse.aspx?RedirectPa th=%3C%0a%0dscript%20a%3D4%3Eqss2EgCS3Kk%3D7%3C%0a%0d%2Fscript%3E&IgnoreRedi rect=true

Referer: https://www.parisssd.org/
Cookie: SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; SWScreenWidth=240; SWPageNavState=; SWClientWidth=1024; RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2Fdefault.aspx%3FPageID%3D4276; PSN=LjAVScvfF4t8u12OcOc08A==; PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; CSAN=8/YyjPiDJwJtBZxSxX5+iA==; AccountID=Xogon24LhVEF1Gfd40nUZQ==; ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; APIKey=08991e7a-6781-4289ab2a-9d2425fd36b8; Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

Response content-type: text/html

Notification('You have successfully agreed to the Terms Of Use.'); if('False'=='True'){DisplayNotification();} else{window.location= ((result[0].openworkspace == 'true' && 'True' == 'true') ? 'https://www.parisssd.org//myview/' : '< script a=4>qss2EgCS3Kk=7<

/script>');} ";
}
else if (AgreedToTermsOfUse == 2) { //2 denotes that the user has cancelled-out-of or disagreed to terms of use
var success = 'CloseDialogOverlay("WindowMediumModal");' + 'CallController("/s

* The reflected string on the response webpage indicates that the vulnerability test was successful

## 150076 DOM-Based Cross-Site Scripting (XSS)

*https://www.parisssd.org* **Active**

**URL:** https://www.parisssd.org/site/default.aspx?PageType=3%26DomainID=9%26ModuleInstanceID=1043%26ViewID=6446EE88-D30C-497E-9316-3F8874B3E108%26RenderLoc=0%26FlexDataID=9983%26PageID=11

| | | | |
|---|---|---|---|
| **Finding #** | 14849380 | **Severity** | Confirmed Vulnerability - Level 4 |
| **Unique #** | 281f9eba-e895-42cb-be11-8f1f583a40f8 | | |
| **Group** | - | **First Time Detected** | 15 Dec 2021 03:01 GMT |
| **CWE** | CWE-79 | **Last Time Detected** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A7 Cross-Site Scripting (XSS) | **Last Time Tested** | 15 Jan 2022 03:01 GMT |
| **WASC** | WASC-8 CROSS-SITE SCRIPTING | **Times Detected** | 2 |

# WAS Web Application Report

| CVSS V3 Base | 6.1 | CVSS V3 Temporal | 5.8 | CVSS V3 Attack Vector |
|---|---|---|---|---|

## Details

Network

### Threat

This is a type of HTML injection that delivers an attack payload via a property of the browser's Document Object Model (DOM). The DOM represents the rendered form of a site's web page, such as frames, tables, forms, and text. The vulnerability occurs because a web page uses JavaScript to update the DOM with an attackerinfluenced value that either changes the DOM's layout or executes JavaScript of the attacker's choosing. The following example demonstrates a DOM property, document.location, that is used to update the DOM via document.write. The exploit succeeds because the browser interprets the output of document.write as HTML, which the attacker uses to inject a Vulnerable web page: Other XSS vulnerabilities occur when the Web application echoes user-supplied data in an HTML response sent to the Web browser. For example, a Web application might include the user's name as part of a welcome message, or display a home address when confirming a shipping destination. If the user-supplied data contains characters that are interpreted as part of an HTML element instead of literal text, then an attacker can modify the HTML that is received by the victim's Web browser.

### Impact

XSS exploits pose a significant threat to a Web application, its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code. Consequently, any capability or feature available to the Web browser (for example HTML, JavaScript, Flash and Java applets) can be used as part of a compromise.

### Solution

Client-side JavaScript that uses document.write or otherwise modifies the DOM based on DOM properties such as document.location or window.location.href should filter content to ensure it does not contain malicious characters.

Any data collected from the client and displayed in a Web page should be HTML-encoded to ensure the content is rendered as text instead of an HTML element or JavaScript.

More information can be found at the OWASP community site.

## Detection Information

| | |
|---|---|
| **Parameter** | No param has been required for detecting the information. |
| **Authentication** | In order to detect this vulnerability, no authentication has been required. |
| **Access Path** | Here is the path followed by the scanner to reach the exploitable URL: |

https://www.parisssd.org/
https://www.parisssd.org/site/Default.aspx?PageID=11

## Payloads

### #1 Request

GET https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleI nstanceID=1043&ViewID=6446EE88-D30C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=9983&PageID=11

Host: www.parisssd.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15 Accept: */*

*Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.*

### #1 Response

comment: Taint propagation details:

Source:
location JS
call stack:
function: element.innerHTML
Sink:
element.innerHTML

Exploitation back-trace:

alert
appendChild@[native code] p@https://www.parisssd.org/Static/GlobalAssets/Scripts/min/jquery-3.0.0.min.js:2:534
Ha@https://www.parisssd.org/Static/GlobalAssets/Scripts/min/jquery-3.0.0.min.js:3:15453
addFramesetTranslate@https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88D30
C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=9983&PageID=11#q=%22%3E%3Cscript%3Ealert(40000)%3C/script%3E:1781:32
https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88-
D30C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=9983&PageID=11#q=%22%3E%3Cscript%3Ealert(40000)%3C/script%3E:1409:23
j@https://www.parisssd.org/Static/GlobalAssets/Scripts/min/jquery-3.0.0.min.js:2:29593 https://www.parisssd.org/Static/GlobalAssets/Scripts/min/jquery-
3.0.0.min.js:2:29903
nrWrapper@https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88-
D30C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=9983&PageID=11#q=%22%3E%3Cscript%3Ealert(40000)%3C/script%3E:1950:25192
N/A

## 150086 Server accepts unnecessarily large POST request body

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| **Finding #** | 5938098 | **Severity** | Information Gathered - Level 3 |
| **Unique #** | e043f5da-4c17-4308-b16e-2a232917f430 | | |
| **Group** | Information Gathered | | |
| **CWE** | CWE-130, CWE-1032 | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | | |
| **WASC** | - | | |

## Details

### Threat

The scanner successfully sent a POST request with content type of application/x-www-form-urlencoded and 65536 bytes length random text data. Accepting request bodies with unnecessarily large size could help attacker to use less connections to achieve Layer 7 DDoS of web server. More information can be found at the here

### Impact

Potentially could result in a successful application-layer DDoS attack.

### Solution

Limit the size of the request body to each form's requirements. For example, a search form with 256-char search field should not accept more than 1KB value. Server-specific details can be found here.

## Results

Server responded 200 to unnecessarily large random request body(over 64 KB) for URL https://www.parisssd.org/ums/Users/SecurityController.aspx, significantly increasing attacker's chances to prolong slow HTTP POST attack.

# WAS Web Application Report

## 150210 Information Disclosure via Response Header

https://www.parisssd.org

| | | | |
|---|---|---|---|
| **Finding #** | 5938096 | **Severity** | Information Gathered - Level 3 |
| **Unique #** | 7d453548-93f9-42b8-b999-badf86cb6649 | | |
| **Group** | Information Gathered | | |
| **CWE** | CWE-16, CWE-201 | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | | |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | | |

## Details

### Threat

HTTP response headers like 'Server', 'X-Powered-By', 'X-AspNetVersion', 'X-AspNetMvcVersion' could disclose information about the platform and technologies used by the website. The HTTP response include one or more such headers.

### Impact

The headers can potentially be used by attackers for fingerprinting and launching attacks specific to the technologies and versions used by the web application.

These response headers are not necessary for production sites and should be disabled. **Solution**

Disable such response headers, remove them from the response, or make sure that the header value does not contain information which could be used to fingerprint the server-side components of the web application.

## Results

One or more response headers disclosing information about the application platform were present on the following pages:
(Only first 50 such pages are reported)

GET https://www.parisssd.org/ response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/Static/GlobalAssets/Scripts/min/sri-failover.min.js response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-Light.css response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-Italic.css response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-Regular.css response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-SemiBold.css response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd-theme-default.css response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static/App_Themes/SW/jquery.jgrowl.css response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static//site/assets/styles/system_2560.css response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static//site/assets/styles/apps.css response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static/App_Themes/SW/jQueryUI.css response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static/GlobalAssets/webfonts/SchoolwiresMobile_2320.css response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static//site/assets/styles/dashboard.css response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static/GlobalAssets/Styles/Grid.css response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static/GlobalAssets/WCM-2550/WCM.js response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static/GlobalAssets/WCM-2550/API.js response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static/GlobalAssets/Scripts/min/jquery-3.0.0.min.js response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static//GlobalAssets/Scripts/min/jquery-migrate-1.4.1.min.js response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static/GlobalAssets/Scripts/ThirdParty/tether/tether.min.js response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd.min.js response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/cms/lib03/TN01920488/Centricity/domain/4/icons/favicon.ico response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

GET https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=4&IgnoreRedirect=true response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/Domain/4 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/Page/1 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/156 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/11 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/268 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/157 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/159 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/158 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/161 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/209 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/247 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/235 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/397 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/394 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
GET https://www.parisssd.org/domain/400 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/392 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/393 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/390 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/391 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/413 response code: 200

Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/363 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/362 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/site/Default.aspx?PageID=11 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/site/Default.aspx?PageID=13 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/site/Default.aspx?PageID=9 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/162 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/408 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

GET https://www.parisssd.org/domain/240 response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

## 150261 Subresource Integrity (SRI) Not Implemented

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| **Finding #** | 5938109 | **Severity** | Information Gathered - Level 3 |
| **Unique #** | c121773e-3567-4cc6-95aa-9ad48447ecb1 | | |
| **Group** | Information Gathered | | |
| **CWE** | CWE-693 | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**
The integrity attribute is missing in script and/or link elements. Subresource Integrity (SRI) is a standard browser security feature that verifies the value of the integrity attribute in

**Impact**
Absence of SRI checks means it is impossible to verify that the third-party resources are delivered without any unexpected manipulation.

**Solution**
All script and link elements that load external content should include the integrity attribute to ensure that the content is trustworthy.

More information:
Subresource Integrity article by Mozilla
OWASP Third-Party JavaScript Management Cheat Sheet

## Results

Externally loaded Javascript and CSS resources without integrity checks:

Parent link : https://www.parisssd.org/
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=4&IgnoreRedirect=true
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/Domain/4
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/Page/1
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/domain/156
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js

//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/domain/11
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/domain/268
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/domain/157
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/domain/159
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/domain/158
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js

//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/domain/161
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js //extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/domain/209
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/domain/247
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/domain/235
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/domain/397
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/domain/394
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js

//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/domain/400
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme Parent link : https://www.parisssd.org/domain/392
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/domain/393
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme

Parent link : https://www.parisssd.org/domain/390
Found following resource links without integrity checks (only first 10 links are reported)
//extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
//extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
//extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js
//extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
//extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js
//extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
//extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
//fonts.googleapis.com/css?family=Pathway+Gothic+One|Archivo+Narrow:400,700|Oswald:400,700|Oranienbaum|Carme
Please check there may be more pages with subresource links without integrity checks.

## 150202 Missing header: X-Content-Type-Options

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| **Finding #** | 5938110 | **Severity** | Information Gathered - Level 2 |
| **Unique #** | fb275569-882c-48cd-b894-3a028e494d52 | | |
| **Group** | Information Gathered | | |
| **CWE** | CWE-16, CWE-1032 | **Detection Date** | 15 Jan 2022 03:01 GMT |

# WAS Web Application Report

| | |
|---|---|
| OWASP | A6 Security Misconfiguration |
| WASC | WASC-15 APPLICATION MISCONFIGURATION |

## Details

### Threat

The X-Content-Type-Options response header is not present. WAS reports missing X-Content-Type-Options header on each crawled link for both static and dynamic responses. The scanner performs the check not only on 200 responses but 4xx and 5xx responses as well. It's also possible the QID will be reported on directory-level links.

### Impact

All web browsers employ a content-sniffing algorithm that inspects the contents of HTTP responses and also occasionally overrides the MIME type provided by the server. If X-Content-Type-Options header is not present, browsers can potentially be tricked into treating non-HTML response as HTML. An attacker can then potentially leverage the functionality to perform a cross-site scripting (XSS) attack. This specific case is known as a Content-Sniffing XSS (CS-XSS) attack.

### Solution

It is recommended to disable browser content sniffing by adding the X-Content-Type-Options header to the HTTP response with a value of 'nosniff'. Also, ensure that the 'Content-Type' header is set correctly on responses.

## Results

X-Content-Type-Options: Header missing
Response headers on link: GET https://www.parisssd.org/ response code: 200
Content-Type: text/html; charset=utf-8
Content-Length: 229493
Connection: keep-alive
Date: Sat, 15 Jan 2022 03:03:58 GMT
Cache-Control: no-cache, no-store
Pragma: no-cache
Expires: -1
Server: Microsoft-IIS/8.5
Strict-Transport-Security: max-age=31536000; includeSubDomains;
X-XSS-Protection: 1; mode=block
X-AspNet-Version: 4.0.30319
Set-Cookie: RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fdefault.aspx%3FPageID%3D1; path=/; secure
Set-Cookie: PSN=LjAVScvfF4t8u12OcOc08A==; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: CSAN=8/YyjPiDJwJtBZxSxX5+iA==; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: AccountID=Xogon24LhVEF1Gfd40nUZQ==; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fdefault.aspx%3FPageID%3D1; secure; domain=www.parisssd.org; path=/ Set-Cookie: SWScreenWidth=240; domain=www.parisssd.org; path=/
Set-Cookie: SWClientWidth=1024; domain=www.parisssd.org; path=/
Set-Cookie: SWPageNavState=; domain=www.parisssd.org; path=/
CancelRedirectTo=; expires=Fri, 14-Jan-2022 19: 03:58 GMT; path=/; secure
X-Powered-By: ASP.NET
Content-Security-Policy: frame-ancestors 'self' https://*.ally.ac;
X-Frame-Options: SAMEORIGIN
X-Cache: Miss from cloudfront
Via: 1.1 b014854bd0108b7ed0058504b69ccb5a.cloudfront.net (CloudFront) X-Amz-Cf-Pop: SFO53-C1
X-Amz-Cf-Id: u7ok-W-oxiClFOmSO-l0Bay4EJ5izflISIdNMhUR4OqYSCO547DWFA==

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://www.parisssd.org/ response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Scripts/min/sri-failover.min.js response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-Light.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-Italic.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-Regular.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-SemiBold.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd-theme-default.css response code: 200

GET https://www.parisssd.org/Static/App_Themes/SW/jquery.jgrowl.css response code: 200
GET https://www.parisssd.org/Static//site/assets/styles/system_2560.css response code: 200
GET https://www.parisssd.org/Static//site/assets/styles/apps.css response code: 200
GET https://www.parisssd.org/Static/App_Themes/SW/jQueryUI.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/webfonts/SchoolwiresMobile_2320.css response code: 200
GET https://www.parisssd.org/Static//site/assets/styles/dashboard.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Styles/Grid.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/WCM-2550/WCM.js response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/WCM-2550/API.js response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Scripts/min/jquery-3.0.0.min.js response code: 200
GET https://www.parisssd.org/Static//GlobalAssets/Scripts/min/jquery-migrate-1.4.1.min.js response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Scripts/ThirdParty/tether/tether.min.js response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd.min.js response code: 200
GET https://www.parisssd.org/cms/lib03/TN01920488/Centricity/domain/4/icons/favicon.ico response code: 200
GET https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=4&IgnoreRedirect=true response code: 200
GET https://www.parisssd.org/Domain/4 response code: 200
GET https://www.parisssd.org/Page/1 response code: 200
GET https://www.parisssd.org/domain/156 response code: 200
GET https://www.parisssd.org/domain/11 response code: 200
GET https://www.parisssd.org/domain/268 response code: 200
GET https://www.parisssd.org/domain/157 response code: 200
GET https://www.parisssd.org/domain/159 response code: 200
GET https://www.parisssd.org/domain/158 response code: 200
GET https://www.parisssd.org/domain/161 response code: 200
GET https://www.parisssd.org/domain/209 response code: 200
GET https://www.parisssd.org/domain/247 response code: 200
GET https://www.parisssd.org/domain/235 response code: 200
GET https://www.parisssd.org/domain/397 response code: 200
GET https://www.parisssd.org/domain/394 response code: 200
GET https://www.parisssd.org/domain/400 response code: 200
GET https://www.parisssd.org/domain/392 response code: 200
GET https://www.parisssd.org/domain/393 response code: 200
GET https://www.parisssd.org/domain/390 response code: 200
GET https://www.parisssd.org/domain/391 response code: 200
GET https://www.parisssd.org/domain/413 response code: 200
GET https://www.parisssd.org/domain/363 response code: 200
GET https://www.parisssd.org/domain/362 response code: 200
GET https://www.parisssd.org/site/Default.aspx?PageID=11 response code: 200
GET https://www.parisssd.org/site/Default.aspx?PageID=13 response code: 200
GET https://www.parisssd.org/site/Default.aspx?PageID=9 response code: 200
GET https://www.parisssd.org/domain/162 response code: 200
GET https://www.parisssd.org/domain/408 response code: 200
GET https://www.parisssd.org/domain/240 response code:
200

## 150208 Missing header: Referrer-Policy

https://www.parisssd.org

| | | | |
|---|---|---|---|
| **Finding #** | 5938097 | **Severity** | Information Gathered - Level 2 |
| **Unique #** | 932fe1b5-a41c-44b7-81ca-697794cfd3de | | |
| **Group** | Information Gathered | | |
| **CWE** | CWE-16, CWE-1032 | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | | |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | | |

### Details

**Threat**

No Referrer Policy is specified for the link. WAS checks for the missing Referrer Policy on all static and dynamic pages. It checks for one of the following Referrer Policy in the response headers:

1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin

If the Referrer Policy header is not found , WAS checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

**Impact**

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

**Solution**

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

## Results

Referrer-Policy: Header missing
Response headers on link: GET https://www.parisssd.org/ response code: 200
Content-Type: text/html; charset=utf-8
Content-Length: 229493
Connection: keep-alive
Date: Sat, 15 Jan 2022 03:03:58 GMT
Cache-Control: no-cache, no-store
Pragma: no-cache
Expires: -1
Server: Microsoft-IIS/8.5
Strict-Transport-Security: max-age=31536000; includeSubDomains;
X-XSS-Protection: 1; mode=block
X-AspNet-Version: 4.0.30319
Set-Cookie: RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fdefault.aspx%3FPageID%3D1; path=/; secure
Set-Cookie: PSN=LjAVScvfF4t8u12OcOc08A==; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: CSAN=8/YyjPiDJwJtBZxSxX5+iA==; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: AccountID=Xogon24LhVEF1Gfd40nUZQ==; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fdefault.aspx%3FPageID%3D1; secure; domain=www.parisssd.org; path=/
Set-Cookie: SWScreenWidth=240; domain=www.parisssd.org; path=/
Set-Cookie: SWClientWidth=1024; domain=www.parisssd.org; path=/
Set-Cookie: SWPageNavState=; domain=www.parisssd.org; path=/
CancelRedirectTo=; expires=Fri, 14-Jan-2022 19: 03:58 GMT; path=/; secure
X-Powered-By: ASP.NET
Content-Security-Policy: frame-ancestors 'self' https://*.ally.ac;
X-Frame-Options: SAMEORIGIN
X-Cache: Miss from cloudfront
Via: 1.1 b014854bd0108b7ed0058504b69ccb5a.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: SFO53-C1
X-Amz-Cf-Id: u7ok-W-oxiClFOmSO-l0Bay4EJ5izflISIdNMhUR4OqYSCO547DWFA==

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://www.parisssd.org/ response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Scripts/min/sri-failover.min.js response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-Light.css response code: 200

GET https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-Italic.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-Regular.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-SemiBold.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd-theme-default.css response code: 200
GET https://www.parisssd.org/Static/App_Themes/SW/jquery.jgrowl.css response code: 200
GET https://www.parisssd.org/Static//site/assets/styles/system_2560.css response code: 200
GET https://www.parisssd.org/Static//site/assets/styles/apps.css response code: 200
GET https://www.parisssd.org/Static/App_Themes/SW/jQueryUI.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/webfonts/SchoolwiresMobile_2320.css response code: 200
GET https://www.parisssd.org/Static//site/assets/styles/dashboard.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Styles/Grid.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/WCM-2550/WCM.js response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/WCM-2550/API.js response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Scripts/min/jquery-3.0.0.min.js response code: 200
GET https://www.parisssd.org/Static//GlobalAssets/Scripts/min/jquery-migrate-1.4.1.min.js response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Scripts/ThirdParty/tether/tether.min.js response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd.min.js response code: 200
GET https://www.parisssd.org/cms/lib03/TN01920488/Centricity/domain/4/icons/favicon.ico response code: 200
GET https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=4&IgnoreRedirect=true response code: 200
GET https://www.parisssd.org/Domain/4 response code: 200
GET https://www.parisssd.org/Page/1 response code: 200
GET https://www.parisssd.org/domain/156 response code: 200
GET https://www.parisssd.org/domain/11 response code: 200
GET https://www.parisssd.org/domain/268 response code: 200
GET https://www.parisssd.org/domain/157 response code: 200
GET https://www.parisssd.org/domain/159 response code: 200
GET https://www.parisssd.org/domain/158 response code: 200
GET https://www.parisssd.org/domain/161 response code: 200
GET https://www.parisssd.org/domain/209 response code: 200
GET https://www.parisssd.org/domain/247 response code: 200
GET https://www.parisssd.org/domain/235 response code: 200
GET https://www.parisssd.org/domain/397 response code: 200
GET https://www.parisssd.org/domain/394 response code: 200
GET https://www.parisssd.org/domain/400 response code: 200
GET https://www.parisssd.org/domain/392 response code: 200
GET https://www.parisssd.org/domain/393 response code: 200
GET https://www.parisssd.org/domain/390 response code: 200
GET https://www.parisssd.org/domain/391 response code: 200
GET https://www.parisssd.org/domain/413 response code: 200
GET https://www.parisssd.org/domain/363 response code: 200
GET https://www.parisssd.org/domain/362 response code: 200
GET https://www.parisssd.org/site/Default.aspx?PageID=11 response code: 200
GET https://www.parisssd.org/site/Default.aspx?PageID=13 response code: 200
GET https://www.parisssd.org/site/Default.aspx?PageID=9 response code: 200
GET https://www.parisssd.org/domain/162 response code: 200
GET https://www.parisssd.org/domain/408 response code: 200
GET https://www.parisssd.org/domain/240 response code: 200

## 150262 Missing header: Feature-Policy

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| **Finding #** | 5938108 | **Severity** | Information Gathered - Level 2 |
| **Unique #** | 7ddc96e1-bfaa-47fa-b852-20efe4edfabe | | |
| **Group** | Information Gathered | | |
| **CWE** | CWE-16, CWE-1032 | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | | |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | | |

### Details

**Threat**

The Feature-Policy response header is not present.

# WAS Web Application Report

### Impact

Feature Policy allows web developers to selectively enable, disable, and modify the behavior of certain APIs and web features such as "geolocation","camera", "usb", "fullscreen", "animations" etc in the browser.

These policies restrict what APIs the site can access or modify the browser's default behavior for certain features.

### Solution

It is recommended to set the Feature-Policy header to selectively enable, disable, and modify the behavior of certain APIs and web features.

References:
- https://www.w3.org/TR/feature-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

## Results

Feature-Policy: Header missing
Response headers on link: GET https://www.parisssd.org/ response code: 200
Content-Type: text/html; charset=utf-8
Content-Length: 229493
Connection: keep-alive
Date: Sat, 15 Jan 2022 03:03:58 GMT
Cache-Control: no-cache, no-store
Pragma: no-cache
Expires: -1
Server: Microsoft-IIS/8.5
Strict-Transport-Security: max-age=31536000; includeSubDomains;
X-XSS-Protection: 1; mode=block
X-AspNet-Version: 4.0.30319
Set-Cookie: RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fdefault.aspx%3FPageID%3D1; path=/; secure
Set-Cookie: PSN=LjAVScvfF4t8u12OcOc08A==; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: CSAN=8/YyjPiDJwJtBZxSxX5+iA==; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: AccountID=Xogon24LhVEF1Gfd40nUZQ==; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fdefault.aspx%3FPageID%3D1; secure; domain=www.parisssd.org; path=/ Set-Cookie: SWScreenWidth=240; domain=www.parisssd.org; path=/
Set-Cookie: SWClientWidth=1024; domain=www.parisssd.org; path=/
Set-Cookie: SWPageNavState=; domain=www.parisssd.org; path=/
CancelRedirectTo=; expires=Fri, 14-Jan-2022 19: 03:58 GMT; path=/; secure
X-Powered-By: ASP.NET
Content-Security-Policy: frame-ancestors 'self' https://*.ally.ac;
X-Frame-Options: SAMEORIGIN
X-Cache: Miss from cloudfront
Via: 1.1 b014854bd0108b7ed0058504b69ccb5a.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: SFO53-C1
X-Amz-Cf-Id: u7ok-W-oxiClFOmSO-l0Bay4EJ5izflISIdNMhUR4OqYSCO547DWFA==

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://www.parisssd.org/ response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Scripts/min/sri-failover.min.js response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-Light.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-Italic.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-Regular.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-SemiBold.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd-theme-default.css response code: 200
GET https://www.parisssd.org/Static/App_Themes/SW/jquery.jgrowl.css response code: 200
GET https://www.parisssd.org/Static//site/assets/styles/system_2560.css response code: 200
GET https://www.parisssd.org/Static//site/assets/styles/apps.css response code: 200
GET https://www.parisssd.org/Static/App_Themes/SW/jQueryUI.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/webfonts/SchoolwiresMobile_2320.css response code: 200
GET https://www.parisssd.org/Static//site/assets/styles/dashboard.css response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Styles/Grid.css response code: 200

GET https://www.parisssd.org/Static/GlobalAssets/WCM-2550/WCM.js response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/WCM-2550/API.js response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Scripts/min/jquery-3.0.0.min.js response code: 200
GET https://www.parisssd.org/Static//GlobalAssets/Scripts/min/jquery-migrate-1.4.1.min.js response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Scripts/ThirdParty/tether/tether.min.js response code: 200
GET https://www.parisssd.org/Static/GlobalAssets/Scripts/ThirdParty/shepherd/shepherd.min.js response code: 200
GET https://www.parisssd.org/cms/lib03/TN01920488/Centricity/domain/4/icons/favicon.ico response code: 200
GET https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=4&IgnoreRedirect=true response code: 200
GET https://www.parisssd.org/Domain/4 response code: 200
GET https://www.parisssd.org/Page/1 response code: 200
GET https://www.parisssd.org/domain/156 response code: 200
GET https://www.parisssd.org/domain/11 response code: 200
GET https://www.parisssd.org/domain/268 response code: 200
GET https://www.parisssd.org/domain/157 response code: 200
GET https://www.parisssd.org/domain/159 response code: 200
GET https://www.parisssd.org/domain/158 response code: 200
GET https://www.parisssd.org/domain/161 response code: 200
GET https://www.parisssd.org/domain/209 response code: 200
GET https://www.parisssd.org/domain/247 response code: 200
GET https://www.parisssd.org/domain/235 response code: 200
GET https://www.parisssd.org/domain/397 response code: 200
GET https://www.parisssd.org/domain/394 response code: 200
GET https://www.parisssd.org/domain/400 response code: 200
GET https://www.parisssd.org/domain/392 response code: 200
GET https://www.parisssd.org/domain/393 response code: 200
GET https://www.parisssd.org/domain/390 response code: 200
GET https://www.parisssd.org/domain/391 response code: 200
GET https://www.parisssd.org/domain/413 response code: 200
GET https://www.parisssd.org/domain/363 response code: 200
GET https://www.parisssd.org/domain/362 response code: 200
GET https://www.parisssd.org/site/Default.aspx?PageID=11 response code: 200
GET https://www.parisssd.org/site/Default.aspx?PageID=13 response code: 200
GET https://www.parisssd.org/site/Default.aspx?PageID=9 response code: 200
GET https://www.parisssd.org/domain/162 response code: 200
GET https://www.parisssd.org/domain/408 response code: 200
GET https://www.parisssd.org/domain/240 response code:
200

## 150009 Links Crawled

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| **Finding #** | 5913861 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | 61018a94-b03f-498d-9c83-8ec7222de161 | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)- Certain requests from QID 150172 (Requests Crawled)

### Impact
N/A

### Solution
N/A

## Results

Duration of crawl phase (seconds): 2474.00
Number of links: 754
(This number excludes form requests, ajax links (included in QID 150148) and links re-requested during authentication.)

https://www.parisssd.org/
https://www.parisssd.org/#
https://www.parisssd.org/.
https://www.parisssd.org//cms/Module/SelectSurvey/TakeSurveyAction.aspx?DisplayHeader=
https://www.parisssd.org//cms/UserControls/ModuleView/ModuleViewRendererWrapper.aspx?DomainID=11&PageID=15&ModuleInstanceID=
https://www.parisssd.org//cms/UserControls/ModuleView/ModuleViewRendererWrapper.aspx?DomainID=156&PageID=757&ModuleInstanceID=
https://www.parisssd.org//cms/UserControls/ModuleView/ModuleViewRendererWrapper.aspx?DomainID=157&PageID=758&ModuleInstanceID=
https://www.parisssd.org//cms/UserControls/ModuleView/ModuleViewRendererWrapper.aspx?DomainID=158&PageID=1737&ModuleInstanceID=
https://www.parisssd.org//cms/UserControls/ModuleView/ModuleViewRendererWrapper.aspx?DomainID=159&PageID=760&ModuleInstanceID=
https://www.parisssd.org//cms/UserControls/ModuleView/ModuleViewRendererWrapper.aspx?DomainID=161&PageID=761&ModuleInstanceID=
https://www.parisssd.org//cms/UserControls/ModuleView/ModuleViewRendererWrapper.aspx?DomainID=268&PageID=1943&ModuleInstanceID=
https://www.parisssd.org//cms/UserControls/ModuleView/ModuleViewRendererWrapper.aspx?DomainID=4&PageID=1&ModuleInstanceID=
https://www.parisssd.org//cms/lib/TN01920488/Centricity/Domain/10/20727971_106138643438079_6043615046632945 69_n.jpg
https://www.parisssd.org//cms/lib/TN01920488/Centricity/Domain/9/Capture.PNG https://www.parisssd.org//cms/module/selectsurvey/TakeSurvey.aspx?SurveyID=108
https://www.parisssd.org//site/Default.aspx?PageID=1382
https://www.parisssd.org//site/Default.aspx?PageID=2&PageType=17&DomainID=4&ModuleInstanceID=1&EventDateID=
https://www.parisssd.org//site/UserControls/Calendar/CalendarChannelListWrapper.aspx?DomainID=
https://www.parisssd.org//site/UserControls/Calendar/CalendarController.aspx/DeleteRegistration
https://www.parisssd.org//site/UserControls/Calendar/CalendarController.aspx/GetEvents
https://www.parisssd.org//site/UserControls/Calendar/CalendarController.aspx/UpdateCalendarFollow
https://www.parisssd.org//site/UserControls/Calendar/CalendarFilterListWrapper.aspx?ModuleInstanceID=
https://www.parisssd.org//site/UserControls/Calendar/CalendarFilterNewWrapper.aspx?DomainID=4&ModuleInstanceID=1
https://www.parisssd.org//site/UserControls/Calendar/CalendarPrint.aspx?ModuleInstanceID=1&PageID=2&Date=
https://www.parisssd.org//site/UserControls/Calendar/CalendarPrint.aspx?ModuleInstanceID=1&PageID=2&DomainID=4&Date
= https://www.parisssd.org//site/UserControls/Calendar/CalendarSearchListWrapper.aspx?DomainID=
https://www.parisssd.org//site/UserControls/Calendar/CategoryFilterListWrapper.aspx?ModuleInstanceID=
https://www.parisssd.org//site/UserControls/Calendar/CategoryFilterNewWrapper.aspx?DomainID=4&ModuleInstanceID=1
https://www.parisssd.org//site/UserControls/Calendar/CategoryLegendWrapper.aspx?ModuleInstanceID=1
https://www.parisssd.org//site/UserControls/Calendar/EventDetailWrapper.aspx?ModuleInstanceID=
https://www.parisssd.org//site/UserControls/Calendar/EventExport.aspx?ModuleInstanceID=1&StartDate=
https://www.parisssd.org//site/UserControls/Calendar/EventExportByDateRangeWrapper.aspx
https://www.parisssd.org//site/UserControls/Calendar/EventListViewWrapper.aspx?ModuleInstanceID=
https://www.parisssd.org//site/UserControls/Calendar/MyEventsListWrapper.aspx?ModuleInstanceID=1&StartDate=
https://www.parisssd.org//site/UserControls/Calendar/MyEventsWrapper.aspx?ModuleInstanceID=1
https://www.parisssd.org//site/default.aspx https://www.parisssd.org/Domain/14 https://www.parisssd.org/Domain/15
https://www.parisssd.org/Domain/156 https://www.parisssd.org/Domain/157 https://www.parisssd.org/Domain/158
https://www.parisssd.org/Domain/159 https://www.parisssd.org/Domain/161 https://www.parisssd.org/Domain/162
https://www.parisssd.org/Domain/209 https://www.parisssd.org/Domain/232 https://www.parisssd.org/Domain/234
https://www.parisssd.org/Domain/235 https://www.parisssd.org/Domain/240 https://www.parisssd.org/Domain/244
https://www.parisssd.org/Domain/247 https://www.parisssd.org/Domain/276 https://www.parisssd.org/Domain/297
https://www.parisssd.org/Domain/299 https://www.parisssd.org/Domain/337 https://www.parisssd.org/Domain/362
https://www.parisssd.org/Domain/363 https://www.parisssd.org/Domain/390 https://www.parisssd.org/Domain/391
https://www.parisssd.org/Domain/392 https://www.parisssd.org/Domain/393 https://www.parisssd.org/Domain/394
https://www.parisssd.org/Domain/397 https://www.parisssd.org/Domain/398 https://www.parisssd.org/Domain/399
https://www.parisssd.org/Domain/4 https://www.parisssd.org/Domain/4# https://www.parisssd.org/Domain/400
https://www.parisssd.org/Domain/401 https://www.parisssd.org/Domain/413 https://www.parisssd.org/Domain/6
https://www.parisssd.org/Domain/9 https://www.parisssd.org/Errors/404.aspx
https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest
https://www.parisssd.org/GlobalAssets/Scripts/ThirdParty/jquery.listfilter.js https://www.parisssd.org/Page/1
https://www.parisssd.org/Page/1# https://www.parisssd.org/Page/10 https://www.parisssd.org/Page/1096
https://www.parisssd.org/Page/1096# https://www.parisssd.org/Page/11 https://www.parisssd.org/Page/1171
https://www.parisssd.org/Page/12 https://www.parisssd.org/Page/13 https://www.parisssd.org/Page/14
https://www.parisssd.org/Page/1432 https://www.parisssd.org/Page/1432# https://www.parisssd.org/Page/1451
https://www.parisssd.org/Page/1452 https://www.parisssd.org/Page/1560 https://www.parisssd.org/Page/1702
https://www.parisssd.org/Page/1737 https://www.parisssd.org/Page/1737# https://www.parisssd.org/Page/18
https://www.parisssd.org/Page/1805

https://www.parisssd.org/Page/1931
https://www.parisssd.org/Page/1931#
https://www.parisssd.org/Page/1940
https://www.parisssd.org/Page/1940#
https://www.parisssd.org/Page/1941
https://www.parisssd.org/Page/1941#
https://www.parisssd.org/Page/1942
https://www.parisssd.org/Page/1942#
https://www.parisssd.org/Page/1943
https://www.parisssd.org/Page/1943#
https://www.parisssd.org/Page/2
https://www.parisssd.org/Page/2#
https://www.parisssd.org/Page/2059
https://www.parisssd.org/Page/2059#
https://www.parisssd.org/Page/2060
https://www.parisssd.org/Page/2060#
https://www.parisssd.org/Page/2085
https://www.parisssd.org/Page/2090
https://www.parisssd.org/Page/2091
https://www.parisssd.org/Page/2102
https://www.parisssd.org/Page/2162
https://www.parisssd.org/Page/2162#
https://www.parisssd.org/Page/2163
https://www.parisssd.org/Page/2163#
https://www.parisssd.org/Page/2164
https://www.parisssd.org/Page/2164#
https://www.parisssd.org/Page/2165
https://www.parisssd.org/Page/2165#
https://www.parisssd.org/Page/2166
https://www.parisssd.org/Page/2166#
https://www.parisssd.org/Page/2257
https://www.parisssd.org/Page/2327
https://www.parisssd.org/Page/2327#
https://www.parisssd.org/Page/2380
https://www.parisssd.org/Page/2380#
https://www.parisssd.org/Page/2462
https://www.parisssd.org/Page/2509
https://www.parisssd.org/Page/2510
https://www.parisssd.org/Page/2513
https://www.parisssd.org/Page/2587
https://www.parisssd.org/Page/2751
https://www.parisssd.org/Page/2751#
https://www.parisssd.org/Page/2761
https://www.parisssd.org/Page/2963
https://www.parisssd.org/Page/304
https://www.parisssd.org/Page/3044
https://www.parisssd.org/Page/3044#
https://www.parisssd.org/Page/318
https://www.parisssd.org/Page/319
https://www.parisssd.org/Page/320
https://www.parisssd.org/Page/3239
https://www.parisssd.org/Page/3783
https://www.parisssd.org/Page/3856
https://www.parisssd.org/Page/3860
https://www.parisssd.org/Page/3861
https://www.parisssd.org/Page/3862
https://www.parisssd.org/Page/3863
https://www.parisssd.org/Page/3909
https://www.parisssd.org/Page/3929
https://www.parisssd.org/Page/3929#
https://www.parisssd.org/Page/3932
https://www.parisssd.org/Page/3932#
https://www.parisssd.org/Page/3933
https://www.parisssd.org/Page/3933#
https://www.parisssd.org/Page/3936
https://www.parisssd.org/Page/3936#
https://www.parisssd.org/Page/3960
https://www.parisssd.org/Page/3960#
https://www.parisssd.org/Page/3962
https://www.parisssd.org/Page/3962#
https://www.parisssd.org/Page/4139
https://www.parisssd.org/Page/4149
https://www.parisssd.org/Page/4276

https://www.parisssd.org/Page/4340
https://www.parisssd.org/Page/4454
https://www.parisssd.org/Page/4596
https://www.parisssd.org/Page/4596#
https://www.parisssd.org/Page/4604
https://www.parisssd.org/Page/4604#
https://www.parisssd.org/Page/4606
https://www.parisssd.org/Page/4606#
https://www.parisssd.org/Page/4608
https://www.parisssd.org/Page/4608#
https://www.parisssd.org/Page/4609
https://www.parisssd.org/Page/4609#
https://www.parisssd.org/Page/4611
https://www.parisssd.org/Page/4611#
https://www.parisssd.org/Page/4614
https://www.parisssd.org/Page/4614#
https://www.parisssd.org/Page/4616
https://www.parisssd.org/Page/4616#
https://www.parisssd.org/Page/4626
https://www.parisssd.org/Page/4626#
https://www.parisssd.org/Page/4628
https://www.parisssd.org/Page/4628#
https://www.parisssd.org/Page/4629
https://www.parisssd.org/Page/4629#
https://www.parisssd.org/Page/4648
https://www.parisssd.org/Page/4648#
https://www.parisssd.org/Page/4685
https://www.parisssd.org/Page/4688
https://www.parisssd.org/Page/4706
https://www.parisssd.org/Page/4708
https://www.parisssd.org/Page/4708#
https://www.parisssd.org/Page/4711
https://www.parisssd.org/Page/4711#
https://www.parisssd.org/Page/4715
https://www.parisssd.org/Page/4715#
https://www.parisssd.org/Page/4719
https://www.parisssd.org/Page/4719#
https://www.parisssd.org/Page/4729
https://www.parisssd.org/Page/4729#
https://www.parisssd.org/Page/4738
https://www.parisssd.org/Page/4738#
https://www.parisssd.org/Page/4745
https://www.parisssd.org/Page/4745#
https://www.parisssd.org/Page/4767
https://www.parisssd.org/Page/4768
https://www.parisssd.org/Page/4769
https://www.parisssd.org/Page/4873
https://www.parisssd.org/Page/4888
https://www.parisssd.org/Page/4890
https://www.parisssd.org/Page/4891
https://www.parisssd.org/Page/4892
https://www.parisssd.org/Page/4894
https://www.parisssd.org/Page/5141
https://www.parisssd.org/Page/5173
https://www.parisssd.org/Page/5305
https://www.parisssd.org/Page/5342
https://www.parisssd.org/Page/5342#
https://www.parisssd.org/Page/5344
https://www.parisssd.org/Page/5344#
https://www.parisssd.org/Page/5345
https://www.parisssd.org/Page/5345#
https://www.parisssd.org/Page/5346
https://www.parisssd.org/Page/5346#
https://www.parisssd.org/Page/5347
https://www.parisssd.org/Page/5347#
https://www.parisssd.org/Page/5348
https://www.parisssd.org/Page/5348#
https://www.parisssd.org/Page/5349
https://www.parisssd.org/Page/5349#
https://www.parisssd.org/Page/5350
https://www.parisssd.org/Page/5350#
https://www.parisssd.org/Page/5351
https://www.parisssd.org/Page/5351#

https://www.parisssd.org/Page/5352
https://www.parisssd.org/Page/5352#
https://www.parisssd.org/Page/5353
https://www.parisssd.org/Page/5353#
https://www.parisssd.org/Page/5354
https://www.parisssd.org/Page/5354#
https://www.parisssd.org/Page/5451
https://www.parisssd.org/Page/5451#
https://www.parisssd.org/Page/5452
https://www.parisssd.org/Page/5452#
https://www.parisssd.org/Page/757
https://www.parisssd.org/Page/757#
https://www.parisssd.org/Page/758
https://www.parisssd.org/Page/758#
https://www.parisssd.org/Page/760
https://www.parisssd.org/Page/760#
https://www.parisssd.org/Page/761
https://www.parisssd.org/Page/761#
https://www.parisssd.org/Page/767
https://www.parisssd.org/Page/768
https://www.parisssd.org/Page/9
https://www.parisssd.org/SignInSecure.aspx?SecurePage=https%3A%2F%2Fwww.parisssd.org%2FSignIn.aspx
https://www.parisssd.org/SignInSecure.aspx?SecurePage=https://www.parisssd.org/SignIn.aspx
https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-Light.ttf?tiwypa https://www.parisssd.org/Static/GlobalAssets/webfonts/Opensans-Regular.ttf https://www.parisssd.org/Static/GlobalAssets/webfonts/arrow-icon.ttf?ta8730 https://www.parisssd.org/called
https://www.parisssd.org/cms/Tools/OnScreenAlerts/UserControls/OnScreenAlertDialogListWrapper.aspx?OnScreenAlertCookie=
https://www.parisssd.org/cms/lib/TN01920488/Centricity/Domain/390/PSSD%20Logo%20FLATTENED-01.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/Domain/4/reward%20schools.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/Domain/8/boy%20mask.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/Domain/8/kid%20at%20lapto.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/Domain/9/school%20messenger.JPG
https://www.parisssd.org/cms/lib/TN01920488/Centricity/Domain/9/school%2520messenger.JPG
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/18/large/100%201.jpg?rnd=0.596915798074061
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/18/large/100%204.jpg?rnd=0.874585764424217
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/18/large/100%205.jpg?rnd=0.688254453562319
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/18/large/100%206.jpg?rnd=0.966906373839316
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/18/large/7%20resized.jpg?rnd=0.111369644343559
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/18/large/lisa%20twins.jpg?rnd=0.220343269044693
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/18/large/old%20ladies.jpg?rnd=0.275674971414579
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/18/large/parade%203.jpg?rnd=0.000854781829218744
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/18/large/parade%204.jpg?rnd=0.0145320152000208
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/19/large/100%203.jpg?rnd=0.91967070098951
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/19/large/100%207.jpg?rnd=0.824063741054416
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/19/large/2pp1.jpg?rnd=0.499864666955483
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/19/large/music.jpg?rnd=0.560698032174584
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/19/large/parade%201.jpg?rnd=0.29401299277973
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/19/large/parade%202.jpg?rnd=0.774761760502477
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/19/large/paradeshow2.jpg?rnd=0.0763658648712402
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/19/large/pp9.jpg?rnd=0.464503818407889
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/19/large/tree%20ed.jpg?rnd=0.223080050769765
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/5th%20grade%20capital2.jpg?rnd=0.843724123595154
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/PE%20Program2.jpg?rnd=0.0384917091757486
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/PE%20Program3.jpg?rnd=0.608626292836213
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/ResizerImage355X389.jpg?rnd=0.507166424071028
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/book%20fair1.jpg?rnd=0.0594600811877568
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/book%20fair2.jpg?rnd=0.0811462295619521
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/crosser.jpg?rnd=0.497652573742742
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/dress.jpg?rnd=0.778544049606912
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/ixl1.jpg?rnd=0.523238387668151
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/moon1.jpg?rnd=0.484233771676306
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/patriot%20day2.jpg?rnd=0.878080834577829
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/pes1.jpg?rnd=0.0106159593028091
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/pes10.jpg?rnd=0.725109218957419
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/pes2.jpg?rnd=0.535115795459187
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/pes3.jpg?rnd=0.00764642143978105
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/pes30.jpg?rnd=0.15776393290505
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/pes31.jpg?rnd=0.797849428280187
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/pes4.jpg?rnd=0.436831880098596
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/pes50.jpg?rnd=0.592855771348279
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/pes51.jpg?rnd=0.163255236653264
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/pes53.jpg?rnd=0.549792992672787
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/pes6.jpg?rnd=0.511387247830344
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/pes7.jpg?rnd=0.597282715419905

https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/pes8.jpg?rnd=0.266707072158673
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/pes9.jpg?rnd=0.869920360329524
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/strings.jpg?rnd=0.672493429702005
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/supplies.jpg?rnd=0.909985594409511
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/web10.jpg?rnd=0.636465461755388
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/web13.jpg?rnd=0.577441374108867
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/web3.jpg?rnd=0.530458195382011
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/20/large/web30.jpg?rnd=0.574409025057409
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/PE%20Program1.jpg?rnd=0.579408542522885
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/ResizerImage355X236.jpg?rnd=0.185267458290452
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/art.jpg?rnd=0.641572984234231
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/book%20fair3.jpg?rnd=0.109603492594139
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/christmas1.jpg?rnd=0.433865042605375
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/dress1.jpg?rnd=0.25850221061078
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/kids%20club.jpg?rnd=0.913155518431755
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/moon2.jpg?rnd=0.980149642089452
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/patriot%20day4.jpg?rnd=0.841953258887843
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/pes1.jpg?rnd=0.387860795663605
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/pes10.jpg?rnd=0.454854555639836
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/pes11.jpg?rnd=0.599657587520619
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/pes20.jpg?rnd=0.503531237367322
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/pes3.jpg?rnd=0.550477756443656
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/pes32.jpg?rnd=0.62030895548887
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/pes33.jpg?rnd=0.135593962453117
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/pes54.jpg?rnd=0.0736001152887941
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/pes55.jpg?rnd=0.569079868760463
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/pes56.jpg?rnd=0.151938647568197
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/pes6.jpg?rnd=0.907611896706564
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/pes7.jpg?rnd=0.44110784374229
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/pes8.jpg?rnd=0.999896945897442
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/quad1.jpg?rnd=0.903275344475766
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/web12.jpg?rnd=0.42044652645497
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/web6.jpg?rnd=0.248240673098825
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/21/large/web8.jpg?rnd=0.110122855338325
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/100%20Years.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/2nd%20Grade%20Christmas%20Program.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/5th%20Graders%20Visit%20the%20Capital.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/Elegant%20Dinner%20at%20Rhea%202.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/Elegant%20Dinner%20at%20Rhea.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/Honoring%20a%20Veteran%20and%20Board%20Member%20John%20Steele.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/IMS%20FFA%20Awards%20at%20State%20Convention.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/Jason%20Coffield%20is%20PreK%20Story%20Hour%20Guest.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/March%20Madness%20IXL%20WInners%20at%20PES%203rd%20Grade.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/Straing%20at%20Quad%20State.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/Strings%20Christmas%20Program.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/boys%20basketball.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/football%20champions.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/girls%20basketball.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/ims%20banner.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/ims%20steam2.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/patriot%20day1.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/patriot%20day2.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/patriot%20day3.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/rhea%20princess1.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/rhea%20princess2.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/rhea%20pumpkin%20patch.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/rhea%20pumpkin%20patch2.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/rhea%20steam.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/rhea%20super%20heros.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/wildlife%20refuge1.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/ModuleInstance/3828/large/wildlife%20refuge2.jpg
https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/_admin.txt
https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/_default.txt
https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt
https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642215942584
https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt
https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642215938740
https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217018270
https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217020707
https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt
https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642215937352
https://www.parisssd.org/cms/lib/TN01920488/Centricity/domain/4/icons/favicon.ico

https://www.parisssd.org/cms/lib03/TN01920488/Centricity/Domain/4//PowerSchool/ParentPortalWelcome.htm
https://www.parisssd.org/cms/lib03/TN01920488/Centricity/Domain/4/PowerSchool/ParentPortalWelcome.htm
https://www.parisssd.org/cms/lib03/TN01920488/Centricity/Domain/4/PowerSchool/ParentPortalWelcome_files/colorschememapping.xml https://www.parisssd.org/cms/lib03/TN01920488/Centricity/Domain/4/PowerSchool/ParentPortalWelcome_files/editdata.mso
https://www.parisssd.org/cms/lib03/TN01920488/Centricity/Domain/4/PowerSchool/ParentPortalWelcome_files/filelist.xml
https://www.parisssd.org/cms/lib03/TN01920488/Centricity/Domain/4/PowerSchool/ParentPortalWelcome_files/themedata.thmx
https://www.parisssd.org/cms/lib03/TN01920488/Centricity/domain/4/icons/favicon.ico
https://www.parisssd.org/cms/lib2/SW00000032/Centricity/Domain/4/scripts/templateDropdown.js
https://www.parisssd.org/cms/module/selectsurvey/TakeSurvey.aspx?SurveyID=108 https://www.parisssd.org/crossdomain.xml
https://www.parisssd.org/default.aspx?PageID=1 https://www.parisssd.org/domain/103 https://www.parisssd.org/domain/104
https://www.parisssd.org/domain/105 https://www.parisssd.org/domain/107 https://www.parisssd.org/domain/11
https://www.parisssd.org/domain/11# https://www.parisssd.org/domain/110 https://www.parisssd.org/domain/112
https://www.parisssd.org/domain/114 https://www.parisssd.org/domain/115 https://www.parisssd.org/domain/116
https://www.parisssd.org/domain/123 https://www.parisssd.org/domain/124 https://www.parisssd.org/domain/126
https://www.parisssd.org/domain/130 https://www.parisssd.org/domain/131 https://www.parisssd.org/domain/134
https://www.parisssd.org/domain/135 https://www.parisssd.org/domain/136 https://www.parisssd.org/domain/137
https://www.parisssd.org/domain/138 https://www.parisssd.org/domain/140 https://www.parisssd.org/domain/141
https://www.parisssd.org/domain/143 https://www.parisssd.org/domain/145 https://www.parisssd.org/domain/148
https://www.parisssd.org/domain/150 https://www.parisssd.org/domain/151 https://www.parisssd.org/domain/154
https://www.parisssd.org/domain/156 https://www.parisssd.org/domain/156# https://www.parisssd.org/domain/157
https://www.parisssd.org/domain/157# https://www.parisssd.org/domain/158 https://www.parisssd.org/domain/158#
https://www.parisssd.org/domain/159 https://www.parisssd.org/domain/159# https://www.parisssd.org/domain/161
https://www.parisssd.org/domain/161# https://www.parisssd.org/domain/162
https://www.parisssd.org/domain/162#
https://www.parisssd.org/domain/165
https://www.parisssd.org/domain/169
https://www.parisssd.org/domain/171
https://www.parisssd.org/domain/173
https://www.parisssd.org/domain/174
https://www.parisssd.org/domain/175
https://www.parisssd.org/domain/177
https://www.parisssd.org/domain/178
https://www.parisssd.org/domain/181
https://www.parisssd.org/domain/184
https://www.parisssd.org/domain/185
https://www.parisssd.org/domain/188
https://www.parisssd.org/domain/19
https://www.parisssd.org/domain/193
https://www.parisssd.org/domain/194
https://www.parisssd.org/domain/196
https://www.parisssd.org/domain/203
https://www.parisssd.org/domain/204
https://www.parisssd.org/domain/205
https://www.parisssd.org/domain/209
https://www.parisssd.org/domain/209#
https://www.parisssd.org/domain/210
https://www.parisssd.org/domain/211
https://www.parisssd.org/domain/212
https://www.parisssd.org/domain/213
https://www.parisssd.org/domain/214
https://www.parisssd.org/domain/215
https://www.parisssd.org/domain/216
https://www.parisssd.org/domain/217
https://www.parisssd.org/domain/218
https://www.parisssd.org/domain/221
https://www.parisssd.org/domain/222
https://www.parisssd.org/domain/225
https://www.parisssd.org/domain/227
https://www.parisssd.org/domain/228
https://www.parisssd.org/domain/230
https://www.parisssd.org/domain/231
https://www.parisssd.org/domain/235
https://www.parisssd.org/domain/235#
https://www.parisssd.org/domain/240
https://www.parisssd.org/domain/240#
https://www.parisssd.org/domain/242
https://www.parisssd.org/domain/243
https://www.parisssd.org/domain/247
https://www.parisssd.org/domain/247#
https://www.parisssd.org/domain/248
https://www.parisssd.org/domain/249
https://www.parisssd.org/domain/255
https://www.parisssd.org/domain/256

https://www.parisssd.org/domain/257
https://www.parisssd.org/domain/260
https://www.parisssd.org/domain/261
https://www.parisssd.org/domain/262
https://www.parisssd.org/domain/263
https://www.parisssd.org/domain/264
https://www.parisssd.org/domain/265
https://www.parisssd.org/domain/266
https://www.parisssd.org/domain/268
https://www.parisssd.org/domain/268#
https://www.parisssd.org/domain/27
https://www.parisssd.org/domain/271
https://www.parisssd.org/domain/276
https://www.parisssd.org/domain/276#
https://www.parisssd.org/domain/281
https://www.parisssd.org/domain/283
https://www.parisssd.org/domain/284
https://www.parisssd.org/domain/285
https://www.parisssd.org/domain/286
https://www.parisssd.org/domain/287
https://www.parisssd.org/domain/292
https://www.parisssd.org/domain/295
https://www.parisssd.org/domain/299
https://www.parisssd.org/domain/299#
https://www.parisssd.org/domain/303
https://www.parisssd.org/domain/305
https://www.parisssd.org/domain/308
https://www.parisssd.org/domain/309
https://www.parisssd.org/domain/310
https://www.parisssd.org/domain/311
https://www.parisssd.org/domain/313
https://www.parisssd.org/domain/314
https://www.parisssd.org/domain/315
https://www.parisssd.org/domain/318
https://www.parisssd.org/domain/320
https://www.parisssd.org/domain/322
https://www.parisssd.org/domain/327
https://www.parisssd.org/domain/331
https://www.parisssd.org/domain/337
https://www.parisssd.org/domain/337#
https://www.parisssd.org/domain/339
https://www.parisssd.org/domain/340
https://www.parisssd.org/domain/341
https://www.parisssd.org/domain/342
https://www.parisssd.org/domain/344
https://www.parisssd.org/domain/345
https://www.parisssd.org/domain/348
https://www.parisssd.org/domain/352
https://www.parisssd.org/domain/353
https://www.parisssd.org/domain/354
https://www.parisssd.org/domain/356
https://www.parisssd.org/domain/362
https://www.parisssd.org/domain/362#
https://www.parisssd.org/domain/363
https://www.parisssd.org/domain/363#
https://www.parisssd.org/domain/364
https://www.parisssd.org/domain/365
https://www.parisssd.org/domain/366
https://www.parisssd.org/domain/367
https://www.parisssd.org/domain/370
https://www.parisssd.org/domain/371
https://www.parisssd.org/domain/372
https://www.parisssd.org/domain/375
https://www.parisssd.org/domain/376
https://www.parisssd.org/domain/377
https://www.parisssd.org/domain/379
https://www.parisssd.org/domain/380
https://www.parisssd.org/domain/381
https://www.parisssd.org/domain/382
https://www.parisssd.org/domain/383
https://www.parisssd.org/domain/384
https://www.parisssd.org/domain/385
https://www.parisssd.org/domain/386

https://www.parisssd.org/domain/387
https://www.parisssd.org/domain/388
https://www.parisssd.org/domain/389
https://www.parisssd.org/domain/390
https://www.parisssd.org/domain/390#
https://www.parisssd.org/domain/391
https://www.parisssd.org/domain/391#
https://www.parisssd.org/domain/392
https://www.parisssd.org/domain/392#
https://www.parisssd.org/domain/393
https://www.parisssd.org/domain/393#
https://www.parisssd.org/domain/394
https://www.parisssd.org/domain/394#
https://www.parisssd.org/domain/397
https://www.parisssd.org/domain/397#
https://www.parisssd.org/domain/398
https://www.parisssd.org/domain/398#
https://www.parisssd.org/domain/399
https://www.parisssd.org/domain/399#
https://www.parisssd.org/domain/400
https://www.parisssd.org/domain/400#
https://www.parisssd.org/domain/401
https://www.parisssd.org/domain/401#
https://www.parisssd.org/domain/402
https://www.parisssd.org/domain/403
https://www.parisssd.org/domain/404
https://www.parisssd.org/domain/405
https://www.parisssd.org/domain/406
https://www.parisssd.org/domain/408
https://www.parisssd.org/domain/408#
https://www.parisssd.org/domain/413
https://www.parisssd.org/domain/413#
https://www.parisssd.org/domain/414
https://www.parisssd.org/domain/415
https://www.parisssd.org/domain/420
https://www.parisssd.org/domain/421
https://www.parisssd.org/domain/422
https://www.parisssd.org/domain/423
https://www.parisssd.org/domain/424
https://www.parisssd.org/domain/425
https://www.parisssd.org/domain/426
https://www.parisssd.org/domain/427
https://www.parisssd.org/domain/428
https://www.parisssd.org/domain/429
https://www.parisssd.org/domain/430
https://www.parisssd.org/domain/431
https://www.parisssd.org/domain/432
https://www.parisssd.org/domain/433
https://www.parisssd.org/domain/55 https://www.parisssd.org/domain/56
https://www.parisssd.org/domain/57 https://www.parisssd.org/domain/58
https://www.parisssd.org/domain/60 https://www.parisssd.org/domain/62
https://www.parisssd.org/domain/65 https://www.parisssd.org/domain/66
https://www.parisssd.org/domain/67 https://www.parisssd.org/domain/68
https://www.parisssd.org/domain/69 https://www.parisssd.org/domain/70
https://www.parisssd.org/domain/71 https://www.parisssd.org/domain/72
https://www.parisssd.org/domain/74 https://www.parisssd.org/domain/75
https://www.parisssd.org/domain/77 https://www.parisssd.org/domain/78
https://www.parisssd.org/domain/79 https://www.parisssd.org/domain/81
https://www.parisssd.org/domain/86 https://www.parisssd.org/domain/90
https://www.parisssd.org/domain/91 https://www.parisssd.org/domain/93
https://www.parisssd.org/domain/94 https://www.parisssd.org/domain/95
https://www.parisssd.org/domain/96
https://www.parisssd.org/errors/500.aspx?aspxerrorpath=/site/UserControls/Calendar/EventDetailWrapper.asp
x https://www.parisssd.org/harrisonc https://www.parisssd.org/inmanms https://www.parisssd.org/mcleese
https://www.parisssd.org/myview/ https://www.parisssd.org/parises https://www.parisssd.org/pressonl
https://www.parisssd.org/rheaes https://www.parisssd.org/site/.
https://www.parisssd.org/site/Default.aspx?PageID=11
https://www.parisssd.org/site/Default.aspx?PageID=1120
https://www.parisssd.org/site/Default.aspx?PageID=12&DomainID=9
https://www.parisssd.org/site/Default.aspx?PageID=13 https://www.parisssd.org/site/Default.aspx?PageID=1382
https://www.parisssd.org/site/Default.aspx?PageID=14&DomainID=10
https://www.parisssd.org/site/Default.aspx?PageID=2&DomainID=4
https://www.parisssd.org/site/Default.aspx?PageID=4269 https://www.parisssd.org/site/Default.aspx?PageID=9

https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=10&SectionMax=15&DirectoryType=6
https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=4&SectionMax=15&DirectoryType=6
https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=4&SectionMax=15&DirectoryType=6#
https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=8&SectionMax=15&DirectoryType=6
https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=9&SectionMax=15&DirectoryType=6
https://www.parisssd.org/site/Default.aspx?PageType=4&DomainID=10&ModuleInstanceID=2375&PageID=13
https://www.parisssd.org/site/Default.aspx?PageType=4&DomainID=268&ModuleInstanceID=2048&PageID=194
0
https://www.parisssd.org/site/Default.aspx?PageType=4&DomainID=268&ModuleInstanceID=2049&PageID=194
1
https://www.parisssd.org/site/Default.aspx?PageType=4&DomainID=268&ModuleInstanceID=2050&PageID=194
2 https://www.parisssd.org/site/Default.aspx?PageType=4&DomainID=8&ModuleInstanceID=1863&PageID=9
https://www.parisssd.org/site/Default.aspx?PageType=4&DomainID=9&ModuleInstanceID=1058&PageID=11
https://www.parisssd.org/site/Default.aspx?PageType=6&SiteID=10&SearchString=
https://www.parisssd.org/site/Default.aspx?PageType=6&SiteID=4&SearchString=
https://www.parisssd.org/site/Default.aspx?PageType=6&SiteID=4&SearchString=#
https://www.parisssd.org/site/Default.aspx?PageType=6&SiteID=8&SearchString=
https://www.parisssd.org/site/Default.aspx?PageType=6&SiteID=9&SearchString=
https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=10&IgnoreRedirect=true
https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=4
https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=4&IgnoreRedirect=true
https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=4&IgnoreRedirect=true#
https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=8&IgnoreRedirect=true
https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=9&IgnoreRedirect=true
https://www.parisssd.org/site/Default.aspx?PageType=9&SiteID=4
https://www.parisssd.org/site/Default.aspx?PageType=9&SiteID=4#
https://www.parisssd.org/site/SiteController.aspx/CancelledTermsOfUse
https://www.parisssd.org/site/SiteController.aspx/EndEmulationMode
https://www.parisssd.org/site/SiteController.aspx/EndPreviewConfigMode
https://www.parisssd.org/site/SiteController.aspx/EndPreviewMode
https://www.parisssd.org/site/SiteController.aspx/NotShowNotification
https://www.parisssd.org/site/SiteController.aspx/UpdateAgreedToTermsOfUse
https://www.parisssd.org/site/UserControls/Notification/NotificationWrapper.aspx?RedirectPath=http%3a%2f%2fwww.parisssd.org%2fdefault.aspx%3fPageID%3d1&IgnoreRedirect=
https://www.parisssd.org/site/UserControls/Notification/NotificationWrapper.aspx?RedirectPath=http%3a%2f%2fwww.parisssd.org%2fdefault.aspx%3fPageID
%3d1&IgnoreRedirect=true&NotificationType=U
https://www.parisssd.org/site/UserControls/Notification/NotificationWrapper.aspx?RedirectPath=http%3a%2f%2fwww.parisssd.org%2fmyview%2fdefault.aspx&IgnoreRedirect=true&NotificationType=U
https://www.parisssd.org/site/UserControls/SiteSearch/SearchResultsWrapper.aspx?PageIndex=
https://www.parisssd.org/site/UserControls/TermsOfUse/TermsOfUse.aspx?RedirectPath=http%3a%2f%2fwww.parisssd.org%2fdefault.aspx%3fPageID%3d1&IgnoreRedirect=true
https://www.parisssd.org/site/UserControls/TermsOfUse/TermsOfUse.aspx?RedirectPath=http%3a%2f%2fwww.parisssd.org%2fmyview%2fdefault.aspx&IgnoreRedirect=true
https://www.parisssd.org/site/default.aspx?PageType=14&DomainID=10&PageID=13&ModuleInstanceID=2375&IsMoreExpandedView=True
https://www.parisssd.org/site/default.aspx?PageType=14&DomainID=10&PageID=13&ModuleInstanceID=54&ViewID=606008db-225b-4ad2-8f7b-9ebac54372c1&IsMoreExpandedView=True
https://www.parisssd.org/site/default.aspx?PageType=14&DomainID=363&PageID=3962&ModuleInstanceID=4327&ViewID=1e008a8a-8e8a-4ca0-9472-a8f4a723a4a7&IsMoreExpandedView=True
https://www.parisssd.org/site/default.aspx?PageType=14&DomainID=398&PageID=4685&ModuleInstanceID=5227&ViewID=9d7780dc-000e-458b-ba39-cfc84059b040&IsMoreExpandedView=True
https://www.parisssd.org/site/default.aspx?PageType=14&DomainID=399&PageID=4688&ModuleInstanceID=5230&ViewID=9d7780dc-000e-458b-ba39-cfc84059b040&IsMoreExpandedView=True
https://www.parisssd.org/site/default.aspx?PageType=14&DomainID=4&PageID=1&ModuleInstanceID=3839&ViewID=1e008a8a-8e8a-4ca0-9472-a8f4a723a4a7&IsMoreExpandedView=True
https://www.parisssd.org/site/default.aspx?PageType=14&DomainID=4&PageID=1&ModuleInstanceID=3839&ViewID=1e008a8a-8e8a-4ca0-9472-a8f4a723a4a7&IsMoreExpandedView=True#
https://www.parisssd.org/site/default.aspx?PageType=14&DomainID=8&PageID=9&ModuleInstanceID=1863&IsMoreExpandedView=True https://www.parisssd.org/site/default.aspx?
PageType=14&DomainID=9&ModuleInstanceID=1043&PageID=11&ViewID=C83D46AC-74FE-4857-8C9A-
5922A80225E2&IsMoreExpandedView=True&GroupByField=&GroupYear=0&GroupMonth

https://www.parisssd.org/site/default.aspx?PageType=14&DomainID=9&PageID=11&ModuleInstanceID=1043&ViewID=c83d46ac-74fe-4857-8c9a-5922a80225e2&IsMoreExpandedView=True
https://www.parisssd.org/site/default.aspx?PageType=14&DomainID=9&PageID=11&ModuleInstanceID=1058&IsMoreExpandedView=True
https://www.parisssd.org/site/default.aspx?PageType=19
https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88-D30C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=10025&PageID=11
https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88-D30C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=10040&PageID=11
https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88D30C-497E-9316-
3F8874B3E108&RenderLoc=0&FlexDataID=10040&PageID=11&Comments=true
https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88-D30C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=10041&PageID=11
https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88D30C-497E-9316-
3F8874B3E108&RenderLoc=0&FlexDataID=10041&PageID=11&Comments=true
https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88-D30C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=10046&PageID=11
https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88D30C-497E-9316-
3F8874B3E108&RenderLoc=0&FlexDataID=10046&PageID=11&Comments=true
https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88-D30C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=10061&PageID=11
https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88D30C-497E-9316-
3F8874B3E108&RenderLoc=0&FlexDataID=10061&PageID=11&Comments=true
https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88-D30C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=8755&PageID=11
https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88D30C-497E-9316-
3F8874B3E108&RenderLoc=0&FlexDataID=9956&PageID=11&Comments=true
https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88-D30C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=9973&PageID=11
https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88D30C-497E-9316-
3F8874B3E108&RenderLoc=0&FlexDataID=9973&PageID=11&Comments=true

https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88D30C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=9974&PageID=11&Comments=true
https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88-D30C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=9983&PageID=11 https://www.parisssd.org/site/default.aspx?PageType=3&DomainID=9&ModuleInstanceID=1043&ViewID=6446EE88D30C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=9983&PageID=11&Comments=true https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=1058&ViewID=DEDCCD34-7C24-4AF2-812A-33C0075398BC&RenderLoc=0&FlexDataID=10248&PageID=11&Tag=&Comments=true
https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=1126&ViewID=503a3e79-9340-40fd-8d85-f3b476c2baf0&RenderLoc=0&FlexDataID=169&PageID=1096
https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=1126&ViewID=503a3e79-9340-40fd-8d85-f3b476c2baf0&RenderLoc=0&FlexDataID=169&PageID=1096#
https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=1126&ViewID=503a3e79-9340-40fd-8d85-f3b476c2baf0&RenderLoc=0&FlexDataID=170&PageID=1096
https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=1126&ViewID=503a3e79-9340-40fd-8d85-f3b476c2baf0&RenderLoc=0&FlexDataID=170&PageID=1096#
https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=1126&ViewID=503a3e79-9340-40fd-8d85-f3b476c2baf0&RenderLoc=0&FlexDataID=171&PageID=1096
https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=1126&ViewID=503a3e79-9340-40fd-8d85-f3b476c2baf0&RenderLoc=0&FlexDataID=172&PageID=1096
https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=1863&ViewID=DEDCCD34-7C24-4AF2-812A-33C0075398BC&RenderLoc=0&FlexDataID=9990&PageID=9&Tag=&Comments=true
https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=2375&ViewID=DEDCCD34-7C24-4AF2-812A-33C0075398BC&RenderLoc=0&FlexDataID=10215&PageID=13&Tag=&Comments=true
https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=3839&ViewID=C9E0416E-F0E7-4626-AA7BC14D59F72F85&RenderLoc=0&FlexDataID=10033&PageID=1&Comments=true
https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=3839&ViewID=C9E0416E-F0E7-4626-AA7BC14D59F72F85&RenderLoc=0&FlexDataID=10045&PageID=1&Comments=true
https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=3839&ViewID=C9E0416E-F0E7-4626-AA7BC14D59F72F85&RenderLoc=0&FlexDataID=10058&PageID=1&Comments=true
https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=3839&ViewID=C9E0416E-F0E7-4626-AA7BC14D59F72F85&RenderLoc=0&FlexDataID=10078&PageID=1&Comments=true
https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=3839&ViewID=C9E0416E-F0E7-4626-AA7BC14D59F72F85&RenderLoc=0&FlexDataID=10080&PageID=1&Comments=true https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=6754&ViewID=ed695a1c-ef13-4546-b4eb-4fefcdd4f389&RenderLoc=0&FlexDataID=9840&PageID=1&Comments=true
https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=6754&ViewID=ed695a1c-ef13-4546-b4eb-4fefcdd4f389&RenderLoc=0&FlexDataID=9943&PageID=1&Comments=true https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=6920&ViewID=5C8B25C6C8F8-4BD5-923B-8A7C70A93DDA&RenderLoc=0&FlexDataID=10060&PageID=1&Comments=true https://www.parisssd.org/site/default.aspx?pagetype=15&SiteID=
https://www.parisssd.org/site/handlers/filedownload.ashx?moduleinstanceid=2049&dataid=1503&FileName=PESLunch.htm
https://www.parisssd.org/site/handlers/filedownload.ashx?moduleinstanceid=3839&dataid=10045&FileName=
https://www.parisssd.org/site/handlers/filedownload.ashx?moduleinstanceid=3839&dataid=10065&FileName=October%204.PNG https://www.parisssd.org/site/handlers/filedownload.ashx?moduleinstanceid=3839&dataid=5660&FileName=
https://www.parisssd.org/site/handlers/filedownload.ashx?moduleinstanceid=3839&dataid=9681&FileName=
https://www.parisssd.org/site/handlers/filedownload.ashx?moduleinstanceid=3839&dataid=9924&FileName=
https://www.parisssd.org/site/handlers/filedownload.ashx?moduleinstanceid=3839&dataid=9927&FileName=
https://www.parisssd.org/site/handlers/filedownload.ashx?moduleinstanceid=3839&dataid=9944&FileName=
https://www.parisssd.org/site/mobile/default.aspx?DomainID=10 https://www.parisssd.org/site/mobile/default.aspx?DomainID=8
https://www.parisssd.org/site/mobile/default.aspx?DomainID=9
https://www.parisssd.org/ums/App_Themes/Schoolwires/StyleSheet.css
https://www.parisssd.org/ums/Users/SecurityController.aspx https://www.parisssd.org/ums/Users/Users.aspx
http://www.parisssd.org/default.aspx?PageID=1 http://www.parisssd.org/myview/default.aspx
http://www.parisssd.org/site/default.aspx?PageType=19

## 150010 External Links Discovered

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| **Finding #** | 5913860 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | a6d9e339-7916-4cbb-8640-f617a7e3270e | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

**Impact**

N/A

**Solution**
N/A

## Results

Number of links: 1001 https://www.google-analytics.com/analytics.js
https://help.blackboard.com/Terms_of_Use
https://www.tn.gov/content/dam/tn/health/documents/cedep/novel-coronavirus/Isolation-QuarantineRelease.pdf
https://fonts.gstatic.com/s/oswald/v40/TK3_WkUHHAIjg75cFRf3bXL8LICs1_FvsUZiYySUhiCXAA.woff
https://fonts.gstatic.com/s/oswald/v40/TK3_WkUHHAIjg75cFRf3bXL8LICs1xZosUZiYySUhiCXAA.woff
https://fonts.googleapis.com/css?family=Pathway%2BGothic%2BOne%7CArchivo%2BNarrow%3A400%2C700%7COswald%3A400%2C700%7COranienbaum%7CCarme
https://ajax.googleapis.com/ajax/libs/swfobject/2.2/swfobject.js
https://js-agent.newrelic.com/nr-1212.min.js
https://extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
https://extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
https://extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
https://extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js https://extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js https://extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
https://extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js https://extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
https://extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=0&SectionID=0&PageID=0&HitDate=1%2F14%2F2022+9%3A04%3A50+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.95.77&jsonp=jQuery300005101485847514542_1642215890677&_=1642215890678
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=0&SectionID=0&PageID=1&HitDate=1%2F14%2F2022+9%3A03%3A58+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.16.27&jsonp=jQuery30005758944685836372_1642215838604&_=1642215838605
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=0&SectionID=0&PageID=1&HitDate=1%2F14%2F2022+9%3A04%3A52+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.95.77&jsonp=jQuery30006135344724937886_1642215892617&_=1642215892618
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=0&SectionID=4&PageID=1&HitDate=1%2F14%2F2022+9%3A04%3A50+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.16.27&jsonp=jQuery30006693666739212087_1642215890611&_=1642215890612
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=6&SectionID=11&PageID=15&HitDate=1%2F14%2F2022+9%3A04%3A58+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.16.27&jsonp=jQuery300009969110870690201_1642215898963&_=1642215898964
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=6&SectionID=156&PageID=757&HitDate=1%2F14%2F2022+9%3A04%3A57+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.95.77&jsonp=jQuery30008858882303763935_1642215897602&_=1642215897603
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=6&SectionID=157&PageID=758&HitDate=1%2F14%2F2022+9%3A05%3A02+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.16.27&jsonp=jQuery300036758553354924806_1642215902968&_=1642215902969
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=6&SectionID=159&PageID=760&HitDate=1%2F14%2F2022+9%3A05%3A06+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.16.27&jsonp=jQuery30006630740250729695_1642215906767&_=1642215906768
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=6&SectionID=268&PageID=1943&HitDate=1%2F14%2F2022+9%3A05%3A00+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.95.77&jsonp=jQuery30007551692268491761_1642215900398&_=1642215900399
https://googleads.g.doubleclick.net/pagead/id
https://www.youtube.com/
https://www.youtube.com/api/stats/qoe?cpn=4mdvu4p5C2MKTuVT&el=embedded&ns=yt&fexp=23748146%2C23983296%2C24001373%2C24002022%2C24002025%2C24007246%2C24064557%2C24080738%2C24082661%2C24127418%2
0.000:ER&cmt=0.000:0.000,0.000:0.000&error=0.000:html5.missingapi:0.000:nocodecs.1;a6s.0&vis=0.000:0&bh=0.000:0.000
https://www.youtube.com/api/stats/qoe?cpn=4mdvu4p5C2MKTuVT&el=embedded&ns=yt&fexp=23748146%2C23983296%2C24001373%2C24002022%2C24002025%2C24007246%2C24064557%2C24080738%2C24082661%2C24127418%2

https://www.youtube.com/api/stats/qoe?cpn=BYJ1MTwWHGgSb-ZN&el=embedded&ns=yt&fexp=23748146%2C23983296%2C24001373%2C24002022%2C24002025%2C24007246%2C24064557%2C24080738%2C24082661%2C24127418%2C24129402%2C241353
1
0.000:ER&cmt=0.000:0.000,0.000:0.000&error=0.000:html5.missingapi:0.000:nocodecs.1;a6s.0&vis=0.000:0&bh=0.000:0.000
https://www.youtube.com/api/stats/qoe?cpn=BYJ1MTwWHGgSb-

ZN&el=embedded&ns=yt&fexp=23748146%2C23983296%2C24001373%2C24002022%2C24002025%2C24007246%2C24064557%2C24080738%2C24082661%2C24127418%2C24129402%2C24135311

https://www.youtube.com/api/stats/qoe?cpn=hvjaB6Lwry6-Mg-Y&el=embedded&ns=yt&fexp=23748146%2C23983296%2C24001373%2C24002022%2C24002025%2C24007246%2C24064557%2C24080738%2C24082661%2C24127418%2C24129402%2C24135310

https://www.youtube.com/api/stats/qoe?cpn=v8AbEZnmDEPAcv1d&el=embedded&ns=yt&fexp=23748146%2C23983296%2C24001373%2C24002022%2C24002025%2C24007246%2C24064557%2C24080738%2C24082661%2C24127418%20.000:ER&cmt=0.000:0.000,0.000:0.000&error=0.000:html5.missingapi:0.000:nocodecs.1;a6s.0&vis=0.000:0&bh=0.000:0.000
https://www.youtube.com/api/stats/qoe?cpn=v8AbEZnmDEPAcv1d&el=embedded&ns=yt&fexp=23748146%2C23983296%2C24001373%2C24002022%2C24002025%2C24007246%2C24064557%2C24080738%2C24082661%2C24127418%2

https://www.youtube.com/channel/UCb-d0cvJKJxTENMUBlM5YLA
https://www.youtube.com/channel/UCb-d0cvJKJxTENMUBlM5YLA?feature=emb_ch_name_ex
https://www.youtube.com/embed/7jXurafSDT0 https://www.youtube.com/generate_204?7DJ92g
https://www.youtube.com/generate_204?OTid3A
https://www.youtube.com/generate_204?VUtfuQ
https://www.youtube.com/signin?context=popup&next=https%3A%2F%2Fwww.youtube.com%2Fpost_login https://www.youtube.com/supported_browsers https://www.youtube.com/watch?v=7jXurafSDT0
https://www.youtube.com/watch?v=7jXurafSDT0&feature=emb_imp_woyt
https://www.youtube.com/youtubei/v1/log_event?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y9_11qcW8
https://www.blackboard.com/blackboard-web-community-manager-privacy-statement https://tsba.net/paris-board-of-education-policy-manual/
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Caf&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cam&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Car&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Caz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cbe&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cbg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cbn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cbs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cca&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cceb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cco&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ccs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ccy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cda&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cde&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cel&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ceo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ces&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cet&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ceu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cfa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cfi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cfr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cfy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cga&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cgd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cgl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cgu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cha&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Chaw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Chi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Chmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Chr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cht&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Chu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Chy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cid&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cig&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cis&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cit&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ciw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cja&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cjw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cka&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ckk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ckm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ckn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cko&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cku&hl=en&anno=0&ie=UTF8

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cky&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cla&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Clb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Clo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Clt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Clv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cmg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cmi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cmk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cml&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cmr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cms&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cmt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cmy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cne&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cnl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cno&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cny&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cpa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cpl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cps&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cpt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cro&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cru&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Csd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Csi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Csk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Csl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Csm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Csn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cso&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Csq&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Csr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cst&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Csu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Csv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Csw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cta&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cte&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ctg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cth&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ctl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ctr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cuk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cur&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cuz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cvi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cxh&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cyi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cyo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Czh-CN&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Czh-TW&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Czu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Caf&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cam&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Car&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Caz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cbe&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cbg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cbn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cbs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cca&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cceb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cco&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Ccs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Ccy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cda&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cde&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cel&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Ceo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Ces&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cet&hl=en&anno=0&ie=UTF8

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Ceu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cfa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cfi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cfr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cfy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cga&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cgd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cgl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cgu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cha&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Chaw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Chi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Chmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Chr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cht&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Chu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Chy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cid&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cig&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cis&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cit&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Ciw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cja&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cjw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cka&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Ckk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Ckm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Ckn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cko&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cku&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cky&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cla&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Clb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Clo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Clt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Clv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cmg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cmi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cmk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cml&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cmr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cms&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cmt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cmy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cne&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cnl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cno&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cny&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cpa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cpl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cps&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cpt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cro&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cru&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Csd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Csi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Csk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Csl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Csm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Csn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cso&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Csq&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Csr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cst&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Csu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Csv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Csw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cta&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cte&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Ctg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cth&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Ctl&hl=en&anno=0&ie=UTF8

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Ctr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cuk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cur&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cuz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cvi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cxh&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cyi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Cyo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Czh-CN&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Czh-TW&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FDomain%2F4&langpair=en%7Czu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Caf&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cam&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Car&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Caz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cbe&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cbg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cbn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cbs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cca&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cceb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cco&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Ccs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Ccy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cda&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cde&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cel&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Ceo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Ces&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cet&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Ceu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cfa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cfi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cfr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cfy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cga&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cgd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cgl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cgu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cha&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Chaw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Chi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Chmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Chr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cht&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Chu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Chy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cid&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cig&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cis&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cit&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Ciw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cja&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cjw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cka&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Ckk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Ckm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Ckn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cko&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cku&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cky&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cla&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Clb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Clo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Clt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Clv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cmg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cmi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cmk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cml&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cmr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cms&hl=en&anno=0&ie=UTF8

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cmt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cmy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cne&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cnl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cno&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cny&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cpa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cpl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cps&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cpt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cro&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cru&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Csd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Csi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Csk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Csl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Csm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Csn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cso&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Csq&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Csr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cst&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Csu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Csv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Csw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cta&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cte&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Ctg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cth&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Ctl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Ctr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cuk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cur&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cuz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cvi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cxh&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cyi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Cyo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Czh-CN&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Czh-TW&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2FPage%2F1&langpair=en%7Czu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Caf&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cam&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Car&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Caz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cbe&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cbg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cbn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cbs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cca&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cceb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cco&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Ccs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Ccy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cda&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cde&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cel&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Ceo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Ces&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cet&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Ceu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cfa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cfi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cfr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cfy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cga&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cgd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cgl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cgu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cha&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Chaw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Chi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Chmn&hl=en&anno=0&ie=UTF8

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Chr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cht&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Chu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Chy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cid&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cig&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cis&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cit&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Ciw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cja&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cjw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cka&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Ckk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Ckm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Ckn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cko&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cku&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cky&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cla&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Clb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Clo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Clt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Clv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cmg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cmi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cmk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cml&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cmr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cms&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cmt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cmy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cne&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cnl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cno&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cny&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cpa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cpl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cps&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cpt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cro&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cru&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Csd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Csi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Csk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Csl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Csm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Csn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cso&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Csq&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Csr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cst&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Csu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Csv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Csw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cta&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cte&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Ctg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cth&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Ctl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Ctr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cuk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cur&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cuz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cvi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cxh&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cyi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Cyo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Czh-CN&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Czh-TW&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F11&langpair=en%7Czu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Caf&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cam&hl=en&anno=0&ie=UTF8

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Car&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Caz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cbe&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cbg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cbn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cbs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cca&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cceb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cco&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Ccs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Ccy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cda&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cde&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cel&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Ceo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Ces&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cet&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Ceu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cfa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cfi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cfr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cfy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cga&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cgd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cgl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cgu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cha&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Chaw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Chi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Chmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Chr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cht&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Chu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Chy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cid&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cig&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cis&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cit&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Ciw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cja&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cjw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cka&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Ckk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Ckm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Ckn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cko&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cku&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cky&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cla&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Clb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Clo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Clt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Clv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cmg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cmi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cmk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cml&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cmr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cms&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cmt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cmy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cne&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cnl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cno&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cny&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cpa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cpl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cps&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cpt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cro&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cru&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Csd&hl=en&anno=0&ie=UTF8

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Csi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Csk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Csl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Csm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Csn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cso&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Csq&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Csr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cst&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Csu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Csv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Csw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cta&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cte&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Ctg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cth&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Ctl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Ctr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cuk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cur&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cuz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cvi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cxh&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cyi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Cyo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Czh-CN&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Czh-TW&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F156&langpair=en%7Czu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Caf&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cam&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Car&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Caz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cbe&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cbg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cbn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cbs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cca&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cceb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cco&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Ccs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Ccy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cda&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cde&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cel&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Ceo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Ces&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cet&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Ceu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cfa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cfi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cfr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cfy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cga&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cgd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cgl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cgu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cha&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Chaw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Chi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Chmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Chr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cht&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Chu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Chy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cid&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cig&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cis&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cit&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Ciw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cja&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cjw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cka&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Ckk&hl=en&anno=0&ie=UTF8

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Ckm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Ckn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cko&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cku&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cky&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cla&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Clb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Clo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Clt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Clv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cmg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cmi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cmk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cml&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cmr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cms&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cmt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cmy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cne&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cnl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cno&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cny&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cpa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cpl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cps&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cpt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cro&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cru&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Csd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Csi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Csk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Csl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Csm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Csn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cso&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Csq&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Csr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cst&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Csu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Csv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Csw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cta&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cte&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Ctg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cth&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Ctl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Ctr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cuk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cur&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cuz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cvi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cxh&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cyi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Cyo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Czh-CN&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Czh-TW&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F157&langpair=en%7Czu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Ccs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Ccy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Cel&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Cet&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Ceu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Cfr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Cfy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Cga&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Ckm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Cml&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Cnl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Cro&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Ctl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Cuk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Cur&hl=en&anno=0&ie=UTF8

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Cuz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Cxh&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Cyi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Cyo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F158&langpair=en%7Czu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Caf&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cam&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Car&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Caz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cbe&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cbg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cbn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cbs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cca&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cceb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cco&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Ccs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Ccy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cda&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cde&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cel&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Ceo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Ces&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cet&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Ceu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cfa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cfi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cfr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cfy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cga&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cgd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cgl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cgu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cha&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Chaw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Chi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Chmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Chr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cht&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Chu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Chy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cid&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cig&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cis&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cit&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Ciw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cja&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cjw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cka&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Ckk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Ckm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Ckn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cko&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cku&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cky&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cla&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Clb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Clo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Clt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Clv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cmg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cmi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cmk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cml&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cmr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cms&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cmt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cmy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cne&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cnl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cno&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cny&hl=en&anno=0&ie=UTF8

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cpa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cpl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cps&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cpt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cro&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cru&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Csd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Csi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Csk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Csl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Csm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Csn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cso&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Csq&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Csr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cst&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Csu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Csv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Csw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cta&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cte&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Ctg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cth&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Ctl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Ctr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cuk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cur&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cuz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cvi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cxh&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cyi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Cyo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Czh-CN&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Czh-TW&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F159&langpair=en%7Czu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Caf&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cam&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Car&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Caz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cbe&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cbg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cbn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cbs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cca&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cceb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cco&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Ccs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Ccy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cda&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cde&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cel&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Ceo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Ces&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cet&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Ceu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cfa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cfi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cfr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cfy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cga&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cgd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cgl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cgu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cha&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Chaw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Chi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Chmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Chr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cht&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Chu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Chy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cid&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cig&hl=en&anno=0&ie=UTF8

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cis&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cit&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Ciw&hl=en&anno=0&ie=UTF8

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cja&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cjw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cka&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Ckk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Ckm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Ckn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cko&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cku&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cky&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cla&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Clb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Clo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Clt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Clv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cmg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cmi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cmk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cml&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cmr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cms&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cmt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cmy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cne&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cnl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cno&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cny&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cpa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cpl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cps&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cpt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cro&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cru&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Csd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Csi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Csk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Csl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Csm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Csn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cso&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Csq&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Csr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cst&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Csu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Csv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Csw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cta&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cte&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Ctg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cth&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Ctl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Ctr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cuk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cur&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cuz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cvi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cxh&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cyi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Cyo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Czh-CN&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Czh-TW&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fdomain%2F268&langpair=en%7Czu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en%7Caf&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en%7Cam&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en

%7Car&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Caz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cbe&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cbg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cbn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cbs&hl=en&anno=0&ie=UTF8

%7Cca&hl=en&anno=0&ie=UTF8

%7Cceb&hl=en&anno=0&ie=UTF8

%7Cco&hl=en&anno=0&ie=UTF8

%7Ccs&hl=en&anno=0&ie=UTF8
%7Ccy&hl=en&anno=0&ie=UTF8

%7Cda&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cde&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cel&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Ceo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Ces&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cet&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Ceu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cfa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cfi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cfr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cfy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cga&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cgd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cgl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cgu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cha&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Chaw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Chi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Chmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Chr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cht&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Chu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en


https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en

%7Chy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cid&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cig&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cis&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cit&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Ciw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cja&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cjw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cka&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Ckk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Ckm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Ckn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cko&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cku&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cky&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cla&hl=en&anno=0&ie=UTF8

%7Clb&hl=en&anno=0&ie=UTF8

%7Clo&hl=en&anno=0&ie=UTF8

%7Clt&hl=en&anno=0&ie=UTF8

%7Clv&hl=en&anno=0&ie=UTF8
%7Cmg&hl=en&anno=0&ie=UTF8

%7Cmi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cmk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cml&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cmr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cms&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cmt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cmy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cne&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cnl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cno&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cny&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en

%7Cpa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cpl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cps&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cpt&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cro&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cru&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Csd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Csi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Csk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Csl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Csm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Csn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cso&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Csq&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Csr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cst&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Csu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Csv&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Csw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cta&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cte&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Ctg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cth&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Ctl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Ctr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Cuk&hl=en&anno=0&ie=UTF8

%7Cur&hl=en&anno=0&ie=UTF8

%7Cuz&hl=en&anno=0&ie=UTF8

%7Cvi&hl=en&anno=0&ie=UTF8

%7Cxh&hl=en&anno=0&ie=UTF8

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en

https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en

%7Cyi&hl=en&anno=0&ie=UTF8

%7Cyo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en%7CzhCN&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en%7CzhTW&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageType%3D7%26SiteID%3D4%26IgnoreRedirect%3Dtrue&langpair=en
%7Czu&hl=en&anno=0&ie=UTF8
https://bam-cell.nr-data.net/1/e84461d315?a=23252431&v=1212.e95d35c&to=Z1MEZEtSVkoFBxIKX14ZJ2NpHEtQEAFJB1VWVxNcTR1ZShQc&rst=2133&ck=1&ref=https://www.parisssd.org/Page/1&qt=15&ap=25&be=219&fe=2102&dc=307&af=err,xhr,ins&perf=%7B%22timing%22:%7B%22of%22:1642215892446,%22n%22:0,%22f%22:0,%22dn%22:0,%22dne%22:0,%22c%22:0,%22ce%22:0,%22rq%22:0,%22rp%22:0,%22rpe%22:284,%22dl%22:144,%22di%22:306,%22ds%22:306,%22de%22:308,%22dc%22:2086,%22l%22:2086,%22le%22:2102%7D,%22navigation%22:%7B%7D%7D&jsonp=NREUM.setToken https://bam-cell.nr-data.net/1/e84461d315?a=23252431&v=1212.e95d35c&to=Z1MEZEtSVkoFBxIKX14ZJ2NpHEtQEAFJB1VWVxNcTR1ZShQc&rst=2436&ck=1&ref=https://www.parisssd.org/Domain/4&ap=137&be=606&fe=2336&dc=714&af=err,xhr,ins&perf=%7B%22timing%22:%7B%22of%22:1642215890142,%22n%22:0,%22f%22:0,%22dn%22:0,%22dne%22:0,%22c%22:0,%22ce%22:0,%22rq%22:0,%22rp%22:0,%22rpe%22:678,%22dl%22:432,%22di%22:713,%22ds%22:713,%22de%22:715,%22dc%22:2332,%22l%22:2332,%22le%22:2338%7D,%22navigation%22:%7B%7D%7D&jsonp=NREUM.setToken
http://www.inmanschool.com/
http://www.rheaschool.com/
http://www.blackboard.com/
http://www.pariselementaryschool.com/

## 150020 Links Rejected By Crawl Scope or Exclusion List

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| **Finding #** | 5913851 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | dbfe4366-3e17-47a2-a547-1fa9ee7b3589 | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

**Impact**

Links listed here were neither crawled or tested by the Web application scanning engine.

**Solution**

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.e

### Results

Links not permitted:
(This list includes links from QIDs: 150010,150026,150041,150143,150170)

External links discovered:
https://www.google-analytics.com/analytics.js
https://help.blackboard.com/Terms_of_Use
https://www.tn.gov/content/dam/tn/health/documents/cedep/novel-coronavirus/Isolation-QuarantineRelease.pdf
https://fonts.gstatic.com/s/oswald/v40/TK3_WkUHHAIjg75cFRf3bXL8LICs1_FvsUZiYySUhiCXAA.woff
https://fonts.gstatic.com/s/oswald/v40/TK3_WkUHHAIjg75cFRf3bXL8LICs1xZosUZiYySUhiCXAA.woff
https://fonts.googleapis.com/css?family=Pathway%2BGothic%2BOne%7CArchivo%2BNarrow%3A400%2C700%7COswald%3A400%2C700%7COranienbaum%7CCarme
https://ajax.googleapis.com/ajax/libs/swfobject/2.2/swfobject.js https://js-agent.newrelic.com/nr-1212.min.js
https://extend.schoolwires.com/creative/scripts/creative/accessibility/creative.accessible.navigation.app.min.js
https://extend.schoolwires.com/creative/scripts/creative/responsive/creative-responsive-menu-v2/creative.responsive.menu.v2.min.js
https://extend.schoolwires.com/creative/scripts/creative/responsive/jacinda.viewFullSite.min.js
https://extend.schoolwires.com/creative/scripts/creative/rotate/cs.rs.photo.gallery.rotator.min.js https://extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/creativeIcons.v3.min.js https://extend.schoolwires.com/creative/scripts/creative/tools/creative-icons-v3/css/creativeIcons.min.css
https://extend.schoolwires.com/creative/scripts/creative/tools/creative-translate/creative.translate.min.js https://extend.schoolwires.com/creative/scripts/joel/mod-events/joel.mod-events.min.js
https://extend.schoolwires.com/creative/subscription_library/centralizedFiles/CSS/drt-default-css.css
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=0&SectionID=0&PageID=0&HitDate=1%2F14%2F2022+9%3A04%3A50+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.95.77&jsonp=jQuery30000510148584751454 2_1642215890677&_=1642215890678
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=0&SectionID=0&PageID=1&HitDate=1%2F14%2F2022+9%3A03%3A58+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.16.27&jsonp=jQuery30005758944685836372_1642215838604&_=1642215838605
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=0&SectionID=0&PageID=1&HitDate=1%2F14%2F2022+9%3A04%3A52+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.95.77&jsonp=jQuery30006135344724937886_1642215892617&_=1642215892618
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=0&SectionID=4&PageID=1&HitDate=1%2F14%2F2022+9%3A04%3A50+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.16.27&jsonp=jQuery30006693666739212087_1642215890611&_=1642215890612
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=6&SectionID=11&PageID=15&HitDate=1%2F14%2F2022+9%3A04%3A58+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.16.27&jsonp=jQuery300009969110870690201_1642215898963&_=1642215898964
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=6&SectionID=156&PageID=757&HitDate=1%2F14%2F2022+9%3A04%3A57+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.95.77&jsonp=jQuery30008858882303763935_1642215897602&_=1642215897603
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=6&SectionID=157&PageID=758&HitDate=1%2F14%2F2022+9%3A05%3A02+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.16.27&jsonp=jQuery30003675855335492 4806_1642215902968&_=1642215902969
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=6&SectionID=159&PageID=760&HitDate=1%2F14%2F2022+9%3A05%3A06+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.16.27&jsonp=jQuery30006630740250729695_1642215906767&_=1642215906768
https://analytics.schoolwires.com/analytics.asmx/Insert?AccountNumber=H%2Fj%2B%2FCzBuQdtlFJDdmlQwA%3D%3D&SessionID=ba9092dc-b3f7-4d49-9fccfe46f11a8e06&SiteID=4&ChannelID=6&SectionID=268&PageID=1943&HitDate=1%2F14%2F2022+9%3A05%3A00+PM&Browser=Safari+12.1&OS=Unknown&IPAddress=10.61.95.77&jsonp=jQuery30007551692268491761_1642215900398&_=1642215900399
https://googleads.g.doubleclick.net/pagead/id
https://www.youtube.com/
https://www.youtube.com/api/stats/qoe?cpn=4mdvu4p5C2MKTuVT&el=embedded&ns=yt&fexp=23748146%2C23983296%2C24001373%2C24002022%2C24002025%2C24007246%2C24064557%2C24080738%2C24082661%2C24127418%20.000:ER&cmt=0.000:0.000,0.000:0.000&error=0.000:html5.missingapi:0.000:nocodecs.1;a6s.0&vis=0.000:0&bh=0.000:0.000
https://www.youtube.com/api/stats/qoe?cpn=4mdvu4p5C2MKTuVT&el=embedded&ns=yt&fexp=23748146%2C23983296%2C24001373%2C24002022%2C24002025%2C24007246%2C24064557%2C24080738%2C24082661%2C24127418%2

https://www.youtube.com/api/stats/qoe?cpn=BYJ1MTwWHGgSb-ZN&el=embedded&ns=yt&fexp=23748146%2C23983296%2C24001373%2C24002022%2C24002025%2C24007246%2C24064557%2C24080738%2C24082661%2C24127418%2C24129402%2C2413531 0.000:ER&cmt=0.000:0.000,0.000:0.000&error=0.000:html5.missingapi:0.000:nocodecs.1;a6s.0&vis=0.000:0&bh=0.000:0.000
https://www.youtube.com/api/stats/qoe?cpn=BYJ1MTwWHGgSb-ZN&el=embedded&ns=yt&fexp=23748146%2C23983296%2C24001373%2C24002022%2C24002025%2C24007246%2C24064557%2C24080738%2C24082661%2C24127418%2C24129402%2C2413531

https://www.youtube.com/api/stats/qoe?cpn=hvjaB6Lwry6-MgY&el=embedded&ns=yt&fexp=23748146%2C23983296%2C24001373%2C24002022%2C24002025%2C24007246%2C24064557%2C24080738%2C24082661%2C24127418%2C24129402%2C24135310

https://www.youtube.com/api/stats/qoe?cpn=v8AbEZnmDEPAcv1d&el=embedded&ns=yt&fexp=23748146%2C23983296%2C24001373%2C24002022%2C24002025%2C24007246%2C24064557%2C24080738%2C24082661%2C24127418%20.000:ER&cmt=0.000:0.000,0.000:0.000&error=0.000:html5.missingapi:0.000:nocodecs.1;a6s.0&vis=0.000:0&bh=0.000:0.000
https://www.youtube.com/api/stats/qoe?cpn=v8AbEZnmDEPAcv1d&el=embedded&ns=yt&fexp=23748146%2C23983296%2C24001373%2C24002022%2C24002025%2C24007246%2C24064557%2C24080738%2C24082661%2C24127418%2

https://www.youtube.com/channel/UCb-d0cvJKJxTENMUBlM5YLA
https://www.youtube.com/channel/UCb-d0cvJKJxTENMUBlM5YLA?feature=emb_ch_name_ex
https://www.youtube.com/embed/7jXurafSDT0 https://www.youtube.com/generate_204?7DJ92g

https://www.youtube.com/generate_204?OTid3A
https://www.youtube.com/generate_204?VUtfuQ
https://www.youtube.com/signin?context=popup&next=https%3A%2F%2Fwww.youtube.com%2Fpost_login
https://www.youtube.com/supported_browsers https://www.youtube.com/watch?v=7jXurafSDT0
https://www.youtube.com/watch?v=7jXurafSDT0&feature=emb_imp_woyt
https://www.youtube.com/youtubei/v1/log_event?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y9_11qcW8
https://www.blackboard.com/blackboard-web-community-manager-privacy-statement https://tsba.net/paris-board-of-education-policy-manual/
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Caf&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cam&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Car&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Caz&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cbe&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cbg&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cbn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cbs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cca&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cceb&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cco&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ccs&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ccy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cda&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cde&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cel&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ceo&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ces&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cet&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ceu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cfa&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cfi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cfr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cfy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cga&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cgd&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cgl&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cgu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cha&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Chaw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Chi&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Chmn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Chr&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cht&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Chu&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Chy&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cid&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cig&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cis&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cit&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ciw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cja&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cjw&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cka&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ckk&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ckm&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Ckn&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cko&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cku&hl=en&anno=0&ie=UTF8
https://translate.google.com/translate?u=https%3A%2F%2Fwww.parisssd.org%2F&langpair=en%7Cky&hl=en&anno=0&ie=UTF8

## 150021 Scan Diagnostics

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| **Finding #** | 5913853 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | c59be862-5e4e-4316-8477-74ad6a54caac | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |

# WAS Web Application Report

**OWASP** -

**WASC** -

## Details

### Threat
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

### Impact
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

### Solution
No action is required.

## Results

Loaded 3 exclude list entries.
Loaded 0 allow list entries.
HTML form authentication unavailable, no WEBAPP entry found
Target web application page https://www.parisssd.org/ fetched. Status code:200, Content-Type:text/html, load time:2 milliseconds.
Batch #0 VirtualHostDiscovery: estimated time < 1 minute (70 tests, 0 inputs)
VirtualHostDiscovery: 70 vulnsigs tests, completed 69 requests, 3 seconds. Completed 69 requests of 70 estimated requests (98.5714%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 56 requests, 9 seconds. Completed 56 requests of 56 estimated requests (100%). All tests completed.
Maximum request count reached: 1000
Collected 80001 links overall in 0 hours 41 minutes duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 271) + files:(0 x 655) + directories:(9 x 100) + paths:(0 x 755) = total (900) Batch
#0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 755 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 783 requests, 26 seconds. Completed 783 requests of 900 estimated requests (87%). All tests completed.
Batch #0 WS enumeration: estimated time < 10 minutes (11 tests, 786 inputs)
WS enumeration: 11 vulnsigs tests, completed 1826 requests, 88 seconds. Completed 1826 requests of 8646 estimated requests (21.1196%). All tests completed.
Batch #1 URI parameter manipulation (no auth): estimated time < 30 minutes (82 tests, 163 inputs)
Batch #1 URI parameter manipulation (no auth): 82 vulnsigs tests, completed 15527 requests, 1223 seconds. Completed 15527 requests of 13366 estimated requests (116.168%). All tests completed.
Batch #1 Form parameter manipulation (no auth): estimated time < 1 minute (82 tests, 6 inputs)
Batch #1 Form parameter manipulation (no auth): 82 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 492 estimated requests (0%). All tests completed.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 10 minutes (8 tests, 163 inputs)
Batch #1 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 3368 requests, 320 seconds. Completed 3368 requests of 3912 estimated requests (86.0941%). All tests completed.
Batch #1 Form blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 6 inputs)
Batch #1 Form blind SQL manipulation (no auth): 8 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 144 estimated requests (0%). All tests completed.
Batch #1 URI parameter time-based tests (no auth): estimated time < 10 minutes (14 tests, 163 inputs)
Batch #1 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 2282 requests, 88 seconds. Completed 2282 requests of 2282 estimated requests (100%). All tests completed.
Batch #1 Form field time-based tests (no auth): estimated time < 1 minute (14 tests, 6 inputs)
Batch #1 Form field time-based tests (no auth): 14 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 84 estimated requests (0%). All tests completed.
Batch #1 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): estimated time < 1 minute (1 tests, 163 inputs)
Batch #1 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): 1 vulnsigs tests, completed 163 requests, 25 seconds. Completed 163 requests of 163 estimated requests (100%). All tests completed.
Batch #1 Form field time-based tests for Apache Struts Vulnerabilities (no auth): estimated time < 1 minute (1 tests, 6 inputs)
Batch #1 Form field time-based tests for Apache Struts Vulnerabilities (no auth): 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 6 estimated requests (0%). All tests completed.
Batch #2 URI parameter manipulation (no auth): estimated time < 10 minutes (82 tests, 62 inputs)
Batch #2 URI parameter manipulation (no auth): 82 vulnsigs tests, completed 5147 requests, 182 seconds. Completed 5147 requests of 5084 estimated requests (101.239%). All tests completed.
Batch #2 URI blind SQL manipulation (no auth): estimated time < 10 minutes (8 tests, 62 inputs)
Batch #2 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 1776 requests, 47 seconds. Completed 1776 requests of 1488 estimated requests (119.355%). All tests completed.
Batch #2 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 62 inputs)
Batch #2 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 868 requests, 12 seconds. Completed 868 requests of 868 estimated requests (100%). All tests completed.
Batch #2 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): estimated time < 1 minute (1 tests, 62 inputs)
Batch #2 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): 1 vulnsigs tests, completed 62 requests, 5 seconds. Completed 62 requests of 62 estimated requests (100%). All tests completed.
Batch #3 URI parameter manipulation (no auth): estimated time < 10 minutes (82 tests, 111 inputs)
Batch #3 URI parameter manipulation (no auth): 82 vulnsigs tests, completed 10652 requests, 820 seconds. Completed 10652 requests of 9102 estimated requests (117.029%). All tests completed.
Batch #3 Form parameter manipulation (no auth): estimated time < 10 minutes (82 tests, 33 inputs)
Batch #3 Form parameter manipulation (no auth): 82 vulnsigs tests, completed 3103 requests, 342 seconds. Completed 3103 requests of 2706 estimated requests (114.671%). All tests completed.

Batch #3 URI blind SQL manipulation (no auth): estimated time < 10 minutes (8 tests, 111 inputs)
Batch #3 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 1920 requests, 214 seconds. Completed 1920 requests of 2664 estimated requests (72.0721%). All tests completed.
Batch #3 Form blind SQL manipulation (no auth): estimated time < 10 minutes (8 tests, 33 inputs)
Batch #3 Form blind SQL manipulation (no auth): 8 vulnsigs tests, completed 528 requests, 71 seconds. Completed 528 requests of 792 estimated requests (66.6667%). All tests completed.
Batch #3 URI parameter time-based tests (no auth): estimated time < 10 minutes (14 tests, 111 inputs)
Batch #3 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 1526 requests, 61 seconds. Completed 1526 requests of 1554 estimated requests (98.1982%). All tests completed.
Batch #3 Form field time-based tests (no auth): estimated time < 1 minute (14 tests, 33 inputs)
Batch #3 Form field time-based tests (no auth): 14 vulnsigs tests, completed 462 requests, 142 seconds. Completed 462 requests of 462 estimated requests (100%). All tests completed.
Batch #3 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): estimated time < 1 minute (1 tests, 111 inputs)
Batch #3 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): 1 vulnsigs tests, completed 109 requests, 16 seconds. Completed 109 requests of 111 estimated requests (98.1982%). All tests completed.
Batch #3 Form field time-based tests for Apache Struts Vulnerabilities (no auth): estimated time < 1 minute (1 tests, 33 inputs)
Batch #3 Form field time-based tests for Apache Struts Vulnerabilities (no auth): 1 vulnsigs tests, completed 33 requests, 6 seconds. Completed 33 requests of 33 estimated requests (100%). All tests completed.
Batch #4 WebCgiOob: estimated time < 1 hour (54 tests, 1 inputs)
Batch #4 WebCgiOob: 54 vulnsigs tests, completed 583 requests, 64 seconds. Completed 583 requests of 44545 estimated requests (1.30879%). All tests completed.
No XML requests found. Skipping XXE tests.
Batch #4 DOM XSS exploitation: estimated time < 1 minute (4 tests, 1247 inputs)
Batch #4 DOM XSS exploitation: 4 vulnsigs tests, completed 1616 requests, 3615 seconds. No tests to execute.
Batch #4 HTTP call manipulation: estimated time < 1 minute (38 tests, 0 inputs)
Batch #4 HTTP call manipulation: 38 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Open Redirect analysis: estimated time < 1 minute (2 tests, 42 inputs)
Batch #4 Open Redirect analysis: 2 vulnsigs tests, completed 84 requests, 192 seconds. Completed 84 requests of 84 estimated requests (100%). All tests completed.
CSRF tests will not be launched because the scan is not successfully authenticated. Batch #4 File Inclusion analysis: estimated time < 10 minutes (1 tests, 755 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 9 requests, 3 seconds. Completed 9 requests of 755 estimated requests (1.19205%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 6 hours (46 tests, 15 inputs)
Batch #4 Cookie manipulation: 46 vulnsigs tests, completed 346208 requests, 53330 seconds. Completed 346208 requests of 319554 estimated requests (108.341%). XSS optimization removed 2233 links. All tests completed.
Batch #4 Header manipulation: estimated time < 3 hours (46 tests, 583 inputs)
Batch #4 Header manipulation: 46 vulnsigs tests, completed 35694 requests, 3934 seconds. Completed 35694 requests of 73458 estimated requests (48.591%). XSS optimization removed 16907 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 150 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 159 requests, 18 seconds. Completed 159 requests of 150 estimated requests (106%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 2 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 2 requests, 1 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #4 httpoxy detector: estimated time < 10 minutes (1 tests, 661 inputs)
Batch #4 httpoxy detector: 1 vulnsigs tests, completed 661 requests, 66 seconds. Completed 661 requests of 661 estimated requests (100%). All tests completed.
Batch #4 httpoxy detector(form): estimated time < 1 minute (1 tests, 2 inputs)
Batch #4 httpoxy detector(form): 1 vulnsigs tests, completed 2 requests, 1 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #4 Struts timebased detector: estimated time < 1 minute (1 tests, 199 inputs)
Batch #4 Struts timebased detector: 1 vulnsigs tests, completed 199 requests, 18 seconds. Completed 199 requests of 199 estimated requests (100%). All tests completed.
Login Brute Force manipulation estimated time: no tests enabled
Login Brute Force manipulation estimated time: no tests enabled
Batch #4 insecurely served cred forms detector (no auth): estimated time < 1 minute (1 tests, 1 inputs)
Batch #4 insecurely served cred forms detector (no auth): 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 200 requests, 12 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 271) + files:(0 x 655) + directories:(4 x 100) + paths:(11 x 755) = total (8705) Batch #5 Path XSS manipulation: estimated time < 30 minutes (15 tests, 755 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 7352 requests, 391 seconds. Completed 7352 requests of 8705 estimated requests (84.4572%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 271) + files:(0 x 655) + directories:(1 x 100) + paths:(0 x 755) = total (100) Batch #5 Tomcat Vuln manipulation: estimated time < 1 minute (1 tests, 755 inputs)
Batch #5 Tomcat Vuln manipulation: 1 vulnsigs tests, completed 24 requests, 1 seconds. Completed 24 requests of 100 estimated requests (24%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 271) + files:(0 x 655) + directories:(16 x 100) + paths:(0 x 755) = total (1600)
Batch #5 Time based path manipulation: estimated time < 10 minutes (16 tests, 767 inputs)
Batch #5 Time based path manipulation: 16 vulnsigs tests, completed 96 requests, 862 seconds. Completed 96 requests of 1600 estimated requests (6%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(4 x 271) + files:(18 x 655) + directories:(131 x 100) + paths:(18 x 755) = total (39564)
Batch #5 Path manipulation: estimated time < 1 hours (171 tests, 755 inputs)
Batch #5 Path manipulation: 171 vulnsigs tests, completed 6000 requests, 171 seconds. Completed 6000 requests of 39564 estimated requests (15.1653%). Module did not finish.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 5 hours (121 tests, 1 inputs)
Batch #5 WebCgiGeneric: 121 vulnsigs tests, completed 295 requests, 9 seconds. Completed 295 requests of 127595 estimated requests (0.2312%). All tests completed.
Total requests made: 451149
Average server response time: 0.67 seconds

Average browser load time: 0.67 seconds

150026 Maximum Number of Links Reached During Crawl

# WAS Web Application Report

| | | | |
|---|---|---|---|
| **Finding #** | 5913854 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | 013a0012-b163-46e2-a7ad-5c17c7d0c4b7 | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

## Details

### Threat
The maximum number of links specified for this scan has been reached. The links crawled to reach this threshold can include requests made via HTML form submissions and links requested in anonymous and authenticated states. Consequently, the list of links crawled (QID 150009) may reflect a lower number than the combination of links and forms requested during the crawl.

### Impact
Some links that lead to different areas of the site's functionality may have been missed.

### Solution
Increase the maximum number of links in order to ensure broader coverage of the Web application. It is important to note that increasing the number of links crawled can dramatically increase the time required to test the Web application.

## Results

Maximum request count reached: 1000

150028 Cookies Collected *https://www.parisssd.org*

| | | | |
|---|---|---|---|
| **Finding #** | 5913857 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | 76e6bb8f-624b-4e1b-b2f2-3da4519a17a5 | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

## Details

### Threat
The cookies listed in the Results section were set by the web application during the crawl phase.

### Impact
Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

### Solution
Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

# WAS Web Application Report

## Results

Total cookies: 22
PSN=LjAVScvfF4t8u12OcOc08A==; secure; HttpOnly; path=/ First set at URL: https://www.parisssd.org/
PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; secure; HttpOnly; path=/ First set at URL: https://www.parisssd.org/
CSAN=8/YyjPiDJwJtBZxSxX5+iA==; secure; HttpOnly; path=/ First set at URL: https://www.parisssd.org/
AccountID=Xogon24LhVEF1Gfd40nUZQ==; secure; HttpOnly; path=/ First set at URL: https://www.parisssd.org/
APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8; secure; HttpOnly; path=/ First set at URL: https://www.parisssd.org/
SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; secure; HttpOnly; path=/ First set at URL: https://www.parisssd.org/
RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fdefault.aspx%3FPageID%3D1; secure; path=/ First set at URL: https://www.parisssd.org/
YSC=0jSZpPP_uQM; secure; HttpOnly; domain=.youtube.com; path=/ First set at URL: https://www.youtube.com/embed/7jXurafSDT0
VISITOR_INFO1_LIVE=ijOnbOJwHss; secure; HttpOnly; expires=Thu, 14-Jul-2022 03:03:52 GMT; domain=.youtube.com; path=/ First set at URL: https://www.youtube.com/embed/7jXurafSDT0
SWScreenWidth=240; path=/ First set at URL: https://www.parisssd.org/
SWClientWidth=1024; path=/ First set at URL: https://www.parisssd.org/
SWPageNavState=; path=/ First set at URL: https://www.parisssd.org/
JSESSIONID=7fef3b37b811635f; secure; domain=.nr-data.net; SameSite=None; path=/ First set at URL: https://bam-cell.nr-data.net/1/e84461d315?a=23252431&v=1212.e95d35c&to=Z1MEZEtSVkoFBxIKX14ZJ2NpHEtQEAFJB1VWVxNcTR1ZShQc&rst=2436&ck=1&ref=https://www.parisssd.org/Domain/4&ap=137&be=606&fe=2336&dc=714&af=err,xhr,ins&perf=%7B%22timing%22:%7B%22of%22:1642215890142,%22n%22:0,%22f%22:0,%22dn%22:0,%22dne%22:0,%22c%22:0,%22ce%22:0,%22rq%22:0,%22rp%22:0,%22rpe%22:678,%22dl%22:432,%22di%22:713,%22ds%22:713,%22de%22:715,%22dc%22:2332,%22l%22:2332,%22le%22:2338%7D,%22navigation%22:%7B%7D%7D&jsonp=NREUM.setToken
PID="61e23f1808c0fb770c118759"; secure; HttpOnly; expires=Sun, 15-Jan-2023 03:27:20 GMT; SameSite=None; path=/ First set at URL: https://www.smore.com/g9jf1-welcome-to-7th-grade?embed=1
smore=30812589fdcf3e121b6ce9b11d0b82105801001cb8b6f376db344fa2a8b013b1b302c63e; path=/ First set at URL: https://www.smore.com/g9jf1-welcome-to-7th-grade?embed=1
RF="g9jf1"; expires=Sat, 22-Jan-2022 03:27:21 GMT; SameSite=Lax; path=/ First set at URL: https://www.smore.com/app/reporting/view/g9jf1?slug=&httpref=nb2hi4dthixs653xo4xhaylsnfzxg43efzxxezzpmrxw2yljnyxtgnrx&sep_type=
ARRAffinity=9a5f816afccb0c6428494c106734a76a9805f026440d5f77e2bdbeb85088d454; domain=www.warrencountyschools.org; path=/ First set at URL: http://www.warrencountyschools.org/userfiles/3125/LoveMyFirstGrade%5B1%5D.jpg
ASP.NET_SessionId=h1p0ta4u3hap11ay2nx2xkdk; secure; HttpOnly; SameSite=Lax; path=/ First set at URL: https://www.parisssd.org/cms/module/selectsurvey/TakeSurvey.aspx?SurveyID=108
SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; secure; expires=Sat, 05-Feb-2022 03:34:13 GMT; path=/ First set at URL: https://www.parisssd.org/cms/module/selectsurvey/TakeSurvey.aspx?SurveyID=108
SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; secure; expires=Tue, 25-Jan-2022 03:34:24 GMT; path=/ First set at URL: https://www.parisssd.org//cms/Module/SelectSurvey/TakeSurveyAction.aspx?DisplayHeader=
vuid=pl738660029.204287156; secure; expires=Mon, 15-Jan-2024 03:37:10 GMT; domain=.vimeo.com; SameSite=None; path=/ First set at URL: https://player.vimeo.com/video/654314314
_gat_BBTracker=1; expires=Sat, 15-Jan-2022 03:38:57 GMT; domain=parisssd.org; path=/ First set at URL: https://www.parisssd.org/Page/1940#sw-maincontent

## 150054 Email Addresses Collected

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| **Finding #** | 5938105 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | 23627230-ff79-4f56-97c0-08cc8d65dd32 | | |
| **Group** | Information Gathered | | |
| **CWE** | CWE-359 | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

## Details

### Threat

The email addresses listed in the Results section were collected from the returned HTML content during the crawl phase.

### Impact

Email addresses may help a malicious user with brute force and phishing attacks.

### Solution

Review the email list to see if they are all email addresses you want to expose.

## Results

Number of emails: 5 allyson.palmer@parisssd.org first seen at
https://www.parisssd.org/domain/137 angie.hawkins@parisssd.org first seen at
https://www.parisssd.org/Page/1171 carl.mcmaster@usablelife.com first seen at
https://www.parisssd.org/Page/2090 info-co@parisssd.org first seen at
https://www.parisssd.org/ info@parisssd.org first seen at
https://www.parisssd.org/site/Default.aspx?PageID=11

## 150066 Summary of .NET ViewState Fields

https://www.parisssd.org

| | | | |
|---|---|---|---|
| **Finding #** | 5938107 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | 38fb984d-43af-48a2-b173-617fcfcc6e1f | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**

One or more forms were detected that include a .NET ViewState field. Descriptive information about these fields is included in the Results section.

**Impact**

No specific security concerns are raised by this information. In general, the use of ViewState fields should be reviewed to ensure that they are implemented correctly within server-side code. ViewState objects should be encrypted or include an HMAC to prevent tampering. ViewState objects should not contain unnecessary static content that would make the field size large and therefore negatively impact performance.

**Solution**

This is merely informational data about the Web application. No further action is required.

### Results

__VIEWSTATE statistics:
Fields analyzed: 7
Average size (bytes): 533.14
Median size (bytes): 52.00
Maximum size (bytes): 1448.00
Approximate percentage of bytes used by __VIEWSTATE values within all pages inspected by the crawler: 0.00 (3732.00 out of 227995479.00)

## 150082 Protection against Clickjacking

https://www.parisssd.org

| | | | |
|---|---|---|---|
| **Finding #** | 5938095 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | 4047effe-52bf-4d30-9766-e471e02d7656 | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**

The URLs listed have protection against Clickjacking. The protection is implemented via the X-Frame-Options response header.

**Impact**

X-Frame-Options header is used to prevent framing of the page.

**Solution**

N/A

# WAS Web Application Report

## Results

https://www.parisssd.org/ https://www.parisssd.org/Domain/4
https://www.parisssd.org/Page/1 https://www.parisssd.org/domain/11
https://www.parisssd.org/domain/156 https://www.parisssd.org/domain/157
https://www.parisssd.org/domain/158 https://www.parisssd.org/domain/159
https://www.parisssd.org/domain/268
https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=4&IgnoreRedirect=true

### 150099 Cookies Issued Without User Consent

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| **Finding #** | 5938100 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | 9408b741-2b61-4281-b8a2-99770c91f727 | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

## Details

**Threat**
The cookies listed in the Results section were issued from the web application during the crawl without accepting any opt-in dialogs.

**Impact**
Cookies may be set without user explicitly agreeing to accept them.

**Solution**
Review the application to ensure that all cookies listed are supposed to be issued without user opt-in. If the EU Cookie law is applicable for this web application, ensure these cookies require user opt-in or have been classified as exempt by your organization.

## Results

Total cookies: 11
PSN=LjAVScvfF4t8u12OcOc08A==; secure; HttpOnly; path=/ First set at URL: https://www.parisssd.org/
PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; secure; HttpOnly; path=/ First set at URL: https://www.parisssd.org/
CSAN=8/YyjPiDJwJtBZxSxX5+iA==; secure; HttpOnly; path=/ First set at URL: https://www.parisssd.org/
AccountID=Xogon24LhVEF1Gfd40nUZQ==; secure; HttpOnly; path=/ First set at URL: https://www.parisssd.org/
APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8; secure; HttpOnly; path=/ First set at URL: https://www.parisssd.org/
SWSessionID=45254ece-d98c-47e1-b7e4-f6d06ba08145; secure; HttpOnly; path=/ First set at URL: https://www.parisssd.org/
RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fdefault.aspx%3FPageID%3D1; secure; path=/ First set at URL: https://www.parisssd.org/
CancelRedirectTo=; secure; expires=Sat, 15-Jan-2022 13:47:10 GMT; path=/ First set at URL: https://www.parisssd.org/
YSC=tcjkPPjVnzw; secure; HttpOnly; domain=.youtube.com; path=/ First set at URL: https://www.youtube.com/embed/7jXurafSDT0
VISITOR_INFO1_LIVE=iBzTqFQcBgs; secure; HttpOnly; expires=Thu, 14-Jul-2022 21:47:11 GMT; domain=.youtube.com; path=/ First set at URL: https://www.youtube.com/embed/7jXurafSDT0
JSESSIONID=7d6b1a333e23f159; secure; domain=.nr-data.net; SameSite=None; path=/ First set at URL: https://bam-cell.nr-data.net/1/e84461d315?
a=23252431&v=1212.e95d35c&to=Z1MEZEtSVkoFBxIKX14ZJ2NpHFxcAgUTD0QeVxVAQQ%3D%3D&rst=3124&ck=1&ref=https://www.parisssd.org/
&ap=81&be=573&fe=3100&dc=675&af=err,xhr,ins&perf=%7B%22timing%22:%7B%22of%22:1642283230156,%22n%22:0,%22f%22:0,%22dn%22:0,%22dne%22:0,%22c%22:0,%22ce%22:0,%22rq
%22:0,%22rp%22:0,%22rpe%22:644,%22dl%22:447,%22di%22:674,%22ds%22:674,%22de%22:675,%22dc%22:3096,%22l%22:3096,%22le%22:3100%7D,%22navigation%22:%7B%7D
%7D&jsonp=NREUM.setToken

### 150101 Third-party Cookies Collected

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| **Finding #** | 5913859 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | 387f631e-5d50-41d7-b780-f834c685aff1 | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |

| | |
|---|---|
| OWASP | - |
| WASC | - |

## Details

### Threat
The cookies listed in the Results section were received from third-party web application(s) during the crawl phase.

### Impact
Cookies may contain sensitive information about the user. Cookies sent via HTTP may be sniffed.

### Solution
Review cookie values to ensure that sensitive information such as passwords are not present within them.

## Results

Total cookies: 9
YSC=0jSZpPP_uQM; secure; HttpOnly; domain=.youtube.com; path=/ First set at URL: https://www.youtube.com/embed/7jXurafSDT0
VISITOR_INFO1_LIVE=ijOnbOJwHss; secure; HttpOnly; expires=Thu, 14-Jul-2022 03:03:52 GMT; domain=.youtube.com; path=/ First set at URL: https://www.youtube.com/embed/7jXurafSDT0
JSESSIONID=7fef3b37b811635f; secure; domain=.nr-data.net; SameSite=None; path=/ First set at URL: https://bam-cell.nr-data.net/1/e84461d315?a=23252431&v=1212.e95d35c&to=Z1MEZEtSVkoFBxIKX14ZJ2NpHEtQEAFJB1VWVxNcTR1ZShQc&rst=2436&ck=1&ref=https://www.parisssd.org/Domain/4&ap=137&be=606&fe=2336&dc=714&af=err,xhr,ins&perf=%7B%22timing%22:%7B%22of%22:1642215890142,%22n%22:0,%22f%22:0,%22dn%22:0,%22dne%22:0,%22c%22:0,%22ce%22:0,%22rq%22:0,%22rp%22:0,%22rpe%22:678,%22dl%22:432,%22di%22:713,%22ds%22:713,%22de%22:715,%22dc%22:2332,%22l%22:2332,%22le%22:2338%7D,%22navigation%22:%7B%7D%7D&jsonp=NREUM.setToken
PID="61e23f1808c0fb770c118759"; secure; HttpOnly; expires=Sun, 15-Jan-2023 03:27:20 GMT; SameSite=None; path=/ First set at URL: https://www.smore.com/g9jf1-welcome-to-7th-grade?embed=1
smore=30812589fdcf3e121b6ce9b11d0b82105801001cb8b6f376db344fa2a8b013b1b302c63e; path=/ First set at URL: https://www.smore.com/g9jf1-welcome-to-7th-grade?embed=1
RF="g9jf1"; expires=Sat, 22-Jan-2022 03:27:21 GMT; SameSite=Lax; path=/ First set at URL: https://www.smore.com/app/reporting/view/g9jf1?slug=&httpref=nb2hi4dthixs653xo4xhaylsnfzxg43efzxxezzpmrxw2yljnyxtgnrx&sep_type=
ARRAffinity=9a5f816afccb0c6428494c106734a76a9805f026440d5f77e2bdbeb85088d454; domain=www.warrencountyschools.org; path=/ First set at URL: http://www.warrencountyschools.org/userfiles/3125/LoveMyFirstGrade%5B1%5D.jpg
vuid=pl738660029.204287156; secure; expires=Mon, 15-Jan-2024 03:37:10 GMT; domain=.vimeo.com; SameSite=None; path=/ First set at URL: https://player.vimeo.com/video/654314314
_gat_BBTracker=1; expires=Sat, 15-Jan-2022 03:38:57 GMT; domain=parisssd.org; path=/ First set at URL: https://www.parisssd.org/Page/1940#sw-maincontent

## 150106 Content of crossdomain.xml

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| Finding # | 5938101 | Severity | Information Gathered - Level 1 |
| Unique # | 40fe3fc5-742a-458c-a571-26864a30422a | | |
| Group | Information Gathered | | |
| CWE | CWE-16, CWE-1032 | Detection Date | 15 Jan 2022 03:01 GMT |
| OWASP | - | | |
| WASC | - | | |

## Details

**Threat**
The content of the crossdomain.xml file appears in the Results section.

**Impact**
N/A

**Solution**
N/A

## Results

```
<?xml version="1.0" encoding="utf-8" ?>
<cross-domain-policy>
<site-control permitted-cross-domain-policies="none"/>
<!--<site-control permitted-cross-domain-policies="master-only"/>-->
<allow-http-request-headers-from domain="*" headers="*" secure="true"/> </cross-domain-
policy>
```

### 150115 Authentication Form found

https://www.parisssd.org

| | | | |
|---|---|---|---|
| **Finding #** | 5938103 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | d4b45baa-1c2c-4cd0-a7c0-26622f3a88aa | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

## Details

**Threat**
Authentication Form was found during the web application crawling.

**Impact**
N/A

**Solution**
N/A

## Results

Authentication form found at: https://www.parisssd.org/SignIn.aspx
Action uri: https://www.parisssd.org/SignIn.aspx
Fields: __VIEWSTATE, __VIEWSTATEGENERATOR, WasNoName_T_2_, WasNoName_P_3_

### 150126 Links With High Resource Consumption

https://www.parisssd.org

| | | | |
|---|---|---|---|
| **Finding #** | 5913856 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | c2259850-a738-4b27-8b99-e33e6ee4becc | | |
| **Group** | Information Gathered | | |

| | | | |
|---|---|---|---|
| CWE | - | Detection Date | 15 Jan 2022 03:01 GMT |
| OWASP | - | | |
| WASC | - | | |

## Details

### Threat
The list of links with lowest bytes/sec which are assumed to be resources with highest resource consumption. The links in the list have slower transfer times speeds to an average resource on the server. This may indicate that the links are more CPU or DB intensive than majority of links.

The latency of the network and file size have no effect on calculations.

### Impact
The links with high resource consumption could be used to perform DOS on the server by just performing GET Flooding. Attackers could more easily take the server down if there are huge resource hogs on it, performing less request.

### Solution
Find the root cause of resources slow download speed.

If the cause is a real CPU strain or complex DB queries performed, there may be a need for re-engineering of the web application or defense measures should be in place. Examples of defense against DOS that is targeted towards high resource consumption links are Load Balancers and Rate Limiters.

## Results

1854.100000 bytes/sec https://www.parisssd.org//site/UserControls/Calendar/CalendarSearchListWrapper.aspx?DomainID=
80956.300000 bytes/sec https://www.parisssd.org/cms/lib03/TN01920488/Centricity/Domain/4/PowerSchool/ParentPortalWelcome_files/colorschememapping.xml
107102.800000 bytes/sec https://www.parisssd.org/site/handlers/filedownload.ashx?moduleinstanceid=3839&dataid=10065&FileName=October%204.PNG
4268259.200000 bytes/sec https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-Light.woff?tiwypa
4444144.700000 bytes/sec https://www.parisssd.org/Static/GlobalAssets/webfonts/Opensans-Regular.woff
11381537.800000 bytes/sec https://www.parisssd.org//cms/lib/TN01920488/Centricity/Domain/9/Capture.PNG
13916534.100000 bytes/sec https://www.parisssd.org//cms/lib/TN01920488/Centricity/Domain/10/20727971_106138643438079_604361504663294569_n.jpg
17173881.600000 bytes/sec https://www.parisssd.org/cms/lib/TN01920488/Centricity/Domain/9/school%20messenger.JPG
28801040.300000 bytes/sec https://www.parisssd.org/Static/GlobalAssets/webfonts/Opensans-Regular.ttf
32082047.800000 bytes/sec https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-Light.ttf?tiwypa

## 150148 AJAX Links Crawled

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| Finding # | 5913852 | Severity | Information Gathered - Level 1 |
| Unique # | 9415c986-8893-493a-9ad2-54dc3fa1b7de | | |
| Group | Information Gathered | | |
| CWE | - | Detection Date | 15 Jan 2022 03:01 GMT |
| OWASP | - | | |
| WASC | - | | |

## Details

### Threat
The list of unique AJAX links crawled by the scanner appears in the Results section. The link may be either a URL with fragment (#) or a Selenium script. To open a URL with fragment, open it in browser. To open a Selenium script, use Qualys Browser Recorder Chrome extension. The number of AJAX links reported is limited to 1000.

### Impact

N/A

**Solution**
N/A

## Results

Number of ajax links: 362
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>id=MoreLinkButton3839</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>id=attachmentdialog-close</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>id=channel-navigation</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>id=pmi-3797</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>id=rs-photo-gallery-container-3797</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>id=sw-search-button</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>id=videodialog-close</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[10]/DIV[1]/BUTTON[1]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[11]/DIV[1]/BUTTON[1]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[12]/DIV[1]/BUTTON[1]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[13]/DIV[1]/BUTTON[1]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[14]/DIV[1]/BUTTON[1]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[15]/DIV[1]/BUTTON[1]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[1]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[100]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[101]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[102]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[103]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[104]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[105]</td><td></td></tr></tbody></table></body></html>

<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[10]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[11]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[12]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[13]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[14]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[15]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[16]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[17]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[18]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[19]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[1]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[20]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[21]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[22]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[23]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[24]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[25]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[26]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[27]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[28]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[29]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[2]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[30]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[31]</td><td></td></tr></tbody></table></body></html>

<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[32]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[33]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[34]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[35]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[36]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[37]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[38]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[39]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[3]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[40]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[41]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[42]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[43]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[44]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[45]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[46]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[47]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[48]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[49]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[4]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[50]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[51]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[52]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[53]</td><td></td></tr></tbody></table></body></html>

<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[54]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[55]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[56]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[57]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[58]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[59]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[5]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[60]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[61]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[62]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[63]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[64]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[65]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[66]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[67]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[68]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[69]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[6]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[70]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[71]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[72]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[73]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[74]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[75]</td><td></td></tr></tbody></table></body></html>

<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[76]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[77]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[78]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[79]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[7]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[80]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[81]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[82]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[83]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[84]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[85]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[86]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[87]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[88]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[89]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[8]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[90]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[91]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[92]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[93]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[94]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[95]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[96]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[97]</td><td></td></tr></tbody></table></body></html>

<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[98]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[99]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[9]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[3]/DIV[1]/DIV[2]/DIV[1]/DIV[1]/DIV[1]/A[1]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[3]/DIV[1]/DIV[2]/DIV[1]/DIV[1]/DIV[1]/A[2]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[3]/DIV[1]/DIV[2]/DIV[1]/DIV[1]/DIV[1]/A[3]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[3]/DIV[1]/DIV[3]/A[1]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[3]/DIV[1]/DIV[3]/A[2]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[3]/DIV[3]/DIV[1]/DIV[3]/A[3]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[6]/DIV[1]/BUTTON[1]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[7]/DIV[1]/BUTTON[1]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[8]/DIV[1]/BUTTON[1]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>click</td><td>xpath=//BODY[1]/DIV[9]/DIV[1]/BUTTON[1]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>fireEvent</td><td>id=sw-search-input</td><td>focus</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>fireEvent</td><td>id=ui-btn-signin</td><td>focus</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>fireEvent</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[1]/A[1]</td><td>focus</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>fireEvent</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]</td><td>blur</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>fireEvent</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[3]/DIV[2]/DIV[1]/DIV[1]/A[1]</td><td>focus</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>mouseOut</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>mouseOver</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]</td><td></td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>id=sw-search-button</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>id=sw-search-input</td><td>b</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[1]/A[1]</td><td>a</td></tr></tbody></table></body></html>

<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[100]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[101]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[102]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[103]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[104]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[105]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[10]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[11]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[12]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[13]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[14]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[15]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[16]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[17]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[18]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[19]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[1]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[20]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[21]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[22]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[23]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[24]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[25]/A[1]</td><td>a</td></tr></tbody></table></body></html>

<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[26]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[27]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[28]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[29]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[2]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[30]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[31]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[32]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[33]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[34]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[35]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[36]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[37]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[38]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[39]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[3]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[40]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[41]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[42]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[43]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[44]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[45]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[46]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[47]/A[1]</td><td>a</td></tr></tbody></table></body></html>

<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[48]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[49]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[4]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[50]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[51]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[52]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[53]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[54]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[55]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[56]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[57]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[58]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[59]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[5]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[60]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[61]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[62]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[63]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[64]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[65]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[66]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[67]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[68]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[69]/A[1]</td><td>a</td></tr></tbody></table></body></html>

<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[6]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[70]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[71]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[72]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[73]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[74]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[75]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[76]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[77]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[78]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[79]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[7]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[80]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[81]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[82]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[83]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[84]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[85]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[86]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[87]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[88]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[89]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[8]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[90]/A[1]</td><td>a</td></tr></tbody></table></body></html>

<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[91]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[92]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[93]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[94]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[95]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[96]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[97]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[98]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[99]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]/UL[1]/LI[9]/A[1]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]/DIV[3]/DIV[1]/DIV[1]/DIV[2]/DIV[2]/DIV[2]</td><td>a</td></tr></tbody></table></body></html>
<?xml version="1.0" encoding="UTF-8"?><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://selenium-ide.openqa.org/profiles/test-case"><title>replay</title></head><body><table><thead><tr><td colspan="3">AJAX
Link</td></tr></thead><tbody><tr><td>open</td><td>https://www.parisssd.org/</td><td></td></tr><tr><td>pause</td><td>1000</td><td></td></tr><tr><td>typeKeys</td><td>xpath=//BODY[1]</td><td>a</td></tr></tbody></table></body></html> https://www.parisssd.org/#sw-maincontent
https://www.parisssd.org/Domain/4#sw-maincontent https://www.parisssd.org/Page/1#sw-maincontent https://www.parisssd.org/Page/1096#sw-maincontent https://www.parisssd.org/Page/1432#sw-maincontent https://www.parisssd.org/Page/1737#sw-maincontent https://www.parisssd.org/Page/1931#sw-maincontent https://www.parisssd.org/Page/1940#sw-maincontent
https://www.parisssd.org/Page/1941#sw-maincontent https://www.parisssd.org/Page/1942#sw-maincontent https://www.parisssd.org/Page/1943#sw-maincontent
https://www.parisssd.org/Page/2#calendar1/20220115/month https://www.parisssd.org/Page/2#sw-maincontent https://www.parisssd.org/Page/2059#sw-maincontent
https://www.parisssd.org/Page/2060#sw-maincontent https://www.parisssd.org/Page/2162#sw-maincontent https://www.parisssd.org/Page/2163#sw-maincontent
https://www.parisssd.org/Page/2164#sw-maincontent https://www.parisssd.org/Page/2165#sw-maincontent https://www.parisssd.org/Page/2166#sw-maincontent
https://www.parisssd.org/Page/2327#sw-maincontent https://www.parisssd.org/Page/2380#sw-maincontent https://www.parisssd.org/Page/2751#sw-maincontent
https://www.parisssd.org/Page/3044#sw-maincontent https://www.parisssd.org/Page/3929#sw-maincontent https://www.parisssd.org/Page/3932#sw-maincontent
https://www.parisssd.org/Page/3933#sw-maincontent https://www.parisssd.org/Page/3936#sw-maincontent https://www.parisssd.org/Page/3960#sw-maincontent
https://www.parisssd.org/Page/3962#sw-maincontent https://www.parisssd.org/Page/4596#sw-maincontent https://www.parisssd.org/Page/4604#sw-maincontent
https://www.parisssd.org/Page/4606#sw-maincontent https://www.parisssd.org/Page/4608#sw-maincontent https://www.parisssd.org/Page/4609#sw-maincontent
https://www.parisssd.org/Page/4611#sw-maincontent https://www.parisssd.org/Page/4614#sw-maincontent https://www.parisssd.org/Page/4616#sw-maincontent
https://www.parisssd.org/Page/4626#sw-maincontent https://www.parisssd.org/Page/4628#sw-maincontent https://www.parisssd.org/Page/4629#sw-maincontent
https://www.parisssd.org/Page/4648#sw-maincontent https://www.parisssd.org/Page/4708#sw-maincontent https://www.parisssd.org/Page/4711#sw-maincontent
https://www.parisssd.org/Page/4715#sw-maincontent https://www.parisssd.org/Page/4719#sw-maincontent https://www.parisssd.org/Page/4729#sw-maincontent
https://www.parisssd.org/Page/4738#sw-maincontent https://www.parisssd.org/Page/4745#sw-maincontent https://www.parisssd.org/Page/5342#sw-maincontent
https://www.parisssd.org/Page/5344#sw-maincontent
https://www.parisssd.org/Page/5345#sw-maincontent https://www.parisssd.org/Page/5346#sw-maincontent https://www.parisssd.org/Page/5347#sw-maincontent
https://www.parisssd.org/Page/5348#sw-maincontent https://www.parisssd.org/Page/5349#sw-maincontent https://www.parisssd.org/Page/5350#sw-maincontent
https://www.parisssd.org/Page/5351#sw-maincontent https://www.parisssd.org/Page/5352#sw-maincontent https://www.parisssd.org/Page/5353#sw-maincontent
https://www.parisssd.org/Page/5354#sw-maincontent https://www.parisssd.org/Page/5451#sw-maincontent https://www.parisssd.org/Page/5452#sw-maincontent
https://www.parisssd.org/Page/757#sw-maincontent https://www.parisssd.org/Page/758#sw-maincontent https://www.parisssd.org/Page/760#sw-maincontent
https://www.parisssd.org/Page/761#sw-maincontent
https://www.parisssd.org/Static/GlobalAssets/webfonts/OpenSans-Light.svg?tiwypa#OpenSans-Light
https://www.parisssd.org/Static/GlobalAssets/webfonts/Opensans-Regular.svg#Opensans-Regular
https://www.parisssd.org/Static/GlobalAssets/webfonts/arrow-icon.svg?ta8730#icomoon
https://www.parisssd.org/domain/11#sw-maincontent https://www.parisssd.org/domain/156#sw-maincontent https://www.parisssd.org/domain/157#sw-maincontent
https://www.parisssd.org/domain/158#sw-maincontent https://www.parisssd.org/domain/159#sw-maincontent https://www.parisssd.org/domain/161#sw-maincontent

https://www.parisssd.org/domain/162#sw-maincontent https://www.parisssd.org/domain/209#sw-maincontent https://www.parisssd.org/domain/235#sw-maincontent
https://www.parisssd.org/domain/240#sw-maincontent https://www.parisssd.org/domain/247#sw-maincontent https://www.parisssd.org/domain/268#sw-maincontent
https://www.parisssd.org/domain/276#sw-maincontent https://www.parisssd.org/domain/299#sw-maincontent https://www.parisssd.org/domain/337#sw-maincontent
https://www.parisssd.org/domain/362#sw-maincontent https://www.parisssd.org/domain/363#sw-maincontent https://www.parisssd.org/domain/390#sw-maincontent
https://www.parisssd.org/domain/391#sw-maincontent https://www.parisssd.org/domain/392#sw-maincontent https://www.parisssd.org/domain/393#sw-maincontent
https://www.parisssd.org/domain/394#sw-maincontent https://www.parisssd.org/domain/397#sw-maincontent https://www.parisssd.org/domain/398#sw-maincontent
https://www.parisssd.org/domain/399#sw-maincontent https://www.parisssd.org/domain/400#sw-maincontent https://www.parisssd.org/domain/401#sw-maincontent
https://www.parisssd.org/domain/408#sw-maincontent https://www.parisssd.org/domain/413#sw-maincontent https://www.parisssd.org/domain/96#sw-maincontent
https://www.parisssd.org/site/Default.aspx?PageID=11#sw-maincontent
https://www.parisssd.org/site/Default.aspx?PageID=12&DomainID=9#calendar8/20220117/event/4855 https://www.parisssd.org/site/Default.aspx?PageID=13#sw-maincontent https://www.parisssd.org/site/Default.aspx?PageID=14&DomainID=10#calendar9/20220118/event/4942
https://www.parisssd.org/site/Default.aspx?PageID=14&DomainID=10#calendar9/20220120/event/4943
https://www.parisssd.org/site/Default.aspx?PageID=14&DomainID=10#calendar9/20220124/event/4944
https://www.parisssd.org/site/Default.aspx?PageID=2&DomainID=4#calendar1/20220117/event/4840
https://www.parisssd.org/site/Default.aspx?PageType=15&SiteID=4&SectionMax=15&DirectoryType=6#sw-maincontent
https://www.parisssd.org/site/Default.aspx?PageType=6&SiteID=4&SearchString=#sw-maincontent
https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=4&IgnoreRedirect=true#sw-maincontent https://www.parisssd.org/site/Default.aspx?PageType=9&SiteID=4#sw-maincontent
https://www.parisssd.org/site/default.aspx?PageType=14&DomainID=4&PageID=1&ModuleInstanceID=3839&ViewID=1e008a8a-8e8a-4ca0-9472-a8f4a723a4a7&IsMoreExpandedView=True#swmaincontent https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=1126&ViewID=503a3e79-9340-40fd-8d85-f3b476c2baf0&RenderLoc=0&FlexDataID=169&PageID=1096#sw-maincontent https://www.parisssd.org/site/default.aspx?PageType=3&ModuleInstanceID=1126&ViewID=503a3e79-9340-40fd-8d85-f3b476c2baf0&RenderLoc=0&FlexDataID=170&PageID=1096#sw-maincontent

Number of ajax links discarded due to crawl optimization: 27928
Smart Scan Optimizations - All Optimizations enabled.

## 150152 Forms Crawled

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| **Finding #** | 5913855 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | 50667f1b-60ee-40d1-9605-89a25bb481c7 | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**

The Results section lists the unique forms that were identified and submitted by the scanner. The forms listed in this QID do not include authentication forms (i.e. login forms), which are reported separately under QID 150115.

The scanner does a redundancy check on forms by inspecting the form fields. Forms determined to be the redundant based on identical form fields will not be tested. If desired, you can enable 'Include form action URI in form uniqueness calculation' in the WAS option profile to have the scanner also consider the form's action attribute in the redundancy check.

NOTE: Any regular expression specified under 'Redundant Links' are not applied to forms. Forms (unique or redundant) are not reported under QID 150140.

**Impact**

N/A

### Solution
N/A

## Results

Total internal forms seen (this count includes duplicate forms): 4

Crawled forms (Total: 2)
NOTE: This does not include authentication forms. Authentication forms are reported separately in QID 150115
Form #:1 Action URI:https://www.parisssd.org/ums/Users/SecurityController.aspx (found at: https://www.parisssd.org/ums/Users/Users.aspx)
Form Fields: __VIEWSTATE, __VIEWSTATEGENERATOR

Form #:2 Action URI:https://www.parisssd.org//cms/Module/SelectSurvey/TakeSurveyAction.aspx?DisplayHeader= (found at: https://www.parisssd.org/cms/module/selectsurvey/TakeSurvey.aspx?SurveyID=108)
Form Fields: cookieexists, AdminOrOwnerEditResponse, AdminOrOwnerResponseID, SurveyID, EmailAddressID, EmailMessageID, EID, ResponseType, SurveyComplete, DoneClicked and 23 more field(s).

NOTE: Forms with exactly the same form fields were considered identical even if they had different action URI. Only one such form is crawled, the other forms with exactly the same form fields are considered duplicate and are not crawled. If they are different forms and each of them should be crawled then change the scan settings accordingly.

The following forms were not crawled as their fields matched Form #1 above:
Form Action URI: https://www.parisssd.org/ums/App_Themes/Schoolwires/SecurityController.aspx
Form Action URI: https://www.parisssd.org/errors/500.aspx?aspxerrorpath=%2fsite%2fUserControls%2fCalendar%2fEventDetailWrapper.aspx

## 150170 Logout Links Discovered

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| **Finding #** | 5938102 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | ad0b3325-d885-45a1-97a3-c3544bb84a92 | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

## Details

### Threat
The logout links discovered by the scanner are provided in the Results section. These links were present on the web application, but were not crawled since crawling these links would terminate the active authenticated session and negatively impact the crawling.

Logout links are identified automatically based on common logout regex patterns used by web applications. If the automatic identification technique does not work for your web application, you can configure a custom Logout Regular Expression for the web app under 'Exclusions' in the WAS UI.

### Impact
N/A

### Solution
N/A

## Results

Number of logout links detected: 5
https://www.parisssd.org/site/handlers/filedownload.ashx?moduleinstanceid=5126&dataid=7282&FileName=Leave%20Without%20Pay%20Form.pdf
https://www.parisssd.org/site/handlers/filedownload.ashx?moduleinstanceid=5126&dataid=7283&FileName=Maternity%20Sick%20Leave%20Request%20Form.pdf
https://www.parisssd.org/site/handlers/filedownload.ashx?moduleinstanceid=5126&dataid=7286&FileName=PERLEAV_.pdf
https://www.parisssd.org/site/handlers/filedownload.ashx?moduleinstanceid=5126&dataid=7287&FileName=Request%20Personal%20Leave.pdf
https://www.parisssd.org/site/handlers/filedownload.ashx?moduleinstanceid=5126&dataid=7289&FileName=SICKLEAV_.pdf

# WAS Web Application Report

## 150172 Requests Crawled

https://www.parisssd.org

| | | | |
|---|---|---|---|
| **Finding #** | 5913862 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | 888bf594-9b92-477b-927f-21c0655dd0b7 | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

## Details

### Threat
The QID reports list of requests crawled by the Web application scanner appear in the Results section.

### Impact
N/A

### Solution
N/A

## Results

Number of crawled XHRs: 324
Method GET URI https://www.parisssd.org/Generator/TokenGenerator.ashx/ProcessRequest (Count: 2)
Method GET URI https://www.parisssd.org/GlobalUserControls/Attachment/AttachmentView.js (Count: 2)
Method GET URI https://www.parisssd.org/Static//GlobalAssets/Scripts/ThirdParty/galleria-custom-129_2520/galleria-1.2.9.min.js (Count: 1)
Method GET URI https://www.parisssd.org/Static//GlobalAssets/Scripts/ThirdParty/jquery.dropdown.js (Count: 1)
Method GET URI https://www.parisssd.org/Static//GlobalAssets/Scripts/ThirdParty/jquery.fullcalendar1.6.1.js (Count: 1)
Method GET URI https://www.parisssd.org/Static//GlobalAssets/Scripts/ThirdParty/jquery.listfilter.js (Count: 2)
Method GET URI https://www.parisssd.org/Static//GlobalAssets/Scripts/ThirdParty/mustache.js (Count: 2)
Method GET URI https://www.parisssd.org/Static//GlobalAssets/Scripts/Utilities_2560.js (Count: 2)
Method GET URI https://www.parisssd.org/Static//GlobalAssets/Scripts/min/ModuleViewRenderer_2460.js (Count: 2)
Method GET URI https://www.parisssd.org/Static//GlobalAssets/Scripts/min/external-combined.min.js (Count: 2)
Method GET URI https://www.parisssd.org/Static/GlobalAssets/Scripts/sw-ada.js (Count: 2)
Method GET URI https://www.parisssd.org/Static/GlobalAssets/WCM-2550/lib/flatpickr.js (Count: 2)
Method GET URI https://www.parisssd.org/Static/GlobalAssets/WCM-2550/lib/polyfill-assign.js (Count: 2)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642215942584 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217227772 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217227816 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217229762 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217233603 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217234798 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217236278 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217238558 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217240529 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217240788 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217244271 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217247270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217247907 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217249720 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217253681 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217253691 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217255327 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217259270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217259287 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217261047 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217265271 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217265325 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217266736 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217269692 (Count: 1)

Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217271270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217272772 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217274710 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217276270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217277791 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217280271 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217281802 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217283360 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217286817 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217289333 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217289443 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217294646 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217294755 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217296445 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217300897 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217302360 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217304270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217306294 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217307795 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217309346 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217312772 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217314270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217315270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217317675 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217320339 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217320788 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217323515 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217325348 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217326607 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217330270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217331706 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217331973 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217336569 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217336654 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217338270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217342368 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217342425 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217345772 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217348270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217349805 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217351503 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217353270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217354497 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217356269 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217358270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217359550 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217361565 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217363270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217365270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217366543 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217368283 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217370806 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217371361 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217372790 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217375280 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217379918 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217379929 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217382269 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/inmanms.txt?_=1642217386753 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642215938740 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217018270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217020707 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217022270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217023572 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217026270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217028763 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217028844 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217031270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217033270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217036875 (Count: 1)

Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217039529 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217039738 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217042270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217045803 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217045869 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217047768 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217051730 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217051794 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217053616 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217057270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217057333 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217058796 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217063270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217064316 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217064648 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217067914 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217070270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217070281 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217073519 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217075769 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217078274 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217080777 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217082381 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217084572 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217086757 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217089704 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217092344 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217094591 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217094902 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217098607 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217100680 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217100769 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217107270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217107325 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217109339 (Count: 1) Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217112711 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217112763 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217114270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217118282 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217119813 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217123270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217123291 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217124725 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217128271 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217128685 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217130271 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217133529 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217135280 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217135793 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217137947 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217140723 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217142849 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217144270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217146270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217147807 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217149487 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217151684 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217153737 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217155270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217157270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217159270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217160814 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217162278 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217164652 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217166309 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217167657 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217170521 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217175291 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217178270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217178283 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217180269 (Count: 1)

Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217220922 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642217220934 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642218119785 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642218120351 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642218125285 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642218126339 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642218126764 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642218129941 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642218132270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642218132489 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642218137281 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642218137606 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642218138922 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/parises.txt?_=1642218141518 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642215937352 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217386537 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217388269 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217391952 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217392393 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217398276 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217398287 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217399611 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217404769 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217405908 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217408648 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217409852 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217411303 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217413516 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217415270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217416846 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217418953 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217420754 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217422344 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217424291 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217425544 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217426926 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217429270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217430721 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217432335 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217433863 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217435738 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217437270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217438616 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217441270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217442874 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217444645 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217446398 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217448270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217450311 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217451698 (Count: 1) Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217453271 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217454524 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217456847 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217458594 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217459752 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217462270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217464270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217465786 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217468271 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217469743 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217471835 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217473737 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217475270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217476776 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217479585 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217482270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217483816 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217485759 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217486921 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217489619 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217490715 (Count: 1)

Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217494820 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217496919 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217496934 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217500270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217502896 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217503289 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217505270 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217508733 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217508817 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217510269 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217514691 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217514719 (Count: 1)
Method GET URI https://www.parisssd.org/cms/lib/TN01920488/Centricity/Template/9/setup/rheaes.txt?_=1642217949942 (Count: 1)

Number of External XHRs: 52

## 150176 JavaScript Libraries Detected

https://www.parisssd.org

| | | | |
|---|---|---|---|
| **Finding #** | 5938104 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | eb93ff2d-b18f-409b-99e1-dec05f1c8fba | | |
| **Group** | Information Gathered | | |
| **CWE** | CWE-200 | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**

The JavaScript libraries discovered by the scanner are provided in the Results section. The discovered libraries are reported only once based on the page on which they were first detected.

Each library is reported along with other information such as the URL of page on which it was first found, the version, and the URL of the .js file.

**Impact**

N/A

**Solution**

N/A

### Results

Number of unique JS libraries: 9
Javascript library : METAGeneratorReports
Version : Microsoft Visual Studio .NET 7.1
Found on the following page(only first page is reported):
https://www.parisssd.org/cms/module/selectsurvey/TakeSurvey.aspx?SurveyID=108
==========

Javascript library : METAGeneratorReports
Version : Microsoft Word 12
Found on the following page(only first page is reported):
https://www.parisssd.org/cms/lib03/TN01920488/Centricity/Domain/4/PowerSchool/ParentPortalWelcome.htm

==========

Javascript library : Mustache
Version : 0.5.0-dev

Found on the following page(only first page is reported):
https://www.parisssd.org/

==========

Javascript library : Raphael
Version : 2.0.1
Found on the following page(only first page is reported):
https://www.parisssd.org/site/UserControls/Calendar/CalendarPrint.aspx?ModuleInstanceID=1&PageID=2&Date=

==========

Javascript library : jQuery
Version : 3.0.0
Script uri : https://www.parisssd.org/Static/GlobalAssets/Scripts/min/jquery-3.0.0.min.js
Found on the following page(only first page is reported): https://www.parisssd.org/

==========

Javascript library : jQuery.migrate
Version : 1.4.1
Script uri : https://www.parisssd.org/Static//GlobalAssets/Scripts/min/jquery-migrate-1.4.1.min.js
Found on the following page(only first page is reported): https://www.parisssd.org/

==========

Javascript library : jQuery.ui.autocomplete
Version : 1.12.0
Script uri : https://www.parisssd.org/Static//GlobalAssets/Scripts/min/jquery-ui-1.12.0.min.js
Found on the following page(only first page is reported): https://www.parisssd.org/

==========

Javascript library : jQuery.ui.dialog
Version : 1.12.0
Script uri : https://www.parisssd.org/Static//GlobalAssets/Scripts/min/jquery-ui-1.12.0.min.js
Found on the following page(only first page is reported): https://www.parisssd.org/

==========

Javascript library : jQuery.ui.tooltip
Version : 1.12.0
Script uri : https://www.parisssd.org/Static//GlobalAssets/Scripts/min/jquery-ui-1.12.0.min.js
Found on the following page(only first page is reported): https://www.parisssd.org/

==========

## 150204 Missing header: X-XSS-Protection

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| **Finding #** | 5938111 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | 885c8409-4e9f-478a-81c8-4ebeb47b0a16 | | |
| **Group** | Information Gathered | | |
| **CWE** | CWE-16, CWE-1032 | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration | | |
| **WASC** | WASC-15 APPLICATION MISCONFIGURATION | | |

### Details

**Threat**

The X-XSS-Protection response header is not present.

**Impact**

The X-XSS-Protection response header provides a layer of protection against reflected cross-site scripting (XSS) attacks by instructing browsers to abort rendering a page in which a reflected XSS attack has been detected. This is a best-effort second line of defense measure which helps prevent an attacker from using evasion techniques to avoid the neutralization mechanisms that the filters use by default. When configured appropriately, browser-level XSS filters can provide additional layers of defense against web application attacks.

Note that HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security the X-XSS-Protection header should be set on 4xx and 5xx responses as well.

### Solution

It is recommend to set X-XSS-Protection header with value set to '1; mode=block' on all the relevant responses to activate browser's XSS filter.

**NOTE:** The X-XSS-Protection header is not supported by all browsers. Google Chrome and Safari are some of the browsers which support it, Firefox on the other hand does not support the header. X-XSS-Protection header does not guarantee a complete protection against XSS. For better protection against XSS attacks, the web application should use secure coding principles. Also, consider leveraging the Content-Security-Policy (CSP) header, which is supported by all browsers.

Using X-XSS-Protection could have unintended side effects, please understand the implications carefully before using it.

References:
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection
- https://blog.innerht.ml/the-misunderstood-x-xss-protection/
- https://www.mbsd.jp/blog/20160407.html
- https://www.chromium.org/developers/design-documents/xss-auditor

## Results

X-Xss-Protection: Header missing
Response headers on link: GET https://www.parisssd.org/cms/lib/TN01920488/Centricity/Domain/9/school%2520messenger.JPG response code: 400
Content-Type: text/html; charset=utf-8
Content-Length: 3420
Connection: keep-alive
Date: Sat, 15 Jan 2022 03:26:46 GMT
Cache-Control: private
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Content-Security-Policy: frame-ancestors 'self' https://*.ally.ac;
X-Frame-Options: SAMEORIGIN
X-Cache: Error from cloudfront
Via: 1.1 b014854bd0108b7ed0058504b69ccb5a.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: SFO53-C1
X-Amz-Cf-Id: 7C8KUaDQgawBh8xPeeWshaIZSGNQvlk2HK49D0k61wNZmkuCyUiZTw==
Set-Cookie: PSN=LjAVScvfF4t8u12OcOc08A==; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: CSAN=8/YyjPiDJwJtBZxSxX5+iA==; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: AccountID=Xogon24LhVEF1Gfd40nUZQ==; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; secure; HttpOnly; domain=www.parisssd.org; path=/
Set-Cookie: RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fsite%2FDefault.aspx%3FPageID%3D1382; secure; domain=www.parisssd.org; path=/ Set-Cookie: SWScreenWidth=240; domain=www.parisssd.org; path=/
Set-Cookie: SWClientWidth=1024; domain=www.parisssd.org; path=/ Set-Cookie: SWPageNavState=; domain=www.parisssd.org; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://www.parisssd.org/cms/lib/TN01920488/Centricity/Domain/9/school%2520messenger.JPG response code: 400

## 150247 Information Disclosure

https://www.parisssd.org

| Finding # | 5938106 | Severity | Information Gathered - Level 1 |
|---|---|---|---|

# WAS Web Application Report

| | |
|---|---|
| **Unique #** | 88be3abb-ed2f-4cf7-a70f-7c522b188c92 |
| **Group** | Information Gathered |
| **CWE** | CWE-200 |
| **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - |
| **WASC** | - |

## Details

### Threat
Information disclosure is an application weakness in revealing sensitive data, such as technical details of the system or environment.

This check reports the various technologies used by the web application based on the information available in different components of the Request-Response.

### Impact
An attacker may use sensitive data to exploit the target web application, its hosting network, or its users.

### Solution
Ensure that your web servers do not reveal any sensitive information about your technology stack and system details

Please review the issues reported below:

## Results

Number of technologies detected: 1
Technology name: IIS Matched
Components: header match:
Server:Microsoft-IIS/8.5
Matched links: Reporting only first 3 links
https://www.parisssd.org/
https://www.parisssd.org/Domain/4
https://www.parisssd.org/site/Default.aspx?PageType=7&SiteID=4&IgnoreRedirect=true

### 150277 Cookie without SameSite attribute

*https://www.parisssd.org*

| | |
|---|---|
| **Finding #** | 5938099 |
| **Severity** | Information Gathered - Level 1 |
| **Unique #** | 7eb71c63-a27c-4ef5-ba80-225e4acee657 |
| **Group** | Information Gathered |
| **CWE** | CWE-16, CWE-1032 |
| **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | A6 Security Misconfiguration |
| **WASC** | - |

## Details

### Threat
The cookies listed in the Results section are missing the SameSite attribute.

### Impact

The SameSite cookie attribute is an effective countermeasure against cross-site request forgery (CSRF) attacks. Note that a missing SameSite attribute does not mean the web application is automatically vulnerable to CSRF. The scanner will report QID 150071 if a CSRF vulnerability is detected.

**Solution**
Consider adding the SameSite attribute to the cookie(s) listed.

More information:
DZone article
OWASP CSRF Prevention Cheat Sheet

## Results

Total cookies: 13
SWClientWidth=1024; path=/; domain=www.parisssd.org | First set at URL: https://www.parisssd.org/
SWPageNavState=; path=/; domain=www.parisssd.org | First set at URL: https://www.parisssd.org/
SWScreenWidth=240; path=/; domain=www.parisssd.org | First set at URL: https://www.parisssd.org/
_gat_BBTracker=1; expires=Sat Jan 15 03:38:57 2022; path=/; domain=parisssd.org | First set at URL: https://www.parisssd.org/Page/1940#sw-maincontent
RedirectTo=http%3A%2F%2Fwww.parisssd.org%2Fdefault.aspx%3FPageID%3D1; path=/; domain=www.parisssd.org; secure | First set at URL: https://www.parisssd.org/
SelectSurveyASPAnonymousUserID=AnonymousUserID=1788; expires=Sat Feb 5 03:34:13 2022; path=/; domain=www.parisssd.org; max-age=1813877; secure | First set at URL: https://www.parisssd.org/cms/module/selectsurvey/TakeSurvey.aspx?SurveyID=108
SelectSurveyNetASPAdvancedCookie=Survey64.39.108.126, 130.176.157.81108=2713; expires=Tue Jan 25 03:34:24 2022; path=/; domain=www.parisssd.org; max-age=863488; secure | First set at URL: https://www.parisssd.org//cms/Module/SelectSurvey/TakeSurveyAction.aspx?DisplayHeader=
APIKey=08991e7a-6781-4289-ab2a-9d2425fd36b8; path=/; domain=www.parisssd.org; secure; httponly | First set at URL: https://www.parisssd.org/
AccountID=Xogon24LhVEF1Gfd40nUZQ==; path=/; domain=www.parisssd.org; secure; httponly | First set at URL: https://www.parisssd.org/
CSAN=8/YyjPiDJwJtBZxSxX5+iA==; path=/; domain=www.parisssd.org; secure; httponly | First set at URL: https://www.parisssd.org/
PSDB=uNDbgFqxPMInUVu5K8fPIiHjXaf850+fQPXkSEauRGA=; path=/; domain=www.parisssd.org; secure; httponly | First set at URL: https://www.parisssd.org/
PSN=LjAVScvfF4t8u12OcOc08A==; path=/; domain=www.parisssd.org; secure; httponly | First set at URL: https://www.parisssd.org/
SWSessionID=ba9092dc-b3f7-4d49-9fcc-fe46f11a8e06; path=/; domain=www.parisssd.org; secure; httponly | First set at URL: https://www.parisssd.org/

### 38116 SSL Server Information Retrieval

https://www.parisssd.org

| | | | |
|---|---|---|---|
| **Finding #** | 5938117 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | 313f5f3b-081a-4f5c-9285-20cb341ba894 | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

## Details

**Threat**

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

**Impact**
N/A

**Solution**
N/A

## SSL Data

**Flags** -

**Protocol** tcp

**Virtual Host** www.parisssd.org

**IP** 18.64.236.66

**Port** 443

**Result** #table cols="6" CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE SSLv2_PROTOCOL_IS_DISABLED _ _ _ _ _ SSLv3_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1.1_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1.2_PROTOCOL_IS_ENABLED _ _ _ _ _ TLSv1.2 COMPRESSION_METHOD None _ _ _ ECDHE-RSA-AES128-SHA256 ECDH RSA SHA256 AES(128) MEDIUM ECDHE-RSA-AES256-SHA384 ECDH RSA SHA384 AES(256) HIGH ECDHE-RSA-AES128-GCM-SHA256 ECDH RSA AEAD AESGCM(128) MEDIUM ECDHE-RSA-AES256-GCM-SHA384 ECDH RSA AEAD AESGCM(256) HIGH ECDHE-RSA-CHACHA20-POLY1305 ECDH RSA AEAD CHACHA20/POLY1305(256) HIGH TLSv1.3_PROTOCOL_IS_ENABLED _ _ _ _ _ TLS13-AES-128-GCM-SHA256 N/A N/A AEAD AESGCM(128) MEDIUM TLS13-AES-256-GCM-SHA384 N/A N/A AEAD AESGCM(256) HIGH TLS13-CHACHA20-POLY1305-SHA256 N/A N/A AEAD CHACHA20/POLY1305(256) HIGH

## Info List

**Info #1**

### Ciphers

| Name | Auth | Encryption | Grade | Key Exchange | Mac | Protocol |
|---|---|---|---|---|---|---|
| ECDHE-RSA-AES128-SHA256 | RSA | AES(128) | MEDIUM | ECDH | SHA256 | TLSv1.2 |
| ECDHE-RSA-AES128-SHA256 | RSA | AES(256) | HIGH | ECDH | SHA384 | TLSv1.2 |
| ECDHE-RSA-AES128-SHA256 | RSA | AESGCM(128) | MEDIUM | ECDH | AEAD | TLSv1.2 |
| ECDHE-RSA-AES128-SHA256 | RSA | AESGCM(256) | HIGH | ECDH | AEAD | TLSv1.2 |
| ECDHE-RSA-AES128-SHA256 | RSA | CHACHA20/POLY1305(256) | HIGH | ECDH | AEAD | TLSv1.2 |

**Info #2**

### Ciphers

| Name | Auth | Encryption | Grade | Key Exchange | Mac | Protocol |
|---|---|---|---|---|---|---|
| TLS13-AES-128-GCM-SHA256 | N/A | AESGCM(128) | MEDIUM | N/A | AEAD | TLSv1.3 |
| TLS13-AES-128-GCM-SHA256 | N/A | AESGCM(256) | HIGH | N/A | AEAD | TLSv1.3 |
| TLS13-AES-128-GCM-SHA256 | N/A | CHACHA20/POLY1305(256) | HIGH | N/A | AEAD | TLSv1.3 |

# WAS Web Application Report

## 38291 SSL Session Caching Information

https://www.parisssd.org

| | | | |
|---|---|---|---|
| **Finding #** | 5938114 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | a8c30e0f-8971-4339-b225-44c38815e9fe | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

**Impact**

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

**Solution**

N/A

### SSL Data

| | |
|---|---|
| **Flags** | - |
| **Protocol** | tcp |
| **Virtual Host** | www.parisssd.org |
| **IP** | 18.64.236.66 |
| **Port** | 443 |
| **Result** | TLSv1.2 session caching is enabled on the target. TLSv1.3 session caching is disabled on the target. |
| **OWASP** | - |
| **WASC** | - |

### Details

**Threat**

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

**Impact**

N/A

**Solution**

N/A

# WAS Web Application Report

## SSL Data

| | |
|---|---|
| **Flags** | - |
| **Protocol** | tcp |
| **Virtual Host** | www.parisssd.org |
| **IP** | 18.64.236.66 |
| **Port** | 443 |
| **Result** | #table cols=2 my_version target_version 0304 0303 0399 0303 0400 0303 0499 0303 |

38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| **Finding #** | 5938118 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | 3b23fd75-e751-4673-9cd5-38ad1d661fdc | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

## Details

**Threat**

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

**Impact**

N/A

**Solution**

N/A

## SSL Data

| | |
|---|---|
| **Flags** | - |
| **Protocol** | tcp |
| **Virtual Host** | www.parisssd.org |
| **IP** | 18.64.236.66 |
| **Port** | 443 |
| **Result** | #table cols="6" NAME GROUP KEY-SIZE FORWARD-SECRET CLASSICAL-STRENGTH QUANTUM-STRENGTH TLSv1.2 _ _ _ _ _ ECDHE x25519 256 yes 128 low ECDHE secp256r1 256 yes 128 low ECDHE secp384r1 384 yes 192 low TLSv1.3 _ _ _ _ _ ECDHE x25519 256 yes 128 low ECDHE secp256r1 256 yes 128 low ECDHE secp384r1 384 yes 192 low |

## Info List

**Info #1**

### Kexs

| Kex | Group | Protocol | Key Size | | Classical | Quantum |
|---|---|---|---|---|---|---|
| ECDHE | | TLSv1.2 | 256 | yes | 128 | low |

| | | | | | | |
|---|---|---|---|---|---|---|
| ECDHE | | TLSv1.2 | 256 | yes | 128 | low |
| ECDHE | | TLSv1.2 | 384 | yes | 192 | low |
| ECDHE | | TLSv1.3 | 256 | yes | 128 | low |
| ECDHE | | TLSv1.3 | 256 | yes | 128 | low |
| ECDHE | | TLSv1.3 | 384 | yes | 192 | low |



## 38706 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

| | | | |
|---|---|---|---|
| **Finding #** | 5938119 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | 7cf2bfed-1188-40b5-a71b-fa982eb7c284 | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |
| **WASC** | - | | |

### Details

**Threat**

The following is a list of detected SSL/TLS protocol properties.

**Impact**

Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of nonAEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

**Solution**

N/A

### SSL Data

| | |
|---|---|
| **Flags** | - |
| **Protocol** | tcp |
| **Virtual Host** | www.parisssd.org |

# WAS Web Application Report

| | |
|---|---|
| **IP** | 18.64.236.66 |
| **Port** | 443 |
| **Result** | #table cols="2" NAME STATUS TLSv1.2 _ Extended_Master_Secret no Encrypt_Then_MAC no Heartbeat no Truncated_HMAC no Cipher_priority_controlled_by server OCSP_stapling no SCT_extension no TLSv1.3 _ Heartbeat no Cipher_priority_controlled_by server OCSP_stapling no SCT_extension no |

## Info List

**Info #1**

### Props

| Name | Value | Protocol |
|---|---|---|
| Extended Master Secret | no | TLSv1.2 |
| Encrypt Then MAC | no | TLSv1.2 |
| Heartbeat | no | TLSv1.2 |
| Truncated HMAC | no | TLSv1.2 |
| Cipher priority controlled by | server | TLSv1.2 |
| OCSP stapling | no | TLSv1.2 |
| SCT extension | no | TLSv1.2 |
| Heartbeat | no | TLSv1.3 |
| Cipher priority controlled by | server | TLSv1.3 |
| OCSP stapling | no | TLSv1.3 |
| SCT extension | no | TLSv1.3 |

38718 Secure Sockets Layer (SSL) Certificate Transparency Information



| | | | |
|---|---|---|---|
| **Finding #** | 5938113 | **Severity** | Information Gathered - Level 1 |
| **Unique #** | 3dafbf7f-51d2-46ed-b370-82e46da48ee4 | | |
| **Group** | Information Gathered | | |
| **CWE** | - | **Detection Date** | 15 Jan 2022 03:01 GMT |
| **OWASP** | - | | |

| | |
|---|---|
| WASC | - |

## Details

### Threat

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

### Impact

N/A

### Solution

N/A

## SSL Data

| | |
|---|---|
| Flags | - |
| Protocol | tcp |
| Virtual Host | www.parisssd.org |
| IP | 18.64.236.66 |
| Port | 443 |
| Result | #table cols="6" Source Validated Name URL ID Time Certificate_#0 _ CN=www.parisssd.org _ _ _ Certificate no (unknown) (unknown) 2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784 Thu_01_Jan_1970_12:00:00_AM_GMT Certificate yes DigiCert_Nessie2022_Log nessie2022.ct.digicert.com/log/ 51a3b0f5fd01799c566db837788f0ca47acc1b27cbf79e88429a0dfed48b05e5 Fri_23_Jul_2021_06:14:00_PM_GMT Certificate no (unknown) (unknown) 41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6 Thu_01_Jan_1970_12:00:00_AM_GMT |

## Info List

### Info #1

Certificate Fingerprint:B75E72200C4FFB561C0303B5A72B17AA6FBED9D25B2A6E44589FD608A9BE2718

## 42350 TLS Secure Renegotiation Extension Support Information

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| Finding # | 5938115 | Severity | Information Gathered - Level 1 |
| Unique # | 2d5ccb73-0ab4-42fd-b405-7b1daa462f70 | | |
| Group | Information Gathered | | |
| CWE | - | Detection Date | 15 Jan 2022 03:01 GMT |
| OWASP | - | | |

| | |
|---|---|
| WASC | - |

## Details

**Threat**

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

**Impact**

N/A

**Solution**

N/A

## SSL Data

| | |
|---|---|
| Flags | - |
| Protocol | tcp |
| Virtual Host | www.parisssd.org |
| IP | 18.64.236.66 |
| Port | 443 |
| Result | TLS Secure Renegotiation Extension Status: supported. |

## 86002 SSL Certificate - Information

*https://www.parisssd.org*

| | | | |
|---|---|---|---|
| Finding # | 5938112 | Severity | Information Gathered - Level 1 |
| Unique # | 7b6494e7-9ab5-45bb-812f-064c5225fdc0 | | |
| Group | Information Gathered | | |
| CWE | - | Detection Date | 15 Jan 2022 03:01 GMT |
| OWASP | - | | |
| WASC | - | | |

## Details

**Threat**

SSL certificate information is provided in the Results section.

**Impact**

N/A

**Solution**

N/A

## SSL Data

| | |
|---|---|
| Flags | - |
| Protocol | tcp |

# WAS Web Application Report

| | |
|---|---|
| **Virtual Host** | www.parisssd.org |
| **IP** | 18.64.236.66 |
| **Port** | 443 |
| **Result** | #table cols="2" NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2) (0)Serial_Number _01:9d:e7:6d:25:96:25:e7:ff:d3:92:ea:ac:b4:0b:1a_ (0)Signature_Algorithm sha256WithRSAEncryption (0)ISSUER_NAME _ countryName US _organizationName Amazon _organizationalUnitName Server_CA_1B _commonName Amazon (0)SUBJECT_NAME _ commonName www.parisssd.org (0)Valid_From Jul_23_00:00:00_2021_GMT (0)Valid_Till Aug_21_23:59:59_2022_GMT (0)Public_Key_Algorithm rsaEncryption (0)RSA_Public_Key (2048_bit) (0) _RSA_Public-Key:_(2048_bit) (0) _Modulus: (0) _00:b7:b6:fb:1b:08:7a:c8:a4:5e:86:a9:5b:e2:94: (0) _e6:18:af:9e:0d:b1:8d:bc:1e:43:f3:2b:6b:83:f2: (0) _41:63:9a:0b:77:41:f9:c0:af:ee:7f:37:92:3f:f4: (0) _6f:01:55:aa:1d:93:0f:24:f1:6d:01:c3:48:9d:2e: (0) _f6:fc:45:d3:c2:c8:66:e7:78:d2:c0:b0:5d:78:00: (0) _10:5f:e3:51:a8:a0:8c:1d:2e:8f:32:41:47:2f:9b: (0) _b9:67:08:04:89:88:30:3d:31:d2:59:a1:f6:d7:ba: (0) _3d:ab:b9:72:5a:ad:20:10:b8:0c:8f:76:40:05:14: (0) _e4:02:3a:e3:31:14:f4:4d:5d:d5:80:6c:cf:57:23: (0) _7d:cf:5f:46:1e:08:46:f0:30:99:b9:36:3d:0b:b4: (0) _04:08:6f:d1:7c:99:fe:51:cd:18:4a:82:20:47:5a: (0) _ab:b5:68:a4:24:70:22:a7:c3:08:f1:5b:c0:18:7d: (0) _99:fe:2a:13:b1:da:1c:50:51:df:e3:49:3b:f1:17: (0) _1c:04:d5:99:d7:1c:84:bf:5c:30:f5:83:45:07:3e: (0) _f4:2e:c8:77:31:4a:59:2b:10:61:fc:72:0d:a5:94: (0) _55:b3:a5:6a:7e:01:78:0e:d4:1b:1f:4d:bc:be:60: (0) _ef:e6:96:bc:58:29:4a:e3:6c:6f:c7:7e:2a:87:e0: (0) _c7:71 (0) _Exponent:_65537_(0x10001) (0)X509v3_EXTENSIONS _ (0)X509v3_Authority_Key_Identifier _keyid:59:A4:66:06:52:A0:7B:95:92:3C:A3:94:07:27:96:74:5B:F9:3D:D0 (0)X509v3_Subject_Key_Identifier _1D:5B:C5:2F:AE:73:C0:F1:72:D6:A0:F3:FD:C3:79:8F:AD:6C:39:ED (0)X509v3_Subject_Alternative_Name _DNS:www.parisssd.org,_DNS:tn01920488.schoolwires.net (0)X509v3_Key_Usage critical (0) _Digital_Signature,_Key_Encipherment (0)X509v3_Extended_Key_Usage _TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (0)X509v3_CRL_Distribution_Points (0) _Full_Name: (0) _URI:http://crl.sca1b.amazontrust.com/sca1b.crl (0)X509v3_Certificate_Policies _Policy:_2.23.140.1.2.1 (0)Authority_Information_Access _OCSP_-_URI:http://ocsp.sca1b.amazontrust.com (0) _CA_Issuers_-_URI:http://crt.sca1b.amazontrust.com/sca1b.crt (0)X509v3_Basic_Constraints critical (0) _CA:FALSE (0)CT_Precertificate_SCTs _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5: (0) _BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84 (0) _Timestamp_:_Jul_23_18:14:00.303_2021_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:44:02:20:6C:5D:23:34:BD:0C:6A:D0:32:81:7B:F0: (0) _59:DC:13:35:D2:26:36:71:8B:D9:4C:A7:2D:B2:74:A6: (0) _84:03:A6:2B:02:20:6D:40:81:E2:5B:1B:DC:98:3B:16: (0) _35:8C:2A:2A:BC:88:CC:94:48:A3:64:97:82:75:98:7F: (0) _59:40:C5:49:76:D3 (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_51:A3:B0:F5:FD:01:79:9C:56:6D:B8:37:78:8F:0C:A4: (0) _7A:CC:1B:27:CB:F7:9E:88:42:9A:0D:FE:D4:8B:05:E5 (0) _Timestamp_:_Jul_23_18:14:00.380_2021_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:46:02:21:00:A3:77:D3:BC:71:39:05:AA:63:AD:E4: (0) _36:C8:B3:D5:09:B6:60:5C:2E:25:D3:52:AE:E5:0B:34: (0) _1B:AB:52:99:1D:02:21:00:A8:7B:F5:F2:CE:95:1C:E2: (0) _B5:B8:9E:D4:6A:19:C4:95:BC:86:EF:4A:83:CA:5C:CB: (0) _29:E1:52:0A:46:54:2B:7B (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E: (0) _4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6 (0) _Timestamp_:_Jul_23_18:14:00.282_2021_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:46:02:21:00:C8:27:2C:BD:36:E5:F7:A1:7A:E5:CA: (0) _0A:A1:29:72:52:52:1A:58:73:E3:58:18:37:4C:27:71: (0) _A6:D3:A6:C2:EA:02:21:00:83:C8:3F:75:55:7D:78:10: (0) _2C:21:5F:B3:1E:69:B5:0B:5E:84:8F:C8:16:71:5B:6B: (0) _AD:E9:37:E3:0C:5E:A6:B5 (0)Signature (256_octets) (0) 65:96:80:06:d6:44:45:99:b7:45:7e:8e:c1:60:46:64 (0) dc:6d:f7:3e:69:48:c5:44:e8:1f:2f:60:2b:a0:1e:6e (0) 25:4d:8c:42:23:44:ae:57:98:1f:2b:41:03:04:04:03 (0) 7e:15:02:d1:a0:3f:5f:70:7f:ba:ec:75:4d:d2:6a:13 (0) a0:49:f7:d8:fc:1d:80:bd:20:bd:ba:eb:65:aa:e6:e6 (0) 2c:42:b7:10:46:91:58:fb:00:92:61:b2:60:92:ef:e0 (0) 7d:e7:05:7c:77:58:51:1a:1b:d5:a8:78:7b:ef:d6:0d (0) 65:77:c3:50:dc:5c:7d:31:c9:4b:3e:2c:21:33:fe:d9 (0) c1:00:26:10:cd:44:85:c4:80:92:6e:55:d6:e8:52:ef (0) 6a:d8:d4:69:d9:53:d0:92:ef:ba:a6:ef:35:c8:33:eb (0) 76:a7:03:64:f4:bf:91:7b:83:d5:b8:5a:df:60:70:20 (0) 86:2f:31:f3:8a:bb:76:d9:7e:bd:02:01:7c:83:c8:55 (0) 8e:72:12:10:6e:22:90:84:2a:dc:49:b5:65:46:3a:f9 (0) 41:48:54:72:9e:ad:fb:b4:71:6b:aa:00:96:43:7a:5a (0) 16:e5:92:21:ca:97:89:00:ce:81:a8:06:0d:56:03:25 (0) 62:a8:c3:39:d5:75:5c:d1:70:cc:f6:4a:4d:b2:ae:2c (1)CERTIFICATE_1 _ (1)Version 3_(0x2) (1)Serial_Number _06:7f:94:57:85:87:e8:ac:77:de:b2:53:32:5b:bc:99:8b:56:0d_ (1)Signature_Algorithm sha256WithRSAEncryption (1)ISSUER_NAME _ countryName US _organizationName Amazon _commonName Amazon_Root_CA_1 (1)SUBJECT_NAME _ countryName US _organizationName Amazon _organizationalUnitName Server_CA_1B _commonName Amazon (1)Valid_From Oct_22_00:00:00_2015_GMT (1)Valid_Till Oct_19_00:00:00_2025_GMT (1)Public_Key_Algorithm rsaEncryption (1)RSA_Public_Key (2048_bit) (1) _RSA_Public-Key:_(2048_bit) (1) _Modulus: (1) _00:c2:4e:16:67:dd:ce:bc:6a:c8:37:5a:ec:3a:30: (1) _b0:1d:e6:d1:12:e8:12:28:48:cc:e8:29:c1:b9:6e: (1) _53:d5:a3:eb:03:39:1a:cc:77:87:f6:01:b9:d9:70: (1) _cc:cf:6b:8d:e3:e3:03:71:86:99:6d:cb:a6:94:2a: (1) _4e:13:d6:a7:bd:04:ec:0a:16:3c:0a:eb:39:b1:c4: (1) _b5:58:a3:b6:c7:56:25:ec:3e:52:7a:a8:e3:29:16: (1) _07:b9:6e:50:cf:fb:5f:31:f8:1d:ba:03:4a:62:89: (1) _03:ae:3e:47:f2:0f:27:91:e3:14:20:85:f8:fa:e9: (1) _8a:35:f5:5f:9e:99:4d:e7:6b:37:ef:a4:50:3e:44: (1) _ec:fa:5a:85:66:07:9c:7e:17:6a:55:f3:17:8a:35: (1) _1e:ee:e9:ac:c3:75:4e:58:55:7d:53:6b:0a:6b:9b: (1) _14:42:d7:e5:ac:01:89:b3:ea:a3:fe:cf:c0:2b:0c: (1) _84:c2:d8:53:15:cb:67:f0:d0:88:ca:3a:d1:17:73: (1) _f5:5f:9a:d4:c5:72:1e:7e:01:f1:98:30:63:2a:aa: (1) _f2:7a:2d:c5:e2:02:1a:86:e5:32:3e:0e:bd:11:b4: (1) _cf:3c:93:ef:17:50:10:9e:43:c2:06:2a:e0:0d:68: (1) _be:d3:88:8b:4a:65:8c:4a:d4:c3:2e:4c:9b:55:f4: (1) _86:e5 (1) _Exponent:_65537_(0x10001) (1)X509v3_EXTENSIONS _ (1)X509v3_Basic_Constraints critical (1) _CA:TRUE,_pathlen:0 (1)X509v3_Key_Usage critical (1) _Digital_Signature,_Certificate_Sign,_CRL_Sign (1)X509v3_Subject_Key_Identifier _59:A4:66:06:52:A0:7B:95:92:3C:A3:94:07:27:96:74:5B:F9:3D:D0 (1)X509v3_Authority_Key_Identifier _keyid:84:18:CC:85:34:EC:BC:0C:94:94:2E:08:59:9C:C7:B2:10:4E:0A:08 (1)Authority_Information_Access _OCSP_-_URI:http://ocsp.rootca1.amazontrust.com (1) _CA_Issuers_-_URI:http://crt.rootca1.amazontrust.com/rootca1.cer (1)X509v3_CRL_Distribution_Points (1) _Full_Name: (1) _URI:http://crl.rootca1.amazontrust.com/rootca1.crl (1)X509v3_Certificate_Policies _Policy:_2.23.140.1.2.1 (1)Signature (256_octets) (1) 85:92:be:35:bb:79:cf:a3:81:42:1c:e4:e3:63:73:53 (1) 39:52:35:e7:d1:ad:fd:ae:99:8a:ac:89:12:2f:bb:e7 (1) 6f:9a:d5:4e:72:ea:20:30:61:f9:97:b2:cd:a5:27:02 (1) 45:a8:ca:76:3e:98:4a:83:9e:b6:e6:45:e0:f2:43:f6 (1) 08:de:6d:e8:6e:db:31:07:13:f0:2f:31:0d:93:6d:61 (1) 37:7b:58:f0:fc:51:98:91:28:02:4f:05:76:b7:d3:f0 (1) 1b:c2:e6:5e:d0:66:85:11:0f:2e:81:c6:10:81:29:fe (1) 20:60:48:f3:f2:f0:84:13:53:65:35:15:11:6b:82:51 (1) 40:55:57:5f:18:b5:b0:22:3e:ad:f2:5e:a3:01:e3:c3 (1) b3:f9:cb:41:5a:e6:52:91:bb:e4:36:87:4f:2d:a9:a4 (1) 07:68:35:ba:94:72:cd:0e:ea:0e:7d:57:f2:79:fc:37 (1) c5:7b:60:9e:b2:eb:c0:2d:90:77:0d:49:10:27:a5:38 (1) ad:c4:12:a3:b4:a3:c8:48:b3:15:0b:1e:e2:e2:19:dc (1) c4:76:52:c8:bc:8a:41:78:70:d9:6d:97:b3:4a:8b:78 (1) 2d:5e:b4:0f:a3:4c:60:ca:e1:47:cb:78:2d:12:17:b1 (1) 52:8b:ca:39:2c:bd:b5:2f:c2:33:02:96:ab:da:94:7f (2)CERTIFICATE_2 _ (2)Version 3_(0x2) (2)Serial_Number _06:7f:94:4a:2a:27:cd:f3:fa:c2:ae:2b:01:f9:08:ee:b9:c4:c6_ (2)Signature_Algorithm sha256WithRSAEncryption (2)ISSUER_NAME _ countryName US _stateOrProvinceName Arizona _localityName Scottsdale _organizationName "Starfield_Technologies,_Inc." _commonName Starfield_Services_Root_Certificate_Authority_-_G2 (2)SUBJECT_NAME _ countryName US _organizationName Amazon _commonName Amazon_Root_CA_1 (2)Valid_From May_25_12:00:00_2015_GMT (2)Valid_Till Dec_31_01:00:00_2037_GMT (2)Public_Key_Algorithm rsaEncryption (2)RSA_Public_Key (2048_bit) (2) _RSA_Public-Key:_(2048_bit) (2) _Modulus: (2) _00:b2:78:80:71:ca:78:d5:e3:71:af:47:80:50:74: (2) _7d:6e:d8:d7:88:76:f4:99:68:f7:58:21:60:f9:74: (2) _84:01:2f:ac:02:2d:86:d3:a0:43:7a:4e:b2:a4:d0: (2) _36:ba:01:be:8d:db:48:c8:07:17:36:4c:f4:ee:88: (2) _23:c7:3e:eb:37:f5:b5:19:f8:49:68:b0:de:d7:b9: (2) _76:38:1d:61:9e:a4:fe:82:36:a5:e5:4a:56:e4:45: (2) _e1:f9:fd:b4:16:fa:74:da:9c:9b:35:39:2f:fa:b0: (2) _20:50:06:6c:7a:d0:80:b2:a6:f9:af:ec:47:19:8f: (2) _50:38:07:dc:a2:87:39:58:f8:ba:d5:a9:f9:48:67: (2) _30:96:ee:94:78:5e:6f:89:a3:51:c0:30:86:66:a1: (2) _45:66:ba:54:eb:a3:c3:91:f9:48:dc:ff:d1:e8:30: (2) _2d:7d:2d:74:70:35:d7:88:24:f7:9e:c4:59:6e:bb: (2) _73:87:17:f2:32:46:28:b8:43:fa:b7:1d:aa:ca:b4: (2) _f2:9f:24:0e:2d:4b:f7:71:5c:5e:69:ff:ea:95:02: (2) _cb:38:8a:ae:50:38:6f:db:fb:2d:62:1b:c5:c7:1e: (2) _54:e1:77:e0:67:c8:0f:9c:87:23:d6:3f:40:20:7f: (2) _20:80:c4:80:4c:3e:3b:24:26:8e:04:ae:6c:9a:c8: (2) _aa:0d (2) _Exponent:_65537_(0x10001) (2)X509v3_EXTENSIONS _ (2)X509v3_Basic_Constraints critical (2) _CA:TRUE (2)X509v3_Key_Usage critical (2) _Digital_Signature,_Certificate_Sign,_CRL_Sign (2)X509v3_Subject_Key_Identifier _84:18:CC:85:34:EC:BC:0C:94:94:2E:08:59:9C:C7:B2:10:4E:0A:08 (2)X509v3_Authority_Key_Identifier _keyid:9C:5F:00:DF:AA:01:D7:30:2B:38:88:A2:B8:6D:4A:9C:F2:11:91:83 (2)Authority_Information_Access _OCSP_-_URI:http://ocsp.rootg2.amazontrust.com (2) _CA_Issuers_-_URI:http://crt.rootg2.amazontrust.com/rootg2.cer (2)X509v3_CRL_Distribution_Points (2) _Full_Name: (2) _URI:http://crl.rootg2.amazontrust.com/rootg2.crl (2)X509v3_Certificate_Policies _Policy:_X509v3_Any_Policy (2)Signature (256_octets) (2) 62:37:42:5c:bc:10:b5:3e: |

8b:2c:e9:0c:9b:6c:45:e2 (2) 07:00:7a:f9:c5:58:0b:b9:08:8c:3e:ed:b3:25:3c:b5 (2) 6f:50:e4:cd:35:6a:a7:93:34:96:32:21:a9:48:44:ab (2) 9c:ed:3d:b4:aa:73:6d:e4:7f:16:80:89:6c:cf:28:03 (2) 18:83:47:79:a3:10:7e:30:5b:ac:3b:b0:60:e0:77:d4 (2) 08:a6:e1:1d:7c:5e:c0:bb:f9:9a:7b:22:9d:a7:00:09 (2) 7e:ac:46:17:83:dc:9c:26:57:99:30:39:62:96:8f:ed (2) da:de:aa:c5:cc:1b:3e:ca:43:68:6c:57:16:bc:d5:0e (2) 20:2e:fe:ff:c2:6a:5d:2e:a0:4a:6d:14:58:87:94:e6 (2) 39:31:5f:7c:73:cb:90:88:6a:84:11:96:27:a6:ed:d9 (2) 81:46:a6:7e:a3:72:00:0a:52:3e:83:88:07:63:77:89 (2) 69:17:0f:39:85:d2:ab:08:45:4d:d0:51:3a:fd:5d:5d (2) 37:64:4c:7e:30:b2:55:24:42:9d:36:b0:5d:9c:17:81 (2) 61:f1:ca:f9:10:02:24:ab:eb:0d:74:91:8d:7b:45:29 (2) 50:39:88:b2:a6:89:35:25:1e:14:6a:47:23:31:2f:5c (2) 9a:fa:ad:9a:0e:62:51:a4:2a:a9:c4:f9:34:9d:21:18 (3)CERTIFICATE_3 _ (3)Version 3_(0x2) (3)Serial_Number _a7:0e:4a:4c:34:82:b7:7f_ (3)Signature_Algorithm sha256WithRSAEncryption (3)ISSUER_NAME _ countryName US _organizationName "Starfield_Technologies,_Inc." _organizationalUnitName Starfield_Class_2_Certification_Authority (3)SUBJECT_NAME _ countryName US _stateOrProvinceName Arizona _localityName Scottsdale _organizationName "Starfield_Technologies,_Inc." _commonName Starfield_Services_Root_Certificate_Authority_-_G2 (3)Valid_From Sep_2_00:00:00_2009_GMT (3)Valid_Till Jun_28_17:39:16_2034_GMT (3)Public_Key_Algorithm rsaEncryption (3)RSA_Public_Key (2048_bit) (3) _RSA_Public-Key:_(2048_bit) (3) _Modulus: (3) _00:d5:0c:3a:c4:2a:f9:4e:e2:f5:be:19:97:5f:8e: (3) _88:53:b1:1f:3f:cb:cf:9f:20:13:6d:29:3a:c8:0f: (3) _7d:3c:f7:6b:76:38:63:d9:36:60:a8:9b:5e:5c:00: (3) _80:b2:2f:59:7f:f6:87:f9:25:43:86:e7:69:1b:52: (3) _9a:90:e1:71:e3:d8:2d:0d:4e:6f:f6:c8:49:d9:b6: (3) _f3:1a:56:ae:2b:b6:74:14:eb:cf:fb:26:e3:1a:ba: (3) _1d:96:2e:6a:3b:58:94:89:47:56:ff:25:a0:93:70: (3) _53:83:da:84:74:14:c3:67:9e:04:68:3a:df:8e:40: (3) _5a:1d:4a:4e:cf:43:91:3b:e7:56:d6:00:70:cb:52: (3) _ee:7b:7d:ae:3a:e7:bc:31:f9:45:f6:c2:60:cf:13: (3) _59:02:2b:80:cc:34:47:df:b9:de:90:65:6d:02:cf: (3) _2c:91:a6:a6:e7:de:85:18:49:7c:66:4e:a3:3a:6d: (3) _a9:b5:ee:34:2e:ba:0d:03:b8:33:df:47:eb:b1:6b: (3) _8d:25:d9:9b:ce:81:d1:45:46:32:96:70:87:de:02: (3) _0e:49:43:85:b6:6c:73:bb:64:ea:61:41:ac:c9:d4: (3) _54:df:87:2f:c7:22:b2:26:cc:9f:59:54:68:9f:fc: (3) _be:2a:2f:c4:55:1c:75:40:60:17:85:02:55:39:8b: (3) _7f:05 (3) _Exponent:_65537_(0x10001) (3)X509v3_EXTENSIONS _ (3)X509v3_Basic_Constraints critical (3) _CA:TRUE (3)X509v3_Key_Usage critical (3) _Digital_Signature,_Certificate_Sign,_CRL_Sign (3)X509v3_Subject_Key_Identifier _9C:5F:00:DF:AA:01:D7:30:2B:38:88:A2:B8:6D:4A:9C:F2:11:91:83 (3)X509v3_Authority_Key_Identifier _keyid:BF:5F:B7:D1:CE:DD:1F:86:F4:5B:55:AC:DC:D7:10:C2:0E:A9:88:E7 (3)Authority_Information_Access _OCSP_-_URI:http://o.ss2.us/ (3) _CA_Issuers_-_URI:http://

x.ss2.us/x.cer (3)X509v3_CRL_Distribution_Points (3) _Full_Name: (3) _URI:http://s.ss2.us/r.crl (3)X509v3_Certificate_Policies _Policy:_X509v3_Any_Policy (3)Signature (256_octets) (3) 23:1d:e3:8a:57:ca:7d:e9:17:79:4c:f1:1e:55:fd:cc (3) 53:6e:3e:47:0f:df:c6:55:f2:b2:04:36:ed:80:1f:53 (3) c4:5d:34:28:6b:be:c7:55:fc:67:ea:cb:3f:7f:90:b2 (3) 33:cd:1b:58:10:82:02:f8:f8:2f:f5:13:60:d4:05:ce (3) f1:81:08:c1:dd:a7:75:97:4f:18:b9:6d:de:f7:93:91 (3) 08:ba:7e:40:2c:ed:c1:ea:bb:76:9e:33:06:77:1d:0d (3) 08:7f:53:dd:1b:64:ab:82:27:f1:69:d5:4d:5e:ae:f4 (3) a1:c3:75:a7:58:44:2d:f2:3c:70:98:ac:ba:69:b6:95 (3) 77:7f:0f:31:5e:2c:fc:a0:87:3a:47:69:f0:79:5f:f4 (3) 14:54:a4:95:5e:11:78:12:60:27:ce:9f:c2:77:ff:23 (3) 53:77:5d:ba:ff:ea:59:e7:db:cf:af:92:96:ef:24:9a (3) 35:10:7a:9c:91:c6:0e:7d:99:f6:3f:19:df:f5:72:54 (3) e1:15:a9:07:59:7b:83:bf:52:2e:46:8c:b2:00:64:76 (3) 1c:48:d3:d8:79:e8:6e:56:cc:ae:2c:03:90:d7:19:38 (3) 99:e4:ca:09:19:5b:ff:07:96:b0:a8:7f:34:49:df:56 (3) a9:f7:b0:5f:ed:33:ed:8c:47:b7:30:03:5d:f4:03:8c

## Info List

### Info #1

Certificate Fingerprint:B75E72200C4FFB561C0303B5A72B17AA6FBED9D25B2A6E44589FD608A9BE2718

### Info #2

Certificate Fingerprint:B75E72200C4FFB561C0303B5A72B17AA6FBED9D25B2A6E44589FD608A9BE2718

### Info #3

Certificate Fingerprint:B75E72200C4FFB561C0303B5A72B17AA6FBED9D25B2A6E44589FD608A9BE2718

### Info #4

Certificate Fingerprint:B75E72200C4FFB561C0303B5A72B17AA6FBED9D25B2A6E44589FD608A9BE2718