

Sri Lanka Institute of Information Technology



Individual Assignment

Bug Bounty Report
Server-Side Request Forgery (SSRF)
and
Denial of Service (DoS)

Web Security - IE2062

BSc Honors in Information Technology Specializing in Cyber Security

CASE STUDY NAME	BUG BOUNTY Report 04 - Server-Side Request Forgery (SSRF) and Denial of Service (DoS)
CAMPUS/CENTER	SLIIT KANDY UNI

Student Details

	Student Registration Number	Student Name
1	IT23222854	JAYASINGHE B. I

Table of Contents

Domain – Cisco Customer and Partner Experience Cloud	4
1. Multi Tool Web Vulnerability Scanning	5
1.1 Rapidscan.....	5
1.2 nmap (Validation for rapidscan)	5
1.3 WPSan.....	5
1.3 OWASP ZAP	6
2. Sensitive data Exposure	9
2.1 Retire.js	9
Summary of the above vulnerabilities.	9
2.2 Wappalyzer.....	10
3. Firewall Detection	11
3.1 Wafw00f.....	11
How to mitigate the above Vulnerability	12

1. Multi Tool Web Vulnerability Scanning

1.1 Rapidscan

```
(binosh@BINZ)-[~/Desktop/WS Assingment/Tools/rapidsca  
$ python3 rapidscan.py -u https://id.cisco.com/
```

Out of 80 vulnerabilities checked for <https://id.cisco.com/> **4 vulnerabilities were detected.**

```
Vulnerability Threat Level  
Medium Secure Client Initiated Renegotiation is supported.  
Vulnerability Definition  
Otherwise termed as Plain-Text Injection attack, which allows MITM attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauth  
enticated request that is processed retroactively by a server in a post-renegotiation context.  
Vulnerability Remediation  
Detailed steps of remediation can be found from these resources. https://securingtomorrow.mcafee.com/technical-how-to/tips-securing-ssl-renegotiation/ https://www.digicert.com/news/2011-06-03-ssl  
-renego/
```

1.2 nmap (Validation for rapidscan)

In the above Rapid scan result it posed that there are some open ports. This can be validated by doing a nmap scan on the domain.

PORT	STATE	SERVICE
25/tcp	open	smtp
80/tcp	open	http
443/tcp	open	https








There are 3 open ports that could be discovered from the nmap scan. This also discovered the version of each service that is being used in each port. Concluding that this could be dangerous since an attacker can exploit vulnerabilities known to each version.


1.3 WPSan

```
(binosh@BINZ)-[~/Desktop/WS Assingment/Tools]  
$ wpscan --url id.cisco.com  
  
-----  
WPSecScan®  
WordPress Security Scanner by the WPSecScan Team  
Version 3.8.28  
  
@_WPSecScan_, @ethicalhack3r, @erwan_lr, @firefart  
-----  
[i] Updating the Database ...  
[i] Update completed.  
  
Scan Aborted: The target is responding with a 403, this might be due to a WAF. Please re-try with --random-user-agent
```

1.4 OWASP ZAP

The below high, medium and Low severity vulnerabilities were disclosed from the ZAP scanning.

- >  Vulnerable JS Library
- >  CSP: Failure to Define Directive with No Fallback (57)
- >  CSP: Wildcard Directive (7)
- >  CSP: script-src unsafe-eval (50)
- >  CSP: script-src unsafe-inline (7)
- >  CSP: style-src unsafe-inline (57)
- >  Cross-Domain Misconfiguration (13)
- >  Vulnerable JS Library (2)
- >  Cookie No HttpOnly Flag (40)
- >  Cookie Without Secure Flag (33)
- >  Cookie with SameSite Attribute None (4)
- >  Cookie without SameSite Attribute (57)
- >  Cross-Domain JavaScript Source File Inclusion (2)
- >  Strict-Transport-Security Header Not Set (15)
- >  Timestamp Disclosure - Unix (51)
- >  X-Content-Type-Options Header Missing (27)
- >  Content Security Policy (CSP) Report-Only Header Found
- >  Information Disclosure - Suspicious Comments (15)
- >  Loosely Scoped Cookie (443)
- >  Modern Web Application (2)
- >  Re-examine Cache-control Directives (25)
- >  Retrieved from Cache (7)
- >  User Agent Fuzzer (12)

PII Disclosure	
URL:	https://sproutsocial.com/insights/instagram-drops/
Risk:	 High
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	2347002662267537
CWE ID:	359
WASC ID:	13
Source:	Passive (10062 - PII Disclosure)
Input Vector:	
Description:	The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.
Other Info:	
	Credit Card Type detected: Mastercard

PII Disclosure (High Risk)

URL: <https://sproutsocial.com/insights/instagram-drops/>

Details: This vulnerability exposes Personally Identifiable Information (PII), such as credit card numbers (Mastercard detected) and Social Security Numbers. It has a high impact due to the sensitivity of the data.

CWE ID: 359 (Privacy Violation).

Source: Passive detection using the PII Disclosure rule

Vulnerable JS Library

URL:	https://id.cisco.com/widget-content/js/axios.min.js
Risk:	 High
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	/* axios v0.21.1
CWE ID:	1395
WASC ID:	
Source:	Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:	
Description:	The identified library appears to be vulnerable.

Vulnerable JavaScript Library (High Risk)

URL: <https://id.cisco.com/widget-content/js/axios.min.js>

Details: The JavaScript library "axios v0.21.1" used here is identified as vulnerable, which could allow attackers to exploit weaknesses in outdated software versions.

CWE ID: 1395 (Using Components with Known Vulnerabilities).

Source: Identified through Retire.js.


URL:	https://sproutsocial.com/advocacy-ro-calculator-tool/result/
Risk:	Medium
Confidence:	High
Parameter:	Content-Security-Policy
Attack:	
Evidence:	frame-ancestors 'self' http://sproutsocial.lookbookhq.com https://sproutsocial.lookbookhq.com http://sproutsocial.pathfactory.com https://sproutsocial.pathfactory.com
CWE ID:	693
WASC ID:	15
Source:	Passive (10055 - CSP)
Alert Reference:	10055-13
Input Vector:	Description:

The Content-Security-Policy fails to define one of the directives that has no fallback. Missing/excluding them is the same as allowing anything.

CSP Misconfiguration (Medium Risk):

URL: <https://sproutsocial.com/advocacy-roi-calculator-tool/results/>

Details: The Content Security Policy (CSP) for this URL lacks proper directives, which means fallback security measures are missing. This could potentially allow content injection or other attacks.CWE ID: 693 (Incorrect Configuration).

CSP: Wildcard Directive	
URL:	https://fd.cisco.com/sitemap.xml
Risk:	 Medium
Confidence:	High
Parameter:	Content-Security-Policy
Attack:	
Evidence:	frame-ancestors 'self'
CWE ID:	693
WASC ID:	15
Source:	Passive (10055 - CSP)
Alert Reference:	10055-4
Input Vector:	
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross-Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data

Web Security - IE2062

Year 2 Semester 2 - 2025


CSP: script-src unsafe-eval


URL:	https://id.cisco.com/
Risk:	Medium
Confidence:	High
Parameter:	Content-Security-Policy
Attack:	


default-src 'nonce-7e998c73a2c589efd337470218b6ebc' 'self' ciscold.okta.com id.cisco.com *.oktacdn.com; con
nect-src 'self' ciscold.okta.com ciscold-admin.okta.com id.cisco.com *.oktacdn.com *.mixpanel.com *.mapbox.co
m *.mtls.okta.com ciscold.kerberos.okta.com ciscold.mtls.okta.com *.authenticatorlocalprod.com;8769 http://loca
lhost:8769 http://127.0.0.1:8769 *.authenticatorlocalprod.com:65111 http://localhost:65111 http://127.0.0.1:6
5111 *.authenticatorlocalprod.com:65121 http://localhost:65121 http://127.0.0.1:65121 *.authenticatorlocalpro
d.com:65131 http://localhost:65131 http://127.0.0.1:65131 *.authenticatorlocalprod.com:65141 http://localhost
:65141 http://127.0.0.1:65141 *.authenticatorlocalprod.com:65151 http://localhost:65151 http://127.0.0.1:651
51 https://slimmanager.okta.com data: *.ingest.sentry.io data.pendo.io pendo-static-5634101834153984.storage
googleapis.com pendo-static-5391521872216064.storage.googleapis.com; script-src 'nonce-7e998c73a2c589ef
d337470218b6ebc' 'unsafe-inline' 'nonce-a180-ARJBNtNtUgqEgP' 'unsafe-poll' 'self' 'script:errors' ciscold.adm

Evidence:

CSP: style-src unsafe-inline	
URL:	https://fd.cisco.com/
Risk:	Medium
Confidence:	High
Parameter:	Content-Security-Policy
Attack:	<pre>default-src 'nonce-7e998c73a2c589efd337470218b6ebc' 'self' ciscold.okta.com id.cisco.com *.oktacdn.com; connect-src 'self' ciscold.okta.com ciscold-admin.okta.com id.cisco.com *.oktacdn.com *.mixpanel.com *.mapbox.com *.mtls.okta.com ciscold.kerberos.okta.com ciscold.mtls.okta.com *.authenticatorlocalprod.com; 8769 http://loca host:8769 http://127.0.0.1:8769 *.authenticatorlocalprod.com:65111 http://localhost:65111 http://127.0.0.1:6 5111 *.authenticatorlocalprod.com:65121 http://localhost:65121 http://127.0.0.1:65121 *.authenticatorlocalpr d.com:65131 http://localhost:65131 http://127.0.0.1:65131 *.authenticatorlocalprod.com:65141 http://localhost :65141 http://127.0.0.1:65141 *.authenticatorlocalprod.com:65151 http://localhost:65151 http://127.0.0.1:651 51 https://oinmanager.okta.com data: *.ingest.sentry.io data.pendo.io pendo-static-5634101834153984.storage .googleapis.com pendo-static-5391521872216064.storage.googleapis.com; script-src 'nonce-7e998c73a2c589ef</pre>
Evidence:	

CSP: script-src unsafe-inline	
URL:	https://fd.cisco.com/sitemap.xml
Risk:	 Medium
Confidence:	High
Parameter:	Content-Security-Policy
Attack:	
Evidence:	frame-ancestors 'self'
CWE ID:	693
WASC ID:	15
Source:	Passive (10055 - CSP)
Alert Reference:	10055-5
Input Vector:	
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross-Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data

Cross-Domain Misconfiguration	
URL:	https://fd.cisco.com/assets/css/sections/errors-v2.css
Risk:	 Medium
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	Access-Control-Allow-Origin: *
CWE ID:	264
WASC ID:	14
Source:	Passive (10098 - Cross-Domain Misconfiguration)
Input Vector:	
Description:	
Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.	

Vulnerable JS Library	
URL:	https://id.cisco.com/widget-content/js/bootstrap-custom.min.js
Risk:	 Medium
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	* Bootstrap v3.4.1
CWE ID:	1395
WASC ID:	
Source:	Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:	
Description:	The identified library appears to be vulnerable.

2. Sensitive data Exposure

2.1 Retire.js

This tool is used to detect the use of JavaScript libraries and Node.js modules with known vulnerabilities.



Retire.js ☒ Enabled ☐ Show unknown

axios 0.21.1 Found in <https://id.cisco.com/widget-content/js/axios.min.js> - Vulnerability info:

- High Axios is vulnerable to Inefficient Regular Expression Complexity CVE-2021-3749 GHSA-cph5-mq7f-6fcx [1] [2]
- Medium Axios Cross-Site Request Forgery Vulnerability CVE-2023-45839 GHSA-4w2v-q235-qqgw [1] [2] [3] [4] [5] [6] [7] [8]
- Medium Versions before 1.6.8 depends on follow-redirects before 1.15.6 which could leak the proxy authentication credentials 6300 [1]
- High axios Requests Vulnerable To Possible SSRF and Credential Leakage via Absolute URL CVE-2025-27152 GHSA-jf5l-v2jv-69x6 [1] [2] [3] [4] [5] [6] [7]

bootstrap 3.4.1 Found in <https://id.cisco.com/widget-content/js/bootstrap-custom.min.js> - Vulnerability info:

- Medium Bootstrap Cross-Site Scripting (XSS) vulnerability CVE-2024-6484 GHSA-9mvj-7w8s-pvh2 [1] [2] [3] [4] [5] [6]
- Low Bootstrap before 4.0.0 is end-of-life and no longer maintained. 72 [1]

jquery 2.2.4.min Found in <https://id.cisco.com/widget-content/js/jquery-2.2.4.min.js> - Vulnerability info:

jquery 2.2.4.min Found in <https://id.cisco.com/widget-content/js/jquery-2.2.4.min.js> - Vulnerability info:

- Low jQuery 1.x and 2.x are End-of-Life and no longer receiving security updates 73 162 [1]
- Medium 3rd party CORS request may execute 2432 CVE-2015-9251 GHSA-rmxg-73gg-4p98 [1] [2] [3] [4] [5] [6]
- Medium jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution CVE-2019-11358 4333 GHSA-6c3j-c64m-qhqq [1] [2] [3]
- Medium passing HTML containing <options> elements 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. CVE-2020-11023 4647 GHSA-jpcq-ogw6-v4j6 [1]
- Medium Regexp in its jQuery.htmlPrefilter sometimes may introduce XSS CVE-2020-11022 4642 GHSA-gxr4-xj5j-5px2 [1]

Summary of the above vulnerabilities.

Library	Version	Vulnerability Description	Severity	Reference (CVE/GHSA)	Found at URL
axios	0.21.1	Inefficient Regular Expression Complexity	High	CVE-2021-3749, GHSA-cph5-mq7f-6fcx	http://id.cisco.com/widget-content/js/axios.min.js
		Cross-Site Request Forgery Vulnerability	Medium	CVE-2021-45839, GHSA-4w2v-q235-qqgw	
		Proxy Authentication Bypass (due to follow-redirects issue in versions before 1.1.0)	Medium	CVE-2021-43638, GHSA-7f2c-5w2r-r9gv	
		Vulnerable to SSRF and Denial of Service	High	CVE-2023-22540, GHSA-pjwm-rvh2-66v2	
bootstrap	3.4.1	Cross-Site Scripting (XSS) vulnerability	Medium	CVE-2018-14041, GHSA-6x9g-fm8r-4v4x	http://id.cisco.com/widget-content/js/bootstrap-custom.min.js
		Another XSS vulnerability	Low	CVE-2019-8331, GHSA-6x9g-fm8r-4v4x	
jquery	2.2.4	End-of-Life Version	Low		http://id.cisco.com/widget-content/js/jquery-2.2.4.min.js
		Exposes CORS requests to potential exploitation	Medium		
		Vulnerable to Prototype	Low		

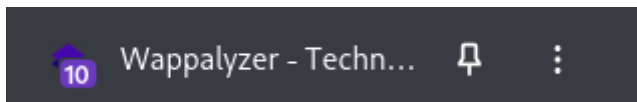
Web Security - IE2062

Year 2 Semester 2 - 2025











		Pollution			
		Issues with HTML Parsing	Low		

2.2 Wappalyzer

<https://id.cisco.com/>



Here are the results of the Wappalyzer detector

Security  Akamai Bot Manager	UI frameworks  Bootstrap
Programming languages  Java	Cookie compliance  OneTrust
CDN  Akamai	RUM  Boomerang  Akamai mPulse
JavaScript libraries  core-js 3.26.1  Boomerang  Axios	

3. Firewall Detection

3.1 Wafw00f

```
(binosh@BINZ)-[~/Desktop/WS Assingment/Tools]
$ wafw00f https://id.cisco.com

      { woof! }
      "
      ****
      / \
     /   \
    /     \
   /       \
  /         \
 /           \
/             \

404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error

~ WAFW00F : v2.3.1 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://id.cisco.com
[*] The site https://id.cisco.com is behind Kona SiteDefender (Akamai) WAF.
[~] Number of requests: 2
```

How to mitigate the above Vulnerability

The first step in improving security is to update important libraries. To fix vulnerabilities like SSRF, CSRF, and Proxy Authentication Bypass, update Axios to the most recent version. To reduce the risk of XSS, update Bootstrap to version 4.3.1 or above. In a same vein, update jQuery to at least 3.5.0 to handle CORS exploitation and prototype pollution.

Updating critical libraries is the first step in enhancing security. Updating Axios to the latest version will address vulnerabilities such as SSRF, CSRF, and Proxy Authentication Bypass; updating Bootstrap to version 4.3.1 or higher will reduce the risk of XSS; updating jQuery to at least 3.5.0 will handle CORS exploitation and prototype pollution; patching is also necessary; if at all possible, replace outdated libraries (such as older versions of jQuery) with actively maintained alternatives or apply custom fixes; and, in order to create a robust defense against potential attacks, follow secure defaults, which include turning on HTTPS and disabling insecure protocols.

Patching is also essential. If possible, replace out-of-date libraries (like earlier iterations of jQuery) with actively maintained alternatives or apply bespoke fixes.

Lastly, make sure that all of your application's settings are secure. Turn off unused library functionality to reduce vulnerability exposure. To build a strong defense against potential attacks, adhere to secure defaults, which include turning on HTTPS and turning off insecure protocols.

Proof of Report Submission



**Cisco Customer and Partner Experience
Cloud** has received **WS Assingment**

Thank you Binosh ,

We have received your Bugcrowd submission for engagement cisco-cpx-vdp.

Submission Details

Submitted
04 May 2025 19:03:52 UTC

Submission ID
5821ebcc-4804-4b81-b94e-88a743beee31

VRT
Application-Level Denial-of-Service (DoS) > App Crash > Malformed
Android Intents

[View Submission Details](#)