Sri Lanka Institute of Information Technology

Report – Cisco

IE2062 - Web security

Submitted by:

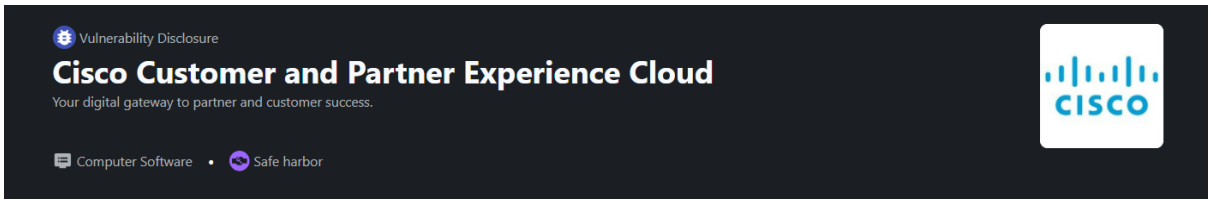
Student Registration Number	Student Name
IT23253476	Bandara S.M.S.N

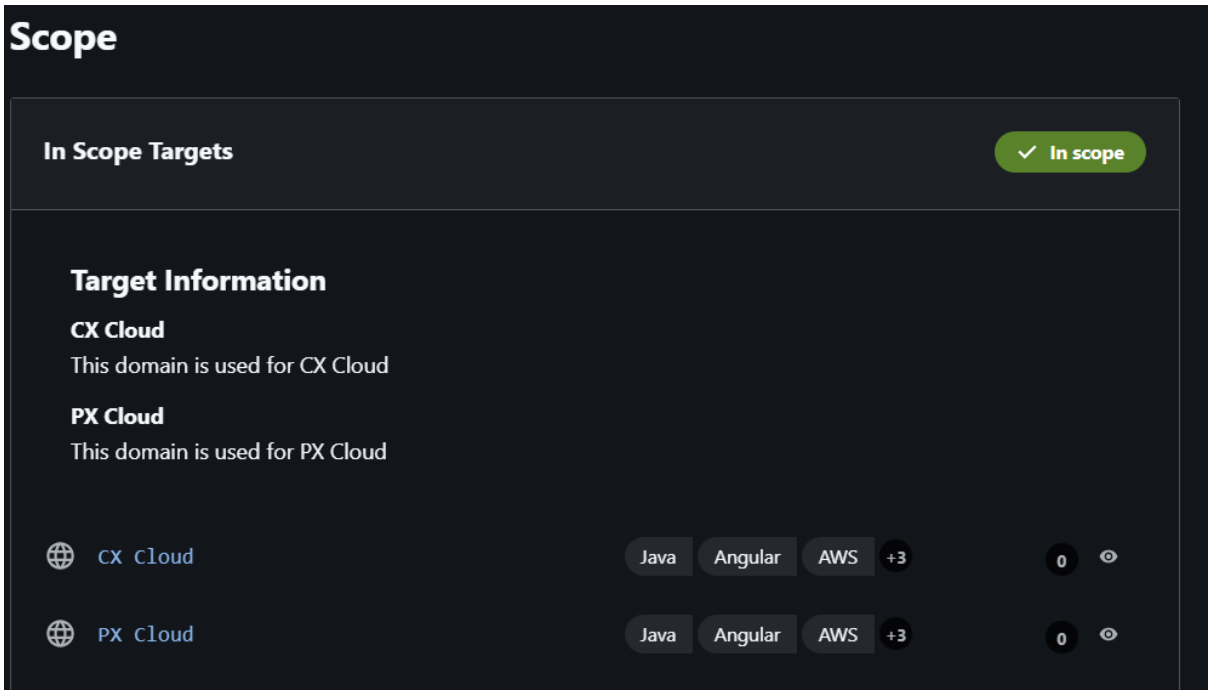
Date of submission

05/05/2025

Table of Contents

1. Domain: https://id.cisco.com/



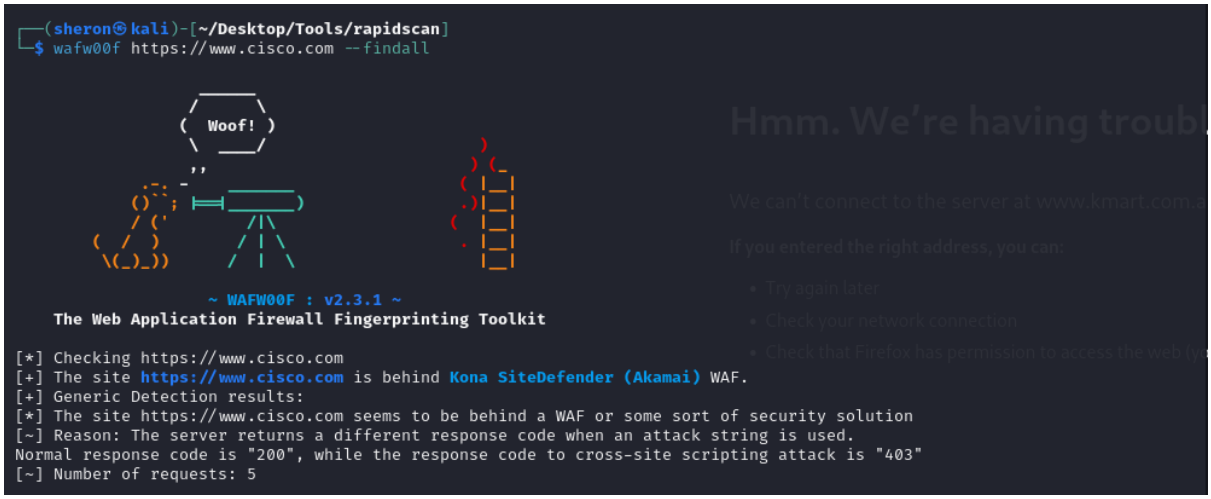


- Link: : https://id.cisco.com/
- Type: Vulnerability Disclosure Program (VDP)
- Category: Software

2. Scanning

2.1. Wafw00f

Wafwoof is a tool that enables the tester to perform a web application firewall scanner. It will find the name of the service provider. This sometimes will help us to find known vulnerabilities of the version used.



The web application is protected by a firewall called Kona SiteDefender (Akmai). It does not have any high severity CVEs, it might be affected by some other attacks such as, bypass techniques. Misconfigurations in the firewall can also lead to exposed IP addresses or partial coverage.

2.2. Retire.js

Retire.js is powerful web browser extension which can be used to identify any vulnerable versions used in the web application. The retire.js has found the following known vulnerabilities.

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-qhgq [1] [2] [3] Medium passing HTML containing <option> 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-cgw6-v4j6 [1] Medium Regex in its jQuery.htmlPrefilter sometimes may introduce XSS CVE-2020-11022 4642 GHSA-gxr4-xjj5-5px2 [1]

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-m8f7-6c5x [1] [2] Medium Axios Cross-Site Request Forgery Vulnerability CVE-2023-45857 GHSA-wf5p-g6vw-rhxx [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-jr5f-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-f7w8-pvh2 [1] [2] [3] [4] [5] [6] Low Bootstrap before 4.0.0 is end-of-life and no longer maintained. 72 [1]

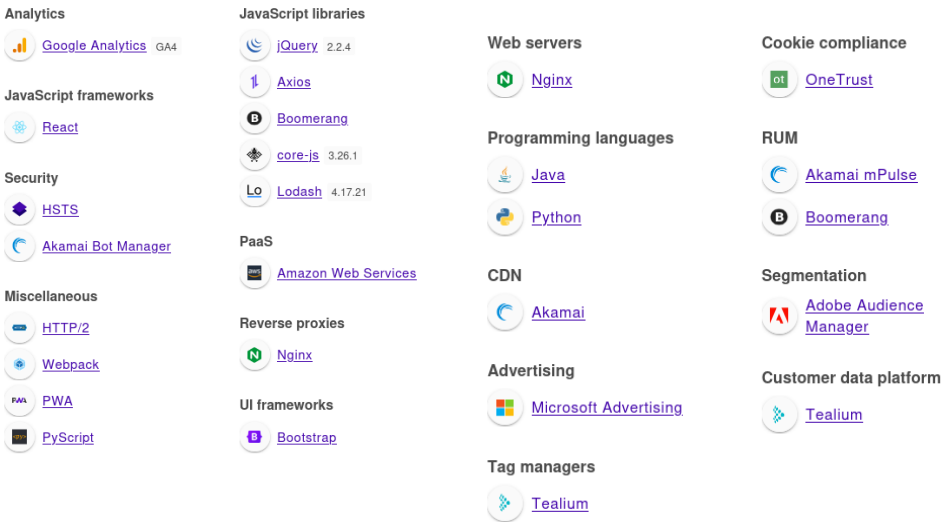
Component Name	CVE	Details
jQuery 2.2.4	CVE-2019-11358	**Object Prototype Pollution**—can lead to security misconfigurations in JavaScript applications.
jQuery 2.2.4	CVE-2020-11022, CVE-2020-11023	**Cross-Site Scripting (XSS) Risks**—certain functions in jQuery allow malicious script injection.
Axios 0.21.1	CVE-2021-3749	**Regular Expression Complexity Issue**—regex vulnerabilities may allow denial-of-service attacks.
Axios 0.21.1	CVE-2023-4587	**Cross-Site Request Forgery (CSRF) Vulnerability**—attackers can trick users into making unintended requests.
Axios (before 1.6.8)	CVE-2025-27152	**Proxy Authentication Credentials Leak**—exposing sensitive authentication details through server requests.
Bootstrap 3.4.1	CVE-2024-6484	**Cross-Site Scripting (XSS) Vulnerability**—older Bootstrap versions have unsafe JavaScript execution methods.

This web application has used many vulnerable versions of popular libraries. These libraries, such as jQuery, Axios, and Boostrap are the main affected components. The CVE numbers can be found because these are already existing vulnerabilities that can be exploited.

There are many vulnerabilities such as object prototype pollution, XSS vulnerabilities, Cross site request forgery (CSRF) and potential proxy authentication credential leaks.

2.3. Wappalyzer

This is chrome extension which helps to find the technologies used in a web application. It will also allow us to see the version that the web application has used. If the attacker can know the version of the technology that has been used, he can look for known vulnerabilities in the version and exploit them.



After inspection of the technologies. There were few technologies which were using vulnerable versions. Technologies such as jQuery, Axios, Boomerang and Lodash were found vulnerable. The following is table with the CVE of the vulnerability that were found within the web application.

Technology	Version	Vulnerability	CVE Identifier
jQuery	2.2.4	Cross-Site Scripting (XSS)	CVE-2020-11022, CVE-2020-11023
Axios	0.21.1	Server-Side Request Forgery (SSRF)	CVE-2020-28168
Boomerang	1.718.0	Possible information disclosure risks	(No confirmed CVEs found)
Lodash	4.17.21	Prototype Pollution	CVE-2020-8203

2.4. Nmap

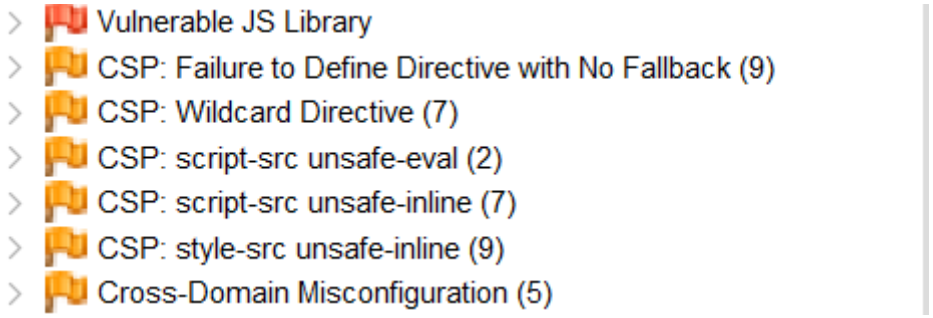
Nmap is a popular tool which is used to reveal any open ports and the services which are running on them. This information will help the attacker to gain information about the system that he can unload his payload.

```
Host is up (0.054s latency).
Other addresses for www.cisco.com (not scanned): 2600:140f:6:1a7::b33 2600:140f:6:18a::b33
rDNS record for 23.208.168.98: a23-208-168-98.deploy.static.akamaitechnologies.com
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp?
443/tcp  open  ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
554/tcp  open  rtsp?
1723/tcp open  pptp?
5060/tcp open  sip?
```

In this web application port 21which is running the FTP service can be vulnerable to brute force attacks, FTP bounces and sniffing attacks. In port 1723 where PPTP service is running is known for weak encryption and brute force attacks. And in port 5060, SIP service is running which can be vulnerable to eavesdropping. So its better to close of any unused ports for better security.

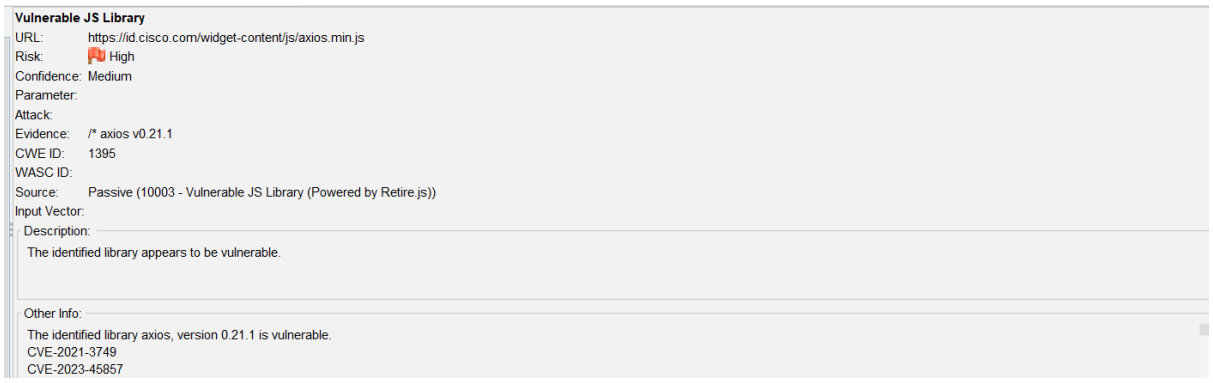
2.5. OWSAP Zap

Owsap Zap is a powerful web application testing tool which enables to identify any hidden vulnerability in a web application. The following were found during the scan.

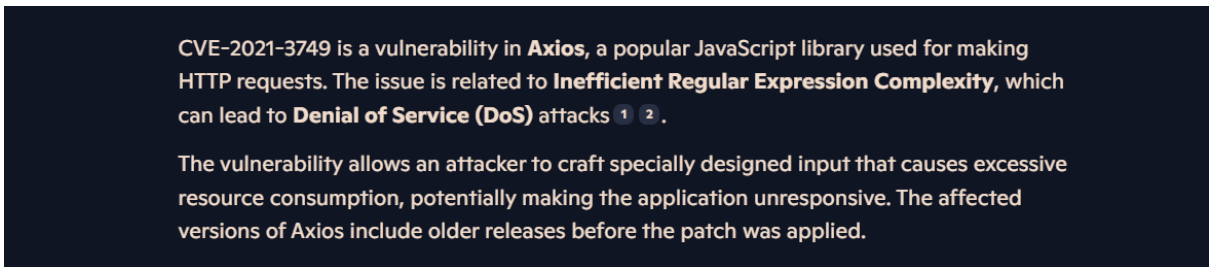


Zap has identified one high severity and few other medium level vulnerabilities.

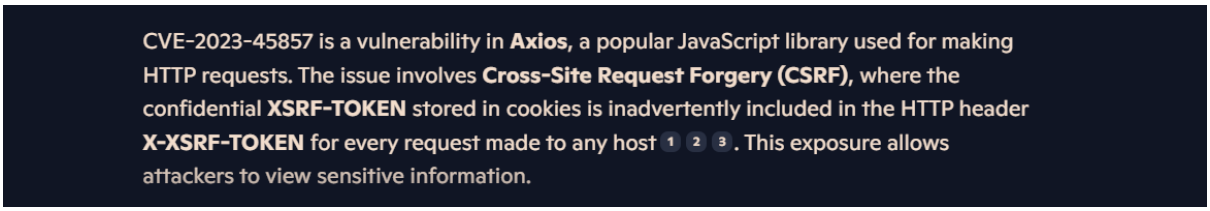
The first vulnerability is related to a vulnerable JavaScript library which is axios used. Its known vulnerabilities are as follows,



- CVE2021-3749



- CVE2023-45857



The following vulnerabilities were also found in vulnerable java script.

- CVE-2020-11023

CVE-2020-11023 is a **Cross-Site Scripting (XSS)** vulnerability in **jQuery** versions **1.0.3 through 3.4.1.** The issue arises when HTML containing `<option>` elements from untrusted sources—**even after sanitization**—is passed to jQuery's DOM manipulation methods like `.html()`, `.append()`, and others. This can lead to **untrusted code execution** [1].

- CVE-2020-11022

CVE-2020-11022 is a **Cross-Site Scripting (XSS)** vulnerability affecting **jQuery versions 1.2 through 3.4.1** [1]. The issue arises when HTML from untrusted sources—**even after sanitization**—is passed to jQuery's DOM manipulation methods like `.html()`, `.append()`, and others, potentially leading to **untrusted code execution** [1].

The other remaining vulnerabilities are regarding missing headers on the website. And the tool has identified due to the missing headers, its possible to perform XSS attacks as a result.

CSP: script-src unsafe-eval

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

default-src 'nonce-d9b859c41577a54aae0d487ddbc645f1' 'self' ciscoid.okta.com id.cisco.com *.oktacdn.com; connect-src 'self' ciscoid.okta.com ciscoid-admin.okta.com id.cisco.com *.oktacdn.com *.mixpanel.com *.mapbox.com *.mtls.okta.com ciscoid.kerberos.okta.com ciscoid.mtls.okta.com *.authenticatorlocalprod.com:8769 http://localhost:8769 http://127.0.0.1:8769 *.authenticatorlocalprod.com:65111 http://localhost:65111 http://127.0.0.1:65111 *.authenticatorlocalprod.com:65121 http://localhost:65121 http://127.0.0.1:65121 *.authenticatorlocalprod.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://127.0.0.1:65151 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-d9b859c41577a54aae0d487ddbc645f1' 'unsafe-inline' 'nonce-rCxG-ATMuu6gGmz8_RzrCw' 'unsafe-eval' 'self' 'report-sample' ciscoid.okta.com id.cisco.com *.oktacdn.com; style-src 'unsafe-inline' 'self' ciscoid.okta.com id.cisco.com *.oktacdn.com; frame-src 'self' ciscoid.okta.com ciscoid-admin.okta.com id.cisco.com login.okta.com *.vidyard.com com-okta-authenticator: api-dbbfec7f.duosecurity.com; img-src 'self' ciscoid.okta.com id.cisco.com *.oktacdn.com *.tiles.mapbox.com *.mapbox.com *.vidyard.com data: data.pendo.io pendo-static-5634101834153984.storage.googleapis.com pendo-static-5391521872216064.storage.googleapis.com blob:; font-src 'self' ciscoid.okta.com id.cisco.com data: *.oktacdn.com fonts.gstatic.com; frame-ancestors 'self' https://*.meraki.com https://*.meraki.ca

Evidence:
CWE ID: 693
WASC ID: 15
Source: Passive (10055 - CSP)
Alert Reference: 10055-10
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 theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

2.6. XSStrike tool

This tool can be used try payloads in a web application. It is possible to test using a test value to a parameter and testing it by crawling through the web site. The following CVE were found because of the scan.

- CVE-2019-11358
- CVE-2015-9251
- CVE-2019-11358

```
┌──(venv)─(sheron㉿kali)-[~/Desktop/Tools/XSStrike]
└─$ python3 xsstrike.py -u "http://cisco.com/search.php?q=test" --crawl


        XSStrike v3.1.5

[~] Crawling the target
[!!] Unable to connect to the target.
--------------------------------------------------------------------------------
[+] Vulnerable component: jquery v1.12.4-aem
[!] Component location: http://cisco.com/etc.clientlibs/clientlibs/granite/jquery.min.js
[!] Total vulnerabilities: 3
[!] Summary: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true
 ...) because of Object.prototype pollution
[!] Severity: low
[!] CVE: CVE-2019-11358
[!] Summary: 3rd party CORS request may execute
[!] Severity: medium
[!] CVE: CVE-2015-9251
[!] Summary: parseHTML() executes scripts in event handlers
[!] Severity: medium
[!] CVE: CVE-2015-9251
--------------------------------------------------------------------------------
[!!] Unable to connect to the target.
--------------------------------------------------------------------------------
[+] Vulnerable component: jquery v1.10.2
[!] Component location: http://cisco.com/etc/designs/cdc/clientlibs/responsive/js/foundation.min.js
[!] Total vulnerabilities: 3
[!] Summary: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true
 ...) because of Object.prototype pollution
[!] Severity: low
[!] CVE: CVE-2019-11358
[!] Summary: 3rd party CORS request may execute
[!] Severity: medium
[!] CVE: CVE-2015-9251
[!] Summary: parseHTML() executes scripts in event handlers
[!] Severity: medium
[!] CVE: CVE-2015-9251
--------------------------------------------------------------------------------
```

2.7. Rapid Scanner

Rapid scanner is a powerful tool which uses about 82 scans to look for vulnerabilities in a web application. This tool gives us the severity level, name, description and mitigation methods to the vulnerability.

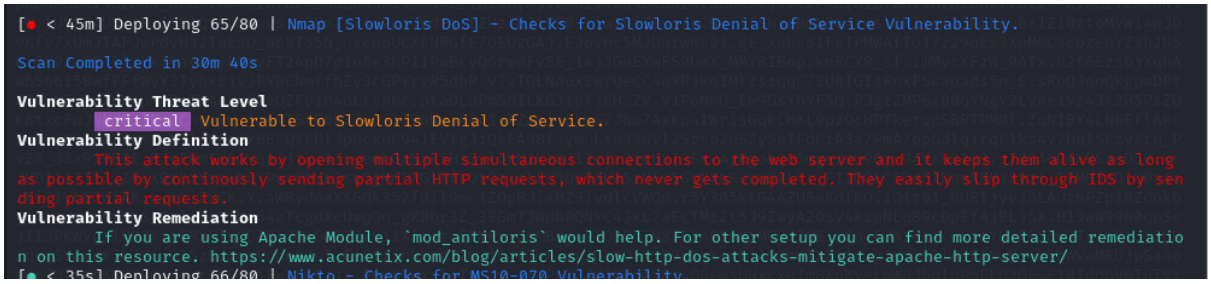
First Vulnerability – A vulnerability related to **XSS** has been identified by the tool XSSer. This was also identified by the earlier scans as well. It might be because of the vulnerable version used the missing headers of the web application.

```
[● <  4m] Deploying 15/80 | XSSer - Checks for Cross-Site Scripting [XSS] Attacks.

Scan Completed in 1s

Vulnerability Threat Level
        critical XSSer found XSS vulnerabilities.
Vulnerability Definition
        An attacker will be able to steal cookies, deface web application or redirect to any third party address that can
 serve malware.
Vulnerability Remediation
        Input validation and Output Sanitization can completely prevent Cross Site Scripting (XSS) attacks. XSS attacks c
an be mitigated in future by properly following a secure coding methodology. The following comprehensive resource provide
s detailed information on fixing this vulnerability. https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Preventio
n_Cheat_Sheet
```

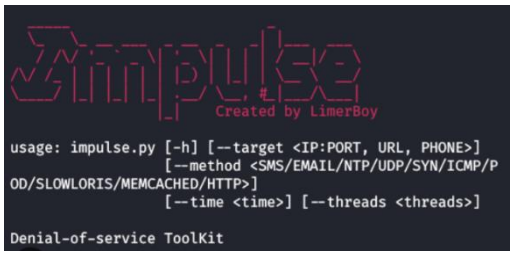
The below scan reveles that there is a missing header which could lead to xss attacks in older browsers.

```
Vulnerability Threat Level
        medium X-XSS Protection is not Present
Vulnerability Definition
        As the target is lacking this header, older browsers will be prone to Reflected XSS attacks.
Vulnerability Remediation
        Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are s
trongly recommended to be upgraded.
```

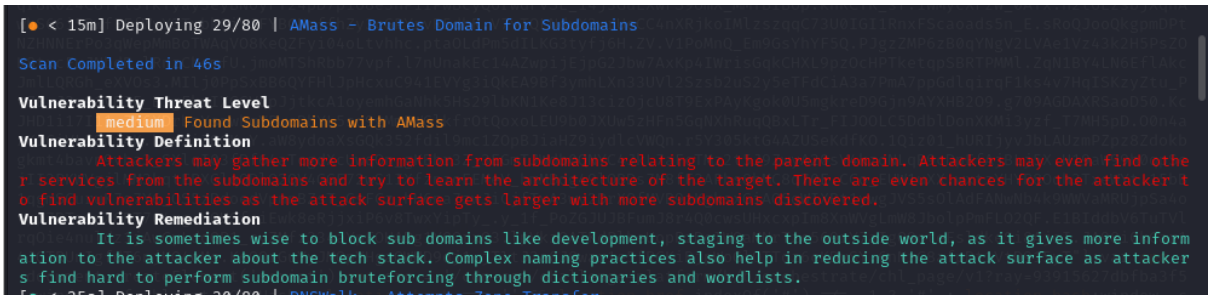
Second Vulnerability – this is a vulnerability related to a DOS. This was discovered by a tool called Slowloris. The attack is conducted by sending partial http requests to the server. Causing denial of service



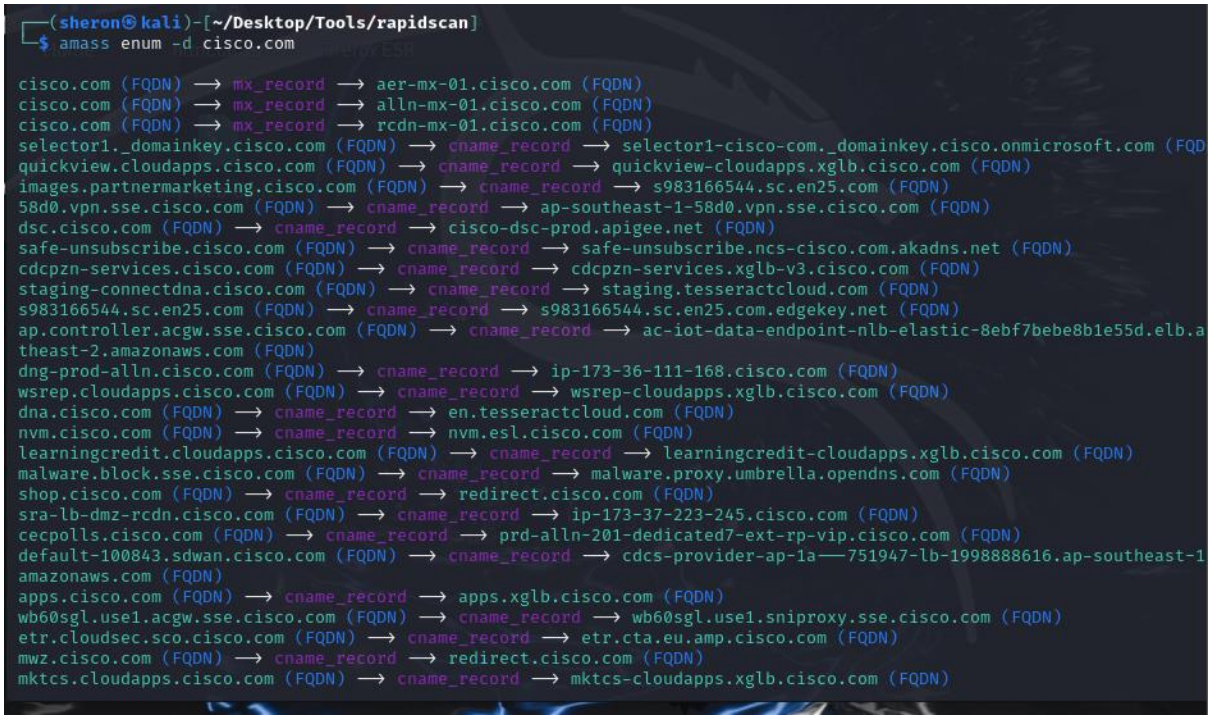
It is possible to use tools like **impulse** to test DoS vulnerabilities. But it is not in scope to test DoS vulnerabilities.



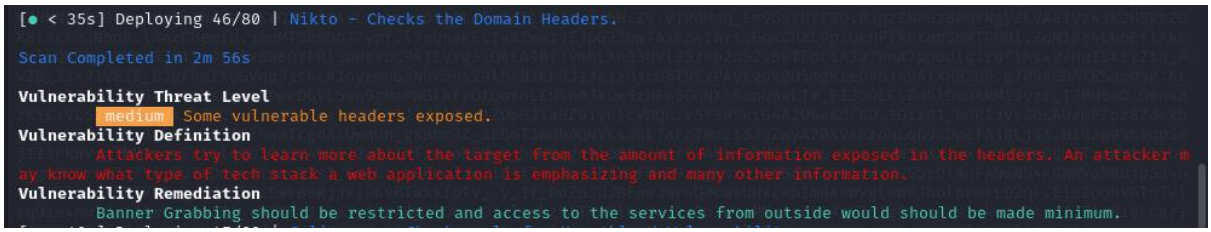
Third Vulnerability – This is a **subdomain enumeration** vulnerablitiy. This helps the attacker to gain crutial information about the architecture of the web application. Amass can be used to do subdomain enumeration.



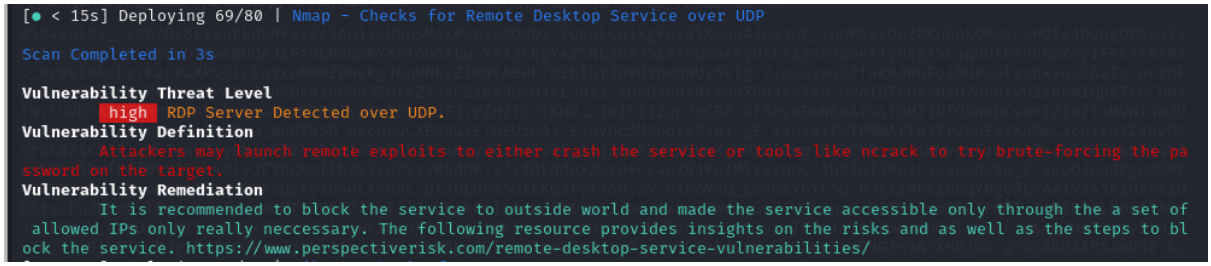
This is a output of an **Amass** scan. It shows details about subdomains as follows.



Fourth vulnerability – Vulnerable headers open is a medium level vulnerability. This can help the attacker to gather information about the target. It gives away the architecture of the website.



Fifth vulnerability – This vulnerability is regarding **RDP over UDP.** Attacker can use a desktop remotely if attacking is possible.



Sixth vulnerability – This is a vulnerability is a **plain text injection attack.** That allows man in the middle attackers to insert data into HTTPs sessions.

3. Affected Components

This tool lets us find the web application details that website is protection. This version and platform information will be crucial for the attacker to bypass and perform malicious acts. According to the scan, it is not protected by a firewall. Meaning this is vulnerable. Attacker can perform malicious act.

Component	Type	Vulnerability	CVE Code	Severity	Impact
jQuery 2.2.4	JavaScript Library	Object Prototype Pollution, Cross-Site Scripting (XSS)	CVE-2019-11358, CVE-2020-11022, CVE-2020-11023	High	Allows unauthorized manipulation of object properties and execution of malicious scripts
Axios 0.21.1	JavaScript Library	Regular Expression Complexity Issue, CSRF Vulnerability, Proxy Authentication Credentials Leak	CVE-2021-3749, CVE-2023-4587, CVE-2025-27152	High	Can allow denial-of-service attacks, unintended user actions, and exposure of sensitive authentication details
Bootstrap 3.4.1	JavaScript Library	Cross-Site Scripting (XSS) Vulnerability	CVE-2024-6484	Medium	Enables execution of malicious scripts, affecting the user interface security
Lodash 4.17.21	JavaScript Library	Prototype Pollution	CVE-2020-8203	Medium	Can allow modification of global JavaScript properties, leading to security misconfigurations
Boomerang 1.718.0	JavaScript Library	Possible Information Disclosure Risks	No confirmed CVEs	Medium	May expose sensitive performance data to unintended parties

FTP Service (Port 21)	Network Protocol	Brute Force Attacks, Sniffing Risks	-	High	Allows attackers to intercept file transfers or escalate privileges through brute-force attempts
PPTP Service (Port 1723)	Network Protocol	Weak Encryption, Brute Force Attacks	-	High	Susceptible to interception and credential theft
SIP Service (Port 5060)	Network Protocol	Eavesdropping Risk	-	High	Potential exposure to unauthorized voice traffic interception
Missing Security Headers	Security Configuration	XSS Risk & Header Exposure	-	High	Can allow execution of unauthorized scripts due to insufficient protection mechanisms
Denial-of-Service (DoS) Vulnerability	Server Protection	Slowloris Attack	-	Critical	Can exhaust server connections, rendering services unavailable
Subdomain Enumeration	Information Disclosure	Exposure of Website Architecture	-	Medium	Allows attackers to gain crucial information about internal systems
RDP over UDP	Remote Desktop Protocol	Brute Force Attacks, Service Crashes	-	High	Attackers can exploit remote access weaknesses and disrupt services
Plain Text Injection	Web Vulnerability	Man-in-the-Middle (MITM) Attack	-	High	Allows attackers to inject arbitrary data into HTTPS sessions, leading to data corruption or phishing risks

4. Vulnerabilities

The following are the most critical vulnerabilities that were identified in the web application.

4.1. XSS

XSS or cross site scripting is used by hackers to run malicious scripts in the web application. Execution of such scripts may lead to,

- **Session Hijacking** – Stealing cookies
- **Credential theft** – fake login forms
- **Phishing attacks** – re directs to malicious sites

- **Malware injection** – can cause download and execute malware on victim
- **Deface the website** – can manipulate the website
- **Bypass access controls** – can manipulate client-side logic to bypass certain logic.

4.2. RDP over UPD

This can cause the following risks

- **Service crashes** – Attackers could possibly exploit this vulnerability to crash RDP service which can cause denial of service.
- **Brute Force Attacks** – By using tools such as ncrack, attackers could try to brute force log in to the system. Causing unauthorized login to system.
- **Exposed Access** – Making RDP service accessible to the outside world increases the attack surface and the server open to be exploited.

4.3. DOS

Denial of service is one of the deadliest vulnerabilities due to its destructive nature. When this vulnerability is exploited, it will render the service un usable. Which could do businesses massive losses. There are many forms of DoS attacks

- Flood Attacks
- Buffer Overflow Attacks
- SYN Flood
- Smurf Attack
- Ping of death

4.4. Plain text injection

Plain Text Injection is a vulnerability where an attacker injects arbitrary text into a web application, causing misleading or manipulated content to be displayed to users. This can be used for content spoofing, phishing, or social engineering attacks by altering messages or error pages,

5. Mitigation

5.1. XSS – Mitigation

Most of the XSS vulnerabilities in this web application is caused by either outdated libraries or due to missing headers. To fix this simply upgrade the Axios, JQuery and boostraps into the latest technologies. And also make sure to add all the missing security headers to prevent attacker from succeeding.

5.2. RDP over UDP – Mitigation

This can be mitigated by restricting access to RDP services by configuring the firewall so that only trusted IP addresses can access the service. Also, regular monitor and patching the service with latest updates is recommended. Finally disable the UDP entirely if not used.

5.3. DoS – Mitigation

In this case make sure to use the latest version of Apache. Other than that make sure to have all technologies updates. Make sure to have unused ports closed. Also make sure to use encrypted communications.

5.4. Plain text injection

To mitigate plain text injection follow the below steps.

- Input validation – make sure that inputs are sanitized
- Content security policy – restrict unauthorized content injection
- Strict user authentication
- Regular security audits

6. Conclusion

The web application www.cisco.com has many vulnerabilities. The most critical ones being XSS attacks due to old components used, plain text injection, and missing headers. This site cannot be recommended to be used until the errors are fixed.