Sri Lanka Institute of Information Technology

Report – Golf Galaxy

IE2062 - Web security

Submitted by:

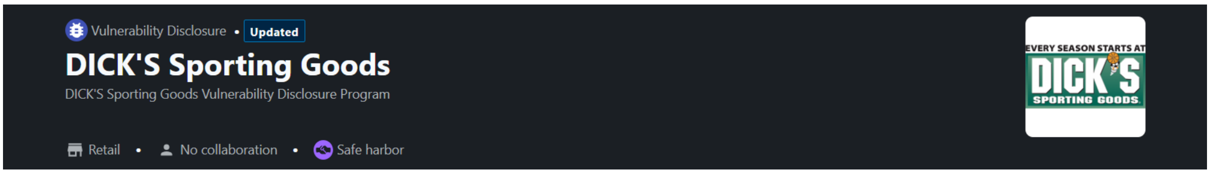
Student Registration Number	Student Name
IT23253476	Bandara S.M.S.N

Date of submission

05/05/2025

Table of Contents

1. Domain: https://www.golfgalaxy.com/

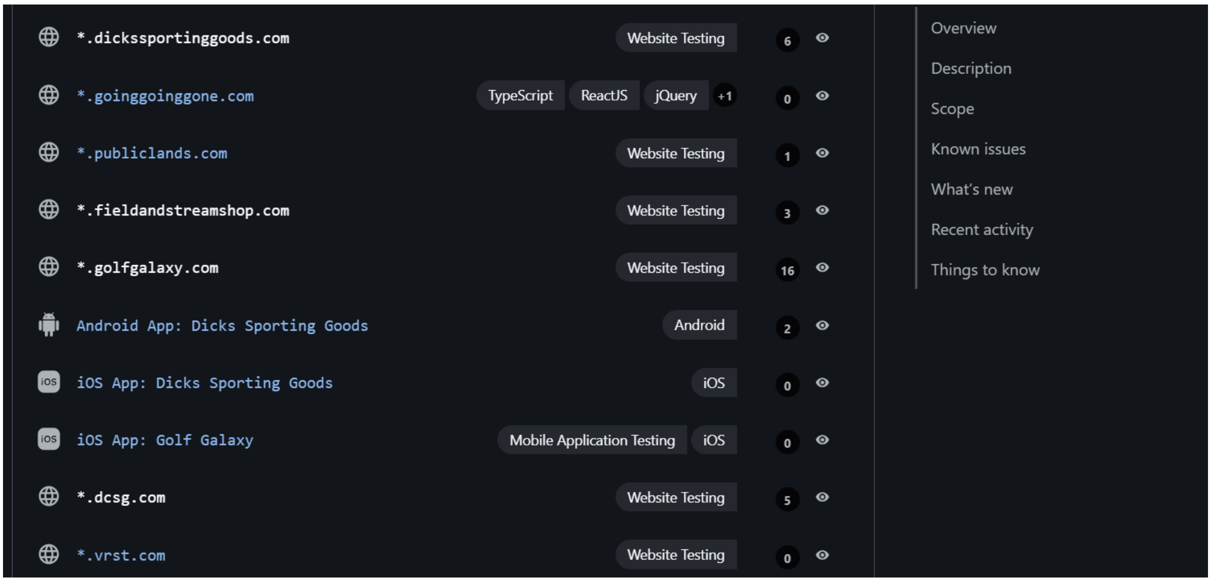


Vulnerability Disclosure • Updated

DICK'S Sporting Goods

DICK'S Sporting Goods Vulnerability Disclosure Program

Retail • No collaboration • Safe harbor



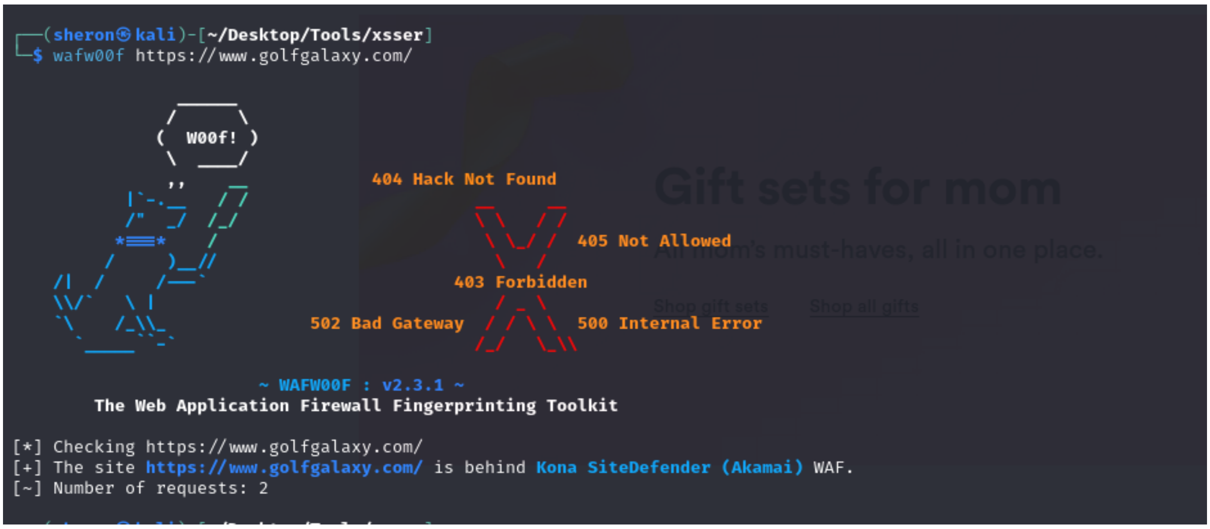
*.dickssportinggoods.com	Website Testing	6
*.goinggoinggone.com	TypeScript ReactJS jQuery +1	0
*.publiclands.com	Website Testing	1
*.fieldandstreamshop.com	Website Testing	3
*.golfgalaxy.com	Website Testing	16
Android App: Dicks Sporting Goods	Android	2
iOS App: Dicks Sporting Goods	iOS	0
iOS App: Golf Galaxy	Mobile Application Testing iOS	0
*.dcsg.com	Website Testing	5
*.vrst.com	Website Testing	0

- Link - https://www.golfgalaxy.com/
- Category – Vulnerability Disclosure Program (VDP)
- Type – Retail Company

2. Scanning

2.1. Wafw00f

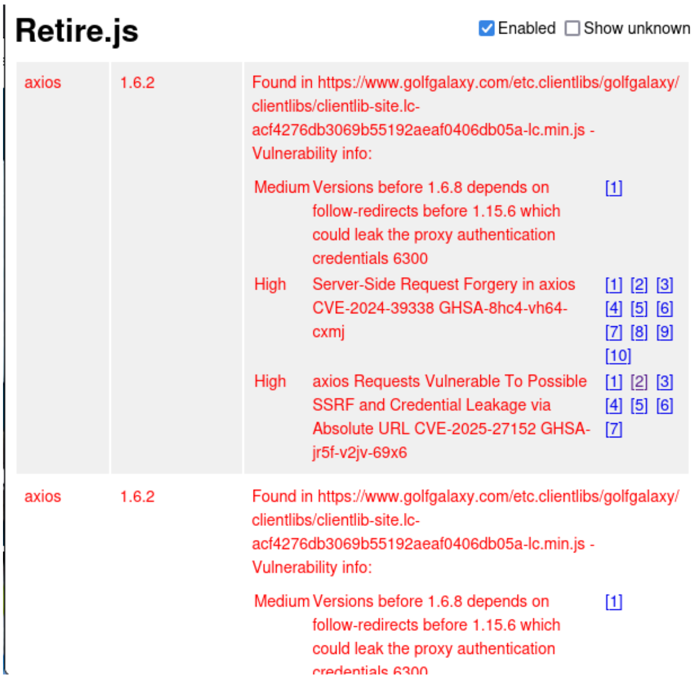
This tool is used to look for the web application firewall used by the web site. By knowing the version, the attacker can try to bypass by exploiting known vulnerabilities of that website. The scan revealed that the web application is using the **Kona Site Defender** firewall.



```
┌──(sheron㉿kali)-[~/Desktop/Tools/xsser]
└─$ wafw00f https://www.golfgalaxy.com/

                    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://www.golfgalaxy.com/
[+] The site https://www.golfgalaxy.com/ is behind Kona SiteDefender (Akamai) WAF.
[~] Number of requests: 2
```

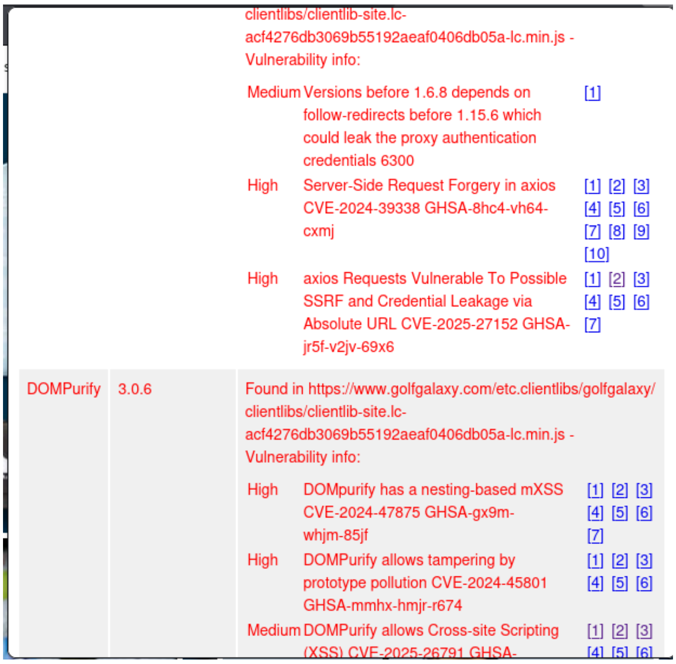
2.2. Retire.js

Retire.js is web page extension which can find vulnerabilities in java script libraries used. It will also give a description of the vulnerability along with links to the full vulnerability details. Scanning the www.golf.galaxy domain the following was discovered.

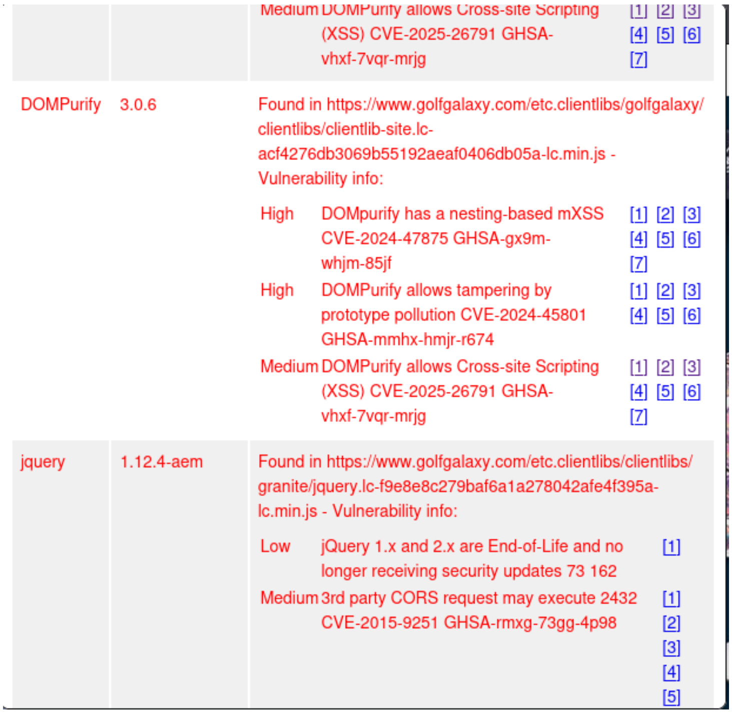


Retire.js ☑ Enabled □ Show unknown

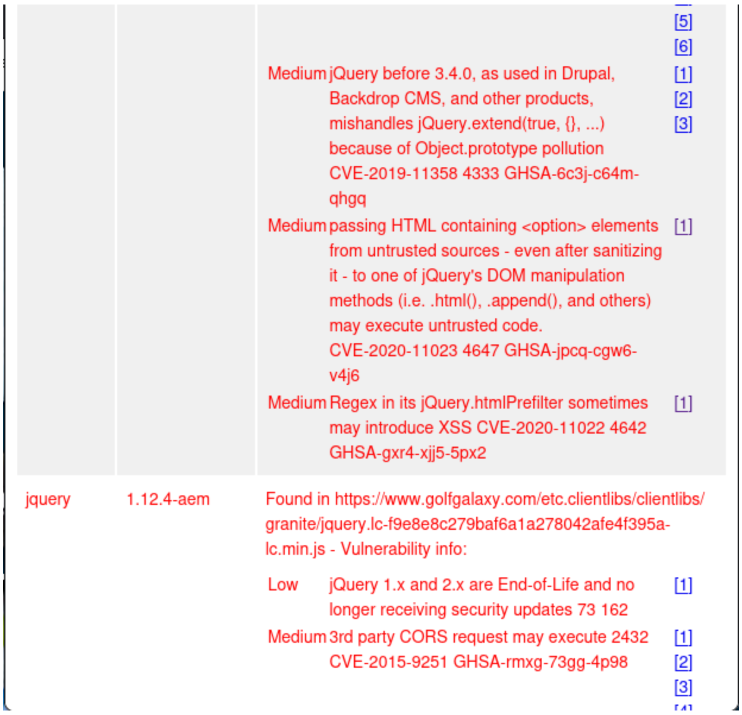
axios	1.6.2	Found in https://www.golfgalaxy.com/etc.clientlibs/golfgalaxy/clientlibs/clientlib-site.lc-acf4276db3069b55192aeaf0406db05a-lc.min.js - Vulnerability info: Medium Versions before 1.6.8 depends on follow-redirects before 1.15.6 which could leak the proxy authentication credentials 6300 [1] High Server-Side Request Forgery in axios CVE-2024-39338 GHSA-8hc4-vh64-cxmj [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] 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]
axios	1.6.2	Found in https://www.golfgalaxy.com/etc.clientlibs/golfgalaxy/clientlibs/clientlib-site.lc-acf4276db3069b55192aeaf0406db05a-lc.min.js - Vulnerability info: Medium Versions before 1.6.8 depends on follow-redirects before 1.15.6 which could leak the proxy authentication credentials 6300 [1]



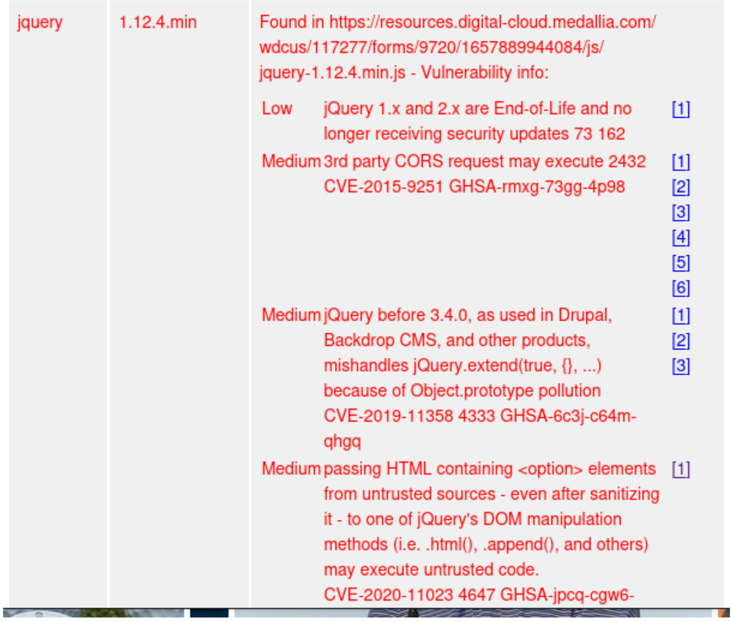
		clientlibs/clientlib-site.lc-acf4276db3069b55192aeaf0406db05a-lc.min.js - Vulnerability info: Medium Versions before 1.6.8 depends on follow-redirects before 1.15.6 which could leak the proxy authentication credentials 6300 [1] High Server-Side Request Forgery in axios CVE-2024-39338 GHSA-8hc4-vh64-cxmj [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] 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]
DOMPurify	3.0.6	Found in https://www.golfgalaxy.com/etc.clientlibs/golfgalaxy/clientlibs/clientlib-site.lc-acf4276db3069b55192aeaf0406db05a-lc.min.js - Vulnerability info: High DOMpurify has a nesting-based mXSS CVE-2024-47875 GHSA-gx9m-whjm-85jf [1] [2] [3] [4] [5] [6] [7] High DOMPurify allows tampering by prototype pollution CVE-2024-45801 GHSA-mmhx-hmjr-r674 [1] [2] [3] [4] [5] [6] Medium DOMPurify allows Cross-site Scripting (XSS) CVE-2025-26791 GHSA- [1] [2] [3] [4] [5] [6]



		Medium	DOMPurify allows Cross-site Scripting (XSS) CVE-2025-26791 GHSA-vhxf-7vqr-mrjg	[1] [2] [3] [4] [5] [6] [7]
DOMPurify	3.0.6		Found in https://www.golfgalaxy.com/etc.clientlibs/golfgalaxy/clientlibs/clientlib-site.lc-acf4276db3069b55192aeaf0406db05a-lc.min.js - Vulnerability info:	
		High	DOMpurify has a nesting-based mXSS CVE-2024-47875 GHSA-gx9m-whjm-85jf	[1] [2] [3] [4] [5] [6] [7]
		High	DOMPurify allows tampering by prototype pollution CVE-2024-45801 GHSA-mmhx-hmjr-r674	[1] [2] [3] [4] [5] [6]
		Medium	DOMPurify allows Cross-site Scripting (XSS) CVE-2025-26791 GHSA-vhxf-7vqr-mrjg	[1] [2] [3] [4] [5] [6] [7]
jquery	1.12.4-aem		Found in https://www.golfgalaxy.com/etc.clientlibs/clientlibs/granite/jquery.lc-f9e8e8c279baf6a1a278042afe4f395a-lc.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]



				[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]
jquery	1.12.4-aem		Found in https://www.golfgalaxy.com/etc.clientlibs/clientlibs/granite/jquery.lc-f9e8e8c279baf6a1a278042afe4f395a-lc.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]



jquery	1.12.4.min		Found in https://resources.digital-cloud.medallia.com/wdcus/117277/forms/9720/1657889944084/js/jquery-1.12.4.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-	[1]

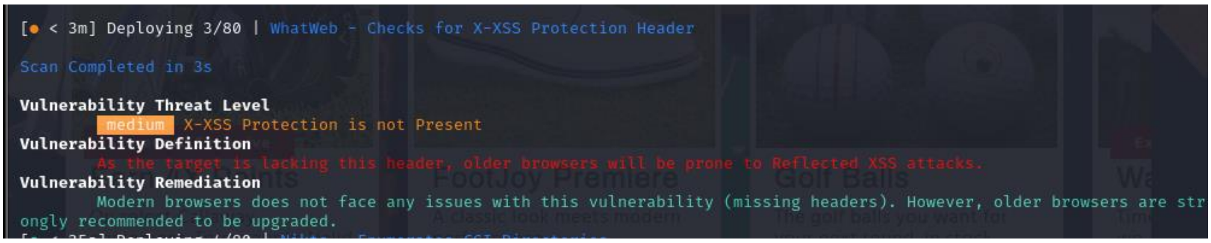
The retire.js has found numerous vulnerabilities in the web application. It has found large amount of high and medium level of severity vulnerabilities. The found vulnerabilities are as follows.

CVE Code	Short Description
CVE-2024-39338	A Server-Side Request Forgery (SSRF) vulnerability in Axios, caused by processing path-relative URLs as protocol-relative URLs2.
CVE-2025-27152	Another SSRF vulnerability in Axios, where absolute URLs bypass the baseURL setting, potentially leading to credential leakage4.
CVE-2024-47875	DOMPurify was vulnerable to nesting-based mXSS attacks, allowing bypass of sanitization and injection of malicious scripts[&#95;{{{CITATION{{{&#95;6{Cross-site Scripting (XSS) in dompurify
CVE-2024-45801	DOMPurify suffered from Prototype Pollution, enabling attackers to bypass depth checks and execute cross-site scripting (XSS) attacks[&#95;{{{CITATION{{{&#95;8{Prototype Pollution in dompurify
CVE-2019-11358	A Prototype Pollution vulnerability in jQuery, where the extend function could modify the Object.prototype, affecting all objects[&#95;{{{CITATION{{{&#95;9{Prototype Pollution in jquery
CVE-2020-11023	In jQuery, passing HTML with <option> elements from untrusted sources to DOM manipulation methods could execute untrusted code12.

2.3. Rapid Scanner

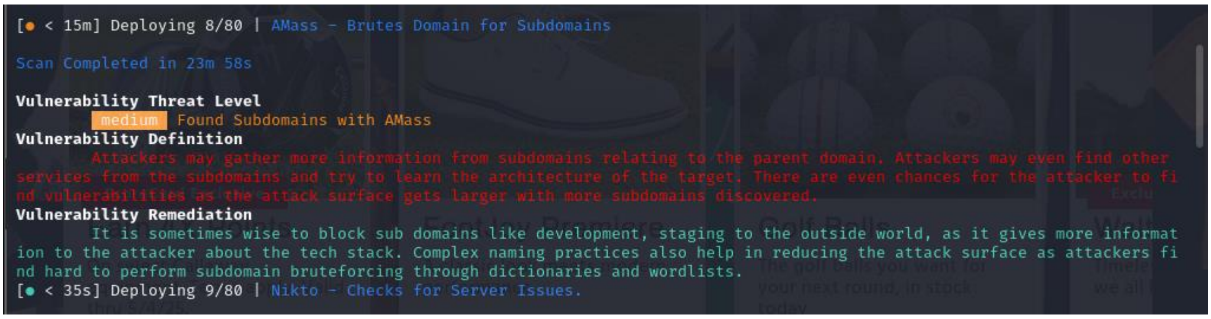
Rapid scanner is a powerful tool to find vulnerabilities in a web application. It uses a combination of 82 tools to find vulnerabilities. After conducting the scanner the following vulnerabilities were discovered.

First Vulnerability – It shows that there is a **XSS (cross site scripting)** due to a missing header. This might not affect to modern browsers, but it may pose a threat to browsers with older versions.



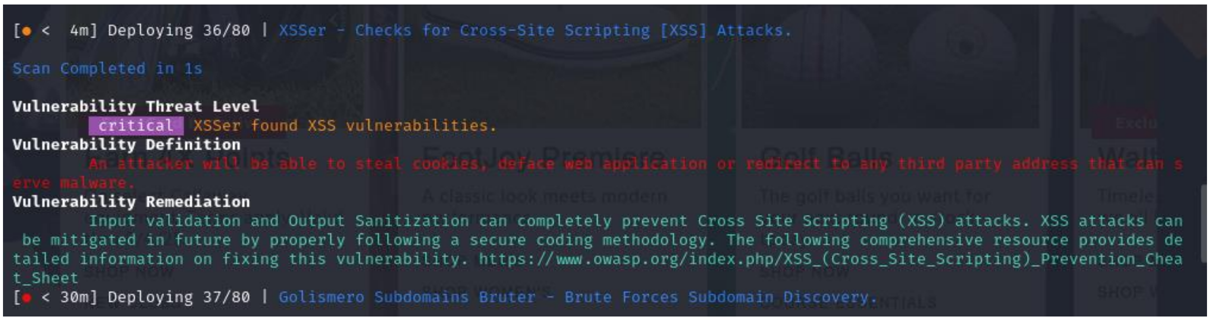
```
[● < 3m] Deploying 3/80 | WhatWeb - Checks for X-XSS Protection Header

Scan Completed in 3s

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 str
ongly recommended to be upgraded.
```

Second Vulnerability – Rapid has found an error in **sub domain enumeration**. It helps the attacker to enumerate subdomains It helps the attacker to gain information to help the damage of the attack done.



```
[● < 15m] Deploying 8/80 | AMass - Brutes Domain for Subdomains

Scan Completed in 23m 58s

Vulnerability Threat Level
         medium  Found Subdomains with AMass
Vulnerability Definition
         Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other
services from the subdomains and try to learn the architecture of the target. There are even chances for the attacker to fi
nd vulnerabilities as the attack surface gets larger with more subdomains discovered.
Vulnerability Remediation
         It is sometimes wise to block sub domains like development, staging to the outside world, as it gives more informat
ion to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface as attackers fi
nd hard to perform subdomain bruteforcing through dictionaries and wordlists.
[● < 35s] Deploying 9/80 | Nikto - Checks for Server Issues.
```

Third Vulnerability – The xxser has found a vulnerability to conduct **xss attacks** through stealing cookies or by redirecting to malicious websites.

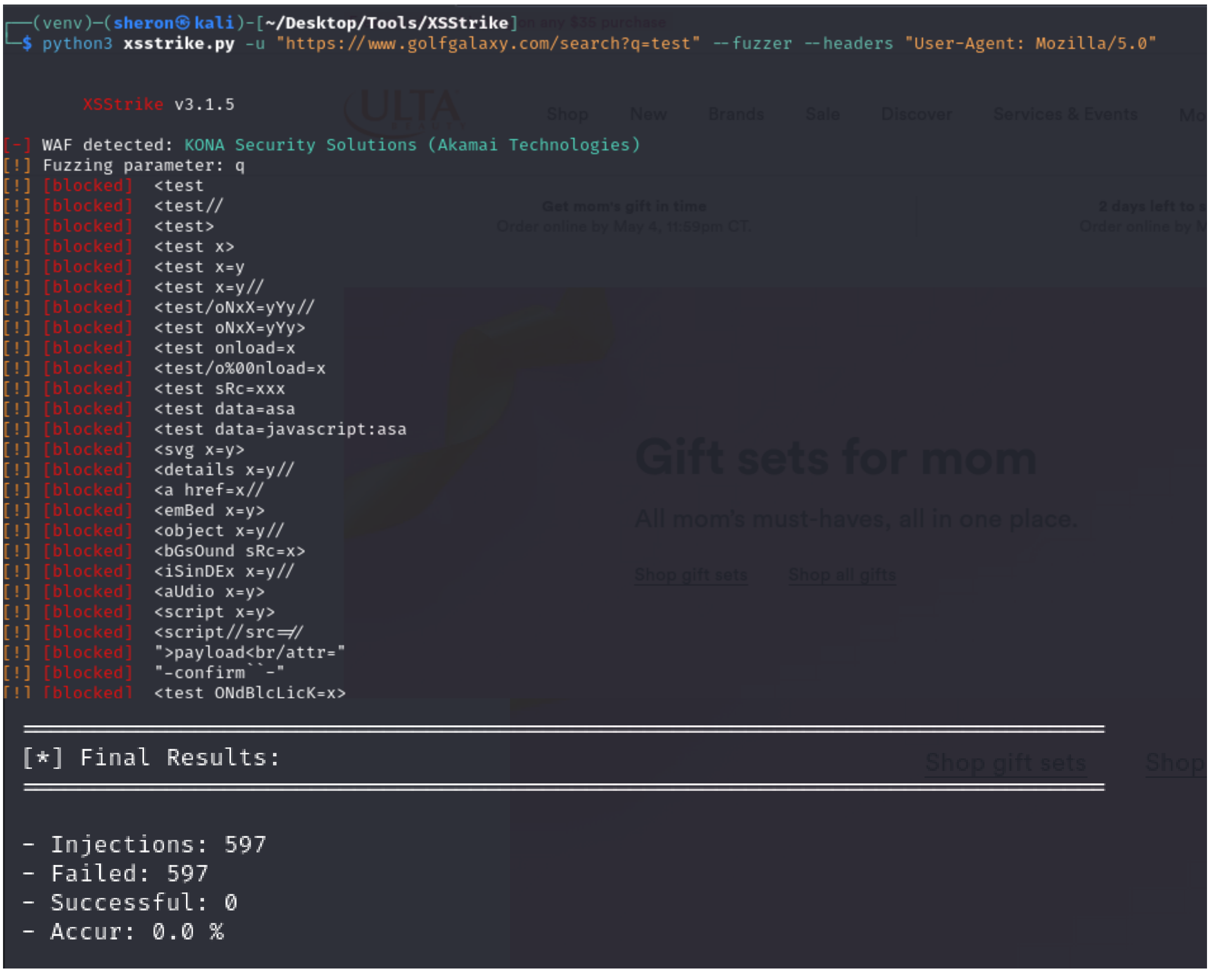


```
[● <  4m] Deploying 36/80 | XSSer - Checks for Cross-Site Scripting [XSS] Attacks.

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 s
erve malware.
Vulnerability Remediation
         Input validation and Output Sanitization can completely prevent Cross Site Scripting (XSS) attacks. XSS attacks can
 be mitigated in future by properly following a secure coding methodology. The following comprehensive resource provides de
tailed information on fixing this vulnerability. https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Chea
t_Sheet
[● < 30m] Deploying 37/80 | Golismero Subdomains Bruter - Brute Forces Subdomain Discovery.
```

Two tools have been used to test for XSS vulnerabilities. They are.

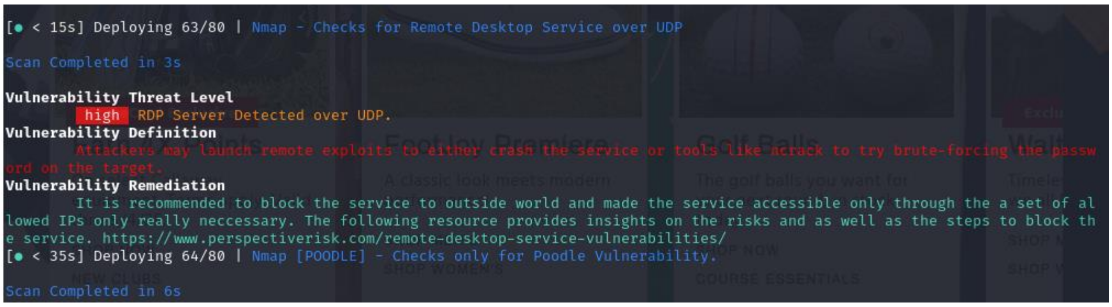
- XSStrike
- XSSer

But neither gave us a successful hit. Suspecting the reason being the firewall blocking the payloads. So further testing is needed to test the payload.



```
┌──(venv)─(sheron㉿kali)-[~/Desktop/Tools/XSStrike]
└─$ python3 xsstrike.py -u "https://www.golfgalaxy.com/search?q=test" --fuzzer --headers "User-Agent: Mozilla/5.0"

        XSStrike v3.1.5

[-] WAF detected: KONA Security Solutions (Akamai Technologies)
[!] Fuzzing parameter: q
[!] [blocked]  <test
[!] [blocked]  <test//
[!] [blocked]  <test>
[!] [blocked]  <test x>
[!] [blocked]  <test x=y
[!] [blocked]  <test x=y//
[!] [blocked]  <test/oNxX=yYy//
[!] [blocked]  <test oNxX=yYy>
[!] [blocked]  <test onload=x
[!] [blocked]  <test/o%00nload=x
[!] [blocked]  <test sRc=xxx
[!] [blocked]  <test data=asa
[!] [blocked]  <test data=javascript:asa
[!] [blocked]  <svg x=y>
[!] [blocked]  <details x=y//
[!] [blocked]  <a href=x//
[!] [blocked]  <emBed x=y>
[!] [blocked]  <object x=y//
[!] [blocked]  <bGsOund sRc=x>
[!] [blocked]  <iSinDEx x=y//
[!] [blocked]  <aUdio x=y>
[!] [blocked]  <script x=y>
[!] [blocked]  <script//src=//
[!] [blocked]  ">payload<br/attr="
[!] [blocked]  "-confirm``-"
[!] [blocked]  <test ONdBlcLicK=x>

 ══════════════════════════════════════════════════════════════════
 [*] Final Results:
 ══════════════════════════════════════════════════════════════════

 - Injections: 597
 - Failed: 597
 - Successful: 0
 - Accur: 0.0 %
```

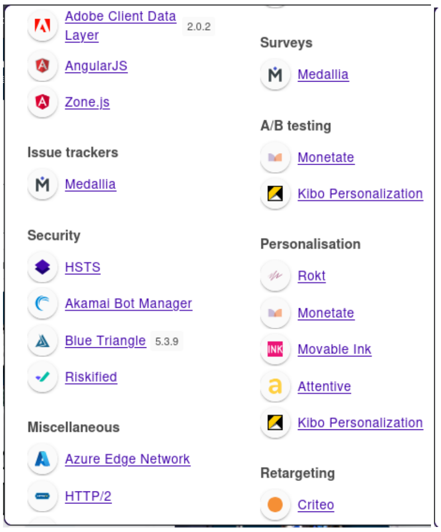
Fourth vulnerability – The vulnerability described in the image relates to the **Remote Desktop Protocol (RDP) being accessible over UDP**. Attackers may exploit the service remotely to crash the server. Brute-force password attacks using tools like ncrack are possible, which compromises system security.



```
[● < 15s] Deploying 63/80 | Nmap - Checks for Remote Desktop Service over UDP

Scan Completed in 3s

Vulnerability Threat Level
        high  RDP Server Detected over UDP.
Vulnerability Definition
        Attackers may launch remote exploits to either crash the service or tools like ncrack to try brute-forcing the passw
ord on the target.
Vulnerability Remediation
        It is recommended to block the service to outside world and made the service accessible only through the a set of al
lowed IPs only really neccessary. The following resource provides insights on the risks and as well as the steps to block th
e service. https://www.perspectiverisk.com/remote-desktop-service-vulnerabilities/
[● < 35s] Deploying 64/80 | Nmap [POODLE] - Checks only for Poodle Vulnerability.

Scan Completed in 6s
```

2.4. Wappalyzer

This is browser extension which can be used to identify what technologies are used in the web application. And also, you can find the versions of the technologies used. Which can be used to carry out attacks.



Adobe Client Data Layer 2.0.2
AngularJS
Zone.js

Issue trackers
Medallia

Security
HSTS
Akamai Bot Manager
Blue Triangle 5.3.9
Riskified

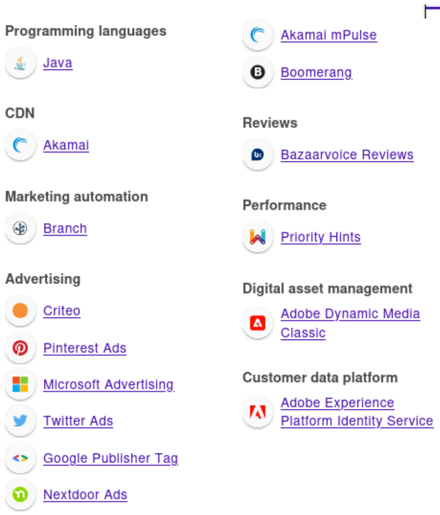
Miscellaneous
Azure Edge Network
HTTP/2

Surveys
Medallia

A/B testing
Monetate
Kibo Personalization

Personalisation
Rokt
Monetate
Movable Ink
Attentive
Kibo Personalization

Retargeting
Criteo



Programming languages
Java

CDN
Akamai

Marketing automation
Branch

Advertising
Criteo
Pinterest Ads
Microsoft Advertising
Twitter Ads
Google Publisher Tag
Nextdoor Ads

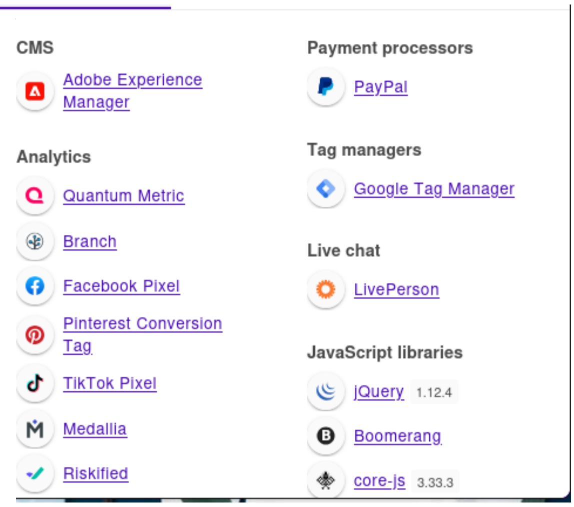
Akamai mPulse
Boomerang

Reviews
Bazaarvoice Reviews

Performance
Priority Hints

Digital asset management
Adobe Dynamic Media Classic

Customer data platform
Adobe Experience Platform Identity Service



CMS
Adobe Experience Manager

Analytics
Quantum Metric
Branch
Facebook Pixel
Pinterest Conversion Tag
TikTok Pixel
Medallia
Riskified

Payment processors
PayPal

Tag managers
Google Tag Manager

Live chat
LivePerson

JavaScript libraries
jQuery 1.12.4
Boomerang
core-js 3.33.3

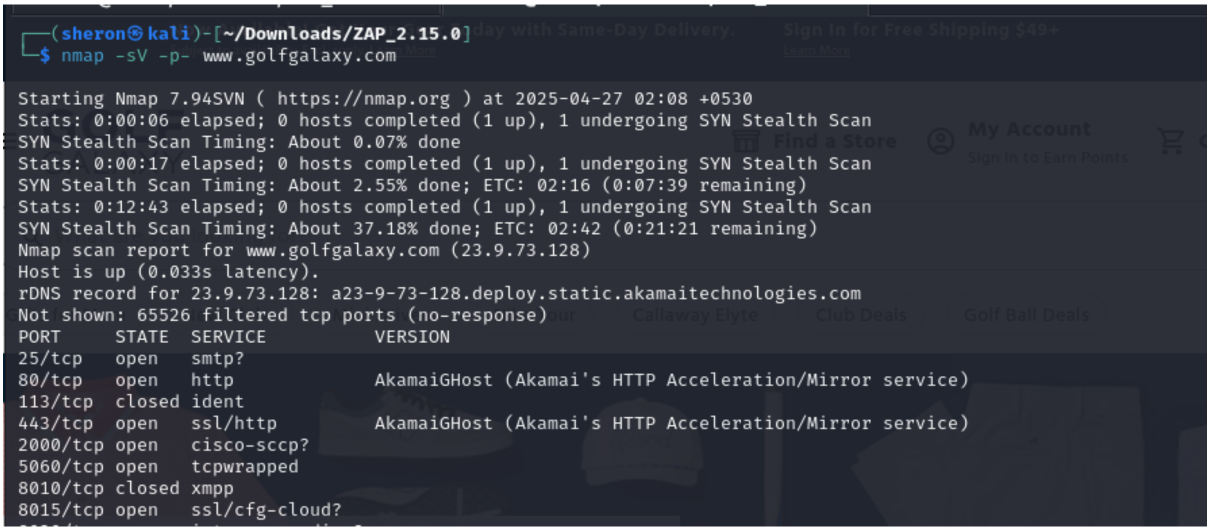
Following were the vulnerabilities of the old versions used. And also, this has confirmed some of the vulnerabilities found from retire.js

Platform Name	CVE Code	Vulnerability Description	Version Used	Latest Version
jQuery	CVE-2020-11022	Prototype pollution vulnerability in jQuery 3.4.0 to 3.5.0 allows attackers to inject properties into JavaScript objects.	3.4.0 to 3.5.0	3.6.0
jQuery	CVE-2020-11023	Cross-site scripting (XSS) vulnerability in jQuery 3.4.0 to 3.5.0 allows attackers to execute arbitrary code.	3.4.0 to 3.5.0	3.6.0
Java	CVE-2022-21449	Vulnerability in Java SE allows unauthenticated attacker to cause a denial of service.	17.0.2 and 18	19
Java	CVE-2021-44228	Remote code execution vulnerability in Apache Log4j 2.x before 2.15.0.	2.0-beta9 to 2.15.0	2.17.1

PayPal	CVE-2019-11358	Cross-site scripting (XSS) vulnerability in PayPal's checkout system.	Before 3.4.0	3.6.0
core-js	CVE-2020-7661	Prototype pollution vulnerability in core-js before 3.6.5 allows attackers to inject properties into JavaScript objects.	Before 3.6.5	3.41.0
Akamai	CVE-2021-22901	Vulnerability in Akamai's CDN allows attackers to bypass security controls.	curl 7.75.0 to 7.76.1	curl 7.77.0
Adobe Experience Manager	CVE-2021-21017	Cross-site scripting (XSS) vulnerability in Adobe Experience Manager versions 6.5.6.0 and earlier.	6.5.6.0 and earlier	6.5.7.0
Adobe Experience Manager	CVE-2021-21018	Arbitrary code execution vulnerability in Adobe Experience Manager versions 6.5.6.0 and earlier.	6.5.6.0 and earlier	6.5.7.0

2.5. Nmap Scan

The nmap scan will reveal any open ports which attacker may attempt to exploit. This tool can be used to get a general idea of what the system does. The nmap scan on this domain revealed the following.



```
┌──(sheron㉿kali)-[~/Downloads/ZAP_2.15.0]
└─$ nmap -sV -p- www.golfgalaxy.com

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-27 02:08 +0530
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.07% done
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.55% done; ETC: 02:16 (0:07:39 remaining)
Stats: 0:12:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 37.18% done; ETC: 02:42 (0:21:21 remaining)
Nmap scan report for www.golfgalaxy.com (23.9.73.128)
Host is up (0.033s latency).
rDNS record for 23.9.73.128: a23-9-73-128.deploy.static.akamaitechnologies.com
Not shown: 65526 filtered tcp ports (no-response)
PORT     STATE  SERVICE         VERSION
25/tcp   open   smtp?
80/tcp   open   http            AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
113/tcp  closed ident
443/tcp  open   ssl/http        AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
2000/tcp open   cisco-sccp?
5060/tcp open   tcpwrapped
8010/tcp closed xmpp
8015/tcp open   ssl/cfg-cloud?
```

3. Components Affected

The following is a summarization of the affected components that were discovered from testing.

Component	Type	Vulnerability	CVE Code	Severity	Impact
Axios	JavaScript Library	Server-Side Request Forgery (SSRF)	**CVE-2024-39338, CVE-2025-27152**	High	Allows an attacker to make unauthorized requests, leading to data leakage and internal service exposure
DOMPurify	JavaScript Library	Cross-Site Scripting (XSS) & Prototype Pollution	**CVE-2024-47875, CVE-2024-45801**	High	Enables attackers to bypass sanitization and execute malicious scripts
jQuery	JavaScript Library	Prototype Pollution	**CVE-2019-11358, CVE-2020-11022, CVE-2020-11023**	Medium to High	Allows modification of object properties, leading to unexpected application behavior
Java	Programming Language	Denial of Service (DoS)	**CVE-2022-21449**	High	Allows unauthenticated attackers to disrupt services
Apache Log4j	Java Logging Utility	Remote Code Execution	**CVE-2021-44228**	Critical	Allows attackers to execute arbitrary code remotely
PayPal Checkout	Payment Service	Cross-Site Scripting (XSS)	**CVE-2019-11358**	Medium	Attackers can inject malicious scripts
core-js	JavaScript Library	Prototype Pollution	**CVE-2020-7661**	Medium	Can lead to unexpected JavaScript behavior
Akamai CDN	Content Delivery Network	Security Bypass	**CVE-2021-22901**	High	Allows attackers to bypass security controls
Adobe Experience Manager	Web CMS	XSS & Arbitrary Code Execution	**CVE-2021-21017, CVE-2021-21018**	High	Can lead to malicious script execution or system compromise
SNMP Service	Network Service	Exposure of community strings	N/A	Medium	Allows unauthorized access to network device information
HTTP/2	Network Protocol	Rapid Reset Attack (DoS)	**CVE-2023-44487**	High	Can overwhelm a server, causing denial of service
RDP Server (UDP)	Remote Access Protocol	Unrestricted access & brute-force risk	N/A	High	Attackers can exploit the service remotely or launch brute-force password attacks
Missing CSP Header	Security Configuration	Increased risk of XSS & injection attacks	N/A	High	Allows script injection that can compromise users

4. Vulnerabilities

4.1. A Server-Side Request Forgery (SSRF)

A Server-Side Request Forgery (SSRF) vulnerability occurs when an attacker can make the server initiate requests to internal or external systems. This can lead to exposure of internal services, sensitive data, or allow the attacker to exploit trust relationships within the network.

4.2. XSS vulnerability

Cross-Site Scripting (XSS) is a vulnerability that allows an attacker to inject malicious scripts into a trusted website. When a user interacts with the compromised page, the script executes in their browser, potentially leading to session hijacking, credential theft, or defacement. There are many types of xss types

- Stored XSS
- Reflected XSS
- DOM XSS

4.3. Prototype pollution

Prototype Pollution is a vulnerability where an attacker can manipulate a JavaScript object's prototype. This can result in unexpected behavior, application crashes, or even remote code execution, depending on how the application processes user-supplied input.

4.4. Sub domain enumeration

Sub domain enumeration helps the attacker to gather more details about the target. Discovering more details will help the attacker to pull of a more sophisticated attack.

4.5. RDP server over UDP

An RDP server exposed over UDP (via the RDP UDP Transport Protocol) can increase the risk of unauthorized access, brute-force attacks, and exploitation of RDP-specific vulnerabilities. UDP-based connections are also harder to monitor and secure compared to TCP.

5. Mitigation Methods

5.1. Server-side request forgery (SSRF) - fix

The owner of the web application can fix the vulnerability by validating and sanitizing the user supplied URLs. Also, the can implement allow lists or whitelists for necessary domains. And also, to protect internal Ip ranges the web application can block the internal Ips.

5.2. Cross site scripting - fix

First of all, should update the older versions of technologies and frame works used. Afterwards should add all the content security policies (CSP) headers to restrict script execution. Also, should validate all user inputs on both client and server side.

5.3. Prototype Pollution - fix

Update all the frameworks used or use unaffected frameworks. And also strictly validate and sanitize JSON and object-based input data.

5.4. Subdomain Enumeration – fix

Remove any unwanted or un used subdomains. Use firewall to detect and bock any traffic related to enumeration.

5.5. RDP server exposed over UDP – fix

The vulnerability can be mitigated by disabling UDP based RDP transport if it is not required. Also make sure to enable firewall and configure it. Also use strong MFA (multi factor authentication) for RDP logins. Finally make sure to stay up to date.

6. Conclusion

The web application has a plethora of vulnerabilities and therefore be used carefully. The required parties should act upon and must fix the given vulnerabilities so that the users can safely use the system