Sri Lanka Institute of Information Technology

Report – Private Internet Access

IE2062 - Web security

Submitted by:

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

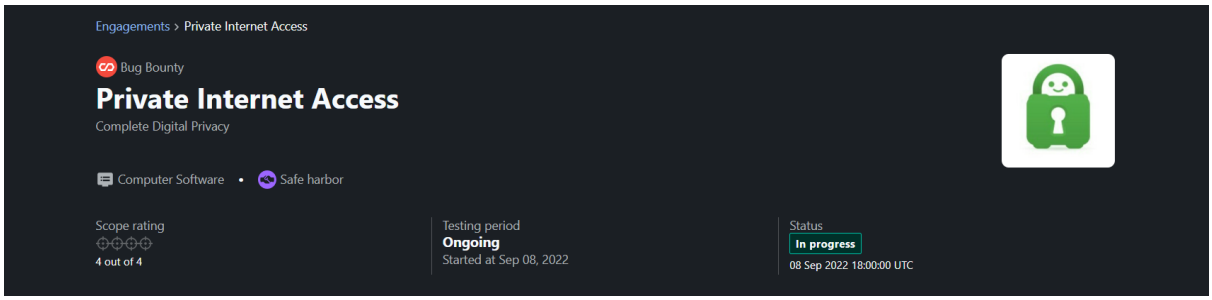
Date of submission

05/05/2025

Table of Contents

1. Domain - https://www.privateinternetaccess.com/ 3
2. Scanning 3
   2.1. Wafw00f 3
   2.2. Wappalyzer 4
   2.3. Retire.js 5
   2.4. Rapid scan 6
   2.5. Amass 9
3. Vulnerability 9
   3.1. XSS 9
   3.2. FTP service 10
4. Mitigation 10
   4.1. XSS – Mitigation 10
   4.2. FTP service – Mitigation 10
5. Vulnerable components 10
6. Conclusion 11

1. Domain - https://www.privateinternetaccess.com/

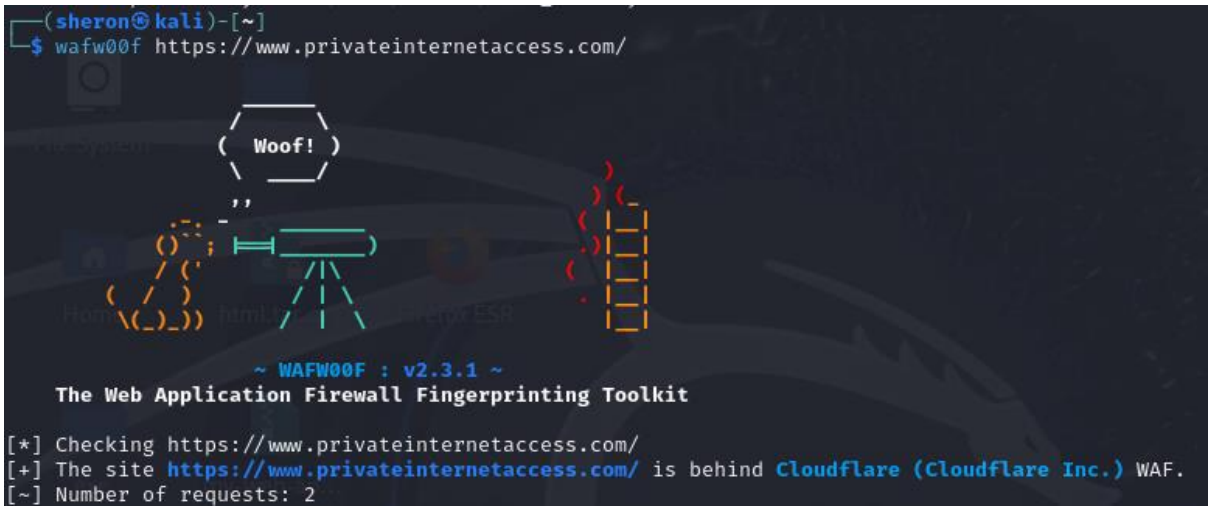


- Link – https://www.privateinternetaccess.com/
- Category – VDP (vulnerability disclosure program)
- Type – Computer software

2. Scanning

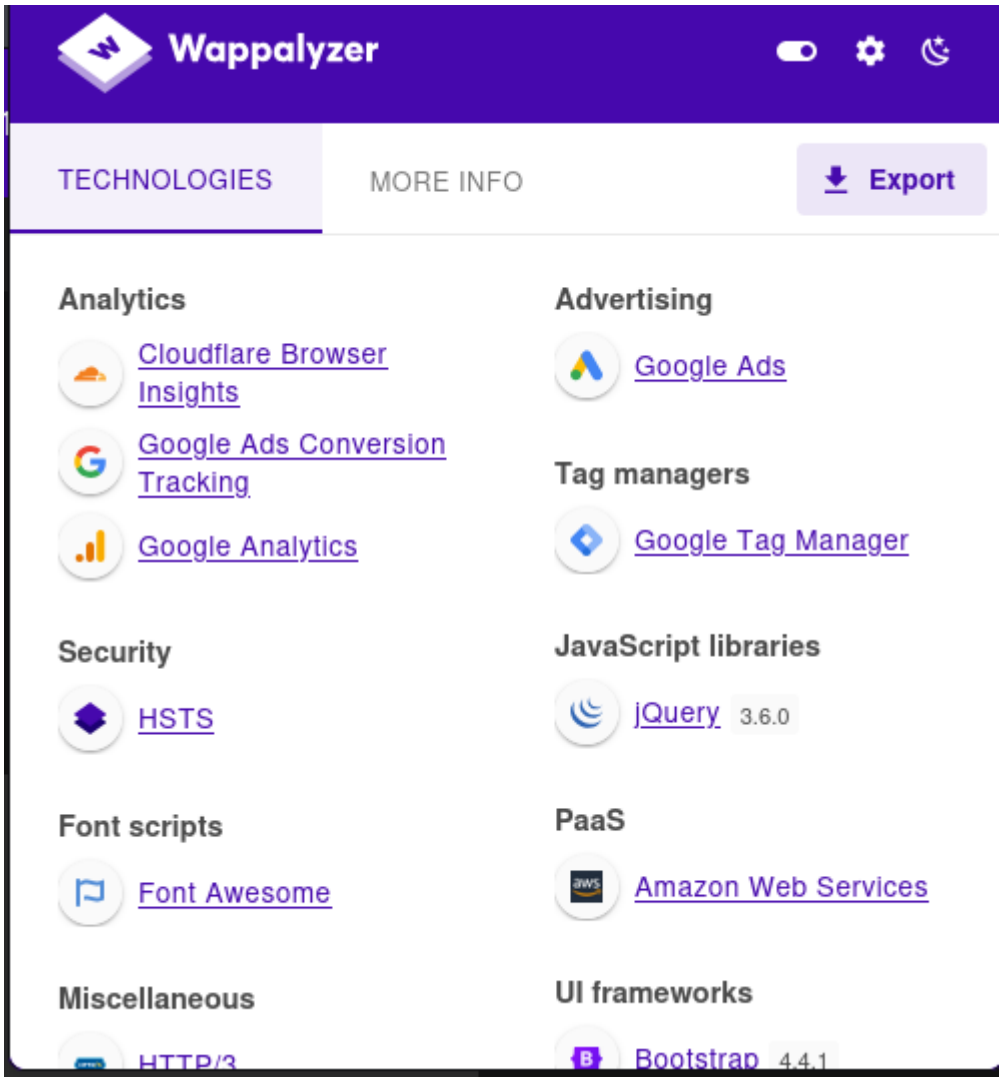
2.1. Wafw00f

This tool is used to find if there is a web application firewall protecting the web application. This information will help the attacker to identify why some of their attacks are not going thorough. And after identifying the firewall used, he can find a way to bypass the firewall to launch attacks. In this web application it uses a firewall Cloudflare.



2.2. Wappalyzer

Wappalzer is a powerful tool which helps to find the technologies used in a web site. This can also reveal the versions used in certain technologies. And some times there might be known vulnerabilities in the versions, potentially enabling the web application to be attacked.



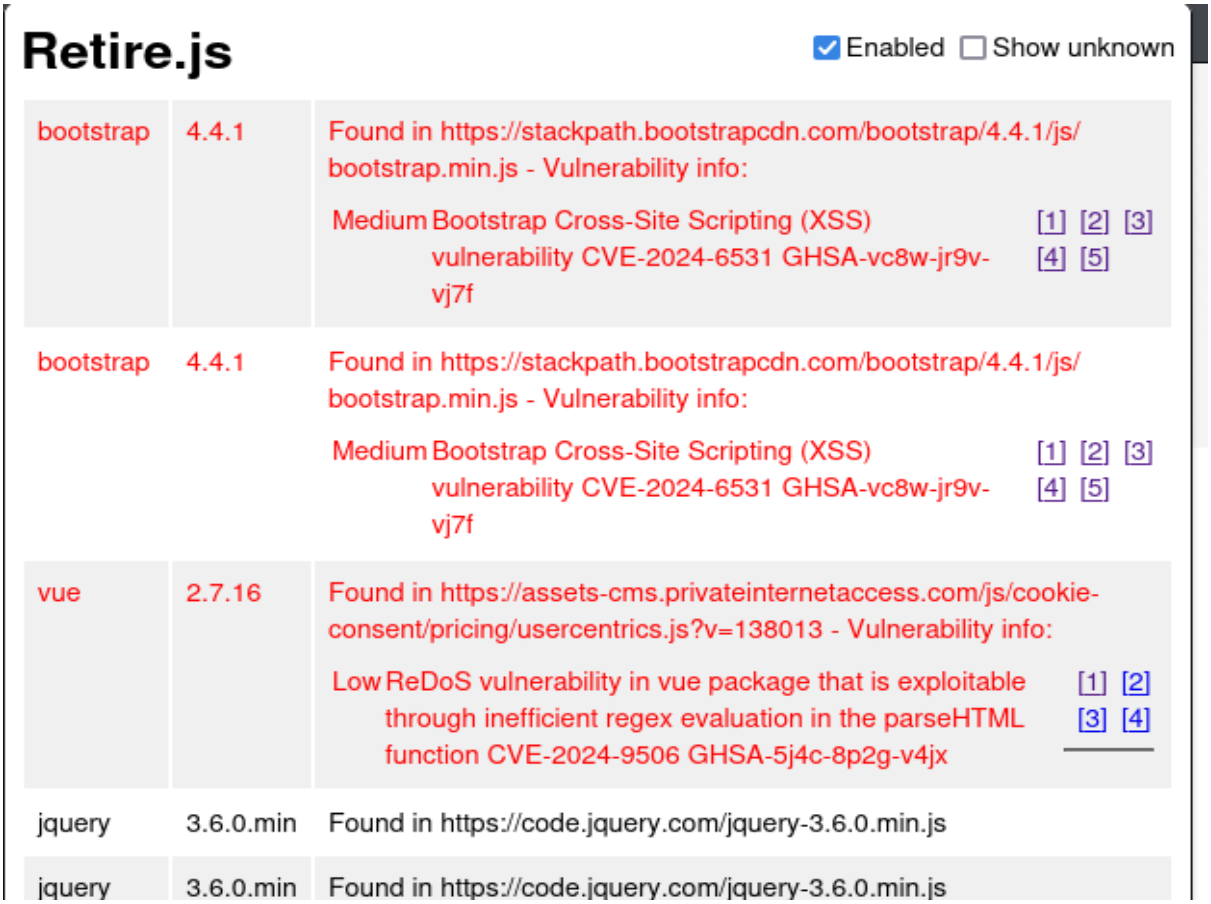
The following vulnerabilities were discovered in he versions that were being used in this site.

Library	Current Version	Latest Version	Security Fixes in Latest Version
Bootstrap	4.4.1	5.3.5	**CVE-2024-6484**: XSS in Carousel component - **CVE-2024-6485**: XSS in Button component - **CVE-2024-6531**: XSS in Carousel component
jQuery	3.6.0	3.7.0	**Prototype Pollution**: Fixed in versions ≥3.4.0 - **Multiple XSS vulnerabilities**: Fixed in versions ≥3.5.0
Leaflet	1.9.4	1.9.4	No direct vulnerabilities reported in this version

2.3. Retire.js

From the initial reconnaissance using the chrome extension retire.js, the vulnerable versions of the javascript libraries used, and a small description of the vulnerability can be retrieved.

According to retire.js, a vulnerability of the boostrap version can be seen. It indicates that a cross-site scripting (XSS) attack is possible with the vulnerable version.



2.4. Rapid scan

Rapid scanner is a powerful tool which can be used to test for vulnerabilities in a web site. It uses a combination of multiple tools to perform 82 scans. This will give us an idea about any existing vulnerabilities in a web application. Following are the found vulnerabilities.

First Vulnerability – This is an **XSS** related vulnerability which was found by the rapid scanner.

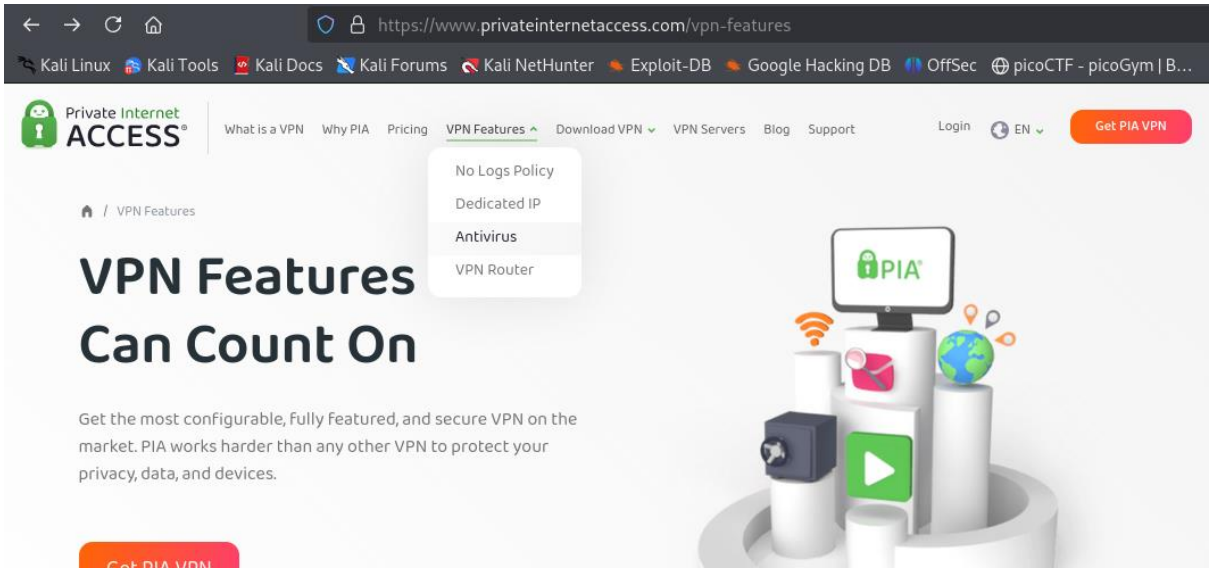
Let us now use the tool **XSStrike** to look for vulnerabilities in the web application.

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

        XSStrike v3.1.5

[~] Crawling the target
──────────────────────────────────────────────────

[+] Vulnerable component: jquery v3.6.0
[!] Component location: https://code.jquery.com/jquery-3.6.0.min.js
[!] Total vulnerabilities: 0
──────────────────────────────────────────────────

[+] Vulnerable component: bootstrap v4.4.1
[!] Component location: https://stackpath.bootstrapcdn.com/bootstrap/4.4.1/js/bootstrap.min.js
[!] Total vulnerabilities: 0
──────────────────────────────────────────────────

[+] Potentially vulnerable objects found at http://www.privateinternetaccess.com/search.php
──────────────────────────────────────────────────
```

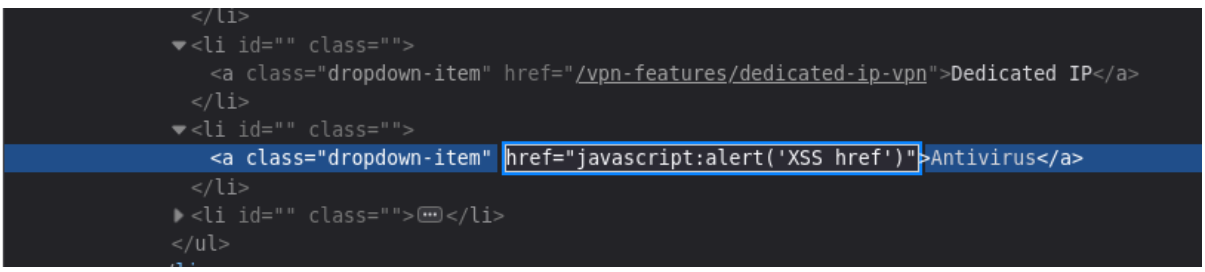
The scanner was able to identify two components jQuery and boostrap libraries and also some poor coding mistakes that allow the attacker to perform XSS attacks.

Proof of concept of a reflected XSS attack

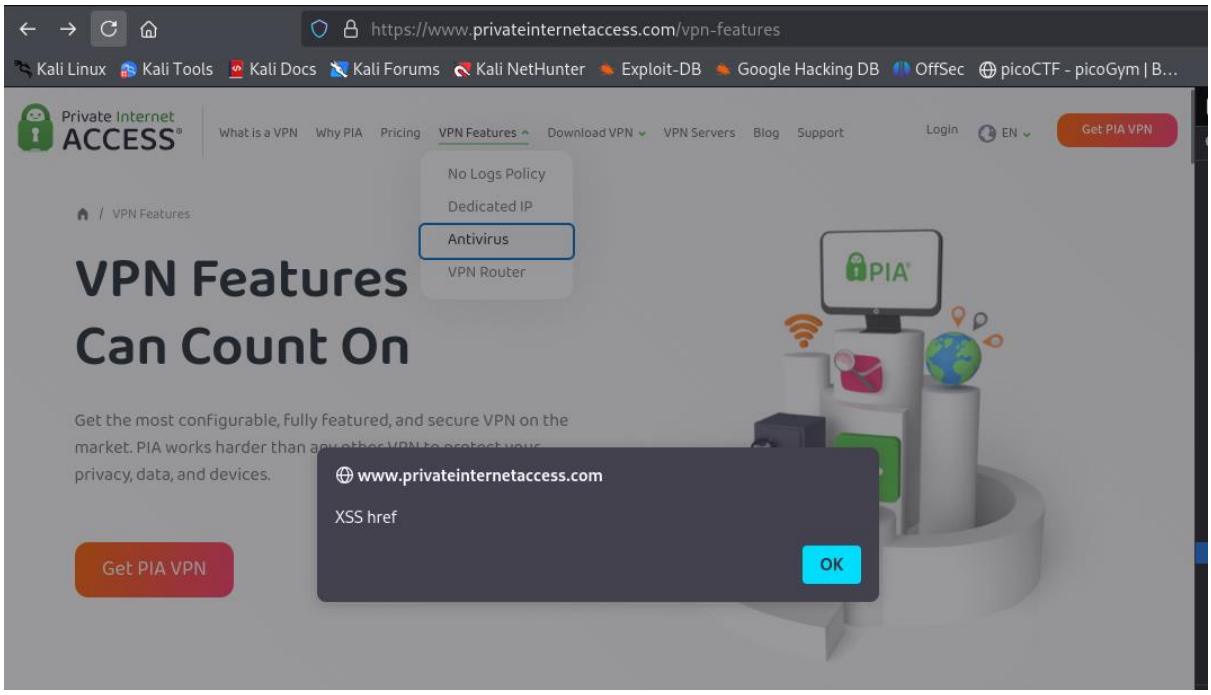
To conduct the exploit first find an <a> tag in the web page and use. Add a href to the <a> tag to run the script.



Now change the values of the original <a> tag into the following.



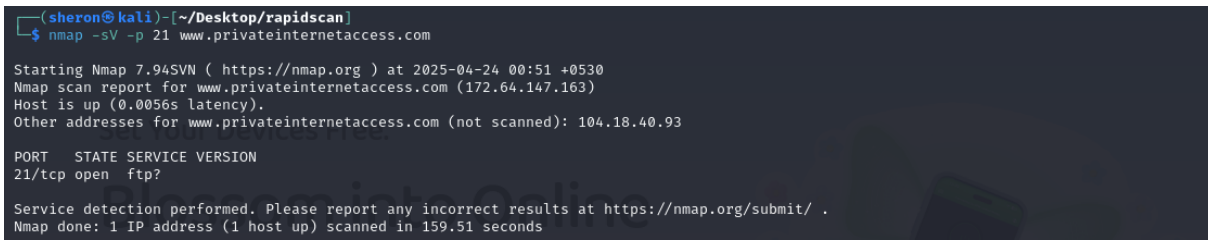
You can see that the attack has **successfully** taken place.



Second Vulnerability - This vulnerability is related to **FTP service,** was discovered was also discovered by the rapid scanner and then was confirmed by the nmap scan.

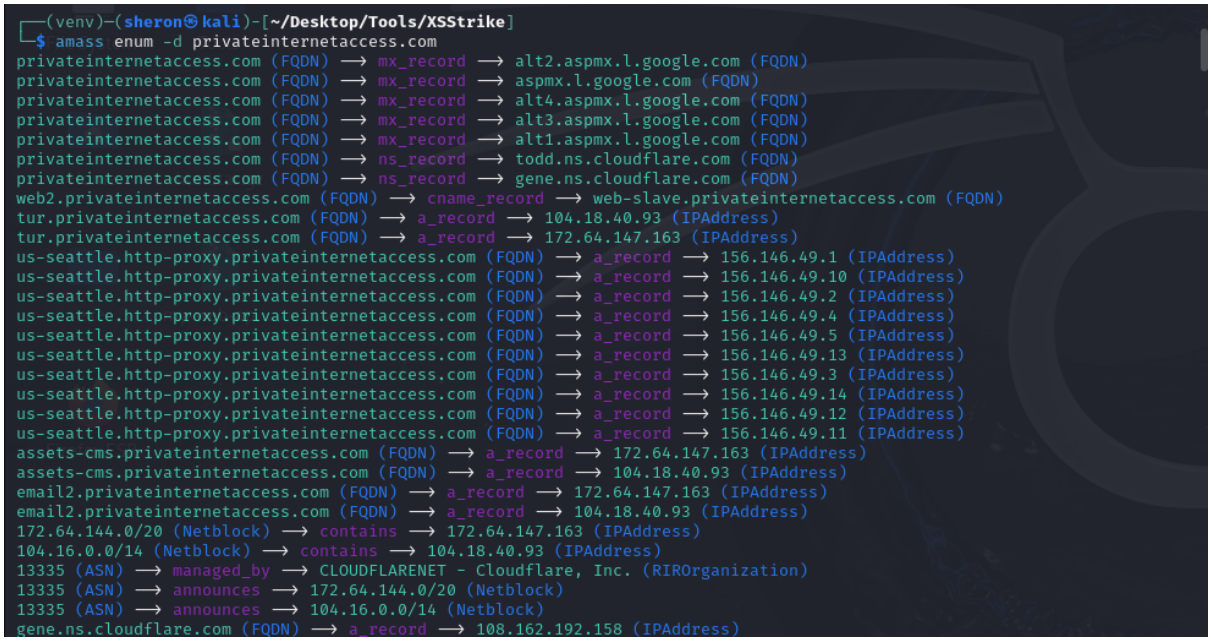
Rapid scan:

Nmap scan:



2.5. Amass

This is a tool which can be used for reconnaissance an as an mapping tool, which is mainly used for subdomain enumeration. The following is a small part of the subdomains discovered.



3. Vulnerability

The following are some of the main vulnerabilities which were identified in the web application.

3.1. XSS

In XSS vulnerabilities, the threat agent can inject malicious scripts (mainly javascripts) into web pages viewed by other users. This vulnerability occurs due to in proper user input sanitisation. The threat agent can run destructive codes, steal cookies or compromise users' systems by exploiting these vulnerabilities. There are many types of XSS attack types. Most popular once being,

- Reflected XSS
- Stored XSS
- DOM XSS

3.2. FTP service

If a FTP server is misconfigured it may cause anonymous access. So that users can log in without credentials. This can lead to unauthorized access to sensitive files or directories. If a server is outdated, it may cause,

- Buffer overflows
- Clear text credential exposure
- Privilege escalation
- Directory Traversal

4. Mitigation

4.1. XSS – Mitigation

Fix for the XSS vulnerability is simply upgrading to newer versions of the boostrap and other libraries and frameworks.

4.2. FTP service – Mitigation

If an FTP port is open, it doesn't necessarily mean that it is vulnerable. But since it is transmitting in plain text there is a chance of man in the middle attacks. So, it is better to use FTP Secure of SFTP as a safety measure. Or if it is not being used better to close the port.

5. Vulnerable components

After scanning the web application some components were found which were vulnerable. It is recommended to get rid of such components.

Component	Version used	Latest Version	Vulnerabilities
Bootstrap	4.4.1	5.3.5	- CVE-2024-6484: XSS in Carousel component - CVE-2024-6485: XSS in Button component - CVE-2024-6531: XSS in Carousel component

jQuery	3.6.0	3.7.0	- Prototype Pollution (Fixed in versions ≥3.4.0) - Multiple XSS vulnerabilities (Fixed in versions ≥3.5.0)
Leaflet	1.9.4	1.9.4	No direct vulnerabilities reported in this version
FTP Service	N/A	N/A	- Anonymous access due to misconfiguration - Buffer overflows - Clear-text credential exposure - Privilege escalation - Directory traversal

6. Conclusion

From the scanning that has been done we can see a an XSS vulnerability and a FTP server outdated vulnerability in this domain. If the version is updated to the latest versions, the vulnerabilities can be mitigated. The website seems to be an older website hence the presence of vulnerabilities in the older versions.