Sri Lanka Institute of Information Technology

Report – World Star Hip Hop

IE2062 - Web security

Submitted by:

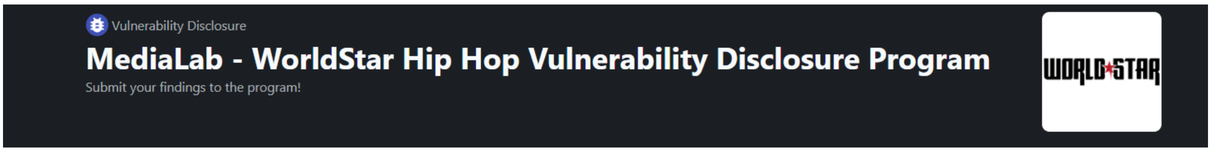
Student Registration Number	Student Name
IT23253476	Bandara S.M.S.N

Date of submission

05/05/2025

Table of Contents

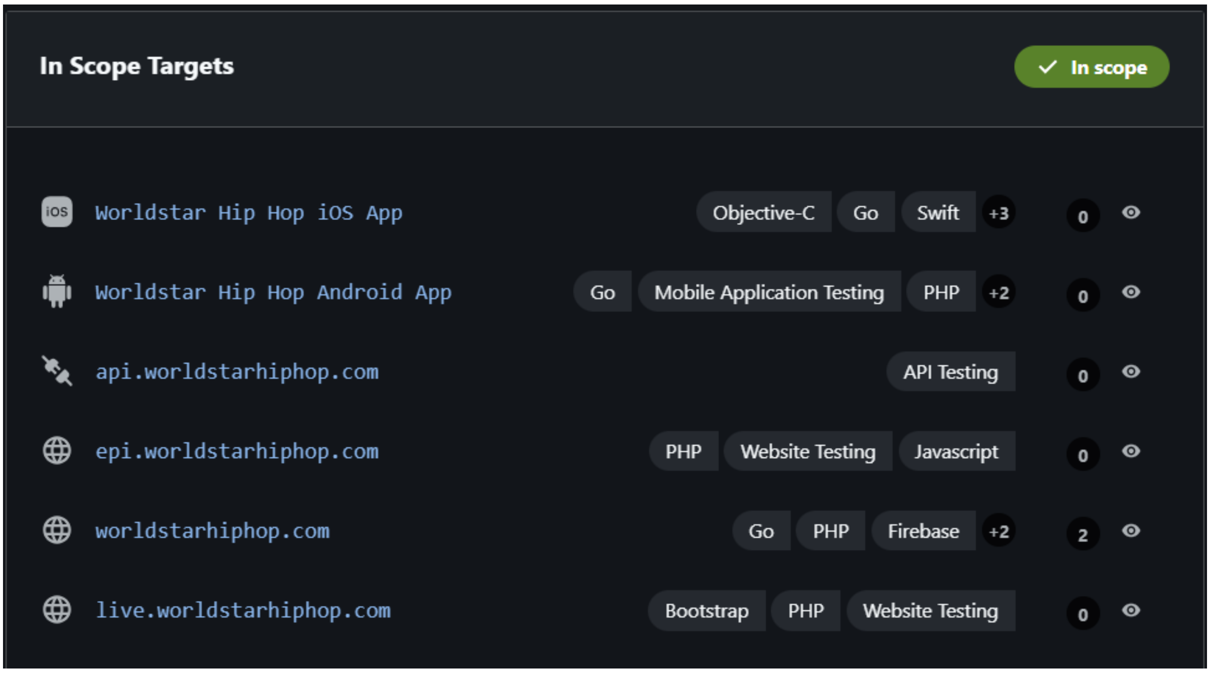
1. Domain: worldstarhiphop.com



Vulnerability Disclosure

MediaLab - WorldStar Hip Hop Vulnerability Disclosure Program

Submit your findings to the program!



In Scope Targets

✓ In scope

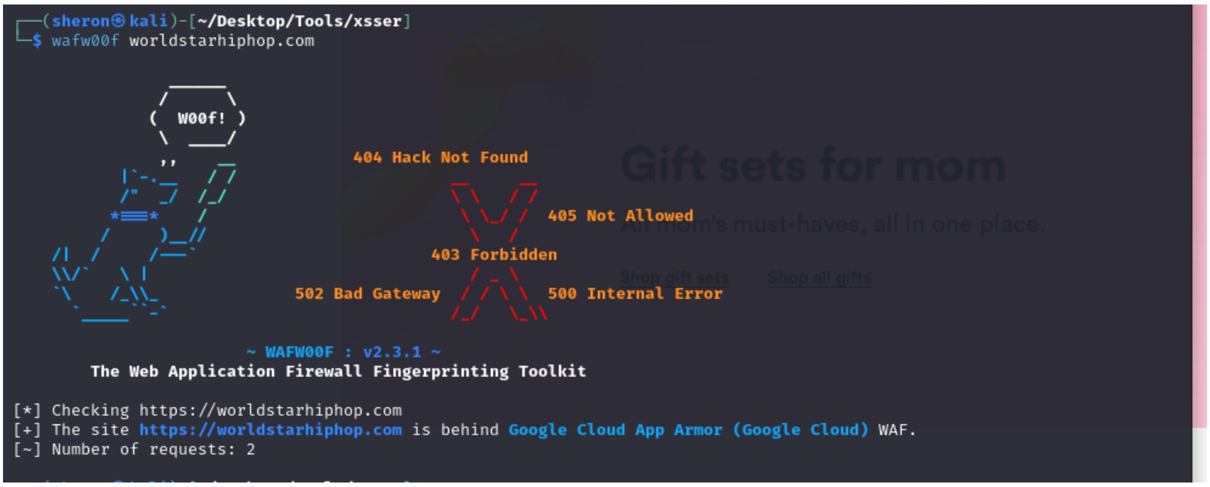
Worldstar Hip Hop iOS App	Objective-C, Go, Swift, +3	0
Worldstar Hip Hop Android App	Go, Mobile Application Testing, PHP, +2	0
api.worldstarhiphop.com	API Testing	0
epi.worldstarhiphop.com	PHP, Website Testing, Javascript	0
worldstarhiphop.com	Go, PHP, Firebase, +2	2
live.worldstarhiphop.com	Bootstrap, PHP, Website Testing	0

- Link: worldstarhiphop.com
- Type: Vulnerability Disclosure Program (VDP)
- Category: Not specified

2. Scanning

2.1. Wafw00f

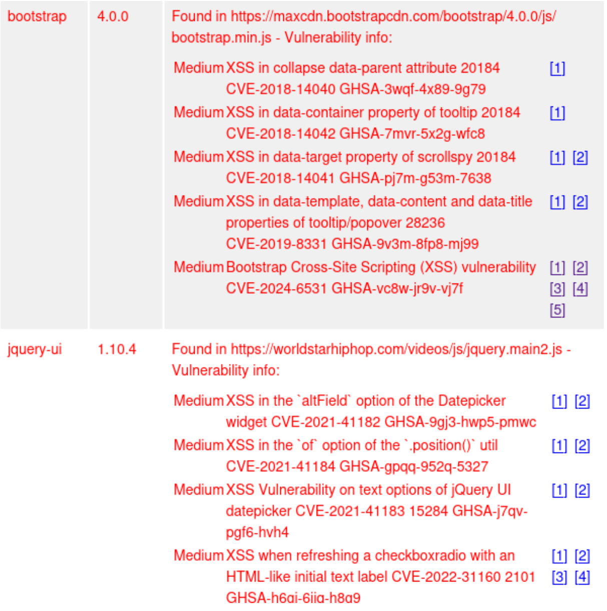
This tool is used to look for the web application firewall used by the web site. By knowing the version, the attacker can try to bypass by exploiting known vulnerabilities of that website. The scan revealed that the web application is using a web application firewall, but it is hidden.



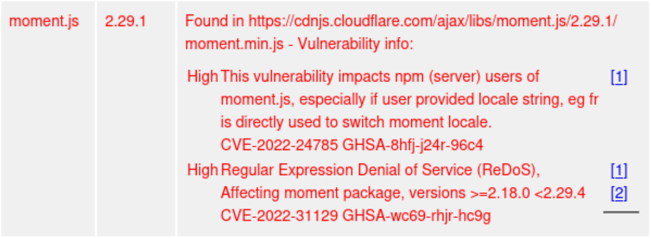
```
┌──(sheron㉿kali)-[~/Desktop/Tools/xsser]
└─$ wafw00f worldstarhiphop.com

                   ______
                  /      \
                 (  W00f! )
                  \  ____/
                  ,,    __            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://worldstarhiphop.com
[+] The site https://worldstarhiphop.com is behind Google Cloud App Armor (Google Cloud) WAF.
[~] Number of requests: 2
```

2.2. Retire.js

Retire.js is a web browser extension which helps to find vulnerable versions of frameworks used in web applications. It provides descriptions and links to details of the found vulnerability.



bootstrap	4.0.0	Found in https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js - Vulnerability info:		
		Medium	XSS in collapse data-parent attribute 20184 CVE-2018-14040 GHSA-3wqf-4x89-9g79	[1]
		Medium	XSS in data-container property of tooltip 20184 CVE-2018-14042 GHSA-7mvr-5x2g-wfc8	[1]
		Medium	XSS in data-target property of scrollspy 20184 CVE-2018-14041 GHSA-pj7m-g53m-7638	[1] [2]
		Medium	XSS in data-template, data-content and data-title properties of tooltip/popover 28236 CVE-2019-8331 GHSA-9v3m-8fp8-mj99	[1] [2]
		Medium	Bootstrap Cross-Site Scripting (XSS) vulnerability CVE-2024-6531 GHSA-vc8w-jr9v-vj7f	[1] [2] [3] [4] [5]
jquery-ui	1.10.4	Found in https://worldstarhiphop.com/videos/js/jquery.main2.js - Vulnerability info:		
		Medium	XSS in the `altField` option of the Datepicker widget CVE-2021-41182 GHSA-9gj3-hwp5-pmwc	[1] [2]
		Medium	XSS in the `of` option of the `.position()` util CVE-2021-41184 GHSA-gpqq-952q-5327	[1] [2]
		Medium	XSS Vulnerability on text options of jQuery UI datepicker CVE-2021-41183 15284 GHSA-j7qv-pgf6-hvh4	[1] [2]
		Medium	XSS when refreshing a checkboxradio with an HTML-like initial text label CVE-2022-31160 2101 GHSA-h6gi-6jiq-h8q9	[1] [2] [3] [4]



moment.js	2.29.1	Found in https://cdnjs.cloudflare.com/ajax/libs/moment.js/2.29.1/moment.min.js - Vulnerability info:		
		High	This vulnerability impacts npm (server) users of moment.js, especially if user provided locale string, eg fr is directly used to switch moment locale. CVE-2022-24785 GHSA-8hfj-j24r-96c4	[1]
		High	Regular Expression Denial of Service (ReDoS), Affecting moment package, versions >=2.18.0 <2.29.4 CVE-2022-31129 GHSA-wc69-rhjr-hc9g	[1] [2]

After inspection the following vulnerabilities are discovered. Since this is the first scan we will not go deeper to find the vulnerability. In the other scans such as rapid, we will discuss the vulnerabilities.

CVE	Affected Component	Version Used	Latest Version	Details
CVE-2018-14040	bootstrap	4.0.0	5.3.0	Medium XSS in collapse data-parent attribute
CVE-2018-14042	bootstrap	4.0.0	5.3.0	Medium XSS in data-container property of tooltip
CVE-2018-14041	bootstrap	4.0.0	5.3.0	Medium XSS in data-target property of scrollspy
CVE-2019-8331	bootstrap	4.0.0	5.3.0	Medium XSS in data-template, data-content, and data-title properties
CVE-2022-6531	bootstrap	4.0.0	5.3.0	Medium Bootstrap Cross-Site Scripting (XSS) vulnerability
CVE-2021-41182	jquery-ui	1.10.4	no longer maintained	Medium XSS in the 'altField' option of the Datepicker widget
CVE-2021-41184	jquery-ui	1.10.4	no longer maintained	Medium XSS in the 'of' option of the 'position' utility
CVE-2021-41183	jquery-ui	1.10.4	no longer maintained	Medium XSS vulnerability in text options of jQuery UI Datepicker
CVE-2022-31160	jquery-ui	1.10.4	no longer maintained	Medium XSS when refreshing a checkboxradio with an HTML-like initial label
CVE-2022-24785	moment.js	2.29.1	2.29.4	High impact vulnerability affecting npm (server) users of moment.js
CVE-2022-31129	moment.js	2.29.1	2.29.4	high impact vulnerability affecting npm (server) users of moment.js

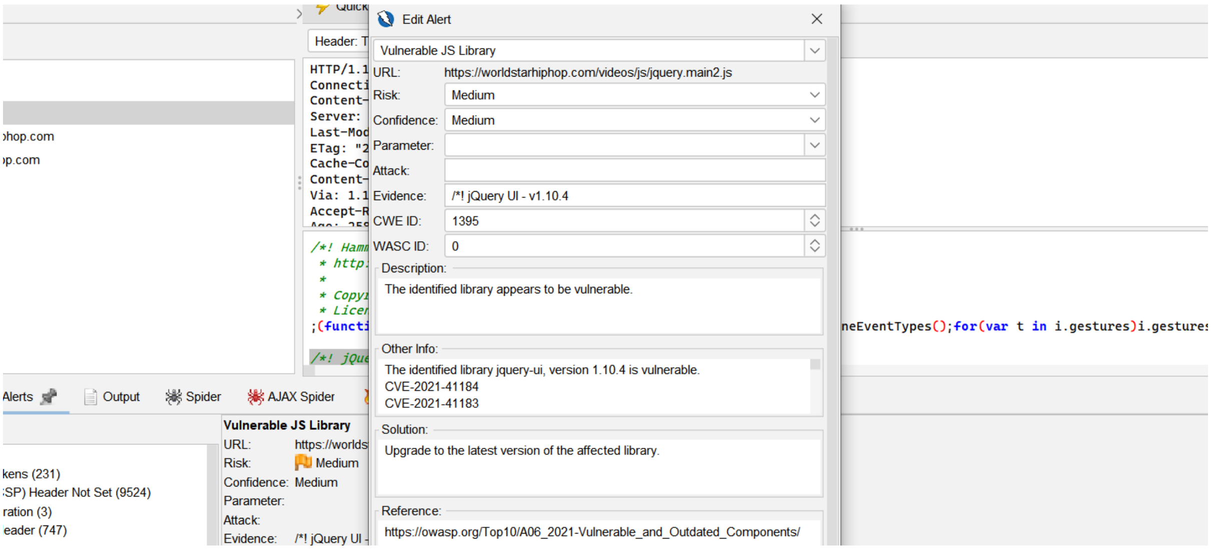
It seems like most of the vulnerabilities are from the boostrap, jquery and moment.js. And most of the vulnerabilities are with regarding to XSS attacks.

2.3. OWSAP ZAP

Zap is free and open source DAST tool (Dynamic Application Testing Tool) which is used to identify vulnerabilities in web applications. After conducting the scan on this domain following vulnerabilities were discovered.

Two vulnerabilities were discovered in the jQuery library. Both of the vulnerabilities are caused by outdated components and two of them are related to cross site scripting. To read more about the vulnerability click the below links.

- CVE-2021-41184 - When accepting the value of*Text options of the Datepicker widget from untrusted sources it may lead to execution of untrusted scripts, causing XSS.
- CVE-2021-41183 – Similar to the above.



Edit Alert

Vulnerable JS Library

URL: https://worldstarhiphop.com/videos/js/jquery.main2.js

Risk: Medium

Confidence: Medium

Parameter:

Attack:

Evidence: /*! jQuery UI - v1.10.4

CWE ID: 1395

WASC ID: 0

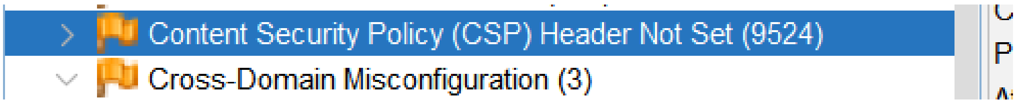
Description:
The identified library appears to be vulnerable.

Other Info:
The identified library jquery-ui, version 1.10.4 is vulnerable.
CVE-2021-41184
CVE-2021-41183

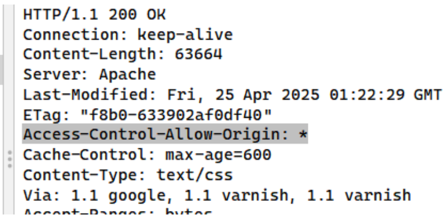
Solution:
Upgrade to the latest version of the affected library.

Reference:
https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Also this domain lacks various security headers leading to vulnerabilities and misconfigurations. Vulnerabilities such as XSS attacks and other mis configs regarding cross domain resource sharing (CORS) on the web server.



Content Security Policy (CSP) Header Not Set (9524)
Cross-Domain Misconfiguration (3)

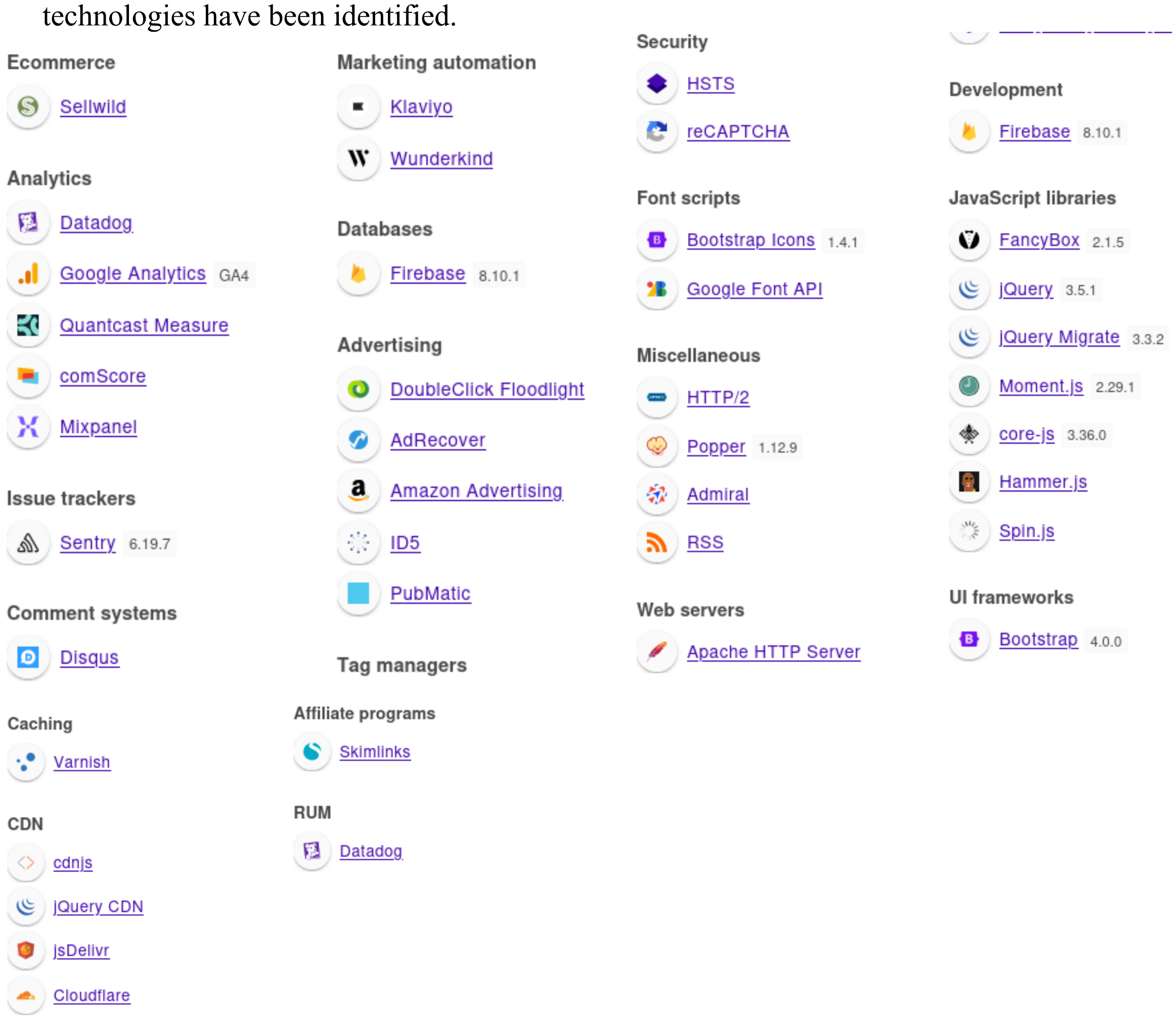


```
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 63664
Server: Apache
Last-Modified: Fri, 25 Apr 2025 01:22:29 GMT
ETag: "f8b0-633902af0df40"
Access-Control-Allow-Origin: *
Cache-Control: max-age=600
Content-Type: text/css
Via: 1.1 google, 1.1 varnish, 1.1 varnish
Accept-Ranges: bytes
```

Mitigation of such errors can be easily done by re configuring the web server and by including the correct security policies to the website.

2.4. Wappalyzer

This is a browser extension which can be added to your browser. It can identify what technologies have been used to build a web site. After letting it scan, The following technologies have been identified.



Ecommerce

Sellwild

Analytics

Datadog

Google Analytics GA4

Quantcast Measure

comScore

Mixpanel

Issue trackers

Sentry 6.19.7

Comment systems

Disqus

Caching

Varnish

CDN

cdnjs

jQuery CDN

jsDelivr

Cloudflare

Marketing automation

Klaviyo

Wunderkind

Databases

Firebase 8.10.1

Advertising

DoubleClick Floodlight

AdRecover

Amazon Advertising

ID5

PubMatic

Tag managers

Affiliate programs

Skimlinks

RUM

Datadog

Security

HSTS

reCAPTCHA

Font scripts

Bootstrap Icons 1.4.1

Google Font API

Miscellaneous

HTTP/2

Popper 1.12.9

Admiral

RSS

Web servers

Apache HTTP Server

Development

Firebase 8.10.1

JavaScript libraries

FancyBox 2.1.5

jQuery 3.5.1

jQuery Migrate 3.3.2

Moment.js 2.29.1

core-js 3.36.0

Hammer.js

Spin.js

UI frameworks

Bootstrap 4.0.0

CVE ID	Technology Used	Version Used	Description of the Vulnerability
CVE-2020-11022	jQuery	3.5.1	Prototype pollution vulnerability allowing attackers to manipulate object properties.
CVE-2020-11023	jQuery	3.5.1	Cross-site scripting (XSS) vulnerability enabling injection of malicious scripts.
CVE-2021-23458	core-js	3.36.0	Prototype pollution vulnerability impacting JavaScript libraries.

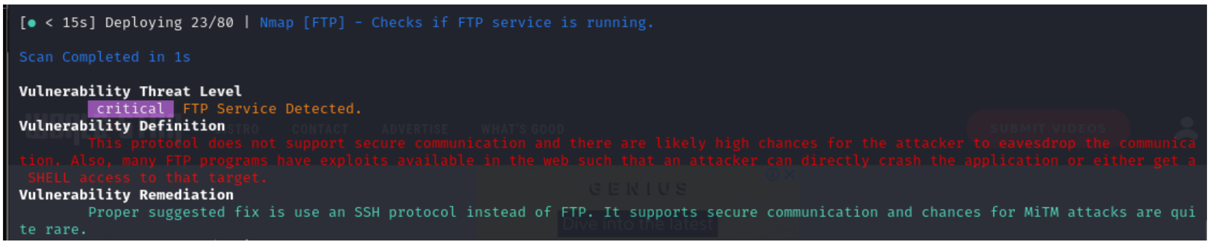
CVE-2021-44228	Apache Log4j	Not specified	Remote code execution vulnerability due to improper input validation.
CVE-2021-45046	Apache Log4j	Not specified	Denial of service vulnerability caused by uncontrolled resource consumption.

In the above table are some of the vulnerabilities that were found in the insecure or old versions of the platform. Vulnerabilities such as XSS, prototype pollution, RCE and DOS attacks can be seen in the table. We will confirm the availability of the by using other tools to look for vulnerabilities.

2.5. Rapid Scan

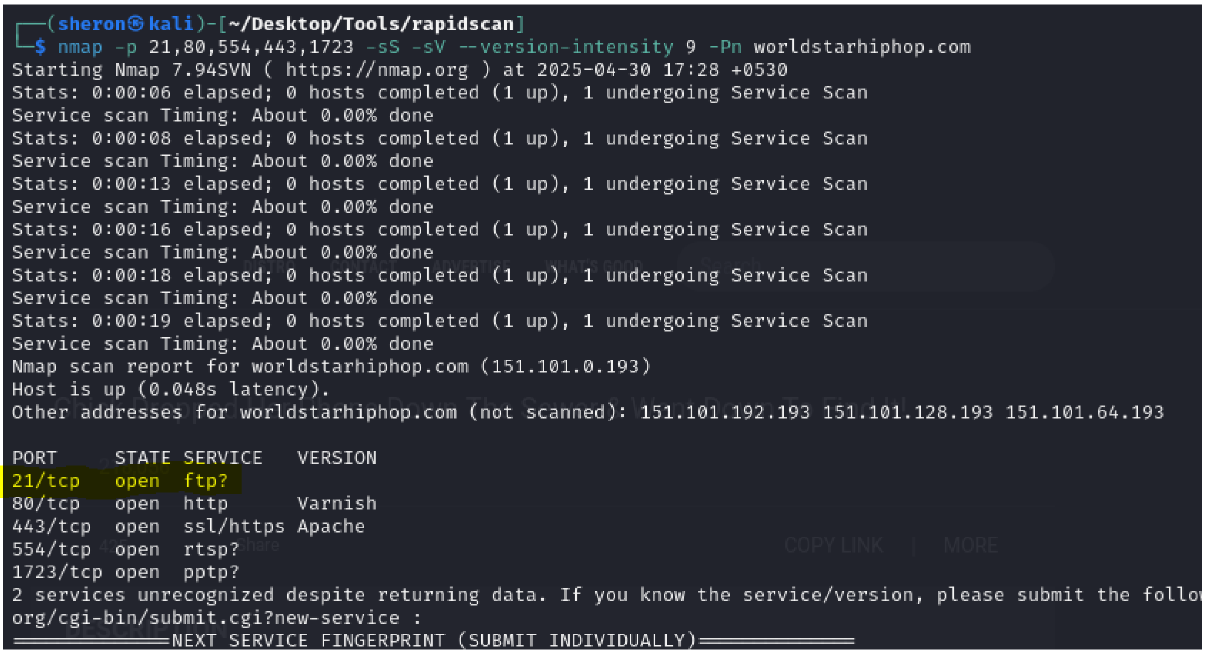
Rapid scan must have powerful tool that allows the tester to look for vulnerabilities using a combination of 82 different scans by using a multitude of tools. After the rapid scan the following errors were found.

First vulnerability – This is a vulnerability caused by port 21 which is typically used to do FTP communication. FTP is vulnerable in nature it could we vulnerable to man in the middle attacks mainly. The below is the screen snap of rapid scanner detecting the vulnerability.



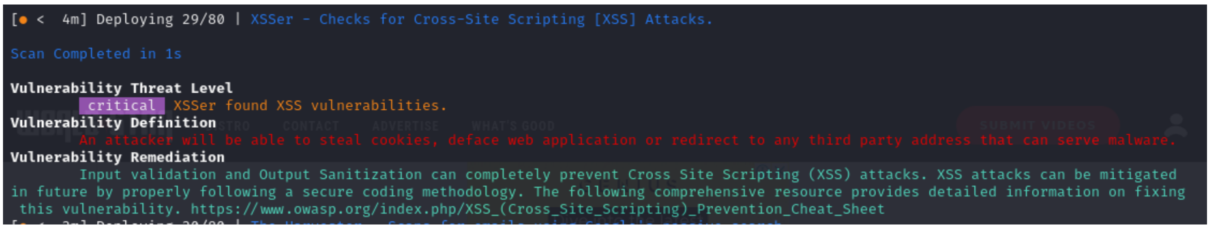
```
[● < 15s] Deploying 23/80 | Nmap [FTP] - Checks if FTP service is running.

Scan Completed in 1s

Vulnerability Threat Level
        critical  FTP Service Detected.
Vulnerability Definition
        This protocol does not support secure communication and there are likely high chances for the attacker to eavesdrop the communica
tion. Also, many FTP programs have exploits available in the web such that an attacker can directly crash the application or either get a
 SHELL access to that target.
Vulnerability Remediation
        Proper suggested fix is use an SSH protocol instead of FTP. It supports secure communication and chances for MiTM attacks are qui
te rare.
```

Let’s confirm to see if the FTP is open by conducting a stealth **nmap scan**. The port 21 is open which is running the FTP service.

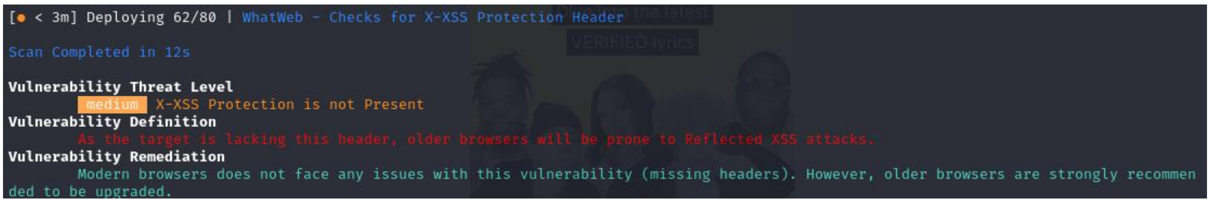


```
┌──(sheron㉿kali)-[~/Desktop/Tools/rapidscan]
└─$ nmap -p 21,80,554,443,1723 -sS -sV --version-intensity 9 -Pn worldstarhiphop.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-30 17:28 +0530
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for worldstarhiphop.com (151.101.0.193)
Host is up (0.048s latency).
Other addresses for worldstarhiphop.com (not scanned): 151.101.192.193 151.101.128.193 151.101.64.193

PORT     STATE SERVICE   VERSION
21/tcp   open  ftp?
80/tcp   open  http      Varnish
443/tcp  open  ssl/https Apache
554/tcp  open  rtsp?
1723/tcp open  pptp?
2 services unrecognized despite returning data. If you know the service/version, please submit the follow
org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
```

Second Vulnerability: The next vulnerability is regarding cross site scripting (XSS). This vulnerability was confirmed earlier as well form Wappalyzer, retire.js and also by zap. Factors such as missing headers, usage of outdated components and misconfigurations has led to this vulnerability. Below are snaps of the tool detecting that XSS attacks are possible by XXSer and WhatWeb detecting a missing header to prevent XSS from happening.

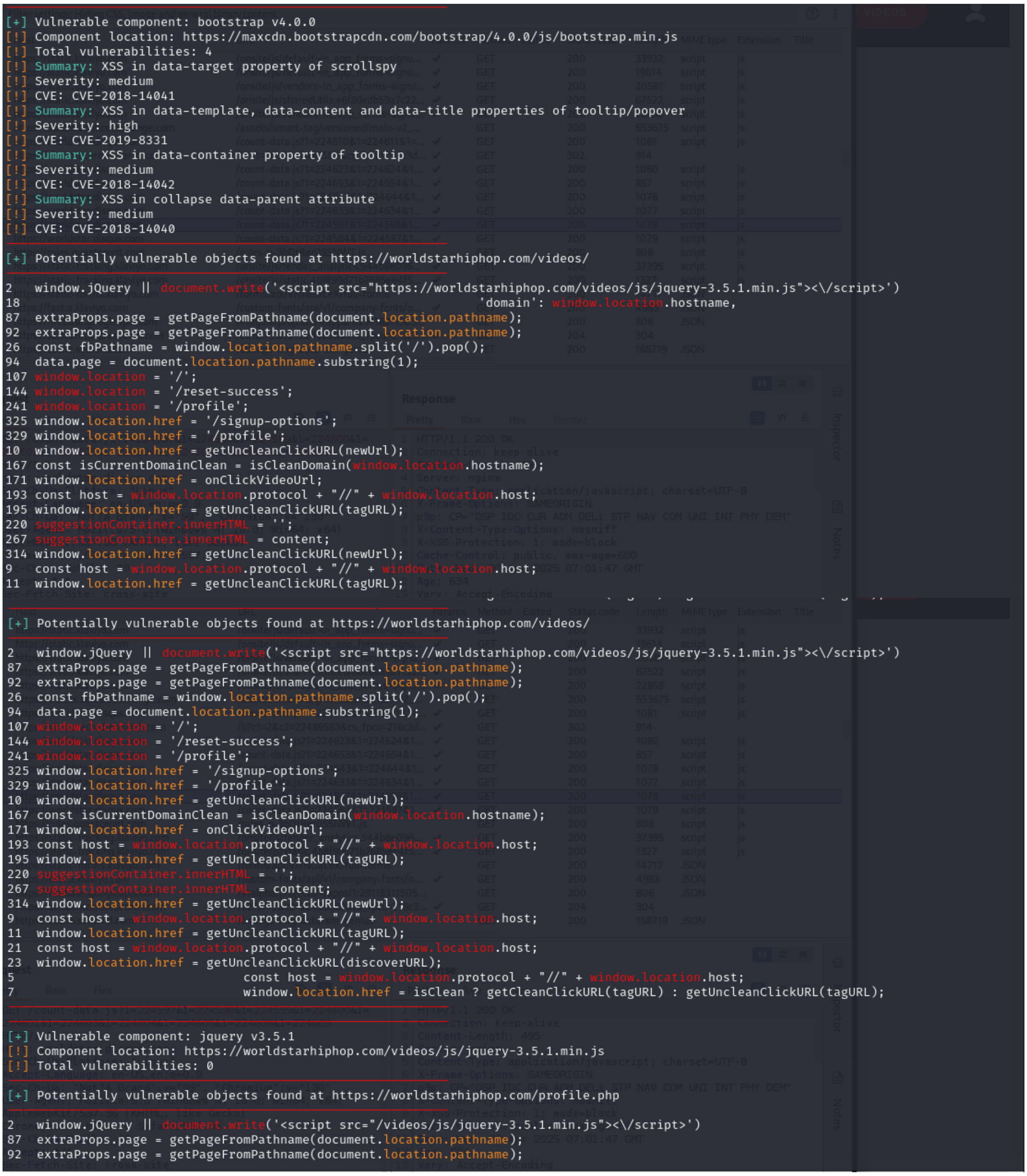


```
[● <  4m] Deploying 29/80 | XSSer - Checks for Cross-Site Scripting [XSS] Attacks.

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 can be mitigated
in future by properly following a secure coding methodology. The following comprehensive resource provides detailed information on fixing
 this vulnerability. https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
```



```
[● < 3m] Deploying 62/80 | WhatWeb - Checks for X-XSS Protection Header

Scan Completed in 12s

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 strongly recommen
ded to be upgraded.
```

The following is a **XSStrike** tool testing for XSS using a payload to check for vulnerabilities using the parameter search=test.



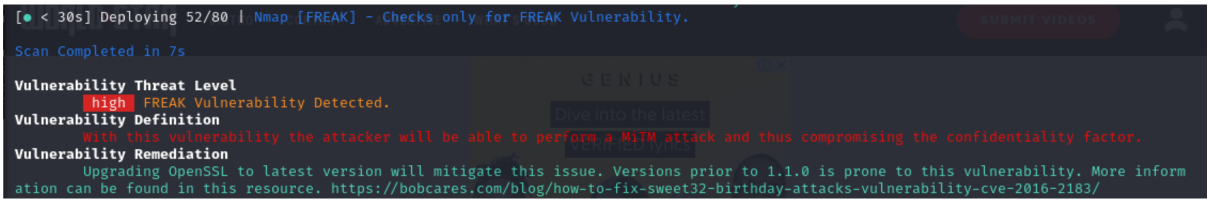
```
[+] Vulnerable component: bootstrap v4.0.0
[!] Component location: https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js
[!] Total vulnerabilities: 4
[!] Summary: XSS in data-target property of scrollspy
[!] Severity: medium
[!] CVE: CVE-2018-14041
[!] Summary: XSS in data-template, data-content and data-title properties of tooltip/popover
[!] Severity: high
[!] CVE: CVE-2019-8331
[!] Summary: XSS in data-container property of tooltip
[!] Severity: medium
[!] CVE: CVE-2018-14042
[!] Summary: XSS in collapse data-parent attribute
[!] Severity: medium
[!] CVE: CVE-2018-14040

[+] Potentially vulnerable objects found at https://worldstarhiphop.com/videos/

2   window.jQuery || document.write('<script src="https://worldstarhiphop.com/videos/js/jquery-3.5.1.min.js"><\/script>')
18                                                          'domain': window.location.hostname,
87  extraProps.page = getPageFromPathname(document.location.pathname);
92  extraProps.page = getPageFromPathname(document.location.pathname);
26  const fbPathname = window.location.pathname.split('/').pop();
94  data.page = document.location.pathname.substring(1);
107 window.location = '/';
144 window.location = '/reset-success';
241 window.location = '/profile';
325 window.location.href = '/signup-options';
329 window.location.href = '/profile';
10  window.location.href = getUncleanClickURL(newUrl);
167 const isCurrentDomainClean = isCleanDomain(window.location.hostname);
171 window.location.href = onClickVideoUrl;
193 const host = window.location.protocol + "//" + window.location.host;
195 window.location.href = getUncleanClickURL(tagURL);
220 suggestionContainer.innerHTML = '';
267 suggestionContainer.innerHTML = content;
314 window.location.href = getUncleanClickURL(newUrl);
9   const host = window.location.protocol + "//" + window.location.host;
11  window.location.href = getUncleanClickURL(tagURL);

[+] Potentially vulnerable objects found at https://worldstarhiphop.com/videos/

2   window.jQuery || document.write('<script src="https://worldstarhiphop.com/videos/js/jquery-3.5.1.min.js"><\/script>')
87  extraProps.page = getPageFromPathname(document.location.pathname);
92  extraProps.page = getPageFromPathname(document.location.pathname);
26  const fbPathname = window.location.pathname.split('/').pop();
94  data.page = document.location.pathname.substring(1);
107 window.location = '/';
144 window.location = '/reset-success';
241 window.location = '/profile';
325 window.location.href = '/signup-options';
329 window.location.href = '/profile';
10  window.location.href = getUncleanClickURL(newUrl);
167 const isCurrentDomainClean = isCleanDomain(window.location.hostname);
171 window.location.href = onClickVideoUrl;
193 const host = window.location.protocol + "//" + window.location.host;
195 window.location.href = getUncleanClickURL(tagURL);
220 suggestionContainer.innerHTML = '';
267 suggestionContainer.innerHTML = content;
314 window.location.href = getUncleanClickURL(newUrl);
9   const host = window.location.protocol + "//" + window.location.host;
11  window.location.href = getUncleanClickURL(tagURL);
21  const host = window.location.protocol + "//" + window.location.host;
23  window.location.href = getUncleanClickURL(discoverURL);
5                                 const host = window.location.protocol + "//" + window.location.host;
7                                 window.location.href = isClean ? getCleanClickURL(tagURL) : getUncleanClickURL(tagURL);

[+] Vulnerable component: jquery v3.5.1
[!] Component location: https://worldstarhiphop.com/videos/js/jquery-3.5.1.min.js
[!] Total vulnerabilities: 0

[+] Potentially vulnerable objects found at https://worldstarhiphop.com/profile.php

2   window.jQuery || document.write('<script src="/videos/js/jquery-3.5.1.min.js"><\/script>')
87  extraProps.page = getPageFromPathname(document.location.pathname);
92  extraProps.page = getPageFromPathname(document.location.pathname);
```

The above snap shots revealed the vulnerable components. This confirms the results of the previous scans. **XSStrike** found the following **vulnerable components,**

- Boostrap
  - CVE-2018-14041 (XSS in data-target property of scrollspy)
  - CVE-2019-8331 (XSS in data-template, data-content and data-title properties of tooltip/popover)

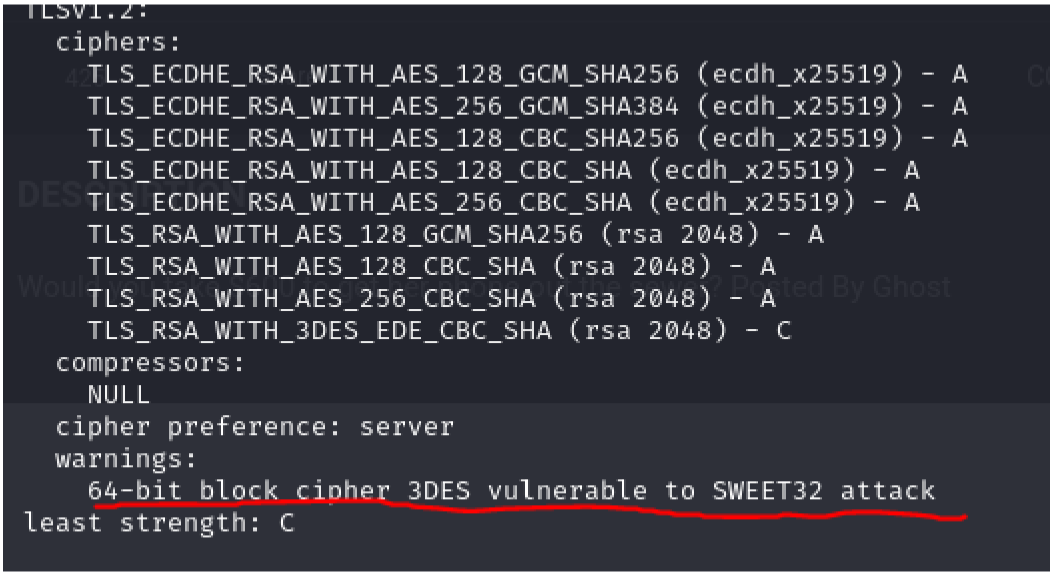
  - CVE-2018-14042 (XSS in data-container property of tooltip)
  - CVE-2018-14040 (XSS in collapse data-parent attribute)
- JQuery – CVEs were not given but the vulnerable code segement is given

Third Vulnerability – This is high severity vulnerability caused by improper handling of SSL/TSL encryption in servers. This allows attacker to force a downgrade of cryptographic protocols. Potentially enabling Man in the Middle attacks (MITM)



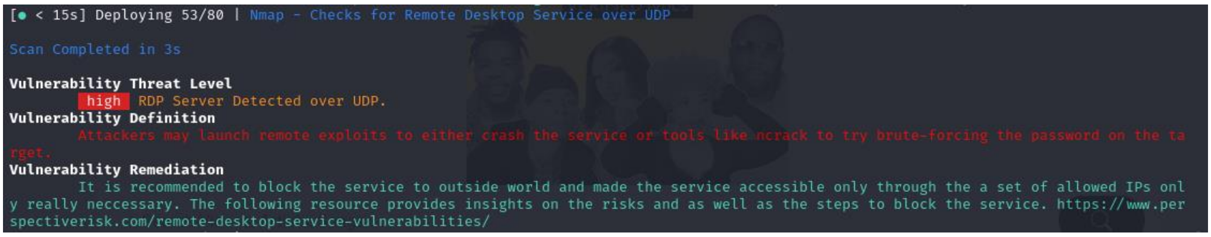
```
[● < 30s] Deploying 52/80 | Nmap [FREAK] - Checks only for FREAK Vulnerability.

Scan Completed in 7s

Vulnerability Threat Level
        high  FREAK Vulnerability Detected.
Vulnerability Definition
        With this vulnerability the attacker will be able to perform a MiTM attack and thus compromising the confidentiality factor.
Vulnerability Remediation
        Upgrading OpenSSL to latest version will mitigate this issue. Versions prior to 1.1.0 is prone to this vulnerability. More inform
ation can be found in this resource. https://bobcares.com/blog/how-to-fix-sweet32-birthday-attacks-vulnerability-cve-2016-2183/
```

This can also be verified by an nmap scan with ssl-enum-scripts. It revealed that 3DES is vulnerable to SWEET32 attack

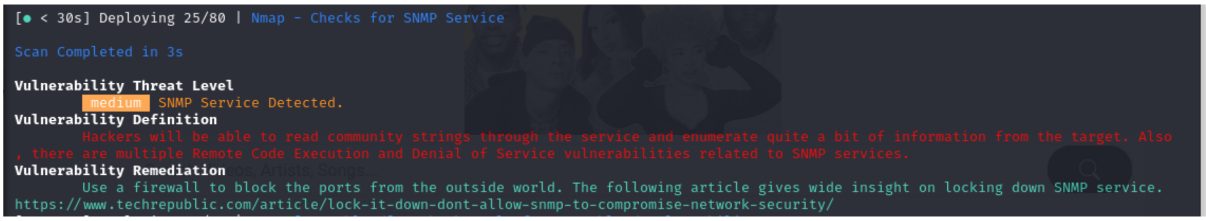


```
TLSv1.2:
  ciphers:
    TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
    TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
    TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
    TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
    TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
  compressors:
    NULL
  cipher preference: server
  warnings:
    64-bit block cipher 3DES vulnerable to SWEET32 attack
least strength: C
```

Forth vulnerability – When RDP servers are over UDP, attackers might be able to launch remote exploits to brute force passwords using tools like ncrack or to crash the service.



```
[● < 15s] Deploying 53/80 | 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 password on the ta
rget.
Vulnerability Remediation
        It is recommended to block the service to outside world and made the service accessible only through the a set of allowed IPs onl
y really neccessary. The following resource provides insights on the risks and as well as the steps to block the service. https://www.per
spectiverisk.com/remote-desktop-service-vulnerabilities/
```



```
[● < 30s] Deploying 25/80 | Nmap - Checks for SNMP Service

Scan Completed in 3s

Vulnerability Threat Level
        medium  SNMP Service Detected.
Vulnerability Definition
        Hackers will be able to read community strings through the service and enumerate quite a bit of information from the target. Also
, there are multiple Remote Code Execution and Denial of Service vulnerabilities related to SNMP services.
Vulnerability Remediation
        Use a firewall to block the ports from the outside world. The following article gives wide insight on locking down SNMP service.
https://www.techrepublic.com/article/lock-it-down-dont-allow-snmp-to-compromise-network-security/
```

3. Affected Components

The following table the collection of vulnerable components found in the web application. The table will have the name of the component, CVE, version, details and details regarding the impact

Component	Type	Vulnerability	CVE Code	Severity	Impact
Bootstrap 4.0.0	JavaScript Library	Multiple XSS vulnerabilities	CVE-2018-14040, CVE-2018-14041, CVE-2018-14042, CVE-2019-8331, CVE-2022-6531	Medium	Allows attackers to execute malicious scripts, potentially leading to data theft or UI manipulation
jQuery UI 1.10.4	JavaScript Library	Multiple XSS vulnerabilities in Datepicker & position utility	CVE-2021-41182, CVE-2021-41183, CVE-2021-41184, CVE-2022-31160	Medium	Allows execution of unauthorized scripts via manipulated UI components
Moment.js 2.29.1	JavaScript Library	Prototype Pollution	CVE-2022-24785, CVE-2022-31129	High	Can allow modification of global JavaScript objects, leading to security bypass risks
Apache Log4j	Logging Framework	Remote Code Execution (RCE) & Denial of Service (DoS)	CVE-2021-44228, CVE-2021-45046	Critical	Allows an attacker to execute arbitrary code remotely or disrupt service
jQuery 3.5.1	JavaScript Library	Prototype Pollution & XSS	CVE-2020-11022, CVE-2020-11023	Medium to High	Can lead to manipulated object properties or unauthorized script execution
FTP Service (Port 21)	Network Service	Unencrypted data transfer	-	High	Can expose credentials and sensitive data to interception
SSL/TLS Encryption	Security Protocol	Downgrade attack due to misconfiguration	-	Critical	Enables Man-in-the-Middle (MITM) attacks and weak cryptographic implementations

RDP over UDP (Port 3389)	Remote Access Protocol	Brute-force attack risk	-	High	Exposes the system to unauthorized remote access and password-cracking attempts
Missing Security Headers	Configuration Issue	Lack of protection against XSS & CORS misconfigurations	-	High	Increases exposure to injection and unauthorized data access risks

4. Vulnerabilities

4.1. FTP service detected

FTP server can lead many security breaches as it transfers data without encryption. It also transmits username and passwords in plain text. Also FTP by default allows anonumous login. Further testing is needed to determine weather this web application allows anonymous login. Also, FTP is weak against brute force attacks. Since it doesn't use any encryption no integrity nor confidentiality

4.2. XSS

This vulnerability is a result of many reasons such as misconfigured headers, omitted headers, usage of vulnerable versions of libraries. Cross site scripting vulnerabilities allow users to run malicious scripts in the web page and allow it to steal sensitive data, perform malicious actions such as CSRF, deliver phishing attacks, spread malware and keylogging.

4.3. SSL/TSL encryption handling

Due to a misconfiguration of the OpenSSL it is possible to downgrade the encryption method used and then perform the attack. This could lead to data theft, enable easy brute force. Unauthorized login and man in the middle attacks.

4.4. RDP over UDP

The threat agent can launch remote exploits to either crash the service or use tools like ncrack to brute force passwords. Which means,

- The system will be a target since RDP is exposed over UDP in port 3389
- Tools such as Ncrack can login to RDP service using brute-force

- RDP vulnerabilities such as DOS attacks can be attempted
- Will hard to monitor attacks

5. Mitigation

5.1. FTP service – mitigation

This can be mitigated by mainly by shifting to a more secure protocol such as ssh. And also fire walls can be used to detect and block unusual behaviour. And if the file transfer protocol is not being used better to completely shut down the port

5.2. XSS – mitigation

This vulnerability can be easily prevented. First update the current security headers. And if there are any missing headers, add them. Next remove all the old vulnerable versions of the libraries used and start using new versions.

5.3. SSL/TSL encryption -mitigation

Upgrading the OpenSSL to a version which is not vulnerable can fix the issue. In newer versions, it is not possible to downgrade the encryption methods hence fixing them.

5.4. RDP over UDP – mitigation

To eliminate the vulnerability, you can simply,

- Block RDP and UDP access form the public networks
- Allow use of RDP only through trusted networks. (or VPNs)
- Use proxy and firewalls to block any unusual activities and restrict access
- If RDP is not in use, disable the service entirely

6. Conclusion

We can see that this web application has some missing security features that might allow attackers to exploit the vulnerabilities found. Some of the vulnerabilities found needs extra testing such as the FTP server and RDP in UDP. But other than that, the vulnerabilities in the outdated technologies are proved. Due to this, it is recommended to fix all the issues mentioned above in the mitigation section to safeguard the web application.