1. Objectives

The objective of this executive summary is to test and detect vulnerabilities identified in the initial design document on an e-commerce website called "https://loadedwithstuff.co.uk/". The tools selected, results as well as recommendations on how to improve the website's security will be discussed. The summary will outline current security standards governed by the following regulations:

- UK GDPR (General Data Protection Regulation of the European Union)
- DPA 2018 (Data Protection Act of 2018)
- PCI DSS (Payment Card Industry Data Security Standard)
- ICO (Information Commissioners Office)

as well as provide recommendations to ensure ongoing compliance.

2. Methodology

Various vulnerability detection and scanning tools exist in the market today. Selecting the correct platform remains key when detecting and scanning for vulnerabilities, specifically on web servers since they are accessible from the internet and remain exposed.

Kali Linux is a superior open-source Linux distribution that is designed to perform penetration testing, computer forensics and reverse engineering amongst other security related tasks (OffSec Services Limited, 2022). Kali Linux contains built-in penetration testing tools and was selected as the platform of choice in order to achieve the objectives stated above. Figure 1 below represents an overview of the tools selected to perform various scanning activities using Kali Linux:

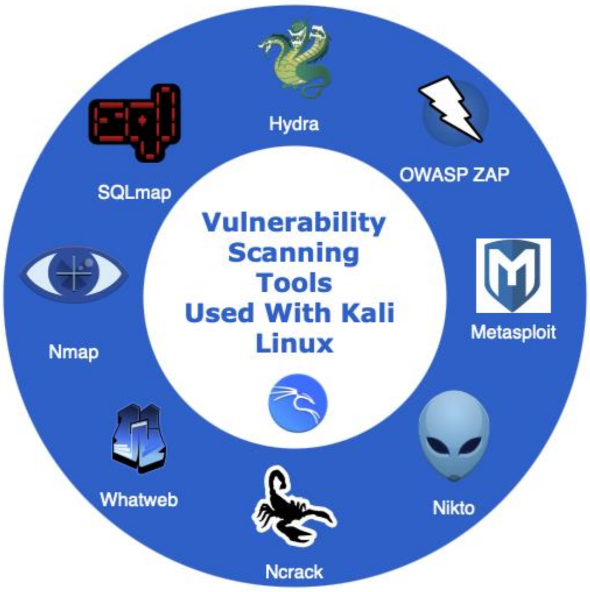


Figure 1: Scanning Tools used with Kali Linux

By utilizing the tools mentioned above, a methodology based on the security threat analysis model STRIDE and the risk management method ISSRM (Information System Security Risk Management) was followed. Using the STRIDE model, six categories of security risks were determined, which can be used to identify possible threats (Shostack, 2009). A listing of the STRIDE threats is shown in Table 1 below.

Table 1: STRIDE model

Threat	**Desired property**
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-reputability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

The ISSRM can be used to raise security requirements for protecting the system based on the threats analysed by STRIDE and to develop countermeasures based on risk and resource management in the e-commerce industry (Abbass et al., 2016). Figure 2 shows the ISSRM domain model.

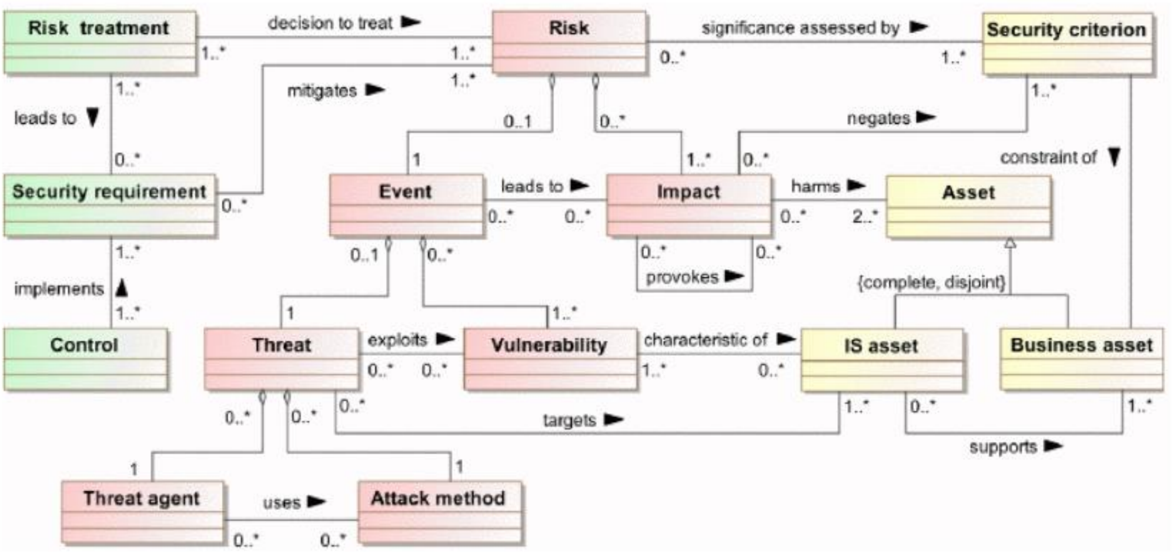
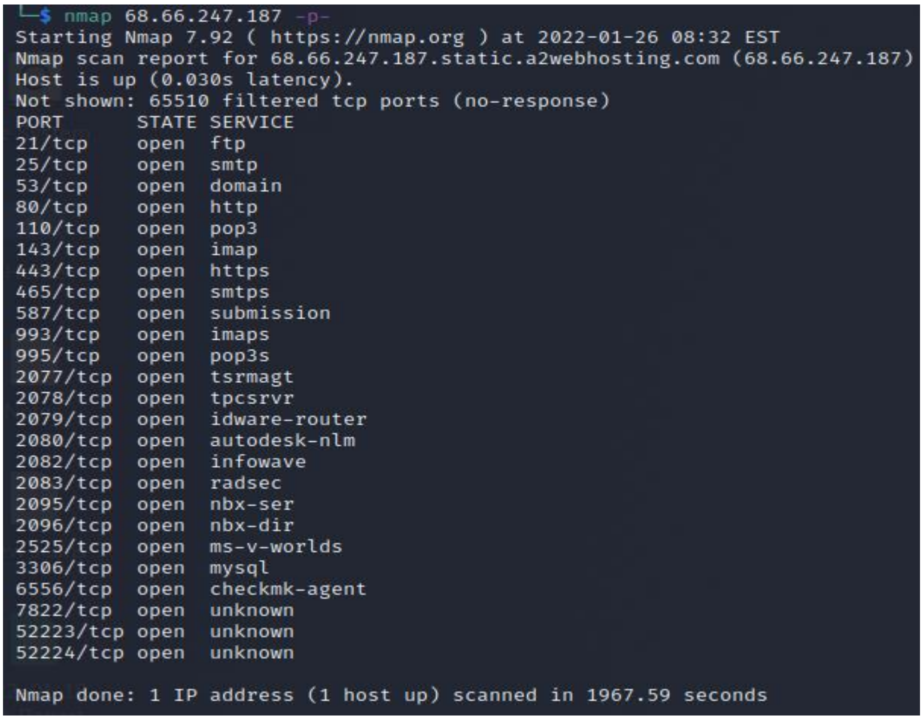


Figure 2: ISSRM Domain Model (Mayer et al., 2008)

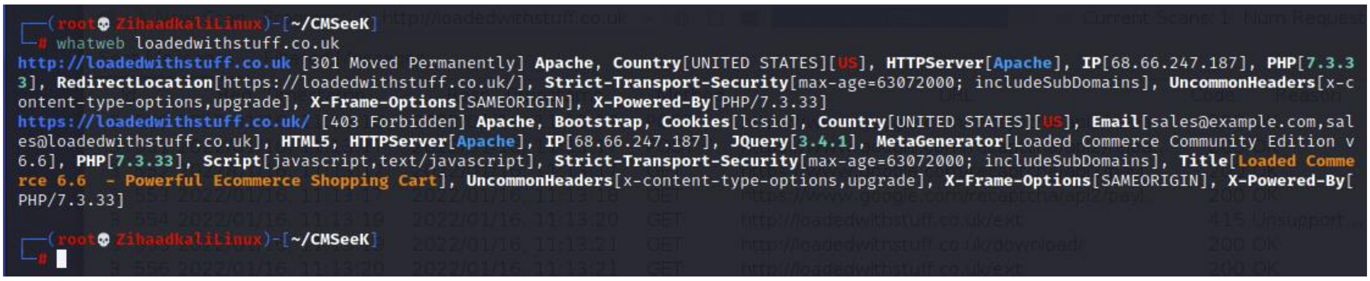
To carry out a risk assessment of the e-commerce website, the website structure needs to be examined. This included information gathering such as open ports, state and services, OS detection and possible applications installed on the server hosting the website (Shah et al., 2019). *Nmap* was used to achieve this information as seen in Figure 3 below. Further detailed scans are listed in Appendix A.



```
└─$ nmap 68.66.247.187 -p-
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-26 08:32 EST
Nmap scan report for 68.66.247.187.static.a2webhosting.com (68.66.247.187)
Host is up (0.030s latency).
Not shown: 65510 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
2077/tcp  open  tsrmagt
2078/tcp  open  tpcsrvr
2079/tcp  open  idware-router
2080/tcp  open  autodesk-nlm
2082/tcp  open  infowave
2083/tcp  open  radsec
2095/tcp  open  nbx-ser
2096/tcp  open  nbx-dir
2525/tcp  open  ms-v-worlds
3306/tcp  open  mysql
6556/tcp  open  checkmk-agent
7822/tcp  open  unknown
52223/tcp open  unknown
52224/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1967.59 seconds
```

Figure 3: Nmap port scan

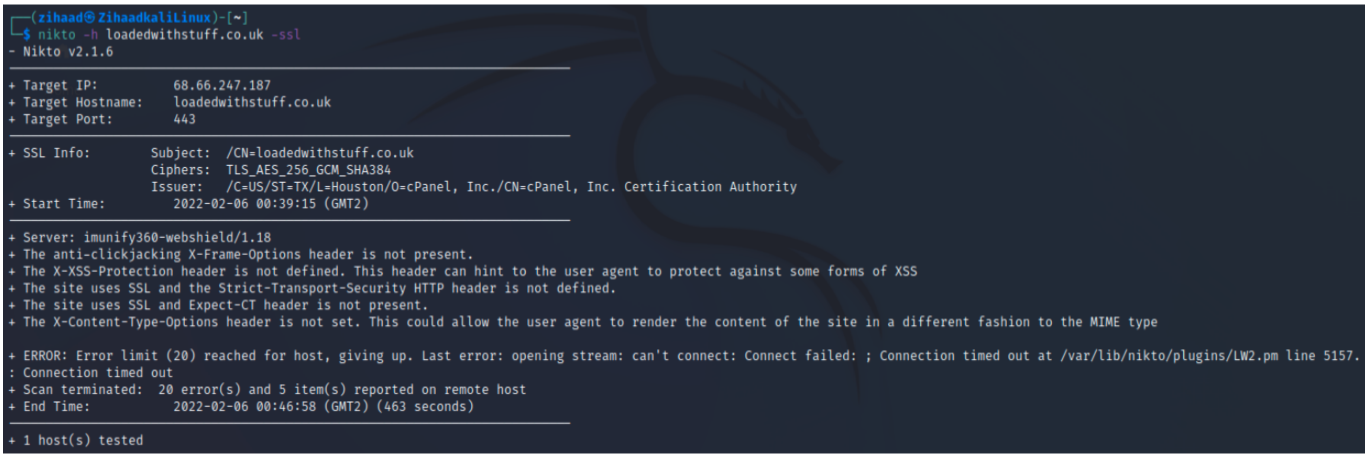
In addition, *Metasploit port scanner* was used to validate the above results obtained from *Nmap* listed in Appendix A. Furthermore *Whatweb* revealed an Apache webserver as well as a Content Management System (CMS) installed i.e. Loaded Commerce v6.6 developed by Softaculous (Softaculous, 2022) as indicated in Figure 4 below.



```
┌──(root💀 ZihaadkaliLinux)-[~/CMSeeK]
└─# whatweb loadedwithstuff.co.uk
http://loadedwithstuff.co.uk [301 Moved Permanently] Apache, Country[UNITED STATES][US], HTTPServer[Apache], IP[68.66.247.187], PHP[7.3.3
3], RedirectLocation[https://loadedwithstuff.co.uk/], Strict-Transport-Security[max-age=63072000; includeSubDomains], UncommonHeaders[x-c
ontent-type-options,upgrade], X-Frame-Options[SAMEORIGIN], X-Powered-By[PHP/7.3.33]
https://loadedwithstuff.co.uk/ [403 Forbidden] Apache, Bootstrap, Cookies[lcsid], Country[UNITED STATES][US], Email[sales@example.com,sal
es@loadedwithstuff.co.uk], HTML5, HTTPServer[Apache], IP[68.66.247.187], JQuery[3.4.1], MetaGenerator[Loaded Commerce Community Edition v
6.6], PHP[7.3.33], Script[javascript,text/javascript], Strict-Transport-Security[max-age=63072000; includeSubDomains], Title[Loaded Comme
rce 6.6  - Powerful Ecommerce Shopping Cart], UncommonHeaders[x-content-type-options,upgrade], X-Frame-Options[SAMEORIGIN], X-Powered-By[
PHP/7.3.33]

┌──(root💀 ZihaadkaliLinux)-[~/CMSeeK]
└─#
```

Figure 4: Whatweb scan

Nikto was then utilized to scan for web server vulnerabilities as indicated in Figure 5 below. Detected vulnerabilities are presented in section 4.



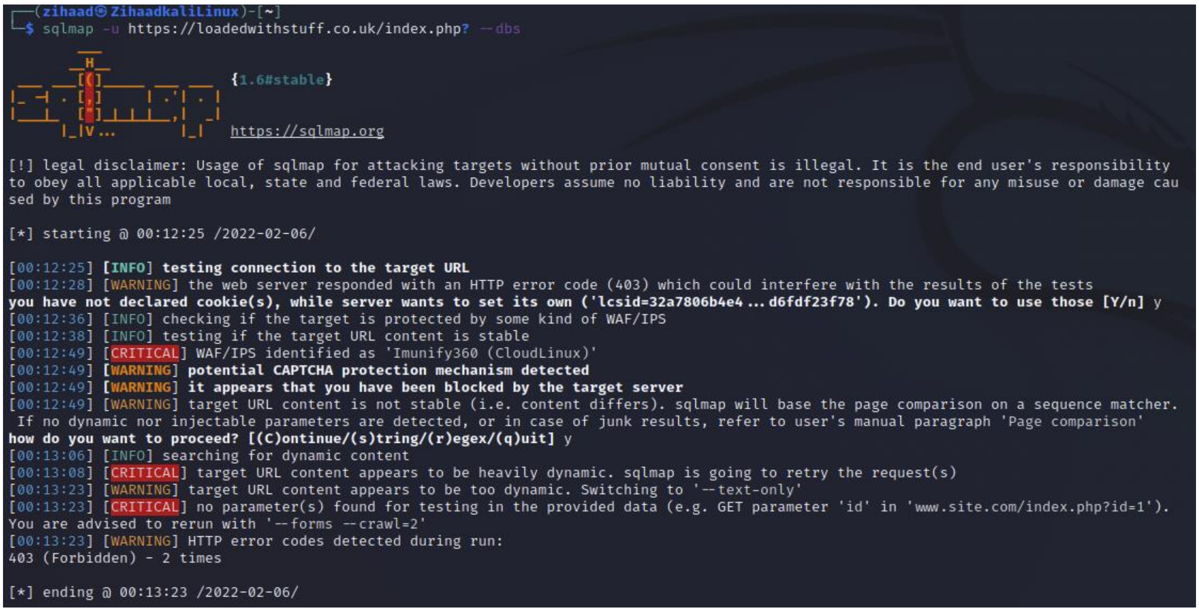
```
┌──(zihaad㉿ZihaadkaliLinux)-[~]
└─$ nikto -h loadedwithstuff.co.uk -ssl
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          68.66.247.187
+ Target Hostname:    loadedwithstuff.co.uk
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=loadedwithstuff.co.uk
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/ST=TX/L=Houston/O=cPanel, Inc./CN=cPanel, Inc. Certification Authority
+ Start Time:         2022-02-06 00:39:15 (GMT2)
---------------------------------------------------------------------------
+ Server: imunify360-webshield/1.18
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: Connect failed: ; Connection timed out at /var/lib/nikto/plugins/LW2.pm line 5157.
: Connection timed out
+ Scan terminated:  20 error(s) and 5 item(s) reported on remote host
+ End Time:           2022-02-06 00:46:58 (GMT2) (463 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure 5: Nikto scan

Additionally *Nikto* detected that Imunify360-webshield/1.18 was installed. According CloudLinux (2022) Imunify360 is a complete security solution designed for Linux servers that provides an Intrusion Detection and Protection System (IPS and IDS), advance web application firewall capabilities as well as being able to block scanners amongst others.

To further enhance the results obtained from *Nikto*, *OWASP ZAP (Zed Attack Proxy)* was utilized. *OWASP ZAP* is one of the most commonly used web application scanners worldwide and is available as open source (OWASP Foundation Inc., 2022). Research has indicated that it is one of the best tools for vulnerability scans in web applications and is characterized by its comprehensive analysis options (Sagar, 2018). This summarizes the vulnerabilities in a clear matrix and evaluates them according to risk and confidence, so that a quick overview of the risk potential is provided. *OWASP ZAP* results are discussed in detail in section 4.

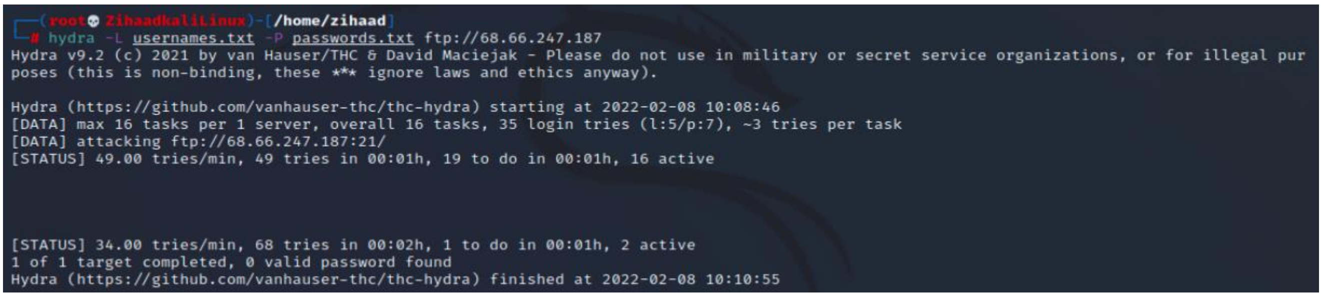
The results obtained from *Nmap* (Figure 3) confirmed that ports 3306 (MySQL) and ports 21 (ftp) was open. *Sqlmap* was then used to detect vulnerabilities in the database and exploit SQL injection parameters (Damele & Stampar, 2022), however this proved to be unsuccessful (indicated in Figure 6 below) since the website had a WAF/IPS (Imunify360) enabled.



```
┌──(zihaad㉿ZihaadkaliLinux)-[~]
└─$ sqlmap -u https://loadedwithstuff.co.uk/index.php? --dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6#stable}
|_ -| . [,]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility
to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage cau
sed by this program

[*] starting @ 00:12:25 /2022-02-06/

[00:12:25] [INFO] testing connection to the target URL
[00:12:28] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the tests
you have not declared cookie(s), while server wants to set its own ('lcsid=32a7806b4e4...d6fdf23f78'). Do you want to use those [Y/n] y
[00:12:36] [INFO] checking if the target is protected by some kind of WAF/IPS
[00:12:38] [INFO] testing if the target URL content is stable
[00:12:49] [CRITICAL] WAF/IPS identified as 'Imunify360 (CloudLinux)'
[00:12:49] [WARNING] potential CAPTCHA protection mechanism detected
[00:12:49] [WARNING] it appears that you have been blocked by the target server
[00:12:49] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher.
 If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] y
[00:13:06] [INFO] searching for dynamic content
[00:13:08] [CRITICAL] target URL content appears to be heavily dynamic. sqlmap is going to retry the request(s)
[00:13:23] [WARNING] target URL content appears to be too dynamic. Switching to '--text-only'
[00:13:23] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1').
You are advised to rerun with '--forms --crawl=2'
[00:13:23] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 2 times

[*] ending @ 00:13:23 /2022-02-06/
```

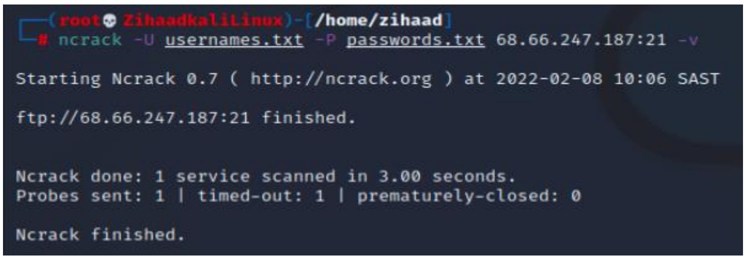
Figure 6: Sqlmap scan

Lastly, brute force attempts were performed using port 21 with *Metasploit*, *Hydra* and *ncrack*. The objective was not to brute force the server by attempting thousands of usernames and passwords, this was merely an exercise to indicate how easy it is to brute force servers when unsecured ports are open. Attempts of brute force are indicated in Figures 7, 8 and 9 below with a few sample username and passwords.



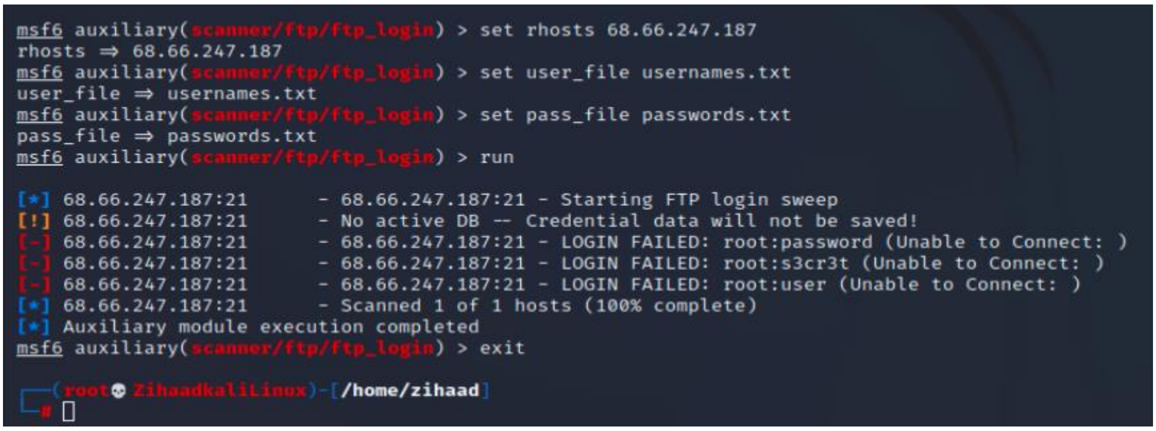
```
┌──(root💀 ZihaadkaliLinux)-[/home/zihaad]
└─# hydra -L usernames.txt -P passwords.txt ftp://68.66.247.187
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal pur
poses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-02-08 10:08:46
[DATA] max 16 tasks per 1 server, overall 16 tasks, 35 login tries (l:5/p:7), ~3 tries per task
[DATA] attacking ftp://68.66.247.187:21/
[STATUS] 49.00 tries/min, 49 tries in 00:01h, 19 to do in 00:01h, 16 active



[STATUS] 34.00 tries/min, 68 tries in 00:02h, 1 to do in 00:01h, 2 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-02-08 10:10:55
```

Figure 7: Hydra Brute force



```
┌──(root💀 ZihaadkaliLinux)-[/home/zihaad]
└─# ncrack -U usernames.txt -P passwords.txt 68.66.247.187:21 -v

Starting Ncrack 0.7 ( http://ncrack.org ) at 2022-02-08 10:06 SAST

ftp://68.66.247.187:21 finished.


Ncrack done: 1 service scanned in 3.00 seconds.
Probes sent: 1 | timed-out: 1 | prematurely-closed: 0

Ncrack finished.
```

Figure 8: Ncrack brute force



```
msf6 auxiliary(scanner/ftp/ftp_login) > set rhosts 68.66.247.187
rhosts ⇒ 68.66.247.187
msf6 auxiliary(scanner/ftp/ftp_login) > set user_file usernames.txt
user_file ⇒ usernames.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set pass_file passwords.txt
pass_file ⇒ passwords.txt
msf6 auxiliary(scanner/ftp/ftp_login) > run

[*] 68.66.247.187:21      - 68.66.247.187:21 - Starting FTP login sweep
[!] 68.66.247.187:21      - No active DB -- Credential data will not be saved!
[-] 68.66.247.187:21      - 68.66.247.187:21 - LOGIN FAILED: root:password (Unable to Connect: )
[-] 68.66.247.187:21      - 68.66.247.187:21 - LOGIN FAILED: root:s3cr3t (Unable to Connect: )
[-] 68.66.247.187:21      - 68.66.247.187:21 - LOGIN FAILED: root:user (Unable to Connect: )
[*] 68.66.247.187:21      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_login) > exit

┌──(root💀 ZihaadkaliLinux)-[/home/zihaad]
└─# ▯
```

Figure 9: Metasploit Brute force

3. Assumptions

A few assumptions were made in order to achieve the desired objectives. These are listed below:

1. There is event logging or recording performed on the access to these servers since various scans were blocked after a few successful attempts.
2. It is possible that false positives may exist with the use of scanning tools i.e. detecting vulnerabilities that in reality may not exist. Vulnerability scanning performed externally (not in the same internal network as the server hosting the website) do not always have access to all of the information (IBM Corporation, 2021).

4. Results

Table 2 below represents vulnerabilities identified in the initial designed document, scanning tools used to test these vulnerabilities, the reason a specific scanning tool was selected as well as the test results and further recommendations.

Table 3 below represents detailed results and recommendation achieved by utilizing *OWASP ZAP*.

Table 2: Summary of Tools, Results and Recommendations

Vulnerability / Threat	Tools Used:	Why was this tool selected?	Summary of Tests / Results	Recommendations
Weak Account Passwords	Hydra, Metasploit & ncrack	Enables brute force attacks with selected usernames and passwords.	Brute force attack was not possible	1. Passwords seem to be strong, limited login attempts are implemented. 2. Always use strong complex passwords.
Exploiting Open Ports	Nmap & Metasploit	Used to determine open ports. Nmap also has the ability to perform service discovery and version detection of applications and operating systems.	21/tcp ftp 25/tcp smtp 53/tcp domain 80/tcp http 110/tcp pop3 143/tcp imap 443/tcp https 465/tcp smtps 587/tcp submission 993/tcp imaps 995/tcp pop3s 2077/tcp tsrmagt 2086/tcp gnunet 2525/tcp ms-v-worlds 3306/tcp mysql 5432/tcp postgresql 52223/tcp unknown 52224/tcp unknown 53/udp domain	1. Shut down port 80 (http) and use port 443 (https) with TLSv1.3 (Server has been tested against SSL labs (Qualys, 2022). Two weak ciphers were found which should be removed. Results listed in Appendix B. 2. Shut down port 21 (ftp), SFTP should be used instead (port 22) 3. Upgrade BIND 9 to version 9.18.0 4. Shut down any unused ports.
Exploiting OS & Web Applications	Whatweb	Identify web technologies used by the website including Content Management Systems (O'Reilly Media, Inc, 2022).	PHP version 7.3.3.3 jQuery version 3.4.1 CMS Detected: Loaded Commerce 6.6 - Powerful Ecommerce Shopping Cart	1. Upgrade PHP to version 7.4 2. Upgrade jQuery to version 3.6.0. 3. Update OS, software packages and kernel to the latest version of RHEL 7.9. 4. Harden OS according to CIS Benchmarks (Center for Internet Security, 2022). 5. Define & maintain a patching policy.
Web Server Vulnerabilities	Nikto	Used to Scan Web Servers for known vulnerabilities	1. Imunify360-webshield/1.18 detected 2. Anti-clickjacking X-Frame-Options header is not present 3. The X-XSS-Protection header is not defined 4. Strict-Transport-Security HTTP header is not defined 5. Expect-CT header is not present 6. X-Content-Type-Options Header is not set.	1. Set the X-Frame-Options header for all responses containing HTML content. The possible values are "DENY", "SAMEORIGIN", or "ALLOW-FROM uri" 2. Explicitly turn off: "X-XSS-Protection: 0" header] 3. Only SSL/TLS connections should be supported 4. Set Certificate Transparency so user agents report Expect-CT failures. "Expect-CT: max-age=604800, report-uri=https://foo.example/report" 5. Set "X-Content-Type-Options: nosniff" (OWASP Cheat Sheet Series, 2021)
	OWASP ZAP	Penetration testing tool designed to test web applications	**Results listed in Table 3**	**Recommendations listed in Table 3**
SQL Injection	Sqlmap	Detecting & exploiting SQL Injection	Tool blocked by target server, WAF/IPS identified as 'Imunify360'	Unable to detect if SQL Injection is possible however preventative measures should be put in place viz. 1. Perform regular database auditing (Lokhande & Meshram, 2013) 2. Implement SQL detection technology i.e. machine learning algorithms (Sivasangari et al., 2021)

Table 3: OWASP ZAP Results and Recommendations

Alerts Found	Description (OWASP Foundation Inc., 2022)	Rating (Priority)	Risk	Recommendations (OWASP Foundation Inc., 2022)
Vulnerable JS Library	Two applications in the JavaScript library has been identified as vulnerable i.e. AngularJS v1.6.9 & jQuery v.3.4.1	8	High	Patch to latest stable releases as follows: AngularJS - 1.8.2 / 21 October 2020 jQuery - 3.6.0 / 2 March 2021
Absence of Anti-CSRF Tokens	Unique tokens used in web-applications to prevent Cross-Site Request Forgery attacks.	6	Medium	1. Use anti-CSRF packages i.e. OWASP CSRFGuard 2. Ensure application is free of cross-site scripting issues 3. Application can be updated to include a temporary valid token
Application Error Disclosure	These are error messages that may disclose sensitive information	6	Medium	Implement custom error pages.
Cookie No HttpOnly Flag	A cookie has been set without the HttpOnly flag and can be accessed by JavaScript.	4	Low	Ensure HttpOnly flag is set for all cookies.
Cookie Without Secure Flag	A cookie has been set without the secure flag and can be accessed via unencrypted connections.	4	Low	Ensure secure flag is set for cookies that contain sensitive information.
Cookie Without SameSite Attribute	A cookie has been set without the SameSite attribute, the cookie can be sent as a result of a ‘cross-site’ request.	4	Low	Ensure SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Server Leaks Information via "X-Powered-By" HTTP Response Header Fields	The web server is leaking information via “X-Powered-By” HTTP response headers. Attackers can use this information to identify components of the web application.	4	Low	Configure Web Server to suppress "X-Powered-By" headers.
Timestamp Disclosure - Unix	Web server discloses time stamp	4	Low	Confirm that the timestamp data is not sensitive, and the data cannot be aggregated to disclose exploitable patterns.
Information Disclosure - Sensitive Information in URL	The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies.	2	Informational	Do not pass sensitive information in URI's
Information Disclosure - Suspicious Comments	The response appears to contain suspicious comments which may help an attacker.	2	Informational	Remove all comments that return information

The above results can be summarized by Figure 10 below:

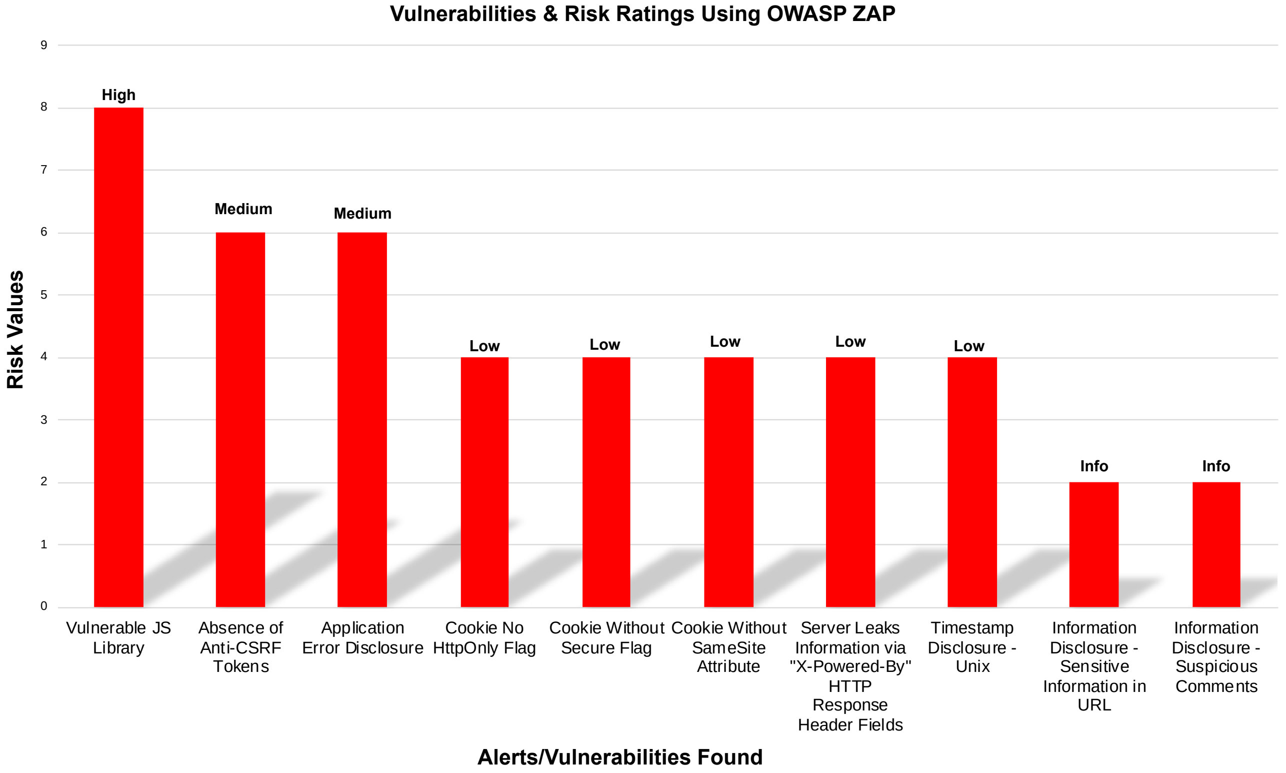
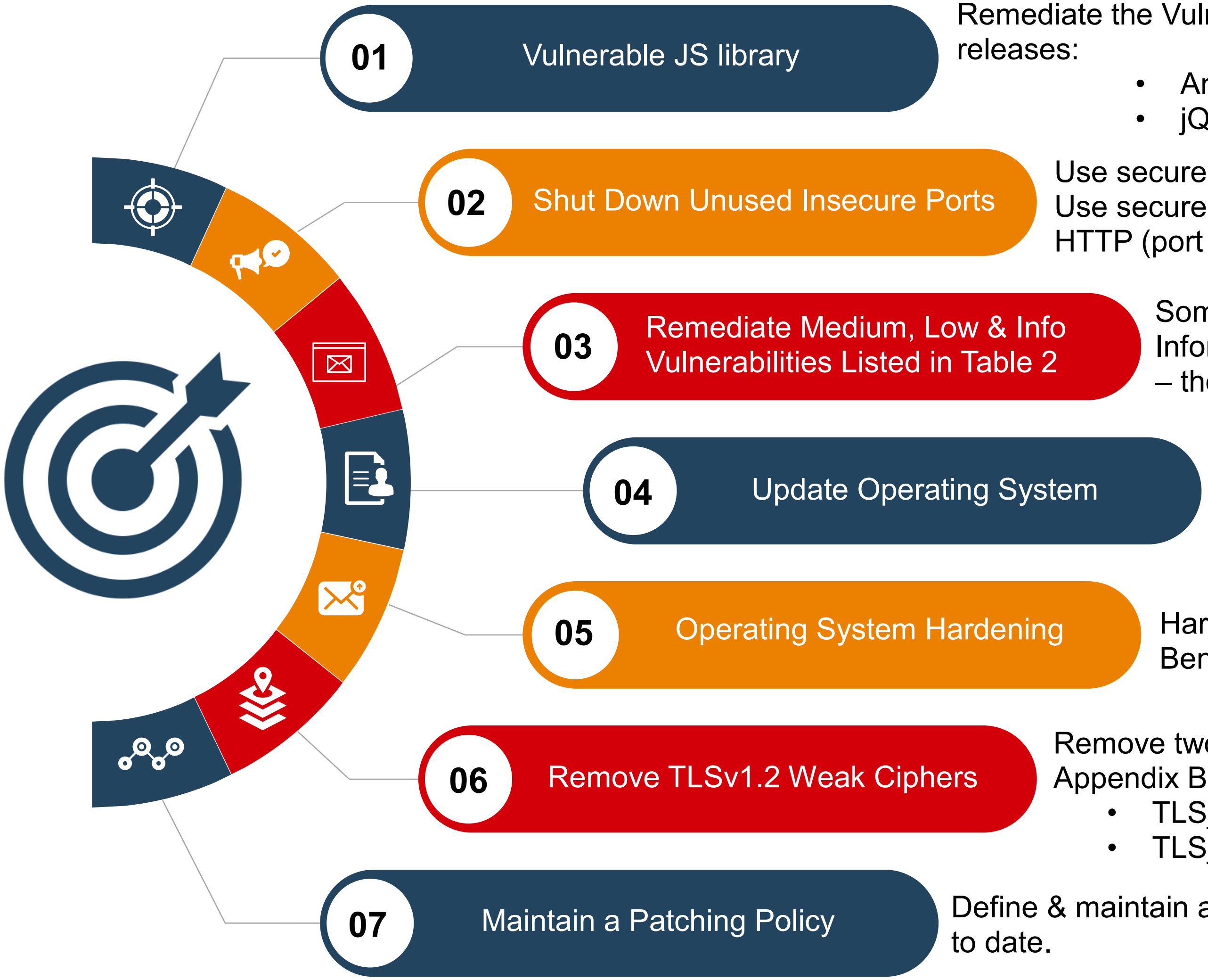


Figure 10: Vulnerabilities & Risk Ratings (OWASP ZAP)

In total there were 10 possible vulnerabilities picked up by *OWASP ZAP*. These vulnerabilities were categorised from a critical risk (represented by number 10) down to an information risk (represented by number 2) perspective. The risk values align with the standard Common Vulnerability and Exposure (CVE) ratings (Imperva, 2021). The detailed *OWASP ZAP* scans can be found in Appendix A.

5. Recommendations

As listed in table 2 and 3 above, all recommendations to enhance the website security are provided in line with GDPR guidelines (ICO, 2022). However, the highest in terms of business priority and the most cost effective ones should be considered first. These are as follows:



01 Vulnerable JS library

Remediate the Vulnerable JS library alert by patching to latest stable releases:

- AngularJS - 1.8.2 / 21 October 2020
- jQuery - 3.6.0 / 2 March 2021

02 Shut Down Unused Insecure Ports

Use secure FTP (SFTP) on port 22 instead of FTP (port 21). Use secure HTTP (HTTPS) with TLSv1.3 only instead of HTTP (port 80). Shut down any other unused ports.

03 Remediate Medium, Low & Info Vulnerabilities Listed in Table 2

Some informational risks affects PCI compliance (e.g. Information Disclosure - Sensitive Information in URL) – these must be remediated.

04 Update Operating System

Update OS, software packages and kernel to the latest version of RHEL 7.9.

05 Operating System Hardening

Harden the operating system according to CIS Benchmarks (Center for Internet Security, 2022)

06 Remove TLSv1.2 Weak Ciphers

Remove two weak ciphers found with TLS v1.2 (more details in Appendix B):

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

07 Maintain a Patching Policy

Define & maintain a patching policy so that applications are kept up to date.

6. References

Abbass, W., Baina, A. & Bellafkih, M. (2016) Improvement of information system security risk management. International Colloquium on Information Science and Technology, 182-187. Available from: https://ieeexplore.ieee.org/document/7805039 [Accessed 11 February 2022].

Center for Internet Security (2022) CIS Benchmarks. Available from: https://www.cisecurity.org/cis-benchmarks/ [Accessed 07 February 2022].

CloudLinux (2022) Introduction. Available from: https://docs.imunify360.com/introduction/ [Accessed 09 February 2022].

Damele & Stampar (2022) sqlmap – Automatic SQL injection and database takeover tool. Available from: https://sqlmap.org/ [Accessed 22 January 2022].

IBM Corporation (2021). Why do false positives occur? Available from: https://www.ibm.com/docs/en/qsip/7.4?topic=manager-management-false-positives [Accessed 09 February 2022].

ICO (2022) Information Commissioners Office – Guide to the General Data Protection Regulation – Security. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ [Accessed 09 February 2022].

Imperva (2021) CVE Vulnerability. Available from: https://www.imperva.com/learn/application-security/cve-cvss-vulnerability/ [Accessed 09 February 2022].

Lokhande, S, P & Meshram, B. (2013) E-Commerce Applications: Vulnerabilities, Attacks and Countermeasures. *International Journal of Advanced Research in Computer Engineering & Technology.* Available from: https://www.researchgate.net/publication/235697382_E-Commerce_Applications_Vulnerabilities_Attacks_and_Countermeasures [Accessed 09 February 2022].

Mayer, N., Dubois, R. & Heymans, P. (2008) Towards a measurement framework for security risk management. University of Namur, Belgium. Available from: http://nmayer.eu/publis/MODSEC08_metrics-risk-management.pdf [Accessed 11 February 2022].

OffSec Services Limited (2022) Kali Linux Features. Available from: https://www.kali.org/features/ [Accessed 08 February 2022].

O’Reilly Media Inc. (2022) The WhatWeb scanner. Available from: https://www.oreilly.com/library/view/web-penetration-testing/9781788623377/4ce1f42c-accd-4b10-b4b7-32aa35129f96.xhtml [Accessed 06 February 2022].

OWASP Foundation Inc. (2022) OWASP Zed Attack Proxy (ZAP). Available from: https://www.zaproxy.org/ [Accessed 23 February 2022].

Qualys (2022) SSL Server Test. Available from: https://www.ssllabs.com/ssltest/analyze.html?d=loadedwithstuff.co.uk [Accessed 07 February 2022].

Sagar, D., Kukreja, S., Brahma, J., Tyagi, S. & Jain, P. (2018) Studying Open Source Vulnerability Scanners For Vulnerabilities in Web Applications. Department of Computer Science and Engineering, Manav Rachna International Institute of Research and Studies, Faridabad, India. Available from: https://www.iioab.org/IIOABJ_9.2_43-49.pdf [Accessed 23 January 2022].

Shah, M., Ahmed, S., Saeed, K., Junaid, M., Khan, H. & Ata-ur-rehman (2019) Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool. 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMet). Available from: https://ieeexplore.ieee.org/abstract/document/8673520 [Accessed 22 February 2022].

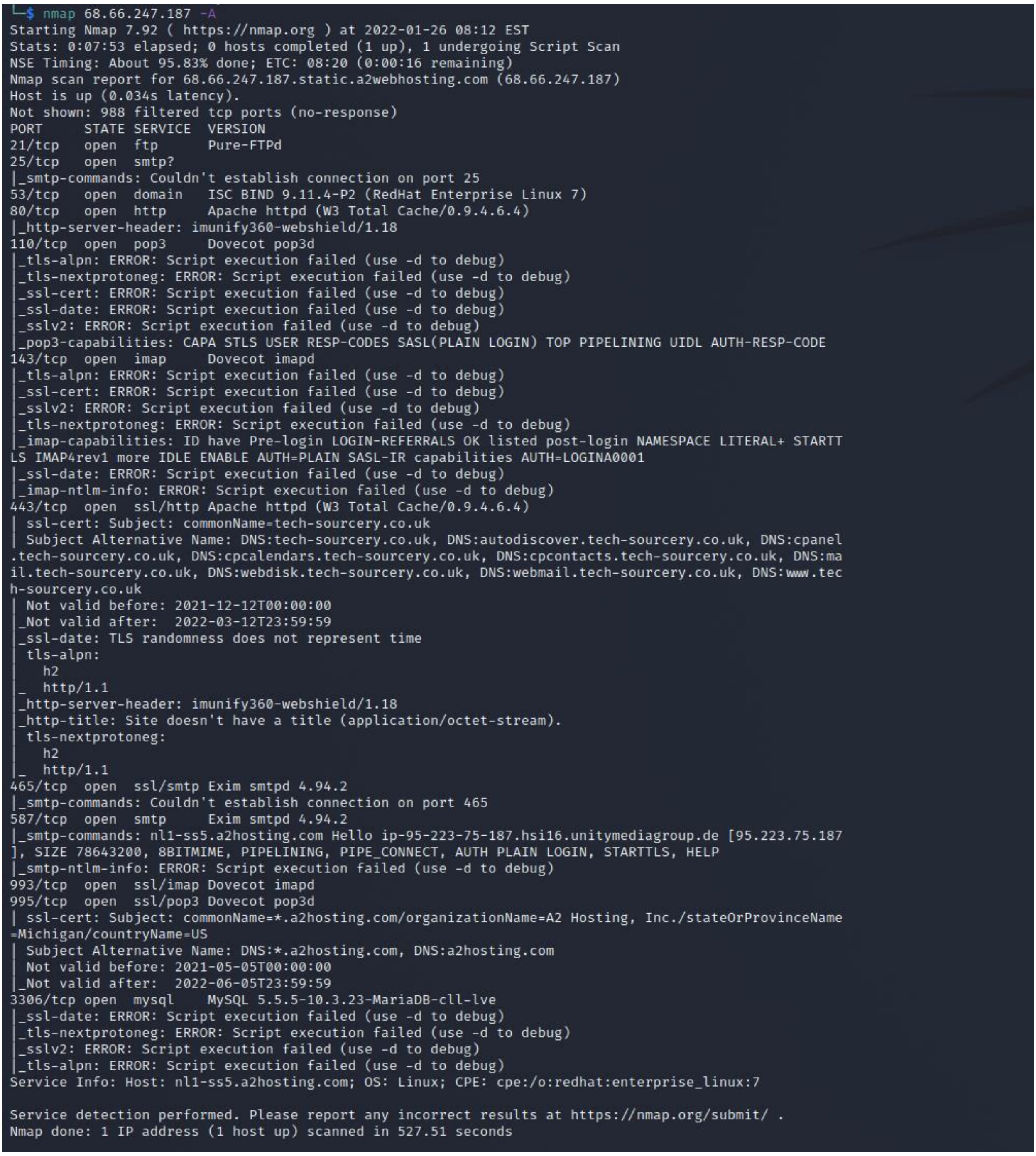
Shostack, A. (2009) “The Threats to Our Products”. Microsoft Security. Available from: https://www.microsoft.com/security/blog/2009/08/27/the-threats-to-our-products/ [Accessed 10 February 2022].

Sivasangari, A., Jyotsna, J., Pravalika, K. (2021) ‘SQL Injection Attack Detection using Machine Learning Algorithm’, *5th International Conference on Trends in Electronics and Informatics (ICOEI)*. India, 3-5 June 2021. USA: IEEE. Available from: https://ieeexplore.ieee.org/document/9452914 [Accessed 10 February 2022].

Softaculous (2022) What is Softaculous. Available from: https://www.softaculous.com/softaculous/ [Accessed 09 February 2022].

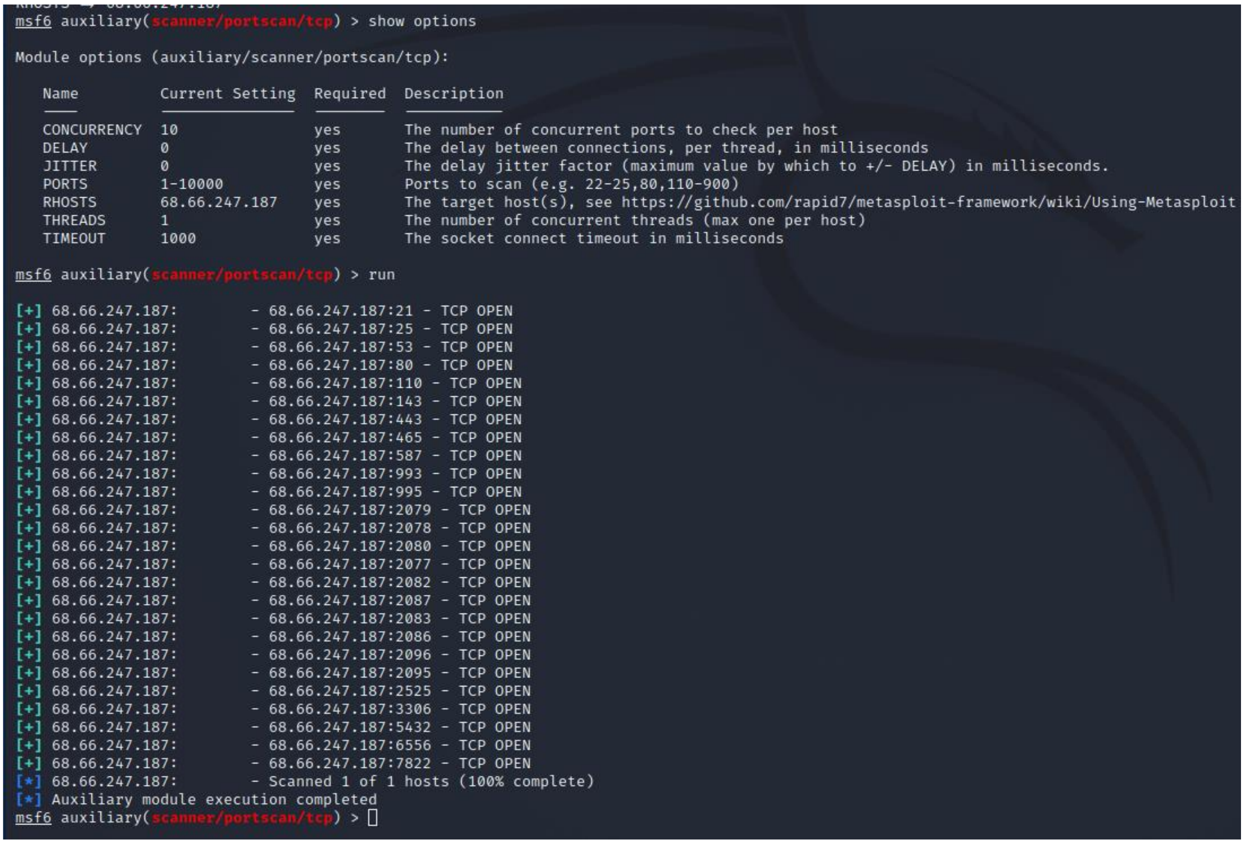
Appendix A

Nmap - -A scan: detecting Red Hat Enterprise Linux 7 as the operating system.



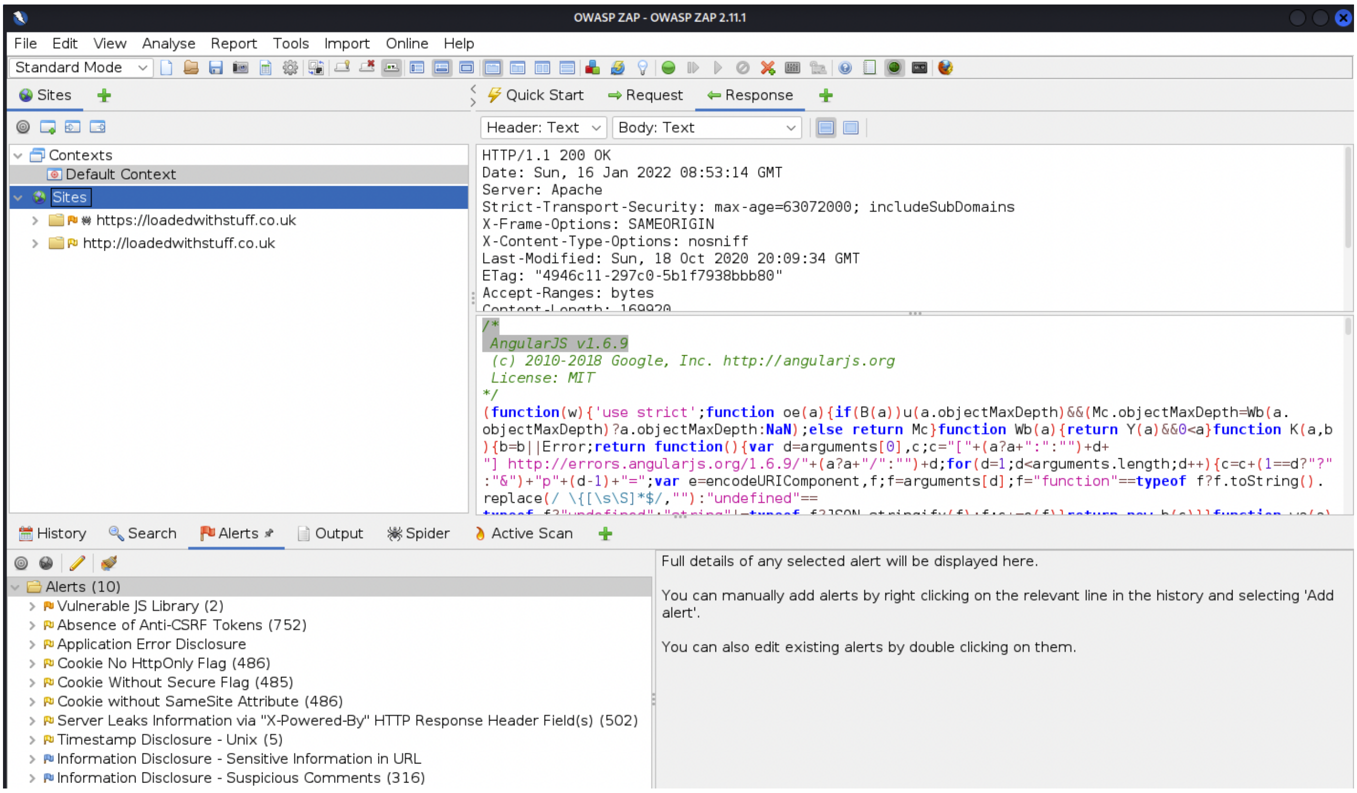
```
└─$ nmap 68.66.247.187 -A
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-26 08:12 EST
Stats: 0:07:53 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 95.83% done; ETC: 08:20 (0:00:16 remaining)
Nmap scan report for 68.66.247.187.static.a2webhosting.com (68.66.247.187)
Host is up (0.034s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      Pure-FTPd
25/tcp   open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
53/tcp   open  domain   ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80/tcp   open  http     Apache httpd (W3 Total Cache/0.9.4.6.4)
|_http-server-header: imunify360-webshield/1.18
110/tcp  open  pop3     Dovecot pop3d
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_pop3-capabilities: CAPA STLS USER RESP-CODES SASL(PLAIN LOGIN) TOP PIPELINING UIDL AUTH-RESP-CODE
143/tcp  open  imap     Dovecot imapd
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_imap-capabilities: ID have Pre-login LOGIN-REFERRALS OK listed post-login NAMESPACE LITERAL+ STARTT
LS IMAP4rev1 more IDLE ENABLE AUTH=PLAIN SASL-IR capabilities AUTH=LOGINA0001
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_imap-ntlm-info: ERROR: Script execution failed (use -d to debug)
443/tcp  open  ssl/http Apache httpd (W3 Total Cache/0.9.4.6.4)
| ssl-cert: Subject: commonName=tech-sourcery.co.uk
| Subject Alternative Name: DNS:tech-sourcery.co.uk, DNS:autodiscover.tech-sourcery.co.uk, DNS:cpanel
.tech-sourcery.co.uk, DNS:cpcalendars.tech-sourcery.co.uk, DNS:cpcontacts.tech-sourcery.co.uk, DNS:ma
il.tech-sourcery.co.uk, DNS:webdisk.tech-sourcery.co.uk, DNS:webmail.tech-sourcery.co.uk, DNS:www.tec
h-sourcery.co.uk
| Not valid before: 2021-12-12T00:00:00
|_Not valid after:  2022-03-12T23:59:59
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|_  http/1.1
|_http-server-header: imunify360-webshield/1.18
|_http-title: Site doesn't have a title (application/octet-stream).
| tls-nextprotoneg:
|   h2
|_  http/1.1
465/tcp  open  ssl/smtp Exim smtpd 4.94.2
|_smtp-commands: Couldn't establish connection on port 465
587/tcp  open  smtp     Exim smtpd 4.94.2
|_smtp-commands: nl1-ss5.a2hosting.com Hello ip-95-223-75-187.hsi16.unitymediagroup.de [95.223.75.187
], SIZE 78643200, 8BITMIME, PIPELINING, PIPE_CONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
|_smtp-ntlm-info: ERROR: Script execution failed (use -d to debug)
993/tcp  open  ssl/imap Dovecot imapd
995/tcp  open  ssl/pop3 Dovecot pop3d
| ssl-cert: Subject: commonName=*.a2hosting.com/organizationName=A2 Hosting, Inc./stateOrProvinceName
=Michigan/countryName=US
| Subject Alternative Name: DNS:*.a2hosting.com, DNS:a2hosting.com
| Not valid before: 2021-05-05T00:00:00
|_Not valid after:  2022-06-05T23:59:59
3306/tcp open  mysql    MySQL 5.5.5-10.3.23-MariaDB-cll-lve
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
Service Info: Host: nl1-ss5.a2hosting.com; OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 527.51 seconds
```

Metasploit – tcp portscan:



```
RHOSTS => 68.66.247.187
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS       68.66.247.187    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   THREADS      1                yes       The number of concurrent threads (max one per host)
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds

msf6 auxiliary(scanner/portscan/tcp) > run

[+] 68.66.247.187:        - 68.66.247.187:21 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:25 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:53 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:80 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:110 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:143 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:443 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:465 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:587 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:993 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:995 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2079 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2078 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2080 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2077 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2082 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2087 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2083 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2086 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2096 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2095 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2525 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:3306 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:5432 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:6556 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:7822 - TCP OPEN
[*] 68.66.247.187:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > 
```

OWASP ZAP Scans:



https://loadedwithstuff.co.uk
http://loadedwithstuff.co.uk

```
HTTP/1.1 200 OK
Date: Sun, 16 Jan 2022 08:53:14 GMT
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubDomains
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Last-Modified: Sun, 18 Oct 2020 20:09:34 GMT
ETag: "4946c11-297c0-5b1f7938bbb80"
Accept-Ranges: bytes
Content-Length: 169920
```

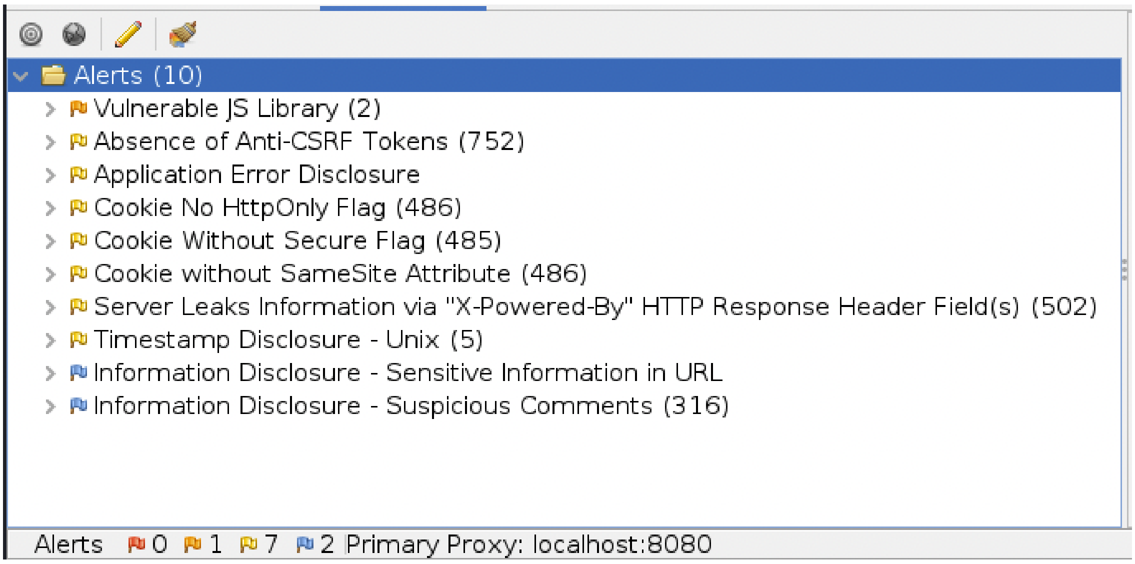
```
/*
 AngularJS v1.6.9
 (c) 2010-2018 Google, Inc. http://angularjs.org
 License: MIT
*/
(function(w){'use strict';function oe(a){if(B(a))u(a.objectMaxDepth)&&(Mc.objectMaxDepth=Wb(a.
objectMaxDepth)?a.objectMaxDepth:NaN);else return Mc}function Wb(a){return Y(a)&&0<a}function K(a,b
){b=b||Error;return function(){var d=arguments[0],c;c="["+(a?a+":":"")+d+
"] http://errors.angularjs.org/1.6.9/"+(a?a+"/":"")+d;for(d=1;d<arguments.length;d++){c=c+(1==d?"?"
:"&")+"p"+(d-1)+"=";var e=encodeURIComponent,f;f=arguments[d];f="function"==typeof f?f.toString().
replace(/ \{[\s\S]*$/,""):"undefined"==
```

Alerts (10)
- Vulnerable JS Library (2)
- Absence of Anti-CSRF Tokens (752)
- Application Error Disclosure
- Cookie No HttpOnly Flag (486)
- Cookie Without Secure Flag (485)
- Cookie without SameSite Attribute (486)
- Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (502)
- Timestamp Disclosure - Unix (5)
- Information Disclosure - Sensitive Information in URL
- Information Disclosure - Suspicious Comments (316)

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.



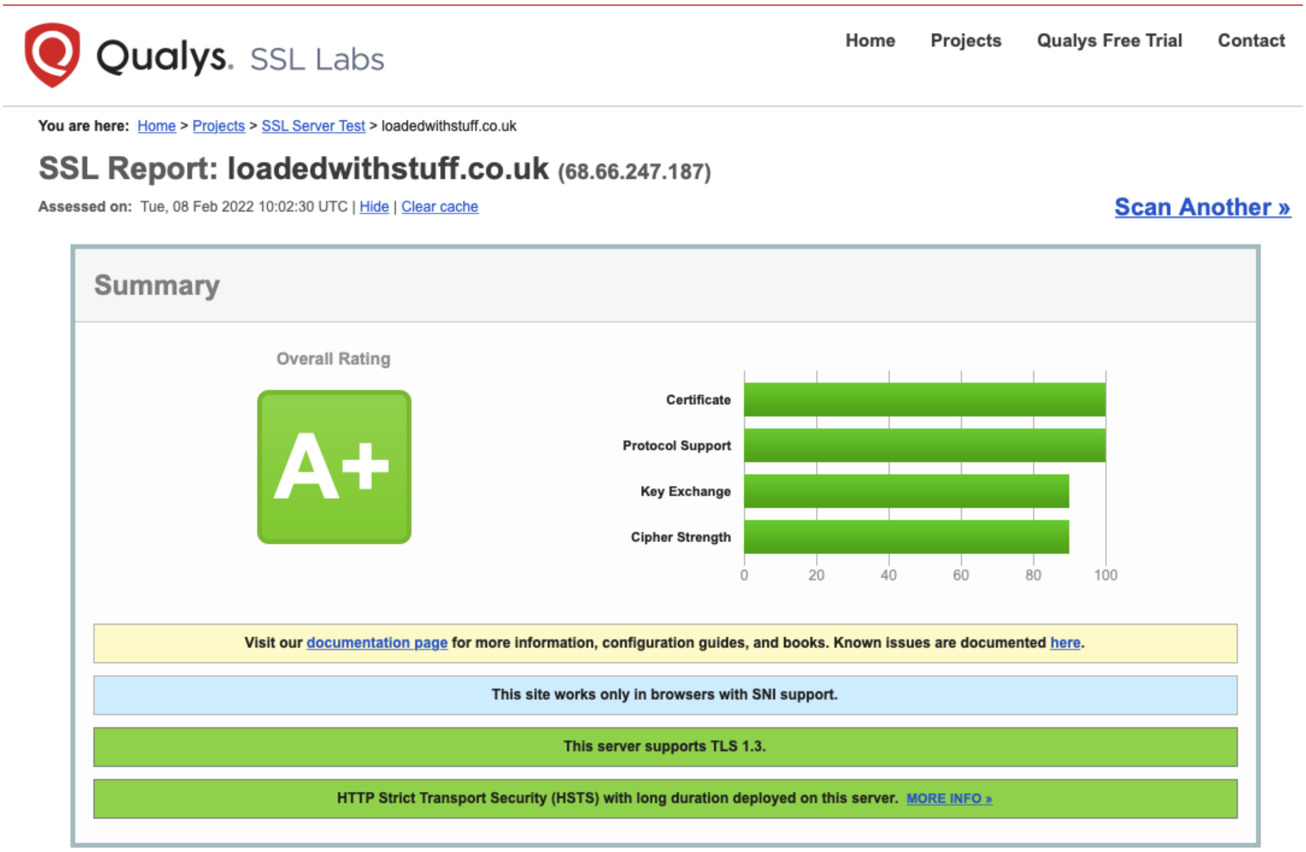
Alerts (10)

- Vulnerable JS Library (2)
- Absence of Anti-CSRF Tokens (752)
- Application Error Disclosure
- Cookie No HttpOnly Flag (486)
- Cookie Without Secure Flag (485)
- Cookie without SameSite Attribute (486)
- Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (502)
- Timestamp Disclosure - Unix (5)
- Information Disclosure - Sensitive Information in URL
- Information Disclosure - Suspicious Comments (316)

Alerts 🟥 0 🟧 1 🟨 7 🟦 2 Primary Proxy: localhost:8080

Appendix B

SSL Report: loadedwithstuff.co.uk



You are here: Home > Projects > SSL Server Test > loadedwithstuff.co.uk

SSL Report: loadedwithstuff.co.uk (68.66.247.187)

Assessed on: Tue, 08 Feb 2022 10:02:30 UTC | Hide | Clear cache

Summary

Overall Rating

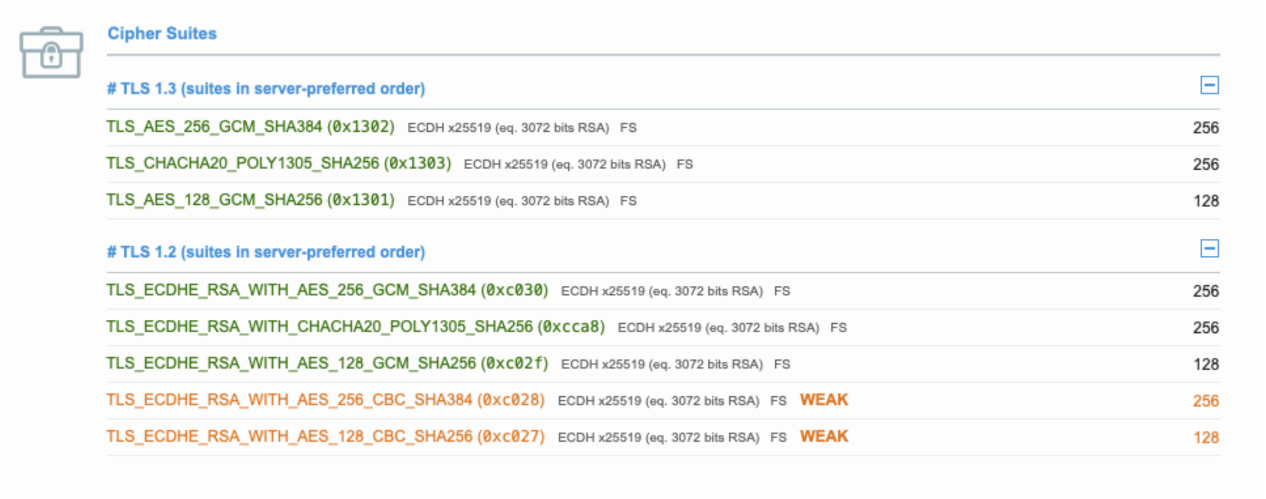
A+

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »



Cipher Suites

TLS 1.3 (suites in server-preferred order)

TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128