

Unit 7 - Scanning Exercise and Collaborative Learning Wiki

Website: <https://loadedwithstuff.co.uk>

Perform scans against your assigned website using the tools available in **Kali Linux**. Answer as many of the following questions as you can:

- What Operating System does the web site utilise?
- What web server software is it running?
- Is it running a CMS (Wordpress, Drupal, etc?)
- What protection does it have (CDN, Proxy, Firewall?)
- Where is it hosted?
- Does it have any open ports?
- Does the site have any known vulnerabilities?
- What versions of software is it using? Are these patched so that they are up to date?

What Operating System does the web site utilise?

Using nmap with OS detection feature: RHEL 7 (Red-Hat Enterprise Linux 7)

```
Nmap scan report for loadedwithstuff.co.uk (68.66.247.187)
Host is up (0.20s latency).
Not shown: 900 filtered tcp ports (no-response), 2 filtered tcp ports (host-unreach), 84 closed tcp ports (conn-refused)
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-title: Site doesn't have a title (application/octet-stream).
|_http-server-header: imunify360-webshield/1.18
110/tcp   open  pop3        Dovecot pop3d
143/tcp   open  imap        Dovecot imapd
443/tcp   open  ssl/http    Apache httpd (W3 Total Cache/0.9.4.6.4)
```

```
Service Info: Host: nl1-ss5.a2hosting.com; OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

NSE: Script Post-scanning.
Initiating NSE at 16:27
Completed NSE at 16:27, 0.00s elapsed
Initiating NSE at 16:27
Completed NSE at 16:27, 0.00s elapsed
Initiating NSE at 16:27
Completed NSE at 16:27, 0.00s elapsed
Read data files from: /usr/bin/../../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1163.83 seconds
```

What web server software is it running?

From the above nmap scans, the web server found is Apache, this is also confirmed by running Nikto:

```
(root@ZihaadkaliLinux)~[~]
# nikto -h https://loadedwithstuff.co.uk
- 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: 2022-01-15 23:07:46 (GMT2)
-----
+ Server: Apache
+ Server banner has changed from 'Apache' to 'imunify360-webshield/1.18' which may suggest a WAF, load balancer or proxy is in place
+ 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.p
m line 5157.
: Connection timed out
+ Scan terminated: 19 error(s) and 5 item(s) reported on remote host
+ End Time: 2022-01-15 23:15:17 (GMT2) (451 seconds)
-----
+ 1 host(s) tested
```

This can also be confirmed by running a simple curl command:

```
(root@ZihaadkaliLinux)~[~]
# curl -v http://loadedwithstuff.co.uk
* Trying 68.66.247.187:80 ...
* Connected to loadedwithstuff.co.uk (68.66.247.187) port 80 (#0)
> GET / HTTP/1.1
> Host: loadedwithstuff.co.uk
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 301 Moved Permanently
< Date: Sun, 16 Jan 2022 08:51:06 GMT
< Server: Apache
< X-Powered-By: PHP/7.3.33
< Strict-Transport-Security: max-age=63072000; includeSubDomains
< X-Frame-Options: SAMEORIGIN
< X-Content-Type-Options: nosniff
< Upgrade: h2,h2c
< Connection: Upgrade
< Location: https://loadedwithstuff.co.uk/
< Content-Length: 0
< Content-Type: text/html; charset=UTF-8
<
* Connection #0 to host loadedwithstuff.co.uk left intact
```

Is it running a CMS (Wordpress, Drupal, etc?)

Kali Linux has a built in tool called “whatweb” in order to detect a CMS (Content Management System), some issues were picked up detecting the CMS but was eventually successful. The source IP addresses were resulting from performing multiple scans were probably blocked by imunify360. After successfully installing a VPN client on Kali Linux – scans were being performed successfully. Screenshots below:


```

root@ZihaadkaliLinux: ~/CMSeeK
File Actions Edit View Help
Quick Start Request Response
Automate
[+] Tip: You can use cmseek via arguments as well check the help menu for more information [+]
Input Description: https://loadedwithstuff.co.uk/
[1] CMS detection and Deep scan
[2] Scan Multiple Sites
[3] Bruteforce CMSs
[U] Update CMSeeK
[R] Rebuild Cache (Use only when you add any custom module)
[0] Exit CMSeeK :(
Enter Your Desired Option:

```

```

CMSEEK by @r3dhax0r
Version 1.1.3 K-RONA
[+] CMS Detection And Deep Scan [+]
[i] Scanning Site: https://loadedwithstuff.co.uk/
[x] Aborting CMSeeK! Couldn't connect to site
Error: <urlopen error timed out>
CMSeeK says ~ Ja mata ne
(root@ZihaadkaliLinux)~[~/CMSeeK]

```

This is probably due to the imunity360 security solution installed

What protection does it have (CDN, Proxy, Firewall?)

Using Nikto and uniscan, it was found to have Imunity360

```

(zihaad@ZihaadkaliLinux)~[~]
$ nikto -h loadedwithstuff.co.uk
- Nikto v2.1.6
+ Target IP: 68.66.247.187
+ Target Hostname: loadedwithstuff.co.uk
+ Target Port: 80
+ Start Time: 2022-01-15 16:26:57 (GMT2)
+ Server: imunity360-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 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 (timeout): Operation now in progress
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time: 2022-01-15 16:33:46 (GMT2) (409 seconds)
+ 1 host(s) tested

```

According to: <https://docs.imunity360.com/introduction/>

“Imunity360 is the security solution for Linux web servers based on machine learning technology which utilizes a multi-layer approach to provide total protection against any types of malicious attacks or abnormal behavior including distributed brute force attacks.”

Where is it hosted?

Using hostingchecker (<https://hostingchecker.com>) it was found to be hosted in Netherlands, Amsterdam

Find out who is hosting any website

To find out where a website is hosted enter the URL address:

It is hosted by: **A2 Hosting, Inc.**

WHOIS information: [Click here](#)

Organization name: **A2 Hosting, Inc**

IP address: **68.66.247.187**

AS(autonomous system) number and organization: **AS55293 A2 Hosting, Inc.**

AS name: **A2HOSTING**

Reverse DNS of the IP: **68.66.247.187.static.a2webhosting.com**

City: **Amsterdam**

Country: **Netherlands**

Does it have any open ports?

Yes, using nmap – the following was obtained:

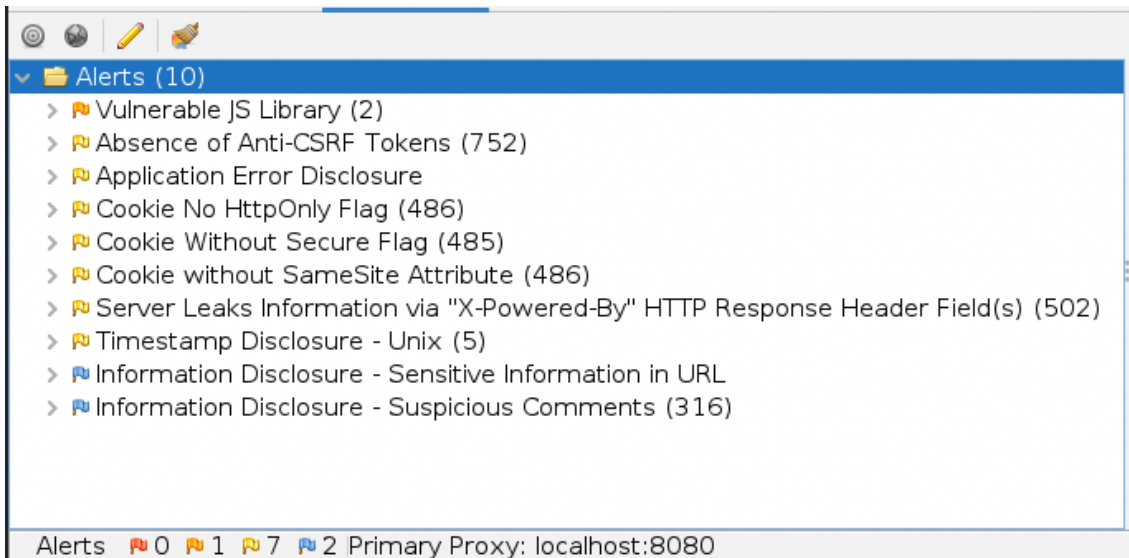
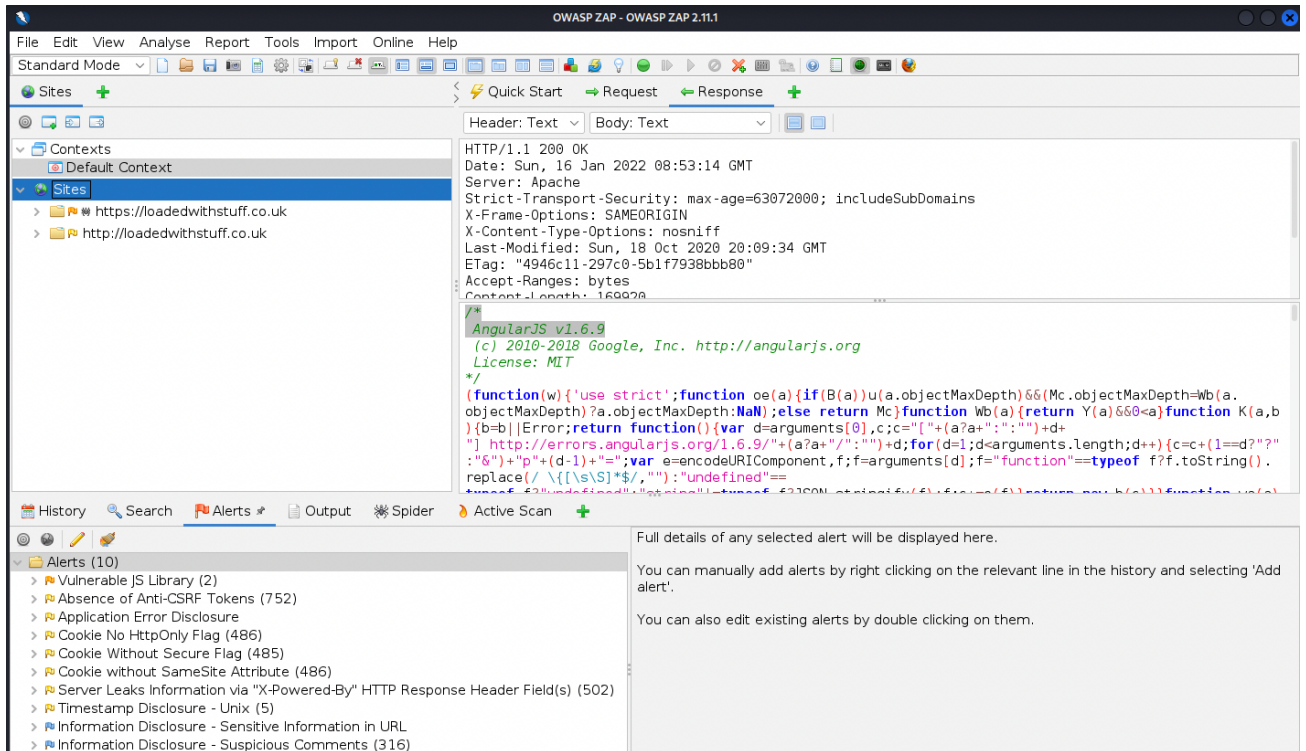
```
(zihaad@ZihaadkaliLinux)-[~]
└─$ nmap -v -A loadedwithstuff.co.uk
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-14 23:47 SAST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:47
Completed NSE at 23:47, 0.00s elapsed
Initiating NSE at 23:47
Completed NSE at 23:47, 0.00s elapsed
Initiating NSE at 23:47
Completed NSE at 23:47, 0.00s elapsed
Initiating Ping Scan at 23:48
Scanning loadedwithstuff.co.uk (68.66.247.187) [2 ports]
Completed Ping Scan at 23:48, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:48
Completed Parallel DNS resolution of 1 host. at 23:48, 0.01s elapsed
Initiating Connect Scan at 23:48
Scanning loadedwithstuff.co.uk (68.66.247.187) [1000 ports]
Discovered open port 80/tcp on 68.66.247.187
Discovered open port 587/tcp on 68.66.247.187
Discovered open port 53/tcp on 68.66.247.187
Discovered open port 3306/tcp on 68.66.247.187
Discovered open port 25/tcp on 68.66.247.187
Discovered open port 993/tcp on 68.66.247.187
Discovered open port 143/tcp on 68.66.247.187
Discovered open port 110/tcp on 68.66.247.187
Discovered open port 21/tcp on 68.66.247.187
Discovered open port 995/tcp on 68.66.247.187
Discovered open port 443/tcp on 68.66.247.187
Discovered open port 465/tcp on 68.66.247.187
Discovered open port 5432/tcp on 68.66.247.187
Discovered open port 2525/tcp on 68.66.247.187
Completed Connect Scan at 23:48, 8.96s elapsed (1000 total ports)
Initiating Service scan at 23:48
```

Does the site have any known vulnerabilities?

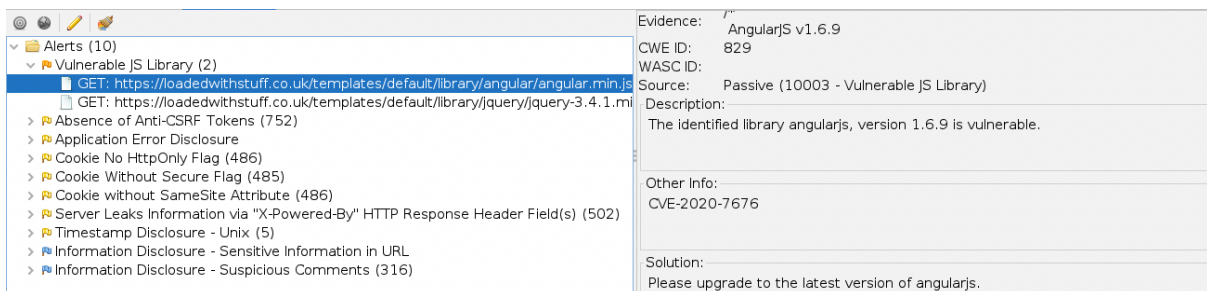
Nikto is an open-source scanner used to detect vulnerabilities in web servers, unfortunately this tool was blocked as well:

```
(zihaad@ZihaadkaliLinux)-[~]
└─$ nikto -h loadedwithstuff.co.uk
- Nikto v2.1.6
-----
+ Target IP: 68.66.247.187
+ Target Hostname: loadedwithstuff.co.uk
+ Target Port: 80
+ Start Time: 2022-01-15 16:26:57 (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 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 (timeout): Operation now in progress
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time: 2022-01-15 16:33:46 (GMT2) (409 seconds)
-----
+ 1 host(s) tested
└─$
```

OWASP ZAP was also used and took about an hour to scan, this produced the following results:

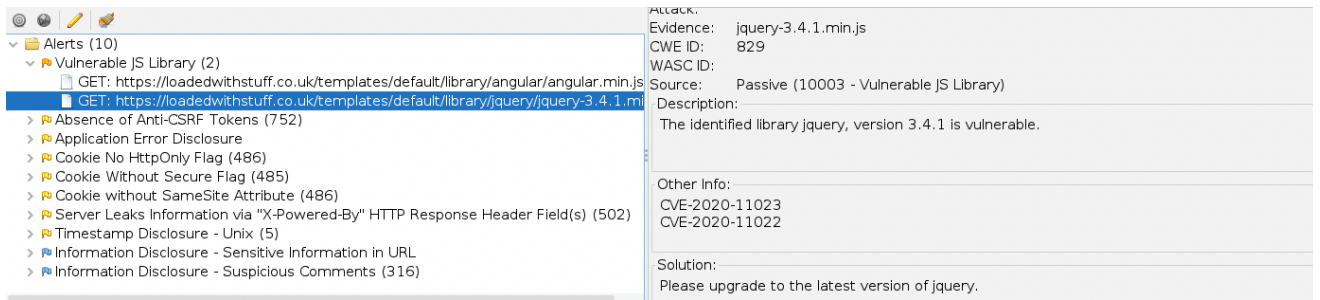


CVE-2020-7676



CVE-2020-11023

CVE-2020-11022



Alerts (10)

- Vulnerable JS Library (2)
 - GET: https://loadedwithstuff.co.uk/templates/default/library/angular/angular.min.js
 - GET: https://loadedwithstuff.co.uk/templates/default/library/jquery/jquery-3.4.1.min.js
- 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)

Attack:

Evidence: jquery-3.4.1.min.js

CWE ID: 829

WASC ID:

Source: Passive (10003 - Vulnerable JS Library)

Description:

The identified library jquery, version 3.4.1 is vulnerable.

Other Info:

CVE-2020-11023

CVE-2020-11022

Solution:

Please upgrade to the latest version of jquery.

What versions of software is it using? Are these patched so that they are up to date?

- AngularJS v1.6.9
- jquery v.3.4.1

Not patched, latest versions are as follows:

AngularJS - Stable release - 1.8.2 / 21 October 2020

jquery - Stable release – 3.6.0 / 2 March 2021