



Sri Lanka Institute of Information Technology

Web Audit - Week 01

IE2062 – Web Security

Submitted by:

Student Registration Number	Student Name
IT19034546	Sandaken B.M.U.

Introduction

- ❖ In this report I have included all the steps and tools that I used to perform this web audit.

What is a Website audit?

- ❖ A complete cyber security audit involves the application of security policies, controls and possible threats that are in relation to all the technical assets, which include websites and web applications. Parts of this audit must be conducted manually by security auditors and the rest using audit software like OpenVas. The most common tool used for testing the safety of a website are the vulnerability scanners. Conducting a proper web audit enables us to find vulnerabilities in web applications and websites which can help reduce cyber-attacks. Cyber-attack techniques like SQL Injections or Cross Site Scripting (XSS) are massive attacks which have threatened the security of the data vastly. Webpage vulnerabilities are the cause of these kind of threats and have highly threatened the web-based systems. The security audit consists of all the hidden and unknown vulnerabilities of a website and its security infrastructure.

Selecting the domain

- ❖ When selecting the domain, I used the “Bug Crowd” which is a web page that is used to find web page vulnerabilities. In that page there is an option known as “Bug Bounty List”. That list consists of many famous websites and web applications, I chose a domain from that list to perform my audit.

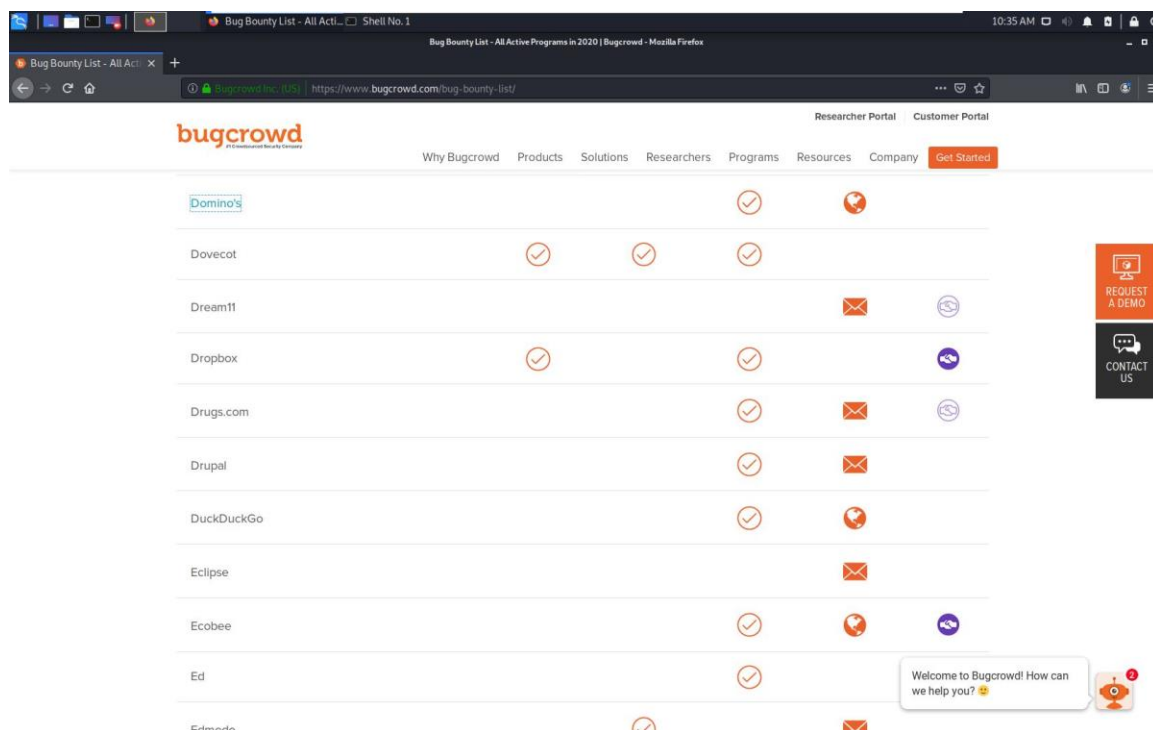


Figure 1

- ❖ Figure 1 shows a few of the domains that were available in the Bug Bounty List.

- ❖ From the above shown list I chose “dominos.com” to perform my web audit.

dominos.com

- ❖ Figure 2 shows the interface of “Domino’s.com”. Domino’s is a worldwide pizza restaurant that have large varieties of pizza and other food items like appetizes and beverages.

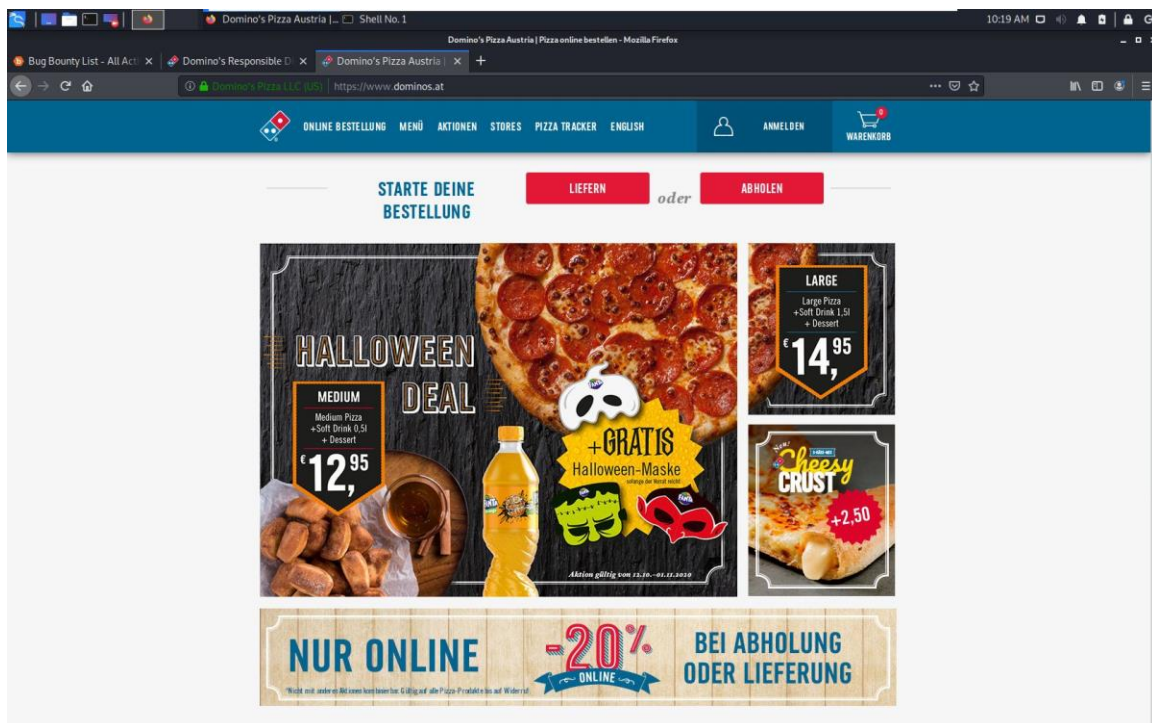


Figure 2

Typical Vulnerabilities Accepted:

- OWASP Top 10 vulnerability categories
- Other vulnerabilities with demonstrated impact

Typical Out of Scope:

- Theoretical vulnerabilities
- Informational disclosure of non-sensitive data
- Low impact session management issues
- Self XSS (user defined payload)

For a full list of program scope please visit the [Responsible Disclosure details page](#)

Figure 3

- ❖ Figure 3 shows the things that we could do to the website and cannot do to the website.
- ❖ In order to find the subdomains of Domino's I used **sublist3r tool**. This tool was available in the GitHub and I installed it to Kali Linux using git cloning. After I ran the sublist3r using the command below.

```
./sublist3r.py -d dominos.com
```

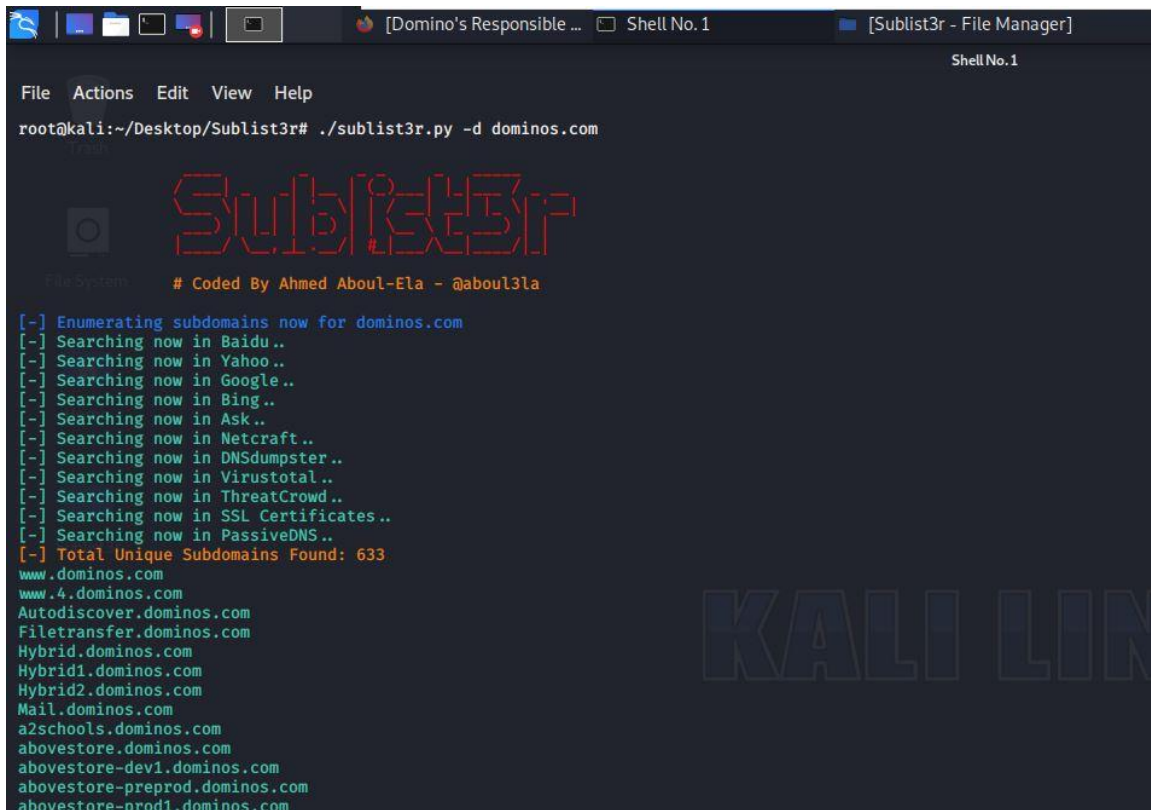


Figure 4

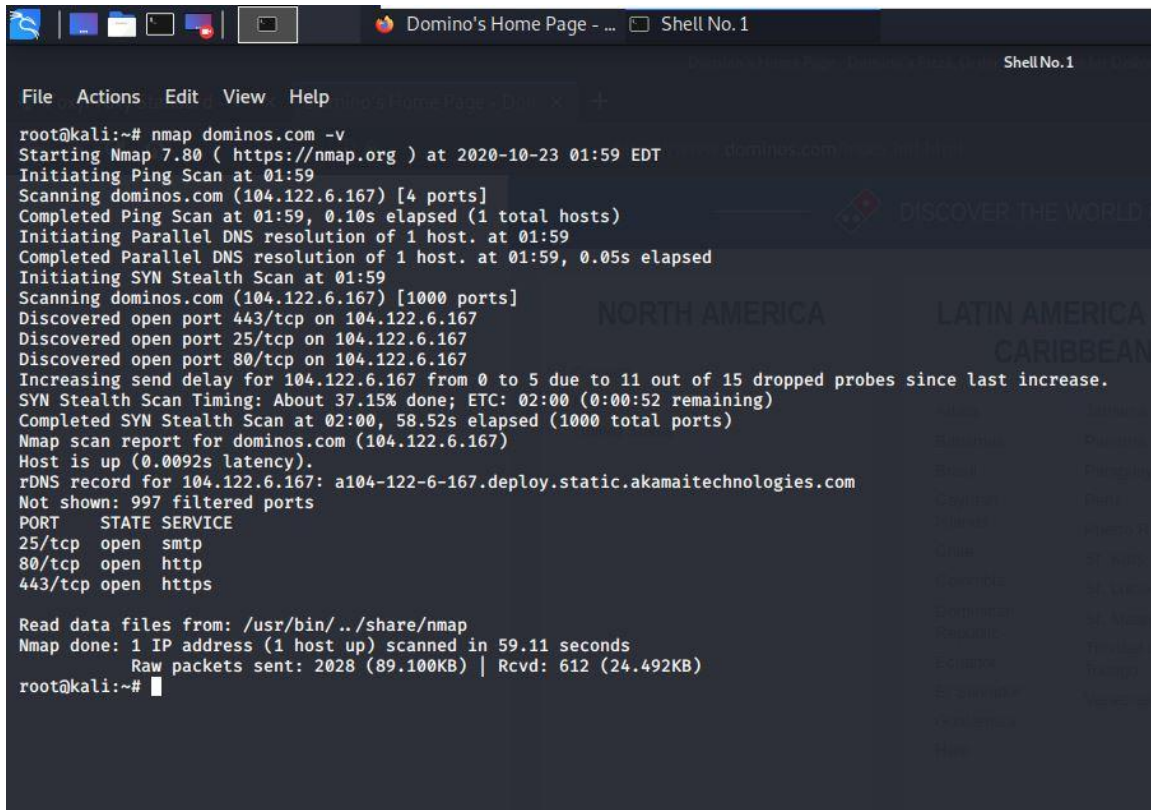
- ❖ In order to conduct the web audit, the selected website must have at least 50 subdomains.
- ❖ According to the scan there are 633 subdomains for the Domino's.com

Web Recon

- ❖ When I first started to create the web audit, I did not use any tool because I was not familiar with the tools hence, I was becoming unsuccessful every time I tried to exploit the domain. At that time, I had made a small assumption that the domain I have chosen is very well secured. However, I watched a few YouTube videos and did a small research online by reading various pdf documents written regarding various the web audits and how to properly conduct it. Then only I understood the various methods of conducting a web audit like recon and exploit. As for my web audit I was using the recon web audit method in which I have to gather all the information relating to my domain, and in order to conduct this type of web audit we have to use various tools. I used various tools like nmap, Amass, netsparker, nikto, pownXSS and burpSuit.

❖

Nmap Tool



```
root@kali:~# nmap dominos.com -v
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-23 01:59 EDT
Initiating Ping Scan at 01:59
Scanning dominos.com (104.122.6.167) [4 ports]
Completed Ping Scan at 01:59, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:59
Completed Parallel DNS resolution of 1 host. at 01:59, 0.05s elapsed
Initiating SYN Stealth Scan at 01:59
Scanning dominos.com (104.122.6.167) [1000 ports]
Discovered open port 443/tcp on 104.122.6.167
Discovered open port 25/tcp on 104.122.6.167
Discovered open port 80/tcp on 104.122.6.167
Increasing send delay for 104.122.6.167 from 0 to 5 due to 11 out of 15 dropped probes since last increase.
SYN Stealth Scan Timing: About 37.15% done; ETC: 02:00 (0:00:52 remaining)
Completed SYN Stealth Scan at 02:00, 58.52s elapsed (1000 total ports)
Nmap scan report for dominos.com (104.122.6.167)
Host is up (0.0092s latency).
rDNS record for 104.122.6.167: a104-122-6-167.deploy.static.akamaitechnologies.com
Not shown: 997 filtered ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 59.11 seconds
Raw packets sent: 2028 (89.100KB) | Rcvd: 612 (24.492KB)
root@kali:~#
```

Figure 5

```
nmap dominos.com -v
```

- ❖ According to Figure 5 Nmap is used to the IP address of the domain.
- ❖ This tool was very useful for me as it helped me identify how many open ports are there for the Domino's.com domain

Amass Tool

```

File Actions Edit View Help
o0+ 000 00+ 00+ #0 00. .W0W .+000 00W.
WW 00 +0W00. 00+ :0 00+ #0 :0W000 00: .. :00
:0W: 00# +W0 00+ :W: +0W00++00W. 000 00#0+00W. #0: 00+
:W00WWW000 + :W00000 0W .0#00W0. :W0WWW000
+00000+. +0000.

v3.3.1
OWASP Amass Project - @owaspamass
In-depth Attack Surface Mapping and Asset Discovery

Usage: amass intel|enum|viz|track|db [options]

-h Show the program usage message
-help Show the program usage message
-version Print the version number of this Amass binary

Subcommands:
amass intel - Discover targets for enumerations
amass enum - Perform enumerations and network mapping
amass viz - Visualize enumeration results
amass track - Track differences between enumerations
amass db - Manipulate the Amass graph database

The user's guide can be found here:
https://github.com/OWASP/Amass/blob/master/doc/user_guide.md

An example configuration file can be found here:
https://github.com/OWASP/Amass/blob/master/examples/config.ini

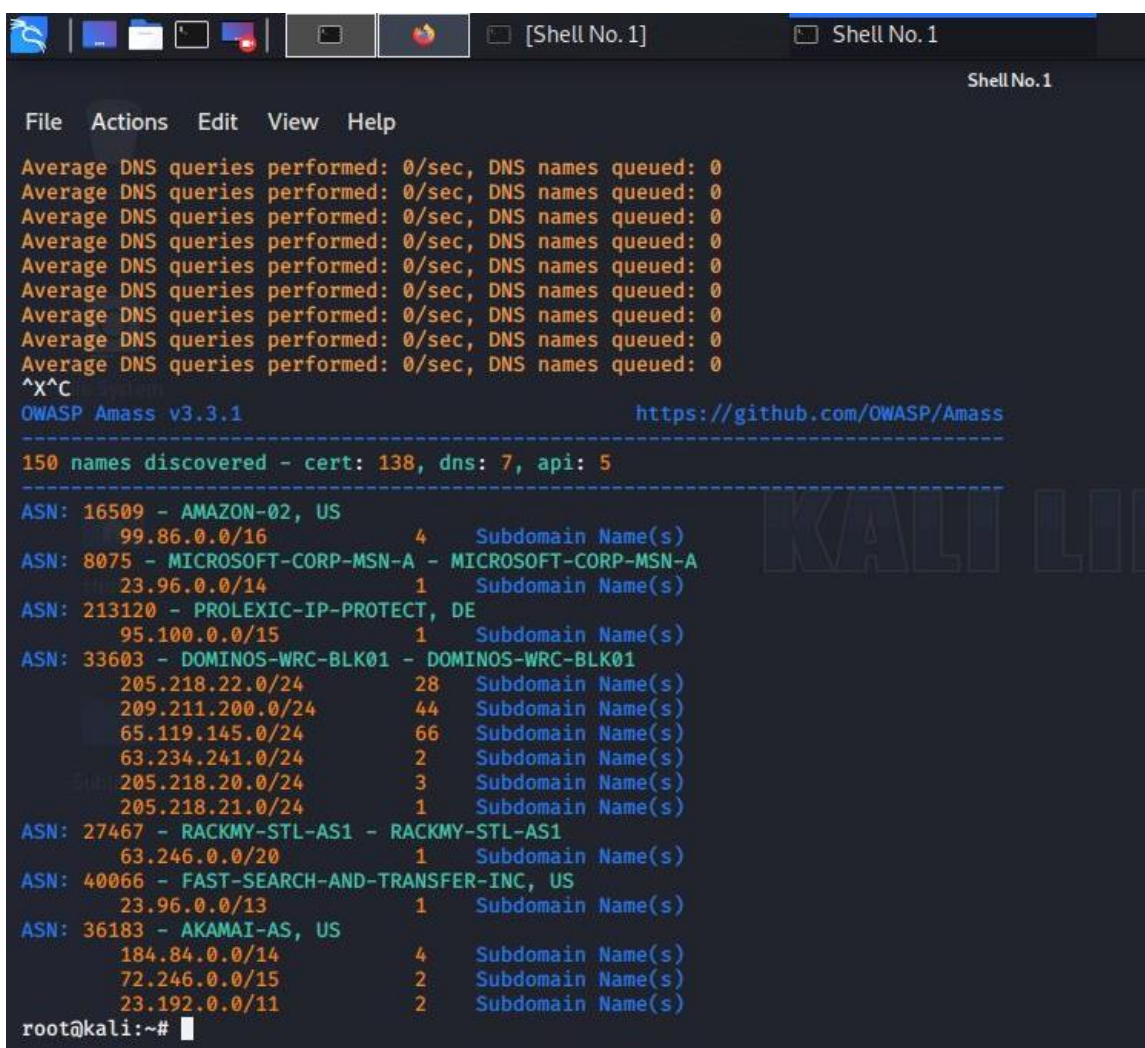
root@kali:~# amass enum -d dominos.com
Querying URLScan for dominos.com subdomains
Querying Sublist3rAPI for dominos.com subdomains
Querying Yahoo for dominos.com subdomains
Querying VirusTotal for dominos.com subdomains
Querying ViewDNS for dominos.com subdomains
Querying ThreatCrowd for dominos.com subdomains

```

Figure 6

amass enum -d dominos.com

- ❖ Above shown in Figure 6 is the Amass Tool which helped me discover the asserts, to get the active and inactive domains and also to get the sub domain of my main domain.
- ❖ I cloned this tool from the GitHub.
- ❖ Link to download this tool: “<https://github.com/OWASP/Amass>”



```
File Actions Edit View Help
Average DNS queries performed: 0/sec, DNS names queued: 0
Average DNS queries performed: 0/sec, DNS names queued: 0
Average DNS queries performed: 0/sec, DNS names queued: 0
Average DNS queries performed: 0/sec, DNS names queued: 0
Average DNS queries performed: 0/sec, DNS names queued: 0
Average DNS queries performed: 0/sec, DNS names queued: 0
Average DNS queries performed: 0/sec, DNS names queued: 0
Average DNS queries performed: 0/sec, DNS names queued: 0
Average DNS queries performed: 0/sec, DNS names queued: 0
^X^C
OWASP Amass v3.3.1 https://github.com/OWASP/Amass
-----
150 names discovered - cert: 138, dns: 7, api: 5
-----
ASN: 16509 - AMAZON-02, US
99.86.0.0/16 4 Subdomain Name(s)
ASN: 8075 - MICROSOFT-CORP-MSN-A - MICROSOFT-CORP-MSN-A
23.96.0.0/14 1 Subdomain Name(s)
ASN: 213120 - PROLEXIC-IP-PROTECT, DE
95.100.0.0/15 1 Subdomain Name(s)
ASN: 33603 - DOMINOS-WRC-BLK01 - DOMINOS-WRC-BLK01
205.218.22.0/24 28 Subdomain Name(s)
209.211.200.0/24 44 Subdomain Name(s)
65.119.145.0/24 66 Subdomain Name(s)
63.234.241.0/24 2 Subdomain Name(s)
Sub 205.218.20.0/24 3 Subdomain Name(s)
205.218.21.0/24 1 Subdomain Name(s)
ASN: 27467 - RACKMY-STL-AS1 - RACKMY-STL-AS1
63.246.0.0/20 1 Subdomain Name(s)
ASN: 40066 - FAST-SEARCH-AND-TRANSFER-INC, US
23.96.0.0/13 1 Subdomain Name(s)
ASN: 36183 - AKAMAI-AS, US
184.84.0.0/14 4 Subdomain Name(s)
72.246.0.0/15 2 Subdomain Name(s)
23.192.0.0/11 2 Subdomain Name(s)
root@kali:~#
```

Figure 7

- ❖ The above Figure 7 shows subdomains and the IP addresses that I have obtained.

Nessus Tool

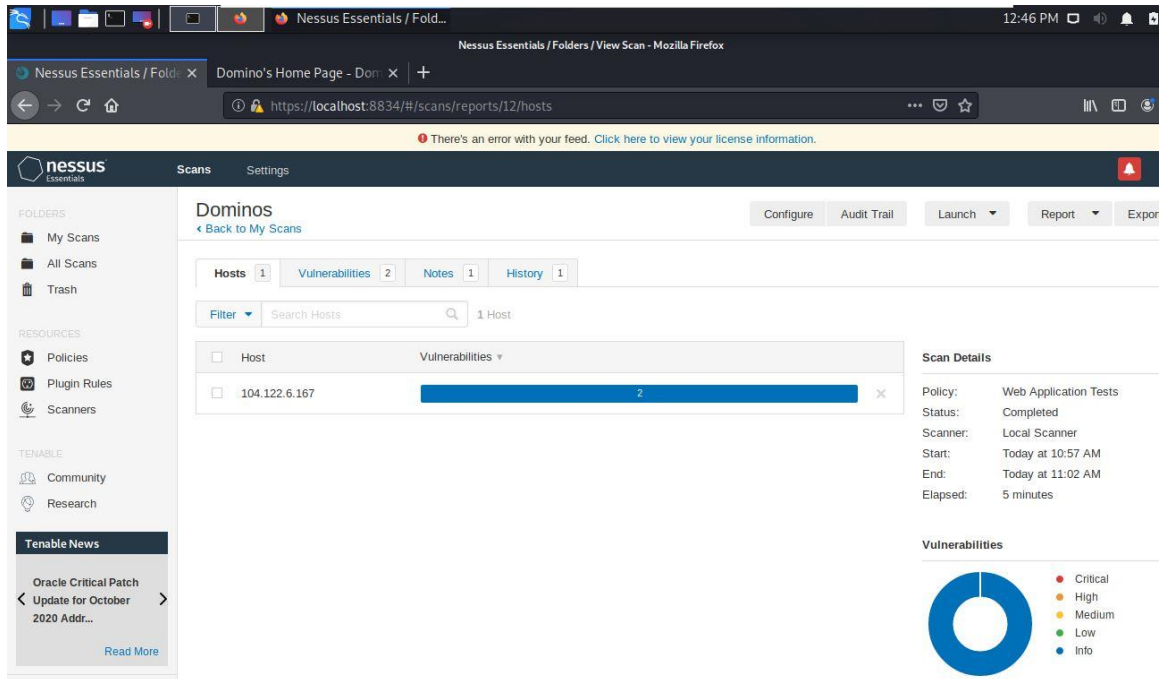


Figure 8

- ❖ According to the above diagram from the report I received from Nessus Tool the `www.dominos.com` domain has only info.
- ❖ Which shows that it is a domain that not vulnerable.

Netsparker Tool

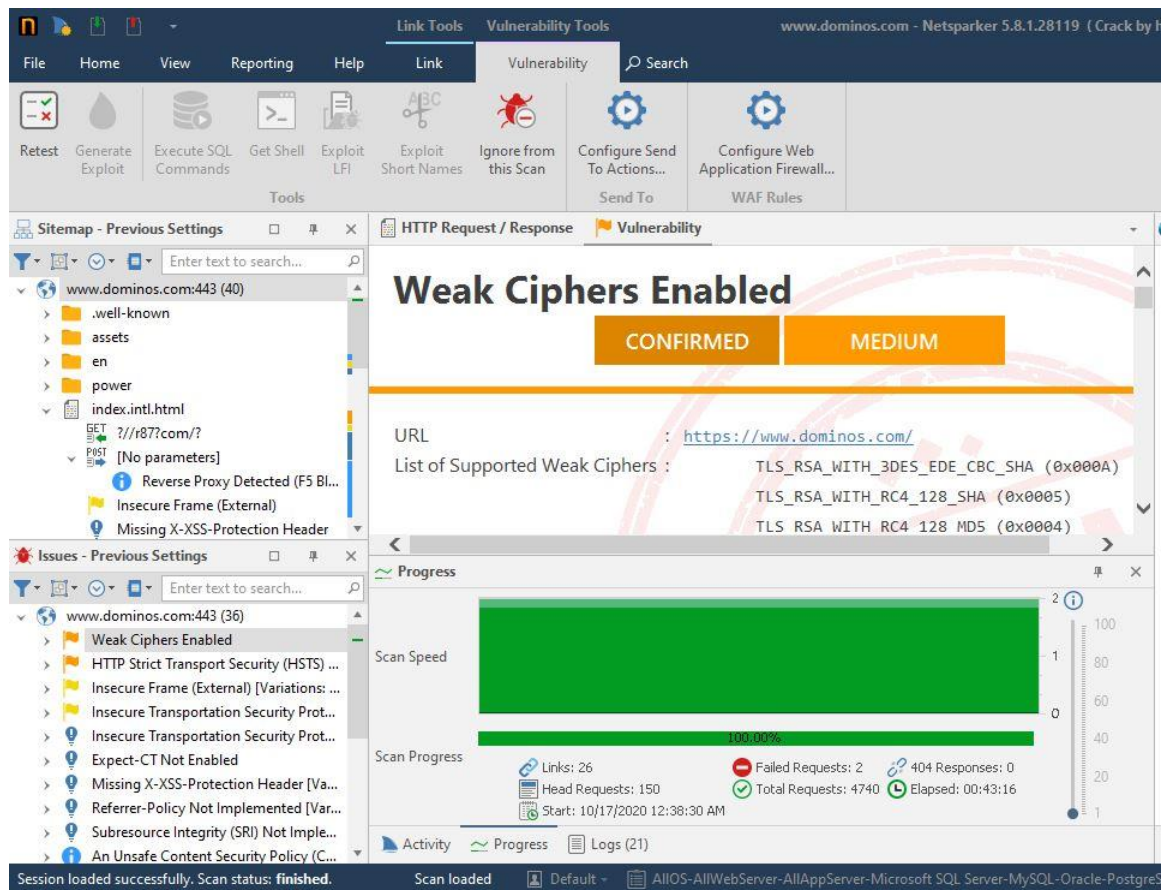
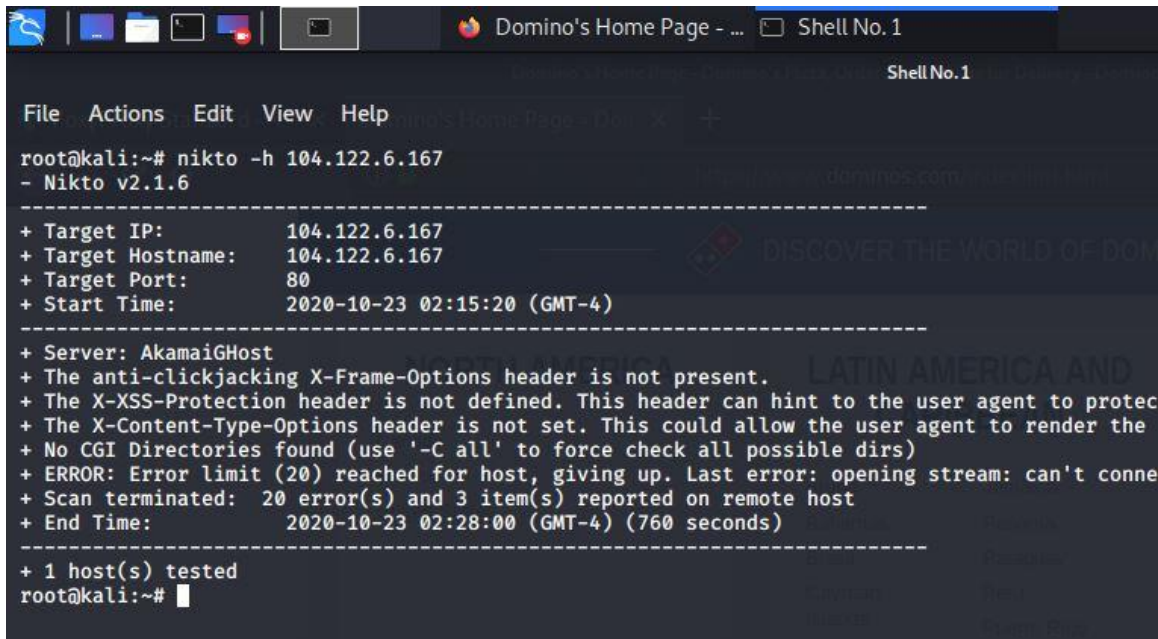


Figure 9

- ❖ The above shown tool in Figure 9 is used to scan vulnerabilities of my <https://www.dominos.com> domain.
- ❖ According to Figure 9 this tool provides more information than the Nessus tool shown in Figure 8.

Nikto Tool



```
root@kali:~# nikto -h 104.122.6.167
- Nikto v2.1.6
-----
+ Target IP: 104.122.6.167
+ Target Hostname: 104.122.6.167
+ Target Port: 80
+ Start Time: 2020-10-23 02:15:20 (GMT-4)
-----
+ Server: AkamaiGHost
+ 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
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time: 2020-10-23 02:28:00 (GMT-4) (760 seconds)
-----
+ 1 host(s) tested
root@kali:~#
```

Figure 10

nikto -h 104.122.6.167

- ❖ The tool shown in the Figure 10 is used to scan for vulnerabilities like clickjacking, XSS and outdated software vulnerabilities found in domains.
- ❖ Nikto is a free command-line vulnerability scanner software.
- ❖ In this tool I did not get any vulnerability or any informations

PwnXSS Tool

```
root@kali:~/PwnXSS# python3 pwnxss.py -u http://www.dominos.com
PWNXSS {v0.5 Final}
https://github.com/pwn0sec/PwnXSS
<<<<<< STARTING >>>>>>
[14:06:32] [INFO] Starting PwnXSS ...
*****
[14:06:32] [INFO] Checking connection to: http://www.dominos.com
[14:06:33] [INFO] Connection established 200
[14:06:33] [WARNING] Target have form with POST method: http://www.dominos.com/power/opt-in-and-opt-out
[14:06:33] [INFO] Collecting form input key....
[14:06:33] [INFO] Form key name: email value: <script>prompt(document.cookie)</script>
[14:06:33] [INFO] Sending payload (POST) method...
[14:06:33] [INFO] Parameter page using (POST) payloads but not 100% yet ...
root@kali:~/PwnXSS#
```

Figure 11

```
python pwnxss -u https://www.dominos.com
```

- ❖ The tool shown in Figure 11 is used to scan XSS vulnerabilities.
- ❖ This tool was also cloned using GitHub.
- ❖ Link to download the tool: “<https://github.com/pwn0sec/PwnXSS>”
- ❖ This tool did not get connected with my domain. Hence, was unsuccessful.

Burp Suite

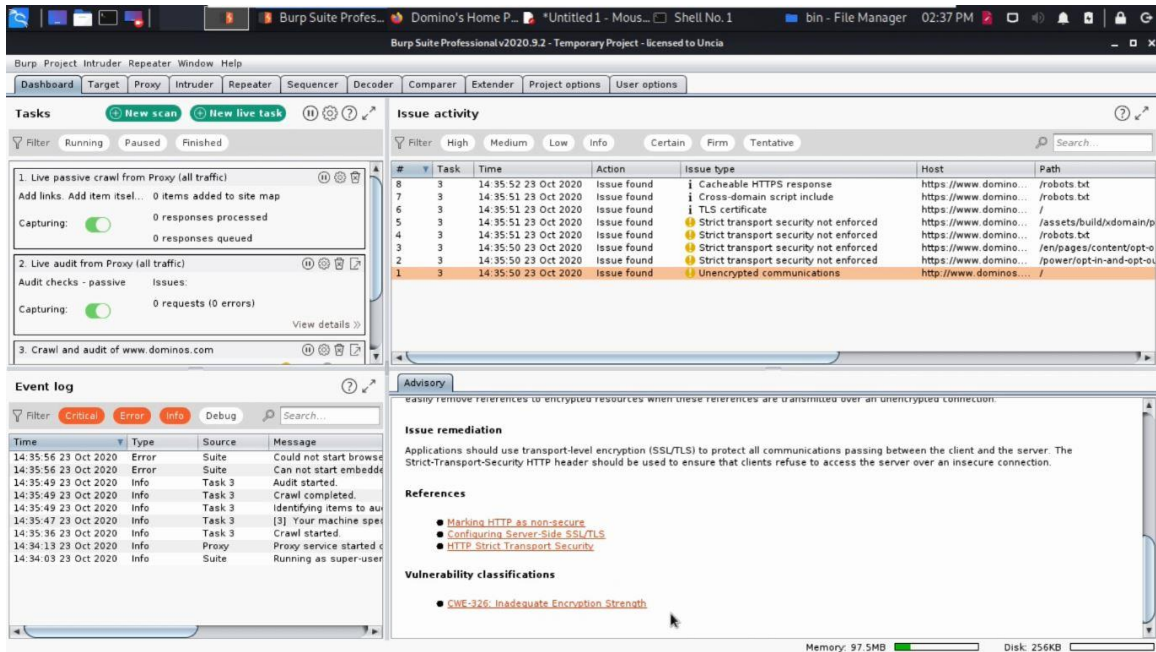


Figure 12

- ❖ The tool shown in Figure 12 was used to the full web scan.
- ❖ By conducting this scan also, I did not reactive any high or critical vulnerabilities, I only get medium and info vulnerabilities. hence, this was not successful.

Conclusion

- ❖ The method I choose to conduct the web audit was recon approach which allows to gather information about the domain. Hence in order to conduct that type of web audit many tools are used. I used some tools as well like nmap, amas, nessus, netparker, nikto, pownxss and burpSuit. All these tools are well known in the industry and have proven to provide accurate results. Each of these tools had their own special functionality. For instance, Nessus is a tool that enables to identify the vulnerabilities of in the domain and categorizes the vulnerability according to the level of security. For instance; low, medium, high and critical levels from which high and critical mean that the domain can be hacked and low and medium means that the domain can be sparsely exploited. By doing this scan for the www.dominos.com domain I received only medium and low vulnerabilities which was medium in rate. Hence, it indicated that the domain can hardly be exploited. Even after using many other tools like Nikto and Pownxss I was not able to scan the dominos.com domain which indicates that it is a highly secured domain.

References

- ❖ <https://www.bugcrowd.com/blog/>
- ❖ <https://www.youtube.com/watch?v=VFCLw1tAflU>
- ❖ <https://www.youtube.com/watch?v=YOx-p4BFTx8>
- ❖ <https://www.security-audit.com/website-security-auditing-and-testing/>
- ❖ <https://github.com/bugcrowd/vulnerability-rating-taxonomy>
- ❖ <https://github.com/ngalongc/bug-bounty-reference/>