



Sri Lanka Institute of Information Technology

## Web Audit

IE2062 – Web Security

Submitted by:

Student Registration Number	Student Name
IT19034614	Tharuka R.P.A.

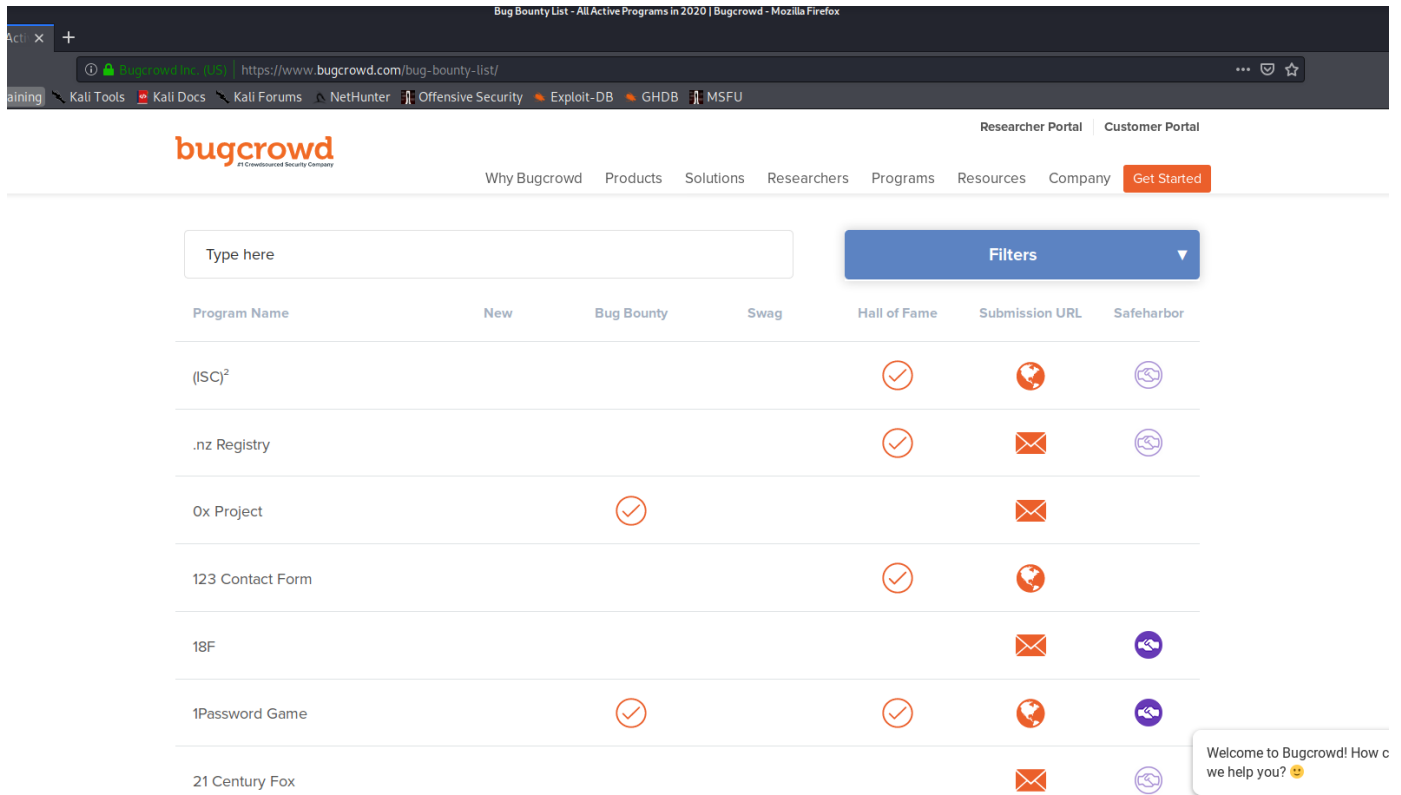
# Introduction

- Website audit

Is a good starting point for anyone who's already having a website and ready to improve its search engine visibility. The website audit is a systematic review of all factors that influence the visibility of the website in search engines. This basic approach offers a detailed overview of any website, all traffic, and individual pages. The audit of the website is only carried out for marketing purposes. The purpose is to find vulnerabilities in web-based campaigns. A full website audit exposes disparities that could lead to Google penalties. Penalties impact search engine ranking on Google's ranking page. The audit also determines how vulnerable the site is to violations of security.

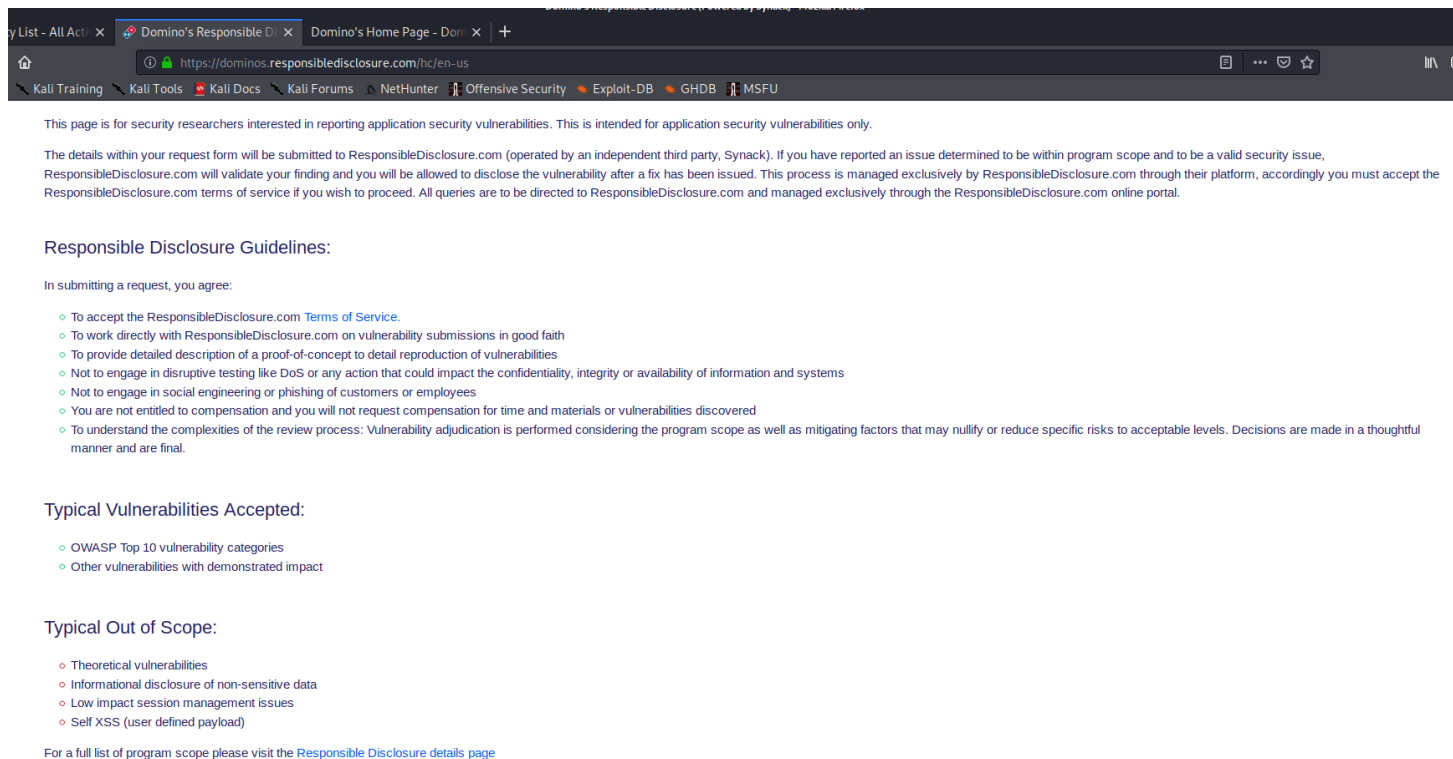
## Domain selection

- I used “ <https://www.bugcrowd.com> ” website to select the domain for web audit.
- There are many websites and web applications in this bug bounty list as in the figure 01.



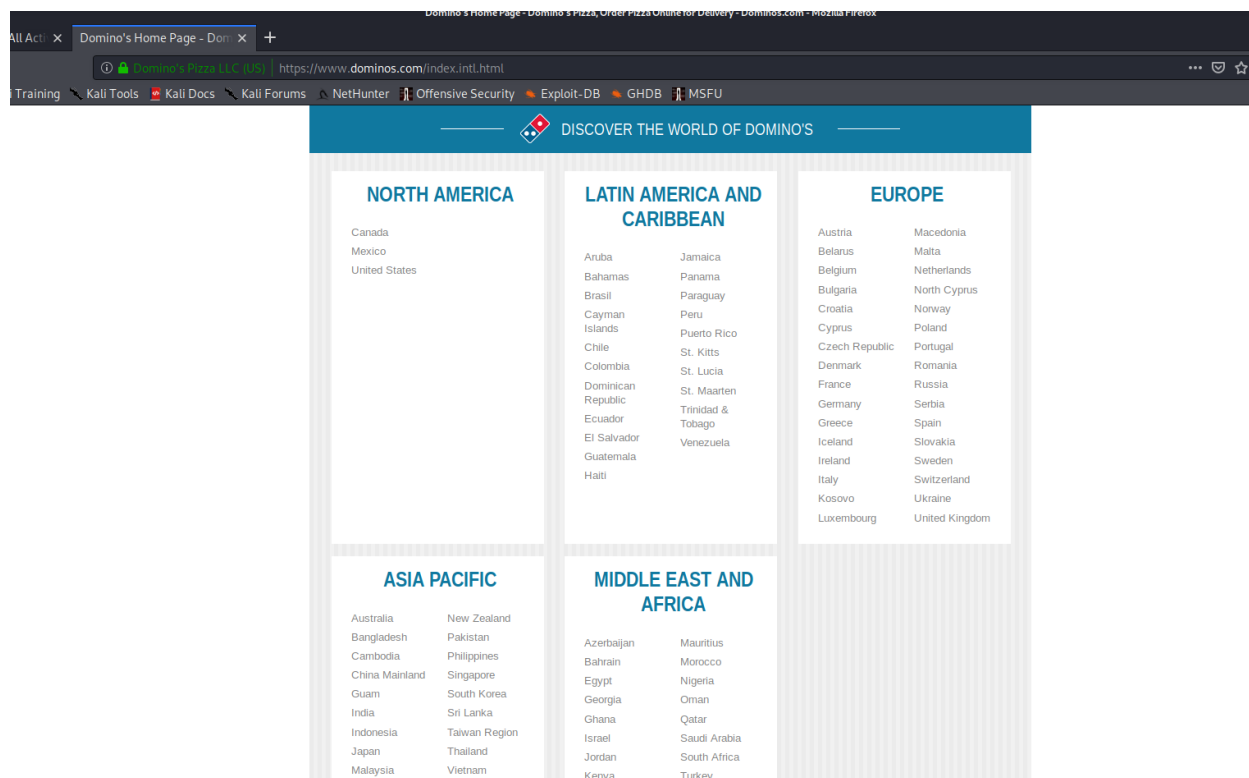
-Figure 01-

- I selected “ **dominos.com** ” from above list as my web audit domain.
- Figure 02 shows do's and don'ts for the selected website.



-Figure 02-

- Interface of my selected domain as shown in the figure 03.



-Figure 03-

## Finding the subdomains

- After selecting the web domain, we have to find the subdomains of the selected domain.
- I used **sublist3r** tool to find the subdomains.
- By using following command, we can get the subdomains.

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

- After running above command, I got the result as shown in the figure 04



```
Shell No. 1
File Actions Edit View Help
root@kali:~/Desktop/Sublist3r# ./sublist3r.py -d dominos.com

SUBLIST3R
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for dominos.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSDumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Total Unique Subdomains Found: 633
www.dominos.com
www.4.dominos.com
Autodiscover.dominos.com
Filetransfer.dominos.com
Hybrid.dominos.com
Hybrid1.dominos.com
Hybrid2.dominos.com
Mail.dominos.com
a2schools.dominos.com
abovestore.dominos.com
abovestore-dev1.dominos.com
abovestore-preprod.dominos.com
abovestore-prod1.dominos.com
abovestore-prod2.dominos.com
abovestore-qa1.dominos.com
abovestore-va-prod1.dominos.com
abovestore-va-prod2.dominos.com
abrfid.dominos.com
```

-Figure 04-

## **Web Recon**

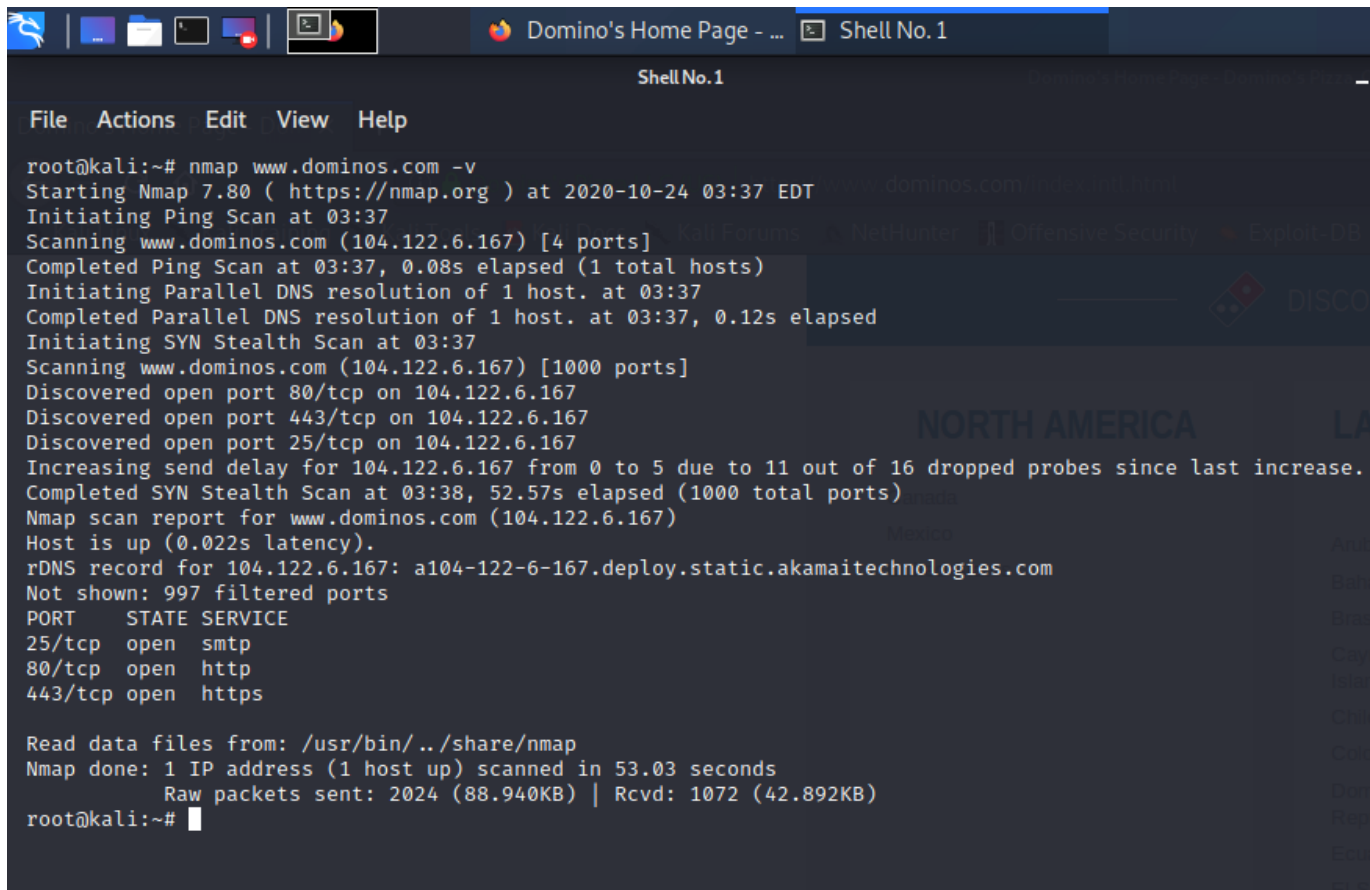
This method lets you explore technologies used on the server and client-side of a target Web application. It is also possible to search many virtual hosts on one IP. Recon is the first step of a penetration test in which the pentester can find the details about the target website as much as possible.

- I am going to use following tools to do web recon
  - Sublist3r
  - Nmap
  - Nessus
  - Netsparker
  - Nikto
  - Amass
  - Burp
- I run sublist3r tool in my previous session an get the results using it.
- Now I am going to use other tools.

## Nmap Tool

- I run **nmap** tool by using below command

**nmap www.dominos.com**



```
root@kali:~# nmap www.dominos.com -v
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-24 03:37 EDT
Initiating Ping Scan at 03:37
Scanning www.dominos.com (104.122.6.167) [4 ports]
Completed Ping Scan at 03:37, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:37
Completed Parallel DNS resolution of 1 host. at 03:37, 0.12s elapsed
Initiating SYN Stealth Scan at 03:37
Scanning www.dominos.com (104.122.6.167) [1000 ports]
Discovered open port 80/tcp on 104.122.6.167
Discovered open port 443/tcp on 104.122.6.167
Discovered open port 25/tcp on 104.122.6.167
Increasing send delay for 104.122.6.167 from 0 to 5 due to 11 out of 16 dropped probes since last increase.
Completed SYN Stealth Scan at 03:38, 52.57s elapsed (1000 total ports)
Nmap scan report for www.dominos.com (104.122.6.167)
Host is up (0.022s 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

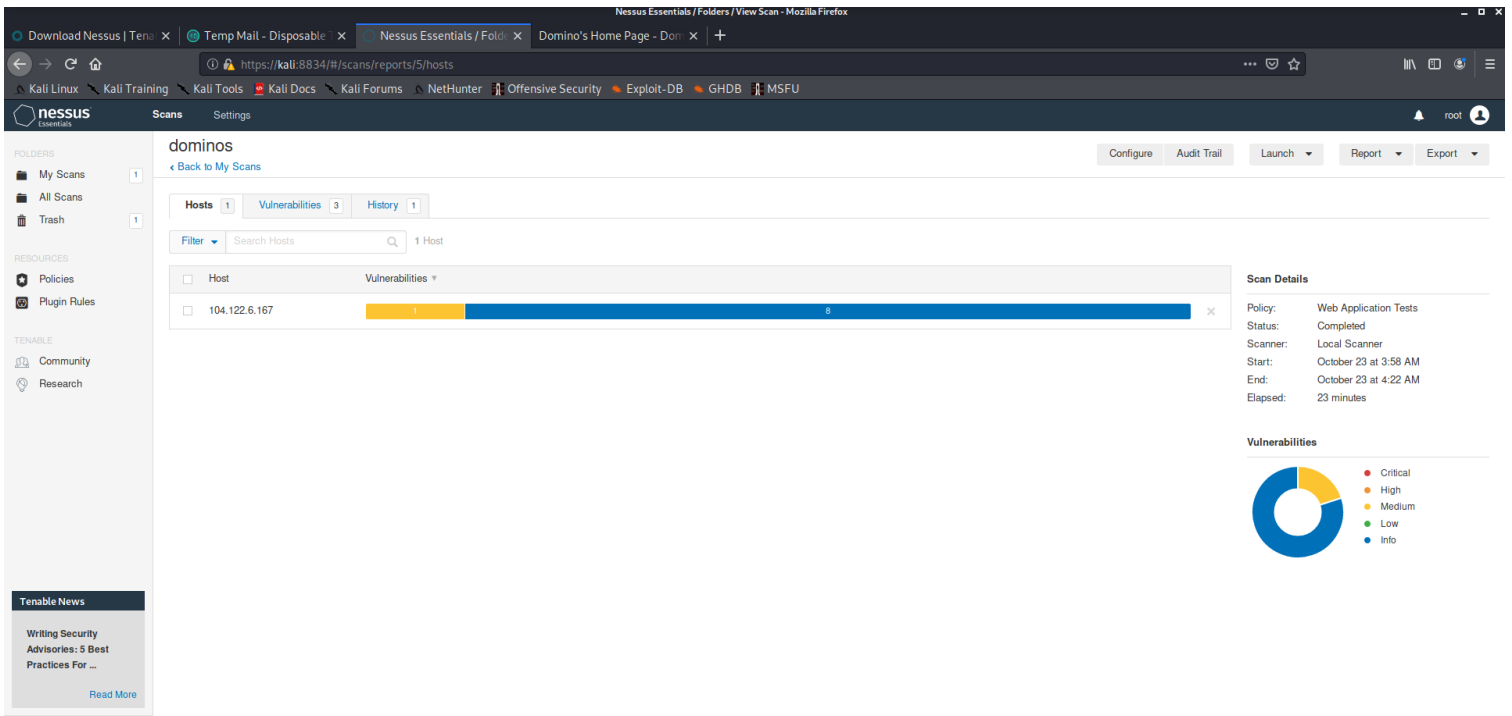
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 53.03 seconds
Raw packets sent: 2024 (88.940KB) | Rcvd: 1072 (42.892KB)
root@kali:~#
```

-Figure 05-

- After running above command, I got the result as shown in the figure 05
- Then I found ip address of my domain and three open ports.

# Nessus Tool

- I got the results after running the nessus scan as figure 06 shows.



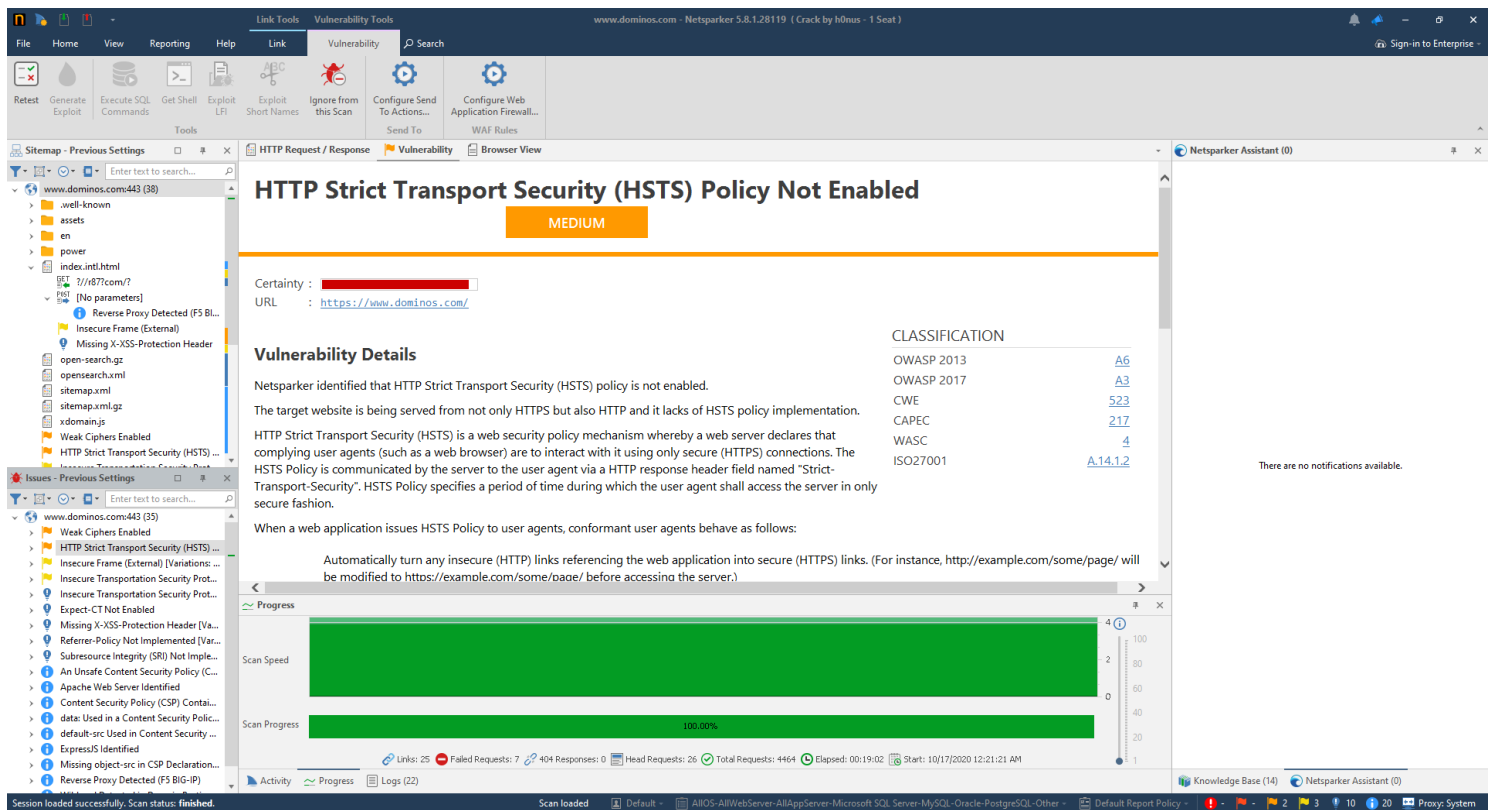
-Figure 06-

- But after nessus scan I can only find medium vulnerability
- There are not any critical vulnerabilities in the nessus scan.



## Netsparker Tool

- **Netsparker** is an automated web application security scanner that enables you to scan websites, web applications and web services and identify security flaws. It can scan all types of web web applications, regardless of the platform or the language with which they are built.
- I run this tool as a windows application and get the results.



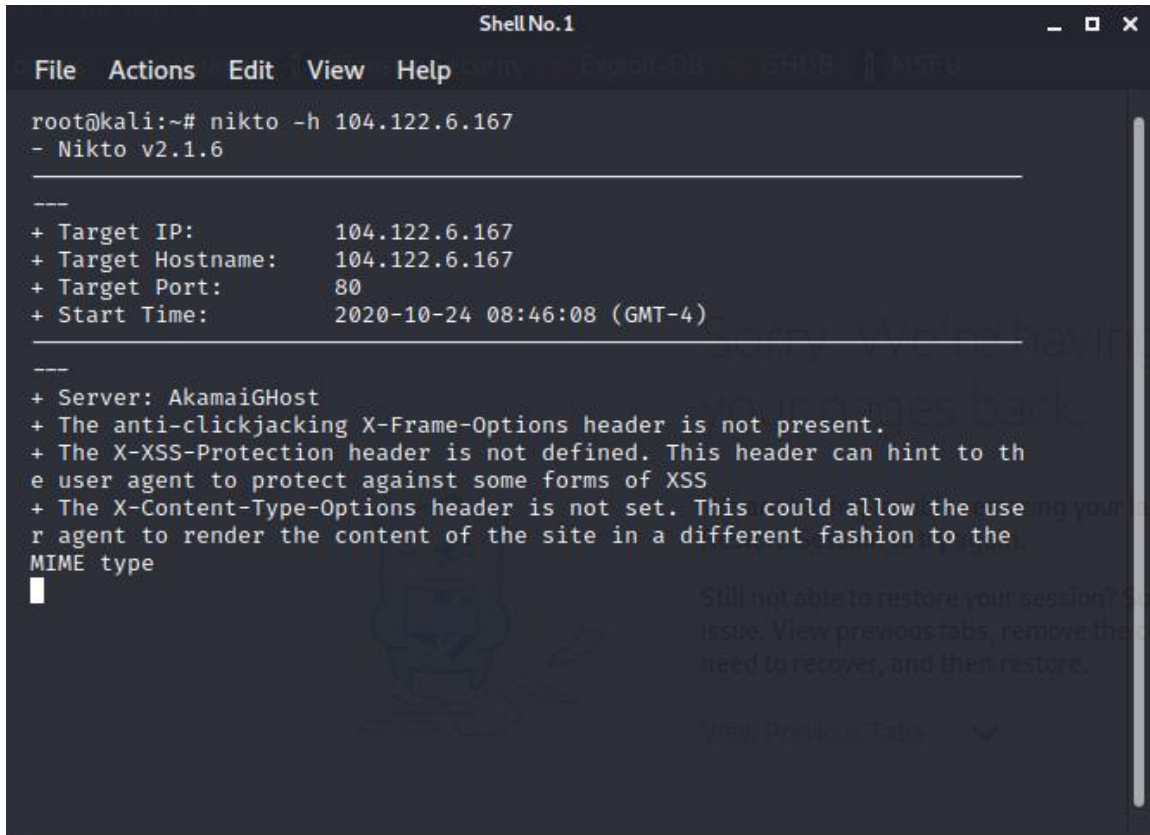
-Figure 07-

- After I run netsparker , I got the result as shown in the figure 07.
- It includes many information than the nessus scanning results.
- In this scan include only medium and low vulnerabilities.
- There are not any critical vulnerabilities found on the netsparker scan.

## Nikto Tool

- Using below command, we can run nikto scanner by using our target domain's ip address.

```
nikto -h 104.122.6.167
```



```
Shell No.1
File Actions Edit View Help
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:         2020-10-24 08:46:08 (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 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
█
```

-Figure 08-

- After running above command, I got the result as shown in the figure 08.
- But I did not find any vulnerabilities or meaningful information after this nikto scanning.

# Amass Tool

- First download the amass tool using following link.

<https://github.com/OWASP/Amass>

- After that I run the amass tool using below command.

**amass enum -d dominos.com**

```

Shell No. 1
File Actions Edit View Help

root@kali:~# amass

      .+++!.:
    +WdqdqddqB          :         .+++..
        Bm#+       .om##.     ,dqdoBW.o dqdo   :dm#BWo         +Wdqdqddq#.    oWdqdqW#+
+dB           dB          #dB +dWdbBdb+       :dB.   +dB        +d:   .:OW+.   .dB +++B#B
8d            db          Bd0   8dB WW         .dB.   Wd+.   .dW.        .dB
WW            Bdo         Bd+: om+   od+   #d.     8do    +Wd#+.     +WdB:
#d            :dW         Bd+   Bd+   dB         :do     doo     oWdqw+     oWdB
od+           ddB        Bd+   Bd+   #d         :dB.     .WdW     .+#dB       odW.
WW            +dWdB.     Bd+   :B      od+   #d         :dWBdB        Bd:   ..        :do
:dW:          od#   +Wo  Bd+       :W: +dWSo++odW.     dB#o+BdW.   #d:     od+
:WdqdWWWdqdB      +       :BWdqdqb      BW   .o#dBdB.   :WdWWWdqb      +oooo.

                                                     v3.7.3
                        OWASP Amass Project - @owaspamass
                    In-depth Attack Surface Mapping and Asset Discovery


Usage: amass intel|enum|viz|track|db|dns [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
    amass dns   - Resolve DNS names at high performance


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

The Amass tutorial can be found here:
https://github.com/OWASP/Amass/blob/master/doc/tutorial.md

root@kali:~# amass enum -d dominos.com
Querying UKGovArchive for dominos.com subdomains
Querying HackerOne for dominos.com subdomains
Querying GoogleCT for dominos.com subdomains
Querying Mnemonic for dominos.com subdomains
Querying Yahoo for dominos.com subdomains

```

-Figure 09-

```
Shell No.1
File Actions Edit View Help
wam.dev1.dominos.com
authproxy-preprod.dominos.com
Average DNS queries performed: 753/sec, Average retries required: 12.35%
tracker-dev.dominos.com
api-dev.dominos.com
nolo-us-dev1.dominos.com
www-dev1.dominos.com
api-dev1.dominos.com
dominos.com
r245.confirmation.dominos.com
r26.confirmation.dominos.com
r247.confirmation.dominos.com
r28.confirmation.dominos.com
r93.your.rewards.dominos.com
r81.your.offers.dominos.com
r82.your.offers.dominos.com
r246.confirmation.dominos.com
r92.your.rewards.dominos.com
r94.your.rewards.dominos.com
r79.your.offers.dominos.com
r78.your.offers.dominos.com
r27.confirmation.dominos.com
r96.your.offers.dominos.com
r105.your.offers.dominos.com
r98.your.offers.dominos.com
r75.your.offers.dominos.com
r89.your.offers.dominos.com
r104.your.offers.dominos.com
r90.your.offers.dominos.com
r80.your.offers.dominos.com
r84.your.offers.dominos.com
r91.your.offers.dominos.com
r97.your.offers.dominos.com
r87.your.offers.dominos.com
r100.your.offers.dominos.com
r85.your.offers.dominos.com
r86.your.offers.dominos.com
r74.your.offers.dominos.com
r103.your.offers.dominos.com
r77.your.offers.dominos.com
r101.your.offers.dominos.com
r83.your.offers.dominos.com
r99.your.offers.dominos.com
r76.your.offers.dominos.com
r95.your.offers.dominos.com
r88.your.offers.dominos.com
r102.your.offers.dominos.com
confirmation.dominos.com
your.rewards.dominos.com
your.offers.dominos.com
Average DNS queries performed: 1803/sec, Average retries required: 36.55%
www-prod4.dominos.com
www-prod3.dominos.com
```

-Figure 10-

```
Shell No.1
File Actions Edit View Help

54.164.0.0/15      2 Subdomain Name(s)
3.208.0.0/12      1 Subdomain Name(s)
18.208.0.0/13      1 Subdomain Name(s)
ASN: 14340 - SALESFORCE - Salesforce.com, Inc.
13.108.0.0/15      1 Subdomain Name(s)
101.53.160.0/19    1 Subdomain Name(s)
ASN: 3215 - AS3215
2.0.0.0/12         1 Subdomain Name(s)
ASN: 35914 - ARMOR-DEFENSE, US
162.218.136.0/22   1 Subdomain Name(s)
199.180.184.0/22   1 Subdomain Name(s)
ASN: 20940 - AKAMAI-ASN1, EU
184.30.208.0/20     1 Subdomain Name(s)
2600:1400::/24      2 Subdomain Name(s)
72.247.178.0/23     14 Subdomain Name(s)
184.24.0.0/19       3 Subdomain Name(s)
184.86.103.0/24     12 Subdomain Name(s)
96.17.150.0/24      14 Subdomain Name(s)
104.64.0.0/10       1 Subdomain Name(s)
ASN: 16509 - AMAZON-02
34.208.0.0/12       6 Subdomain Name(s)
44.224.0.0/11       4 Subdomain Name(s)
50.112.192.0/18     2 Subdomain Name(s)
13.35.176.0/21      4 Subdomain Name(s)
13.57.0.0/16        1 Subdomain Name(s)
13.227.168.0/21     8 Subdomain Name(s)
35.160.0.0/13       4 Subdomain Name(s)
35.181.0.0/16       2 Subdomain Name(s)
13.33.93.0/24       12 Subdomain Name(s)
13.225.25.0/24      4 Subdomain Name(s)
ASN: 30121 - 24-7-AS-IDC-001 - 24/7 Customer, Inc.
66.170.112.0/20     2 Subdomain Name(s)
ASN: 3561 - CENTURYLINK-LEGACY-SAVVIS, US
205.218.0.0/18      58 Subdomain Name(s)
205.139.64.0/20     13 Subdomain Name(s)
205.139.160.0/20    2 Subdomain Name(s)
ASN: 33603 - DOMINOS-WRC-BLK01 - DOMINOS PIZZA, LLC
209.211.200.0/24    97 Subdomain Name(s)
65.119.145.0/24     133 Subdomain Name(s)
63.234.241.0/24     8 Subdomain Name(s)
ASN: 7332 - LIGHTBOUND-AS - IQuest Internet
206.53.224.0/19     1 Subdomain Name(s)
ASN: 8075 - MICROSOFT-CORP-MSN-AS-BLOCK, US
23.96.0.0/14        2 Subdomain Name(s)
52.112.0.0/14       2 Subdomain Name(s)
40.96.0.0/13        3 Subdomain Name(s)
13.64.0.0/11        1 Subdomain Name(s)
ASN: 12154 - INFOUSA - InfoUSA
206.165.240.0/21    5 Subdomain Name(s)

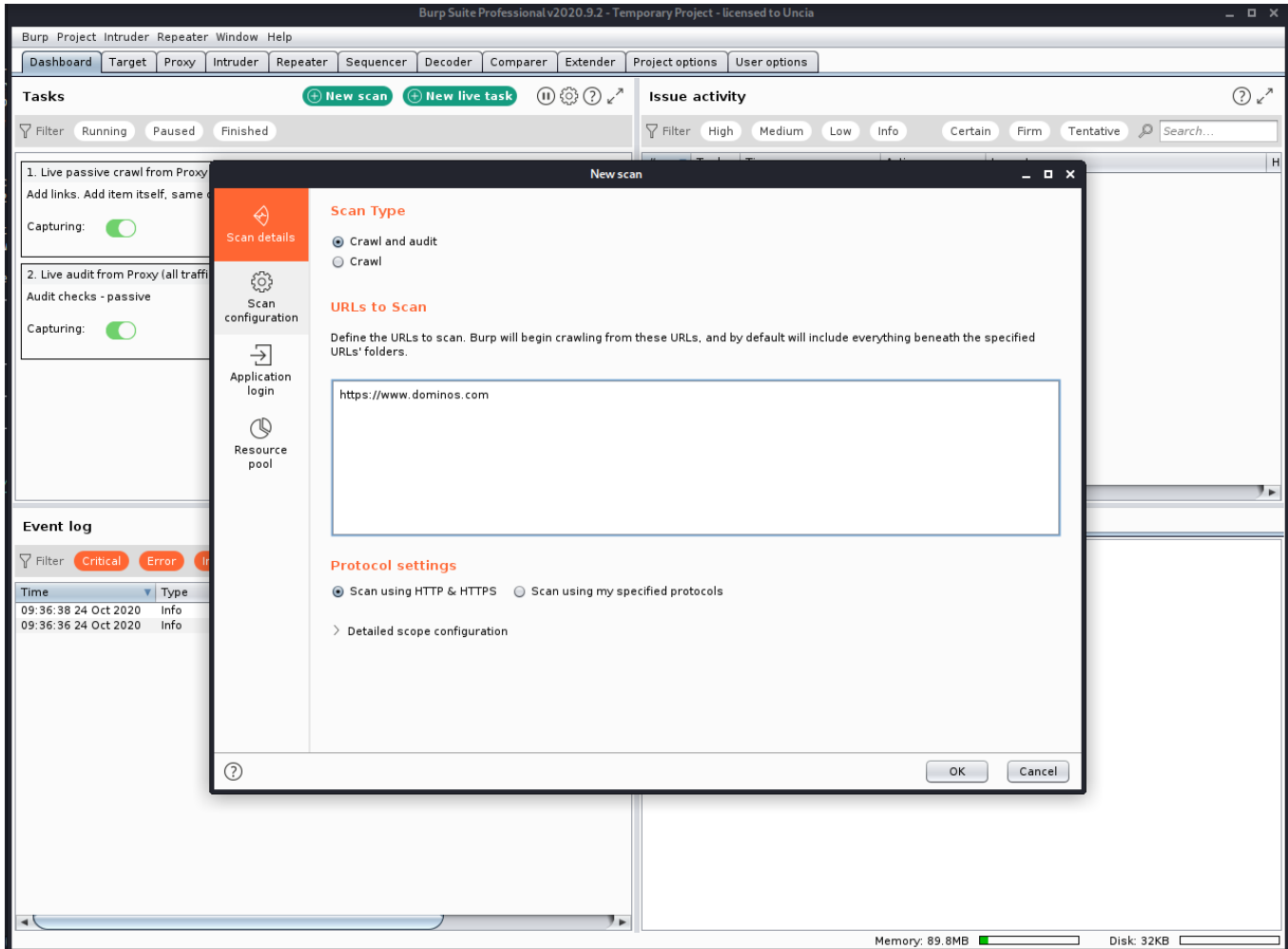
The enumeration has finished
Discoveries are being migrated into the Cayley Graph database
root@kali:~#
```

-Figure 11-

- After running above command, I got the result as shown in the figure 09, 10 and 11.

## Burp Suite Tool

- I run burp suite scanner using my domain's URL as shown in the figure 12.



-Figure 12-

- After running the scanning part, I got the result as shown in the figure 13.

The screenshot displays the Burp Suite interface with the following components:

- Tasks Panel:**
  - 1. Live passive crawl from Proxy (all traffic):** Capturing is enabled. 0 items added to site map, 0 responses processed, 0 responses queued.
  - 2. Live audit from Proxy (all traffic):** Audit checks - passive. Capturing is enabled. 0 requests (0 errors). [View details >](#)
  - 3. Crawl and audit of www.dominos.com:** Default configuration. Capturing is enabled. 65 requests (0 errors), 1 locations crawled. [View details >](#)
- Issue activity Panel:**

#	Task	Time	Action	Issue type	Host	Path
8	3	09:37:49 24 Oct 2020	Issue found	i TLS certificate	https://www.dominio...	/
7	3	09:37:49 24 Oct 2020	Issue found	i Cacheable HTTPS response	https://www.dominio...	/robots.txt
6	3	09:37:49 24 Oct 2020	Issue found	i Cross-domain script include	https://www.dominio...	/robots.txt
5	3	09:37:49 24 Oct 2020	Issue found	o Strict transport security not enforced	https://www.dominio...	/assets/build/domain/proxy.html
4	3	09:37:49 24 Oct 2020	Issue found	o Strict transport security not enforced	https://www.dominio...	/robots.txt
3	3	09:37:48 24 Oct 2020	Issue found	o Strict transport security not enforced	https://www.dominio...	/en/pages/content/opt-out/opt-out
2	3	09:37:48 24 Oct 2020	Issue found	o Strict transport security not enforced	https://www.dominio...	/power/opt-in-and-opt-out
1	3	09:37:48 24 Oct 2020	Issue found	o Unencrypted communications	http://www.dominos....	/
- Event log Panel:**

Time	Type	Source	Message
09:37:50 24 Oct 2020	Error	Suite	Could not start browser. Use 'Embedded Browser Health Check' for more details.
09:37:50 24 Oct 2020	Error	Suite	Can not start embedded browser sandbox because you are running as root. Either switch to run...
09:37:48 24 Oct 2020	Info	Task 3	Audit started.
09:37:48 24 Oct 2020	Info	Task 3	Crawl completed.
09:37:48 24 Oct 2020	Info	Task 3	Identifying items to audit.
09:37:46 24 Oct 2020	Info	Task 3	[3] Your machine specification does not appear to meet the recommended requirements for cr...
09:37:38 24 Oct 2020	Info	Task 3	Crawl started.
09:36:36 24 Oct 2020	Info	Proxy	Proxy service started on 127.0.0.1:8080
09:36:36 24 Oct 2020	Info	Suite	Running as super-user, embedded browser sandbox is not supported.

System status at the bottom: Memory: 93.9MB, Disk: 256KB.

-Figure 13-

## Conclusion

- For my web audit, I have used several tools Which include the following:
  - Sublist3r
  - Nmap
  - Nessus
  - Netsparker
  - Nikto
  - Amass
  - Burpsuit
- However, I have had no high, critical, or important vulnerability in the **dominos.com** domain from the above scans. In my opinion, therefore, **dominos.com** is a much safer web application.

## References

- <https://www.bugcrowd.com/bug-bounty-list>
- <https://github.com/OWASP/Amass>
- <https://www.youtube.com/watch?v=8PaVBe0cbIU>
- <https://www.youtube.com/watch?v=VP9eQhUASYQ>
- <https://tools.kali.org/information-gathering/nikto>