Sri Lanka Institute of Information Technology

Web Audit

IE2062 – Web Security

Submitted by:

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

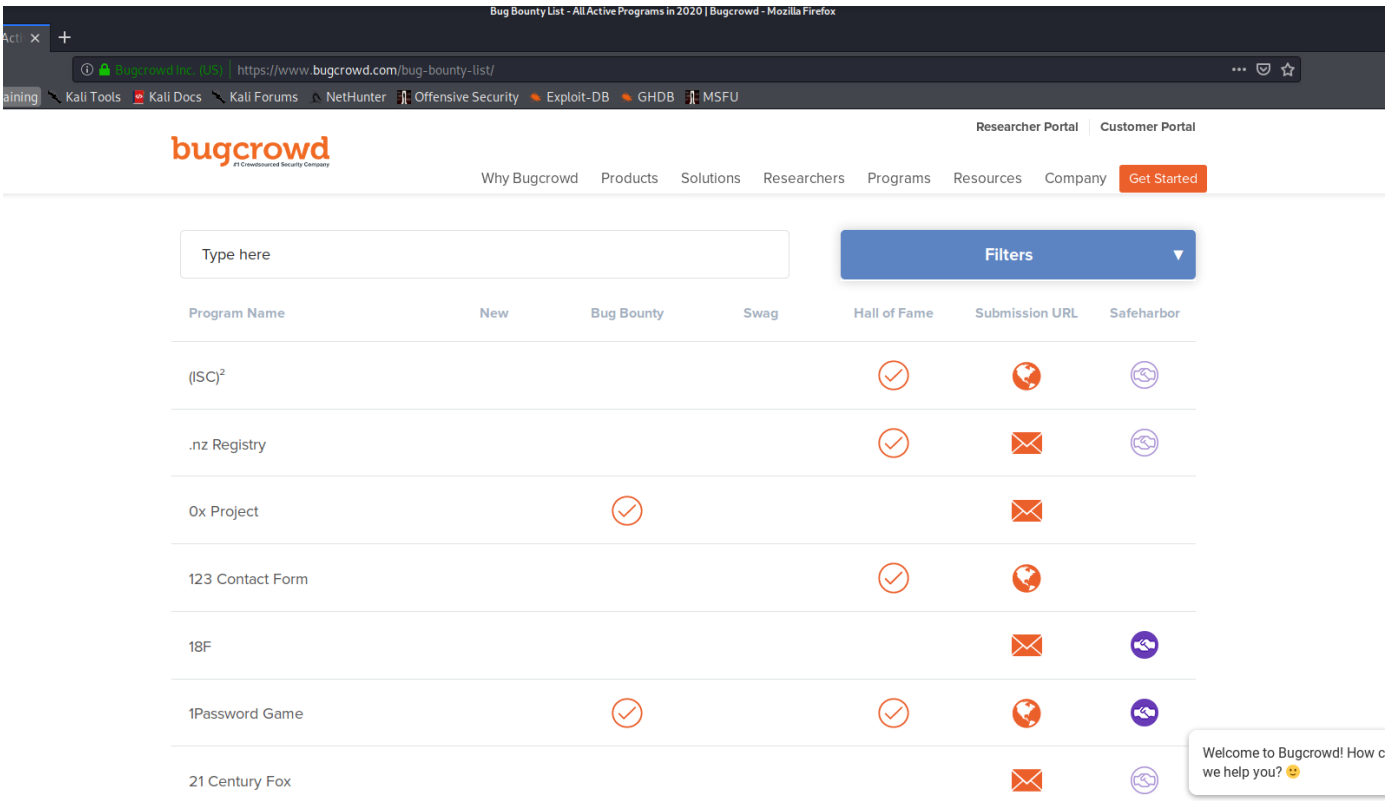
Introduction

- 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.

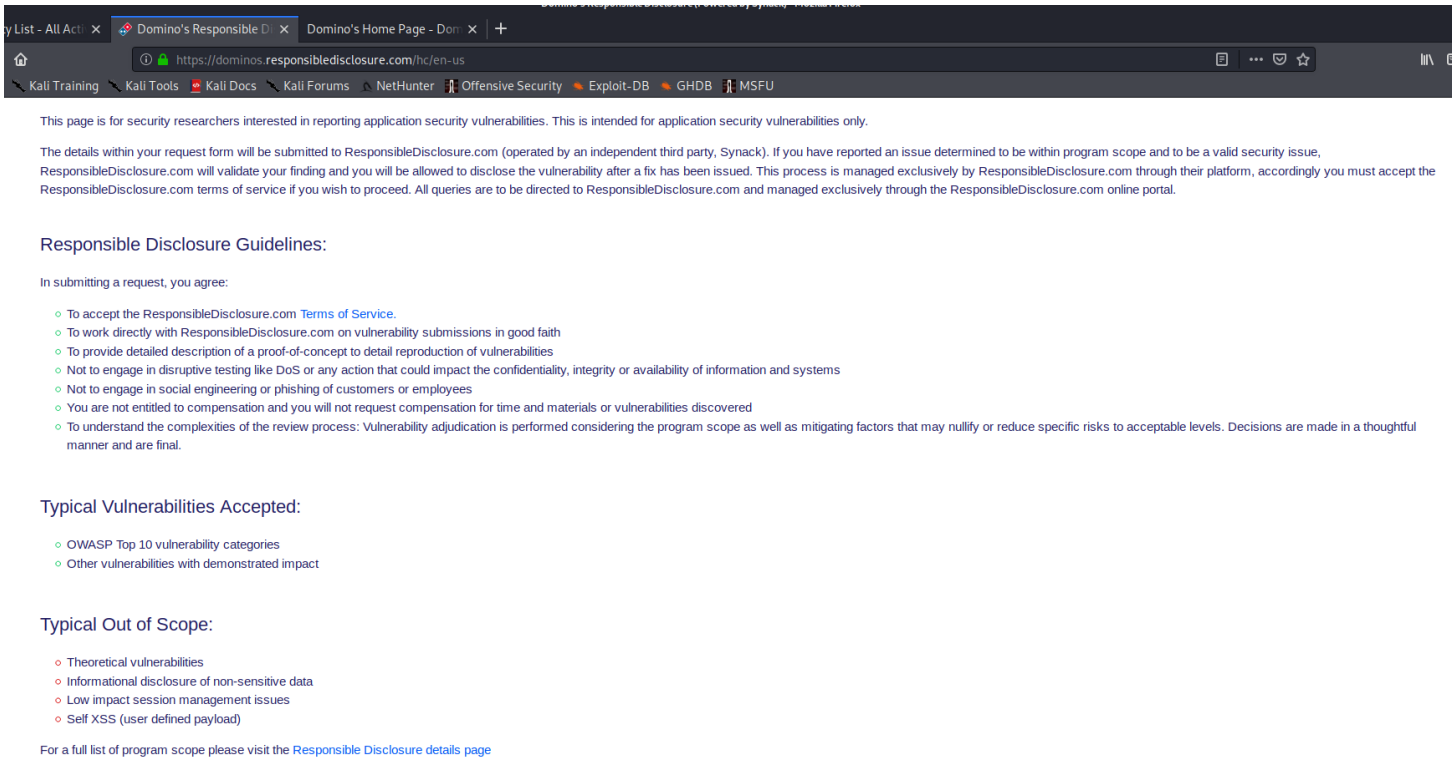
Domain selection

- 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.



This page is for security researchers interested in reporting application security vulnerabilities. This is intended for application security vulnerabilities only.

The details within your request form will be submitted to ResponsibleDisclosure.com (operated by an independent third party, Synack). If you have reported an issue determined to be within program scope and to be a valid security issue, ResponsibleDisclosure.com will validate your finding and you will be allowed to disclose the vulnerability after a fix has been issued. This process is managed exclusively by ResponsibleDisclosure.com through their platform, accordingly you must accept the ResponsibleDisclosure.com terms of service if you wish to proceed. All queries are to be directed to ResponsibleDisclosure.com and managed exclusively through the ResponsibleDisclosure.com online portal.

Responsible Disclosure Guidelines:

In submitting a request, you agree:

- To accept the ResponsibleDisclosure.com Terms of Service.
- To work directly with ResponsibleDisclosure.com on vulnerability submissions in good faith
- To provide detailed description of a proof-of-concept to detail reproduction of vulnerabilities
- Not to engage in disruptive testing like DoS or any action that could impact the confidentiality, integrity or availability of information and systems
- Not to engage in social engineering or phishing of customers or employees
- You are not entitled to compensation and you will not request compensation for time and materials or vulnerabilities discovered
- To understand the complexities of the review process: Vulnerability adjudication is performed considering the program scope as well as mitigating factors that may nullify or reduce specific risks to acceptable levels. Decisions are made in a thoughtful manner and are final.

Typical Vulnerabilities Accepted:

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

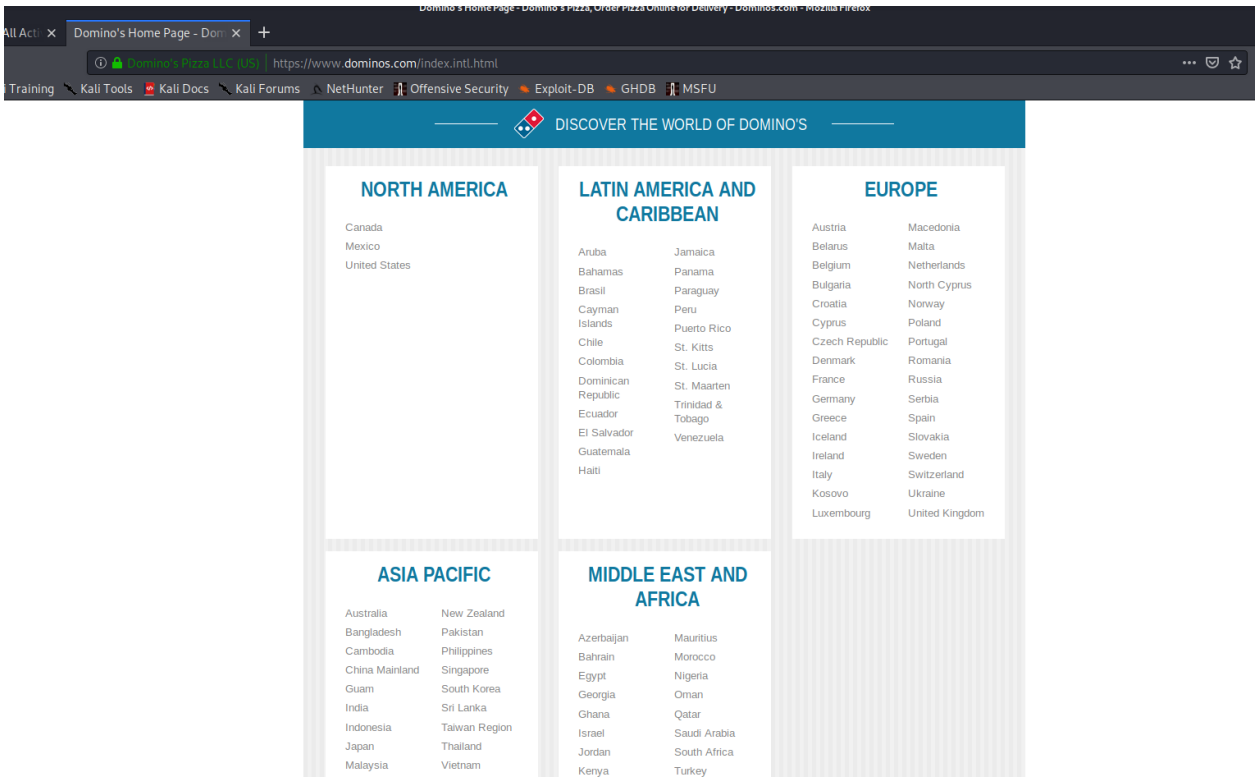
Typical Out of Scope:

- 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 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

-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

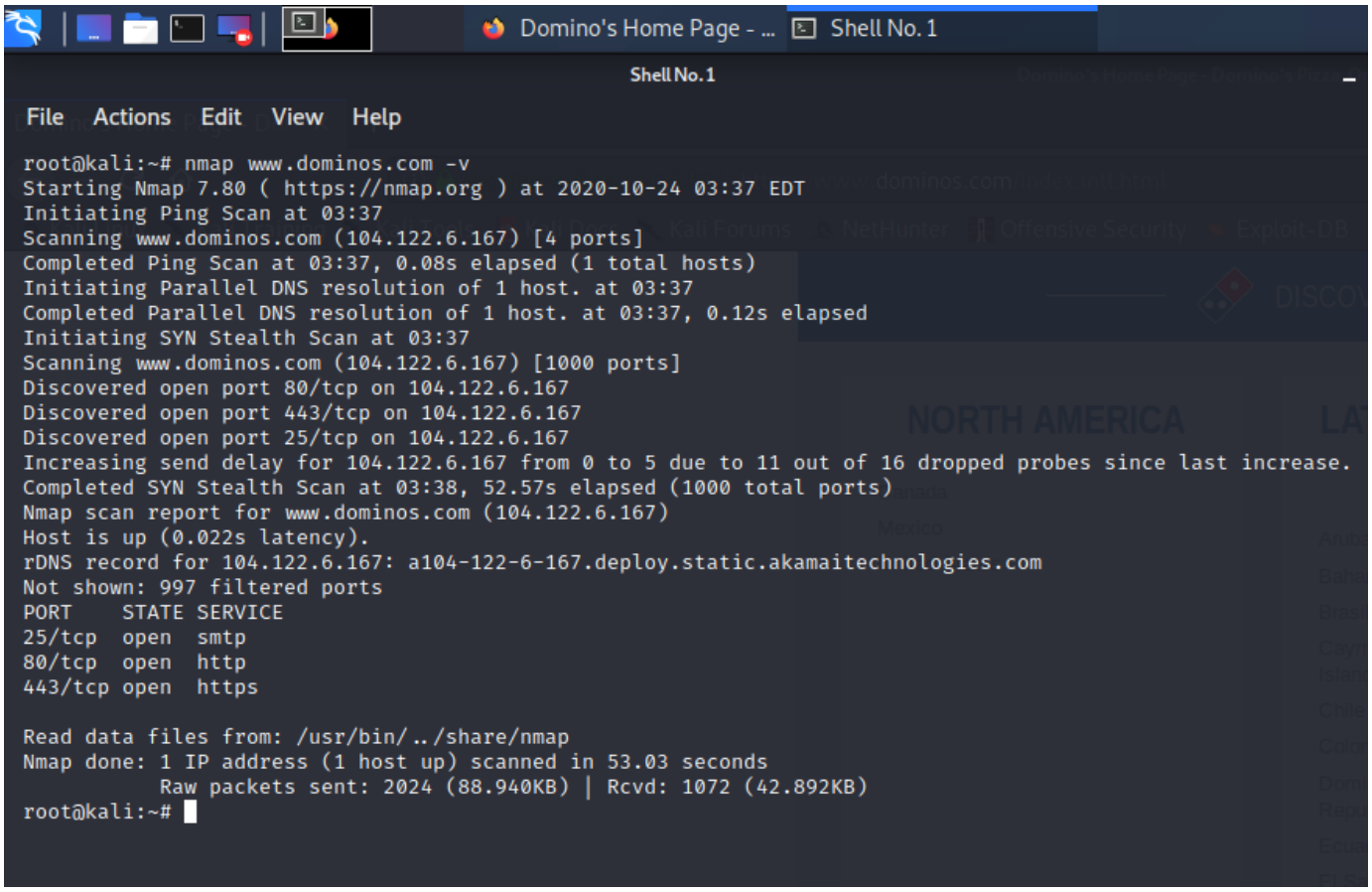
    - Sublist3r
    - Nmap
    - Nessus
    - Netsparker
    - Nikto
    - Amass
    - Burp

- 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

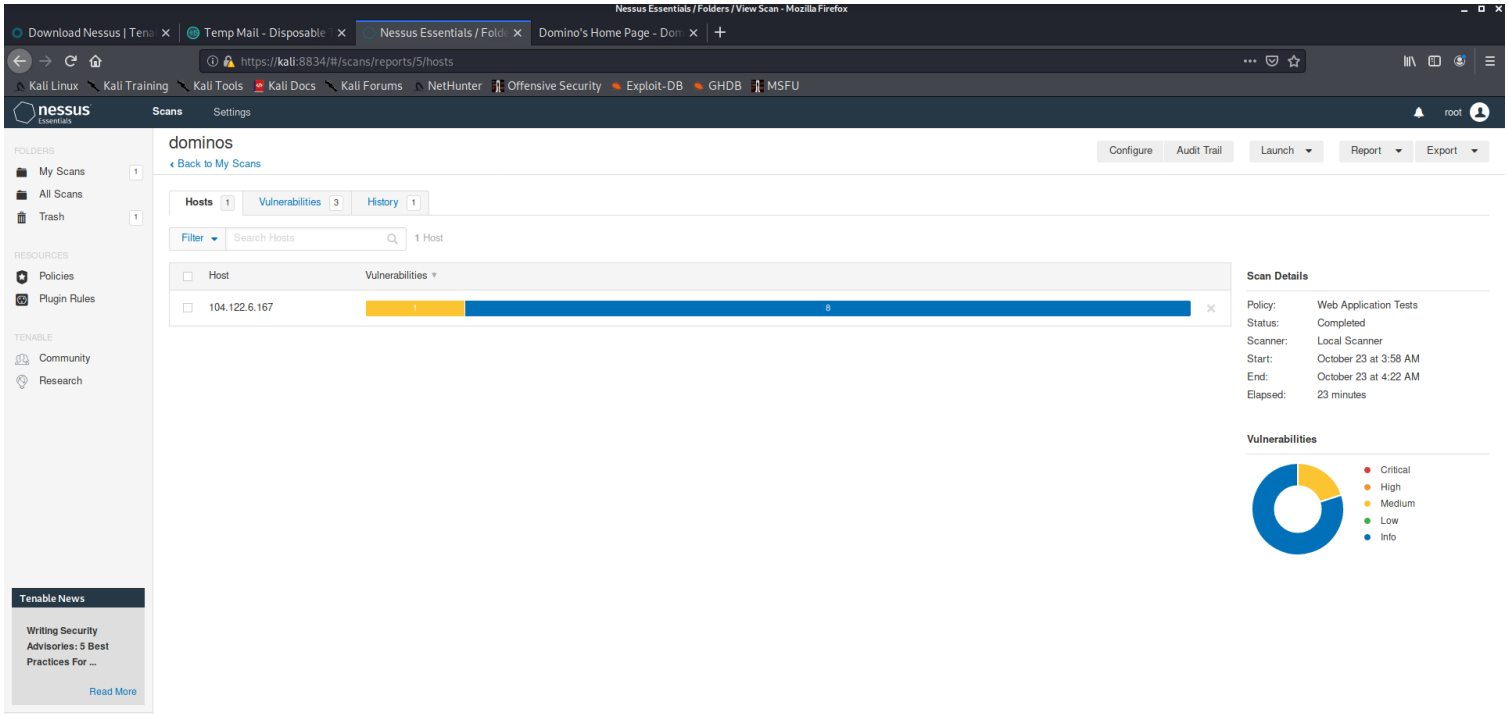


-Figure 05-

- 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.



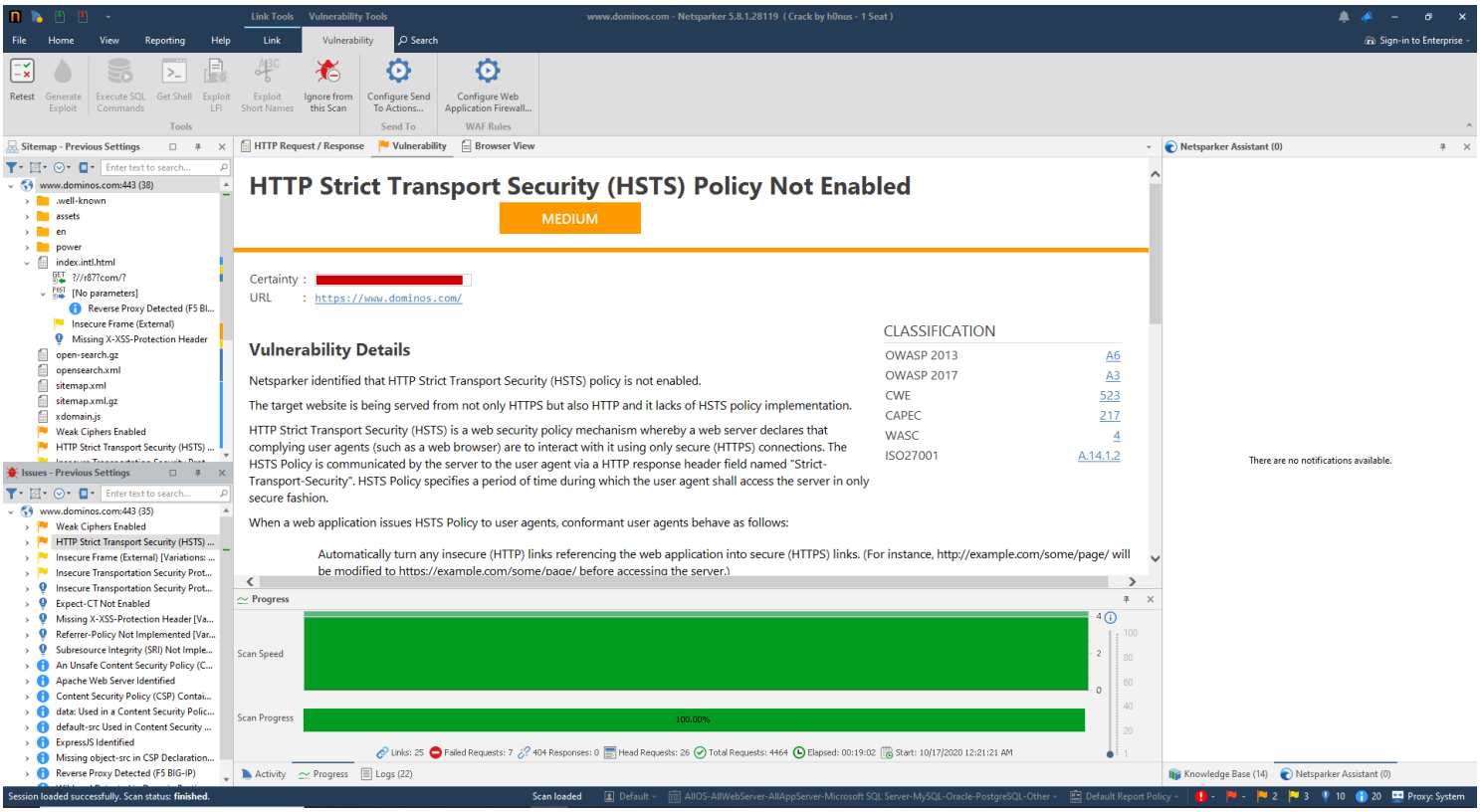
-Figure 06-

- 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.



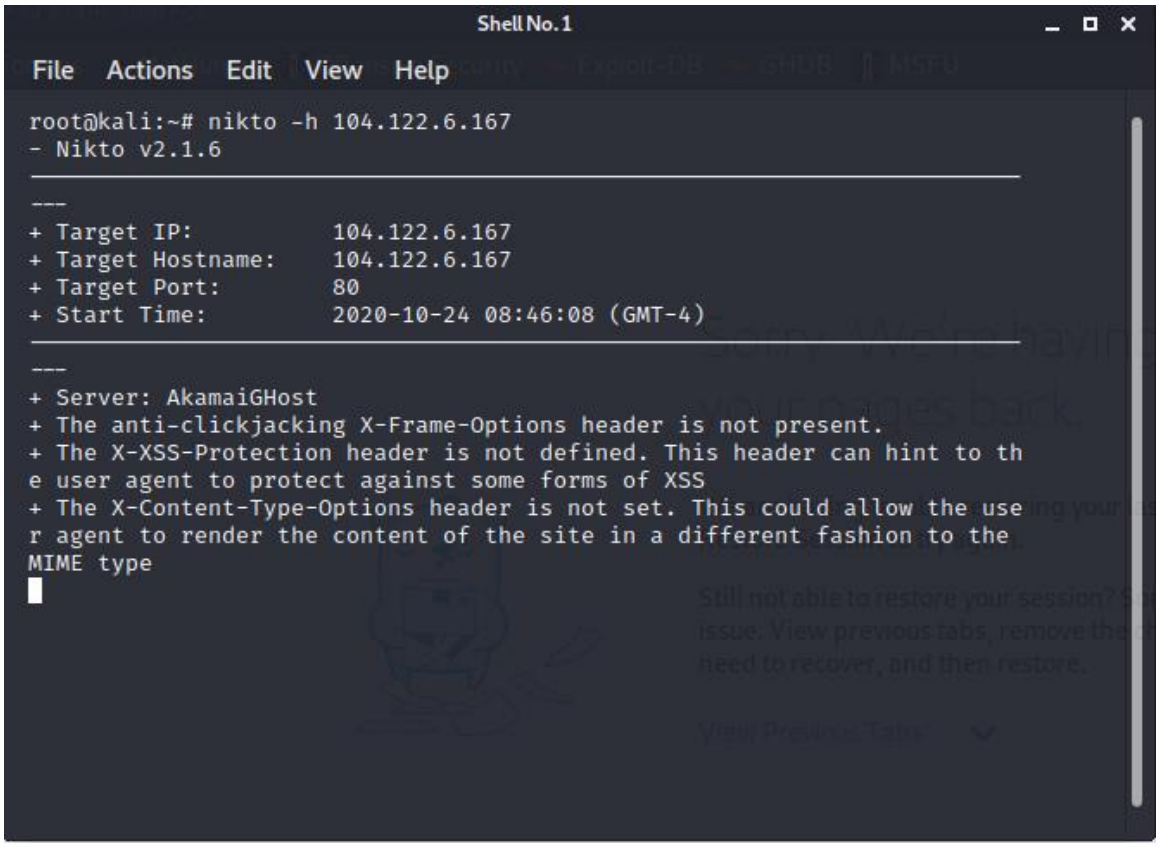
-Figure 07-

- 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



-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

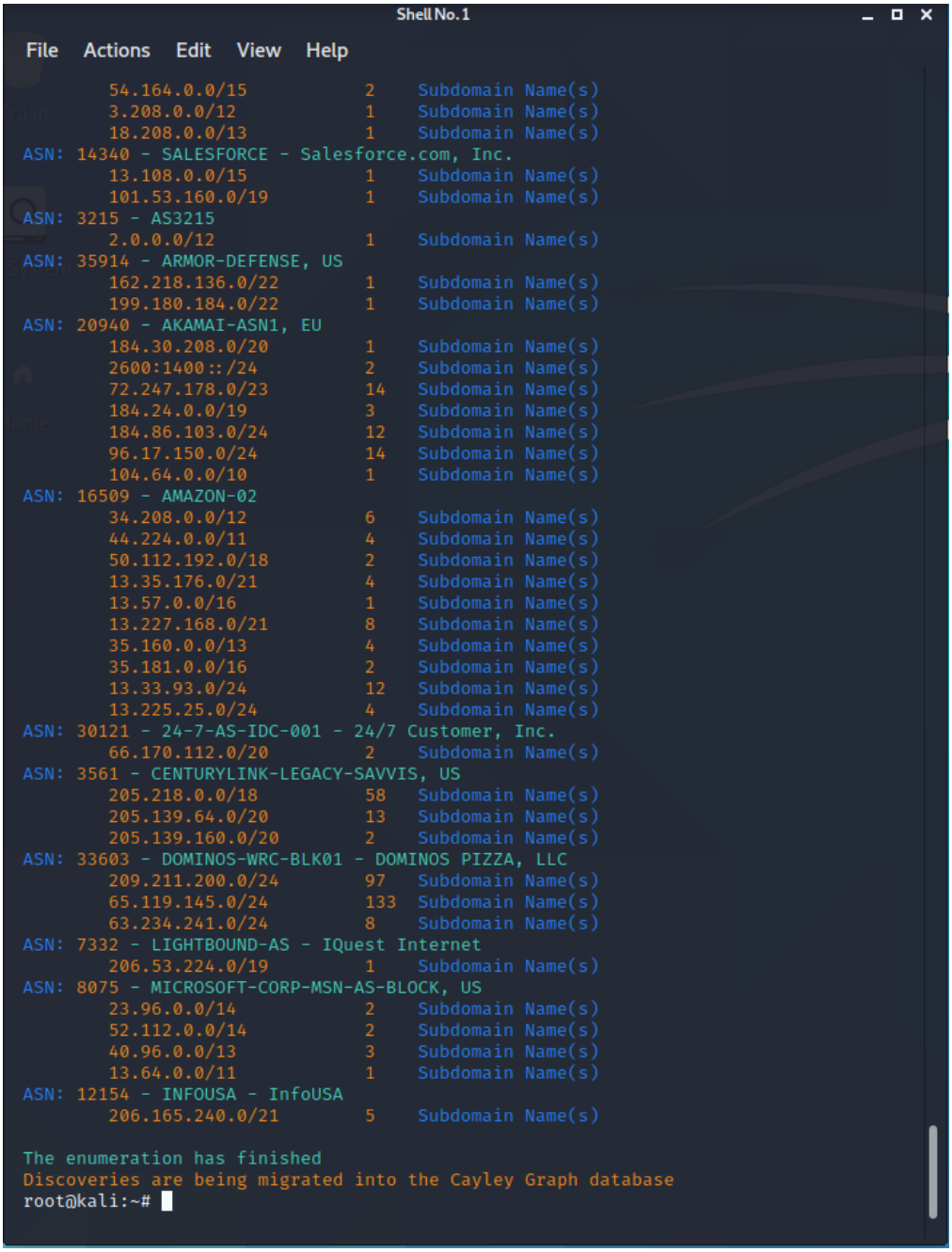
- After that I run the amass tool using below command.

amass enum -d dominos.com

-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-



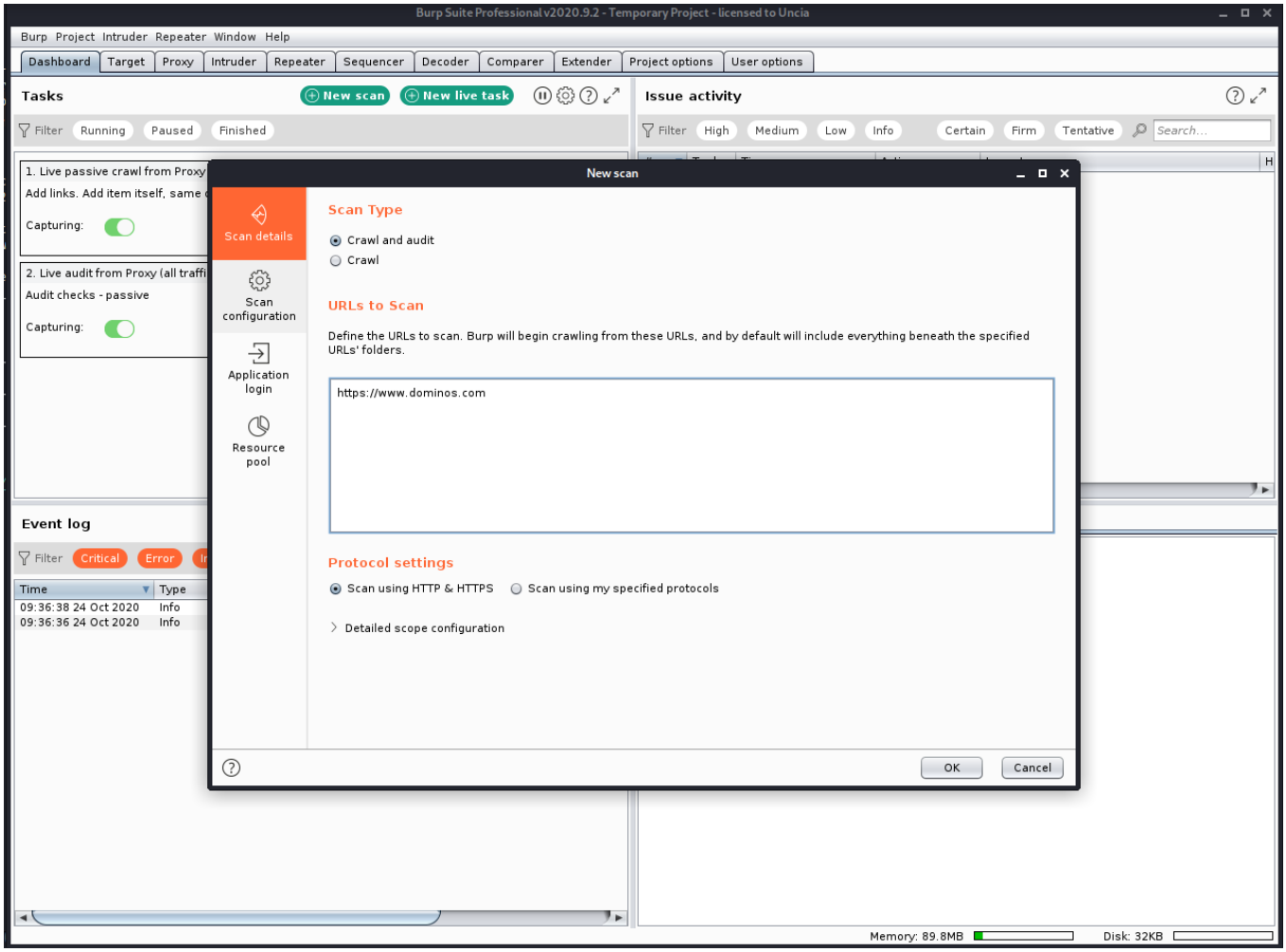
```
Shell No.1
File  Actions  Edit  View  Help
        54.164.0.0/15           2    Subdomain Name(s)
        3.208.0.0/12            1    Subdomain Name(s)
        18.208.0.0/13           1    Subdomain Name(s)
ASN: 14340 - SALESFORCE - Salesforce.com, Inc.
        13.108.0.0/15           1    Subdomain 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.

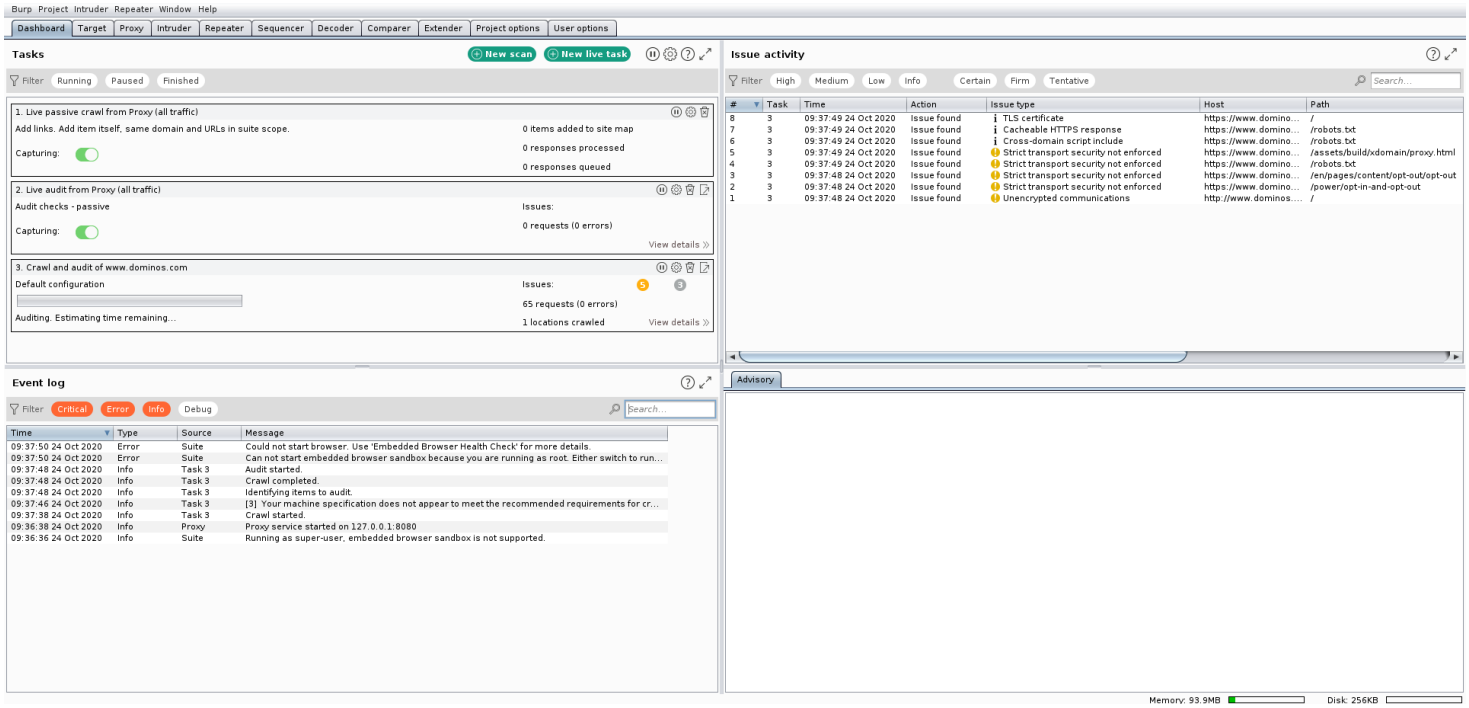
Burp Suite Tool

- 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.



-Figure 13-

Conclusion

- For my web audit, I have used several tools Which include the following:

  - Sublist3r
  - Nmap
  - Nessuss
  - 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