Sri Lanka Institute of Information Technology

Web Audit

Individual Assignment

IE2062 – Web Security

Submitted by:

Student Registration Number	Student Name
IT19039596	Medagedara S.S.

Introduction

What is a web audit?

- Auditing the website is a thorough analysis for all factors affecting search engine visibility. This standard procedure provides a full overview of all websites, traffic and individual pages. For marketing purposes only, the website audit is completed. The aim is to recognize weaknesses in web-based campaigns. The website audit begins with a general website analysis to reveal the actions necessary to enhance SEO. A variety of instruments provide recommendations for raising search web rankings that can include the SEO audit on-site and off-site, such as broken links, duplicate meta-descriptions, HTML validation, web site statistics, mistakes, index pages and site speed. A website audit has many reasons, but in most cases SEO and content marketing are the most important ones. SEO-based website audit finds weak points on the SEO score for a website and contributes to the understanding of the SEO state. The content audit is used to analyze the participation, and to analyze the changes to the content strategy to improve the performance of the website.

- To do a web audit we need to select a web site. For that I used “Bugcrowd” web site. Bugcrowd web site is under the bug bounty program. There are plenty of websites to do web audits. From those web sites we I selected a web site.

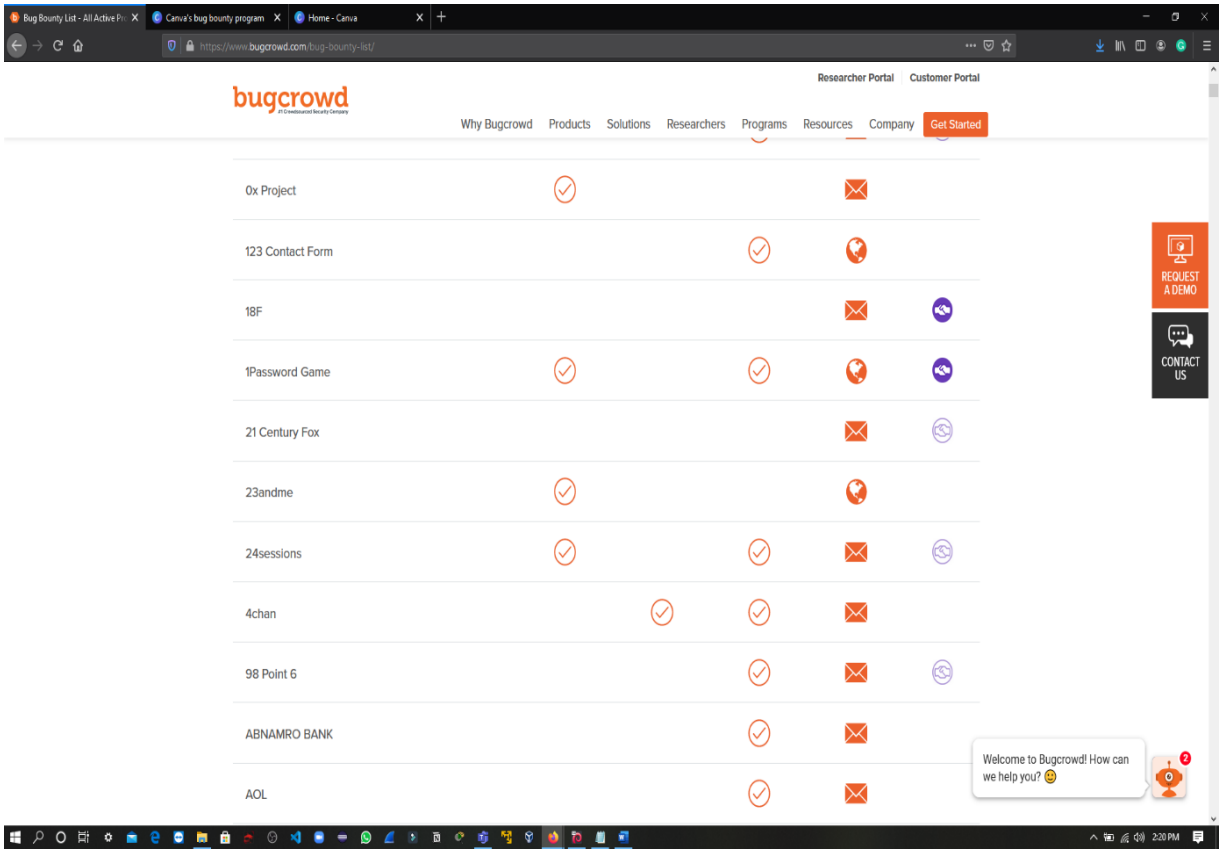


Figure 1.

- Above Figure 1 is about the bugcrowd website that I selected a domain for my web audit.

- And I selected “canva.com” web site to do my web audit.

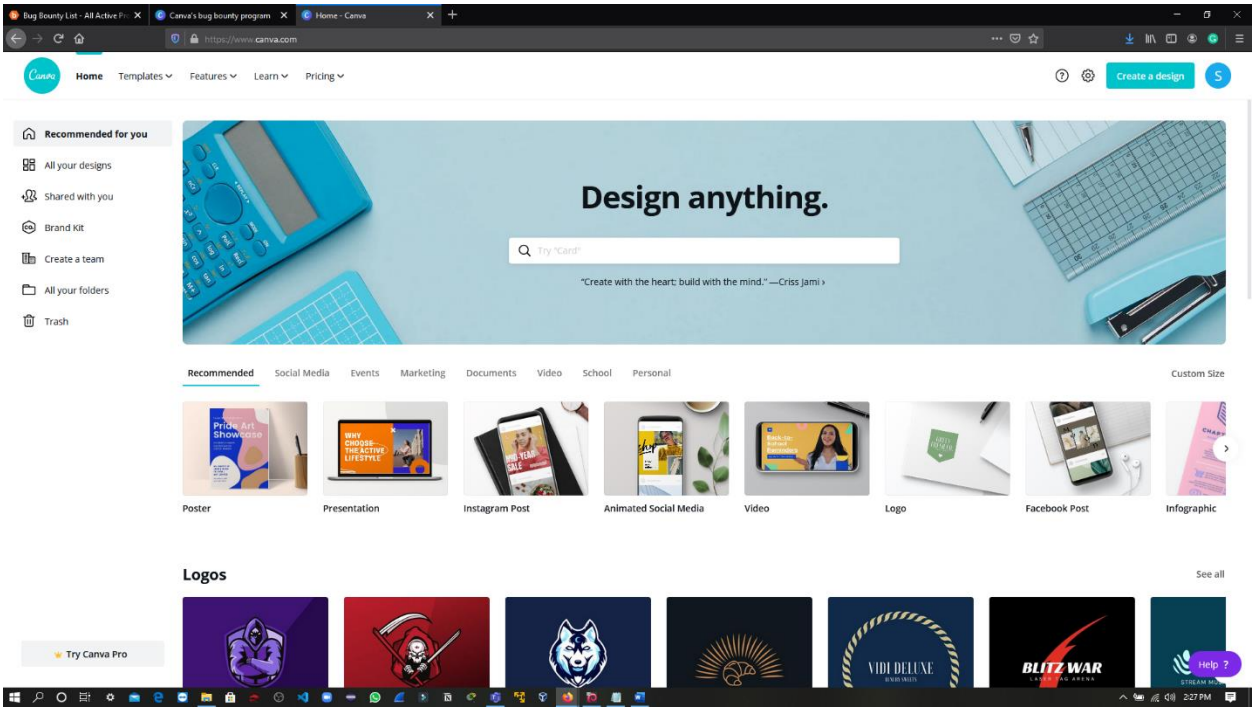


Figure 2.

- Figure 2 shows the canva.com website’s interface.

- Canva is a graphic design platform that allows users to create social media graphics, presentations, posters, documents and other visual contents.

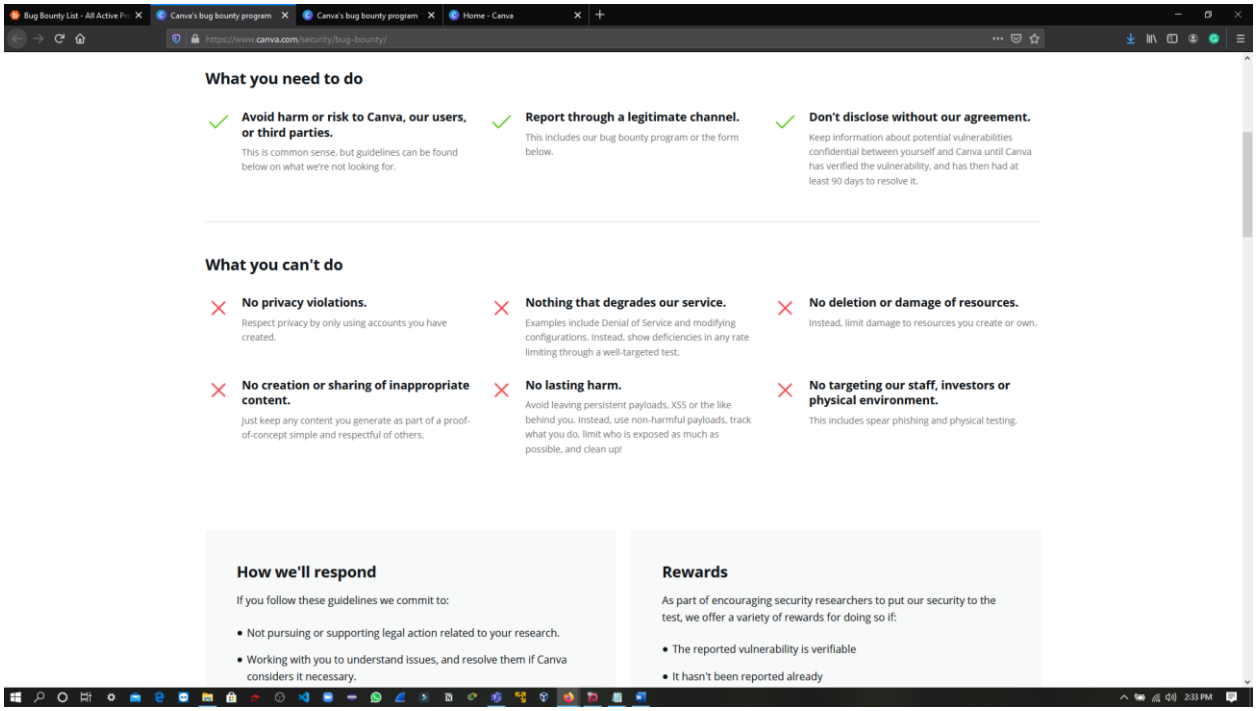


Figure 3.

- As in the above figure they have listed that what they are expecting from us and what they are not expecting us during the web audit.

- What you need to do:

    - Avoid harm or risk to Canva, our users, or third parties
    - Report through a legitimate channel
    - Do not disclose without our agreement.

- What you cannot do:

    - No privacy violations
    - No deletion or damage of resources.
    - No lasting harm
    - Nothing that degrades our service.
    - No creation or sharing of inappropriate content.
    - No targeting our staff, investors or physical environment.

- It is required in our assignment that there must be more than 50 subdomains in the domain that we selected.

- I checked subdomains using “**Sublist3r**” tool.

```
root@kali:~# cd Sublist3r
root@kali:~/Sublist3r# python sublist3r.py -d canva.com

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for canva.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: 122
www.canva.com
1p-sc.canva.com
about.canva.com
about2.canva.com
afe.canva.com
album.canva.com
alpha.canva.com
android.canva.com
animator.canva.com
api.canva.com
assets.canva.com
audio-private.canva.com
audio-public.canva.com
audio-upload.canva.com
banner-static.canva.com
blog.canva.com
button-demo.canva.com
careers.canva.com
category-public.canva.com
cl.canva.com
```

Figure 4.

- According to figure 4 there are 122 subdomains in “canva.com”.

- In my first attempt I tried to exploit the site that I choose without checking up the vulnerabilities of the site using different tools. But those attempts were unsuccessful because the site was much more secure than I assumed. Then I searched for methods to properly conduct a web audit. The "YouTube" videos by **Nahamsec** on this subject gave me an idea about web auditing. According to that video the recon has to be done properly by identifying vulnerabilities and by gathering information about that site as much as possible before attempting the exploitation.
- Link to the you tube video: (https://www.youtube.com/watch?v=amihlWTtkMA)

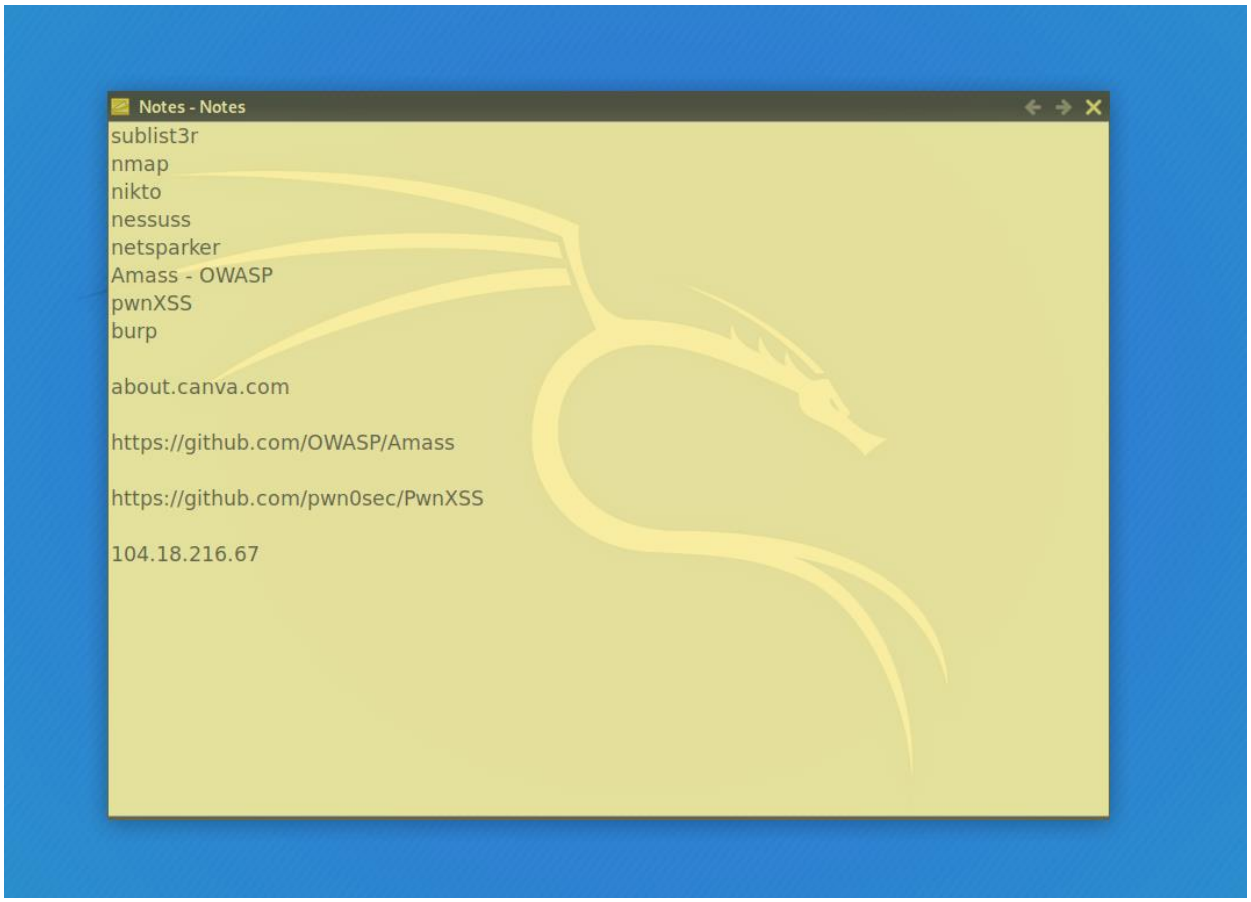


Figure 5.

- As in the figure 5, I created my own note to do the audit. It includes the tools that I used to do the audit.

Web Recon

Nmap Tool

```
File  Actions  Edit  View  Help
root@kali:~# nmap canva.com -v
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-23 01:59 EDT
Initiating Ping Scan at 01:59
Scanning canva.com (104.18.216.67) [4 ports]
Completed Ping Scan at 01:59, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:59
Completed Parallel DNS resolution of 1 host. at 01:59, 0.09s elapsed
Initiating SYN Stealth Scan at 01:59
Scanning canva.com (104.18.216.67) [1000 ports]
Discovered open port 443/tcp on 104.18.216.67
Discovered open port 80/tcp on 104.18.216.67
Discovered open port 8080/tcp on 104.18.216.67
Discovered open port 8443/tcp on 104.18.216.67
Completed SYN Stealth Scan at 02:00, 21.50s elapsed (1000 total ports)
Nmap scan report for canva.com (104.18.216.67)
Host is up (0.032s latency).
Other addresses for canva.com (not scanned): 104.18.215.67 2606:4700::6812:d743 2606:4700::6812:d843
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.91 seconds
           Raw packets sent: 3013 (132.492KB) | Rcvd: 24 (980B)
root@kali:~#
```

Figure 6.

nmap 104.18.216.67 -v

- According to figure 6 I use **Nmap** tool to get information about my domain.
- From that I discovered five open ports and the domain IP address.

Nikto Tool

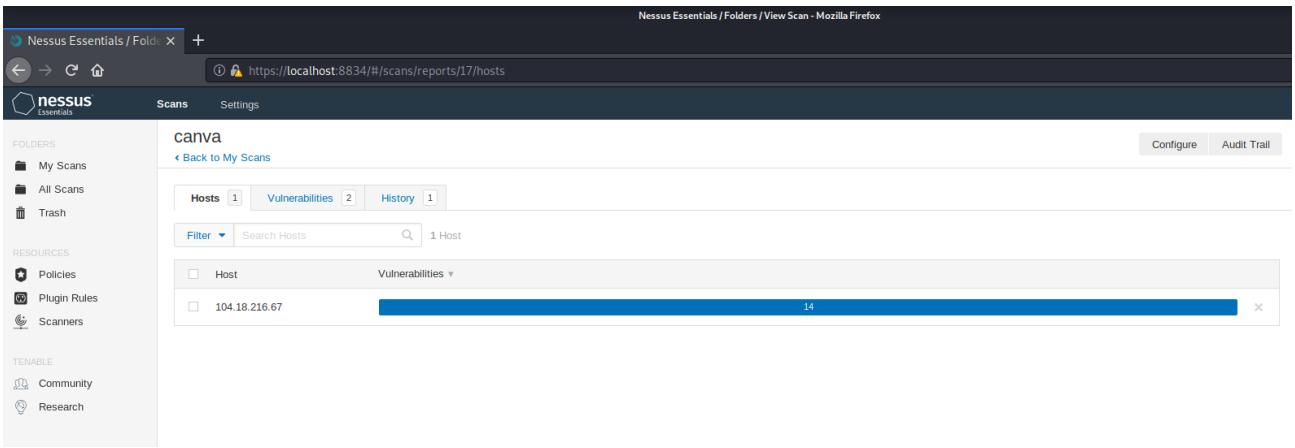
```
File   Actions   Edit   View   Help

root@kali:~# nikto -h 104.18.216.67
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          104.18.216.67
+ Target Hostname:    104.18.216.67
+ Target Port:        80
+ Start Time:         2020-10-19 02:34:40 (GMT-4)
---------------------------------------------------------------------------
+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user ag
+ Uncommon header 'cf-request-id' found, with contents: 05e12a48ca0000d7893316e00
+ The X-Content-Type-Options header is not set. This could allow the user agent t
+ All CGI directories 'found', use '-C none' to test none
```

Figure 7.

nikto -h 104.18.216.67

- As in the figure 7 I used Nikto tool to get information about the domain.
- **Nikto** is a free software command-line vulnerability scanner that scans webservers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received.
- But, using nikto tool I did not get any information or vulnerabilities.

Nessuss Tool



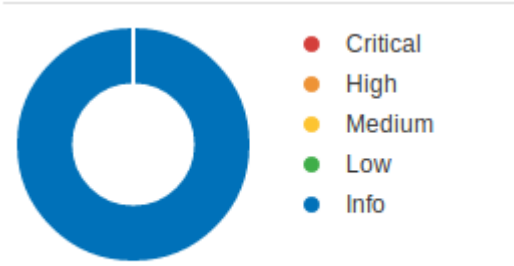


Figure 8, 9.

- As in the Figure 8 and 9, according to nessus report I did not get any high or critical vulnerabilities.
- Therefore, the nessuss scan was not successful.

Netsparker Tool

- Next used netsparker tool to scan my domain and a sub domain. It is more reliable than the nessuss scan because both scans gave lot of information.

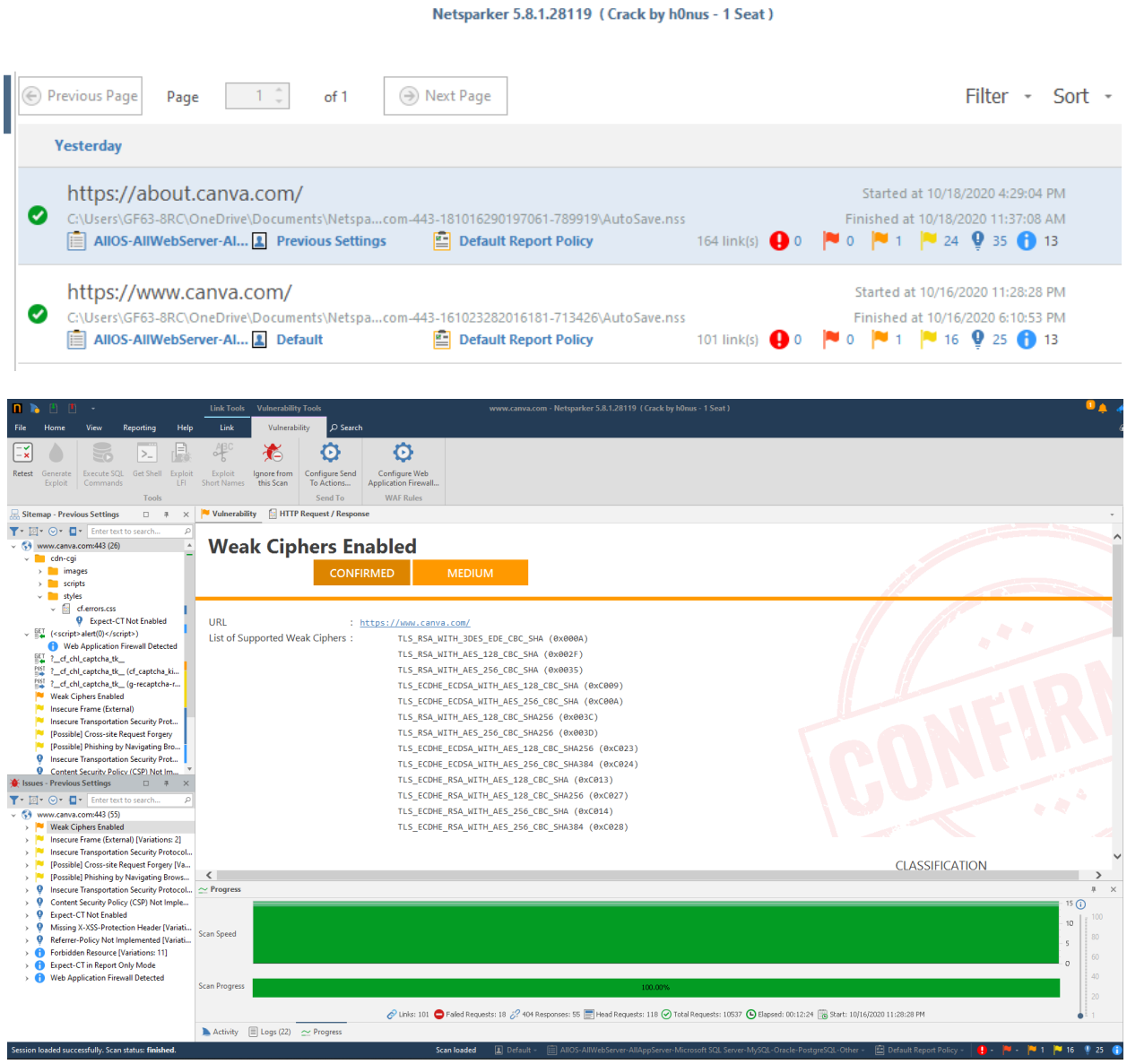


Figure 10,11.

- According to figure 10 and 11, I got only one medium vulnerability from each scan.

Amass Tool

- I used the amass tool for assets discovery.
- Asset discovery invokes keeping a check on the active and inactive assets present in your network. The tools used for this generally analyze the asset clusters and identify the relationships between their, the network, and devices.

```
File   Actions   Edit   View   Help
root@kali:~# amass

                                                                                    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 canva.com
Querying Spyse for canva.com subdomains
Querying Sublist3rAPI for canva.com subdomains
Querying ThreatCrowd for canva.com subdomains
Querying ViewDNS for canva.com subdomains
Querying URLScan for canva.com subdomains
Querying VirusTotal for canva.com subdomains
Querying Yahoo for canva.com subdomains
Querying Baidu for canva.com subdomains
Querying Censys for canva.com subdomains
```

Figure 12.

- Link to download the tool: (https://github.com/OWASP/Amass).

amass, amass enum -d canva.com

```
proxy.cse.canva.com
es-mx.learn.canva.com
ja-jp.learn.canva.com
Average DNS queries performed: 1560/sec, DNS names queued: 0
fr-fr.learn.canva.com
ru-ru.learn.canva.com
id-id.learn.canva.com
de-de.learn.canva.com
docs.developer.canva.com
zh-cn.learn.canva.com
o1006.e.engage.canva.com
o1007.e.engage.canva.com
Average DNS queries performed: 775/sec, DNS names queued: 0

OWASP Amass v3.3.1                                https://github.com/OWASP/Amass
-------------------------------------------------------------------------------
103 names discovered - cert: 12, ext: 7, archive: 1, api: 79, scrape: 3, alt: 1
-------------------------------------------------------------------------------
ASN: 14782 - THEROCKETSCIENCEGROUP
        198.2.128.0/19          2    Subdomain Name(s)
ASN: 19994 - RACKSPACE - RACKSPACE
        166.78.64.0/18          5    Subdomain Name(s)
ASN: 11377 - ASN-SENDGRID, US
        167.89.96.0/20          2    Subdomain Name(s)
        167.89.64.0/19          2    Subdomain Name(s)
ASN: 201229 - DIGITALOCEAN-GERMANY, DE
        188.166.160.0/21        1    Subdomain Name(s)
ASN: 13335 - CLOUDFLARENET
        104.18.208.0/20         152  Subdomain Name(s)
        2606:4700::/32          130  Subdomain Name(s)
        2606:4700::/44          16   Subdomain Name(s)
        162.158.0.0/15          2    Subdomain Name(s)
        2400:cb00:2000::/36     2    Subdomain Name(s)
ASN: 394507 - GOOGLE, US
        34.64.0.0/10            1    Subdomain Name(s)
ASN: 14618 - AMAZON-AES
        34.224.0.0/12           2    Subdomain Name(s)
        52.72.0.0/15            1    Subdomain Name(s)
        18.232.0.0/14           1    Subdomain Name(s)
        34.192.0.0/12           2    Subdomain Name(s)
        35.168.0.0/13           1    Subdomain Name(s)
        3.208.0.0/12            1    Subdomain Name(s)
        54.221.0.0/16           1    Subdomain Name(s)
        23.22.0.0/15            1    Subdomain Name(s)
        54.144.0.0/14           1    Subdomain Name(s)
ASN: 16509 - AMAZON-02
        52.217.64.0/20          1    Subdomain Name(s)
        13.227.136.0/21         4    Subdomain Name(s)
        52.9.0.0/16             3    Subdomain Name(s)
        52.52.0.0/15            3    Subdomain Name(s)
        13.57.0.0/16            3    Subdomain Name(s)
        52.8.0.0/16             3    Subdomain Name(s)
ASN: 15169 - GOOGLE
        35.196.0.0/15           1    Subdomain Name(s)
```

Figure 13.

- As in the figure 13, I got the report including server wise subdomains and their IP addresses.

PwnXSS Tool

- This tool was used to scan for xss vulnerabilities in my domain.

- Link to download the tool: (https://github.com/pwn0sec/PwnXSS).

Python3 pwnxss -u https://www.canva.com

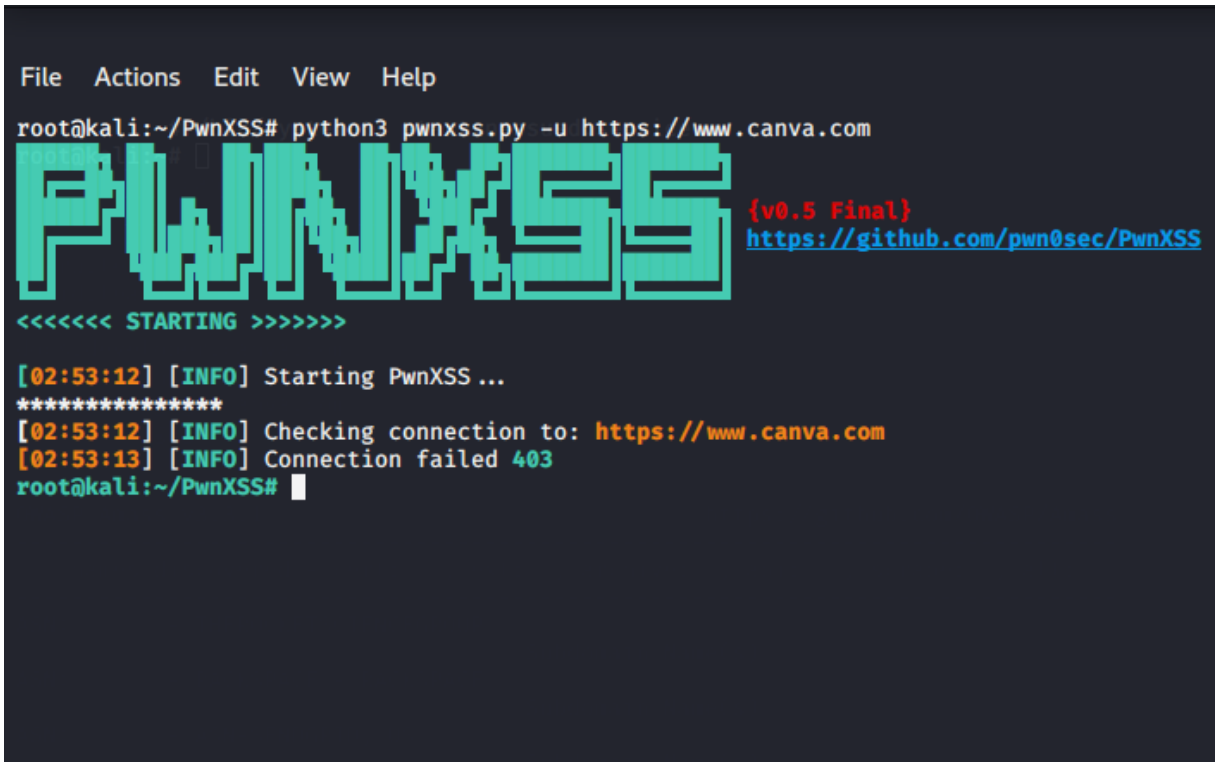


Figure 14.

- This scan was not successful.

- My domain unable to connect with this tool.

Burp Suite

- I used this tool for a full web scan.

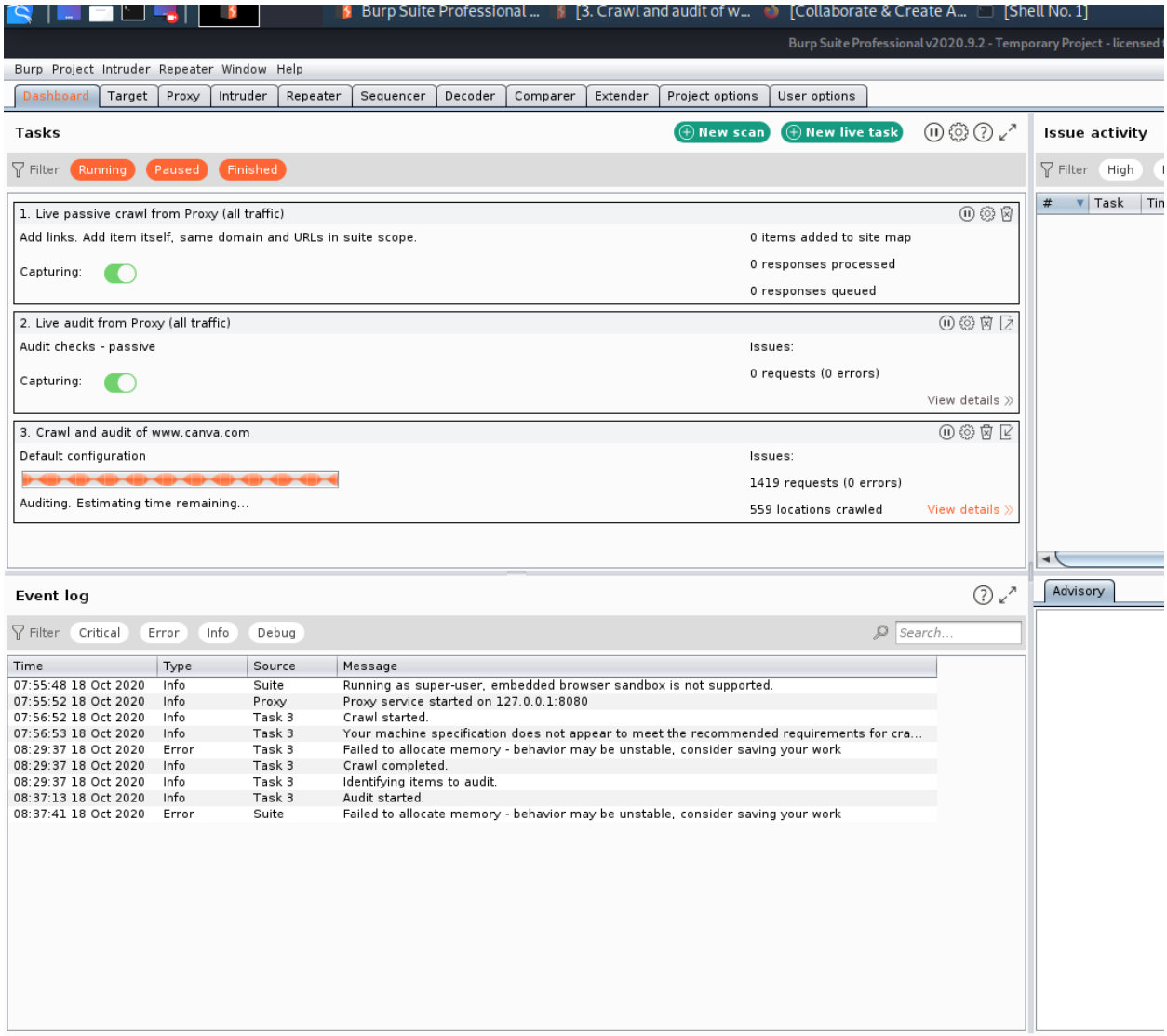


Figure 15.

- As in the figure 15, I did not get any high or critical vulnerabilities in this scan and is was unsuccessful.

Conclusion

- I used many tools to do my web audit. Those are Sublist3r, Nmap, Nikto, Nessuss, Netsparker, Amass, PwnXSS, and Burpsuit. However, from above mentioned scans I did not get any high, critical or impactful vulnerability in **canva.com** domain. Therefore, according to my point of view the canva.com is a much more secure web application.

References

- https://www.udemy.com/android-application-penetration-testing-ethical-hacking/
- https://www.youtube.com/user/Hak5Darren/playlists
- https://www.youtube.com/user/DEFCONConference/videos
- https://www.youtube.com/watch?v=amihlWTtkMA
- https://github.com/ngalongc/bug-bounty-reference/
- https://github.com/bugcrowd/vulnerability-rating-taxonomy
- https://www.bugcrowd.com/blog/