



Sri Lanka Institute of Information Technology

## Web Audit

IE2062 – Web Security

Submitted by:

Student Registration Number	Student Name
IT19051062	A.C.W.B.M Vidanaarachchi

## **Introduction**

What is a Web Audit?

A comprehensive cyber security audit includes the assessment of safety policies, security controls and potential threats to all information technology related assets. This covers websites, as well as web applications. Security auditors have to conduct some parts of the audit manually. By performing a proper web audit, we can find vulnerabilities in that web site or web application. Cyber attack techniques like SQL Injections or Cross Site Scripting (XSS) pose a major threat to data security and may lead to a complete comprise of computer systems. Web vulnerabilities are responsible for these kind of highest security risks associated with web-based systems. All the hidden or unknown vulnerabilities in a website and security infrastructure of the website are included in web security audits. The most common tool used for testing the safety of a website are vulnerability scanners.

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

## Selecting the domain

- To choose a domain I used the “Bug Crowd’s Bug Bounty List “. There many famous and known websites and web applications in that list. Among those domains I selected a domain to perform my web audit.

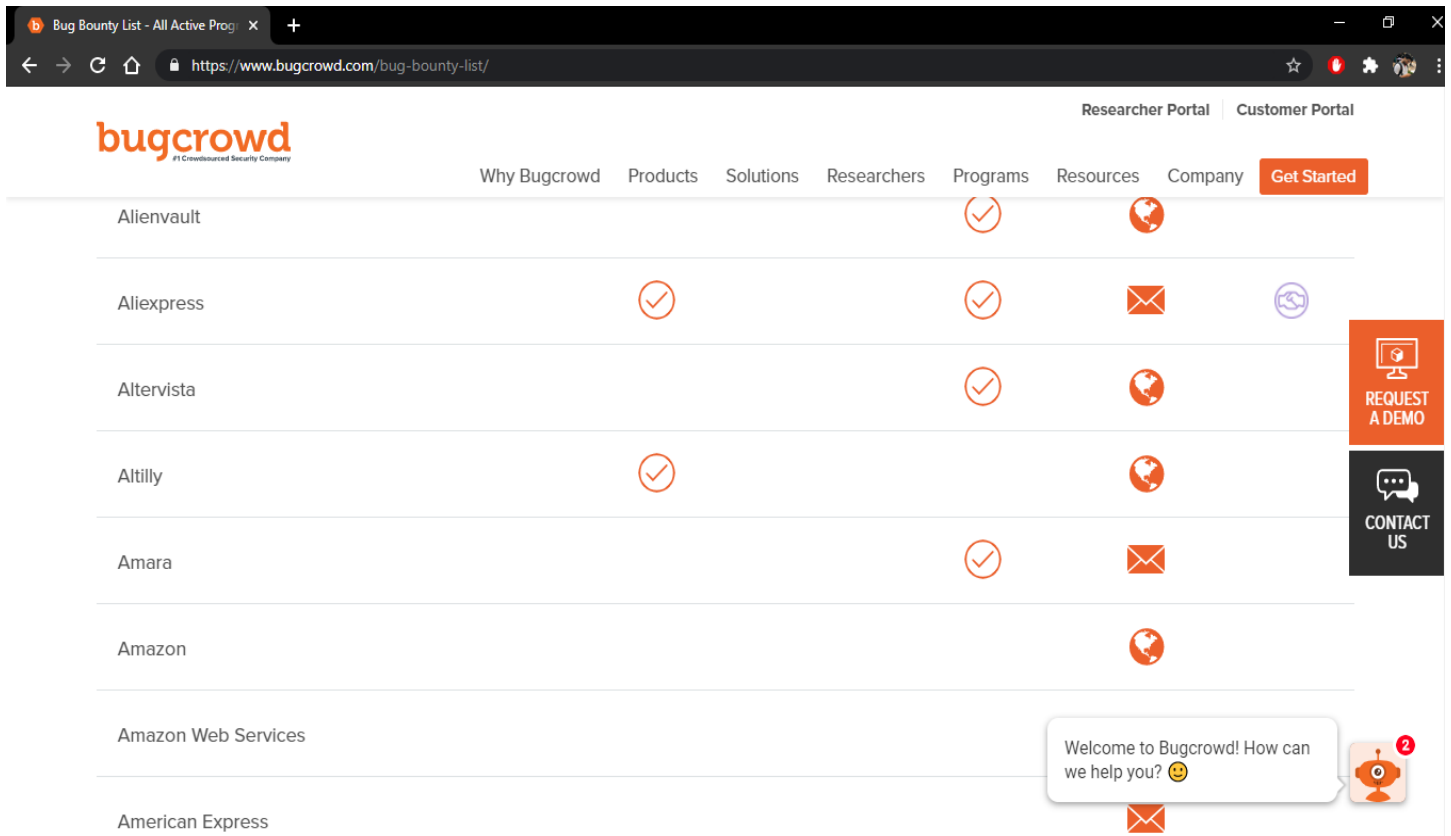


Figure: 1: Bug Bounty list

- Figure 1 shows some of the domains that are listed in the bug crowd bug bounty list.

- From that list I selected “**canva.com**” to perform my web audit

**canva.com**

- The below figure (Figure 2) shows the interface of the “canva.com” and according to the canva.com, canva is a graphic design platform that allows users to create social media graphics, presentations, posters etc.

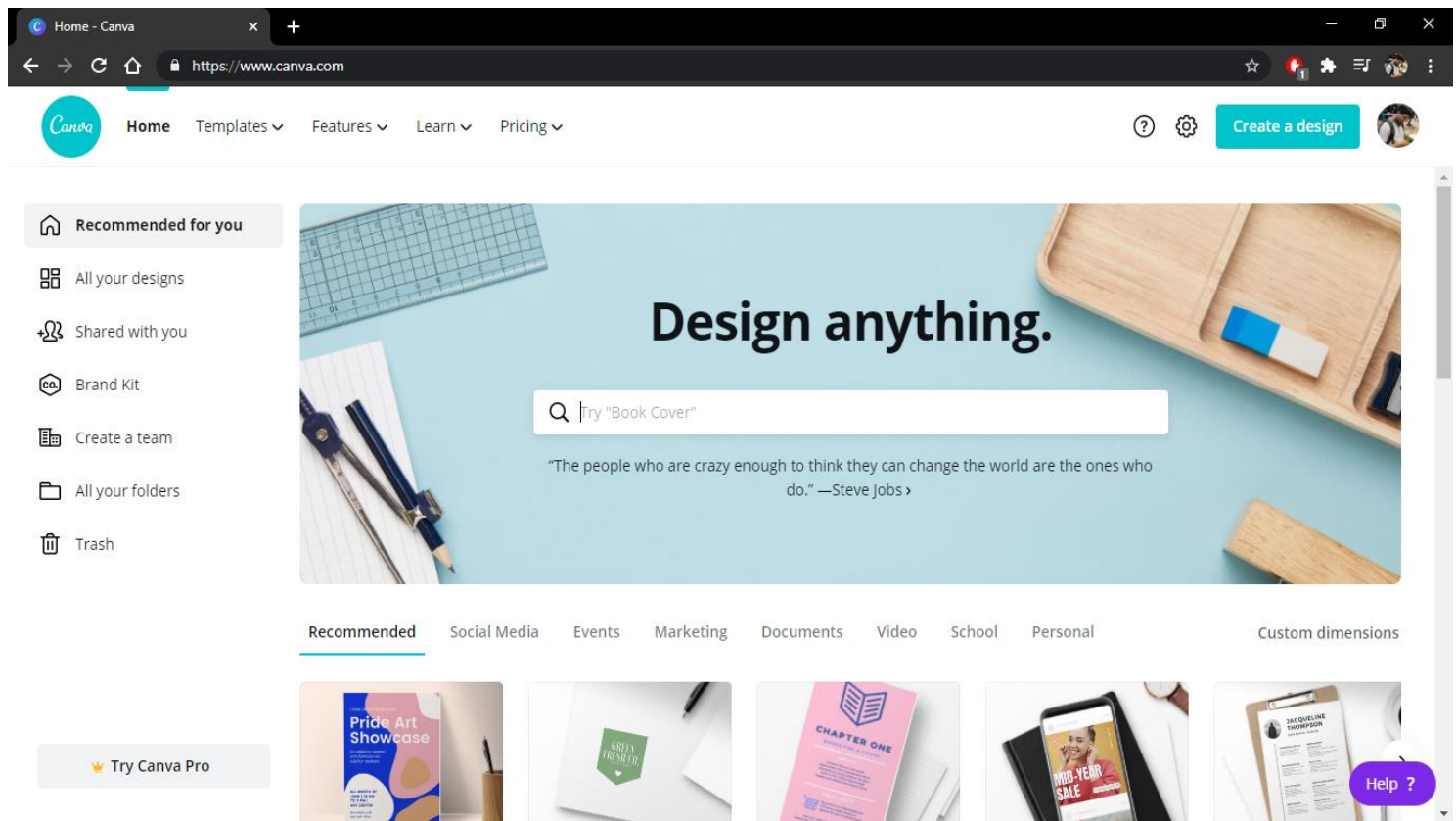


Figure 2: canva.com interface

## What you need to do

- ✓ **Avoid harm or risk to Canva, our users, or third parties.**  
This is common sense, but guidelines can be found below on what we're not looking for.
- ✓ **Report through a legitimate channel.**  
This includes our bug bounty program or the form below.
- ✓ **Don't disclose without our agreement.**  
Keep information about potential vulnerabilities confidential between yourself and Canva until Canva has verified the vulnerability, and has then had at least 90 days to resolve it.

## What you can't do

- ✗ **No privacy violations.**  
Respect privacy by only using accounts you have created.
- ✗ **Nothing that degrades our service.**  
Examples include Denial of Service and modifying configurations. Instead, show deficiencies in any rate limiting through a well-targeted test.
- ✗ **No deletion or damage of resources.**  
Instead, limit damage to resources you create or own.
- ✗ **No creation or sharing of inappropriate content.**  
Just keep any content you generate as part of a proof-of-concept simple and respectful of others.
- ✗ **No lasting harm.**  
Avoid leaving persistent payloads, XSS or the like behind you. Instead, use non-harmful payloads, track what you do, limit who is exposed as much as possible, and clean up!
- ✗ **No targeting our staff, investors or physical environment.**  
This includes spear phishing and physical testing.

Figure: 3: Need to do can't do

- Figure 3 shows the things that we need to do and what we can't do to the website
- To find the subdomains I used sublist3r tool. It is available in the Github and I installed it using git cloning.
- Then I run the sublist3r by giving the below command

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

- There must be at least 50 subdomains for our selected domain to perform the web audit.

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

Warning, you are using a not official version of Sublist3r
# 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
```

Figure: 4: Sublist3r

- Sub domain scan is completed and there are 122 subdomains for canva.com

# Amass

Amass is not pre-installed in Kali Linux I installed it by git cloning, the link is stated below

```
File Actions Edit View Help
```

```
+WQdQdQdQdQd#      Q+WQd#          o8WB:       +WQdQdQdQdQd#.    OWDQdQdW#+  
QdQ#+     .oQd##.     .QdQdoQdW.,OQdQo        :QdQ#QWBo     .Qd#:   .:OW+   ,Qd#++Q#B  
+Qd#      Qd#      #QdB   +QWQdS8Q+         :QW.   +QB   +Q:           ,QD  
Qd       Qd       QdQo  QdB WW     .QW     WQ+   .QW.     oQd#:   ,QD  
WW       QdQo      Qd+: oQ+  oQ+  QB.     SdQo  +WQ#+.     +WQdS:  
#Qd       :QW      Qd+: Qd+  Qd#   :QdQ  QdQo  oWQdW+     OWQDB  
oQd+      QdQ#      Qd+: Qd+  #Qd  Qd.     .WQW     .+Qd#      oQW.  
WW       +QWQdS.  Qd+: :S   oQ+  #Qd   :QWQdQS      Qd+: ..      :Qo  
:QW:      oQd#   +Wo  Qd+      :W: +QWSo+++oQW.  Qd#  Qd#Qo+SdW.   #Qd:   oQ+  
:WQdWWWWWQdQdS      +      :SWQdQdQdQdS  SW     .oSdWWS     :WQdWWWQdQdS  
+OSSES+.                       +OOO.
```

```
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:~# █ I
```

Page 7 of 17

```
File  Actions  Edit  View  Help

Querying Ask for canva.com subdomains
Querying Crtsh for canva.com subdomains
Querying Bing for canva.com subdomains
Querying BufferOver for canva.com subdomains
Querying Censys for canva.com subdomains
Querying CommonCrawl for canva.com subdomains
Querying DNSDB for canva.com subdomains
Querying DNSDumpster for canva.com subdomains
Querying Dogpile for canva.com subdomains
Querying Mnemonic for canva.com subdomains
Querying Exalead for canva.com subdomains
Querying Google for canva.com subdomains
Querying Netcraft for canva.com subdomains
Querying PTRArchive for canva.com subdomains
Querying Entrust for canva.com subdomains
Querying IPv4Info for canva.com subdomains
Querying HackerOne for canva.com subdomains
Querying DNSTable for canva.com subdomains
Querying GoogleCT for canva.com subdomains
Querying HackerTarget for canva.com subdomains
Querying Pastebin for canva.com subdomains
button-demo.canva.com
api.canva.com
support.canva.com
about.canva.com
www.canva.com
learn.canva.com
canva.com
designschool.canva.com
track.canva.com
share.canva.com
status.canva.com
afe.canva.com
typegenius-dynamic.canva.com
media-public.canva.com
video-private.canva.com
email.canva.com
```

Figure: 6: Amass searching for subdomains

- Figure 6 shows that the amass tool is searching for subdomains as the sublist3r
- For run amass scan I used below code

```
amass enum -d canva.com
```



```
Shell No.1
File Actions Edit View Help
OWASP Amass v3.3.1 https://github.com/OWASP/Amass
-----
105 names discovered - alt: 3, dns: 2, cert: 16, archive: 1, api: 76, scrape: 4, ext: 3
-----
ASN: 19994 - RACKSPACE, US
166.78.64.0/18 5 Subdomain Name(s)
ASN: 13335 - CLOUDFLARENET, US
162.158.0.0/15 2 Subdomain Name(s)
2400:cb00:2049::/48 2 Subdomain Name(s)
104.16.0.0/12 156 Subdomain Name(s)
2606:4700::/44 152 Subdomain Name(s)
ASN: 394507 - GOOGLE, US
35.192.0.0/12 1 Subdomain Name(s)
34.64.0.0/10 1 Subdomain Name(s)
ASN: 16509 - AMAZON-02 - AMAZON-02
13.227.150.0/23 4 Subdomain Name(s)
52.217.96.0/20 1 Subdomain Name(s)
52.8.0.0/16 3 Subdomain Name(s)
52.52.0.0/15 3 Subdomain Name(s)
13.57.0.0/16 3 Subdomain Name(s)
52.9.0.0/16 3 Subdomain Name(s)
ASN: 14618 - AMAZON-AES - AMAZON-AES
54.221.0.0/16 1 Subdomain Name(s)
34.192.0.0/12 2 Subdomain Name(s)
35.168.0.0/13 1 Subdomain Name(s)
54.144.0.0/14 1 Subdomain Name(s)
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)
23.22.0.0/15 1 Subdomain Name(s)
3.208.0.0/12 1 Subdomain Name(s)
ASN: 14782 - THEROCKETSCIENCEGROU - THEROCKETSCIENCEGROU
198.2.128.0/19 2 Subdomain Name(s)
ASN: 11377 - ASN-SENDGRID, US
167.89.0.0/18 1 Subdomain Name(s)
167.89.96.0/20 1 Subdomain Name(s)
167.89.64.0/19 2 Subdomain Name(s)
```

Figure: 7: Amass report

## Nmap

Nmap is pre-installed in Kali Linux and it is a free tool for vulnerability scanning. I used nmap to discover the open ports and to find the IP address of the website

Below Figure 8 shows the result of the nmap scan.

- For run nmap I used below command

nmap canva.com

```
Shell No.1
File Actions Edit View Help
root@kali:~# nmap canva.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-18 23:40 EDT
Nmap scan report for canva.com (104.18.216.67)
Host is up (0.028s latency).
Other addresses for canva.com (not scanned): 104.18.215.67 2606:4700::6812:d843 2606:4700::6812:d743
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

Nmap done: 1 IP address (1 host up) scanned in 91.08 seconds
root@kali:~# █
```

Figure: 8: nmap scan

- According to the result IP address is 104.18.216.67. I can use this IP address to my other scans
- And there are 4 open ports with the port state and service

80/tcp	-	http
443/tcp	-	https
8080/tcp	-	http-proxy
8443/tcp	-	https-alt

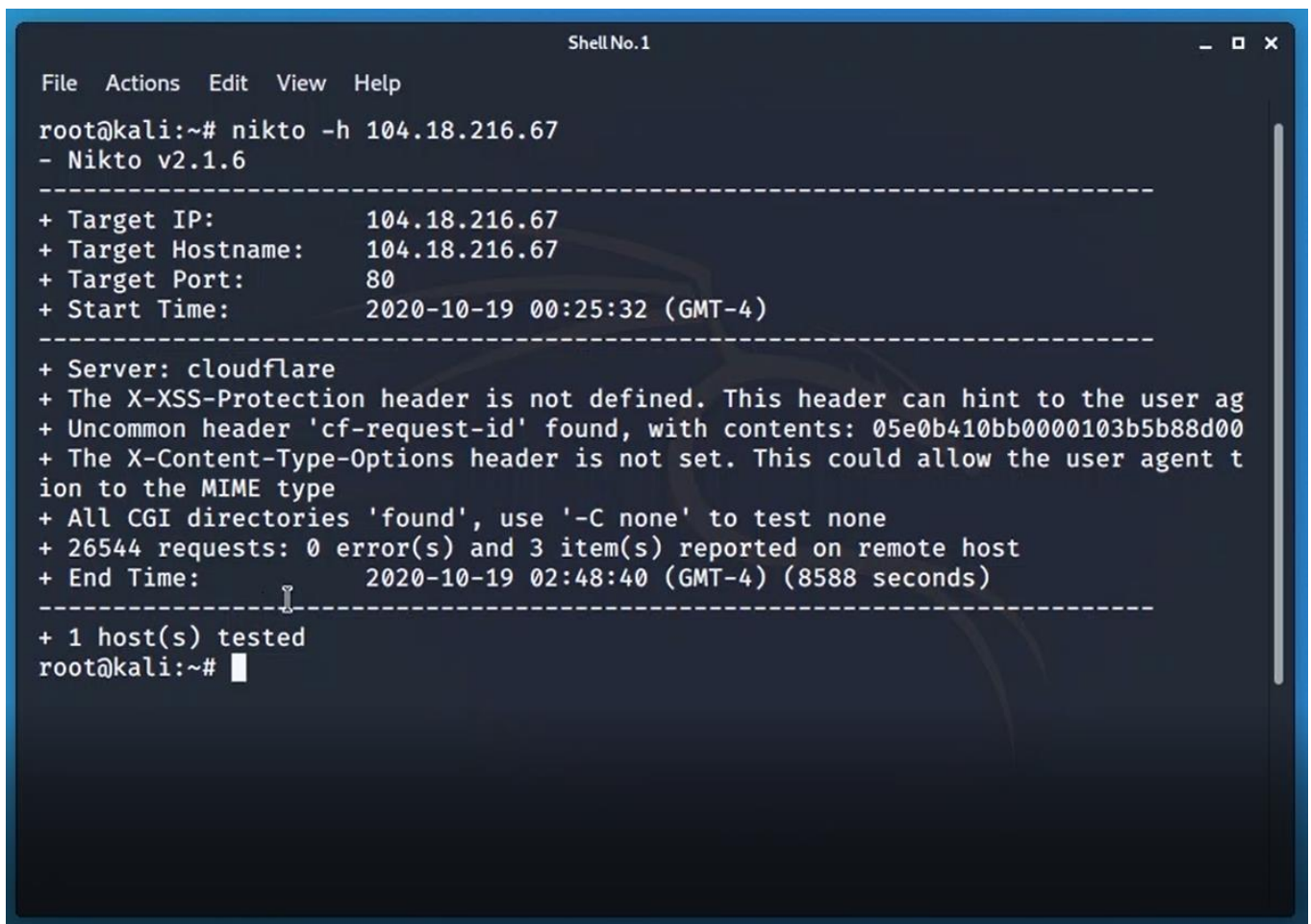
- Above all the ports are open.

## Nikto

This tool is also pre-installed in Kali, it is used for web server scanning and vulnerability assessment.

```
nikto -h 104.18.216.67
```

- The IP address is previously obtained IP address from the nmap scan

A screenshot of a terminal window titled "Shell No.1" with a dark blue background. The terminal shows the command "nikto -h 104.18.216.67" being executed. The output displays scan details such as target IP, hostname, port, and start time, followed by a list of findings including missing security headers and CGI directories. The scan concludes with a summary of requests and the time taken.

```
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 00:25:32 (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: 05e0b410bb0000103b5b88d00
+ The X-Content-Type-Options header is not set. This could allow the user agent t
ion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
+ 26544 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2020-10-19 02:48:40 (GMT-4) (8588 seconds)
-----
+ 1 host(s) tested
root@kali:~# █
```

Figure: 9: nikto scan and result

- This nikto scan shows some vulnerabilities of the selected domain.

# Netsparker

Netsparker is also performing an extreme scan than the Nessus and this scan took about 16 minutes to complete

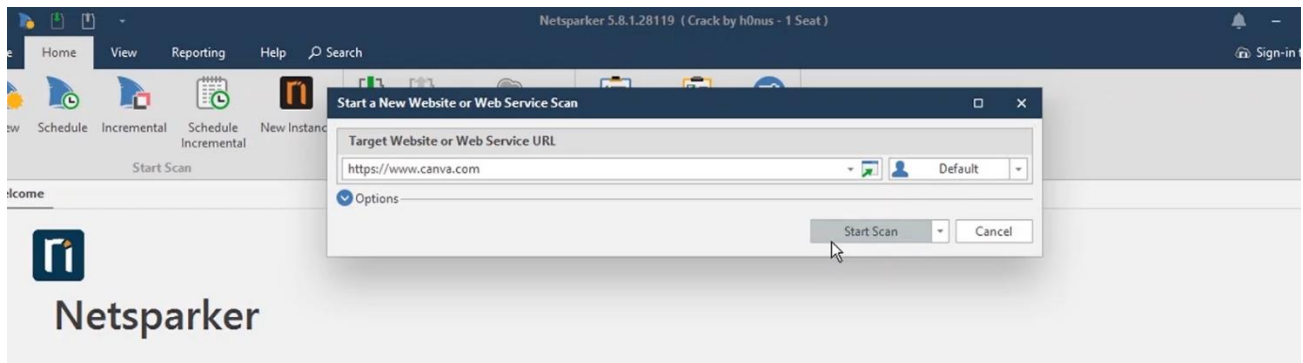


Figure: 9: Netsparker scan

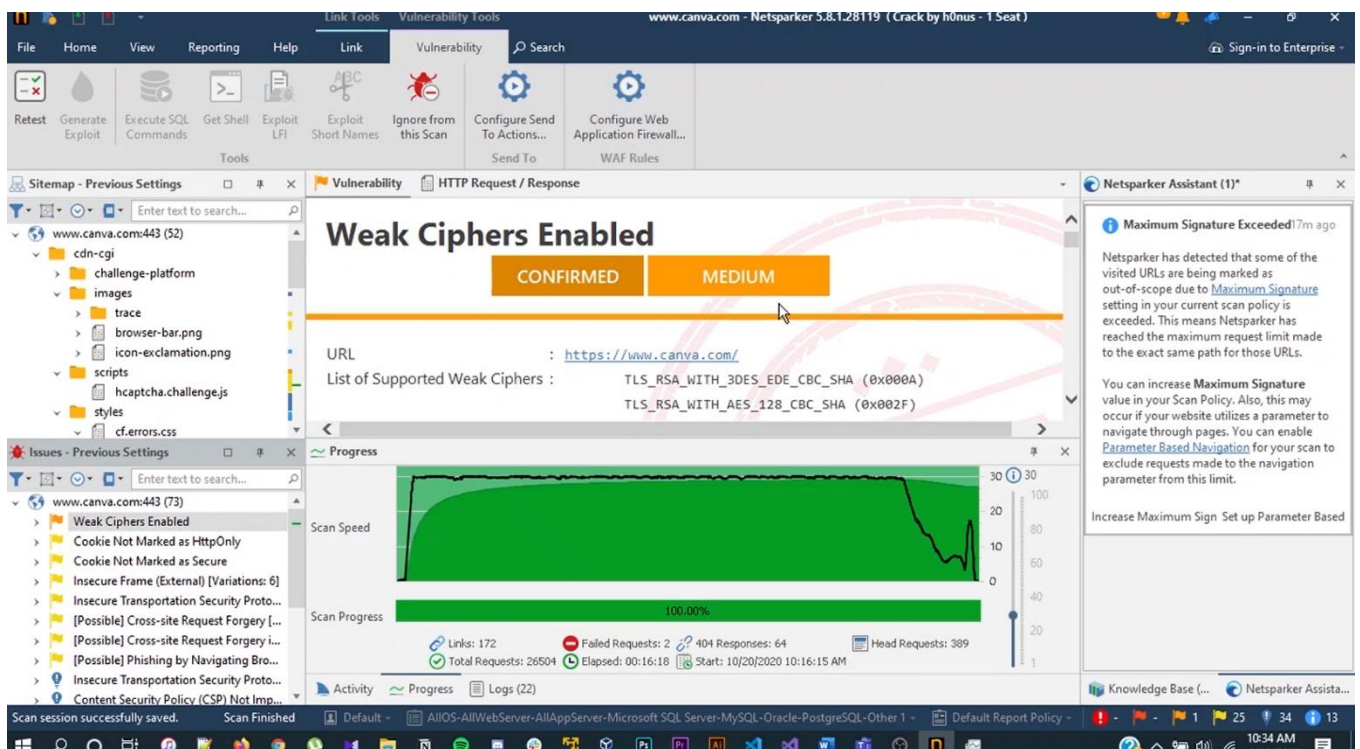


Figure: 10: Netsparker scan report

# Nessus

Then I used nessus to scan the report, but the scan report is not useful, it only showed two information files, one containing open ports as nmap and the other file is about information of the scan. We can't get a decision by using this scan

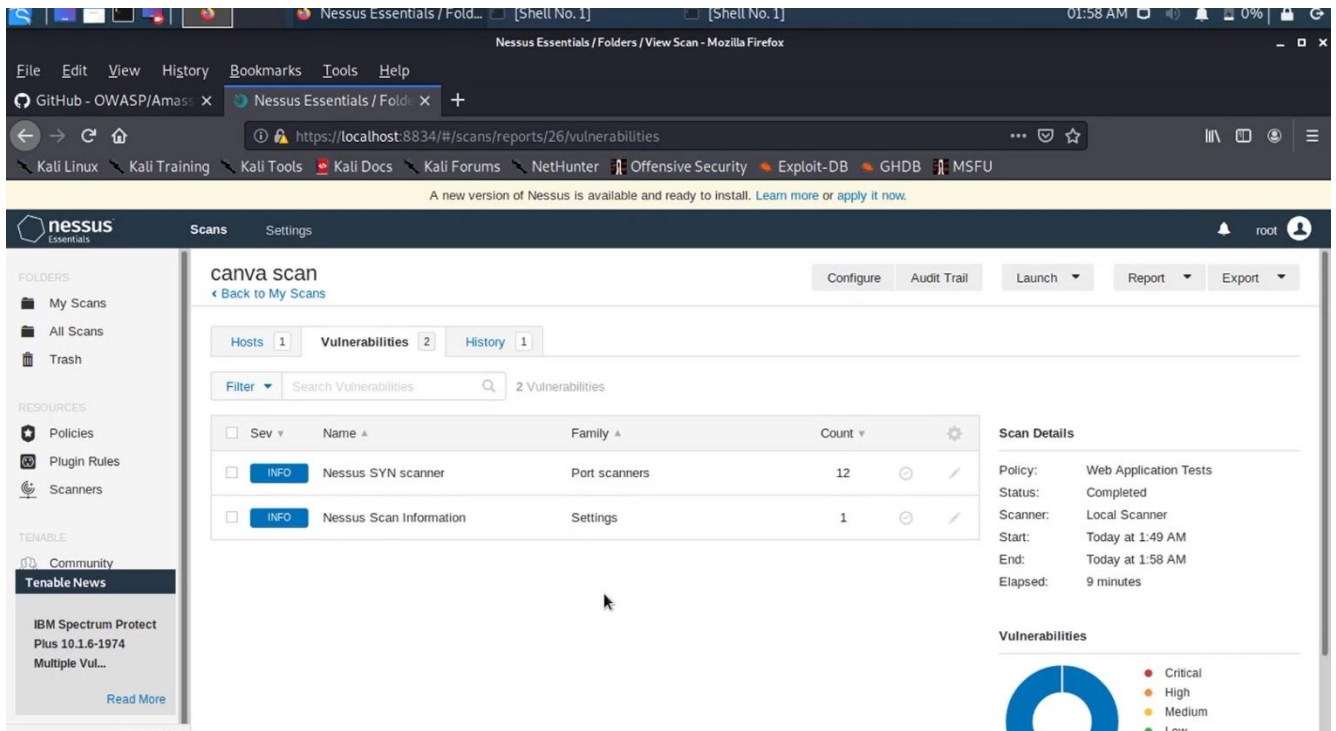


Figure 11: Nessus scan

Port	Hosts
2086 / tcp	104.18.216.67

Port 2087/tcp was found to be open	
Port	Hosts
2087 / tcp / www	104.18.216.67

Port 2096/tcp was found to be open	
Port	Hosts
2096 / tcp / www	104.18.216.67

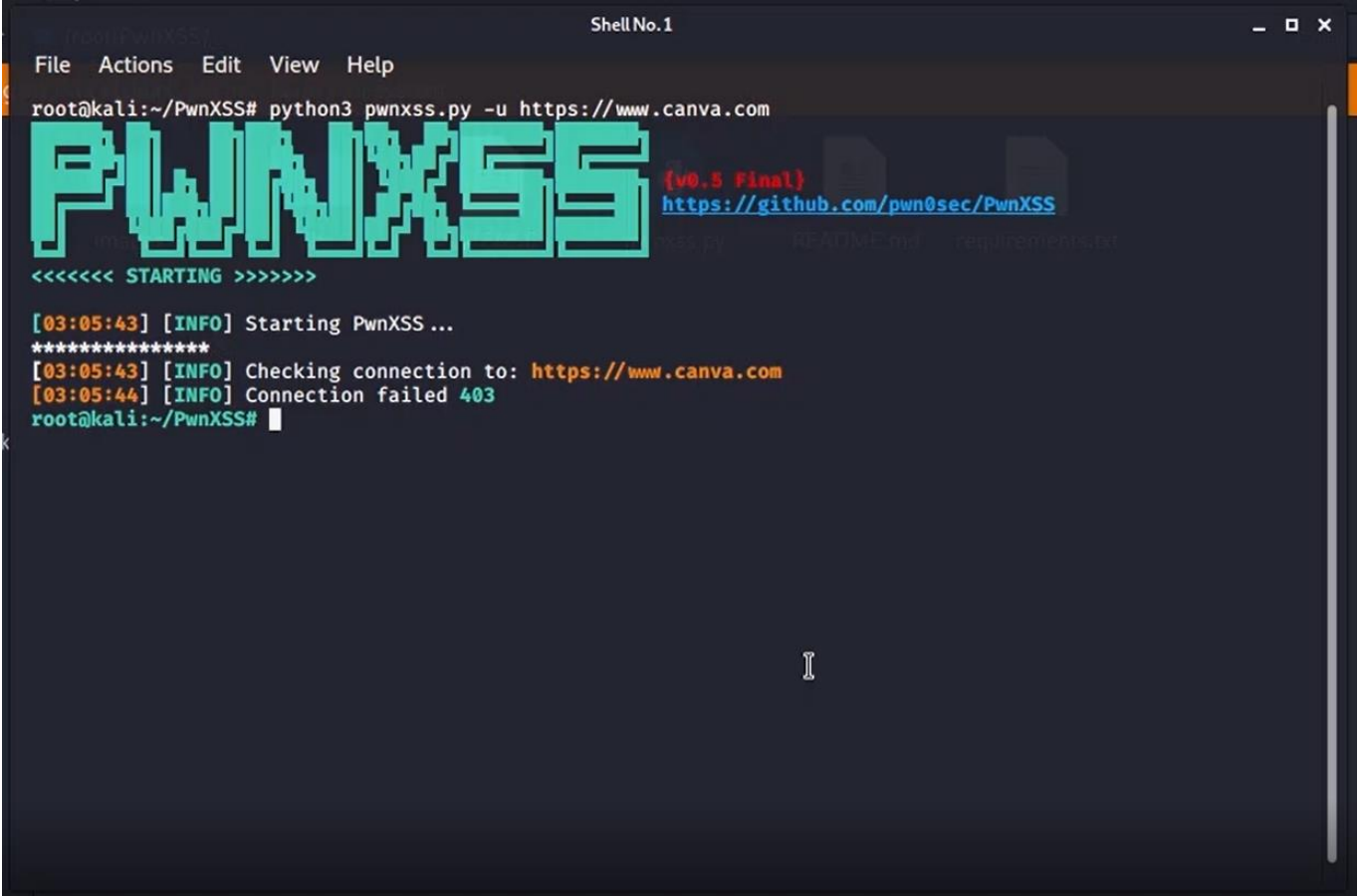
Figure 12: open ports



# PwnXSS

I installed PwnXSS by using git hub but unfortunately the PwnXSS showed an error when the scan was started. (Figure 13)

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



```
root@kali:~/PwnXSS# python3 pwnxss.py -u https://www.canva.com
PWNXSS {v0.3 Final} https://github.com/pwn0sec/PwnXSS
<<<<<< STARTING >>>>>>
[03:05:43] [INFO] Starting PwnXSS ...
*****
[03:05:43] [INFO] Checking connection to: https://www.canva.com
[03:05:44] [INFO] Connection failed 403
root@kali:~/PwnXSS#
```

Figure: 13: PwnXSS with error

- Can't connect with "canva.com"

# BurpSuite

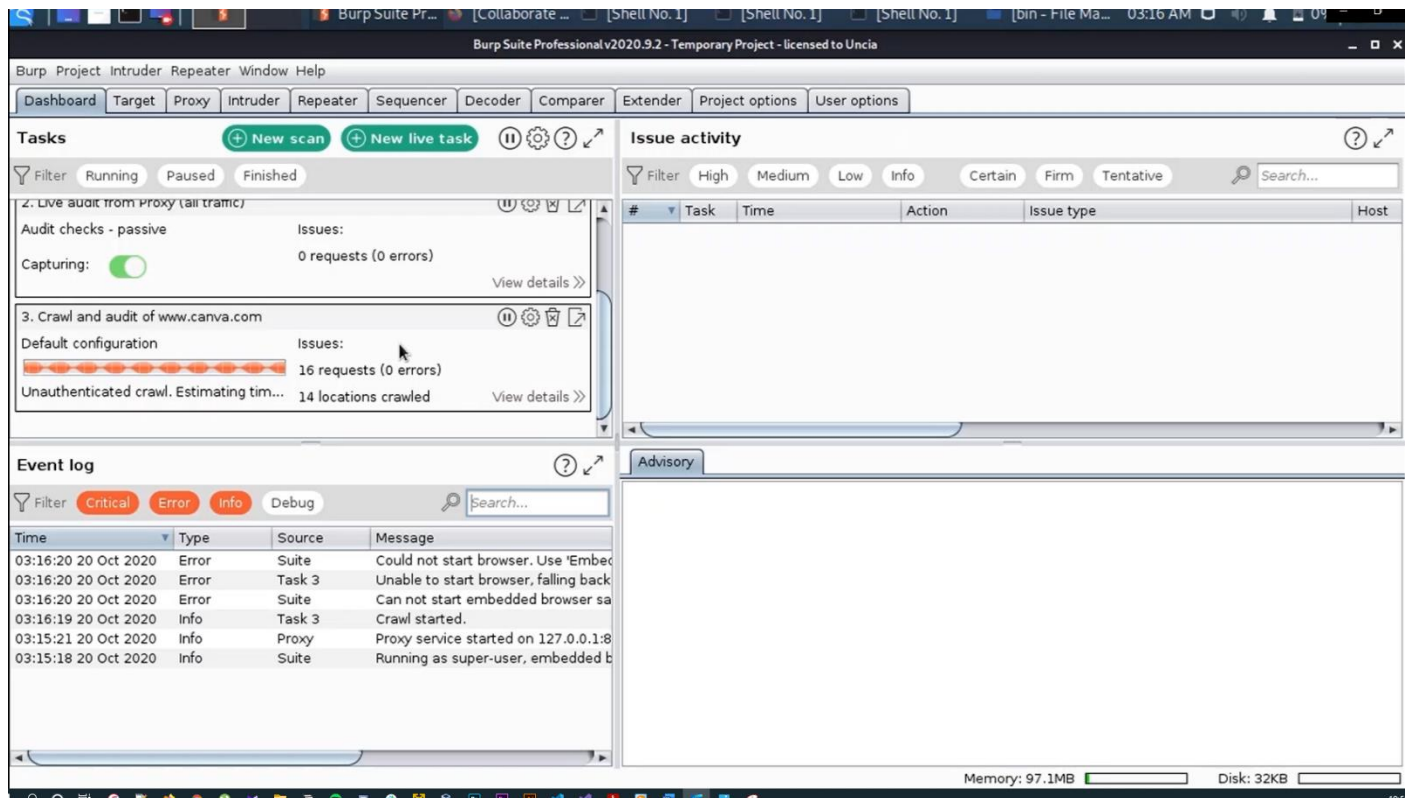


Figure: 14: BurpSuite scan

I used BurpSuite to scan my domain, I leave it to run about two hours, but it did not give any result after two hours. Then I close the scan.

## Conclusion

After many scans I did not get any high/critical vulnerabilities related to my selected domain [www.canva.com](http://www.canva.com) only the Netsparker showed a medium vulnerability. To complete the information gathering part respectively I have used Sublist3r, Amass, Nmap, Nikto, Netsparker, Nessus, PwnXSS and BurpSuite. Therefore, I can conclude that this domain “canva.com” is a secured web application.

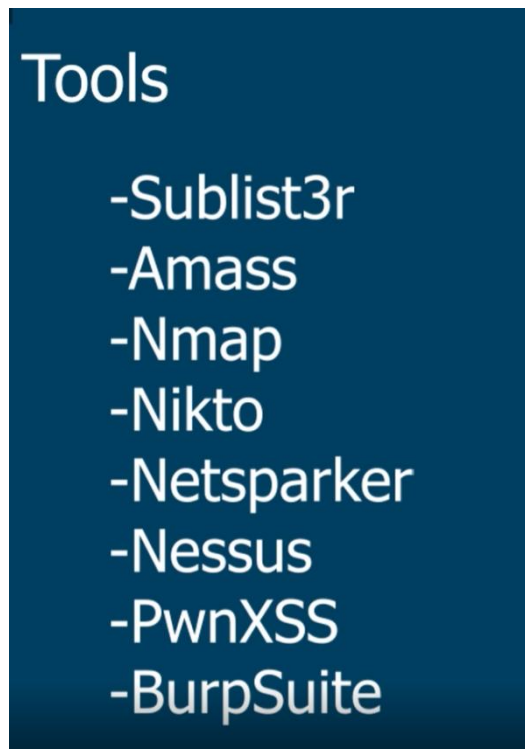


Figure: 14: Summary of tools from video



## References

<https://www.hackerone.com/blog/resources-for-new-hackers>  
[https://www.peerlyst.com/posts/the-everything-bug-bounty-wiki-peerlyst?trk=company\\_page\\_posts\\_panel](https://www.peerlyst.com/posts/the-everything-bug-bounty-wiki-peerlyst?trk=company_page_posts_panel)  
<https://github.com/onlurking/awesome-infosec>  
<https://forum.bugcrowd.com/t/researcher-resources-tutorials/370>  
<https://forum.bugcrowd.com/t/researcher-resources-tools/167>  
<https://forum.bugcrowd.com/t/how-do-you-approach-a-target/293>  
<http://www.amanhardikar.com/mindmaps/Practice.html>  
<https://github.com/djadmin/awesome-bug-bounty>

<https://www.quora.com/How-does-one-become-a-bug-bounty-hunter/answer/Jobert-Abma>  
<https://www.quora.com/How-much-time-did-you-take-from-completely-beginning-hacking-to-your-first-success-or-bug-bounty/answer/Jobert-Abma>  
<https://www.quora.com/How-do-bug-bounty-hunters-find-bugs/answer/Jobert-Abma>  
<https://www.quora.com/How-much-can-I-make-in-my-first-year-as-a-bug-bounty-hunter>  
<https://blog.detectify.com/2019/05/03/meet-the-hacker-inti-de-ceukelaire-while-everyone-is-looking-for-xss-i-am-just-reading-the-docs>  
<http://blog.oath.ninja/basic-bug-bounty-faq>  
<https://twitter.com/spaceraccoonsec>