Sri Lanka Institute of Information Technology

Web Audit Report

(Individual Assignment)

IE2062 – Web Security

Submitted by:

Student Registration Number	**Student Name**
IT19048888	S. P. Athige

Table of Contents

1. Introduction

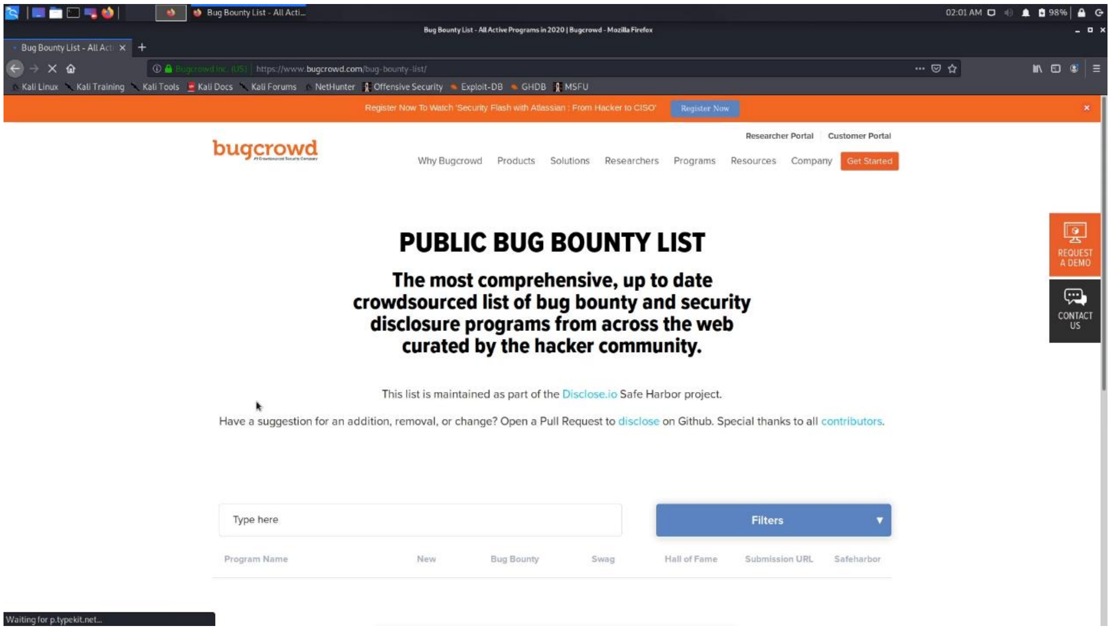
It seems like the news of the newest compromised website includes a report nearly every day. When it does, most believe it will never happen to them. Hackers could search your website at any given point for something they can compromise to use your site and/or server for their nefarious activities. It is essential that you conduct a website security audit if you do not want to fall victim to their tactics. A website security guide that does not mention Website Security Audit as a must is hard to find. For a while now, cybersecurity enthusiasts have highlighted the need for a website security audit. But it is only now that site owners have begun to accept it as a prerequisite for their business. Your web system and its security specifications for bugs & loopholes are analyzed by a reliable website security audit.

A Website Security Audit is a process that tests the web framework, including vulnerability and loophole center, extensions, themes, and other infrastructure. Usually, a comprehensive web security audit includes static & dynamic review of code, business logic error checking, configuration checking, etc.

Both secret vulnerabilities on the website and security infrastructure are included in Website Security audits and are normally followed by a penetration test. While the aim of a security audit is to analyze and locate vulnerable areas, a penetration test focuses on exploiting them. Penetration tests are little more than emulating the situation of a hacker and a real-life attack and leveraging the vulnerabilities to determine the danger associated with each vulnerability. Both automated tools and human acumen allow use of the most accurate security audits.

2. Choosing the Domain

In order to perform this web audit, I have chosen the domain “canva.com”, an online graphic designing platform which published a bug bounty program on Bugcrowd. The main objective of this web audit is to find whether the domain has “OWASP top 10 vulnerabilities for the year 2020”.


Bug Bounty List - All Acti...
02:01 AM 98%
Bug Bounty List - All Active Programs in 2020 | Bugcrowd - Mozilla Firefox
Bug Bounty List - All Acti
Bugcrowd Inc. (US) https://www.bugcrowd.com/bug-bounty-list/
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
Register Now To Watch 'Security Flash with Atlassian : From Hacker to CISO'
Register Now
Researcher Portal
Customer Portal
bugcrowd
Why Bugcrowd
Products
Solutions
Researchers
Programs
Resources
Company
Get Started
REQUEST A DEMO
CONTACT US
Type here
Filters
Waiting for p.typekit.net...

PUBLIC BUG BOUNTY LIST

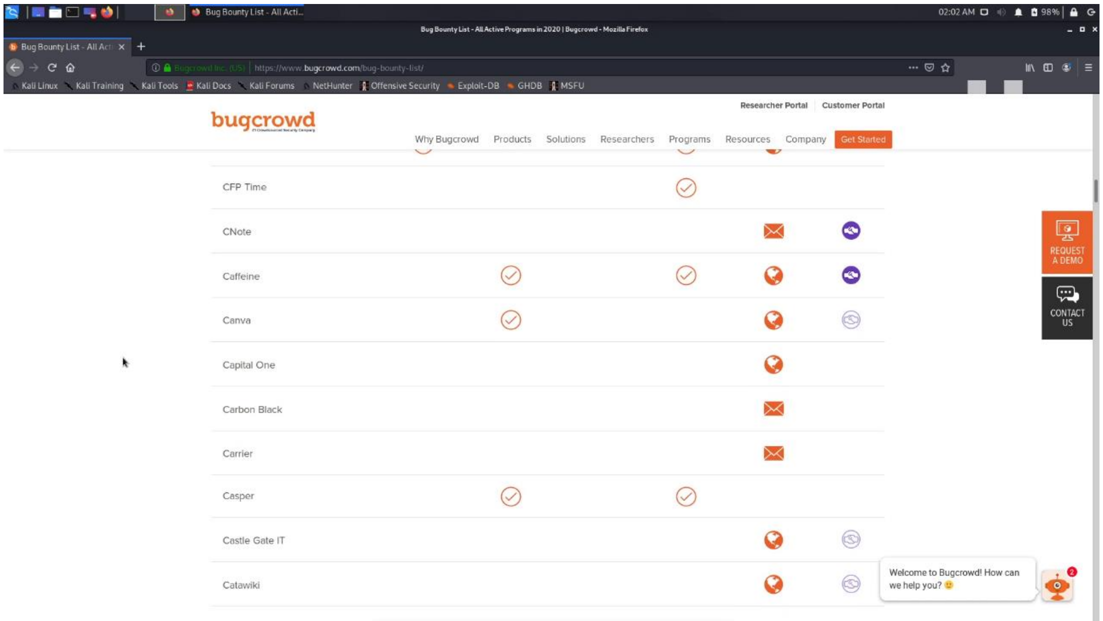
The most comprehensive, up to date crowdsourced list of bug bounty and security disclosure programs from across the web curated by the hacker community.

This list is maintained as part of the Disclose.io Safe Harbor project.

Have a suggestion for an addition, removal, or change? Open a Pull Request to disclose on Github. Special thanks to all contributors.

Program Name	New	Bug Bounty	Swag	Hall of Fame	Submission URL	Safeharbor

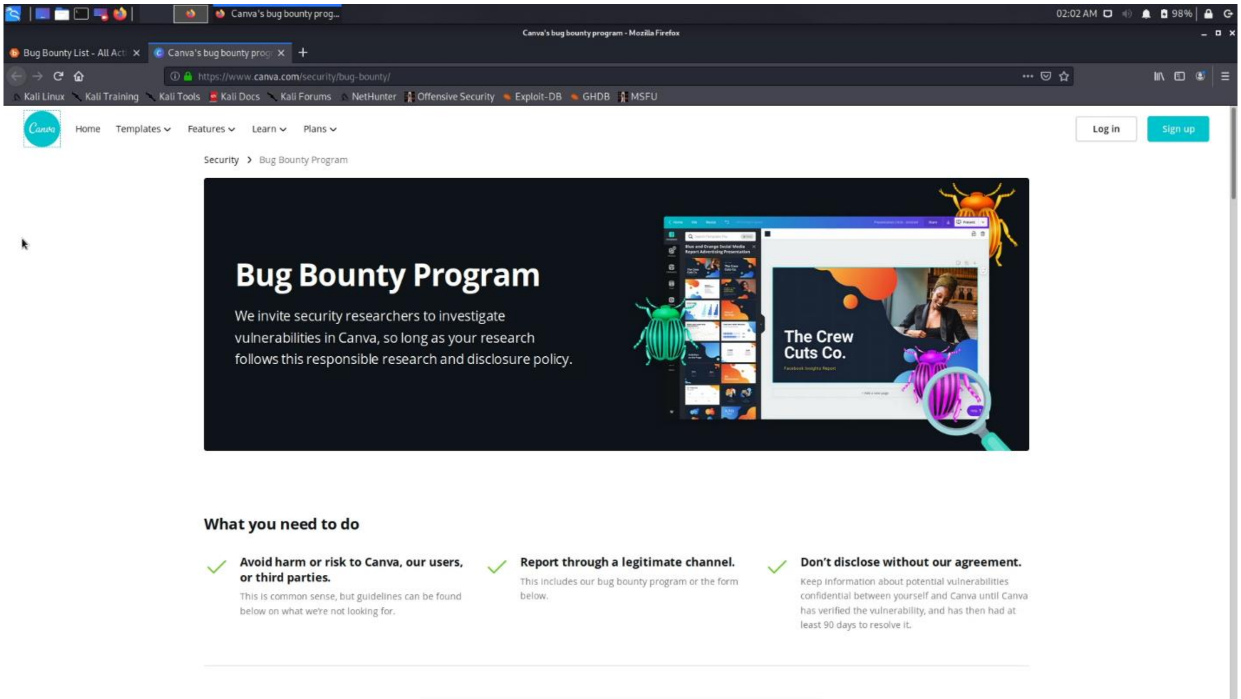
Figure 01: The Bugcrowd platform


Bug Bounty List - All Acti...
02:02 AM 98%
Bug Bounty List - All Active Programs in 2020 | Bugcrowd - Mozilla Firefox
Bug Bounty List - All Acti
Bugcrowd Inc. (US) https://www.bugcrowd.com/bug-bounty-list/
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
Researcher Portal
Customer Portal
bugcrowd
Why Bugcrowd
Products
Solutions
Researchers
Programs
Resources
Company
Get Started
REQUEST A DEMO
CONTACT US
Welcome to Bugcrowd! How can we help you? 🙂

CFP Time				✓		
CNote					✉	●
Caffeine		✓		✓	🌐	●
Canva		✓			🌐	○
Capital One					🌐	
Carbon Black					✉	
Carrier					✉	
Casper		✓		✓		
Castle Gate IT					🌐	○
Catawiki					🌐	○

Figure 02: Choosing canva.com

- In their bug bounty program, “canva.com” has given us some conditions.



Bug Bounty Program

We invite security researchers to investigate vulnerabilities in Canva, so long as your research follows this responsible research and disclosure policy.

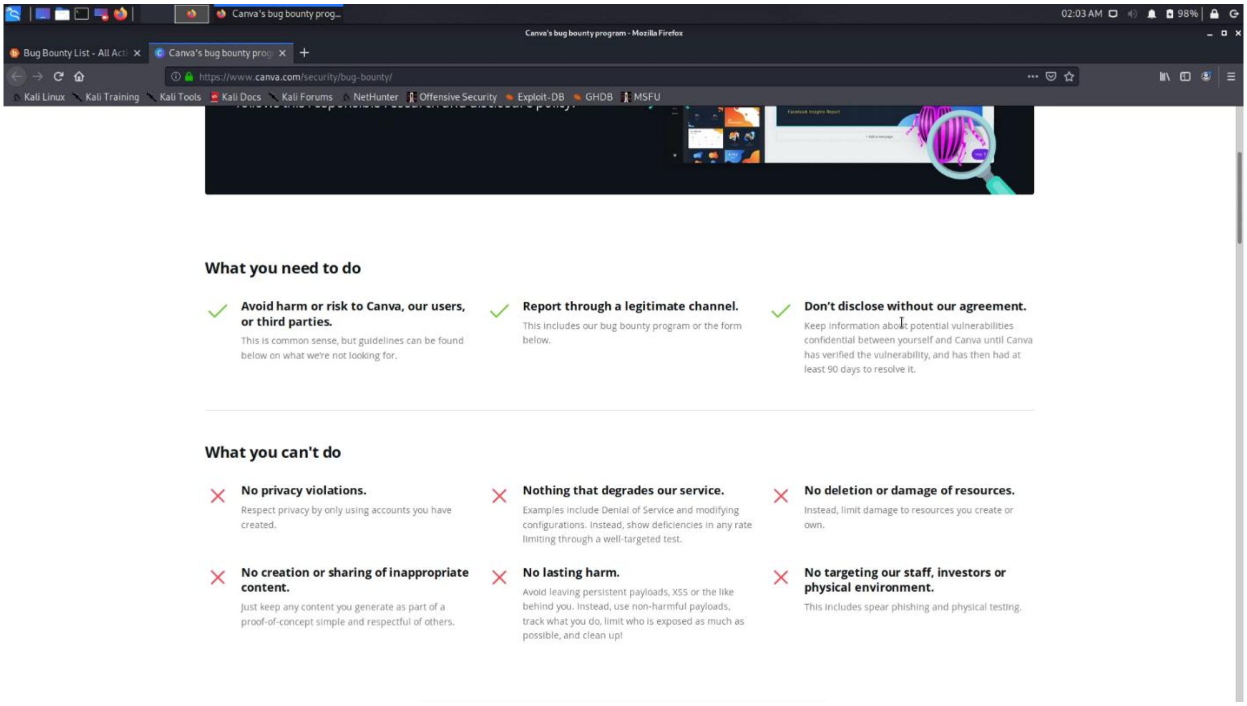
What you need to do

✓ 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.

Figure 03: canva.com bug bounty program



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 04: Conditions (scope & out of scope)

Conditions of the domain

- **Scope**
    - Avoid harm or risk to Canva, our users, or third parties.
    - Report a legitimate channel.
    - Do not disclose our agreement.

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

3. Web Reconnaissance

The term reconnaissance is extracted from the military use, where it applies to a mission to collect information in enemy territory. Recognition is typically a preliminary phase in a computer security context towards a further attack aiming to compromise the target device. For instance, to discover some vulnerable ports, the attacker also uses port scanning. An intruder typically exploits known vulnerabilities of services connected with open ports that have been found after a port scan.

As active and passive, there are two main reconnaissance. Active and passive reconnaissance are also often referred to as passive attacks, somewhat confusingly, since they are merely searching for information rather than actively targeting the targets, as active attacks do.

For ethical hacking, both active and passive reconnaissance are often used, in which white hat hackers use attack methods to determine device flaws such that issues can be taken care of until a real attack falls victim to the device.

The most widely used tool to do reconnaissance of a website is vulnerability scanners. In addition, automated security audits, manual security audits, and professional safety audits are also common options.

Tools used to perform this web audit,

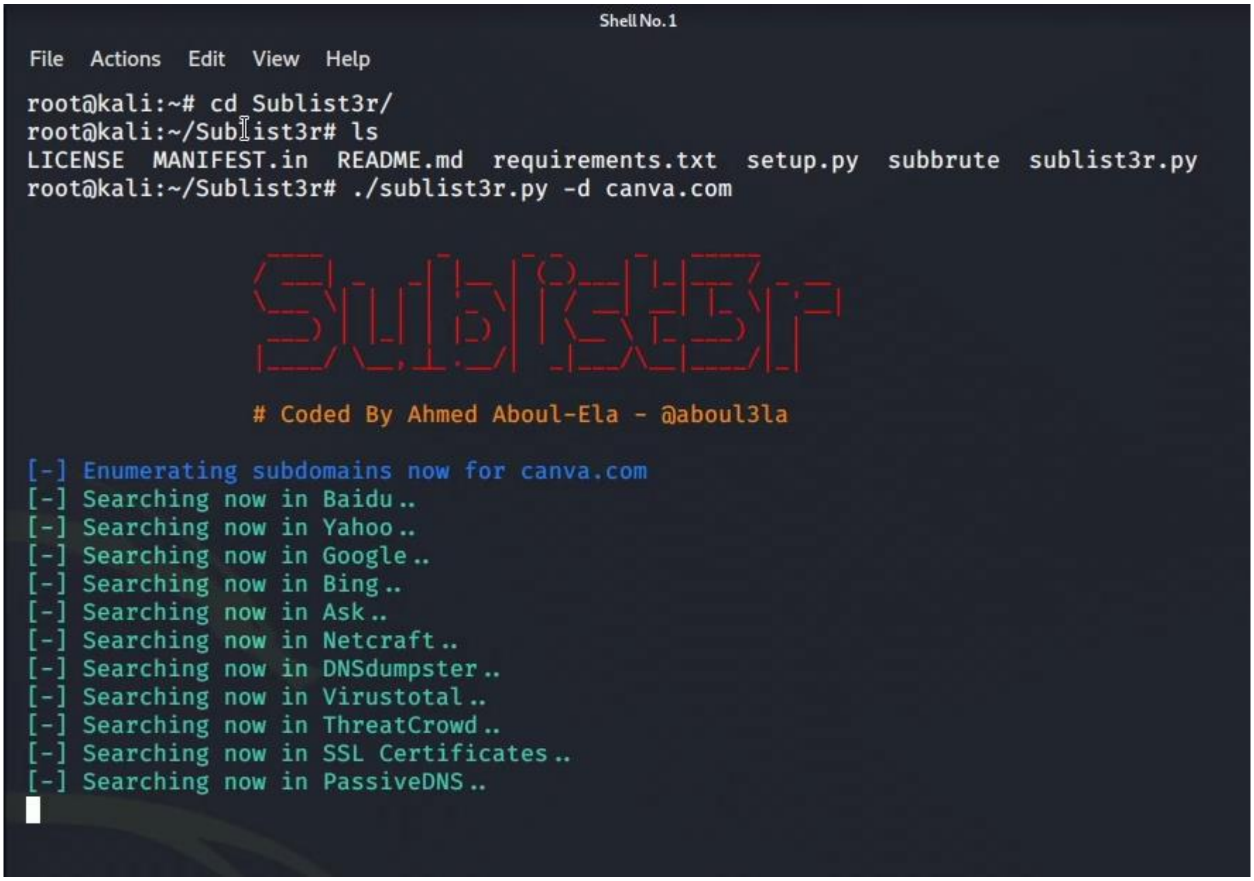
- Sublist3r
- Nmap
- Nikto
- Amass
- PwnXss
- Nessus
- Netsparker
- Burp Suite

3.1 Sublist3r

Sublist3r is a python application designed to use OSINT to enumerate subdomains of websites. It enables penetration testers and bug hunters to gather and collect subdomains for the domain they target. Using several search engines, such as Google, Yahoo, Bing, Baidu, and Query, Sublist3r lists subdomains. Sublist3r also uses Netcraft, Virustotal, ThreatCrowd, DNSdumpster, and ReverseDNS to enumerate subdomains.

- I have run Sublist3r and gather the subdomains of my main domain “canva.com” and I found 122 subdomains of “canva.com”.
- Command to run Sublist3r,

./sublist3r.py -d canva.com

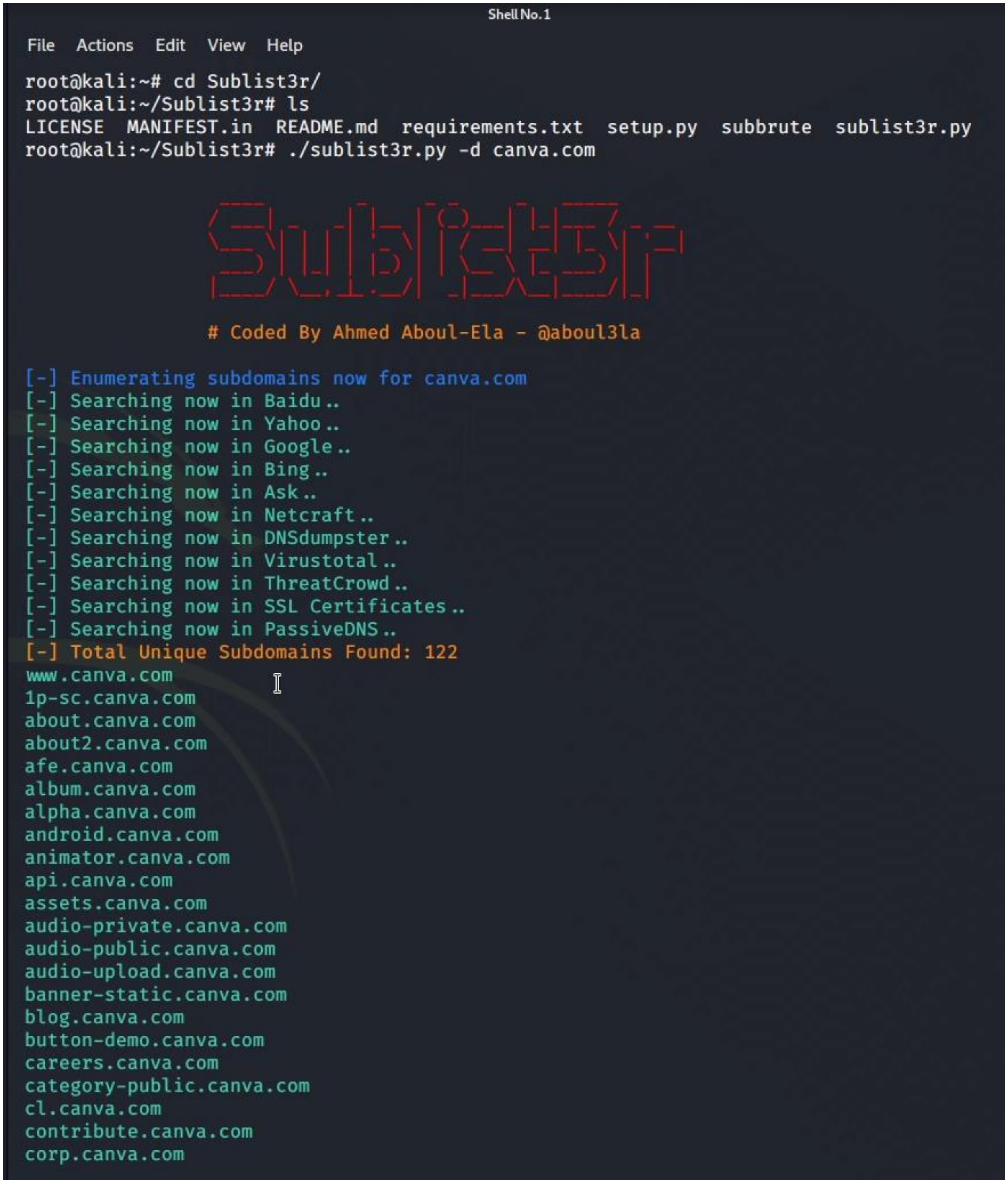


```
root@kali:~# cd Sublist3r/
root@kali:~/Sublist3r# ls
LICENSE  MANIFEST.in  README.md  requirements.txt  setup.py  subbrute  sublist3r.py
root@kali:~/Sublist3r# ./sublist3r.py -d canva.com

                 # 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..
```

Figure 05: Running Sublist3r



```
root@kali:~# cd Sublist3r/
root@kali:~/Sublist3r# ls
LICENSE  MANIFEST.in  README.md  requirements.txt  setup.py  subbrute  sublist3r.py
root@kali:~/Sublist3r# ./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
contribute.canva.com
corp.canva.com
```

Figure 06: Sublist3r Result (122 subdomains)

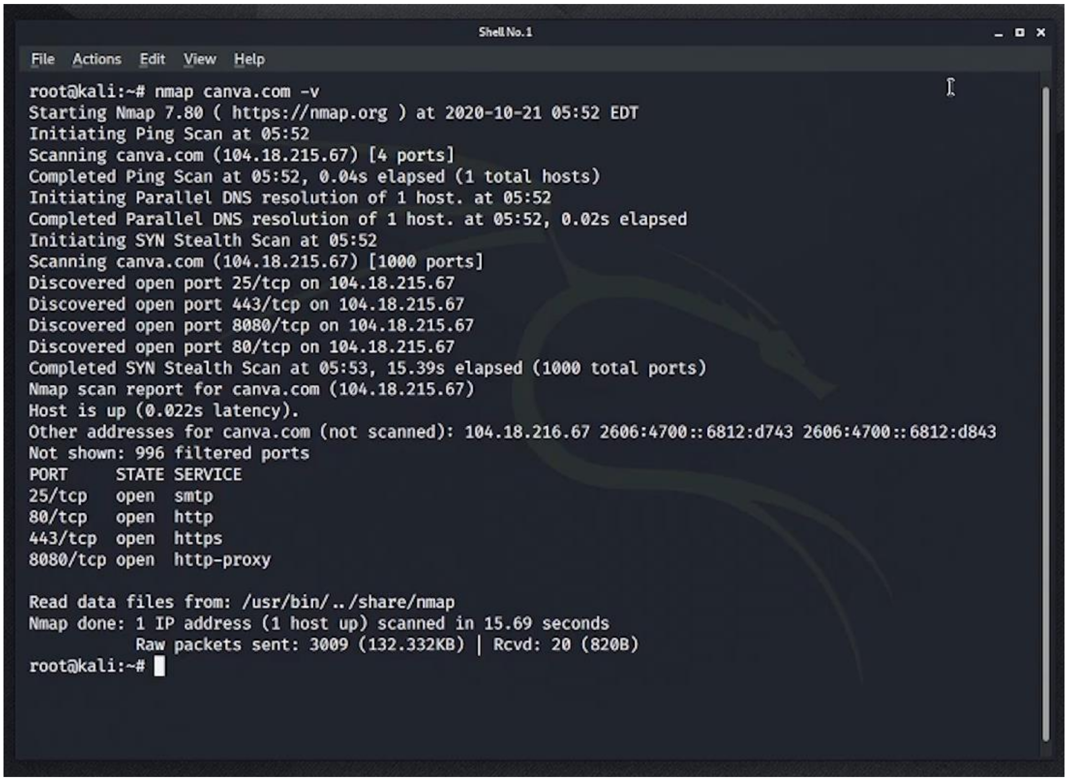
3.2 Nmap (Network Mapper)

Nmap is a free, open-source tool for vulnerability scanning and network discovery, short for Network Mapper. Network administrators use Nmap to assess which devices are operating on their networks, to classify available hosts and facilities, to locate open ports and to detect security risks. Nmap can be used to monitor single hosts, as well as large networks spanning hundreds of thousands of devices and subnet multitudes. Although Nmap has developed over the years and is highly versatile, it is a port-scan tool at its heart, collecting data by sending raw packets to device ports. It listens for answers and decides whether ports are open, closed or filtered by, for example, a firewall in some way. Port discovery or enumeration requires other terminology used for port scanning.

- I have run Nmap and got the IP address of the domain and found the open ports of the domain.
- Command to run Nmap,

  nmap canva.com -v

- IP address of the domain: **104.18.215.67**



```
root@kali:~# nmap canva.com -v
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-21 05:52 EDT
Initiating Ping Scan at 05:52
Scanning canva.com (104.18.215.67) [4 ports]
Completed Ping Scan at 05:52, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:52
Completed Parallel DNS resolution of 1 host. at 05:52, 0.02s elapsed
Initiating SYN Stealth Scan at 05:52
Scanning canva.com (104.18.215.67) [1000 ports]
Discovered open port 25/tcp on 104.18.215.67
Discovered open port 443/tcp on 104.18.215.67
Discovered open port 8080/tcp on 104.18.215.67
Discovered open port 80/tcp on 104.18.215.67
Completed SYN Stealth Scan at 05:53, 15.39s elapsed (1000 total ports)
Nmap scan report for canva.com (104.18.215.67)
Host is up (0.022s latency).
Other addresses for canva.com (not scanned): 104.18.216.67 2606:4700::6812:d743 2606:4700::6812:d843
Not shown: 996 filtered ports
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 15.69 seconds
           Raw packets sent: 3009 (132.332KB) | Rcvd: 20 (820B)
root@kali:~# 
```

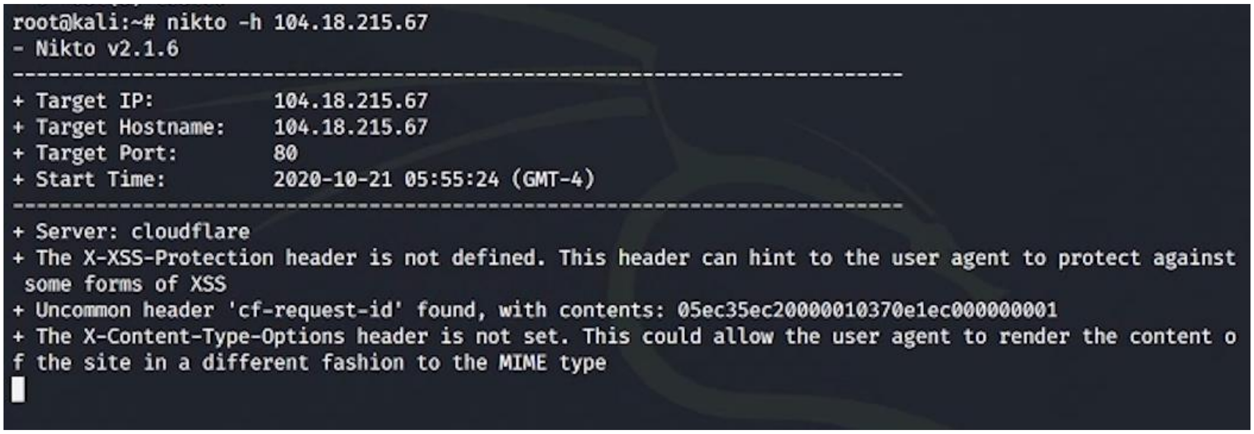
Figure 07: Nmap Result

3.3 Nikto

Nikto is an Open Source web server scanner that conducts extensive tests for various things against web servers, including over 6700 potentially unsafe files / programs, checks for obsolete versions of over 1250 servers, and over 270 servers for version-specific issues. It also tests for server configuration objects, such as multiple index files, options for the HTTP server, and attempts to recognize web servers and applications installed. Items and plugins for scanning are updated regularly and can be updated automatically. Nikto is not built to perform stealthy. Because of that firewalls can detect it.

- I have used Nikto to find vulnerable points of my domain.
- Command to run Nikto,

nikto -h 104.18.215.67



```
root@kali:~# nikto -h 104.18.215.67
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          104.18.215.67
+ Target Hostname:    104.18.215.67
+ Target Port:        80
+ Start Time:         2020-10-21 05:55:24 (GMT-4)
---------------------------------------------------------------------------
+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against
 some forms of XSS
+ Uncommon header 'cf-request-id' found, with contents: 05ec35ec20000010370e1ec000000001
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content o
f the site in a different fashion to the MIME type
█
```

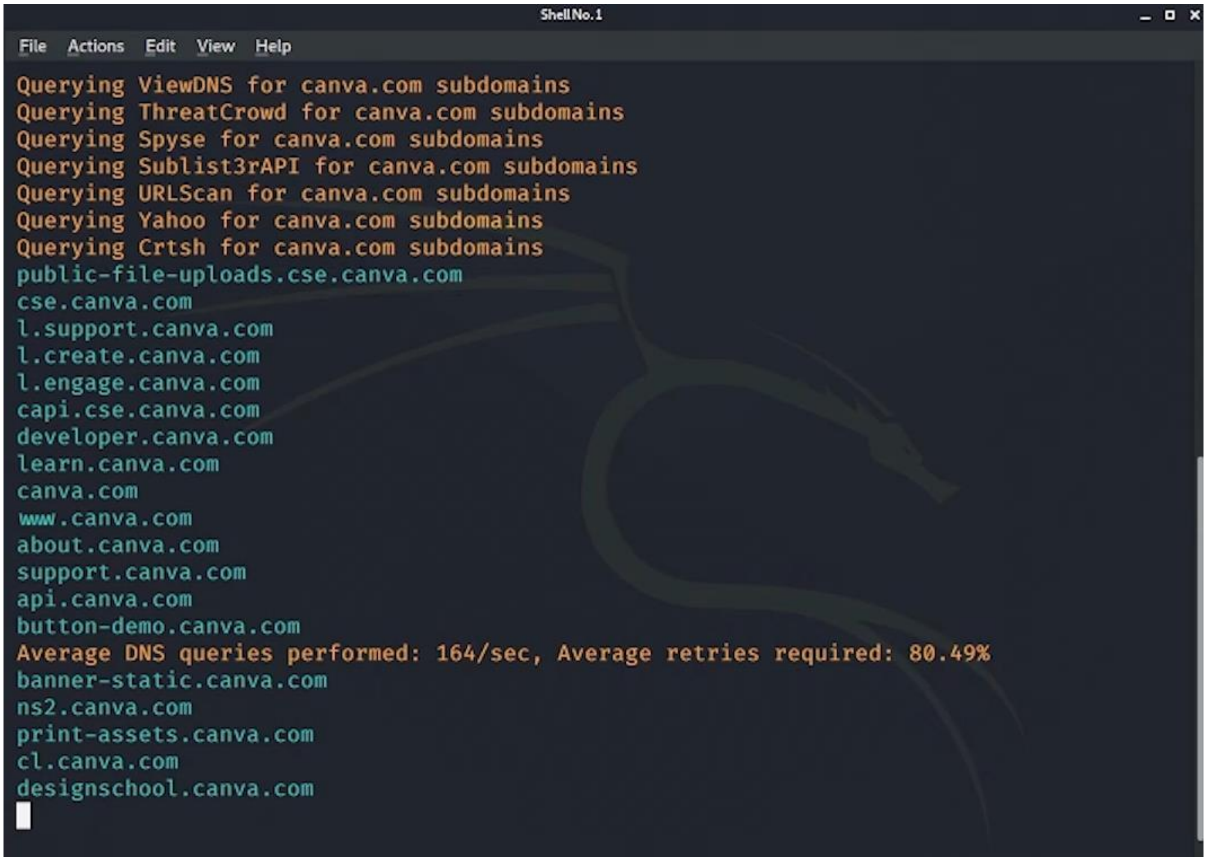
Figure 07: Nikto Result

3.4 Amass

Amass is a mapping and attack surface discovery platform for open source networks that uses information collection and other techniques to scrap all the available data, such as active reconnaissance and external asset discovery. It uses its own internal machinery to accomplish this, and it also integrates seamlessly with various external resources to maximize its results, productivity and strength. This instrument maintains a strong focus on the discovery and scrapping of DNS, HTTP and SSL / TLS data. It has its own strategies to do this and offers many integrations with various API services, such as the SecurityTrails API (spoiler alert!). It also uses various web archiving engines to scrape the bottom of the forgotten data deposits of the internet.

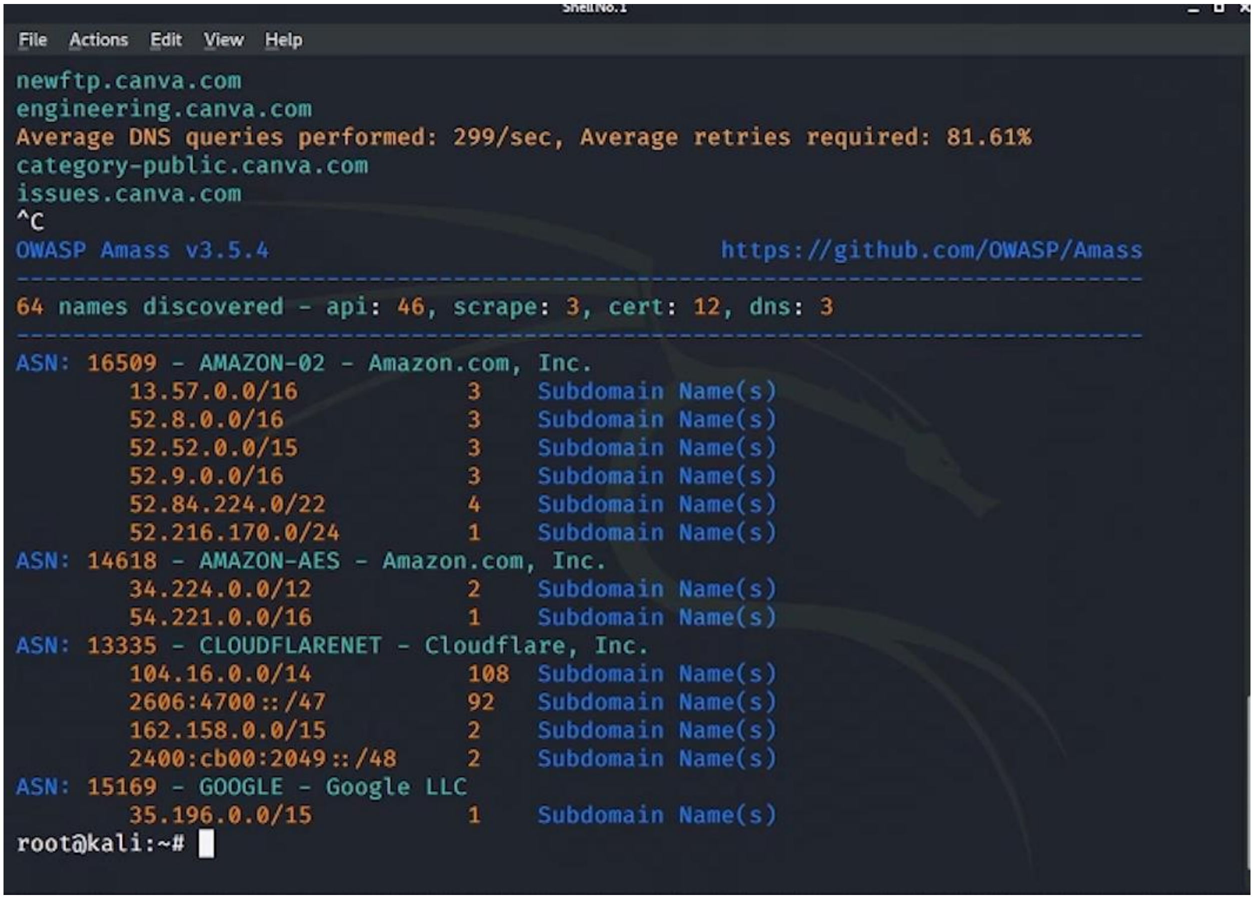
- Command to run Amass,

  amass enum -d canva.com



```
Querying ViewDNS for canva.com subdomains
Querying ThreatCrowd for canva.com subdomains
Querying Spyse for canva.com subdomains
Querying Sublist3rAPI for canva.com subdomains
Querying URLScan for canva.com subdomains
Querying Yahoo for canva.com subdomains
Querying Crtsh for canva.com subdomains
public-file-uploads.cse.canva.com
cse.canva.com
l.support.canva.com
l.create.canva.com
l.engage.canva.com
capi.cse.canva.com
developer.canva.com
learn.canva.com
canva.com
www.canva.com
about.canva.com
support.canva.com
api.canva.com
button-demo.canva.com
Average DNS queries performed: 164/sec, Average retries required: 80.49%
banner-static.canva.com
ns2.canva.com
print-assets.canva.com
cl.canva.com
designschool.canva.com
```

Figure 08: Amass while running



```
newftp.canva.com
engineering.canva.com
Average DNS queries performed: 299/sec, Average retries required: 81.61%
category-public.canva.com
issues.canva.com
^C
OWASP Amass v3.5.4                                 https://github.com/OWASP/Amass
--------------------------------------------------------------------------------
64 names discovered - api: 46, scrape: 3, cert: 12, dns: 3
--------------------------------------------------------------------------------
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
        13.57.0.0/16           3    Subdomain Name(s)
        52.8.0.0/16            3    Subdomain Name(s)
        52.52.0.0/15           3    Subdomain Name(s)
        52.9.0.0/16            3    Subdomain Name(s)
        52.84.224.0/22         4    Subdomain Name(s)
        52.216.170.0/24        1    Subdomain Name(s)
ASN: 14618 - AMAZON-AES - Amazon.com, Inc.
        34.224.0.0/12          2    Subdomain Name(s)
        54.221.0.0/16          1    Subdomain Name(s)
ASN: 13335 - CLOUDFLARENET - Cloudflare, Inc.
        104.16.0.0/14          108  Subdomain Name(s)
        2606:4700::/47         92   Subdomain Name(s)
        162.158.0.0/15         2    Subdomain Name(s)
        2400:cb00:2049::/48    2    Subdomain Name(s)
ASN: 15169 - GOOGLE - Google LLC
        35.196.0.0/15          1    Subdomain Name(s)
root@kali:~#
```

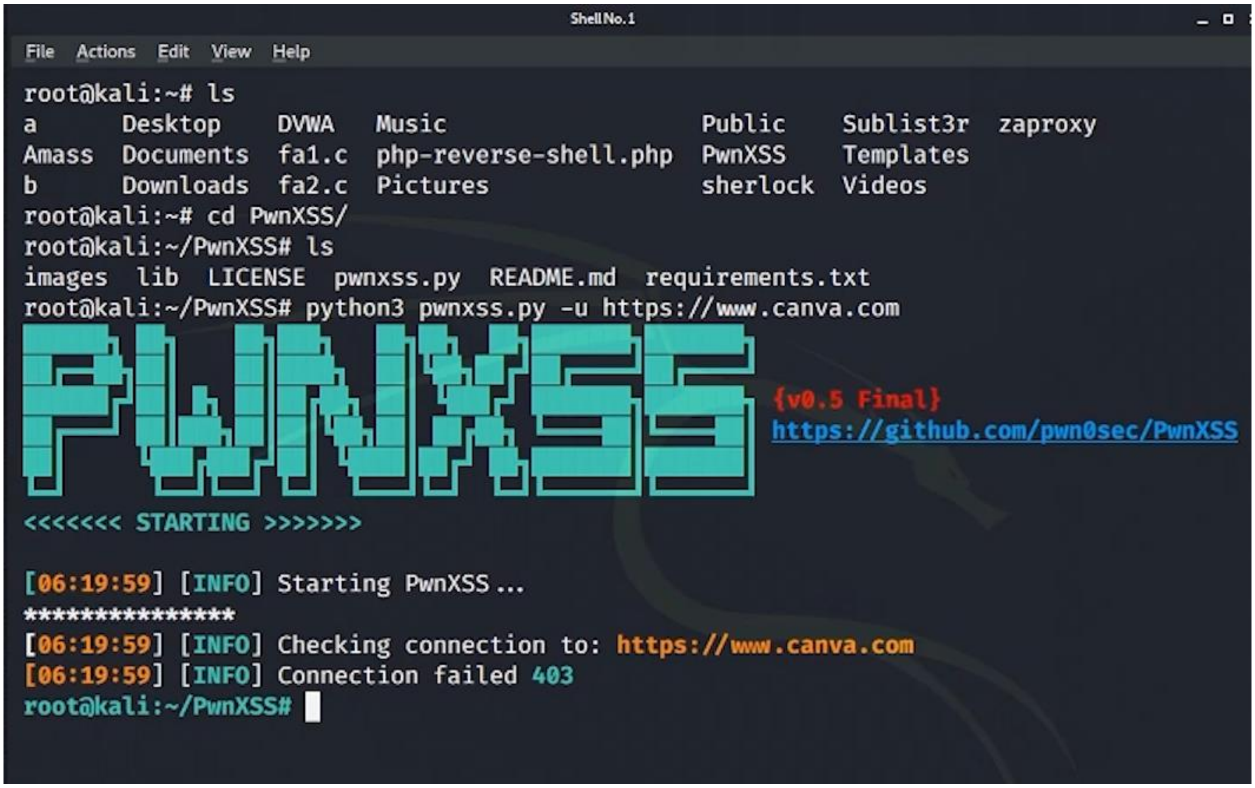
Figure 09: Amass Result

3.5 PwnXss

PwnXss is a XSS scanner made using python 3.7. It is a powerful scanner with many features like, crawling all links in a website, supporting of POST and GET forms, advanced error handling and multiprocessing support.

- I have run PwnXss but unfortunately could not get a proper result because my domain blocked XSS scanning.
- Command to run PwnXss,

python3 pwnxss.py -u https://www.canva.com



```
root@kali:~# ls
a      Desktop    DVWA   Music                  Public    Sublist3r  zaproxy
Amass  Documents  fa1.c  php-reverse-shell.php  PwnXSS    Templates
b      Downloads  fa2.c  Pictures               sherlock  Videos
root@kali:~# cd PwnXSS/
root@kali:~/PwnXSS# ls
images  lib  LICENSE  pwnxss.py  README.md  requirements.txt
root@kali:~/PwnXSS# python3 pwnxss.py -u https://www.canva.com
PWNXSS  {v0.5 Final}
        https://github.com/pwn0sec/PwnXSS

<<<<<<< STARTING >>>>>>>

[06:19:59] [INFO] Starting PwnXSS...
****************
[06:19:59] [INFO] Checking connection to: https://www.canva.com
[06:19:59] [INFO] Connection failed 403
root@kali:~/PwnXSS#
```

Figure 10: PwnXss Result

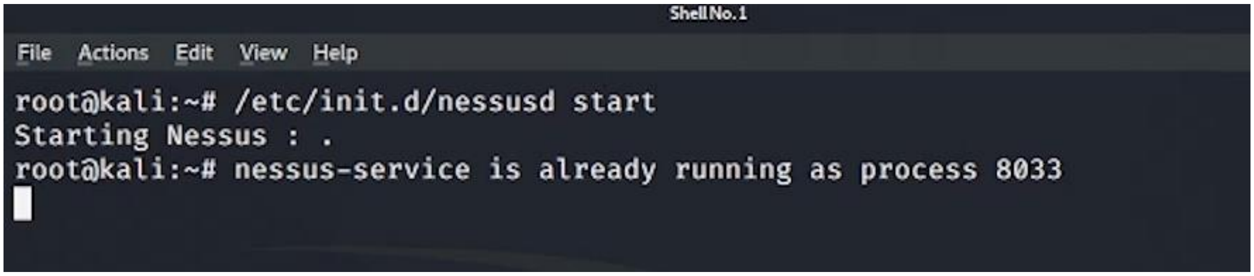
3.6 Nessus

Nessus is one of the many vulnerability scanners, including malicious attacks, used during vulnerability evaluations and penetration testing engagements. In order to detect vulnerabilities, Nessus conducts its scans by using plugins that run against each host on the network. Plugins can be thought of as individual pieces of code used by Nessus to perform individual types of scans on targets. Plugins are varied and large in their capabilities.

- I have run Nessus and found some medium risk vulnerabilities in my domain.
- Command to run Nessus,

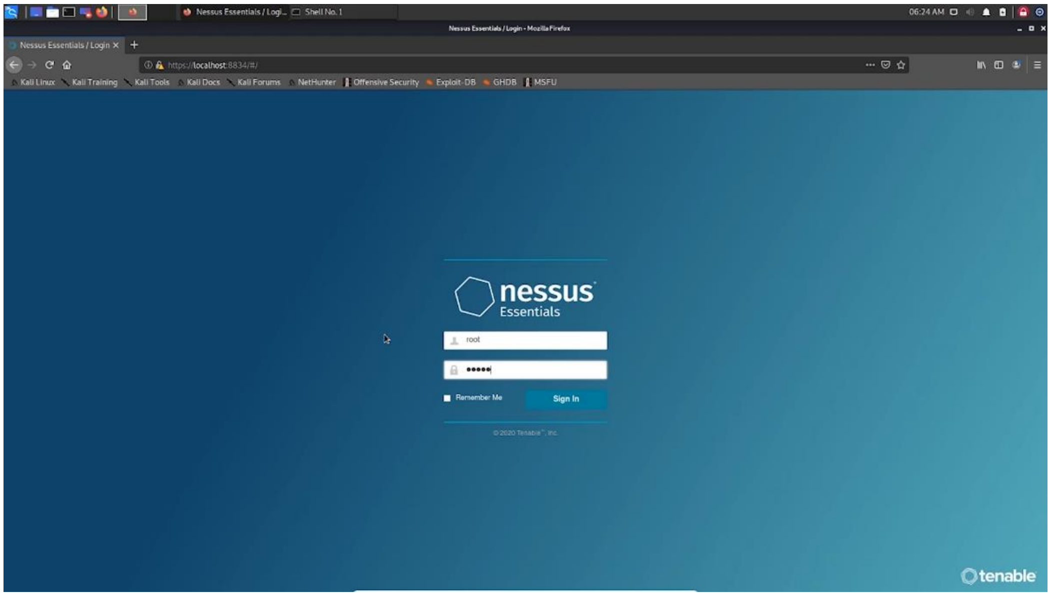
In terminal: **/etc/init.d/nessusd start**

In browser: **<u>https://localhost:8834</u>**



```
root@kali:~# /etc/init.d/nessusd start
Starting Nessus : .
root@kali:~# nessus-service is already running as process 8033
```

Figure 11: Executing Nessus in terminal



https://localhost:8834/#/

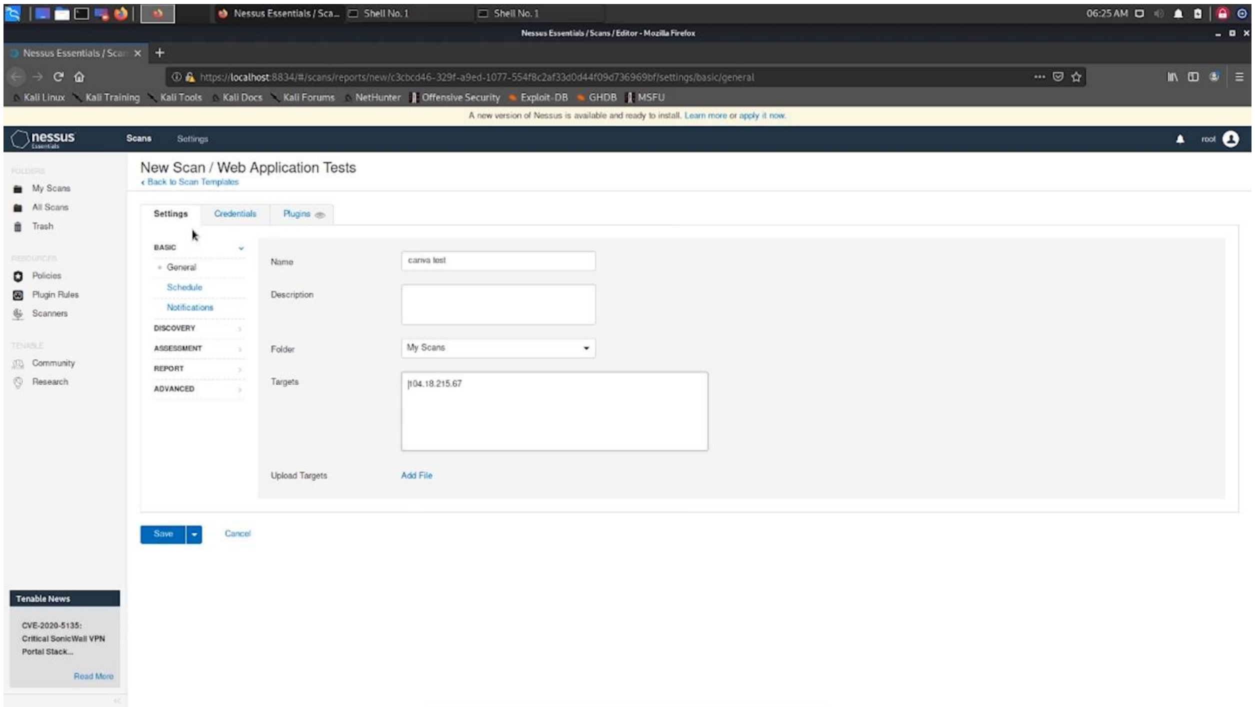
root

●●●●●

□ Remember Me

© 2020 Tenable™, Inc.

Figure 12: Login to Nessus



Nessus Essentials / Scans / Editor - Mozilla Firefox
https://localhost:8834/#/scans/reports/new/c3cbcd46-329f-a9ed-1077-554f8c2af33d0d44f09d736969bf/settings/basic/general
A new version of Nessus is available and ready to install. Learn more or apply it now.
nessus
Scans
Settings
My Scans
All Scans
Trash
Policies
Plugin Rules
Scanners
Community
Research
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Save
Cancel
Tenable News
CVE-2020-5135: Critical SonicWall VPN Portal Stack...
Read More

New Scan / Web Application Tests

‹ Back to Scan Templates

Name: canva test

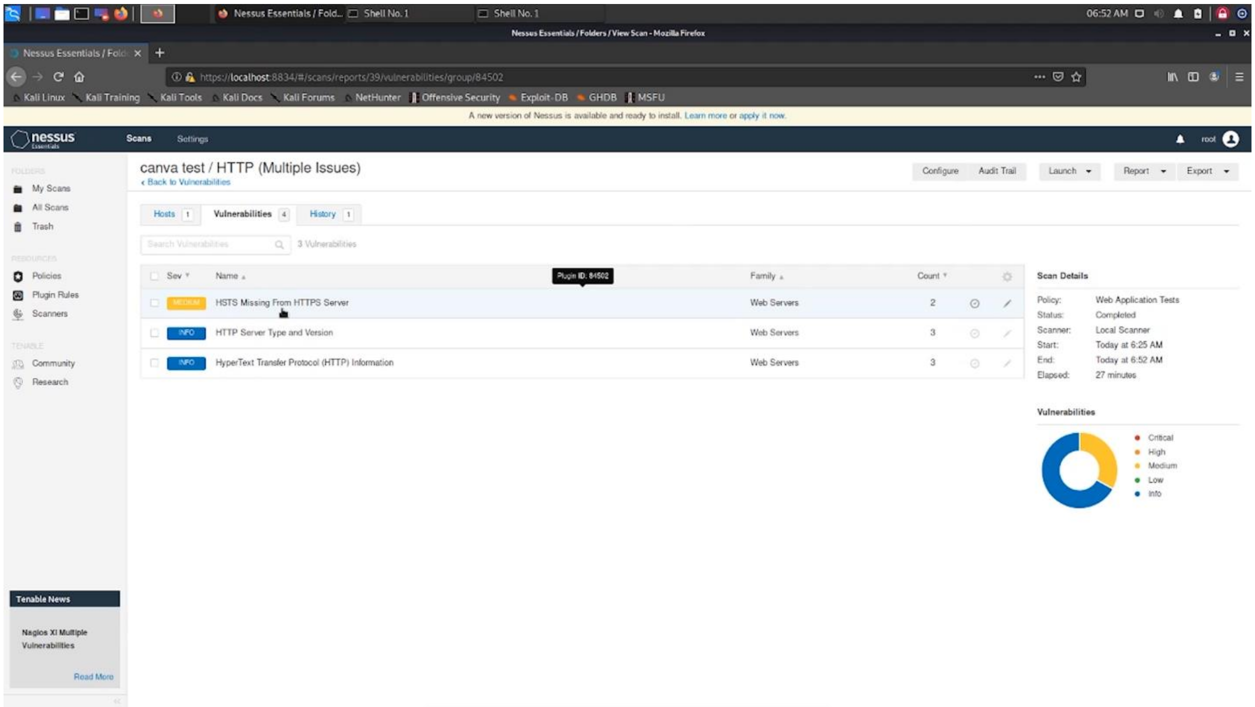
Description:

Folder: My Scans

Targets: 104.18.215.67

Upload Targets: Add File

Figure 13: Starting a new scan in Nessus by giving the domain IP



Nessus Essentials / Folders / View Scan - Mozilla Firefox
https://localhost:8834/#/scans/reports/39/vulnerabilities/group/84502
A new version of Nessus is available and ready to install. Learn more or apply it now.
nessus
Scans
Settings
root
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 4
History 1
Search Vulnerabilities
Plugin ID: 84502
My Scans
All Scans
Trash
Policies
Plugin Rules
Scanners
Community
Research
Critical
High
Medium
Low
Info
Tenable News
Nagios XI Multiple Vulnerabilities
Read More

canva test / HTTP (Multiple Issues)

‹ Back to Vulnerabilities

3 Vulnerabilities

Sev	Name	Family	Count
MEDIUM	HSTS Missing From HTTPS Server	Web Servers	2
INFO	HTTP Server Type and Version	Web Servers	3
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	3

Scan Details

Policy:	Web Application Tests
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 6:25 AM
End:	Today at 6:52 AM
Elapsed:	27 minutes

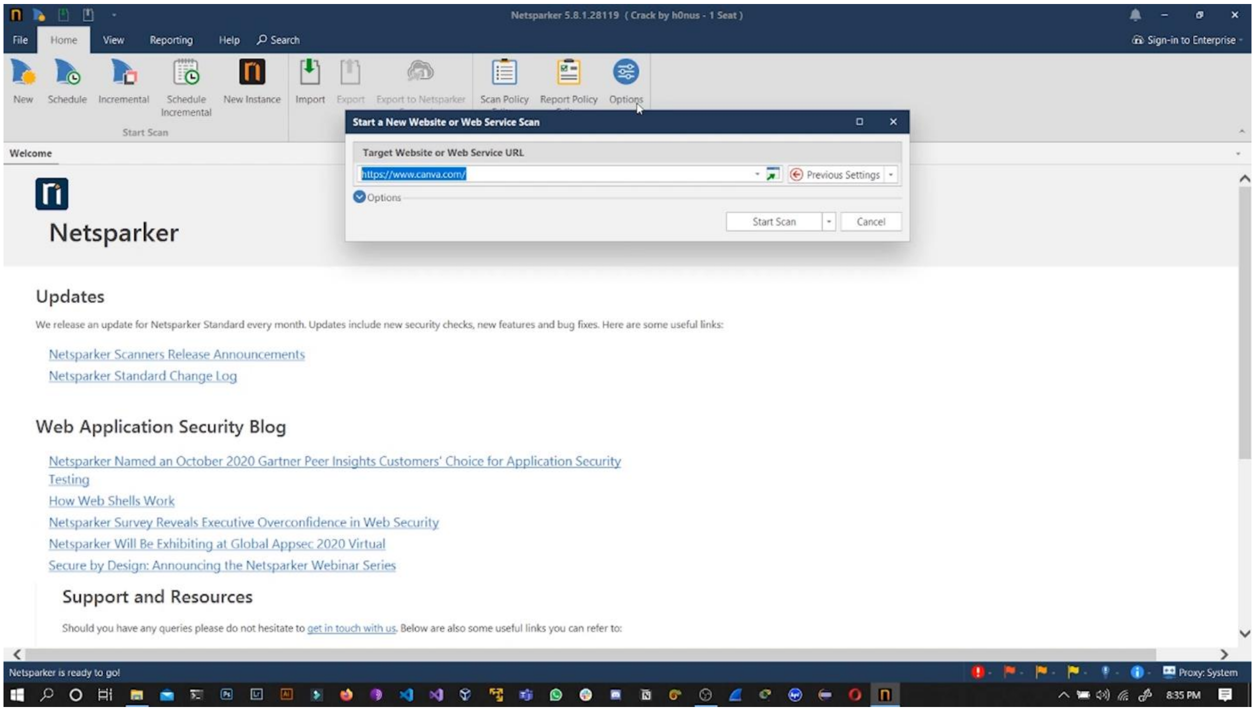
Vulnerabilities

Figure 14: Nessus scan report

3.7 Netsparker

Netsparker is an automatic, but completely configurable, security scanner for web applications that allows you to search websites, web applications and web services and detect security vulnerabilities. All kinds of web applications can be scanned by Netsparker, regardless of the platform or the language in which they are designed. In order to validate known problems, Netsparker is the only online web application security scanner that automatically exploits identified vulnerabilities in a read-only and secure manner. It also offers evidence of the weakness so that you do not have to spend time checking it manually. In the case of a detected SQL injection vulnerability, for example, the database name will be displayed as the exploit proof.

- I have run Netsparker but I could not get a result because of some problem occurred.



Start a New Website or Web Service Scan

Target Website or Web Service URL: https://www.canva.com/

Updates

We release an update for Netsparker Standard every month. Updates include new security checks, new features and bug fixes. Here are some useful links:

Netsparker Scanners Release Announcements
Netsparker Standard Change Log

Web Application Security Blog

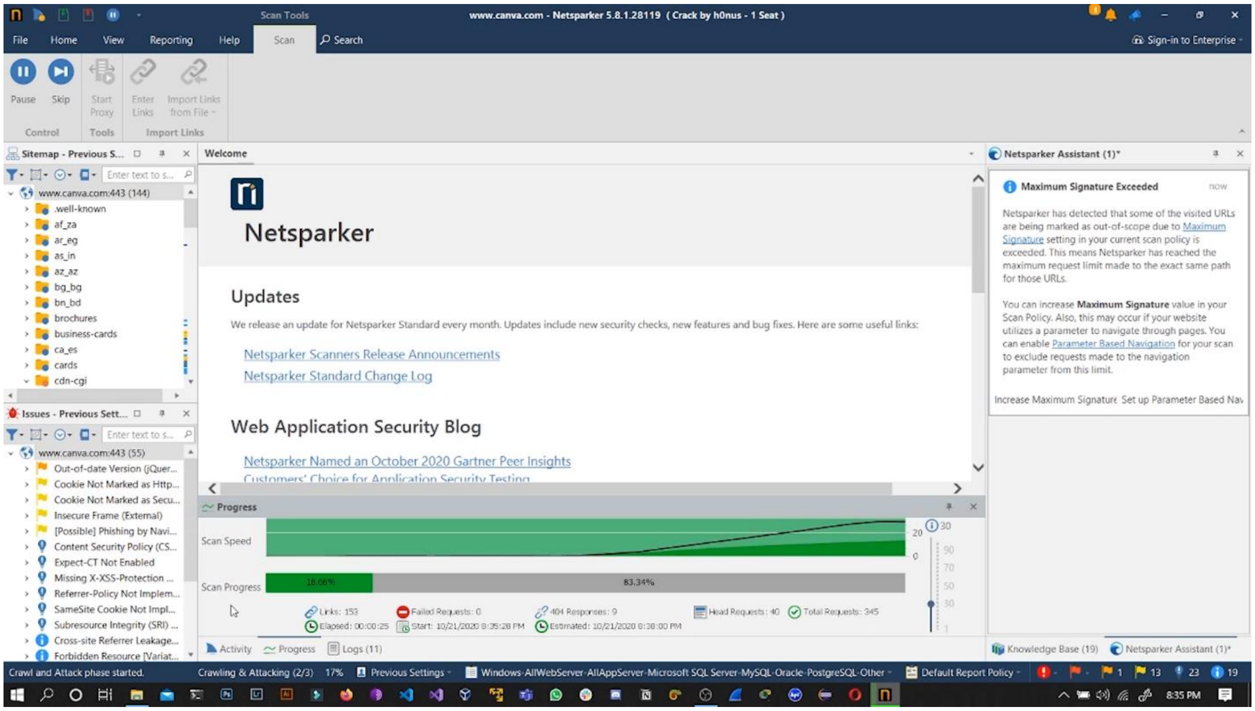
Netsparker Named an October 2020 Gartner Peer Insights Customers' Choice for Application Security Testing
How Web Shells Work
Netsparker Survey Reveals Executive Overconfidence in Web Security
Netsparker Will Be Exhibiting at Global Appsec 2020 Virtual
Secure by Design: Announcing the Netsparker Webinar Series

Support and Resources

Should you have any queries please do not hesitate to get in touch with us. Below are also some useful links you can refer to:

Netsparker is ready to go!

Figure 15: Giving the domain URL to Netsparker



www.canva.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)

Netsparker

Updates

We release an update for Netsparker Standard every month. Updates include new security checks, new features and bug fixes. Here are some useful links:

Netsparker Scanners Release Announcements

Netsparker Standard Change Log

Web Application Security Blog

Netsparker Named an October 2020 Gartner Peer Insights Customers' Choice for Application Security Testing

Netsparker Assistant (1)*

Maximum Signature Exceeded now

Netsparker has detected that some of the visited URLs are being marked as out-of-scope due to Maximum Signature setting in your current scan policy is exceeded. This means Netsparker has reached the maximum request limit made to the exact same path for those URLs.

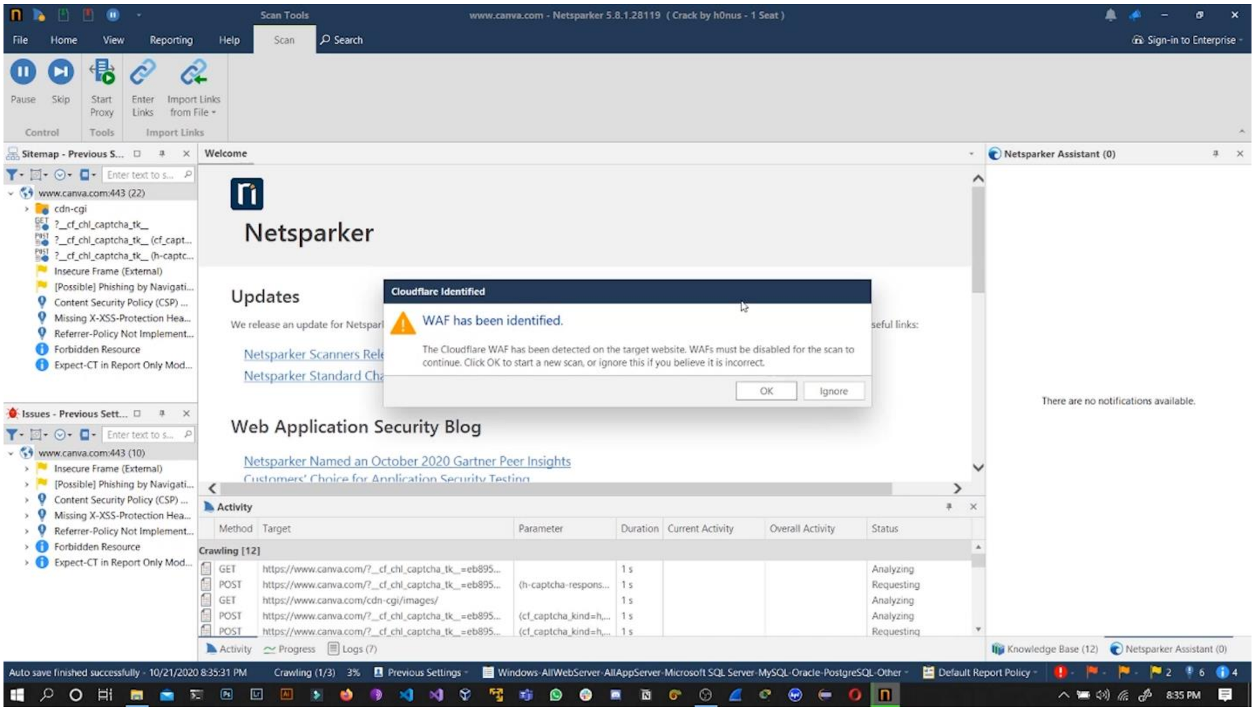
You can increase **Maximum Signature** value in your Scan Policy. Also, this may occur if your website utilizes a parameter to navigate through pages. You can enable Parameter Based Navigation for your scan to exclude requests made to the navigation parameter from this limit.

Increase Maximum Signature Set up Parameter Based Nav

Links: 153 Failed Requests: 0 404 Responses: 9 Head Requests: 40 Total Requests: 345
Elapsed: 00:00:25 Start: 10/21/2020 8:35:28 PM Estimated: 10/21/2020 8:38:00 PM

Crawl and Attack phase started. Crawling & Attacking (2/3) 17% Previous Settings Windows-AllWebServer-AllAppServer-Microsoft SQL Server-MySQL-Oracle-PostgreSQL-Other Default Report Policy

Figure 16: Netsparker while running



www.canva.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)

Cloudflare Identified

WAF has been identified.

The Cloudflare WAF has been detected on the target website. WAFs must be disabled for the scan to continue. Click OK to start a new scan, or ignore this if you believe it is incorrect.

OK Ignore

Netsparker Assistant (0)

There are no notifications available.

```
Method  Target                                         Parameter               Duration  Current Activity  Overall Activity  Status
Crawling [12]
GET     https://www.canva.com/?__cf_chl_captcha_tk__=eb895...                  1 s                                          Analyzing
POST    https://www.canva.com/?__cf_chl_captcha_tk__=eb895...  (h-captcha-respons...  1 s                                 Requesting
GET     https://www.canva.com/cdn-cgi/images/                                  1 s                                          Analyzing
POST    https://www.canva.com/?__cf_chl_captcha_tk__=eb895...  (cf_captcha_kind=h,...  1 s                                 Analyzing
POST    https://www.canva.com/?__cf_chl_captcha_tk__=eb895...  (cf_captcha_kind=h,...  1 s                                 Requesting
```

Auto save finished successfully - 10/21/2020 8:35:31 PM Crawling (1/3) 3% Previous Settings Windows-AllWebServer-AllAppServer-Microsoft SQL Server-MySQL-Oracle-PostgreSQL-Other Default Report Policy

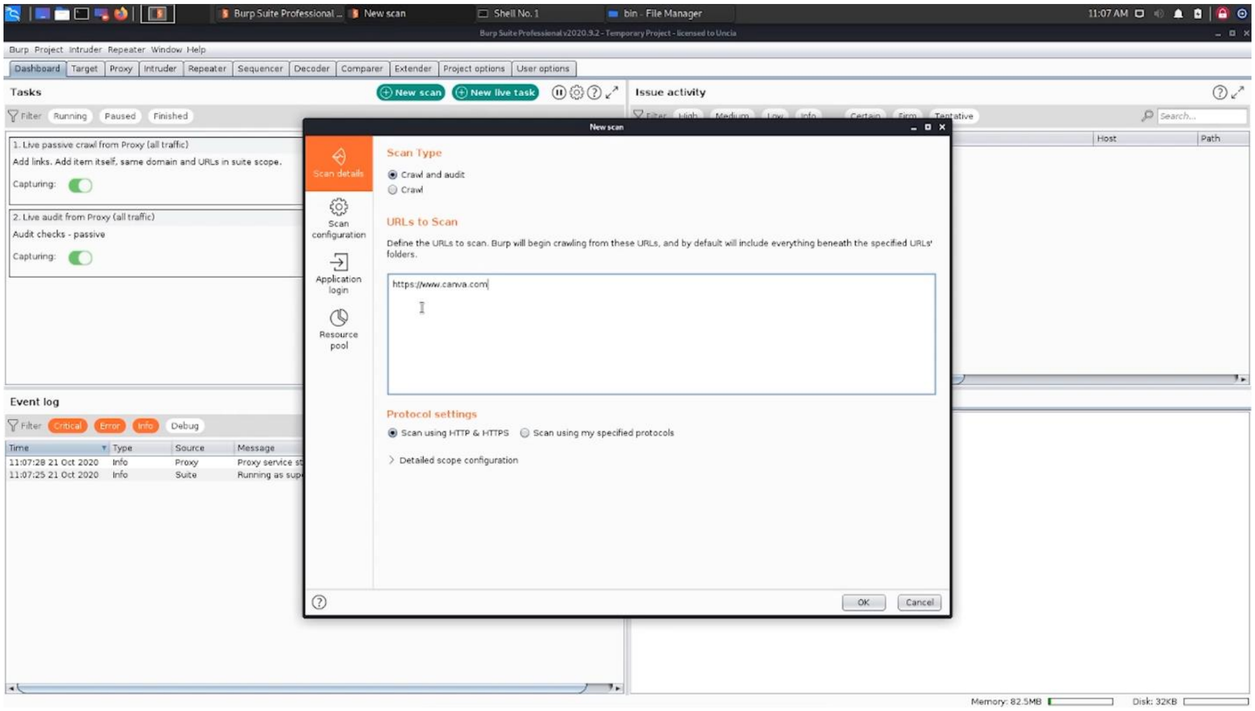
File
Home
View
Reporting
Help
Scan Tools
Scan
Search
Sign-in to Enterprise
Pause
Skip
Start Proxy
Enter Links
Import Links from File
Control
Tools
Import Links
Sitemap - Previous S...
Enter text to s...
www.canva.com:443 (22)
cdn-cgi
?__cf_chl_captcha_tk__
?__cf_chl_captcha_tk__ (cf_capt...
?__cf_chl_captcha_tk__ (h-captc...
Insecure Frame (External)
[Possible] Phishing by Navigati...
Content Security Policy (CSP) ...
Missing X-XSS-Protection Hea...
Referrer-Policy Not Implement...
Forbidden Resource
Expect-CT in Report Only Mod...
Issues - Previous Sett...
www.canva.com:443 (10)
Insecure Frame (External)
[Possible] Phishing by Navigati...
Content Security Policy (CSP) ...
Missing X-XSS-Protection Hea...
Referrer-Policy Not Implement...
Forbidden Resource
Expect-CT in Report Only Mod...
Welcome
Netsparker
Updates
We release an update for Netspar
Netsparker Scanners Rele
Netsparker Standard Cha
seful links:
Web Application Security Blog
Netsparker Named an October 2020 Gartner Peer Insights
Customers' Choice for Application Security Testing
Activity
Progress
Logs (7)
Knowledge Base (12)
Netsparker Assistant (0)
2
6
4
8:35 PM

Figure 17: The occurred problem

3.8 Burp Suite

Burp Suite is a platform for Web Penetration Testing based on Java. It has become an industry-standard set of instruments used by professionals in information security. Burp Suite allows you to recognize vulnerabilities and check vectors of attack that impact web apps. We have built this useful page as a compilation of Burp Suite knowledge and details due to its popularity and scope as well as depth of features. The Burp Suite can be classified as an Interception Proxy in its simplest form. A penetration tester may configure their internet browser to route traffic via the Burp Suite proxy server when browsing their target program. By capturing and analyzing of request to and from the target web application so that they can be evaluated, Burp Suite then acts as a Man In The Middle. In order to evaluate possible parameters or injection points, penetration testers may pause, manipulate and replay individual HTTP requests. To discover potentially unintended application behaviors, crashes and error messages, injection points can be defined for manual as well as automated fuzzing attacks.

- I have run Burp Suite, but I had to stop it in the middle because it took so long and until that I could not get any satisfying feedback.


Burp Suite Professional ...
New scan
Shell No. 1
bin - File Manager
11:07 AM
Burp Suite Professional v2020.9.2 - Temporary Project - licensed to Uncia
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Tasks
New scan
New live task
Filter Running Paused Finished
Issue activity
Filter High Medium Low Info Certain Firm Tentative
Search...
Host
Path
Event log
Filter Critical Error Info Debug
New scan
Scan details
Scan configuration
Application login
Resource pool
OK
Cancel
Memory: 82.5MB
Disk: 32KB

1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing:

2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing:

Time	Type	Source	Message
11:07:28 21 Oct 2020	Info	Proxy	Proxy service st
11:07:25 21 Oct 2020	Info	Suite	Running as sup

Scan Type

● Crawl and audit
○ Crawl

URLs to Scan

Define the URLs to scan. Burp will begin crawling from these URLs, and by default will include everything beneath the specified URLs' folders.

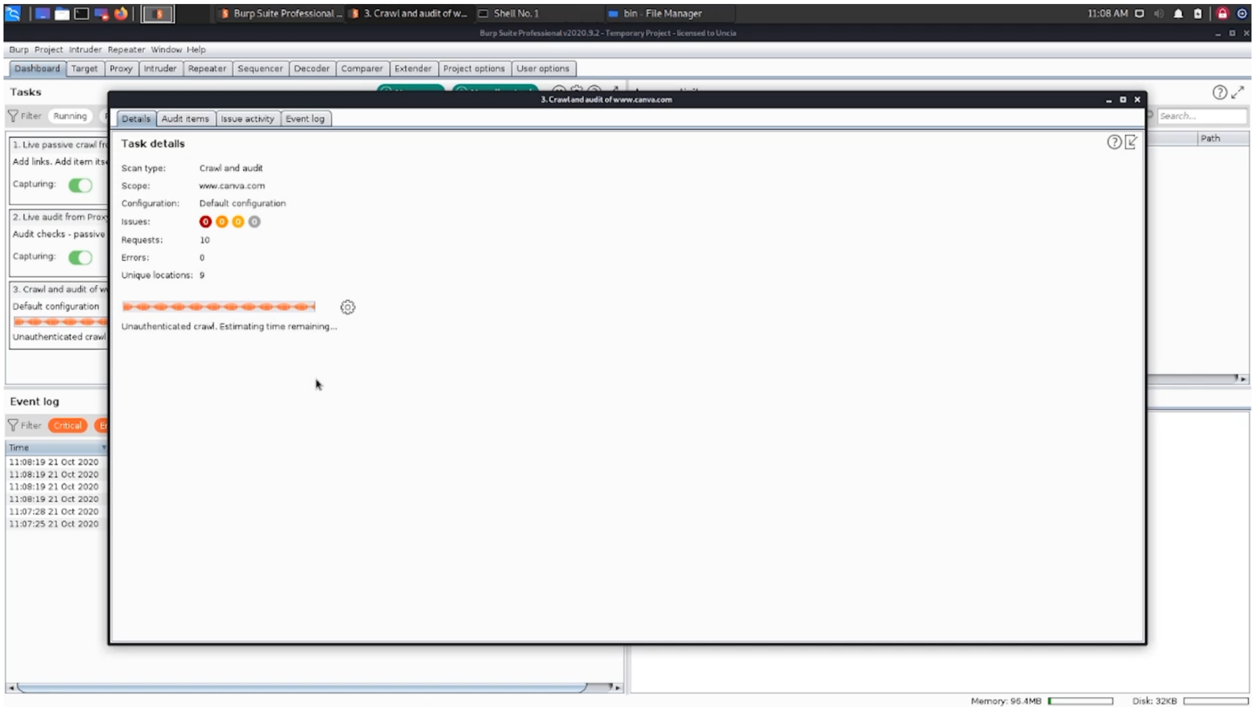
https://www.canva.com

Protocol settings

● Scan using HTTP & HTTPS ○ Scan using my specified protocols

> Detailed scope configuration

Figure 18: Giving the domain URL to Burp Suite


Burp Suite Professional ...
3. Crawl and audit of w...
Shell No. 1
bin - File Manager
11:08 AM
Burp Suite Professional v2020.9.2 - Temporary Project - licensed to Uncia
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Tasks
Filter Running
1. Live passive crawl fr
Add links. Add item its
Capturing:
2. Live audit from Prox
Audit checks - passive
Capturing:
3. Crawl and audit of w
Default configuration
Unauthenticated crawl
Event log
Filter Critical Er
Time
3. Crawl and audit of www.canva.com
Details Audit items Issue activity Event log
Search...
Path
Memory: 96.4MB
Disk: 32KB

Task details

Scan type: Crawl and audit
Scope: www.canva.com
Configuration: Default configuration
Issues: 0 0 0 0
Requests: 10
Errors: 0
Unique locations: 9

Unauthenticated crawl. Estimating time remaining...

```
Time
11:08:19 21 Oct 2020
11:08:19 21 Oct 2020
11:08:19 21 Oct 2020
11:08:19 21 Oct 2020
11:07:28 21 Oct 2020
11:07:25 21 Oct 2020
```

Figure 19: Burp Suite while running

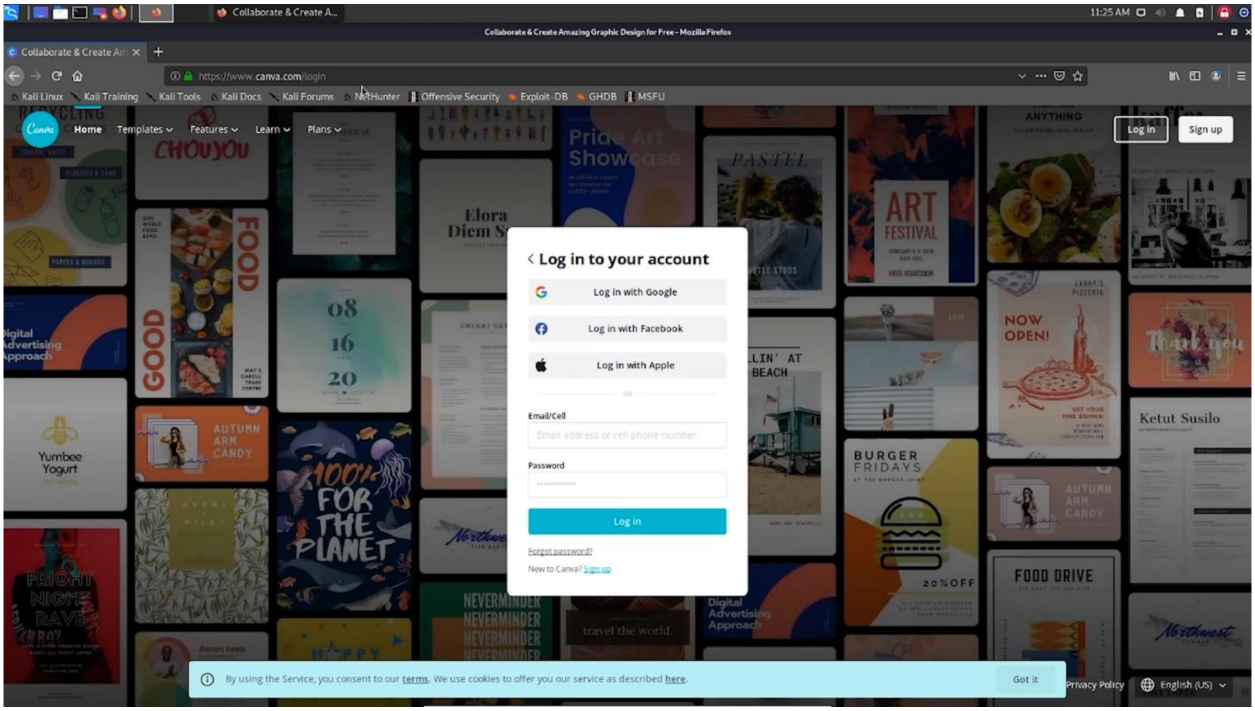
4. Exploitation

In order to find out the seriousness of each vulnerability, the next step in the website security audit is to exploit them. Exploits are operating upon vulnerabilities. Not all exploits, however, function on any weakness. However, it is well understood if any exploit may work on any vulnerability, but some verification needs to be performed to be sure and actually take advantage of it. Luckily, the framework makes this step really simple for you. You need to drag the exploit to exploit a vulnerability and drop it into the vulnerability you want to exploit.

In my web audit I could not find any critical vulnerabilities. However, I have done a Local File Inclusion (LFI) attack by trying to inject a php filter and get the encoded base64 configuration file of the domain's login page. Unfortunately, domain resist the injection and blocked me.

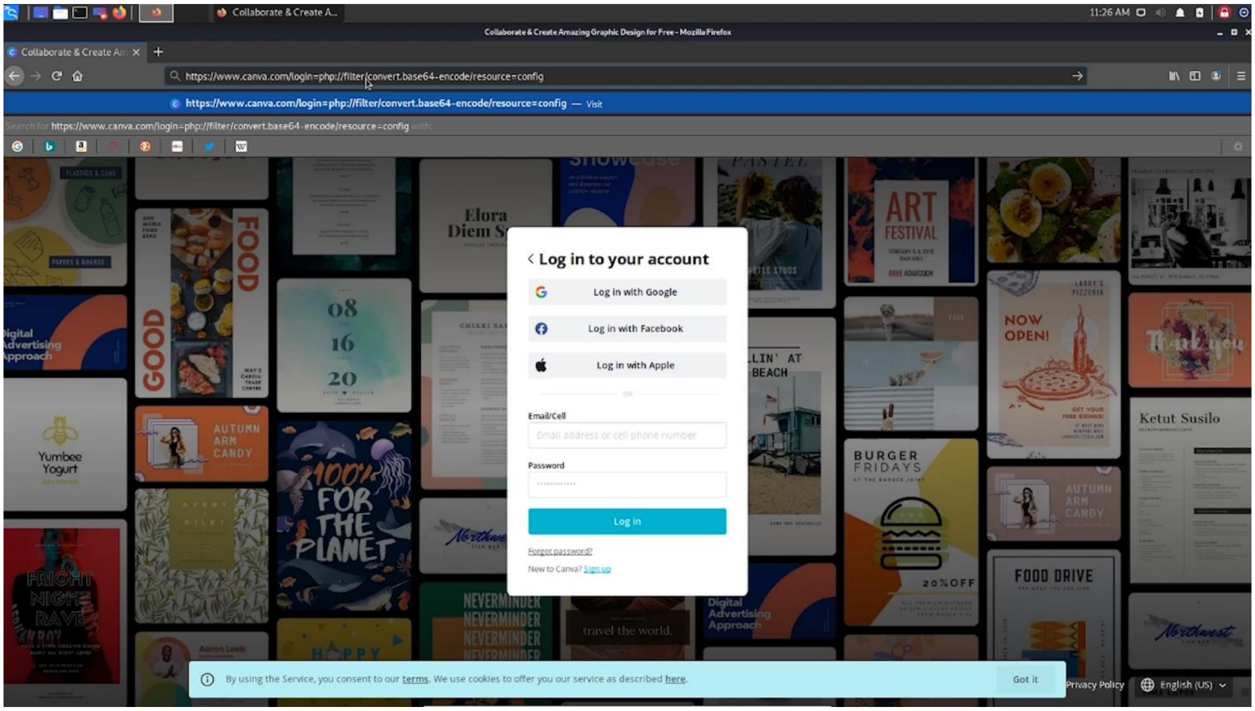
- Code I tried to inject,

=php://filter/convert.base64-encode/resource=config



By using the Service, you consent to our terms. We use cookies to offer you our service as described here. Got it

Figure 20: Domain's login page



Collaborate & Create A...
11:26 AM
Collaborate & Create Amazing Graphic Design for Free - Mozilla Firefox
Collaborate & Create Am
Visit
Search for
with:

```
https://www.canva.com/login=php://filter/convert.base64-encode/resource=config
```

Log in to your account

Log in with Google

Log in with Facebook

Log in with Apple

Email/Cell: Email address or cell phone number

Password: ············

Log in

Forgot password?

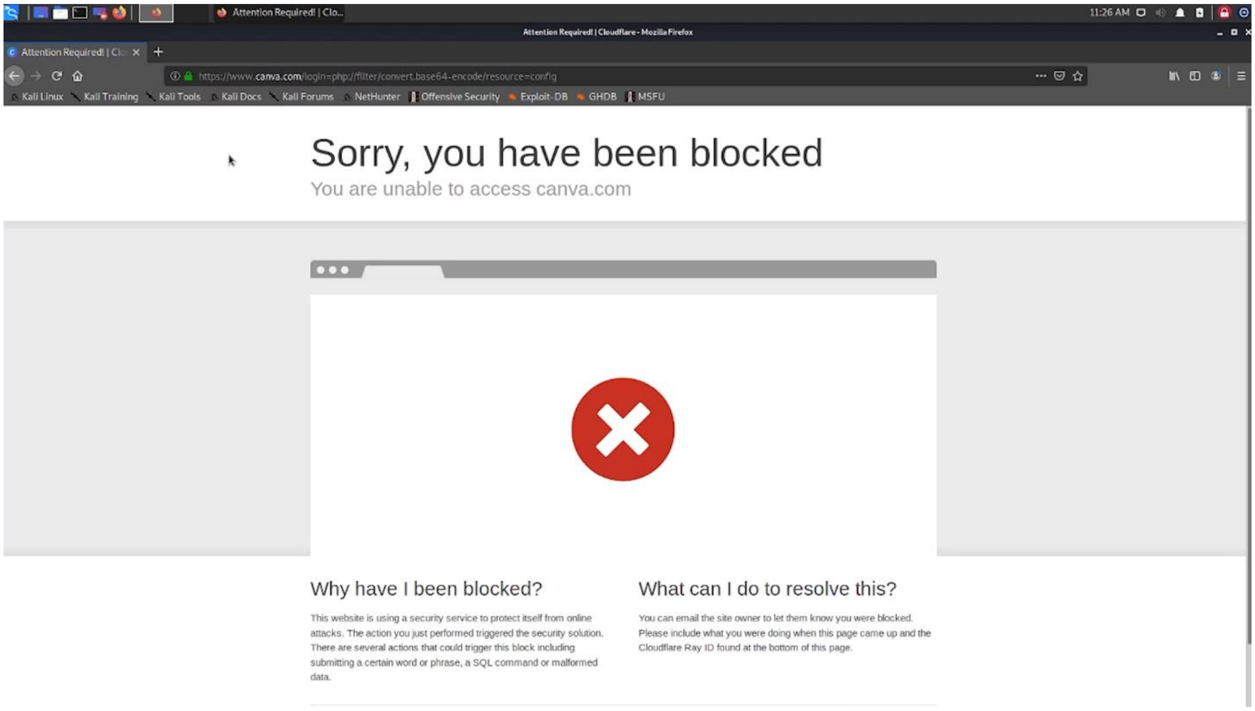
New to Canva? Sign up

By using the Service, you consent to our terms. We use cookies to offer you our service as described here.

Got it

Privacy Policy
English (US)

Figure 21: Injecting the code



```
https://www.canva.com/login=php://filter/convert.base64-encode/resource=config
```

Sorry, you have been blocked

You are unable to access canva.com

Why have I been blocked?

This website is using a security service to protect itself from online attacks. The action you just performed triggered the security solution. There are several actions that could trigger this block including submitting a certain word or phrase, a SQL command or malformed data.

What can I do to resolve this?

You can email the site owner to let them know you were blocked. Please include what you were doing when this page came up and the Cloudflare Ray ID found at the bottom of this page.

Figure 22: Blocked by the server

5. Conclusion

A systematic cyber security audit requires the assessment of security procedures, security measures and possible risks associated with all properties of information technology. While certain aspects of the audit must be conducted manually, the web risk assessment process can be partly automated by tools. By conducting vulnerability scans to identify known web vulnerabilities, it assesses the protection of your web properties. It also helps you recognize other problems with information security, such as flaws in access control, misconfigurations, or lack of certain security mechanisms.

In this web security audit, I have chosen canva.com from Bugcrowd bug bounty platform as my main domain and I have used several automated tools such as Nmap, Nikto, Nessus, Amass, PwnXss, Netsparker, Burp Suite, and Sublist3r to scan the domain and gather information. PwnXss, Netsparker and Burp Suite have not given a proper result. However, other tools have given pretty interesting findings, which are useful. I have done a exploitation by trying to injecting a php code to the domain's login page to get the encoded base 64 configuration file. Unfortunately, the server has blocked me.

After considering all this information, I came to a final decision that, the domain canva.com has a good cyber-attack defense system and it contains less vulnerabilities.

6. References

- "How to Use Nmap: Commands and Tutorial Guide | Varonis", Inside Out Security, 2020. [Online]. Available: https://www.varonis.com/blog/nmap-commands/. [Accessed: 22- Oct- 2020].
- "PHP Filter Functions", W3schools.com, 2020. [Online]. Available: https://www.w3schools.com/php/php_ref_filter.asp. [Accessed: 22- Oct- 2020].
- "pwn0sec/PwnXSS", GitHub, 2020. [Online]. Available: https://github.com/pwn0sec/PwnXSS. [Accessed: 22- Oct- 2020].
- "OWASP Top Ten Web Application Security Risks | OWASP", Owasp.org, 2020. [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed: 22- Oct- 2020].
- Sucuri.net, 2020. [Online]. Available: https://sucuri.net/guides/owasp-top-10-security-vulnerabilities-2020/. [Accessed: 22- Oct- 2020].
- "Bug Bounty List - All Active Programs in 2020 | Bugcrowd", Bugcrowd, 2020. [Online]. Available: https://www.bugcrowd.com/bug-bounty-list/. [Accessed: 22- Oct- 2020].
- 2020. [Online]. Available: https://www.canva.com/security/bug-bounty/. [Accessed: 22- Oct- 2020].