ASSIGNMENT - 4

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

> HTTP
> FTP
> POP

Sniffing : The process of capturing and analyzing the data packets which are passing through the network .Sniffers are used by network/system administrators to monitor and troubleshoot network traffic.Attackers use sniffers to capture data.

Here we need to identify the vulnerabilities of a website we use a tool called wireshark.

Wireshark : network protocol analyzer or an application that captures packets from a network connection.

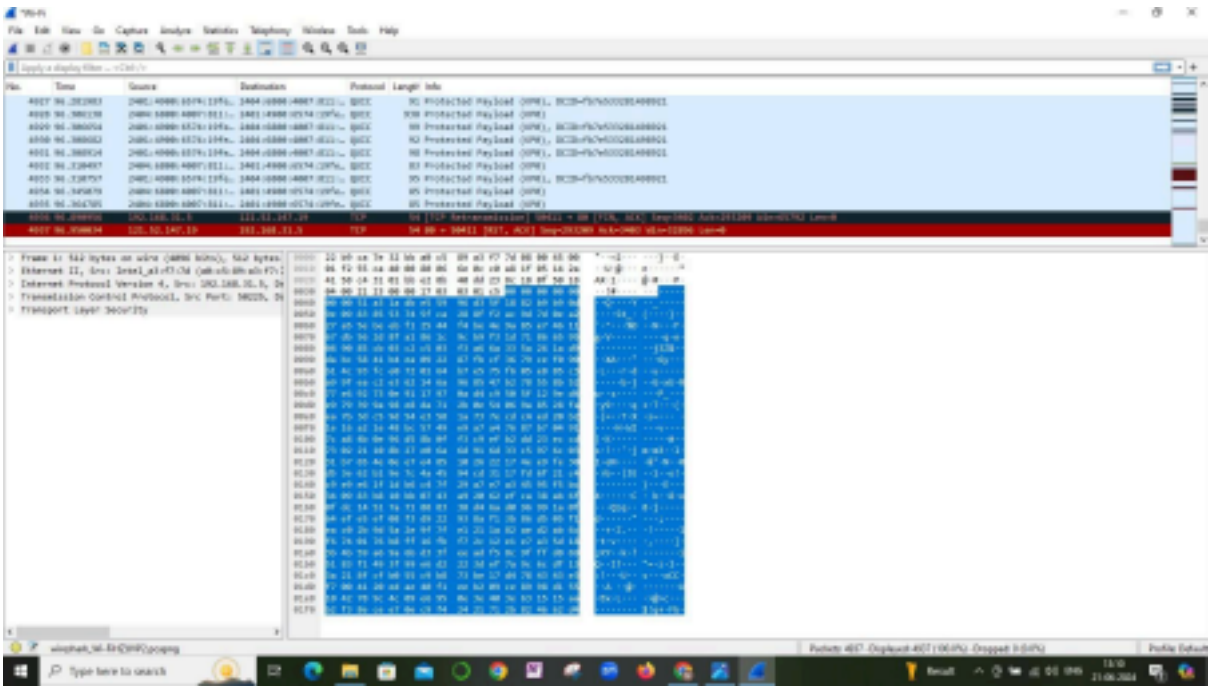
Here we need to website protocols

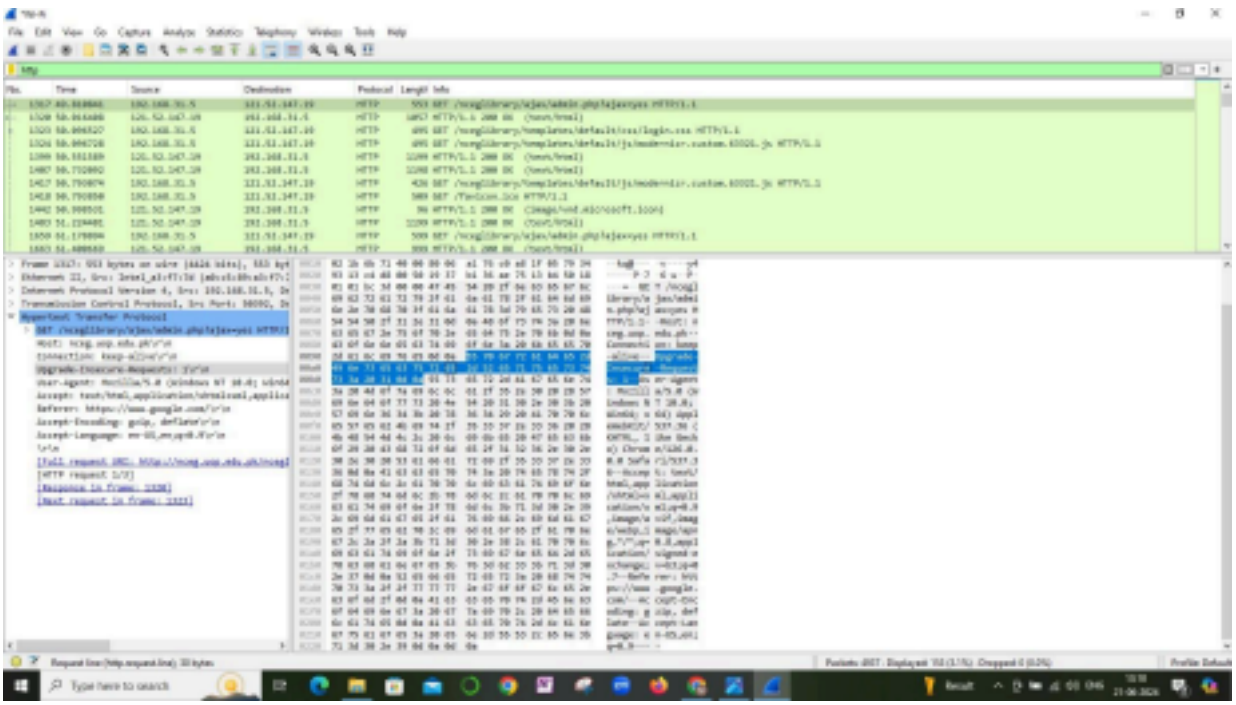
Http protocol : 81
FTP protocol : 20,21
Pop protocol : 110
Now find any website in google browser go to google . and search any website which is having vulnerabilities .

> HTTP

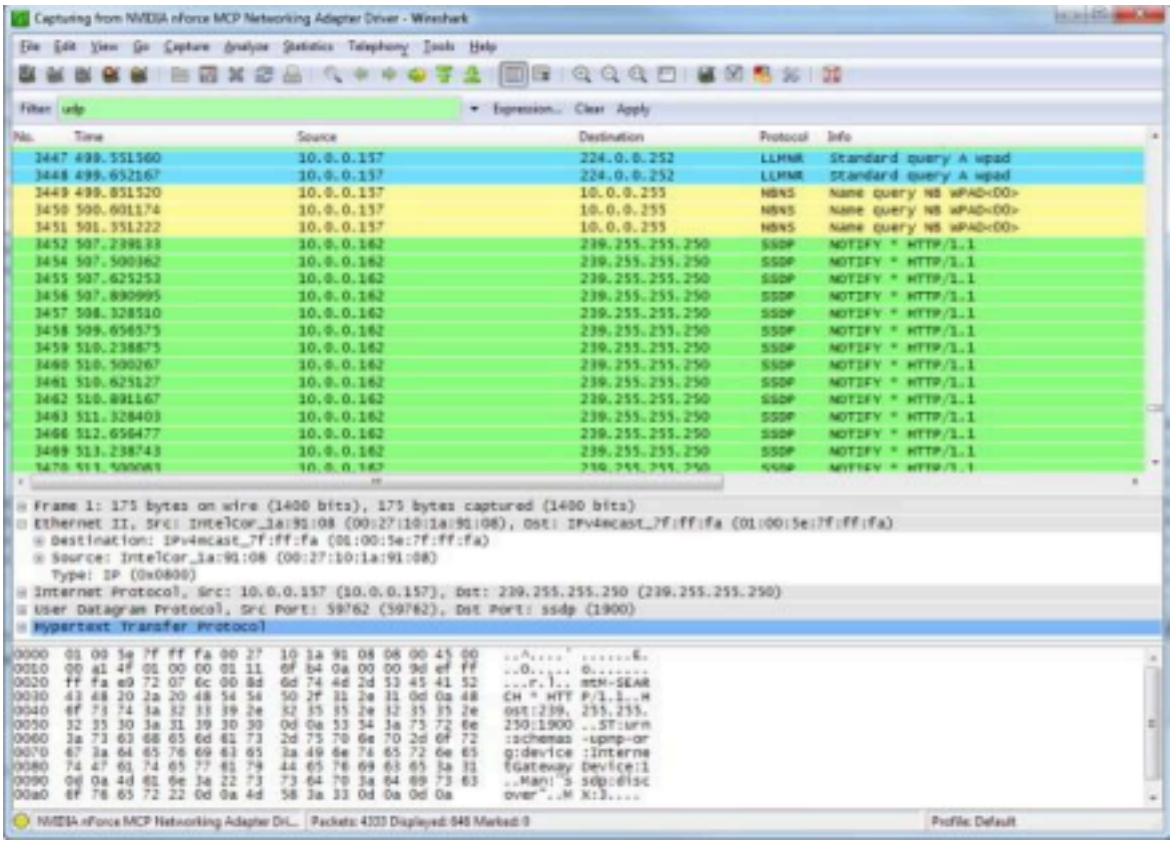
Step 1 : Start your wireshark tool

Step 2: Open browser and search for the websites Which are having

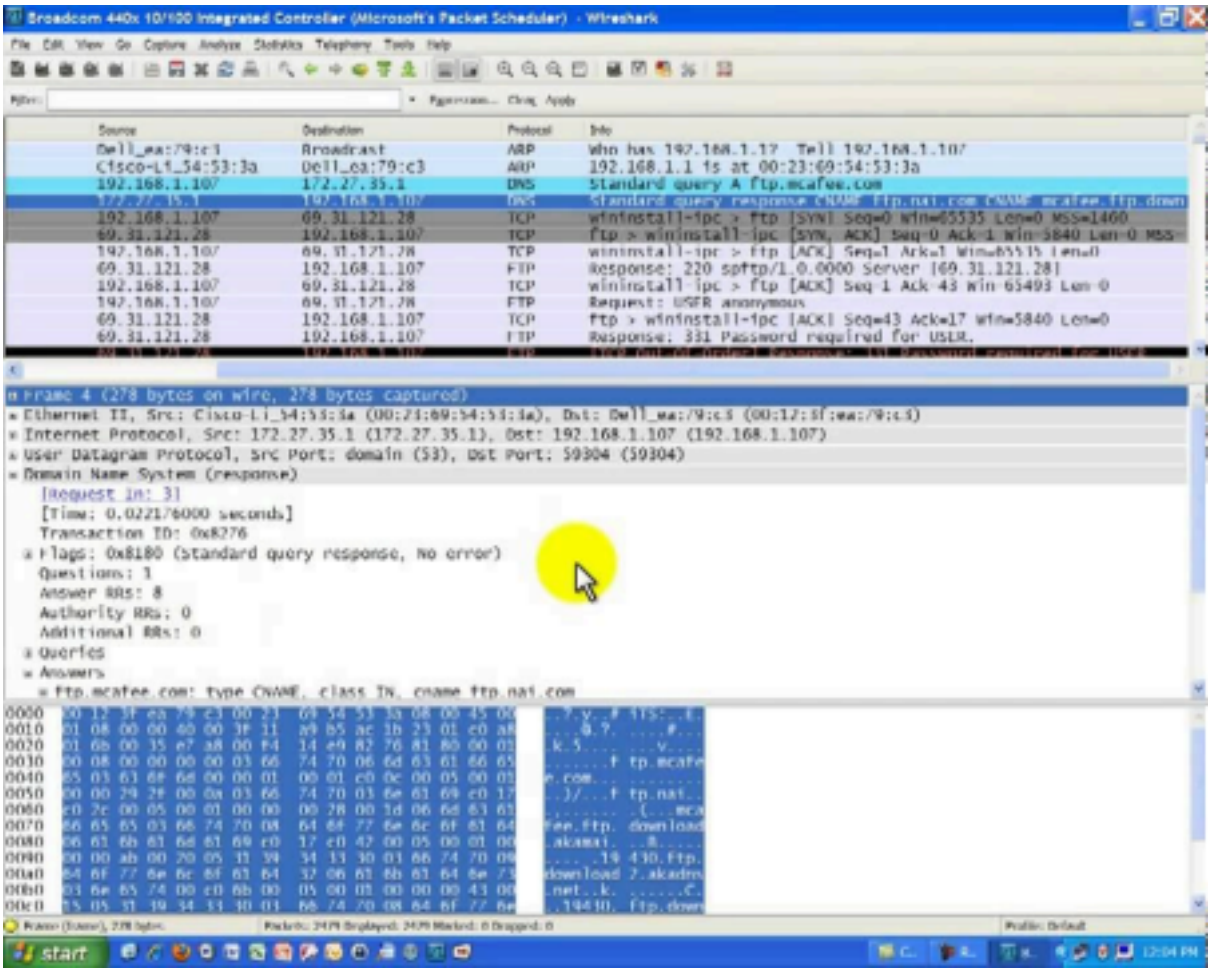




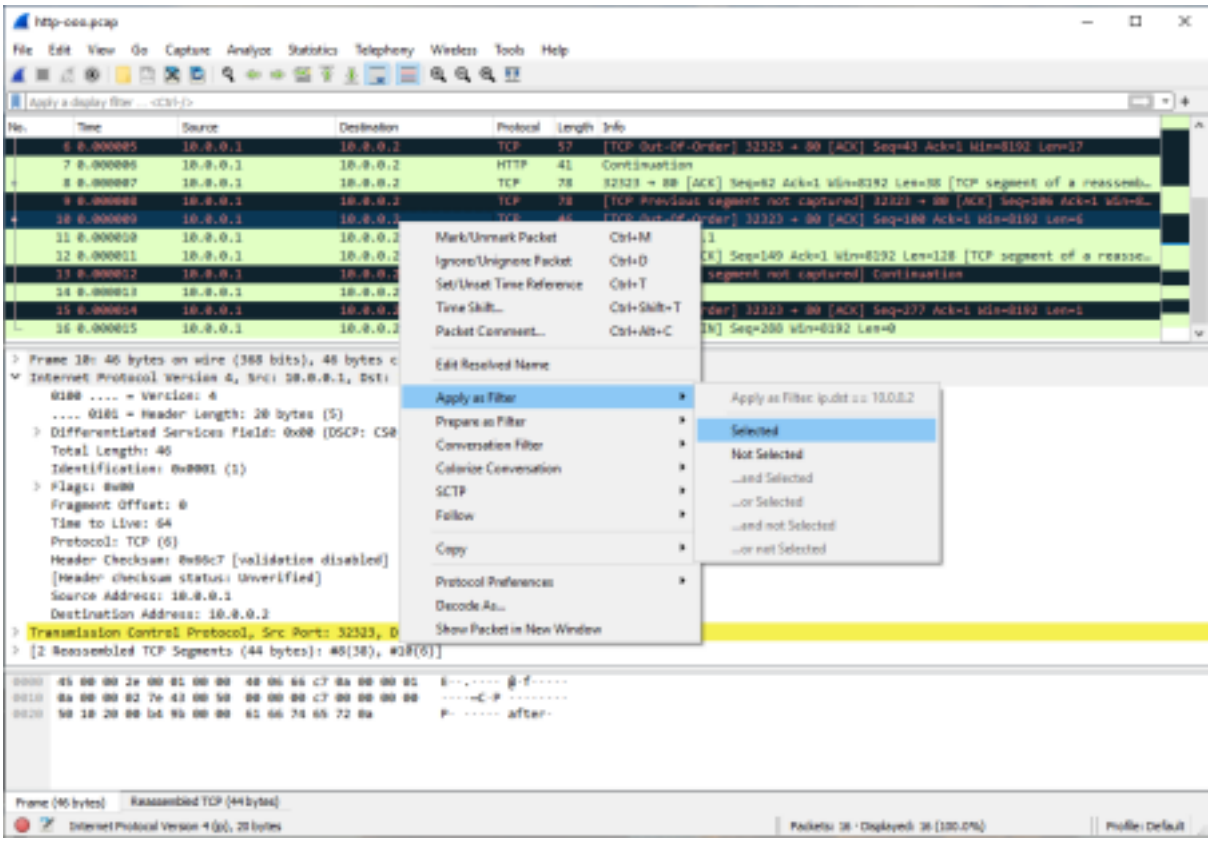
> FTP



> FTP Protocols



> POP



B. Server Hacking - Crack the servers and find the flags

. Exploit the SUNSET Server
. Exploit the DC-1 Server

Here flags means data . Data of a machine

Step 1: we need to import the Sunset server

Step 2 : And start kali linux and Sunset server

Step 3 : Before starting we need to check network settings

Step 4 : the network setting should be in bridge and

nan network

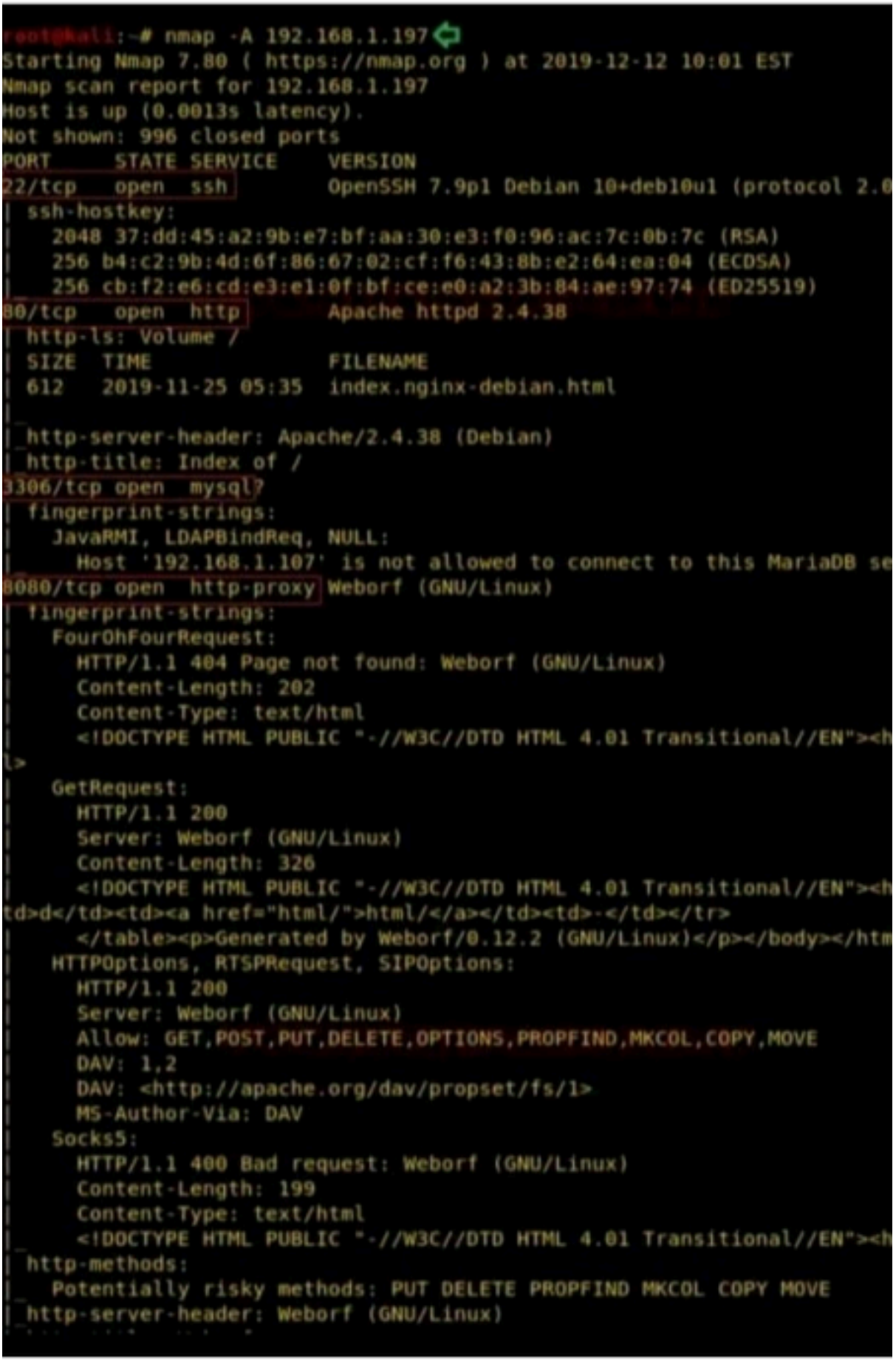
Step 5: After starting both

Step 6 : Give the command to find the ip address of the machine .

Step 7 : we need to find

Ip address(information gathering)
Scanning on open ports Enumerating the ports services-vulnerability in the server-nmap

And then finally we need to exploit and check for any data -flag



C. Perform a Dos attack on windows -10 Virtual Machine And check the perfomance .

DOS attack : denial of service (DOS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other devices unavailable to its intended users by interrupting the devices normal functioning .

We have to start using Windows 10 .
Identify the windows 10 ip address then we need to perform dos attack on win 10 VM

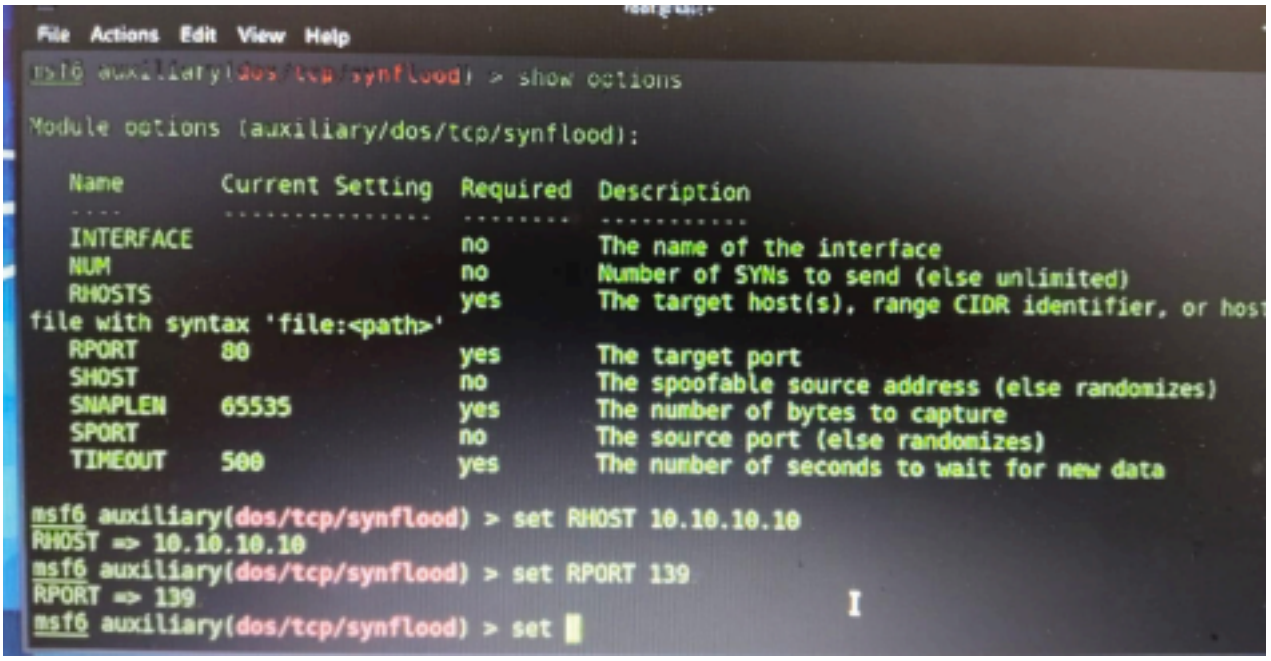
Check the performance in the task manager application IN win 10 we need to check the traffic in wireshark .

Step 1 : Start Kali linux
Step 2: Identify the Windows 10 ip address

Step 3: Then start Performing the Dos attack on the Win 10 VM

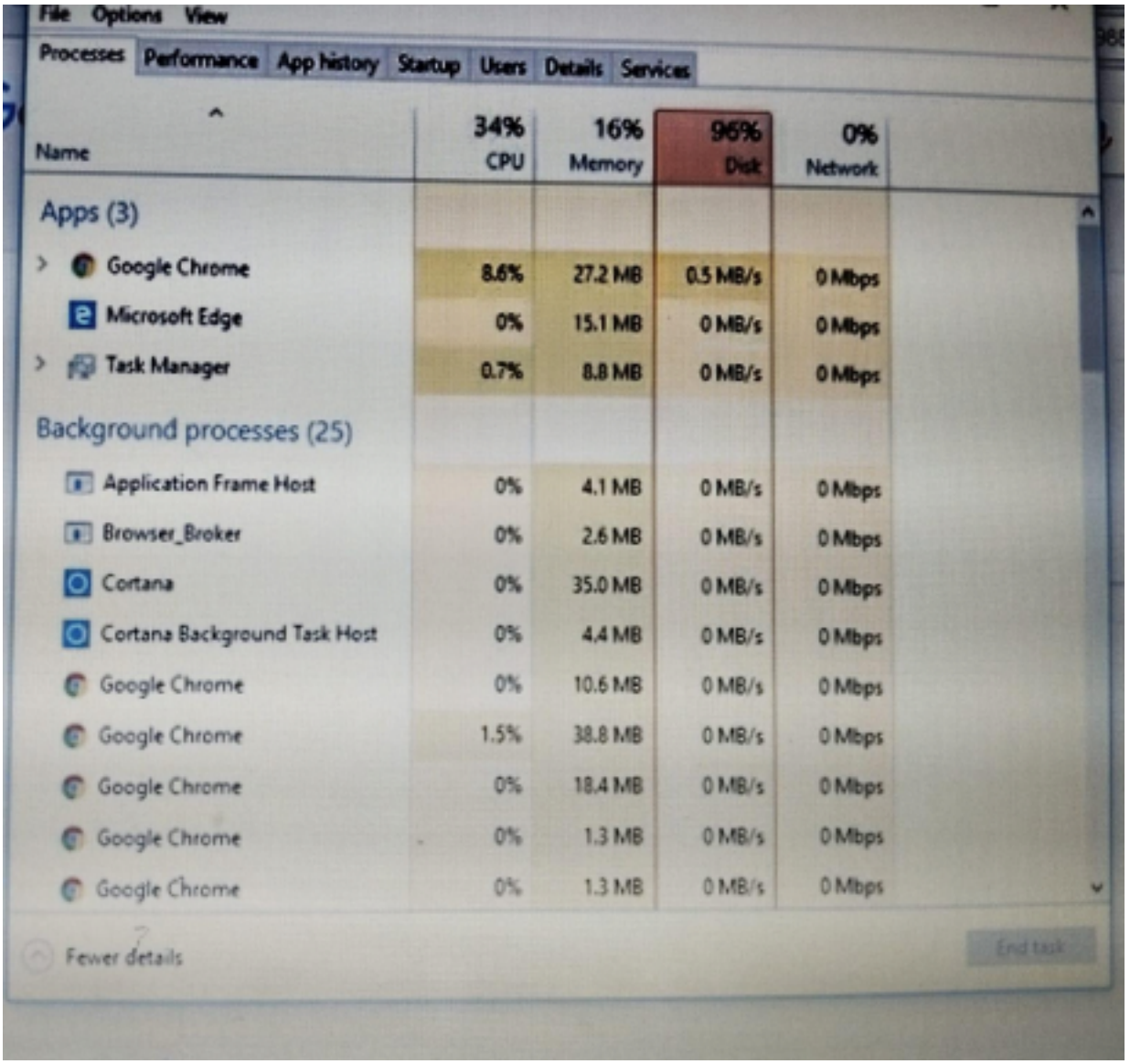
Write set RHOST [Windows 10's IP] and press Enter

- **Write set RPORT 21 and press Enter**
- **Write RHOST [Windows server 2016's IP] and press Enter.**
- **Write set TIMEOUT 20000 and press Enter.**

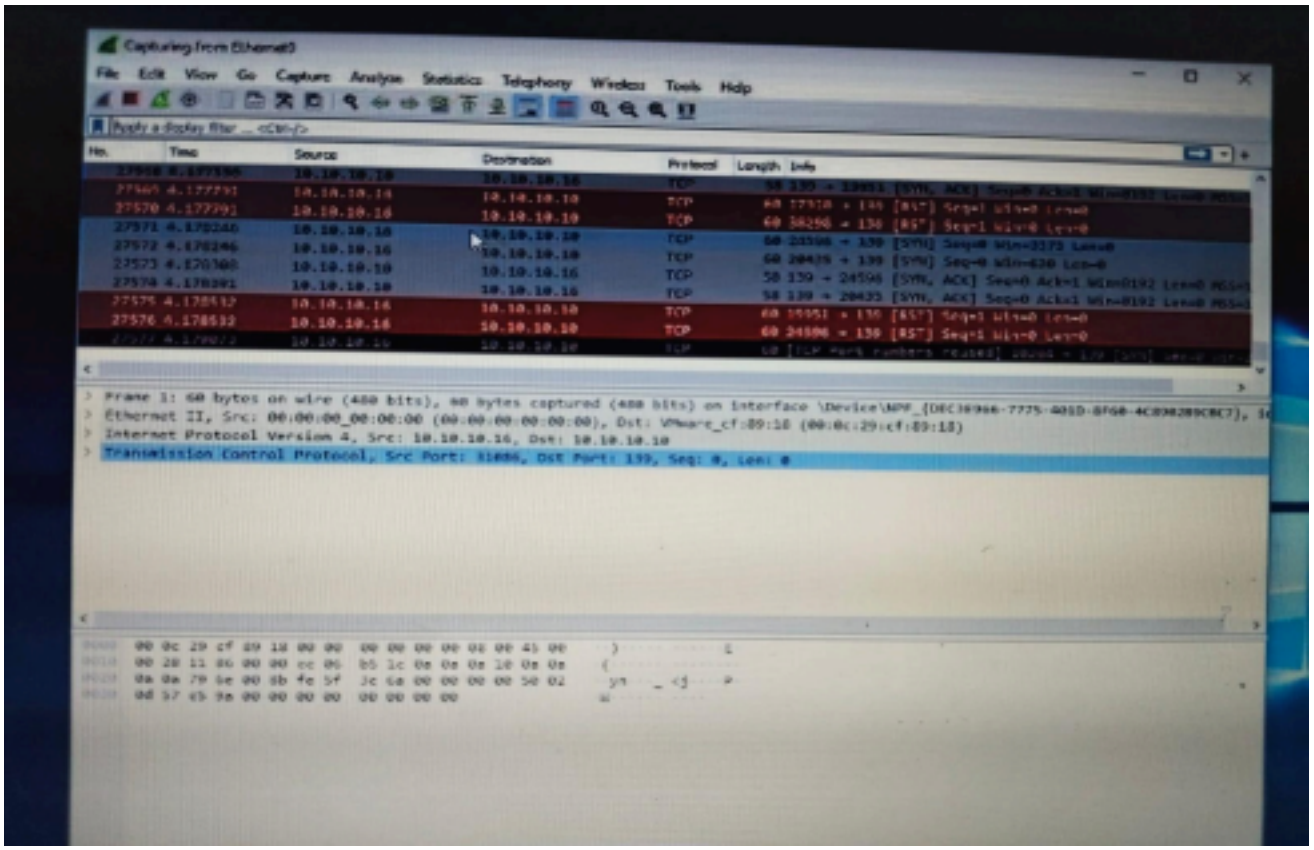


Step 4: Check the performance in the Task Manager

Step 5: Check the Performance in Wireshark



Now we need to check the performance in the wireshark .

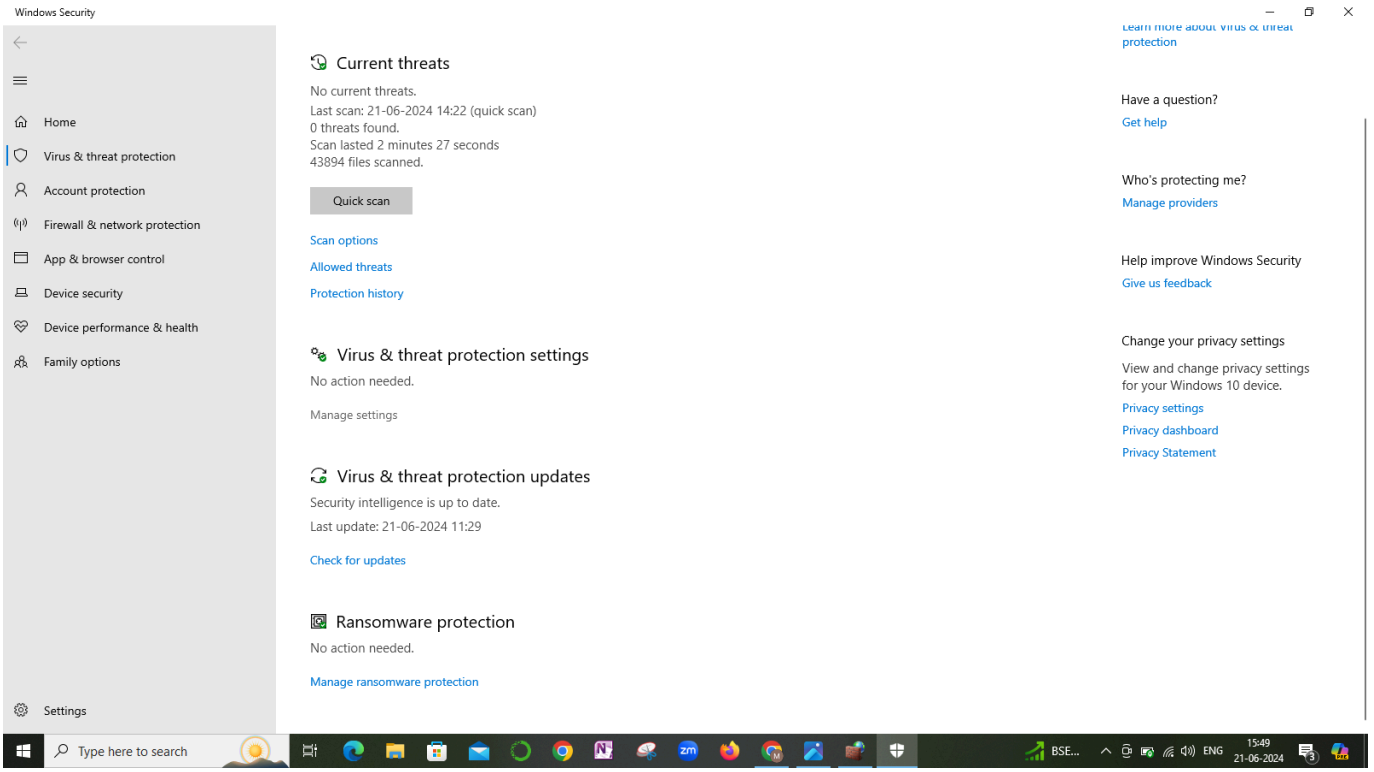

Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{DEC38966-7775-401D-8F68-4CB3B2B9CBC7}, id
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: VMware_cf:89:18 (00:0c:29:cf:89:18)
Internet Protocol Version 4, Src: 10.10.10.16, Dst: 10.10.10.10
Transmission Control Protocol, Src Port: 31886, Dst Port: 139, Seq: 0, Len: 0

ASSIGNMENT - 5

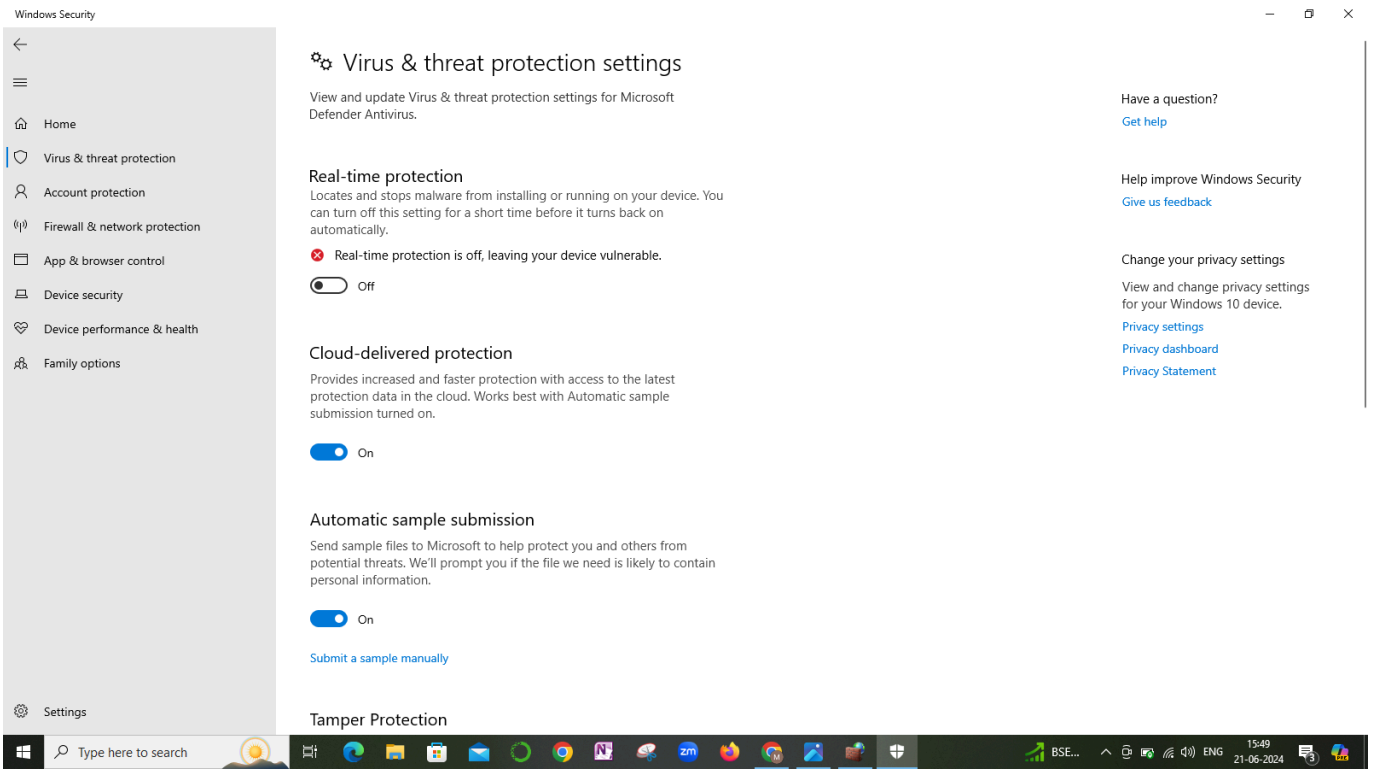
A. Turn off the antivirus and block the Instagram web application and a Standlone application by changing the rules of the firewall.

STEP 1 : Open the settings from windows search bar and navigate to the windows security option.

STEP 2: Now locate the virus and threat protection. And then go to the manage settings option in that page.

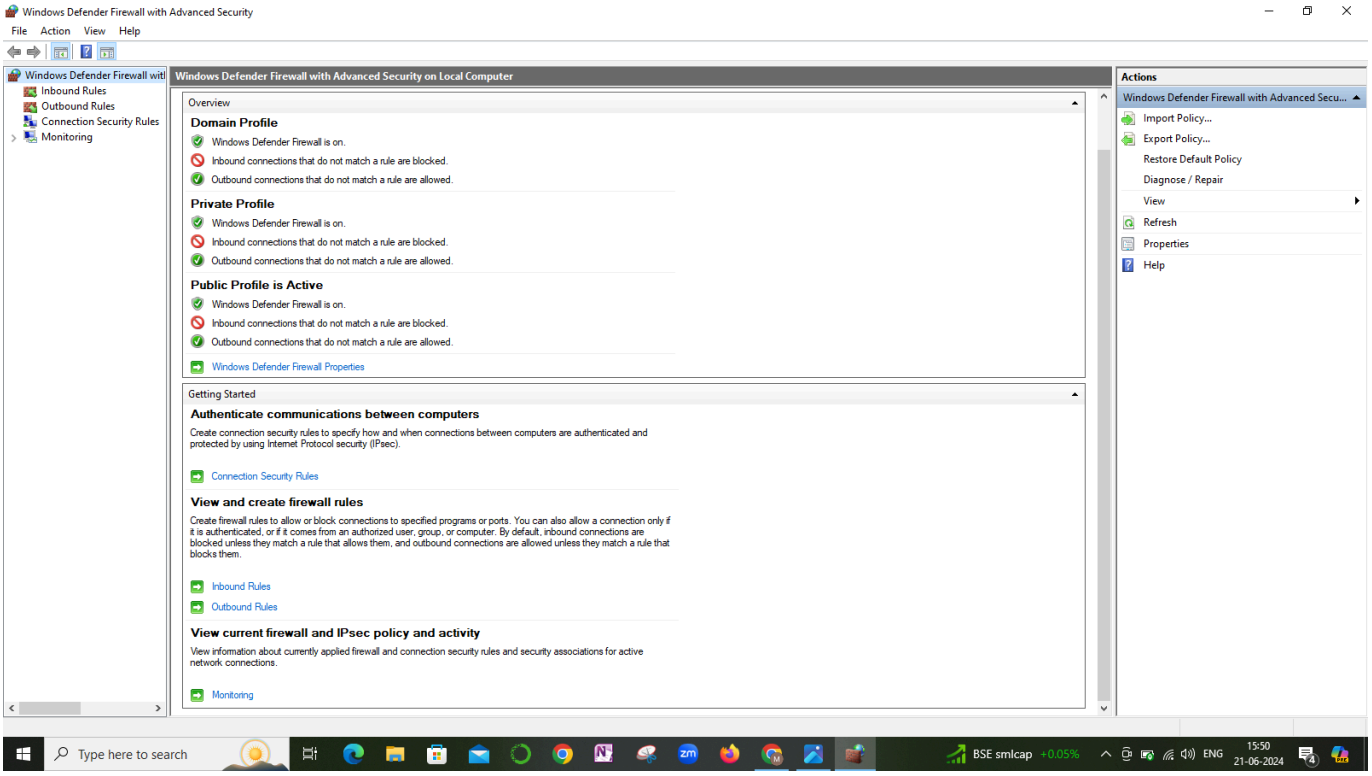


STEP 3 : Now disable the Real-time protection,Automatic sample submission and Cloud-delivered protection options.

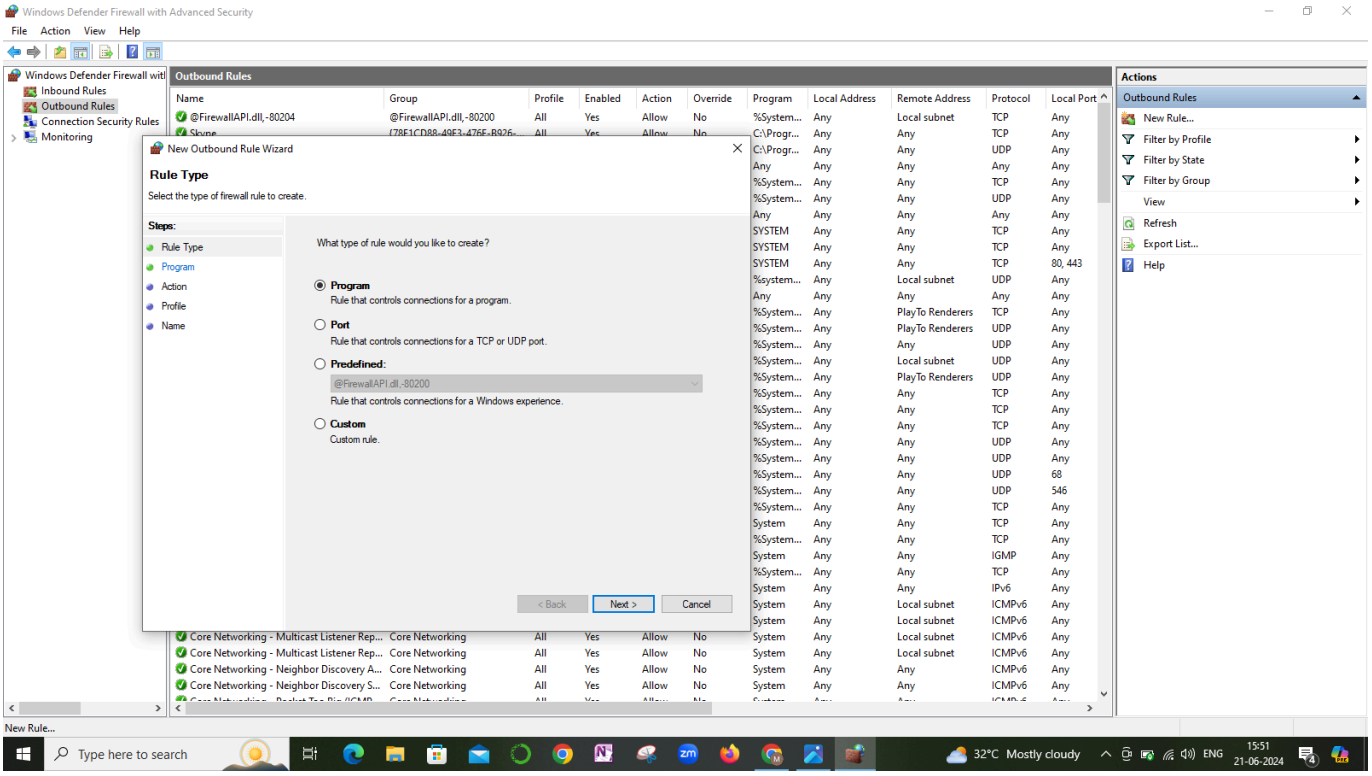


STEP-4: Now, Go back to the windows search bar and type firewall defender. And then you will go to Windows firewall defender and Advanced security.

STEP-5:There in the left-side menu bar, you will find the Outbound rules options.Click on it.

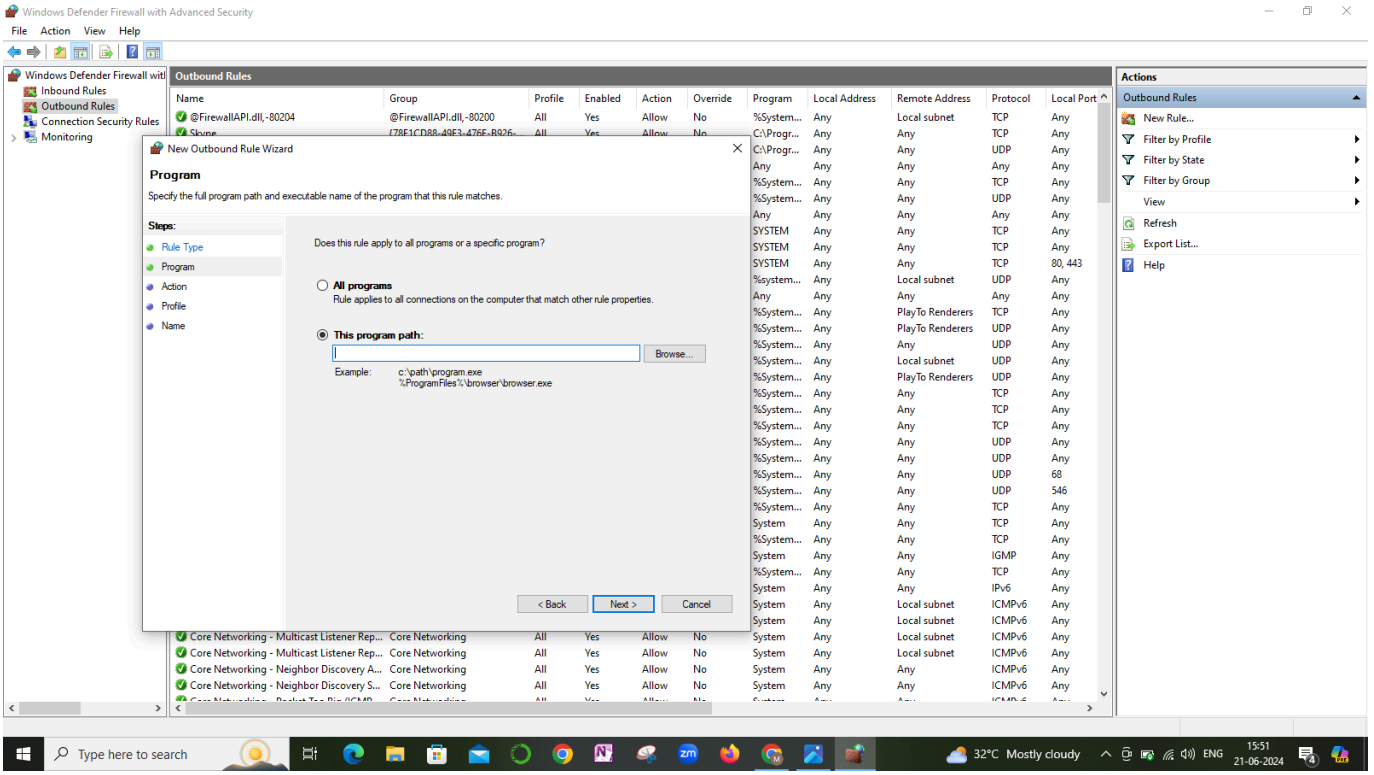


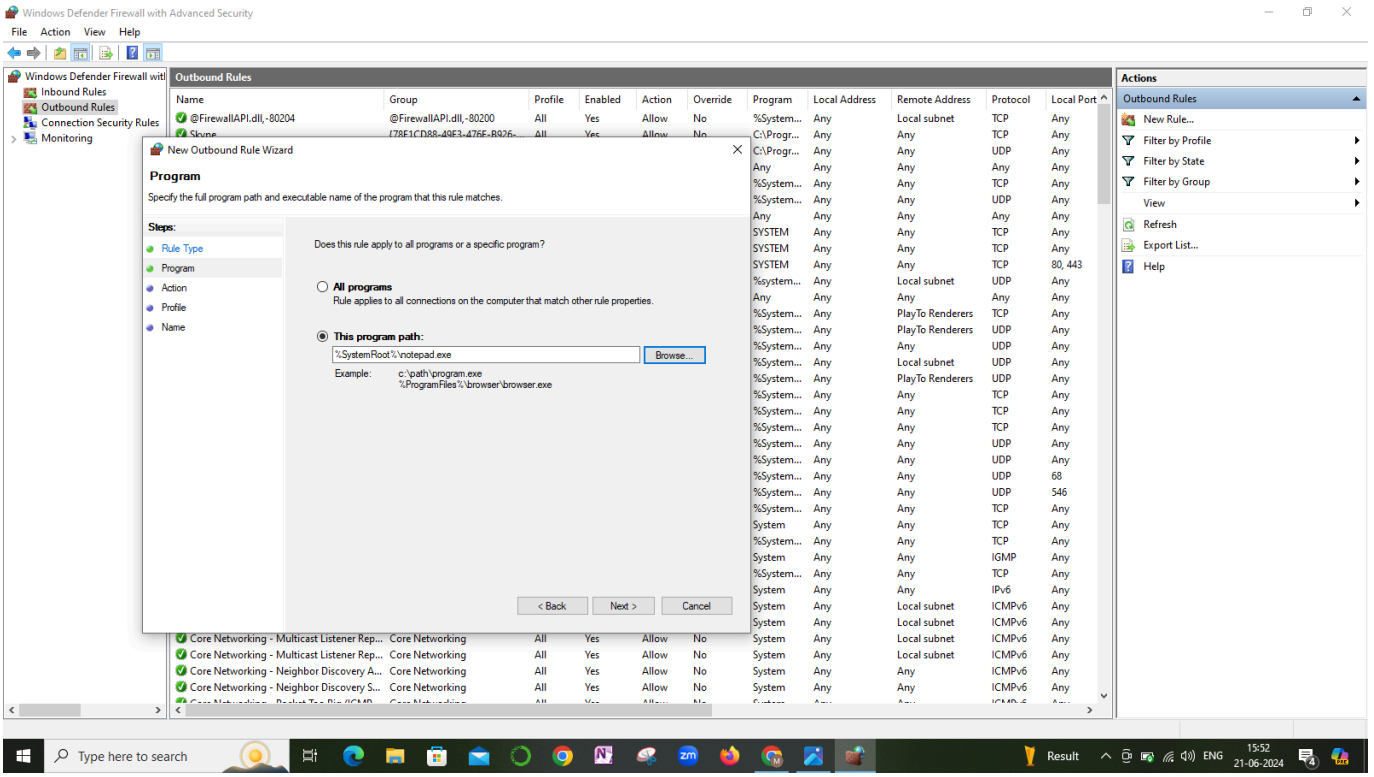
STEP-6:Now you can see a right-side menu bar with outbound rules like new rule,filter by profile,filter by state,etc., Now click on the New Rule option.Then you'll get a pop like below-



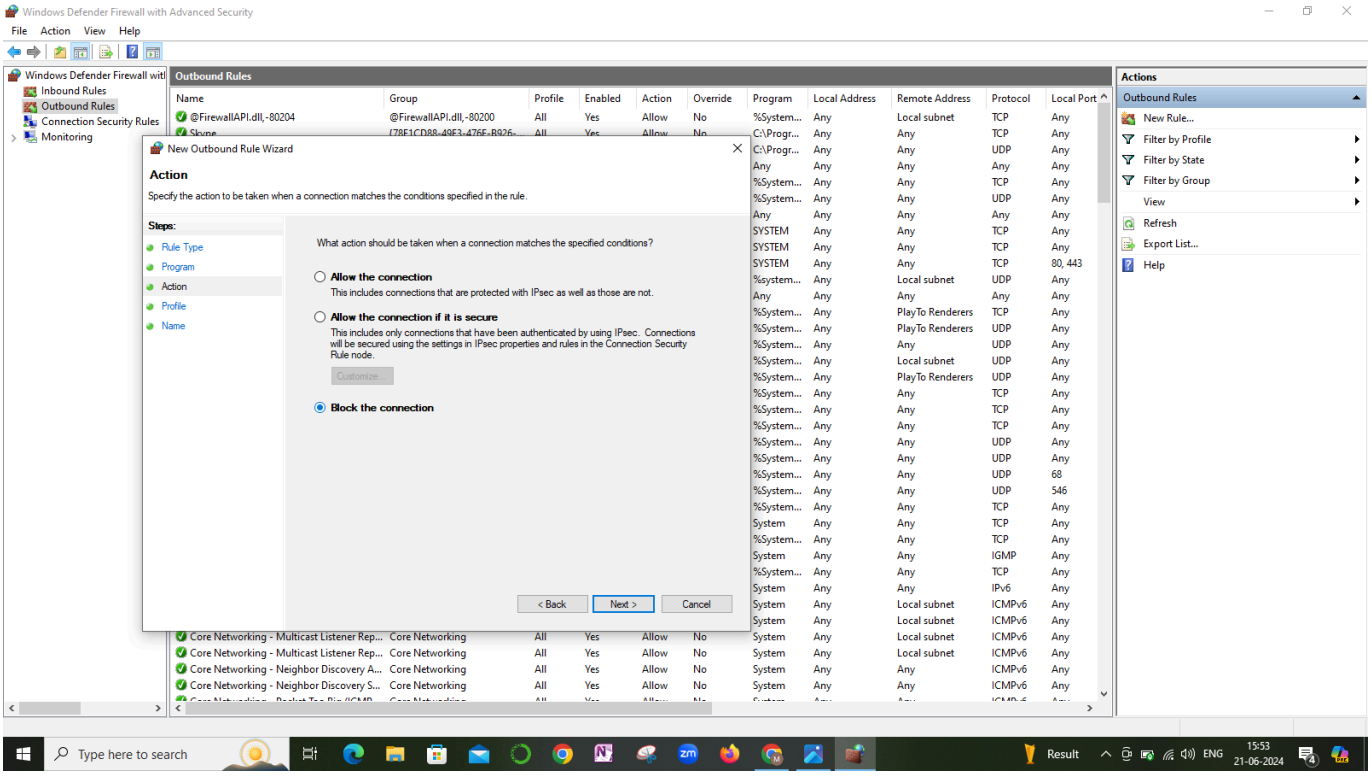
STEP-7: By default we will be in the Rule Type option and it is defaultly selected as program and leave it as it is and click on Next.

STEP-8:So, now move to the Program option on the side menu bar.And it will ask you for whether to create a rule for all programs or specified one.Now choose the This program path and give the path of the standalone application you want to block for and click on Next. Here, I have chosen the Notepad Standalone Application to block.

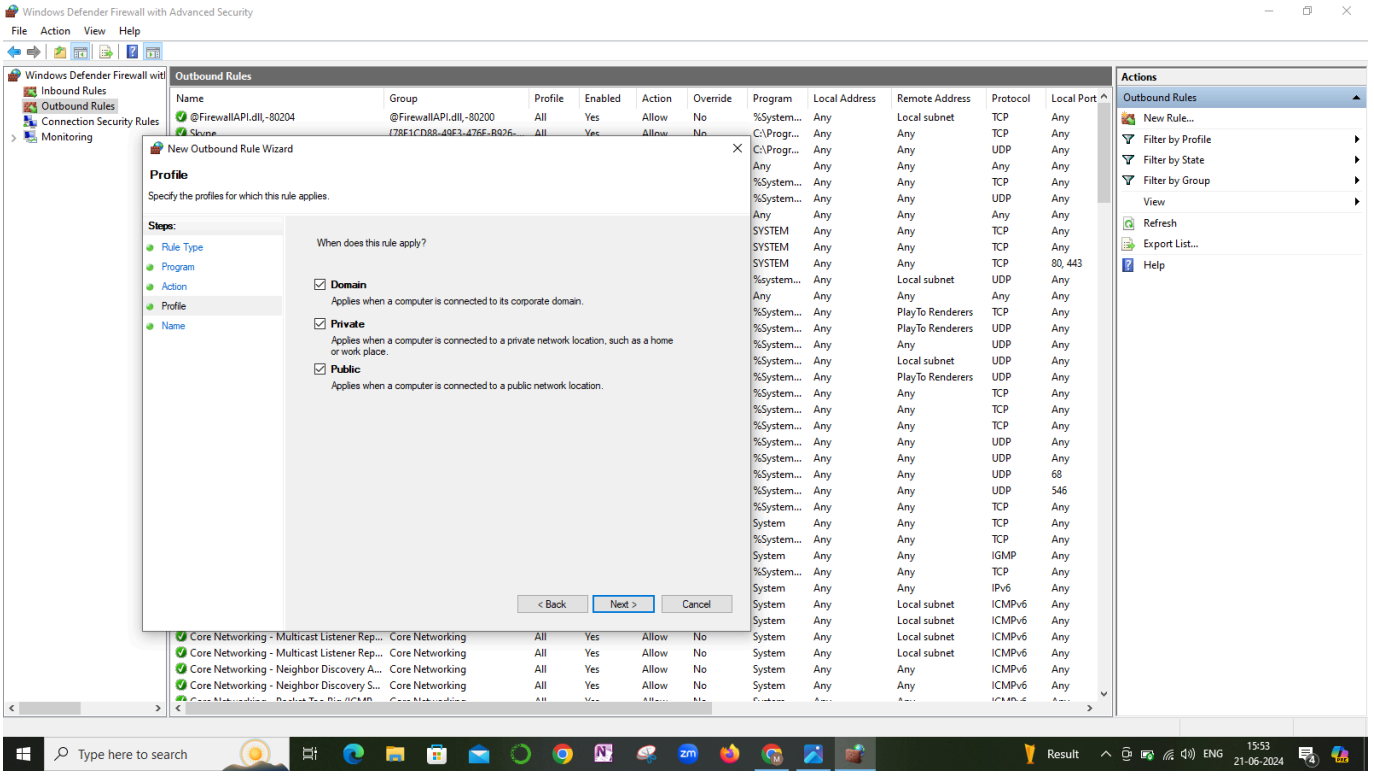




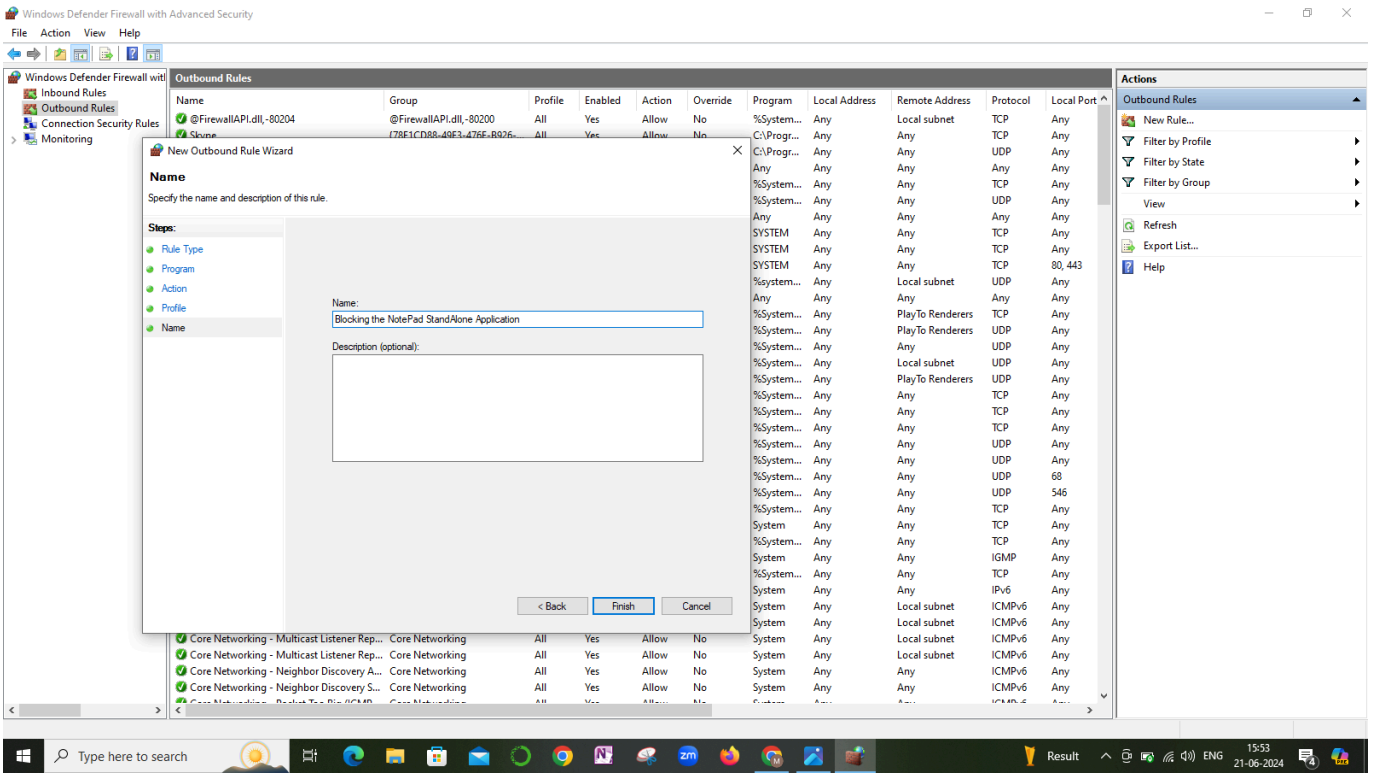
STEP-9: Next in the Actions menu Click on Block the Connection and Click on Next.



STEP-10: Now, enable all the checkboxes to apply the blocking in Domain,Private and even in Public. And then click on Next.



STEP-11:Now, give the name for the rule to complete the process of blocking the connection. And Click on Finish.

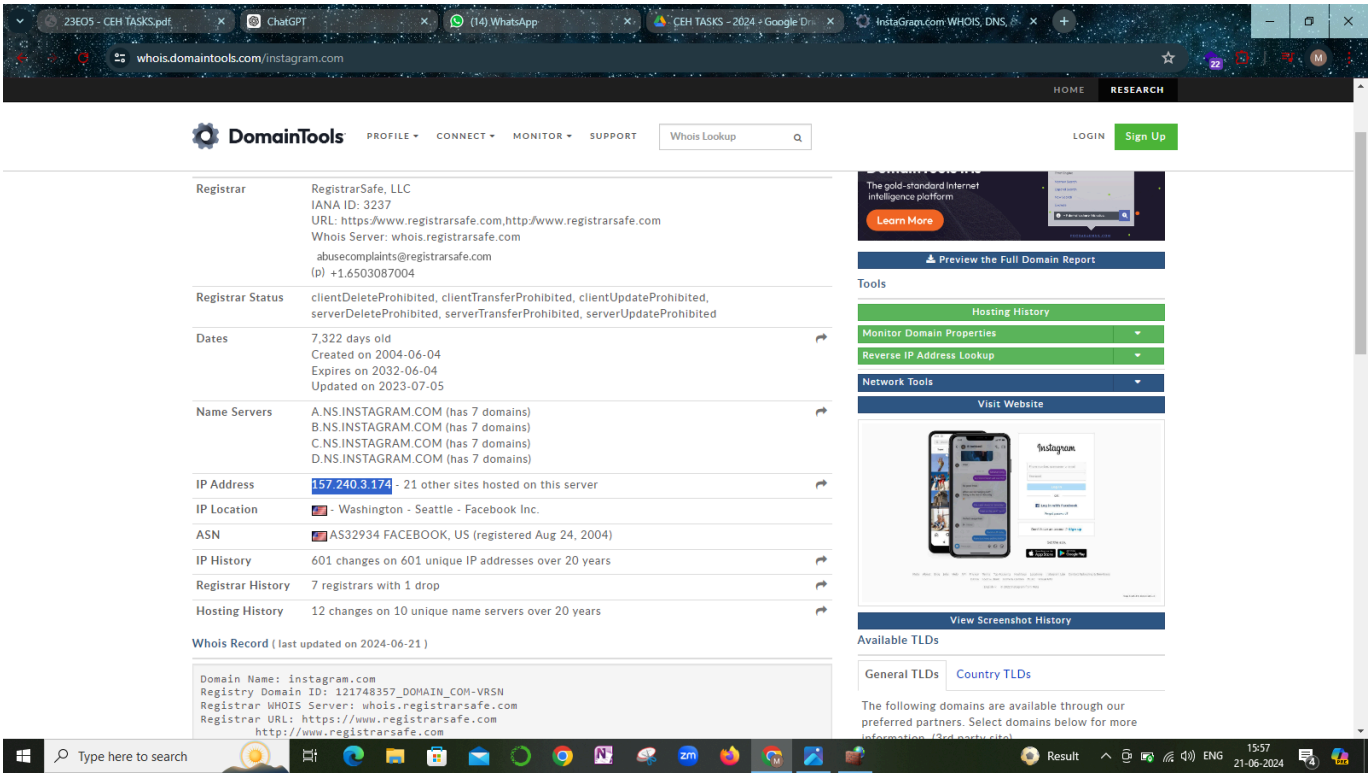


And Now the standalone application i.e, Notepad has been successfully blocked.

Now, we need to block the Instagram Web Application.For that we need to follow the below procedure:

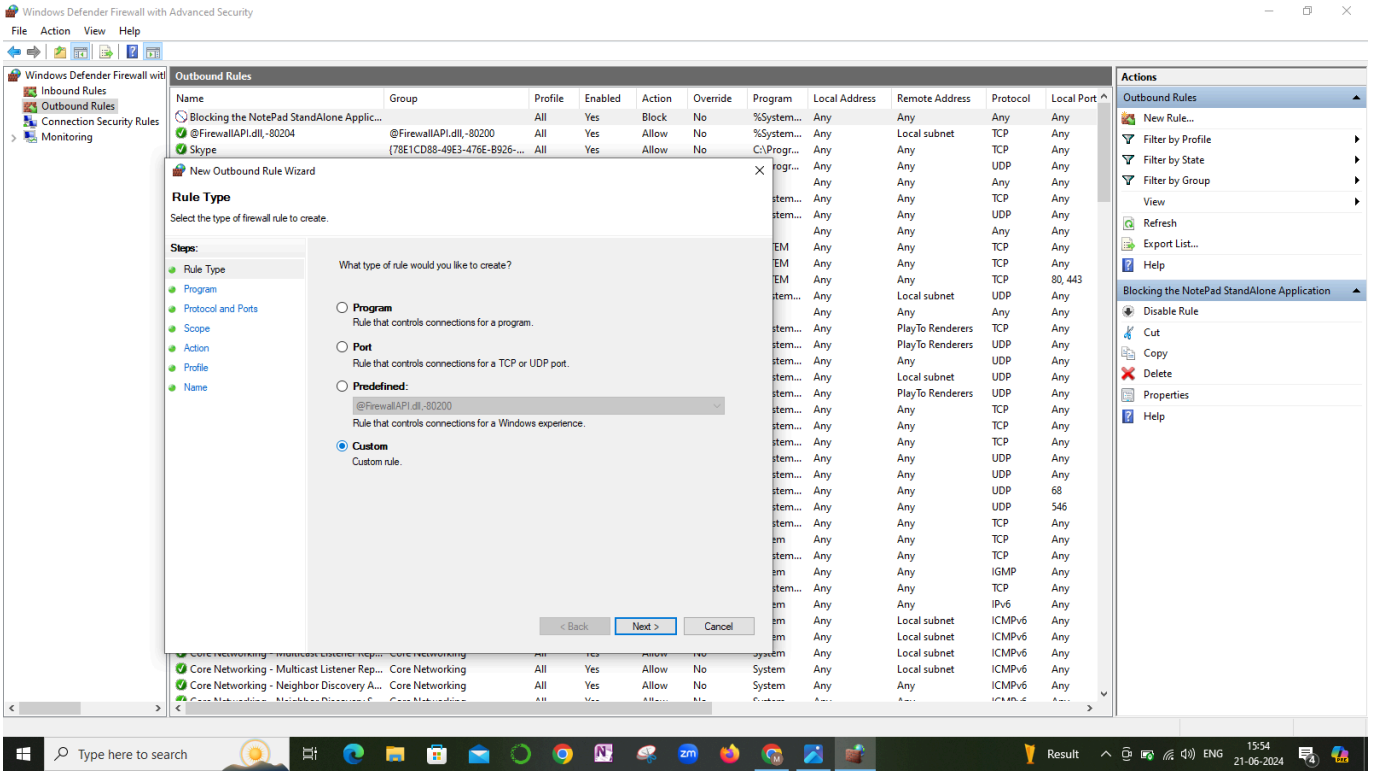
STEP-1: Navigate to Chrome search bar and type www.instagram.com and copy the URL of the webpage.

STEP-2:Now open the WhoIsLookup Domain tool in Google Chrome and paste the URL in the tools search bar.

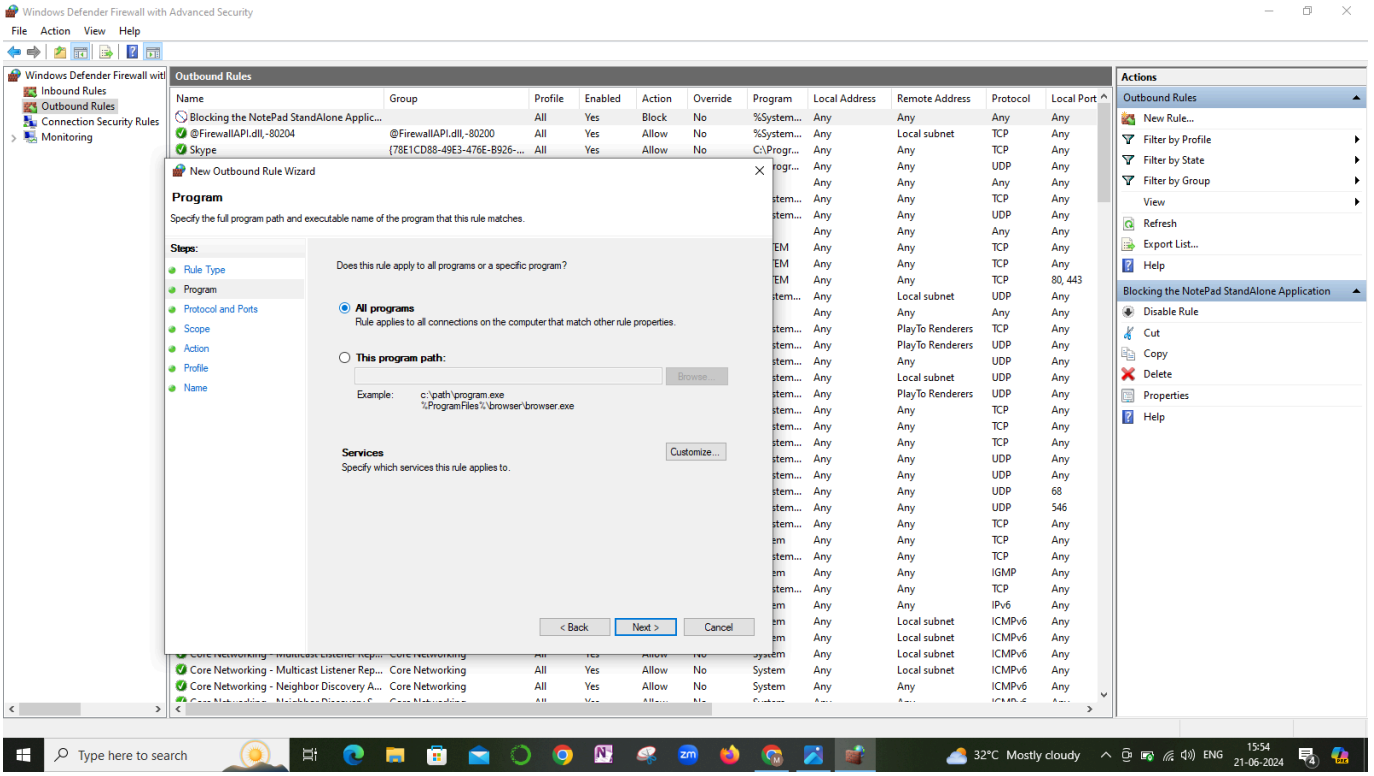


Now, copy the IP-Address of the webpage it gives and Go back to the windows defender settings and navigate to outbound rules and click on the new rule option.

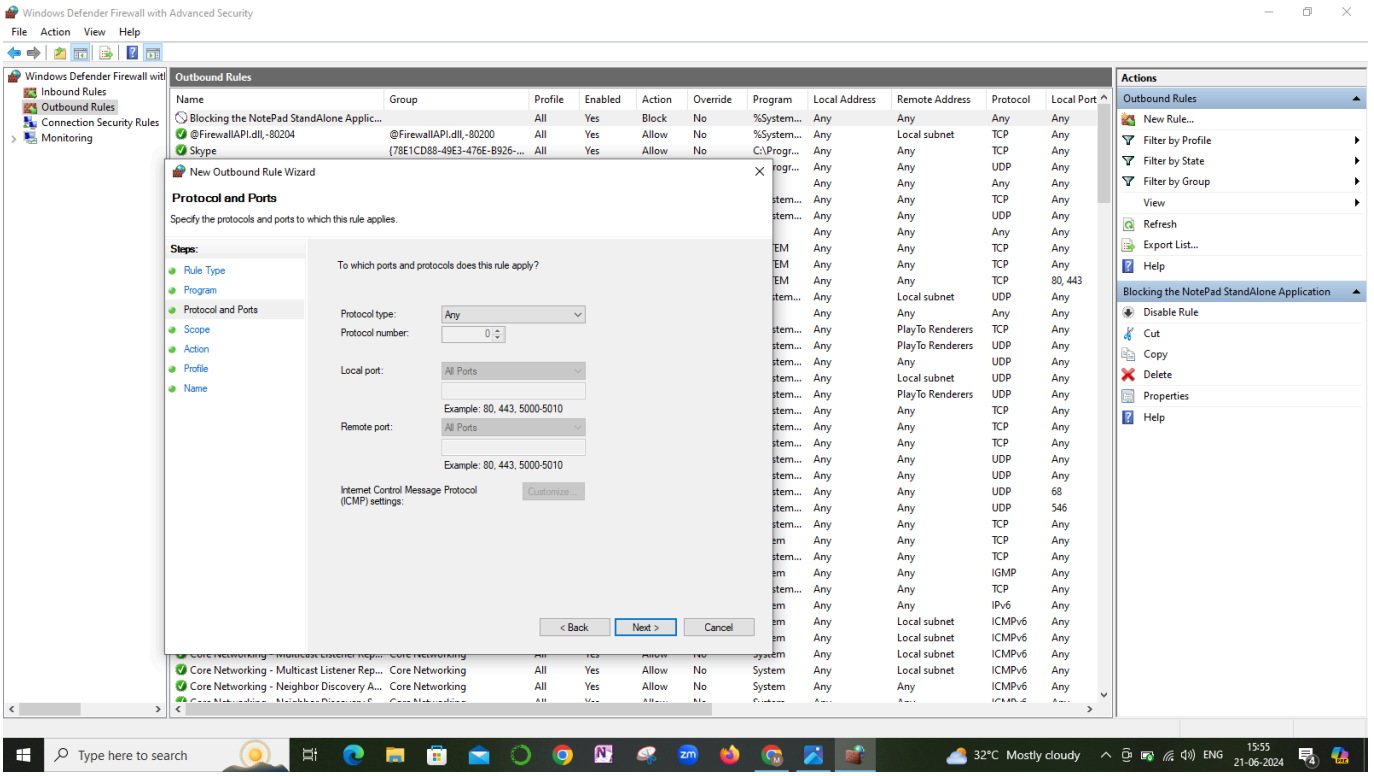
STEP-3: Now, Select the rule type as custom and click on next.



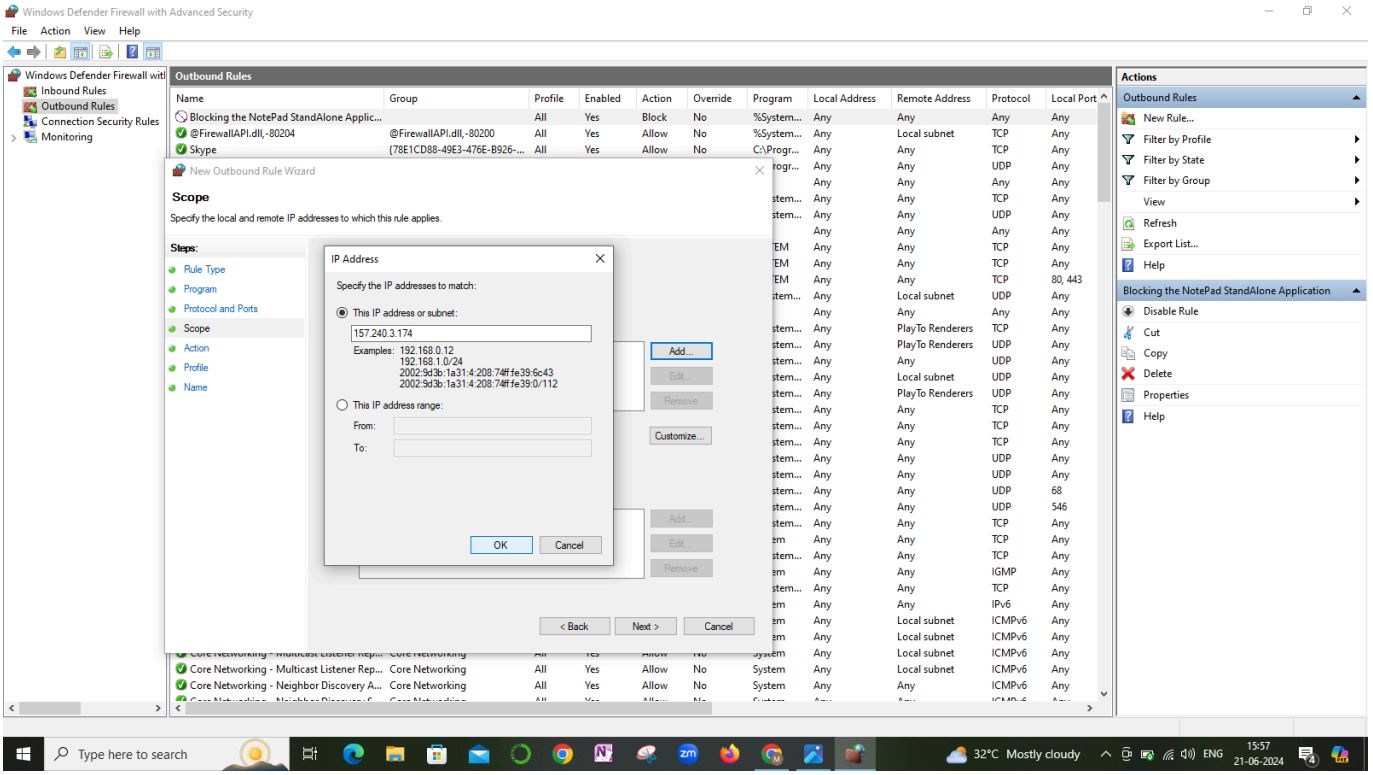
STEP-4:And click on program type as all programs and click on next.

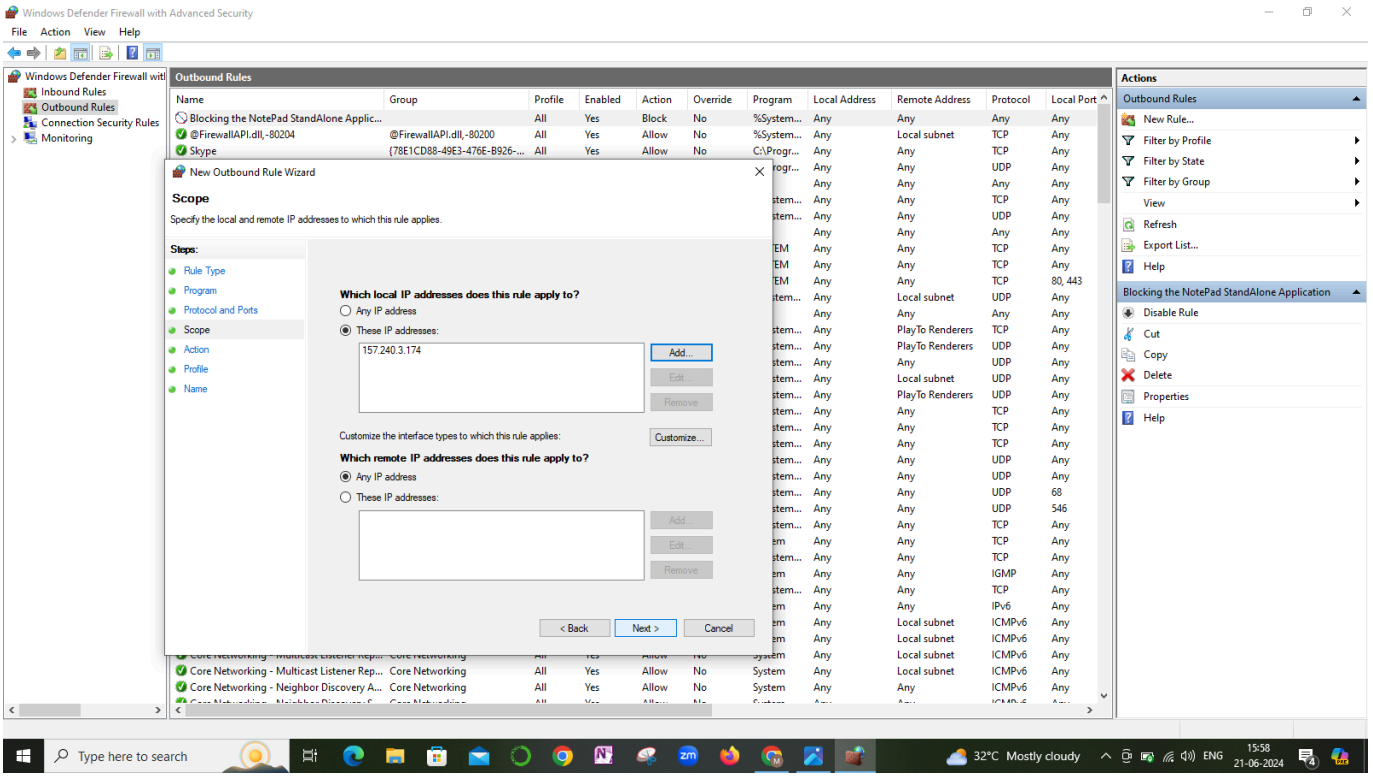


STEP-5: And now leave the protocol type as any by default and click on Next.

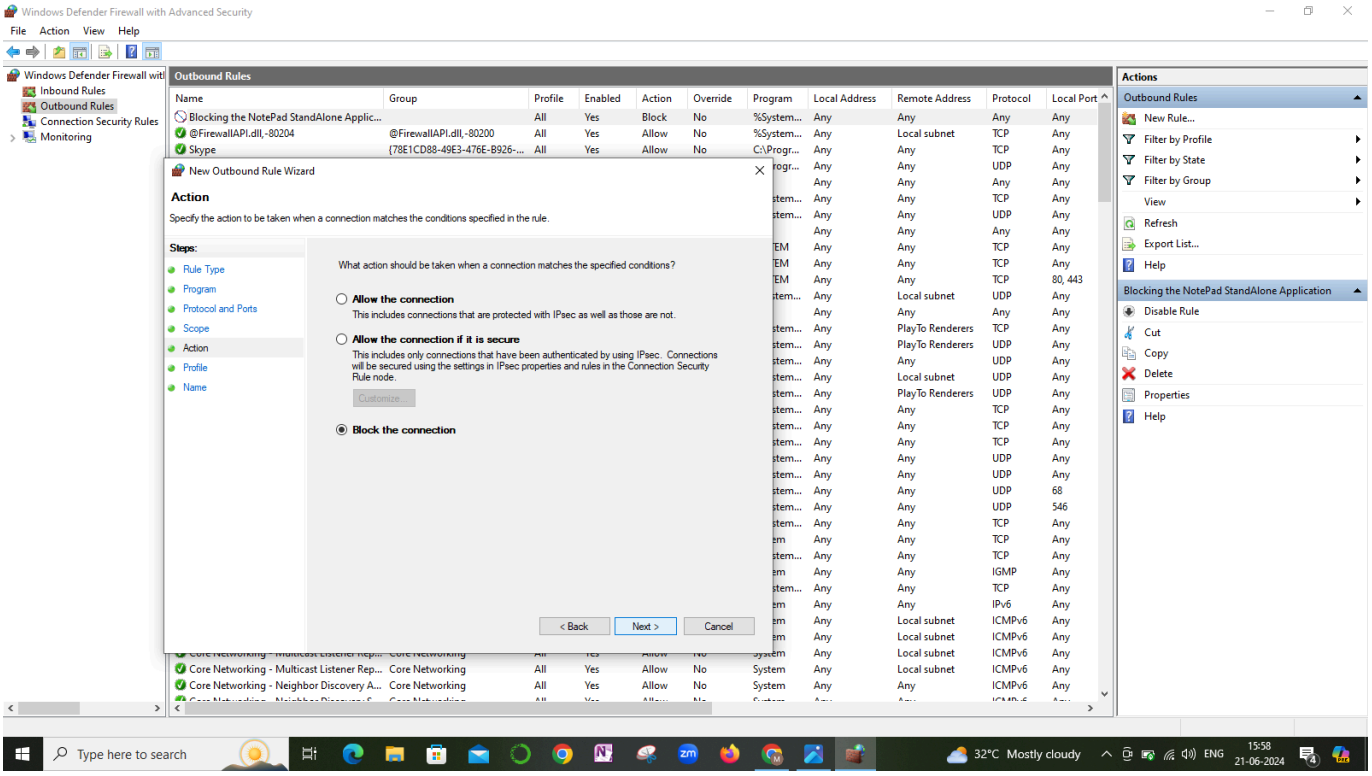


STEP-6: Now, in the scope section select the local ip address it belongs to and add an ip address that is copied from whois lookup tool and paste it in that section as shown below-

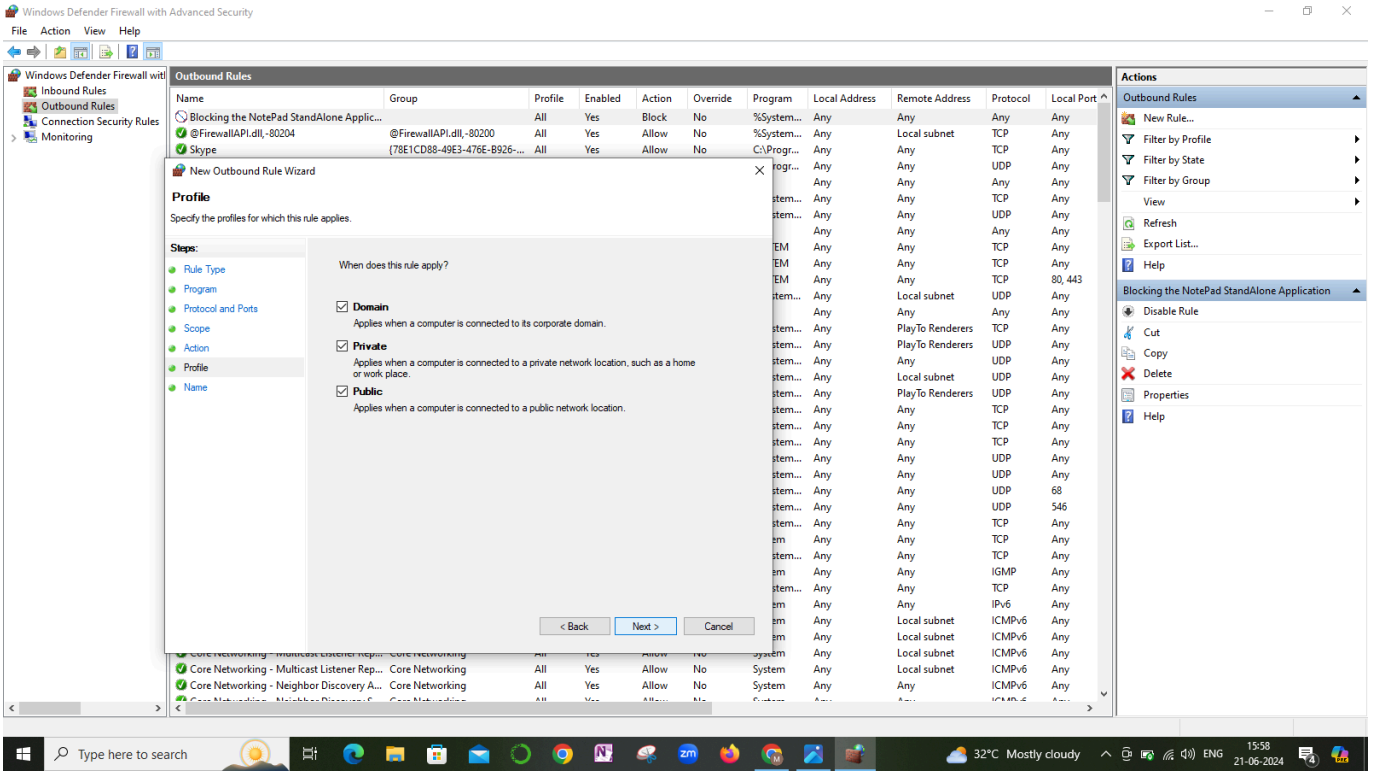


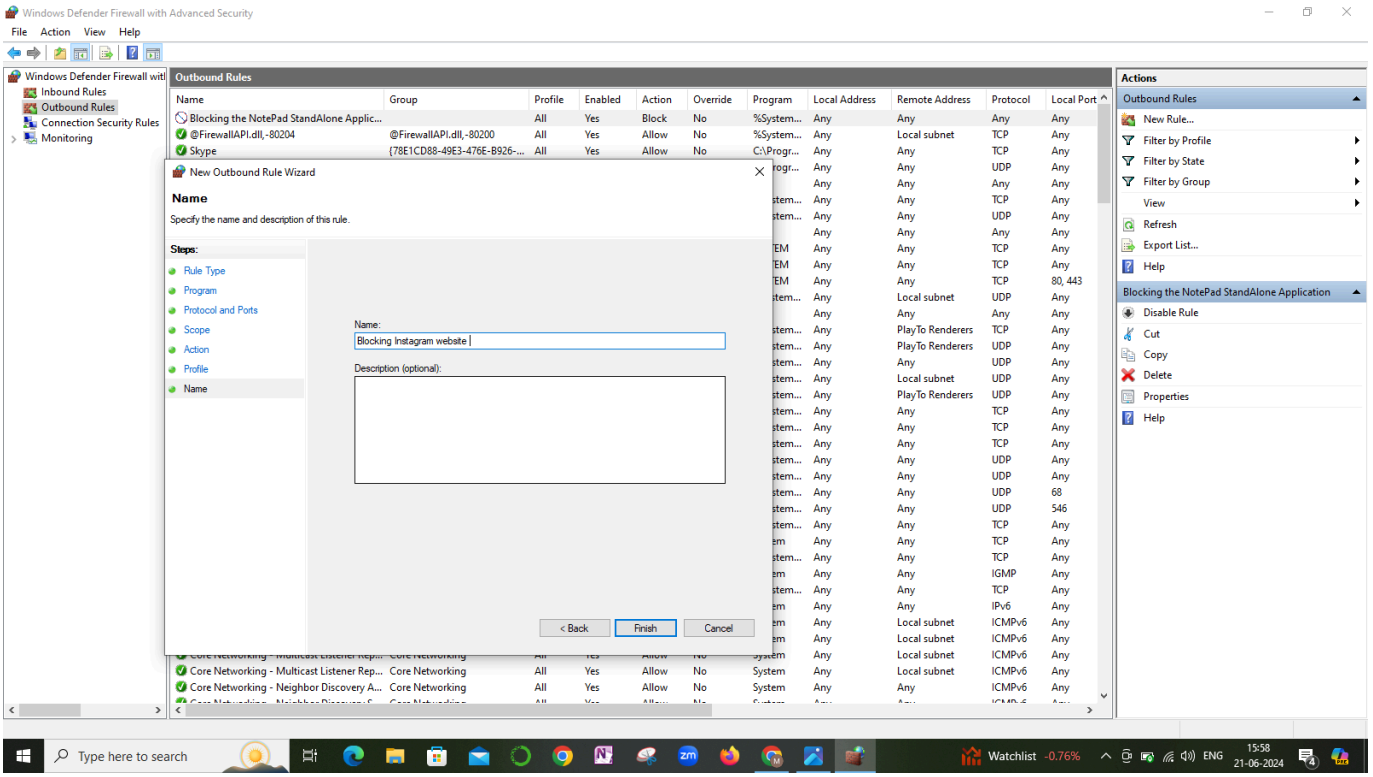


STEP-7: In the Action section select Block the Connection and Click on Next.



STEP-8: Now, enable all profiles to apply the rule and click on next. And then give the name for the rule to complete the process.





Finally we have blocked the instagram web application too.

B. Perform Dos Attack using the golden eye tool on any 2 non-Indian Websites and observe the traffic in Wireshark .

Dos Attack : A type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the devices normal functioning .

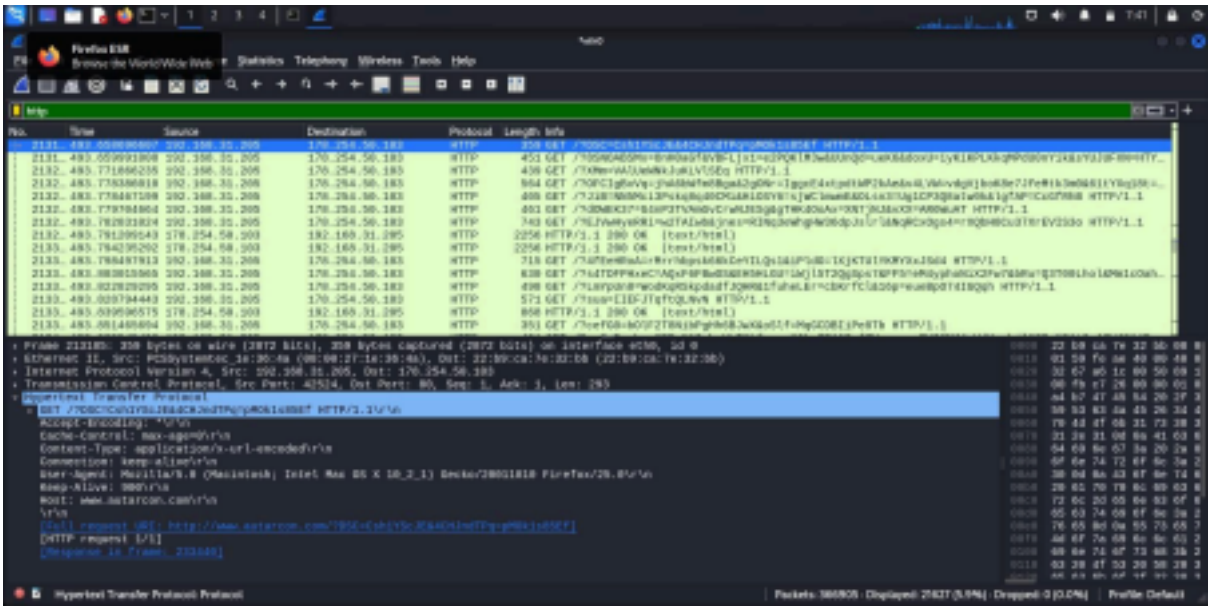
Golden eye: It is free and open source tool

Now here in this we need to perform Dos attack using the golden eye tool on any 2 non-Indian Websites and observe the traffic in Wireshark

Step 1: First open kali linux

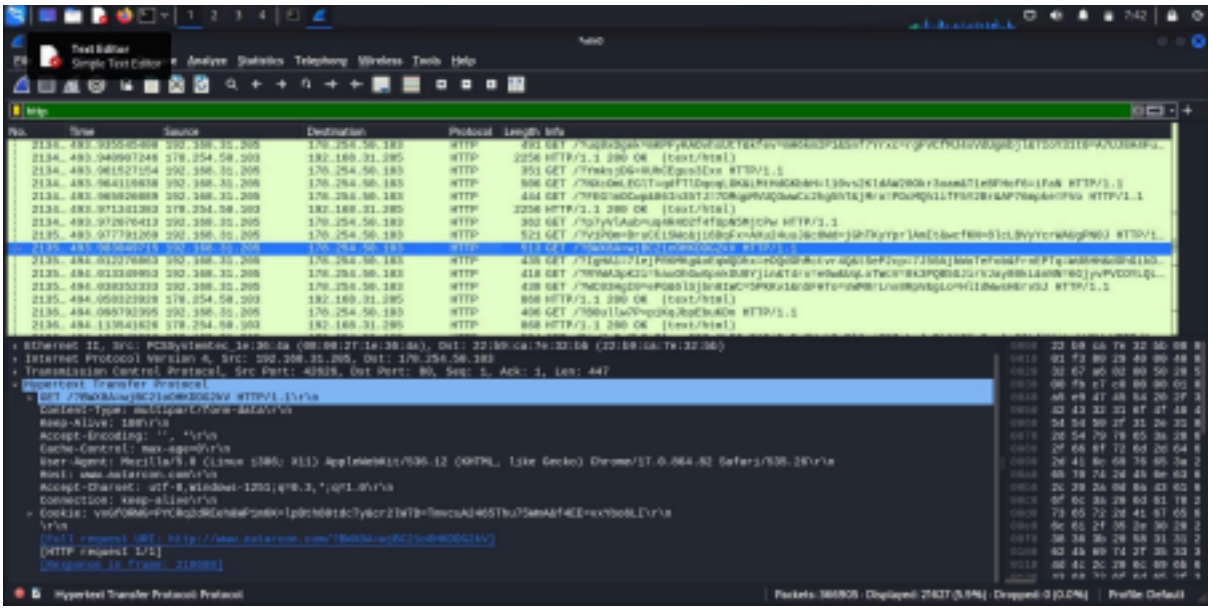
Step 2: Start giving the commands
Step 3:

Step 4 : Verify the traffic in Wireshark



Check for Another Website

Step 2:



Now from this we can Observe that we observed the traffic of two non- Indian websites

C. Perform a backdoor on a target website using the Metasploit.

Performing the backdoor on a target Website using the Metasploit.

A backdoor is a malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.

STEP-1: Collect any Non-indian Website using Google dorks and copy its URL. (OR) get the ip address of that url using whois lookup tool.

STEP-2: Now open the kali linux and type the command " nmap -p -sV 'website url'" or "nmap -p -sV URL ip address".

STEP-3:Later it will give some open ports and their versions. Then search for the FTP open port with the versions "vsftpd 2.3.4" or "ProFtpd 1.3.3c".

STEp-6:Open the root user in the kali linux as we are using the metasploit framework for performing backdoor on a website.So give the command “sudo su”

STEP-5:Later, give the command “msfconsole” to open the Metasploit Framework.

STEP-6:It takes a few seconds to enter into the metasploit framework console in kali. After getting the console search for the backdoor you wanted to exploit. I.e, “search ftp backdoor”.

STEP-7:It will provide you some exploits of the FTP backdoor with its version, exploit name and its description.

STEP-9: For example your target website has FTP open port with the version so called “vsftpd 2.3.4”.

STEP-10:Then you need to choose the exploit using the command- “use exploit/unix/ftp/vsftpd_234_backdoor”.

STEP-11:And then set RHOST for that exploit using the command “set RHOST ip-address”

STEP-12: Later set RPORT as FTP port number using “set RPORT 21” command.

STEP-13: Now run the exploit using the command “exploit”. If it is backdoored, you will get the ftp> console and that will be the output.

ASSIGNMENT - 6

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

A. 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

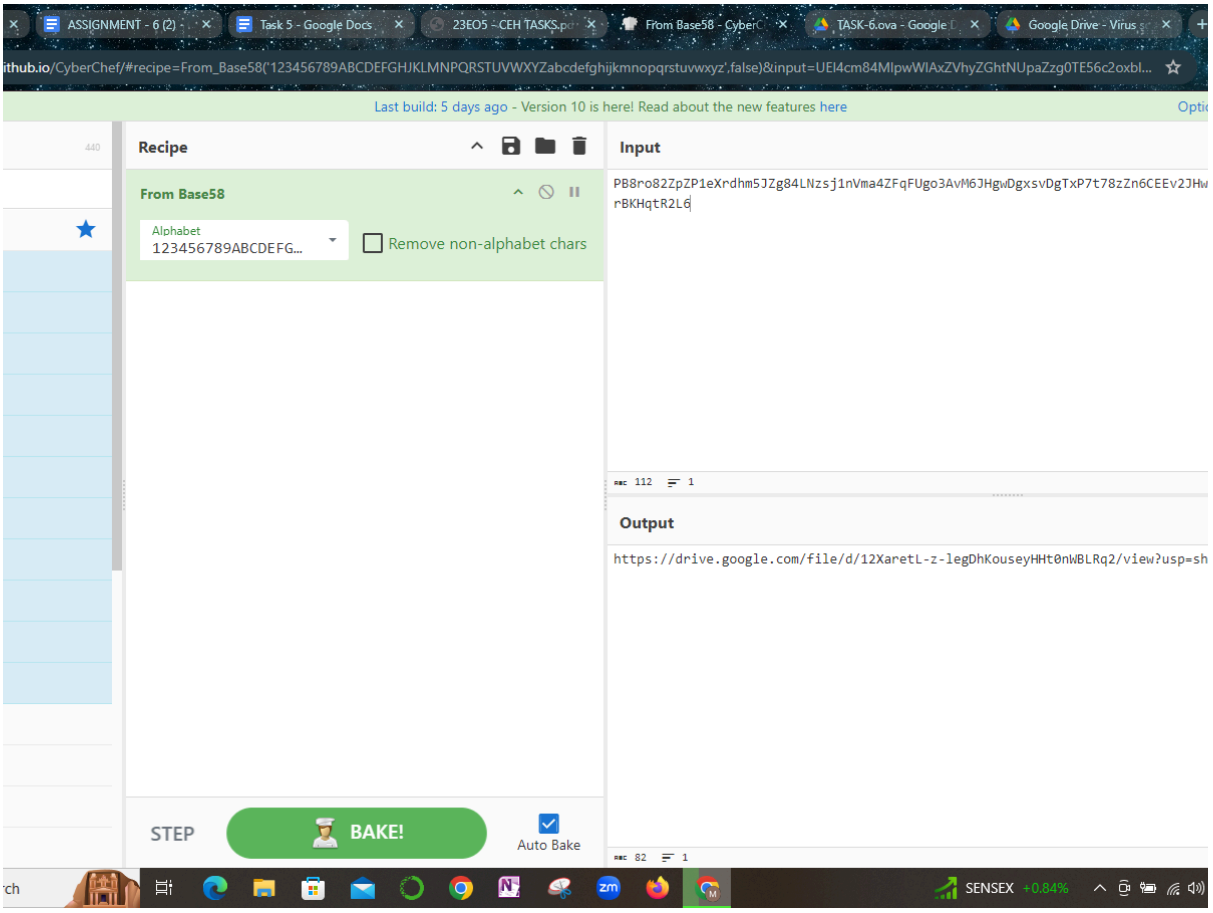
Step 1: First Decrypt the secret data to Get the link

Step 2: Go to the Google and type cyber chef Which is mostly for url decode

Step 3 : Now from there we can observe that the url has been decoded .

Now decrypting the key

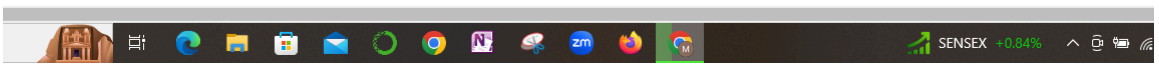
PB8ro82ZpZP1eXrdhm5JZg84LNzsj1nVma4ZFqFUgo3AvM6J HgwDgxsvDgTxP7t78zZn6CEEv2JHwVCMA7PCsxpXFGNQY 2ZbFKQynvrBKHqtR2L6



Google Drive can't scan this file for viruses.

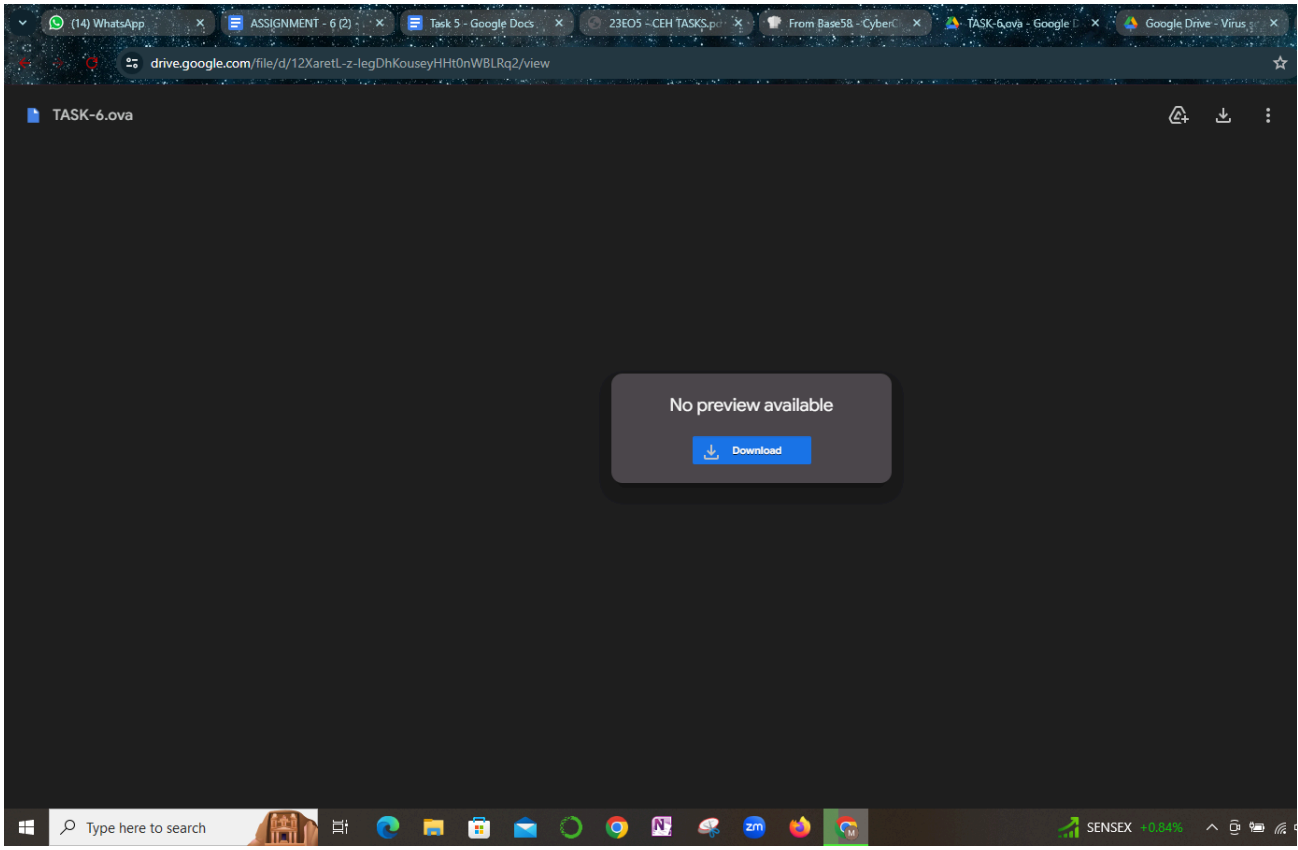
TASK-6.ova (3.2G) is too large for Google to scan for viruses. Would you still like to download this file?

Download anyway

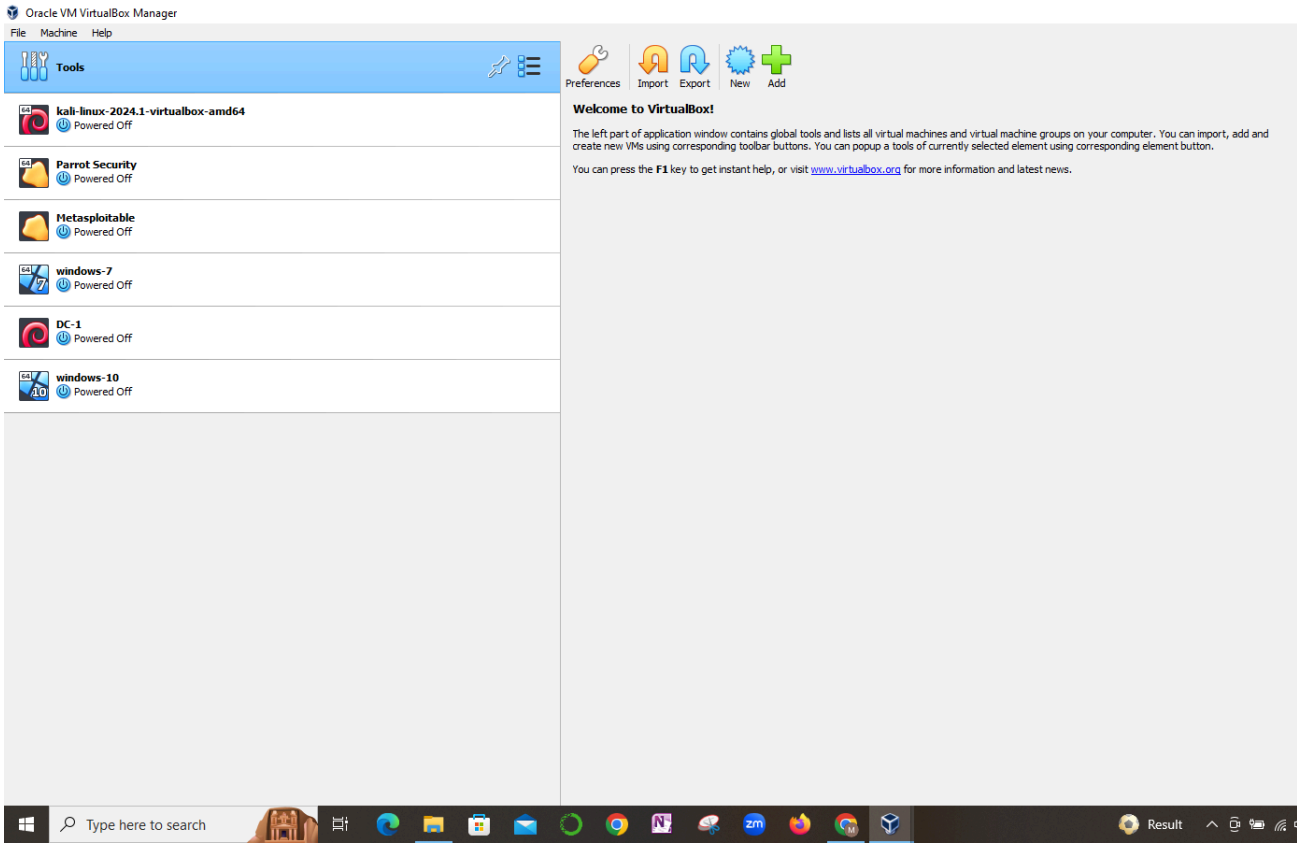


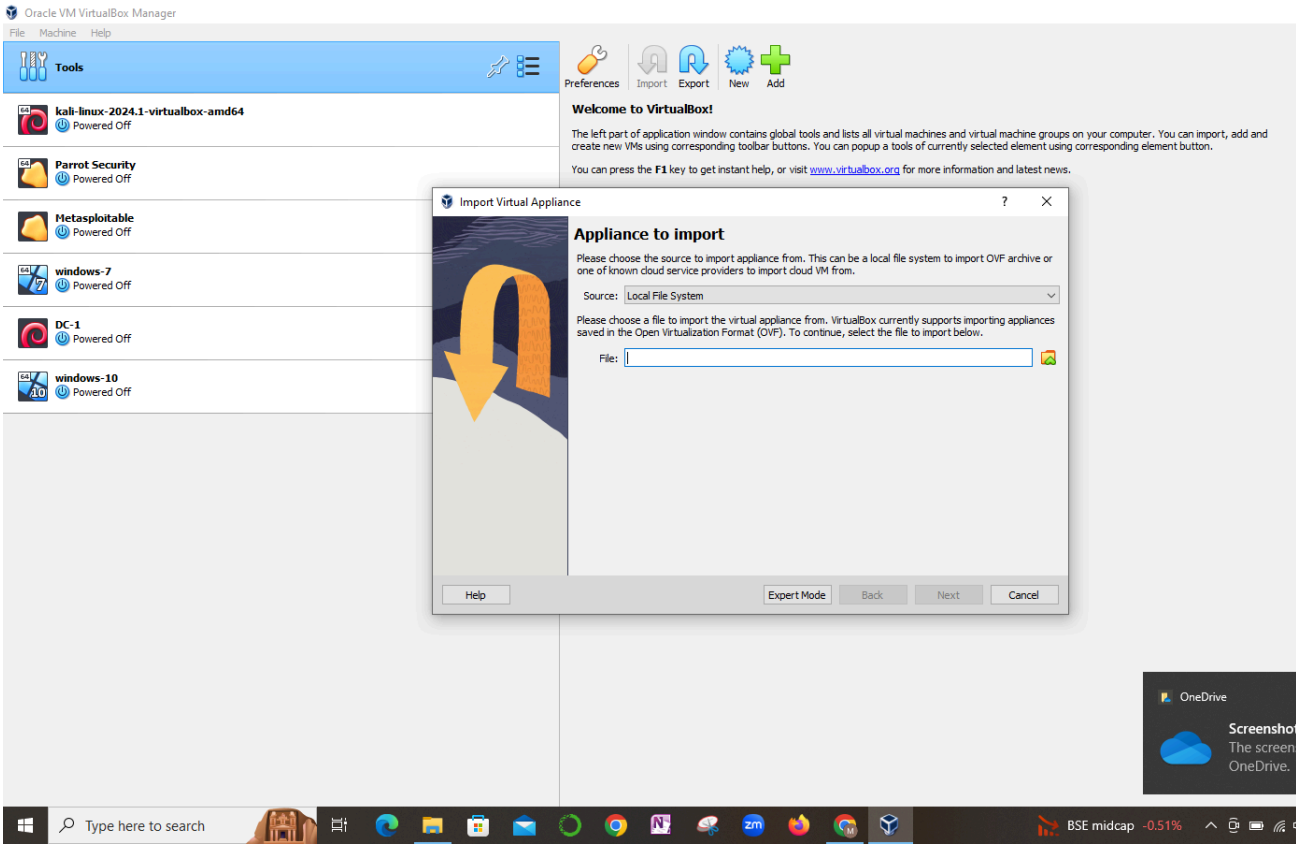
Now from this we need to extract the URL for the decrypted key .

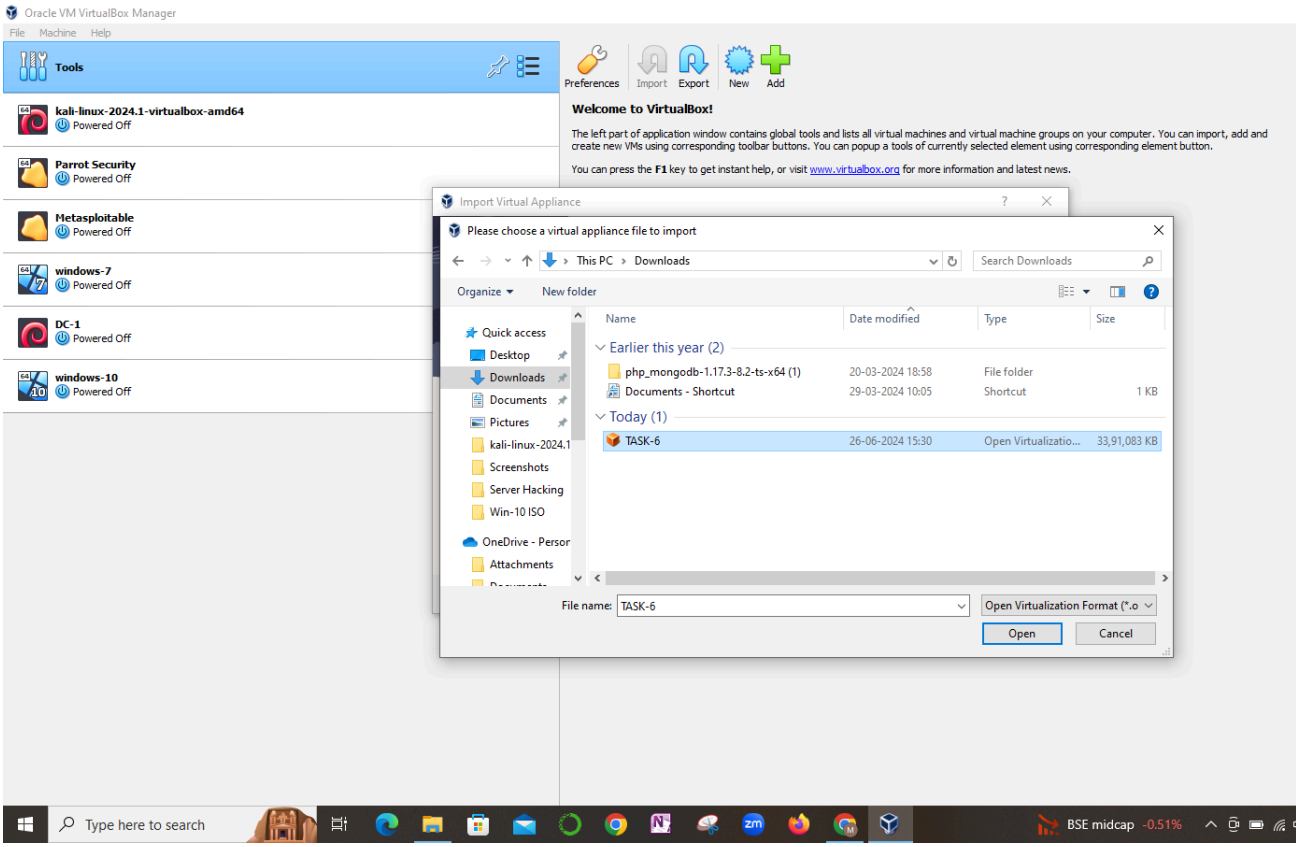
STEP-4: After decrypting download the OVA file from the drive link provided.

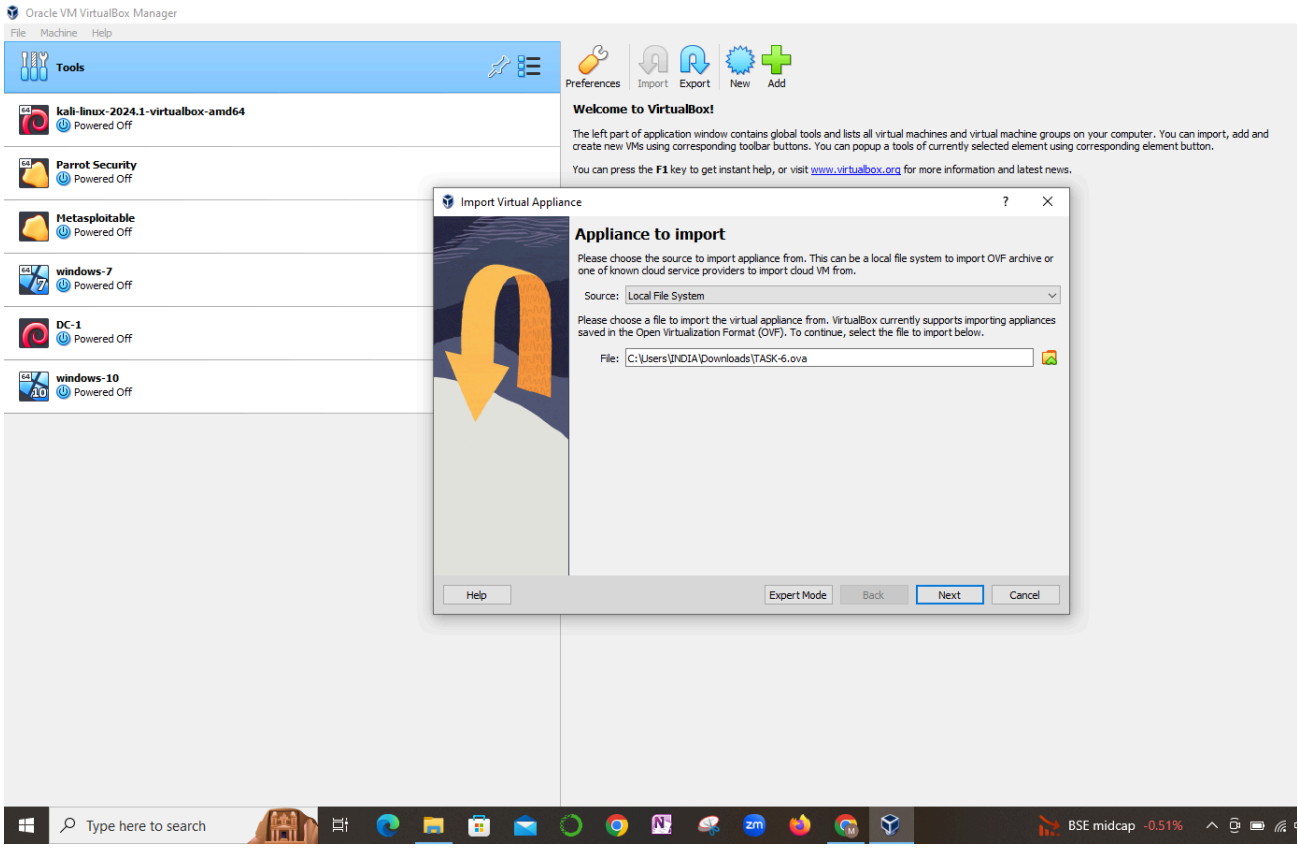


STEP-5: Now , go to kali linux, and navigate to the file option on the left side top options and click on import appliances and select a file under the folder option and click on next and click on finish.

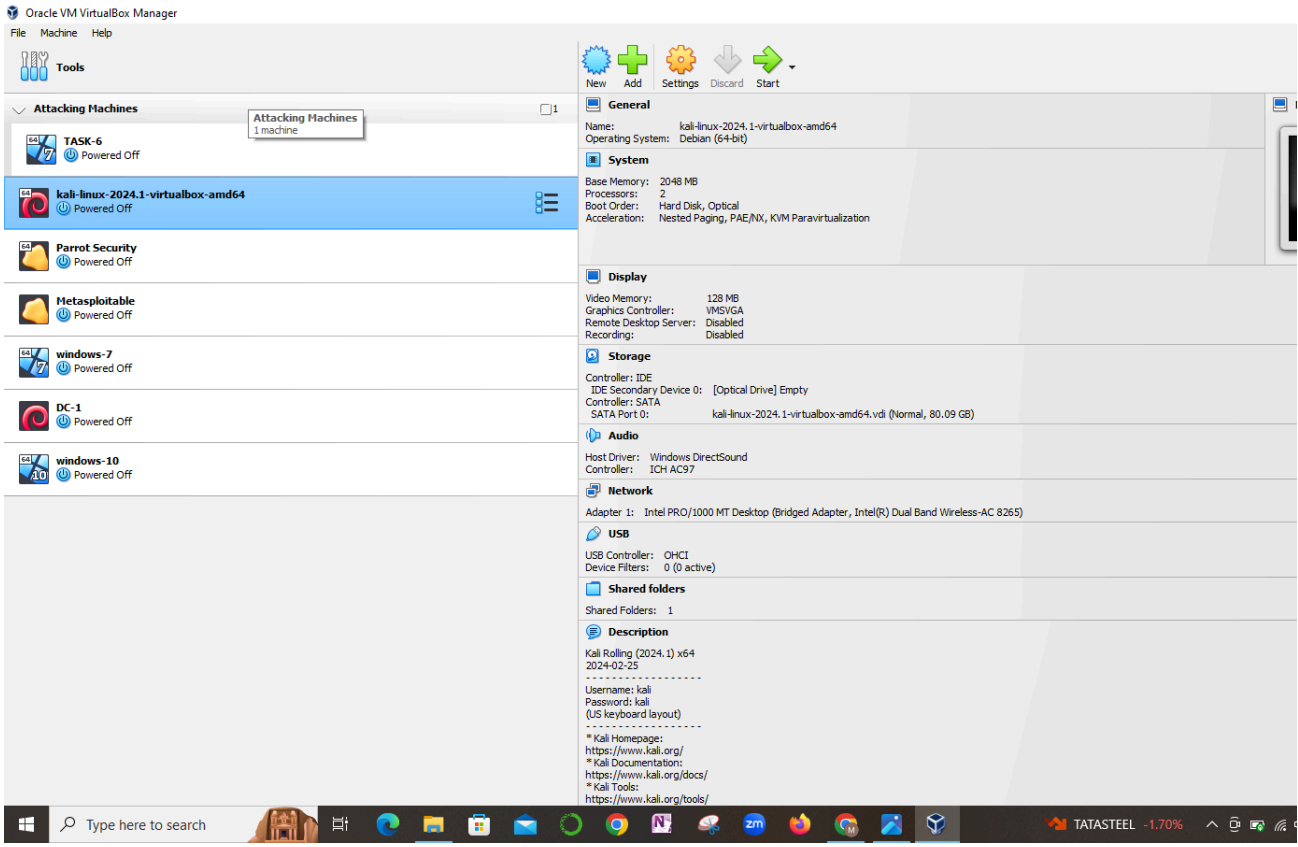



Oracle VM VirtualBox Manager
File Machine Help
Tools
kali-linux-2024.1-virtualbox-amd64
Powered Off
Parrot Security
Powered Off
Metasploitable
Powered Off
windows-7
Powered Off
DC-1
Powered Off
windows-10
Powered Off
Preferences
Import
Export
New
Add
Welcome to VirtualBox!
The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.
You can press the F1 key to get instant help, or visit www.virtualbox.org for more information and latest news.
Import Virtual Appliance
Appliance to import
Please choose the source to import appliance from. This can be a local file system to import OVF archive or one of known cloud service providers to import cloud VM from.
Source: Local File System
Please choose a file to import the virtual appliance from. VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.
File:
Help
Expert Mode
Back
Next
Cancel
OneDrive
Type here to search
BSE midcap -0.51%

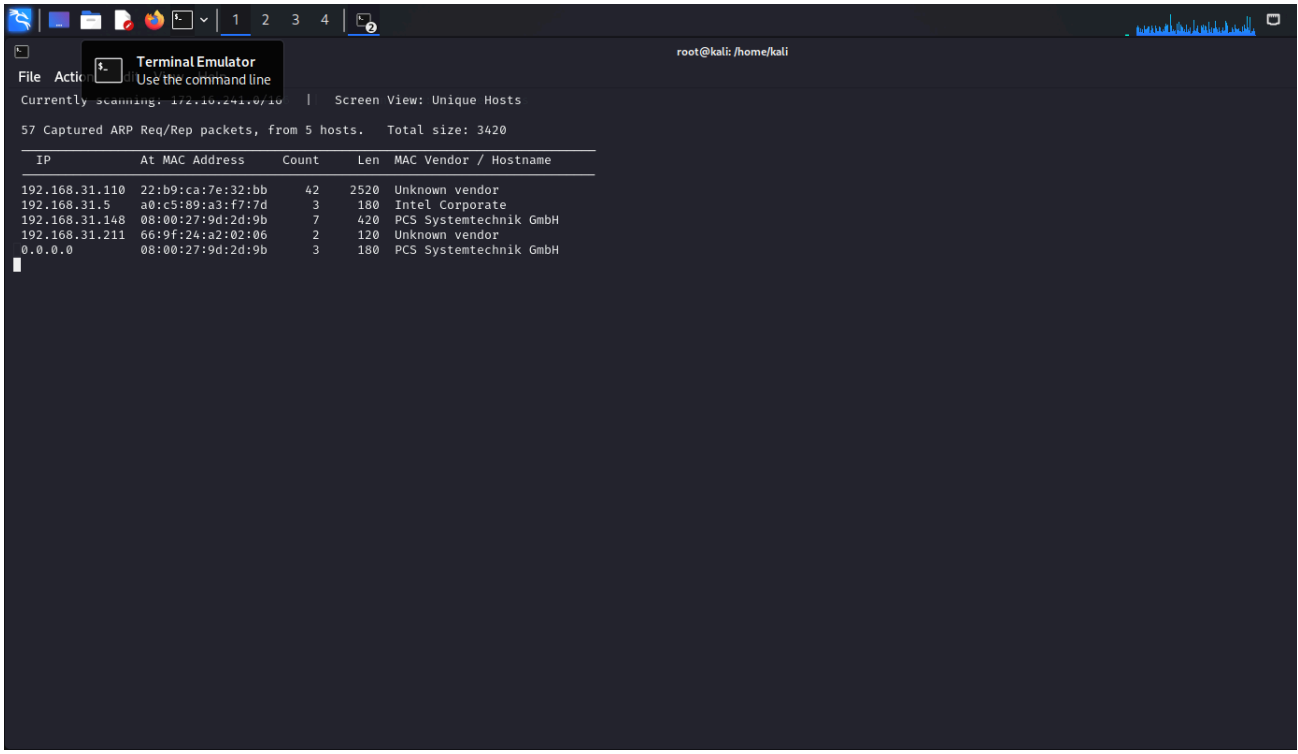

Oracle VM VirtualBox Manager
File Machine Help
Tools
kali-linux-2024.1-virtualbox-amd64
Powered Off
Parrot Security
Powered Off
Metasploitable
Powered Off
windows-7
Powered Off
DC-1
Powered Off
windows-10
Powered Off
Preferences
Import
Export
New
Add
Welcome to VirtualBox!
The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.
You can press the F1 key to get instant help, or visit www.virtualbox.org for more information and latest news.
Import Virtual Appliance
Please choose a virtual appliance file to import
This PC › Downloads
Search Downloads
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
kali-linux-2024.1
Screenshots
Server Hacking
Win-10 ISO
OneDrive - Persor
Attachments
Name
Date modified
Type
Size
Earlier this year (2)
php_mongodb-1.17.3-8.2-ts-x64 (1)
20-03-2024 18:58
File folder
Documents - Shortcut
29-03-2024 10:05
Shortcut
1 KB
Today (1)
TASK-6
26-06-2024 15:30
Open Virtualizatio...
33,91,083 KB
File name: TASK-6
Open Virtualization Format (*.o
Open
Cancel
Type here to search
BSE midcap -0.51%



STEP-6: It's a time taking process and finally the file will be imported as below.



STEP-7:Later, start kali linux and OVA machine. And open kali linux and enter the command “netdiscover”. And the result appears to be like-



B. Gaining Access

Method -2 – Perform Scanning on the imported machine.

Check if it is vulnerable to any exploit

If it is vulnerable, use the exploit to gain access

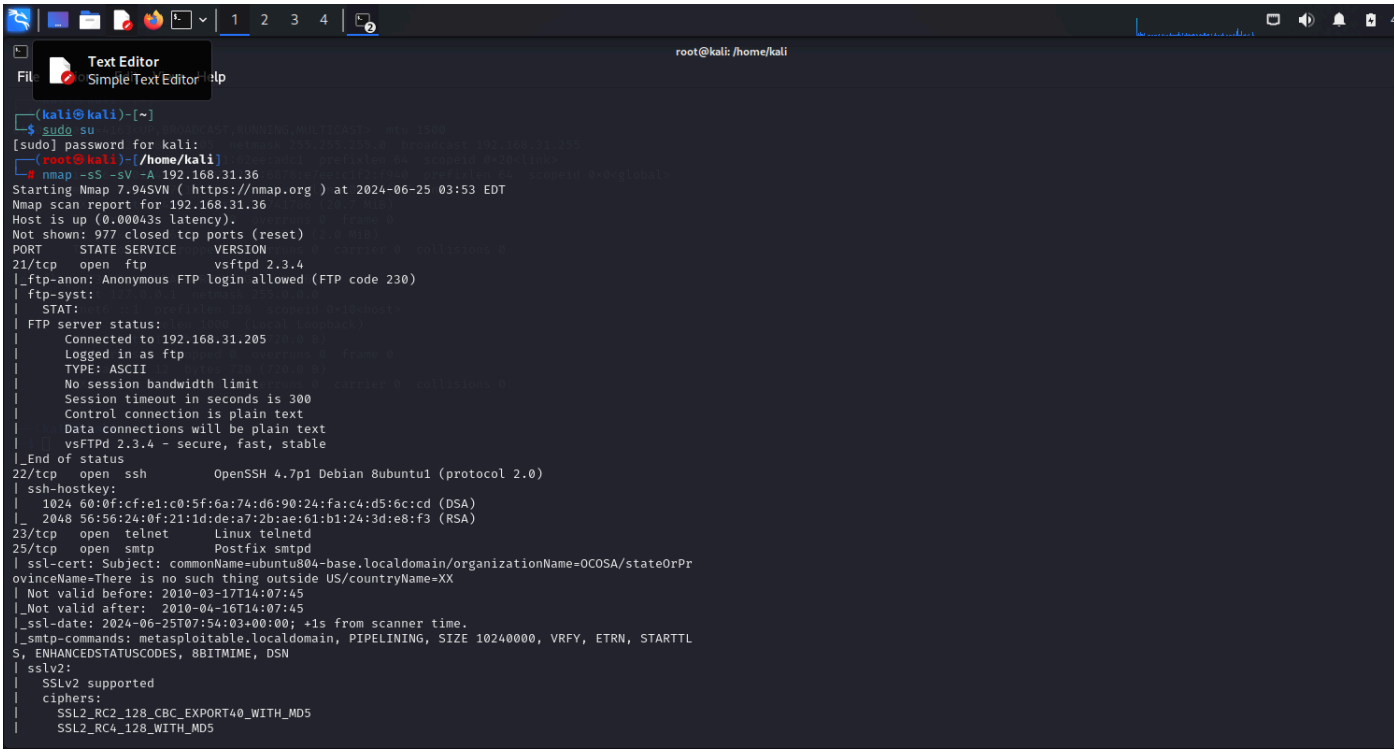
Check the machine, if it consists of any files. .

Steps followed :

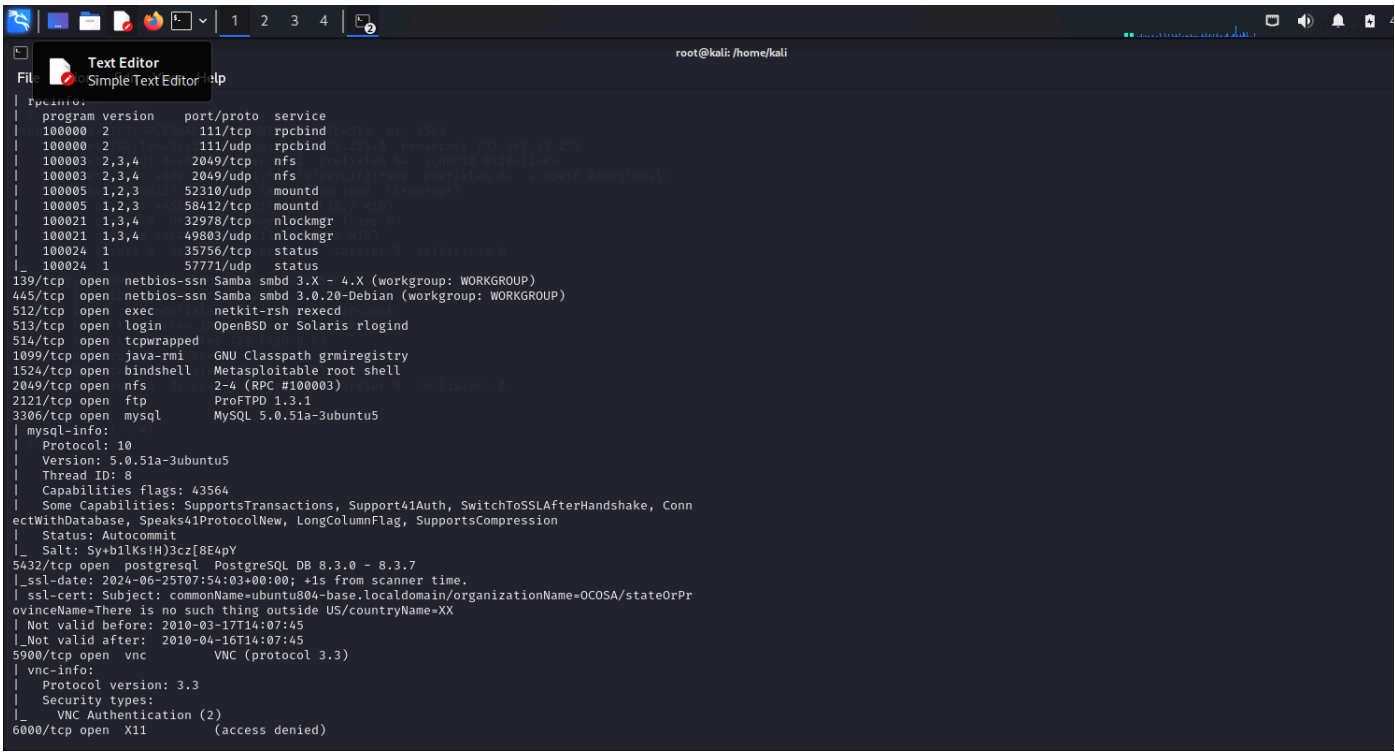
Step 1:Open the VirtualBox Machine and start both Kali Linux and Metasploitable machines.

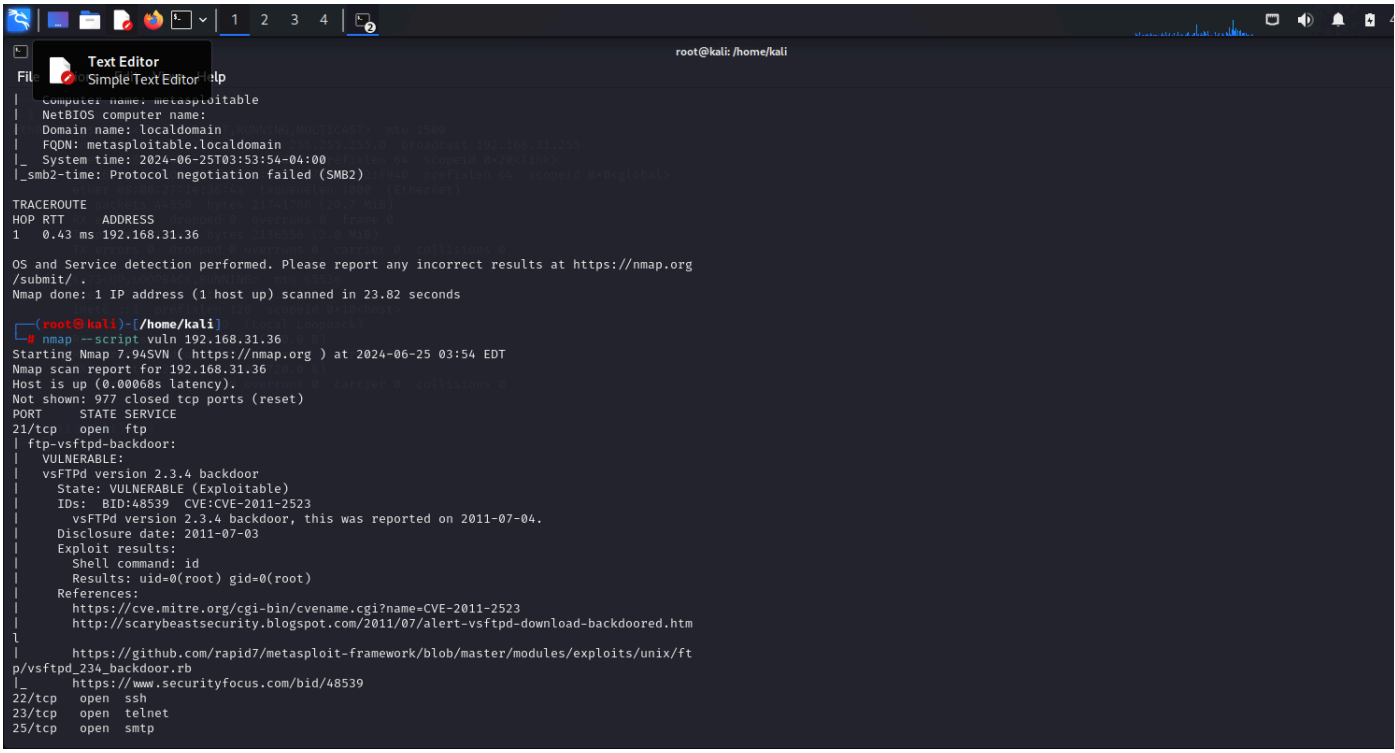
Step 2: Login into the Kali Linux system and to Metasploitable. And then find the Ip address of the Metasploitable machine(because we are going to perform scanning on the Metasploitable machine.)

STEP-3:Now go back to the kali linux system and enter the command “sudo su” to switch to root user.

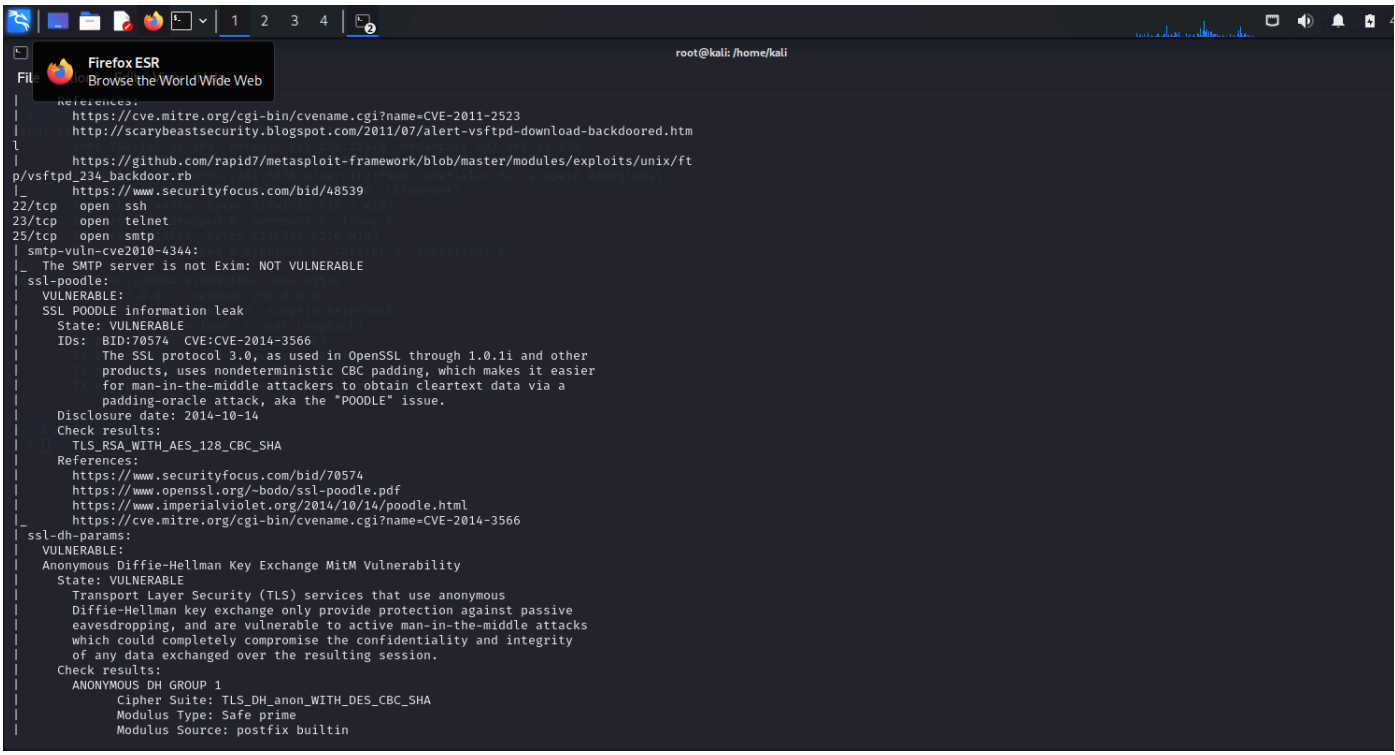


STEP-4:Write the command “nmap -sS -sV -A metasploit-ip address”.Such that it gives the output of all the ports its versions and complete detail.

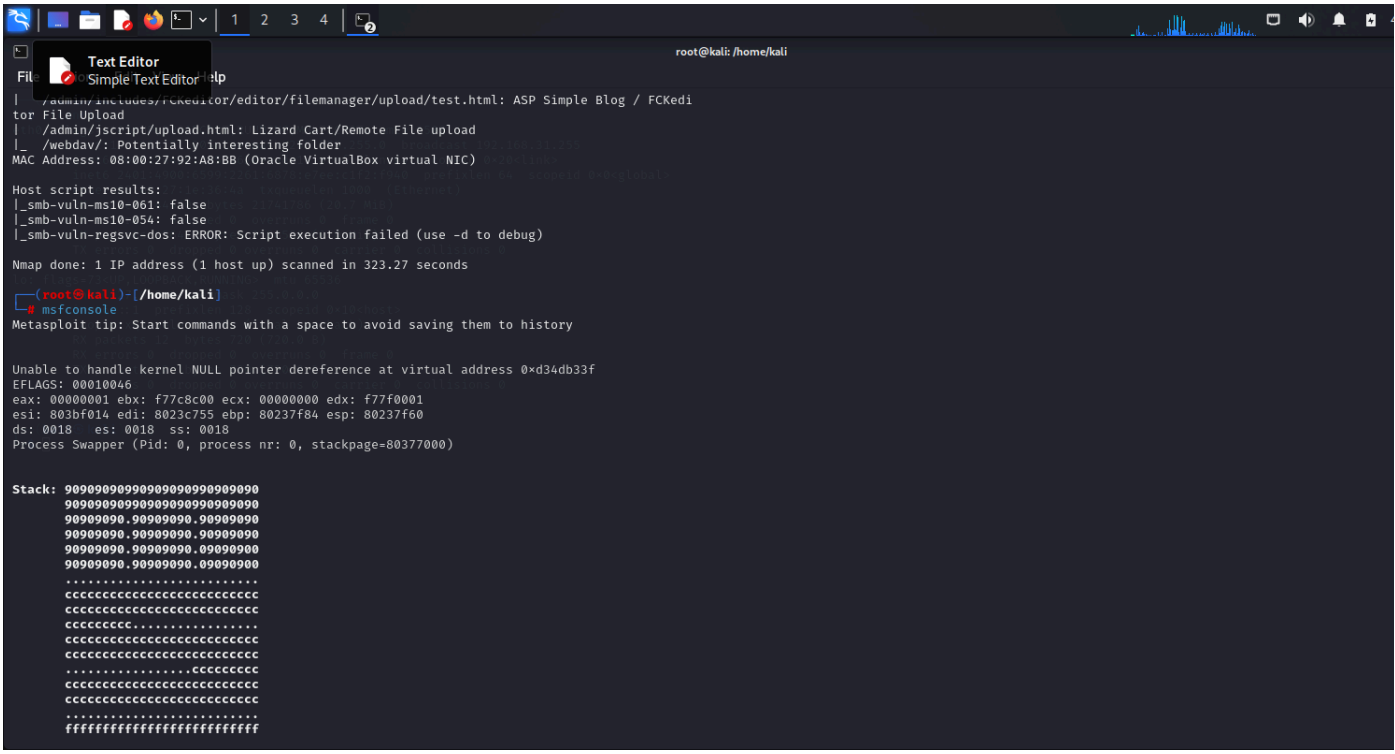




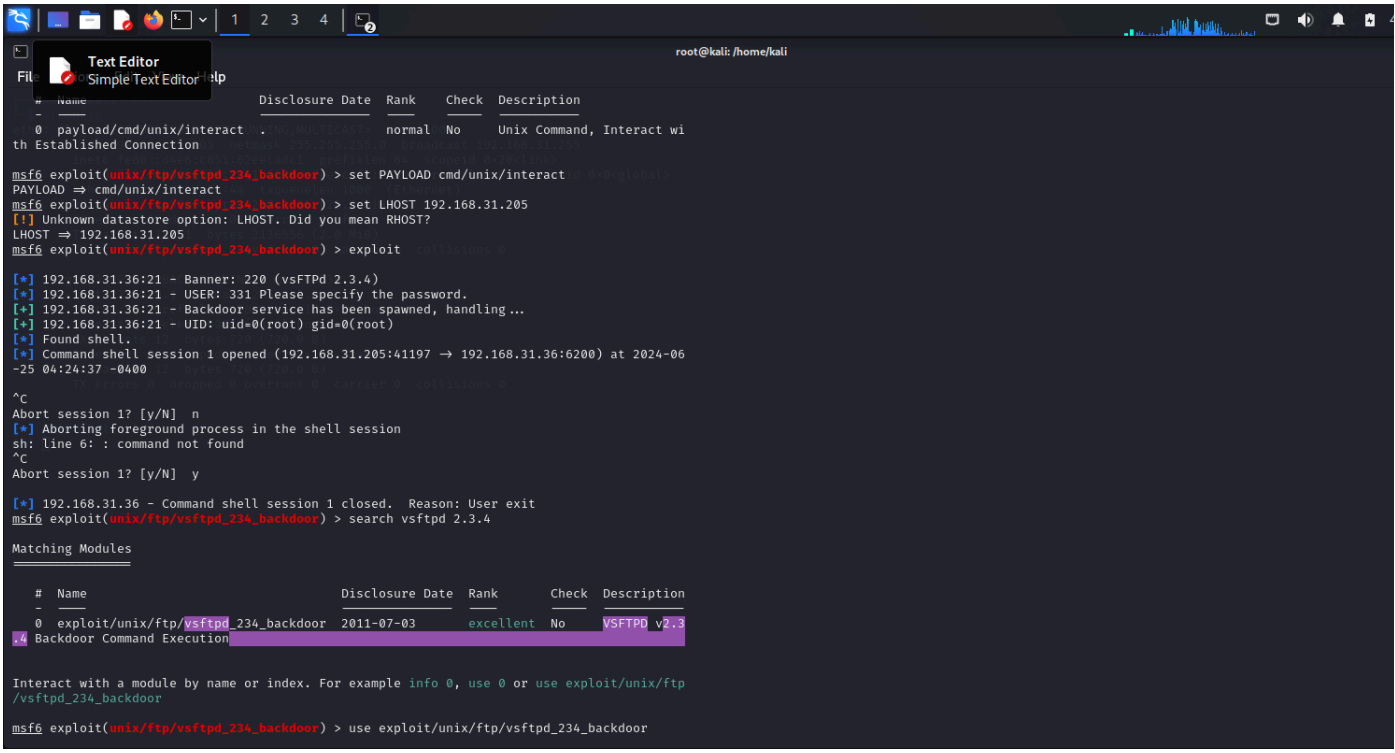
STEP-5:And then give the command “nmap –script vuln “metasploit-ip address” to get the vulnerabilities in that machine.



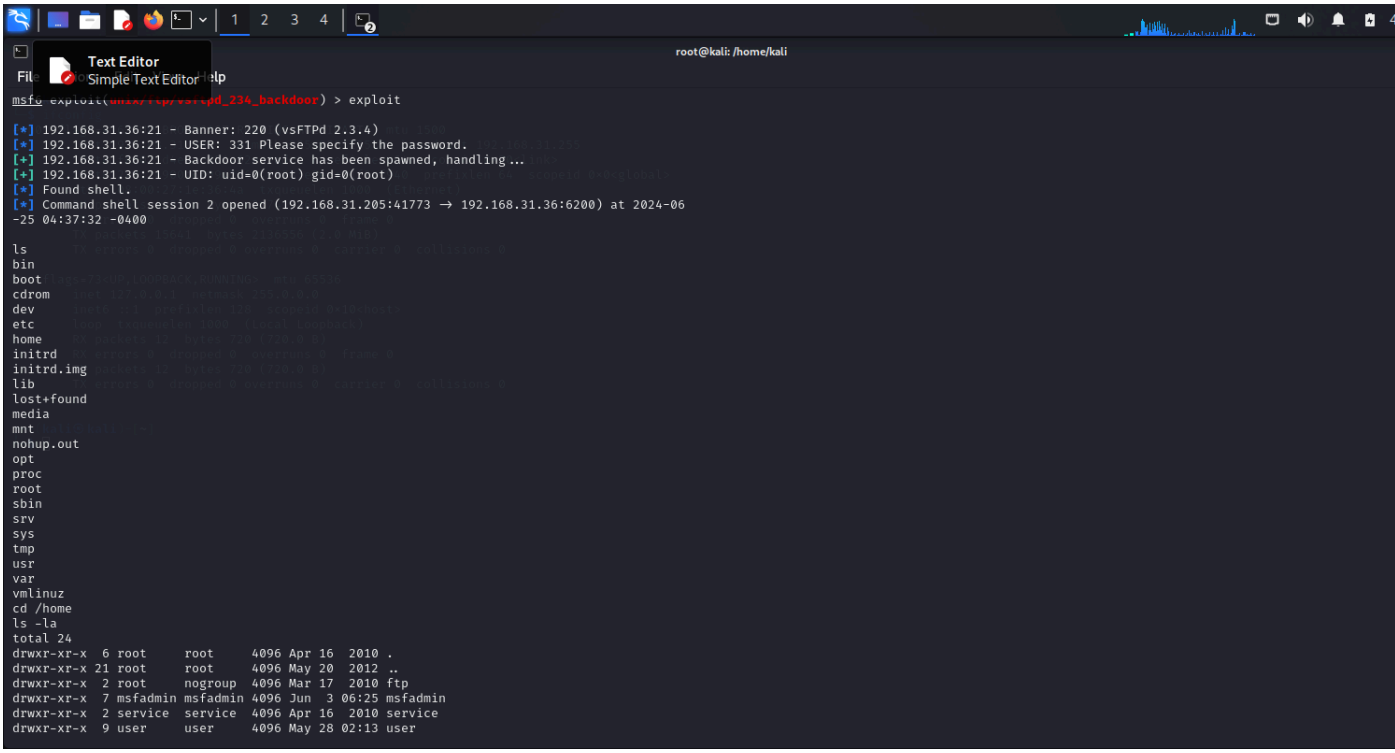
STEP-6:Now start Metasploit framework giving the command “msfconsole”



STEP-7: Search for the exploit version i.e., “search vsftpd 2.3.4”.



STEP-8: Now give the exploit command to enter into exploit console i.e., “use exploit/unix/ftp/vsftpd_234_backdoor”.



STEP-9:Now run the exploit by giving command-”exploit”.

STEP-10: Then the session shell will be created , here now we can check for the further files in the machine and their details.

C. Analyzing the Checksums

<> Check the files in the system

<> Calculate the checksums for it

<> Try to Identify the hidden data inside the Tempered document

<> Identify the FLAG{****}**

Check the files in the system

Calculate the checksum for this

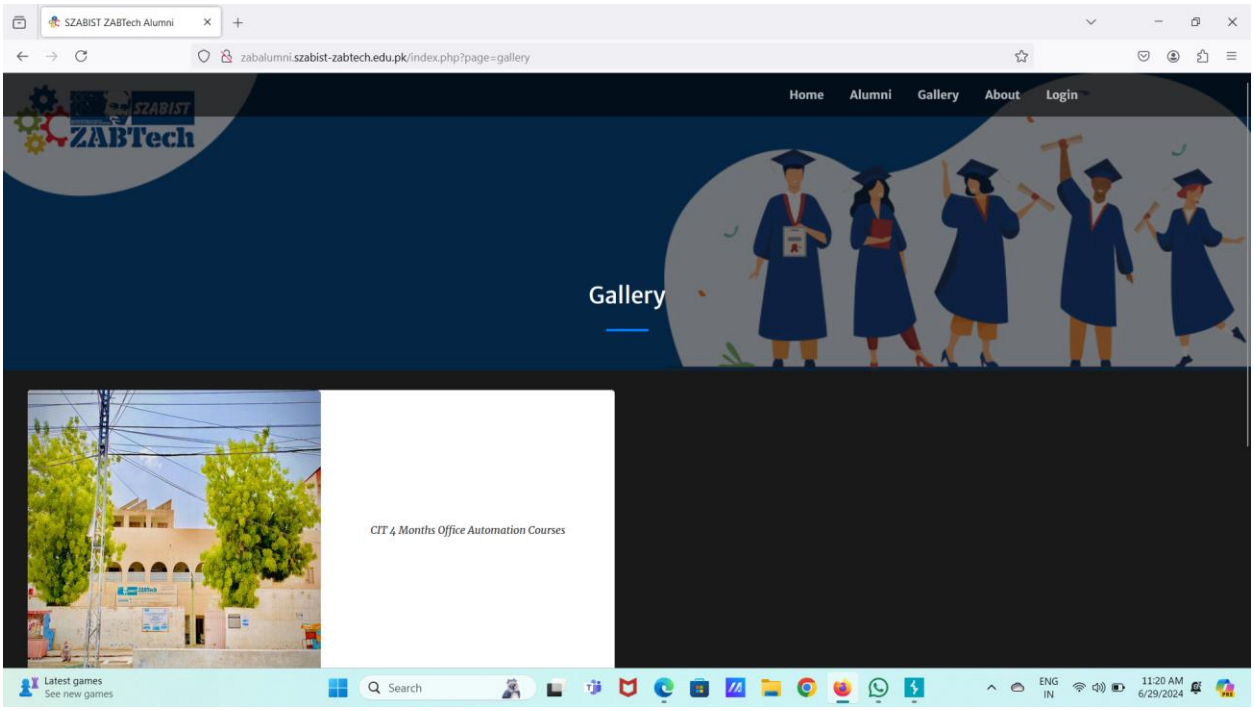
Identifying the hidden data in the files

Now we are able to observe the files in the website

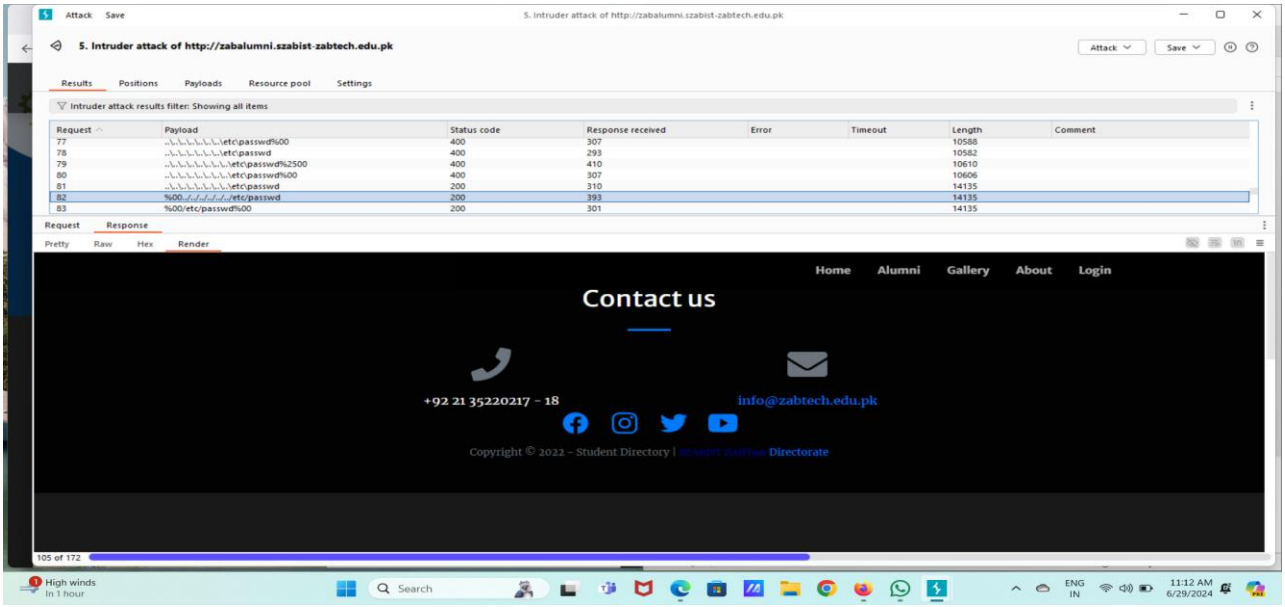
Assignment 7

A. Find 2 websites vulnerable to Directory/Path traversal Vulnerability by using different payloads of Local File Inclusion.

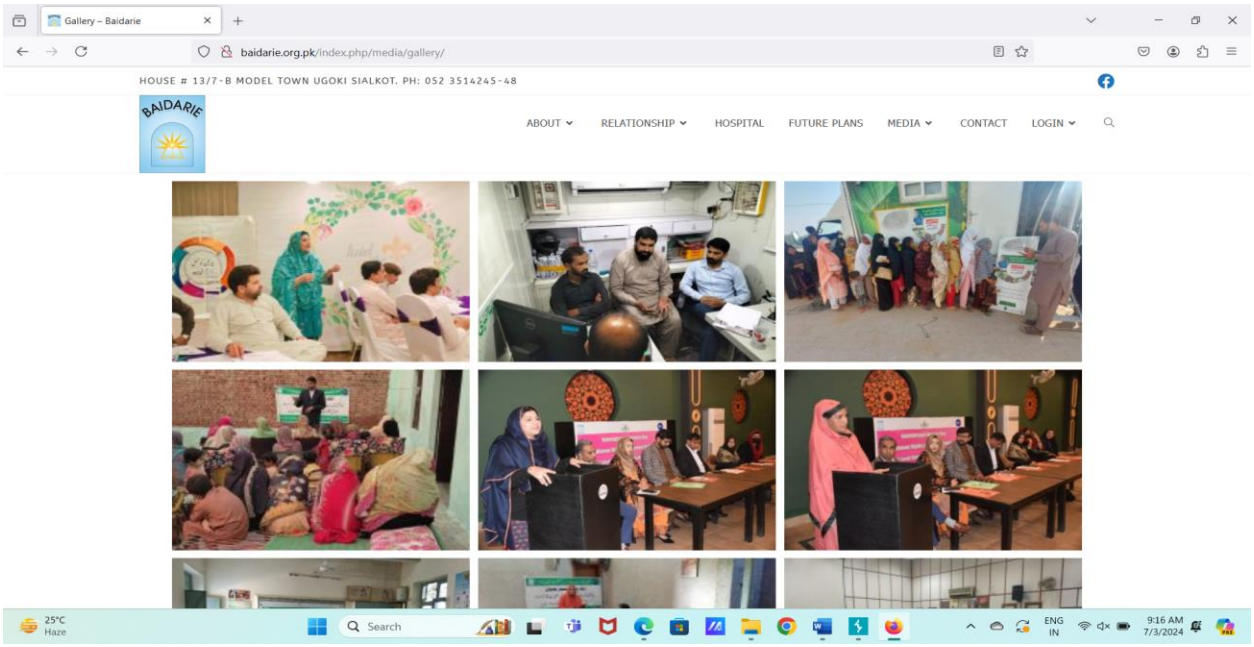
FIRST WEBSITE:



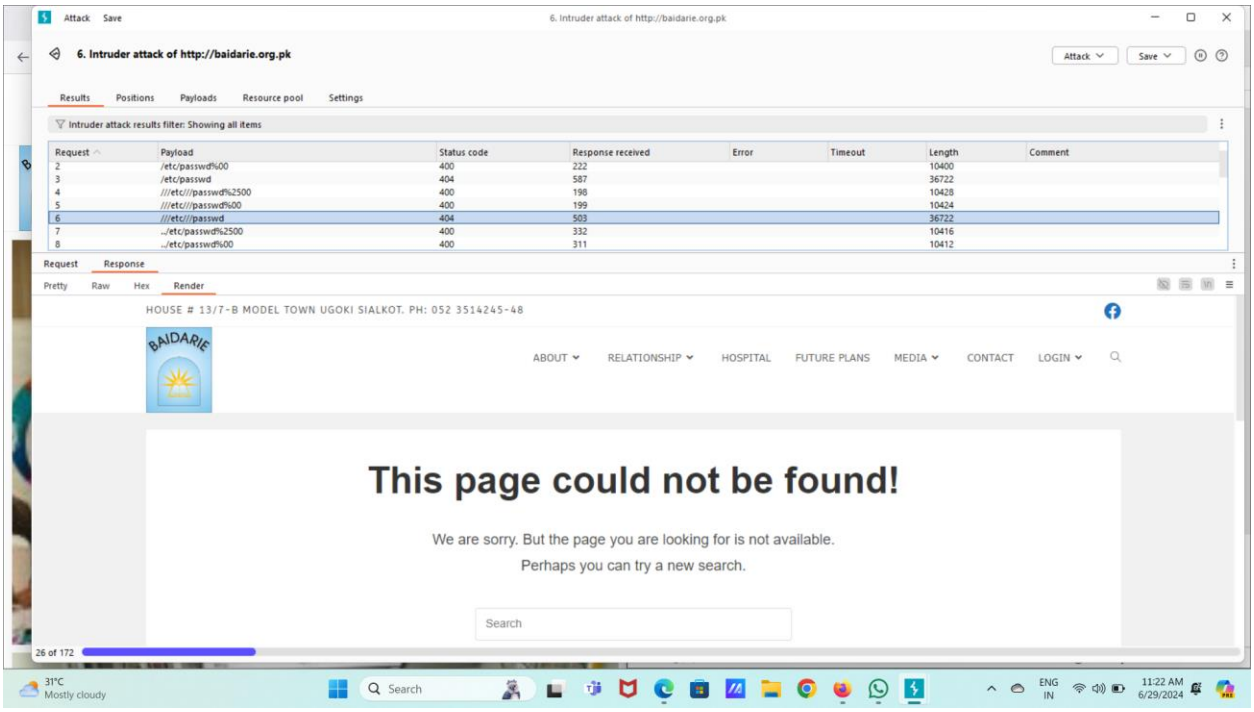
AFTER INCULDE THE LFI TO WEBSITE:



SECOND WEBSITE:

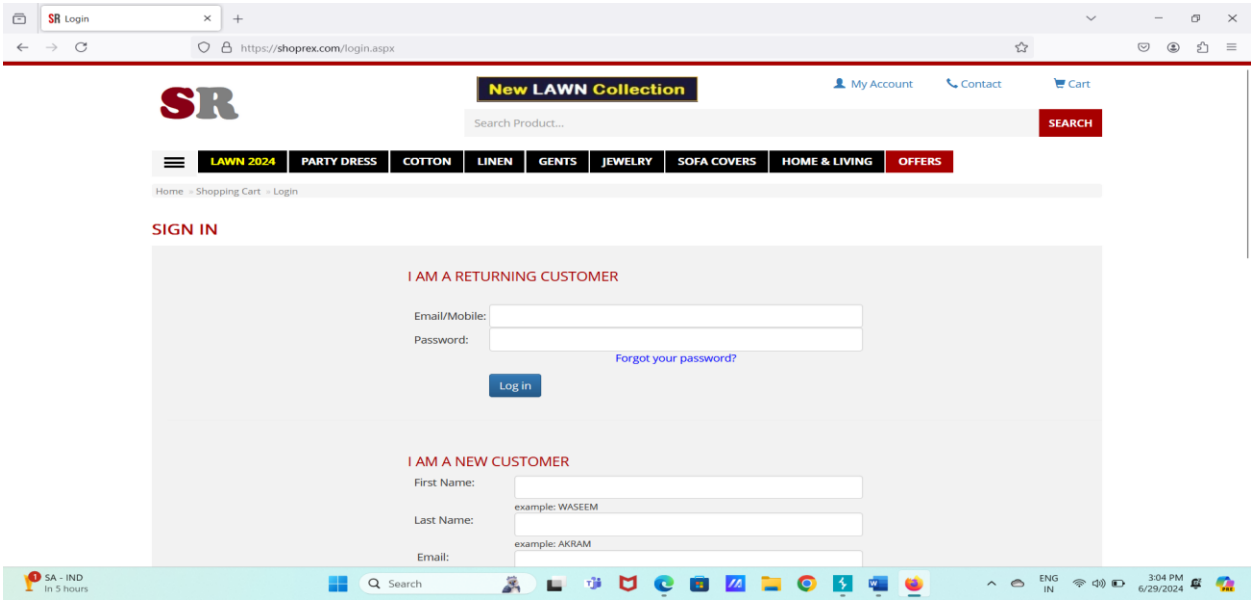


AFTER APPLYING LFI :

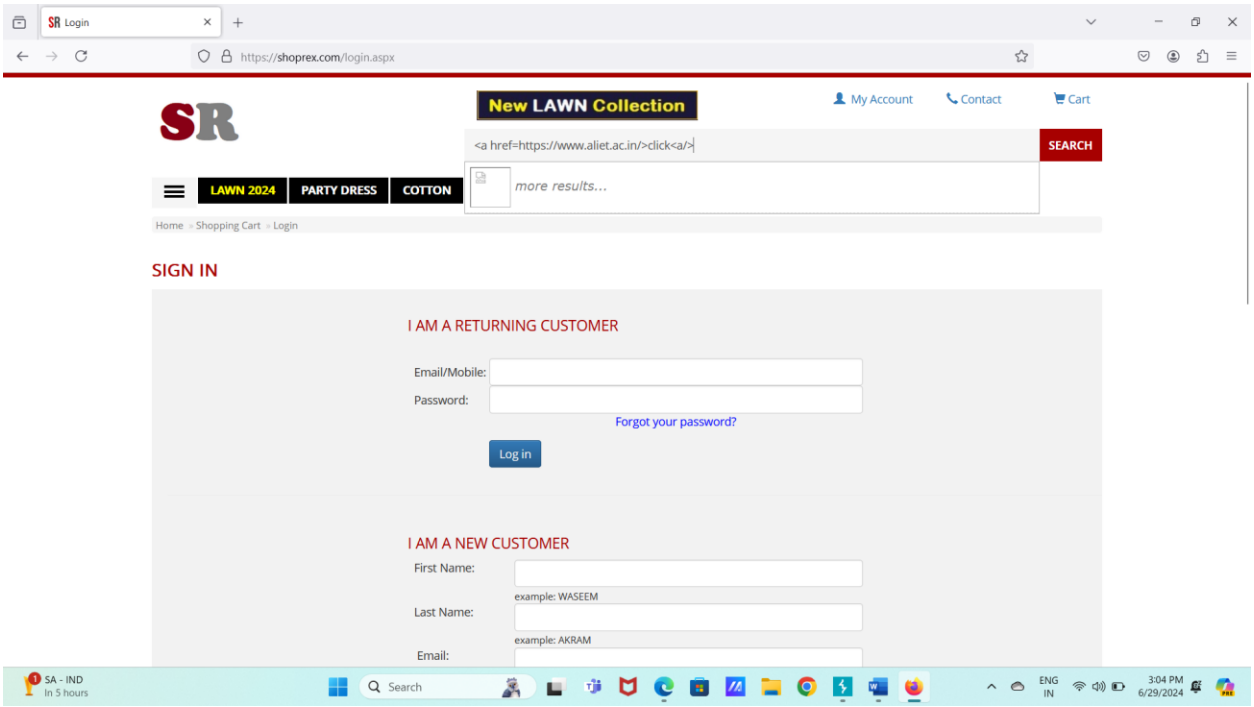


B. Find 2 websites vulnerable to HTML Injection Vulnerability.

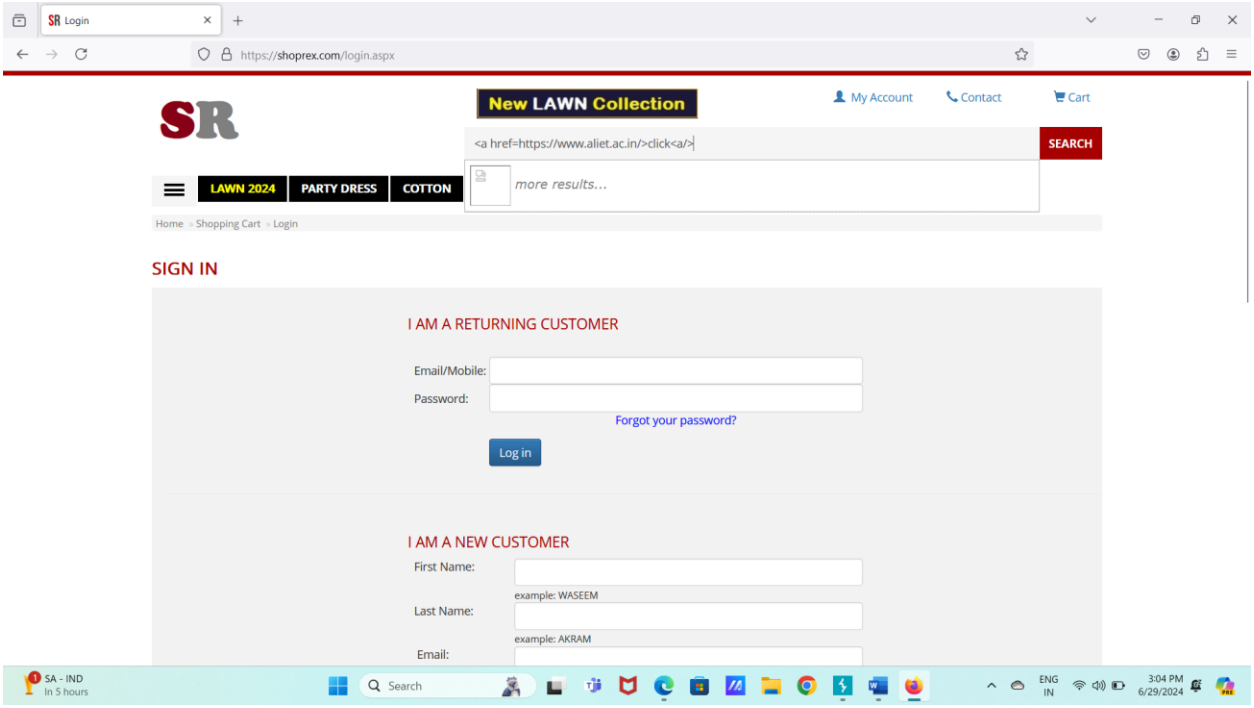
FIRST WEBSITE



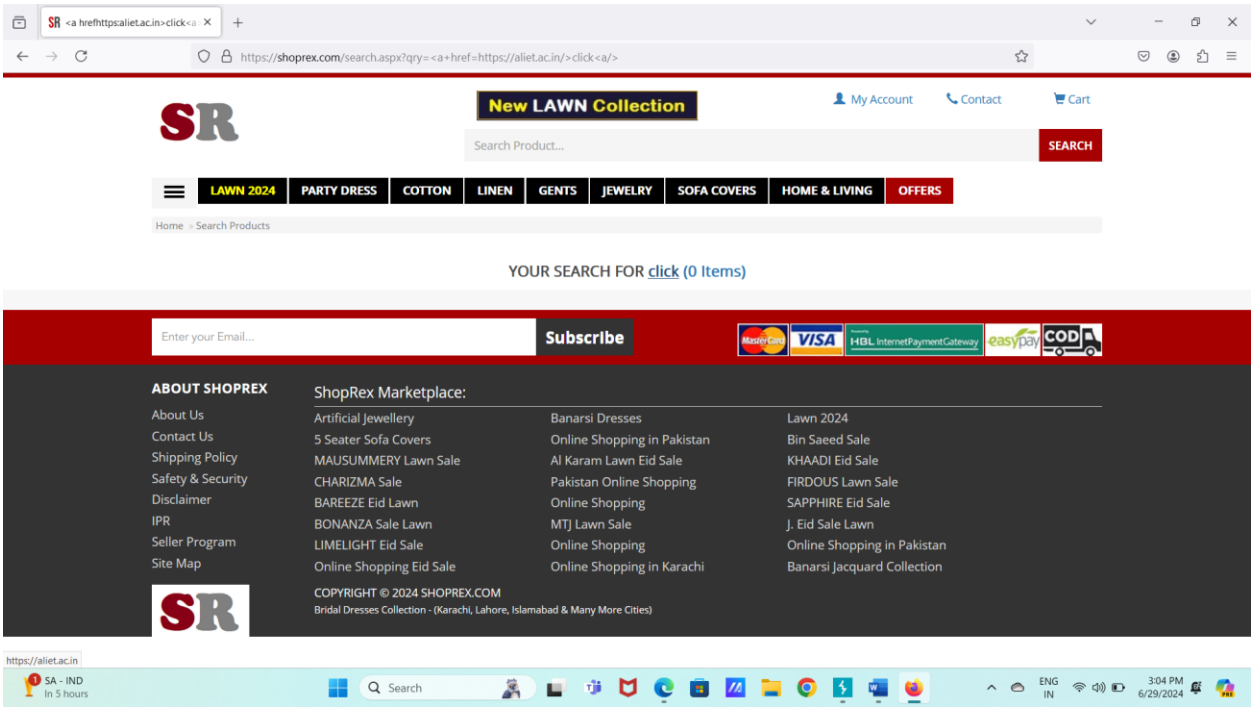
TYPE THE HTML CODE IN SEARCH:



NOW SEARCH THE CODE:

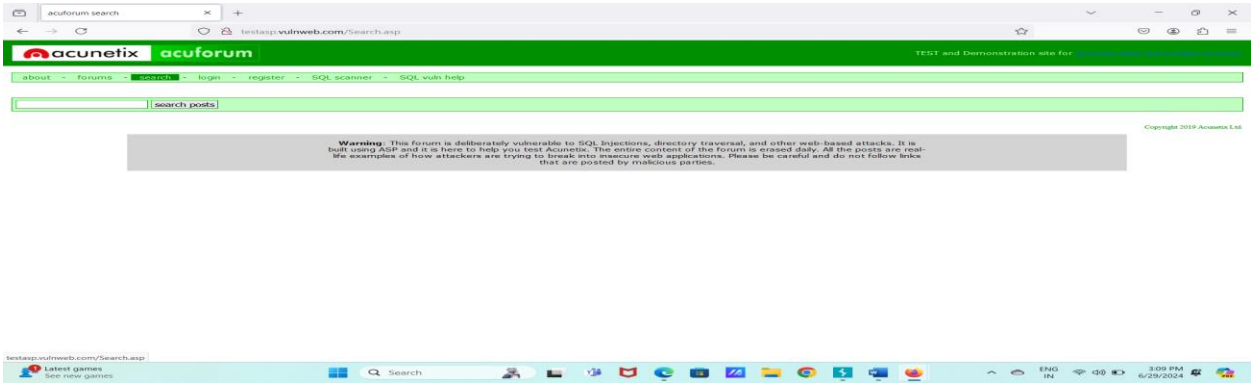


NOW CLICK ON CLICK BUTTON:

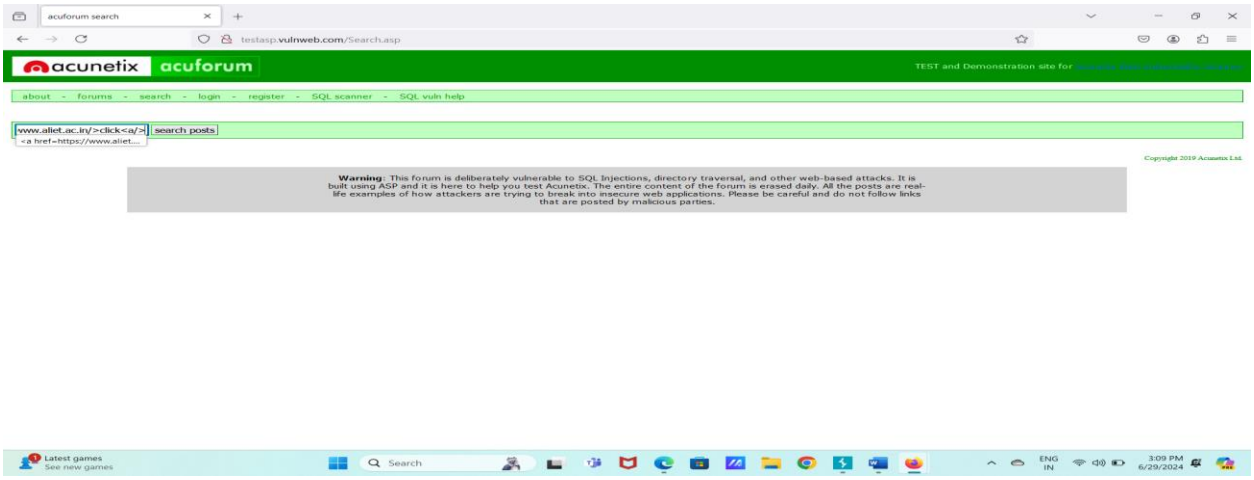


THEN THE PAGE IN OPEN THE WE PROVIDE:

SECOND WEBSITE:

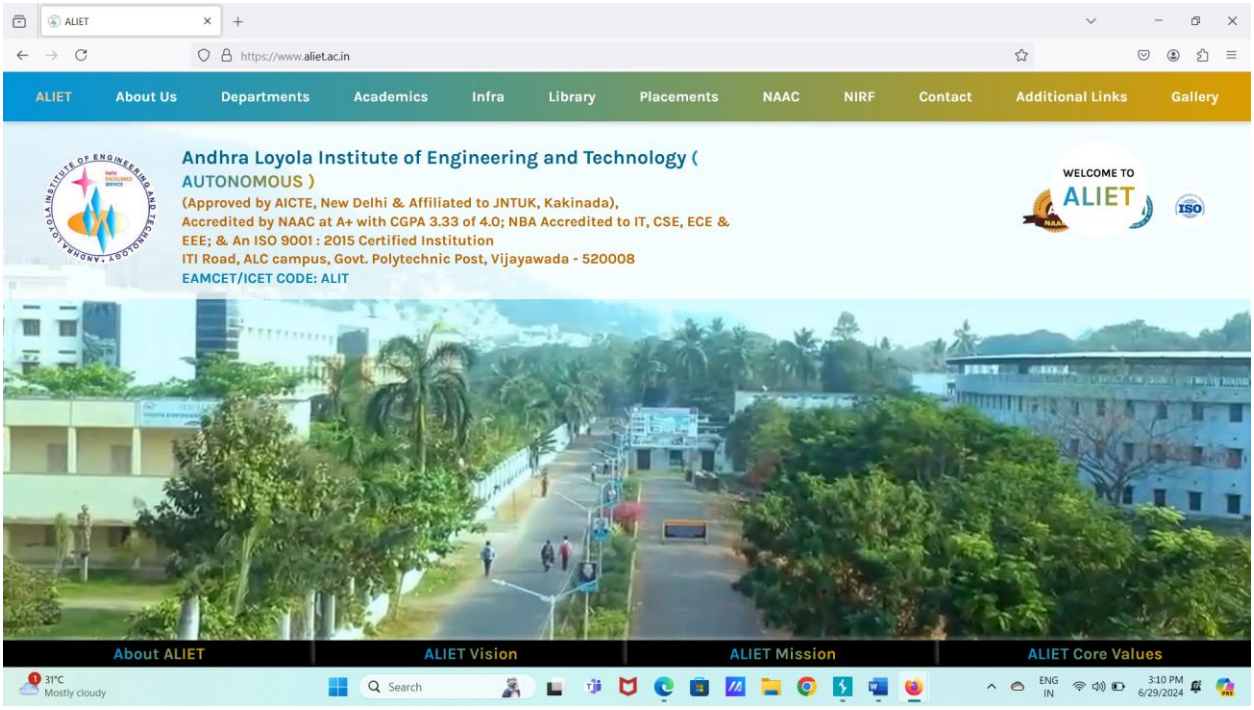


NOW PASTE THE HTML CODE:



NOW CLICK ON BUTTON CLICK:

THEN THE WEBSITE YOU GIVEN IS SHOWN IN THAT:

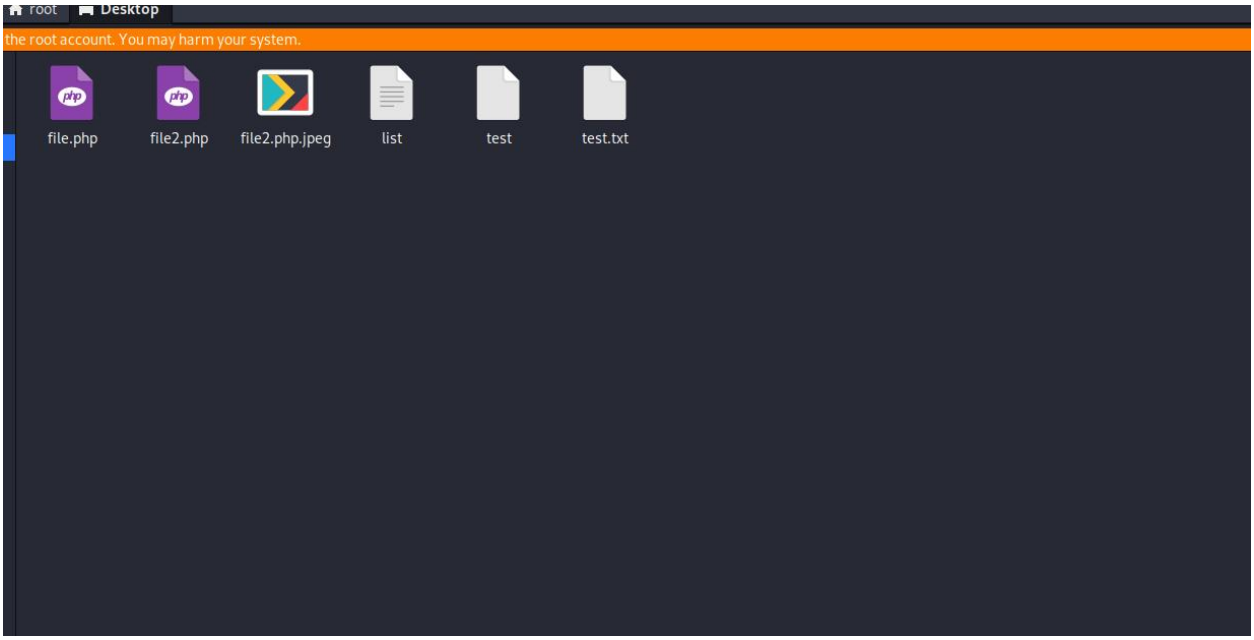


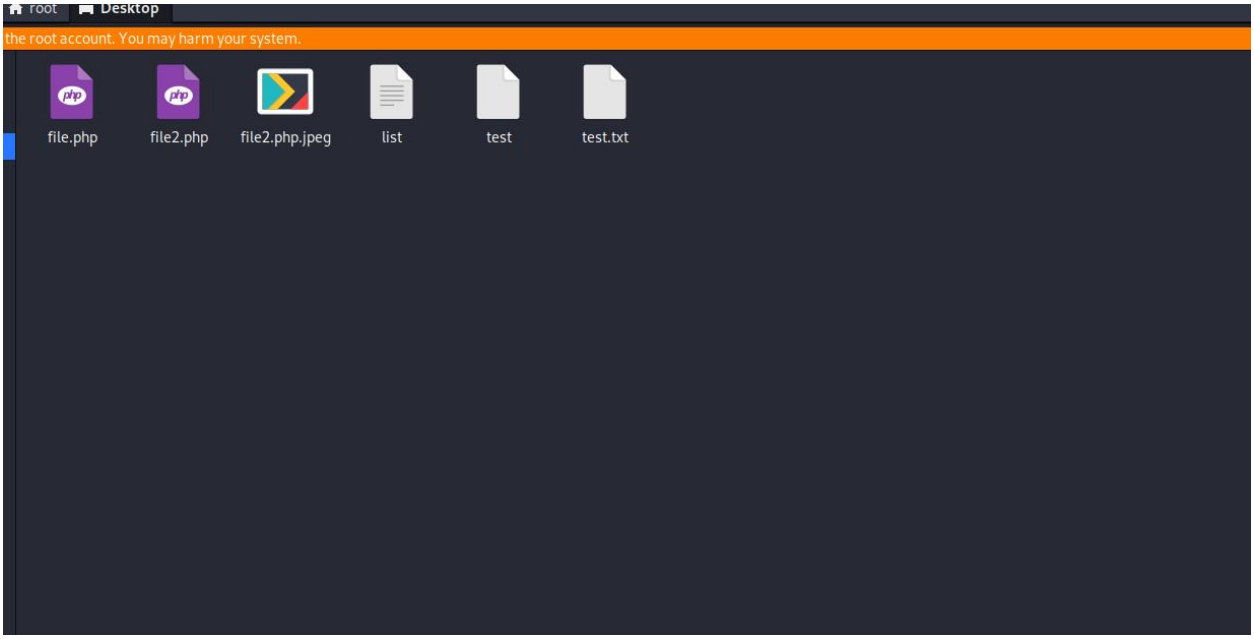
C. Find 2 websites vulnerable to File Upload Vulnerability on each test case below.

a. Uploading larger PDF files than the specified size.

b. Uploading images in the place of pdf.

c. Uploading malicious PHP code in the place of pdf.




root
Desktop
the root account. You may harm your system.
file.php
file2.php
file2.php.jpeg
list
test
test.txt

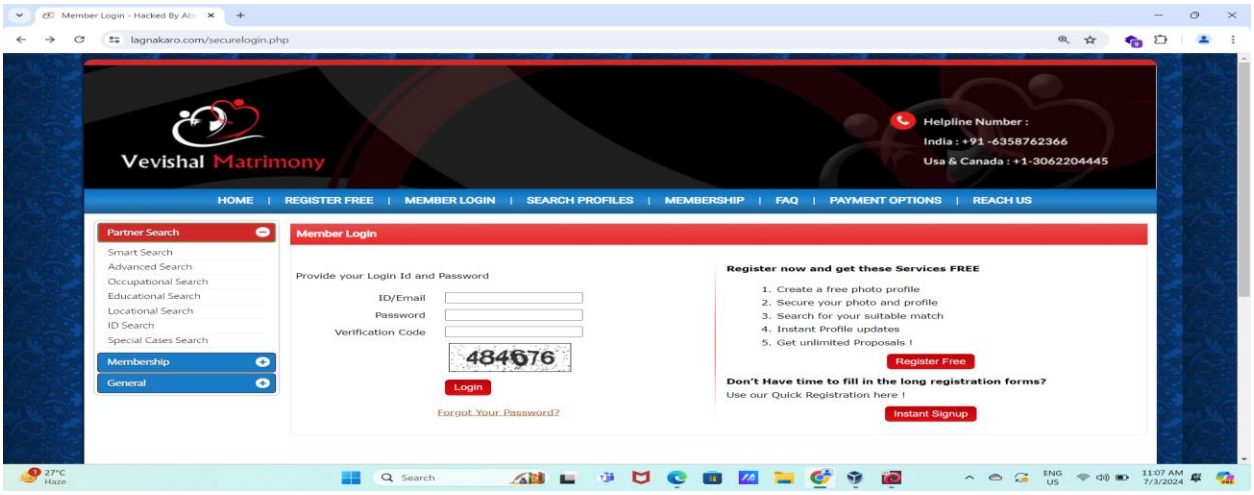
ASSIGNMENT-8

B. Perform SQL Injection on given targets and dump the data from databases

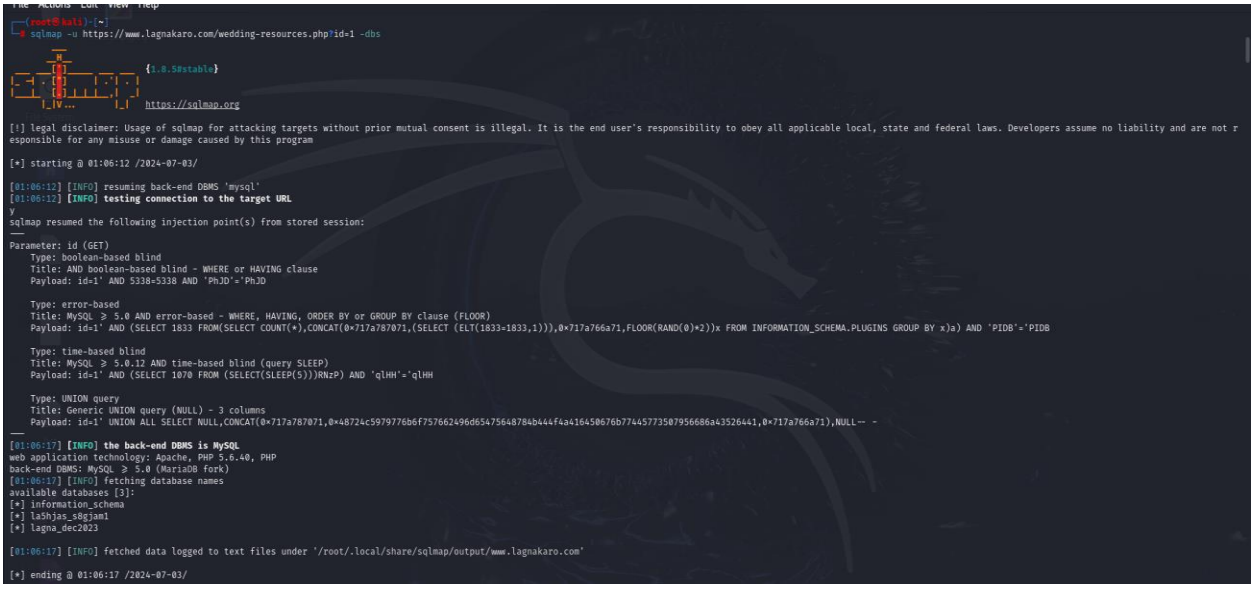
. a. https://www.lagnakaro.com/

b. https://comand.edu.pk/

A)

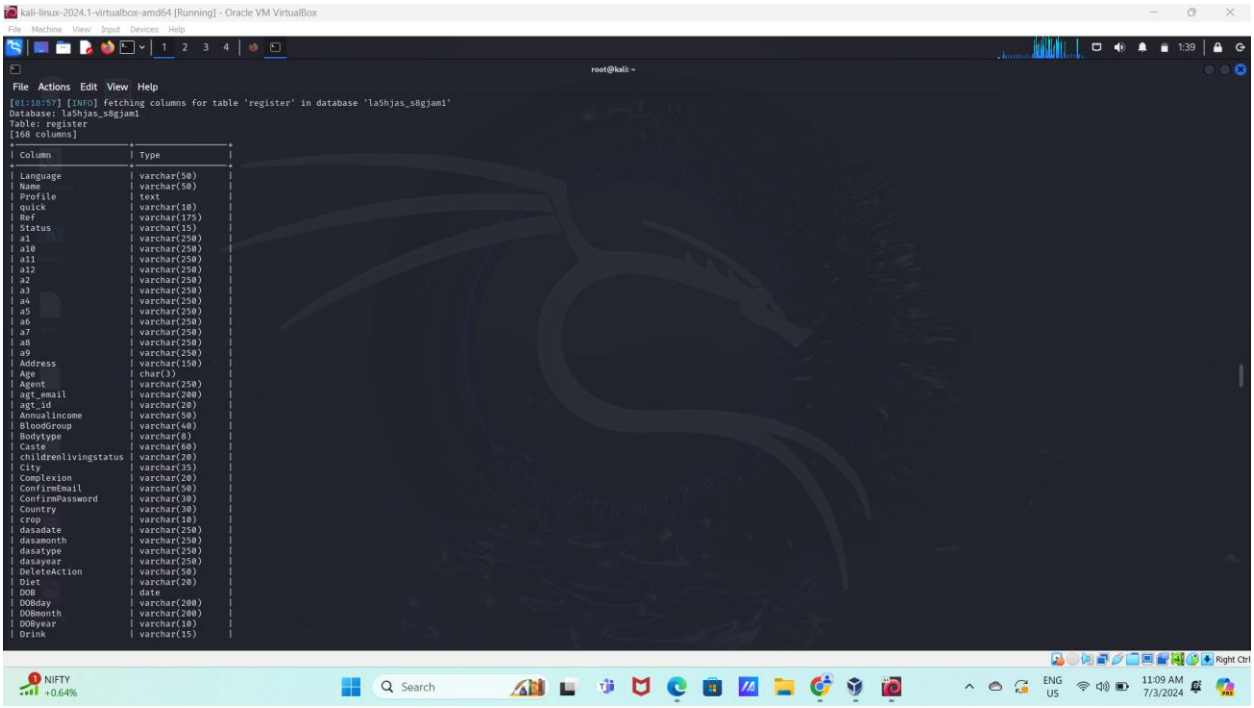


NOW ON SQLMAP SEARCH IT:

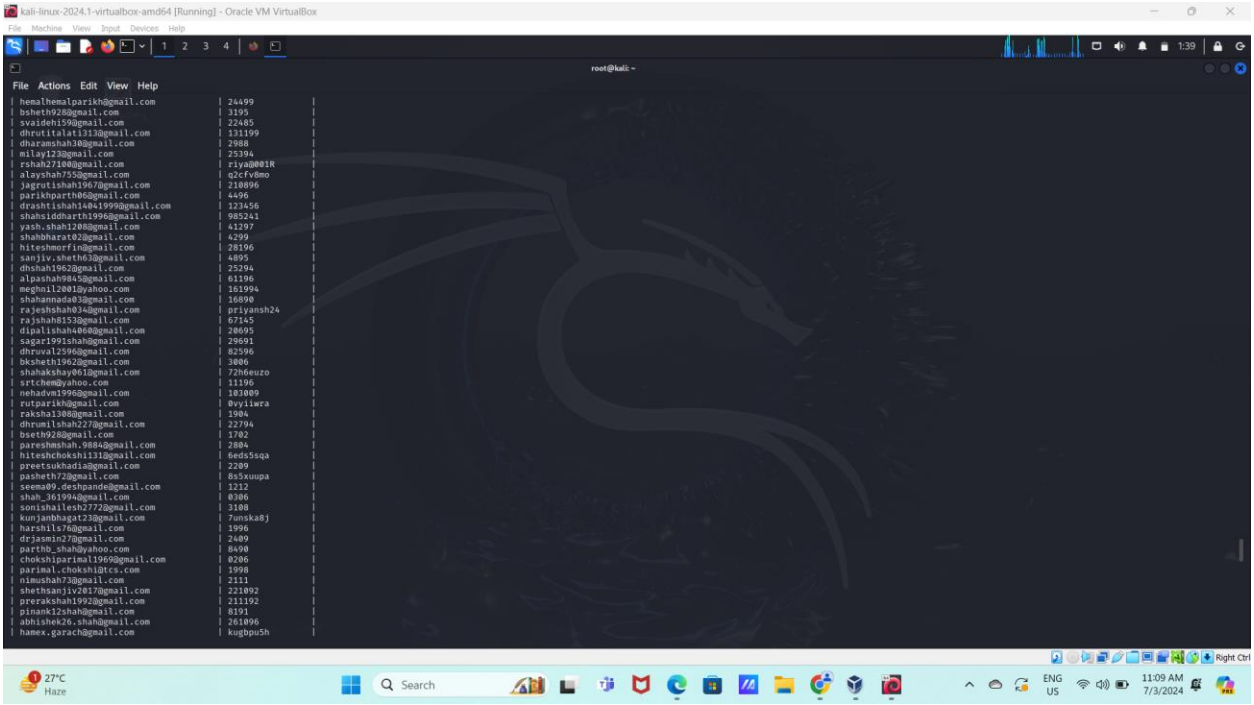


AFTER THAT WE SEEN THREE DATABASES:

NOW OPEN DATABASE



ALSO OPEN THE COLUMS:

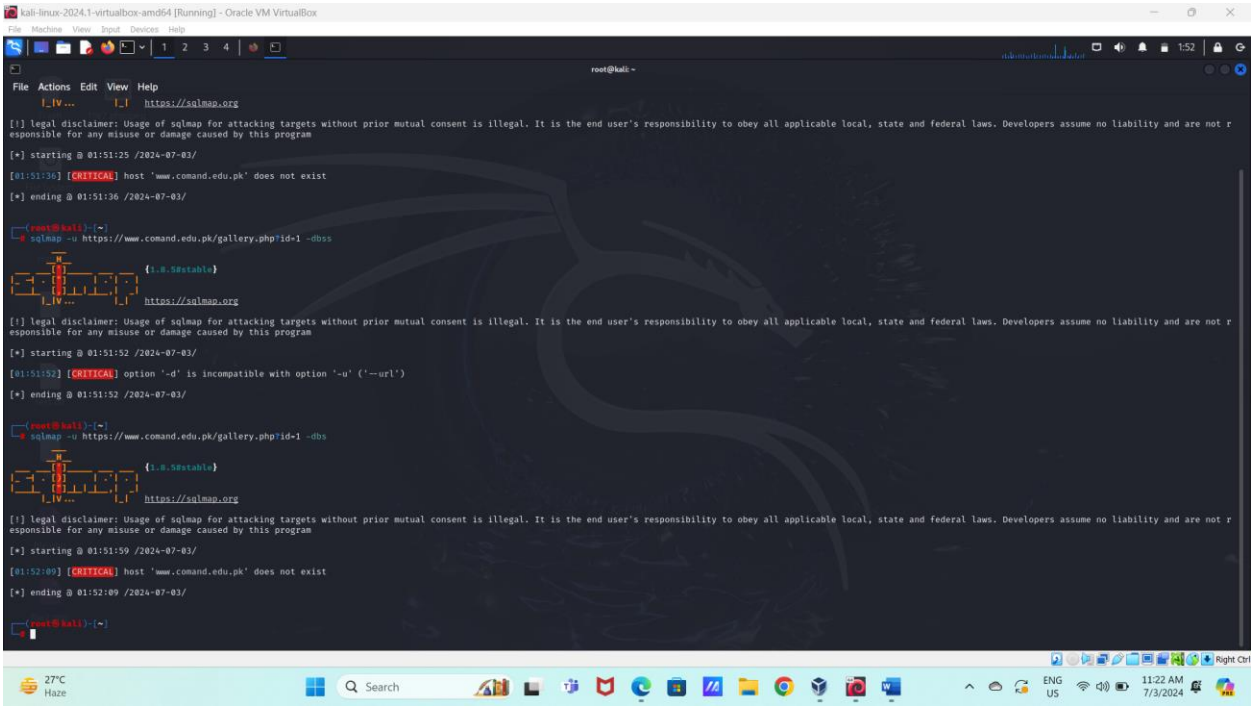


THAT IS THE DATA PRESENT IN TABLES

B)

THE WEBSITE IS NOT THERE

AND ALSO IT CAN’T FIND IN SQLMAP



A. Find websites vulnerable to Insecure Design Flaws on each test case mentioned below.

a. No password policy

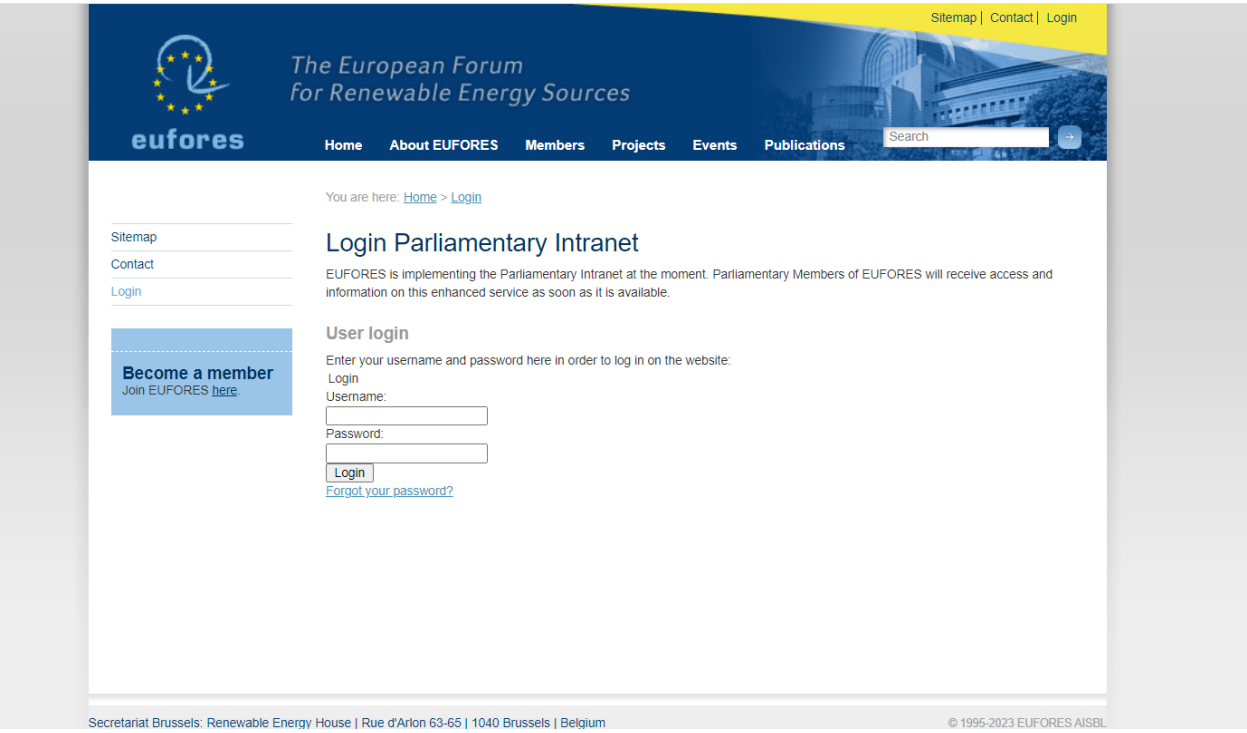
b. Password reset link is not getting expired

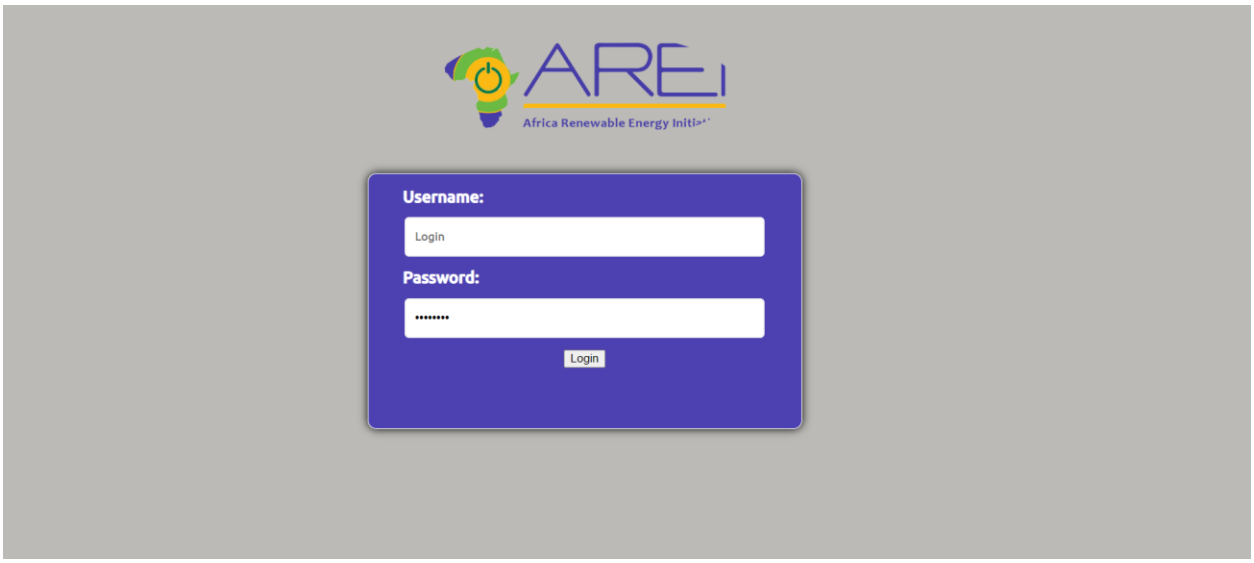
c. Automatic email confirmation bug

d. Password reset link sent with http

e. Exposure of private information (privacy violation)

f. Old session doesn't expire

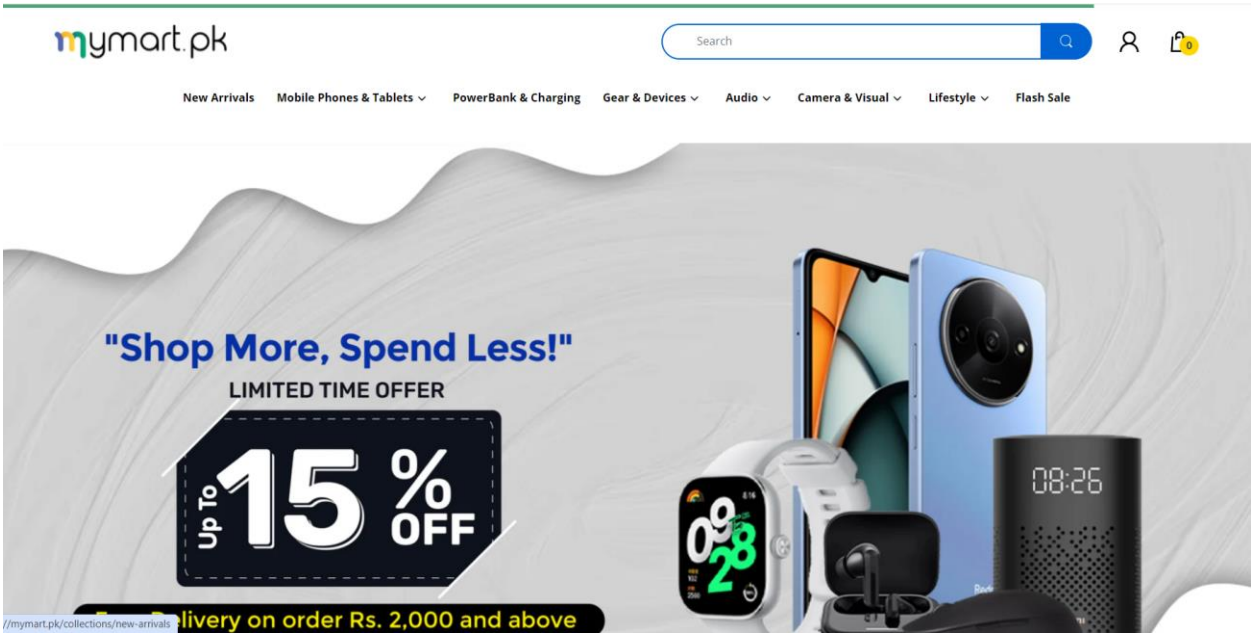




C. Find a website vulnerable to Business Logic Errors on each test case below

. a. Currency Arbitrage

b. Delivery Charges Abuse



SR

New LAWN Collection

My Account | Contact | Cart

Search Product... SEARCH

LAWN 2024 | PARTY DRESS | COTTON | LINEN | GENTS | JEWELRY | SOFA COVERS | HOME & LIVING | OFFERS

Home » Clothing » Women's » Lawn Price in Pakistan

Lawn Dresses 2024 Collection

Lawn Dresses 2024 is the most demanded and loved fabric in Pakistan. This fabric is ideal for Pakistan's weather throughout the year. Its softness and comfortable feel is admired by almost every Pakistani women. To help the audience in Pakistan to select lawn dress for themselves every big ... Read More

BROWS BY CATEGORY : Luxury Embroidery Lawn | Stitched Dresses | Chunri Dress | Digital Lawn | 2 Piece Lawn Dress

FEATURED PRODUCTS

ASSIGNMENT-10

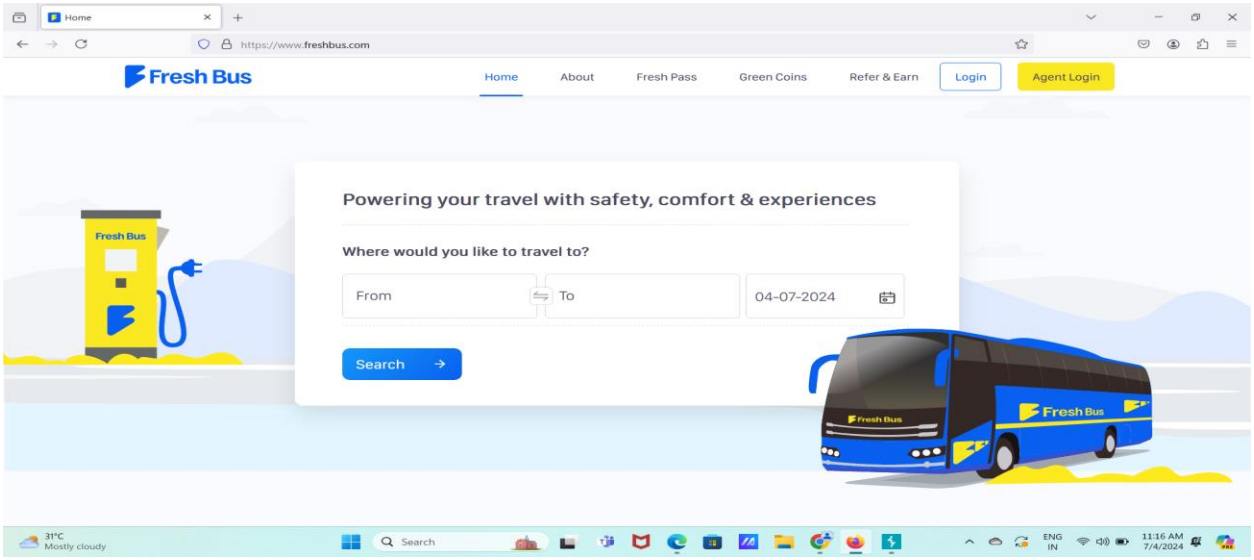
A. Perform No Rate Limiting on the login OTP page of the following websites mentioned below:

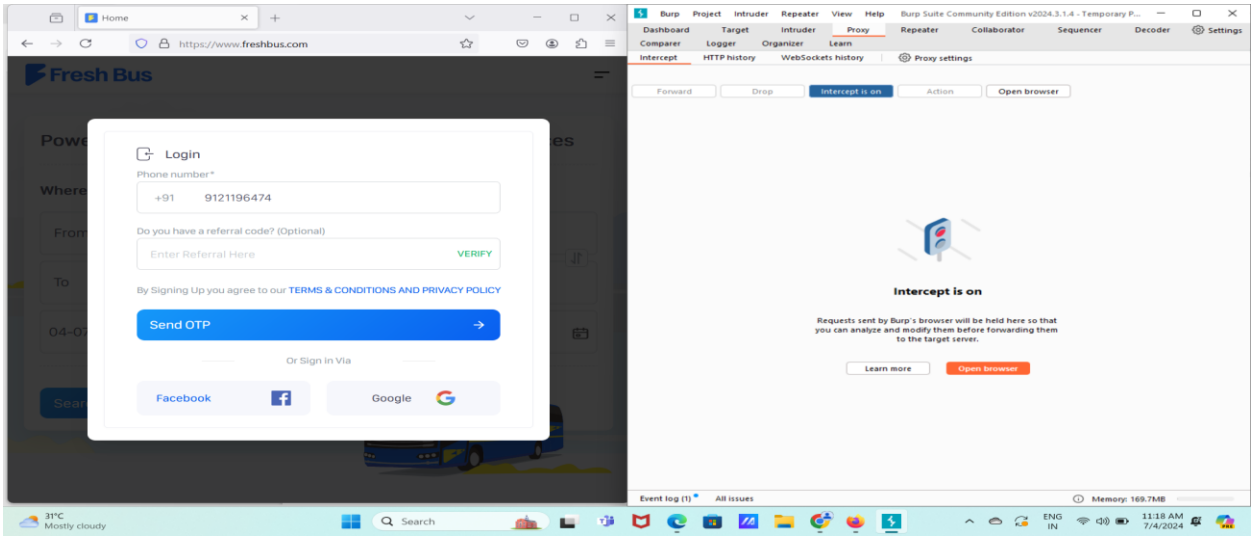
a) https://www.freshbus.com/

b) https://nuego.in/

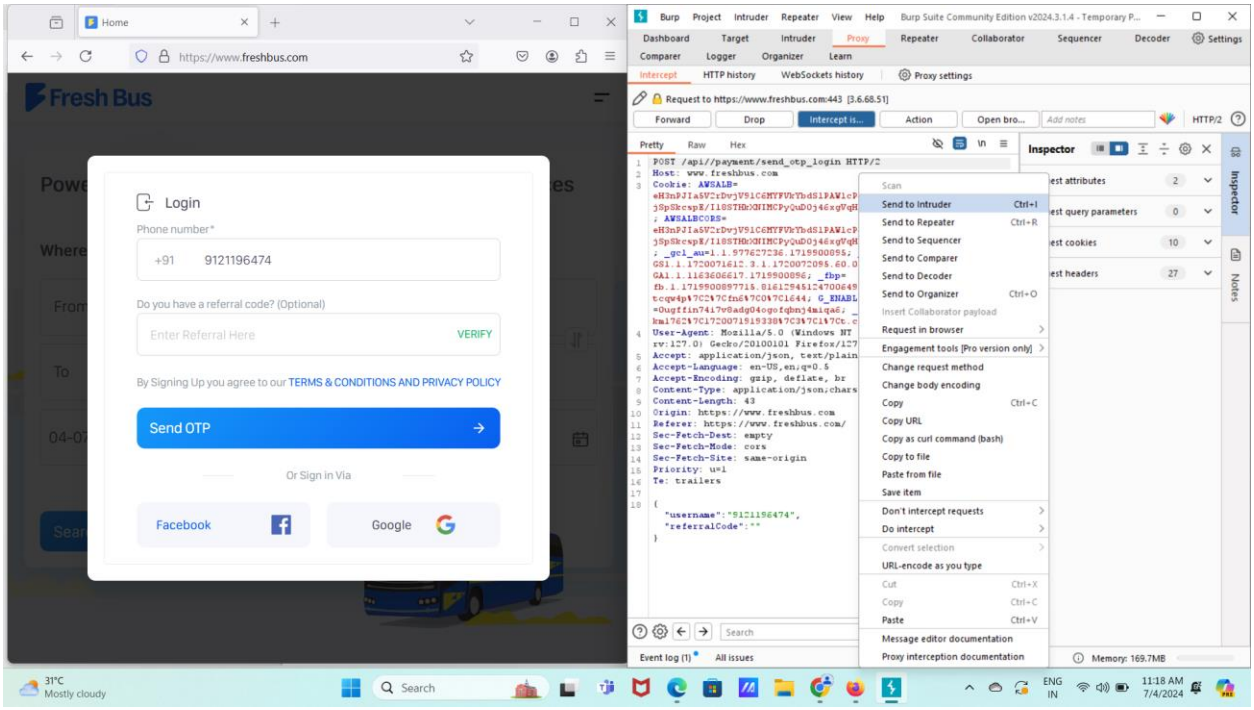
c) https://yolobus.in/

A)

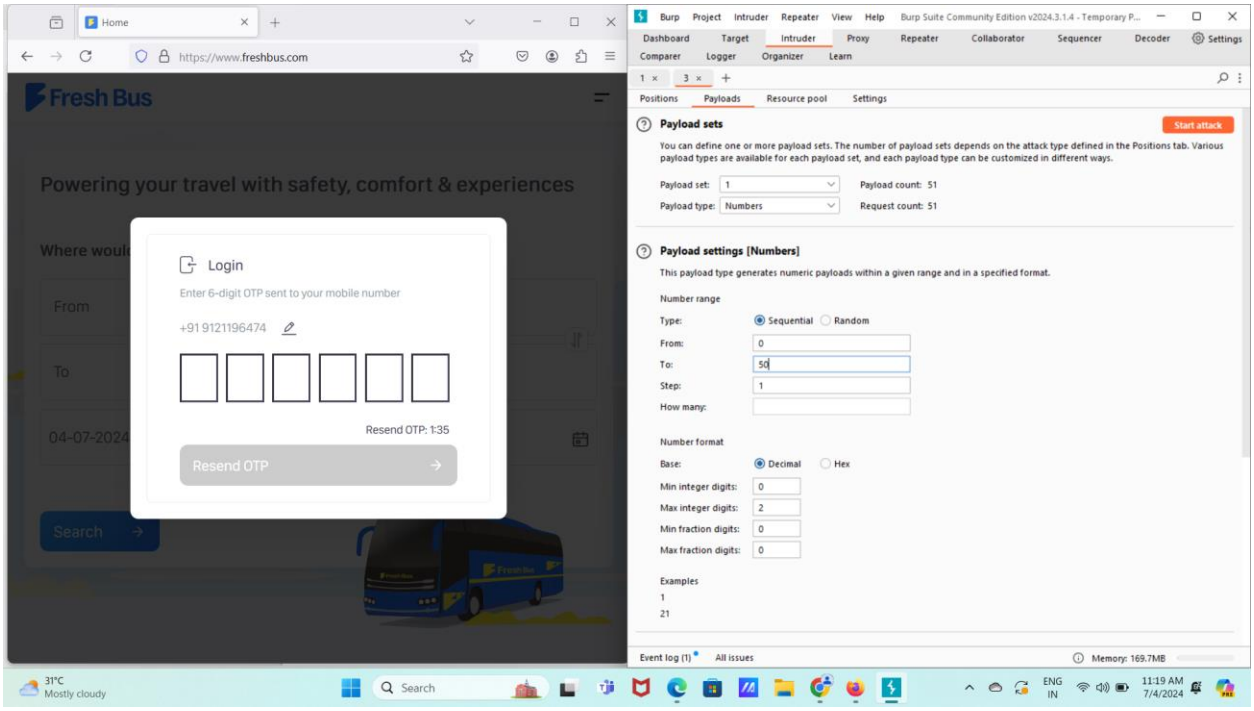




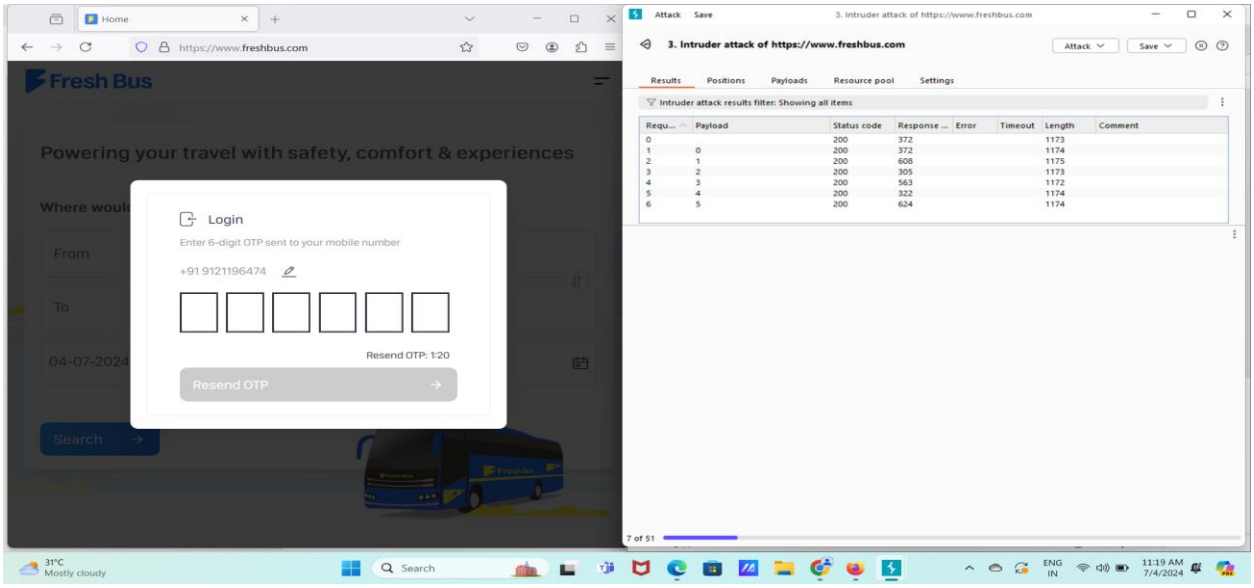
INTERCEPT ON AND LOGIN:

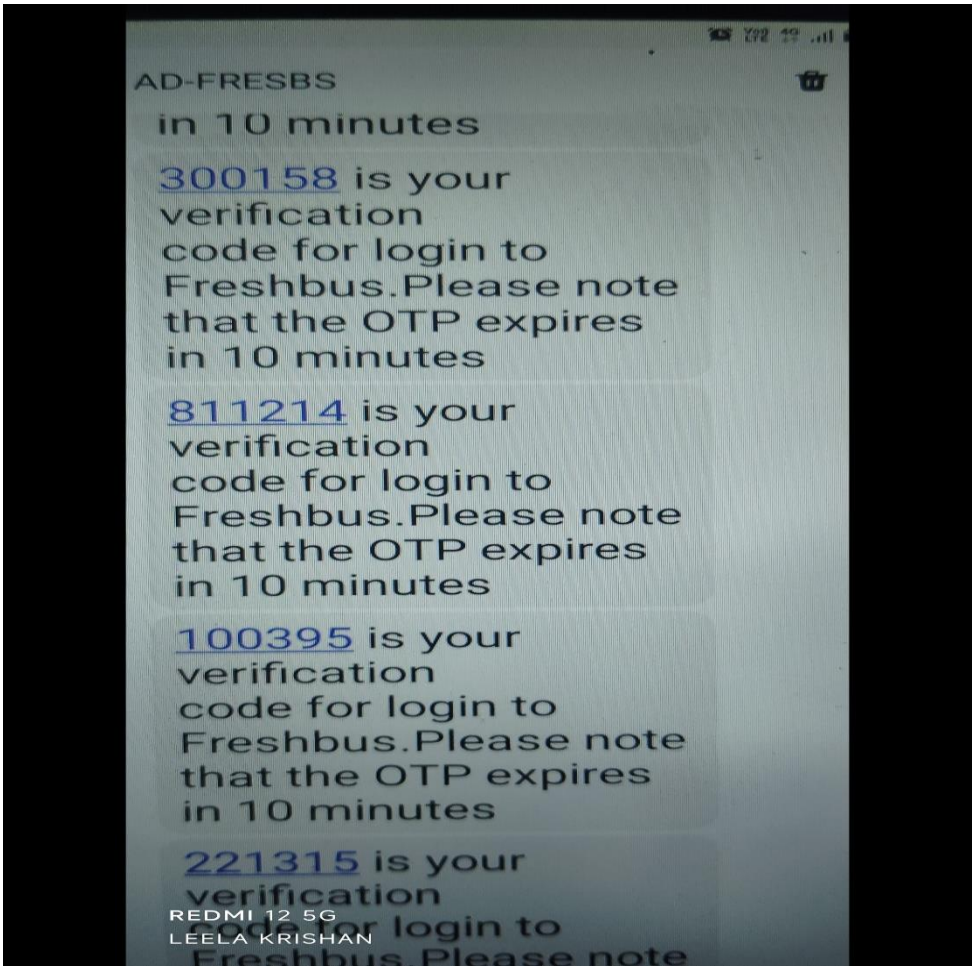


SET PAYLOAD :

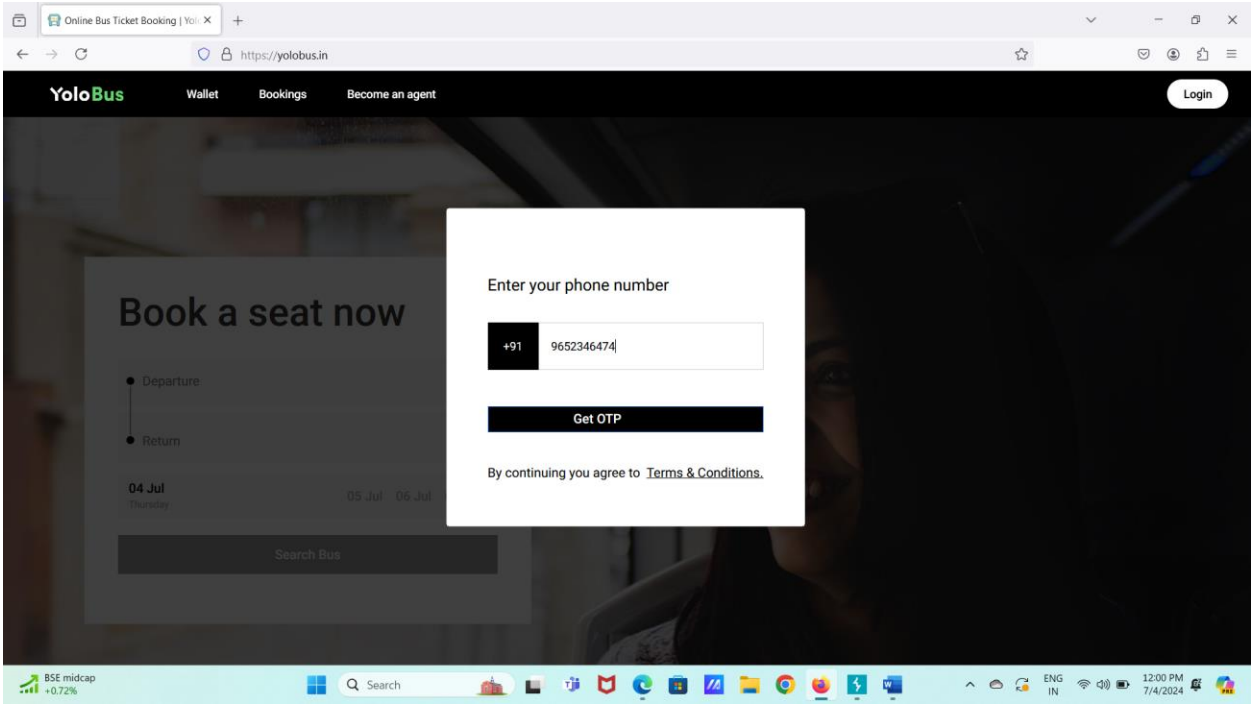


NOW START THE ATTACK:

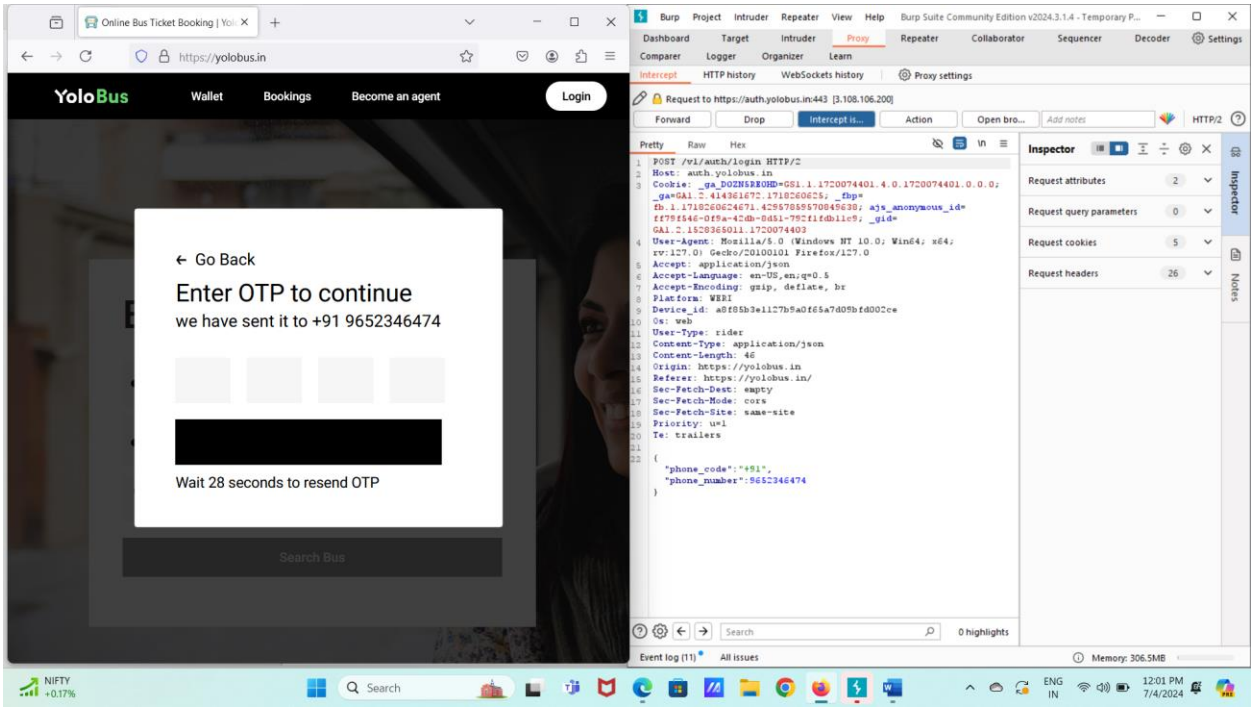

Home
https://www.freshbus.com
Fresh Bus
Powering your travel with safety, comfort & experiences
Where would
From
To
04-07-2024
Search
Login
Enter 6-digit OTP sent to your mobile number
+91 9121196474
Resend OTP: 1:20
Resend OTP
Attack Save
3. Intruder attack of https://www.freshbus.com
Attack
Save
Results
Positions
Payloads
Resource pool
Settings
Intruder attack results filter: Showing all items
Requ... Payload Status code Response ... Error Timeout Length Comment
0 200 372 1173
1 0 200 372 1174
2 1 200 608 1175
3 2 200 305 1173
4 3 200 563 1172
5 4 200 322 1174
6 5 200 624 1174
7 of 51
31°C
Mostly cloudy
Search
ENG
IN
11:19 AM
7/4/2024

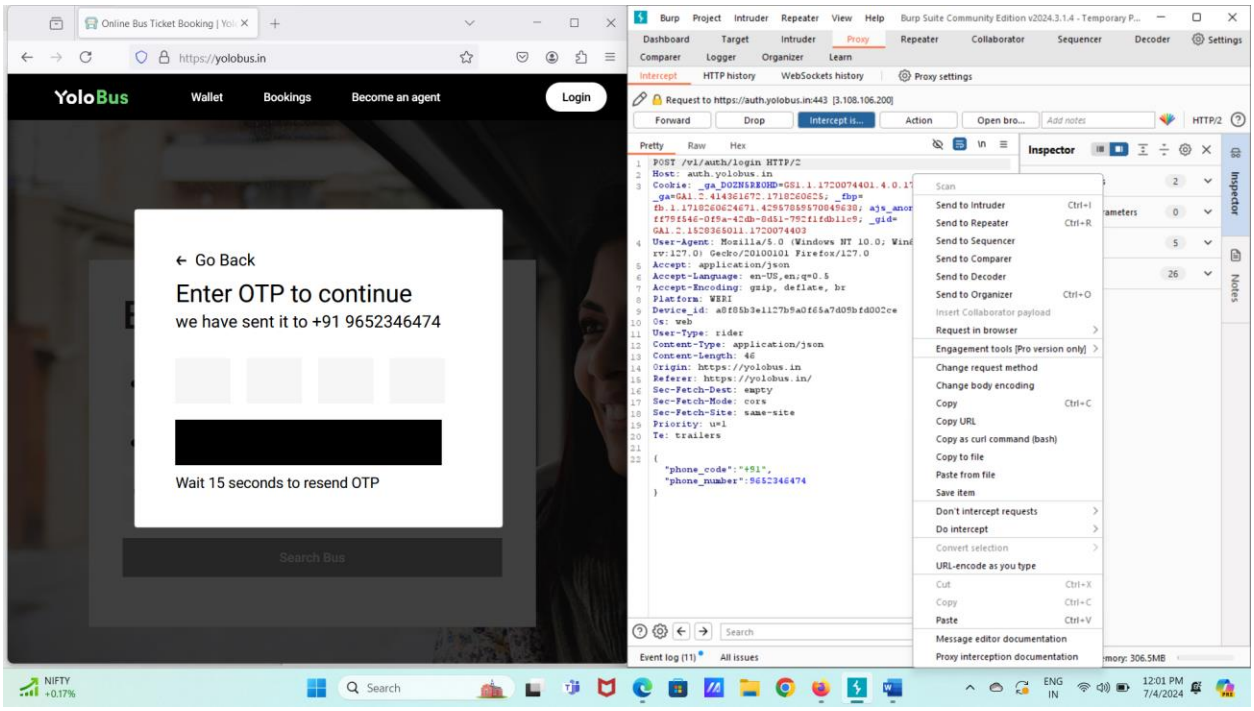

AD-FRESBS
in 10 minutes
300158 is your verification code for login to Freshbus.Please note that the OTP expires in 10 minutes
811214 is your verification code for login to Freshbus.Please note that the OTP expires in 10 minutes
100395 is your verification code for login to Freshbus.Please note that the OTP expires in 10 minutes
221315 is your verification
REDMI 12 5G
LEELA KRISHAN

B)

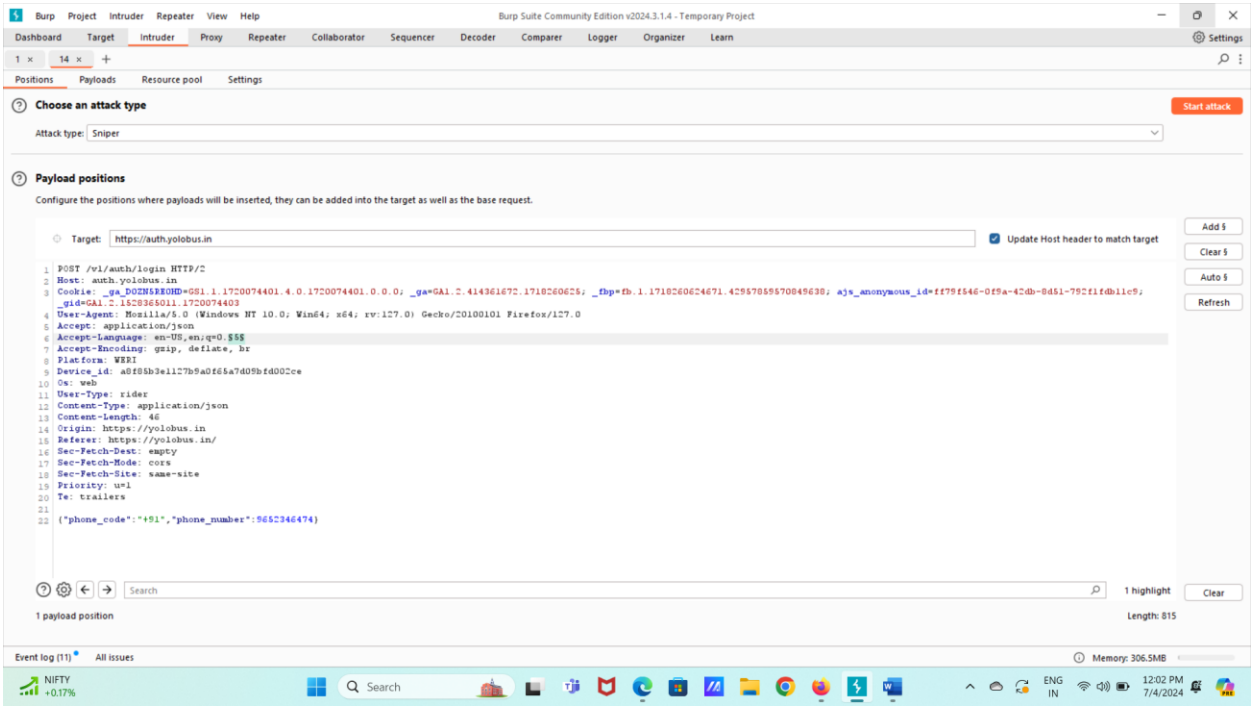


SAME PROCESS:

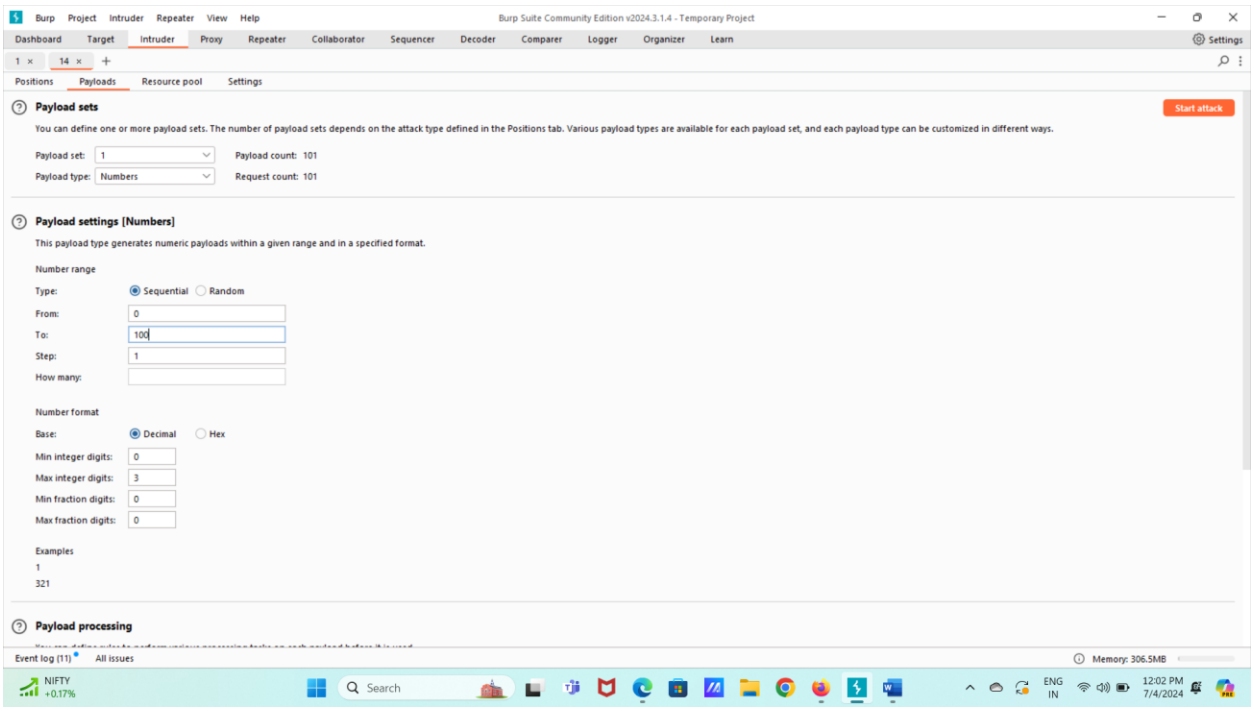




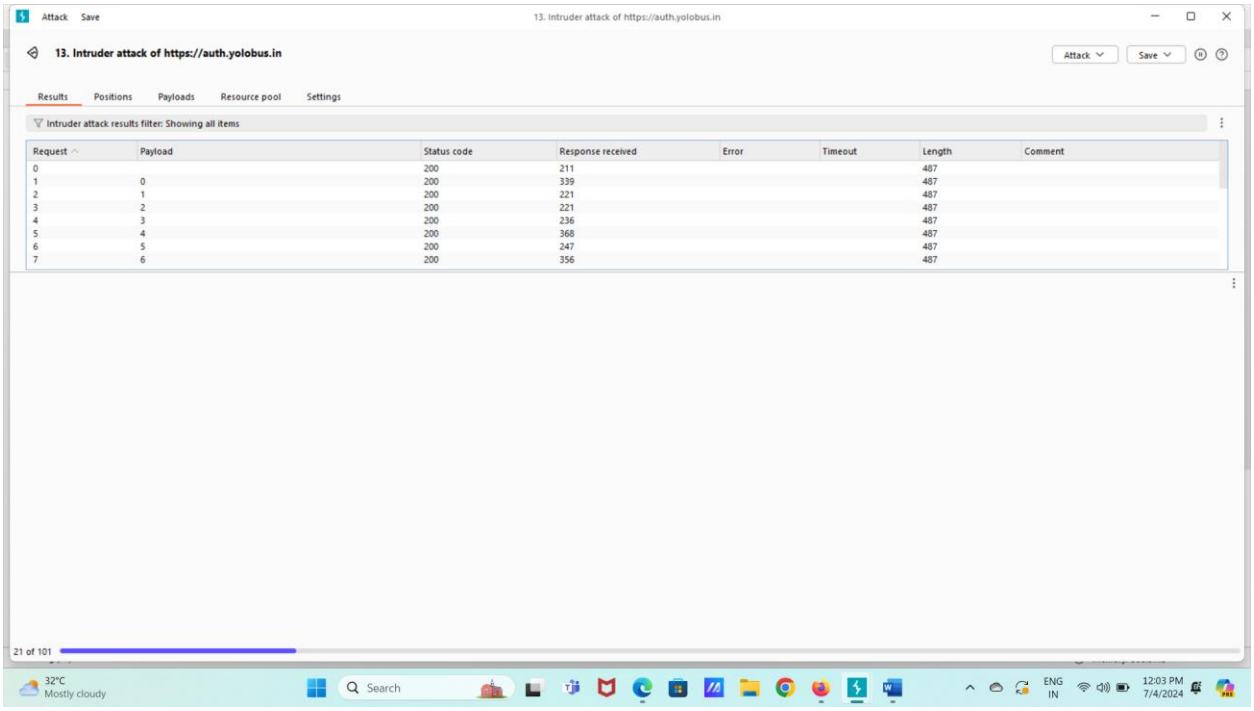
NOW SELECT THE ACCEPT LANGUAGE:



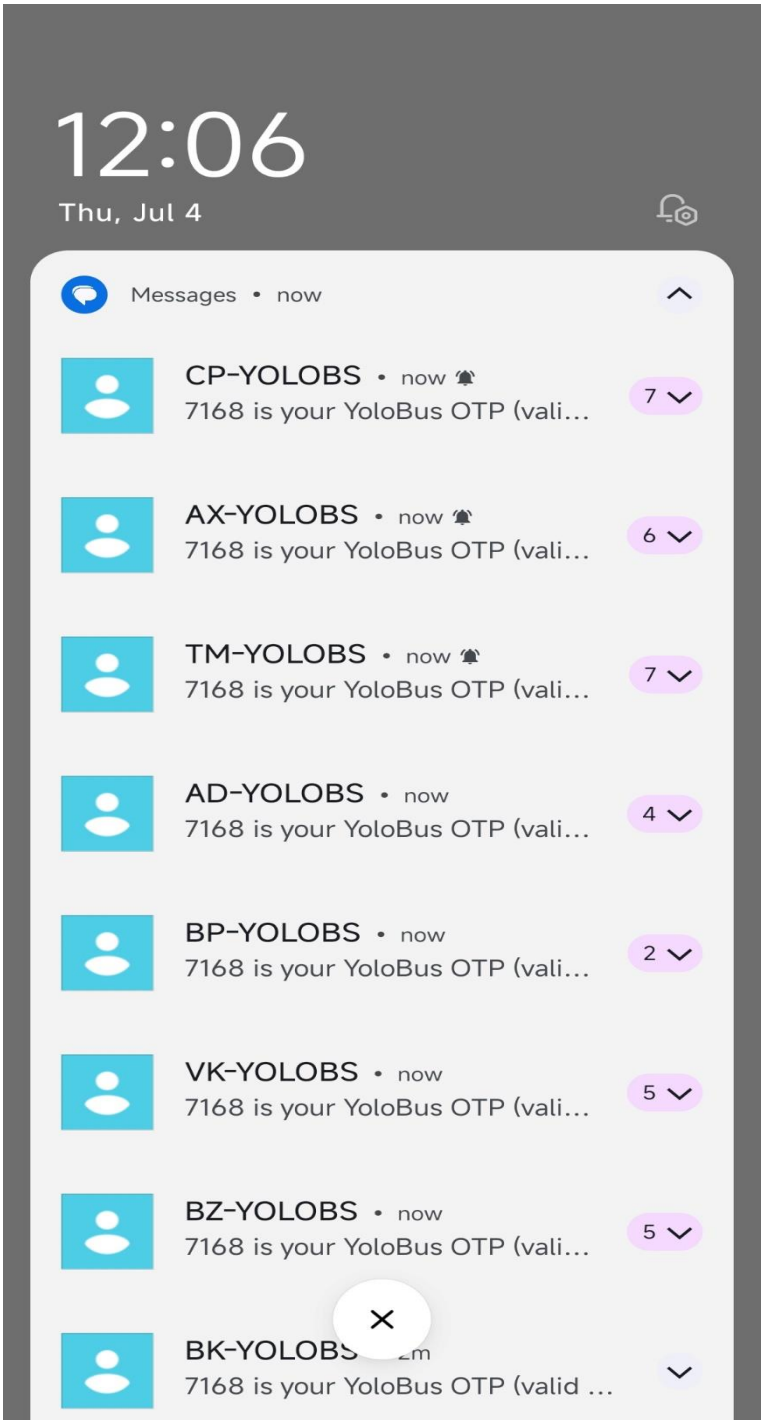
SET PAYLOAD:



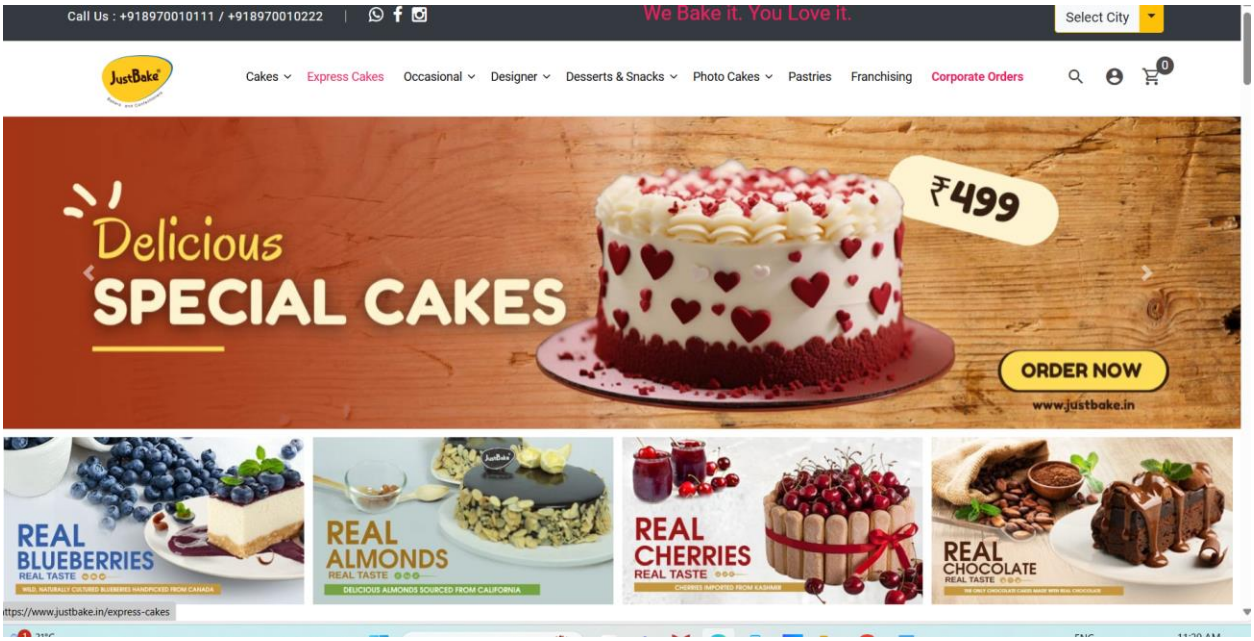
START ATTACK:



THE RESULT:

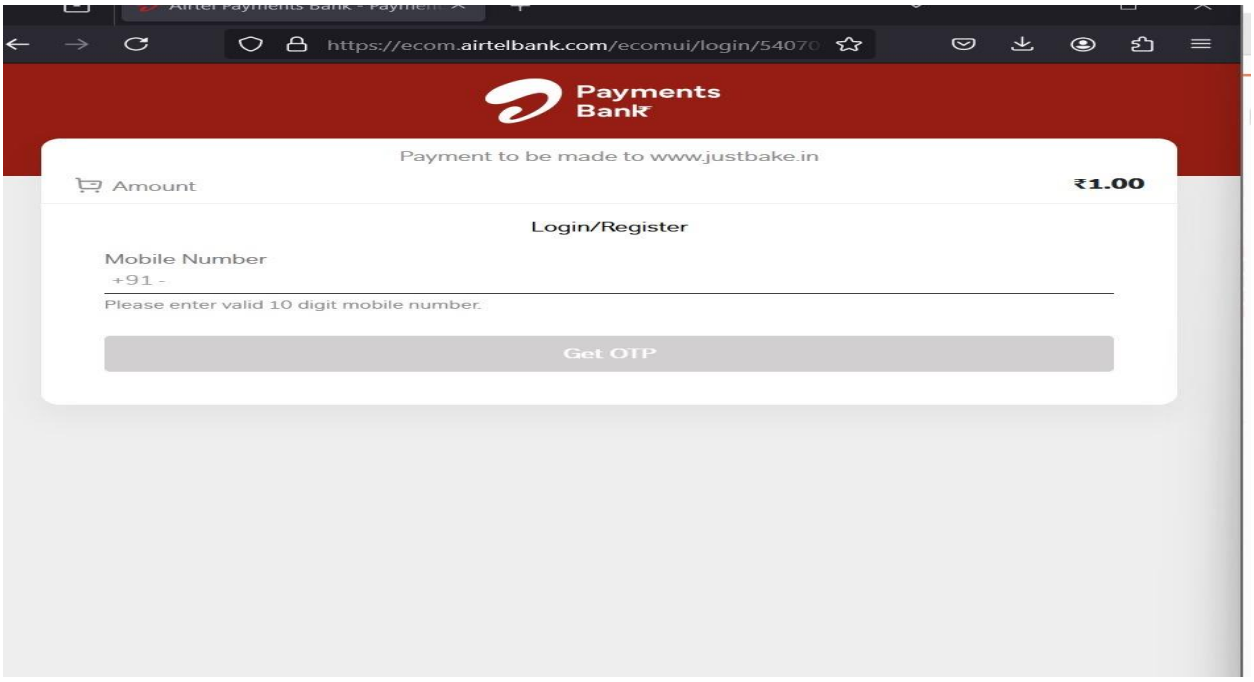

12:06
Thu, Jul 4
Messages • now
CP-YOLOBS • now
7168 is your YoloBus OTP (vali...
7
AX-YOLOBS • now
7168 is your YoloBus OTP (vali...
6
TM-YOLOBS • now
7168 is your YoloBus OTP (vali...
7
AD-YOLOBS • now
7168 is your YoloBus OTP (vali...
4
BP-YOLOBS • now
7168 is your YoloBus OTP (vali...
2
VK-YOLOBS • now
7168 is your YoloBus OTP (vali...
5
BZ-YOLOBS • now
7168 is your YoloBus OTP (vali...
5
BK-YOLOBS
7168 is your YoloBus OTP (valid ...

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



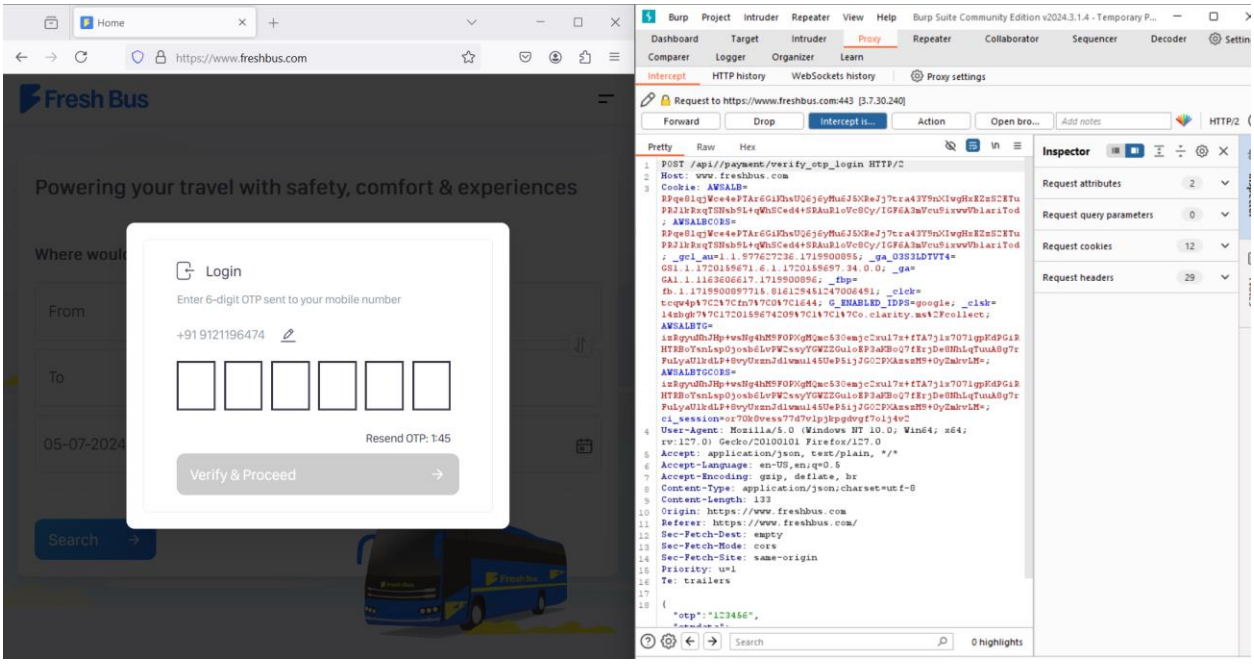
ORDER THE ANY CAKE:

SELECT THE WALLET OPTION AND CHANGE THE AMOUNT AS SHOW BELOW:

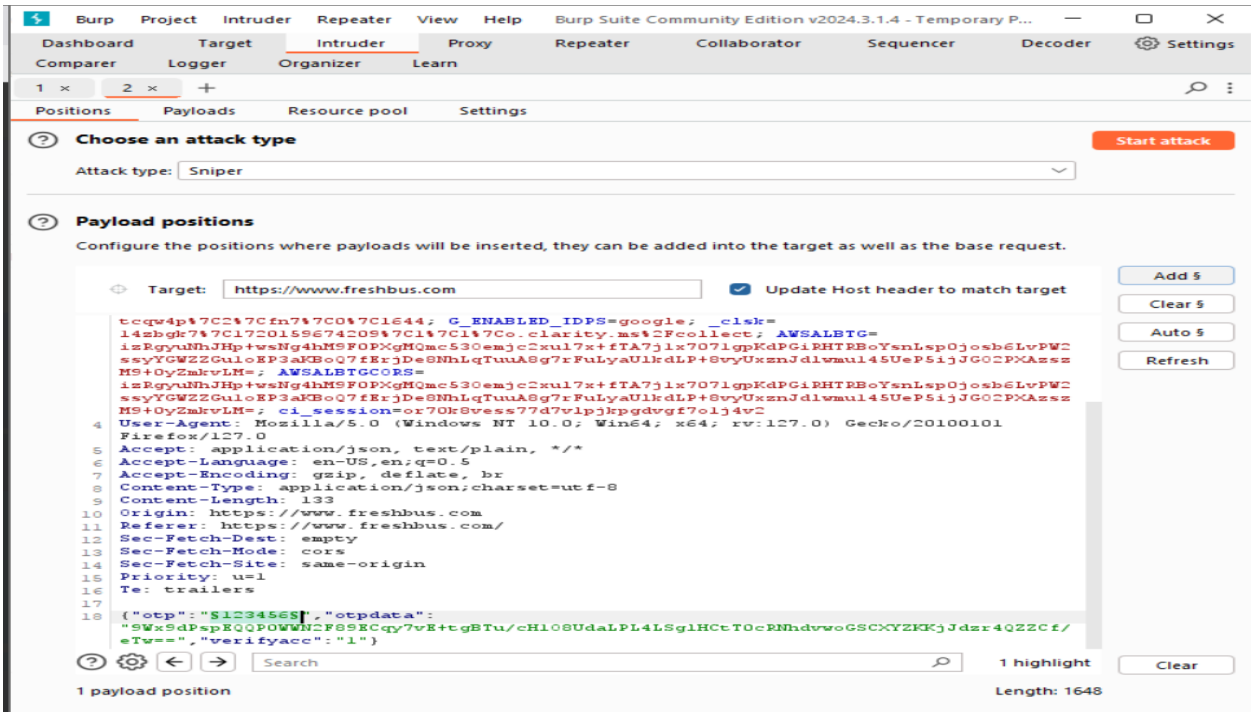


THIS ABOUT PRICE TAMPERING

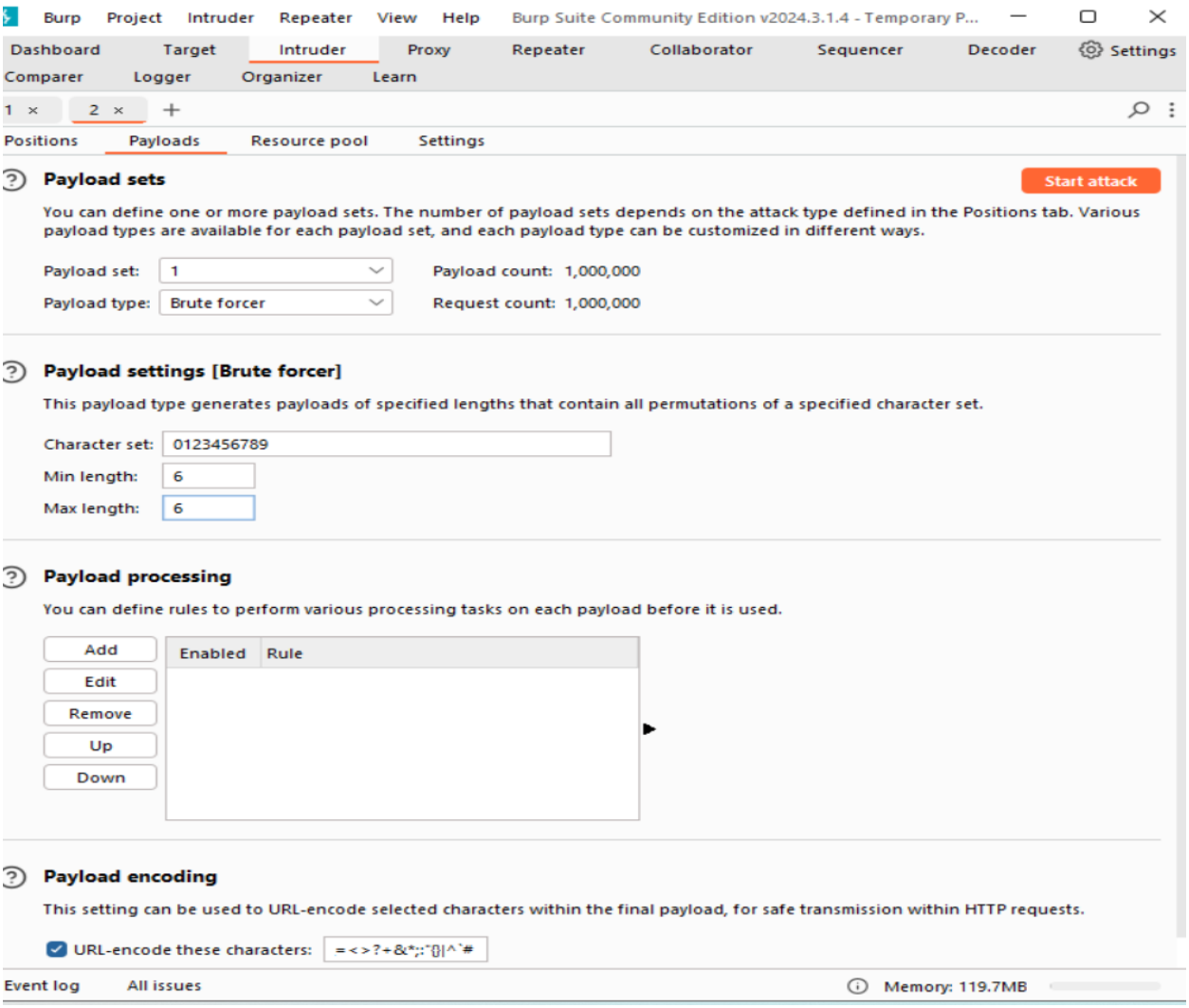
C) Perform Authentication Bypass Exploitation on any website and Prepare clear Documentation. Note: OTP Bypassing



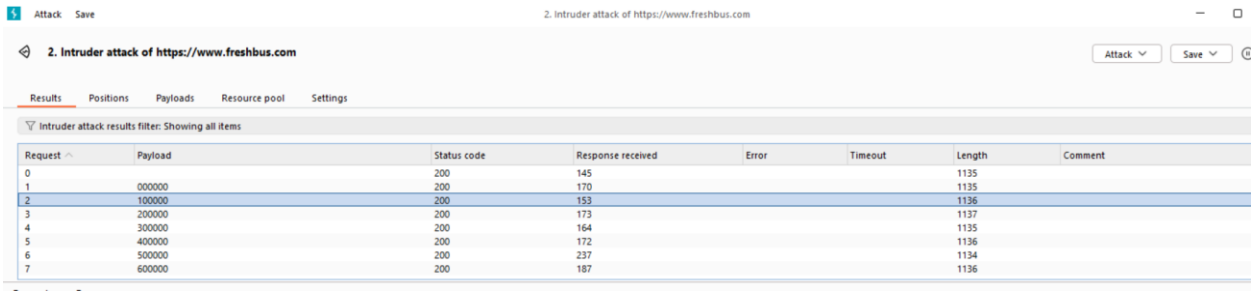
SET THE OTP:



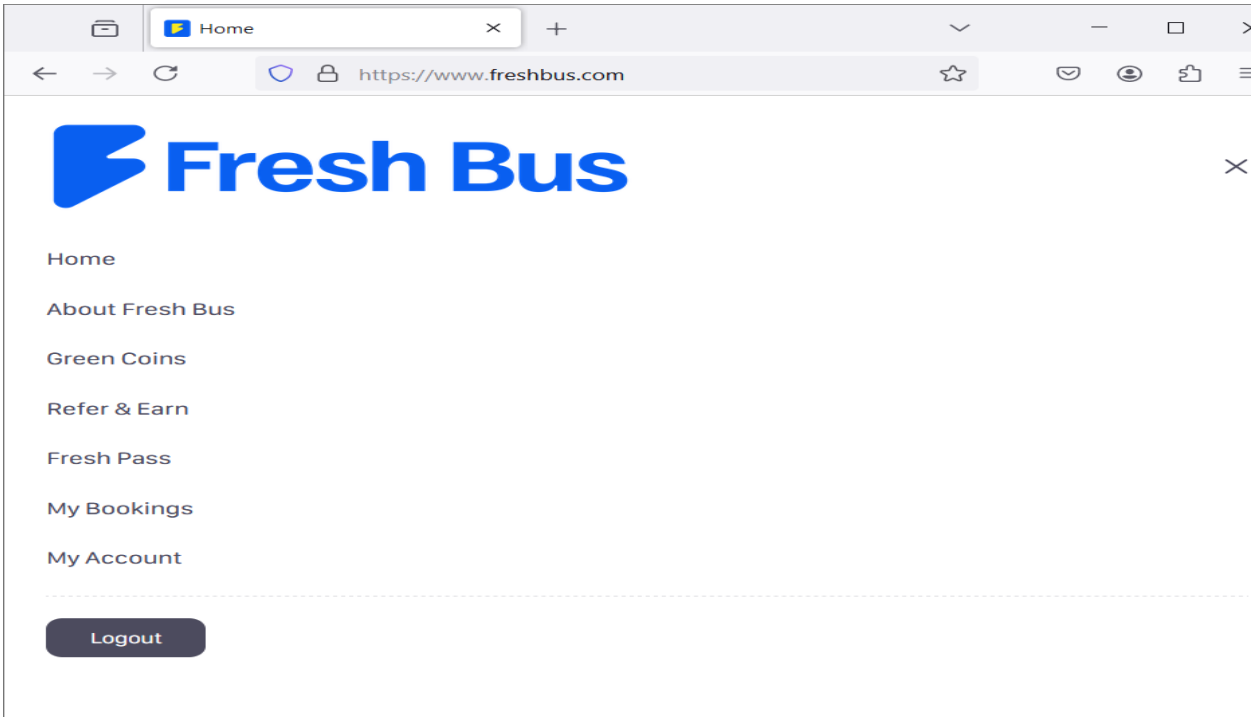
AND SET PAYLOAD:



START ATTACK:

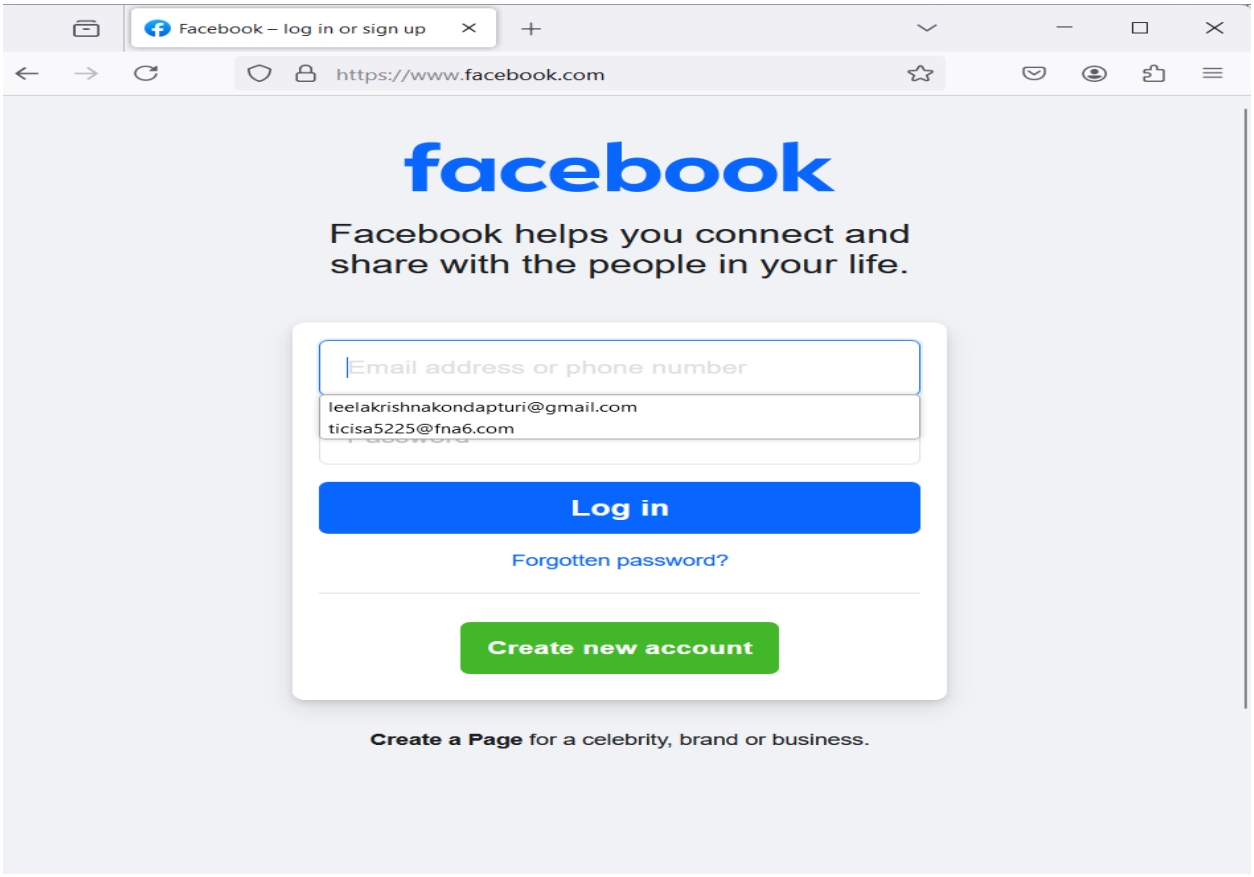


SUCESFULLYLOGIN:

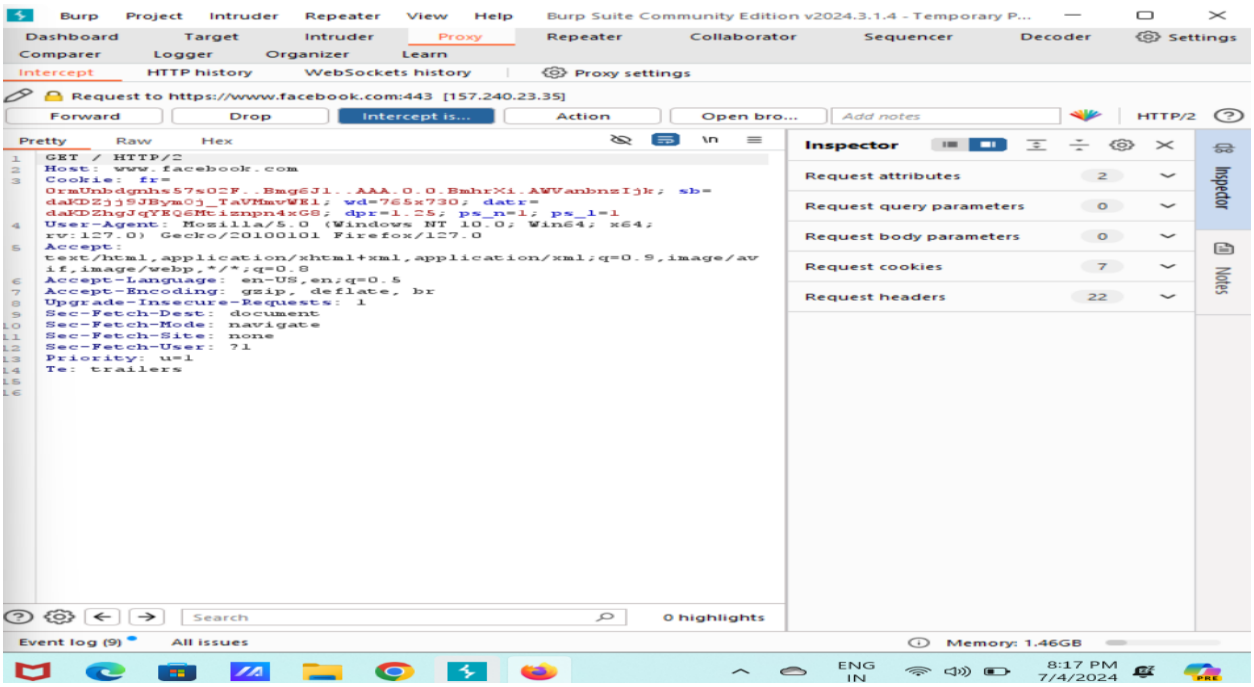

Home
https://www.freshbus.com
Fresh Bus
Home
About Fresh Bus
Green Coins
Refer & Earn
Fresh Pass
My Bookings
My Account
Logout

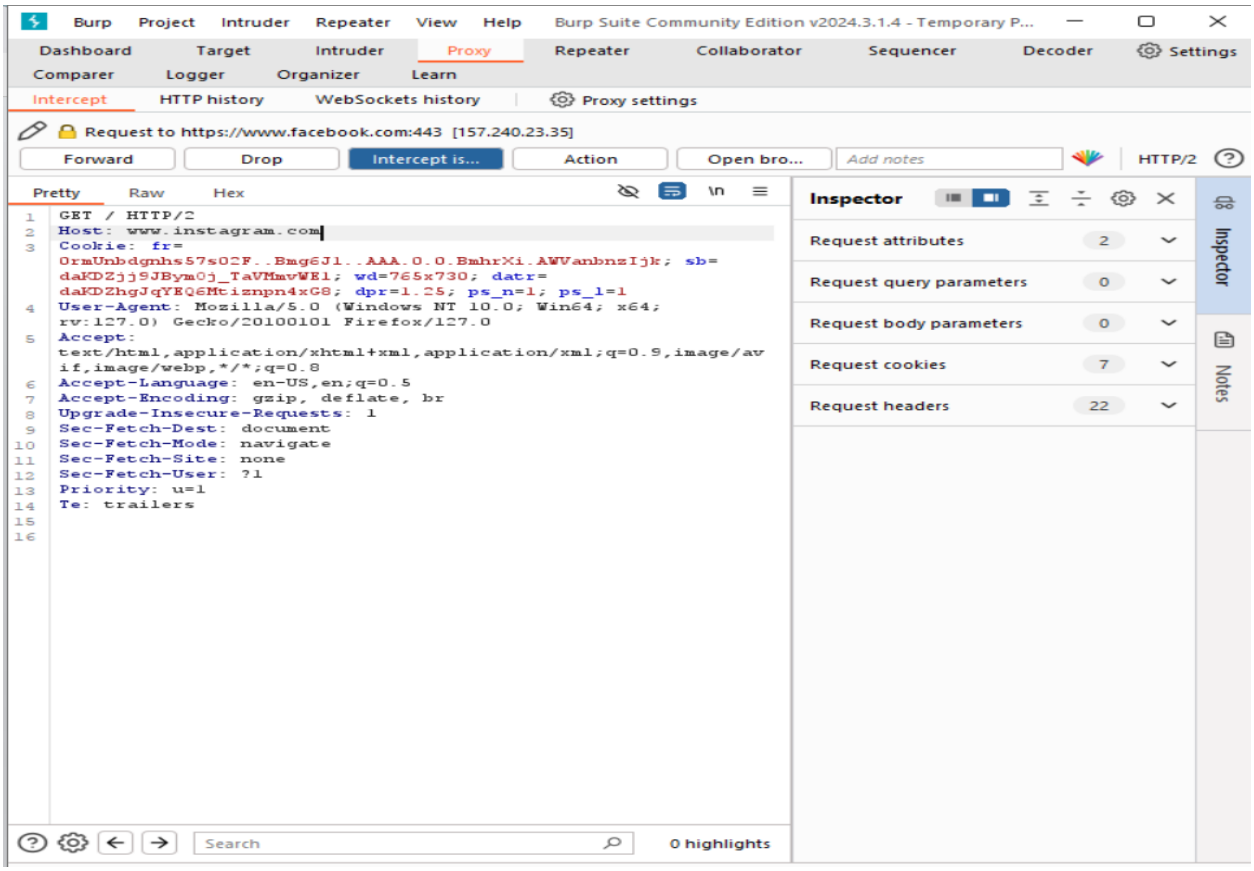
ASSIGNMENT-11

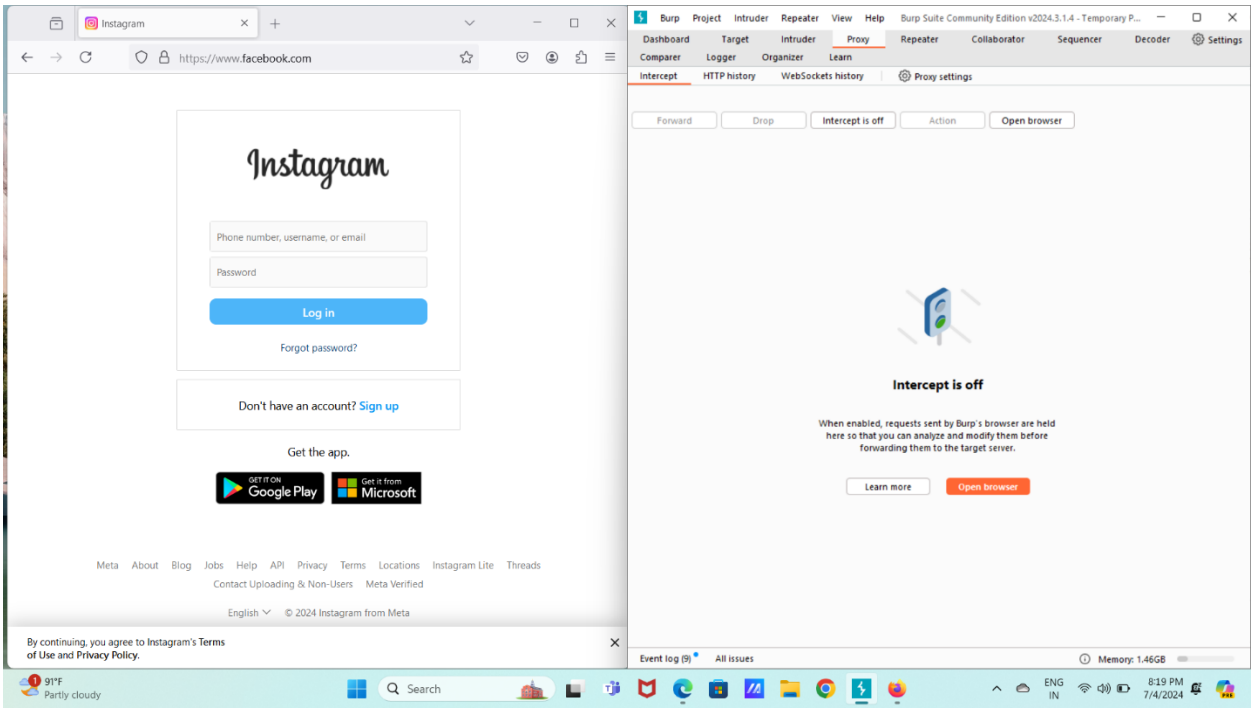
A. Find a website vulnerable to Host Header Injection Vulnerability.



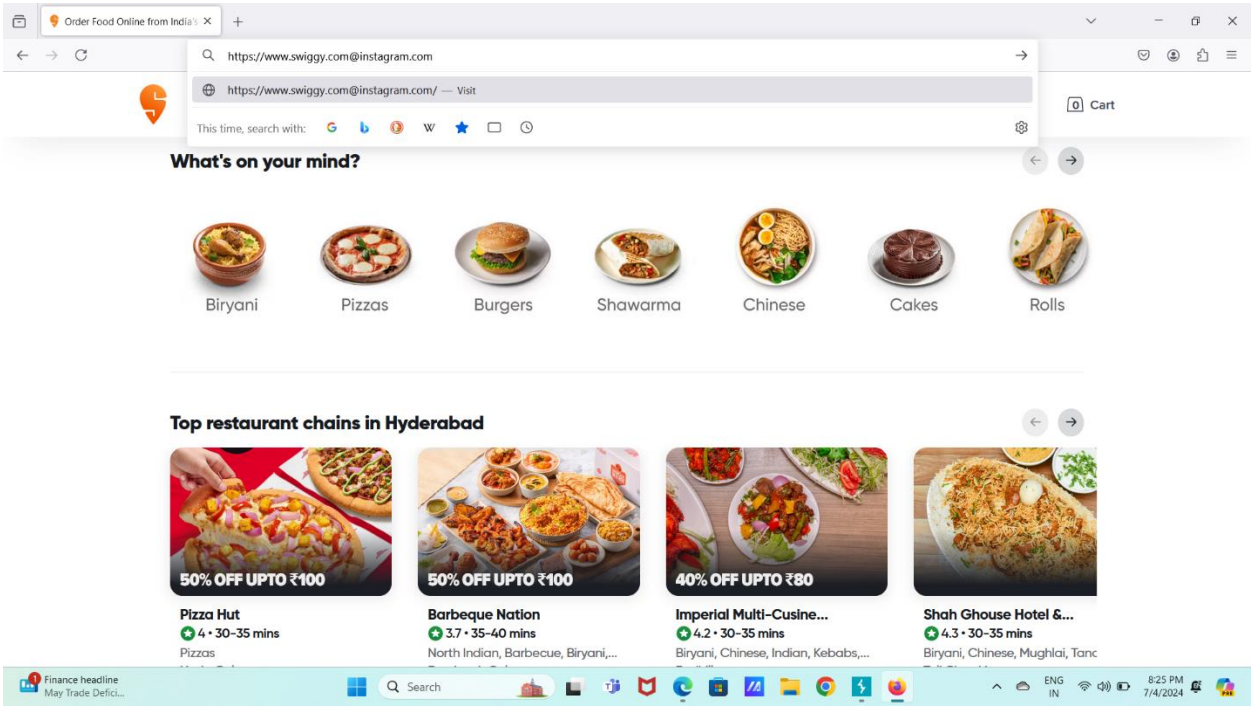
TURN ON THE INTERCEPT:

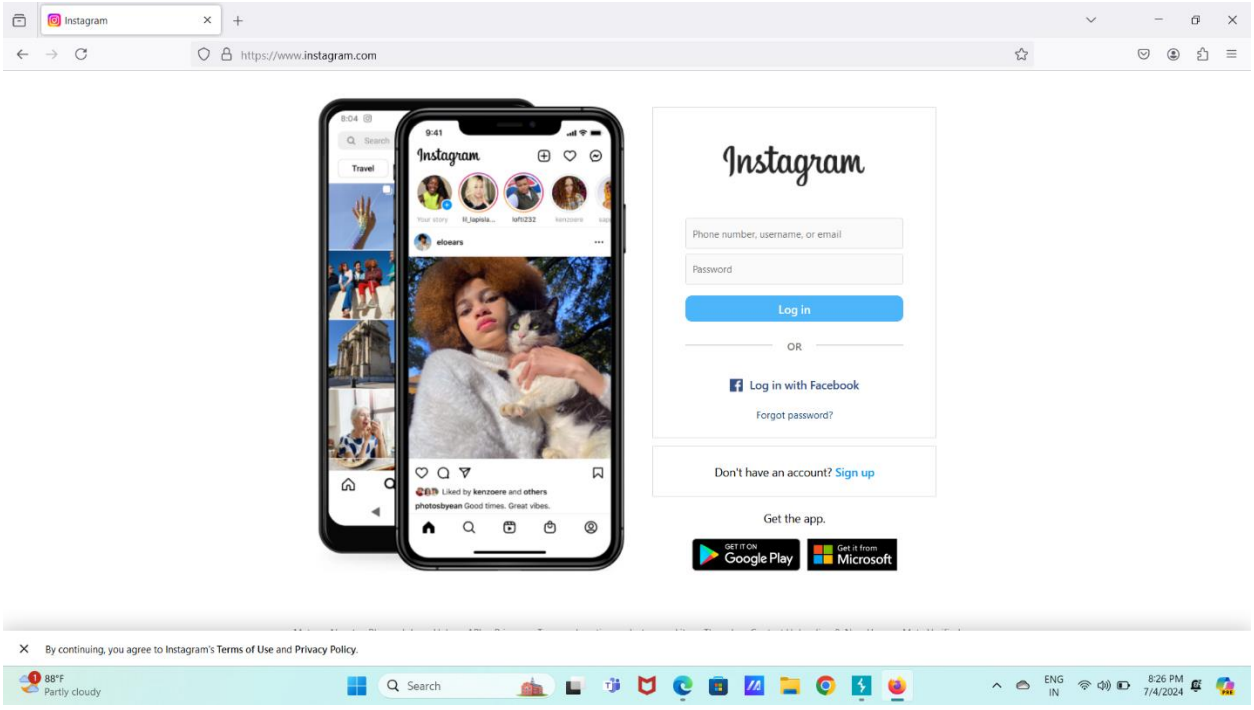

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.3.1.4 - Temporary P...
Dashboard Target Intruder Proxy Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Learn
Intercept HTTP history WebSockets history Proxy settings
Request to https://www.facebook.com:443 [157.240.23.35]
Forward Drop Intercept is... Action Open bro... Add notes HTTP/2
Pretty Raw Hex
GET / HTTP/2
Host: www.facebook.com
Cookie: fr=
0rmUnbdgmhs57s02F..Bmg6J1..AAA.0.0.BmhrXi.AWVanbnzIjk; sb=
daKDZjj9JBym0j_TaVMmvWEl; wd=765x730; datr=
daKDZhgJqYEQ6Mtiznpn4xG8; dpr=1.25; ps_n=1; ps_l=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:127.0) Gecko/20100101 Firefox/127.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=1
Te: trailers
Search 0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 7
Request headers 22
Inspector
Notes
Event log (9) All issues
Memory: 1.46GB
ENG IN 8:17 PM 7/4/2024

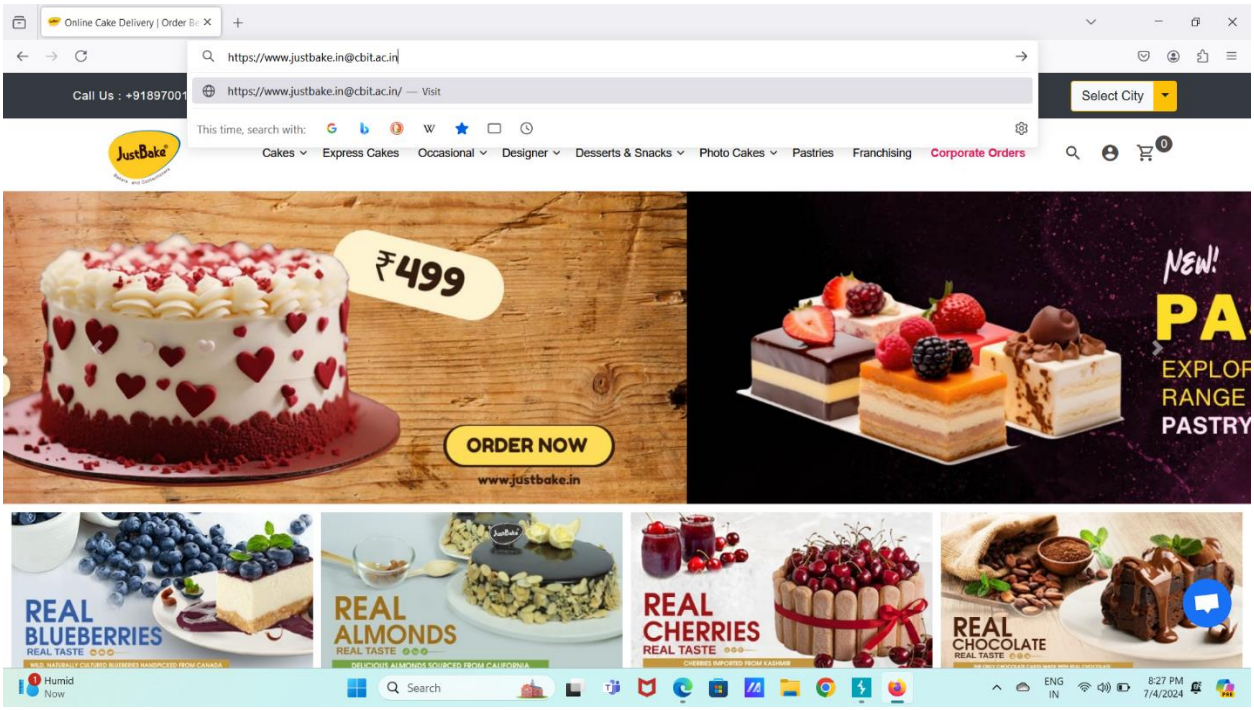

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.3.1.4 - Temporary P...
Dashboard Target Intruder Proxy Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Learn
Intercept HTTP history WebSockets history Proxy settings
Request to https://www.facebook.com:443 [157.240.23.35]
Forward Drop Intercept is... Action Open bro... Add notes HTTP/2
Pretty Raw Hex
GET / HTTP/2
Host: www.instagram.com
Cookie: fr=
0rmUnbdgmhs57s02F..Bmg6J1..AAA.0.0.BmhrXi.AWVanbnzIjk; sb=
daKDZjj9JBym0j_TaVMmvWEl; wd=765x730; datr=
daKDZhgJqYEQ6Mtiznpn4xG8; dpr=1.25; ps_n=1; ps_l=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:127.0) Gecko/20100101 Firefox/127.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=1
Te: trailers
Search 0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 7
Request headers 22
Inspector
Notes



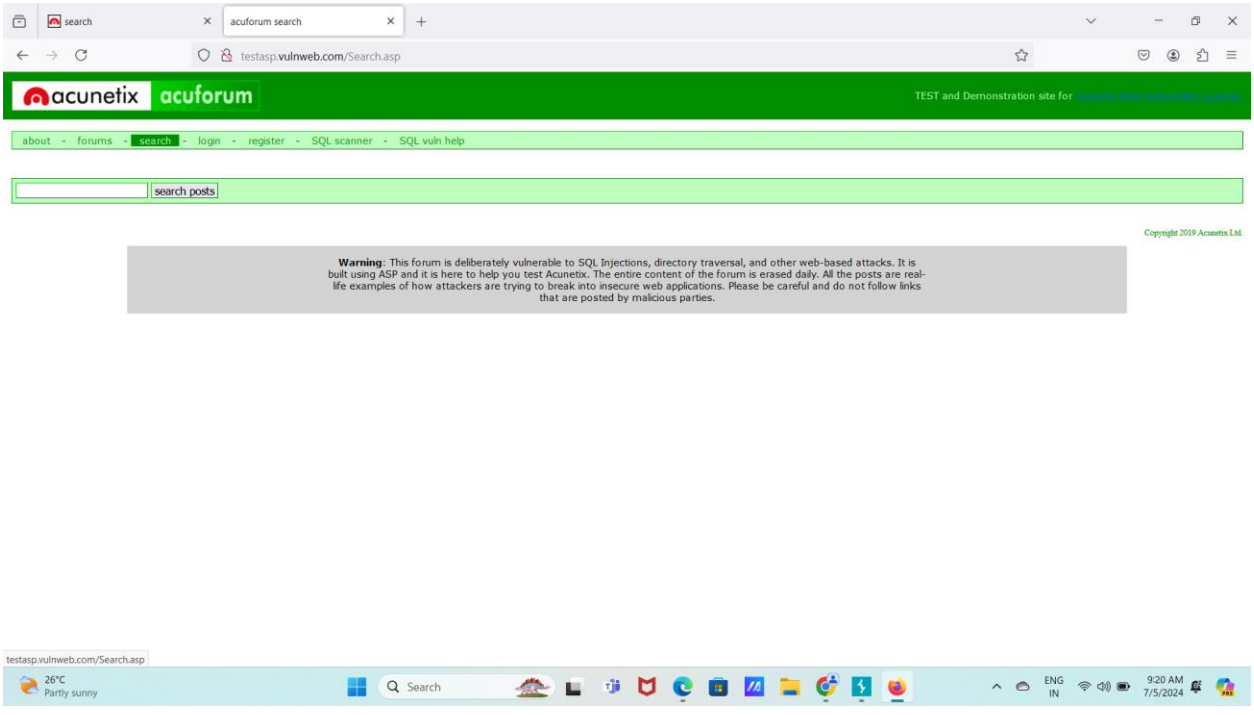
B. Find 2 websites that are vulnerable to Open Redirect / URL Redirection Vulnerability.

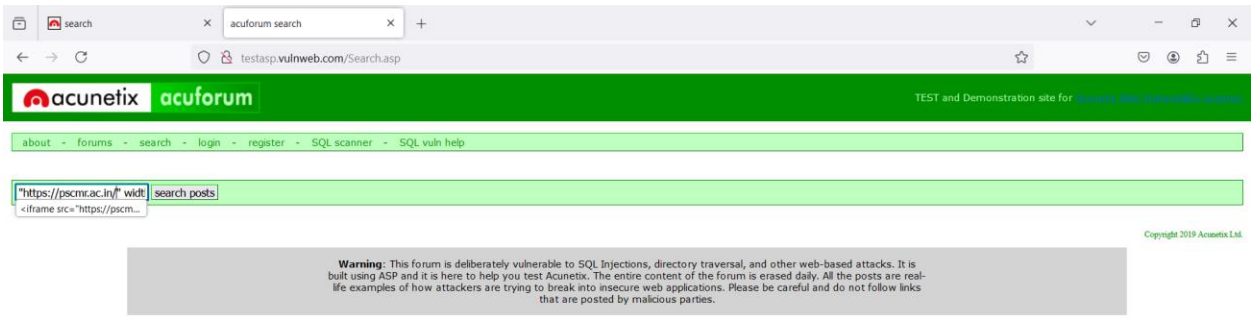


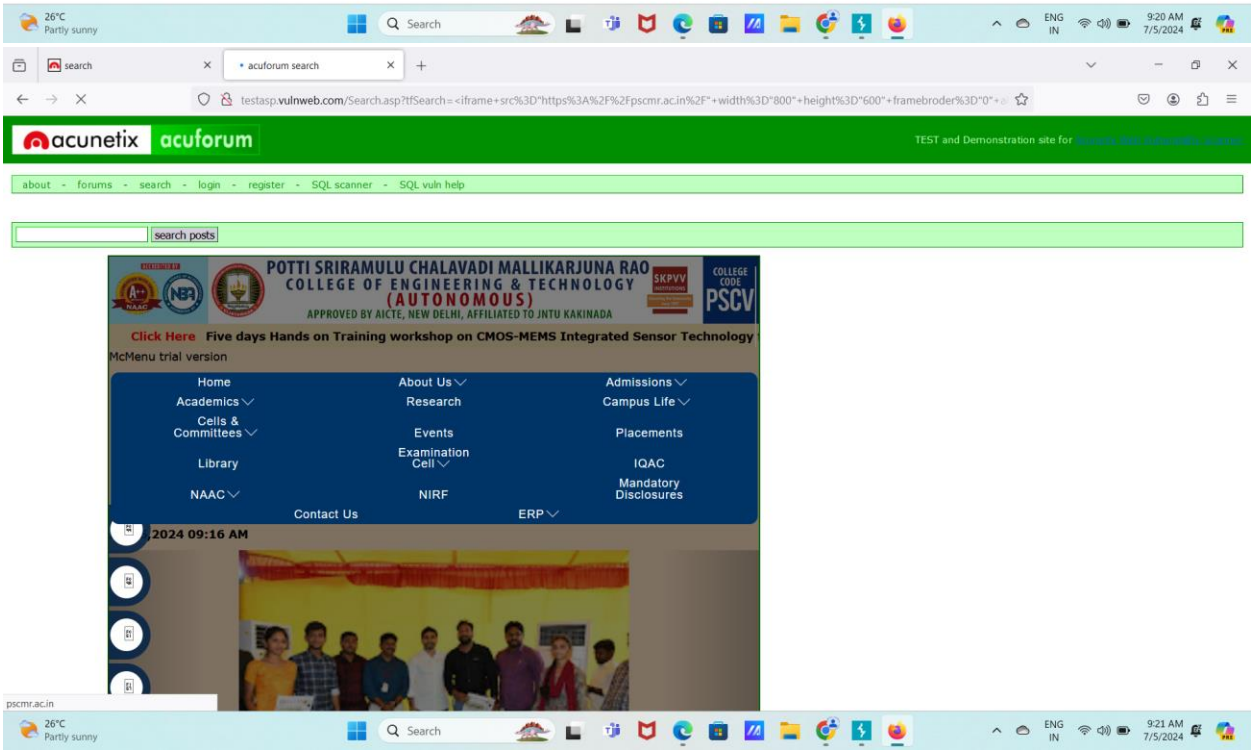

Instagram
https://www.instagram.com
Instagram
Phone number, username, or email
Password
Log in
OR
Log in with Facebook
Forgot password?
Don't have an account? Sign up
Get the app.
GET IT ON Google Play
Get it from Microsoft
By continuing, you agree to Instagram's Terms of Use and Privacy Policy.
88°F
Partly cloudy
Search
ENG
IN
8:26 PM
7/4/2024


Online Cake Delivery | Order Be
https://www.justbake.in@cbit.ac.in
https://www.justbake.in@cbit.ac.in/ — Visit
This time, search with:
Call Us : +9189700
Select City
JustBake
Cakes
Express Cakes
Occasional
Designer
Desserts & Snacks
Photo Cakes
Pastries
Franchising
Corporate Orders
₹499
ORDER NOW
www.justbake.in
NEW!
EXPLOR
RANGE
PASTRY
REAL
BLUEBERRIES
REAL TASTE
REAL
ALMONDS
REAL TASTE
REAL
CHERRIES
REAL TASTE
REAL
CHOCOLATE
REAL TASTE
Humid
Now
Search
ENG
IN
8:27 PM
7/4/2024

C. Find 2 websites that are vulnerable to iFrame Injection Vulnerability.



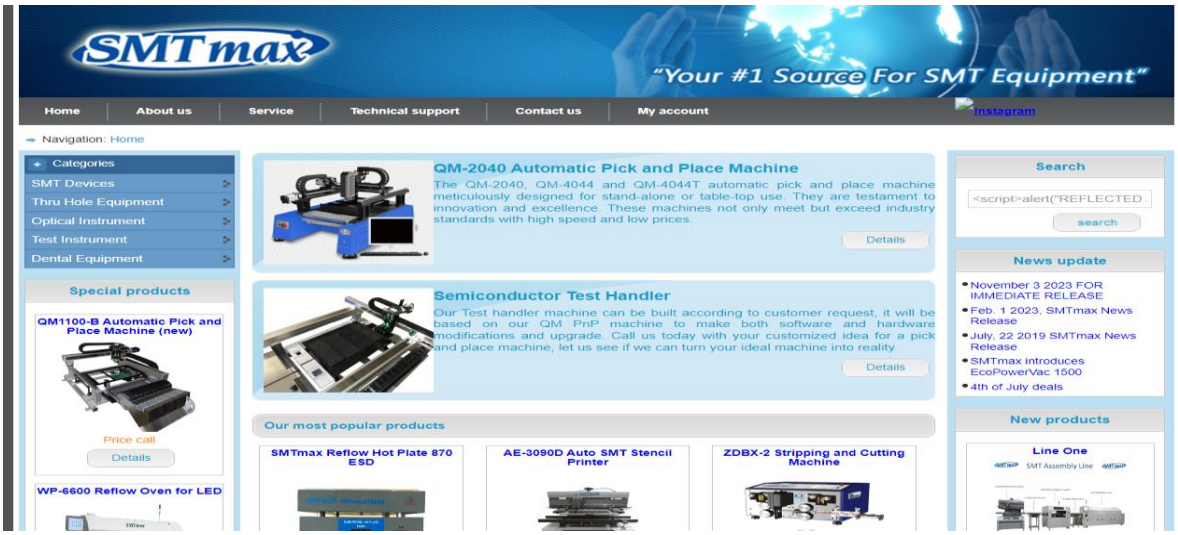

search
acuforum search
testasp.vulnweb.com/Search.asp
acunetix
acuforum
TEST and Demonstration site for
about - forums - search - login - register - SQL scanner - SQL vuln help
"https://pscmr.ac.in/" widt
search posts
<iframe src="https://pscm...
Copyright 2019 Acunetix Ltd.
Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.

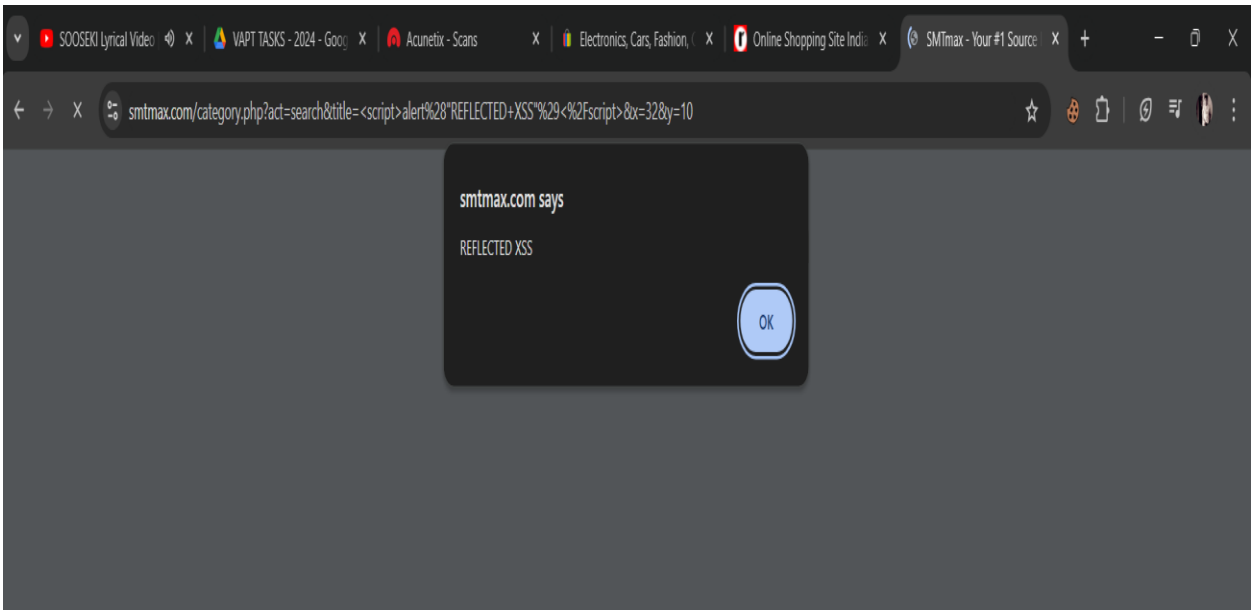

26°C
Partly sunny
Search
ENG
IN
9:20 AM
7/5/2024
search
acuforum search
testasp.vulnweb.com/Search.asp?tfSearch=<iframe+src%3D"https%3A%2F%2Fpscmr.ac.in%2F"+width%3D"800"+height%3D"600"+framebroder%3D"0"+
acunetix
acuforum
TEST and Demonstration site for
about - forums - search - login - register - SQL scanner - SQL vuln help
search posts
POTTI SRIRAMULU CHALAVADI MALLIKARJUNA RAO
COLLEGE OF ENGINEERING & TECHNOLOGY
(AUTONOMOUS)
APPROVED BY AICTE, NEW DELHI, AFFILIATED TO JNTU KAKINADA
SKPVV
COLLEGE CODE PSCV
Click Here Five days Hands on Training workshop on CMOS-MEMS Integrated Sensor Technology
McMenu trial version
Home
About Us
Admissions
Academics
Research
Campus Life
Cells & Committees
Events
Placements
Library
Examination Cell
IQAC
NAAC
NIRF
Mandatory Disclosures
Contact Us
ERP
2024 09:16 AM
pscmr.ac.in
26°C
Partly sunny
Search
ENG
IN
9:21 AM
7/5/2024

ASSIGNMENT – 12

Find cross-site scripting (XSS) Vulnerability Using the Reflected XSS test case in the below-mentioned website: a) Smtmax.com

Using this command: <script>alert("REFLECTED XSS")</script> in the input fields of the website we can get a pop up





3. Find a website that is vulnerable to Broken Access Control Vulnerability.

Website : Vevishal matrimony (https://www.lagnakaro.com/)

Using burp suite, we take the ID and change it