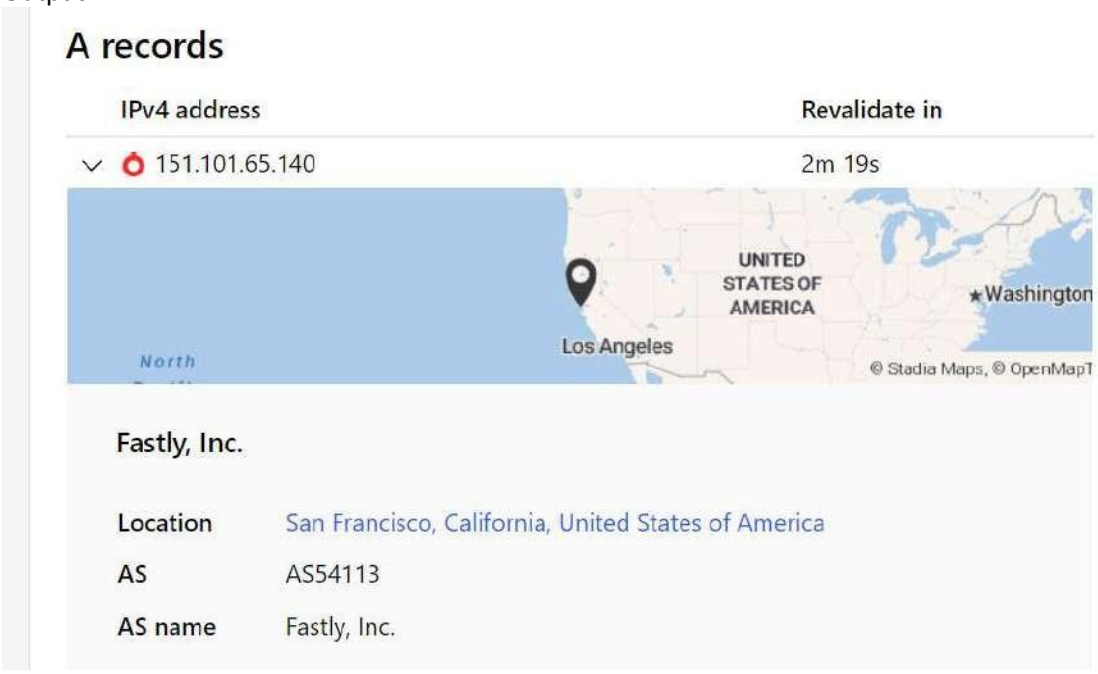
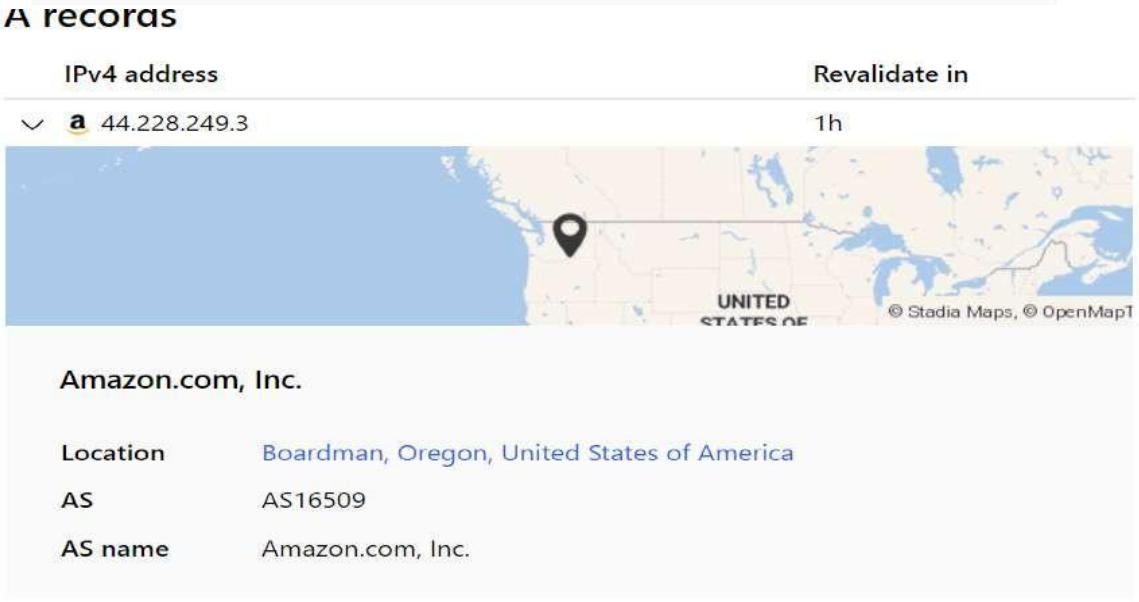
A.Using Nslookup website we get the information such as IP addresses of a given website url or domain name

Output:





A records

IPv4 address	Revalidate in
192.124.249.13	2h

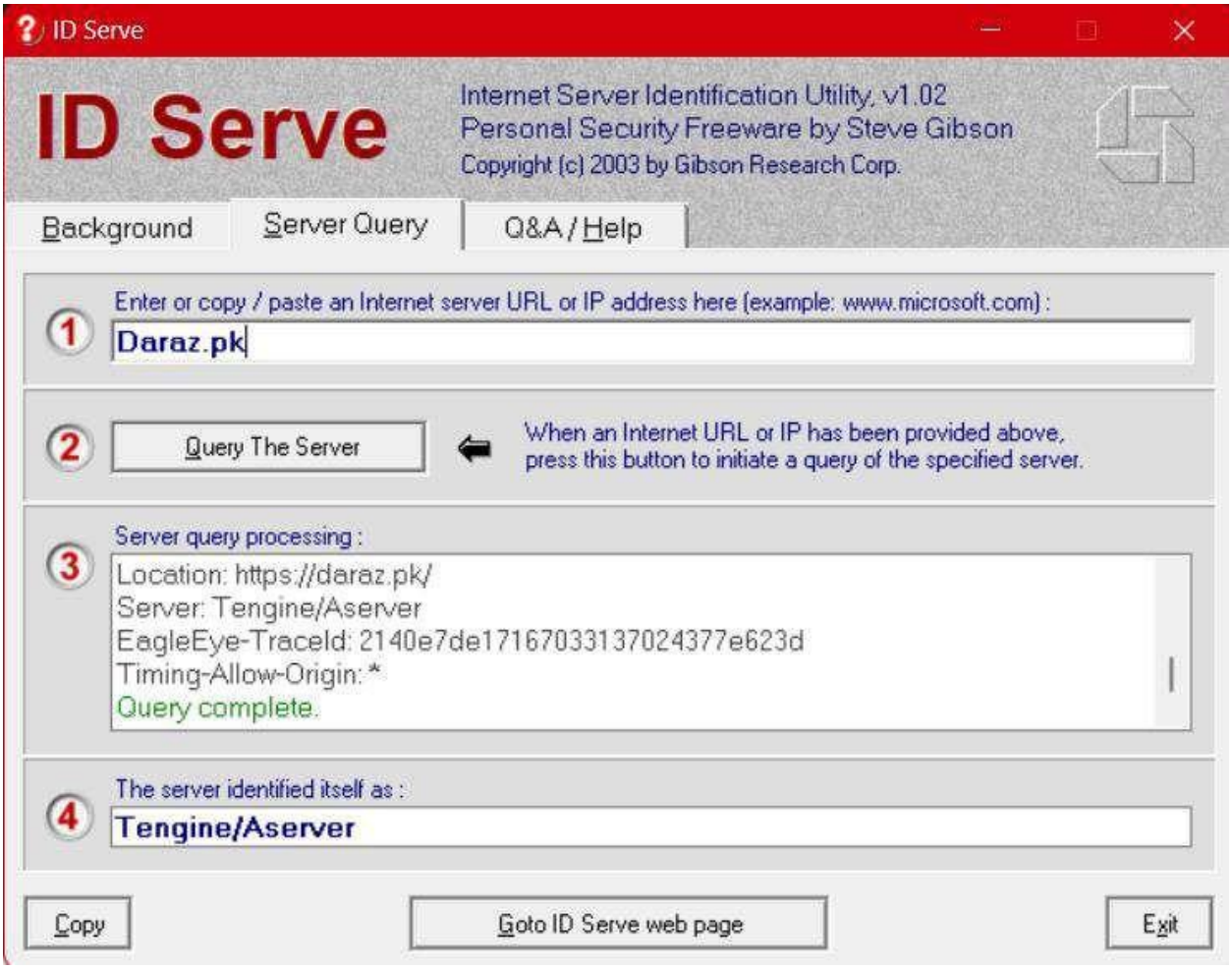
Sucuri

Location	Menifee, California, United States of America
AS	AS30148
AS name	Sucuri

Using smartwhois application we get the additional information about the website

B.Using IDServe we get the information of 2 pakistani websites(Mymart,Daraz)

Output:


ID Serve
ID Serve
Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.
Background
Server Query
Q&A / Help
1
Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com) :
Daraz.pk
2
Query The Server
When an Internet URL or IP has been provided above,
press this button to initiate a query of the specified server.
3
Server query processing :
Location: https://daraz.pk/
Server: Tengine/Aserver
EagleEye-TraceId: 2140e7de17167033137024377e623d
Timing-Allow-Origin: *
Query complete.
4
The server identified itself as :
Tengine/Aserver
Copy
Goto ID Serve web page
Exit

Using Wayback Machines getting information of the mentioned websites(Mymart,Daraz)

Outputs:

2003 2004 2005 2006 2007 2008 2009 2010 2011 **2012** 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023

JAN

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

FEB

			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29			

MAR

				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

APR

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

MAY

		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

JUN

					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

JUL

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

AUG

			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

SEP

						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

OCT

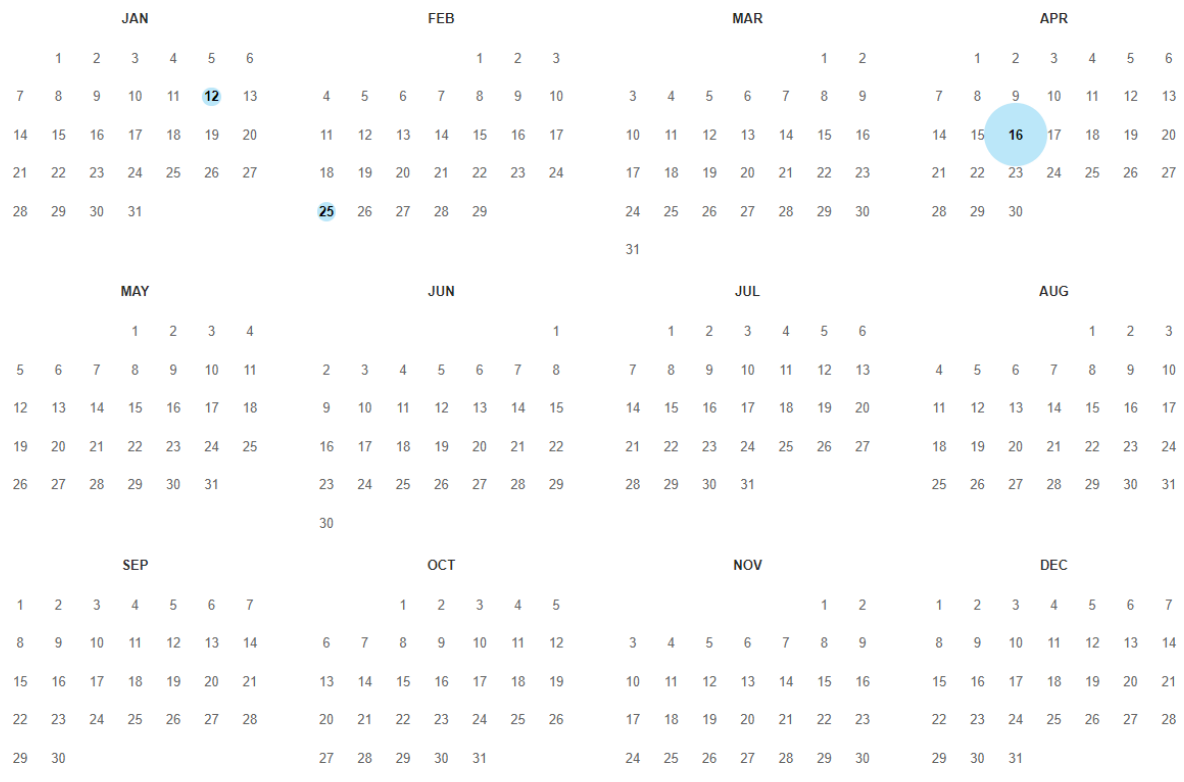
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

NOV

				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

DEC

						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					



C. Using matelgo tool to gather information about any 2 pakistani websites

Output:

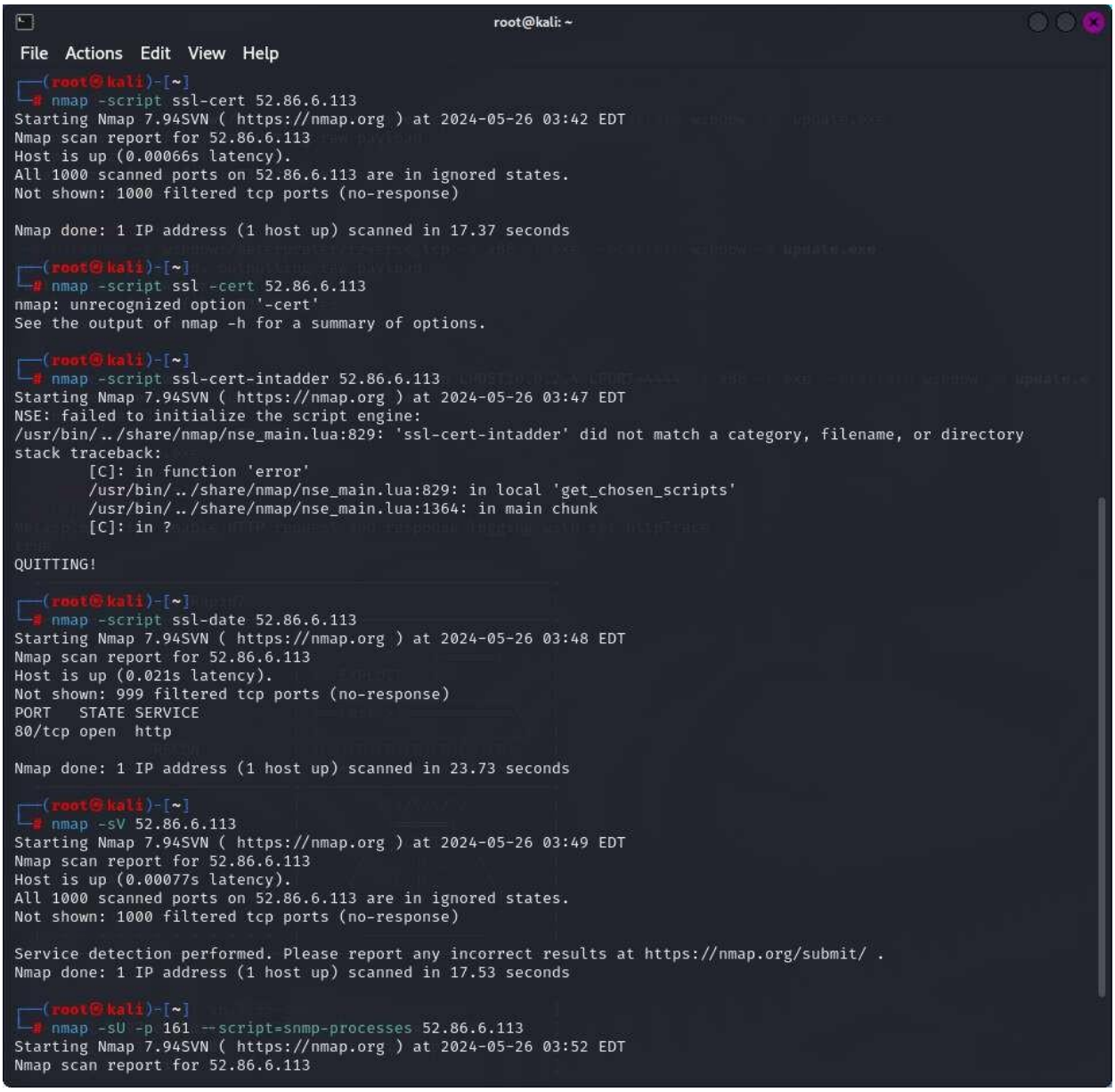
F. Perform enumeration on any Pakistan website :

Output:

Telnet Enumeration :

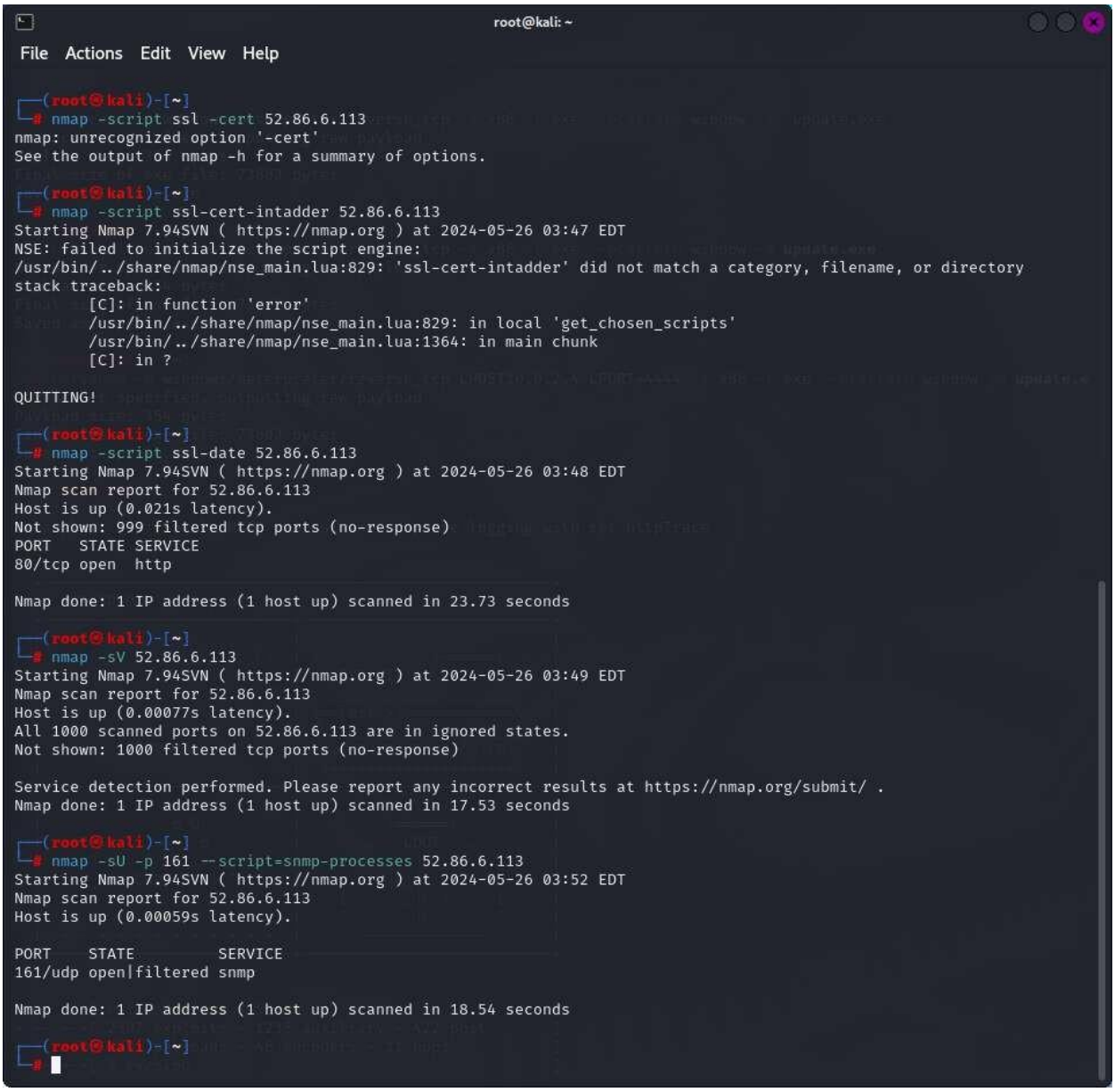
SSL Enumeration:

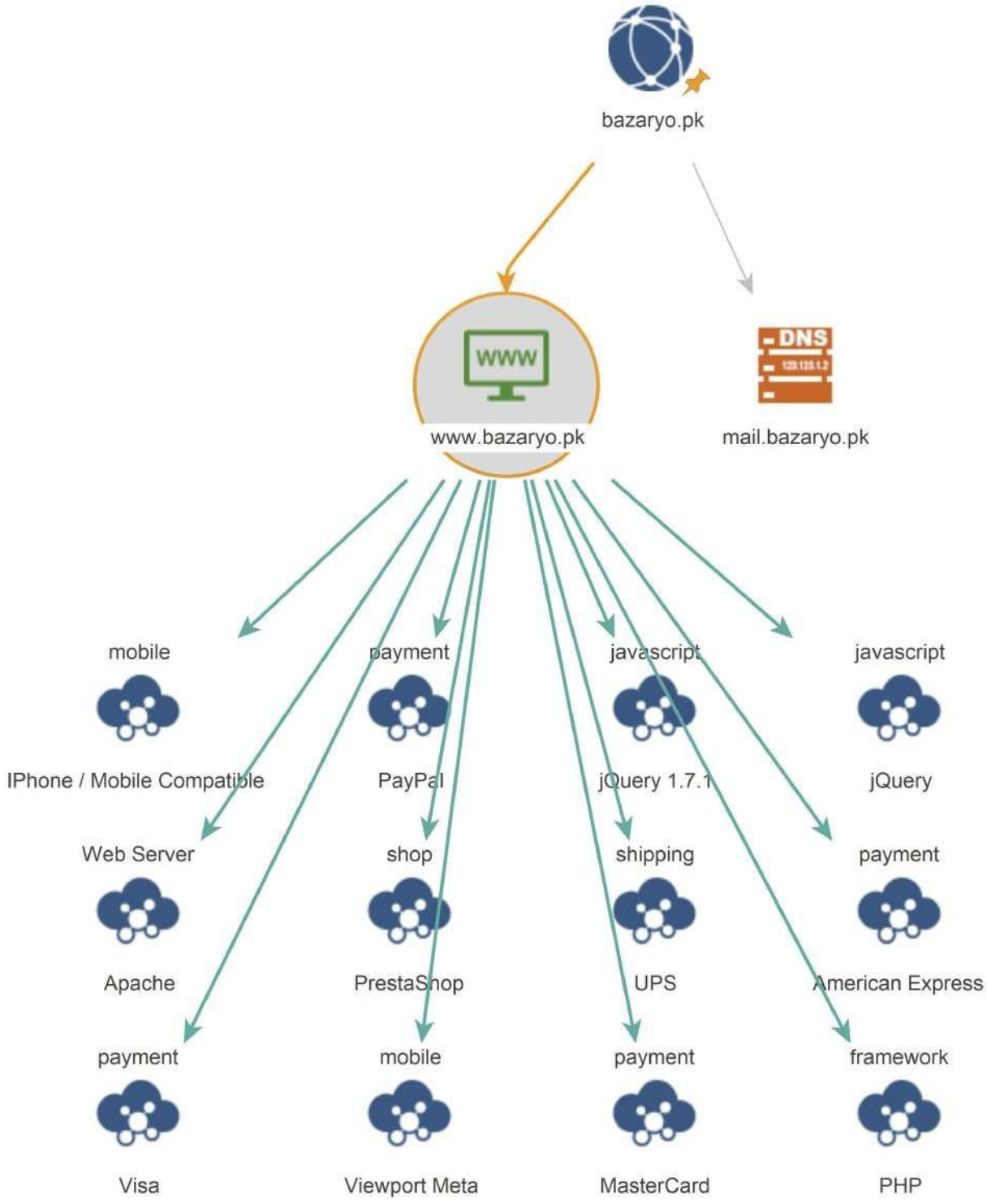
Output:



Snmp enumeration:

Output:


root@kali: ~
File Actions Edit View Help
┌──(root㉿kali)-[~]
└─# nmap -script ssl -cert 52.86.6.113
nmap: unrecognized option '-cert'
See the output of nmap -h for a summary of options.
┌──(root㉿kali)-[~]
└─# nmap -script ssl-cert-intadder 52.86.6.113
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-26 03:47 EDT
NSE: failed to initialize the script engine:
/usr/bin/../share/nmap/nse_main.lua:829: 'ssl-cert-intadder' did not match a category, filename, or directory
stack traceback:
[C]: in function 'error'
/usr/bin/../share/nmap/nse_main.lua:829: in local 'get_chosen_scripts'
/usr/bin/../share/nmap/nse_main.lua:1364: in main chunk
[C]: in ?
QUITTING!
┌──(root㉿kali)-[~]
└─# nmap -script ssl-date 52.86.6.113
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-26 03:48 EDT
Nmap scan report for 52.86.6.113
Host is up (0.021s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 23.73 seconds
┌──(root㉿kali)-[~]
└─# nmap -sV 52.86.6.113
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-26 03:49 EDT
Nmap scan report for 52.86.6.113
Host is up (0.00077s latency).
All 1000 scanned ports on 52.86.6.113 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.53 seconds
┌──(root㉿kali)-[~]
└─# nmap -sU -p 161 --script=snmp-processes 52.86.6.113
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-26 03:52 EDT
Nmap scan report for 52.86.6.113
Host is up (0.00059s latency).
PORT STATE SERVICE
161/udp open|filtered snmp
Nmap done: 1 IP address (1 host up) scanned in 18.54 seconds
┌──(root㉿kali)-[~]
└─#


bazaryo.pk
www.bazaryo.pk
mail.bazaryo.pk
mobile
IPhone / Mobile Compatible
payment
PayPal
javascript
jQuery 1.7.1
javascript
jQuery
Web Server
Apache
shop
PrestaShop
shipping
UPS
payment
American Express
payment
Visa
mobile
Viewport Meta
payment
MasterCard
framework
PHP

1. Top 10 Entities

Total number of entities	15
Total number of links	14

Ranked by Incoming Links

Rank	Type	Value	Incoming links
1	DNS Name	mail.bazaryo.pk	1
2	BuiltWith Technology	IPhone / Mobile Compatible	1
3	BuiltWith Technology	PayPal	1
4	BuiltWith Technology	jQuery 1.7.1	1
5	BuiltWith Technology	jQuery	1
6	BuiltWith Technology	Apache	1
7	BuiltWith Technology	PrestaShop	1
8	BuiltWith Technology	UPS	1
9	BuiltWith Technology	American Express	1
10	BuiltWith Technology	Visa	1

Ranked by Outgoing Links

Rank	Type	Value	Outgoing links
1	Website	www.bazaryo.pk	12
2	Domain	bazaryo.pk	2
3	DNS Name	mail.bazaryo.pk	0
4	BuiltWith Technology	IPhone / Mobile Compatible	0
5	BuiltWith Technology	PayPal	0
6	BuiltWith Technology	jQuery 1.7.1	0
7	BuiltWith Technology	jQuery	0
8	BuiltWith Technology	Apache	0
9	BuiltWith Technology	PrestaShop	0
10	BuiltWith Technology	UPS	0

Ranked by Total Links

Rank	Type	Value	Total links
1	Website	www.bazaryo.pk	13
2	Domain	bazaryo.pk	2
3	DNS Name	mail.bazaryo.pk	1
4	BuiltWith Technology	IPhone / Mobile Compatible	1
5	BuiltWith Technology	PayPal	1
6	BuiltWith Technology	jQuery 1.7.1	1
7	BuiltWith Technology	jQuery	1
8	BuiltWith Technology	Apache	1
9	BuiltWith Technology	PrestaShop	1
10	BuiltWith Technology	UPS	1

2. Entities by Type

BuiltWith Technologys (12)	
American Express	Apache
IPhone / Mobile Compatible	MasterCard
PHP	PayPal
PrestaShop	UPS
Viewport Meta	Visa
jQuery	jQuery 1.7.1

DNS Names (1)
mail.bazaryo.pk

Domains (1)
bazaryo.pk

Websites (1)
www.bazaryo.pk

3. Entity Details

Website

maltego.Website

www.bazaryo.pk

Weight	100
Website	www.bazaryo.pk
SSL Enabled	false
Ports	[80]

Incoming (1)

Domain	bazaryo.pk

Outgoing (12)

BuiltWith Technology	American Express
BuiltWith Technology	Apache
BuiltWith Technology	IPhone / Mobile Compatible
BuiltWith Technology	MasterCard
BuiltWith Technology	PHP
BuiltWith Technology	PayPal
BuiltWith Technology	PrestaShop
BuiltWith Technology	UPS
BuiltWith Technology	Viewport Meta
BuiltWith Technology	Visa
BuiltWith Technology	jQuery
BuiltWith Technology	jQuery 1.7.1

Domain

maltego.Domain

bazaryo.pk

Weight	50
Domain Name	bazaryo.pk
WHOIS Info	Socket not responding: [Errno -2] Name or service not known

Outgoing (2)

DNS Name	mail.bazaryo.pk
Website	www.bazaryo.pk

DNS Name

maltego.DNSName

mail.bazaryo.pk

Weight	100
DNS Name	mail.bazaryo.pk

Incoming (1)

Domain	bazaryo.pk

BuiltWith Technology

maltego.builtwith.Technology

IPhone / Mobile Compatible

Weight	0
Type	mobile
Text	IPhone / Mobile Compatible

BuiltWith Technology Information

Property	Value
Name	IPhone / Mobile Compatible
Description	The website contains code that allows the page to support IPhone / Mobile Content.
Is Premium	no
Type	mobile
Categories	
Link	https://apple.com
First Seen	2020-12-25 08:00:00.000+0000
Last Seen	2024-05-18 07:00:00.000+0000

Incoming (1)

Website	www.bazaryo.pk

BuiltWith Technology

maltego.builtwith.Technology

PayPal

Weight	0
Type	payment
Text	PayPal

BuiltWith Technology Information

Property	Value
Name	PayPal
Description	The website accepts payments with PayPal.
Is Premium	no
Type	payment
Categories	Payment Acceptance
Link	https://paypal.com
First Seen	2020-12-25 08:00:00.000+0000
Last Seen	2024-05-18 07:00:00.000+0000

Incoming (1)

Website	www.bazaryo.pk

BuiltWith Technology

maltego.builtwith.Technology

jQuery 1.7.1

Weight	0
Type	javascript
Text	jQuery 1.7.1

BuiltWith Technology Information

Property	Value
Name	jQuery 1.7.1
Description	jQuery version 1.7.1
Is Premium	no
Type	javascript
Categories	
Link	https://blog.jquery.com/2011/11/21/jquery-1-7-1-released/
First Seen	2020-12-25 08:00:00.000+0000
Last Seen	2024-05-18 07:00:00.000+0000

Incoming (1)

Website	www.bazaryo.pk

BuiltWith Technology

maltego.builtwith.Technology

jQuery

Weight	0
Type	javascript
Text	jQuery

BuiltWith Technology Information

Property	Value
Name	jQuery
Description	JQuery is a fast, concise, JavaScript Library that simplifies how you traverse HTML documents, handle events, perform animations, and add Ajax interactions to your web pages. jQuery is designed to change the way that you write JavaScript.
Is Premium	no
Type	javascript
Categories	JavaScript Library
Link	https://jquery.com
First Seen	2020-12-25 08:00:00.000+0000
Last Seen	2024-05-18 07:00:00.000+0000

Incoming (1)

Website	www.bazaryo.pk

BuiltWith Technology

maltego.builtwith.Technology

Apache

Weight	0
Type	Web Server
Text	Apache

BuiltWith Technology Information

Property	Value
Name	Apache
Description	Apache has been the most popular web server on the Internet since April 1996.
Is Premium	no
Type	Web Server
Categories	
Link	https://httpd.apache.org/
First Seen	2020-12-25 08:00:00.000+0000
Last Seen	2024-05-18 07:00:00.000+0000

Incoming (1)

Website	www.bazaryo.pk

BuiltWith Technology

maltego.builtwith.Technology

PrestaShop

Weight	0
Type	shop
Text	PrestaShop

BuiltWith Technology Information

Property	Value
Name	PrestaShop
Description	OpenSource e-commerce solution that can be used for free.
Is Premium	no
Type	shop
Categories	Open Source
Link	https://www.prestashop.com
First Seen	2020-12-25 08:00:00.000+0000
Last Seen	2024-05-18 07:00:00.000+0000

Incoming (1)

Website	www.bazaryo.pk

BuiltWith Technology

maltego.builtwith.Technology

UPS

Weight	0
Type	shipping
Text	UPS

BuiltWith Technology Information

Property	Value
Name	UPS
Description	US based package delivery company.
Is Premium	no
Type	shipping
Categories	
Link	https://ups.com
First Seen	2020-12-25 08:00:00.000+0000
Last Seen	2024-05-18 07:00:00.000+0000

Incoming (1)

Website	www.bazaryo.pk

BuiltWith Technology

maltego.builtwith.Technology

American Express

Weight	0
Type	payment
Text	American Express

BuiltWith Technology Information

Property	Value
Name	American Express
Description	The website accepts payments with American Express.
Is Premium	no
Type	payment
Categories	Payment Acceptance
Link	https://amex.com
First Seen	2020-12-25 08:00:00.000+0000
Last Seen	2024-05-18 07:00:00.000+0000

Incoming (1)

Website	www.bazaryo.pk

BuiltWith Technology

maltego.builtwith.Technology

Visa

Weight	0
Type	payment
Text	Visa

BuiltWith Technology Information

Property	Value
Name	Visa
Description	The website accepts payments with Visa.
Is Premium	no
Type	payment
Categories	Payment Acceptance
Link	https://visa.com
First Seen	2020-12-25 08:00:00.000+0000
Last Seen	2024-05-18 07:00:00.000+0000

Incoming (1)

Website	www.bazaryo.pk

BuiltWith Technology

maltego.builtwith.Technology

Viewport Meta

Weight	0
Type	mobile
Text	Viewport Meta

BuiltWith Technology Information

Property	Value
Name	Viewport Meta
Description	This page uses the viewport meta tag which means the content may be optimized for mobile content.
Is Premium	no
Type	mobile
Categories	
Link	https://developers.google.com/speed/docs/insights/ConfigureViewport
First Seen	2020-12-25 08:00:00.000+0000
Last Seen	2024-05-18 07:00:00.000+0000

Incoming (1)

Website	www.bazaryo.pk

BuiltWith Technology

maltego.builtwith.Technology

MasterCard

Weight	0
Type	payment
Text	MasterCard

BuiltWith Technology Information

Property	Value
Name	MasterCard
Description	The website accepts payments with MasterCard.
Is Premium	no
Type	payment
Categories	Payment Acceptance
Link	https://mastercard.com
First Seen	2020-12-25 08:00:00.000+0000
Last Seen	2024-05-18 07:00:00.000+0000

Incoming (1)

Website	www.bazaryo.pk

BuiltWith Technology

maltego.builtwith.Technology

PHP

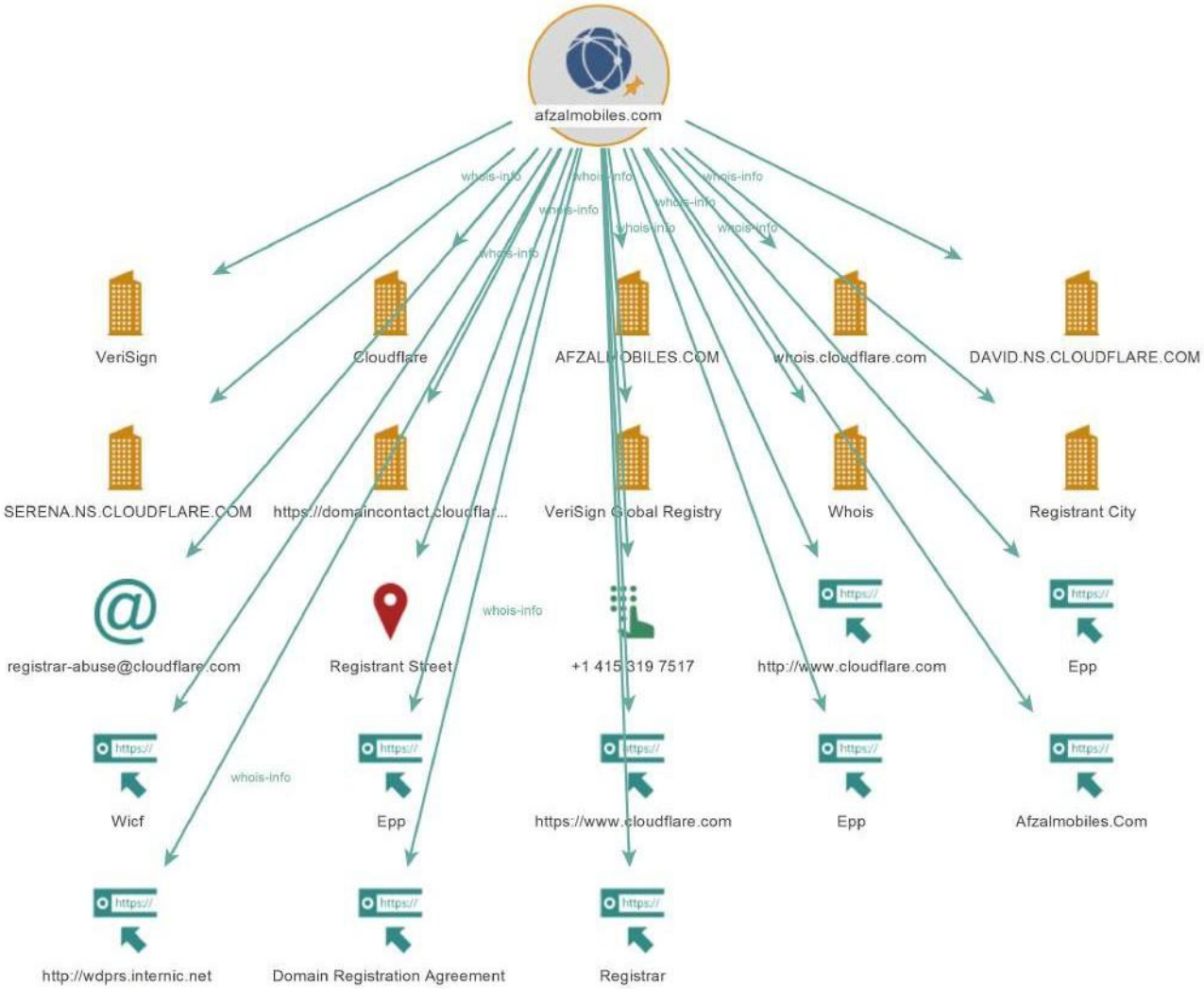
Weight	0
Type	framework
Text	PHP

BuiltWith Technology Information

Property	Value
Name	PHP
Description	PHP is a widely used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML.
Is Premium	no
Type	framework
Categories	
Link	https://www.php.net
First Seen	2020-12-25 08:00:00.000+0000
Last Seen	2024-05-18 07:00:00.000+0000

Incoming (1)

Website	www.bazaryo.pk


afzalmobiles.com
whois-info
VeriSign
Cloudflare
AFZALMOBILES.COM
whois.cloudflare.com
DAVID.NS.CLOUDFLARE.COM
SERENA.NS.CLOUDFLARE.COM
https://domaincontact.cloudfla...
VeriSign Global Registry
Whois
Registrant City
registrar-abuse@cloudflare.com
Registrant Street
+1 415 319 7517
http://www.cloudflare.com
Epp
Wicf
Epp
https://www.cloudflare.com
Epp
Afzalmobiles.Com
http://wdprs.internic.net
Domain Registration Agreement
Registrar

1. Top 10 Entities

Total number of entities	24
Total number of links	23

Ranked by Incoming Links

Rank	Type	Value	Incoming links
1	Phone Number	+1 415 319 7517	1
2	URL	http://www.cloudflare.com	1
3	URL	Epp	1
4	URL	Wicf	1
5	URL	Epp	1
6	URL	https://www.cloudflare.com	1
7	URL	Epp	1
8	Company	VeriSign	1
9	URL	Afzalmobiles.Com	1
10	Company	Cloudflare	1

Ranked by Outgoing Links

Rank	Type	Value	Outgoing links
1	Domain	afzalmobiles.com	23
2	Phone Number	+1 415 319 7517	0
3	URL	http://www.cloudflare.com	0
4	URL	Epp	0
5	URL	Wicf	0
6	URL	Epp	0
7	URL	https://www.cloudflare.com	0
8	URL	Epp	0
9	Company	VeriSign	0
10	URL	Afzalmobiles.Com	0

Ranked by Total Links

Rank	Type	Value	Total links
1	Domain	afzalmobiles.com	23
2	Phone Number	+1 415 319 7517	1
3	URL	http://www.cloudflare.com	1
4	URL	Epp	1
5	URL	Wicf	1
6	URL	Epp	1
7	URL	https://www.cloudflare.com	1
8	URL	Epp	1
9	Company	VeriSign	1
10	URL	Afzalmobiles.Com	1

2. Entities by Type

Companies (10)	
AFZALMOBILES.COM	Cloudflare
DAVID.NS.CLOUDFLARE.COM	Registrant City
SERENA.NS.CLOUDFLARE.COM	VeriSign
VeriSign Global Registry	Whois
https://domaincontact.cloudflareregistrar.com/afzalmobiles.com	whois.cloudflare.com

Domains (1)
afzalmobiles.com

Email Addresses (1)
registrar-abuse@cloudflare.com

Locations (1)
Registrant Street

Phone Numbers (1)
+1 415 319 7517

URLs (10)	
Afzalmobiles.Com	Domain Registration Agreement
Epp	Epp
Epp	Registrar
Wicf	http://wdprs.internic.net
http://www.cloudflare.com	https://www.cloudflare.com

3. Entity Details

Domain

maltego.Domain

afzalmobiles.com

Weight	12
Domain Name	afzalmobiles.com

WHOIS Info	Domain Name: AFZALMOBILES.COM Registry Domain ID: 2734284946_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.cloudflare.com Registrar URL: http://www.cloudflare.com Updated Date: 2023-09-25T20:50:56Z Creation Date: 2022-10-25T09:51:10Z Registry Expiry Date: 2024-10-25T09:51:10Z Registrar: CloudFlare, Inc. Registrar IANA ID: 1910 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: DAVID.NS.CLOUDFLARE.COM Name Server: SERENA.NS.CLOUDFLARE.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-05-26T06:23:23Z <<< For more information on Whois status codes, please visit https://icann.org/epp NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration. TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated and high-volume to access or query the Whois database except as reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time. The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars. Domain Name: AFZALMOBILES.COM Registry Domain ID: 2734284946_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.cloudflare.com Registrar URL: https://www.cloudflare.com Updated Date: 2023-10-13T21:48:10Z Creation Date: 2022-10-25T09:51:10Z Registrar Registration Expiration Date: 2024-10-25T09:51:10Z Registrar: Cloudflare, Inc. Registrar IANA ID: 1910 Domain Status: clienttransferprohibited https://icann.org/epp#clienttransferprohibited Registry Registrant ID: Registrant Name: DATA REDACTED Registrant Organization: DATA REDACTED Registrant Street: DATA REDACTED Registrant City: DATA REDACTED Registrant State/Province: Federal Registrant Postal Code: DATA REDACTED Registrant Country: PK Registrant Phone: DATA REDACTED Registrant Phone Ext: DATA REDACTED Registrant Fax: DATA REDACTED Registrant Fax Ext: DATA REDACTED

Registrant Fax Ext: DATA REDACTED
Registrant Email:
https://domaincontact.cloudflareregistrar.com/afzalmobiles.com
Registry Admin ID:
Admin Name: DATA REDACTED
Admin Organization: DATA REDACTED
Admin Street: DATA REDACTED
Admin City: DATA REDACTED
Admin State/Province: DATA REDACTED
Admin Postal Code: DATA REDACTED
Admin Country: DATA REDACTED
Admin Phone: DATA REDACTED
Admin Phone Ext: DATA REDACTED
Admin Fax: DATA REDACTED
Admin Fax Ext: DATA REDACTED
Admin Email: https://domaincontact.cloudflareregistrar.com/afzalmobiles.com
Registry Tech ID:
Tech Name: DATA REDACTED
Tech Organization: DATA REDACTED
Tech Street: DATA REDACTED
Tech City: DATA REDACTED
Tech State/Province: DATA REDACTED
Tech Postal Code: DATA REDACTED
Tech Country: DATA REDACTED
Tech Phone: DATA REDACTED
Tech Phone Ext: DATA REDACTED
Tech Fax: DATA REDACTED
Tech Fax Ext: DATA REDACTED
Tech Email: https://domaincontact.cloudflareregistrar.com/afzalmobiles.com
Registry Billing ID:
Billing Name: DATA REDACTED
Billing Organization: DATA REDACTED
Billing Street: DATA REDACTED
Billing City: DATA REDACTED
Billing State/Province: DATA REDACTED
Billing Postal Code: DATA REDACTED
Billing Country: DATA REDACTED
Billing Phone: DATA REDACTED
Billing Phone Ext: DATA REDACTED
Billing Fax: DATA REDACTED
Billing Fax Ext: DATA REDACTED
Billing Email: https://domaincontact.cloudflareregistrar.com/afzalmobiles.com
Name Server: david.ns.cloudflare.com
Name Server: serena.ns.cloudflare.com
DNSSEC: unsigned
Registrar Abuse Contact Email: registrar-abuse@cloudflare.com
Registrar Abuse Contact Phone: +1.4153197517
URL of the ICANN WHOIS Data Problem Reporting System:
http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-05-26T06:23:43Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Cloudflare provides more than 13 million domains with the tools to give their global users a faster, more secure, and more reliable internet experience.

NOTICE:

Data in the Cloudflare Registrar WHOIS database is provided to you by Cloudflare
under the terms and conditions at https://www.cloudflare.com/domain-registration-agreement/

By submitting this query, you agree to abide by these terms.

Register your domain name at https://www.cloudflare.com/registrar/

Outgoing (23)	
Company	AFZALMOBILES.COM
Company	Cloudflare
Company	DAVID.NS.CLOUDFLARE.COM
Company	Registrant City
Company	SERENA.NS.CLOUDFLARE.COM
Company	VeriSign
Company	VeriSign Global Registry
Company	Whois
Company	https://domaincontact.cloudflareregistrar.com/afzalmobiles.com
Company	whois.cloudflare.com
Email Address	registrar-abuse@cloudflare.com
Location	Registrant Street
Phone Number	+1 415 319 7517
URL	Afzalmobiles.Com
URL	Domain Registration Agreement
URL	Epp
URL	Epp
URL	Epp
URL	Registrar
URL	Wicf
URL	http://wdprs.internic.net
URL	http://www.cloudflare.com
URL	https://www.cloudflare.com

Phone Number

maltego.PhoneNumber

+1 415 319 7517

Weight	100
Phone Number	+1 415 319 7517
Country Code	
City Code	
Area Code	
Last Digits	

Incoming (1)	
Domain	afzalmobiles.com

URL

maltego.URL

http://www.cloudflare.com

Weight	100
Short title	http://www.cloudflare.com
URL	http://www.cloudflare.com
Title	http://www.cloudflare.com
	URL: http://www.cloudflare.com Up

Incoming (1)

Domain	afzalmobiles.com

URL

maltego.URL

Epp

Weight	100
Short title	Epp
URL	https://icann.org/epp#clientTransferProhibited
Title	Epp
	ited https://icann.org/epp#clientTransferProhibited Na

Incoming (1)

Domain	afzalmobiles.com

URL

maltego.URL

Wicf

Weight	100
Short title	Wicf
URL	https://www.icann.org/wicf
Title	Wicf
	orm: https://www.icann.org/wicf/ >>>

Incoming (1)

Domain	afzalmobiles.com

URL

maltego.URL

Epp

Weight	100
Short title	Epp
URL	https://icann.org/epp
Title	Epp
	isit https://icann.org/epp NOTI

Incoming (1)

Domain	afzalmobiles.com

URL

maltego.URL

https://www.cloudflare.com

Weight	100
Short title	https://www.cloudflare.com
URL	https://www.cloudflare.com
Title	https://www.cloudflare.com
	URL: https://www.cloudflare.com Updat

Incoming (1)

Domain	afzalmobiles.com

URL

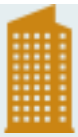
maltego.URL

Epp

Weight	100
Short title	Epp
URL	https://icann.org/epp#clienttransferprohibited
Title	Epp
	ited https://icann.org/epp#clienttransferprohibited Regis

Incoming (1)

Domain	afzalmobiles.com



Company

maltego.Company

VeriSign

Weight	95
Name	VeriSign

Info

Relevance:	0.951893
Count:	8

Incoming (1)

Domain	afzalmobiles.com

URL

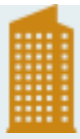
maltego.URL

Afzalmobiles.Com

Weight	100
Short title	Afzalmobiles.Com
URL	https://domaincontact.cloudflareregistrar.com/afzalmobiles.com
Title	Afzalmobiles.Com
	ail: https://domaincontact.cloudflareregistrar.com/afzalmobiles.com Regis

Incoming (1)

Domain	afzalmobiles.com



Company

maltego.Company

Cloudflare

Weight	63
Name	Cloudflare

Info

Relevance:	0.633151
Count:	4

Incoming (1)

Domain	afzalmobiles.com

URL

maltego.URL

http://wdprs.internic.net

Weight	100
Short title	http://wdprs.internic.net
URL	http://wdprs.internic.net
Title	http://wdprs.internic.net
	tem: http://wdprs.internic.net/ >>>

Incoming (1)

Domain	afzalmobiles.com

Company

maltego.Company

AFZALMOBILES.COM

Weight	62
Name	AFZALMOBILES.COM

Info

Relevance:	0.622859
Count:	2

Incoming (1)

Domain	afzalmobiles.com

URL

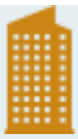
maltego.URL

Domain Registration Agreement

Weight	100
Short title	Domain Registration Agreement
URL	https://www.cloudflare.com/domain-registration-agreement
Title	Domain Registration Agreement
	s at https://www.cloudflare.com/domain-registration-agreement/
	By

Incoming (1)

Domain	afzalmobiles.com



Company

maltego.Company

whois.cloudflare.com

Weight	61
Name	whois.cloudflare.com

Info

Relevance:	0.6125
Count:	2

Incoming (1)

Domain	afzalmobiles.com

URL

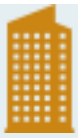
maltego.URL

Registrar

Weight	100
Short title	Registrar
URL	https://www.cloudflare.com/registrar
Title	Registrar
	e at https://www.cloudflare.com/registrar/

Incoming (1)

Domain	afzalmobiles.com



Company

maltego.Company

DAVID.NS.CLOUDFLARE.COM

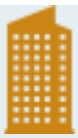
Weight	40
Name	DAVID.NS.CLOUDFLARE.COM

Info

Relevance:	0.406267
Count:	1

Incoming (1)

Domain	afzalmobiles.com



Company

maltego.Company

SERENA.NS.CLOUDFLARE.COM

Weight	40
Name	SERENA.NS.CLOUDFLARE.COM

Info

Relevance:	0.403633
Count:	1

Incoming (1)

Domain	afzalmobiles.com

Company

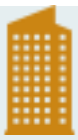
maltego.Company

https://domaincontact.cloudflareregistrar.com/afzalmobiles.com

Weight	39
Name	https://domaincontact.cloudflareregistrar.com/afzalmobiles.com

Info	
Relevance:	0.399376
Count:	3

Incoming (1)	
Domain	afzalmobiles.com



Company

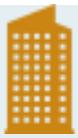
maltego.Company

VeriSign Global Registry

Weight	34
Name	VeriSign Global Registry

Info	
Relevance:	0.340333
Count:	1

Incoming (1)	
Domain	afzalmobiles.com



Company

maltego.Company

Whois

Weight	21
Name	Whois

Info	
Relevance:	0.213246
Count:	2

Incoming (1)	
Domain	afzalmobiles.com

Location

maltego.Location

Registrant Street

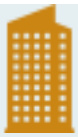
Weight	19
Name	Registrant Street
Country	
City	
Street Address	
Area	
Area Code	
Country Code	
Longitude	0.0
Latitude	0.0

Info

Relevance:	0.199904
Count:	1

Incoming (1)

Domain	afzalmobiles.com



Company

maltego.Company

Registrant City

Weight	19
Name	Registrant City

Info

Relevance:	0.197544
Count:	1

Incoming (1)

Domain	afzalmobiles.com

Email Address

maltego.EmailAddress

registrar-abuse@cloudflare.com

Weight	100
Email Address	registrar-abuse@cloudflare.com

Incoming (1)

Domain	afzalmobiles.com

Level 0 –

```
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
```

Level 1 –

```
bandit1@bandit:~$ cat ./-
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
```

Level 2 –

```
bandit2@bandit:~$ cat "spaces in this filename"
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
```

Level 3 –

```
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
```

Level 4 –

```
bandit4@bandit:~/inhere$ cat ./-file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
```

Level 5 –

```
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

Level 6 –

```
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
```

Level 7 –

```
bandit7@bandit:~$ grep millionth data.txt
millionth       TESKZC0XvTetK0S9xNwm25STk5iWrBvP
```

Level 8 –

```
bandit8@bandit:~$ sort data.txt | uniq -c | grep " 1 " | tr -s ' ' | cut -d ' ' -f3-
EN632PlfYiZbn3PhVK3XOGSlNInNE00t
```

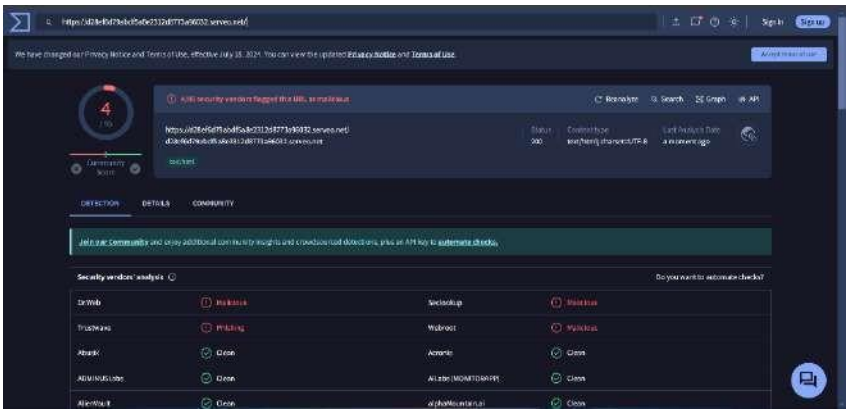
Level 9 –

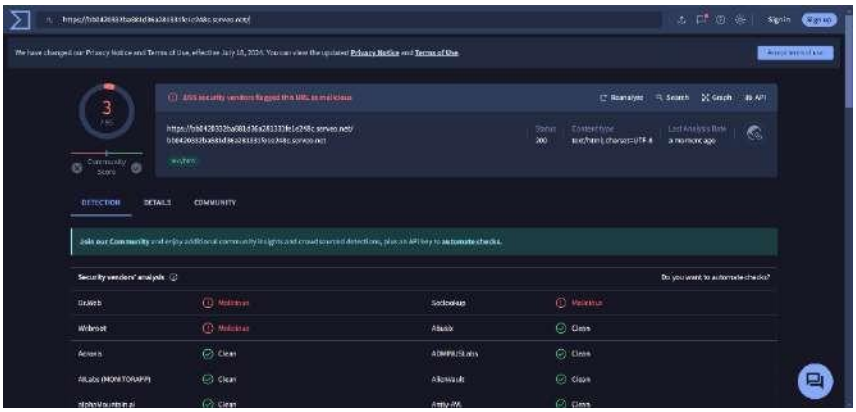
```
bandit9@bandit:~$ strings data.txt | grep '========'
x]T========== theG)"
========== passwordk^
========== is
========== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
```

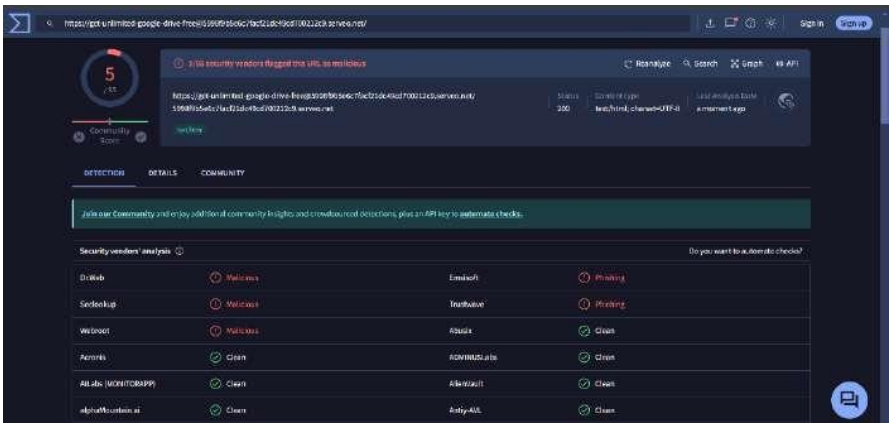
Level 10 –

```
bandit10@bandit:~$ base64 -d data.txt
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
```

Question 1 – Linkedin , Gmail , Microsoft Login Pages checked for vulnerabilities in Virustotal application

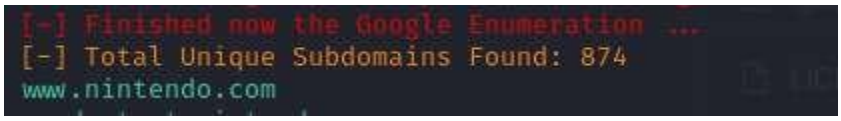


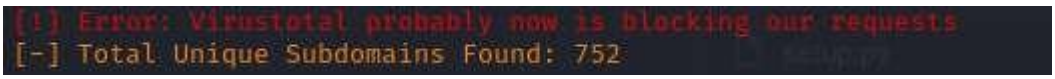


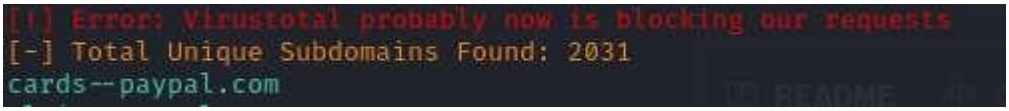


Question 2 –

3 Websites from Hackerone webpage scanned using Pyphisher in kali linux







Question 3 –

SPF record lookup and validation for: daraz.pk

SPF records are published in DNS as TXT records.

The TXT records found for your domain are:
facebook-domain-verification=x9zn5h6laazi1ndto3yz1n1suqi38
_globalsign-domain-verification=PRFY4H72cH8T8FrvwMF3yP_EW6kh2O-2NlcpFVTa
google-site-verification=K6PQAD2j1MFpGAsr9V9qCQ0nIVsER2TPR38uAwjl
MS=ms83592125
_globalsign-domain-verification=An54DkyNgjl2FVXRjela8Qz+2xHQEj58T+wFhAcPTEc=
52cvzt1tc79kvyp58phbf6qg7w2wt1k
google-site-verification=d5xhF81AO6wtiz3_q5WKpK3_uGCHVzB_1GSXYgm-Xc
rovag_verification_token=BE825BD9BF0E403AB58C3EBEE524C85E
mXT/by2NUfyN9NsQh4wHPOhGemk9laFvAaM8S+yiLDg=
21yDxZWuJWHwfY/HG8qbC5LPqmB1MlbKAsqwBecKcM=
v=spf1 include:_spf.google.com ~all

Checking to see if there is a valid SPF record.

DNS: Truncated UDP Reply, SPF records should fit in a UDP packet, retrying TCP

Found v=spf1 record for daraz.pk:
v=spf1 include:_spf.google.com ~all

evaluating...
SPF record passed validation test with pySPF (Python SPF library)!

Return to SPF checking tool (clears form)

Use the back button on your browser to return to the SPF checking tool without clearing the form.

EMKEI'S MAILER

Free online fake mailer with attachments, encryption, HTML editor and advanced settings...

E-mail sent successfully

SPF record lookup and validation for: homeshopping.pk

SPF records are published in DNS as TXT records.

The TXT records found for your domain are:
839oegoqnc1jkdbn9j61h00b5n
v=spf1 ip4:213.136.75.89 ip4:168.119.7.170 include:_spf.google.com ~all""v=spf1 include:servers.mcsv.net ?all

Checking to see if there is a valid SPF record.

Found v=spf1 record for homeshopping.pk:
v=spf1 ip4:213.136.75.89 ip4:168.119.7.170 include:_spf.google.com ~all""v=spf1 include:servers.mcsv.net ?all

evaluating...
Results - PermError SPF Permanent Error: Unknown mechanism found: ~all""v=spf1

Return to SPF checking tool (clears form)

Use the back button on your browser to return to the SPF checking tool without clearing the form.

SPF record lookup and validation for: sabaq.pk

SPF records are published in DNS as TXT records.

The TXT records found for your domain are:
v=spf1 a mx a:smtp.nayatel.com a:smtp3.nayatel.com a:smtp2.nayatel.com a:smtp1.nayatel.com ip4:203.82.48.0/24 ip4:115.186.154.158/32 ip4:115.186.188.0/24 ~all

Checking to see if there is a valid SPF record.

Found v=spf1 record for sabaq.pk:
v=spf1 a mx a:smtp.nayatel.com a:smtp3.nayatel.com a:smtp2.nayatel.com a:smtp1.nayatel.com ip4:203.82.48.0/24 ip4:115.186.154.158/32 ip4:115.186.188.0/24 ~all

evaluating...
SPF record passed validation test with pySPF (Python SPF library)!

Return to SPF checking tool (clears form)

Use the back button on your browser to return to the SPF checking tool without clearing the form.

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.

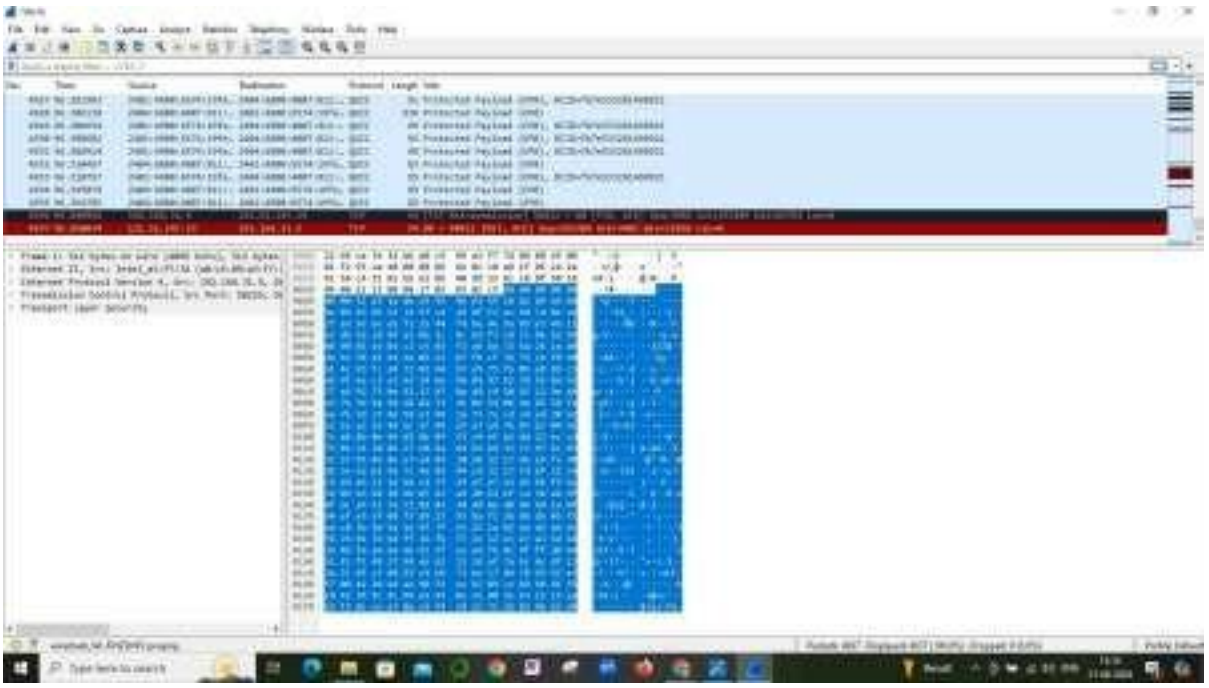
Here we need to website protocols

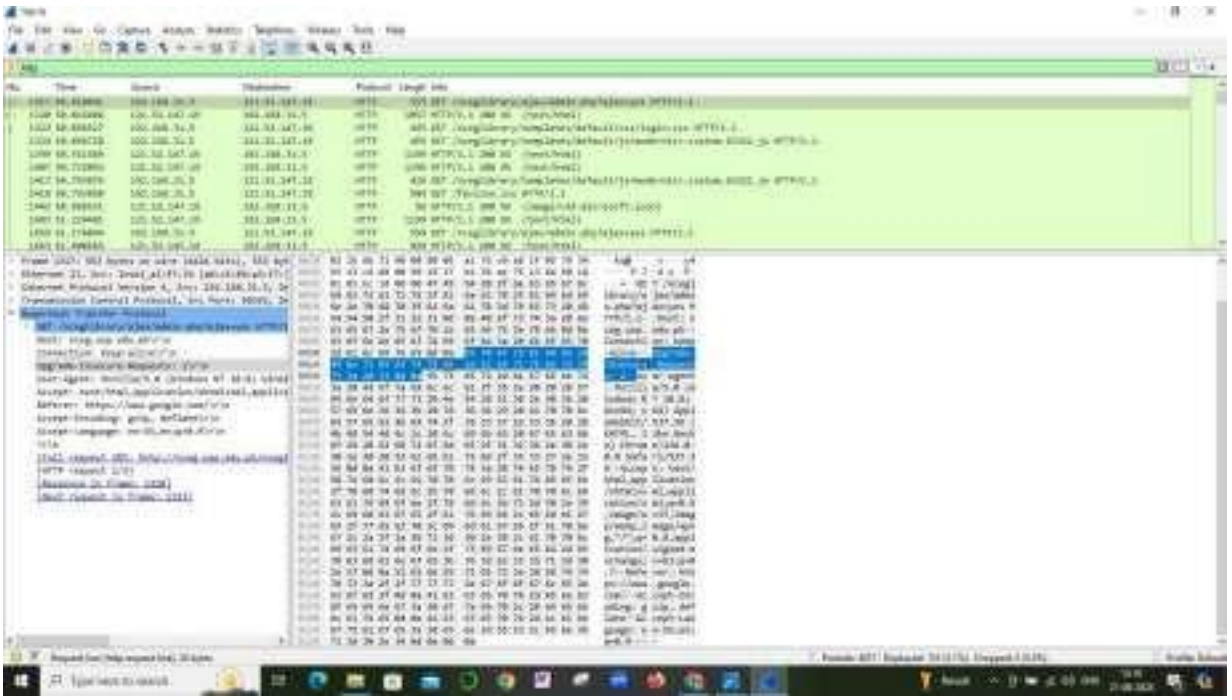
Http protocol : 81
FTP protocol : 20,21
Pop protocol : 110
Now find any website in google browser go to google . and search any website which is having vulnerabilities .

> HTTP

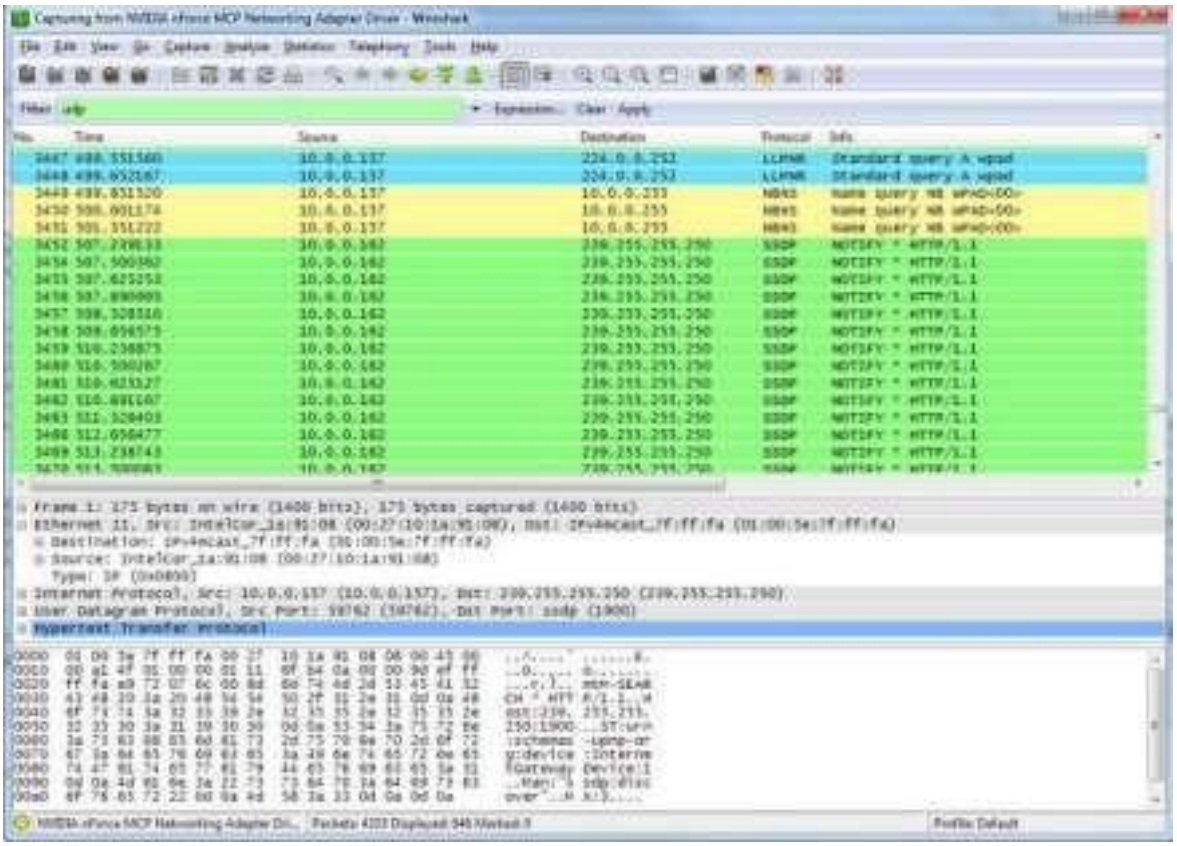
Step 1 : Start your wireshark tool

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

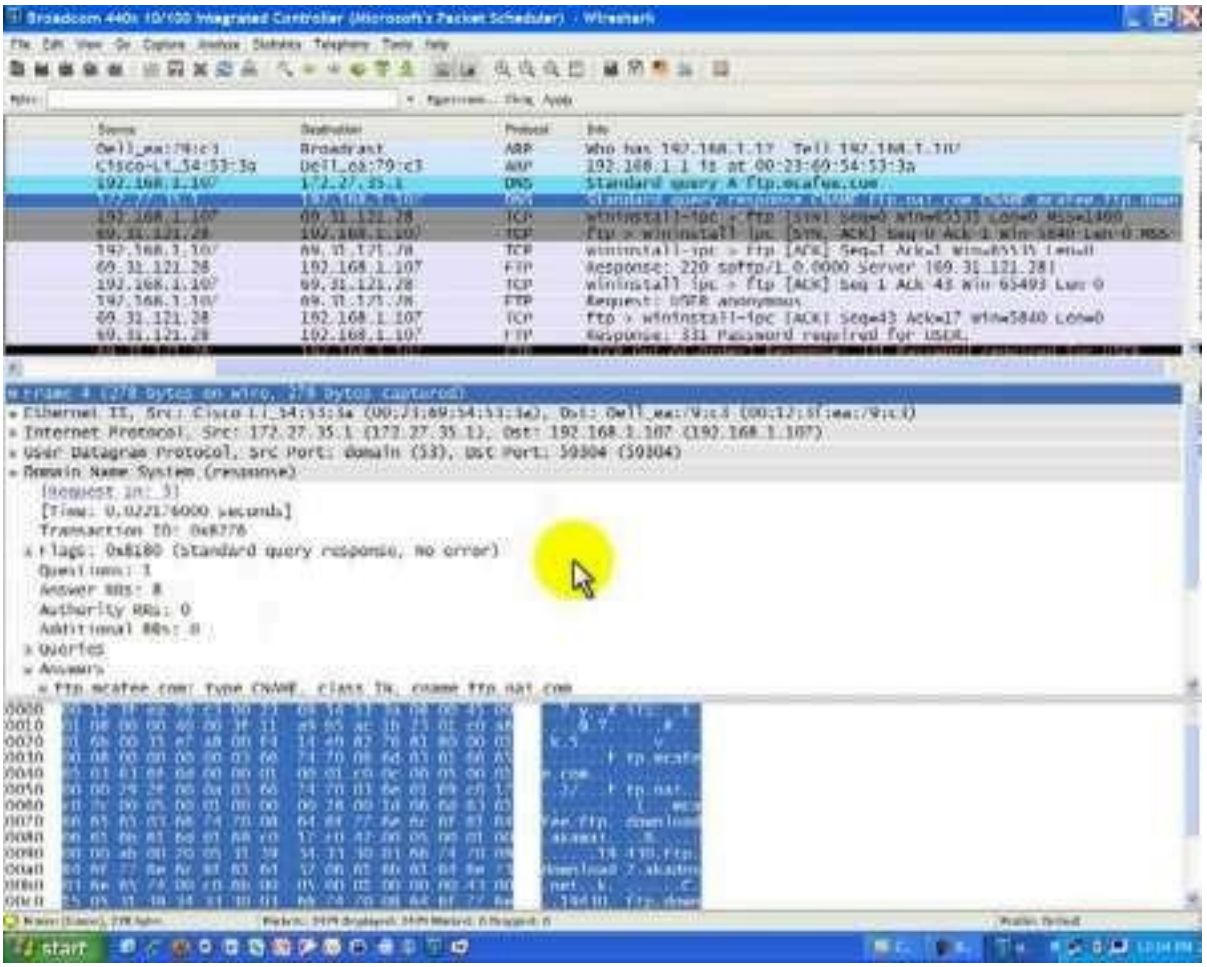




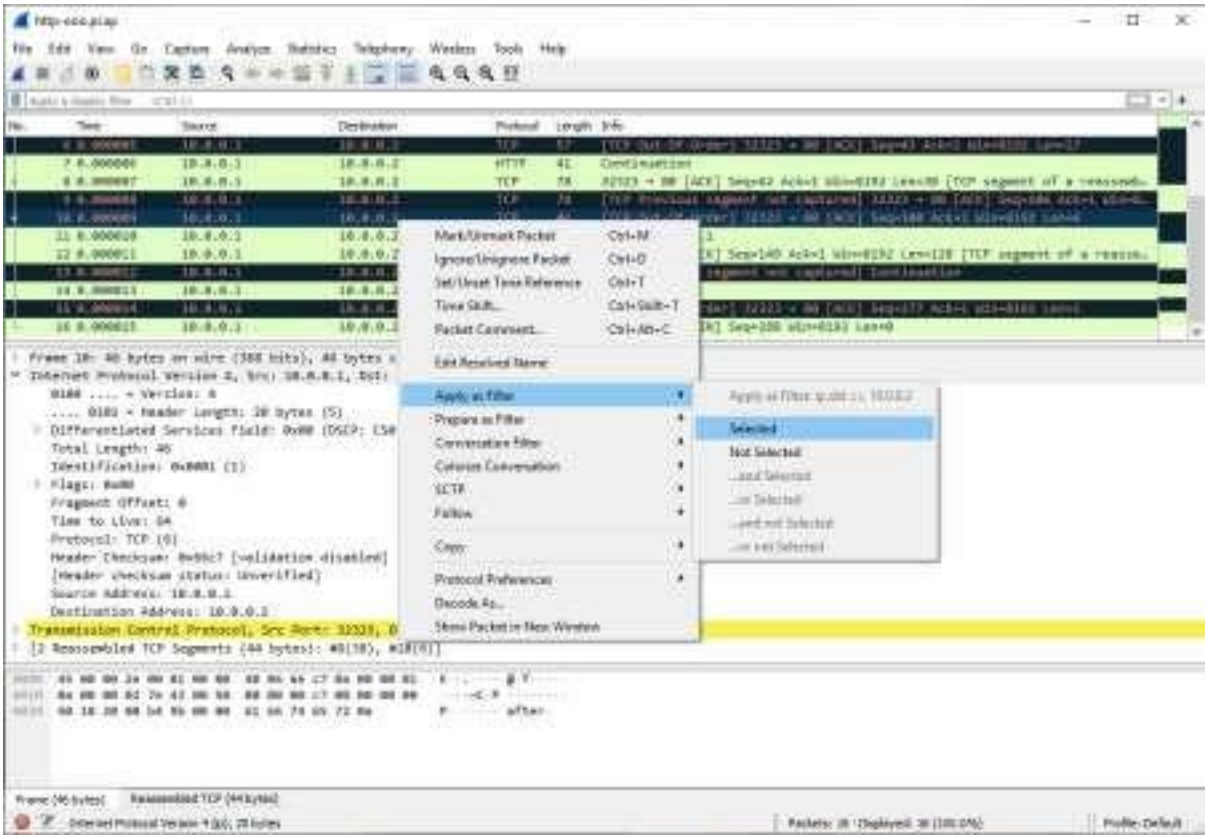
> FTP



> 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

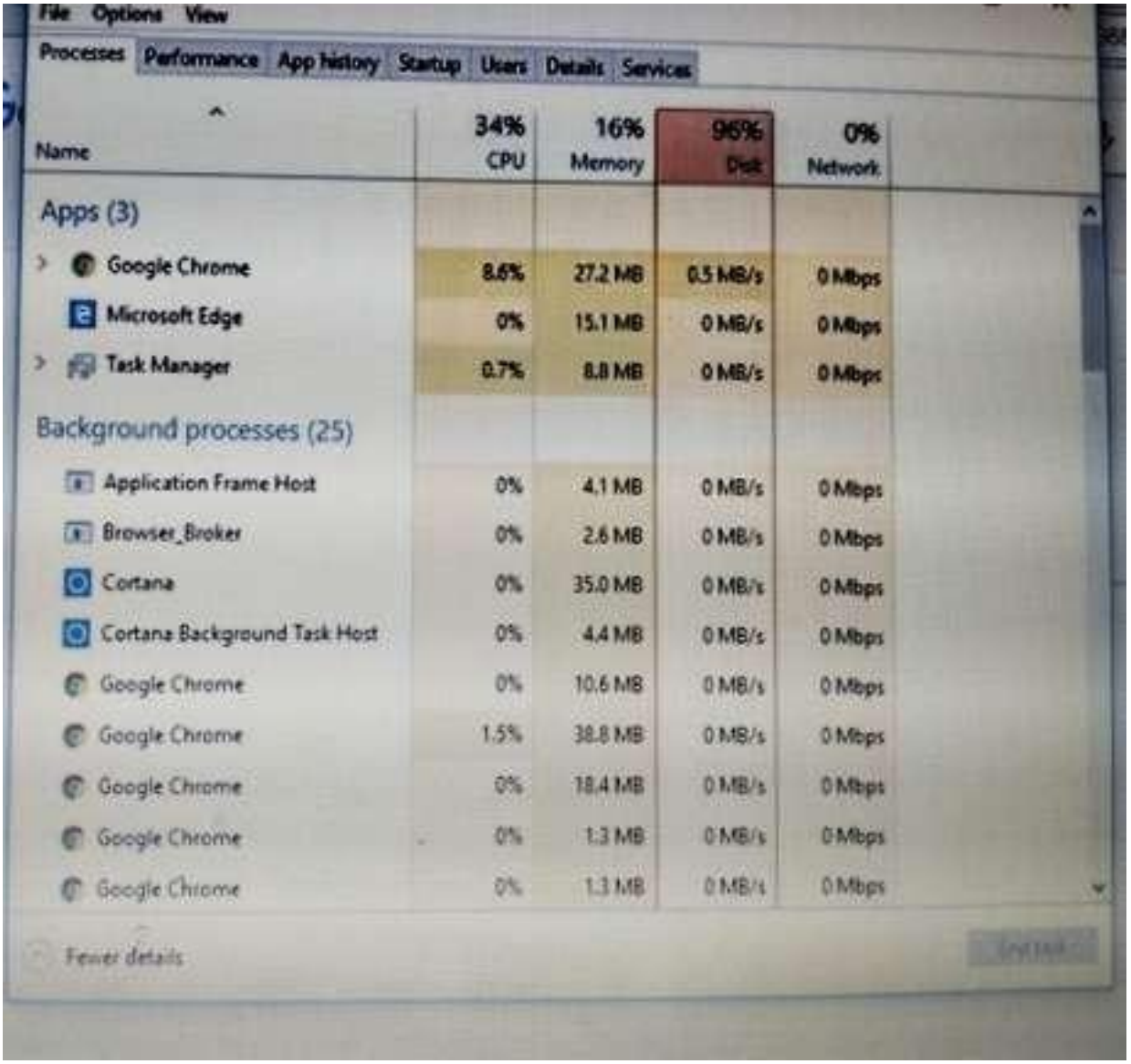
Step 3: Then start Performing the Dos attack on the Win 10 VM

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

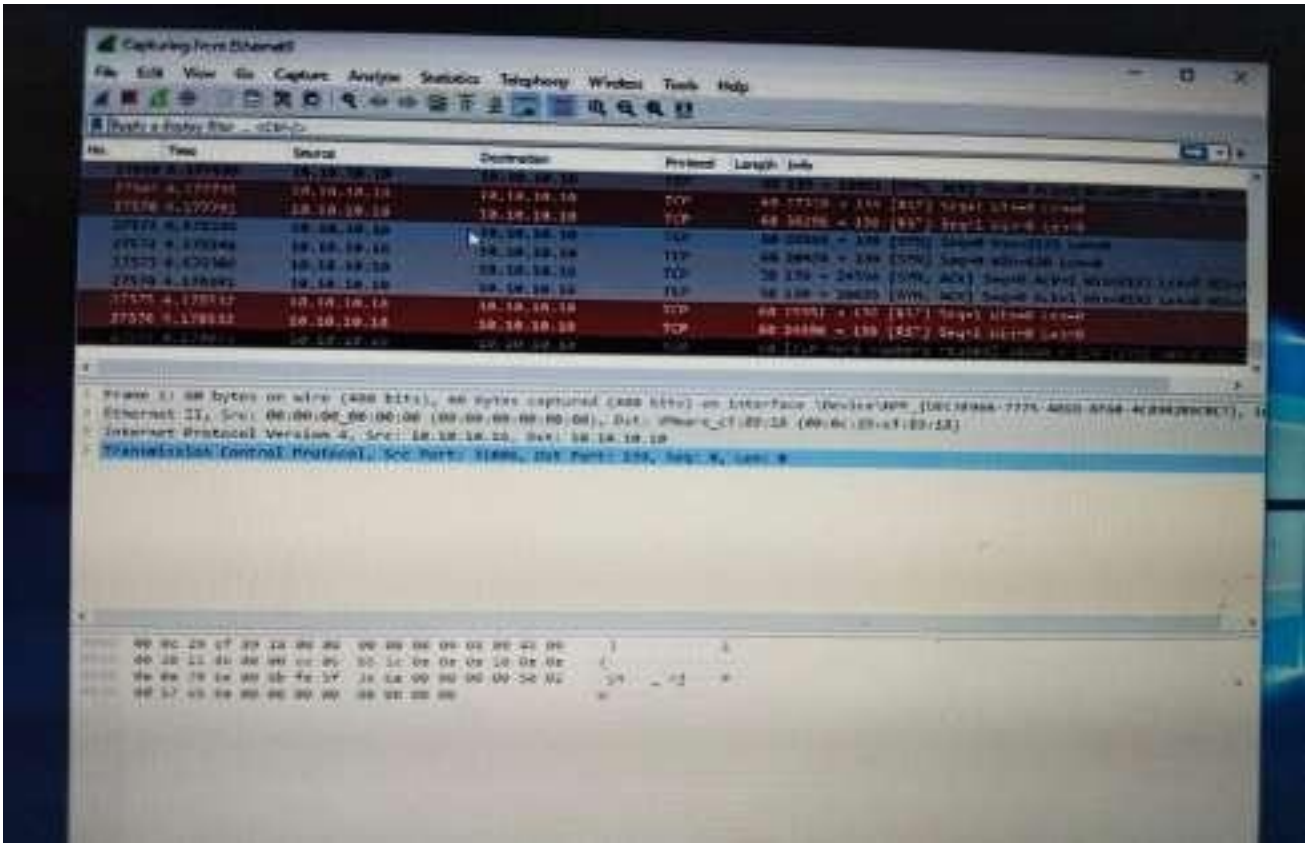
- **Write set RPORT 21 and press Enter**
- **Write RHOST [Windows server 2016's IP] and press Enter.**
- **Write set TIMEOUT 20000 and press Enter.**

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 .

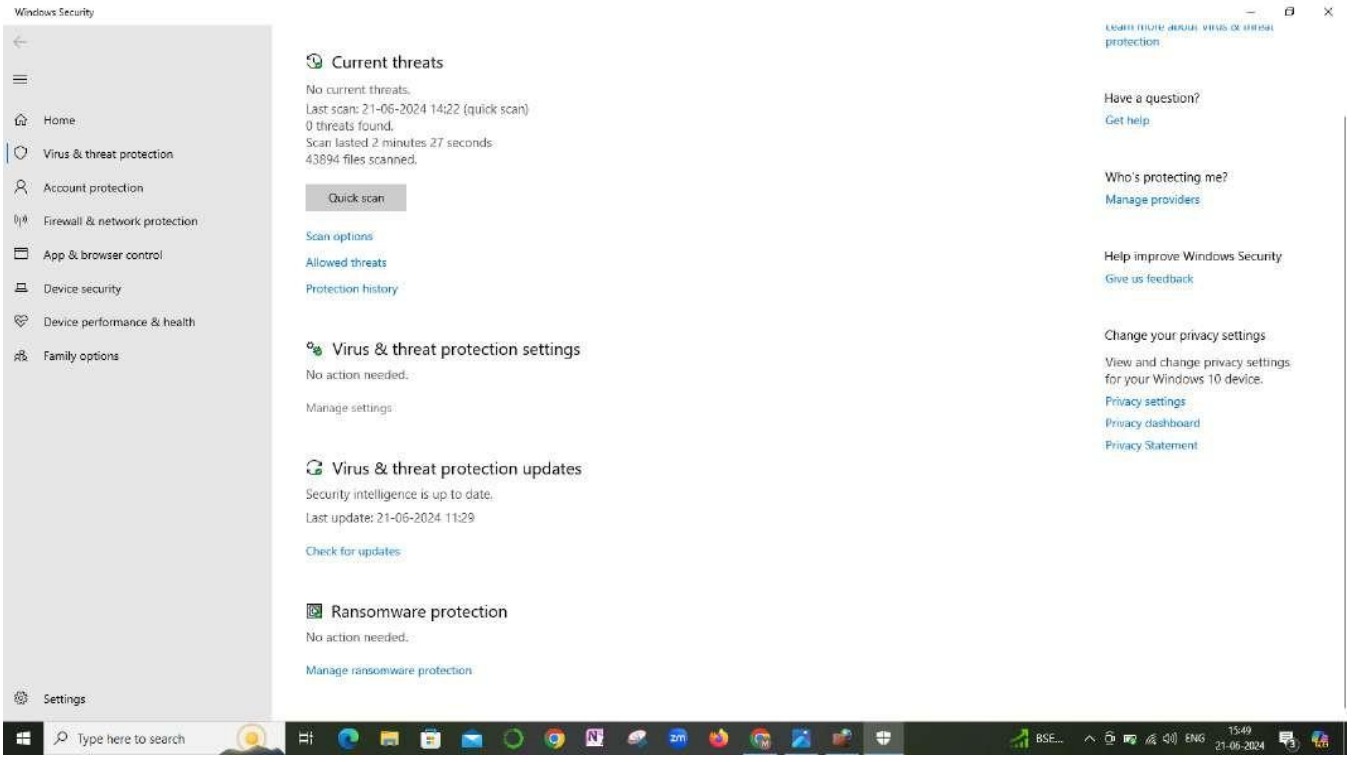


ASSIGNMENT - 5

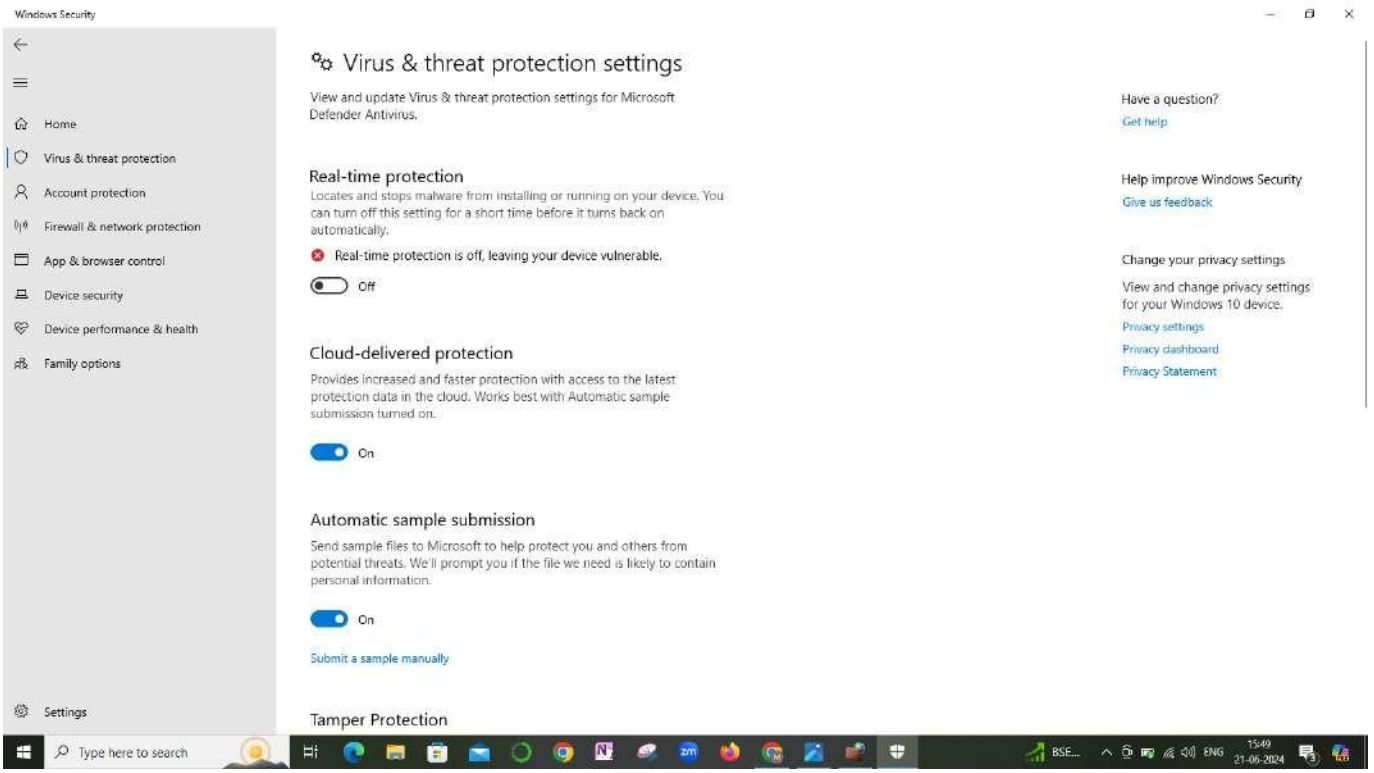
A. Turn off the antivirus and block the Instagram web application and a Standlone application by changing the rules of the firewall.

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

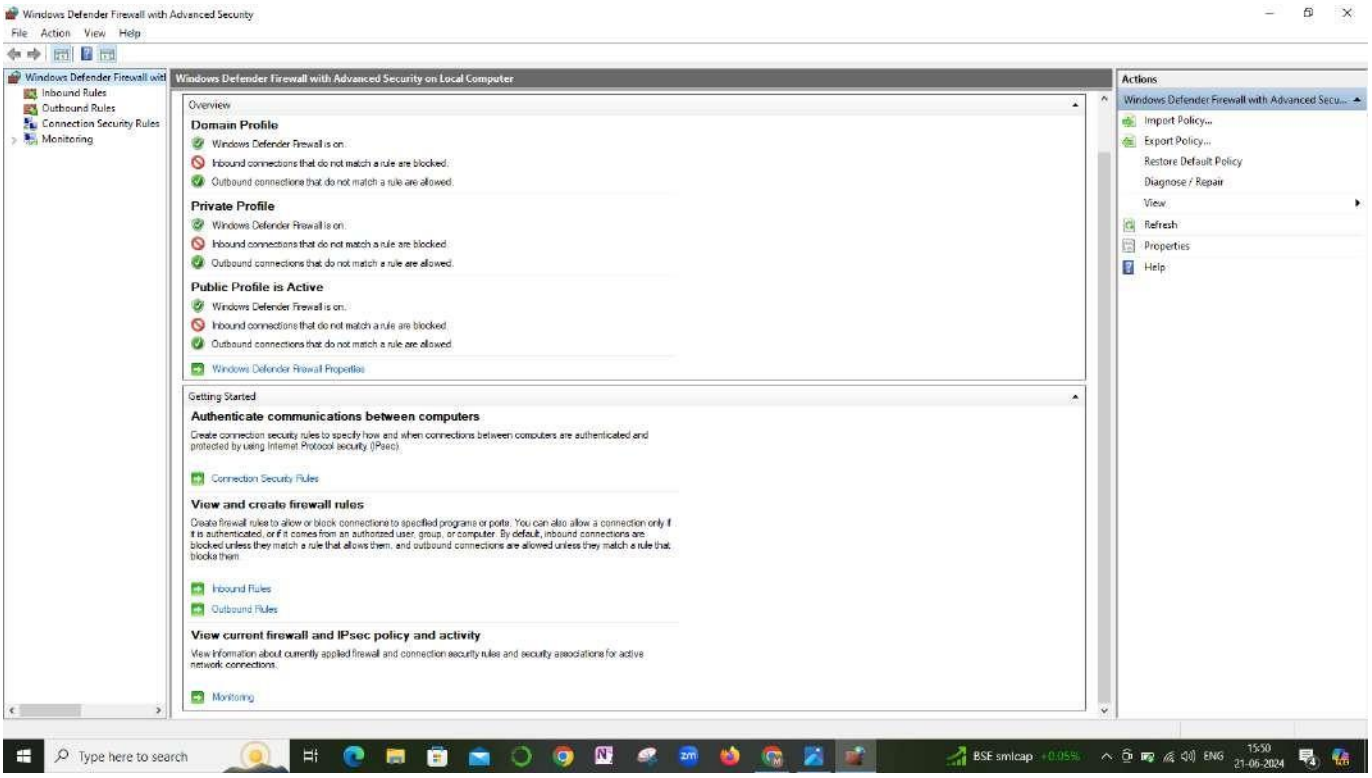
STEP 2: Now locate the virus and threat protection. And then go to the manage settings option in that page.



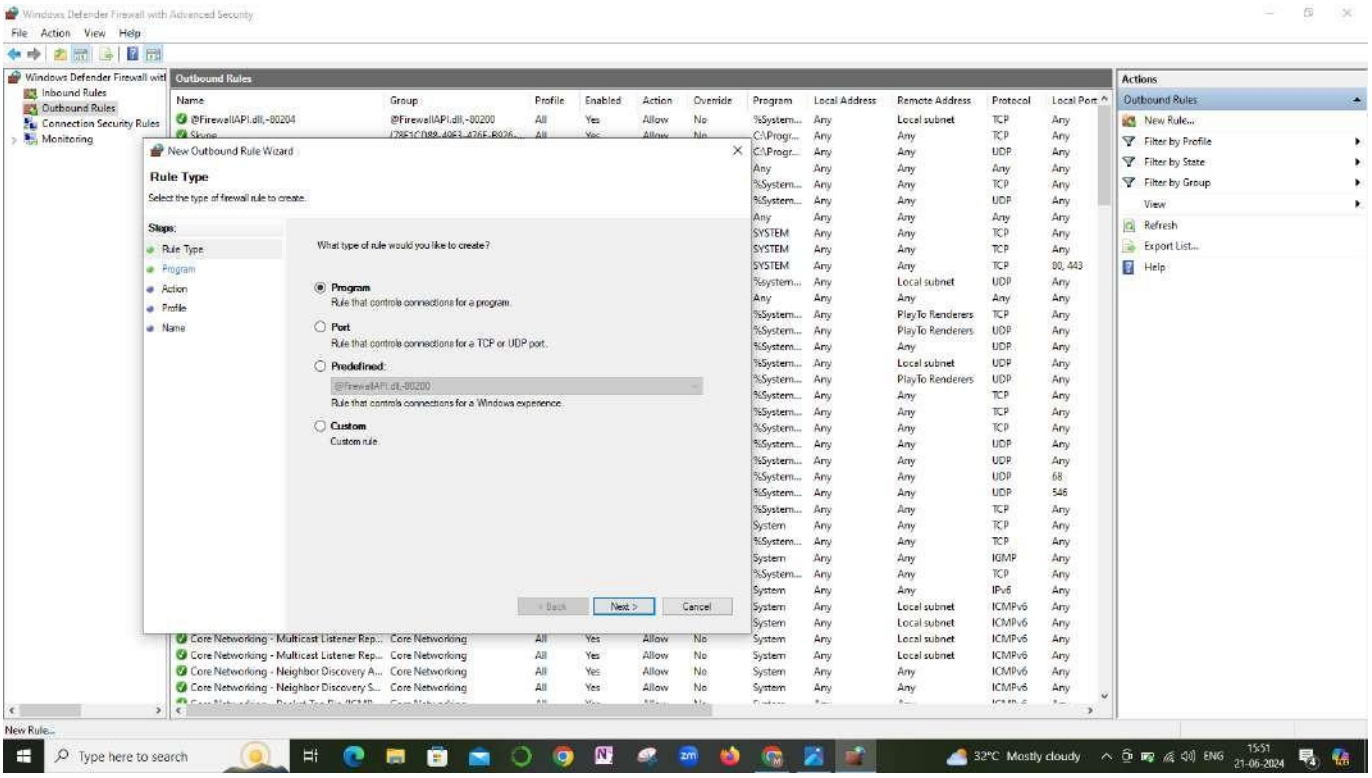
STEP 3 : Now disable the Real-time protection,Automatic sample submission and Cloud-delivered protection options.



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.

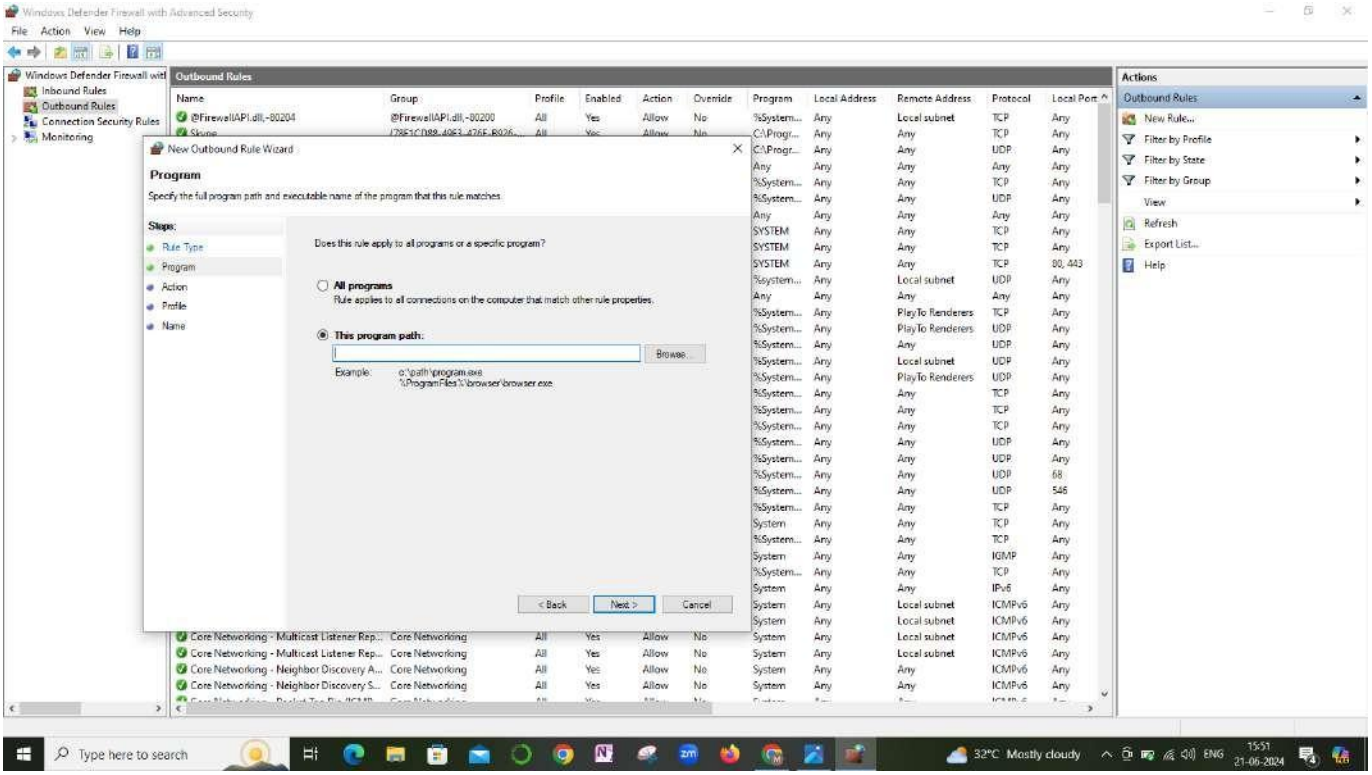


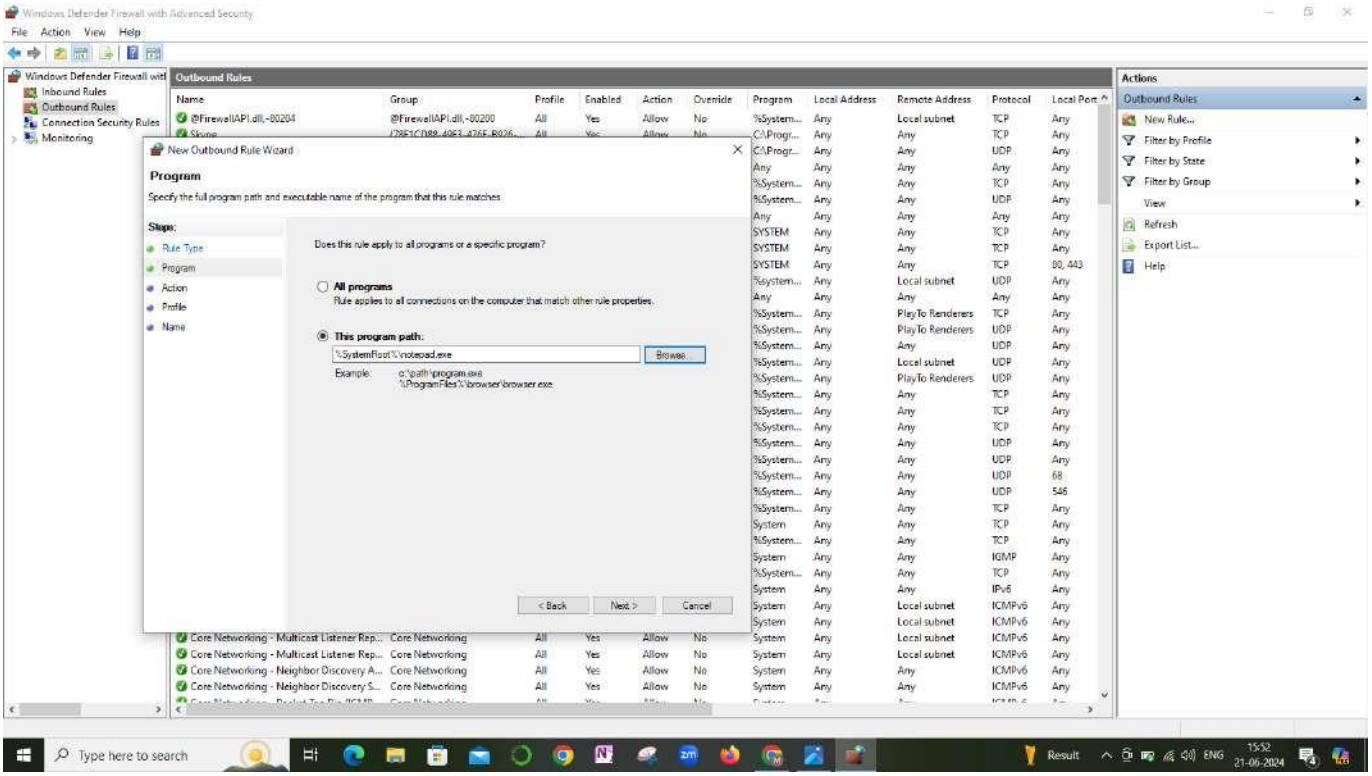
STEP-6:Now you can see a right-side menu bar with outbound rules like new rule,filter by profile,filter by state,etc., Now click on the New Rule option.Then you'll get a pop like below-



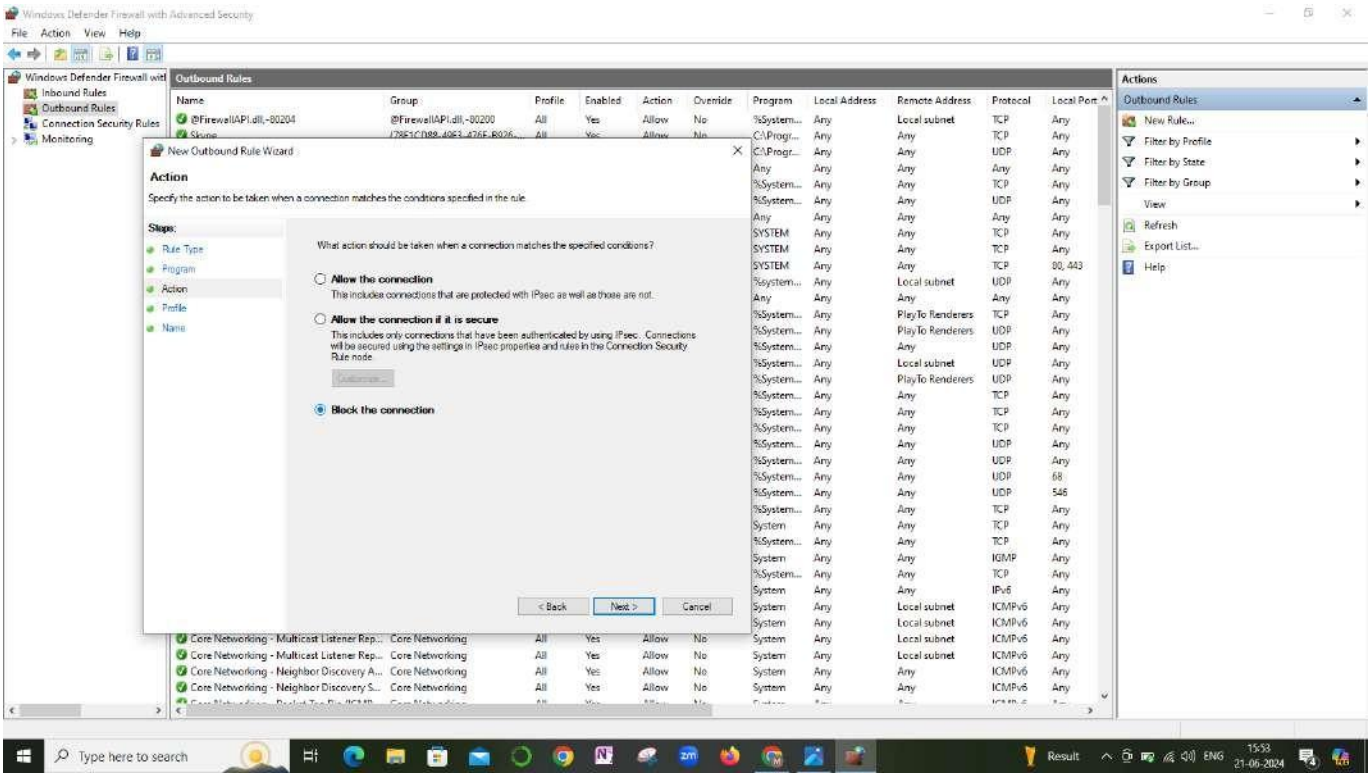
STEP-7: By default we will be in the Rule Type option and it is defaultly selected as program and leave it as it is and click on Next.

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.

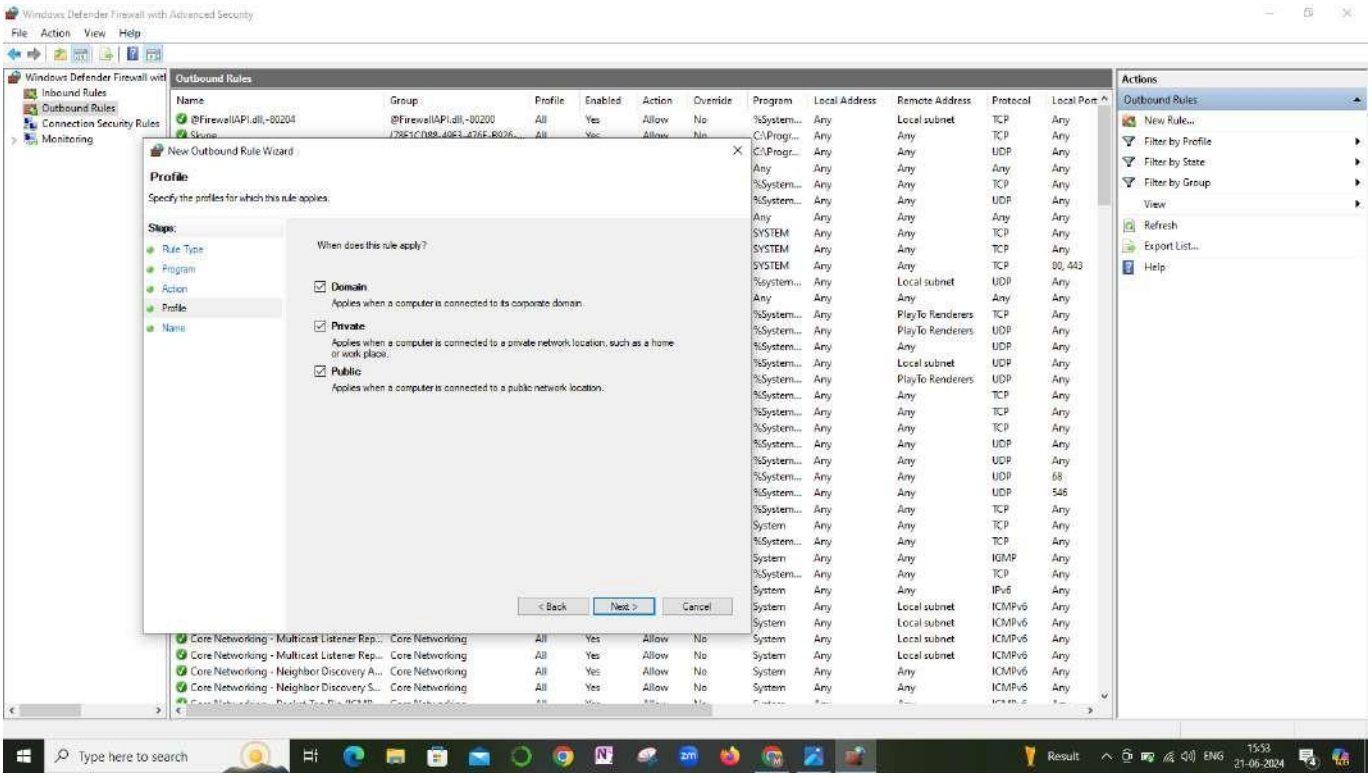




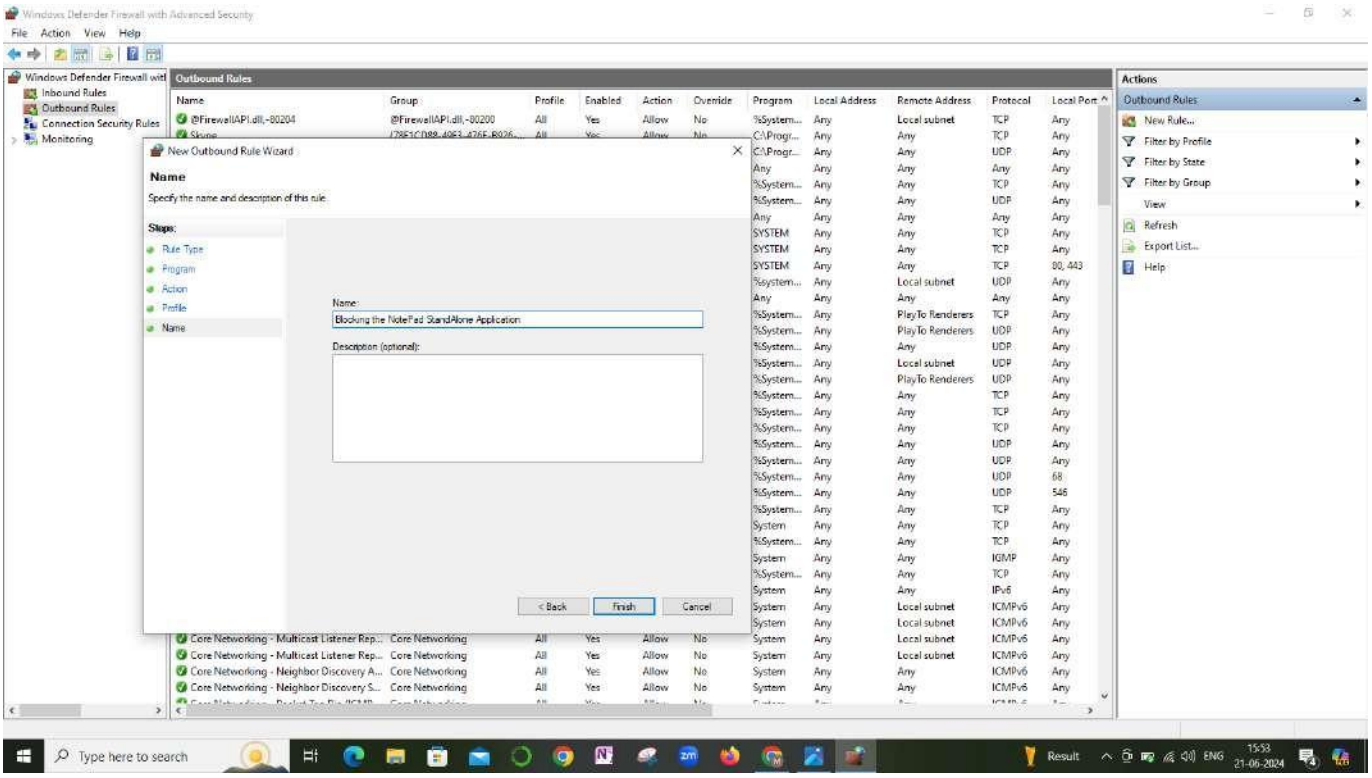
STEP-9: Next in the Actions menu Click on Block the Connection and Click on Next.



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.

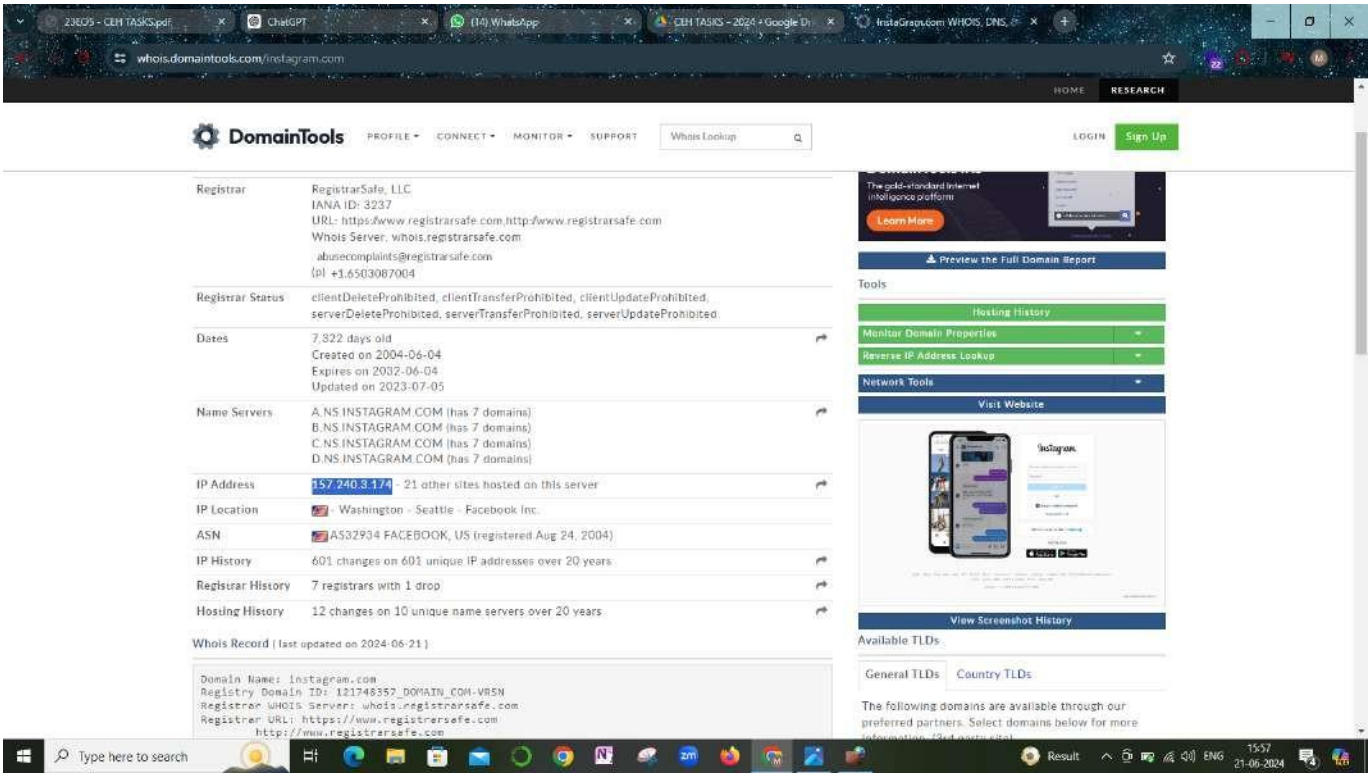


And Now the standalone application i.e, Notepad has been successfully blocked.

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

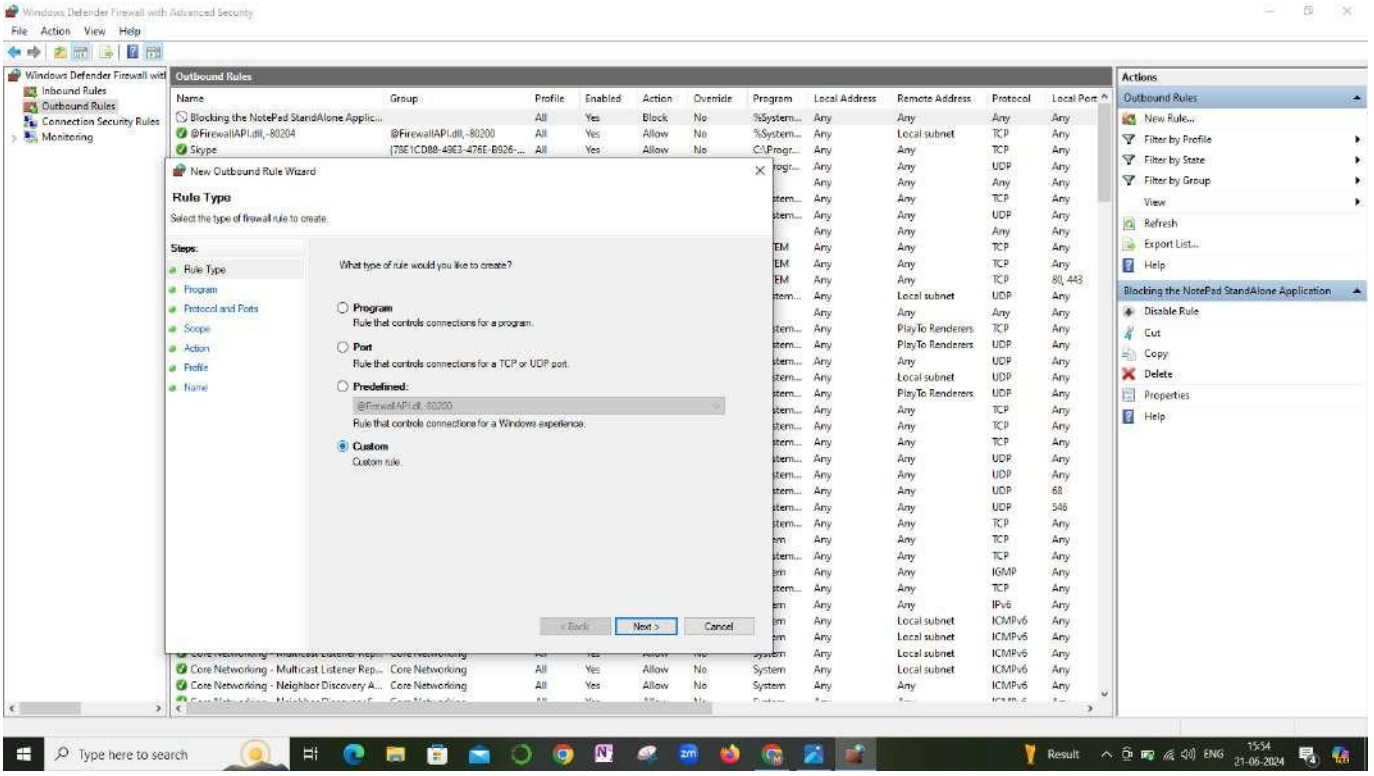
STEP-1: Navigate to Chrome search bar and type www.instagram.com and copy the URL of the webpage.

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

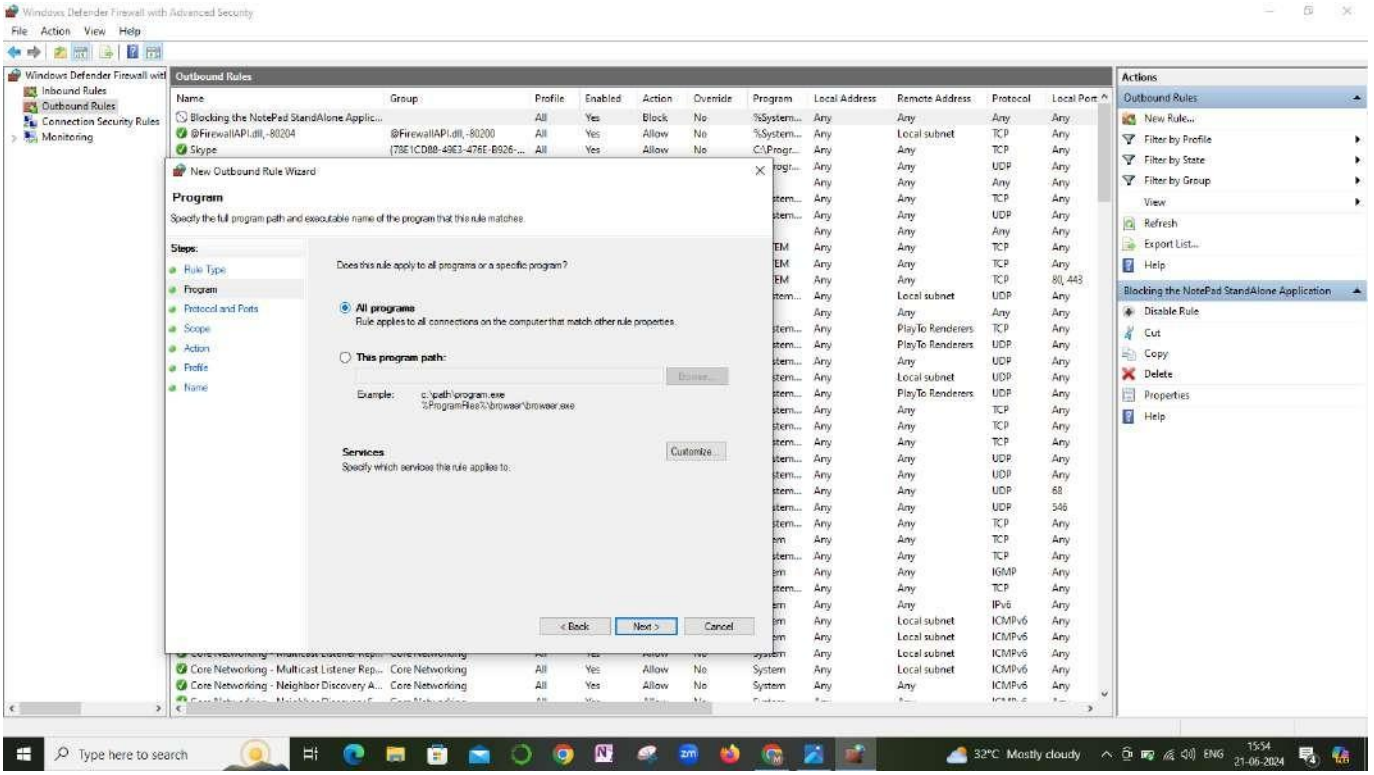


Now, copy the IP-Address of the webpage it gives and Go back to the windows defender settings and navigate to outbound rules and click on the new rule option.

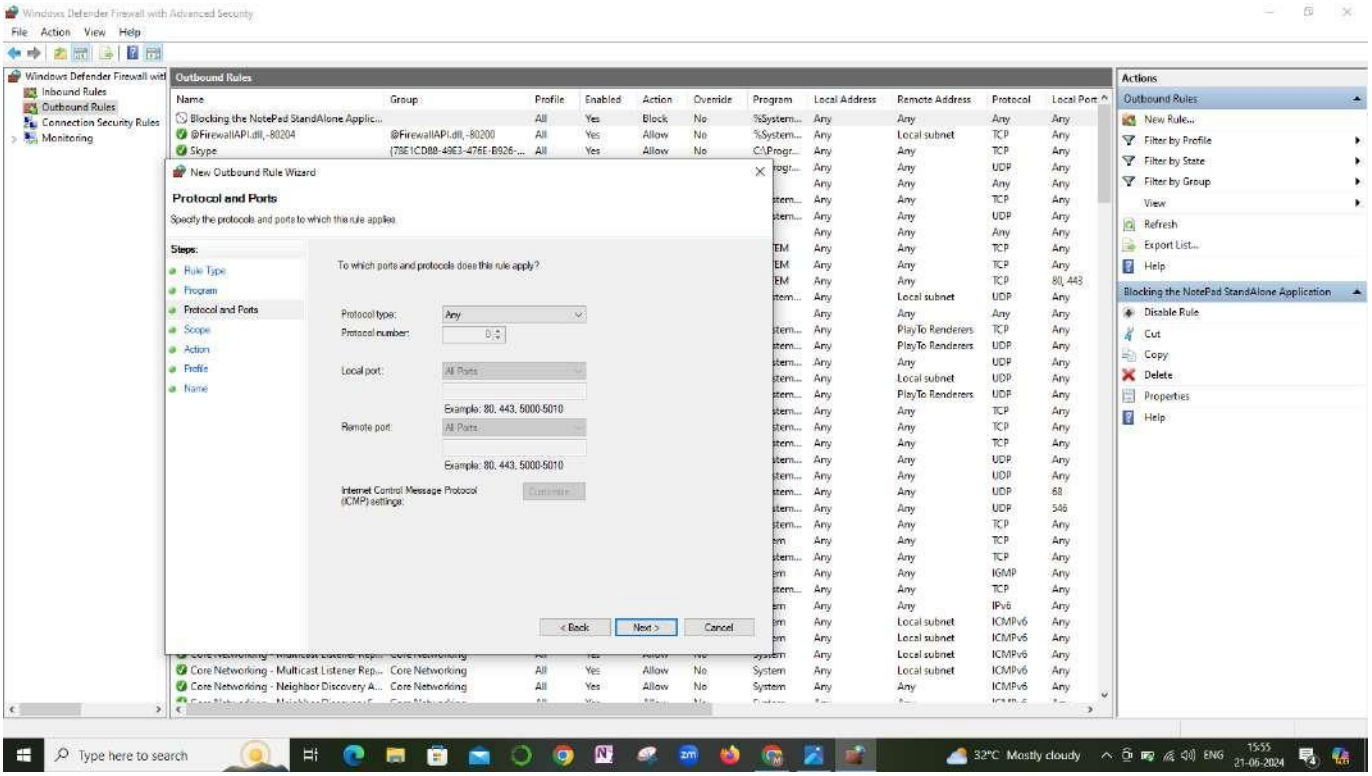
STEP-3: Now, Select the rule type as custom and click on next.



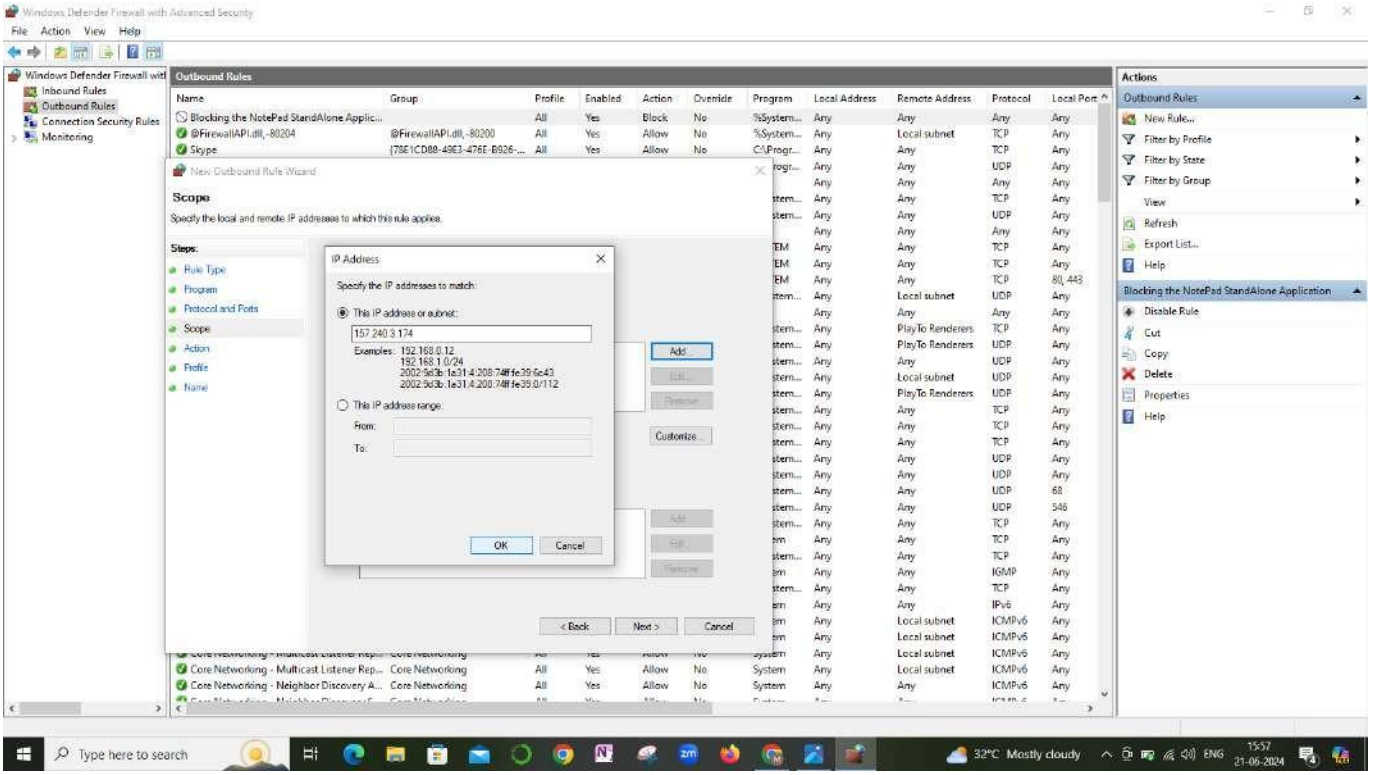
STEP-4:And click on program type as all programs and click on next.

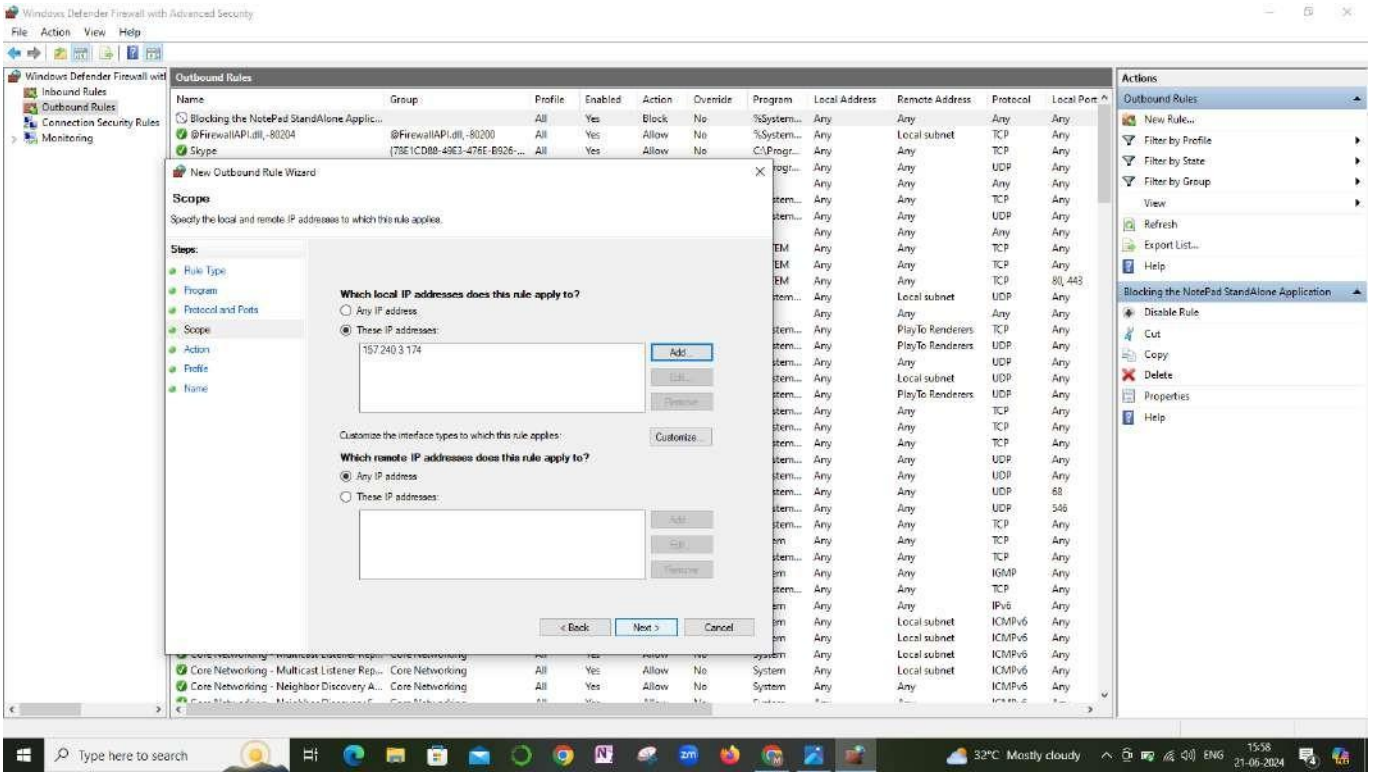


STEP-5: And now leave the protocol type as any by default and click on Next.

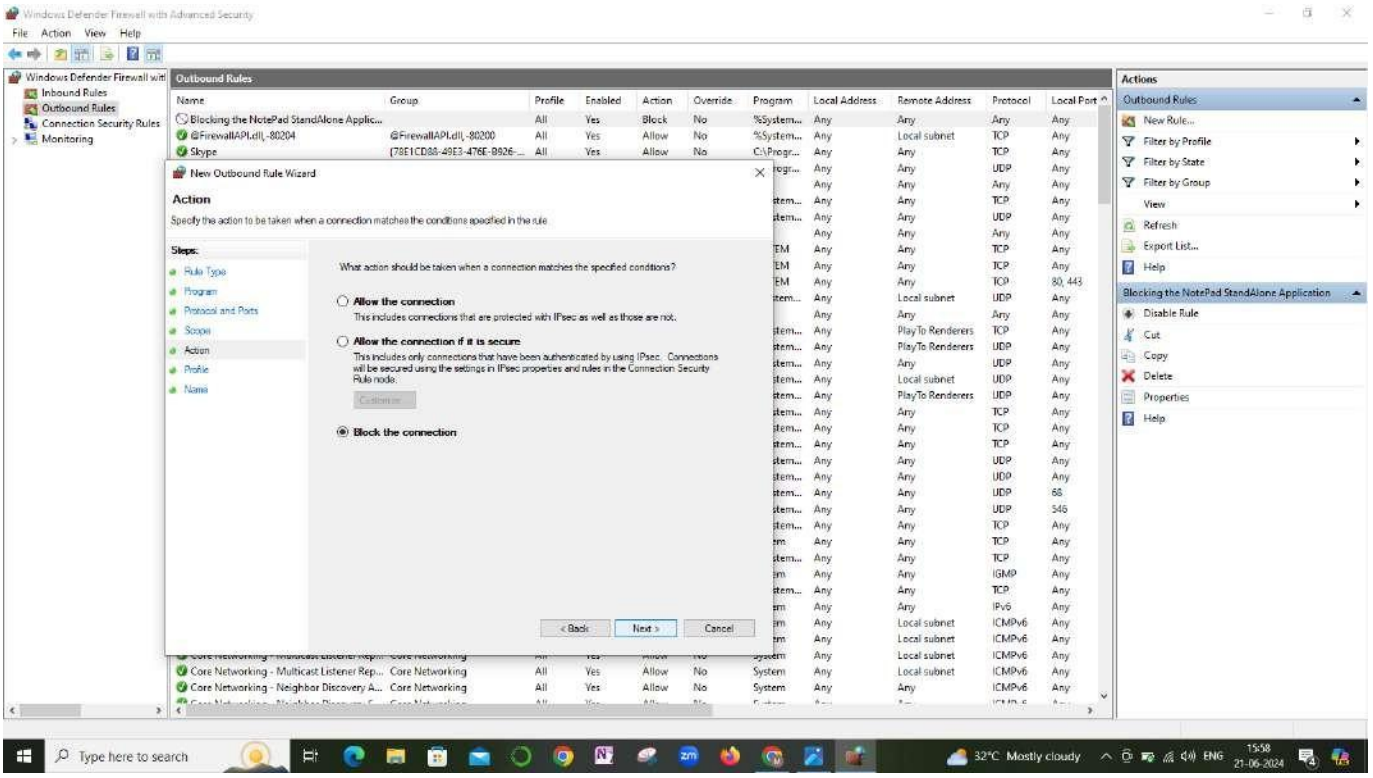


STEP-6: Now, in the scope section select the local ip address it belongs to and add an ip address that is copied from whois lookup tool and paste it in that section as shown below-

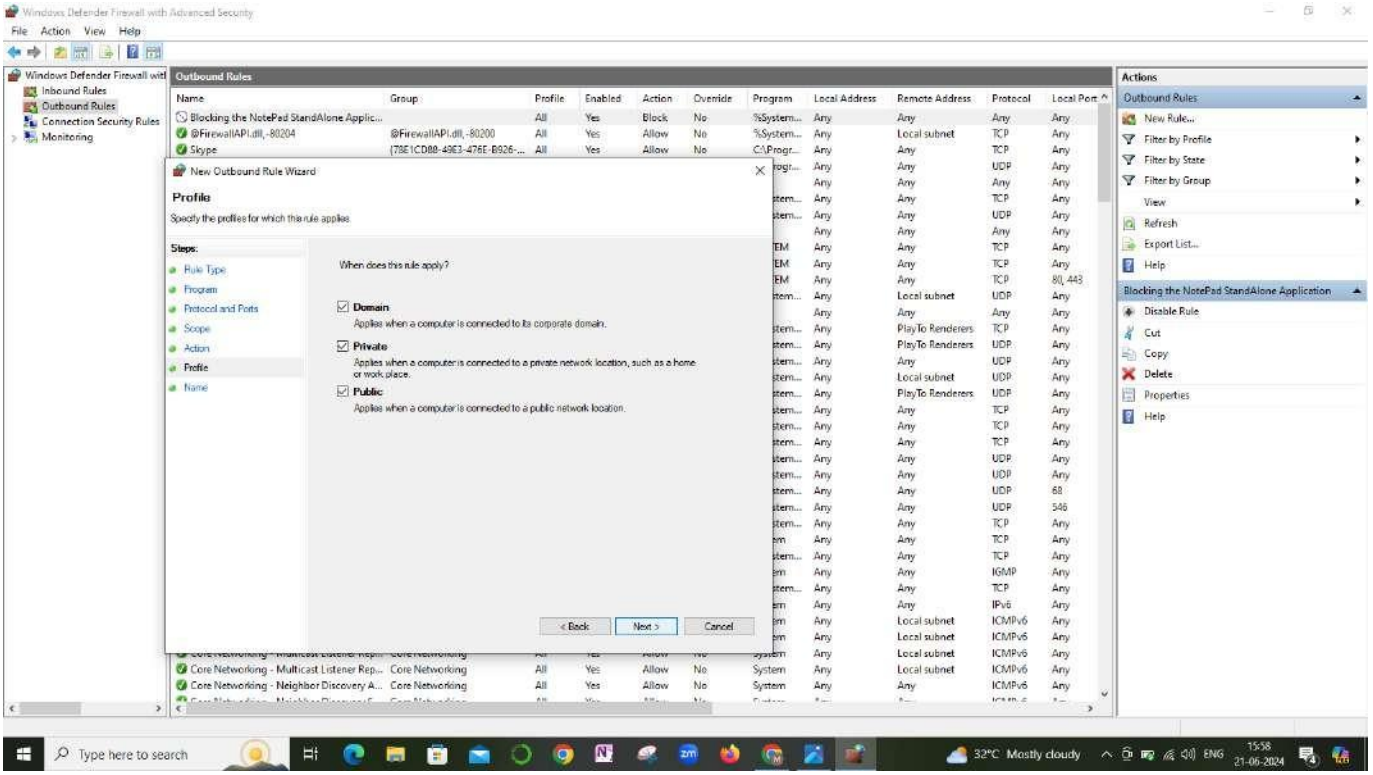


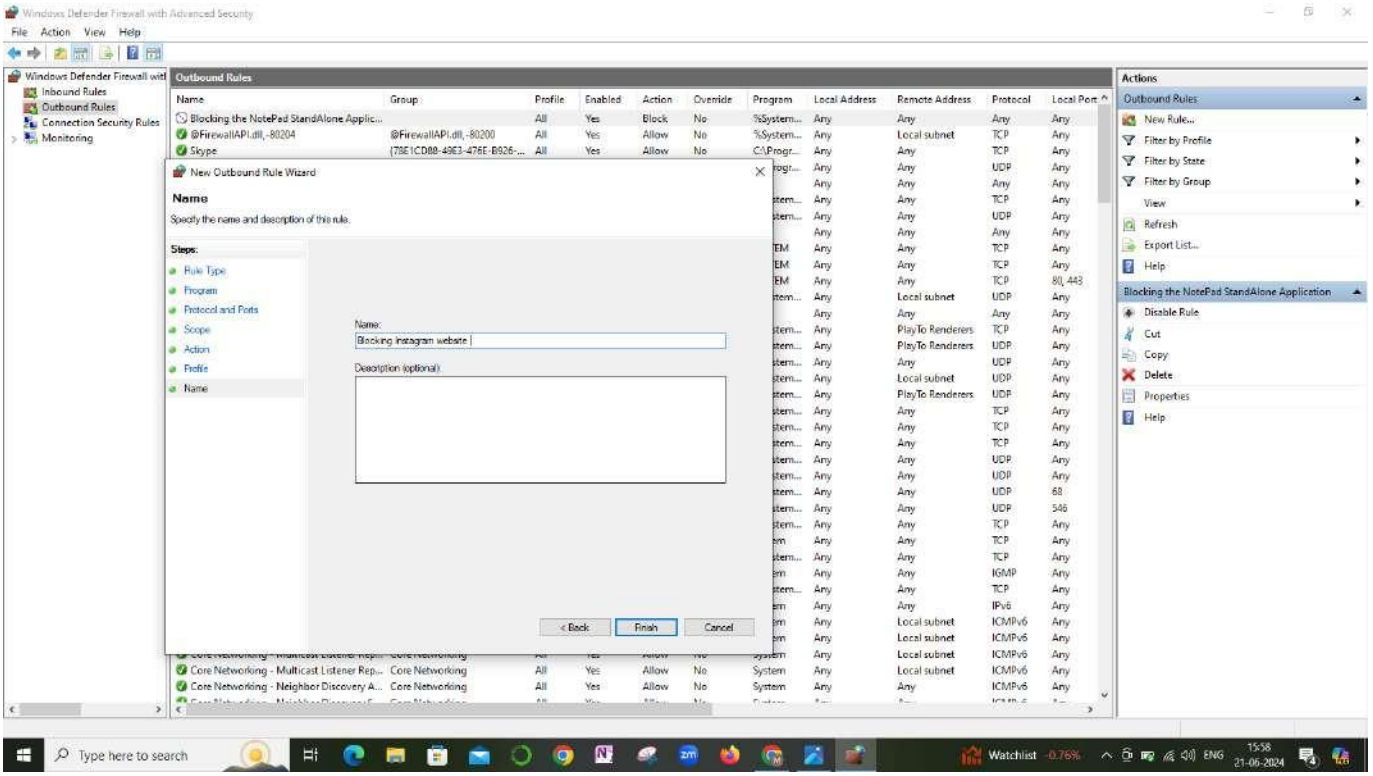


STEP-7: In the Action section select Block the Connection and Click on Next.



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 .

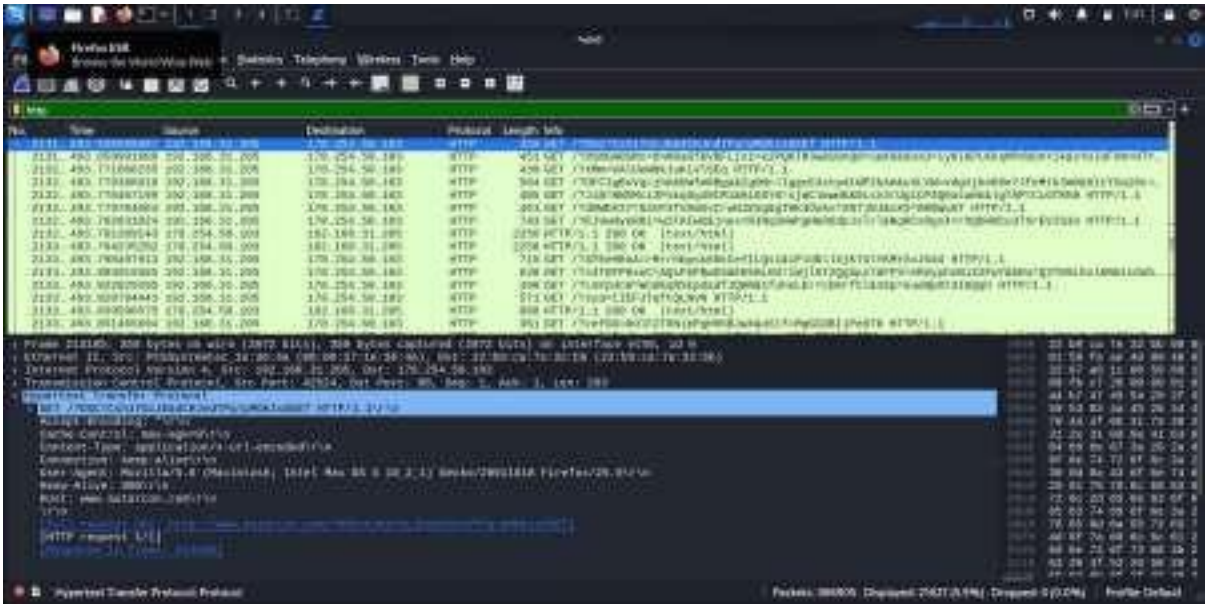
Golden eye: It is free and open source tool

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

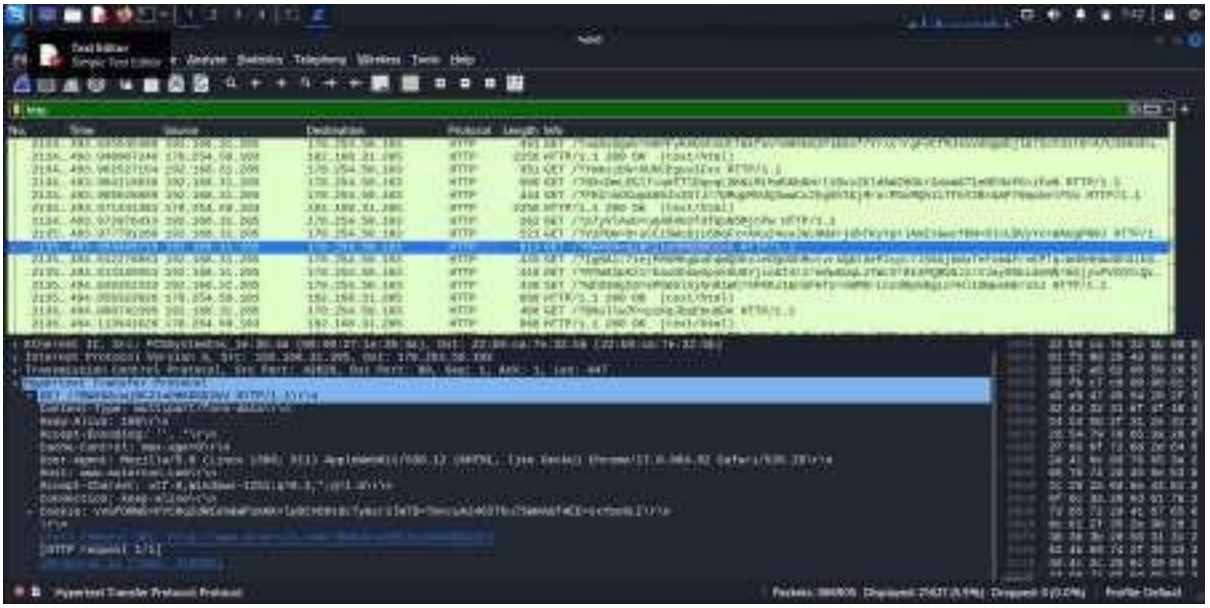
Step 2: Start giving the commands
Step 3:

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

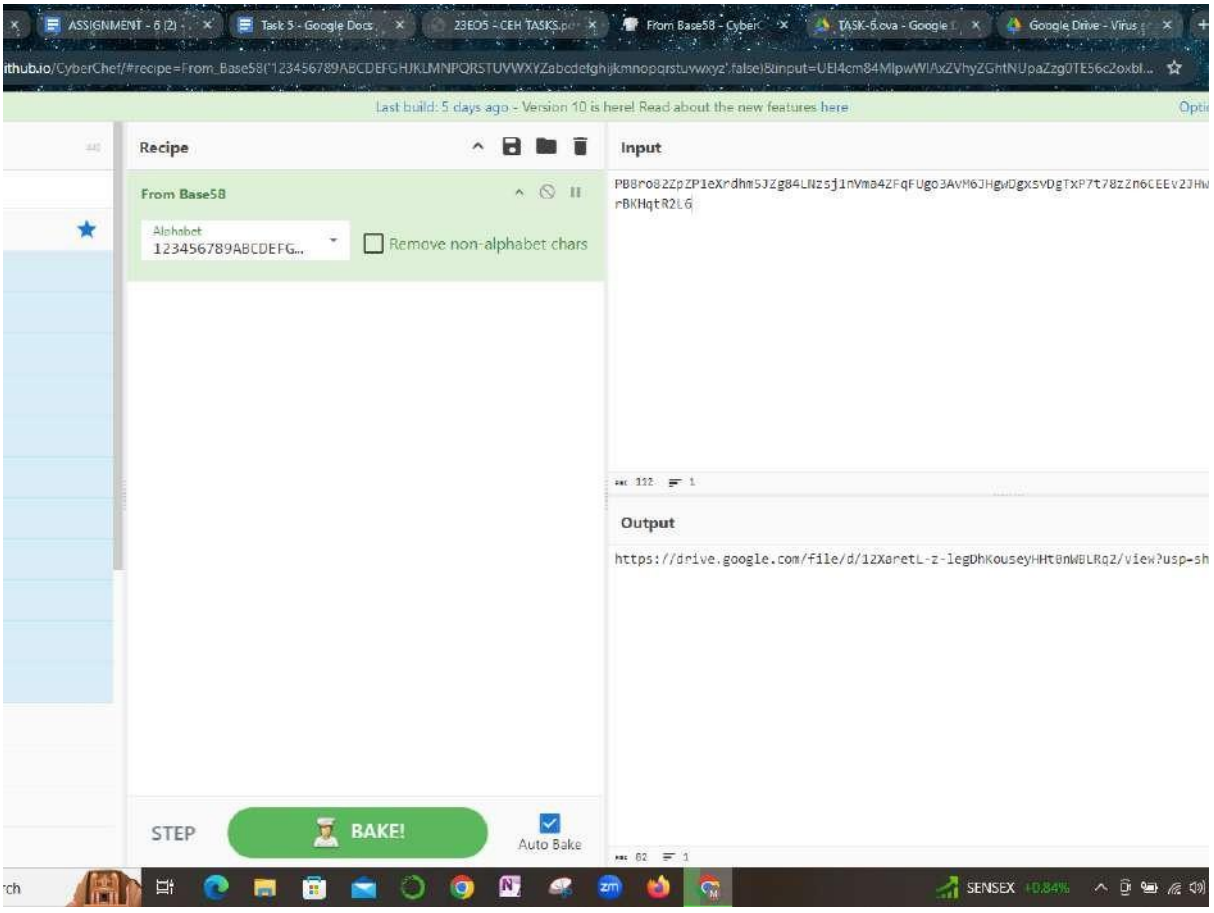
Step 1: First Decrypt the secret data to Get the link

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 .

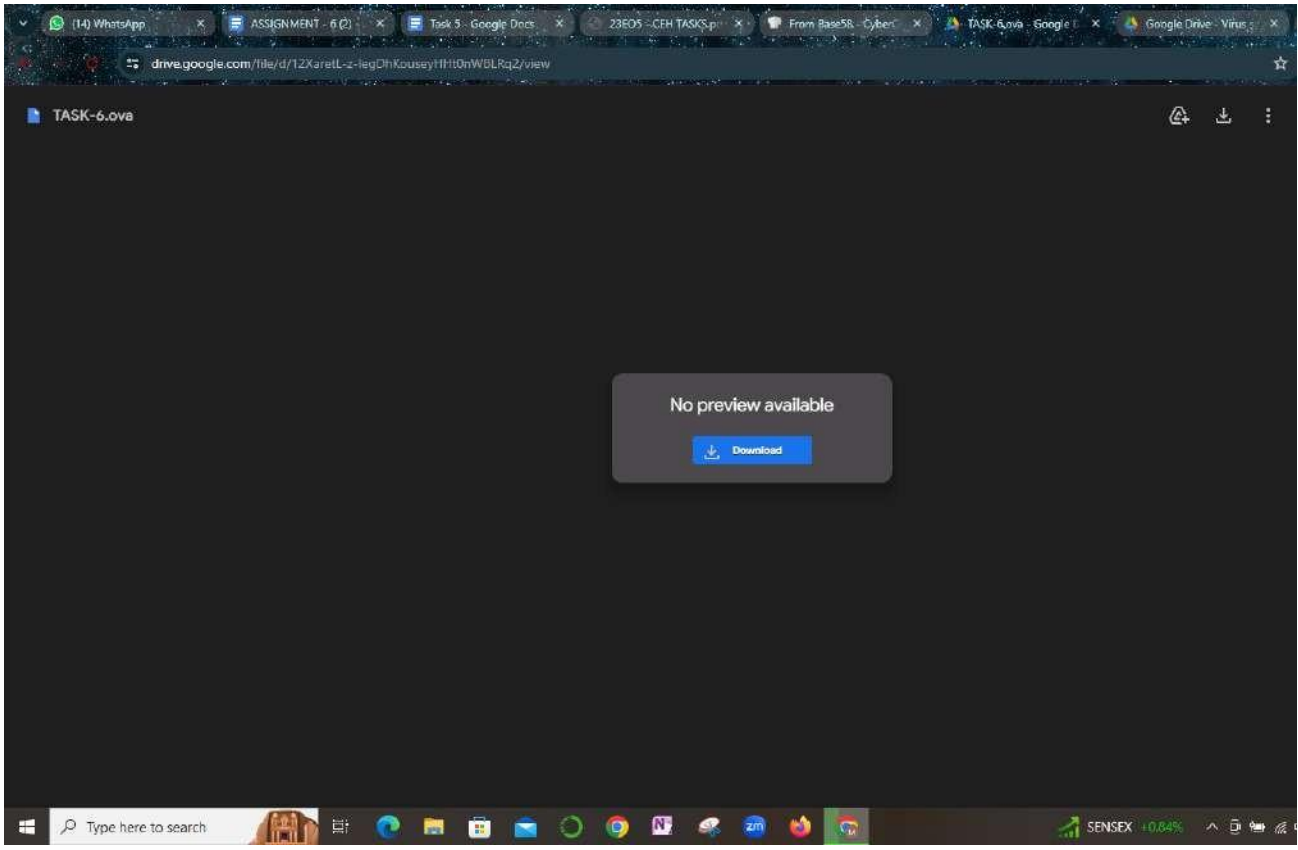
Now decrypting the key

PB8ro82ZpZP1eXrdhm5JZg84LNzsj1nVma4ZFqFUgo3AvM6J HgwDgxsvDgTxP7t78zZn6CEEv2JHwVCMA7PCsxpXFGNQY 2ZbFKQynvrBKHqtR2L6

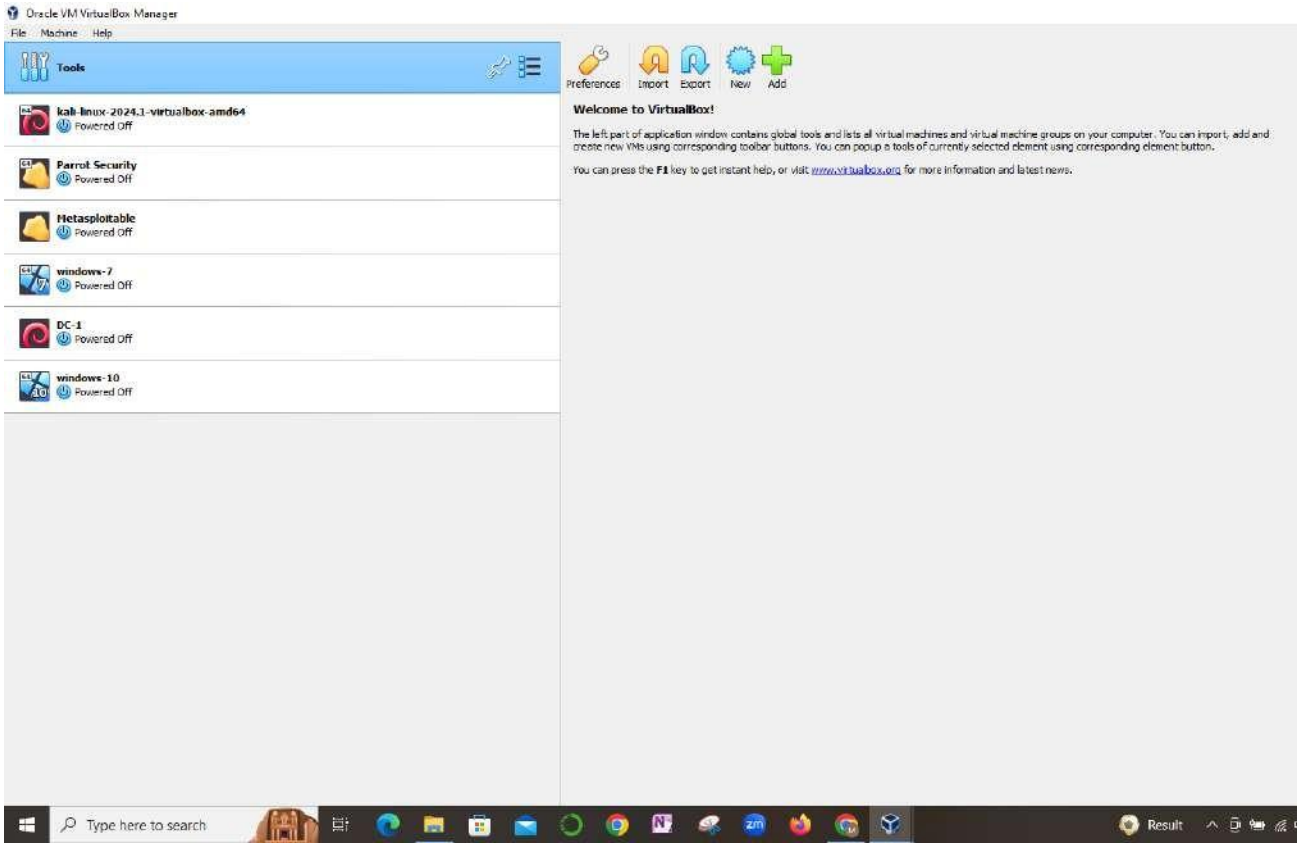


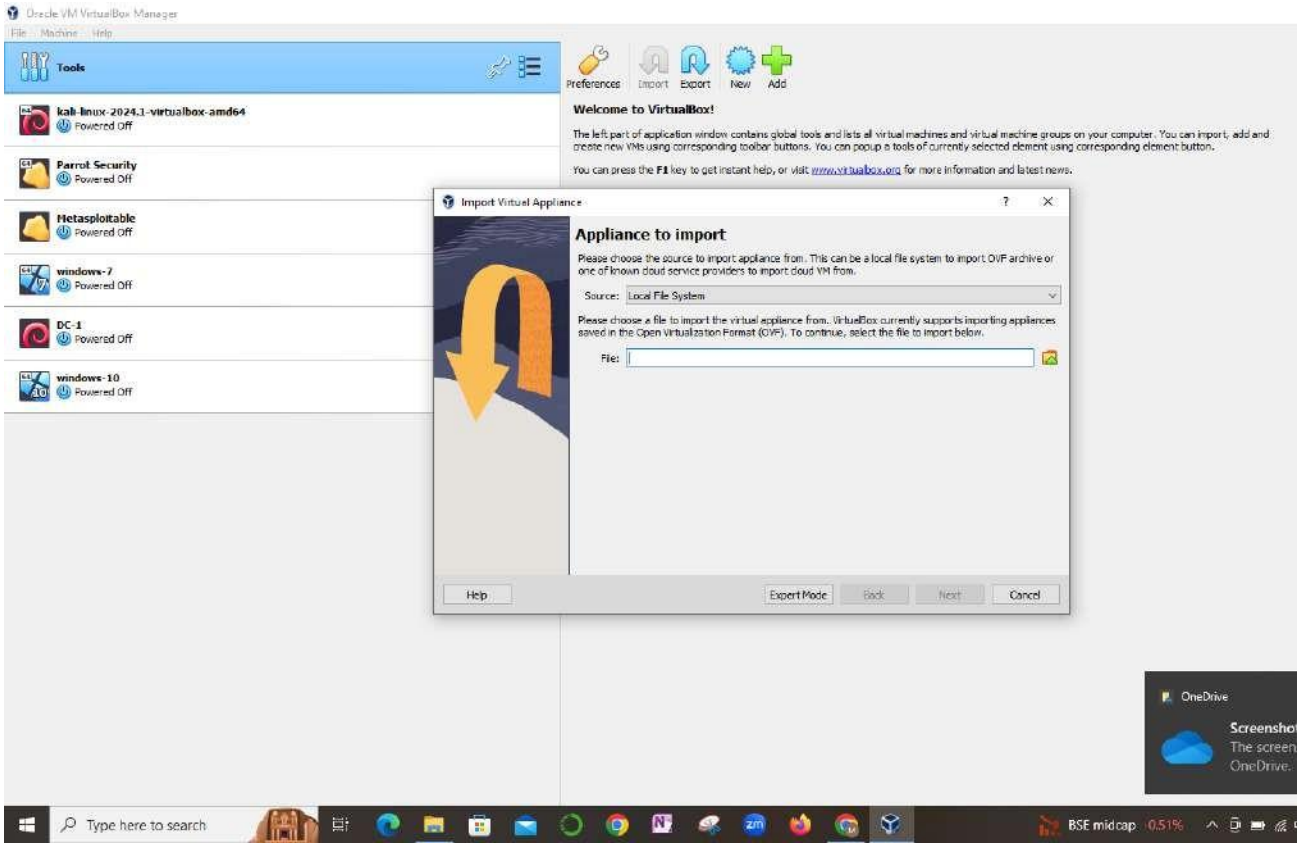
Now from this we need to extract the URL for the decrypted key .

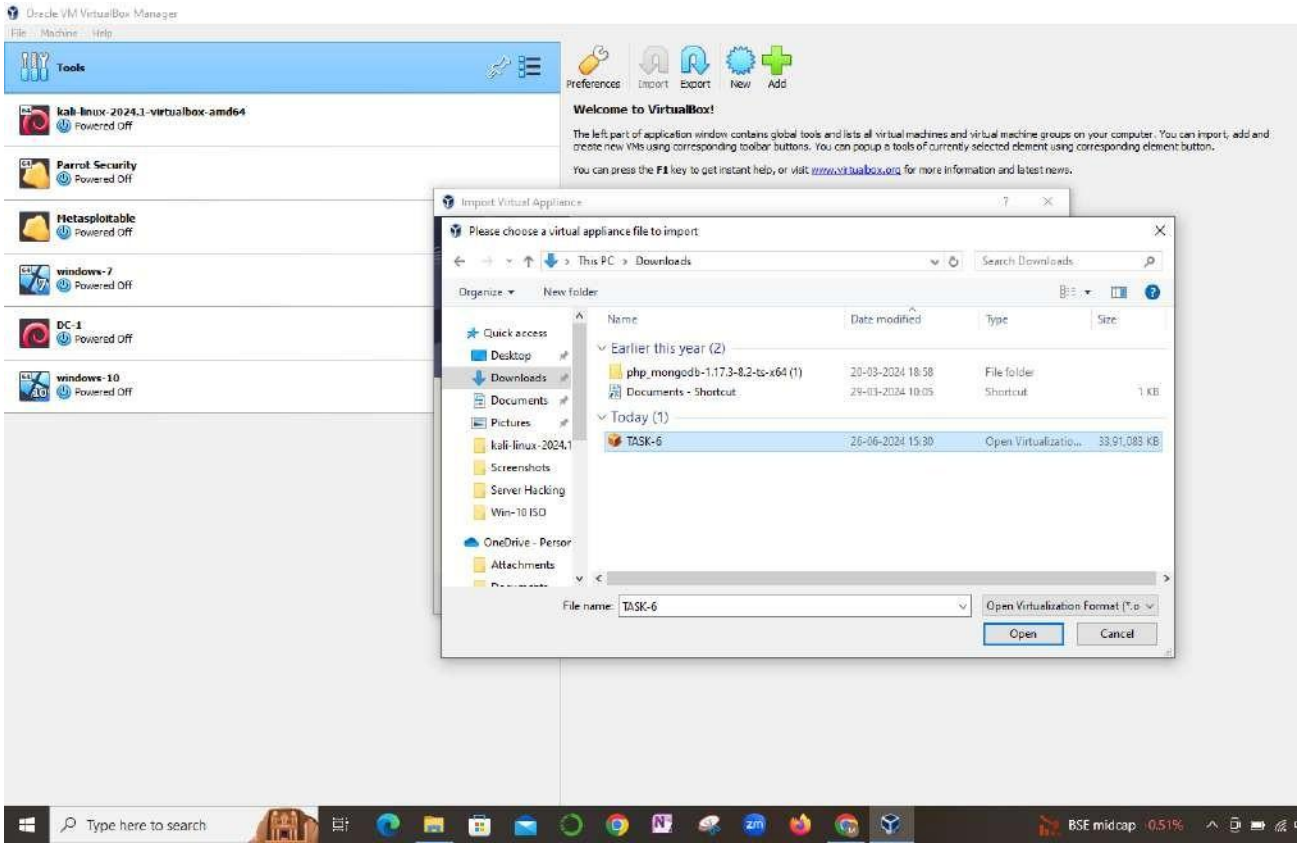
STEP-4: After decrypting download the OVA file from the drive link provided.

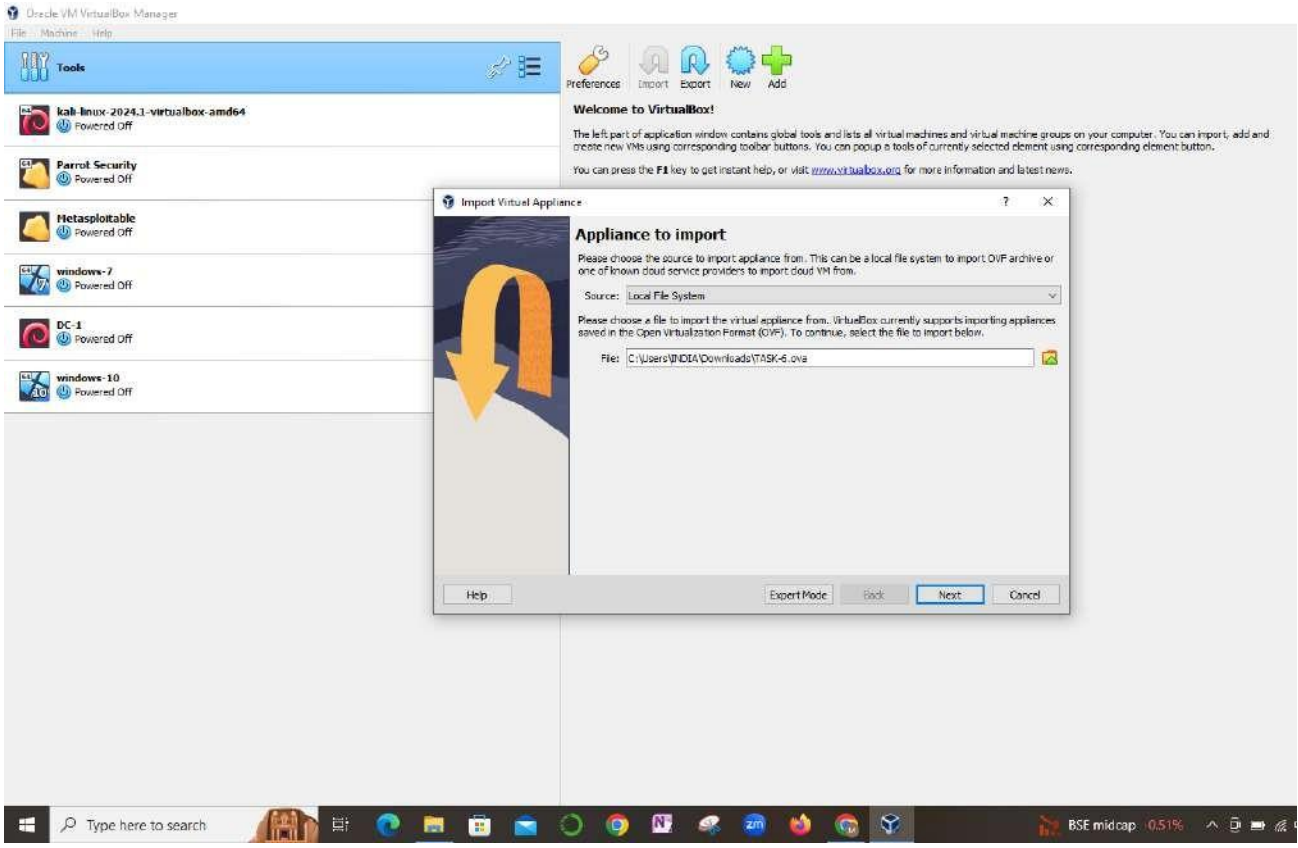


STEP-5: Now , go to kali linux, and navigate to the file option on the left side top options and click on import appliances and select a file under the folder option and click on next and click on finish.

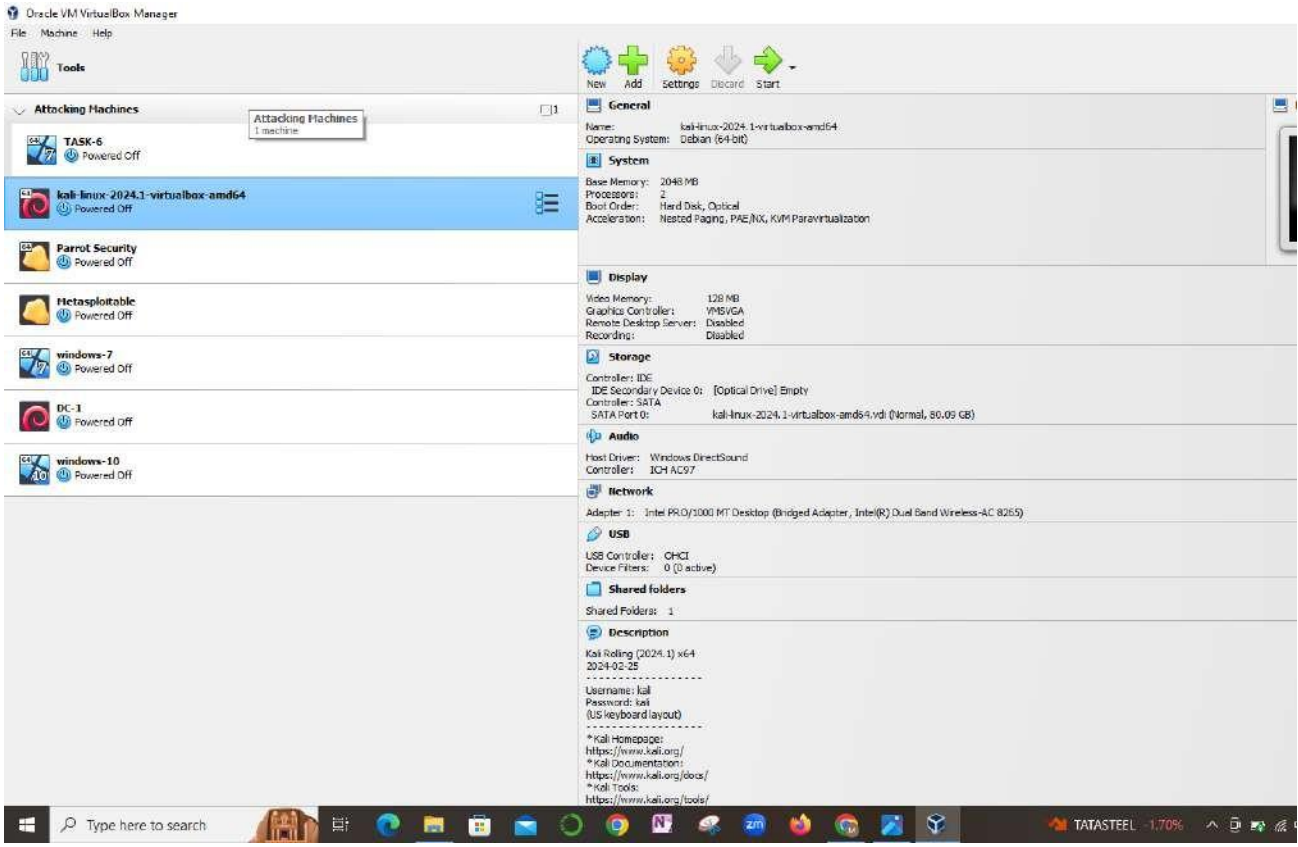



Oracle VM VirtualBox Manager
File Machine Help
Tools
kali-linux-2024.1-virtualbox-amd64
Powered Off
Parrot Security
Powered Off
Metasploitable
Powered Off
windows-7
Powered Off
DC-1
Powered Off
windows-10
Powered Off
Preferences
Import
Export
New
Add
Welcome to VirtualBox!
The left part of application 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%

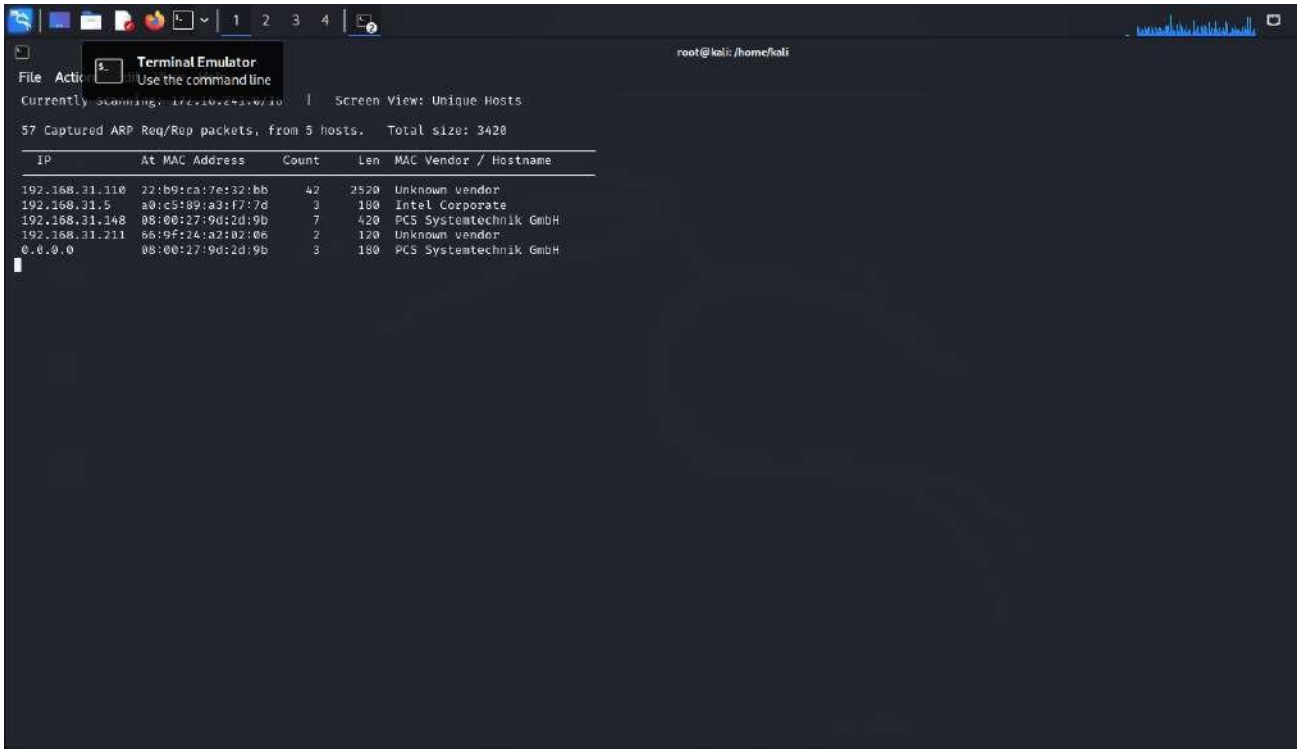

Oracle VM VirtualBox Manager
File Machine Help
Tools
kali-linux-2024.1-virtualbox-amd64
Powered Off
Parrot Security
Powered Off
Metasploitable
Powered Off
windows-7
Powered Off
DC-1
Powered Off
windows-10
Powered Off
Preferences
Import
Export
New
Add
Welcome to VirtualBox!
The left part of application 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

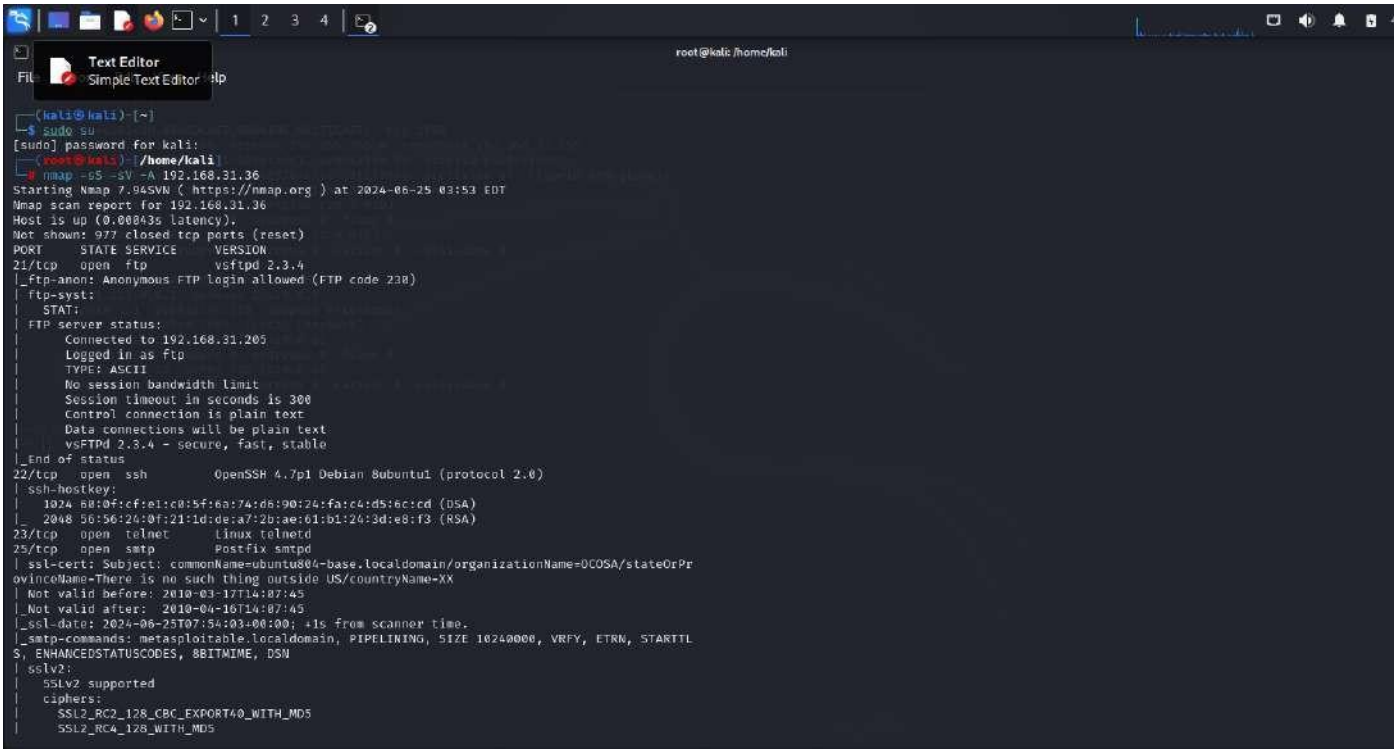
Check the machine, if it consists of any files. .

Steps followed :

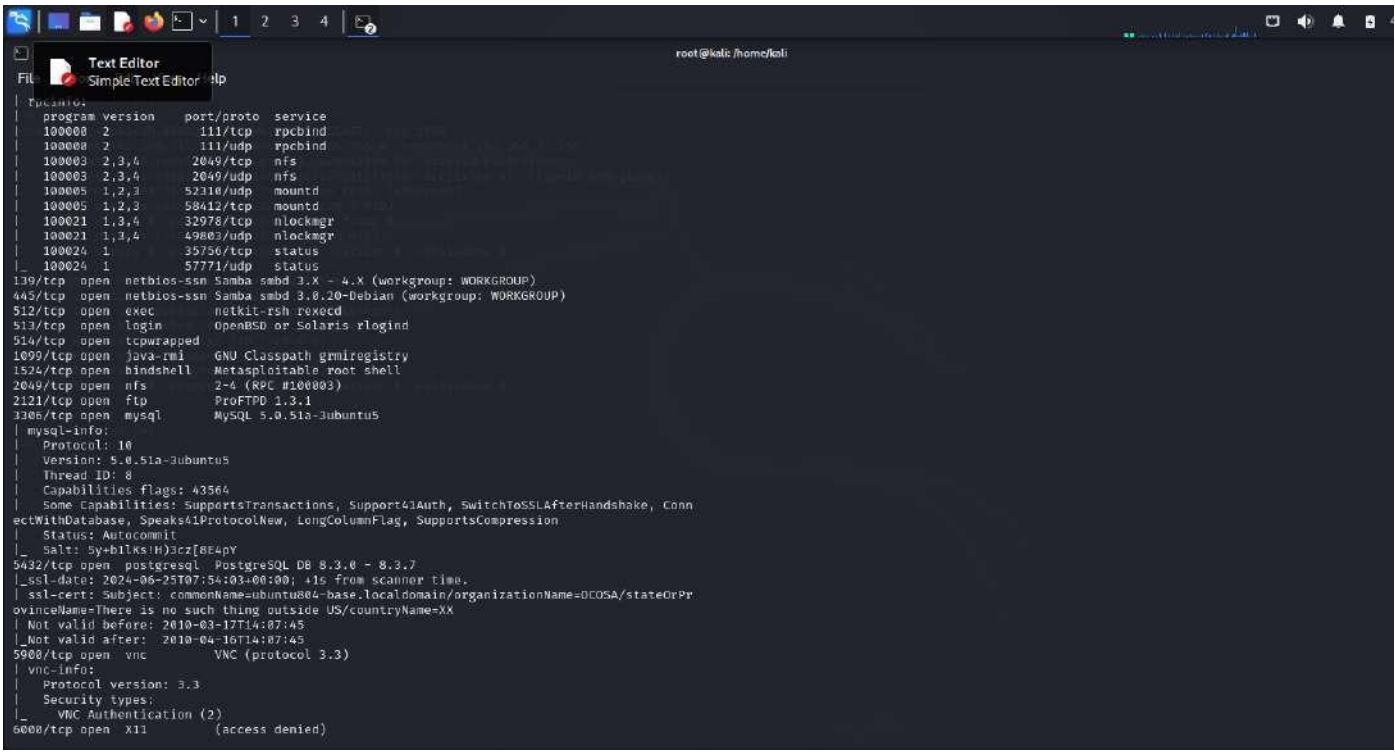
Step 1:Open the VirtualBox Machine and start both Kali Linux and Metasploitable machines.

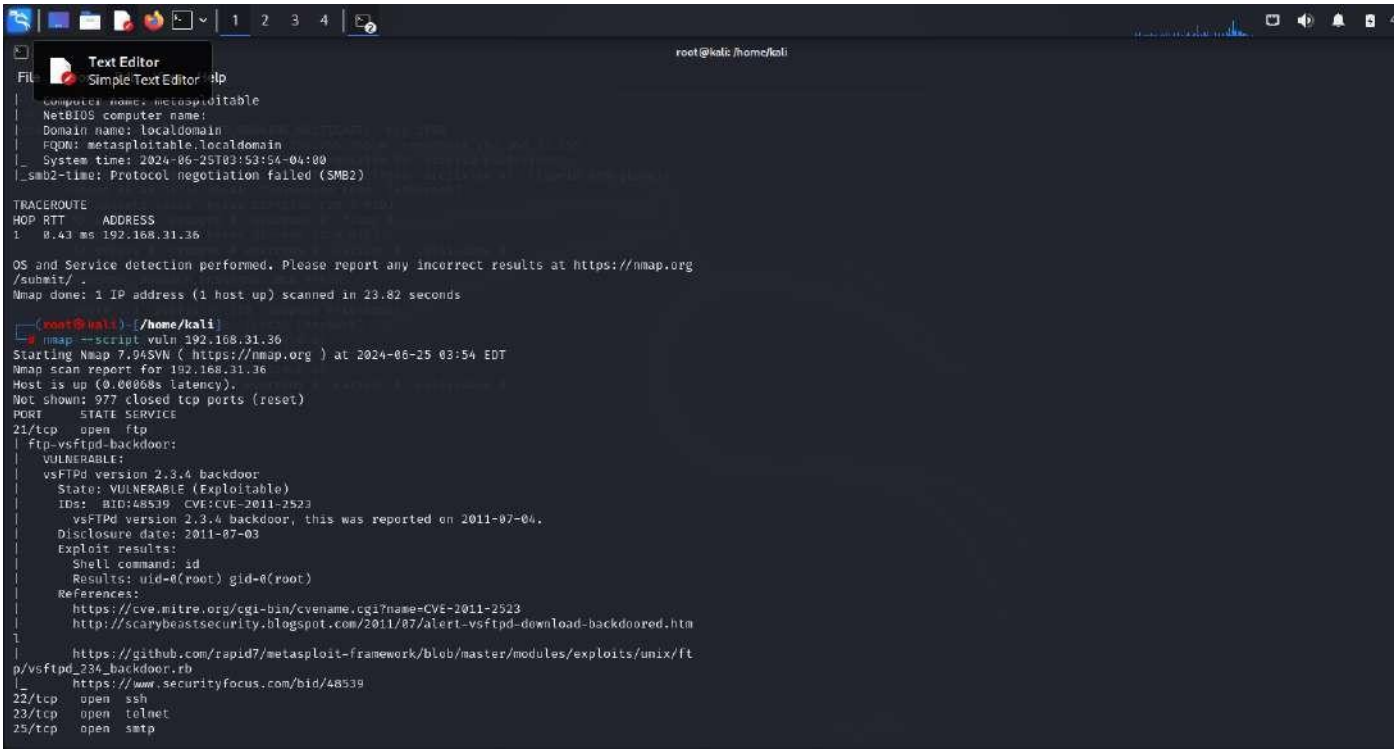
Step 2: Login into the Kali Linux system and to Metasploitable. And then find the Ip address of the Metasploitable machine(because we are going to perform scanning on the Metasploitable machine.)

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

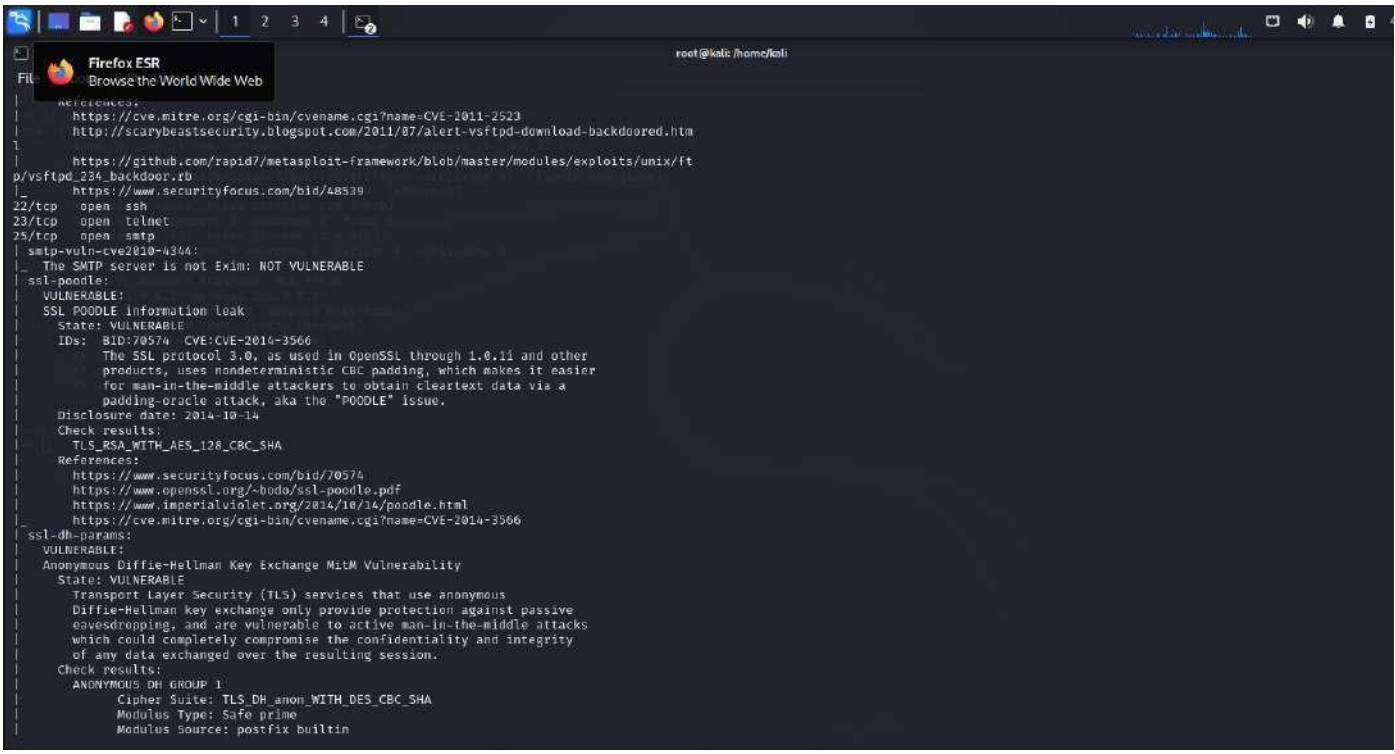


STEP-4:Write the command “nmap -sS -sV -A metasploit-ip address”.Such that it gives the output of all the ports its versions and complete detail.

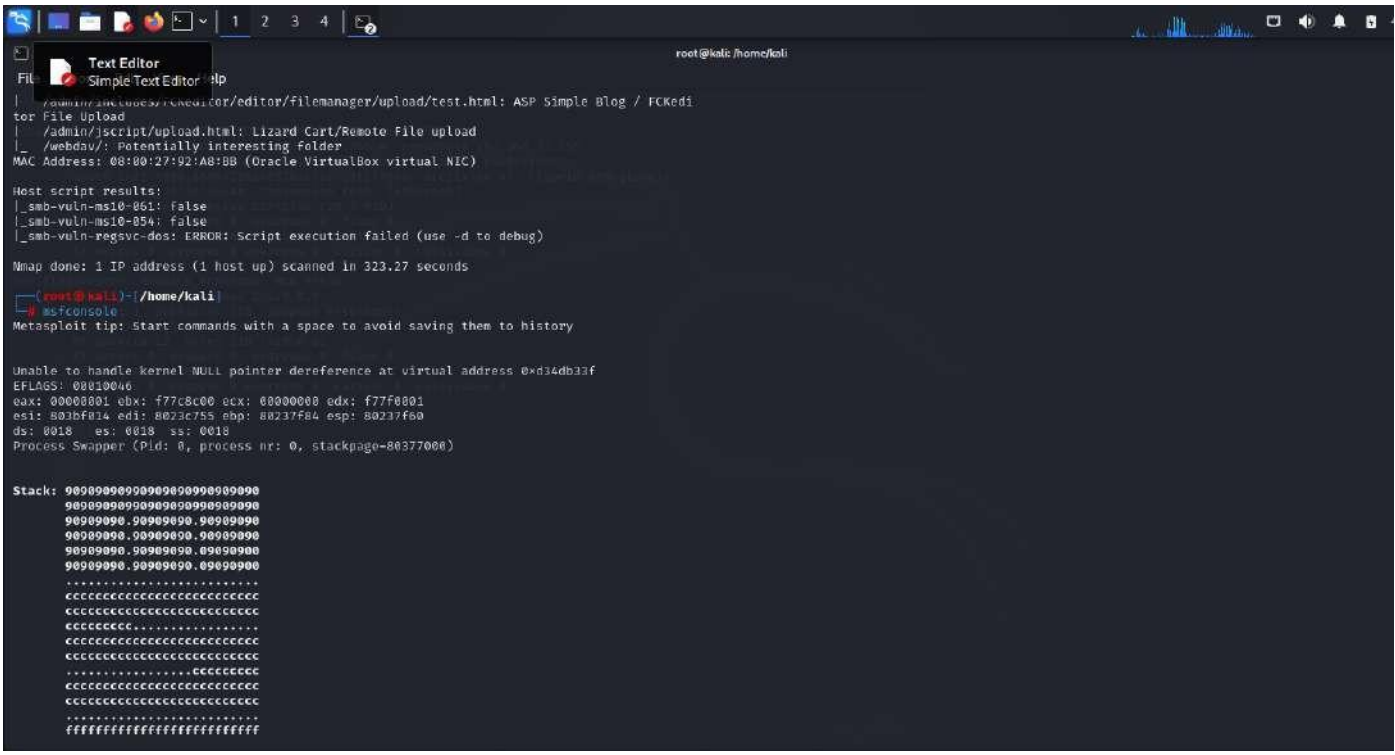




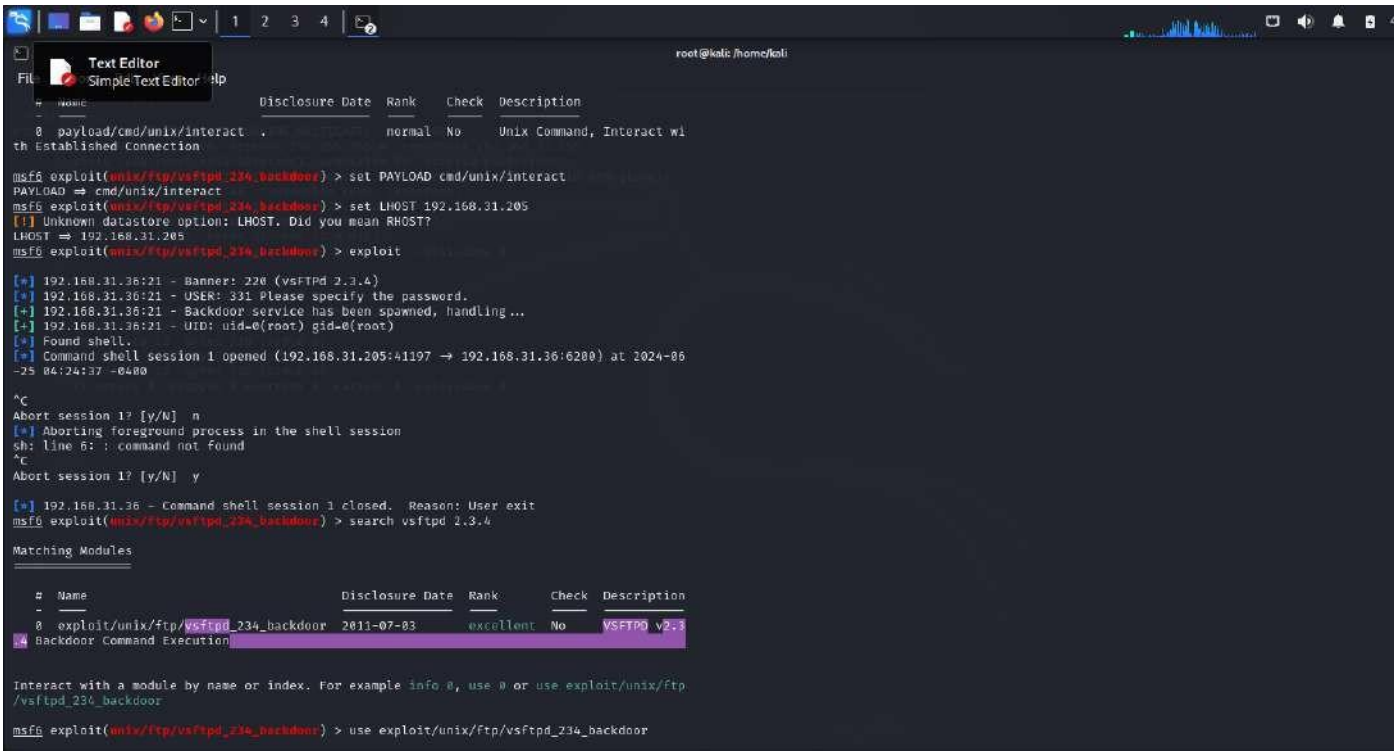
STEP-5:And then give the command “nmap –script vuln “metasploit-ip address” to get the vulnerabilities in that machine.



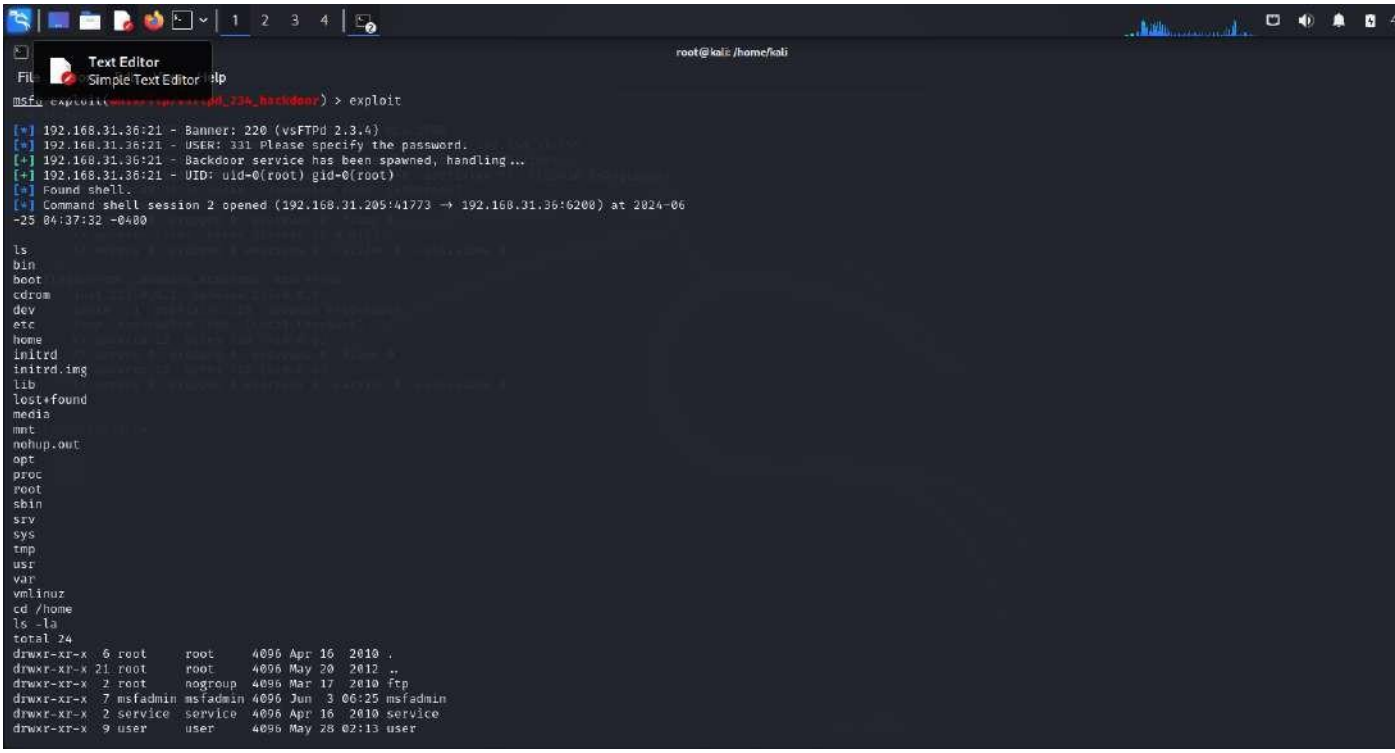
STEP-6:Now start Metasploit framework giving the command “msfconsole”



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

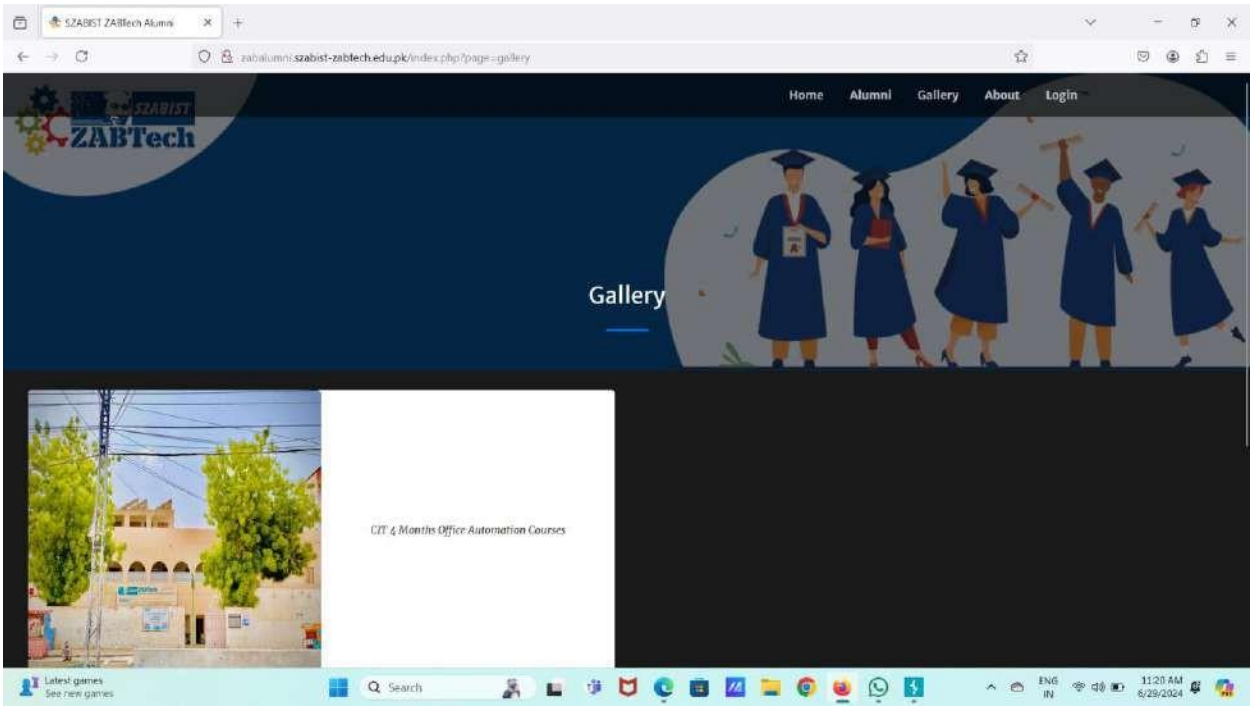
Identifying the hidden data in the files

Now we are able to observe the files in the website

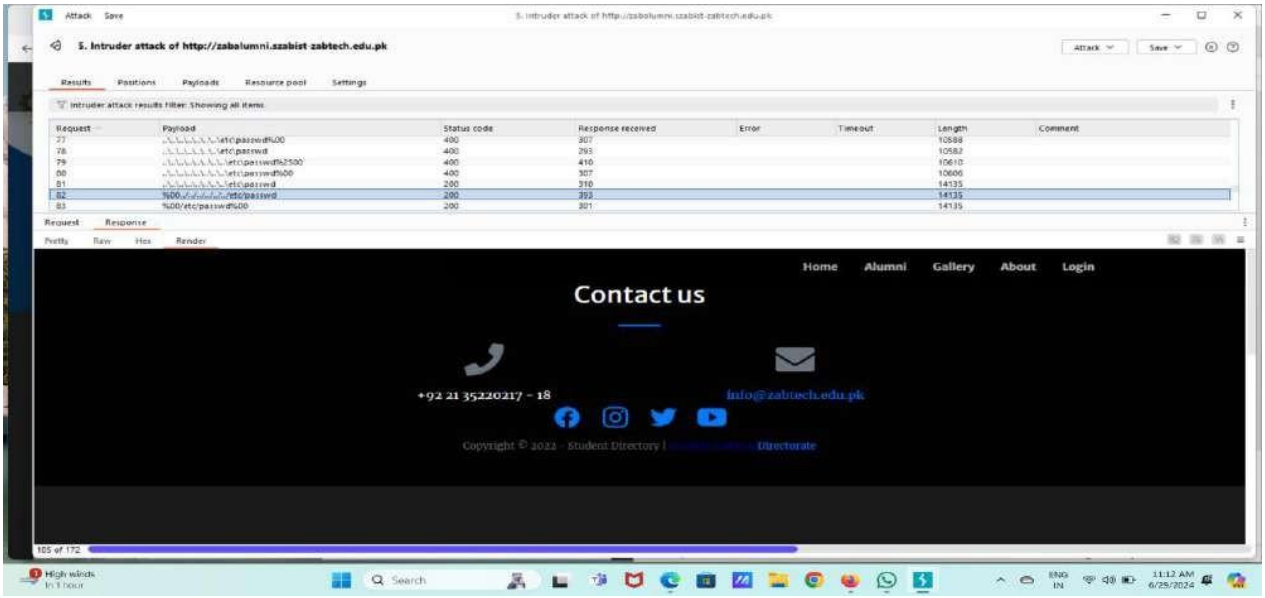
Assignment 7

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

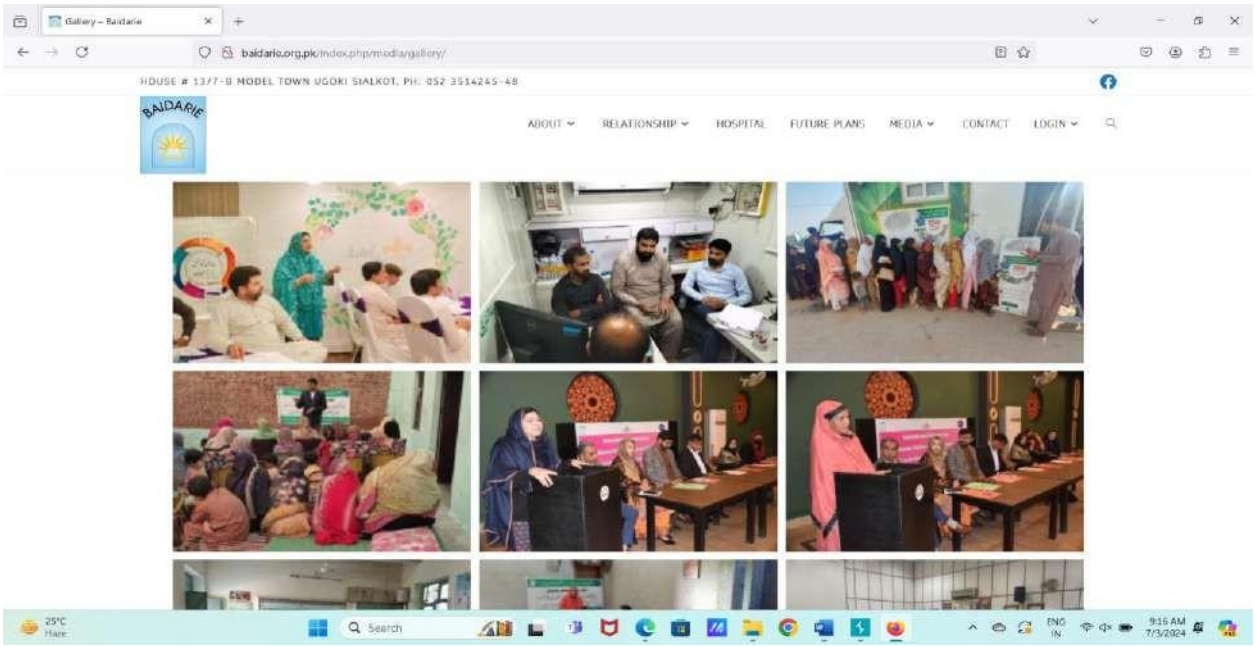
FIRST WEBSITE:



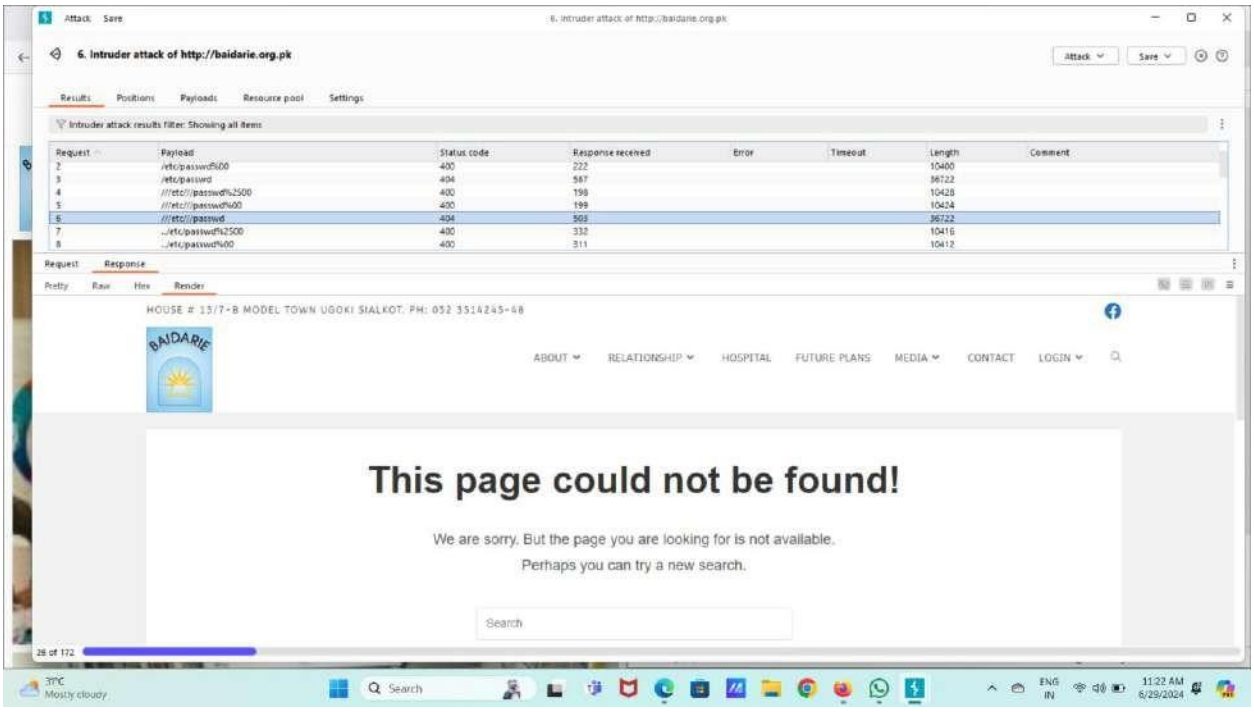
AFTER INCULDE THE LFI TO WEBSITE:



SECOND WEBSITE:

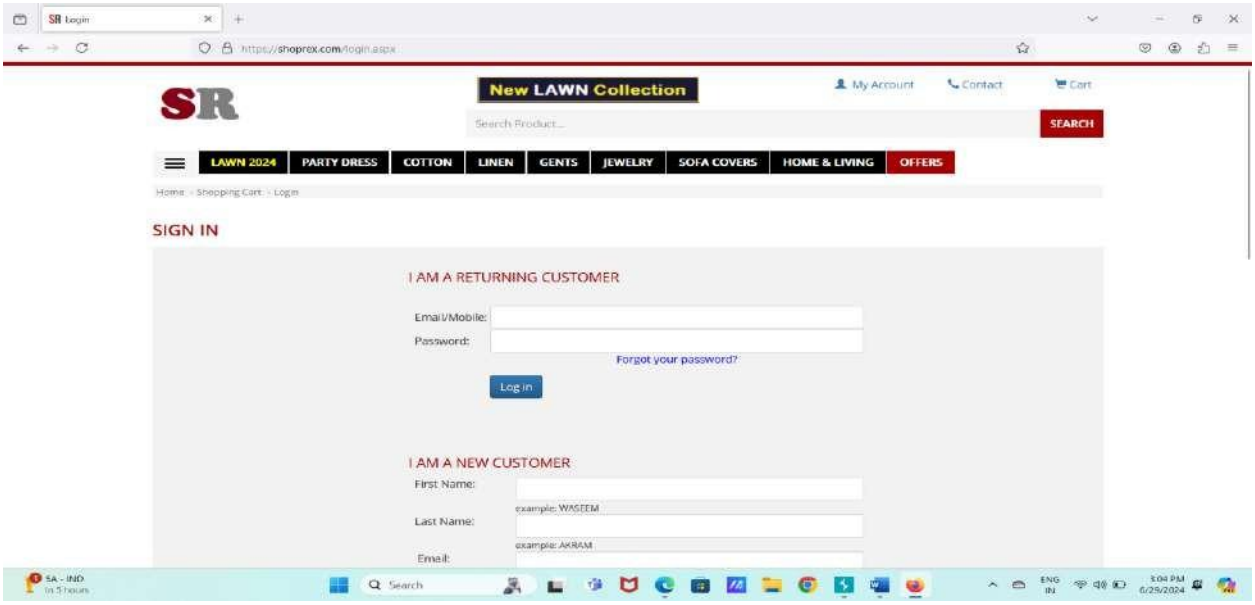


AFTER APPLYING LFI :

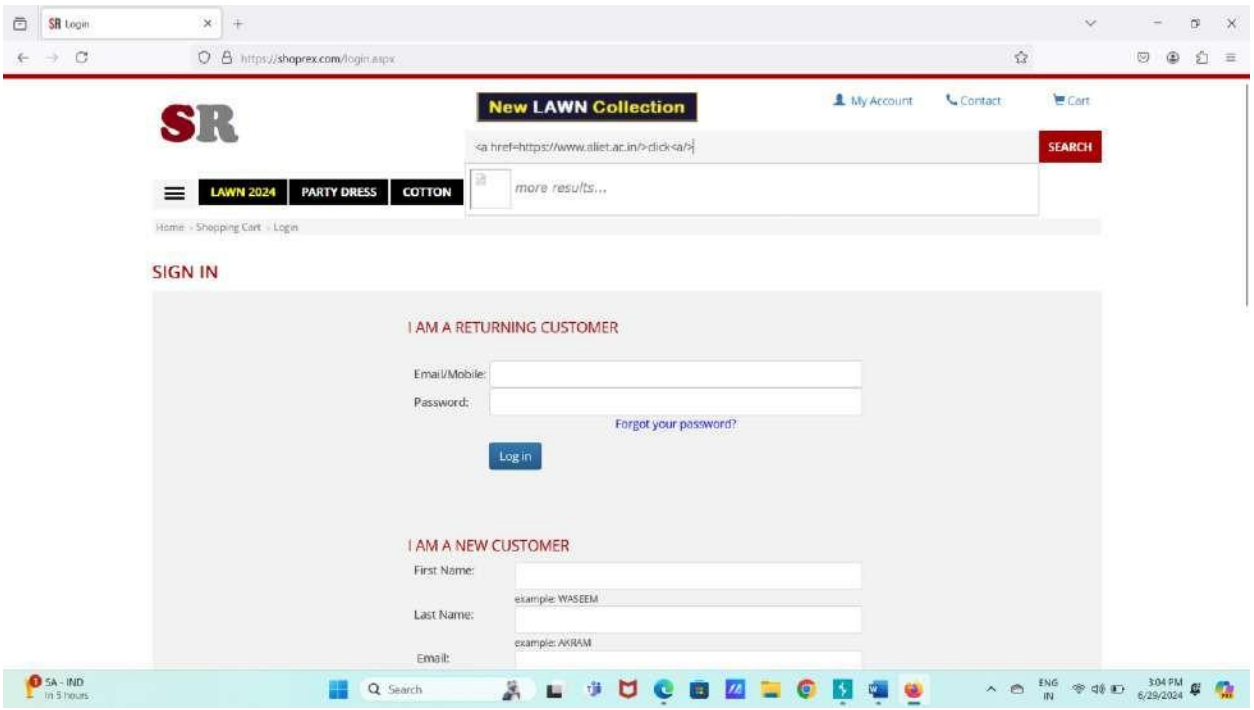


B. Find 2 websites vulnerable to HTML Injection Vulnerability.

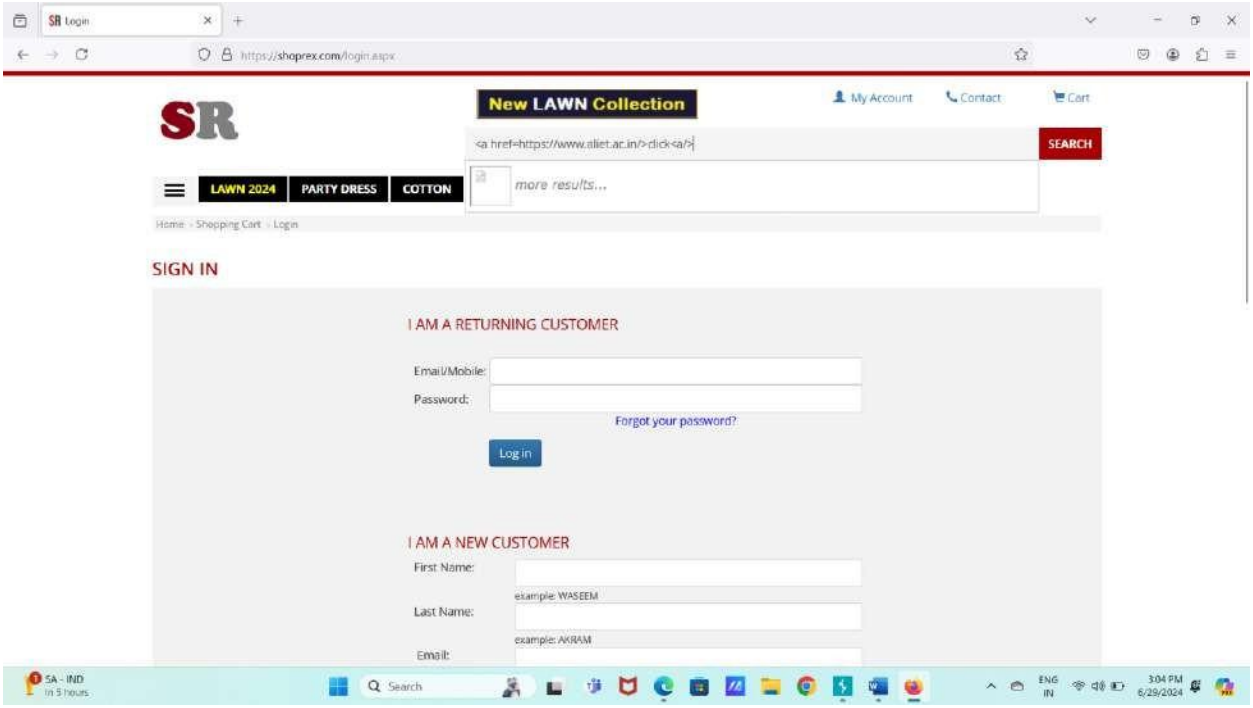
FIRST WEBSITE



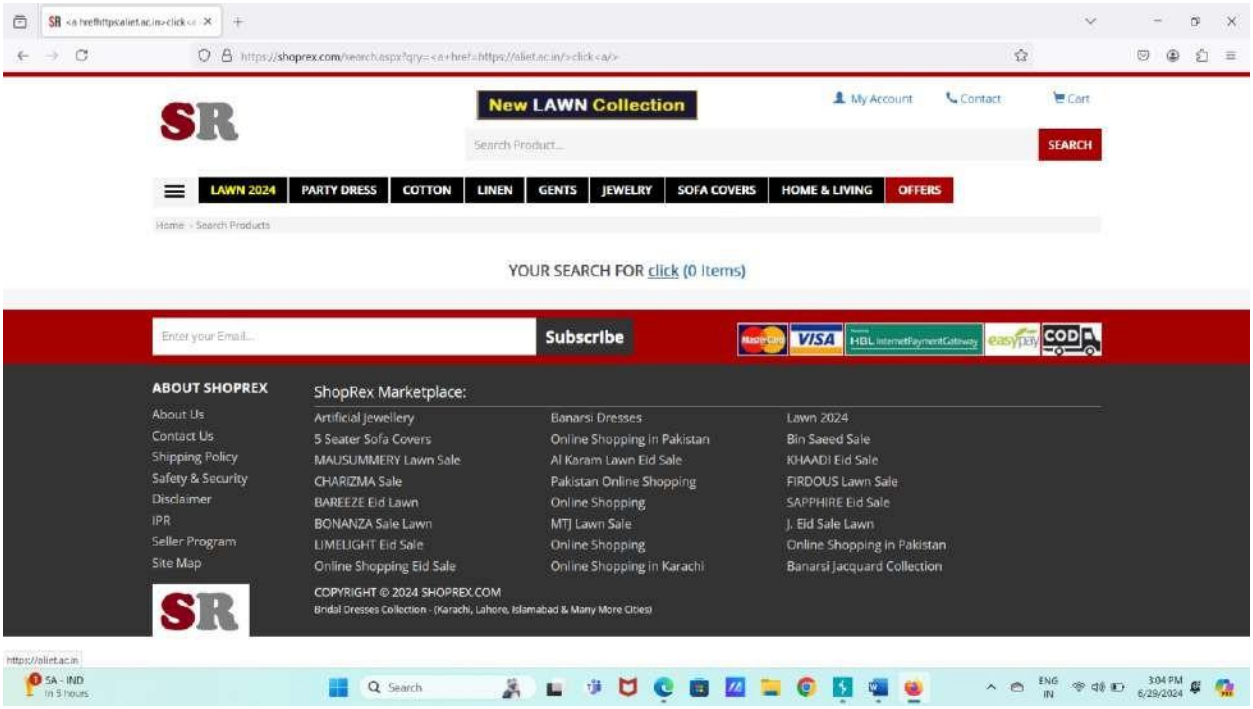
TYPE THE HTML CODE IN SEARCH:



NOW SEARCH THE CODE:



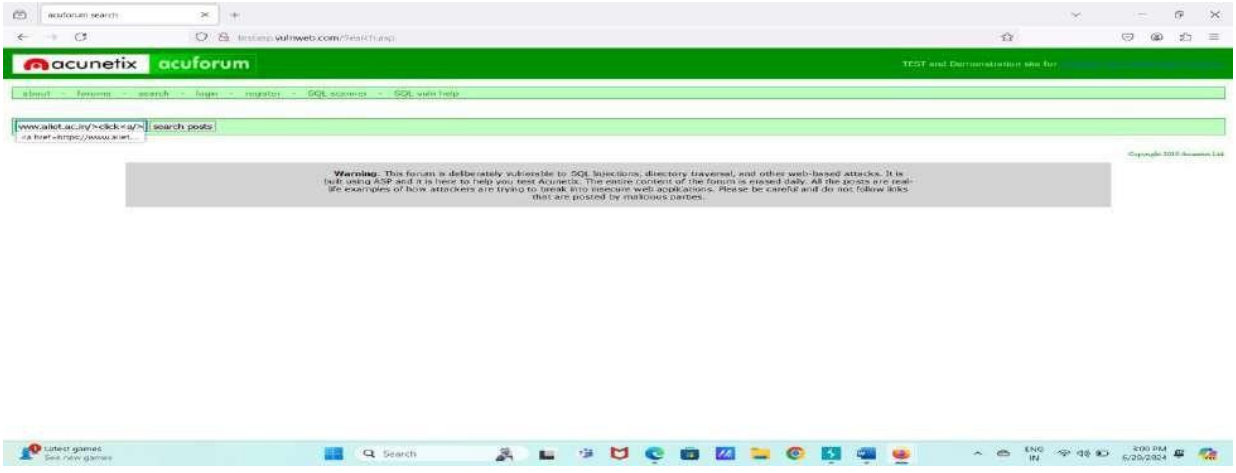
NOW CLICK ON CLICK BUTTON:



THEN THE PAGE IN OPEN THE WE PROVIDE:

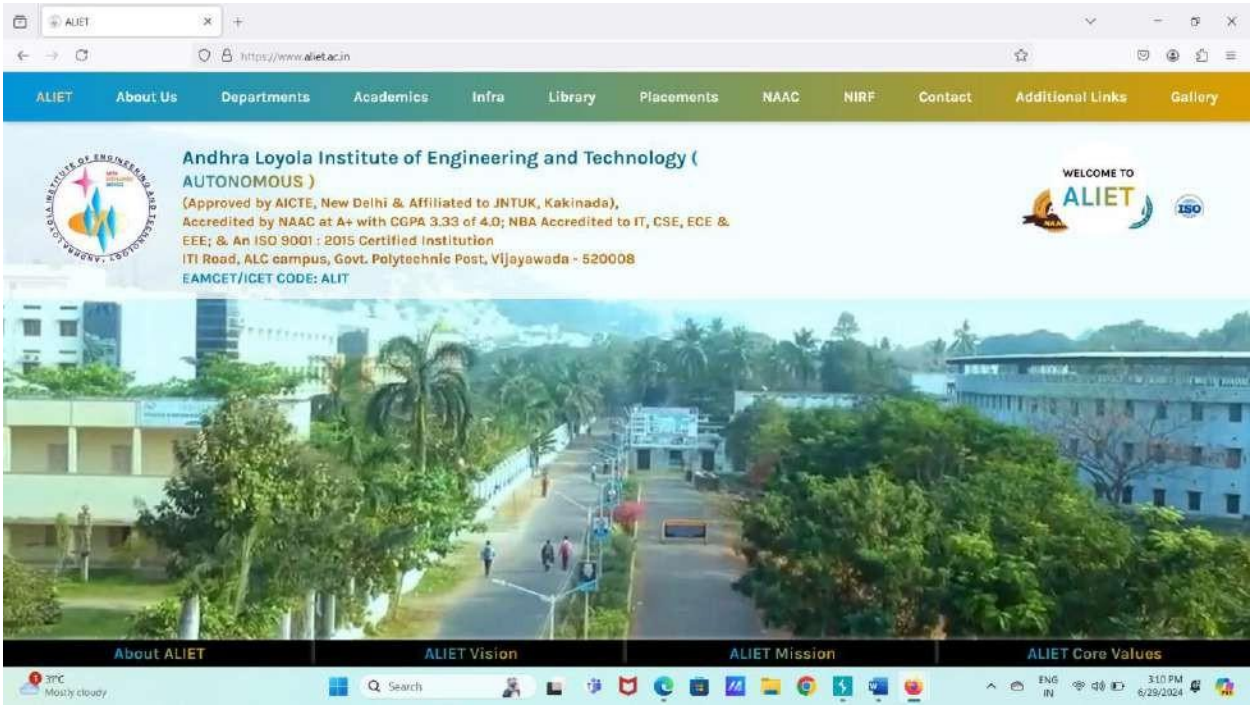
SECOND WEBSITE:

NOW PASTE THE HTML CODE:



NOW CLICK ON BUTTON CLICK:

THEN THE WEBSITE YOU GIVEN IS SHOWN IN THAT:

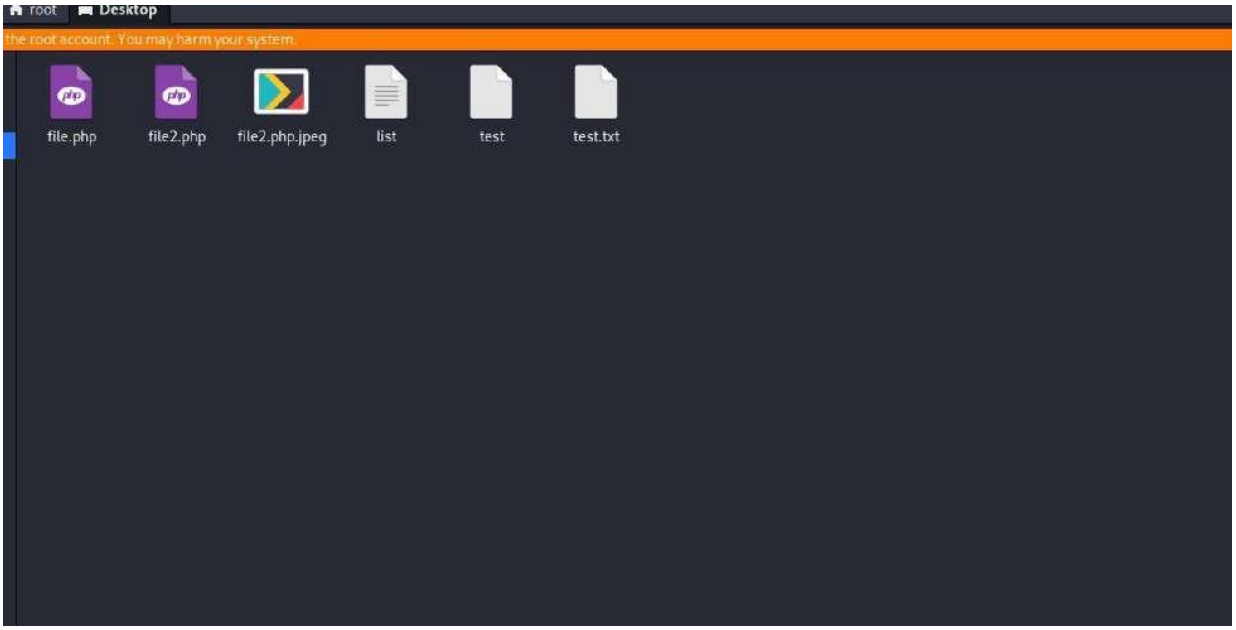


C. Find 2 websites vulnerable to File Upload Vulnerability on each test case below.

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

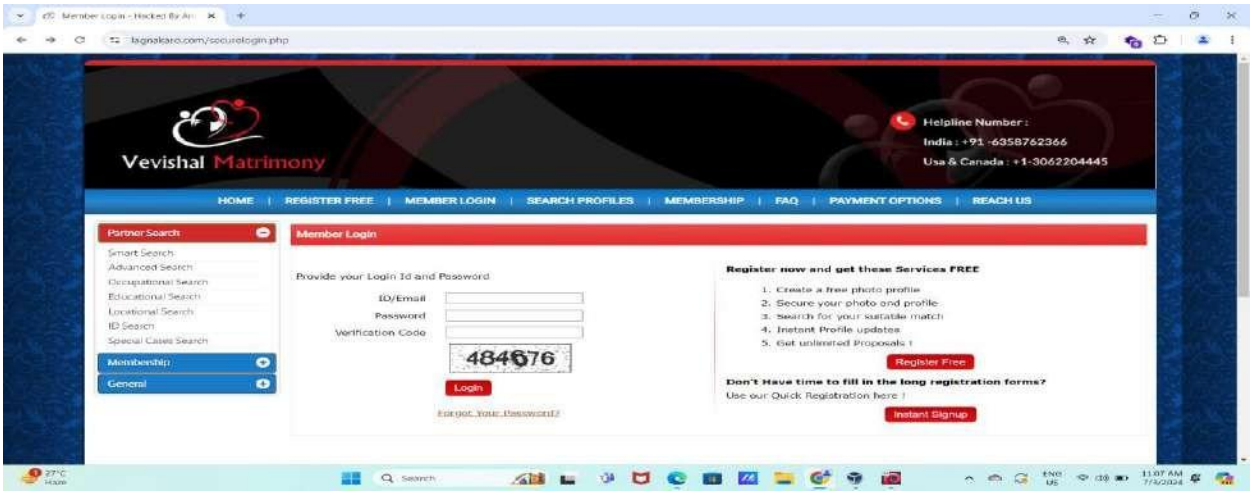
ASSIGNMENT-8

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

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

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

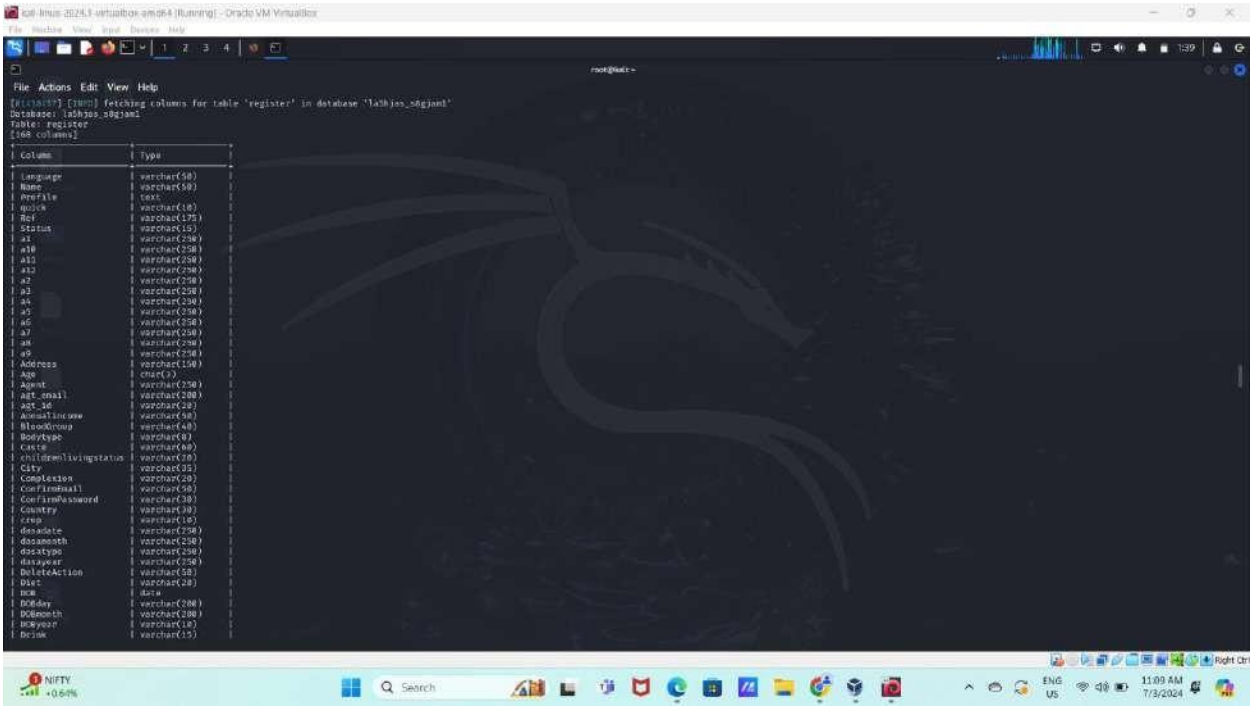
A)



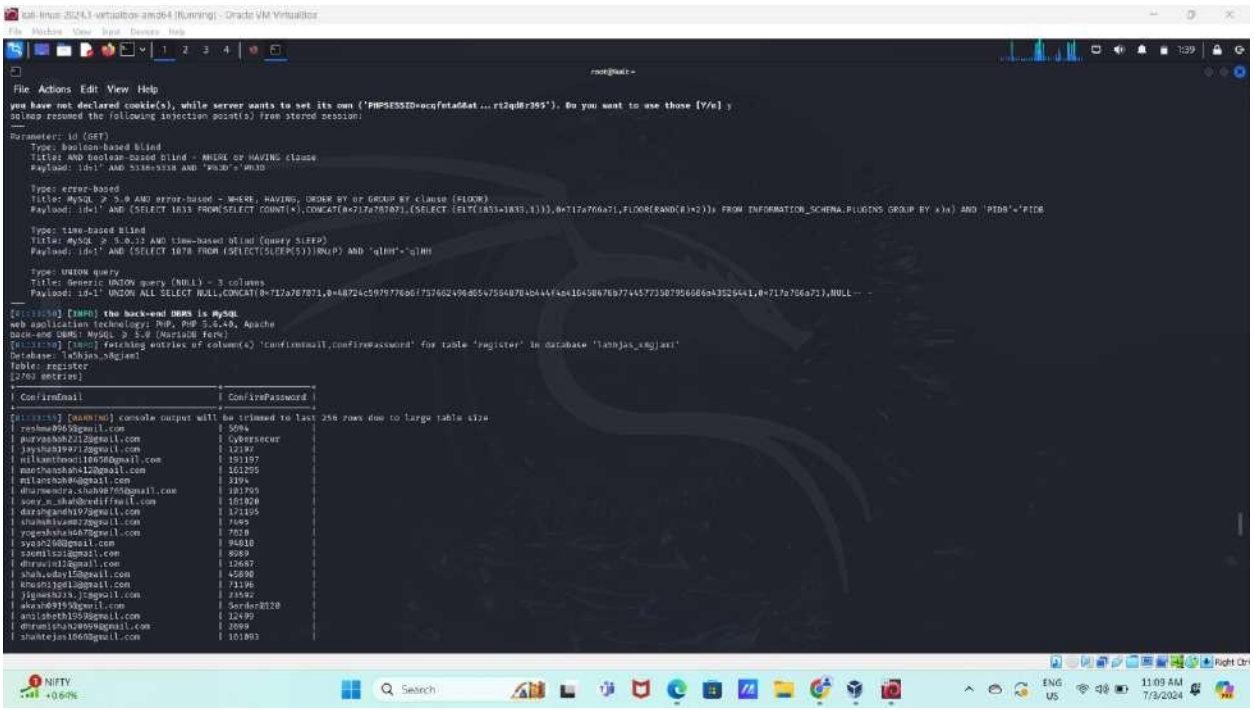
NOW ON SQLMAP SEARCH IT:

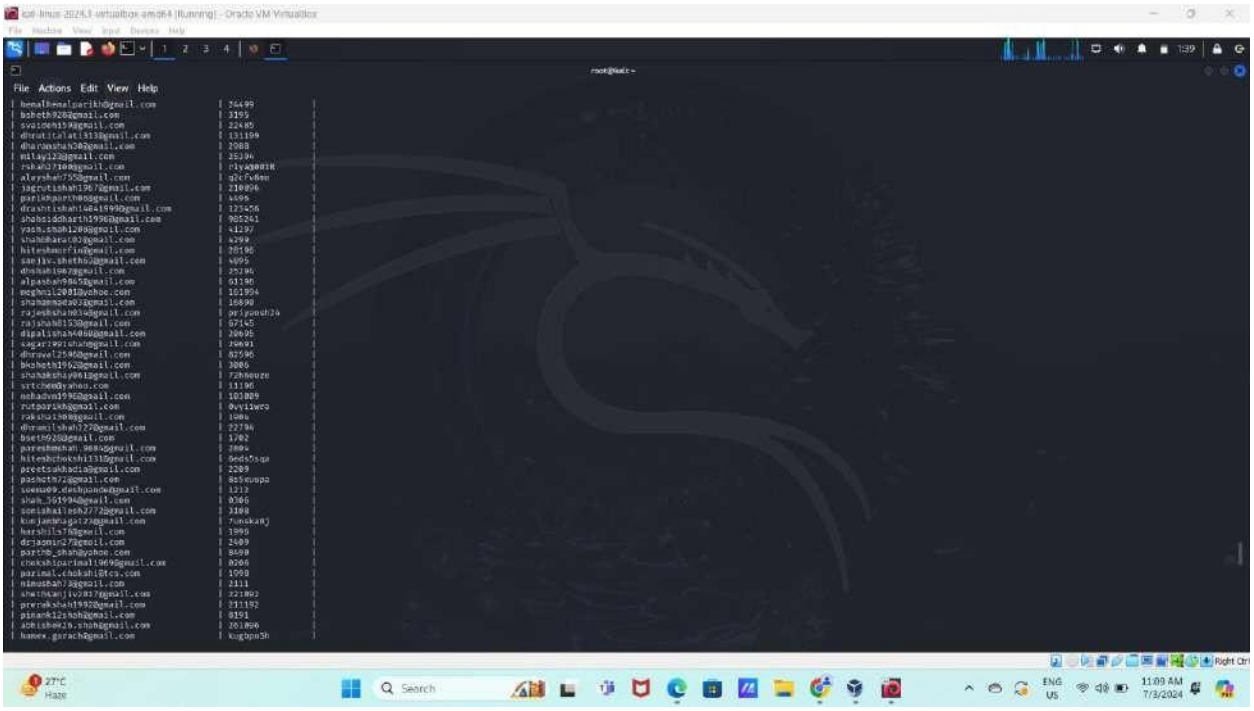
AFTER THAT WE SEEN THREE DATABASES:

NOW OPEN DATABASE



ALSO OPEN THE COLUMS:



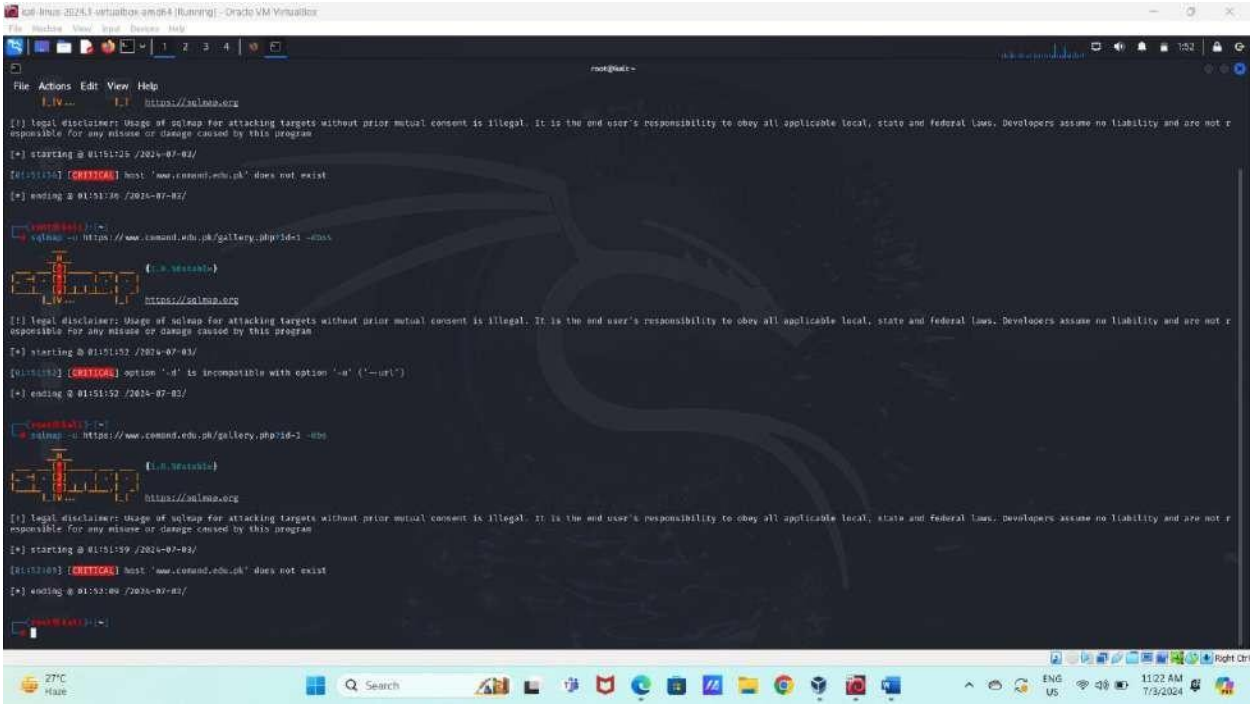


THAT IS THE DATA PRESENT IN TABLES

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

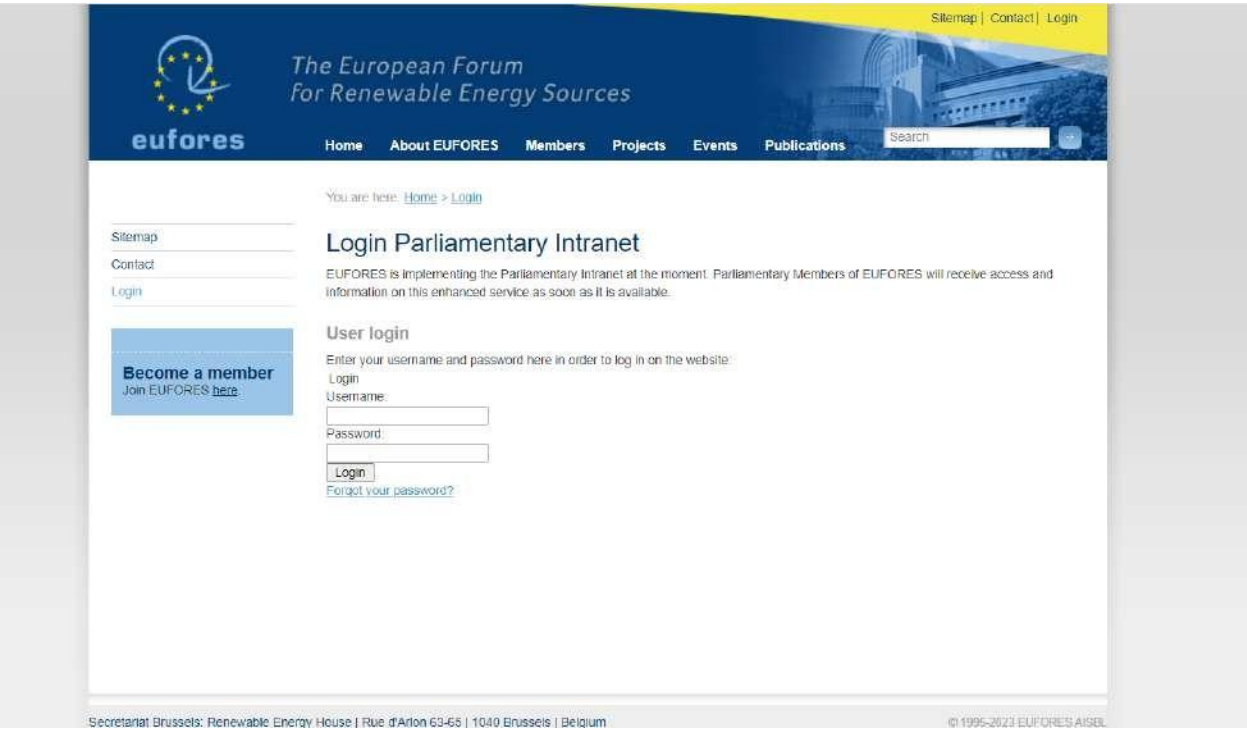
b. Password reset link is not getting expired

c. Automatic email confirmation bug

d. Password reset link sent with http

e. Exposure of private information (privacy violation)

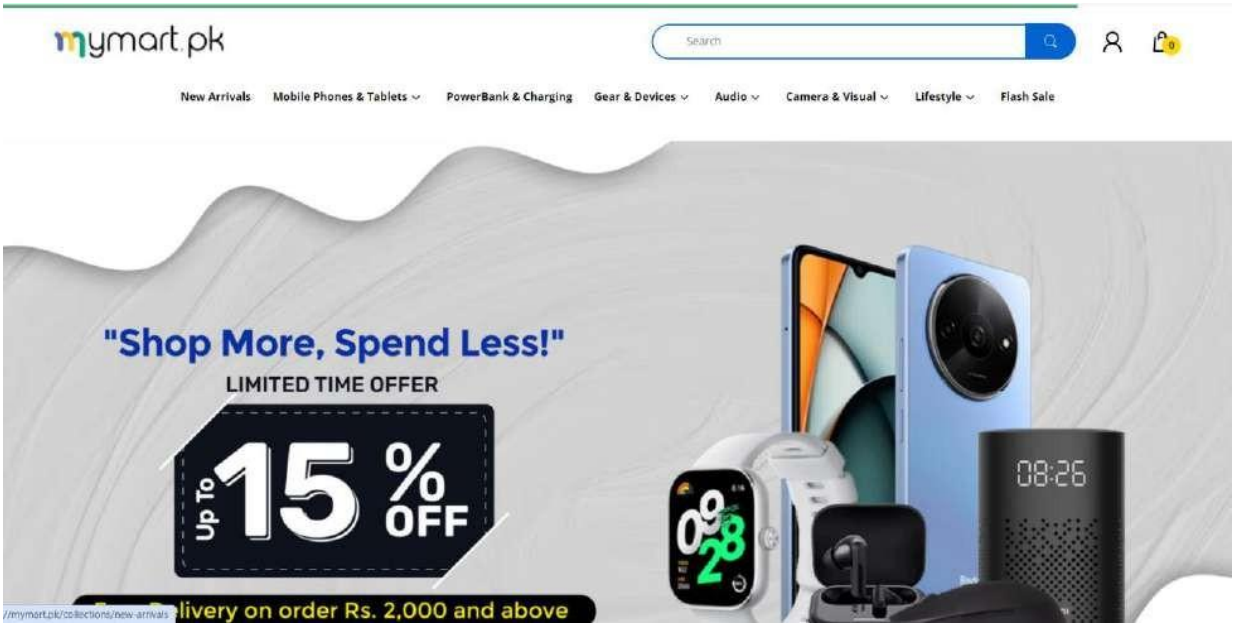
f. Old session doesn't expire



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

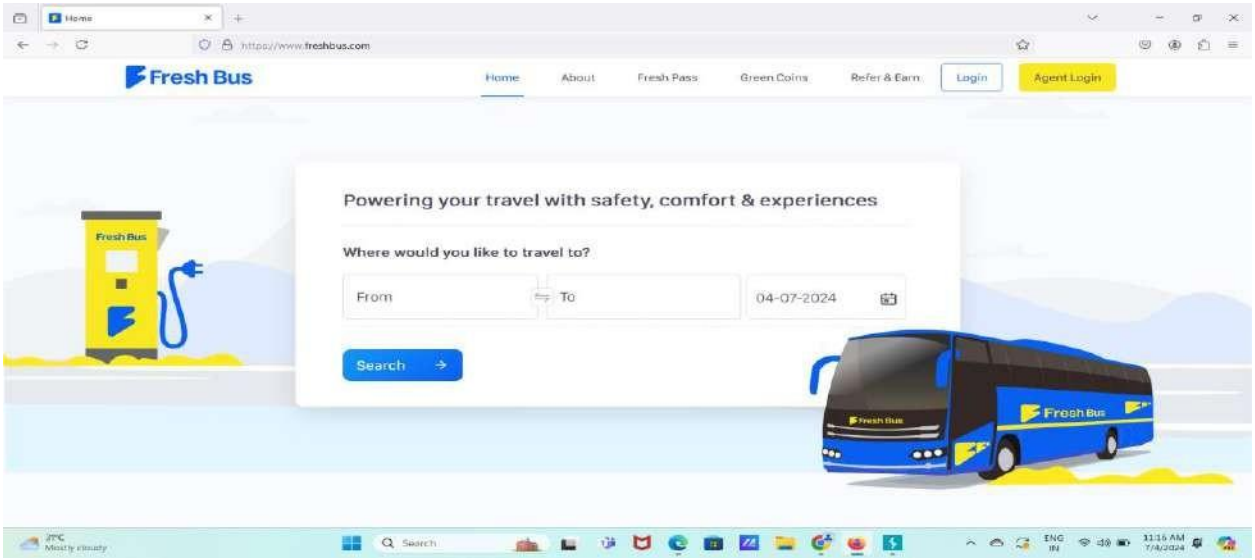
A. Perform No Rate Limiting on the login OTP page of the following websites mentioned below:

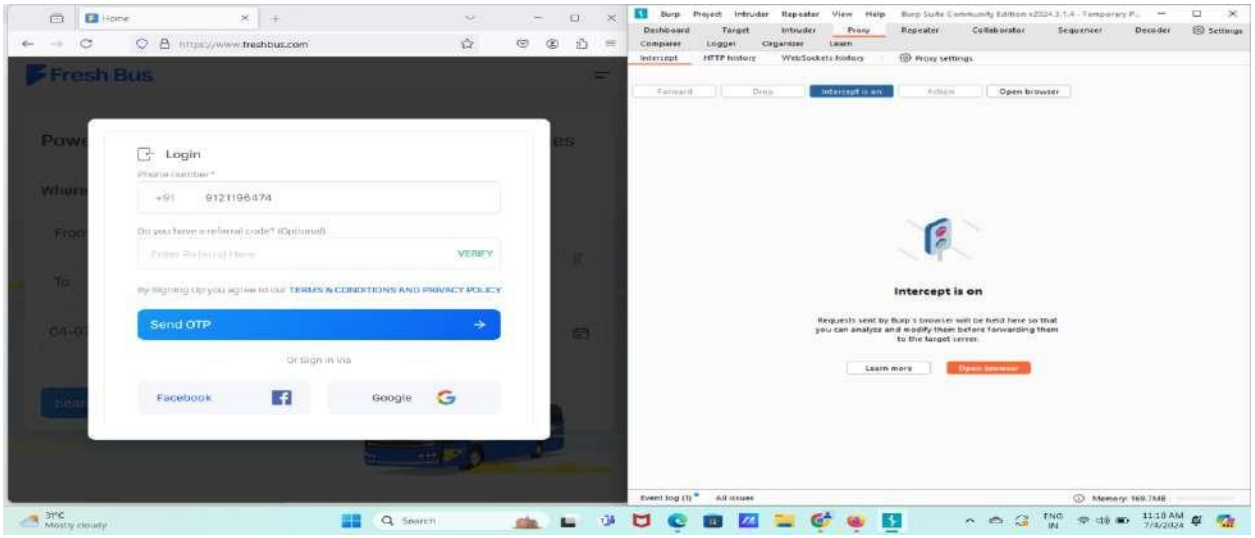
a) https://www.freshbus.com/

b) https://nuego.in/

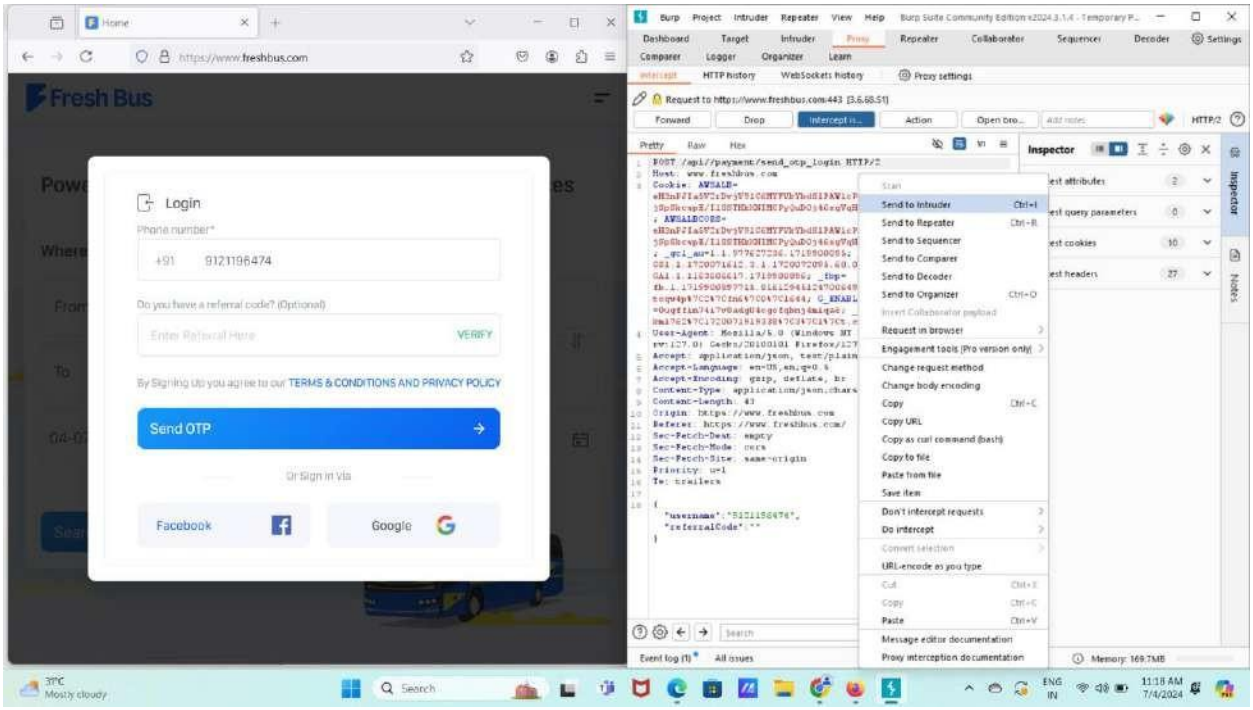
c) https://yolobus.in/

A)

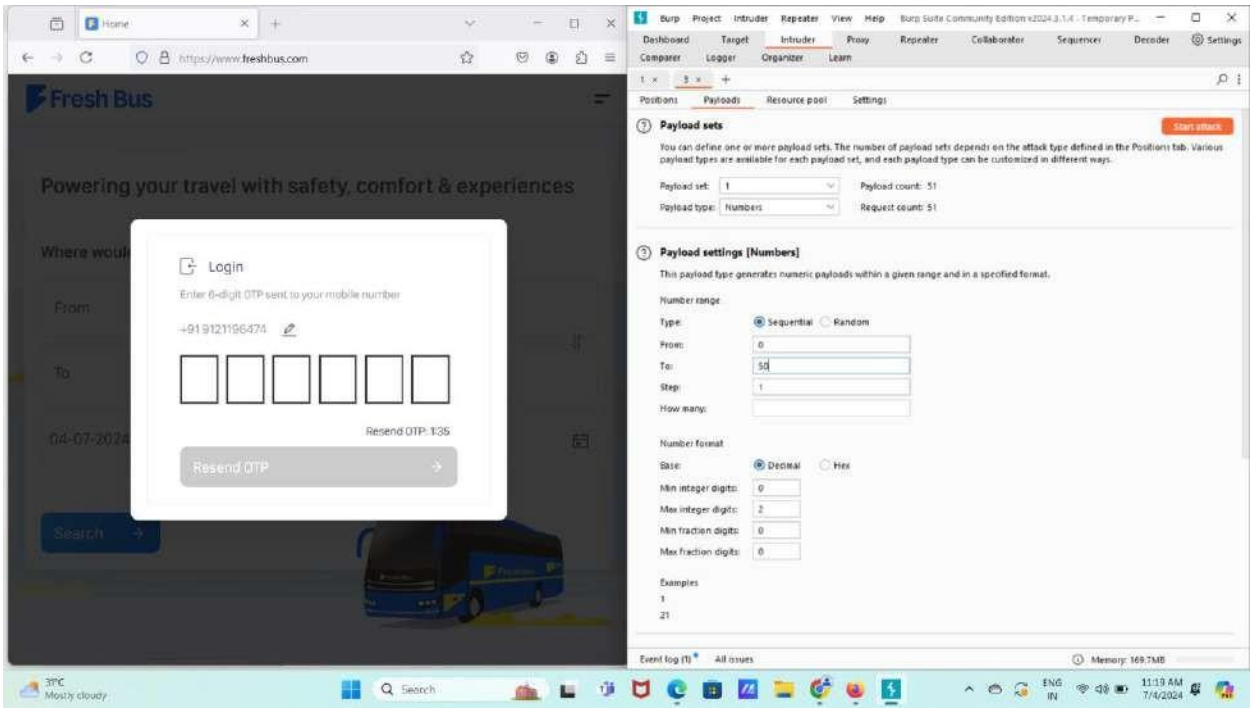




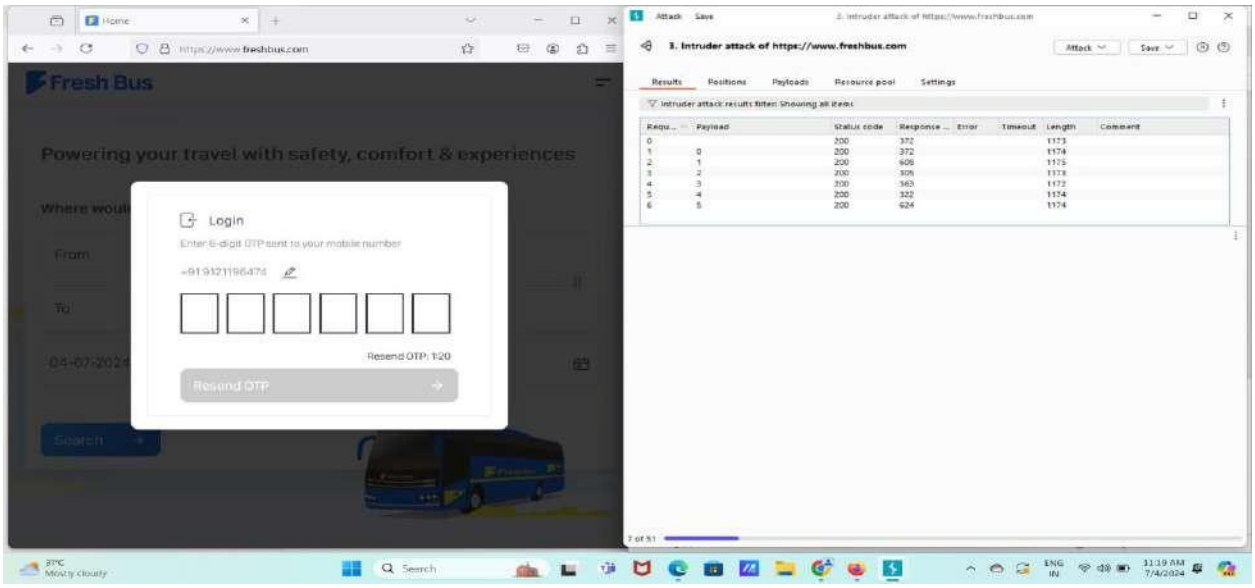
INTERCEPT ON AND LOGIN:

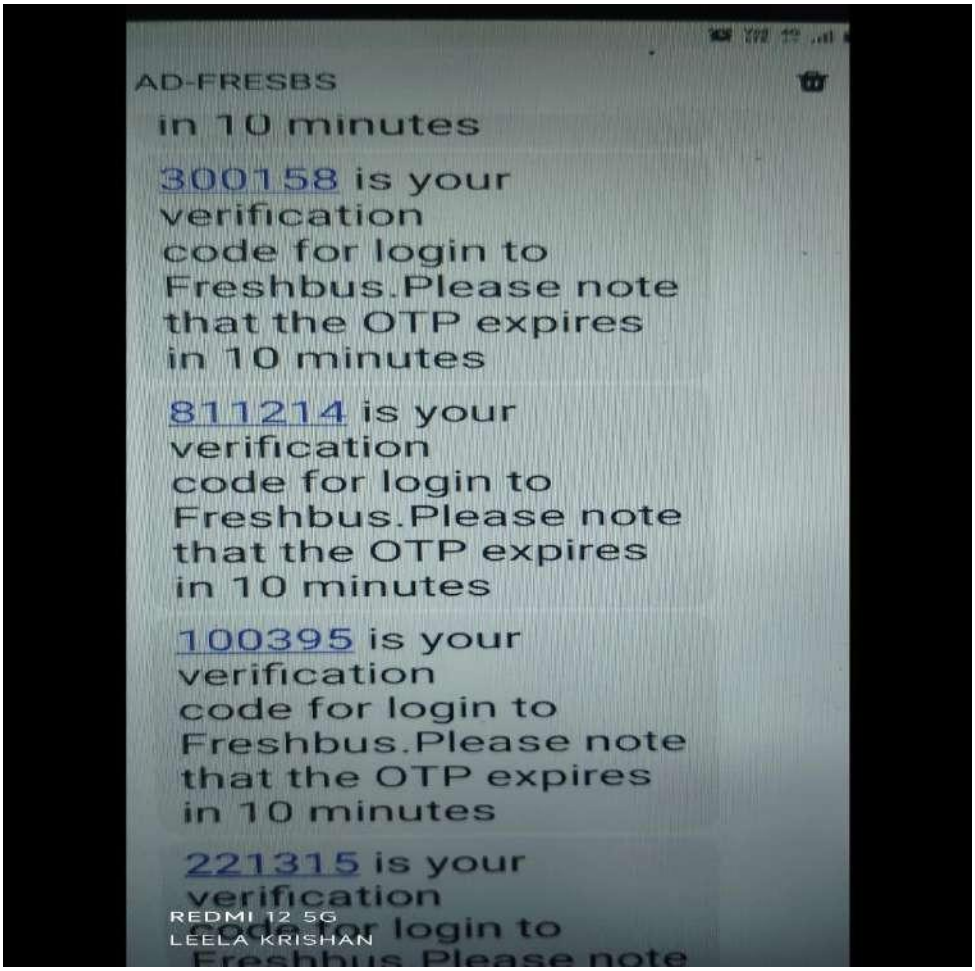


SET PAYLOAD :

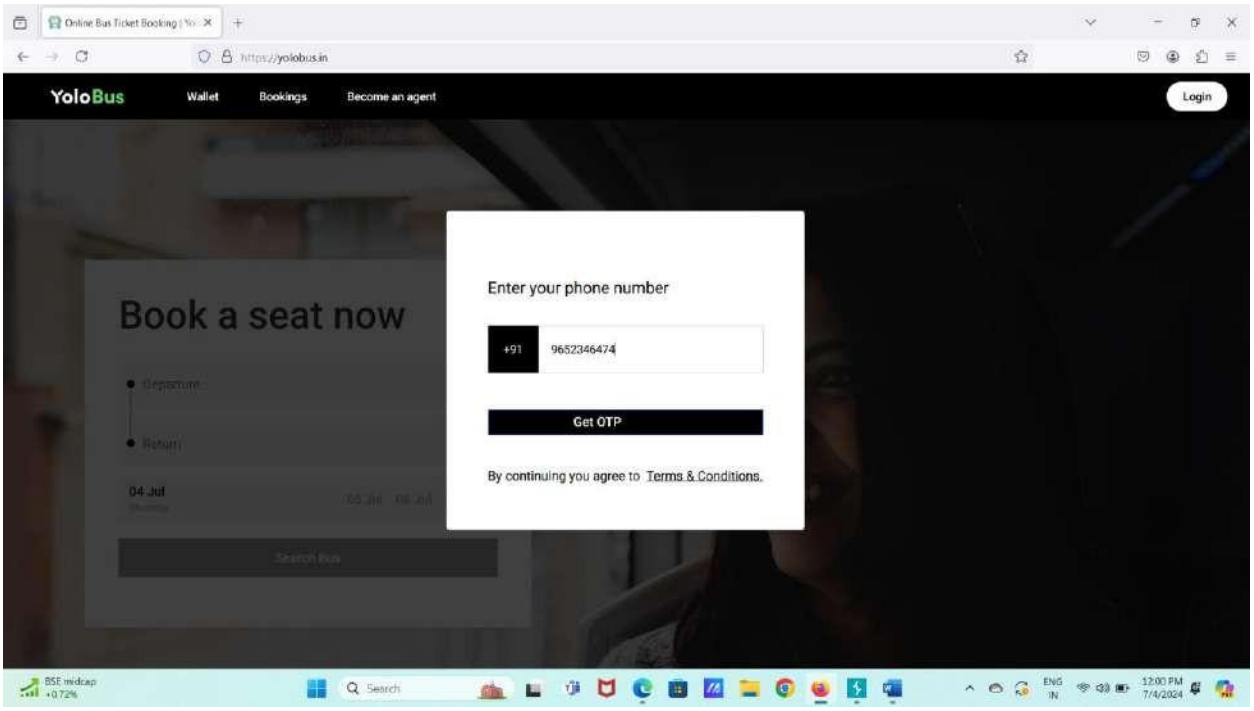


NOW START THE ATTACK:

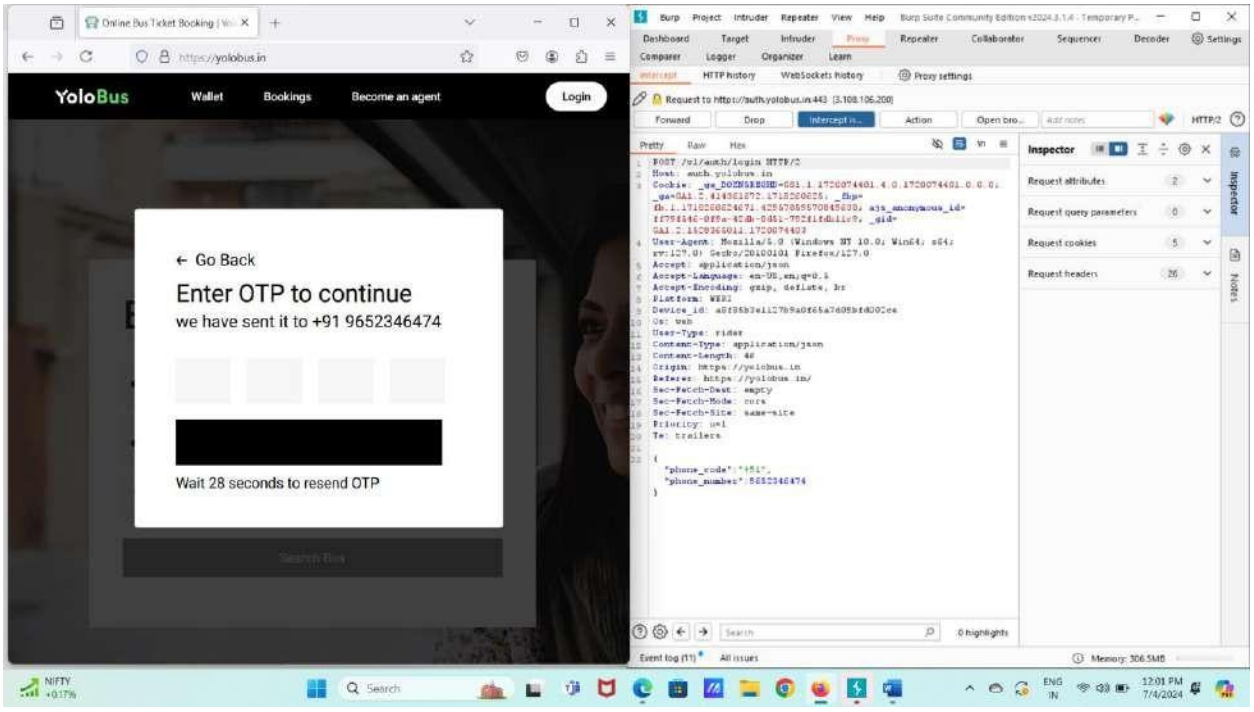

Fresh Bus
Powering your travel with safety, comfort & experiences
Login
Resend OTP
3. Intruder attack of https://www.freshbus.com
Attack
Save
Results
Positions
Payloads
Resource pool
Settings

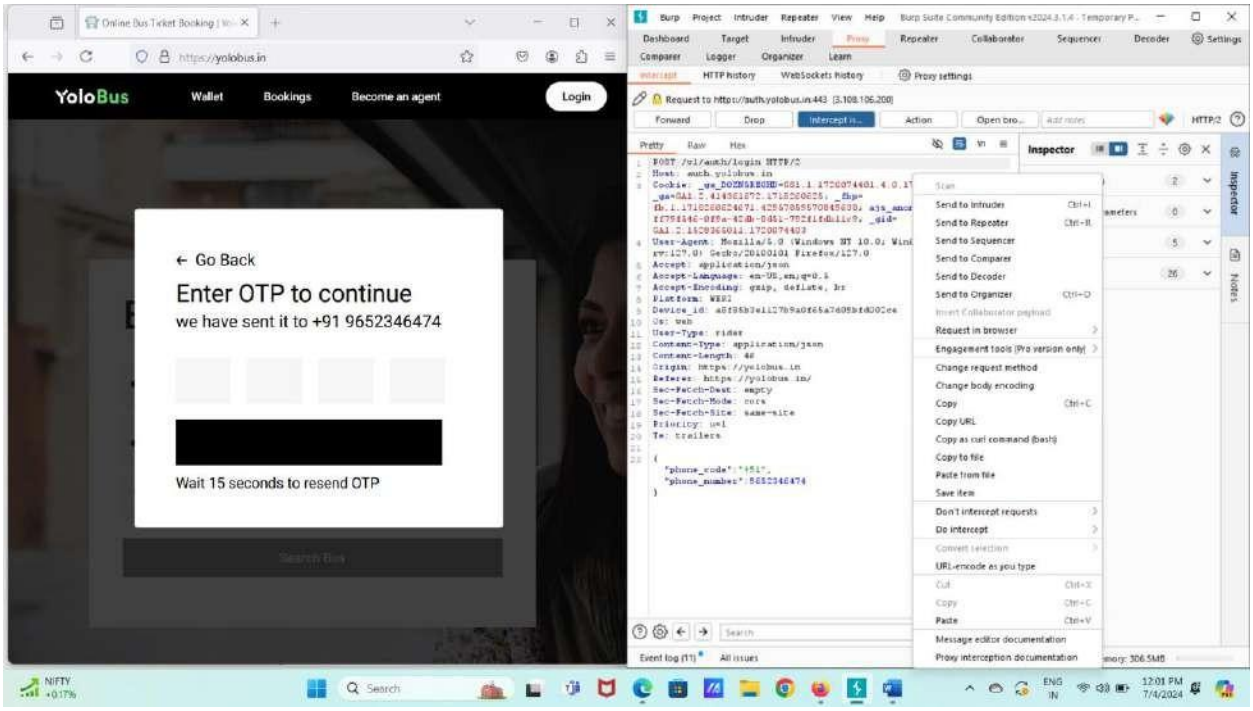

AD-FRESBS
in 10 minutes
300158 is your verification code for login to Freshbus.Please note that the OTP expires in 10 minutes
811214 is your verification code for login to Freshbus.Please note that the OTP expires in 10 minutes
100395 is your verification code for login to Freshbus.Please note that the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

B)

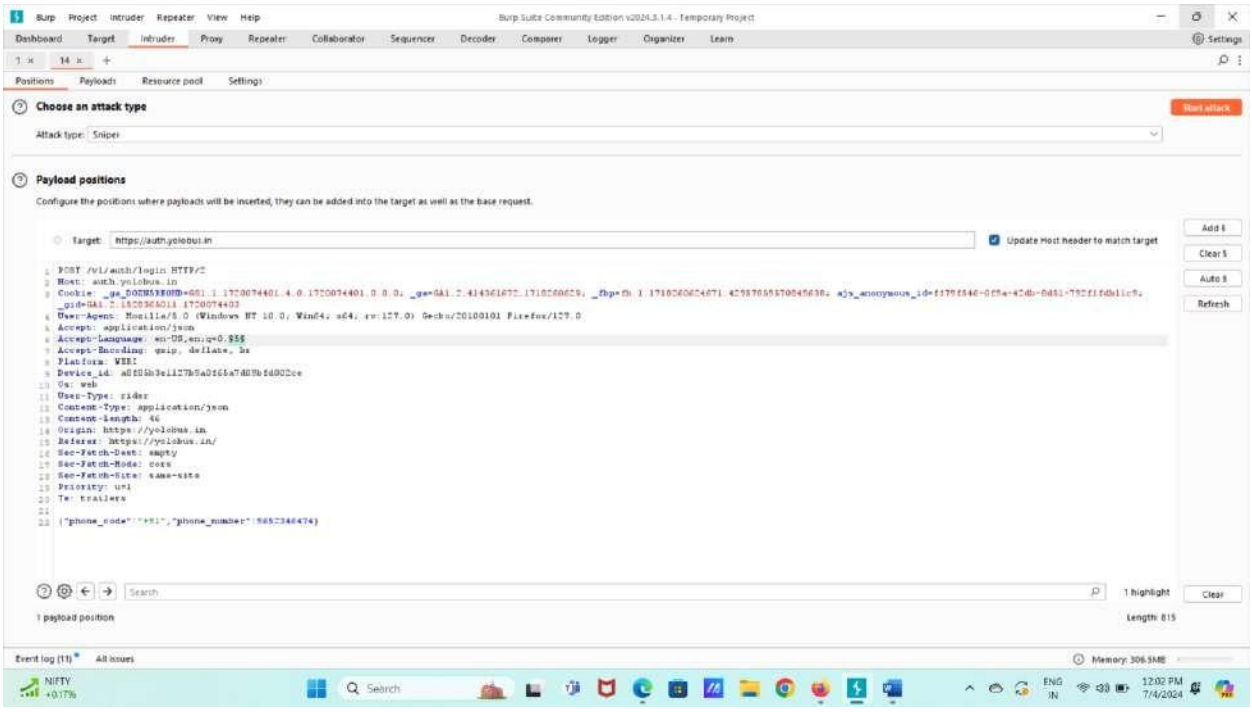


SAME PROCESS:

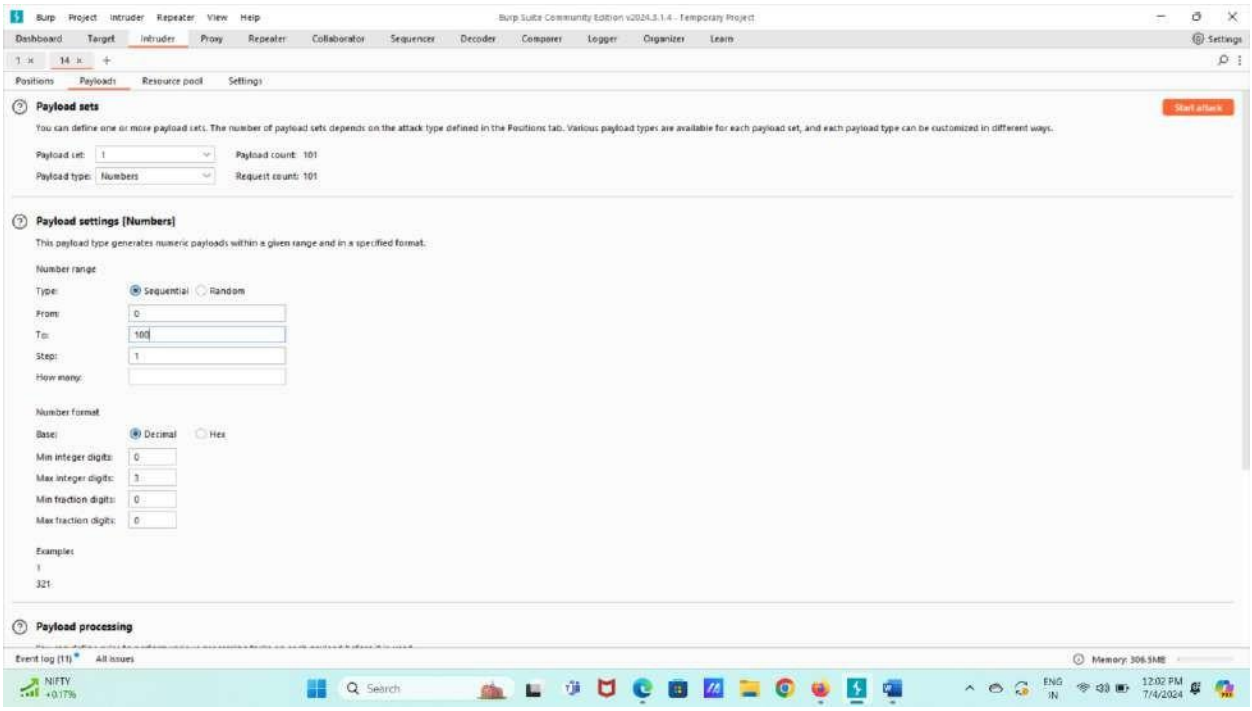




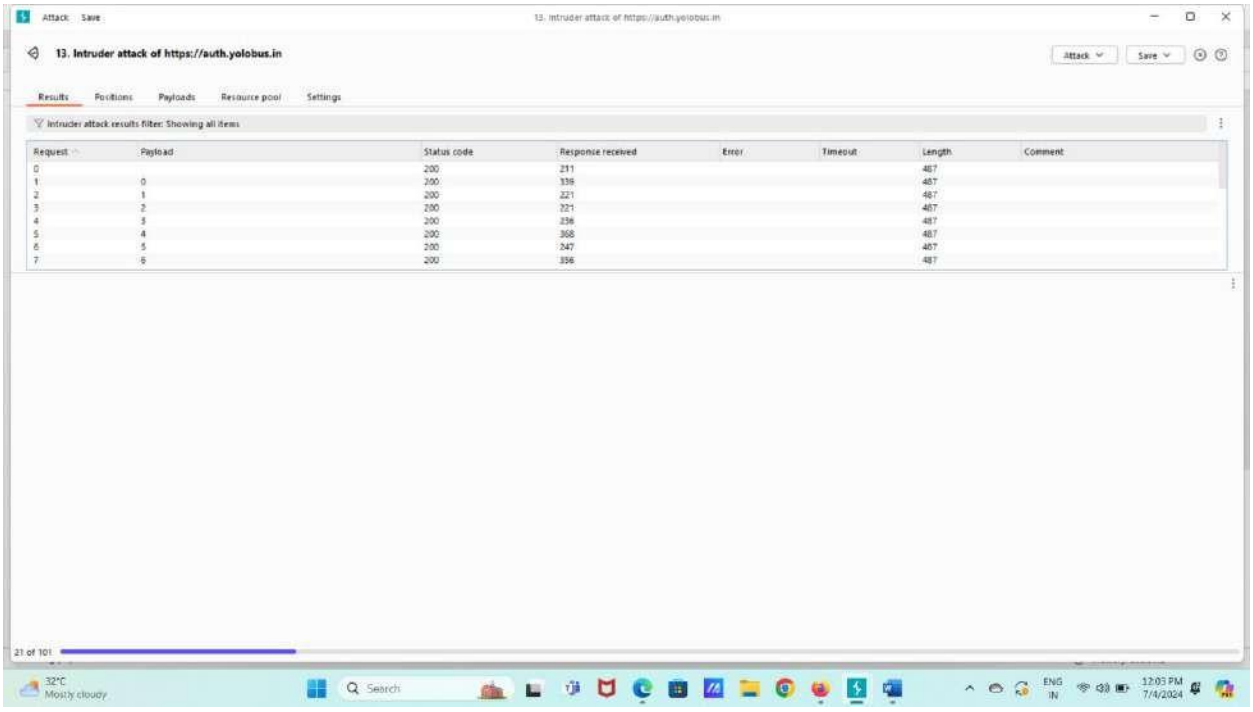
NOW SELECT THE ACCEPT LANGUAGE:



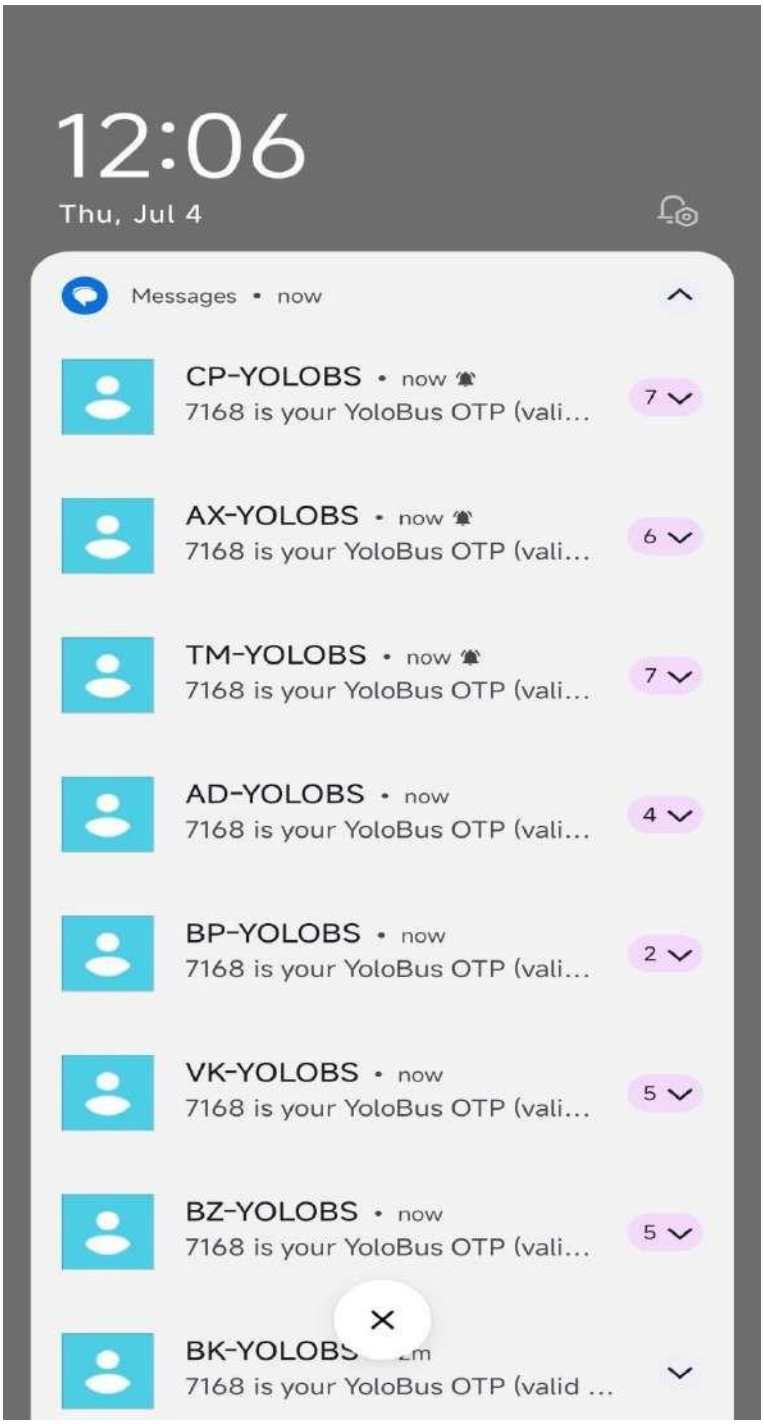
SET PAYLOAD:



START ATTACK:



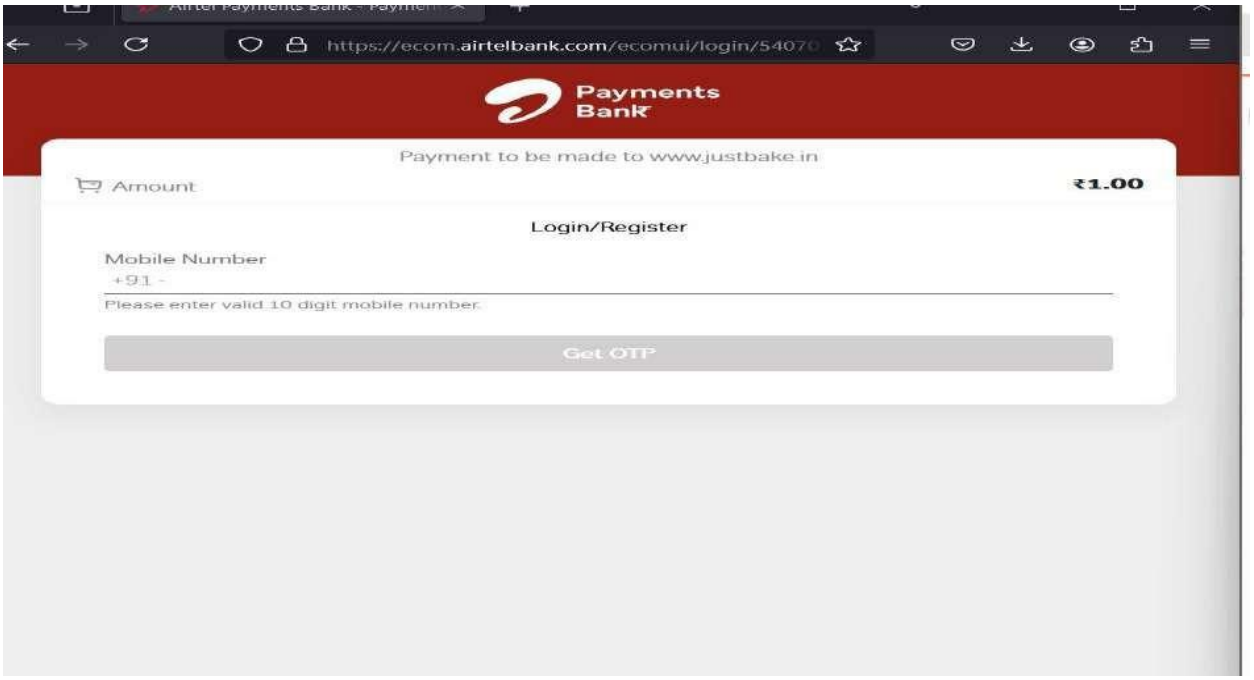
THE RESULT:


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.

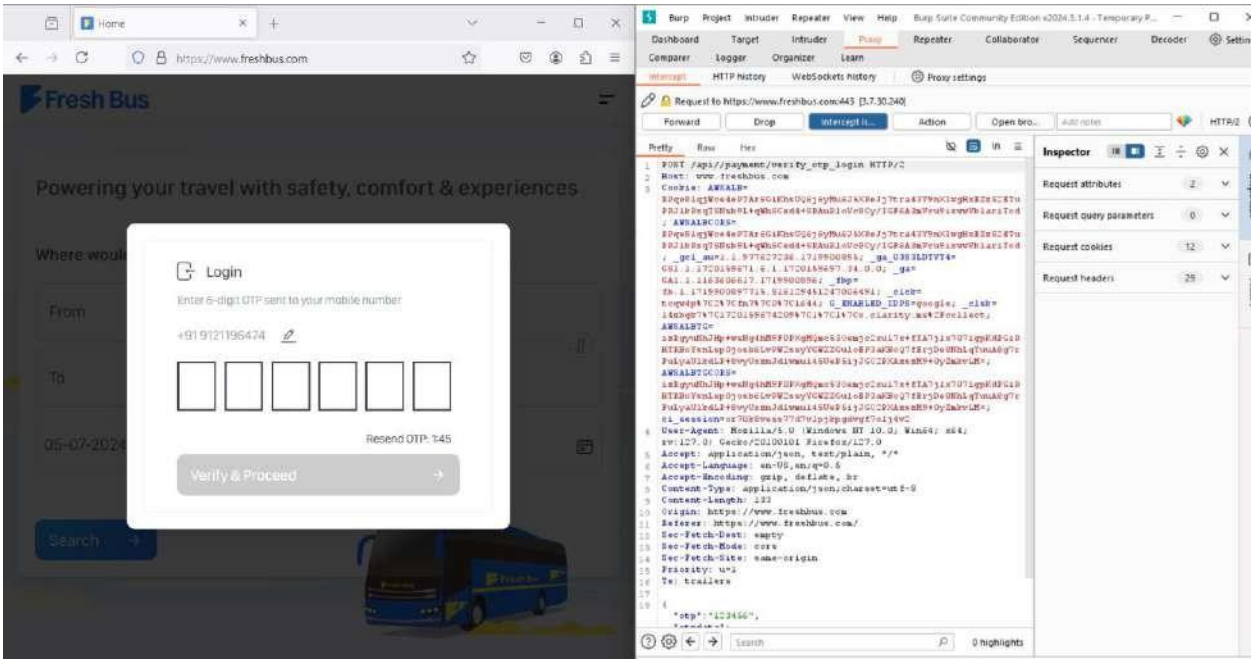
ORDER THE ANY CAKE:

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

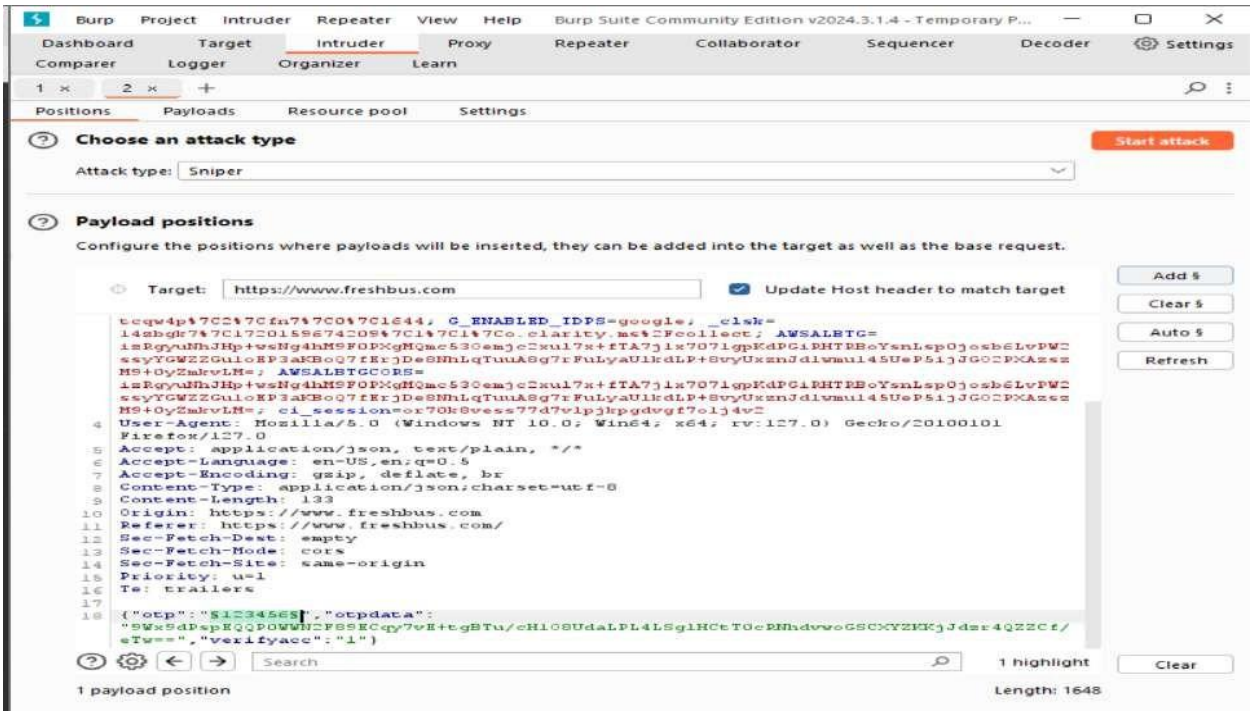


THIS ABOUT PRICE TAMPERING

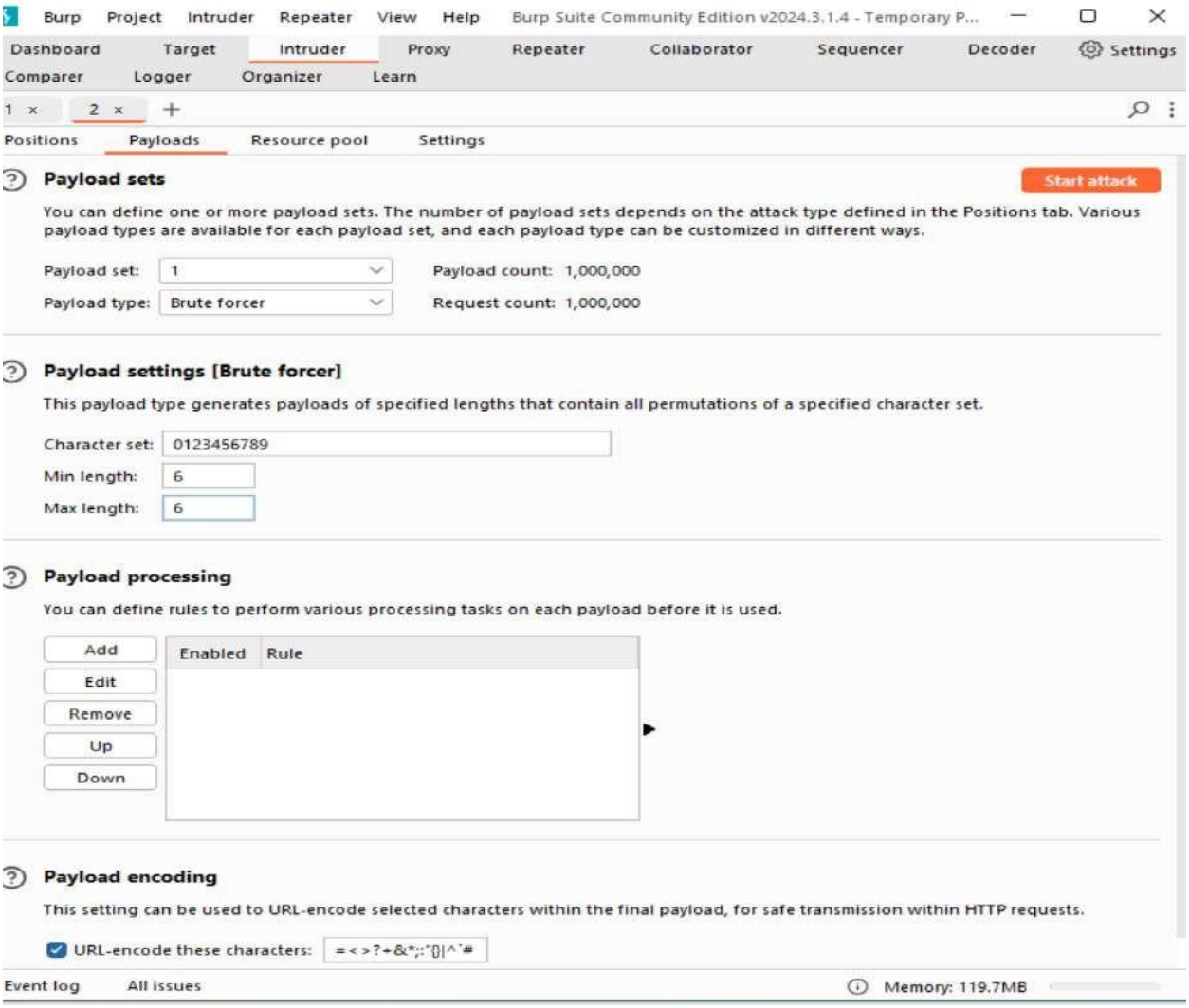
C) Perform Authentication Bypass Exploitation on any website and Prepare clear Documentation. Note: OTP Bypassing



SET THE OTP:

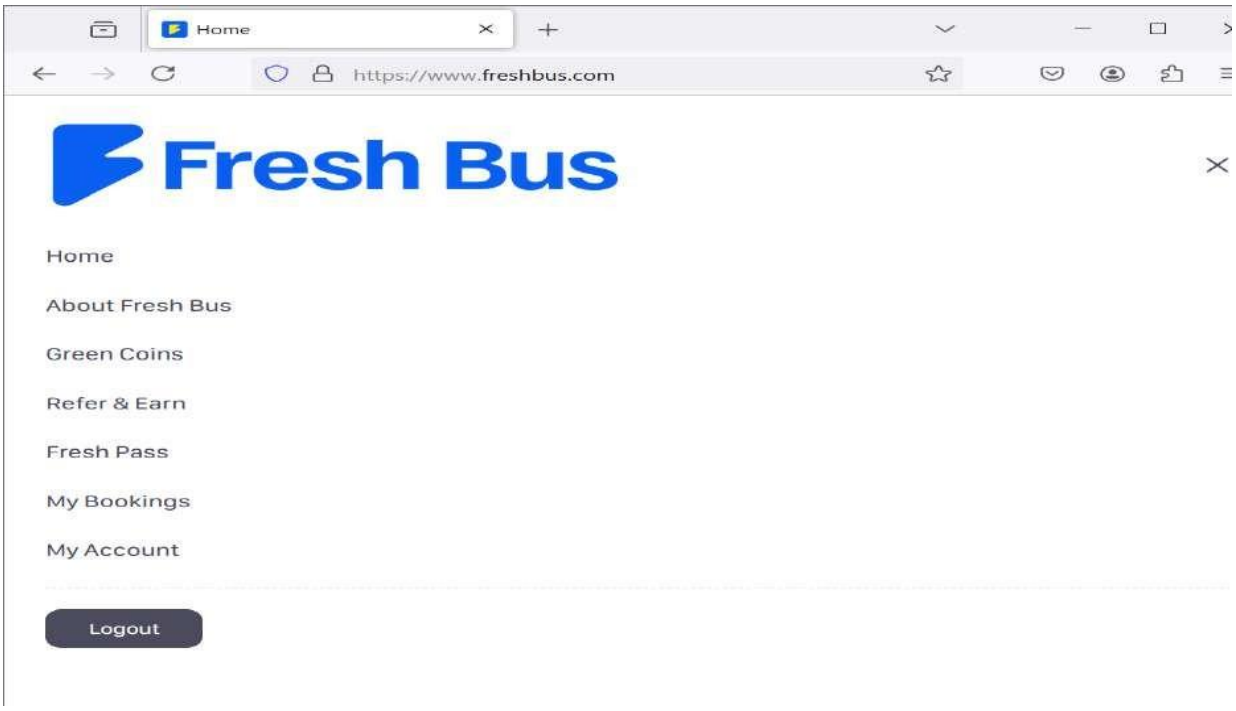


AND SET PAYLOAD:



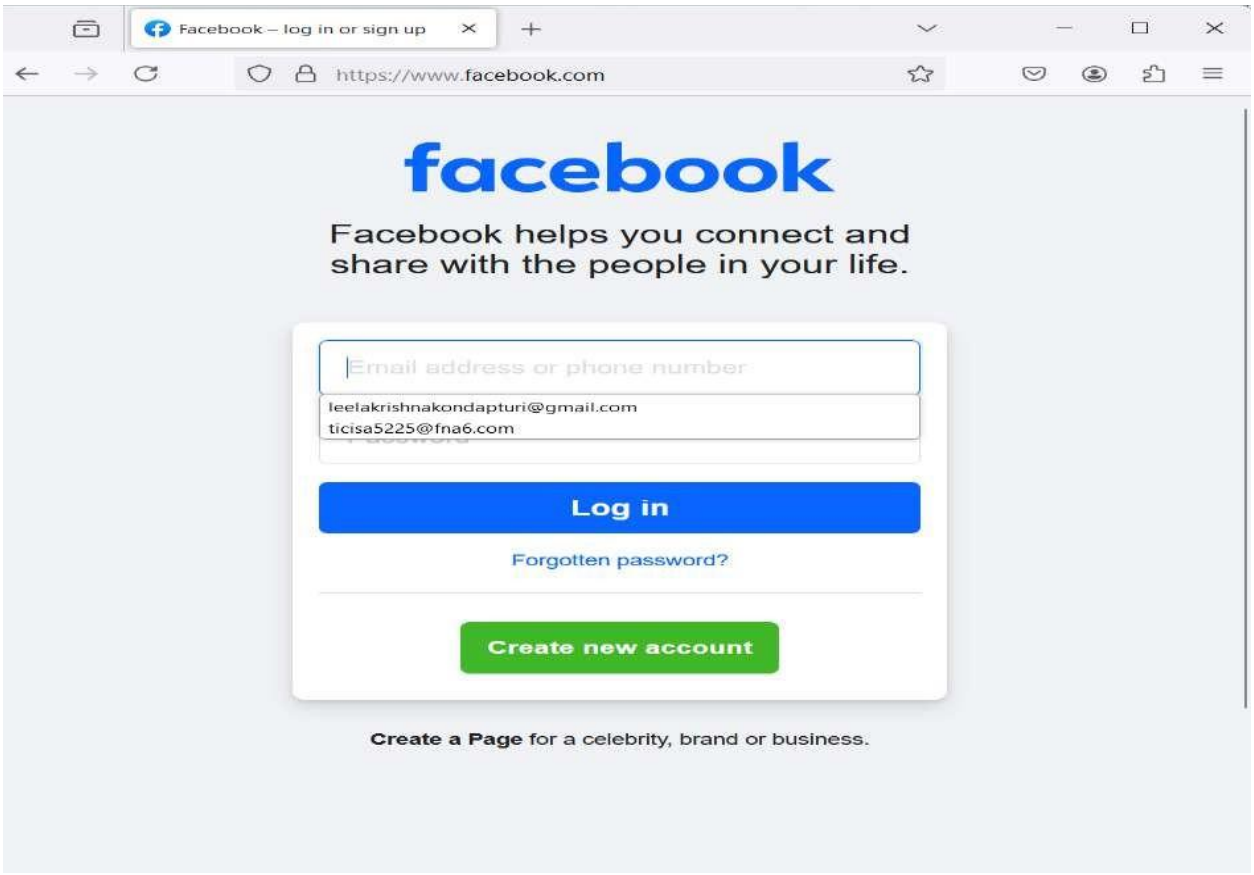
START ATTACK:

SUCESFULLYLOGIN:

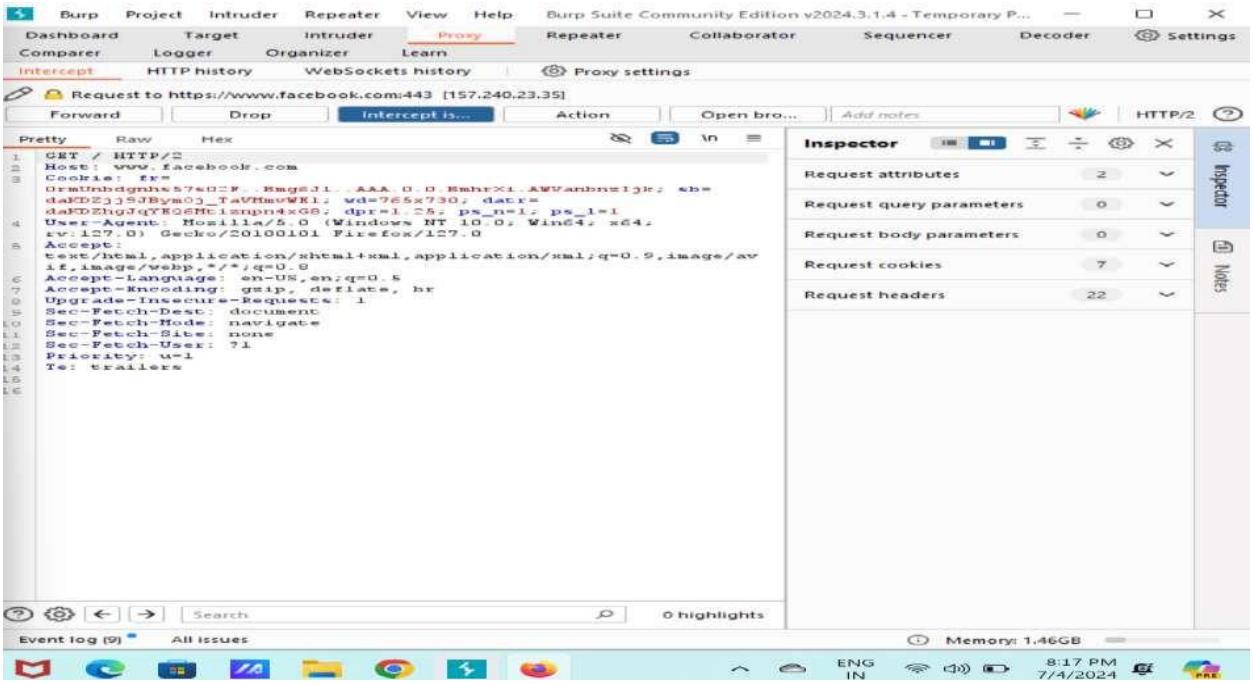

Home
https://www.freshbus.com
Fresh Bus
Home
About Fresh Bus
Green Coins
Refer & Earn
Fresh Pass
My Bookings
My Account
Logout

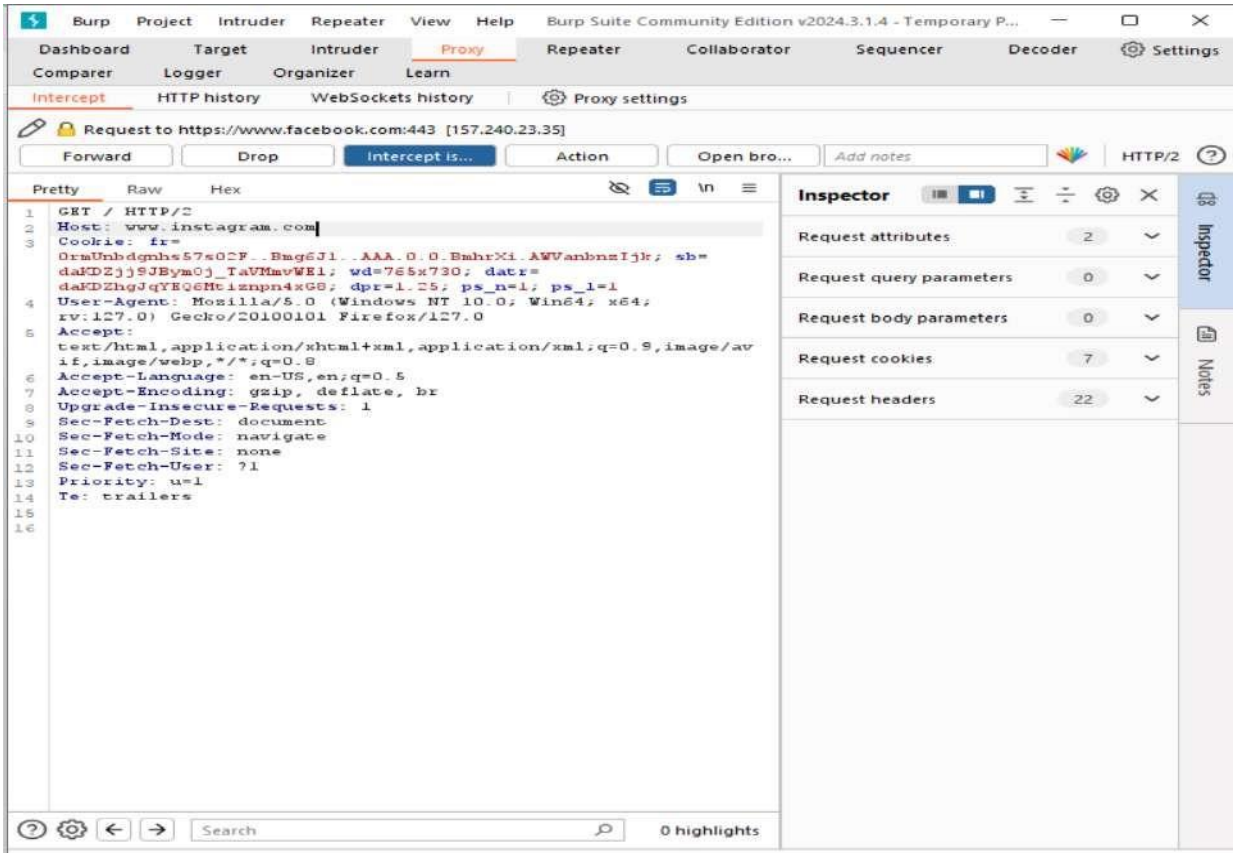
ASSIGNMENT-11

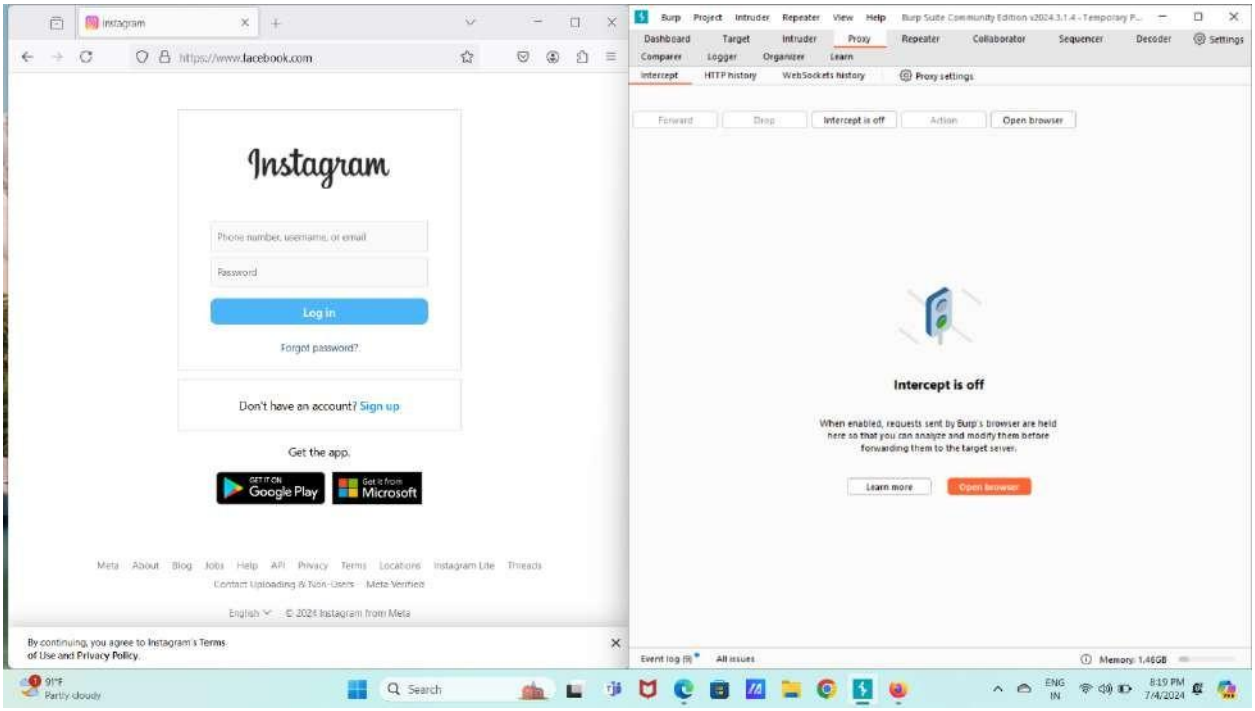
A. Find a website vulnerable to Host Header Injection Vulnerability.



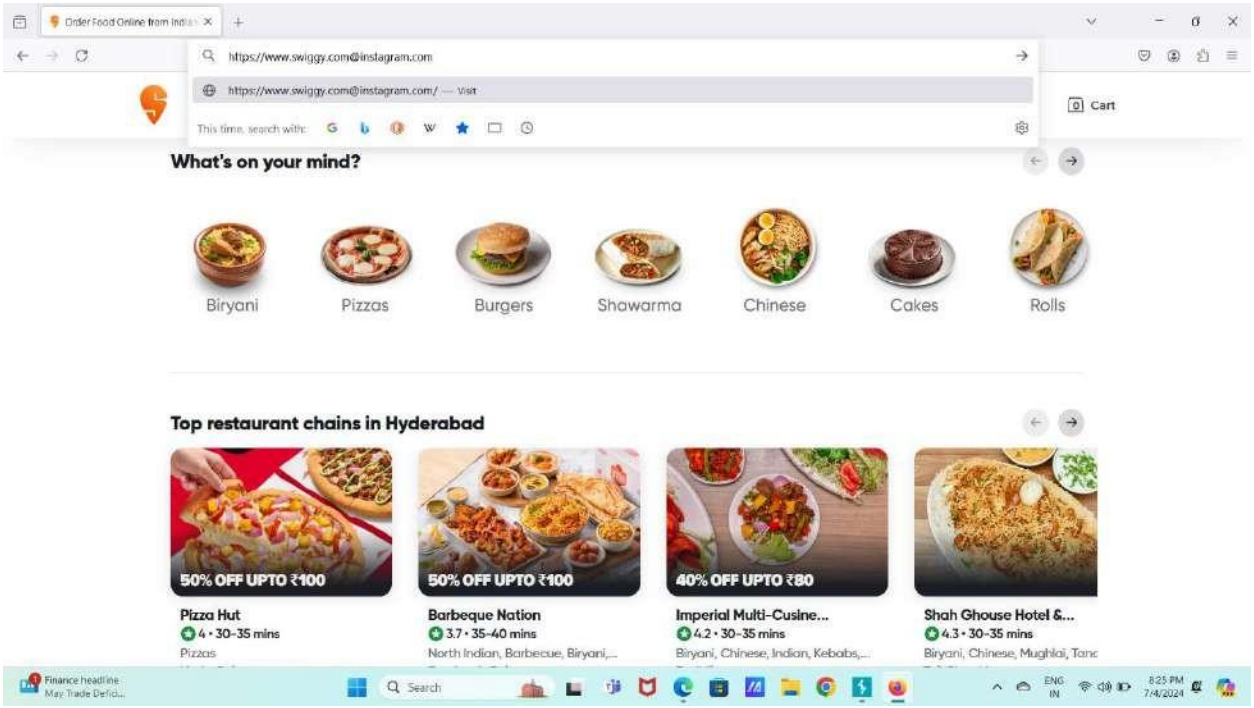
TURN ON THE INTERCEPT:

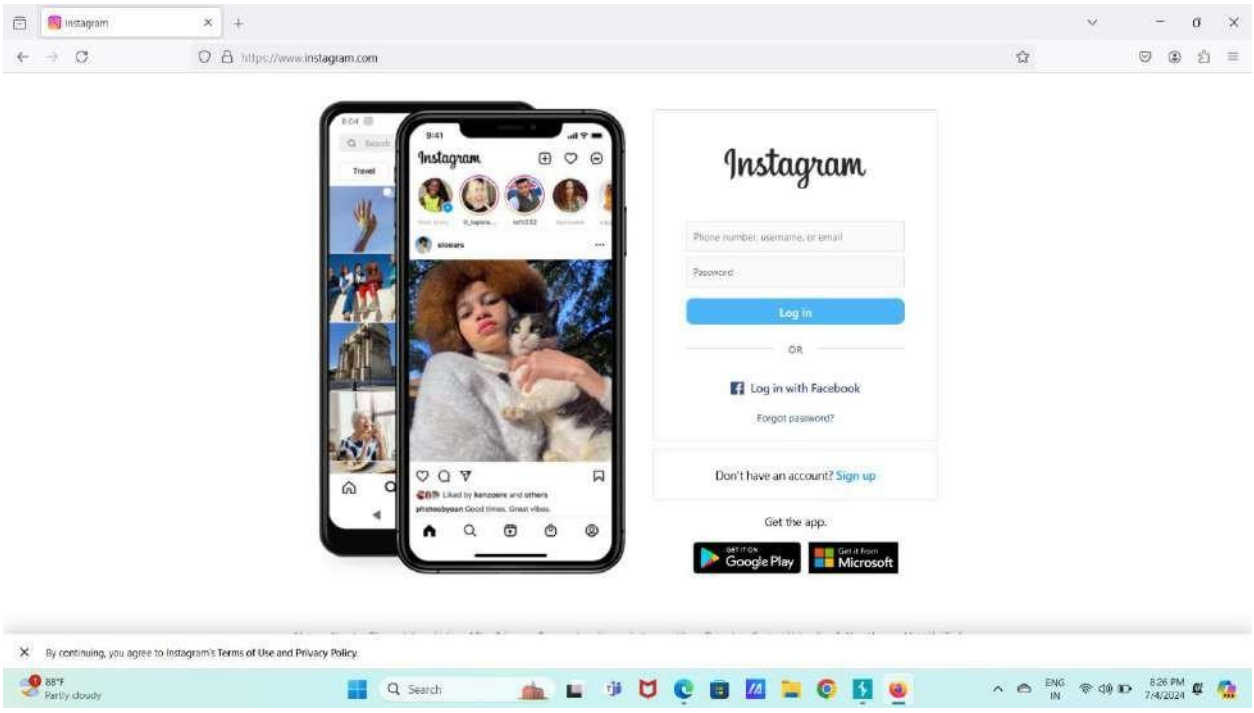

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.3.1.4 - Temporary P...
Dashboard Target Intruder Proxy Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Learn
Intercept HTTP history WebSockets history Proxy settings
Request to https://www.facebook.com:443 [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=
OrmUnbdgmhs57s02F..BmgéJ1..AAA.0.0.BmhrXi.AWVanbnzIjk; sb=
daKDZjj9JBym0j_TaVMmvWE1; 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
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 7
Request headers 22
Search 0 highlights
Event log (9) All issues
Memory: 1.46GB
ENG IN 8:17 PM 7/4/2024

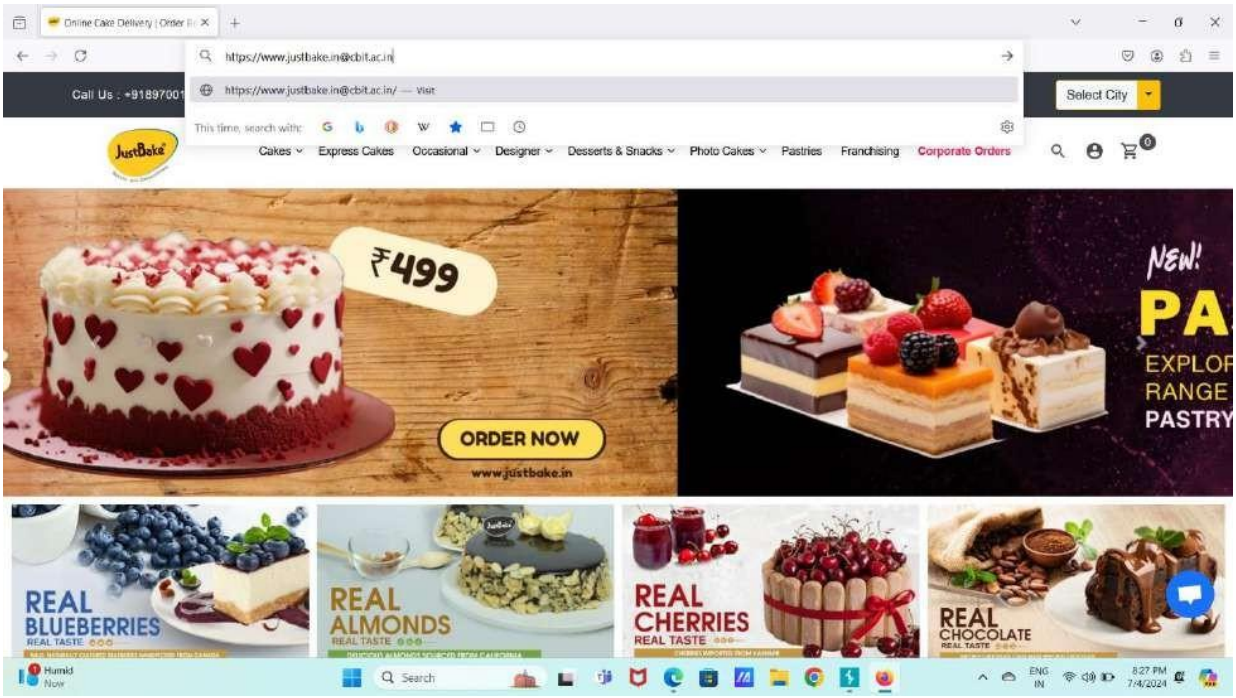

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.3.1.4 - Temporary P...
Dashboard Target Intruder Proxy Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Learn
Intercept HTTP history WebSockets history Proxy settings
Request to https://www.facebook.com:443 [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=
OrmUnbdgmhs57s02F..BmgéJ1..AAA.0.0.BmhrXi.AWVanbnzIjk; sb=
daKDZjj9JBym0j_TaVMmvWE1; 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
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 7
Request headers 22
Search 0 highlights



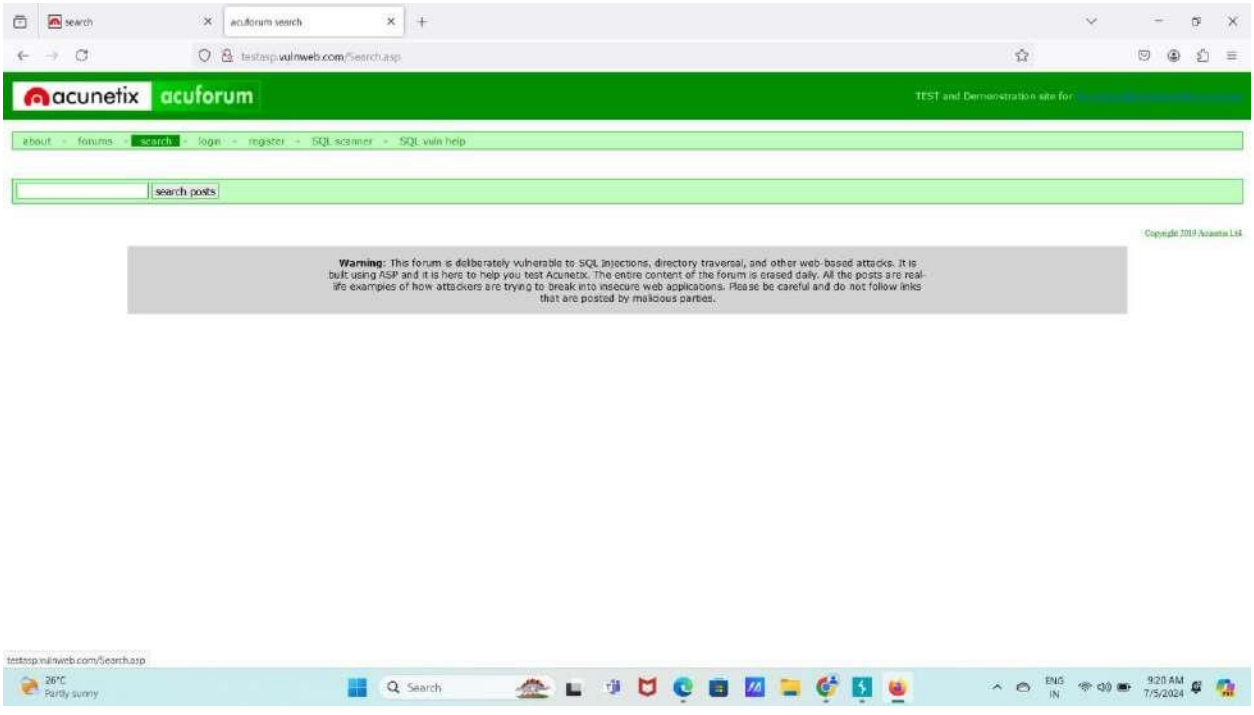
B. Find 2 websites that are vulnerable to Open Redirect / URL Redirection Vulnerability.

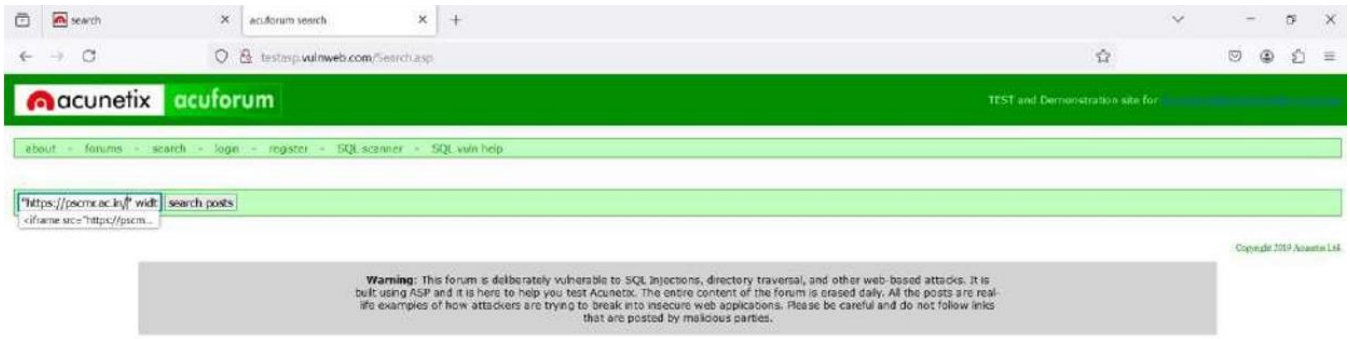


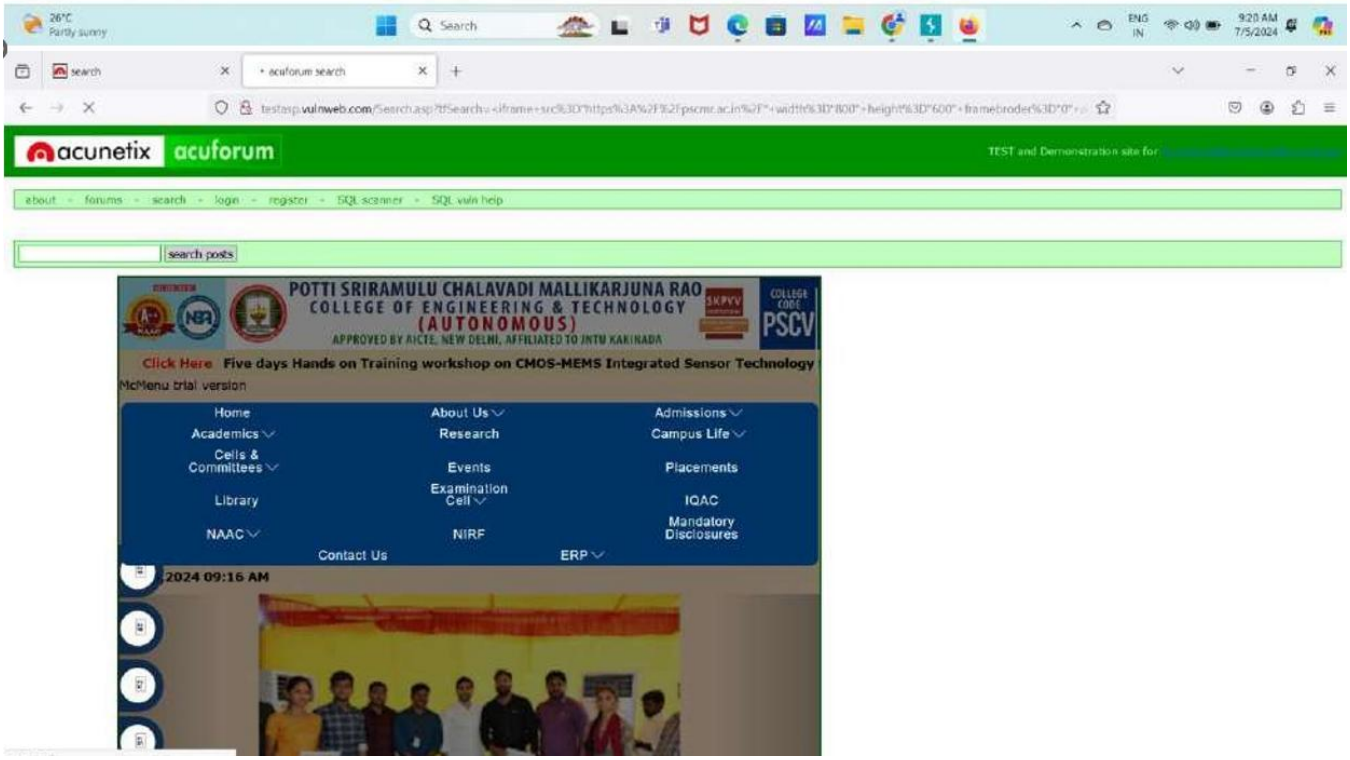

Instagram
https://www.instagram.com
Instagram
Phone number, username, or email
Password
Log in
OR
Log in with Facebook
Forgot password?
Don't have an account? Sign up
Get the app.
Google Play
Microsoft
By continuing, you agree to Instagram's Terms of Use and Privacy Policy.
Search


https://www.justbake.in@cbit.ac.in
Call Us : +91897001
Select City
JustBake
Cakes
Express Cakes
Occasional
Designer
Desserts & Snacks
Photo Cakes
Pastries
Franchising
Corporate Orders
₹499
ORDER NOW
www.justbake.in
NEW!
REAL BLUEBERRIES
REAL ALMONDS
REAL CHERRIES
REAL CHOCOLATE
Search

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



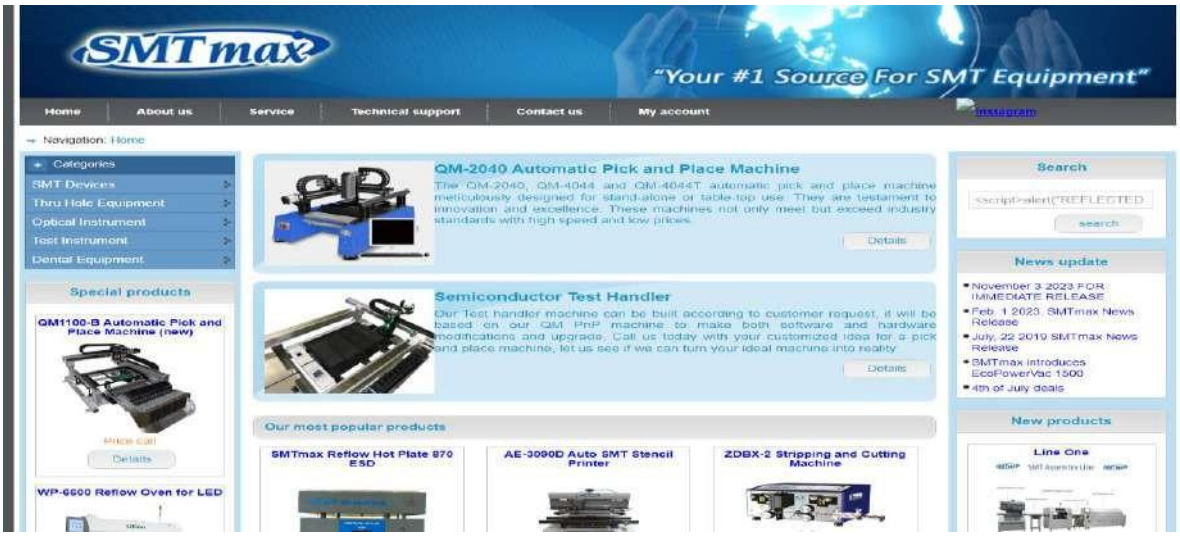

search
acuforum search
testasp.vulnweb.com/Search.asp
acunetix
acuforum
TEST and Demonstration site for
about - forums - search - login - register - SQL scanner - SQL vuln help
"https://pscmr.ac.in/" widt
search posts
<iframe src="https://pscm...
Copyright 2019 Acunetix Ltd
Warning: This forum is deliberately 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.

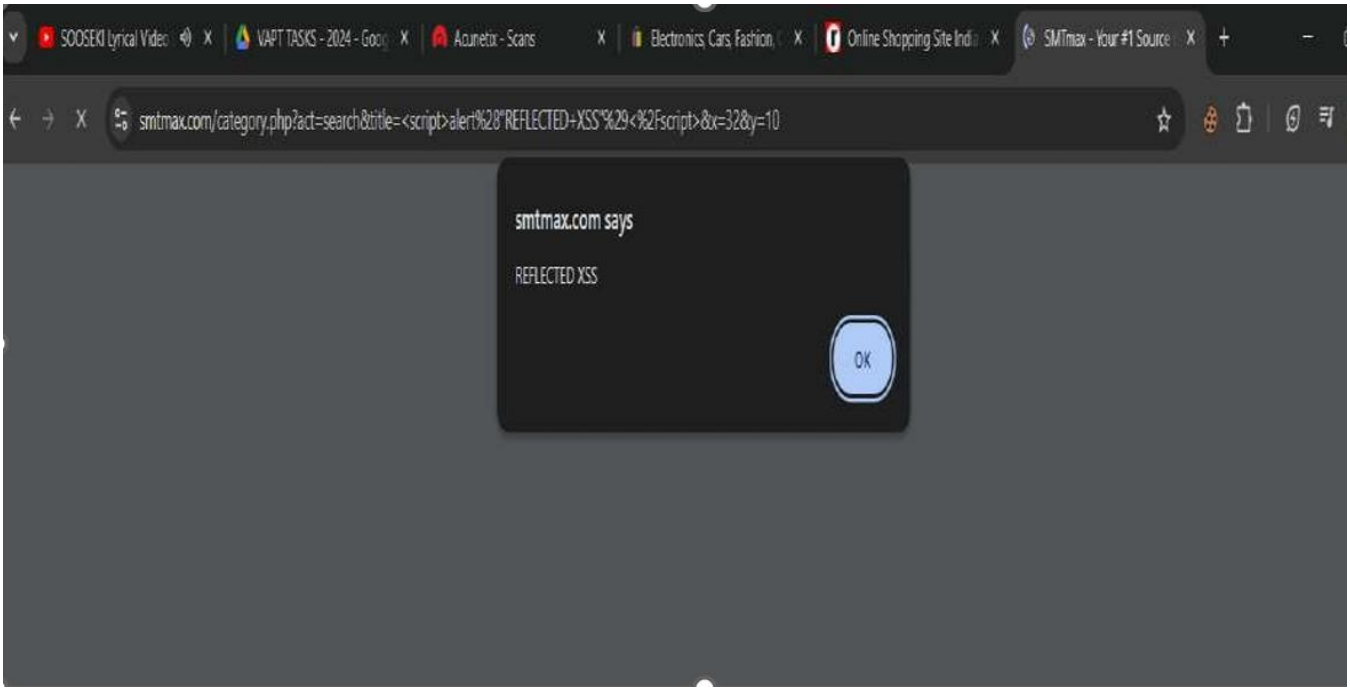

26°C
Partly sunny
Search
ENG
IN
9:20 AM
7/5/2024
search
acuforum search
testasp.vulnweb.com/Search.asp?tfSearch=<iframe+src%3D"https%3A%2F%2Fpscmr.ac.in%2F"+width%3D"800"+height%3D"600"+frameborder%3D"0"+
acunetix
acuforum
TEST and Demonstration site for
about - forums - search - login - register - SQL 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
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

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