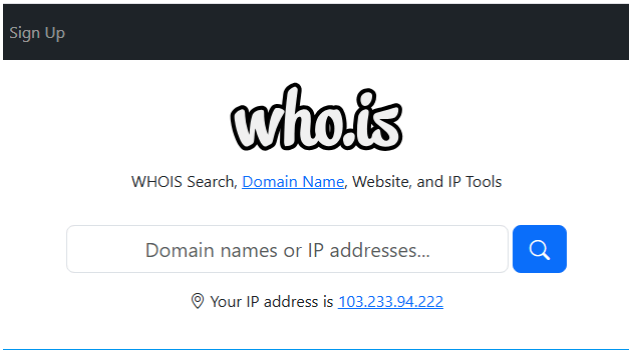
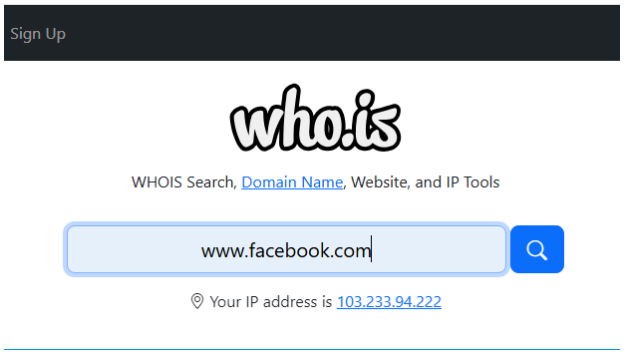
Practical 01

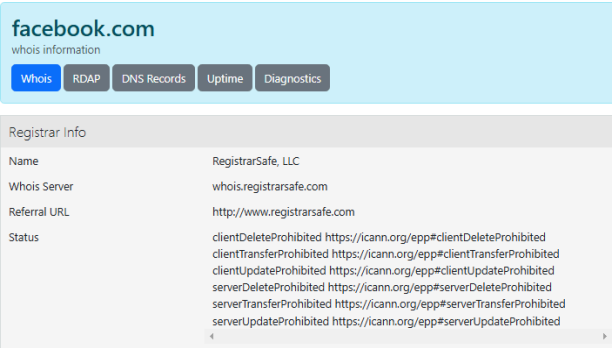
Step 01: Open the WHO.is website.



Step 02: Enter the website name and hit “Enter Button”.

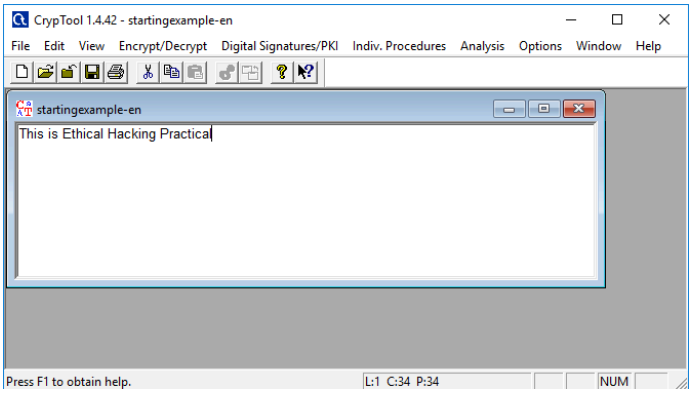


Step 03: It will show you information about the website.

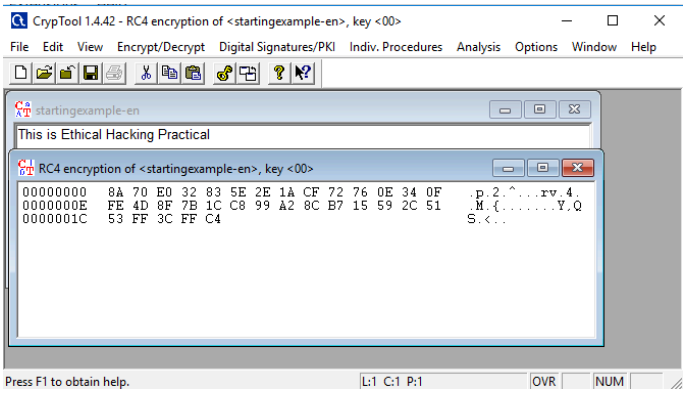


Practical 02

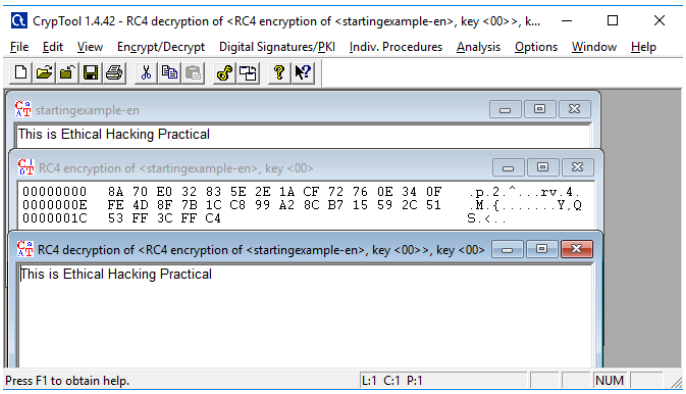
<u>Step 01:</u> Enter the text you want to encrypt.



<u>Step 02:</u> Select the RC4 algorithm from the above “Encrypt/Decrypt” option for Encryption.



<u>Step 03:</u> Use RC4 algorithm for Decryption.



Practical 03

Step 01: Open cmd and type “tracert” command and type “www.facebook.com”.

```
Command Prompt
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Admin>tracert www.facebook.com

Tracing route to star-mini.c10r.facebook.com [57.144.124.1]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2     1 ms    <1 ms    <1 ms  10.10.200.6
  3     1 ms     *        *     103.87.164.1
  4    35 ms    13 ms     2 ms  ae19.pr03.bom1.tfbnw.net [157.240.68.32]
  5     2 ms     2 ms     2 ms  po207.asw01.bom2.tfbnw.net [129.134.51.4]
  6     1 ms     1 ms     1 ms  psw01.bom2.tfbnw.net [129.134.59.154]
  7     4 ms     5 ms     3 ms  163.77.193.125
  8     2 ms     1 ms     1 ms  edge-star-mini-shv-03-bom2.facebook.com [57.144.124.1]

Trace complete.

C:\Users\Admin>_
```

Step 02: Ping few IP addresses of “facebook.com”.

```
C:\Users\Admin>ping 129.134.31.12

Pinging 129.134.31.12 with 32 bytes of data:
Reply from 129.134.31.12: bytes=32 time=2ms TTL=51
Reply from 129.134.31.12: bytes=32 time=2ms TTL=51
Reply from 129.134.31.12: bytes=32 time=2ms TTL=51
Reply from 129.134.31.12: bytes=32 time=3ms TTL=51

Ping statistics for 129.134.31.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\Admin>ping 185.89.218.12

Pinging 185.89.218.12 with 32 bytes of data:
Reply from 185.89.218.12: bytes=32 time=21ms TTL=48
Reply from 185.89.218.12: bytes=32 time=21ms TTL=48
Reply from 185.89.218.12: bytes=32 time=21ms TTL=48
Reply from 185.89.218.12: bytes=32 time=24ms TTL=48

Ping statistics for 185.89.218.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum = 24ms, Average = 21ms
```

Step 03: “Netstat” command.

Command Prompt

```
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Admin>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.75:49672     20.198.118.190:https   ESTABLISHED
  TCP    192.168.1.75:50105     a23-54-82-234:https    LAST_ACK
  TCP    192.168.1.75:50111     a23-212-160-83:https   CLOSE_WAIT
  TCP    192.168.1.75:50112     104.18.5.159:https     TIME_WAIT
  TCP    192.168.1.75:50116     104.17.254.239:https   TIME_WAIT
  TCP    192.168.1.75:50125     server-108-159-80-47:https  TIME_WAIT
  TCP    192.168.1.75:50131     a23-9-218-94:https     ESTABLISHED
  TCP    192.168.1.75:50132     a23-54-82-234:https    ESTABLISHED

C:\Users\Admin>
```

Step 04: “ifconfig” command.

kali@kali: ~

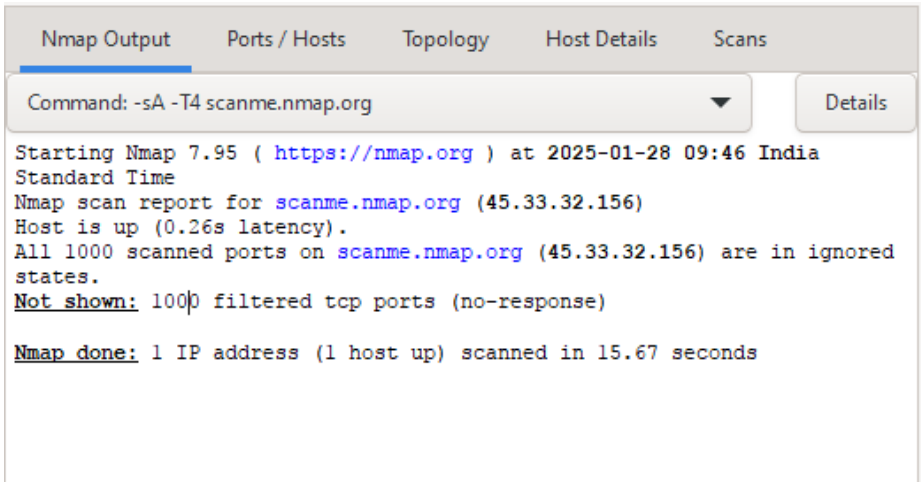
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::8dc6:8056:e98e:fbce  prefixlen 64  scopeid 0x20<link>
        inet6 fd00::dc70:55e0:5da:77ea  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:6e:13:6e  txqueuelen 1000  (Ethernet)
        RX packets 8  bytes 3486 (3.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 4463 (4.3 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 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ sS
```

Practical 04

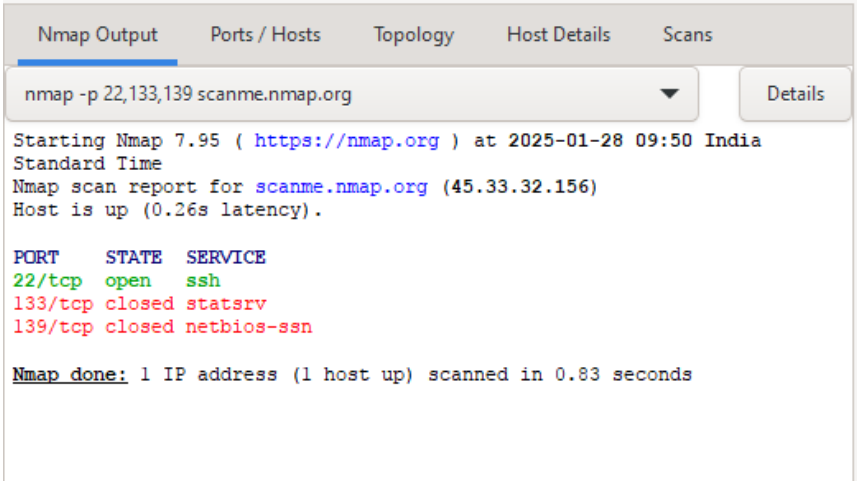
Step 01: ACK -sA (TCP ACK scan)

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



Step 02: SYN(Stealth) Scan (-sS)

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



Step 03: FIN Scan (-sF)

Command: nmap -sF -T4 para

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

nmap -sF -T4 scanme.nmap.org | Details

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-28 09:52 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 16.23 seconds
```

Step 04: NULL Scan (-sN)

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

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

nmap -sN -p 22 scanme.nmap.org | Details

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-28 09:53 India
Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).

PORT    STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 3.00 seconds
```

Step 05: XMAS Scan (-sX)

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

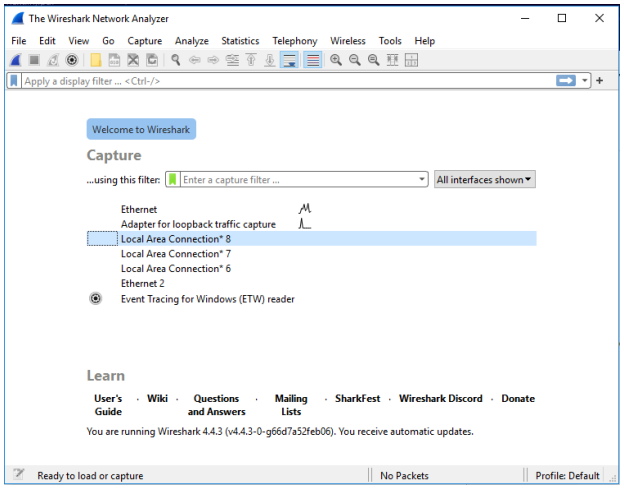
Nmap Output | Ports / Hosts | Topology | Host Details | Scans

nmap -sX -T4 scanme.nmap.org | Details

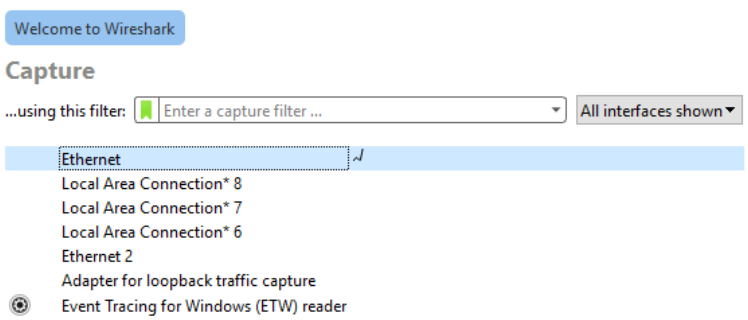
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-28 09:56 India
Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored
states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 18.09 seconds
```

Practical 05

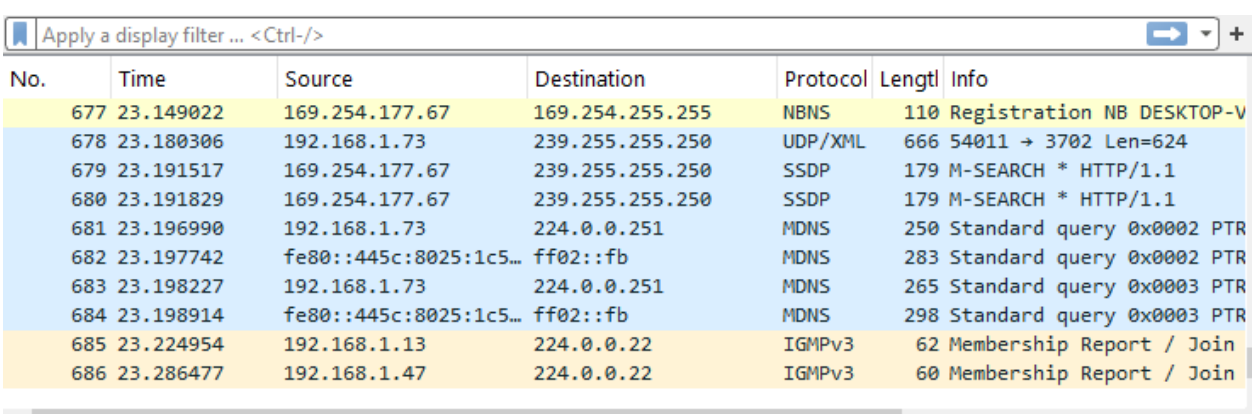
Step 01: Install and Open Wireshark.



Step 02: Select your wired network from the list.

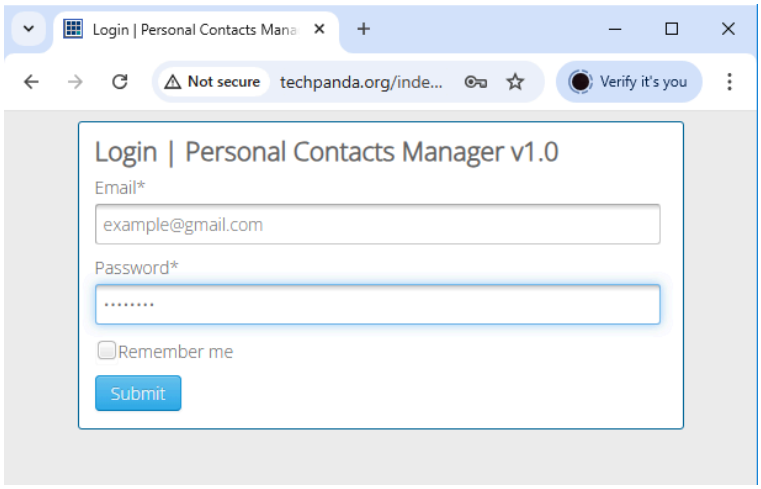


Step 03: The source, Destination and protocols of the packets in the LAN network are displayed.

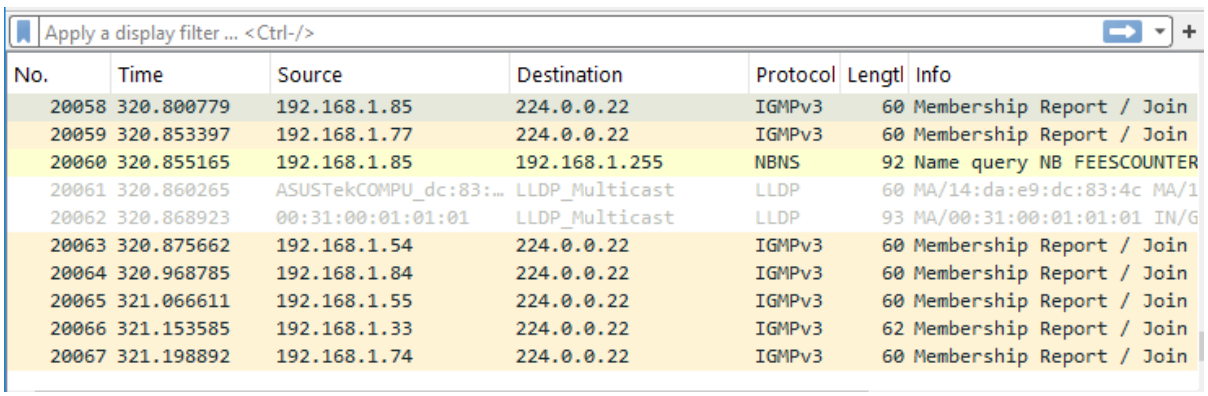


No.	Time	Source	Destination	Protocol	Lengtl	Info
677	23.149022	169.254.177.67	169.254.255.255	NBNS	110	Registration NB DESKTOP-V
678	23.180306	192.168.1.73	239.255.255.250	UDP/XML	666	54011 → 3702 Len=624
679	23.191517	169.254.177.67	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
680	23.191829	169.254.177.67	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
681	23.196990	192.168.1.73	224.0.0.251	MDNS	250	Standard query 0x0002 PTR
682	23.197742	fe80::445c:8025:1c5…	ff02::fb	MDNS	283	Standard query 0x0002 PTR
683	23.198227	192.168.1.73	224.0.0.251	MDNS	265	Standard query 0x0003 PTR
684	23.198914	fe80::445c:8025:1c5…	ff02::fb	MDNS	298	Standard query 0x0003 PTR
685	23.224954	192.168.1.13	224.0.0.22	IGMPv3	62	Membership Report / Join
686	23.286477	192.168.1.47	224.0.0.22	IGMPv3	60	Membership Report / Join

Step 04: Open a ‘http’ website and enter id and password.

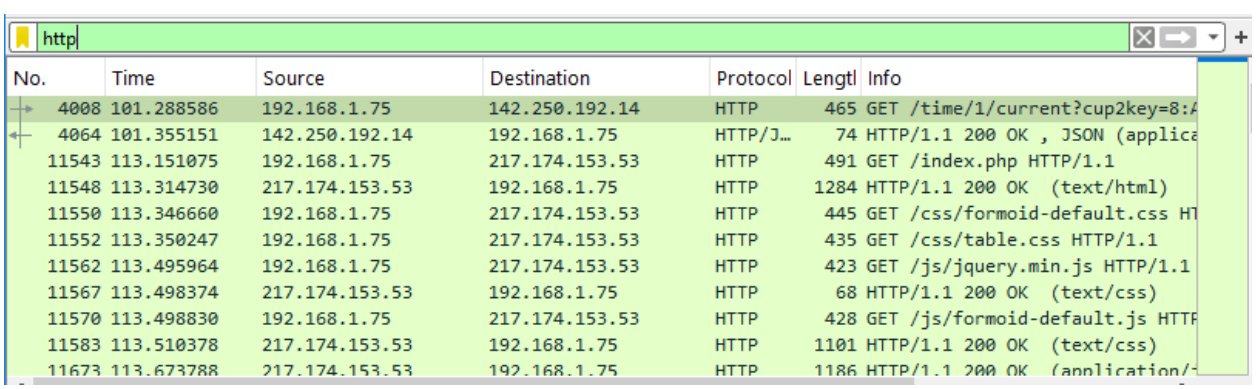


Step 05: The wireshark tool will keep recording the packets.



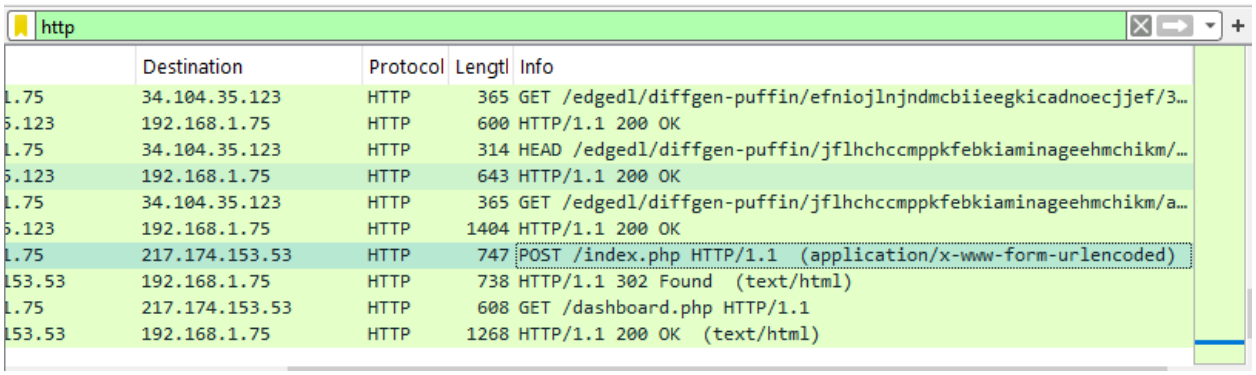
No.	Time	Source	Destination	Protocol	Lengtl	Info
20058	320.800779	192.168.1.85	224.0.0.22	IGMPv3	60	Membership Report / Join
20059	320.853397	192.168.1.77	224.0.0.22	IGMPv3	60	Membership Report / Join
20060	320.855165	192.168.1.85	192.168.1.255	NBNS	92	Name query NB FEESCOUNTER
20061	320.860265	ASUSTekCOMPU_dc:83:…	LLDP_Multicast	LLDP	60	MA/14:da:e9:dc:83:4c MA/1
20062	320.868923	00:31:00:01:01:01	LLDP_Multicast	LLDP	93	MA/00:31:00:01:01:01 IN/G
20063	320.875662	192.168.1.54	224.0.0.22	IGMPv3	60	Membership Report / Join
20064	320.968785	192.168.1.84	224.0.0.22	IGMPv3	60	Membership Report / Join
20065	321.066611	192.168.1.55	224.0.0.22	IGMPv3	60	Membership Report / Join
20066	321.153585	192.168.1.33	224.0.0.22	IGMPv3	62	Membership Report / Join
20067	321.198892	192.168.1.74	224.0.0.22	IGMPv3	60	Membership Report / Join

Step 06: Select http as filter and stop recording.



No.	Time	Source	Destination	Protocol	Lengtl	Info
4008	101.288586	192.168.1.75	142.250.192.14	HTTP	465	GET /time/1/current?cup2key=8:A
4064	101.355151	142.250.192.14	192.168.1.75	HTTP/J…	74	HTTP/1.1 200 OK , JSON (applica
11543	113.151075	192.168.1.75	217.174.153.53	HTTP	491	GET /index.php HTTP/1.1
11548	113.314730	217.174.153.53	192.168.1.75	HTTP	1284	HTTP/1.1 200 OK (text/html)
11550	113.346660	192.168.1.75	217.174.153.53	HTTP	445	GET /css/formoid-default.css HT
11552	113.350247	192.168.1.75	217.174.153.53	HTTP	435	GET /css/table.css HTTP/1.1
11562	113.495964	192.168.1.75	217.174.153.53	HTTP	423	GET /js/jquery.min.js HTTP/1.1
11567	113.498374	217.174.153.53	192.168.1.75	HTTP	68	HTTP/1.1 200 OK (text/css)
11570	113.498830	192.168.1.75	217.174.153.53	HTTP	428	GET /js/formoid-default.js HTTP
11583	113.510378	217.174.153.53	192.168.1.75	HTTP	1101	HTTP/1.1 200 OK (text/css)
11673	113.673788	217.174.153.53	192.168.1.75	HTTP	1186	HTTP/1.1 200 OK (application/

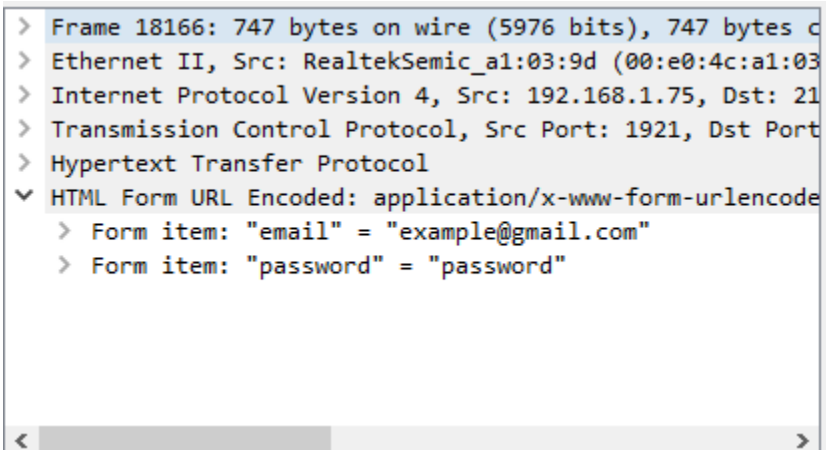
Step 07: Find the POST method for username and password.



http

	Destination	Protocol	Lengtl	Info
1.75	34.104.35.123	HTTP	365	GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/3…
5.123	192.168.1.75	HTTP	600	HTTP/1.1 200 OK
1.75	34.104.35.123	HTTP	314	HEAD /edgedl/diffgen-puffin/jflhchccmppkfebkiaminageehmchikm/…
5.123	192.168.1.75	HTTP	643	HTTP/1.1 200 OK
1.75	34.104.35.123	HTTP	365	GET /edgedl/diffgen-puffin/jflhchccmppkfebkiaminageehmchikm/a…
5.123	192.168.1.75	HTTP	1404	HTTP/1.1 200 OK
1.75	217.174.153.53	HTTP	747	POST /index.php HTTP/1.1 (application/x-www-form-urlencoded)
153.53	192.168.1.75	HTTP	738	HTTP/1.1 302 Found (text/html)
1.75	217.174.153.53	HTTP	608	GET /dashboard.php HTTP/1.1
153.53	192.168.1.75	HTTP	1268	HTTP/1.1 200 OK (text/html)

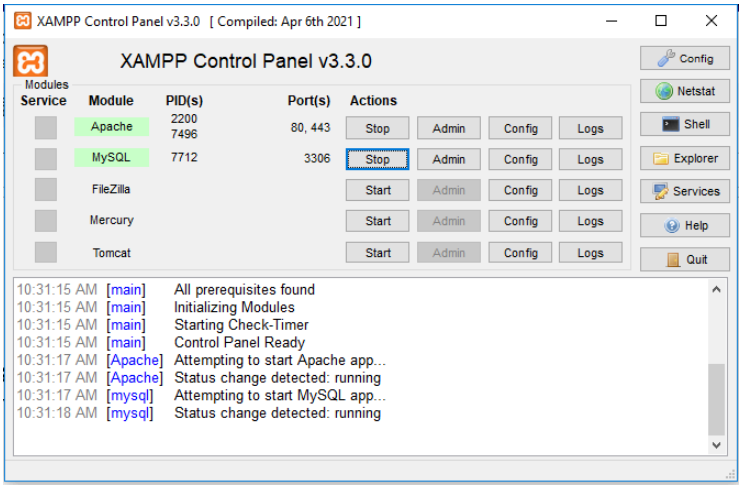
Step 08: U will see the email- id and password that was used to login.



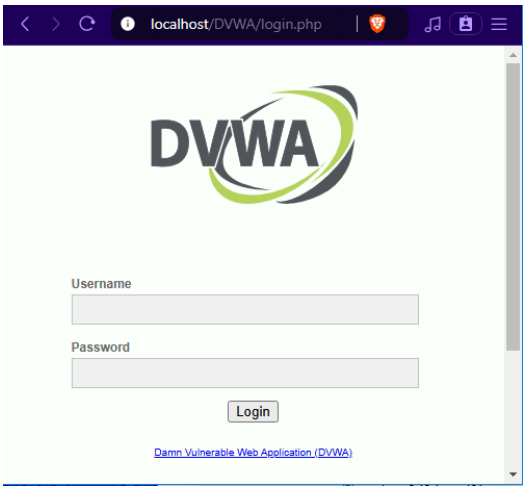
```
> Frame 18166: 747 bytes on wire (5976 bits), 747 bytes c
> Ethernet II, Src: RealtekSemic_a1:03:9d (00:e0:4c:a1:03
> Internet Protocol Version 4, Src: 192.168.1.75, Dst: 21
> Transmission Control Protocol, Src Port: 1921, Dst Port
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencode
  > Form item: "email" = "example@gmail.com"
  > Form item: "password" = "password"
```

Practical 06

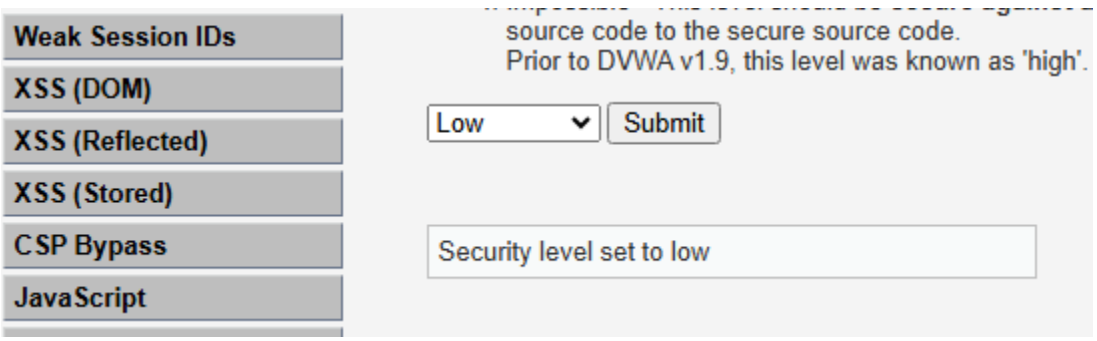
Step 01: Install and Run XAMPP, DVWA and run Apache and MySQL in XAMPP.



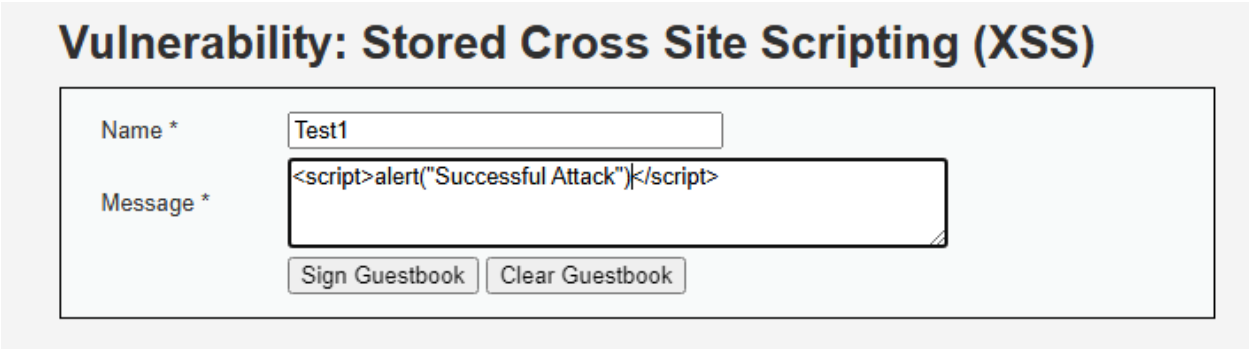
Step 02: Enter " localhost/DVWA/login.php" in a web browser.



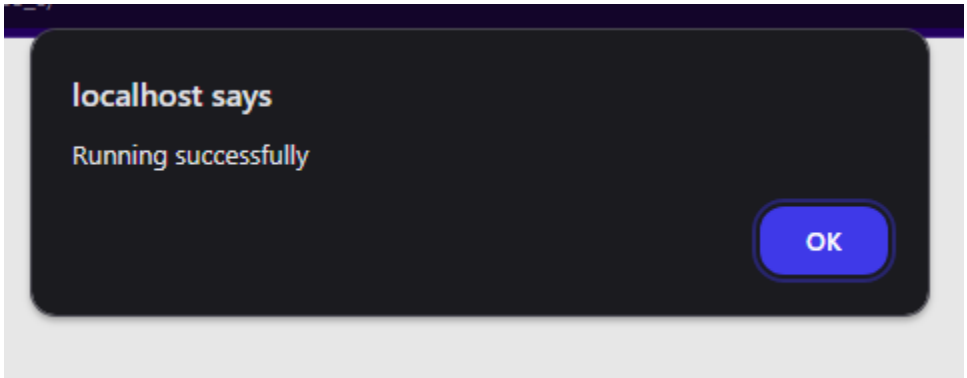
Step 03: After login, go to DVWA Security and set security to "low".



Step 04: Click on XSS(Stored) and type any name and type and type the script you want to inject.

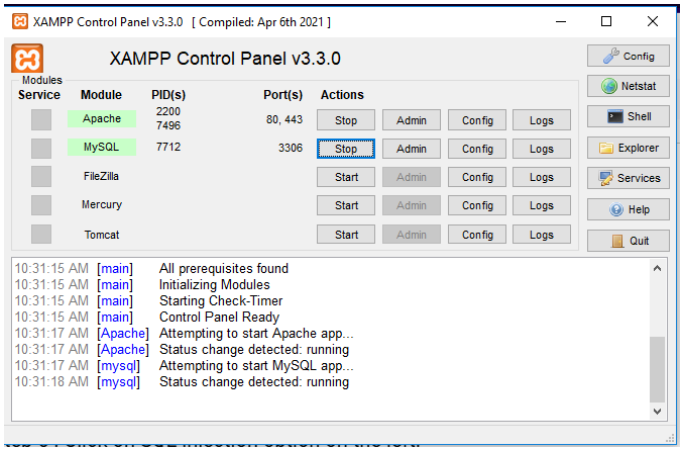


Step 05: The script you enter will be shown.

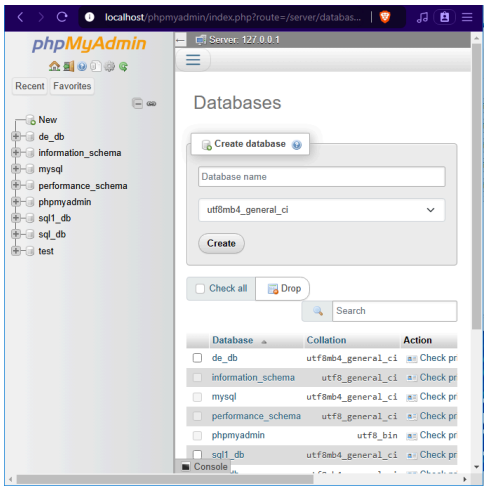


Practical 08

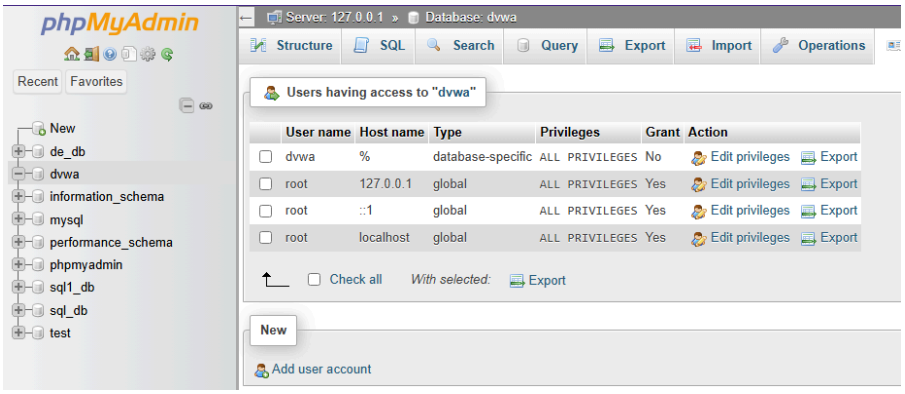
Step 01: Open XAMPP and run Apache and MySQL.



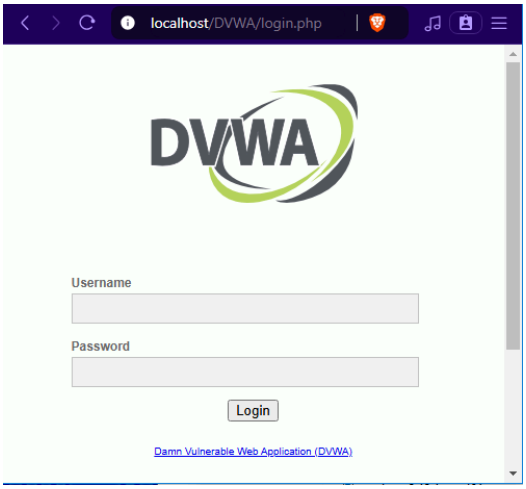
Step 02: Go to the web browser and enter the site localhost/phpmyadmin.



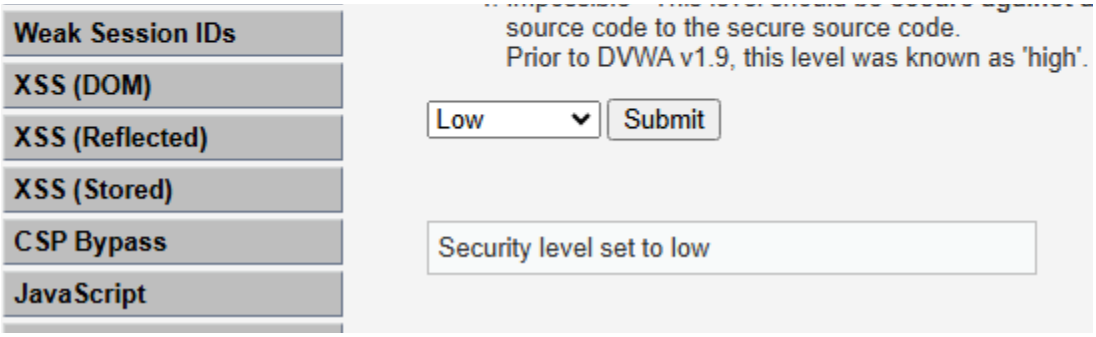
Step 03: Create a database with the name DVWA.



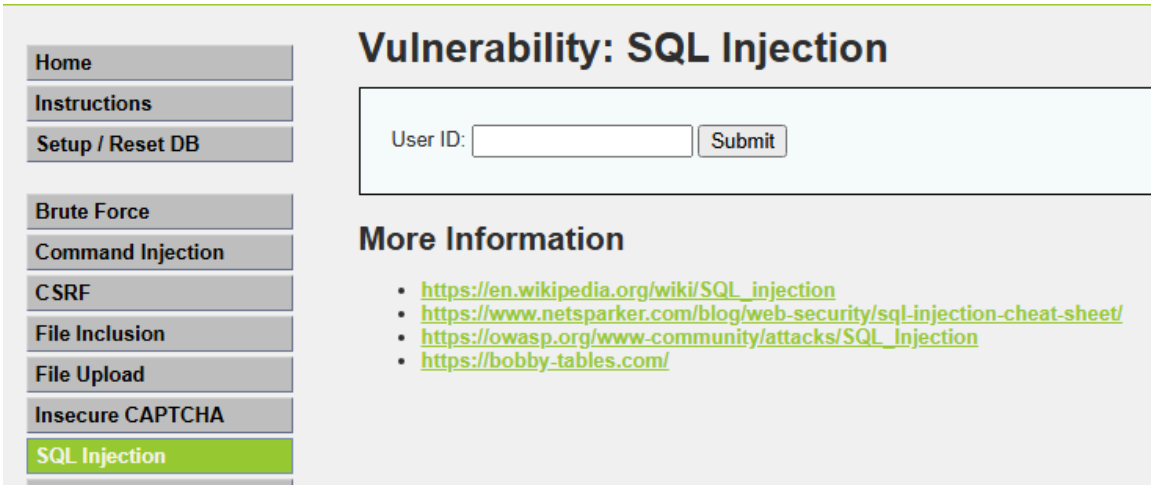
Step 04: Go to site localhost/dvwa/ then login.



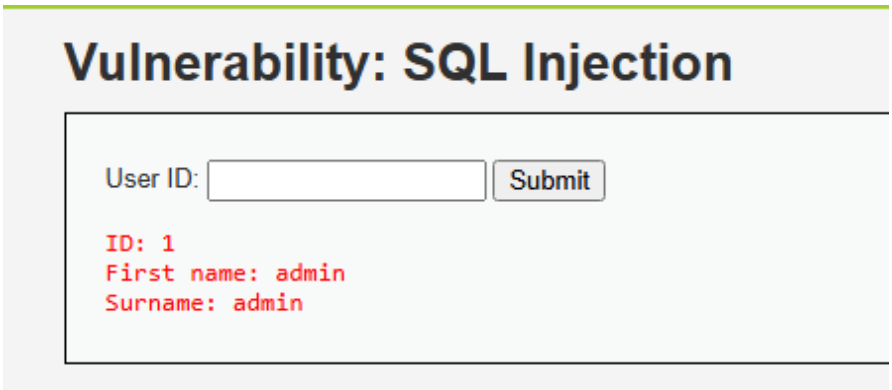
Step 05: Go to the security setting option on the left and set the security level low.



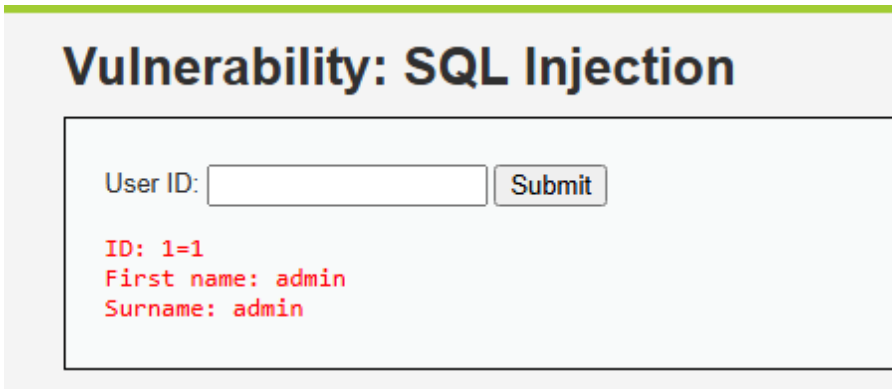
Step 06: Click on SQL injection option on the left.



Step 07: Write "1" in the text box and click on submit.



Step 08: Write "1=1" in the text box and click on submit.



Step 10: Write "1*" in the text box and click on submit.