Index

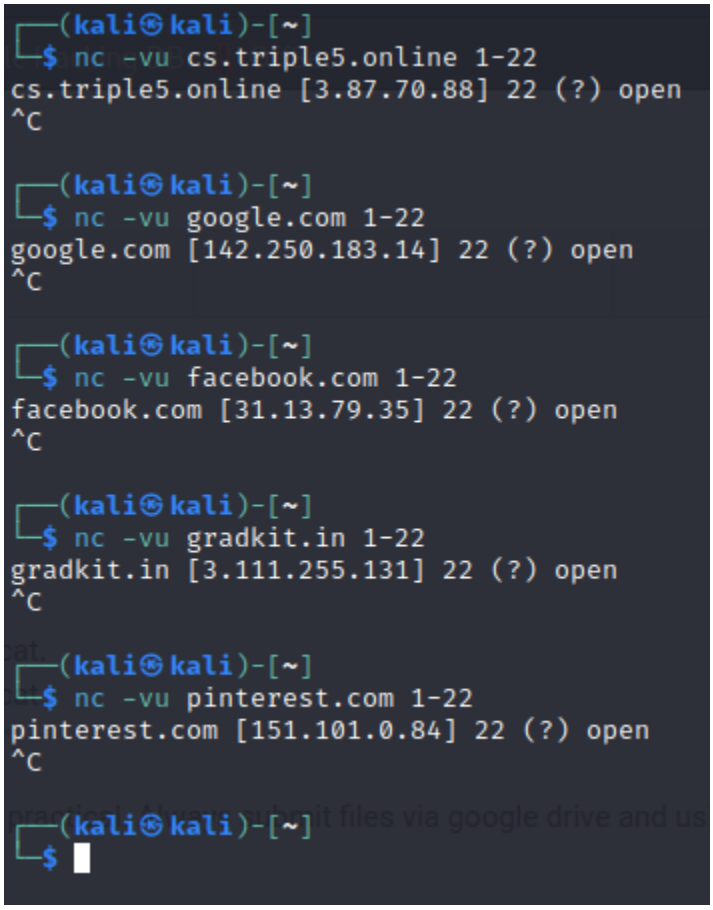
Assignment - 1

Ping at least 5 websites on the internet

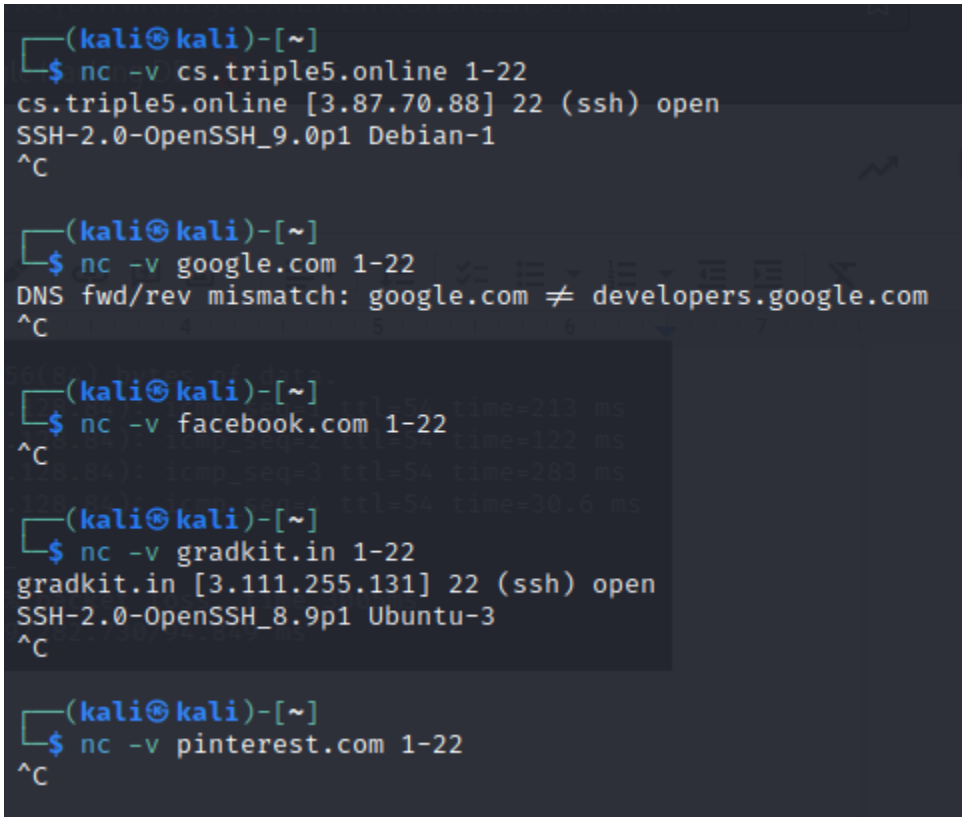
```
┌──(kali㉿kali)-[~]
└─$ ping google.com
PING google.com (142.250.77.78) 56(84) bytes of data.
64 bytes from google.com (142.250.77.78): icmp_seq=1 ttl=117 time=195 ms
64 bytes from google.com (142.250.77.78): icmp_seq=2 ttl=117 time=152 ms
64 bytes from google.com (142.250.77.78): icmp_seq=3 ttl=117 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 ──
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.



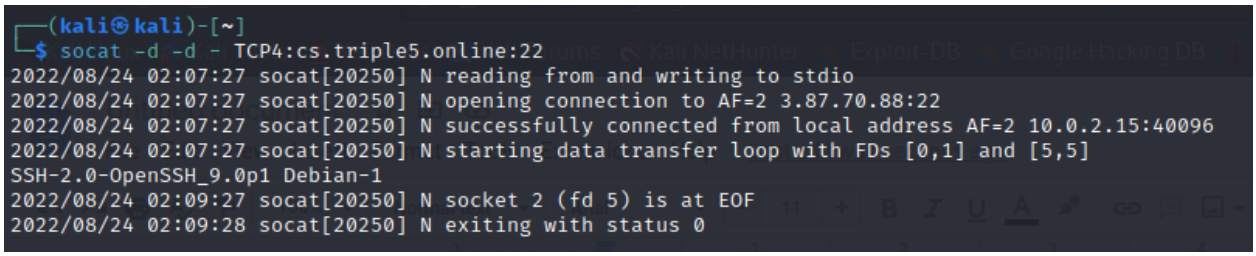
Perform TCP Scan on any Five Hosts and scan port numbers 1-20 with netcat.



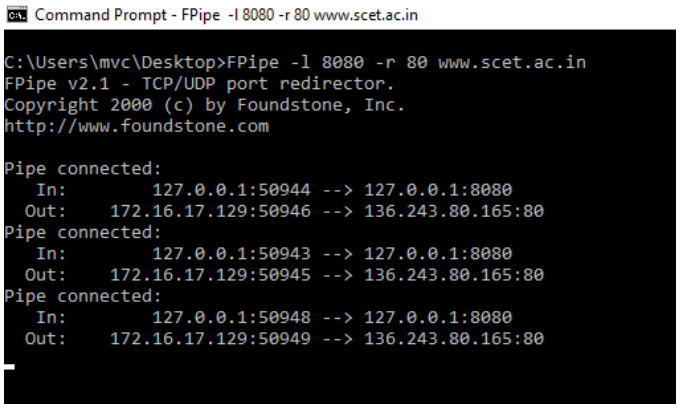
Scan port numbers 80 and 22 of any Five Hosts by giving them input "QUIT".

Assignment - 2

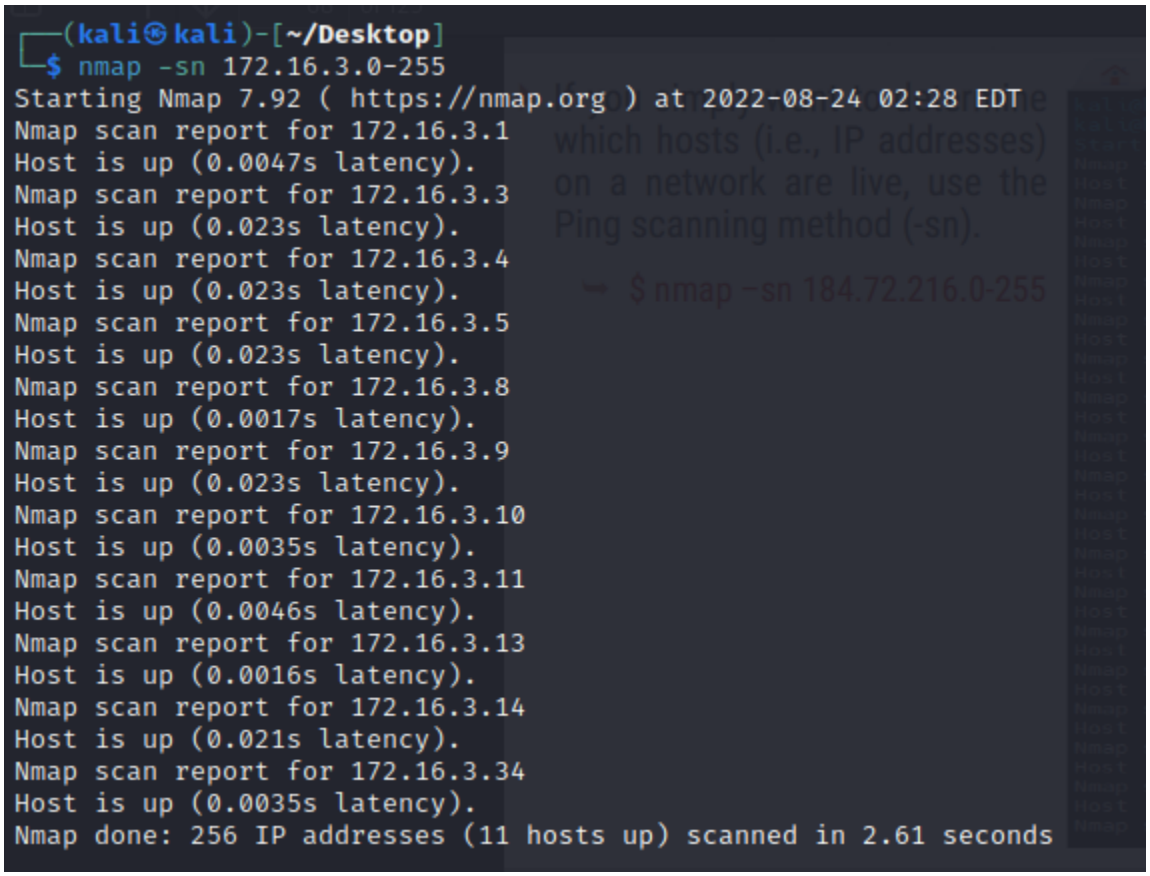
1. Demonstrate the working socat tool



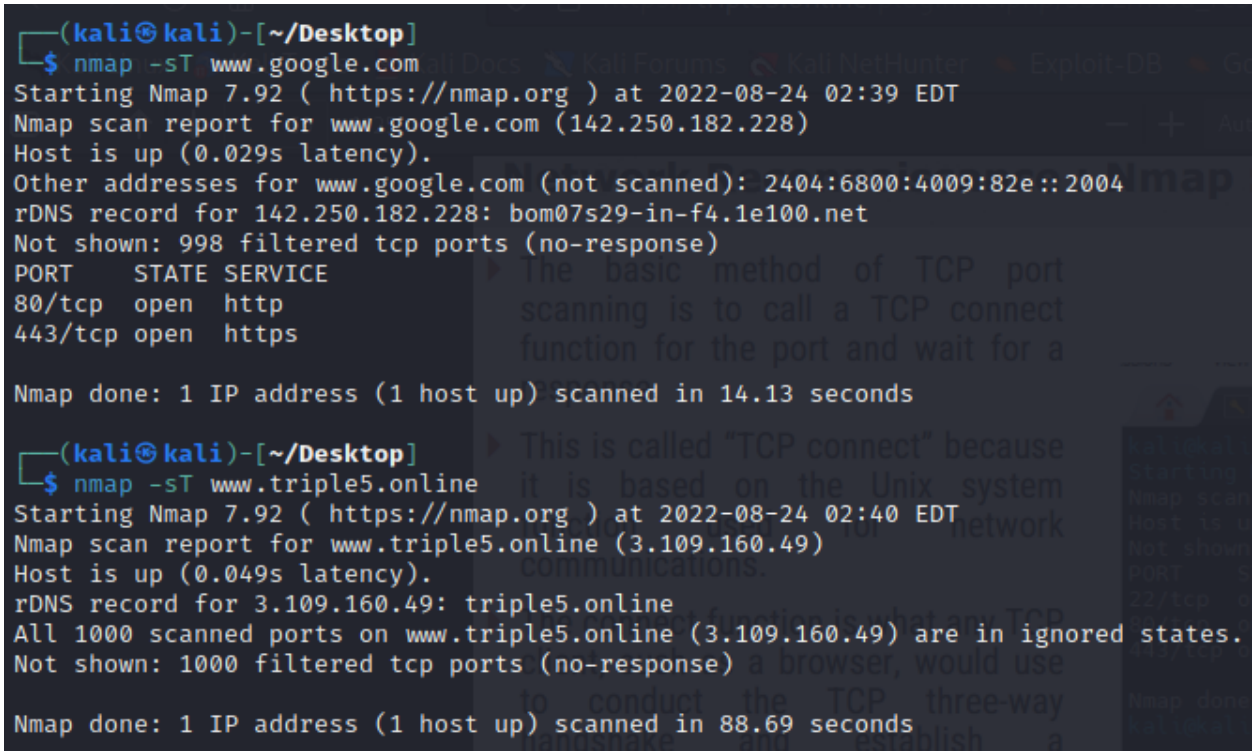
2. Perform port forwarding using Fpipe



3. Identify which hosts are live on the network

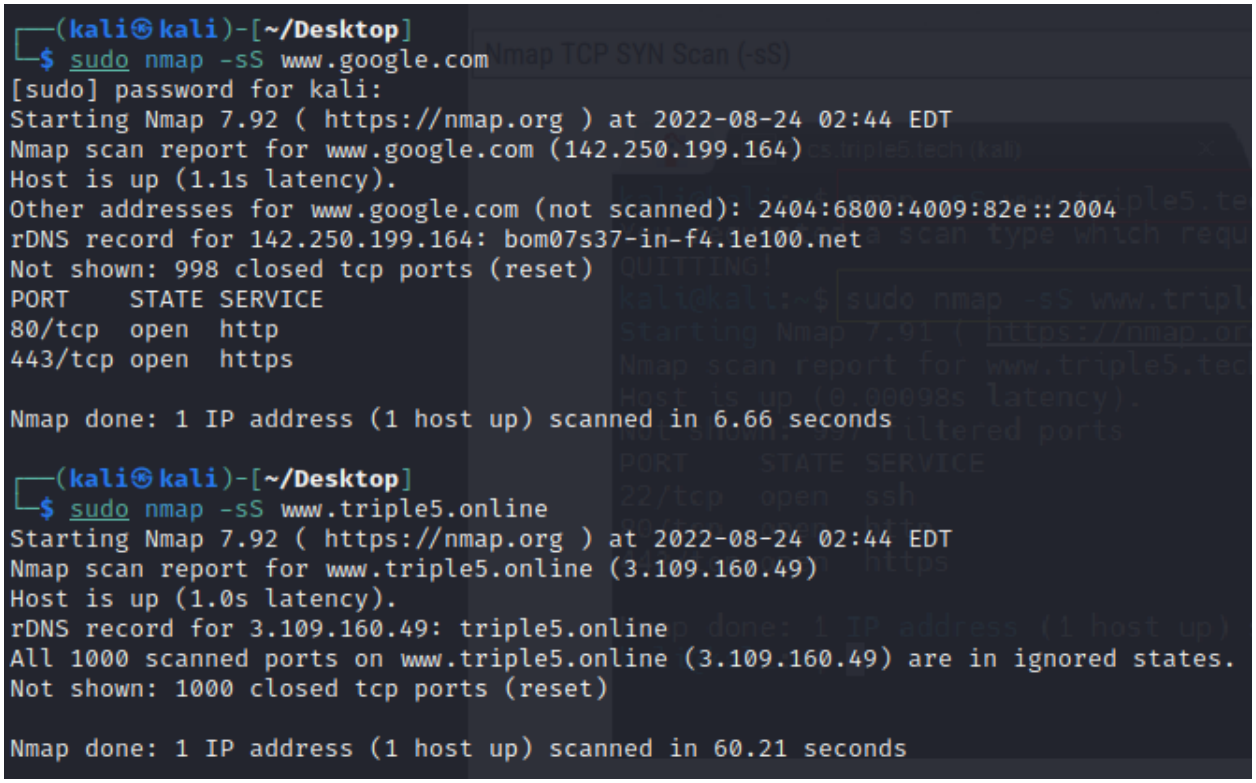


4. Scan all TCP Port of the any two hosts

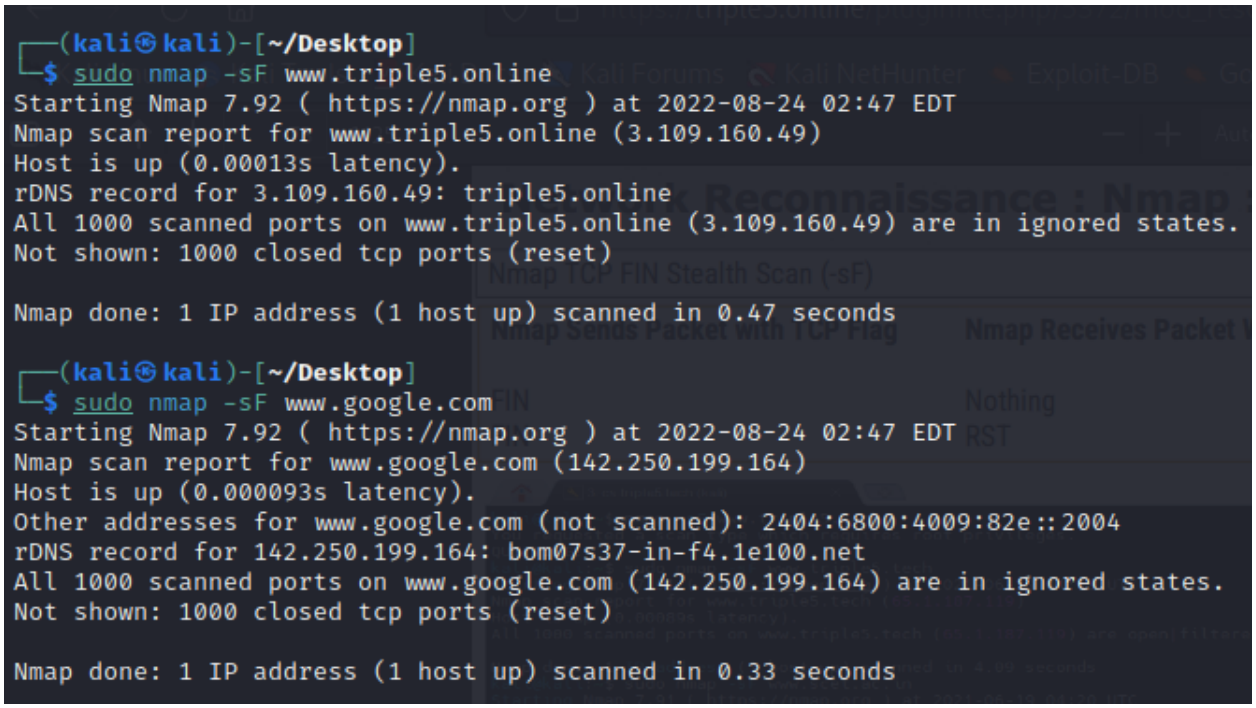


```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sT www.google.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-24 02:39 EDT
Nmap scan report for www.google.com (142.250.182.228)
Host is up (0.029s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82e::2004
rDNS record for 142.250.182.228: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



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).
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
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
```

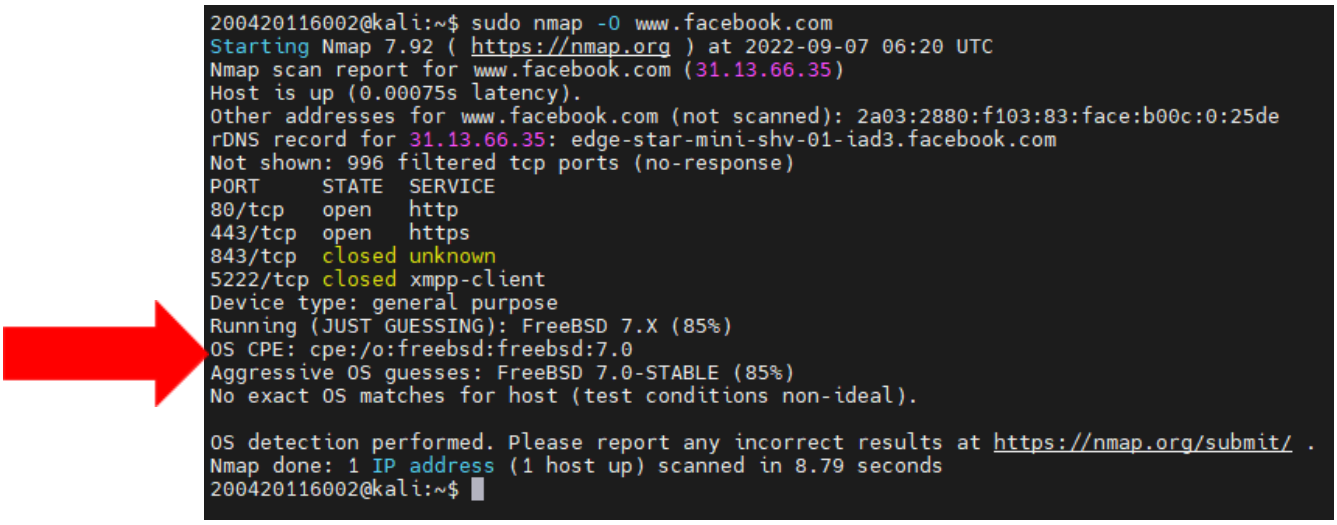
```
41       open|filtered ipv6
42       open          sdrp
43       open          ipv6-route
44       open          ipv6-frag
45       open          idrp
46       open          rsvp
47       open          gre
48       open          dsp
49       open          bna
50       open          esp
51       open          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
```

```
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
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          vrrp
113     open          pgm
114     open          any0hop
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          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
```

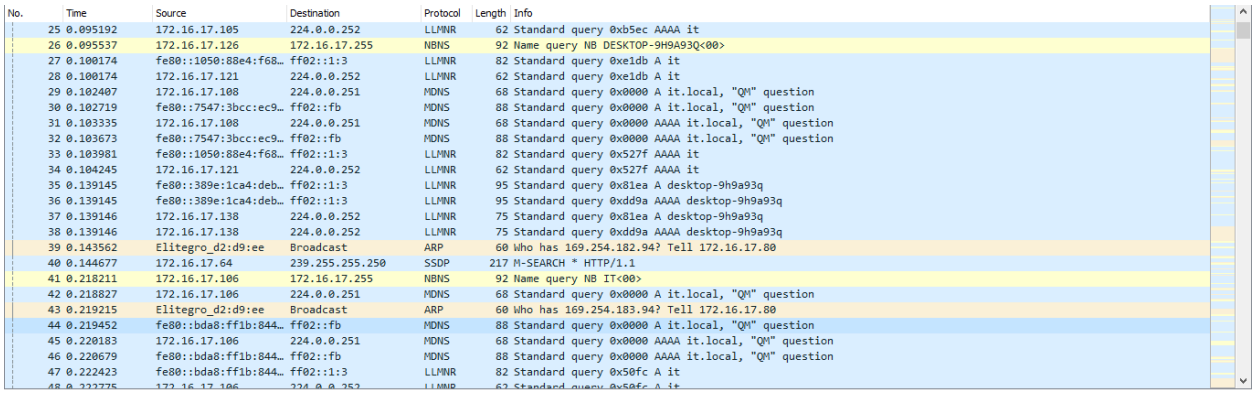
2. Determine which services are available on the host www.scet.ac.in

```
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

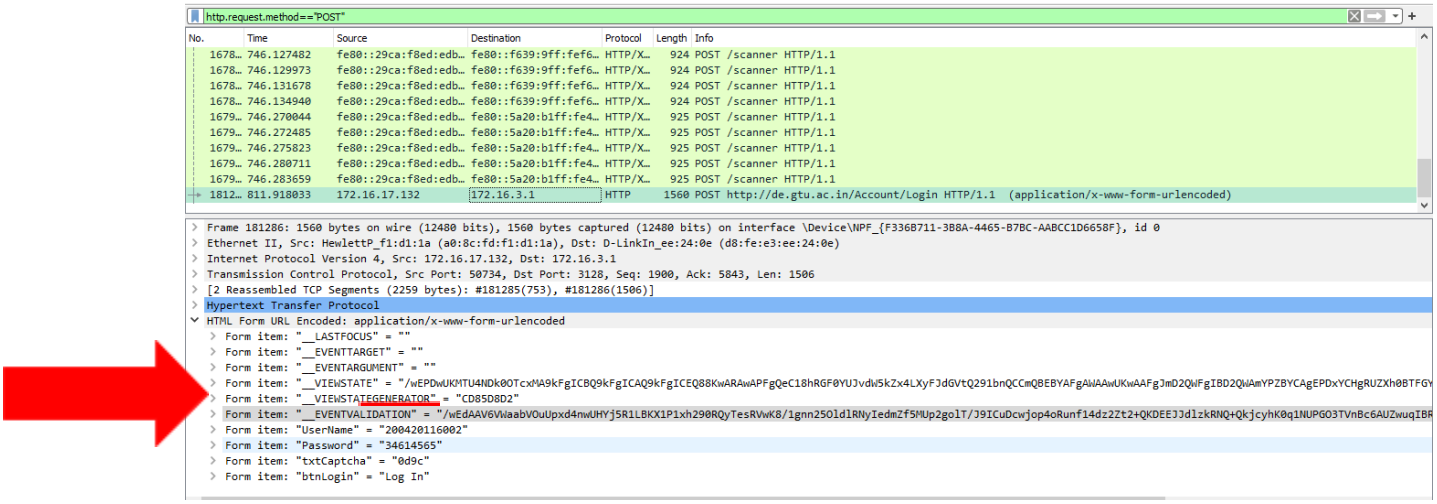


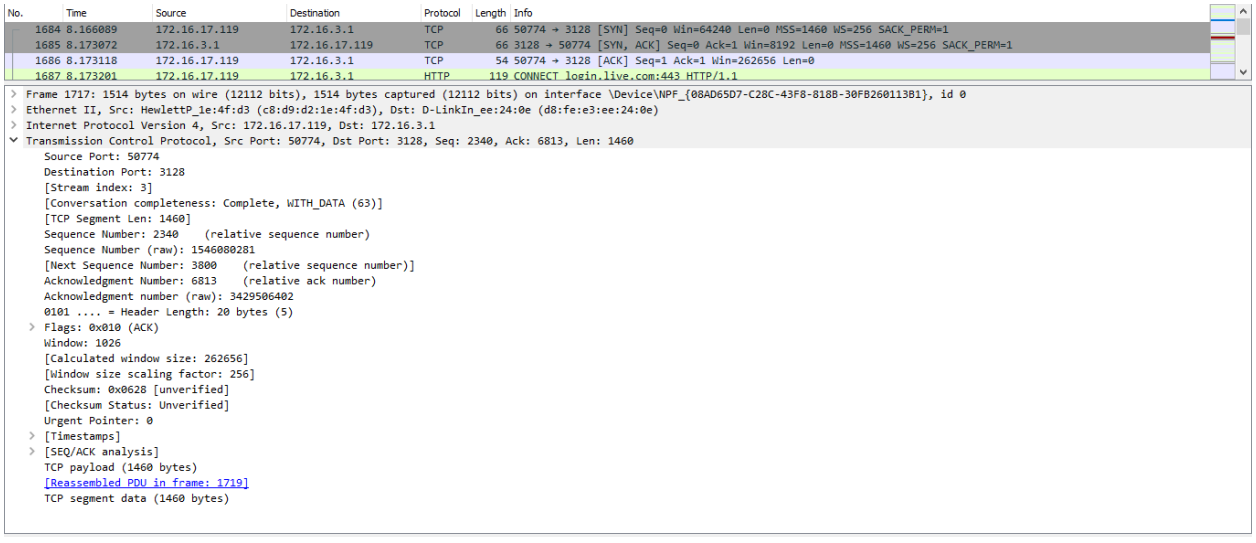
4. Capture Live Packets using Wireshark.



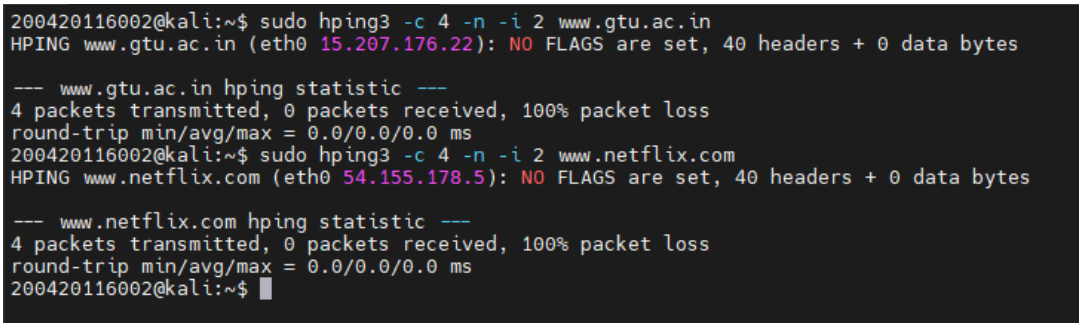
No.	Time	Source	Destination	Protocol	Length	Info
25	0.095192	172.16.17.105	224.0.0.252	LLMNR	62	Standard query 0xb5ec AAAA it
26	0.095537	172.16.17.126	172.16.17.255	NBNS	92	Name query NB DESKTOP-9H9A93Q<00>
27	0.100174	fe80::1050:88e4:f68…	ff02::1:3	LLMNR	82	Standard query 0xe1db A it
28	0.100174	172.16.17.121	224.0.0.252	LLMNR	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	LLMNR	82	Standard query 0x527f AAAA it
34	0.104245	172.16.17.121	224.0.0.252	LLMNR	62	Standard query 0x527f AAAA it
35	0.139145	fe80::389e:1ca4:deb…	ff02::1:3	LLMNR	95	Standard query 0x81ea A desktop-9h9a93q
36	0.139145	fe80::389e:1ca4:deb…	ff02::1:3	LLMNR	95	Standard query 0xdd9a AAAA desktop-9h9a93q
37	0.139146	172.16.17.138	224.0.0.252	LLMNR	75	Standard query 0x81ea A desktop-9h9a93q
38	0.139146	172.16.17.138	224.0.0.252	LLMNR	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<00>
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 169.254.183.94? Tell 172.16.17.80
44	0.219452	fe80::bda8: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::bda8:ff1b:844…	ff02::fb	MDNS	88	Standard query 0x0000 AAAA it.local, "QM" question
47	0.222423	fe80::bda8:ff1b:844…	ff02::1:3	LLMNR	82	Standard query 0x50fc A it
48	0.222775	172.16.17.106	224.0.0.252	LLMNR	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.





7. Demonstrate the usage of hping.



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 fashio
n 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 1P_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 fashio
n 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_75Ulow8DrI
UDkWSbCn5YjCBh6ad9t6ACoYVwOW4O6vS9"; e_fb_vipaddr="AcKrQbsZBWgyicP3gfFp6GHFLXJ4V0kmPB60TwNTJDrBmDT6LiG9K7nXBCxDlDv8Z8Fk90Y"; e_fb_build
user="AcJ207igLWDDoMQQTmu1KiAWgQ67qzRs1SFMrdU2x1jzc8Nw-mr8dV6Uvaqms5Lmnkg"; e_fb_binaryversion="AcLnsIK8oZt7x28ZFr_WCcIkd88zdRpHxQjcV_K
i-GnkP15uiebC37OiNkpKZsR1iaz2hjQ_-pZqAfkflKGIlkvgwUOfCy_K548"; e_proxy="AcIuFd_PgiRJs0C-Q6woMsD0EacGu3Ib9Mb0xVUOhx7Op3pIDe0qqwF25MSVYaL
t6RKilFVH2vsWcSYn"
+ 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 fashio
n 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 fashio
n 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-ig-peak-time' found, with contents: 0
+ Uncommon header 'report-to' found, with contents: {"group": "coep", "max_age": 86400, "endpoints": [{"url": "/security/coep_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="coep"
+ Uncommon header 'x-ig-push-state' found, with contents: c2
+ Uncommon header 'origin-trial' found, with contents: AuqWincgAuXeuu3KypEMnrrFEJHySaesyJS3EaIH40zvafzrU0Irhb7+5QwZpOqMZrPTjgvFl7Z5jJgy
1dNAcQMAAAB6eyJvcmlnaW4iOiJodHRwczovL2luc3RhZ3JhbS5jb206NDQzIiwiZmVhdHVyZSI6IkNyb3NzT3JpZ2luT3BlbmVyUG9saWN5UmVwb3J0aW5nIiwiZXhwaXJ5Ijo
xNjEzNDExNjYyLCJpc1N1YmRvbWFpbiI6dHJ1ZX0=
+ "robots.txt" contains 85 entries which should be manually viewed.
+ Uncommon header 'proxy-status' found, with contents: http_request_error; e_clientaddr="AcL3aegIXFp-88cHMWZg3KqYmiQGVjCQapgbhs_I5ZInID
o35QT8tEpNlwJDfmQ_gbi_L5xq_NDuFmiT"; e_fb_vipaddr="AcKfVNX7Hmy_RDQdJeFjIayPAoKCu7nO6PSeF7YPlb5YnS8CbGUhVQ7mr9u6JLucdD4CnpjF"; e_fb_buil
duser="AcKcvBBJW7W1ffGoudeBA0lJdH6G9caBUU2n6Dr5EgzYvnvvgDOeCj2-Ylq0fXovs98"; e_fb_binaryversion="AcJdFGcJWzbJMJTP104Aecf9y9ZpD7sFf_GXEi
9CAucivByXaUql-oF15mpGO_dg-ge4we0fjDV5sldi0es1-OjB1XAEgtXiCkE"; e_proxy="AcLQtp4qncDxJzCUPUdeM4-qPqgNYiz_jBPG_cciNwL06jEMxG08EA1cXE4FKe
0Dn1aIp_DA0l2Q3Naf"
+ 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/goo
gle/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: x42qhgCYiV013qi6yyBj5uhVKf7YaOdSDubgrZC36F7qfrrTkSrXgg==
+ 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 fashio
n 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; t
op: 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:~$
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; t
op: 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>
```

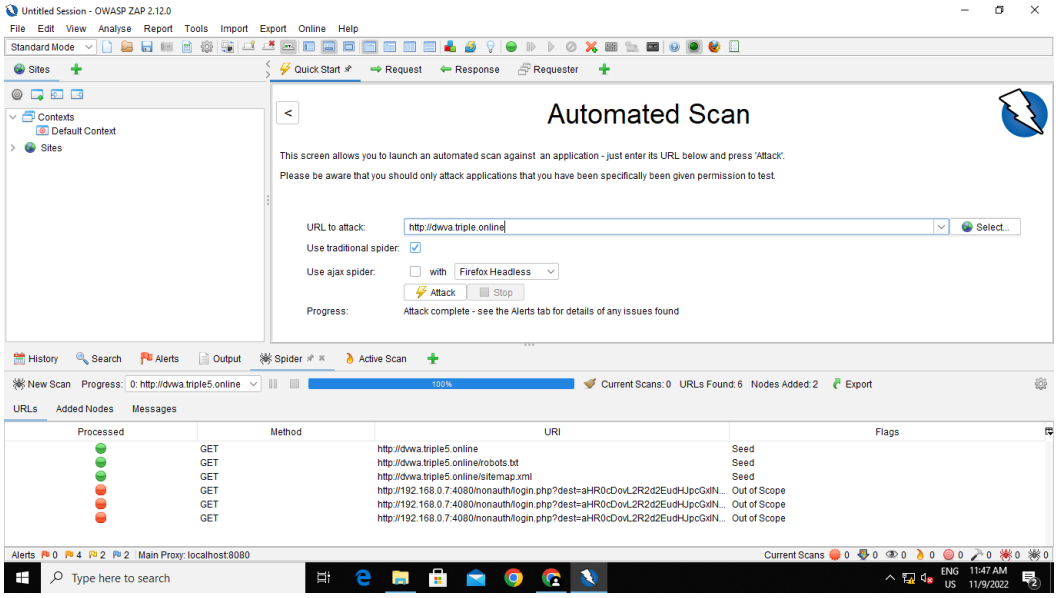
4. Perform Curl Operation on any five websites with request method POST.

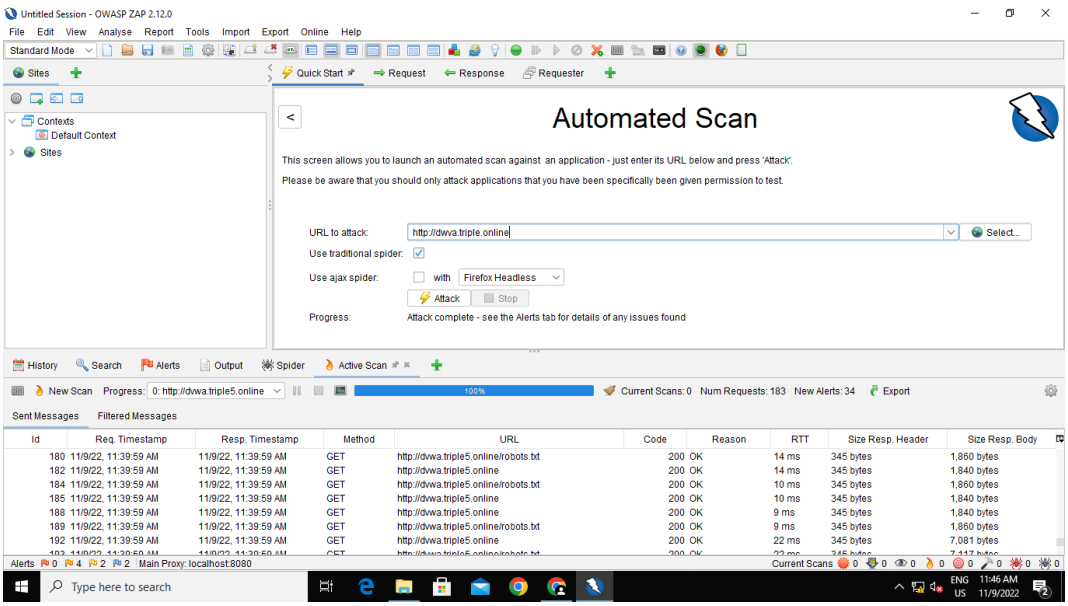
```
200420116002@kali:~$ curl --request POST google.com
<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
  <title>Error 411 (Length Required)!!1</title>
  <style>
    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-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/googlelogo/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) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat;-webkit-background-size:100% 100%}}#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>
```

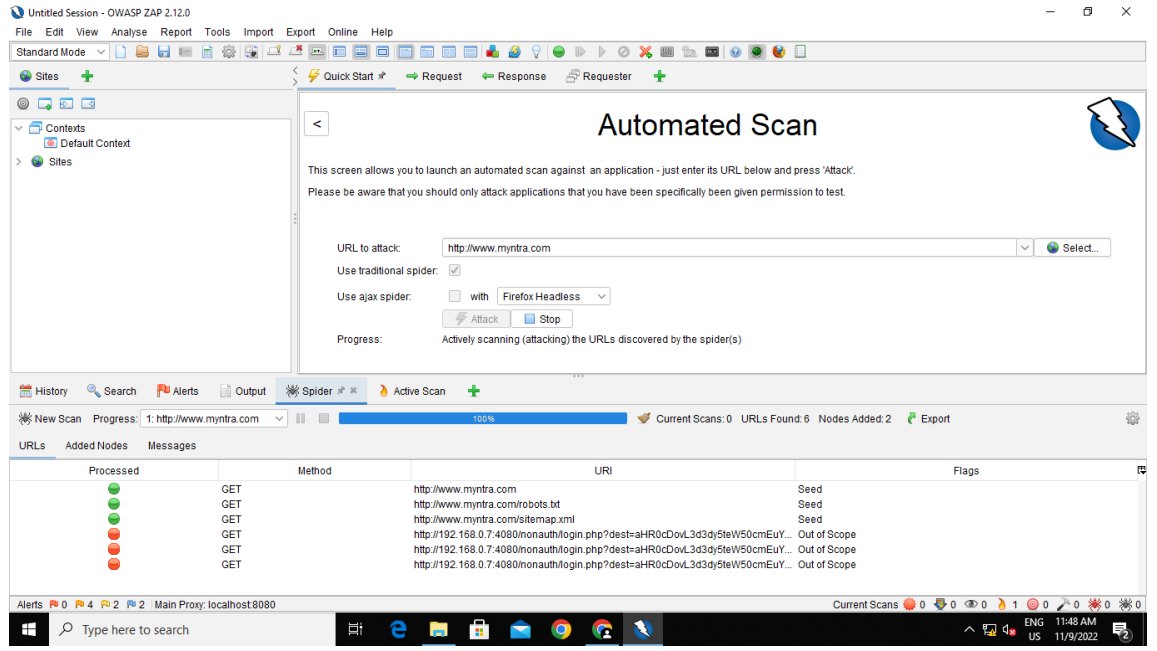
```
200420116002@kali:~$ curl --request POST triple5.online
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://triple5.online/">here</a>.</p>
</body></html>
200420116002@kali:~$ curl --request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

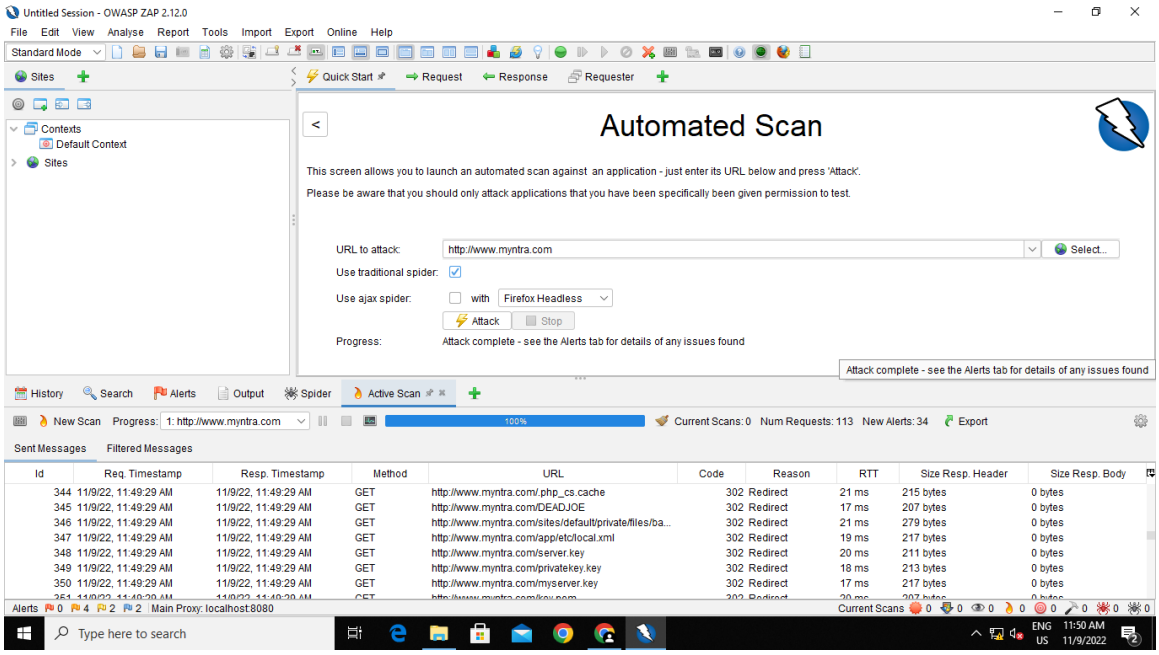
Assignment - 5

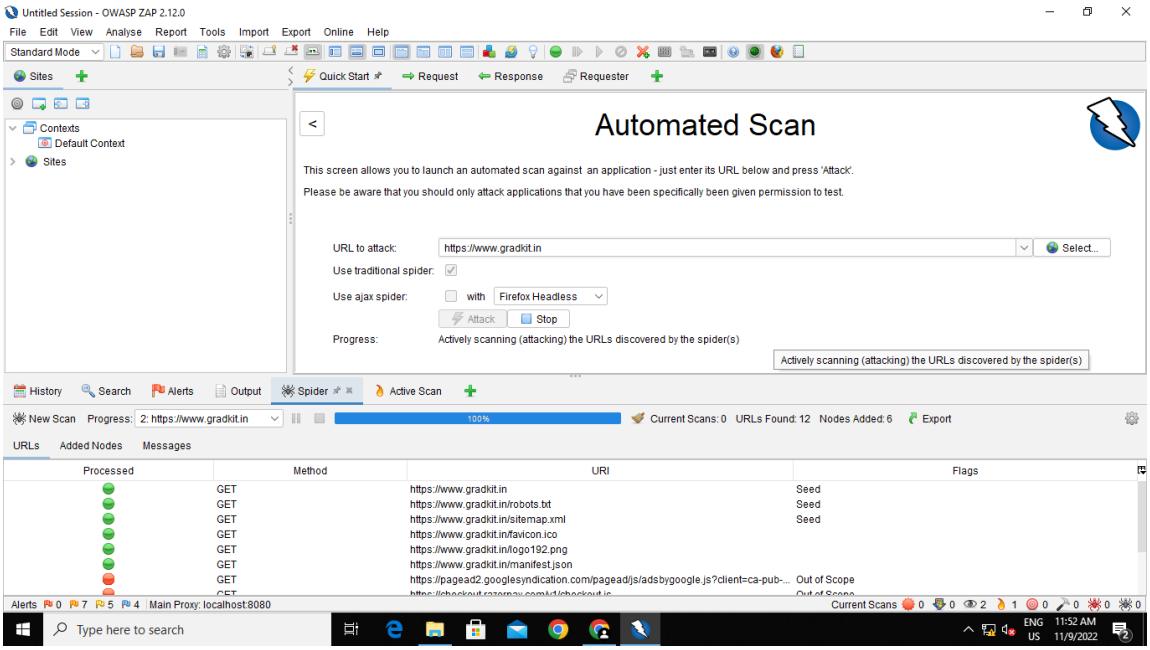
1. Scan at least 3 websites using Zed Attack Proxy. Perform Active Scan and Spider Scan on them and submit the screenshots.

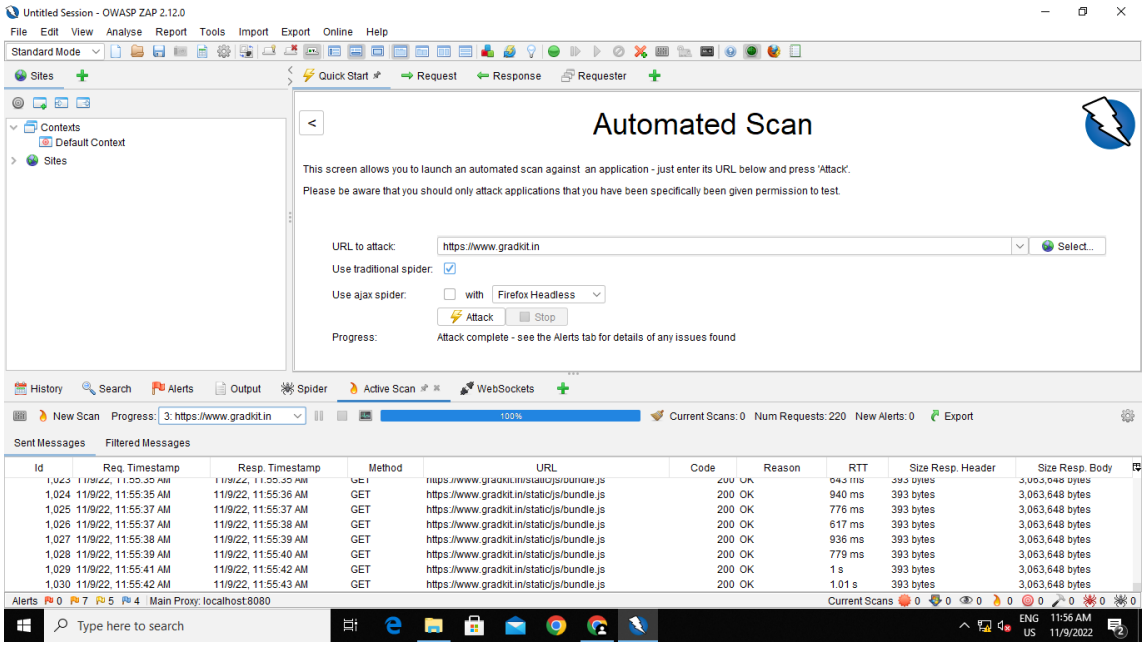





Untitled Session - OWASP ZAP 2.12.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below 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
100%
Current Scans: 0
URLs Found: 6
Nodes Added: 2
Export
URLs
Added Nodes
Messages
Processed
Method
URI
Flags
GET
http://www.myntra.com
Seed
GET
http://www.myntra.com/robots.txt
Seed
GET
http://www.myntra.com/sitemap.xml
Seed
GET
http://192.168.0.7:4080/monauth/login.php?dest=aHR0cDovL3d3dy5teW50cmEuY...
Out of Scope
GET
http://192.168.0.7:4080/monauth/login.php?dest=aHR0cDovL3d3dy5teW50cmEuY...
Out of Scope
GET
http://192.168.0.7:4080/monauth/login.php?dest=aHR0cDovL3d3dy5teW50cmEuY...
Out of Scope
Alerts 0 4 2 2
Main Proxy: localhost:8080
Current Scans
Type here to search
ENG US
11:48 AM
11/9/2022

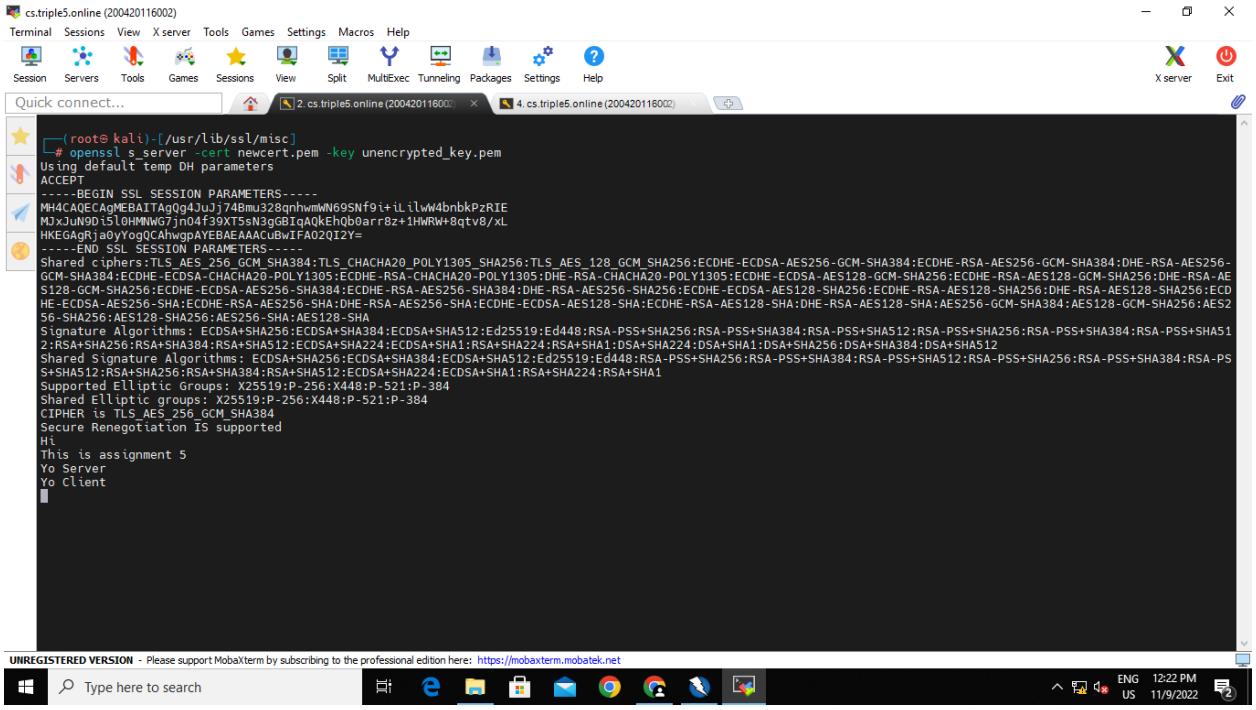

Untitled Session - OWASP ZAP 2.12.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below 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
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
344 11/9/22, 11:49:29 AM 11/9/22, 11:49:29 AM GET http://www.myntra.com/.php_cs.cache 302 Redirect 21 ms 215 bytes 0 bytes
345 11/9/22, 11:49:29 AM 11/9/22, 11:49:29 AM GET http://www.myntra.com/DEADJOE 302 Redirect 17 ms 207 bytes 0 bytes
346 11/9/22, 11:49:29 AM 11/9/22, 11:49:29 AM GET http://www.myntra.com/sites/default/private/files/ba... 302 Redirect 21 ms 279 bytes 0 bytes
347 11/9/22, 11:49:29 AM 11/9/22, 11:49:29 AM GET http://www.myntra.com/app/etc/local.xml 302 Redirect 19 ms 217 bytes 0 bytes
348 11/9/22, 11:49:29 AM 11/9/22, 11:49:29 AM GET http://www.myntra.com/server.key 302 Redirect 20 ms 211 bytes 0 bytes
349 11/9/22, 11:49:29 AM 11/9/22, 11:49:29 AM GET http://www.myntra.com/privatekey.key 302 Redirect 18 ms 213 bytes 0 bytes
350 11/9/22, 11:49:29 AM 11/9/22, 11:49:29 AM GET http://www.myntra.com/myserver.key 302 Redirect 17 ms 217 bytes 0 bytes
Alerts 0 4 2 2
Main Proxy: localhost:8080
Current Scans
Type here to search
ENG US
11:50 AM
11/9/2022


Untitled Session - 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: https://www.gradkit.in
Select...
Use traditional spider:
Use ajax spider: with Firefox Headless
Attack
Stop
Progress: Actively scanning (attacking) the URLs discovered by the spider(s)
Actively scanning (attacking) the URLs discovered by the spider(s)
History Search Alerts Output Spider Active Scan
New Scan Progress: 2: https://www.gradkit.in 100% Current Scans: 0 URLs Found: 12 Nodes Added: 6 Export
URLs Added Nodes Messages
Processed Method URI Flags
GET https://www.gradkit.in Seed
GET https://www.gradkit.in/robots.txt Seed
GET https://www.gradkit.in/sitemap.xml Seed
GET https://www.gradkit.in/favicon.ico
GET https://www.gradkit.in/logo192.png
GET https://www.gradkit.in/manifest.json
GET https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js?client=ca-pub-... Out of Scope
Alerts 0 7 5 4 Main Proxy: localhost:8080
Current Scans
Type here to search
ENG US 11:52 AM 11/9/2022

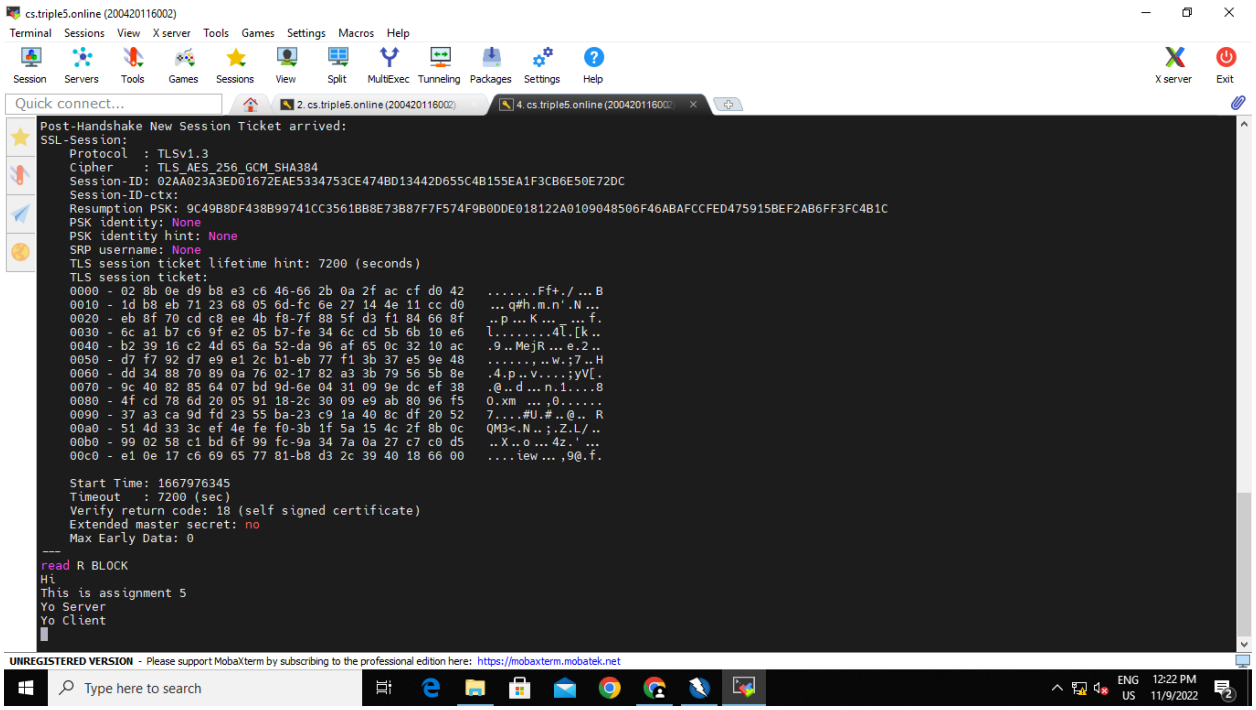

Untitled Session - OWASP ZAP 2.12.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below 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: https://www.gradkit.in
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 WebSockets
New Scan Progress: 3: https://www.gradkit.in 100% Current Scans: 0 Num Requests: 220 New Alerts: 0 Export
Sent Messages Filtered Messages
Id Req. Timestamp Resp. Timestamp Method URL Code Reason RTT Size Resp. Header Size Resp. Body
1,024 11/9/22, 11:55:35 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
Alerts 0 7 5 4 Main Proxy: localhost:8080
Current Scans
Type here to search
ENG US 11:56 AM 11/9/2022

2. Demonstrate the working of OpenSSL and Stunnel.

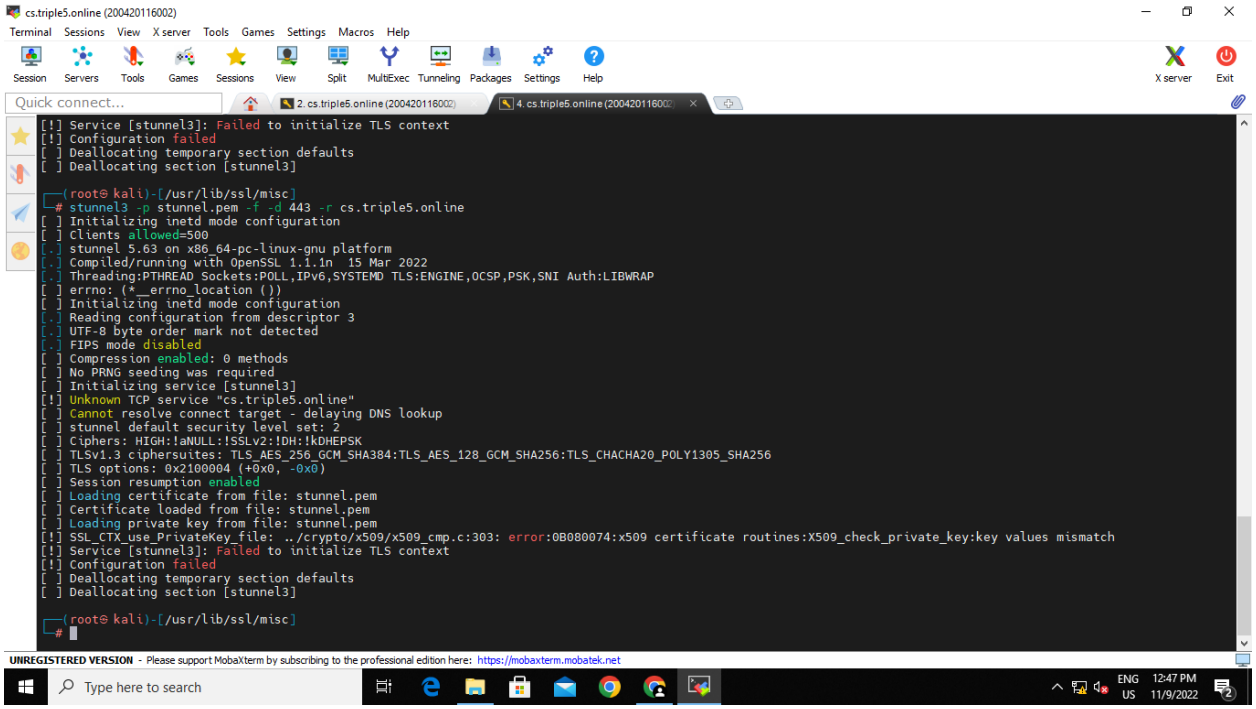
Server



Client

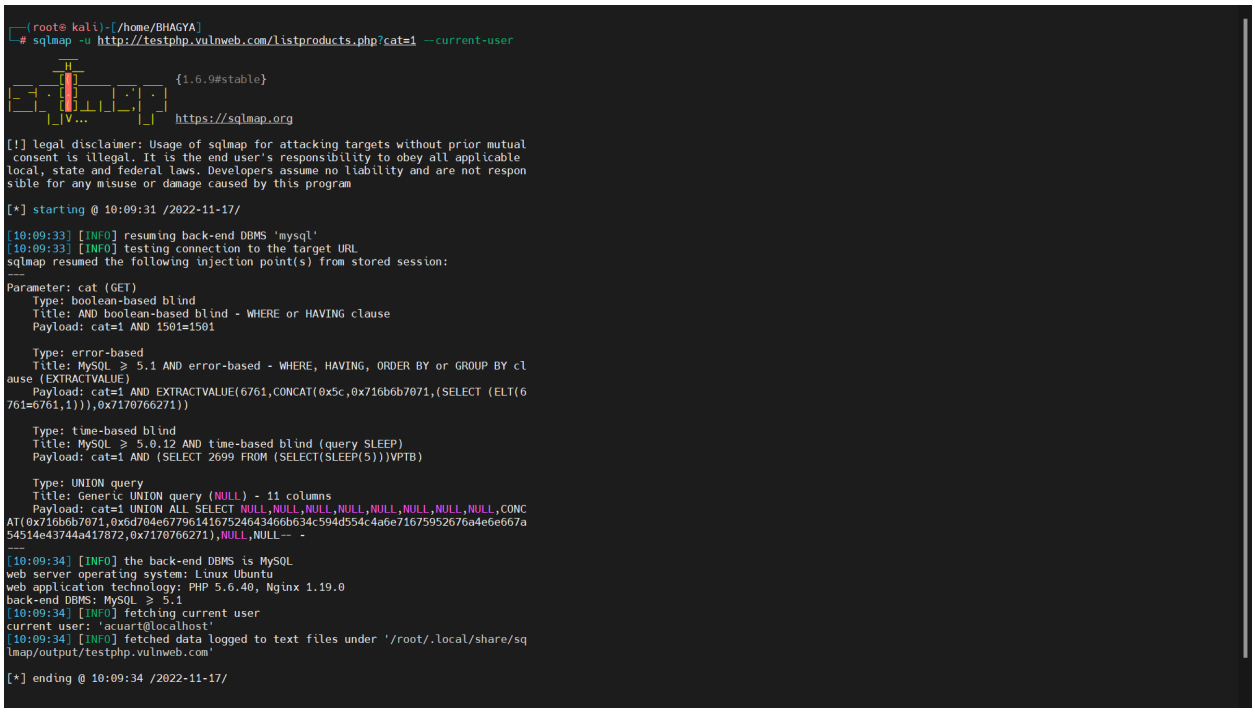


Error


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)
[!] 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 -f -d 443 -r cs.triple5.online
[ ] 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]
[!] Unknown TCP service "cs.triple5.online"
[ ] 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
[!] 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)-[/usr/lib/ssl/misc]
└─#
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
ENG US 12:47 PM 11/9/2022

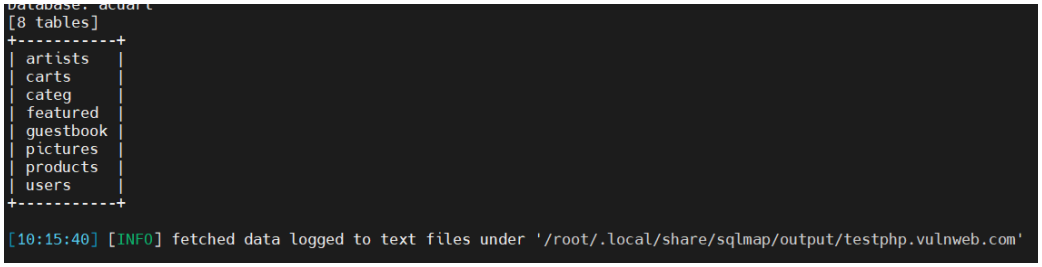
Assignment - 6

1. Apply Automated SQL Injection using SQLMAP.

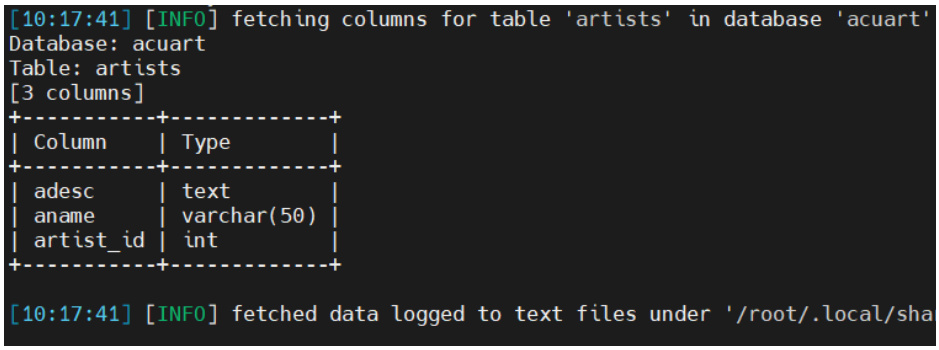


2. Find Database detail of the targeted site.

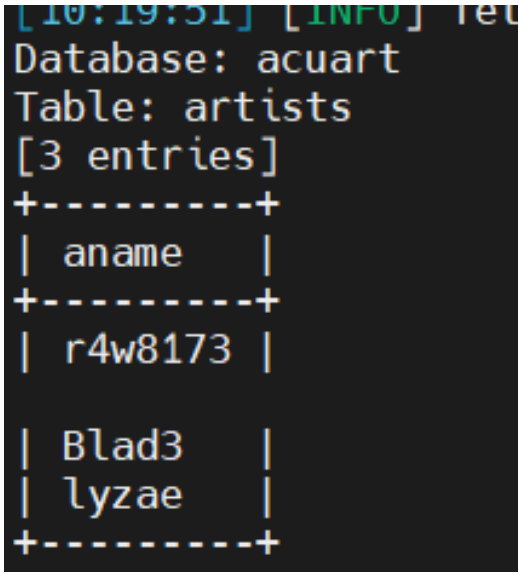
3. Find Table details of the targeted site.



4. Find Column details for the tables.

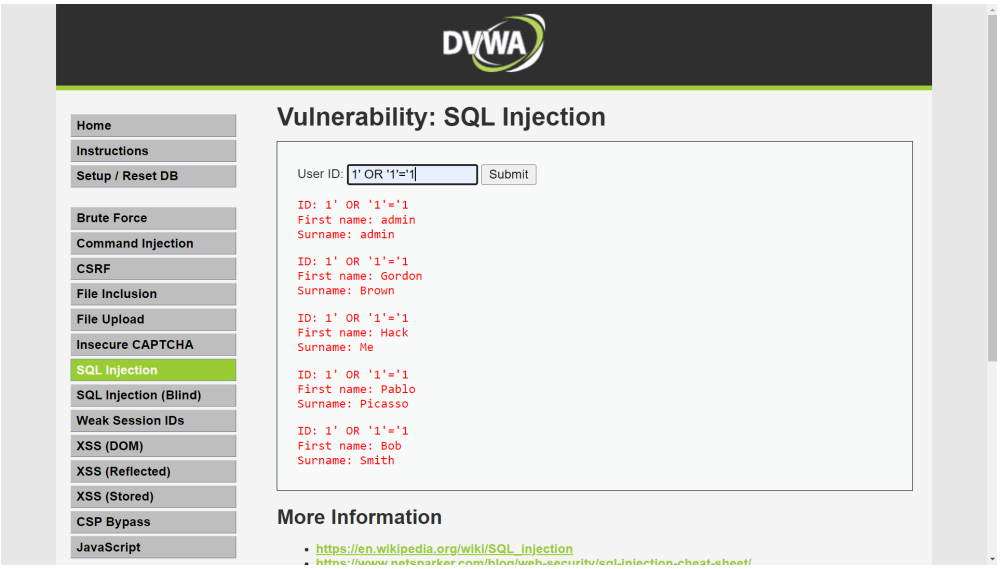


5. Find actual data for the given site.

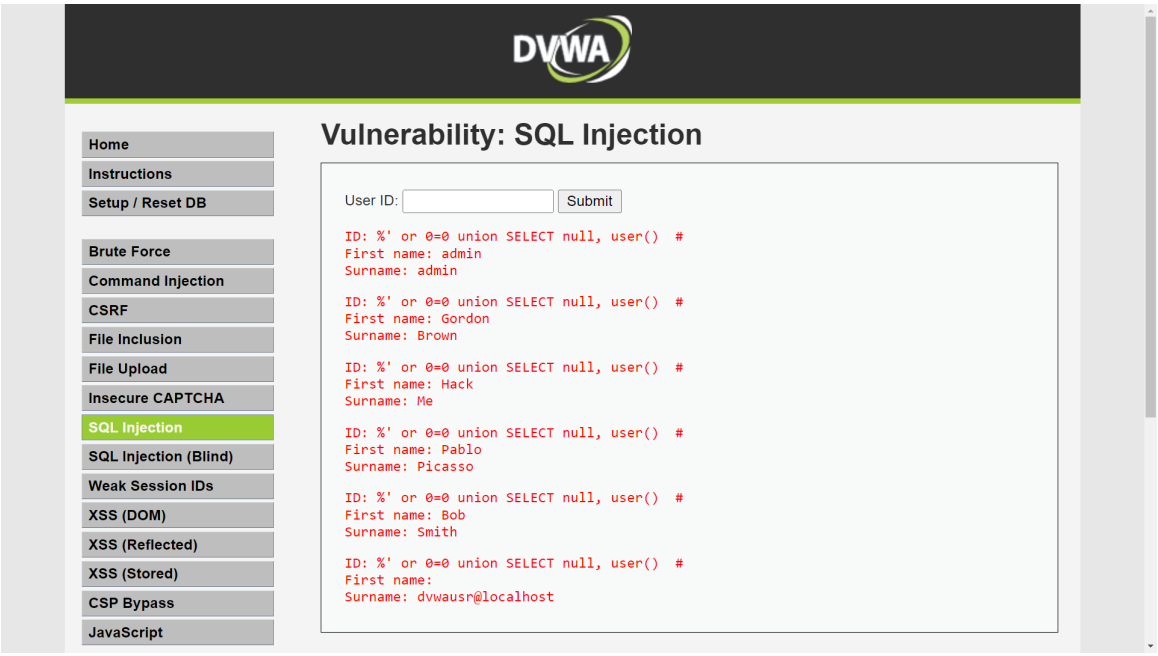


Assignment - 7

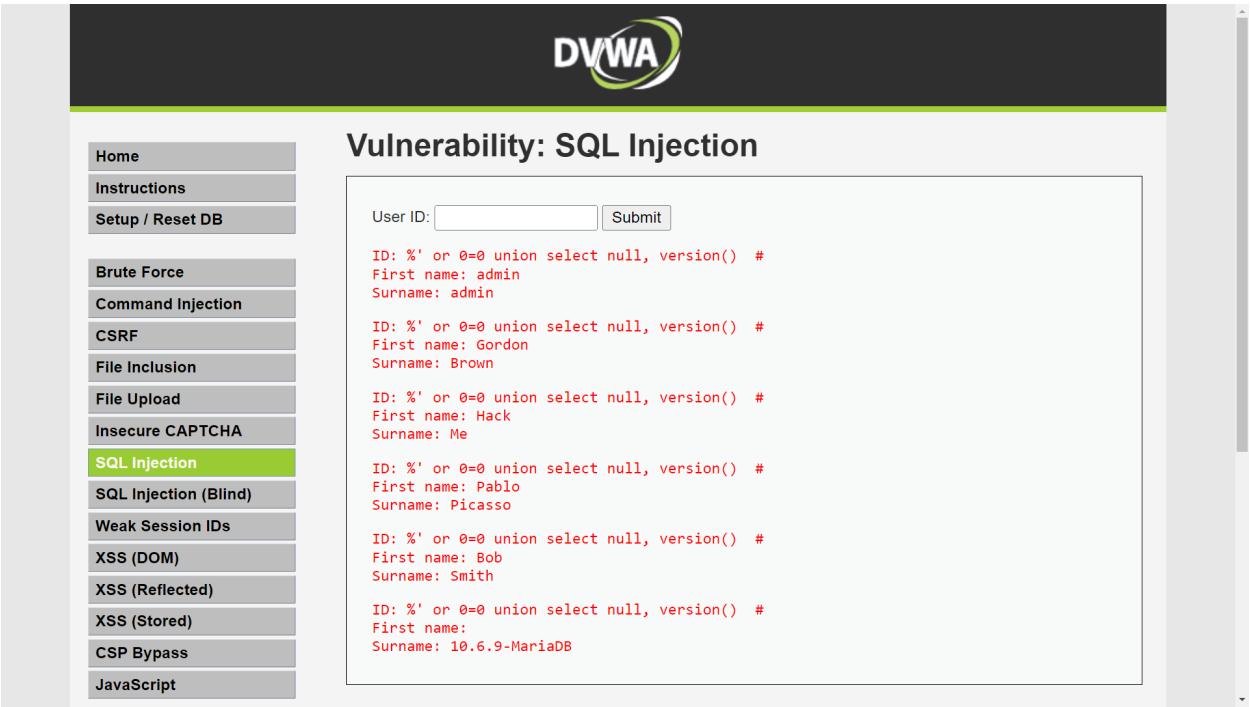
SQL Injection



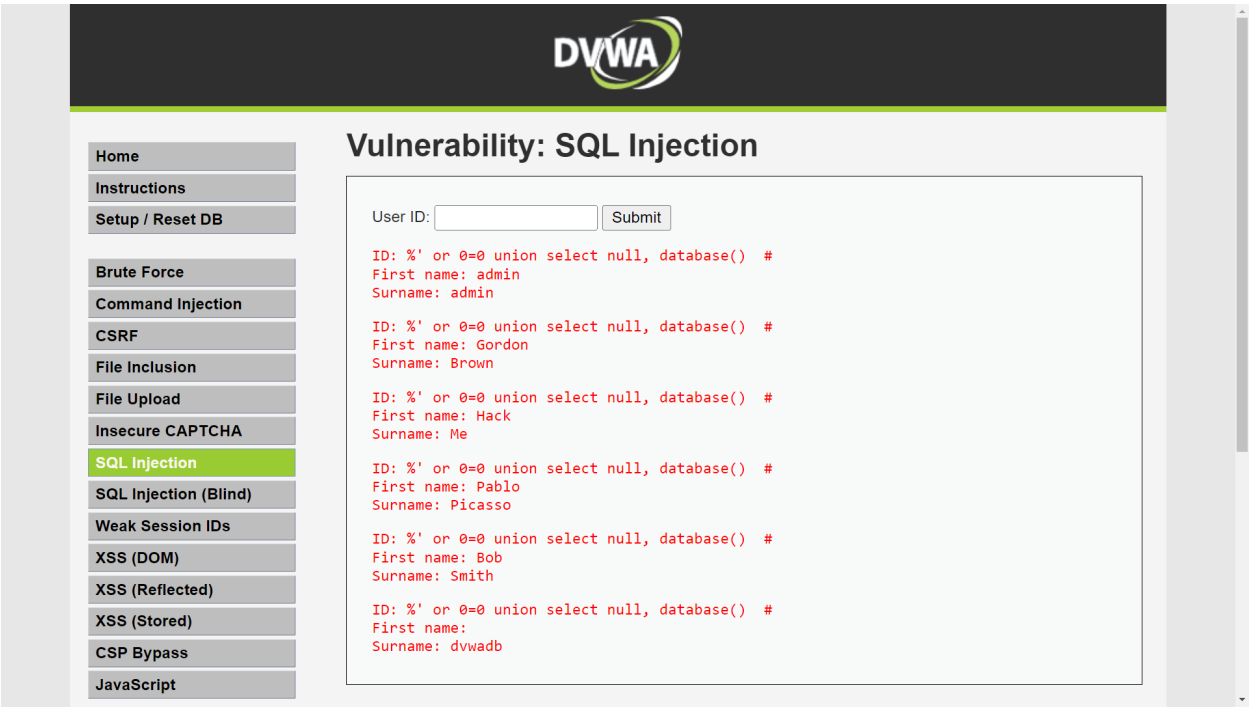
All users



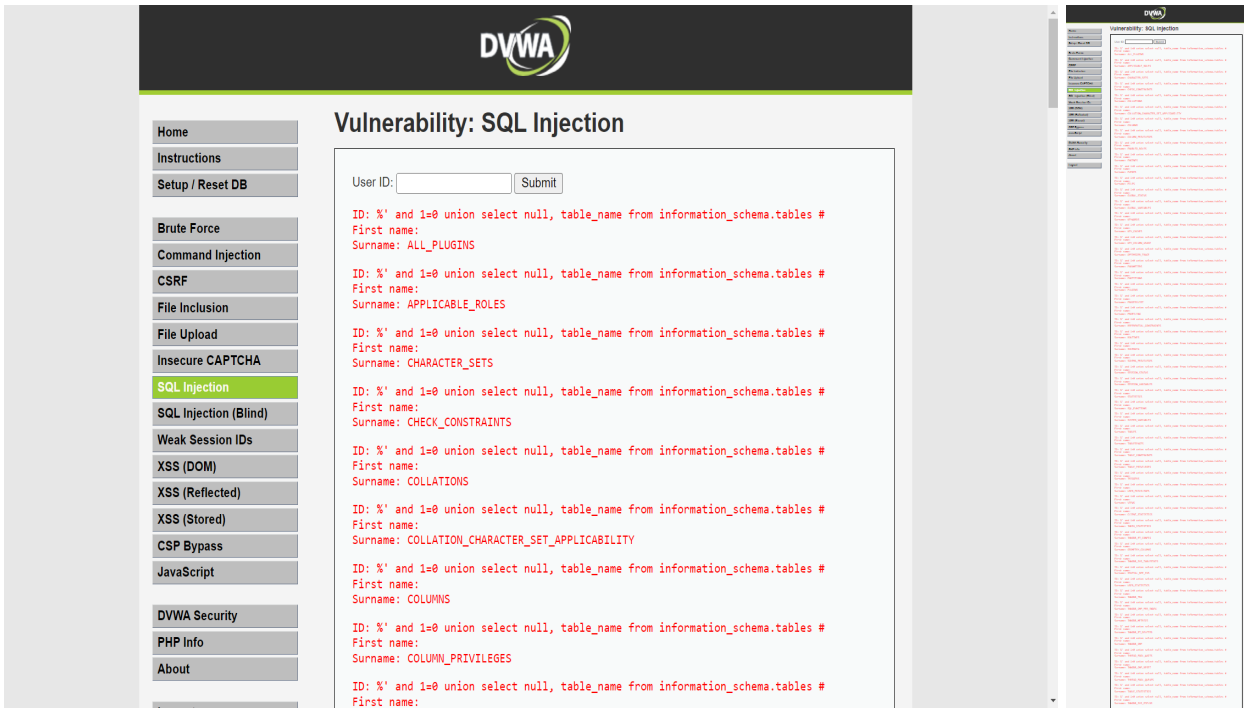
Database user information



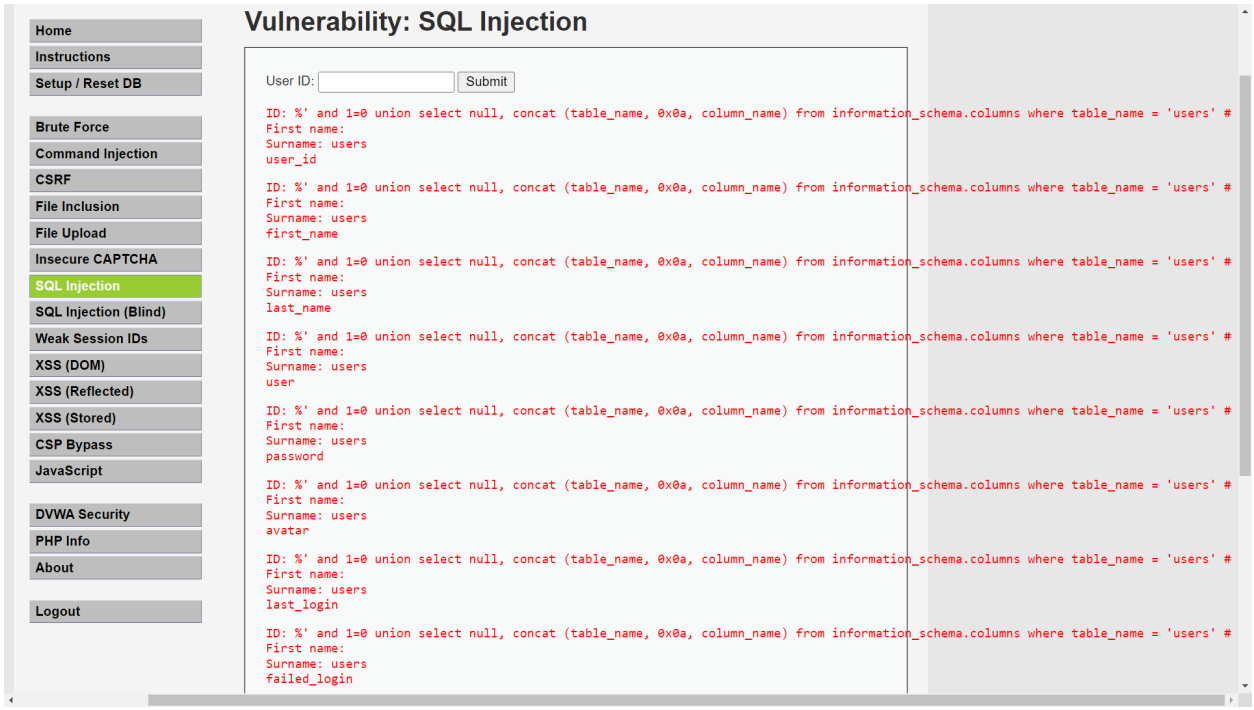
Database version information



Display Database name

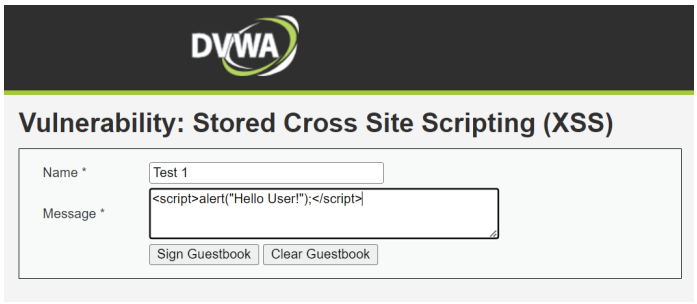


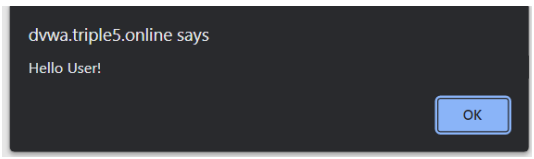
Display Database Tables in information_schema

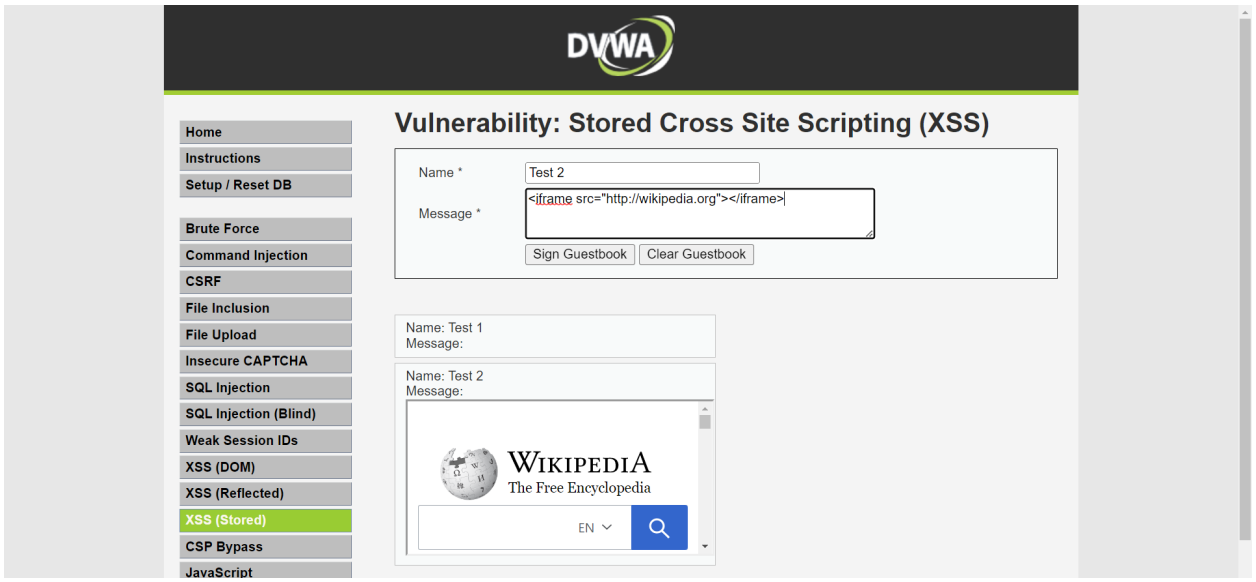


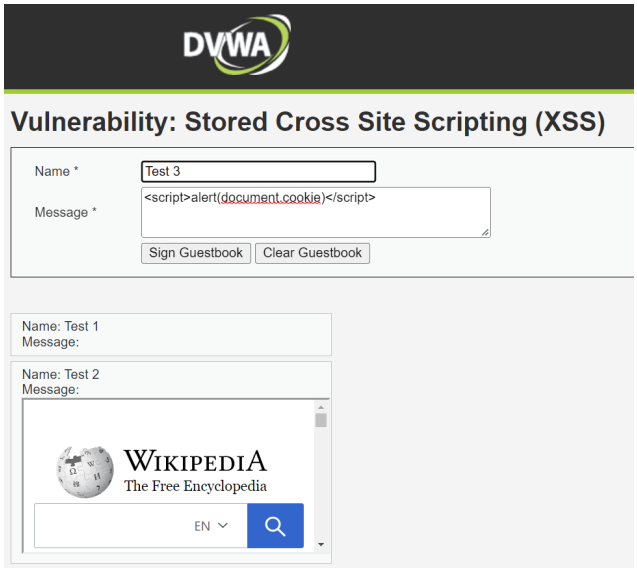
Display column field contents

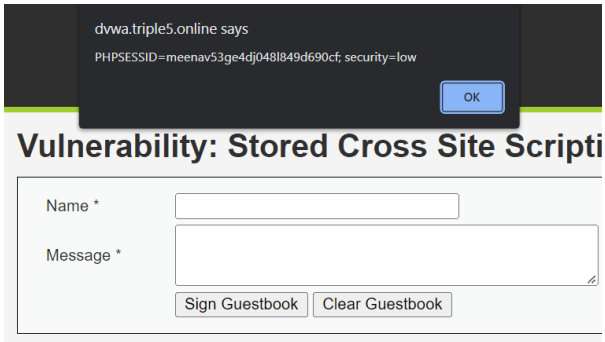
XSS (Cross site scripting)





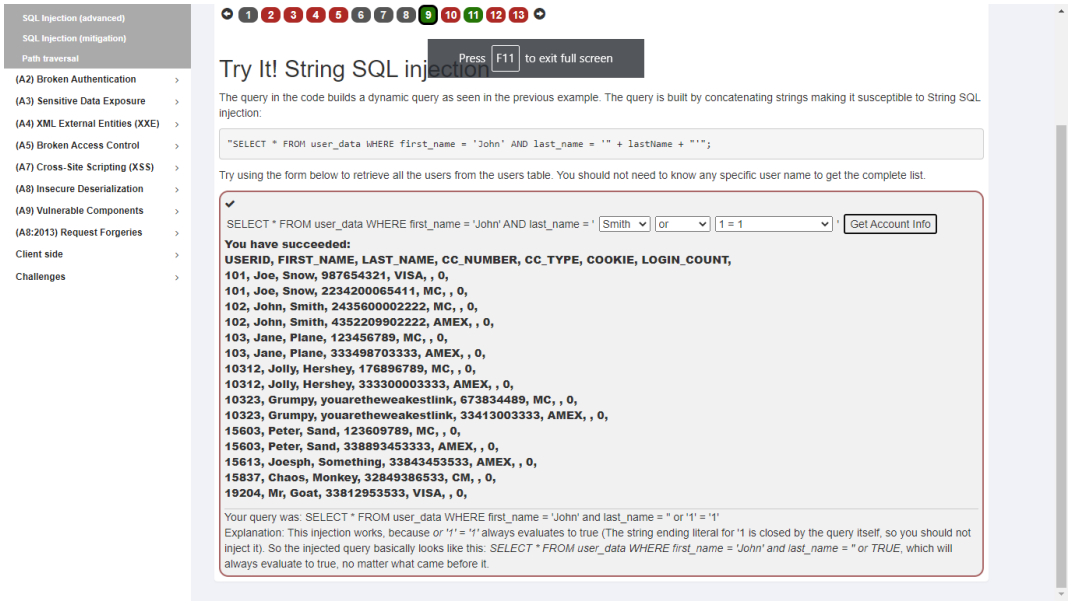


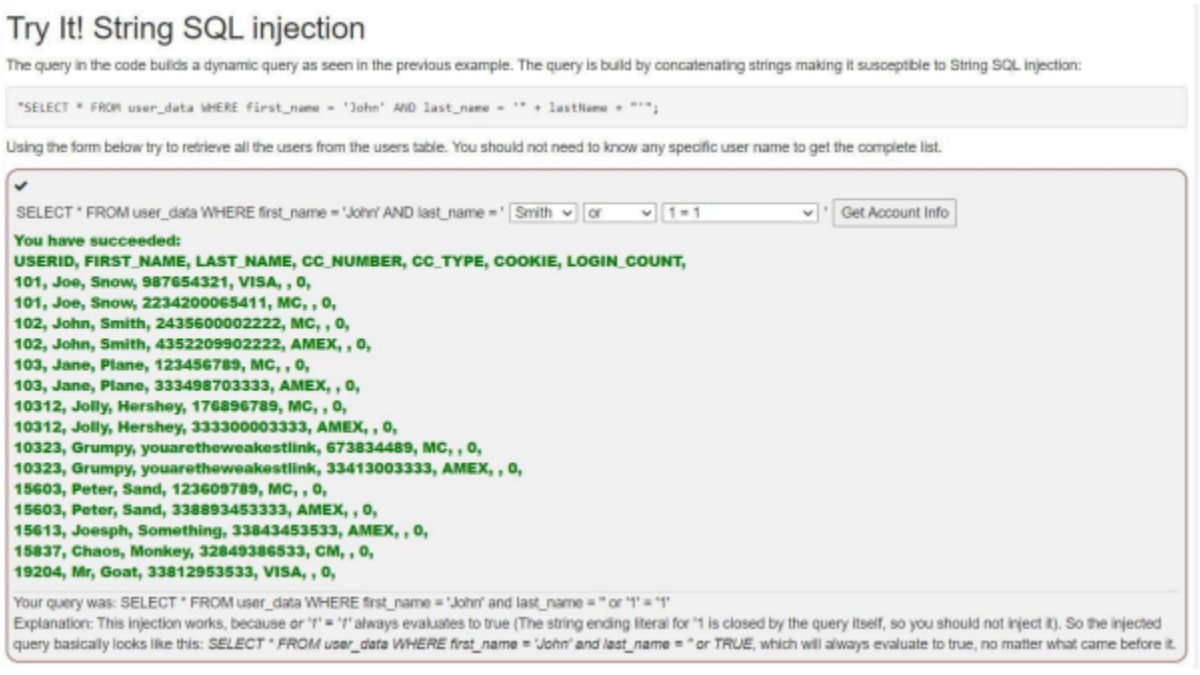




Assignment - 8

1. Apply Automated SQL Injection using SQLMAP.





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

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 + "';
```

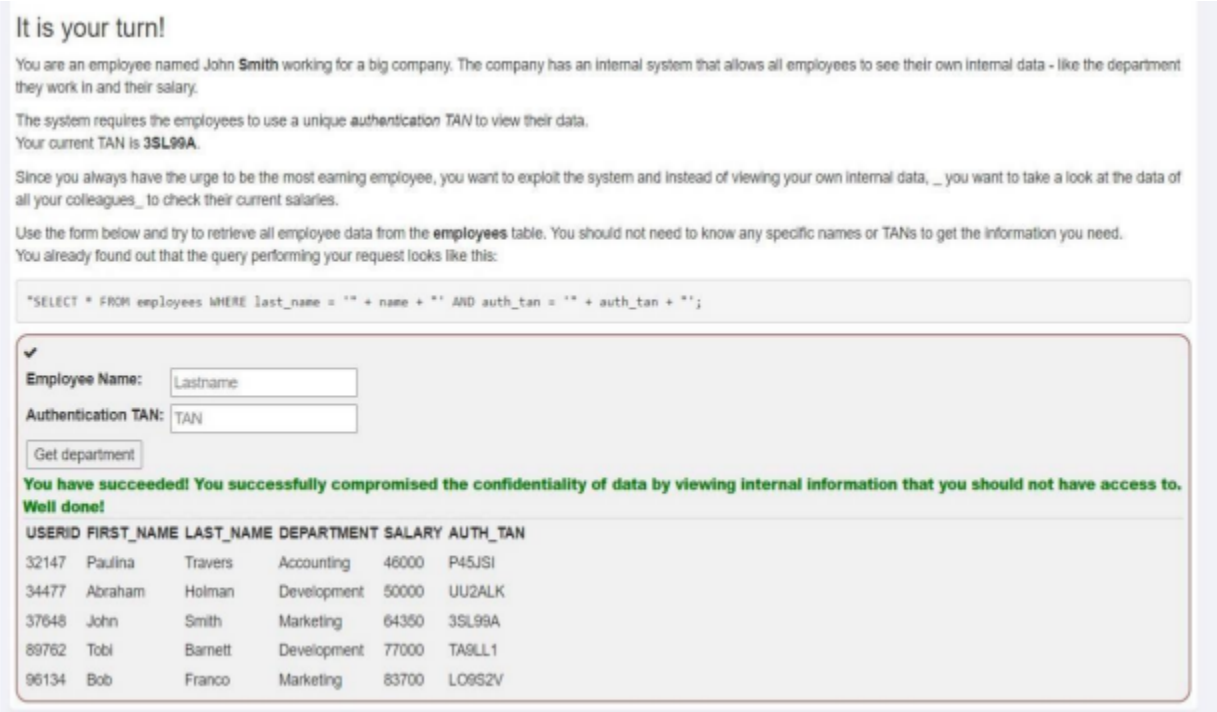
✔

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



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 + "';
```

✔

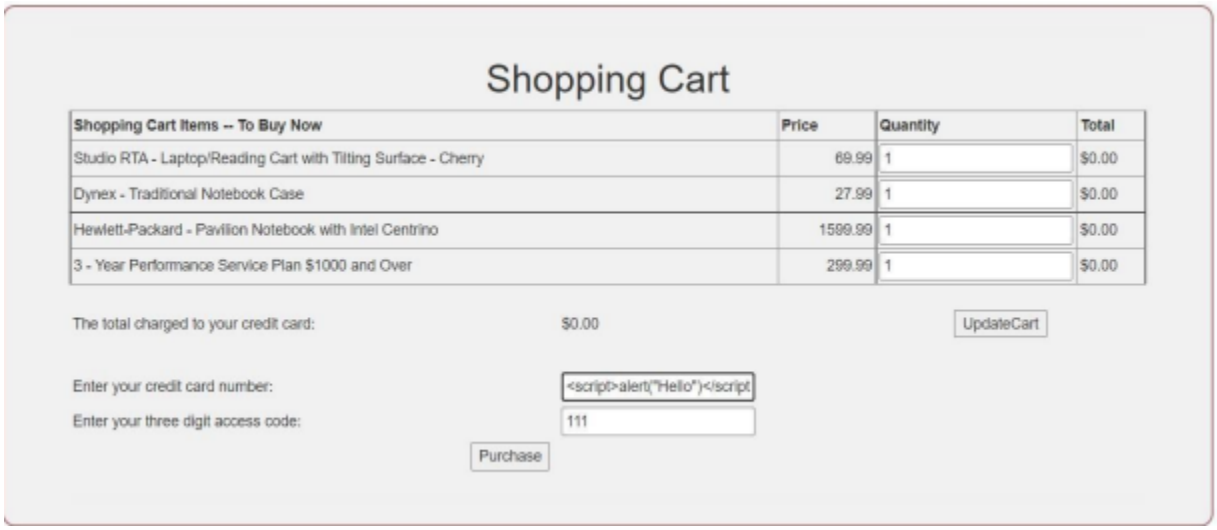
Employee Name: Lastname

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



Shopping Cart

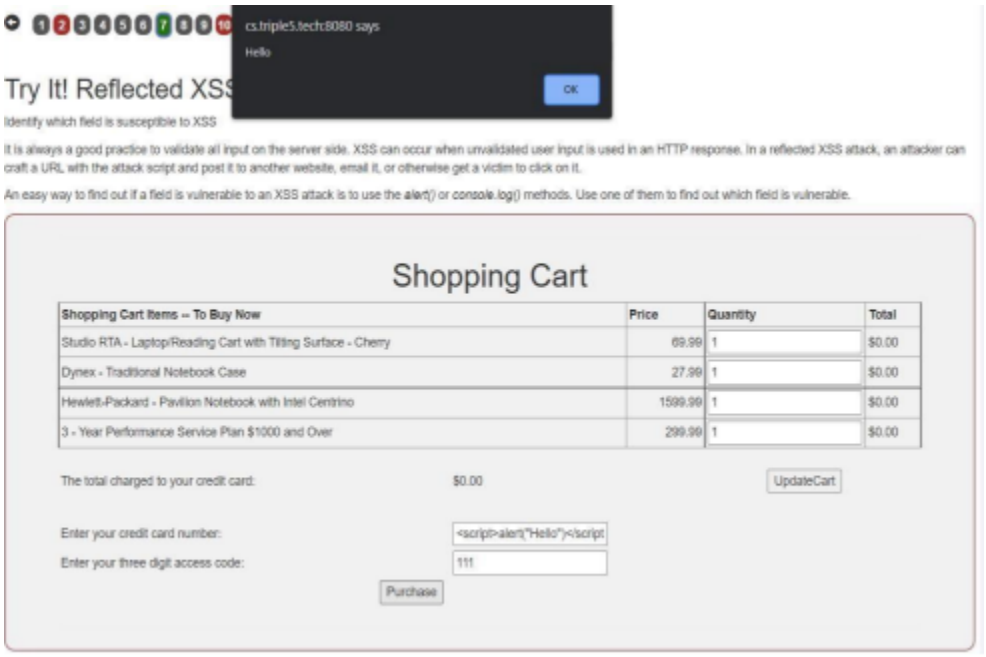
Shopping Cart Items -- To Buy Now	Price	Quantity	Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry	69.99	1	$0.00
Dynex - Traditional Notebook Case	27.99	1	$0.00
Hewlett-Packard - Pavilion Notebook with Intel Centrino	1599.99	1	$0.00
3 - Year Performance Service Plan $1000 and Over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

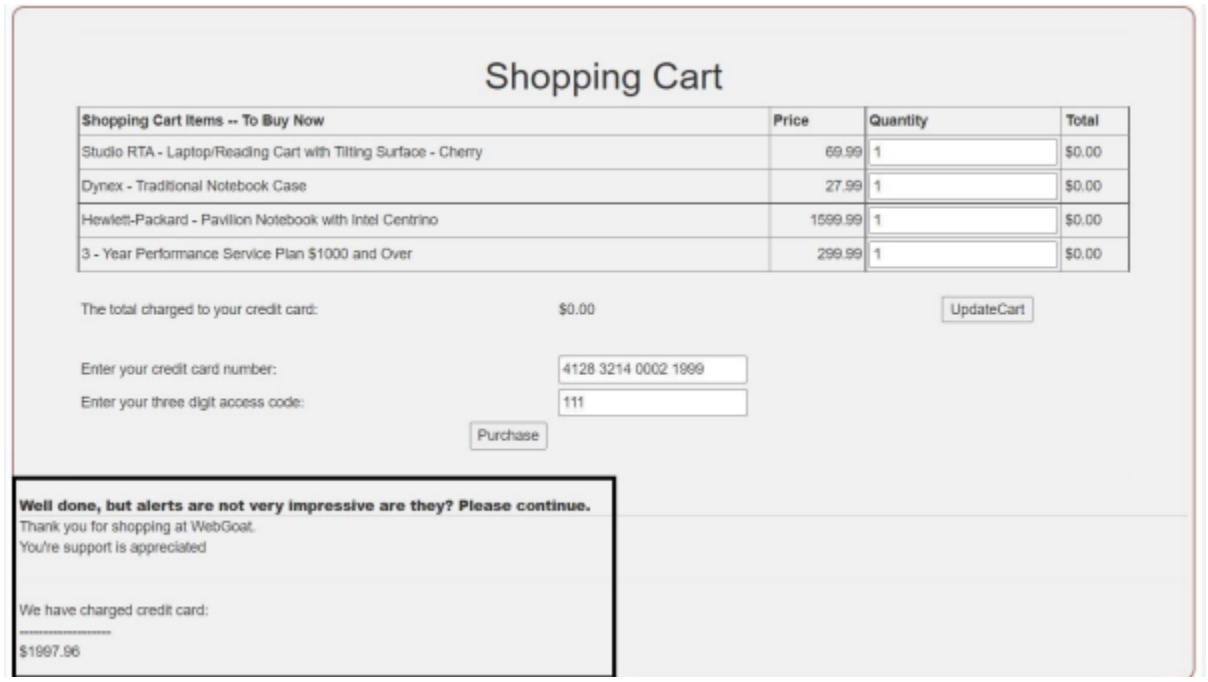
The total charged to your credit card: $0.00 UpdateCart

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

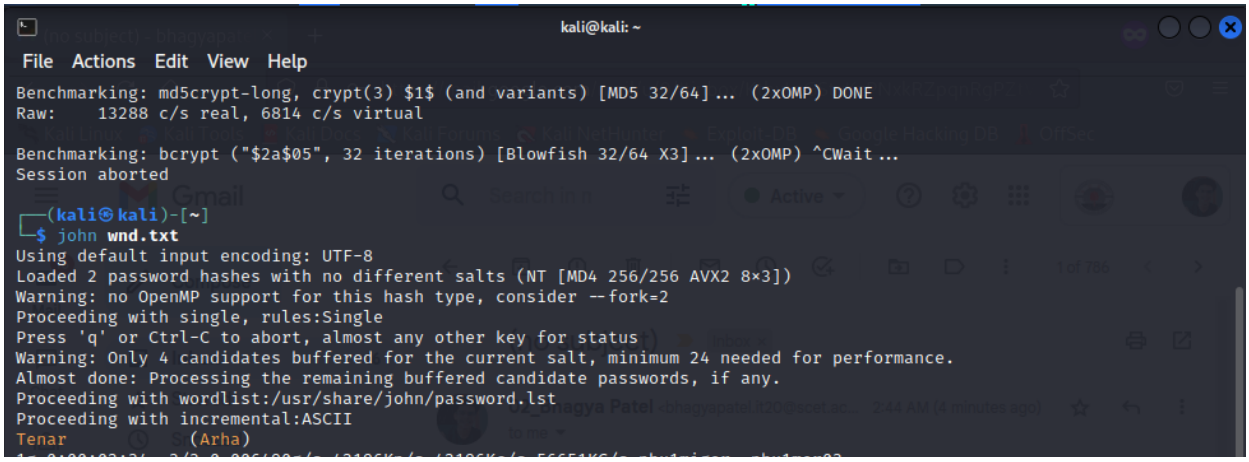
Enter your three digit access code: 111

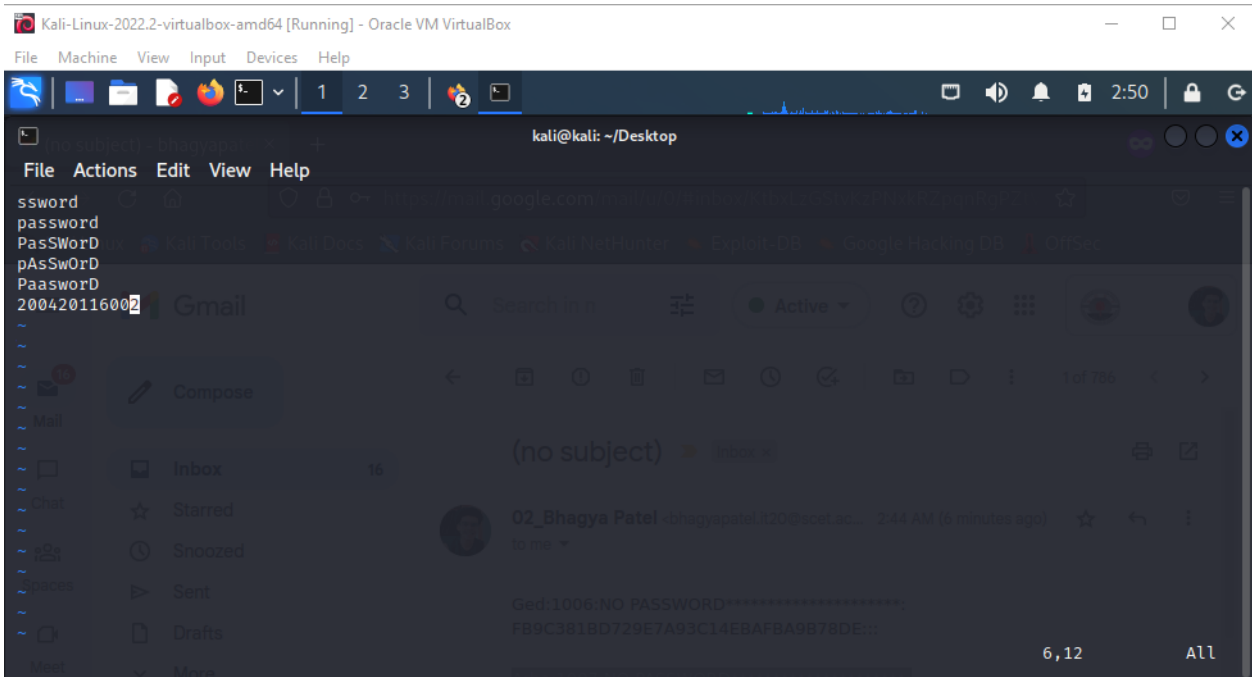
Purchase

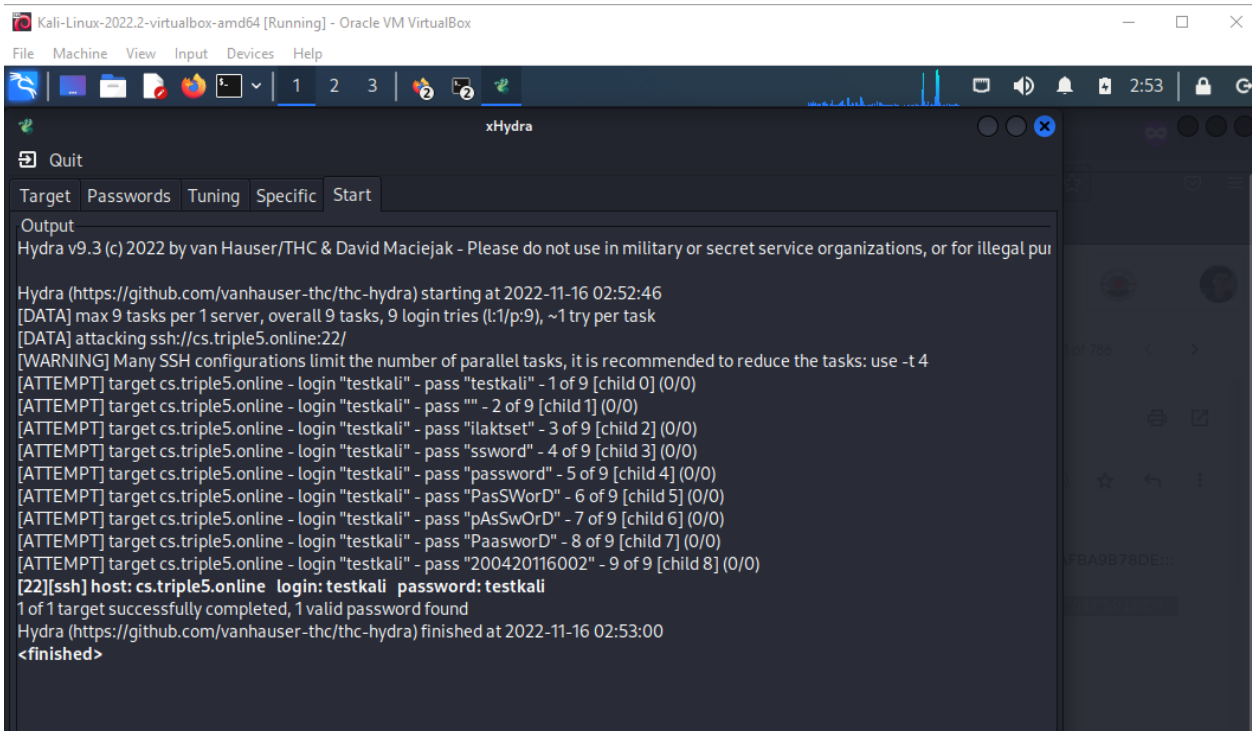

cs.triple5.tech:8080 says
Hello
OK
Try It! Reflected XSS
Identify which field is susceptible to XSS
It is always a good practice to validate all input on the server side. XSS can occur when unvalidated user input is used in an HTTP response. In a reflected XSS attack, an attacker can craft a URL with 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

Perform online attacks and offline attacks of password cracking.






Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3
2:53
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 pur
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