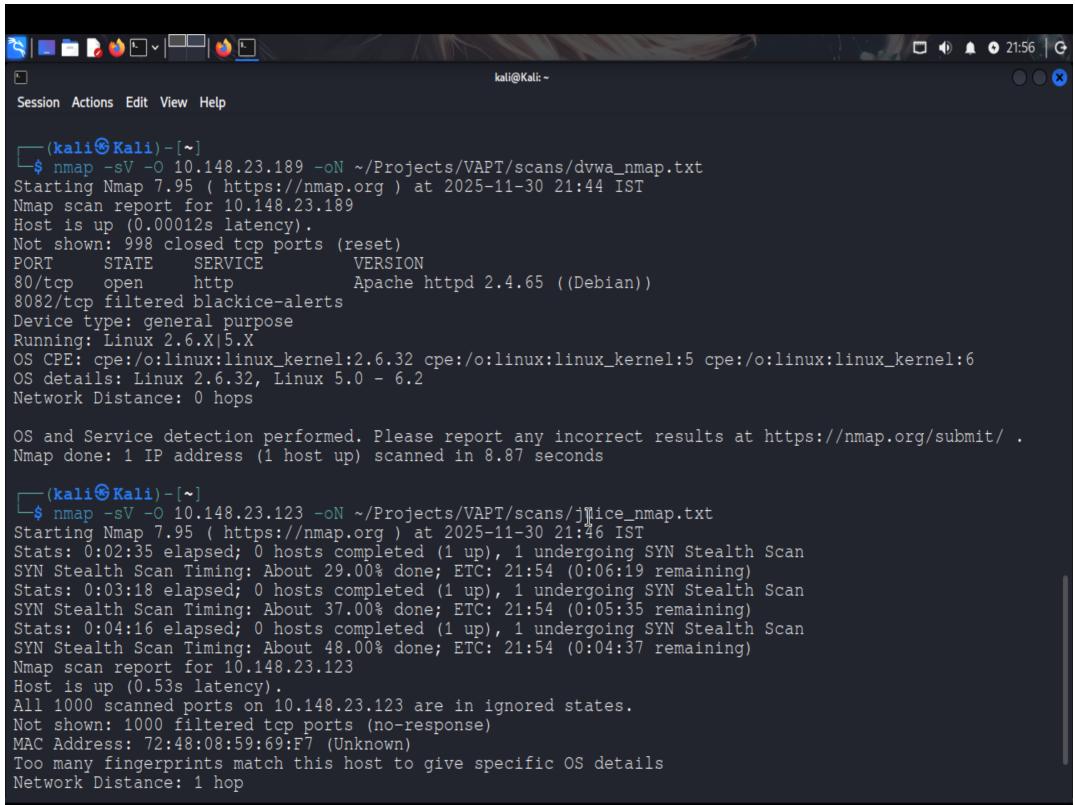


Nmap Scan Results

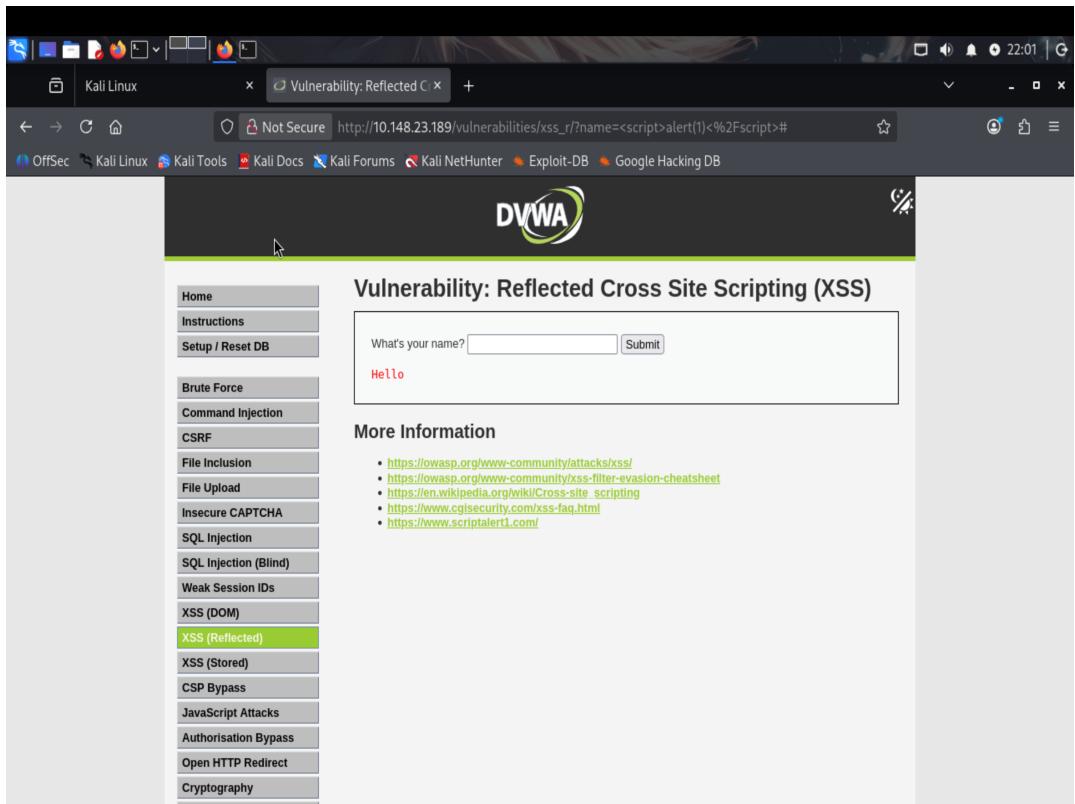


```
(kali㉿Kali)-[~]
└─$ nmap -sV -O 10.148.23.189 -oN ~/Projects/VAPT/scans/dvwa_nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 21:44 IST
Nmap scan report for 10.148.23.189
Host is up (0.00012s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE    SERVICE          VERSION
80/tcp    open     http           Apache httpd 2.4.65 ((Debian))
8082/tcp  filtered blackice-alerts
Device type: general purpose
Running: Linux 2.6.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 2.6.32, Linux 5.0 - 6.2
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.87 seconds

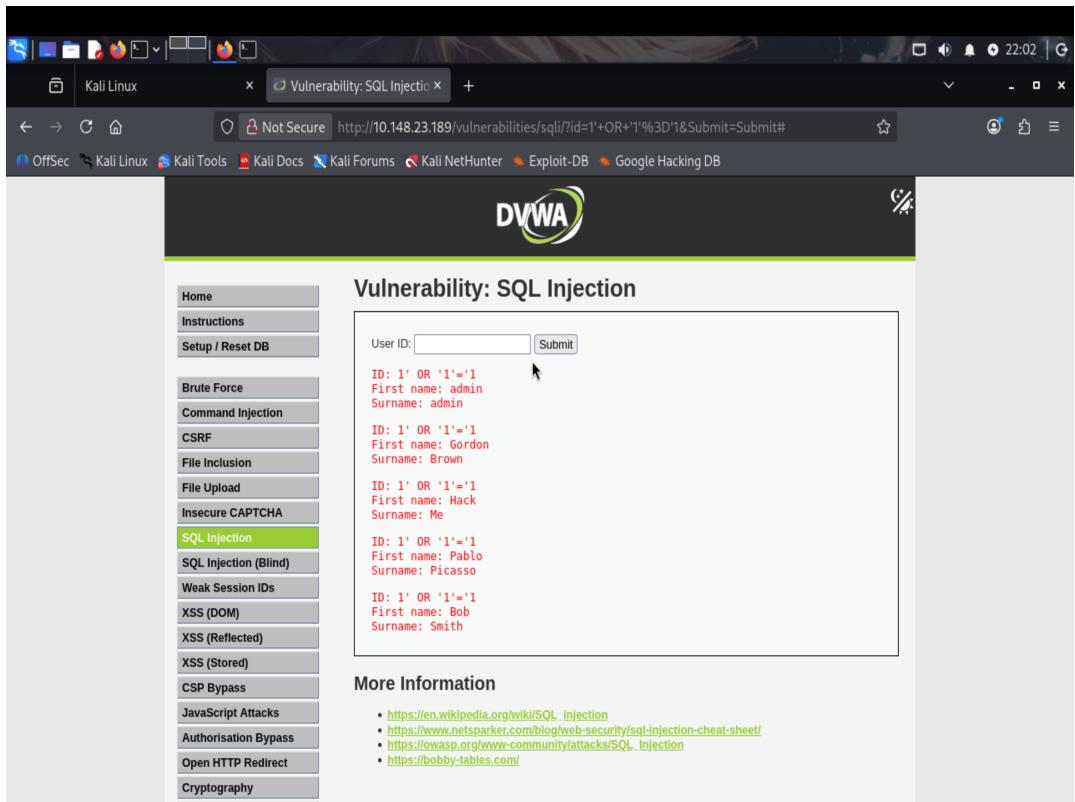
(kali㉿Kali)-[~]
└─$ nmap -sV -O 10.148.23.123 -oN ~/Projects/VAPT/scans/j2lce_nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 21:46 IST
Stats: 0:02:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 29.00% done; ETC: 21:54 (0:06:19 remaining)
Stats: 0:03:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 37.00% done; ETC: 21:54 (0:05:35 remaining)
Stats: 0:04:16 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 48.00% done; ETC: 21:54 (0:04:37 remaining)
Nmap scan report for 10.148.23.123
Host is up (0.53s latency).
All 1000 scanned ports on 10.148.23.123 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 72:48:08:59:69:F7 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

DVWA XSS (Reflected)



A screenshot of a Firefox browser window on a Kali Linux desktop. The address bar shows the URL `http://10.148.23.189/vulnerabilities/xss_r/?name=<script>alert(1)<%2Fscript>#`. The main content is the DVWA logo and the title "Vulnerability: Reflected Cross Site Scripting (XSS)". On the left, a sidebar menu lists various attack types, with "XSS (Reflected)" highlighted in green. Below the title is a form with a text input field containing "Hello" and a submit button. A "More Information" section at the bottom provides links to external resources.

DVWA SQL Injection



A screenshot of a Firefox browser window on a Kali Linux desktop. The address bar shows the URL `http://10.148.23.189/vulnerabilities/sql_injection/?id=1+OR+'1'%3D'1&Submit=Submit#`. The main content is the DVWA logo and the title "Vulnerability: SQL Injection". On the left, a sidebar menu lists various attack types, with "SQL Injection" highlighted in green. Below the title is a form with a text input field containing "User ID: ID: '1' OR '1'='1" and a submit button. A list of user records is displayed below the input field, showing various names and surnames corresponding to different injection queries. A "More Information" section at the bottom provides links to external resources.

DVWA Command Injection

The screenshot shows a Kali Linux desktop environment with a Firefox browser window open to the DVWA Command Injection page at <http://10.148.23.189/vulnerabilities/exec/#>. The DVWA logo is at the top. On the left, a sidebar lists various attack types, with "Command Injection" highlighted. The main content area is titled "Vulnerability: Command Injection" and contains a "Ping a device" section. It shows the output of a ping command to 127.0.0.1:

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.127 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.034 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.060 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.136 ms  
... 127.0.0.1 ping statistics ...  
4 packets transmitted, 4 received, 0% packet loss, time 3074ms  
rtt min/avg/max/mdev = 0.034/0.089/0.136/0.043 ms  
www-data
```

Below this, a "More Information" section lists several links:

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/m/>
- https://owasp.org/www-community/attacks/Command_Injection

Juice Shop XSS

