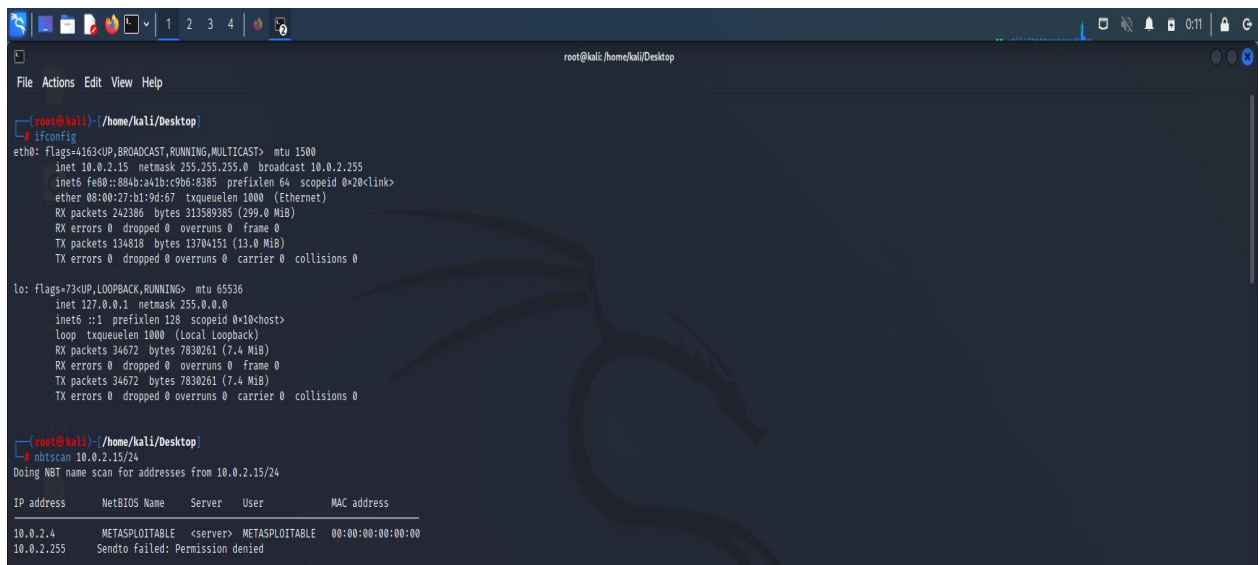


EXPLOITING DVWA

DVWA(Damn Vulnerable Web Application) is a PHP/MySQL web application, whose main goal is to be an aid for security professionals to test their skills and tools in a legal environment.

Step 1: Find the ip address of the pc using- ifconfig. Then find ip of Metasploit using - nbtscan.



```
root@kali: /home/kali/Desktop
File Actions Edit View Help

root@kali: /home/kali/Desktop
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::884b:a41b:c9b6:8385 prefixlen 64 scopeid 0<link>
    ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
    RX packets 242386 bytes 313589385 (299.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 134818 bytes 13704151 (13.0 MiB)
    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 34672 bytes 7830261 (7.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 34672 bytes 7830261 (7.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

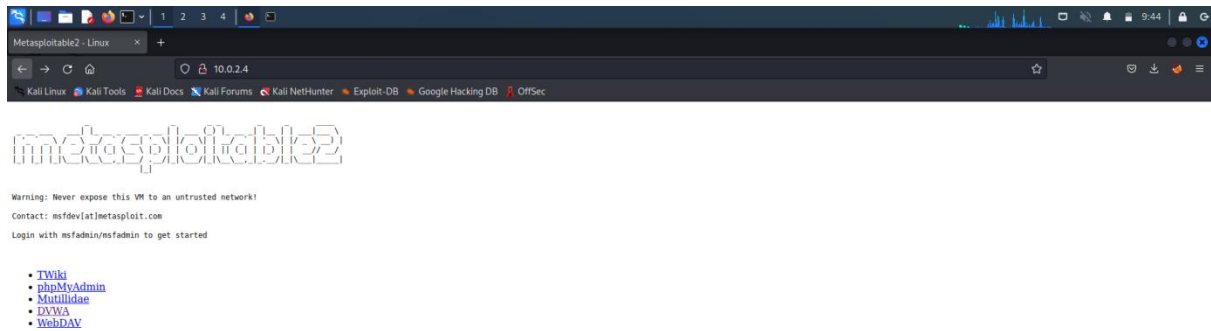
root@kali: /home/kali/Desktop
nbtscan 10.0.2.15/24
Doing NBT name scan for addresses from 10.0.2.15/24

IP address      NetBIOS Name    Server  User      MAC address
-----
10.0.2.4        METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
10.0.2.255      Sendto failed: Permission denied
```

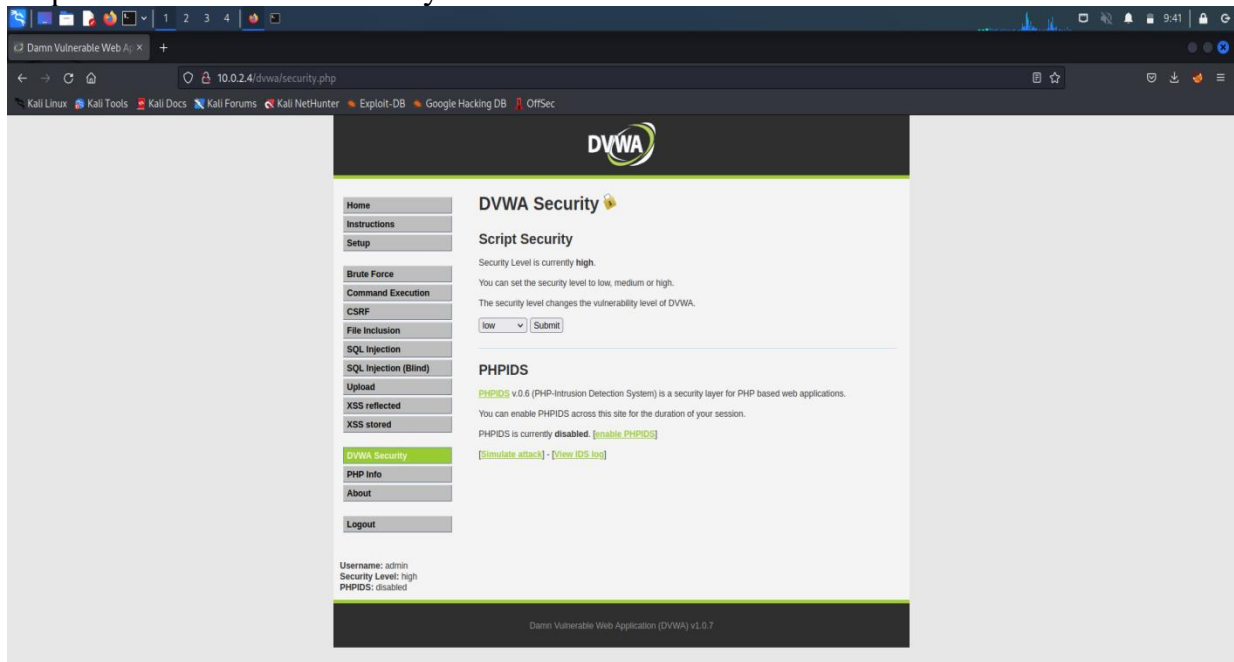
Step 2: Copy the ip of Metasploit and paste it in firefox. Choose the DVWA in order to find the vulnerabilities .

Enter the username and password –

(i.e. username: admin ,password: password)



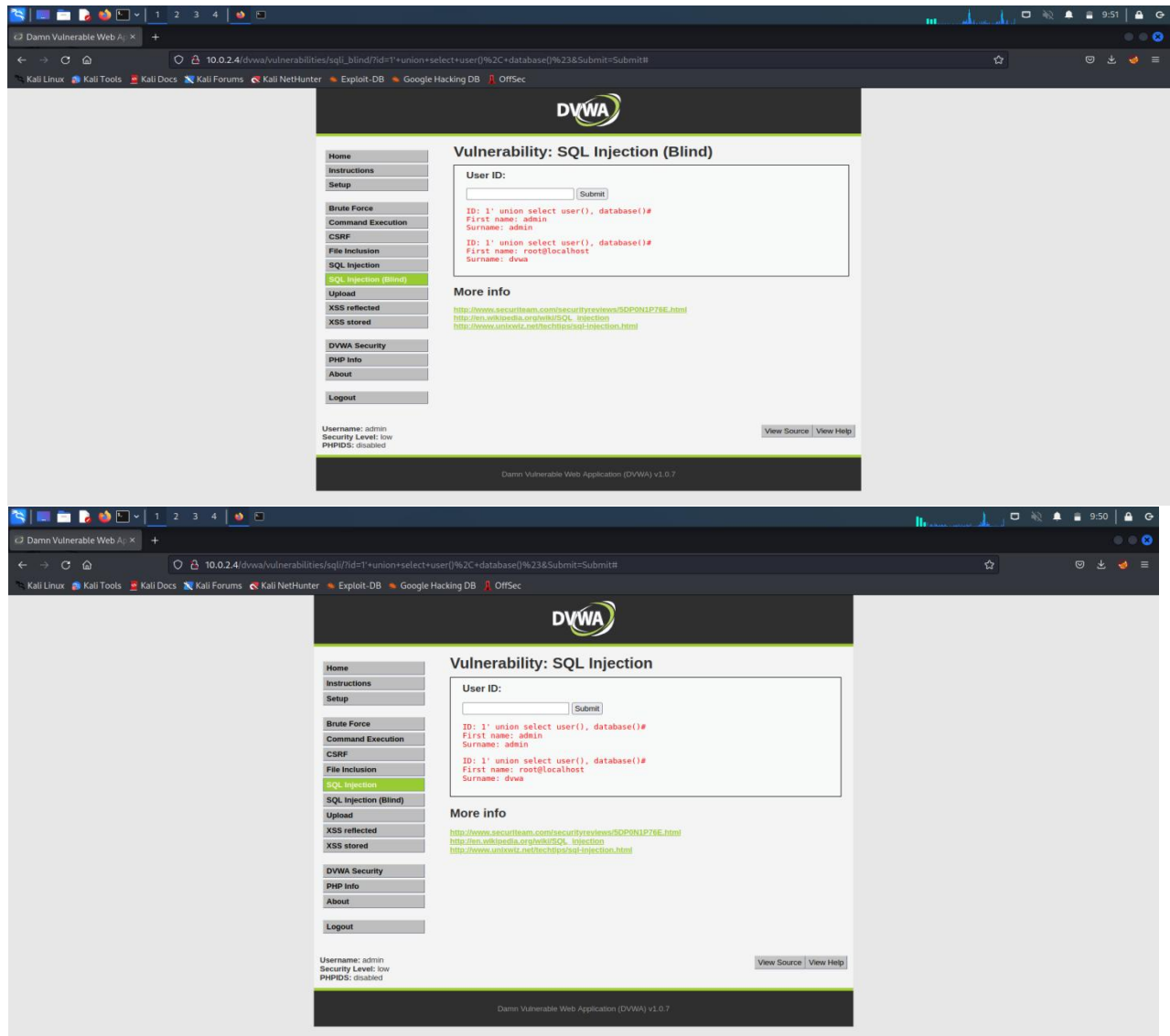
Step 3: Set the DVWA security to low.



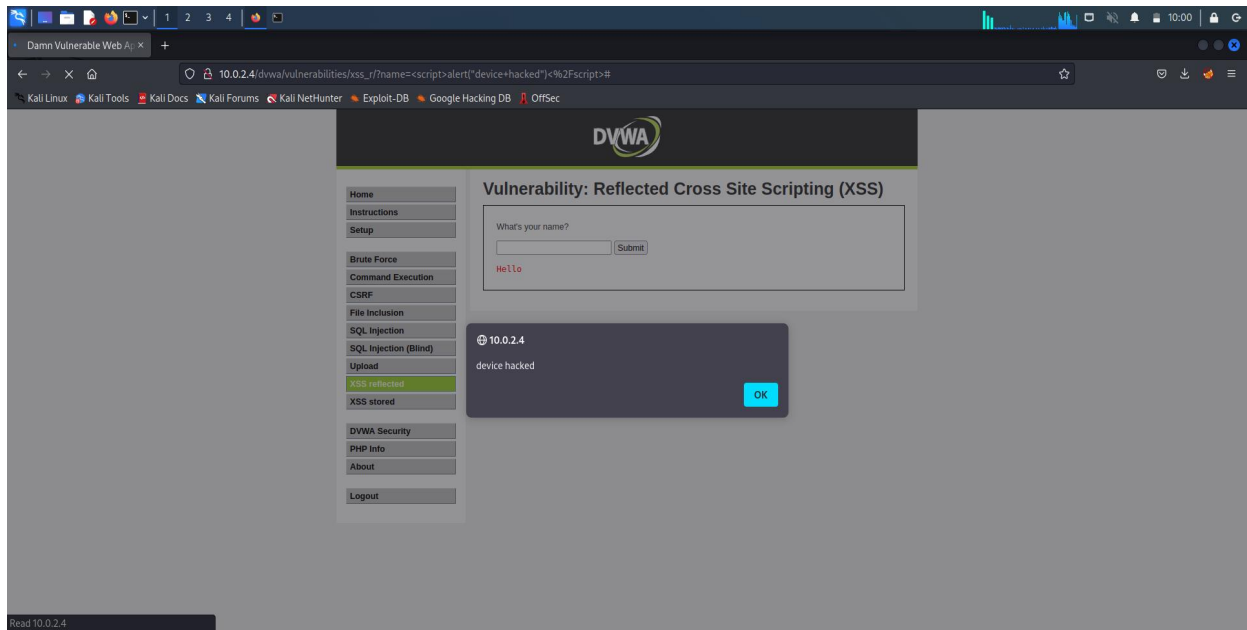
Step 4: SQL Injection – Process by passing the queries, so that we can get unauthorized access.

Step 5: SQL Injection (Blind)- also a kind of SQL injection used to attack data- driven applications using SQL statements.

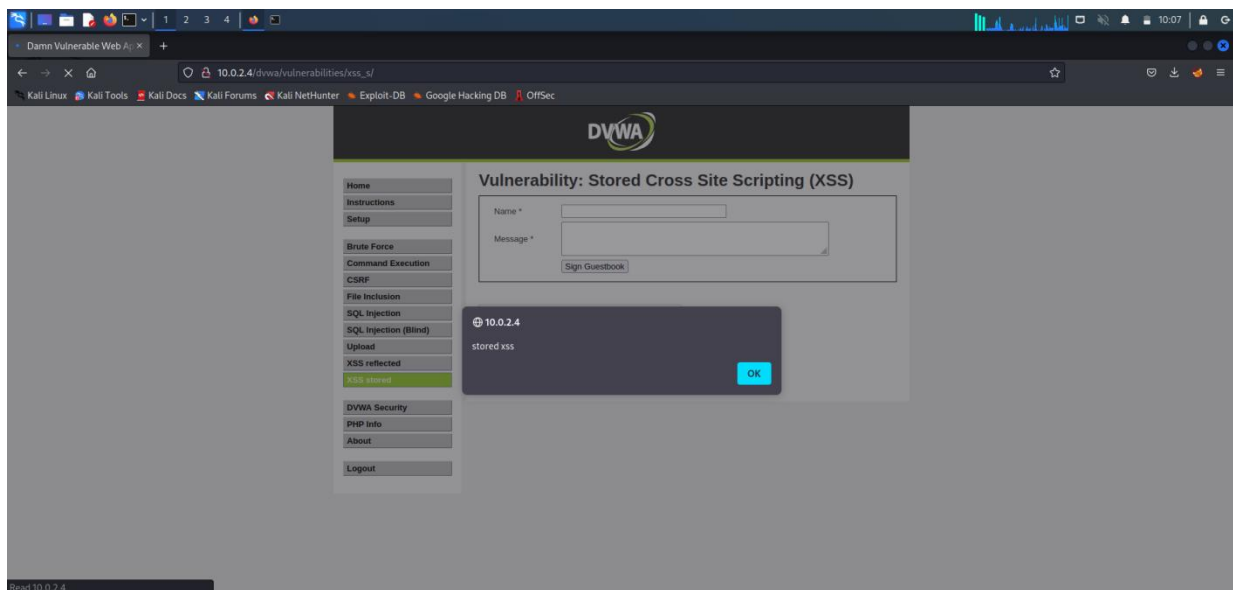
SQL statements are inserted into an entry field for execution.



Step 6: XSS reflected- This is used to add the script. `<script>alert("device hacked")</script>`. This change will be for temporary period of time.



Step 7: XSS stored - This is used to add the script, but the effect here is permanent.



Step 8: To check the vulnerability in the upload , we can upload any files that cause damage or hacking.

