

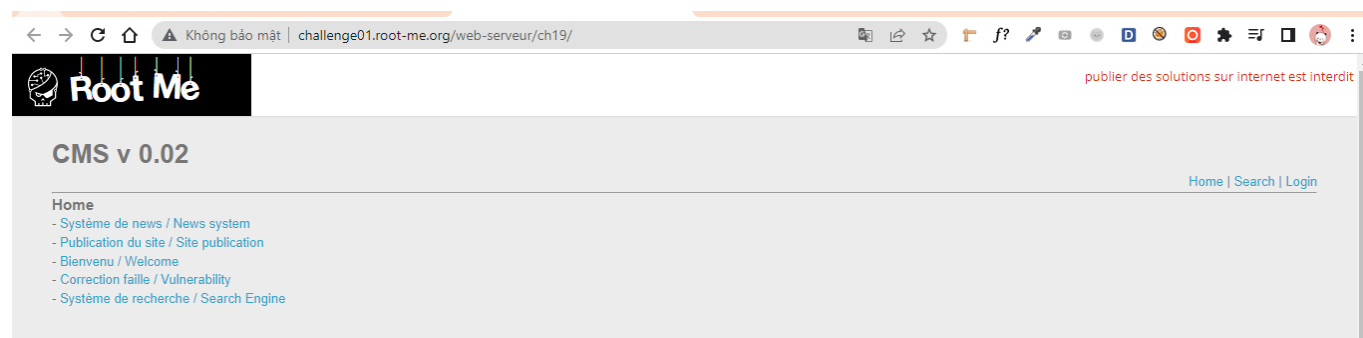
Write up challenge SQL injection - String

Tác giả:

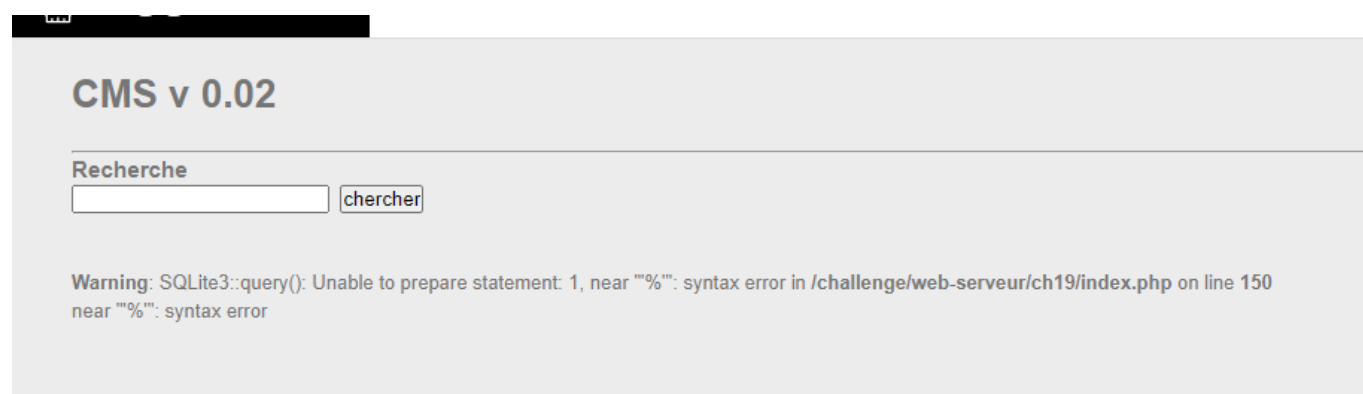
- Nguyễn Mỹ Quỳnh

[Link Challenge](#)

Truy cập challenge ta thấy gồm 3 trang Home | Search | Login



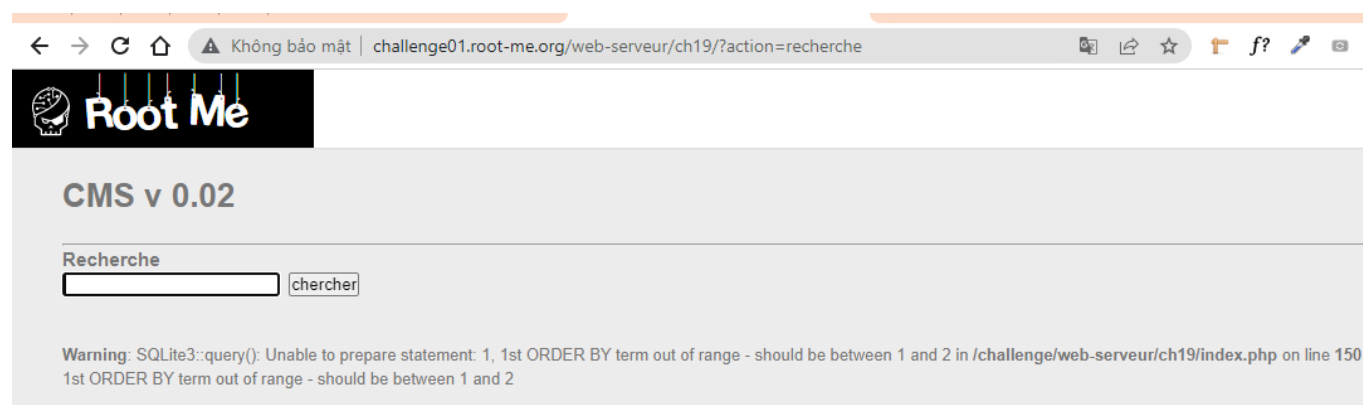
Sau khi test bằng cách nhập `1'` vào ô Recherche trong trang Search em thấy rằng lỗi SQL injection xuất hiện tại đây



Vậy là ta đã biết trang này sử dụng database là SQLite3.

Đầu tiên sử dụng lệnh: `1' order by 1--` để kiểm tra số cột cho phép.

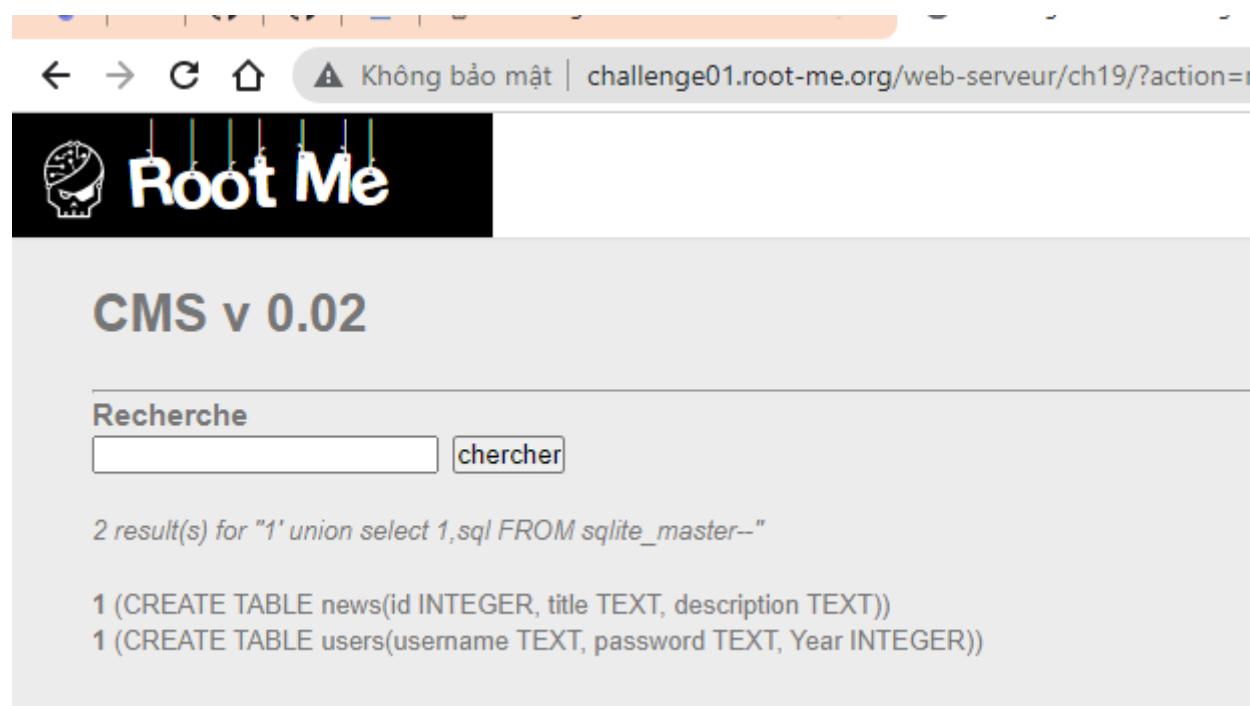
Tăng dần lên đến `1' order by 3--` thì bị lỗi



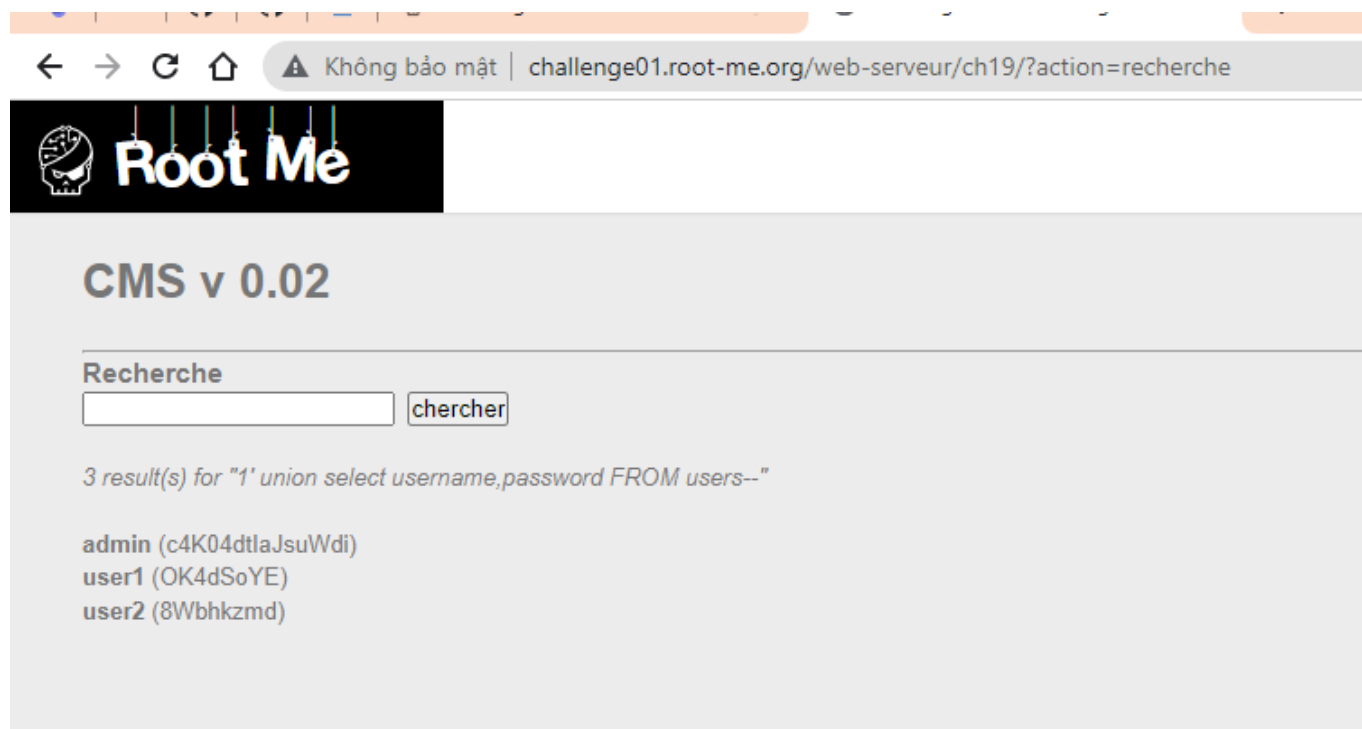
Vậy là database này có 2 cột. Tiếp theo kiểm tra xem cột nào có thể khai thác. Gõ lệnh: `1' union select 1,2--`



Ta thấy có thể khai thác ở cả hai cột. Tiến hành lấy tên table trong SQLite3 `1' union select 1,sql FROM sqlite_master--`



Lấy giá trị từ table users `1' union select username,password FROM users--`. Có được pass admin:



Submit thành công

SQL injection - String

30 Points 

CMS v 0.0.2

Author

g0uZ, 24 December 2012

Level ?








Statement

Retrieve the administrator password

[Start the challenge](#)

13 related ressource(s)

-  [Injection SQL \(Web\)](#)
-  [Blackhat Europe 2009 - Advanced SQL injection whitepaper](#) (Exploitation - We
-  [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 :-)



Flag: c4K04dtlaJsuWdi