

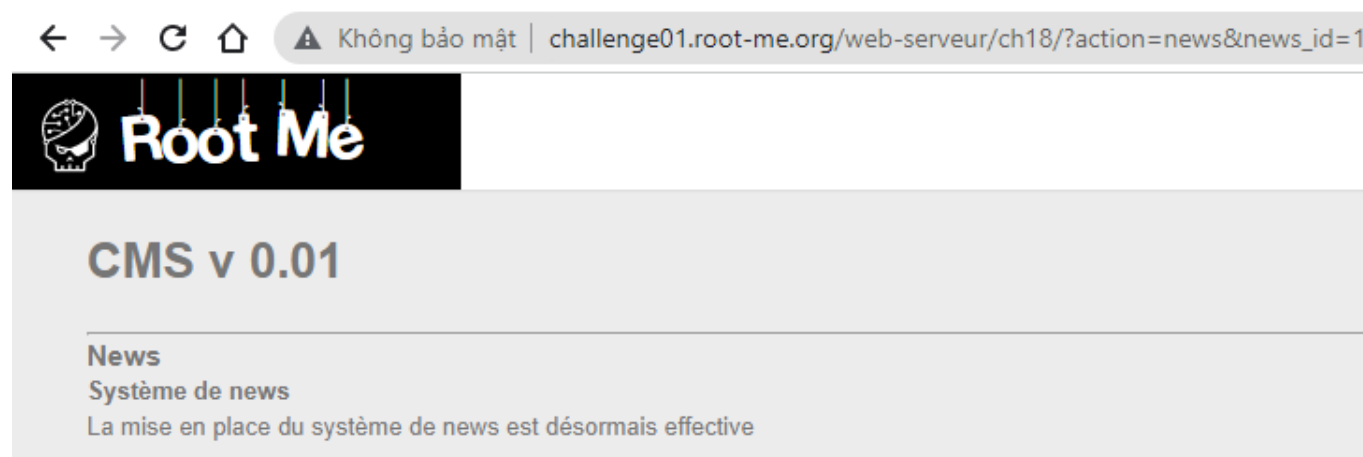
Write up challenge SQL injection - Numeric

Tác giả:

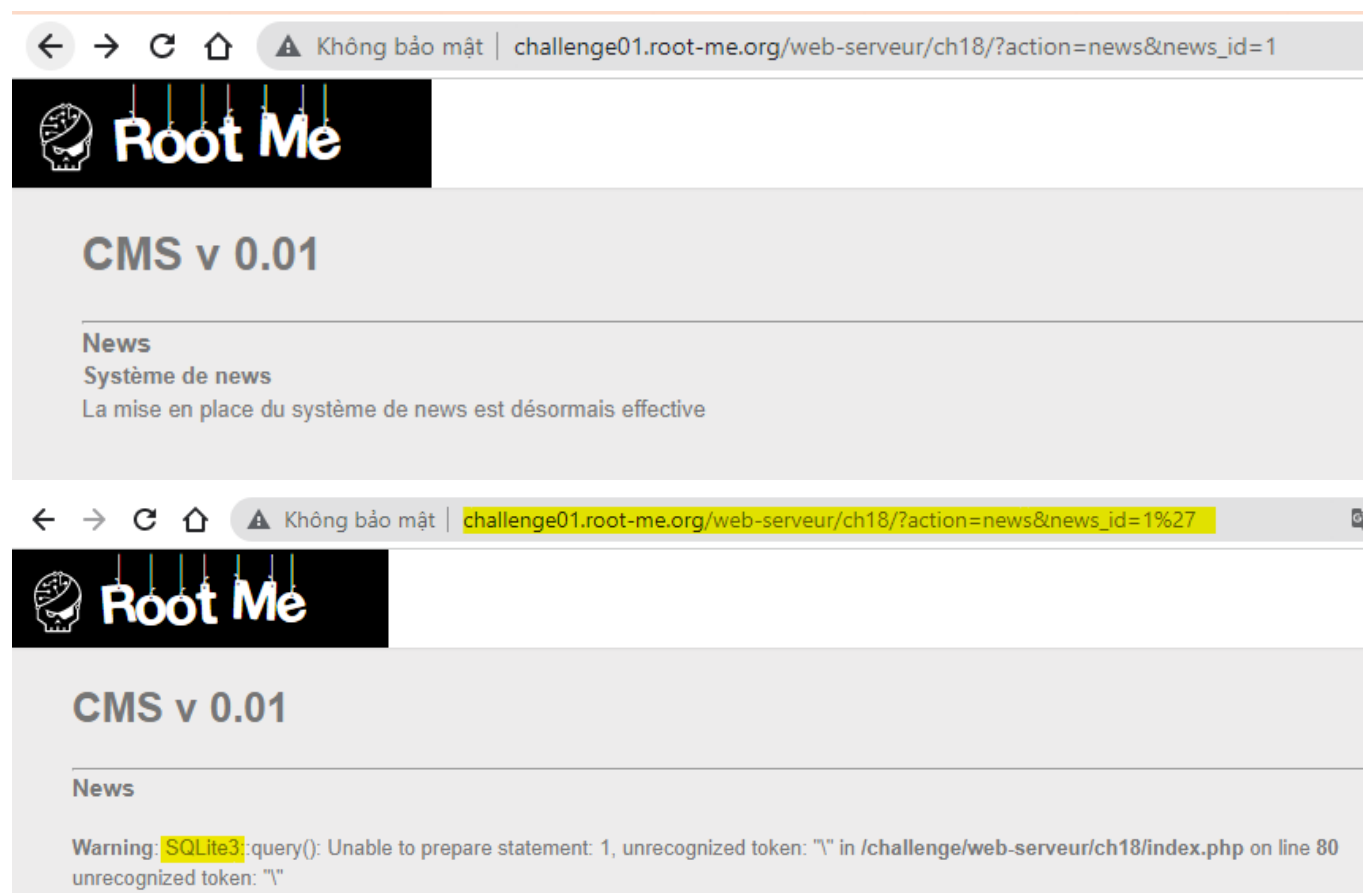
- Nguyễn Mỹ Quỳnh

[Link Challenge](#)

Truy cập challenge ta thấy gồm 2 trang Login và Accueil.

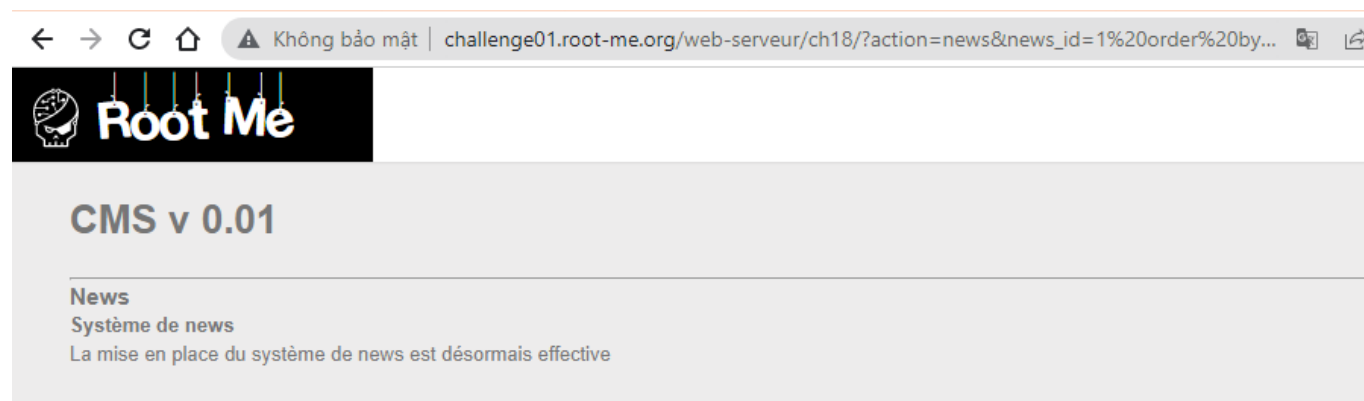


Tiến hành attack thử trang Système de news trong Accueil. Thêm ký tự ' vào sau số 1 thì ta phát hiện lỗi SQL injection

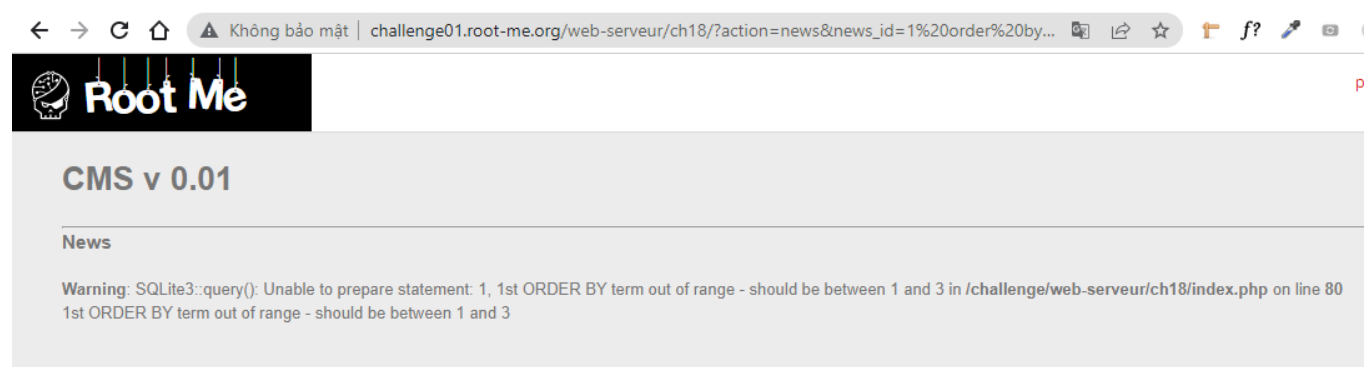


Vậy là ta đã biết trang này sử dụng database là SQLite3.

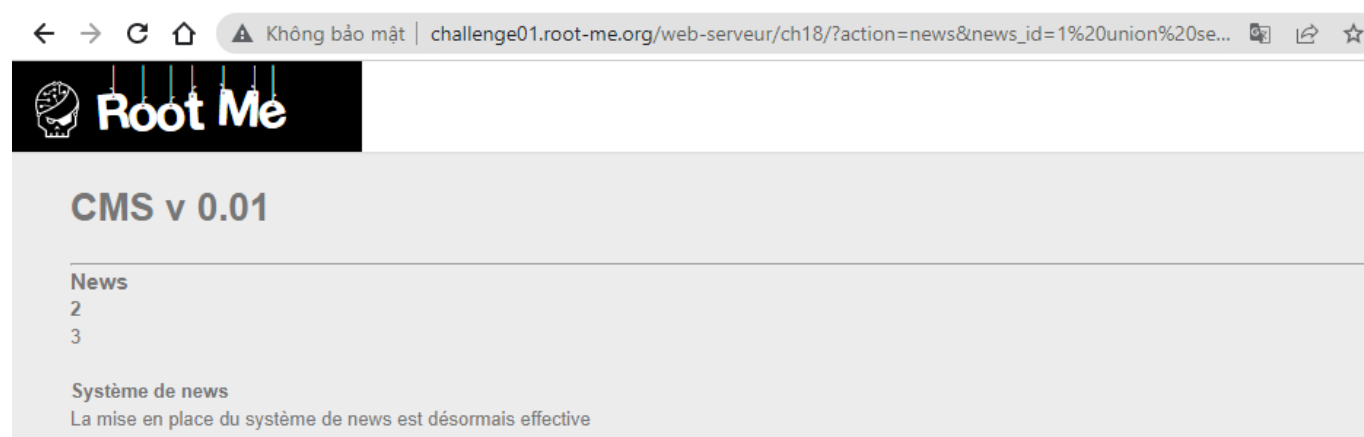
Đầu tiên sử dụng lệnh: `1' order by 1--` để kiểm tra số cột cho phép. Nhưng sau khi thử và thực hiện tiếp thì không có kết quả gì và tên bài này cũng là Numeric nên có vẻ dường như ký tự `'` không cần được sử dụng để ngắt chuỗi. Thử lại với `1 order by 1--`



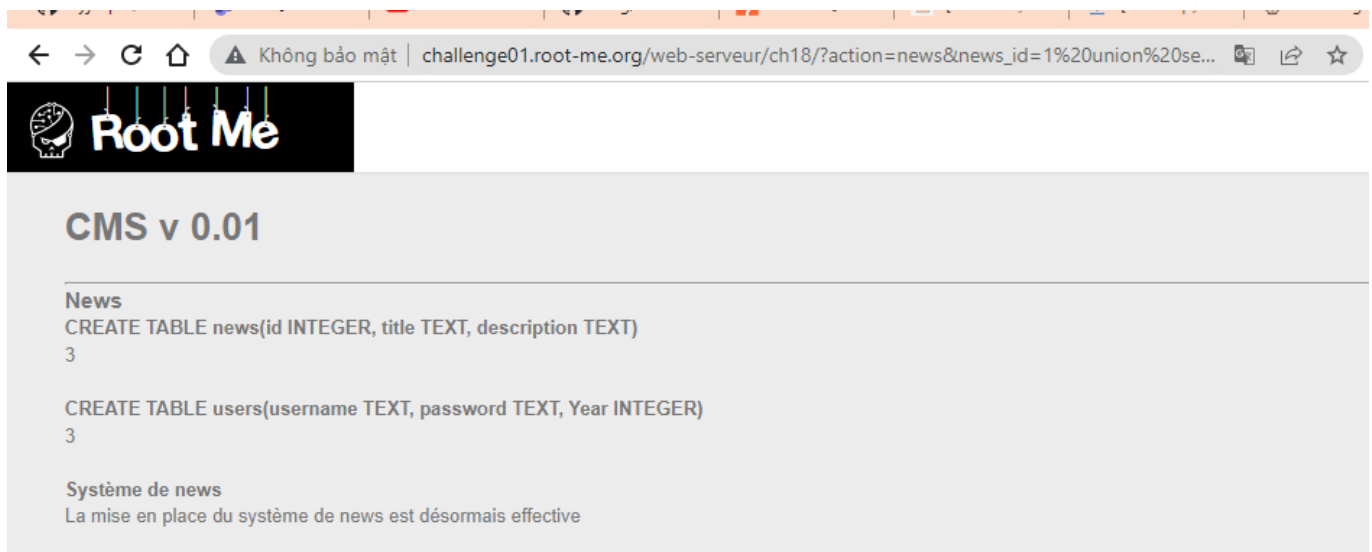
Đến `1 order by 4--` thì bị lỗi



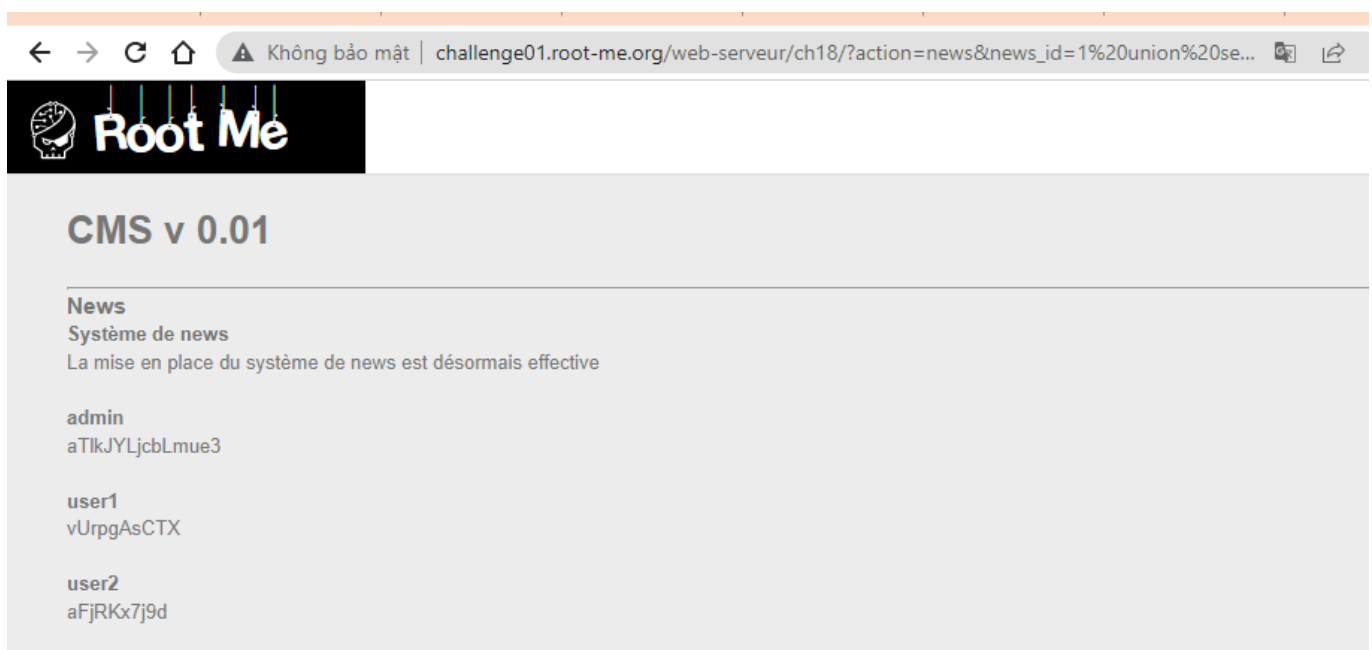
Vậy là database này có 3 cột. Tiếp theo kiểm tra xem cột nào có thể khai thác. Gõ lệnh: `1 union select 1,2,3--`



Ta thấy có thể khai thác tại cột thứ 2 và 3. Tiến hành lấy tên table trong SQLite3 `1 union select 1,sql,3 FROM sqlite_master--`




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





Submit thành công

SQL injection - Numeric

35 Points 

CMS v 0.0.1

Author Level 






g0uZ, 24 December 2012 

Statement

Retrieve the administrator password.

[Start the challenge](#)


13 related ressource(s)

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

Validation

Well done, you won 35 Points

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

 [twittez le !](#)

Flag: aTikJYLjcbLmue3