BÀI TẬP CTF

Bảo mật web và ứng dụng – NT213.M21.ANTN

Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

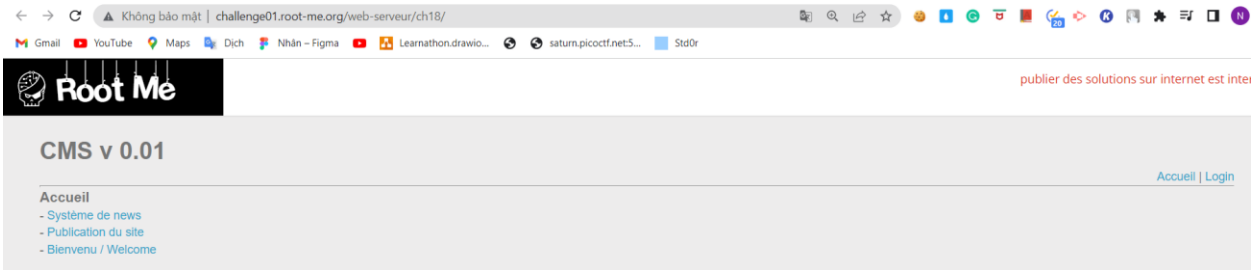
Sinh viên thực hiện: *19520199 – Lê Tôn Nhân*

Challenge 4: SQL injection - Numeric (level medium)

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

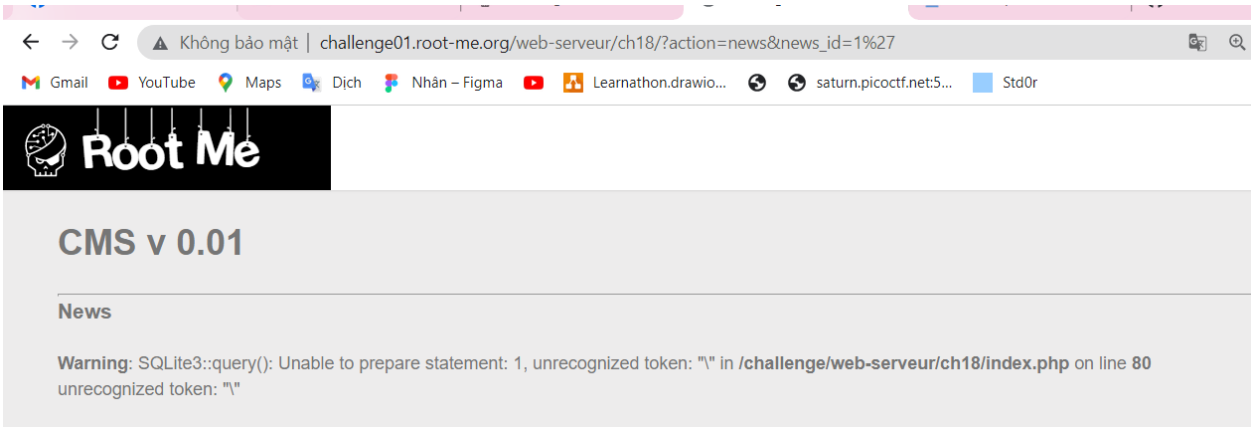
- Bài này yêu cầu ta lấy mật khẩu của administrator

- Truy cập vào challenge ta thấy được trang web như bên dưới



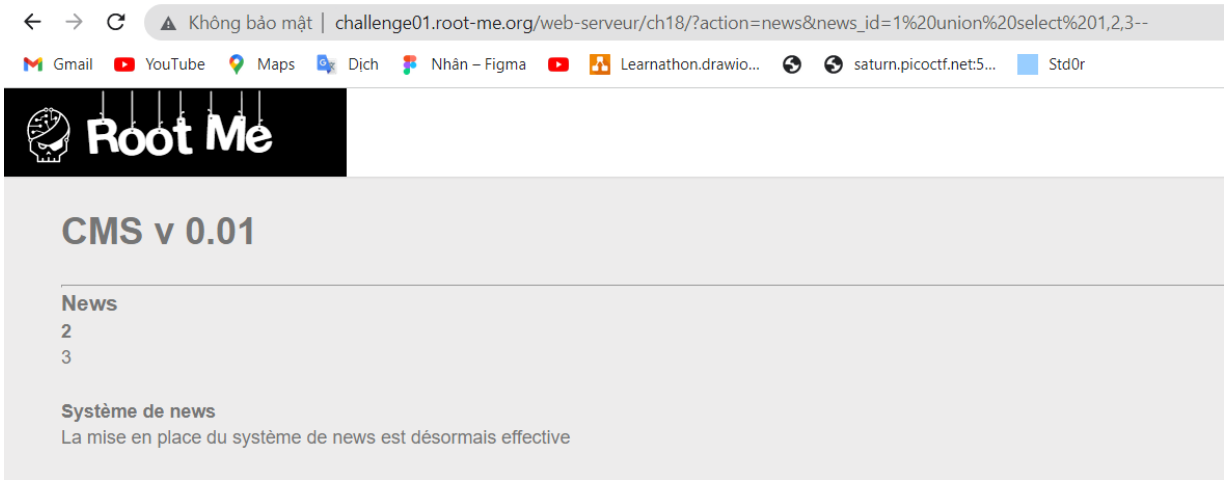
- Khi ta truy cập vào trang Système de news, trên url sẽ có **action=new&new_id=1**. Ở đây rất có thể xảy ra lỗi sqli khi ta GET dữ liệu

- Thử thêm ký tự ‘ vào sau số 1 và ta thấy lỗi xuất hiện. Do đó ta nhận định được rằng bài này xảy ra lỗi sqli khi ta GET dữ liệu, và ta có thể khai thác trực tiếp tại URL

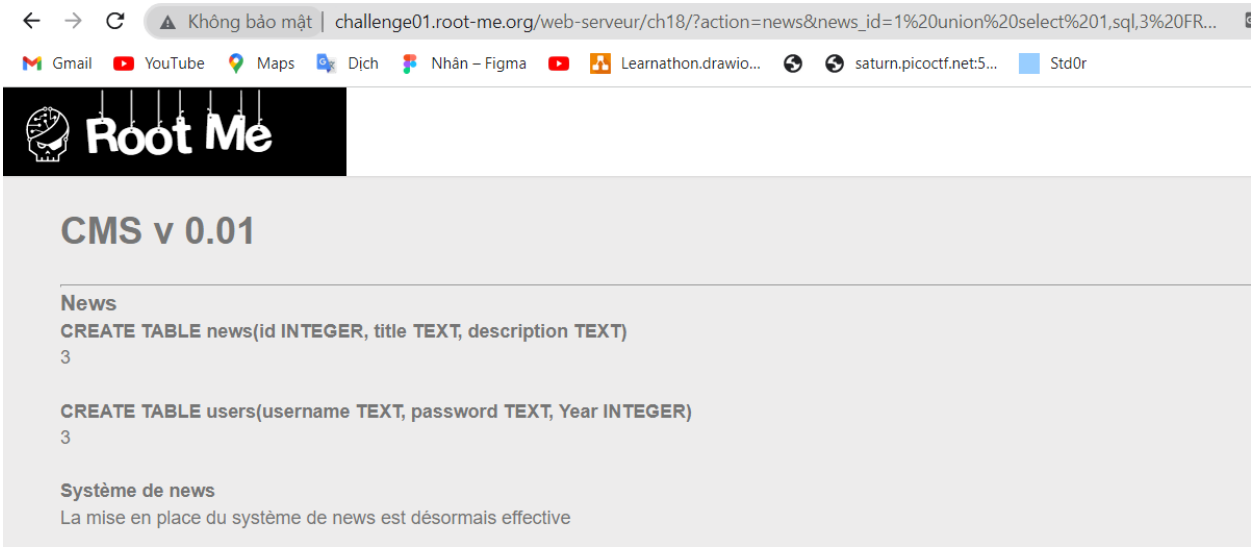


- Dựa vào dòng Warning ta biết được trang này sử dụng database là SQLite3. Giống với bài String ta sẽ sử dụng order by để có thể biết được số cột
- Đối với bài này có 1 lưu ý khác so với bài String là, ký tự ‘ sẽ không có ngắt chuỗi của ta. Đầu vào sẽ nhận 1 số và nếu sau đó là 1 chuỗi thì chuỗi đó sẽ được thực thi riêng. Vậy lệnh khai thác để xem số cột là **1 order by 1--**. Đến phép thử thứ 4 là **1 order by 4--** thì bị lỗi do đó trang này có 3 cột

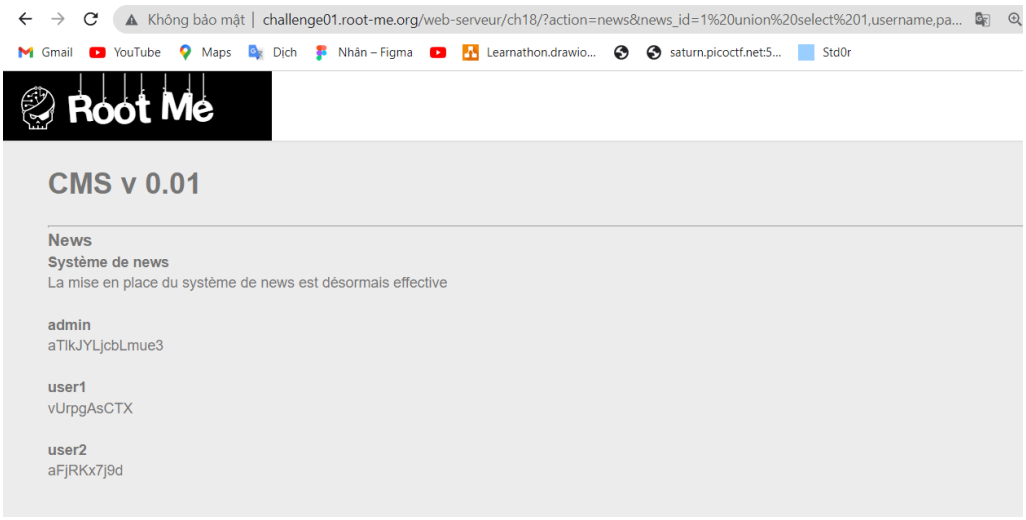
- Tiếp theo kiểm tra các cột này có thể khai thác được không bằng lệnh **1 union select 1,2,3--**



- Kết quả trả về cho ta thấy cột thứ 2 và 3 khai thác được. Tiếp tục ta sẽ lấy tên table bằng lệnh **1 union select 1,sql,3 FROM sqlite_master--**



- Kết quả cho ta biết, trang này có 2 bảng là news và user. Trong bảng users có chứa username và password. Cuối cùng ta thực hiện lấy giá trị của user bằng lệnh **1 union select 1,username,password FROM users--**



- Ta tìm được password của admin là **aTlkJYLjcbLmue3**

FLAG: aTlkJYLjcbLmue3