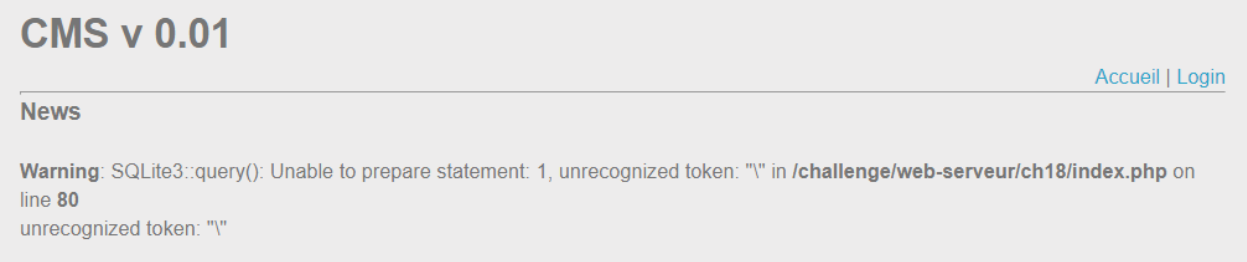
SQL injection - Numeric

Point: 35 Points

Description: Retrieve the administrator password.

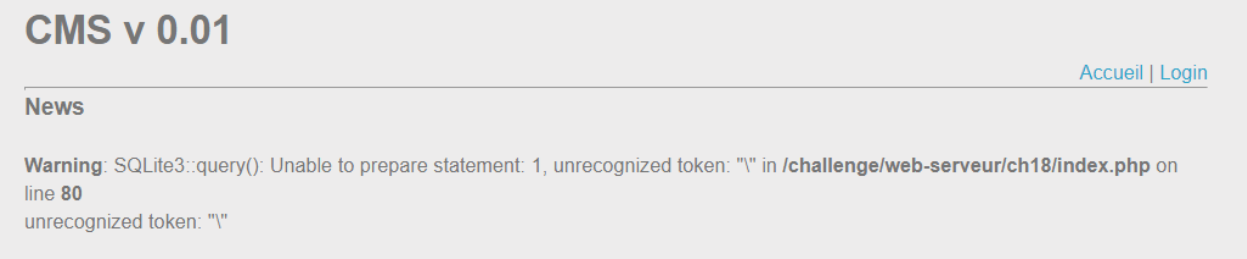
Solution:

Bài này gần giống bài "SQL injection – String". Chỉ khác chỗ input nằm ở đường dẫn trong trang "Home", vì nó có chứa một số parameter để truy vấn. Thử chèn '1 vào news_id. Ta có: news_id='1



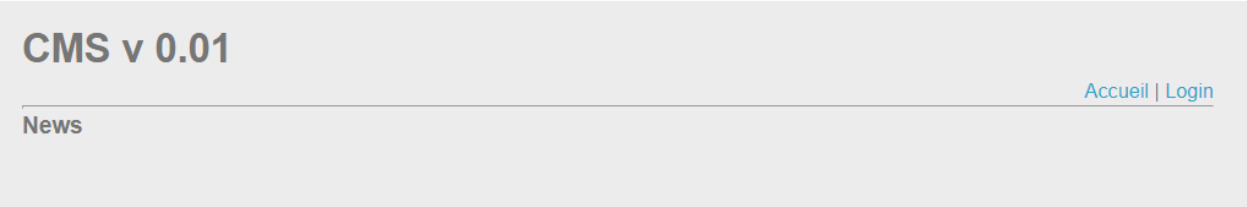
Có lỗi, vậy là có thể SQLi tại đây. Thử :

123' or 1=1 --



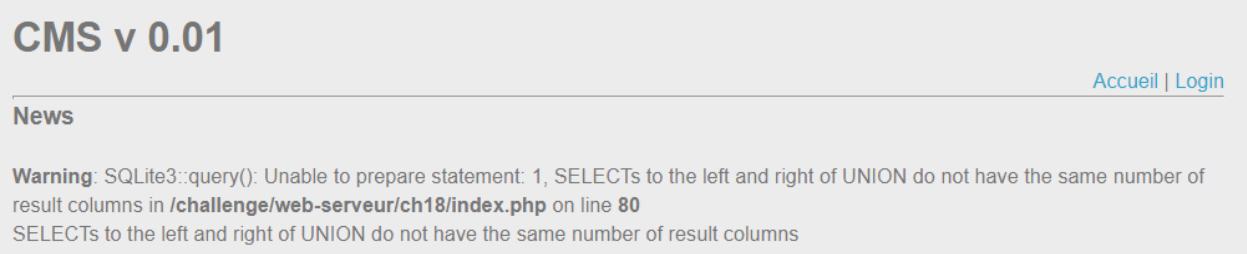
Bị lỗi. Ta nhớ lại tên đề bài là Numeric, vậy là chỉ có thể nhập số, còn nếu ta cố gắng escape chuỗi bằng nháy đơn hoặc nháy kép thì sẽ bị thay thế với **backslash "\"**. Nhập vào:

123 order by 1



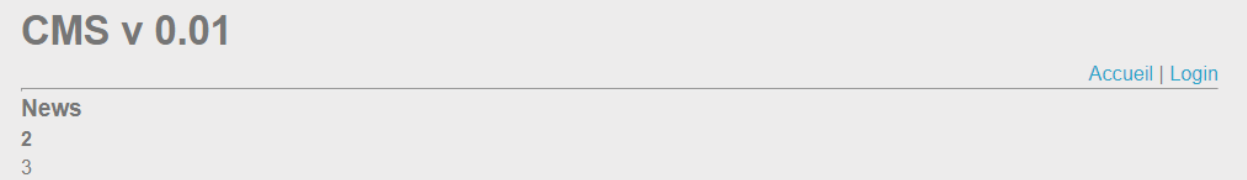
Không lỗi. OK ! Giờ ta làm tương tự bài trước. Xác định số cột trả về

123 union select 1



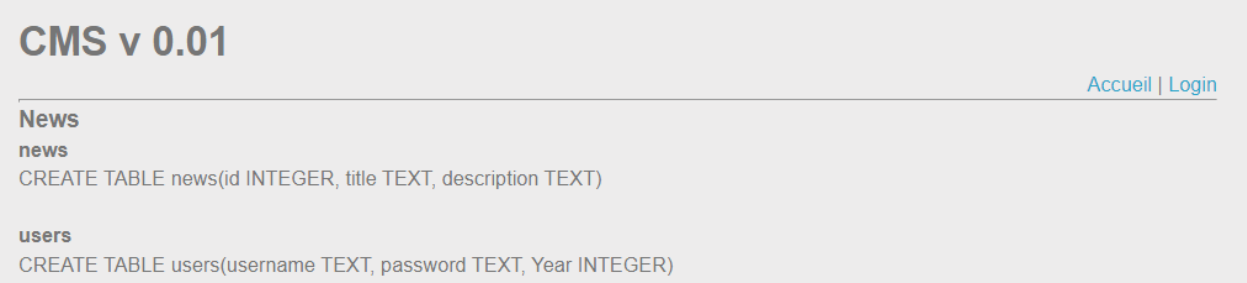
Tăng thêm số lượng cột thêm 1 cho đến khi thành công

123 union select 1, 2, 3



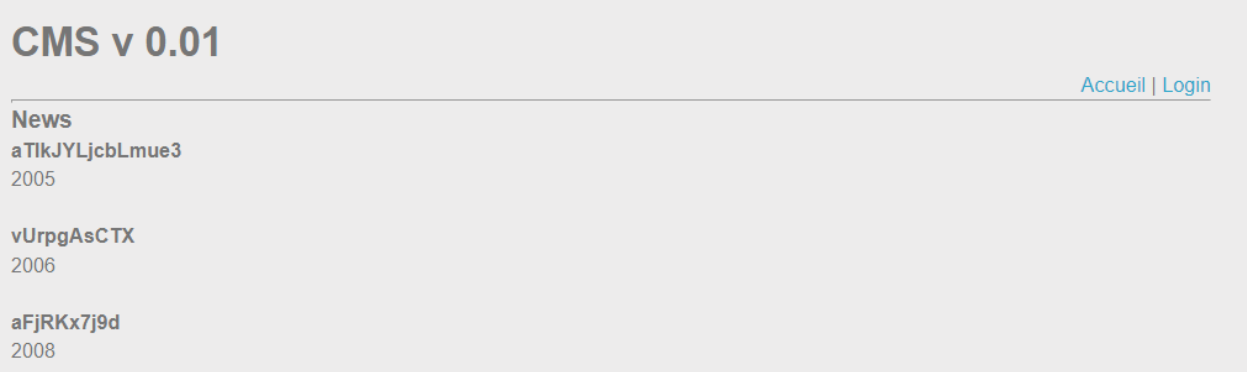
Lấy thông tin từ các **system table**

123 union select type, name, sql from sqlite_master



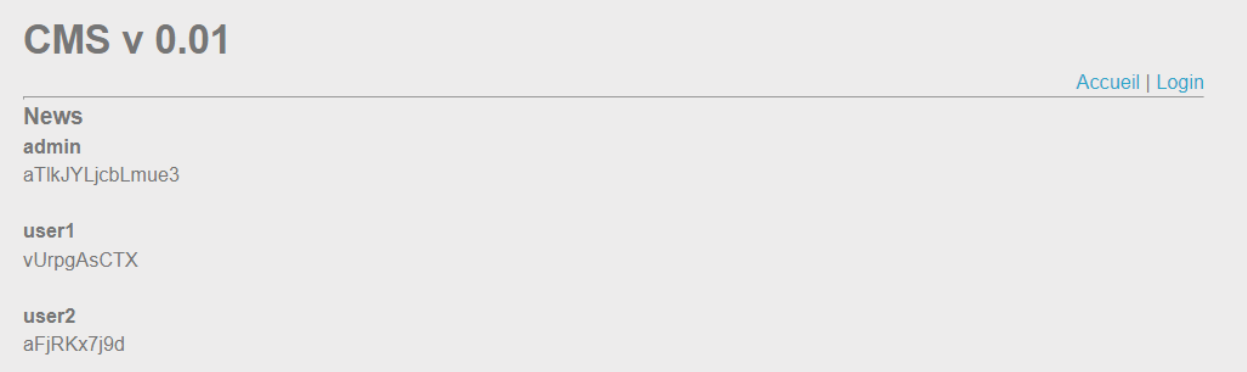
Chúng ta đã biết có bảng **user**. Thực hiện lấy thông tin bảng

123 union select username, password, year from users



Không có hiển thị **username** để xác định **admin**. Nhưng mình có thể thử từng cái vì số lượng ít. Còn không thì ta để ý chỉ có cột 2 và 3 được xuất. Vậy cột một mình điền đại 1 giá trị gì đó, và đưa username và password vào cột 2, 3

123 union select 1, username, password from users



Flag: **aTlkJYLjcbLmue3**