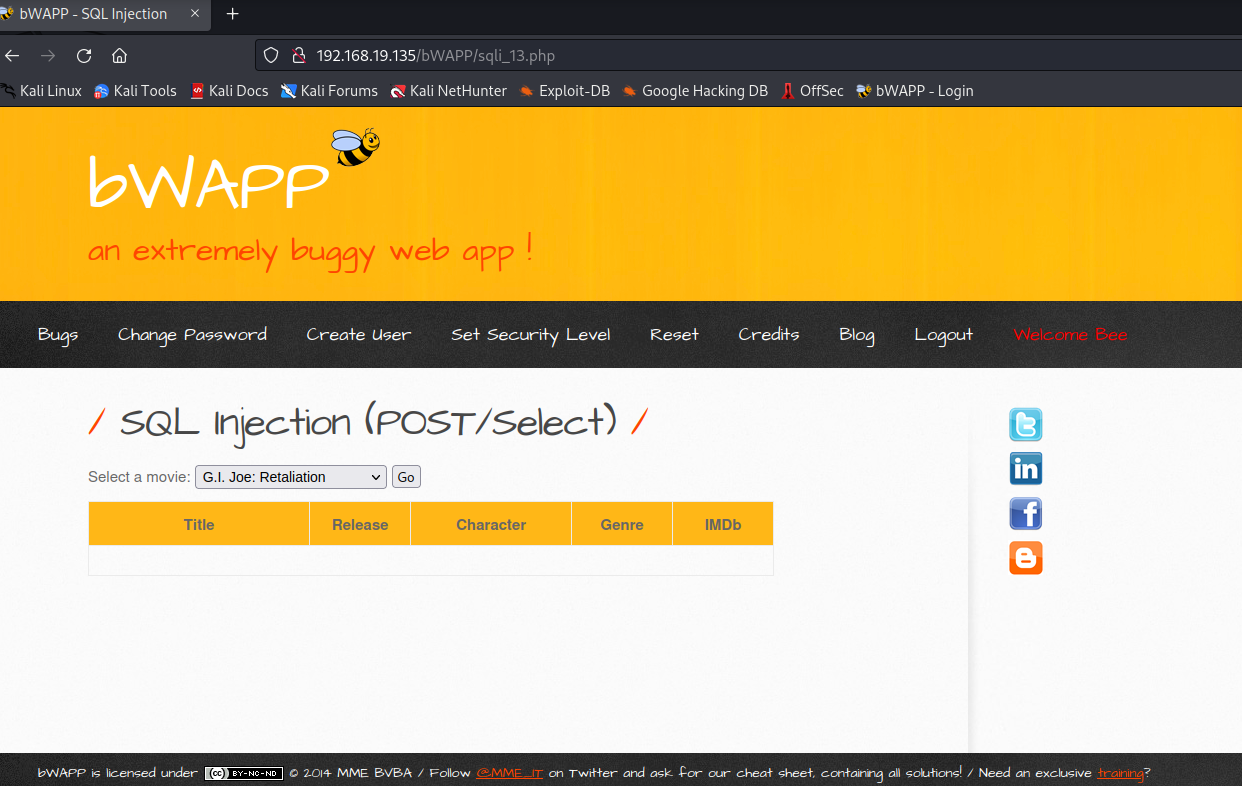
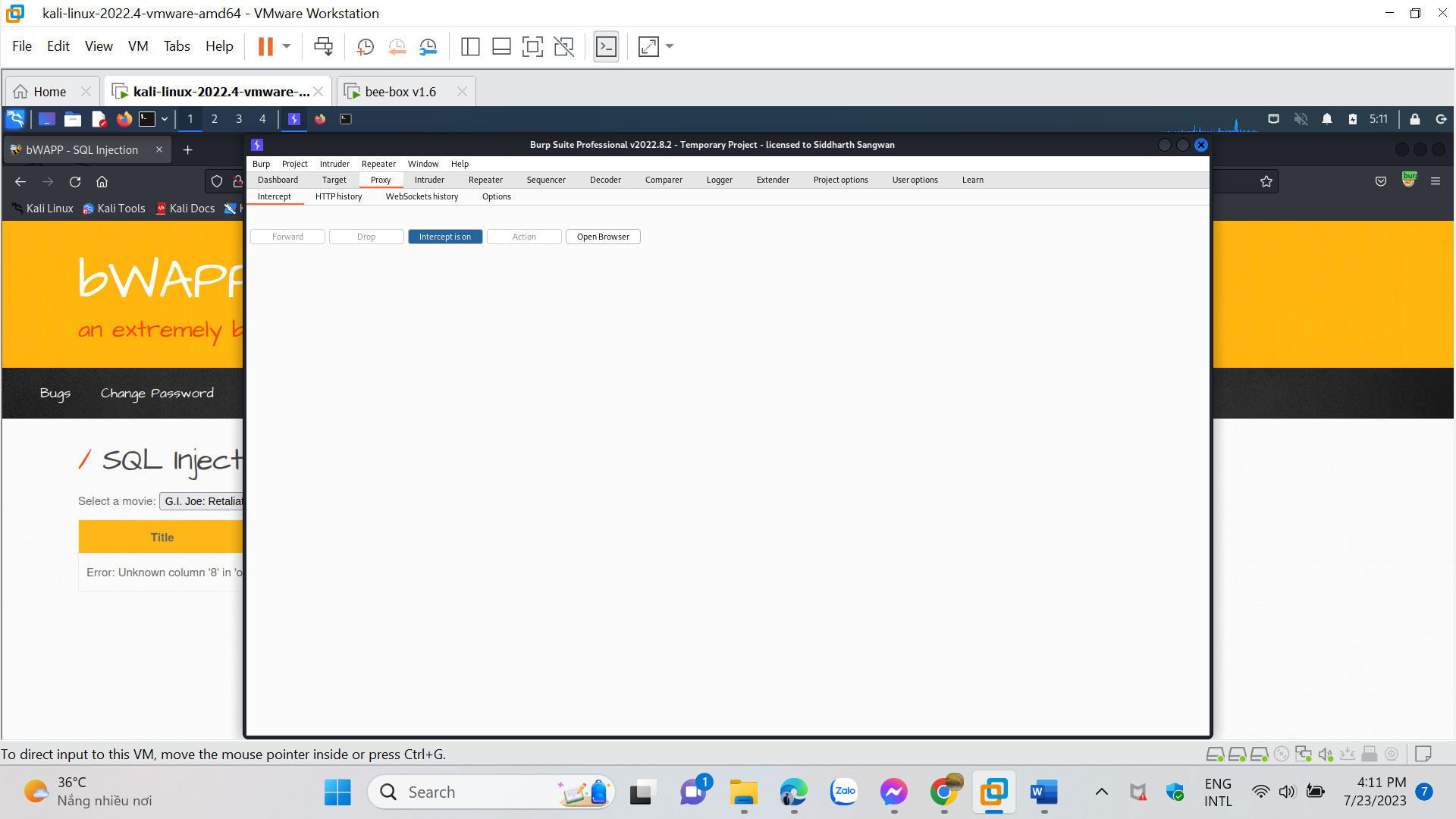
**SQL Injection ( Post/Select)**

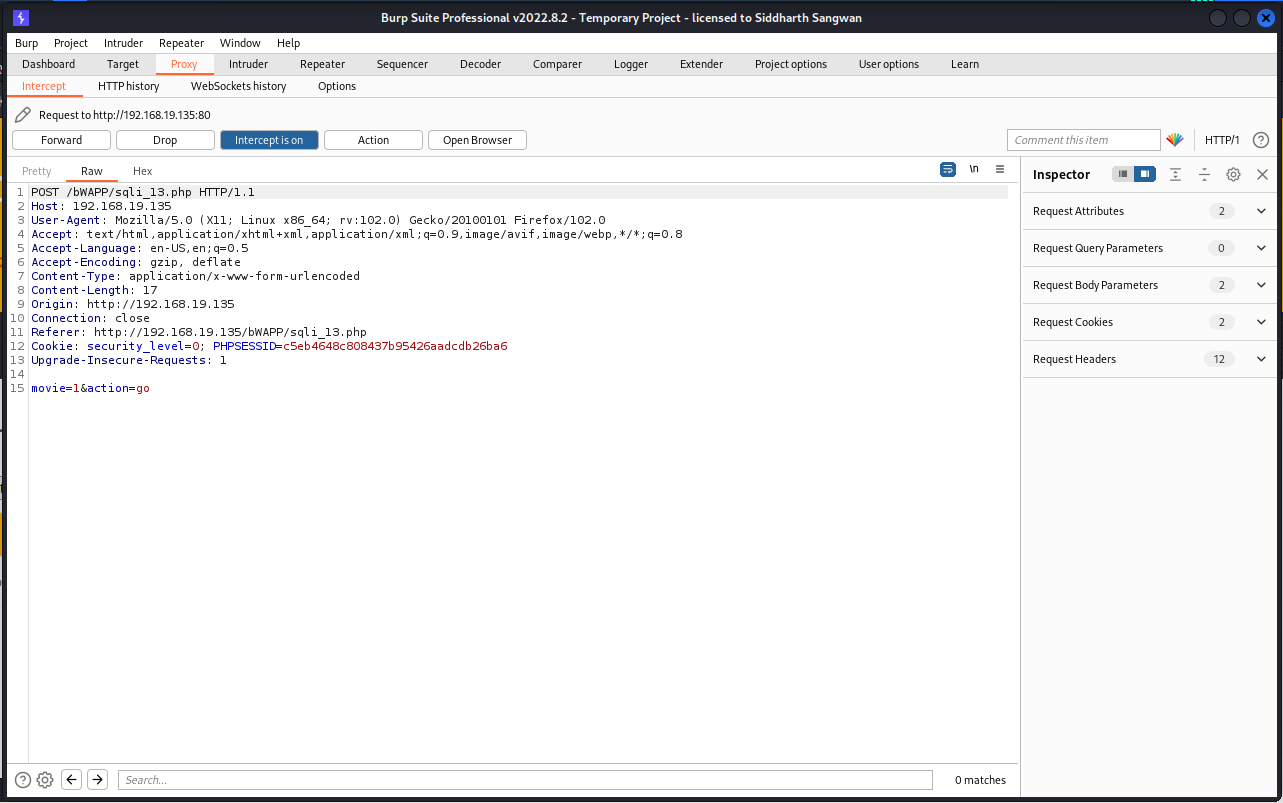
Giao diện bài lab.



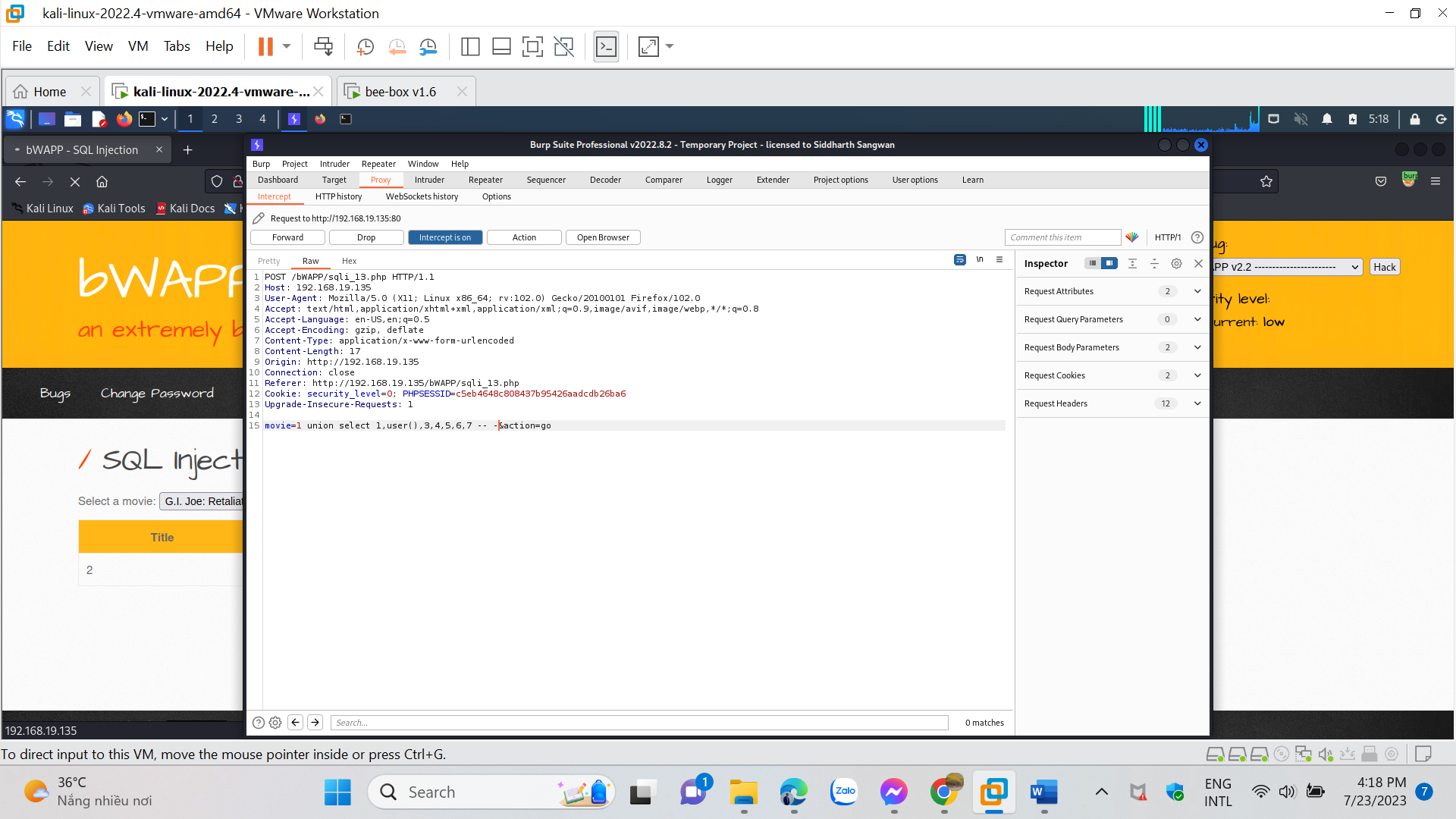
ở bài lab lần này, ta sẽ không thể trực tiếp thực hiện sql injection trên web. Vì vậy ta sẽ sử dụng burp-suite để thao tác bài lab này



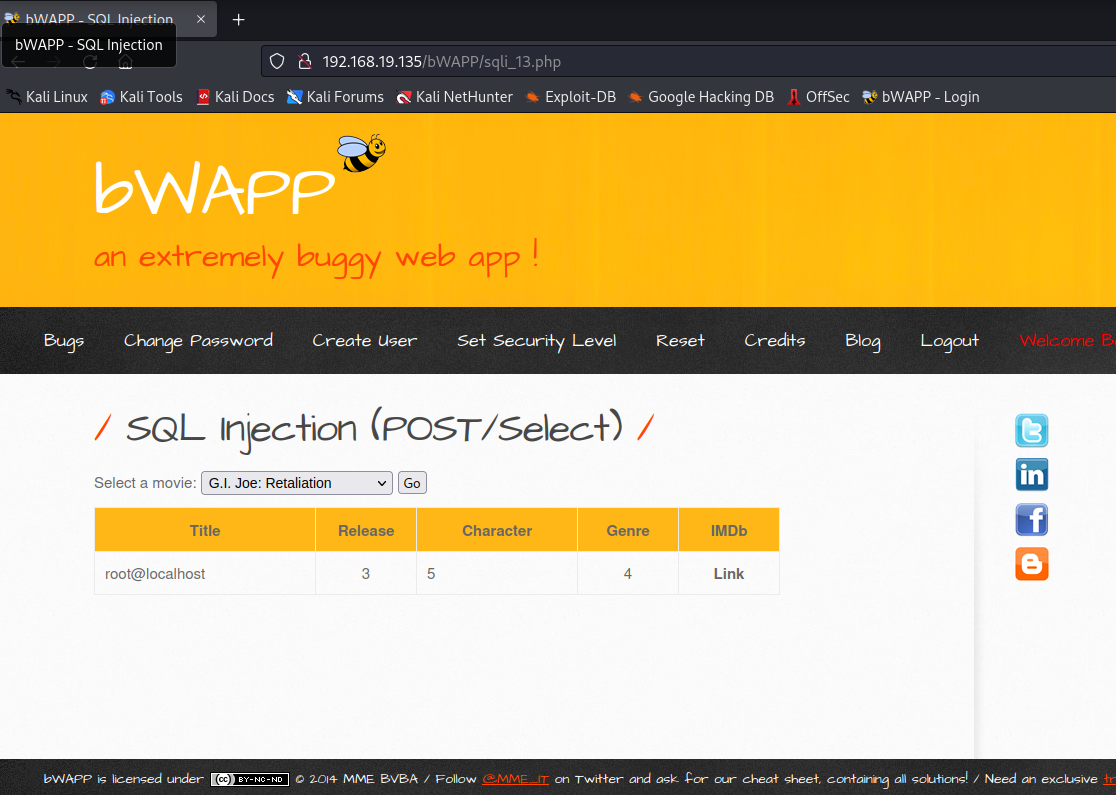
ở đây burp suite của mình đã được kết nối tới trang web. Mở proxy, ở mục intercept, turn on the intercept. Đồng thời ở bài lab thực hiện post



Tại đây thực hiện tương tự như các bài lab sql trước.



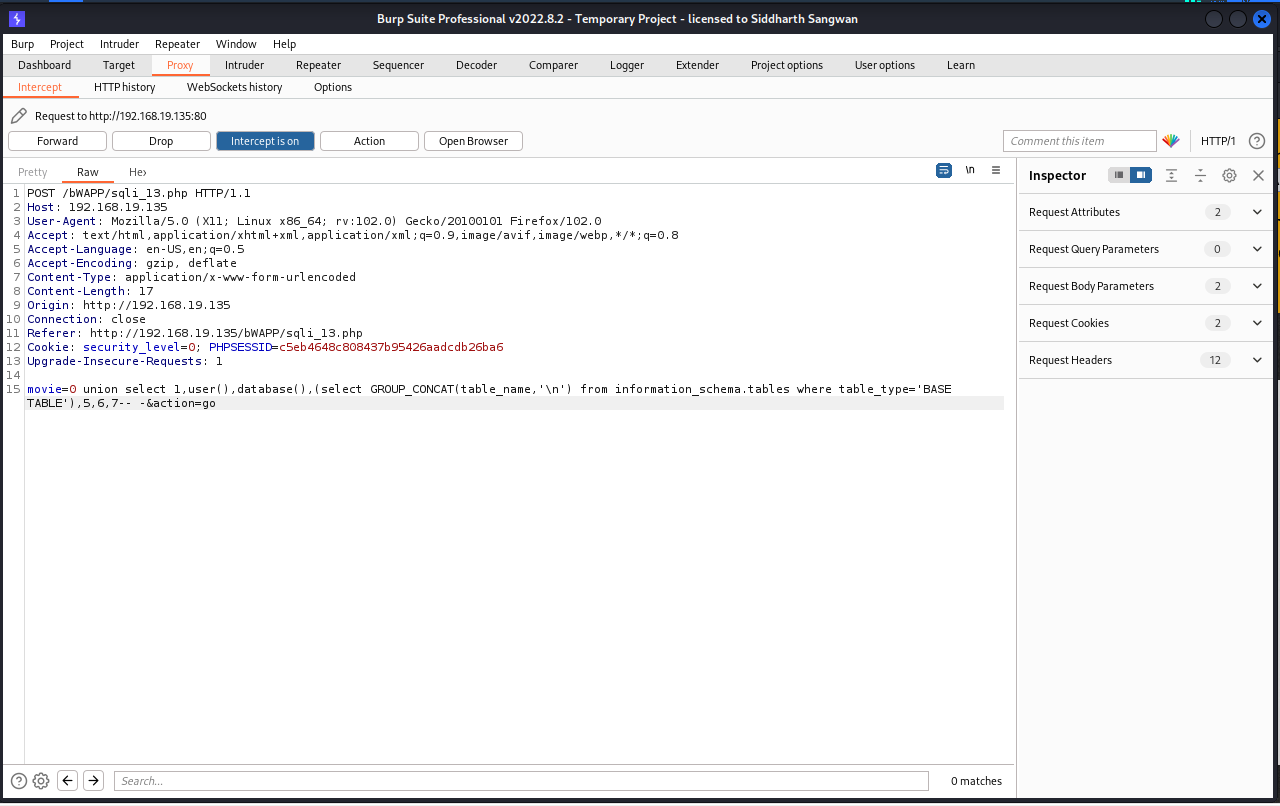
Mình sẽ thử lấy user từ hệ thống qua query union select 1,user(),3,4,5,6,7-- -.sau đó forward

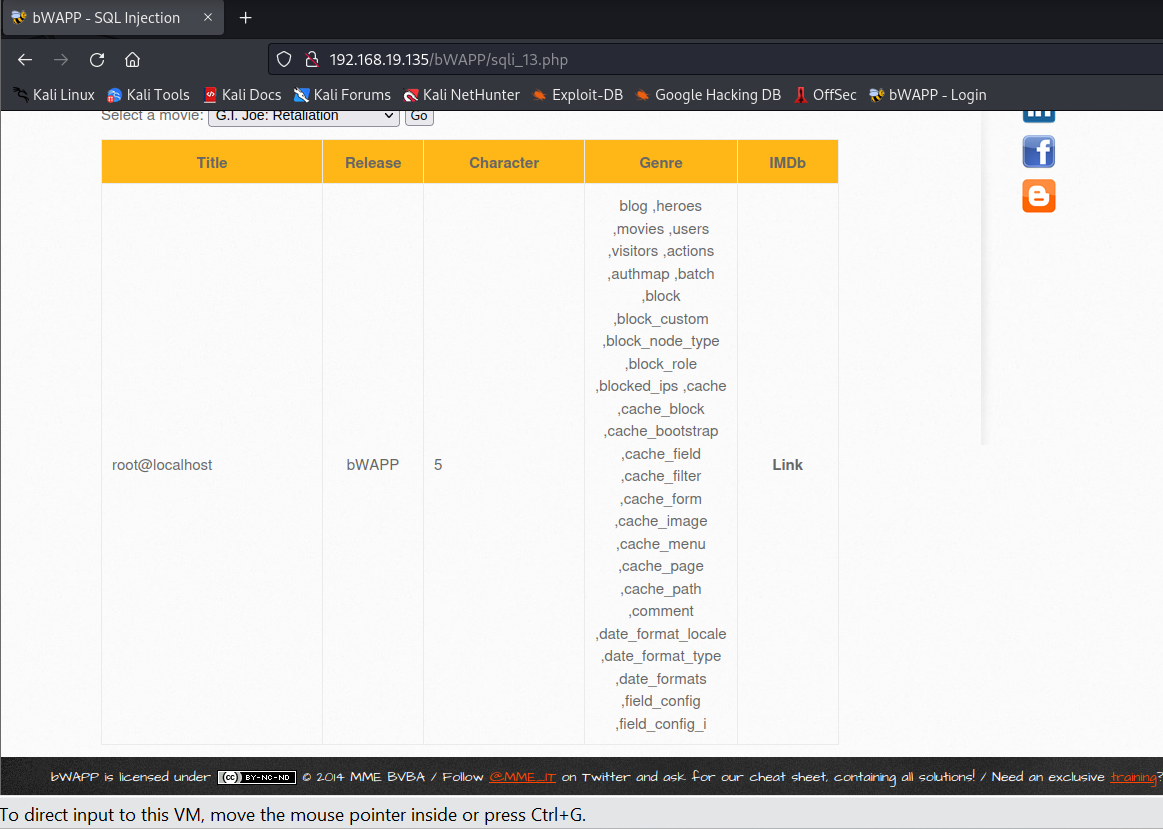


Web sẽ trả về thông tin user.

Ta sẽ thử lấy thông tin các bảng cùng với database và user qua query

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





Vậy là ta đã khai thác thành công trang web .Bài lab lần này có chút thay đổi là phải dùng burp-suite để khai thác. Tuy nhiên cách khai thác không hề thay đổi so với các bài lab trước đó.