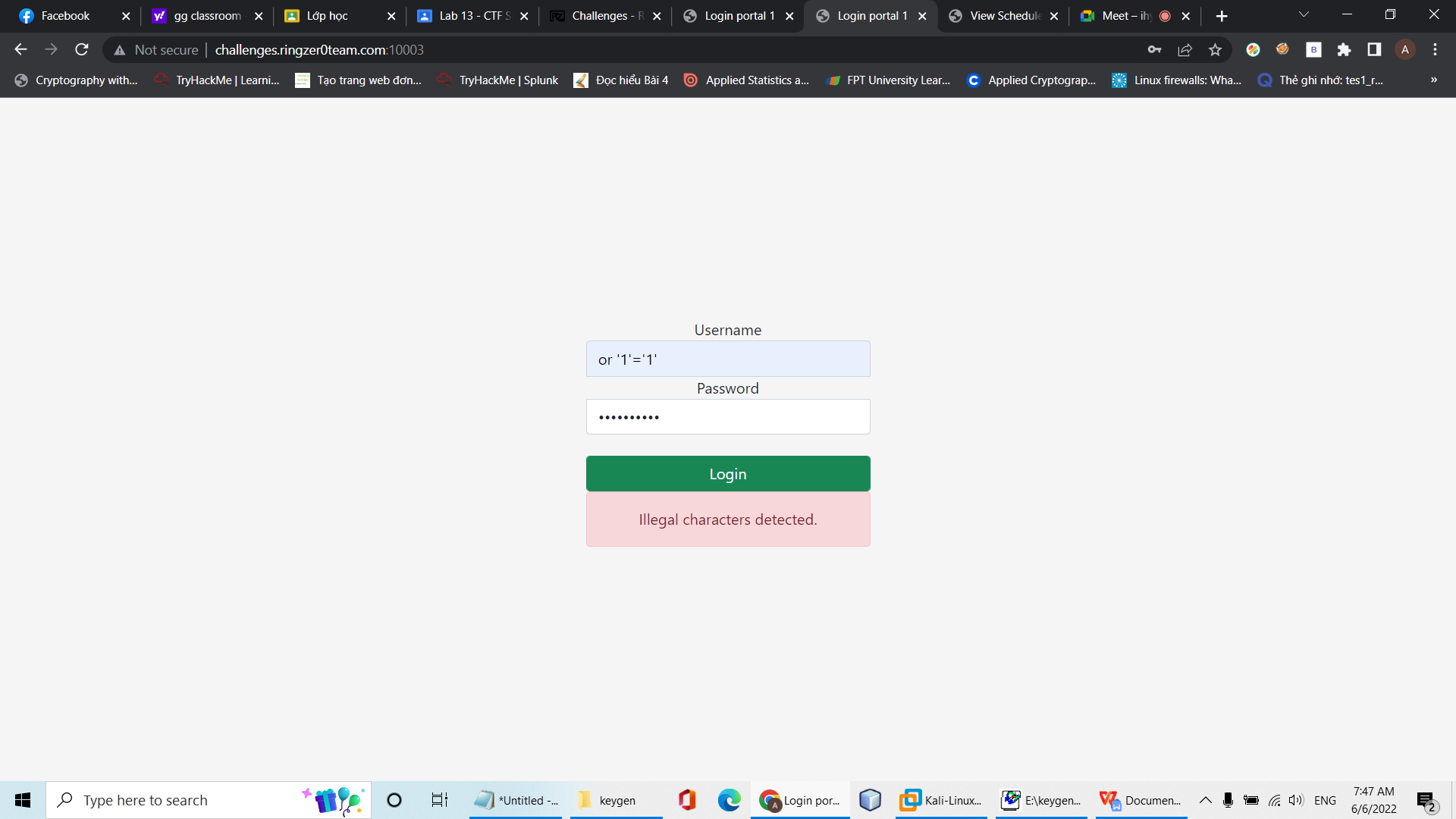
|  |  |
| --- | --- |
| Class | IAW301 |
| Name | Trần Ngọc Anh |
| IC No. | HE151461 |
| Date & Time | 6/6/2022 |

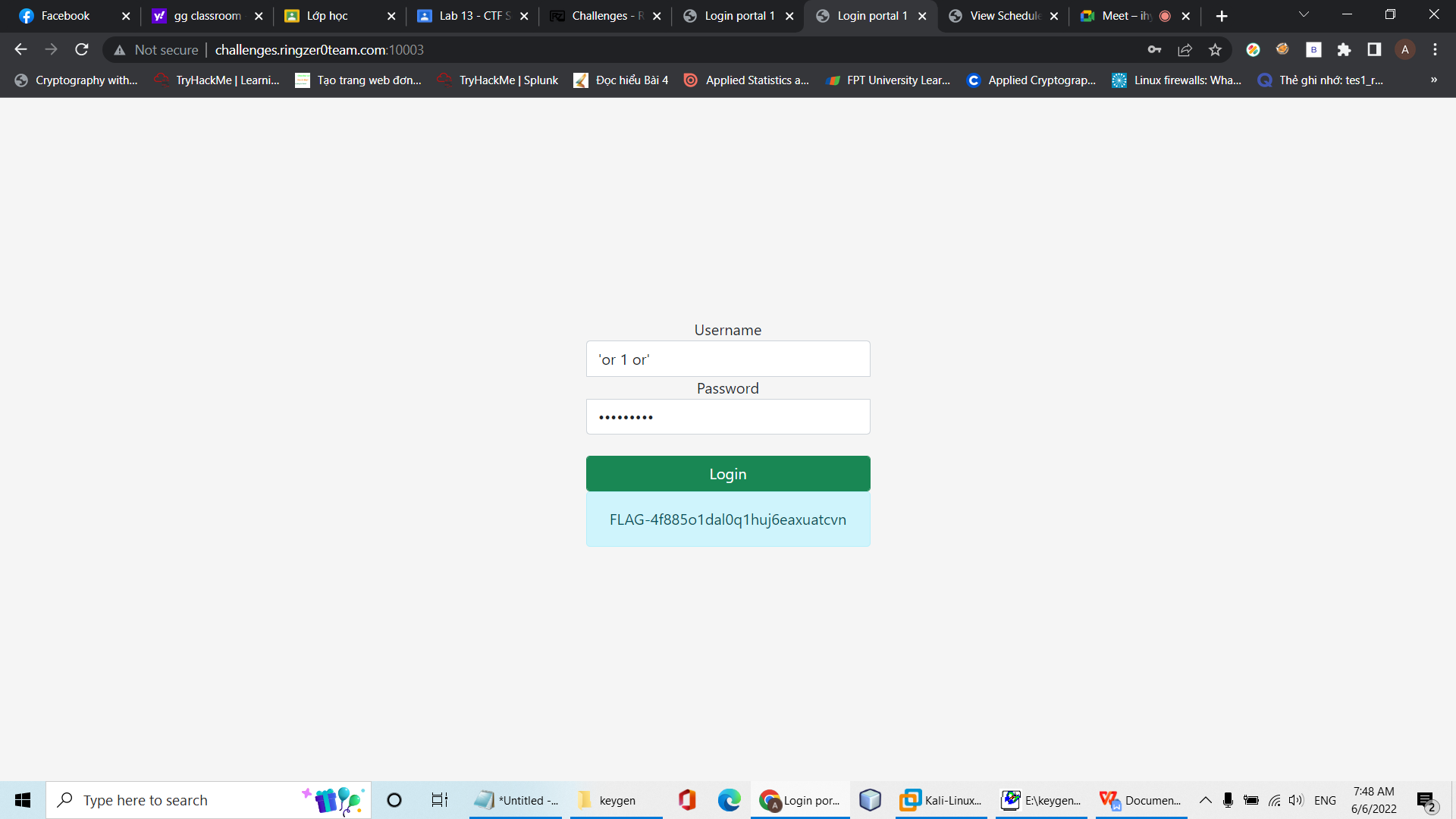
# Lab 13 - CTF Sql Injection

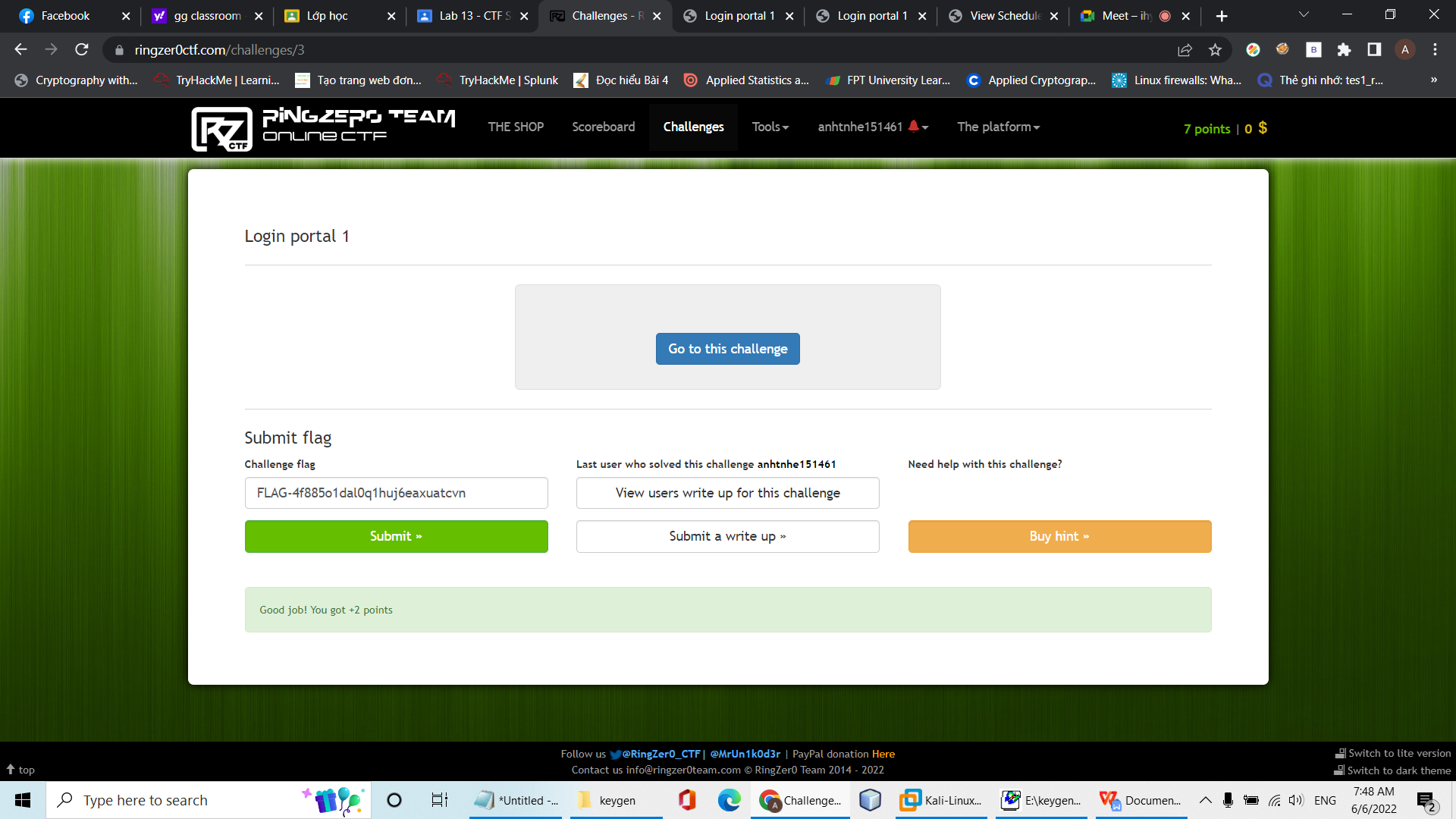
1. **Login portal 1**

- Ở đây sau khi thử thì chúng ta thấy dấu ‘=’ không hợp lệ.



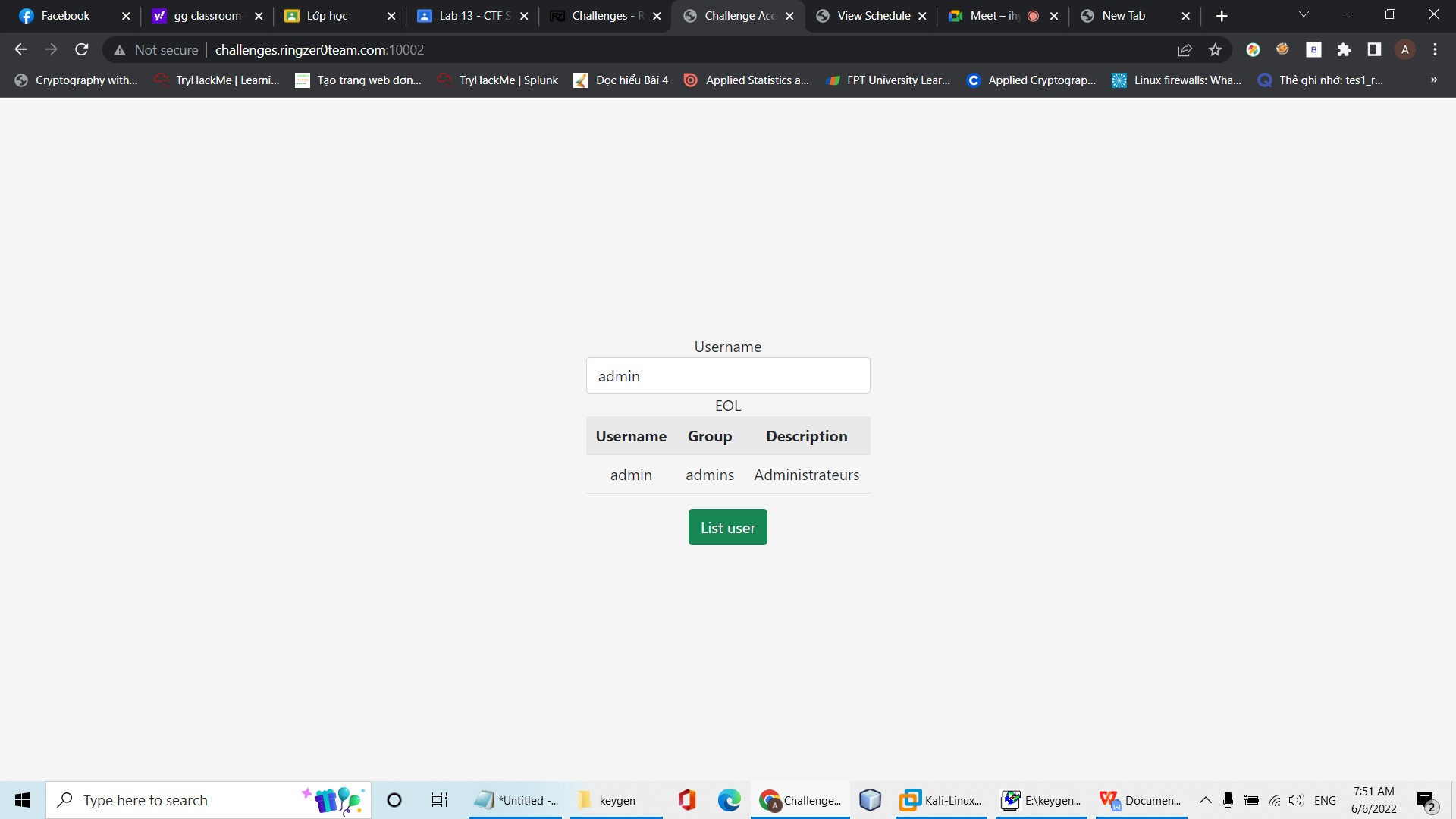
- Vì vậy chúng ta sử dụng một đoạn mã khác để tạo ra câu truy vấn sql luôn đúng và không dùng dấu ‘=’ thì sẽ lấy được flag.

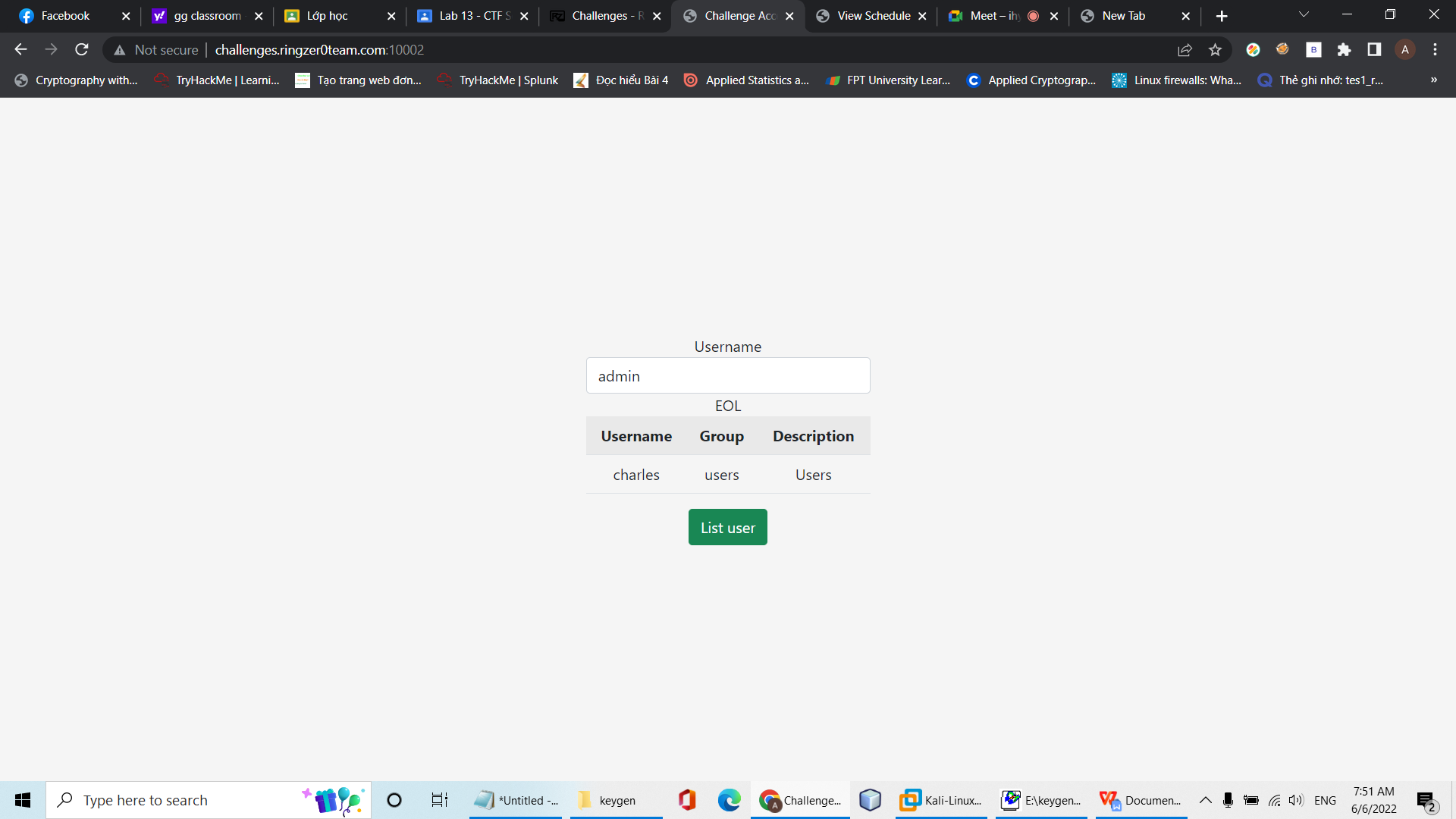


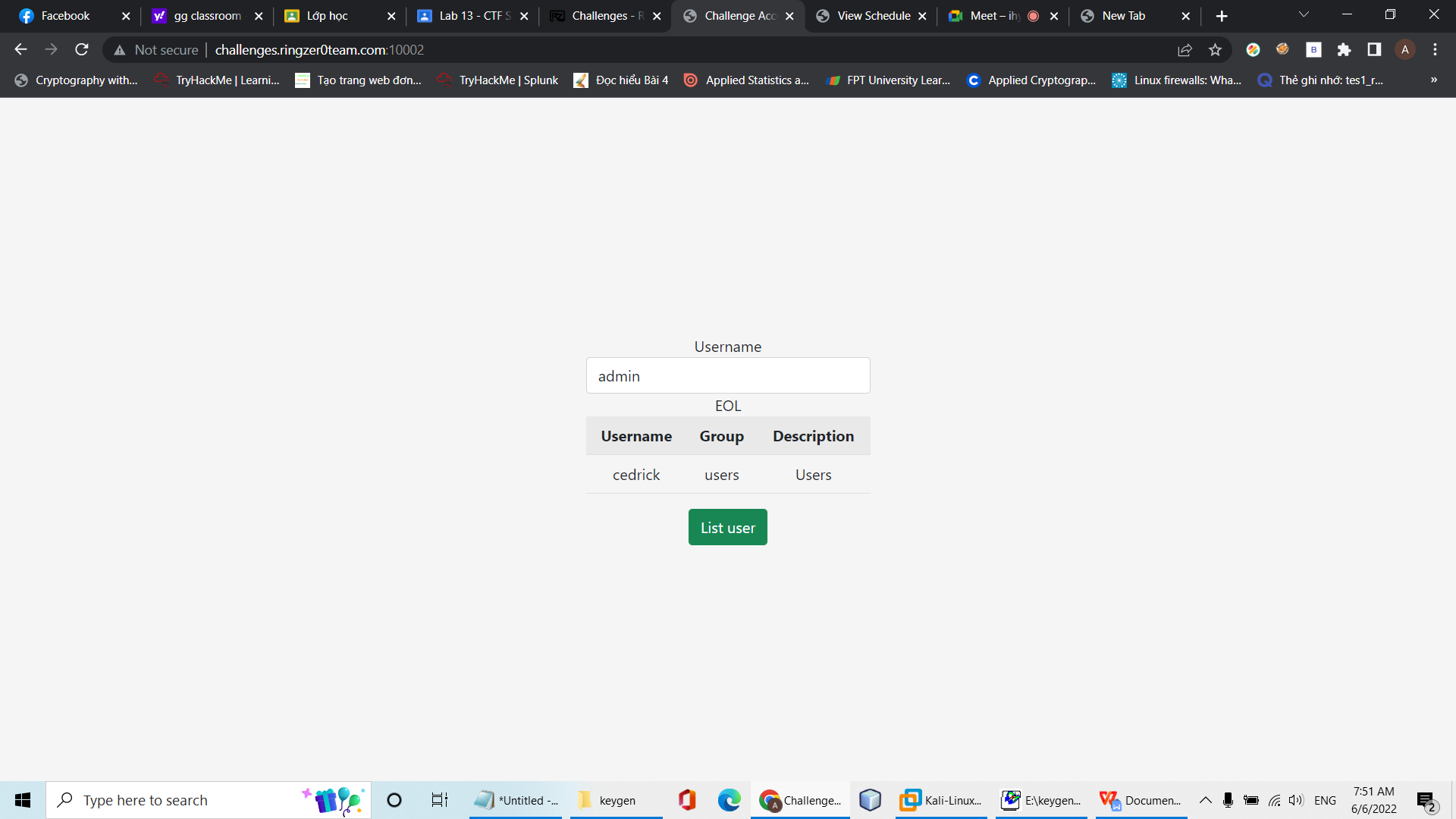


1. **ACL rulezzz the world**

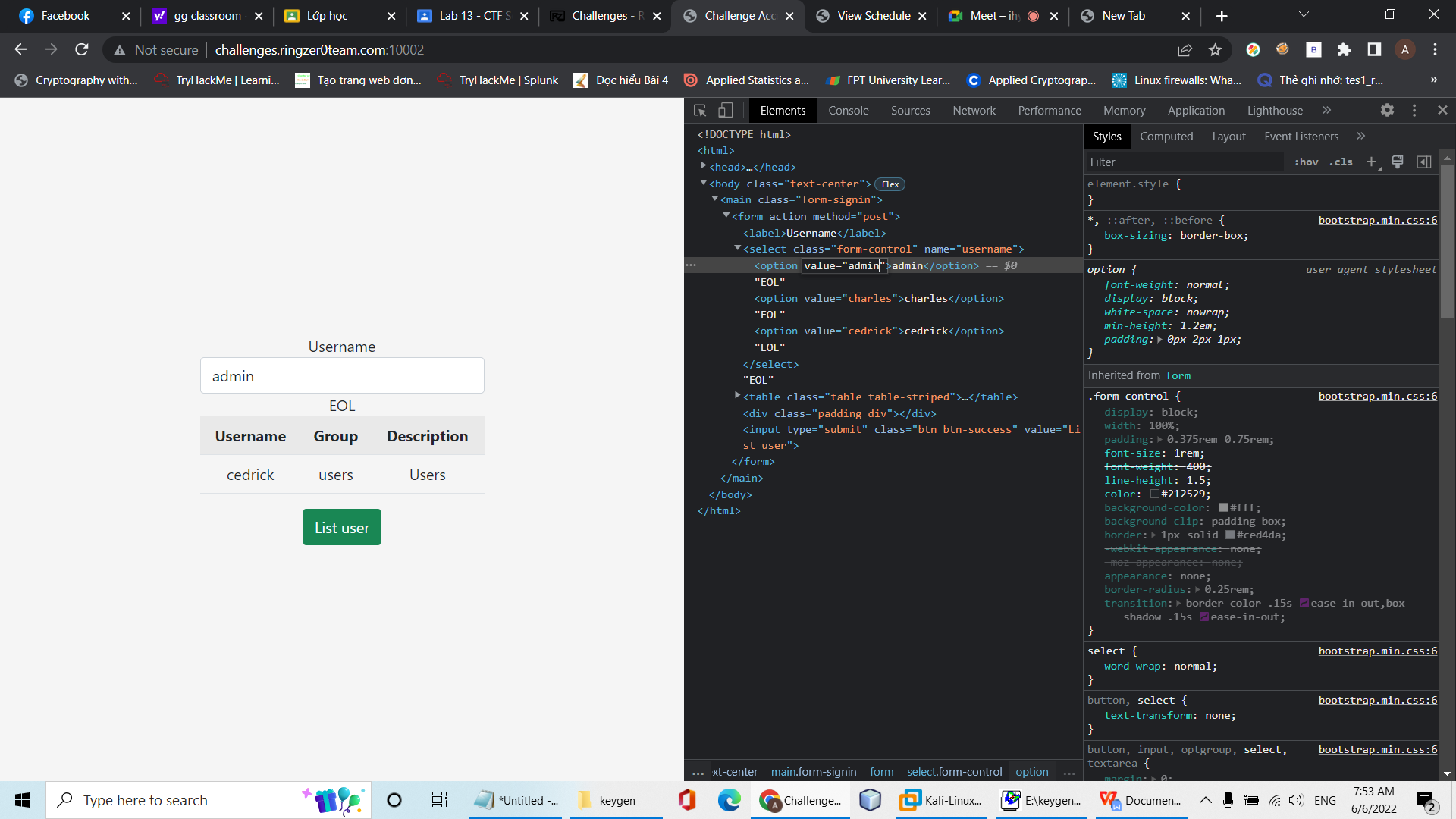
- Đầu tiên ta thấy trang web liệt kê người dùng theo option cho trước.

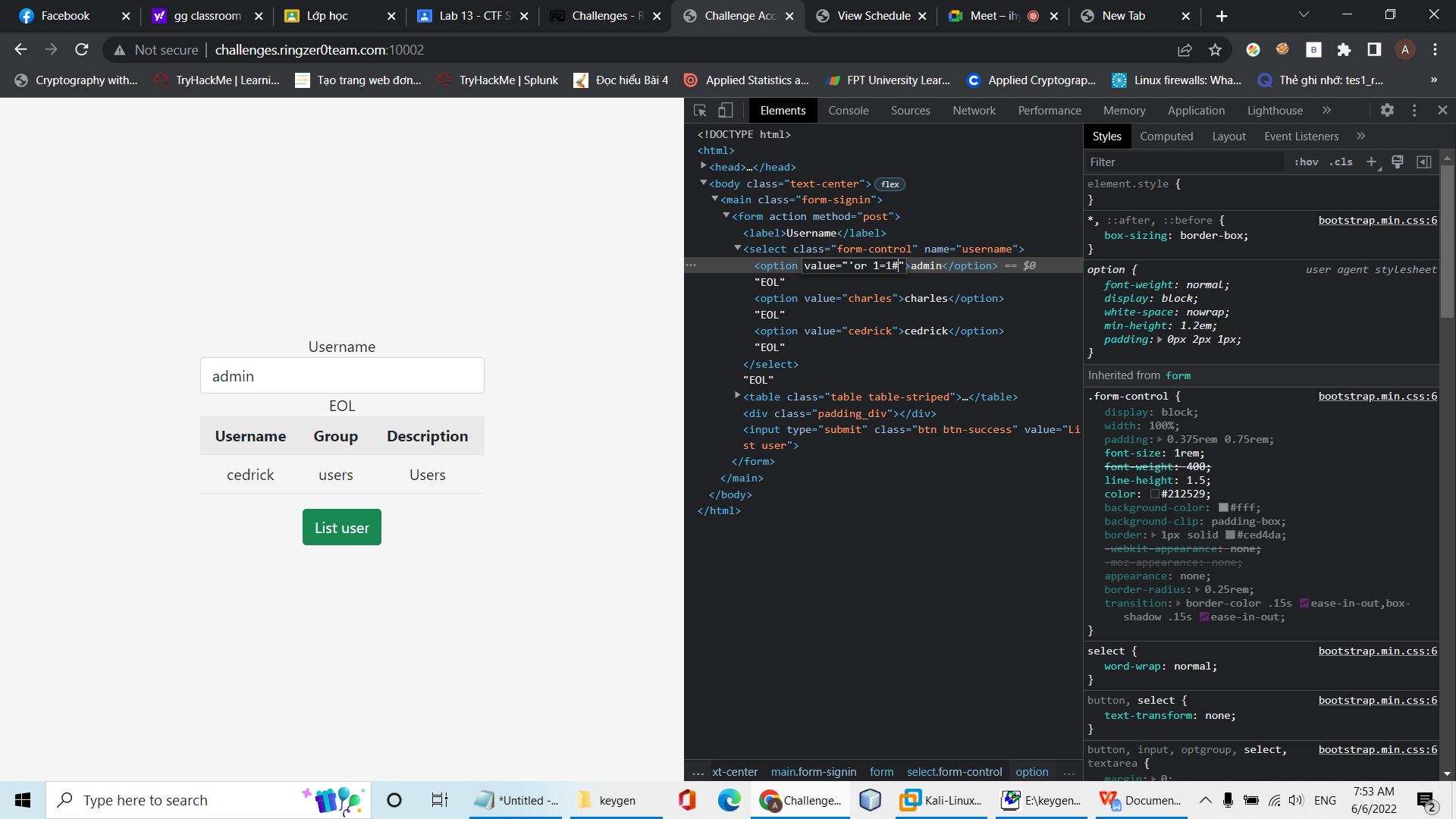


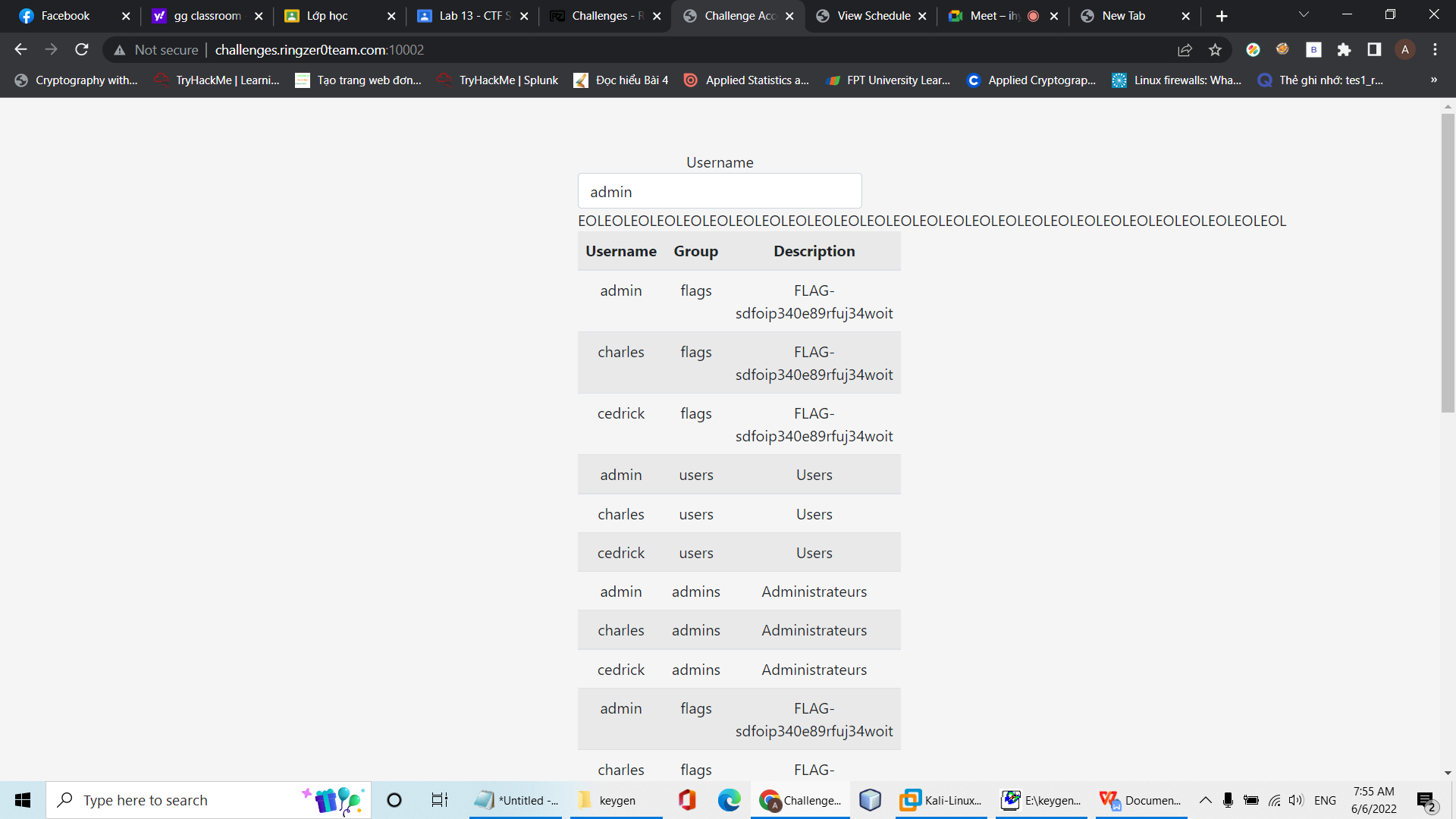


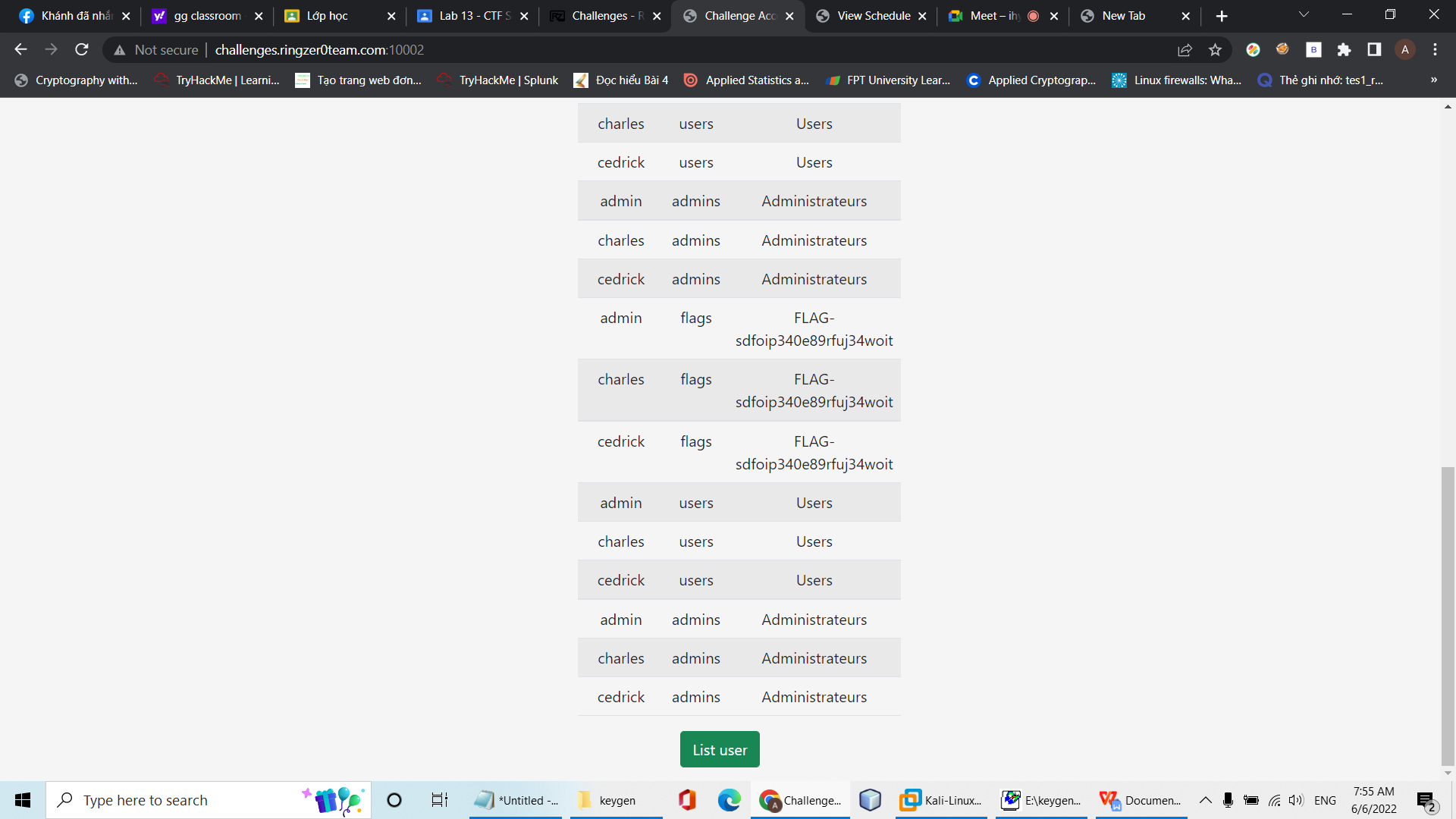


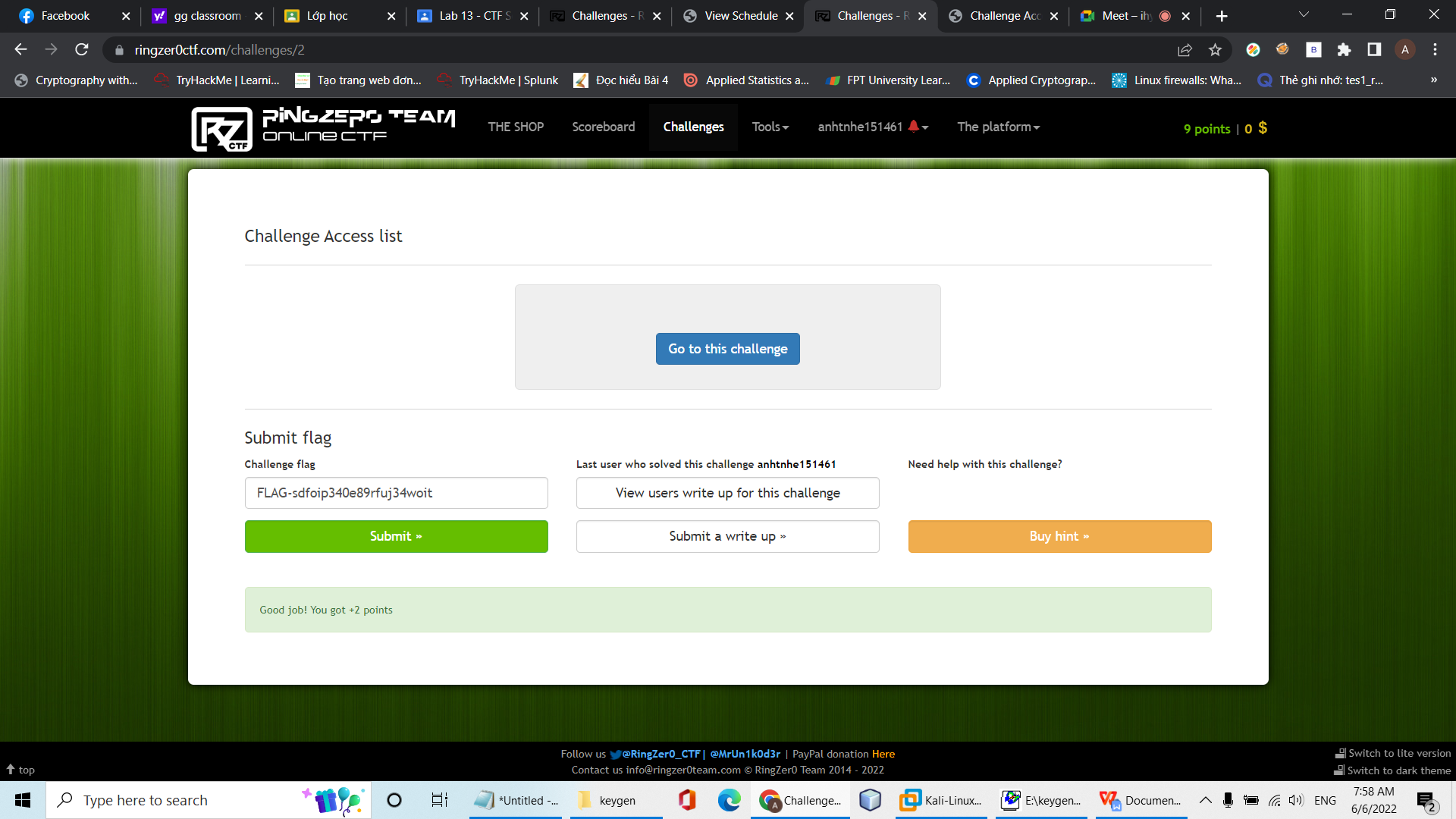
- Vì vậy để khai thác ta chỉ cần F12 để sửa thêm đoạn mã ‘or 1=1# rồi click vào List user sẽ hiện ra tất cả thông tin của các username và sẽ lấy được flag.





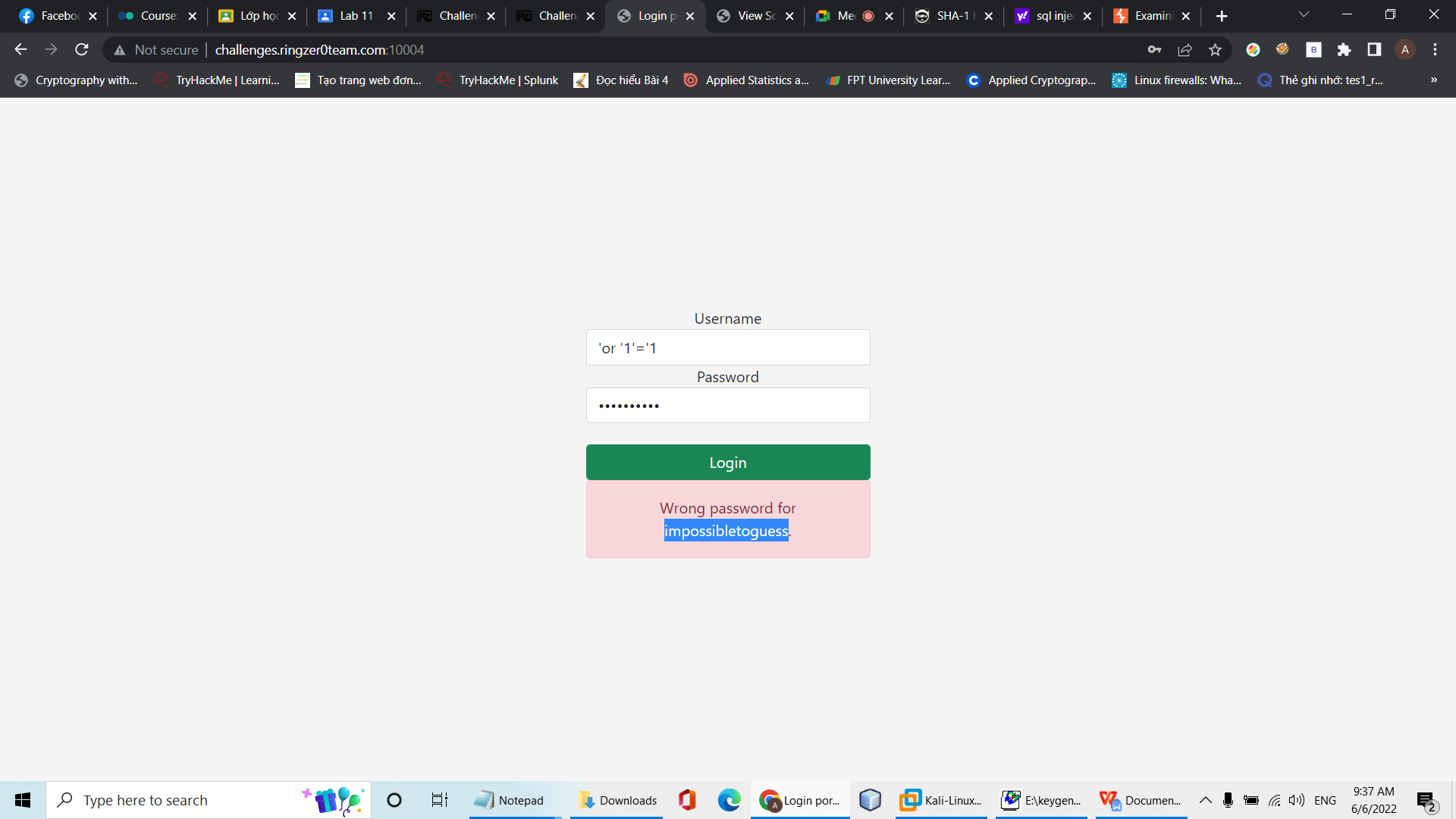




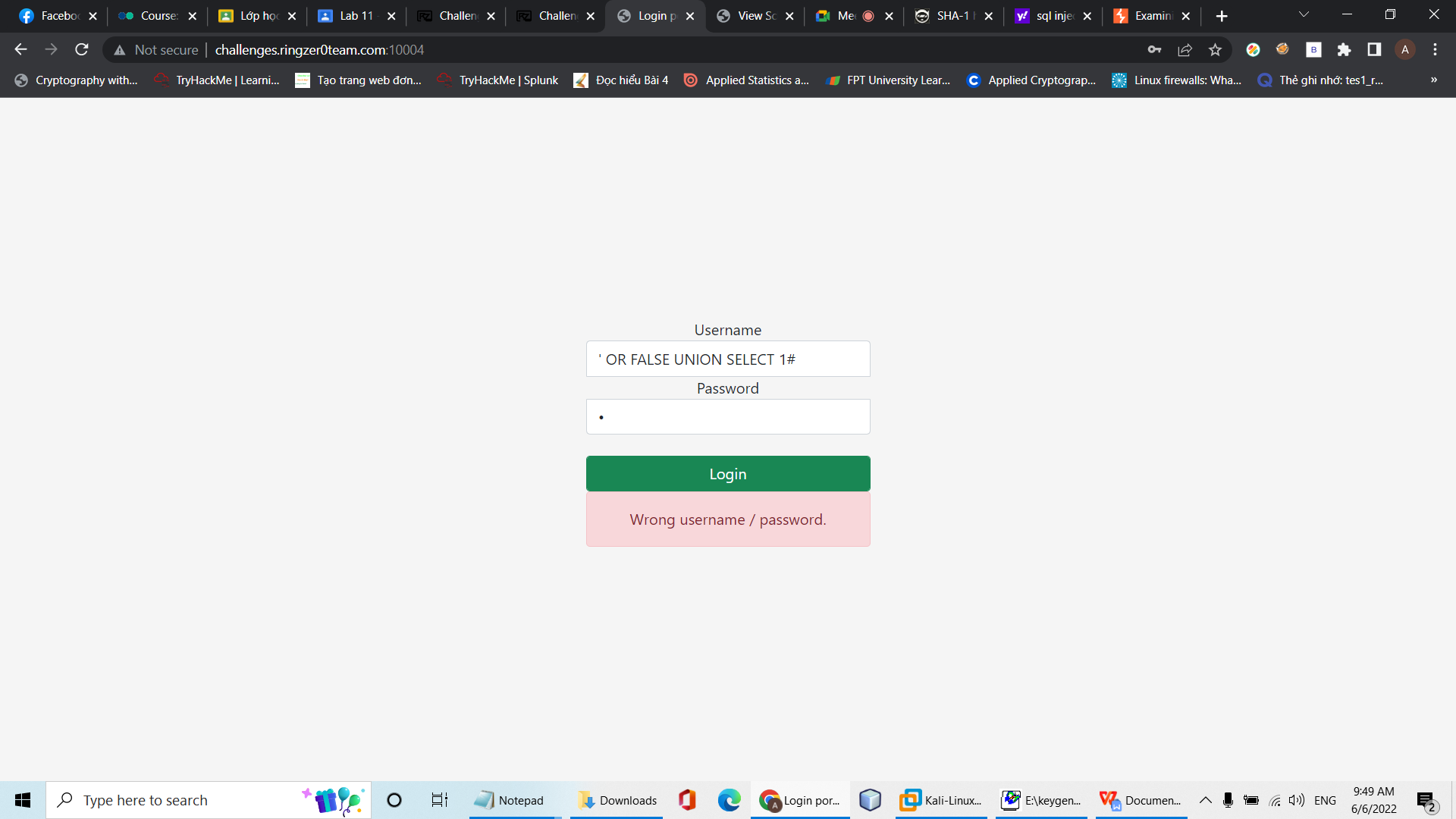


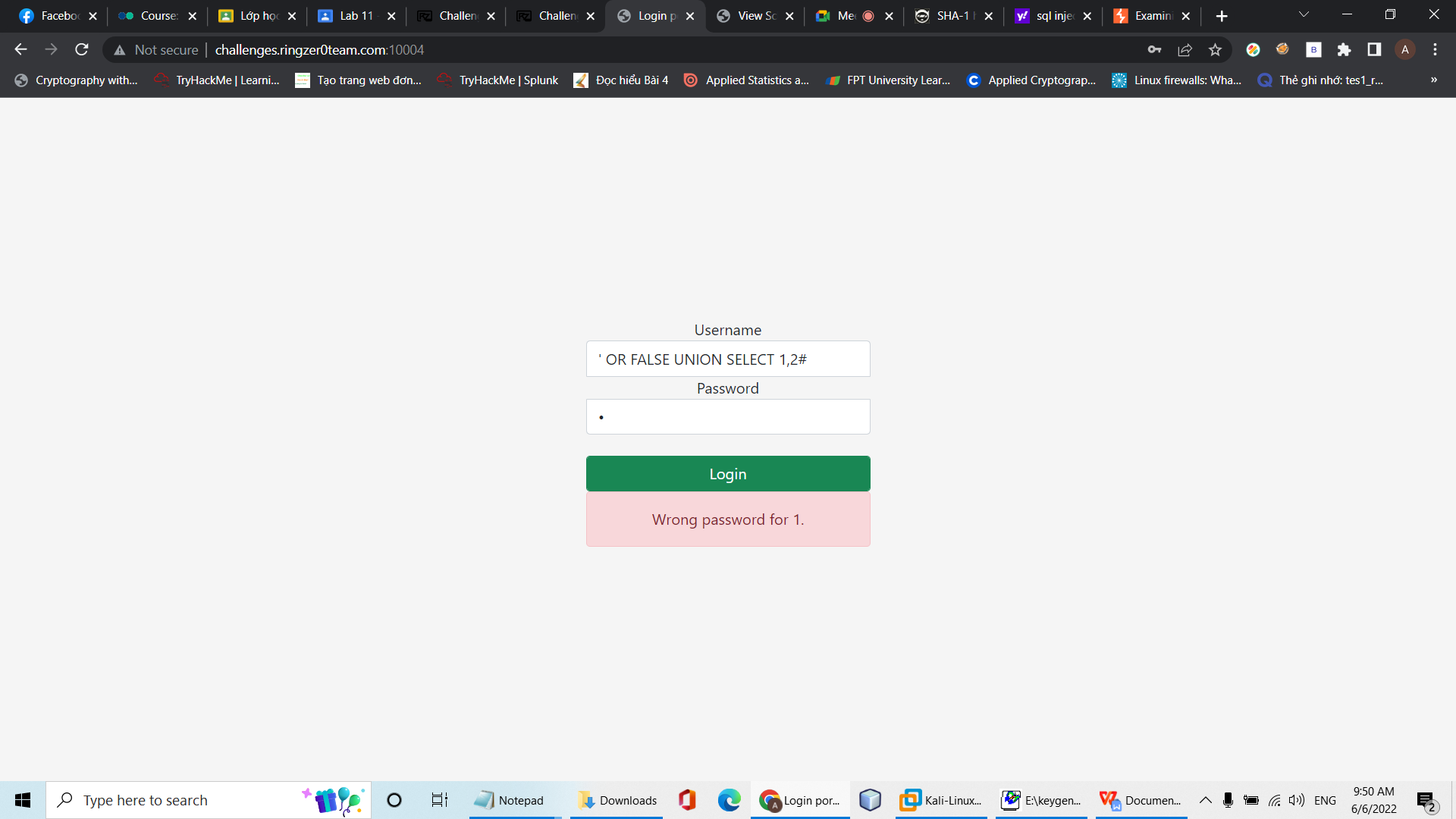
1. **Login portal 2**

- Đầu tiên chúng ta thử xem form đăng nhập có dính lỗi sql injection không và chúng ta thấy được thông tin về username là impossibletoguess.



- Tiếp theo chúng ta thử và biết được câu truy vấn gồm 2 trường thông tin, username ở trước.





- Ở đây chúng ta suy đoán được có lẽ password đã hash rồi mới đem check trong database, tra google thì biết được đó là mã SHA1.

