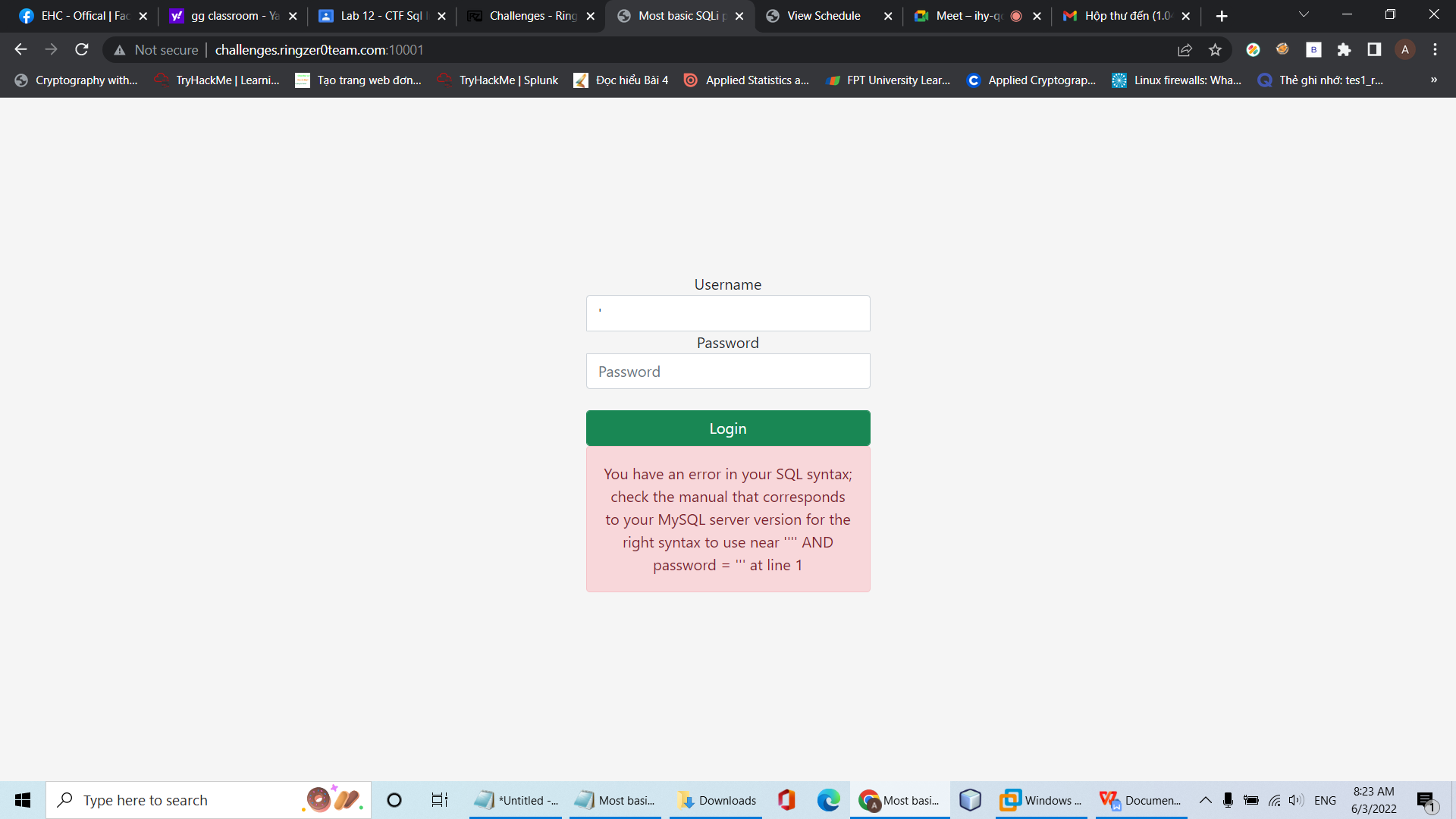
|  |  |
| --- | --- |
| Class | IAW301 |
| Name | Trần Ngọc Anh |
| IC No. | HE151461 |
| Date & Time | 3/6/2022 |

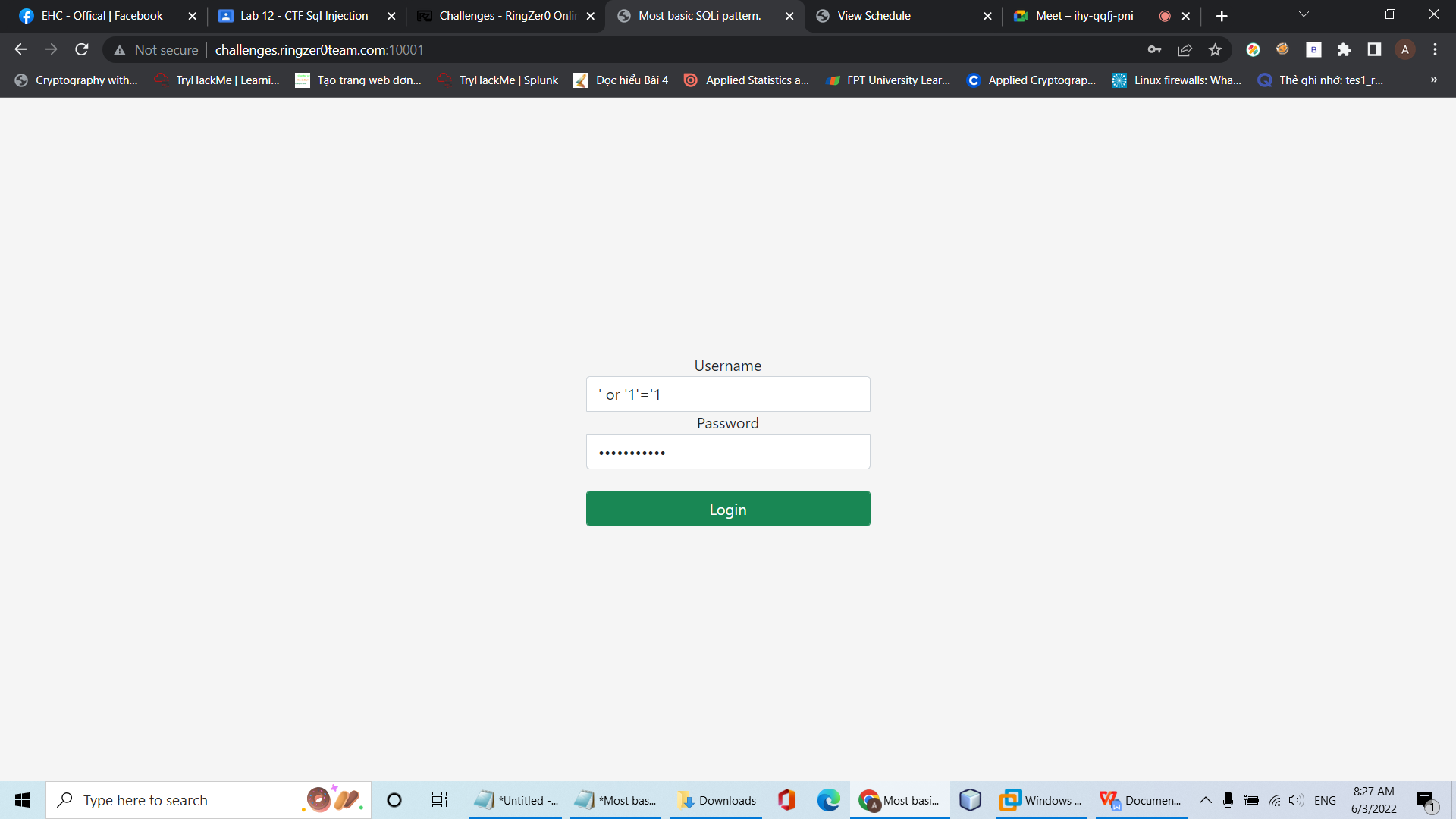
# **Lab 12 - CTF Sql Injection**

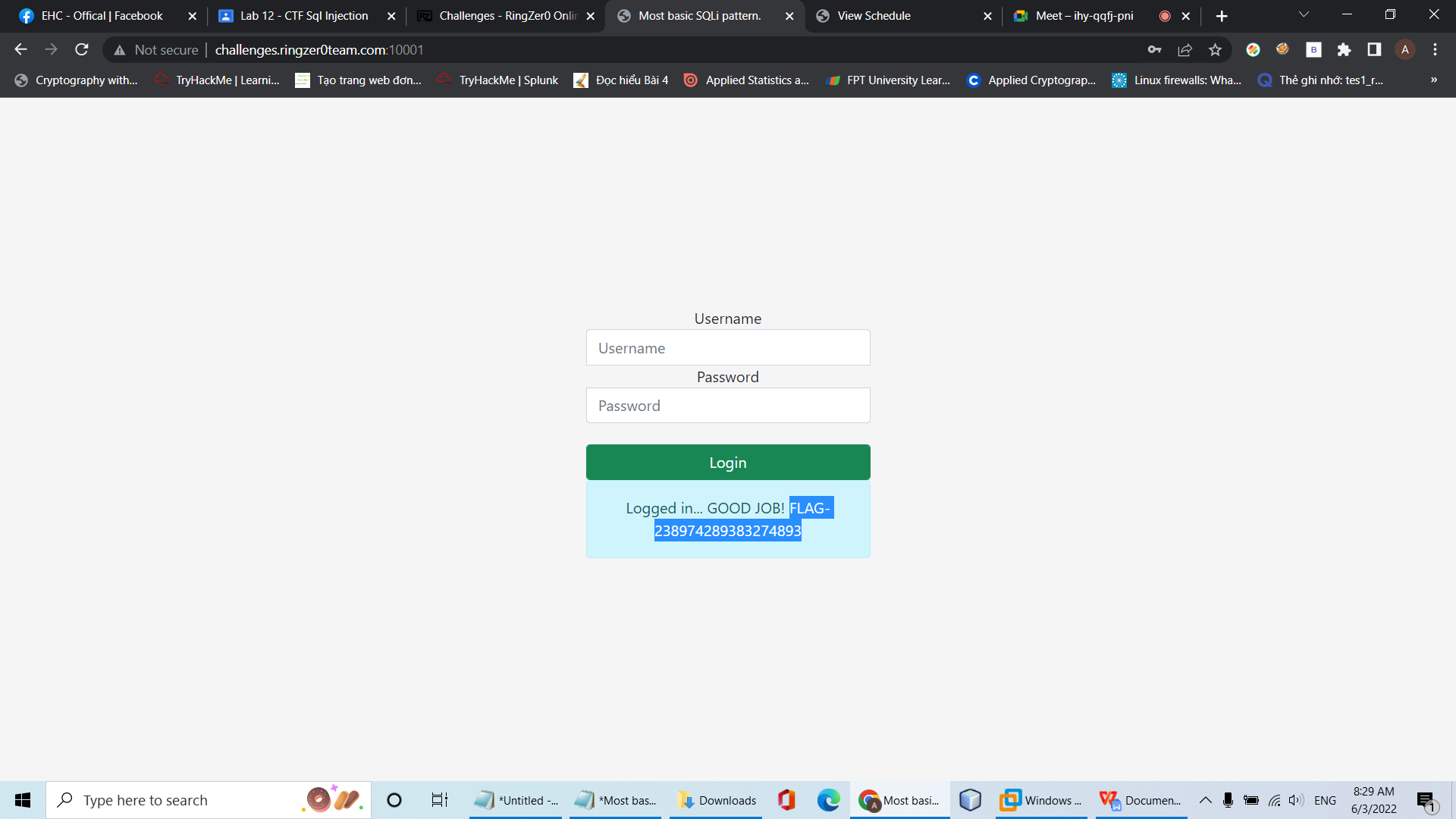
1. **Most basic SQLi pattern**

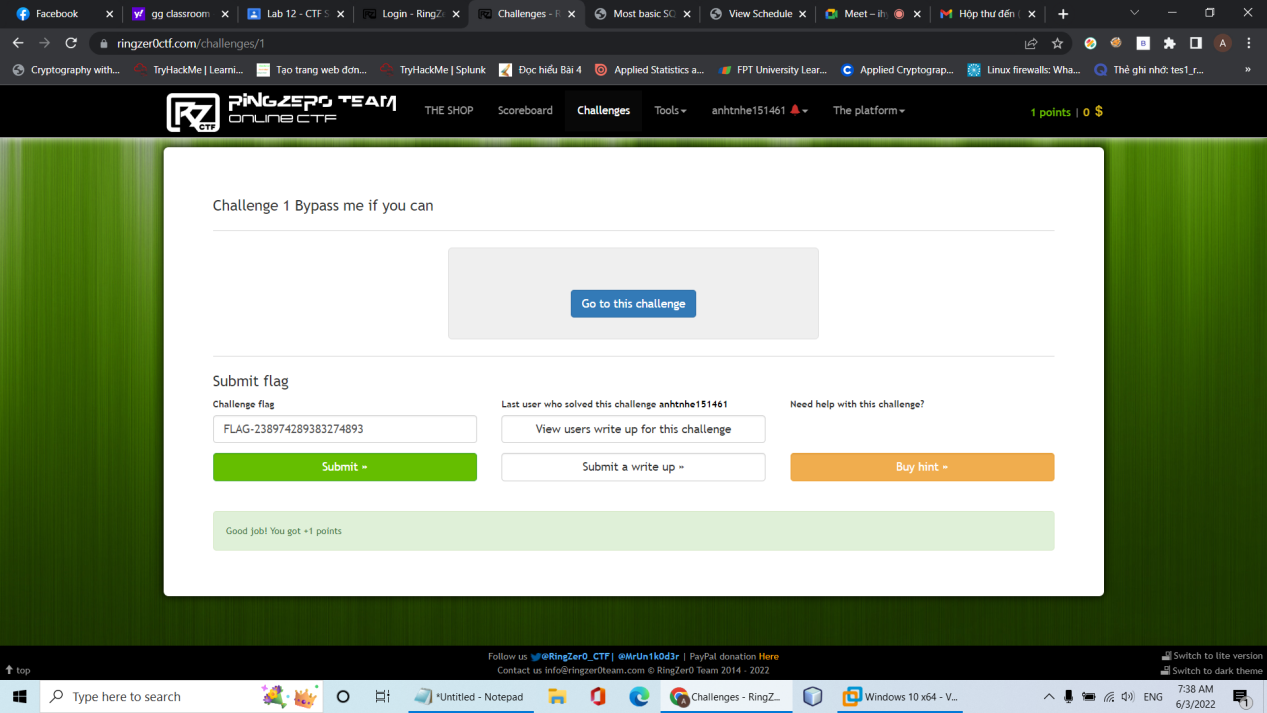
- Đầu tiên ta thử dấu ‘ để kiểm tra xem form có lỗi sql injection không.



- Sau khi chứng minh được có lỗi sql injection chúng ta thử điền ' or '1'='1 vào cả username và password để biến câu truy vấn sql thành luôn đúng và by pass được.

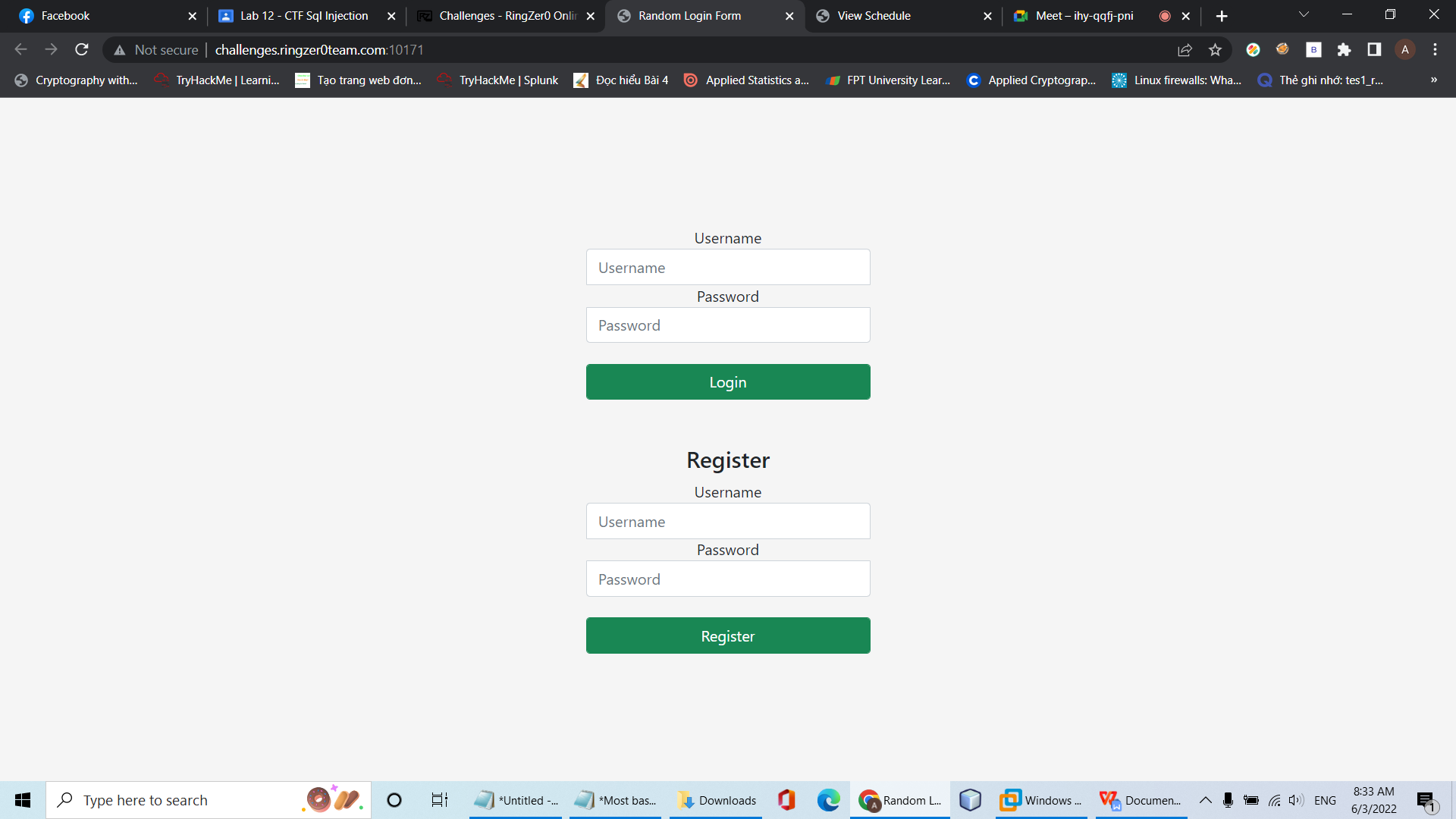




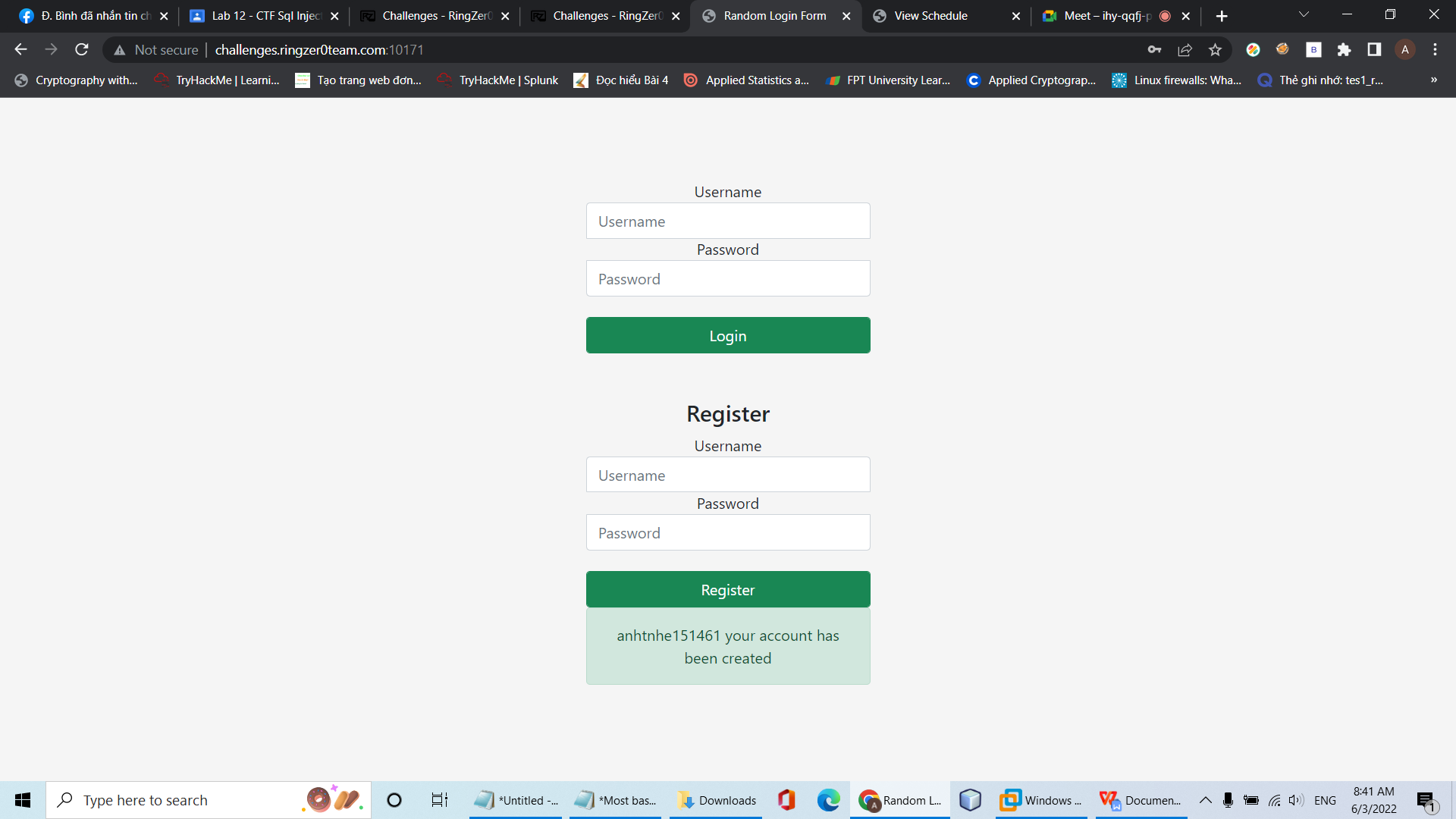


1. **Random Login Form**

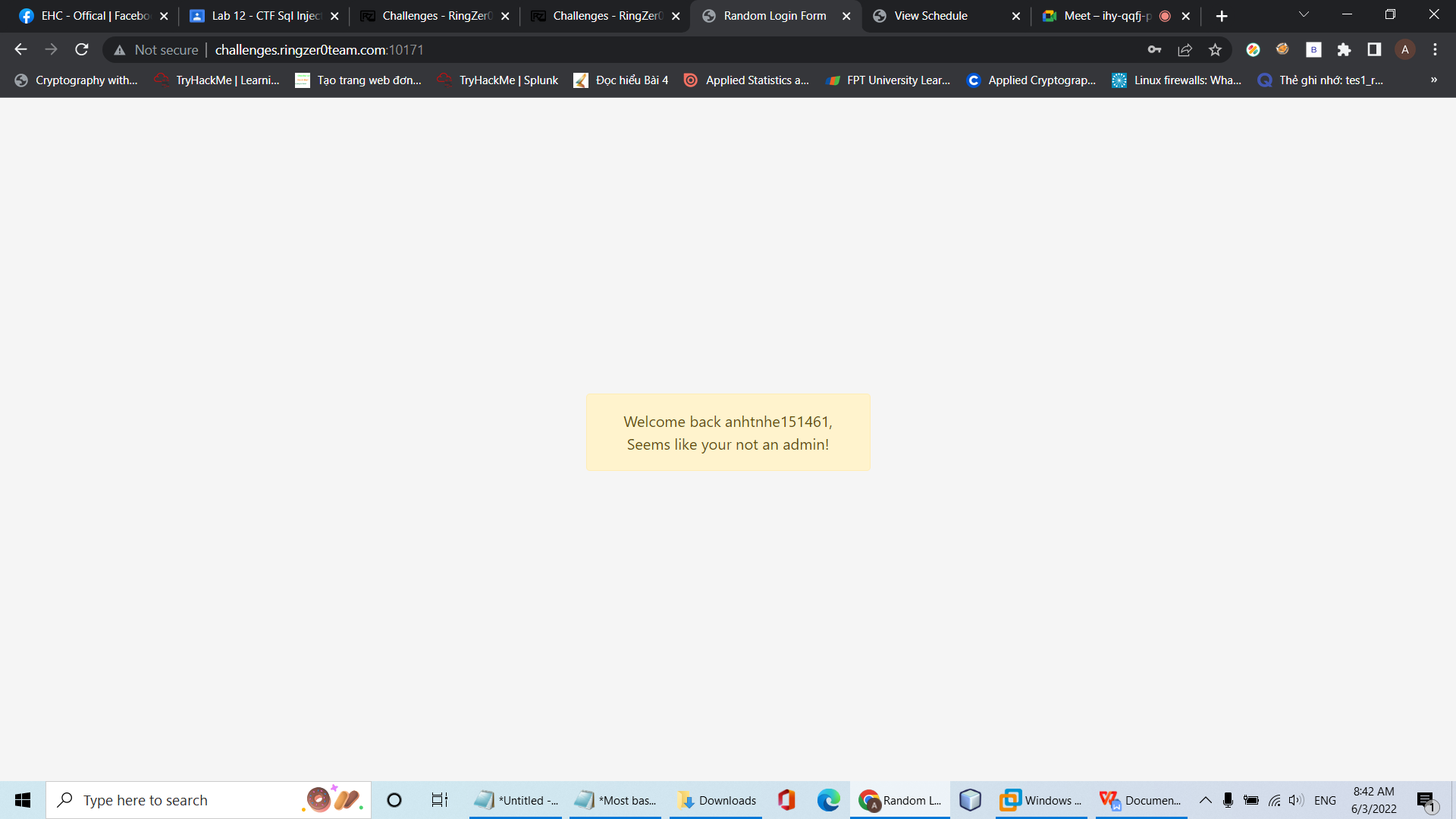
- Nhìn qua trang web có 2 form login với register.



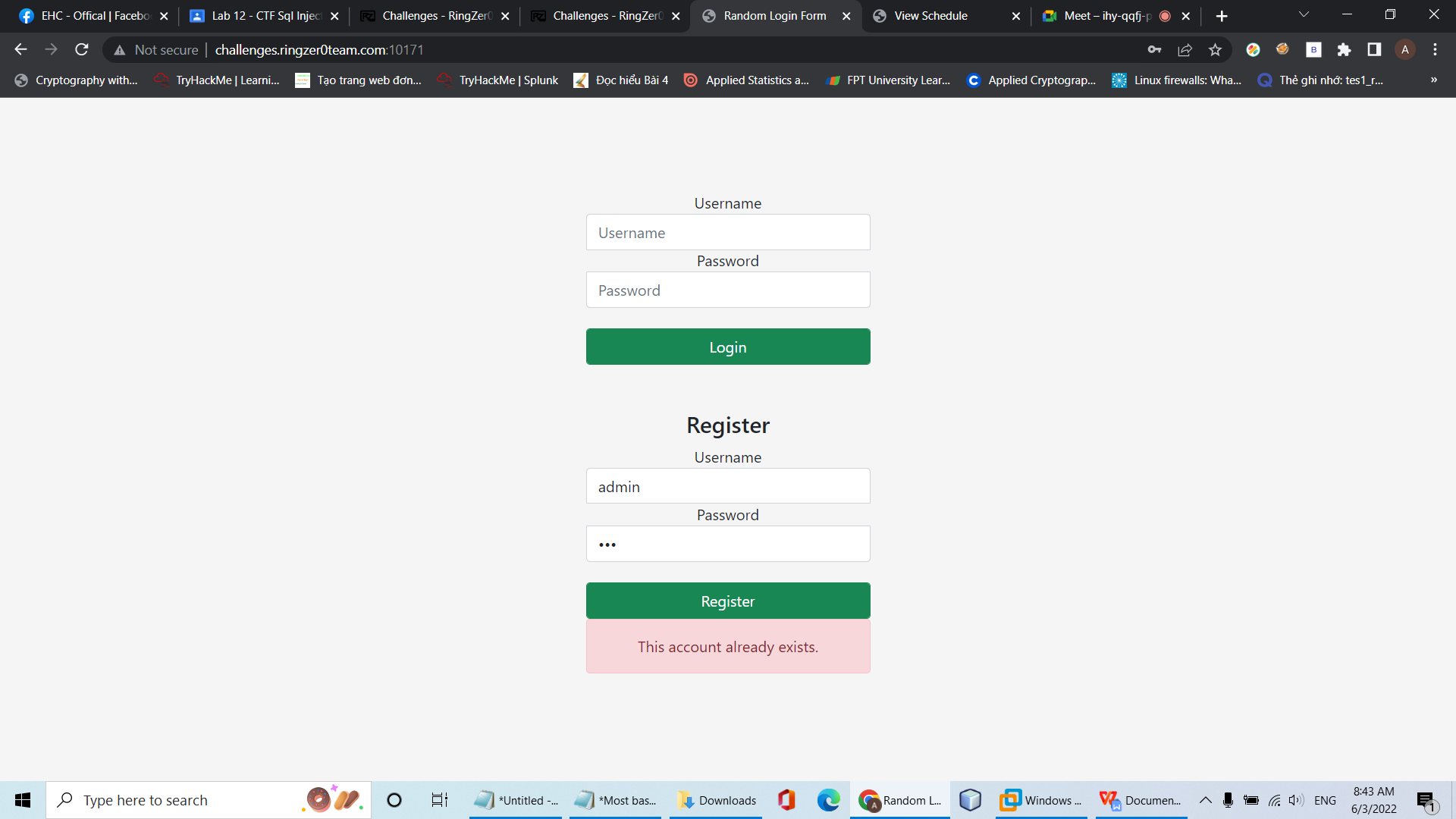
- Đầu tiên chúng ta đăng kí 1 tài khoản mới với username là anhtnhe151461 và password là 123.



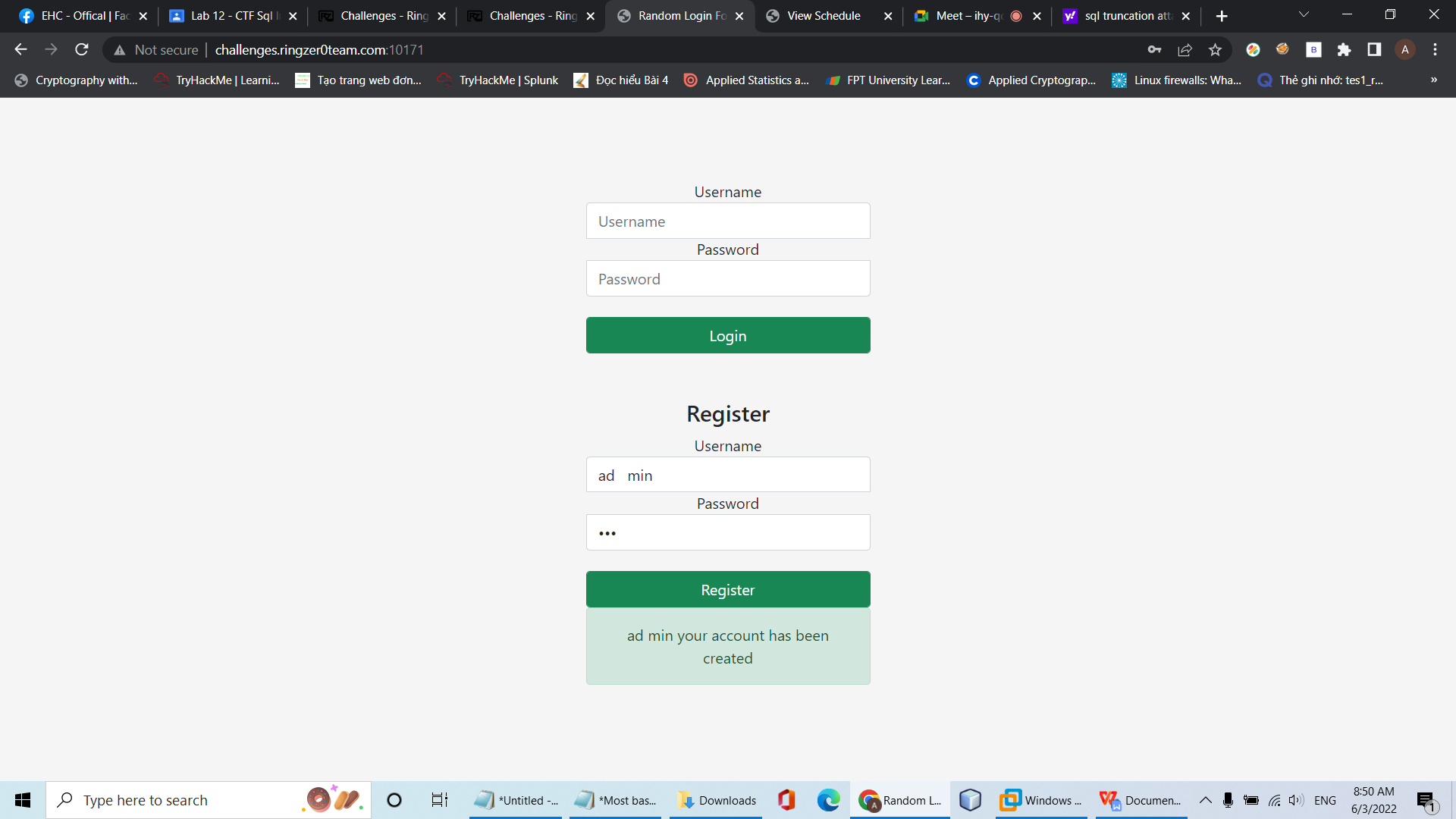
- Sau đó chúng ta thử login với tài khoản vừa tạo và nhận được thông báo đăng nhập thành công nhưng do không phải là admin nên không lấy được flag.

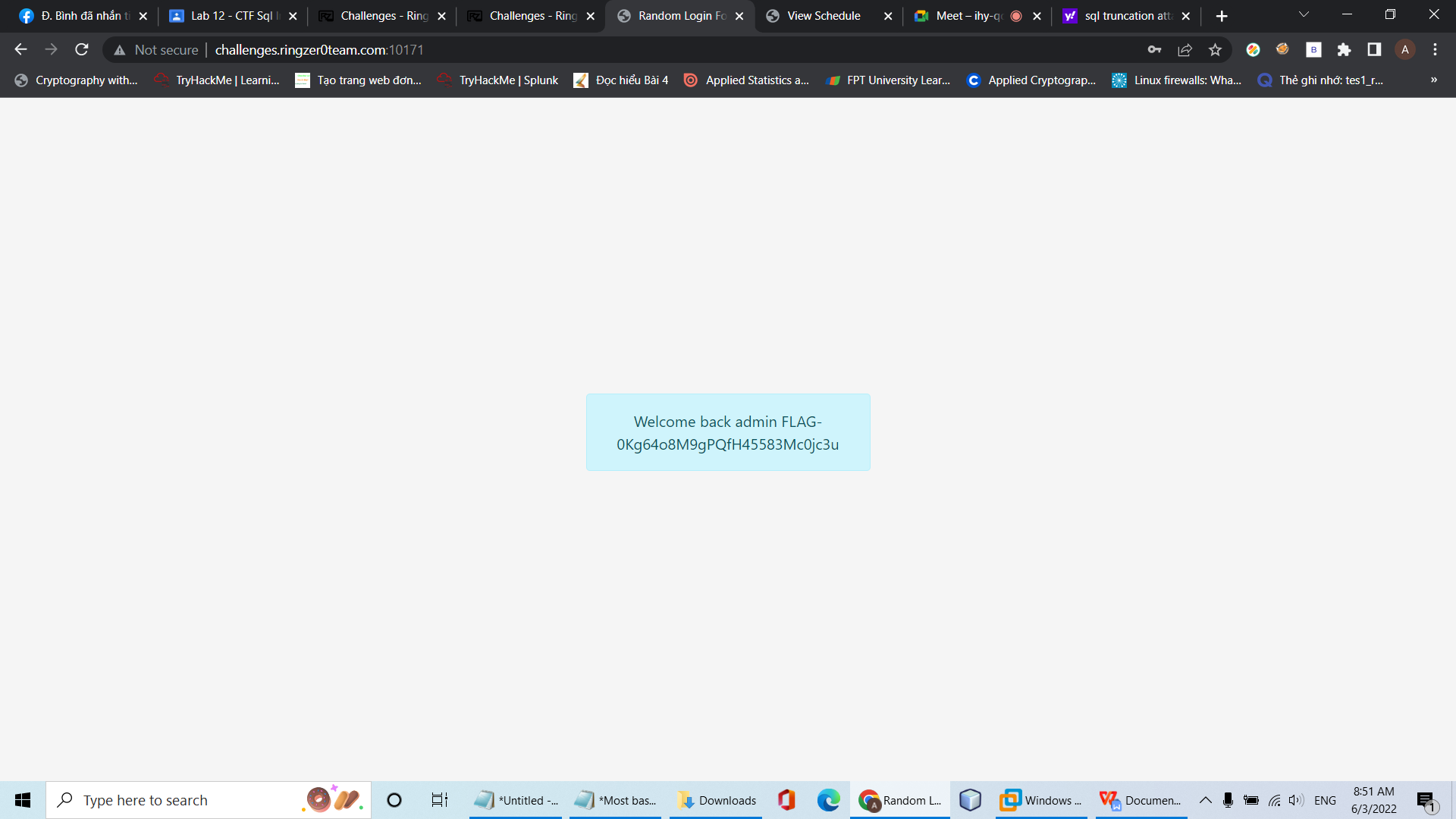


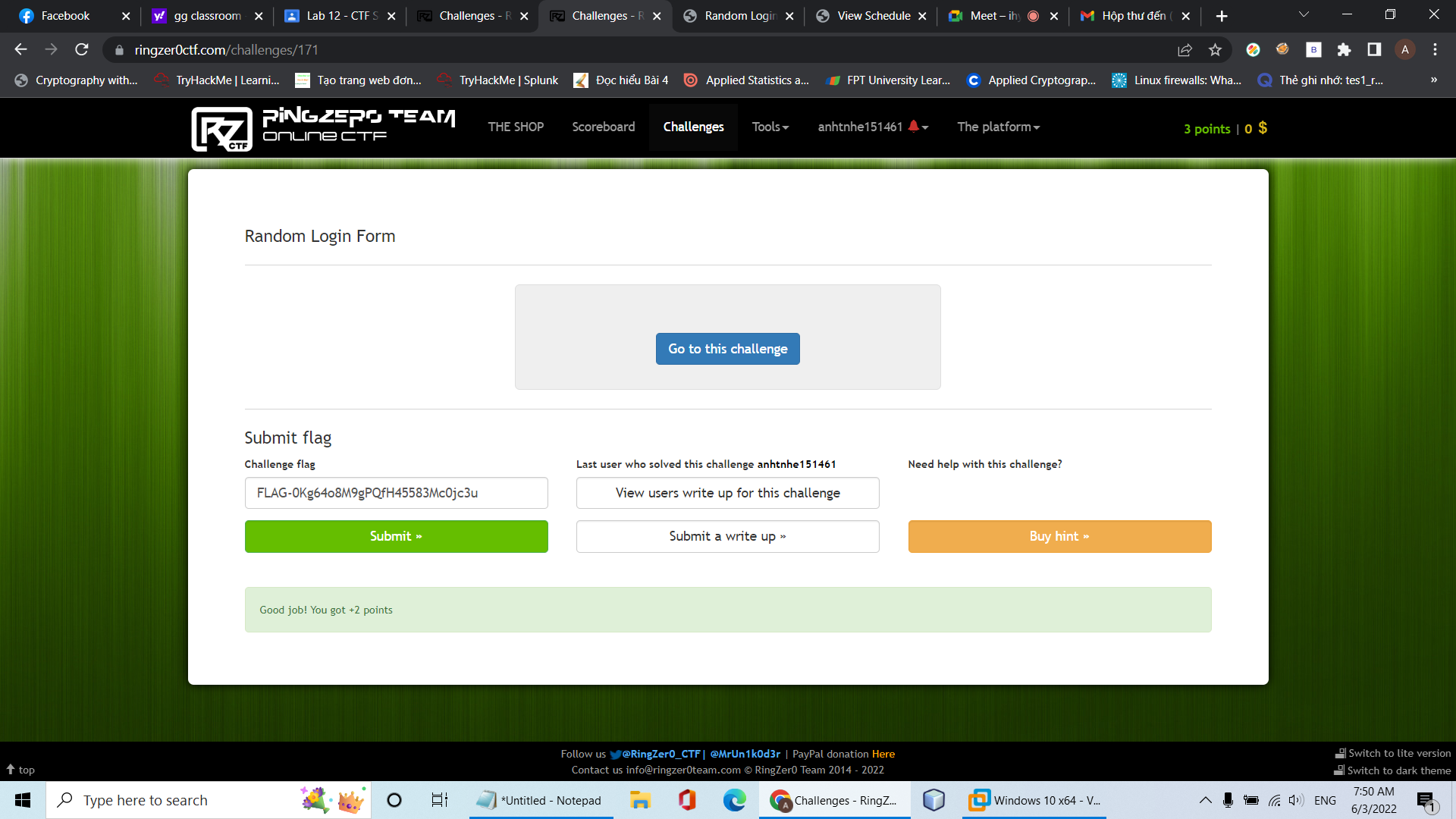
- Quay lại form đăng nhập chúng ta lại thử đăng kí tài khoản admin nhưng không tạo được do trong database đã tồn tại tài khoản này rồi.



- Thử ad min thì sẽ tạo được tài khoản mới trong database và khi login thì hàm trim() sẽ xử lí các dấu khoảng trắng thừa trong chuỗi username để login với quyền admin.



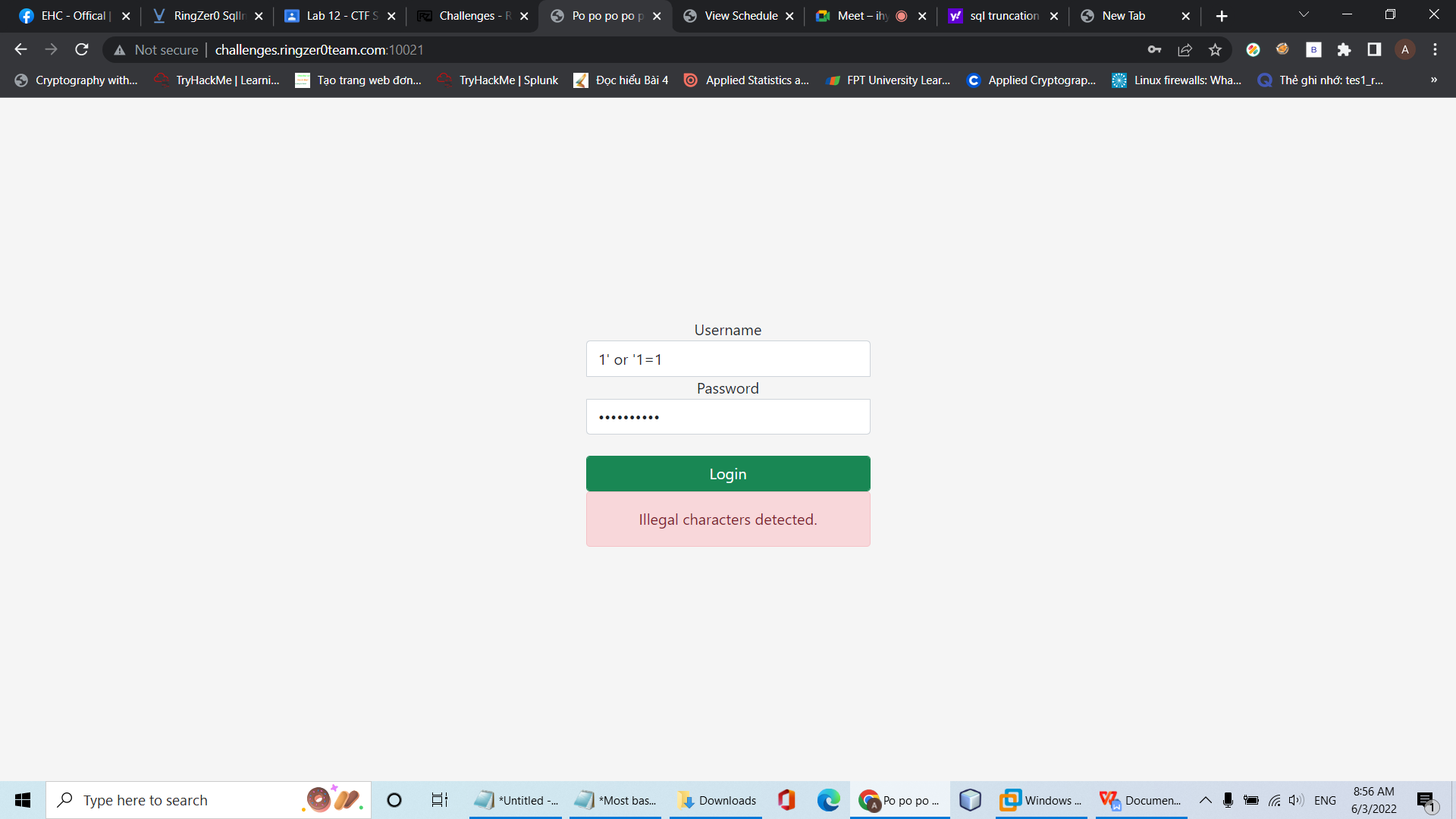




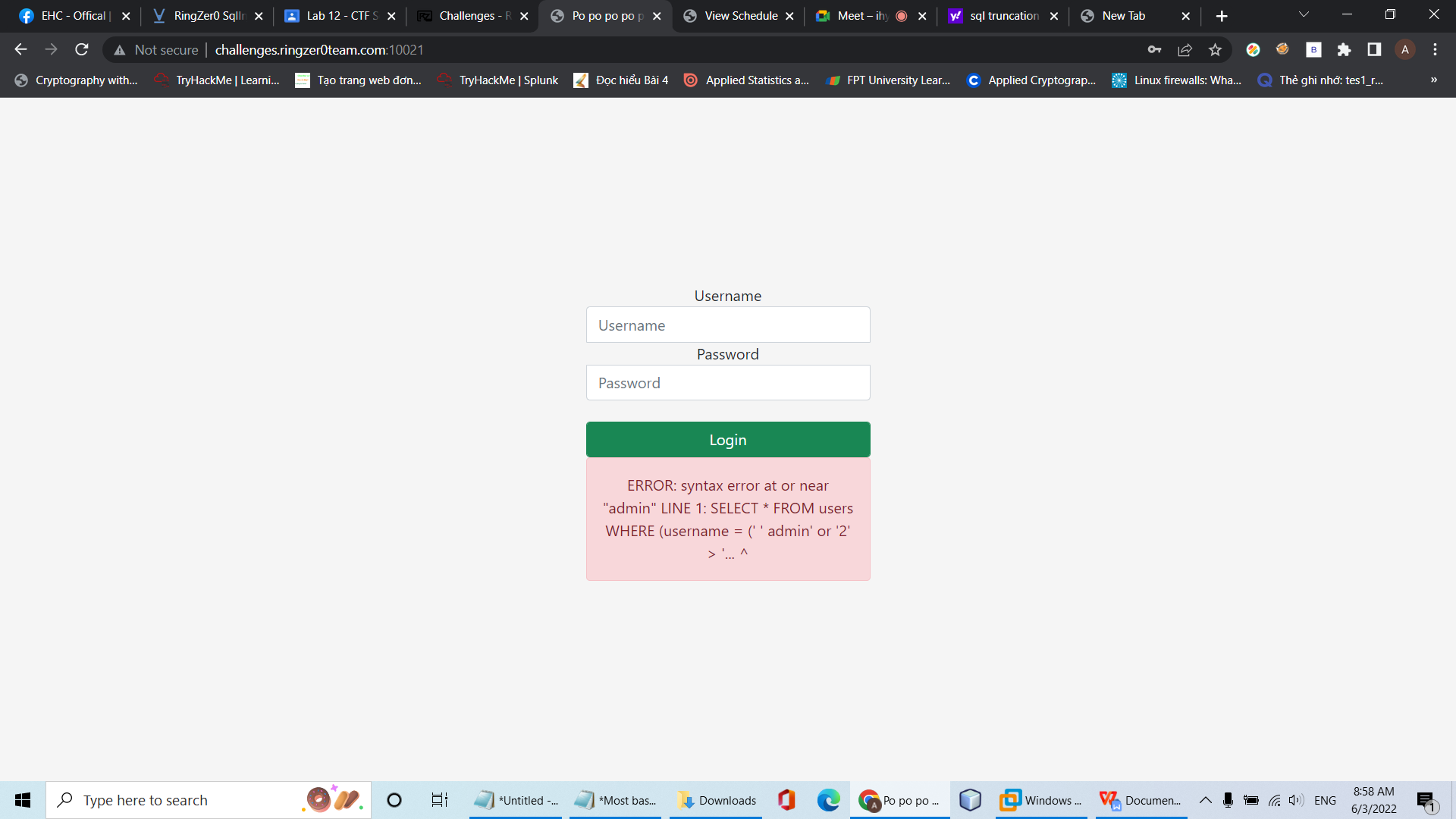
1. **Po po po po postgresql**

- Bài này vẫn là form login nhưng với cơ sở dữ liệu Postgre nên syntax xử lí sẽ khác.

- Thử làm như challenge 1 và thấy lỗi syntax.

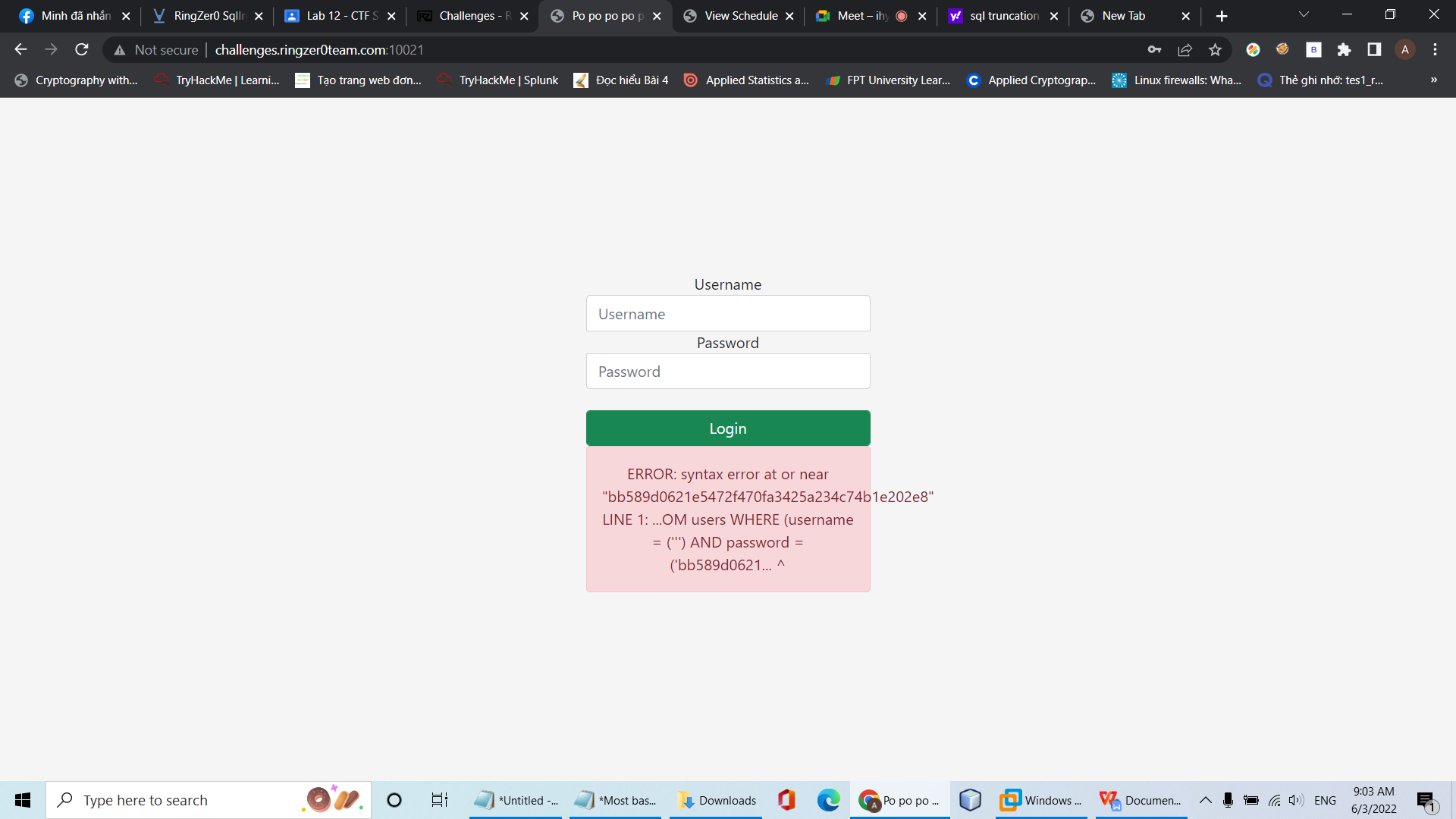


- Thử tiếp một đoạn mã khác ' admin' or '2' > '1 thì cũng vẫn báo lỗi nhưng chúng ta sẽ biết được format của câu lệnh sql ở đây.



- Vì trong câu truy vấn sử dụng dấu () để giới hạn phạm vi của tham số truyền lên nên ta không thể dùng mệnh đề OR để cho kết quả luôn trả về true nữa.

- Ta lại tiếp tục thử username = ‘ và password = ‘ thì thấy rằng trước khi đem so sánh trong database cả 2 trường thông tin này đều bị mã hóa sang một dạng khác.



- Chính vì vậy chúng ta nhập '))OR TRUE -- để username luôn đúng và dấu -- để bỏ qua phần check password ở phía sau là sẽ bypass được challenge này.

