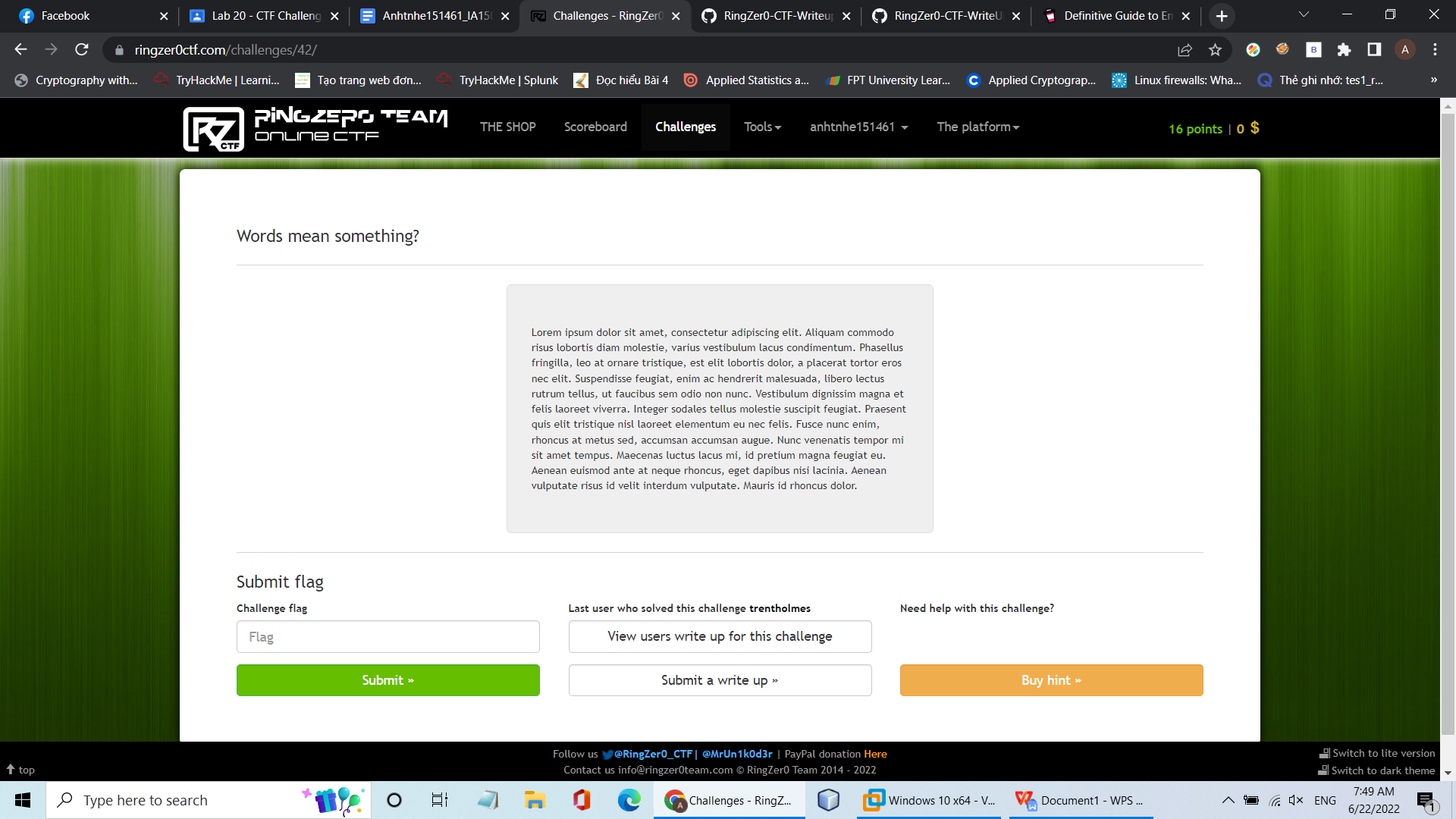
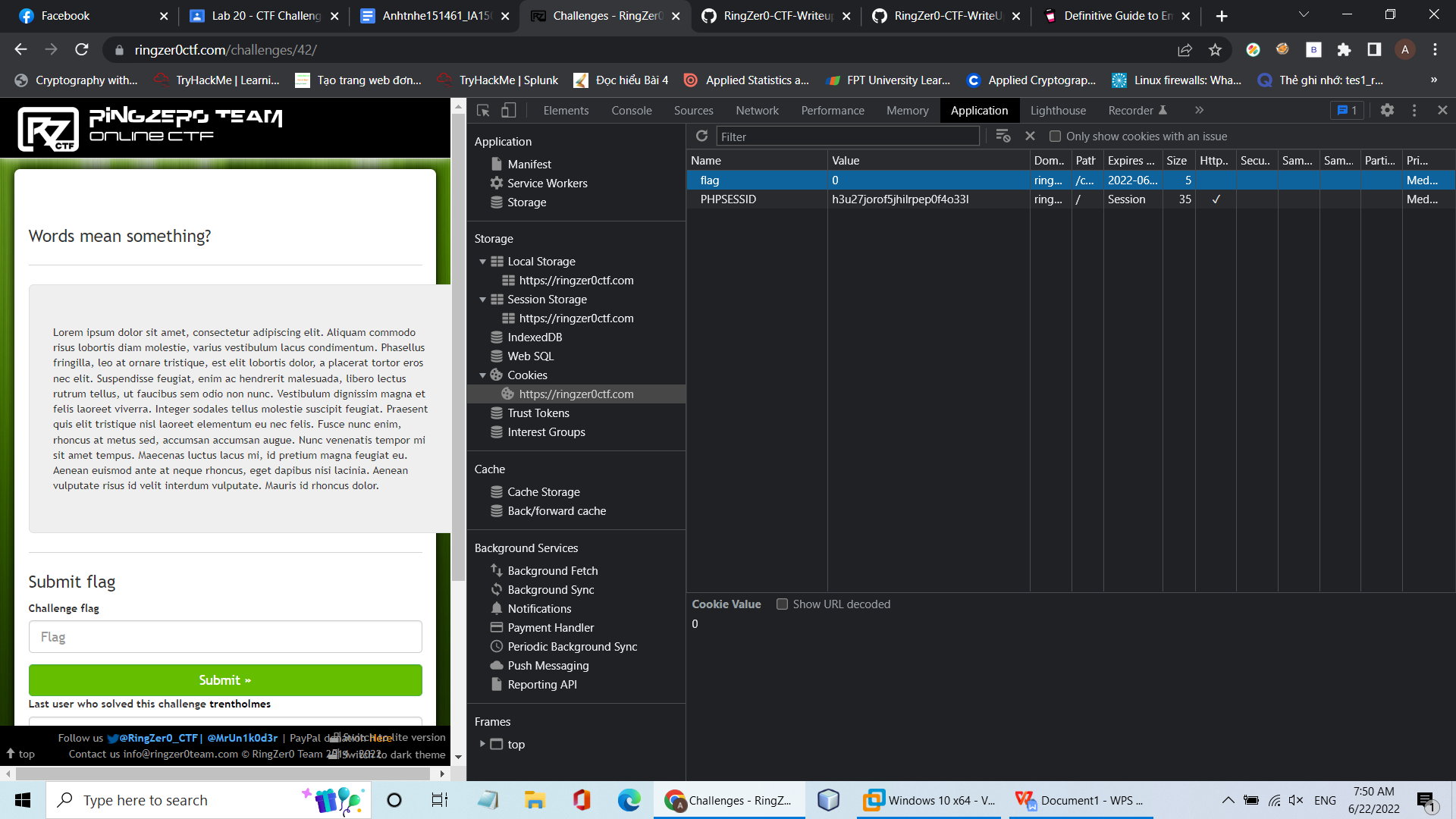
|  |  |
| --- | --- |
| Class | IAW301 |
| Name | Trần Ngọc Anh |
| IC No. | HE151461 |
| Date & Time | 22/6/2022 |

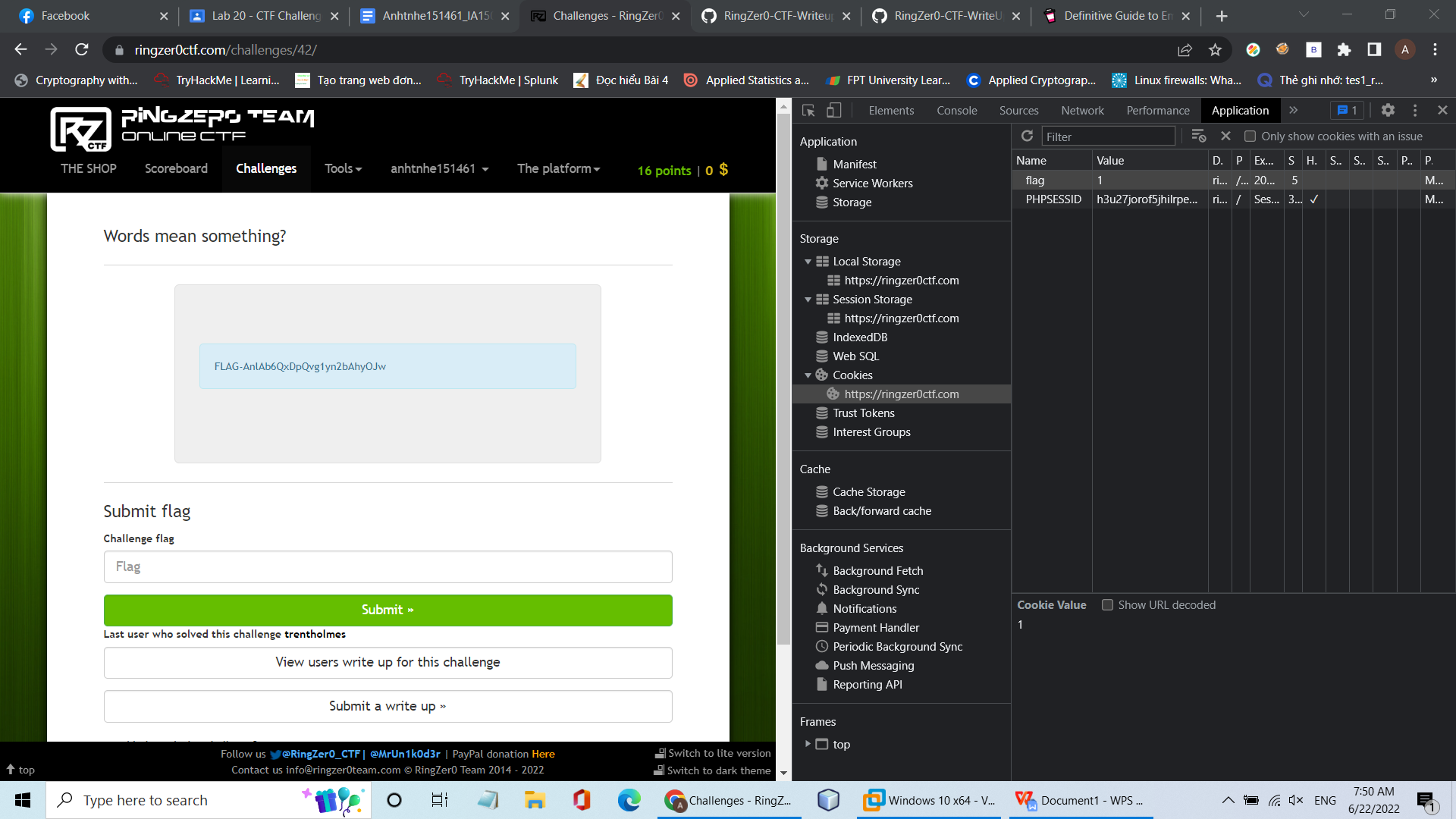
# Lab 20 - CTF Challenge

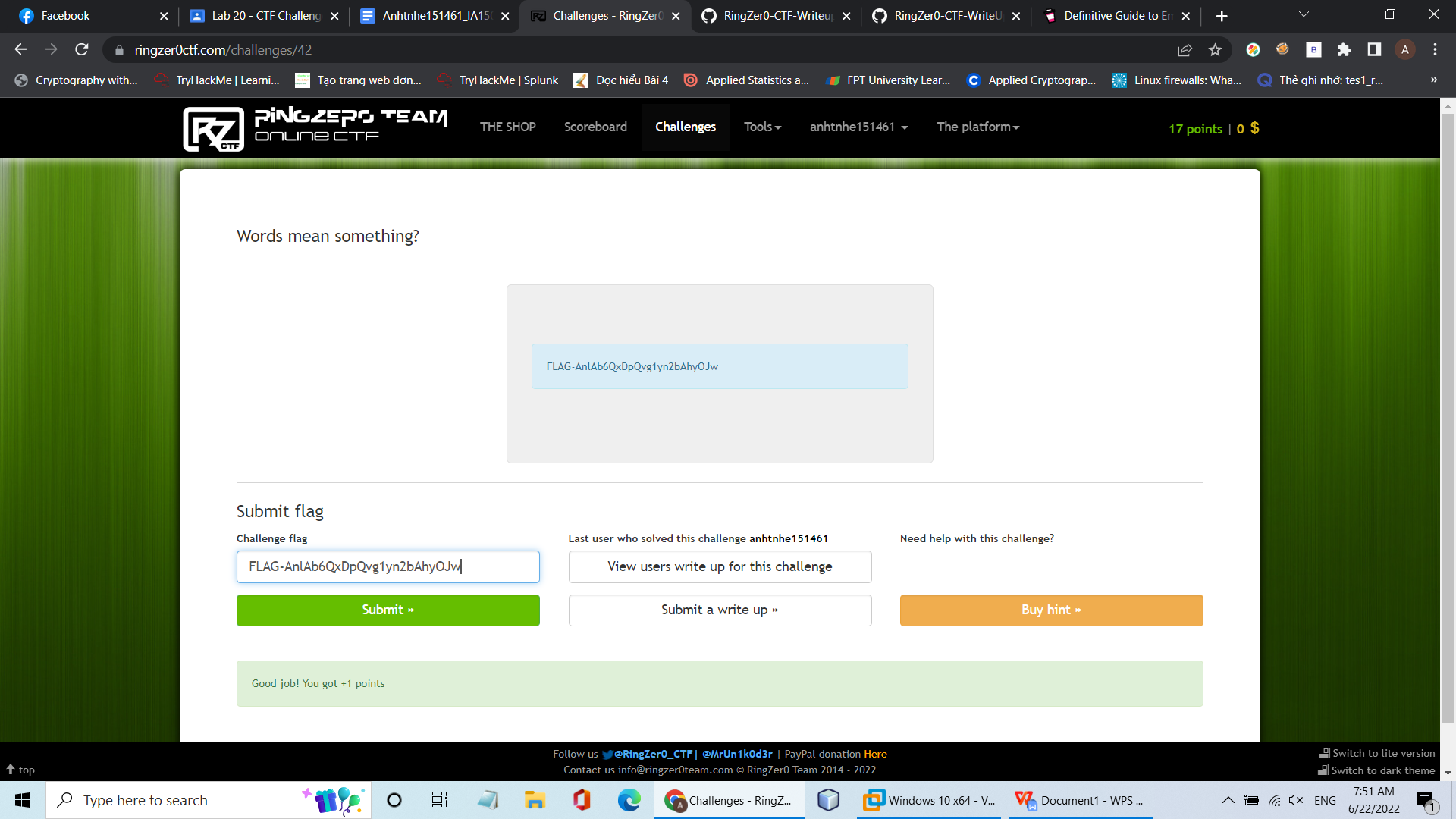
1. **Words mean something?**

- Đầu tiên ta thấy challenge này không có dấu hiệu gì đặc biệt nên xét cookie thì thấy được một flag có value bằng 0 đáng nghi ngờ .Ta thay đổi giá trị của nó sang 1 refresh lại trang web sẽ thấy hiện ra flag.



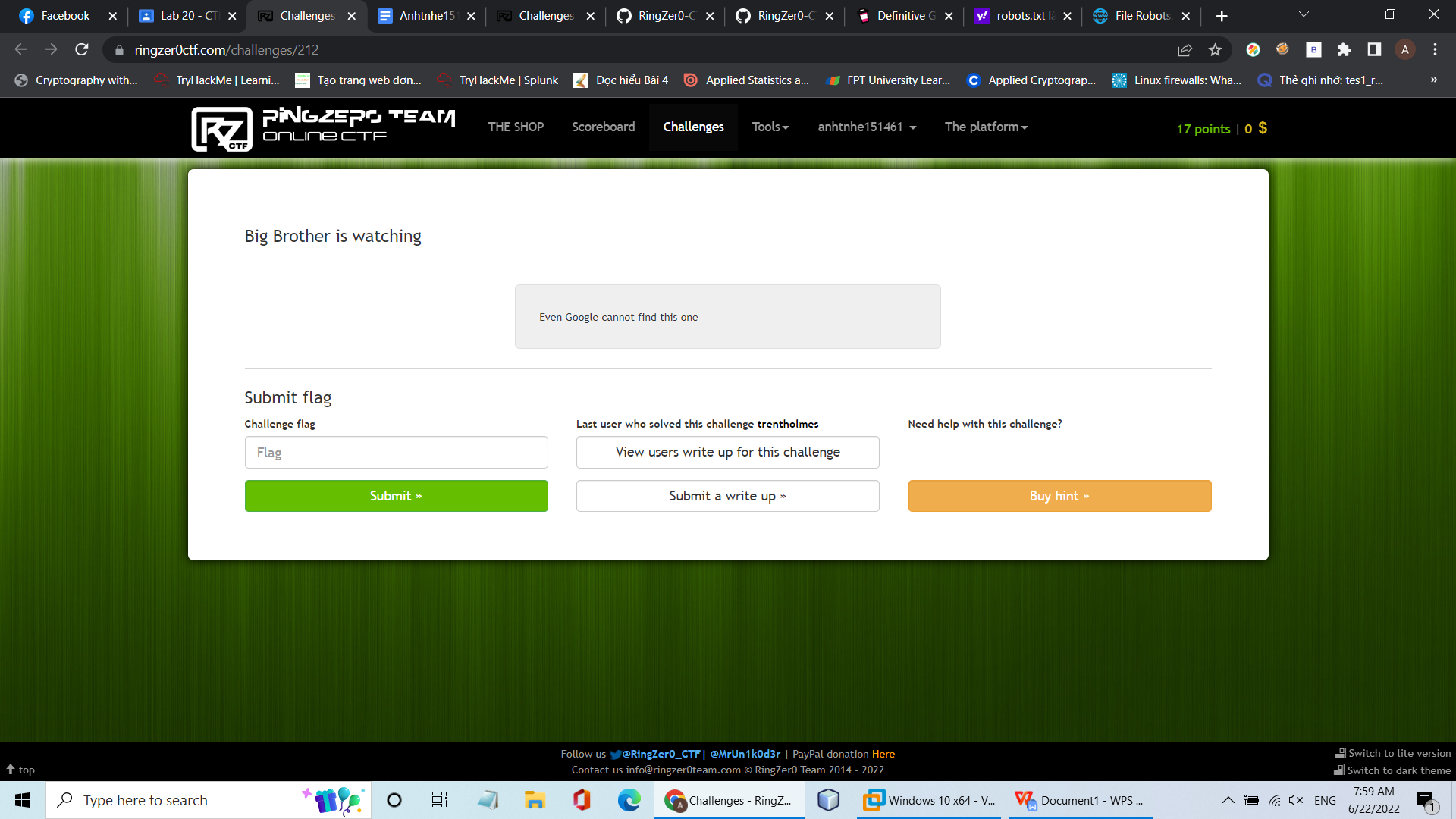






1. **Big Brother is watching**

- Đọc đề bài ta thấy được một hint , phân tích một chút thì ta biết được thêm về một file là robots.txt.

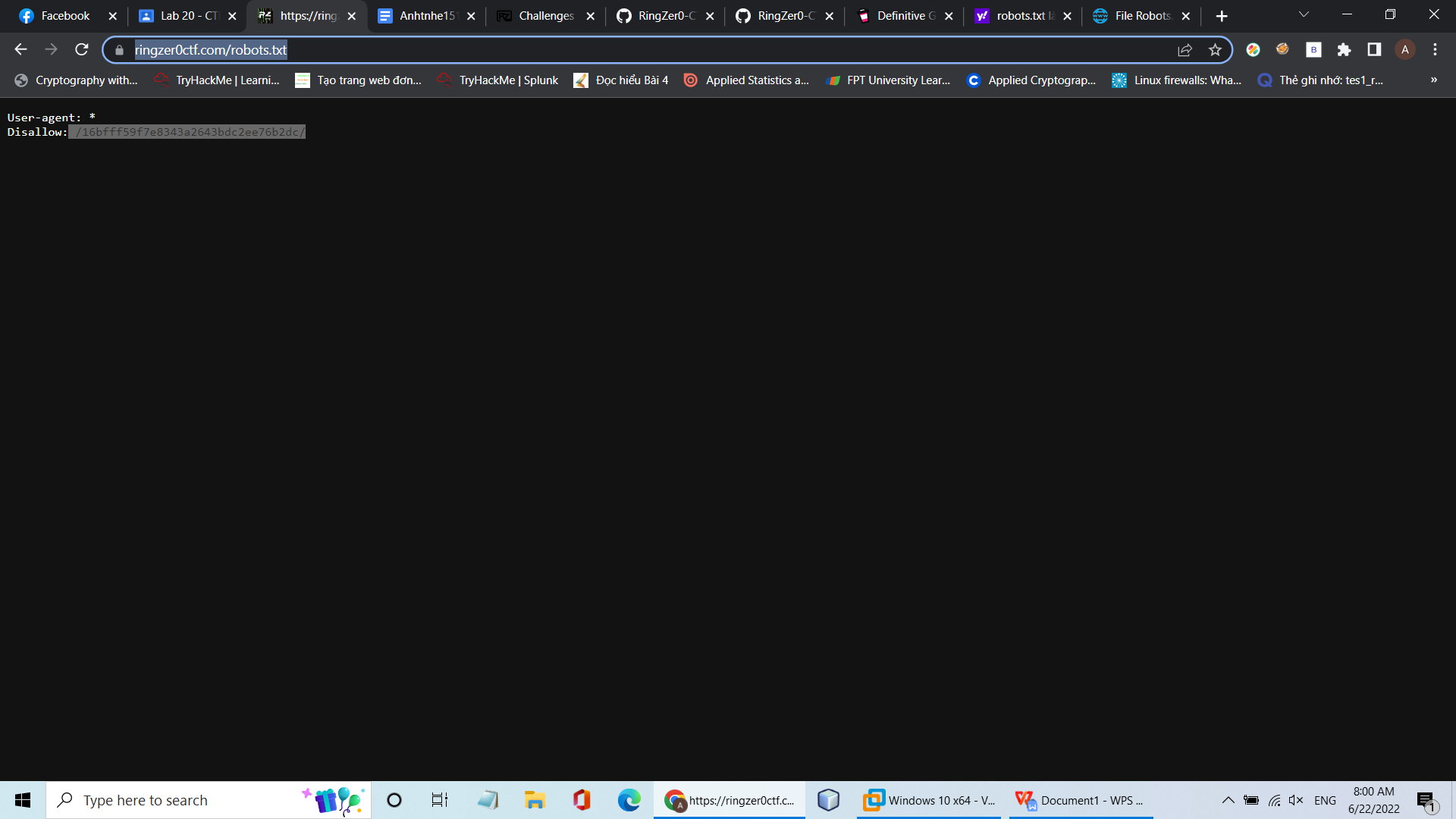


- File robots.txt dùng với mục đích :

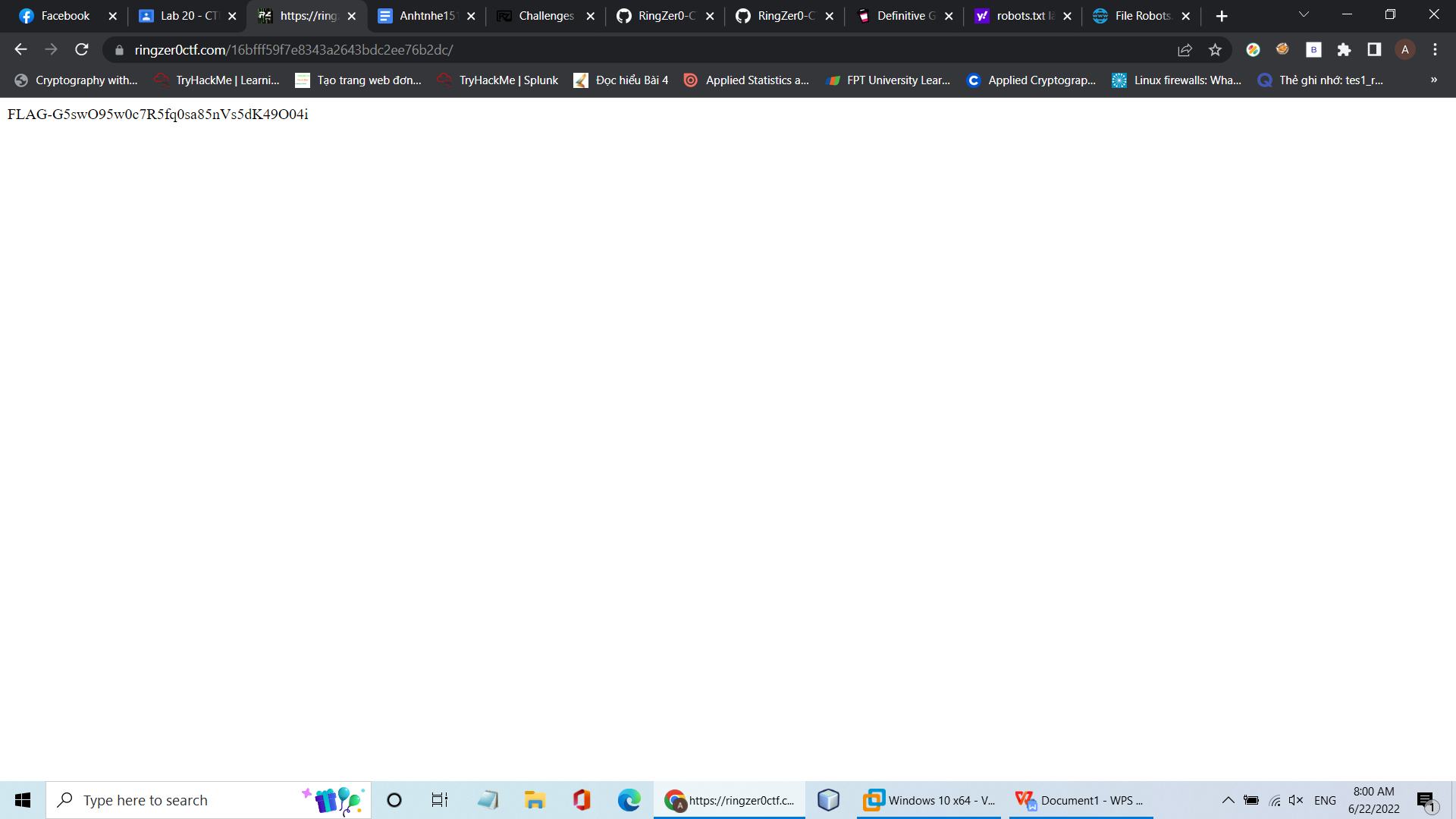
+ Chỉ định vị trí của sơ đồ trang web.

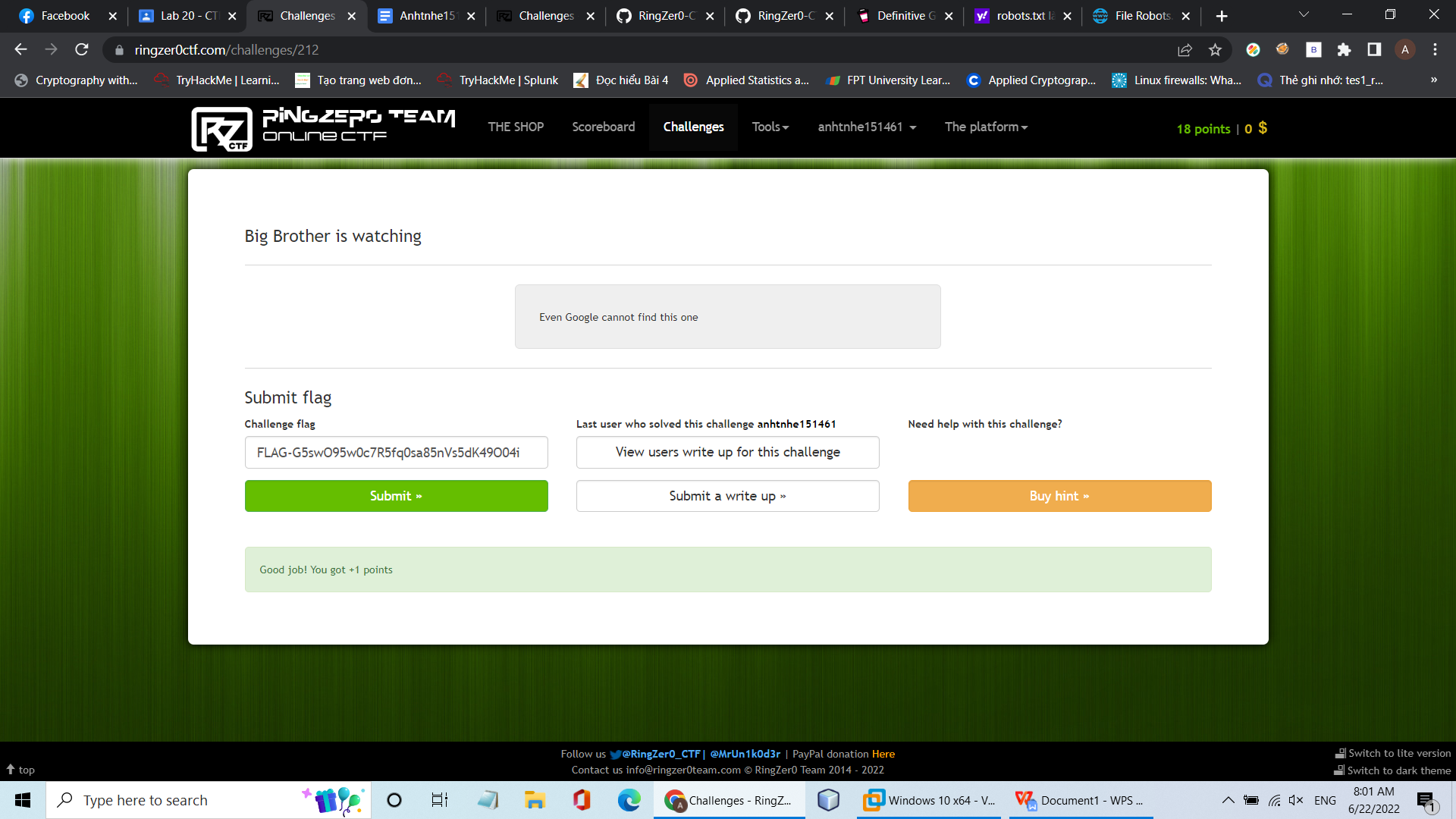
+ Cho phép bot thu thập dữ liệu các mục đã chỉ định.

+ Giữ toàn bộ các phần của trang web ở chế độ riêng tư.



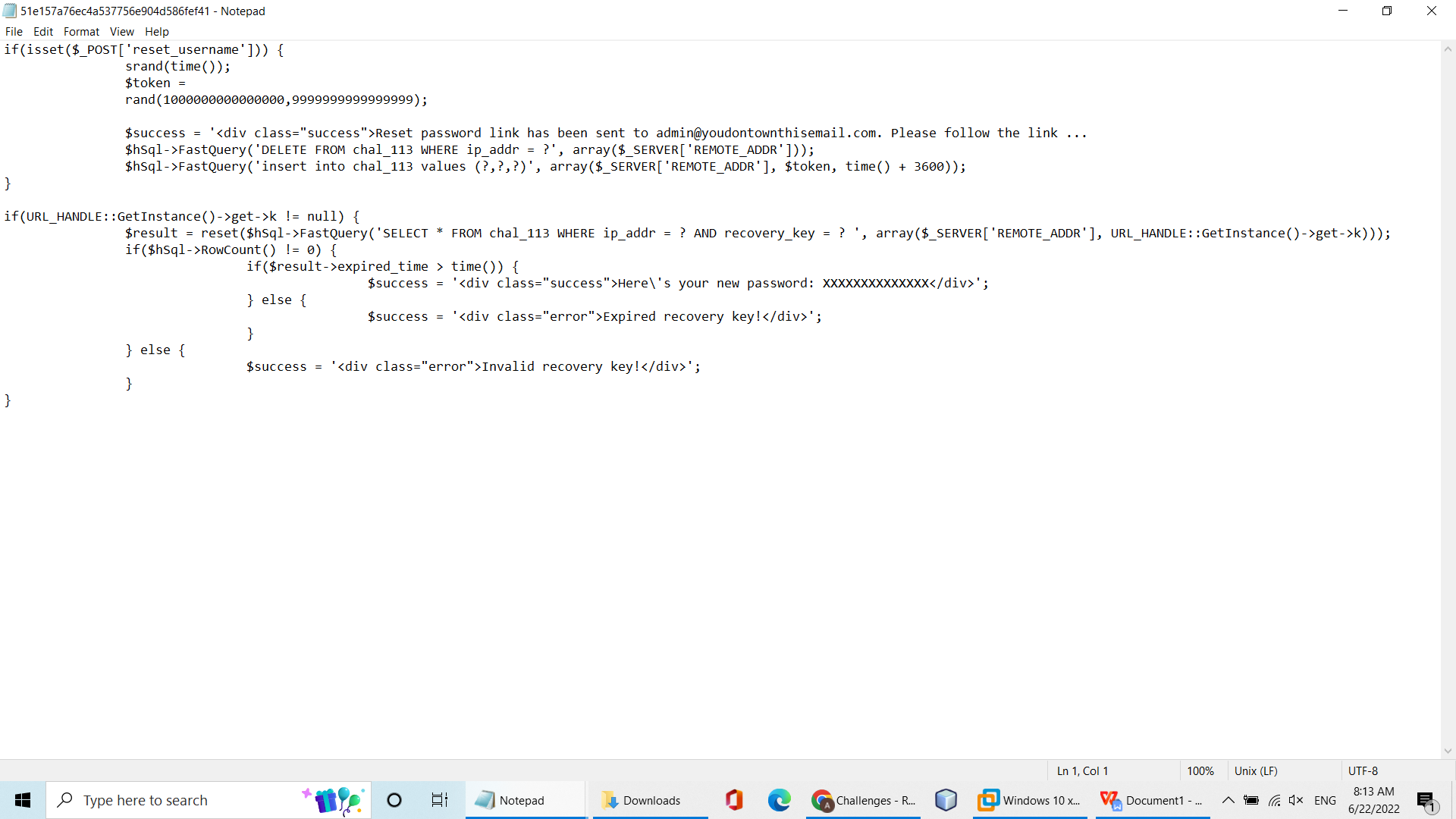
- Sau khi lấy được người dùng không được phép truy cập ta paste lên thanh URL thì sẽ lấy được flag đang được cất giấu ở đây.



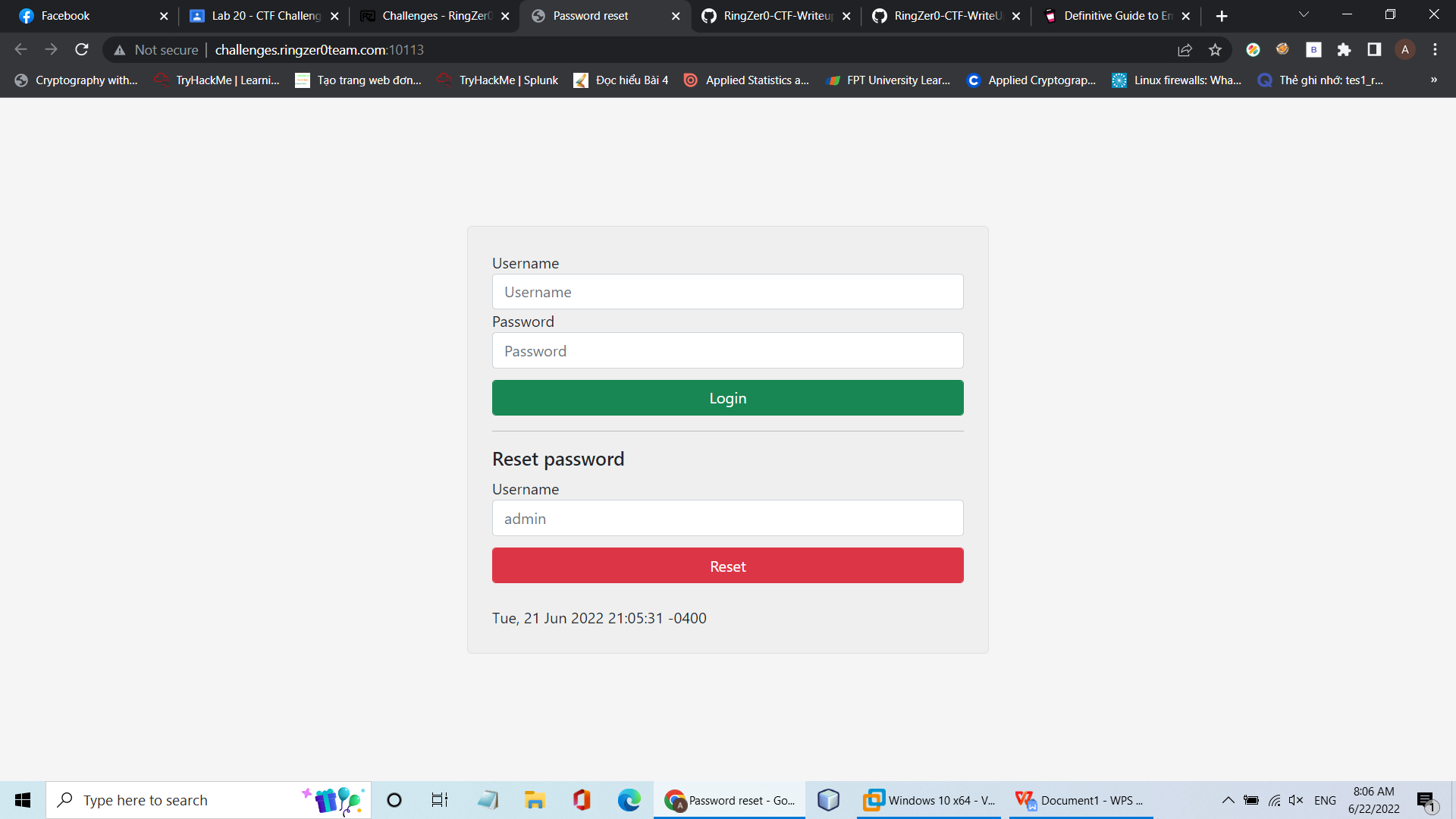


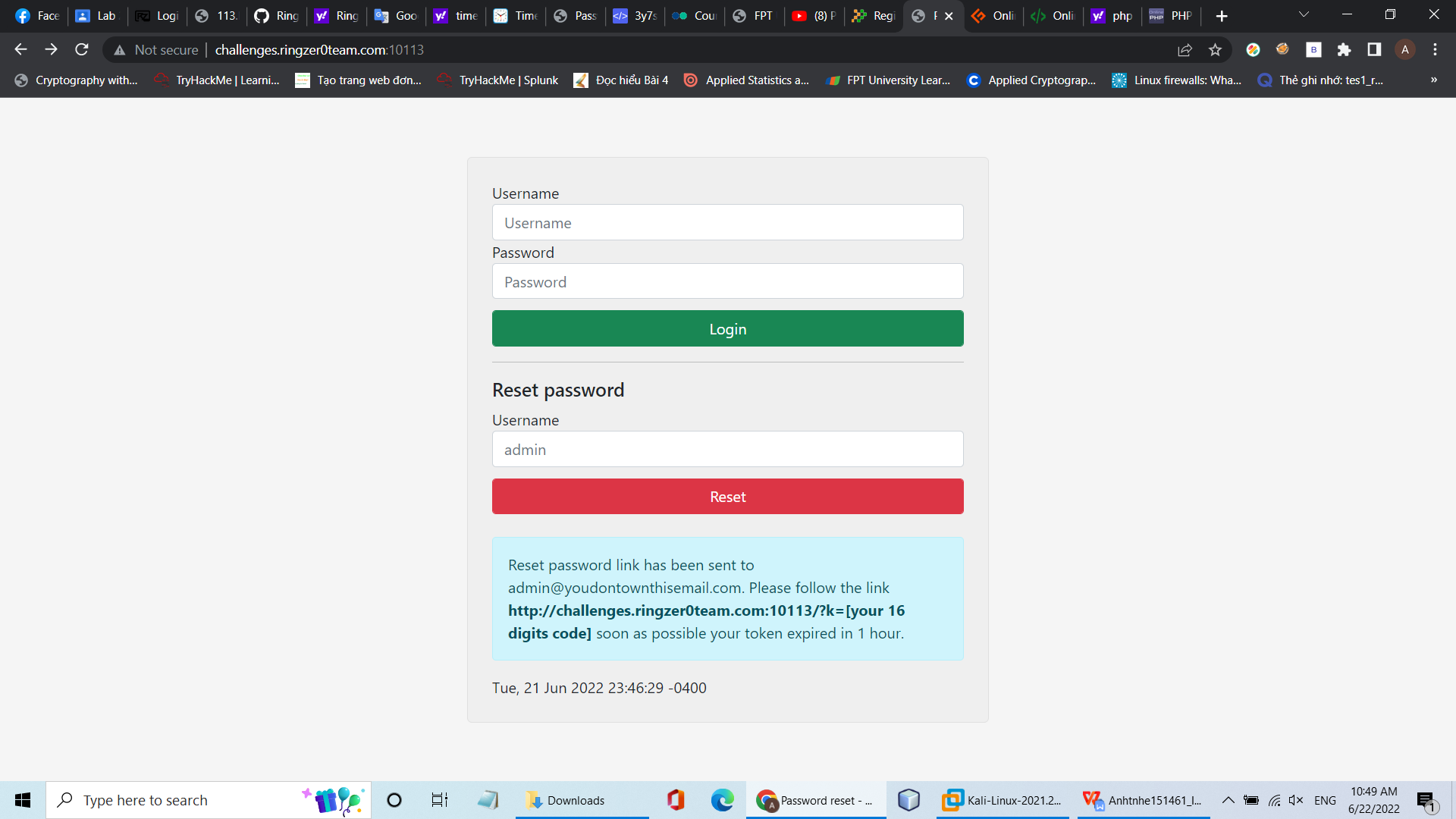
1. **Password reset**

- Ở đây challenge này có cho chúng ta source code của phía back-end. Đầu tiên chúng ta chú ý đến việc token được tạo ngẫu nhiên và truy cập trang web reset mật khẩu với tham số ?k= . Có vẻ hàm srand(time()) sẽ được khai thác để giải được challenge này.

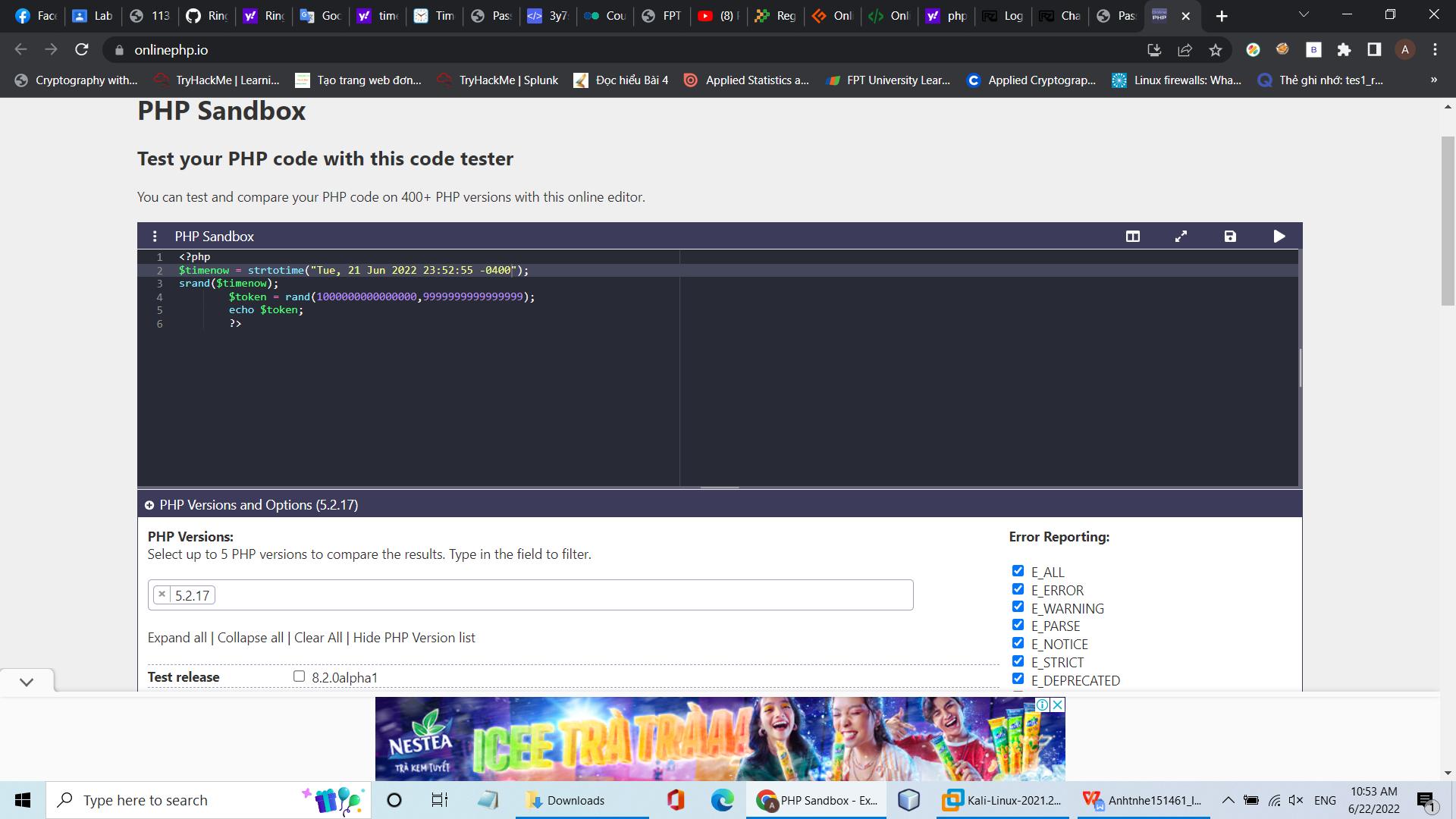


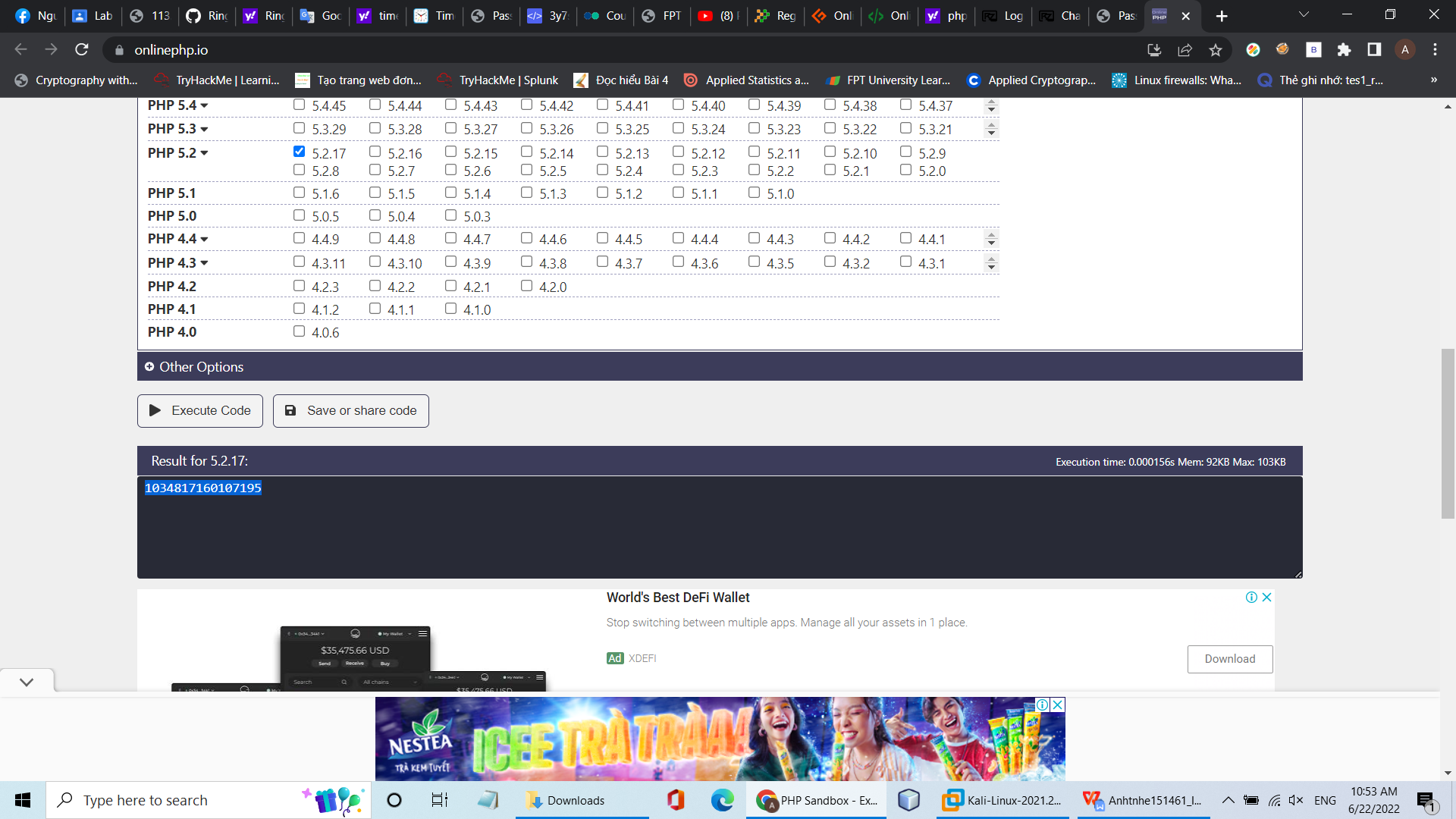
- Ta thấy được sau khi bấm reset thì xuất hiện một token với thời hạn sử dụng là 1 giờ và thời gian của máy chủ web đang sử dụng là UTC (GMT) -4 .





- Sử dụng php phiên bản 5. để compile generate ra token ngẫu nhiên theo thời gian thực , ở đây thời gian thực có ở trong web ( Vì các phiên bản PHP cao hơn không còn hỗ trợ srand() ).





- Sau khi lấy được password reset thì đăng nhập với username là admin và password như ảnh bên dưới thì ta thu được flag và hoàn thành challenge.



