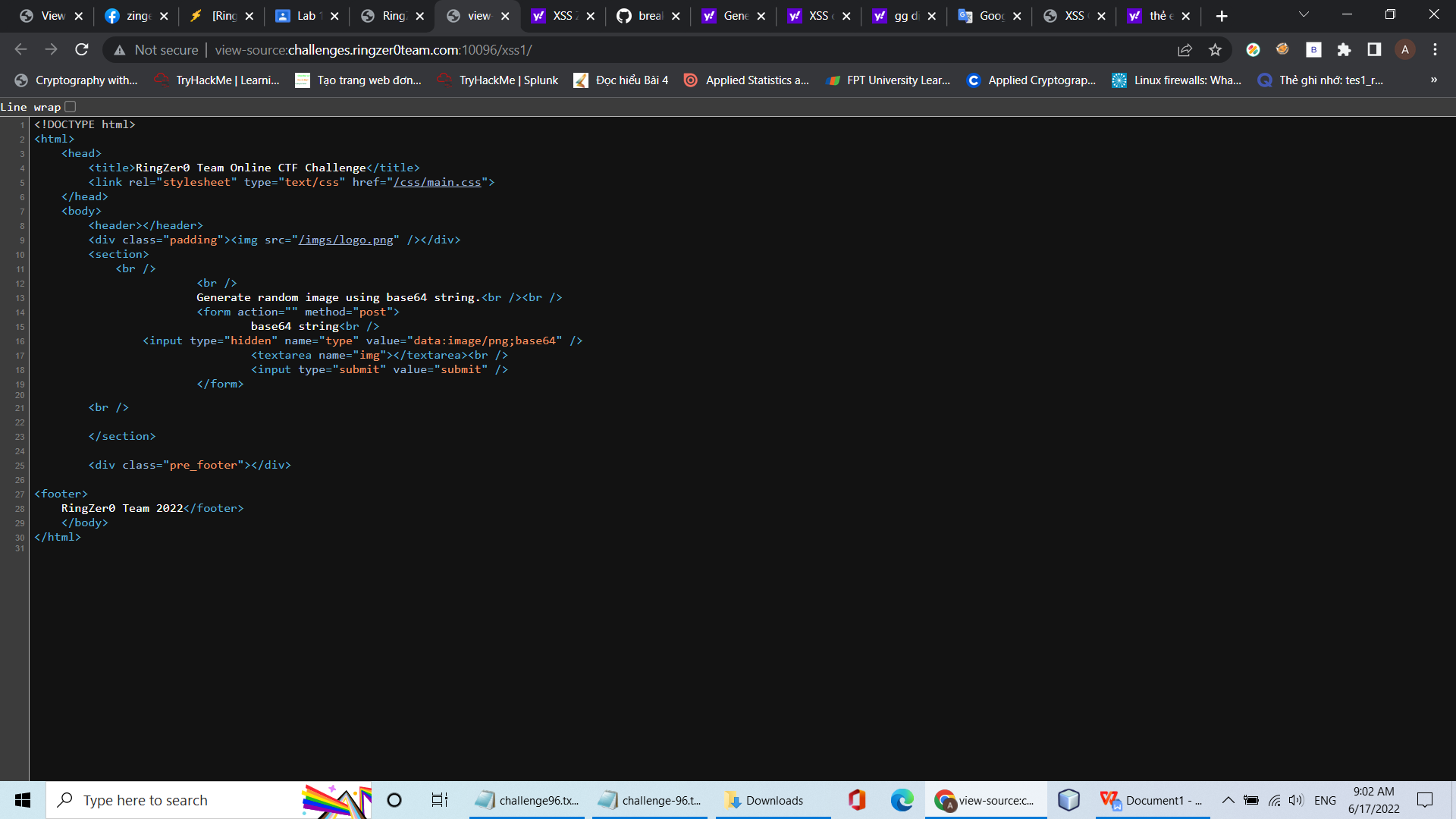
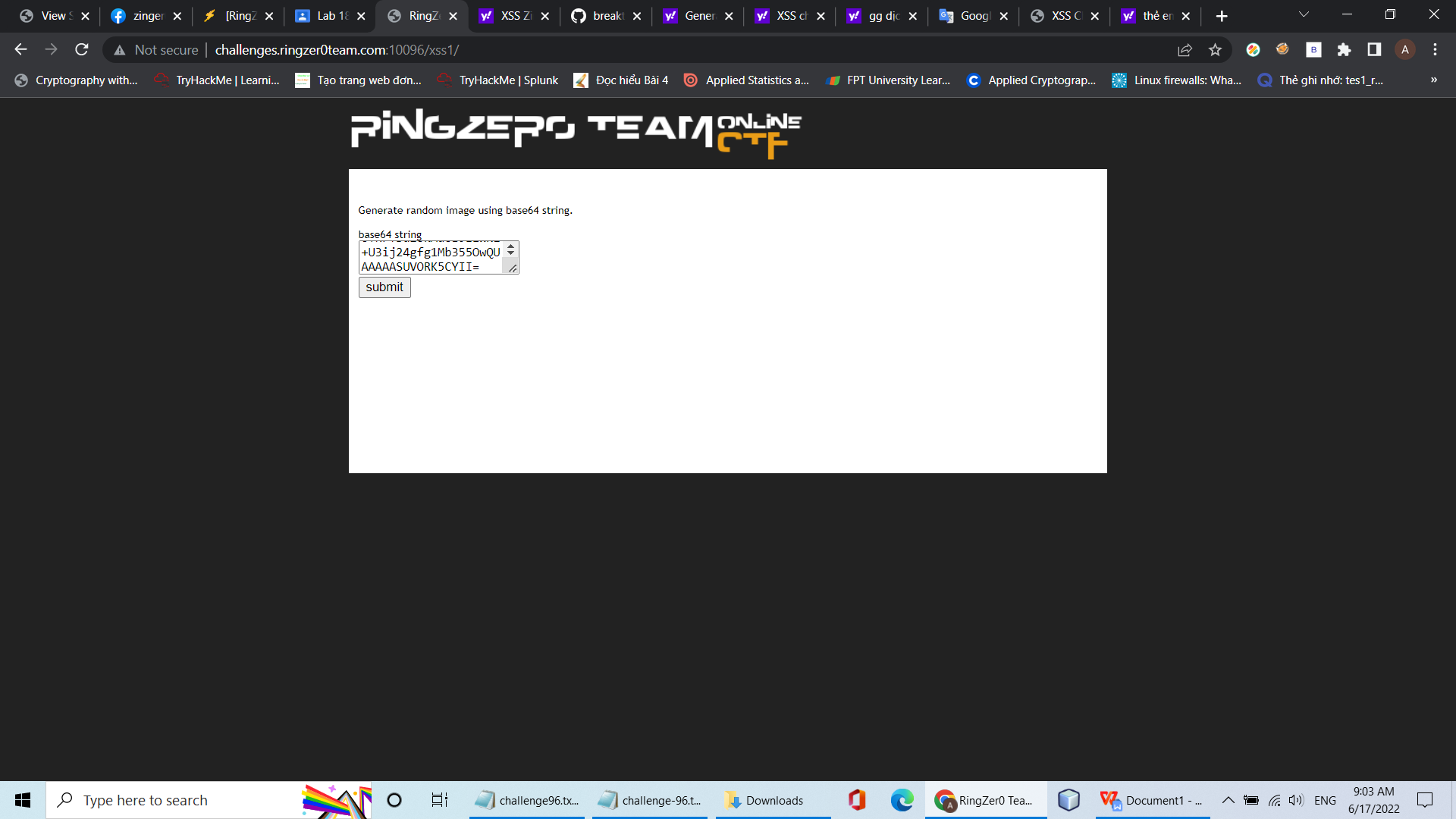
|  |  |
| --- | --- |
| Class | IAW301 |
| Name | Trần Ngọc Anh |
| IC No. | HE151461 |
| Date & Time | 17/6/2022 |

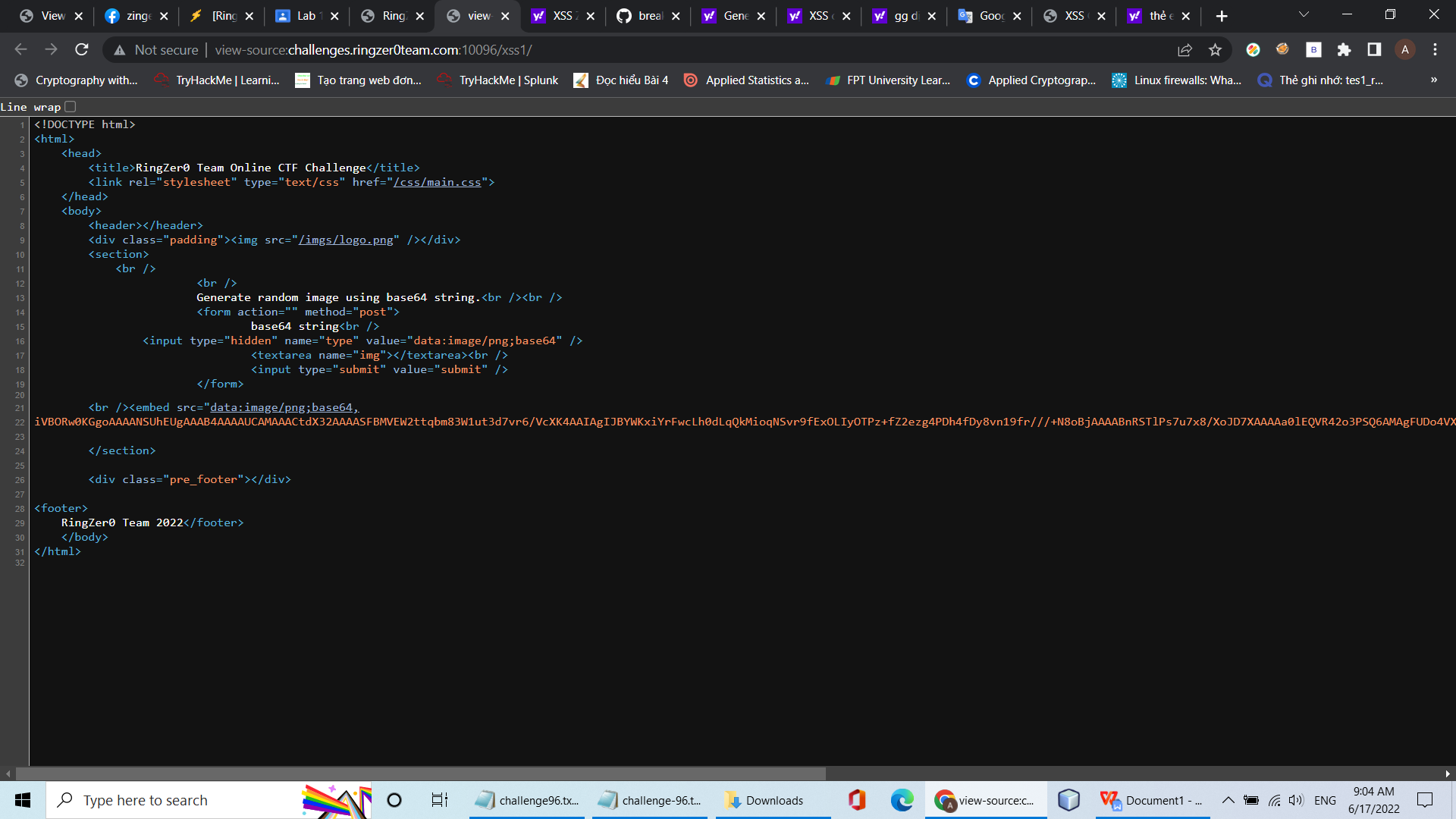
# Lab 18 - CTF XSS Challenge

1. **XSS Challenge 1.**

- Đầu tiên ta thử một base64 của một image bất kì thì thấy được sau khi submit sẽ xuất hiện một thẻ embed với src bằng giá trị hidden của form input + “,”.



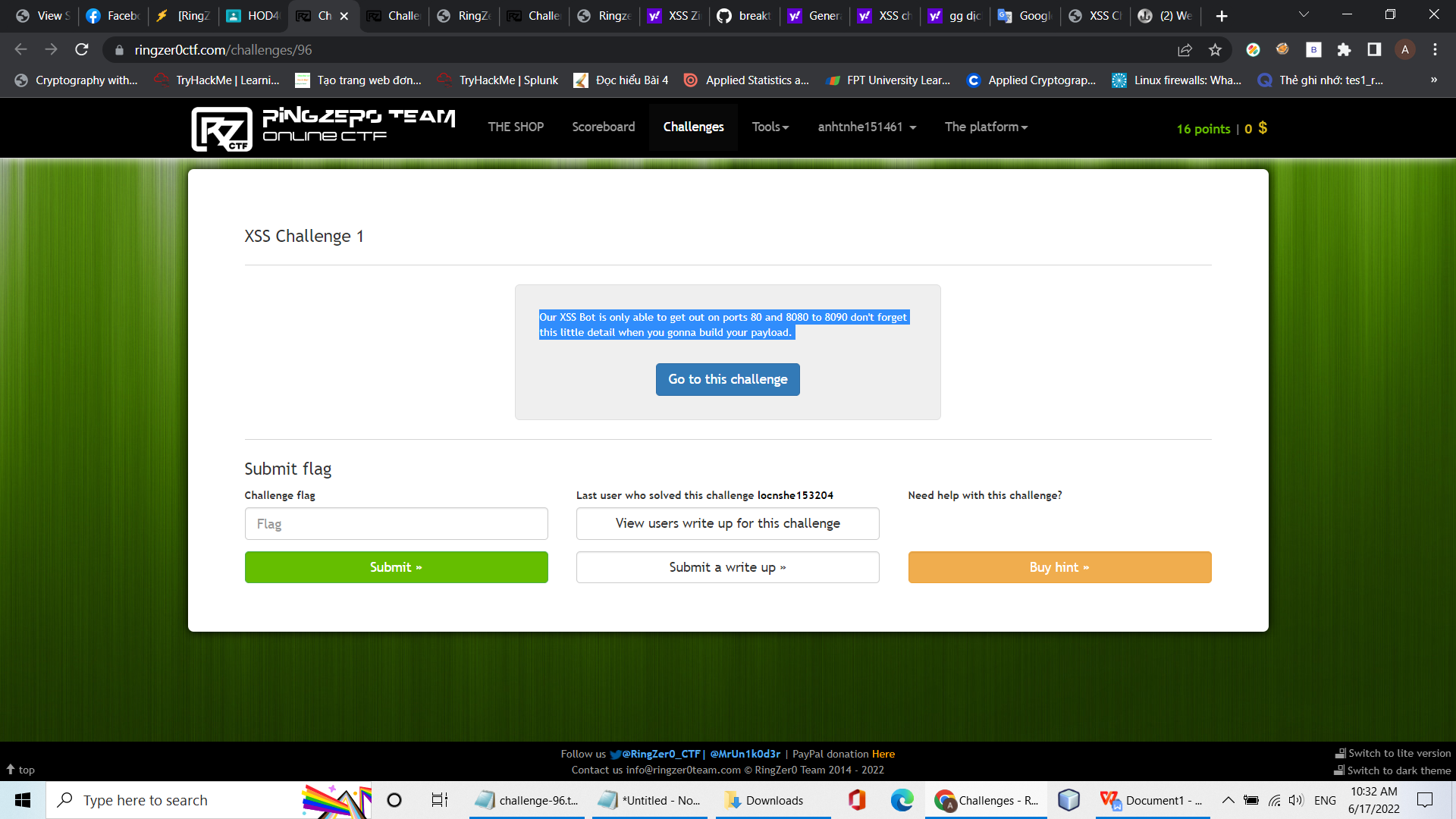


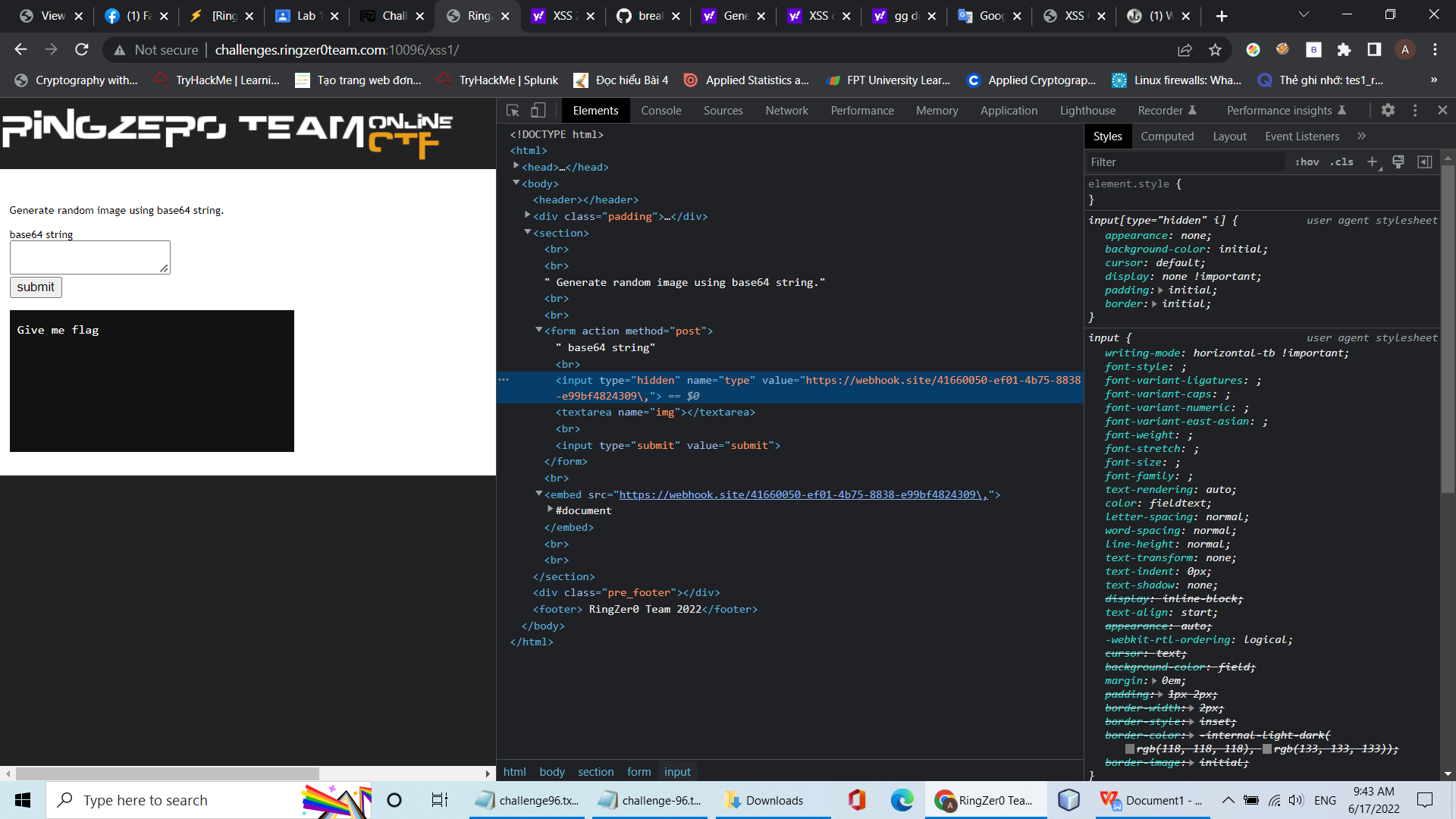


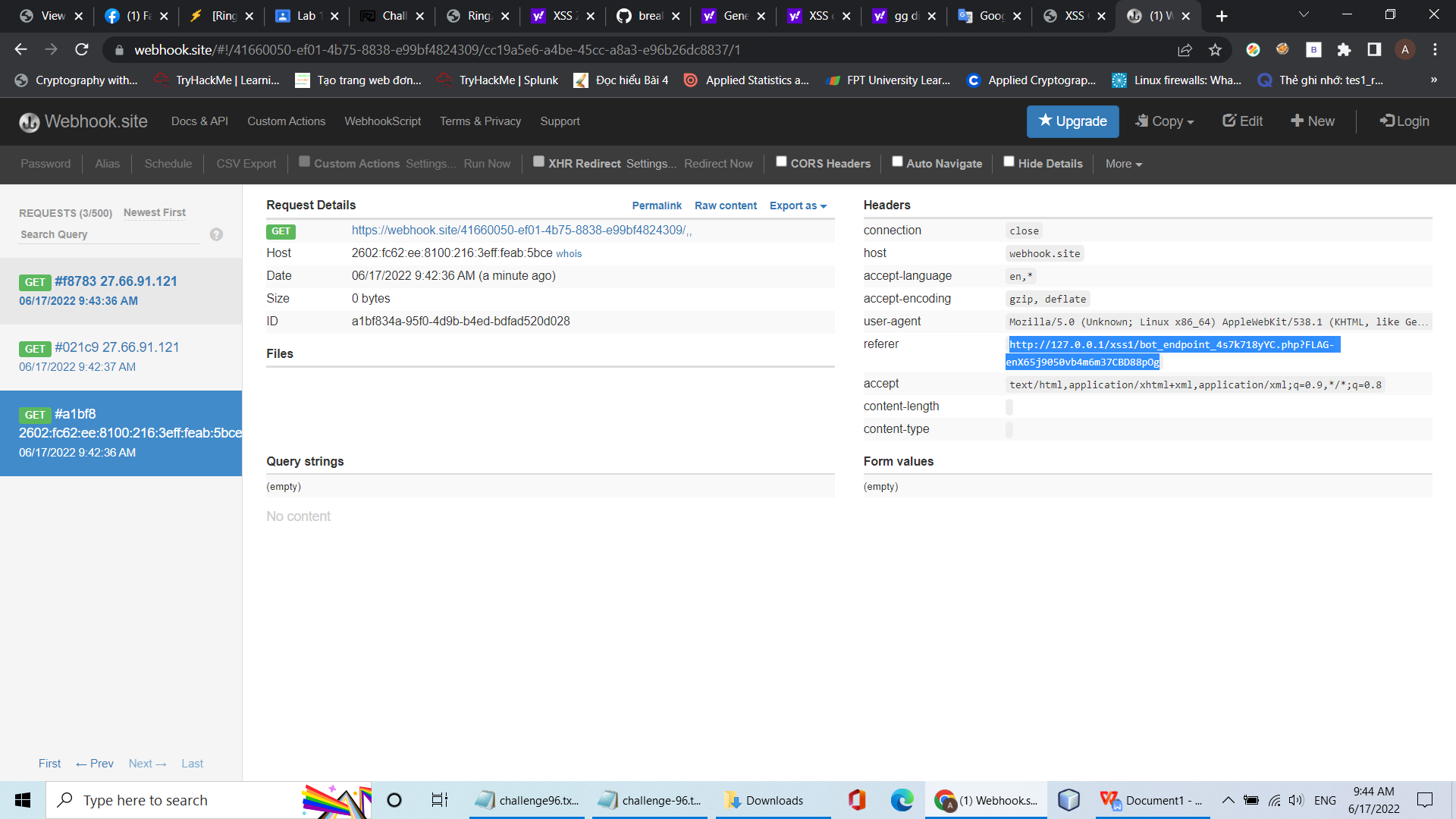
- Vì vậy chúng ta nghĩ tới việc chỉnh sửa value của form hidden input. Sau đó sẽ submit lại form để inject payload vào phần src của embed.

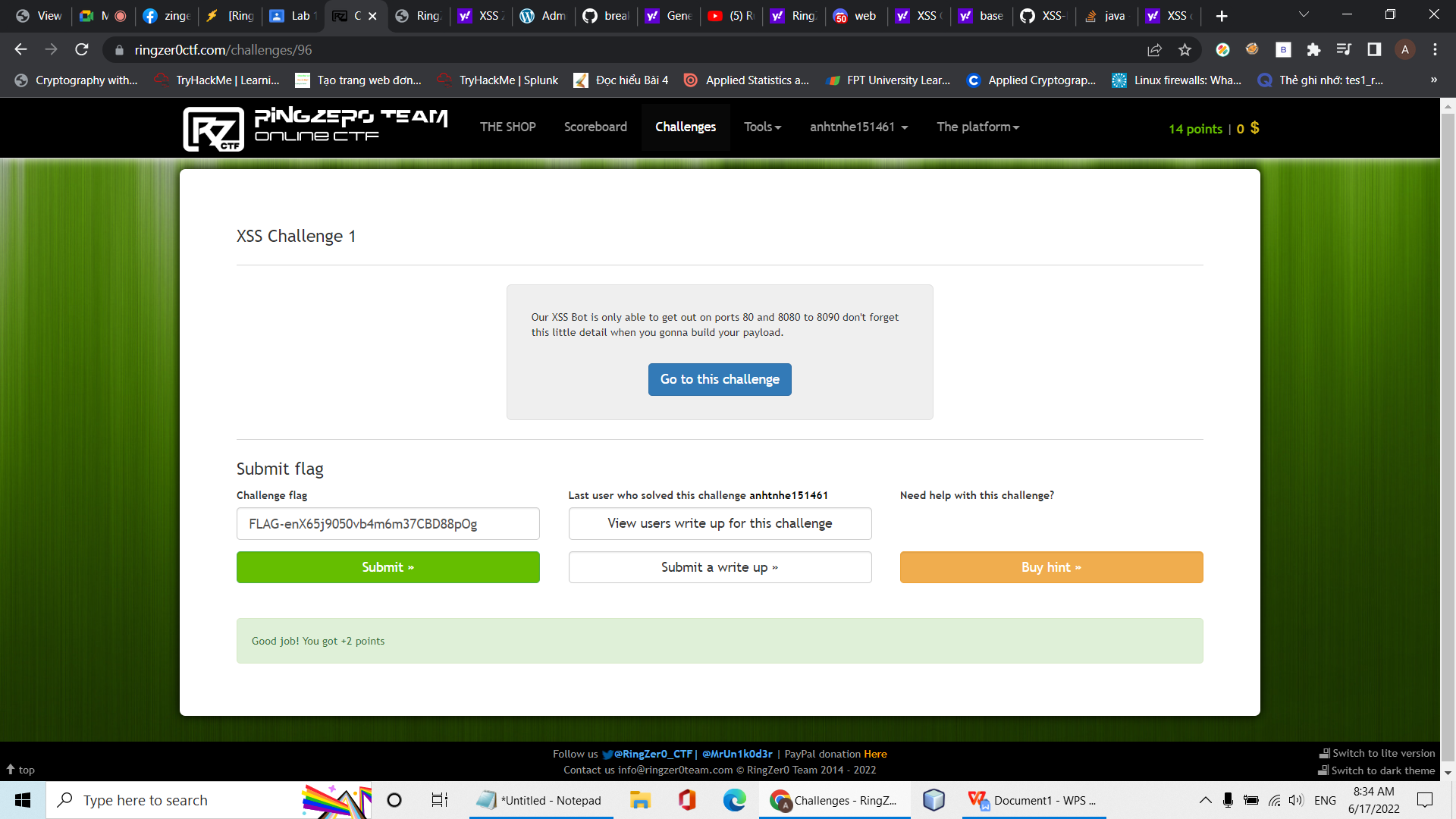
- Quay lại chút đầu đề bài thấy có yêu cầu phải tương tác với cổng 80 hoặc các cổng từ 8080 đến 8090 mà ở challenge này lại đang sử dụng cổng 10096.

- Tham khảo trên mạng thì biết được có một trang tên webhook với mục đích dùng để server của ringzer0team gọi tới webhook của ta trên 1 trong các cổng mà đề bài cho phép để lấy được flag.



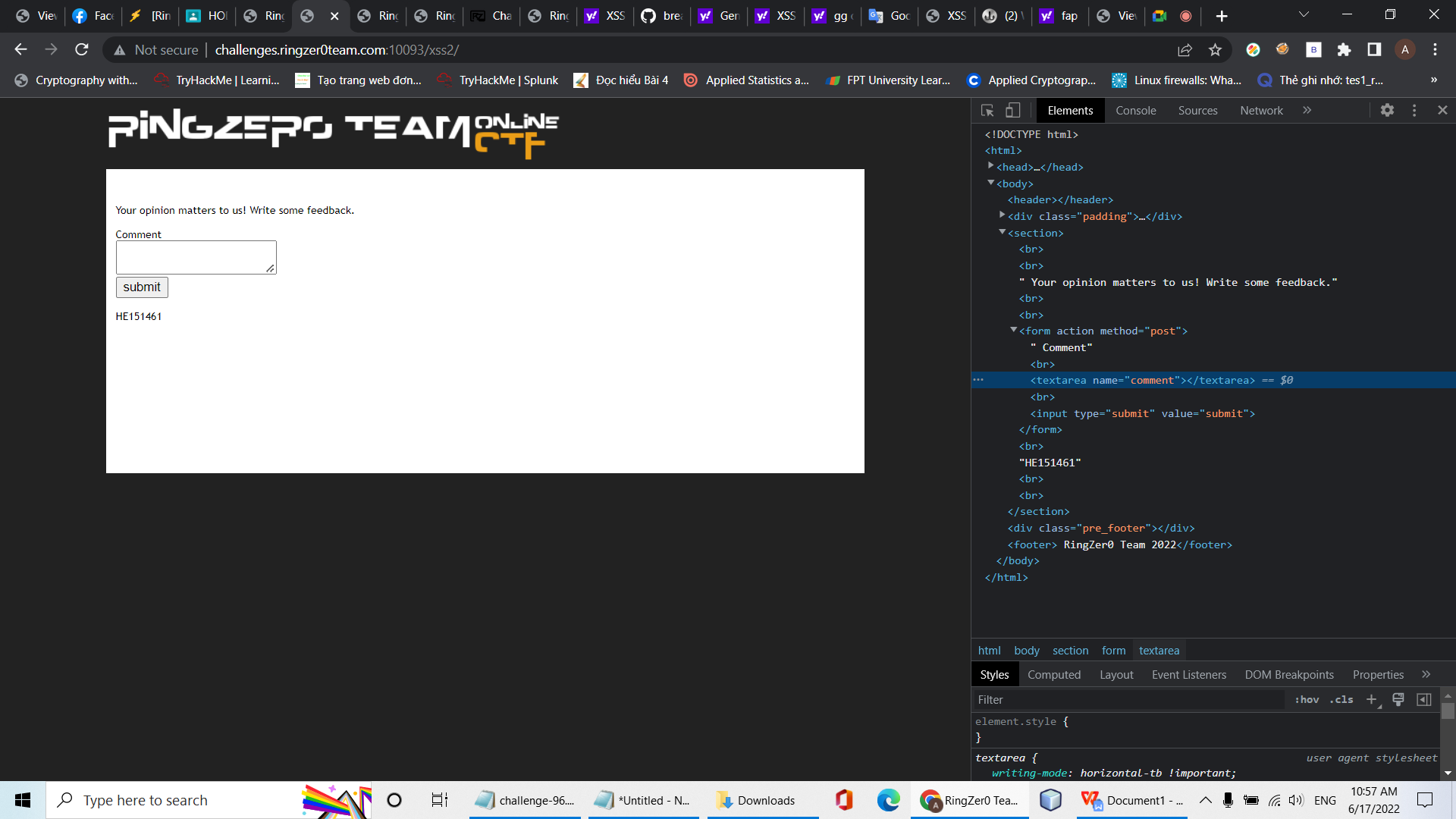




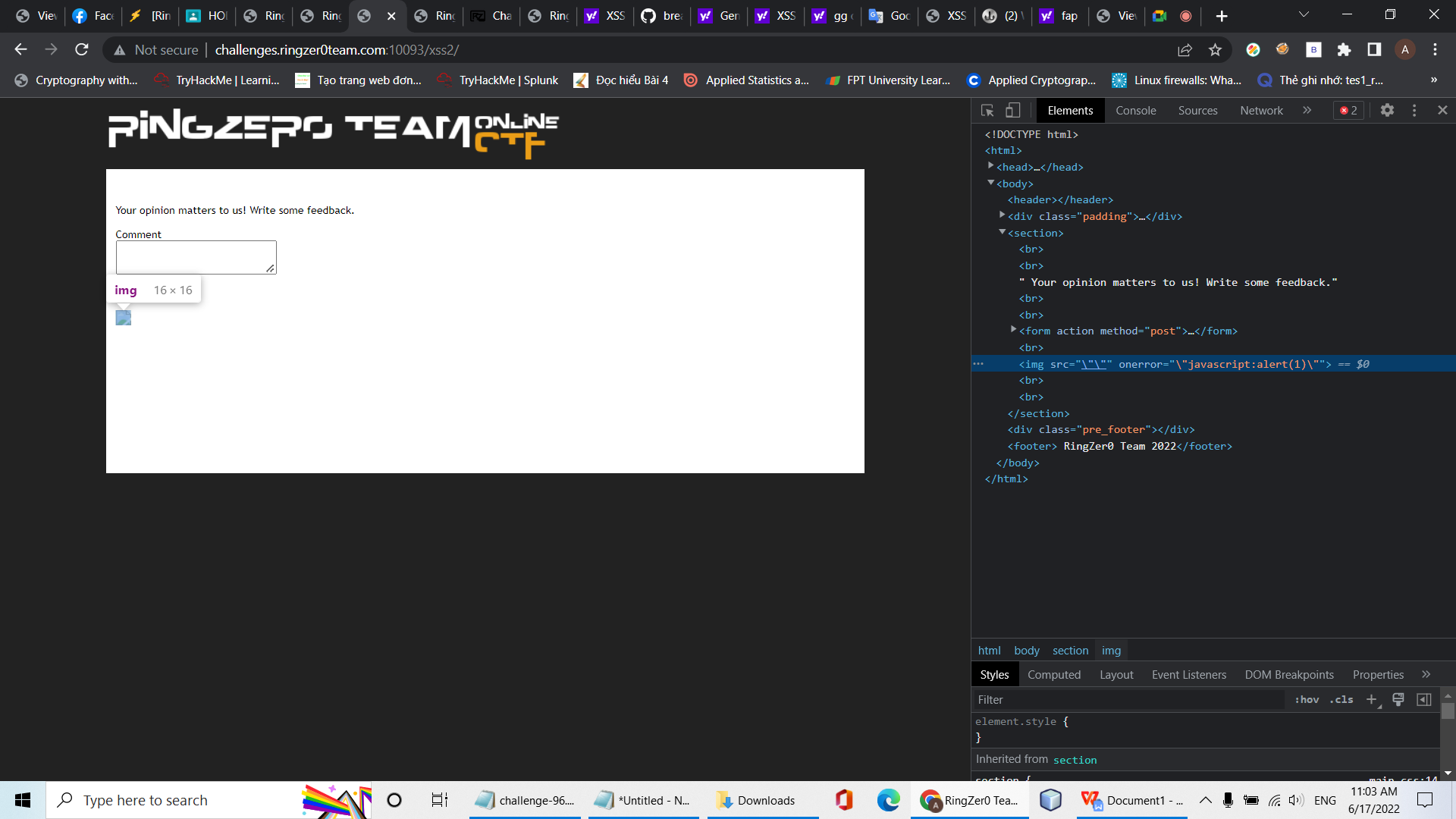


1. **XSS Challenge 2.**

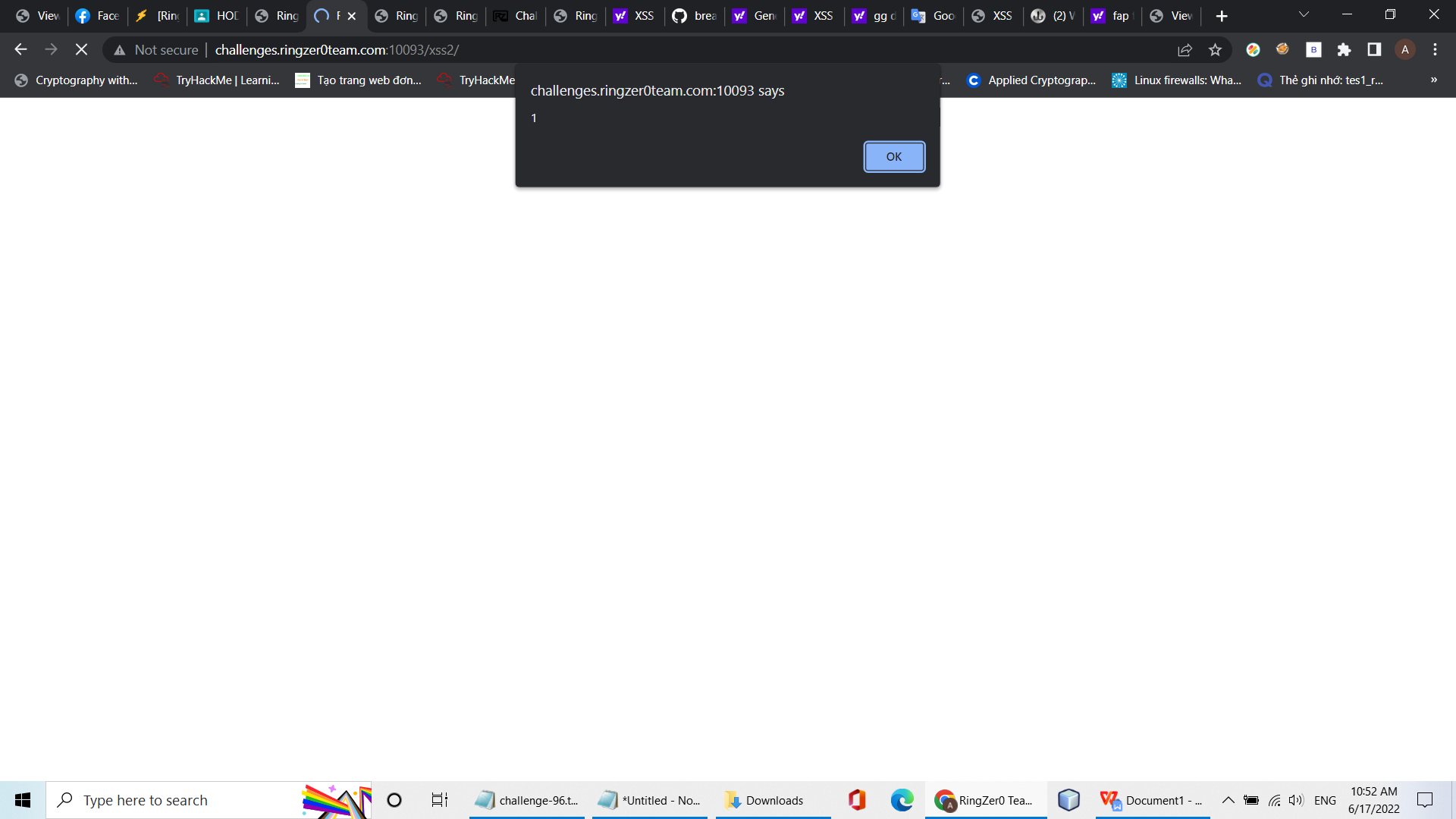
- Đầu tiên chúng ta thử comment để hiển thị ra mã số sinh viên. Thì thấy được ở đây trang web đã inject thêm đoạn comment ta vừa gõ vào phía dưới.



- Ta thử một payload <img src="" onerror="javascript:alert(1)"> thì thấy được các dấu nháy đã bị thêm một dấu \



- Vì vậy ta sẽ bỏ đi các dấu nháy trong payload <img onerror=javascript:alert(1) src= > và đã chứng minh được inject thành công.



- Sau đó ta dùng webhook như challenge 1 sẽ thấy được flag ở referer.

