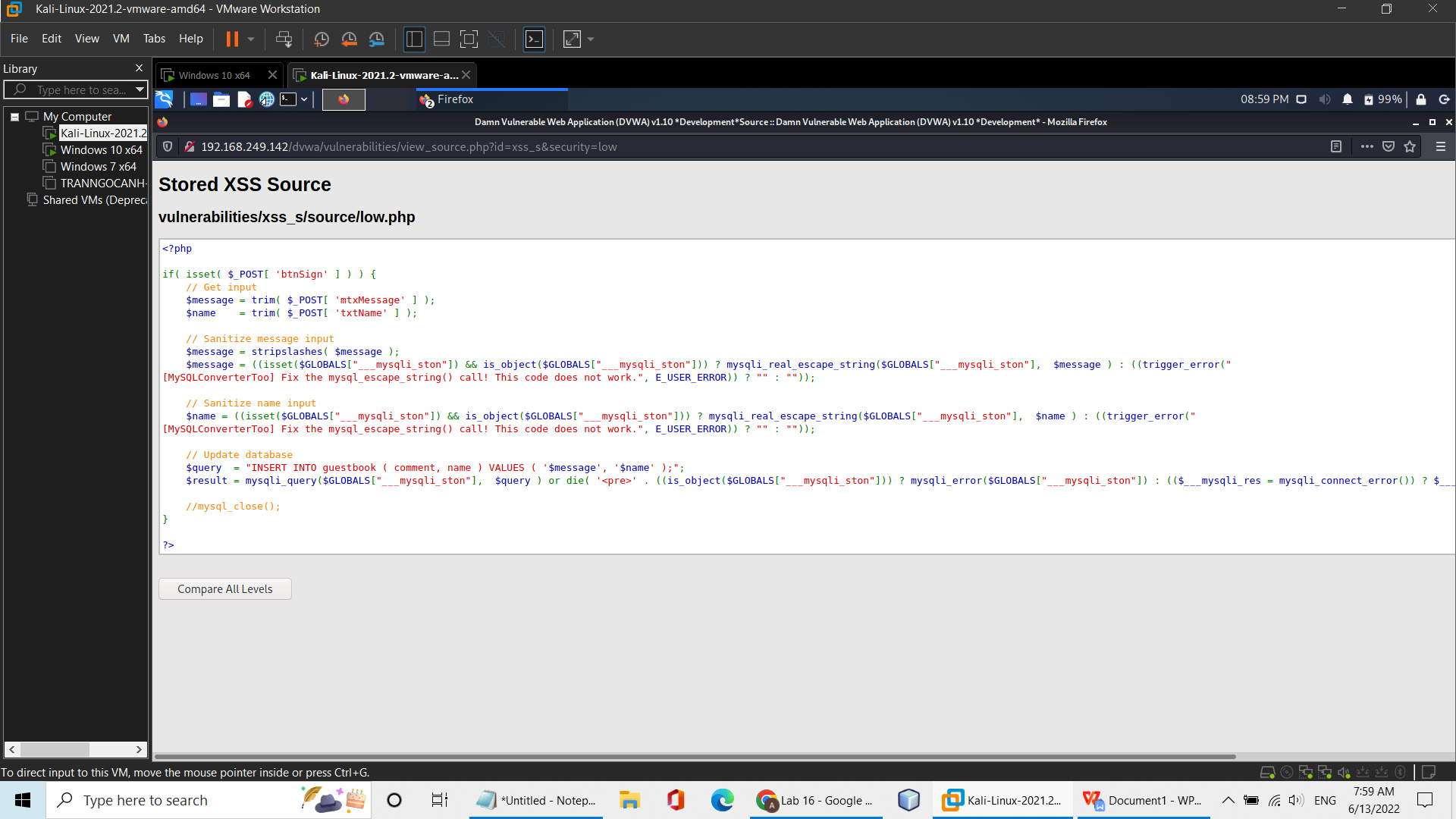
|  |  |
| --- | --- |
| Class | IAW301 |
| Name | Trần Ngọc Anh |
| IC No. | HE151461 |
| Date & Time | 13/6/2022 |

**LAB 16**

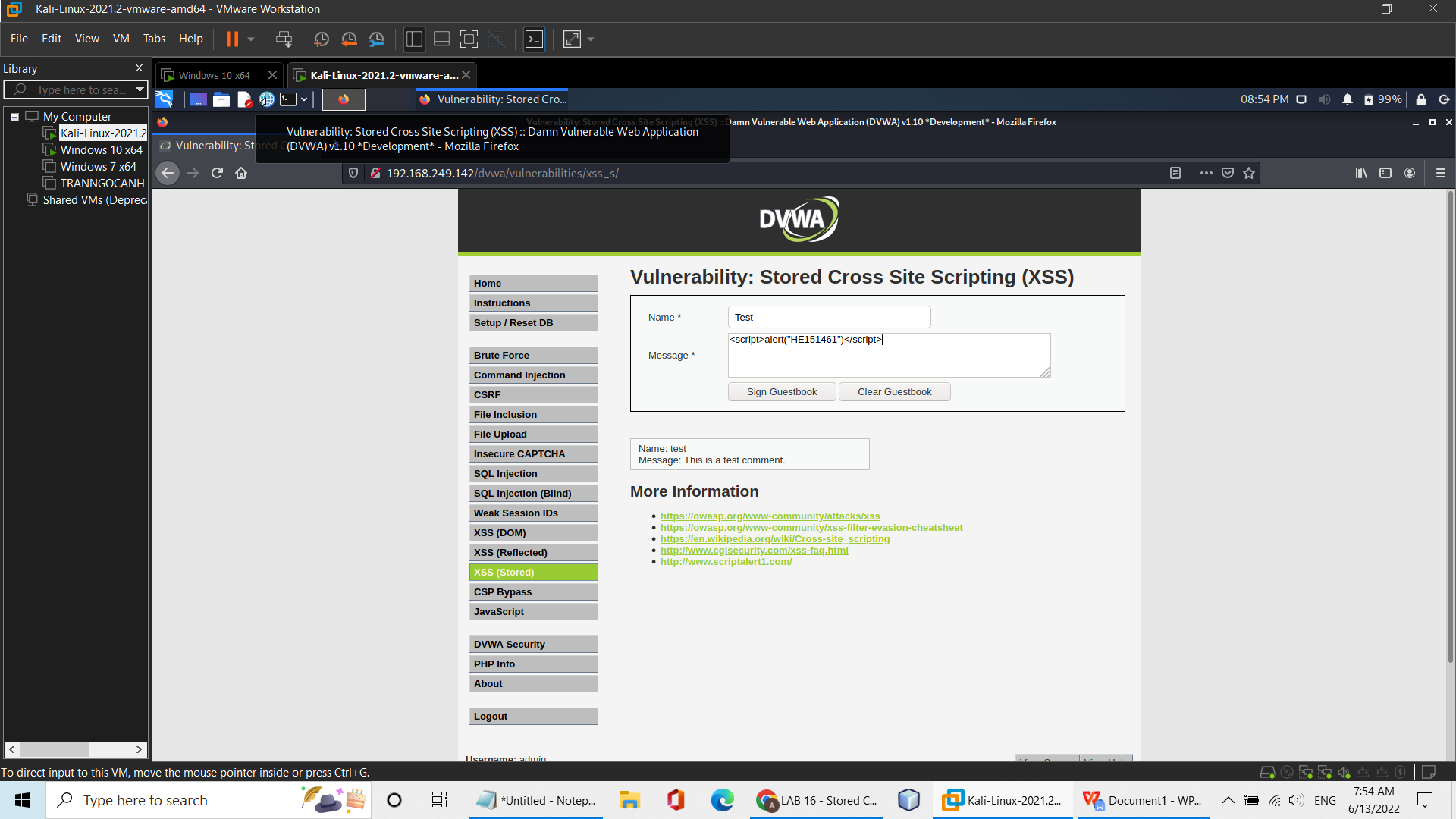
**Stored Cross Site Scripting**

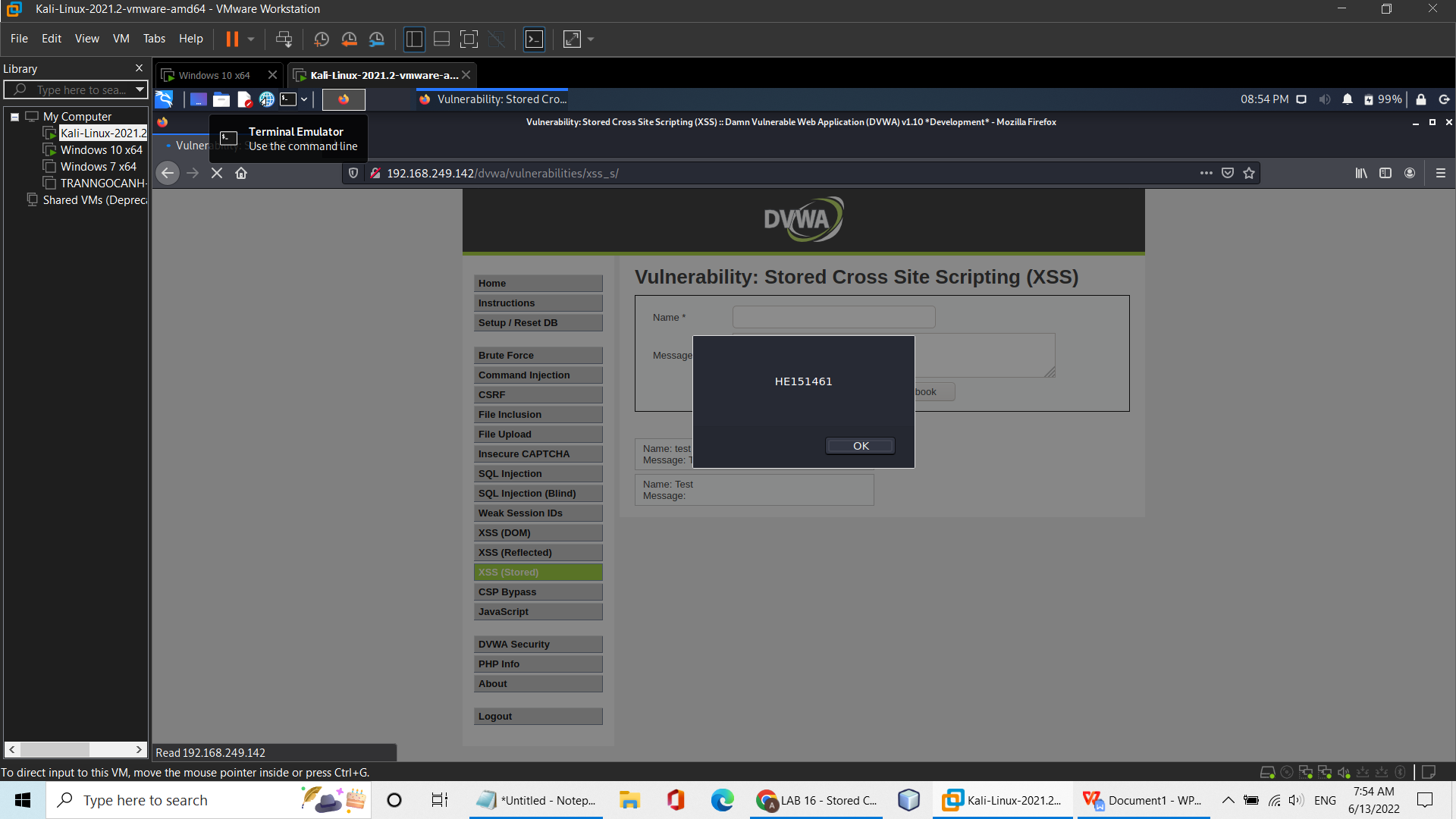
1. **Low**

- Nhìn qua source code chúng ta thấy trường input message chỉ có hàm stripslashes() dùng để xóa đi dấu ‘\’ trong chuỗi.

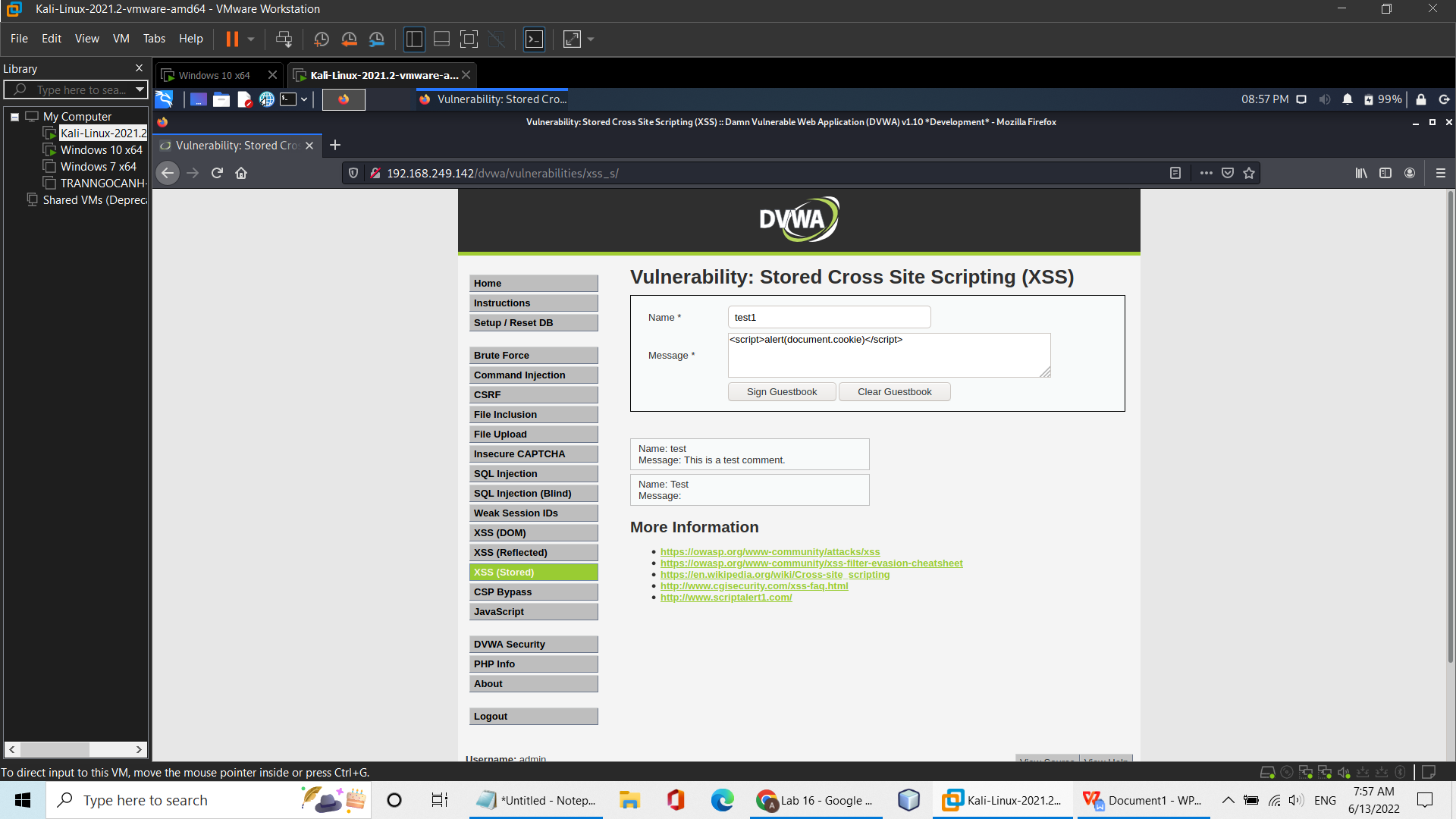


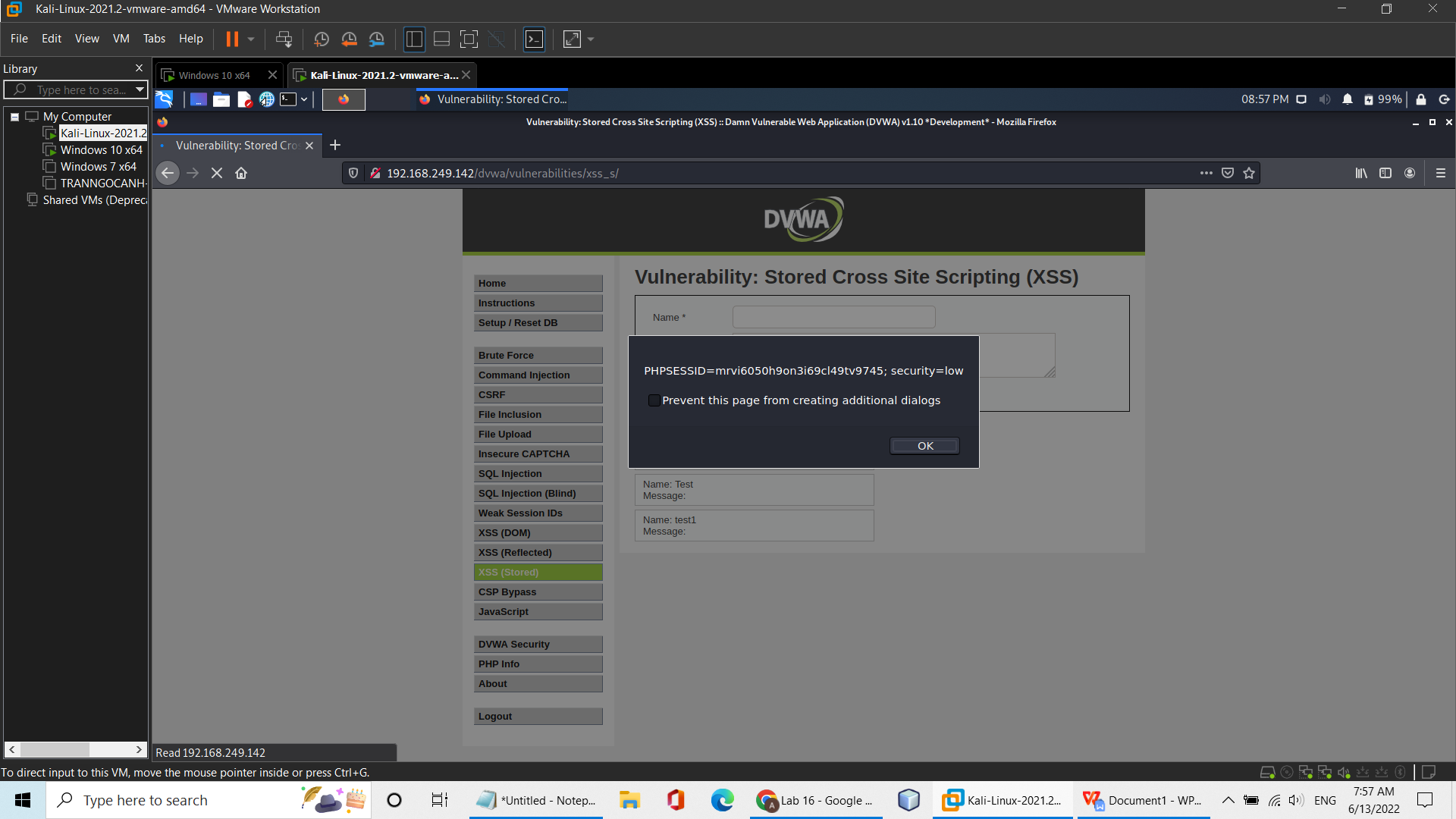
- Vì vậy chúng ta thử khai thác như bình thường inject đoạn code <script>alert("HE151461")</script> .





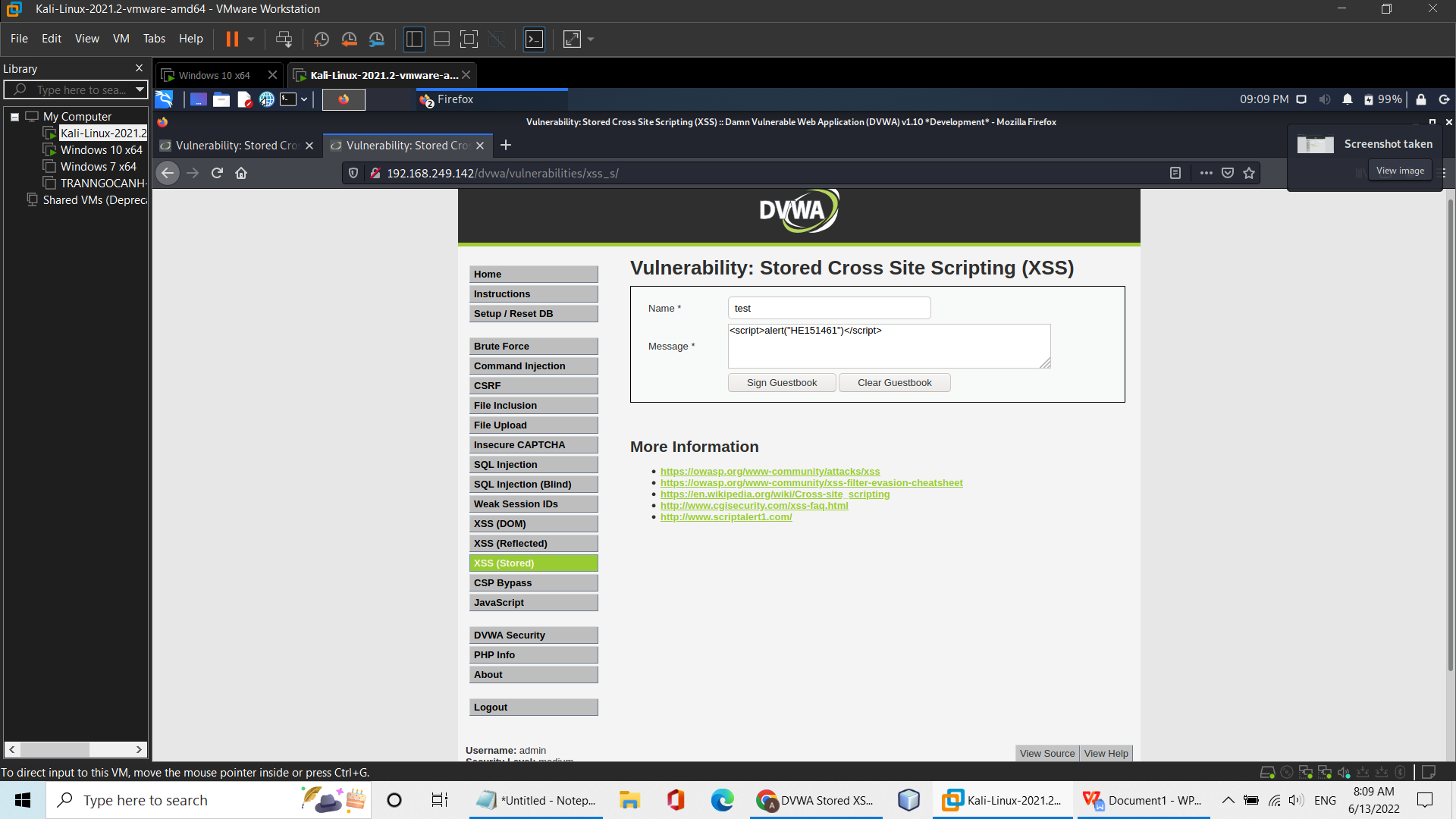
- Sau khi chứng minh có lỗi thành công thì chúng ta khai thác cookie và hoàn thành mức low.<script>alert(document.cookie)</script>

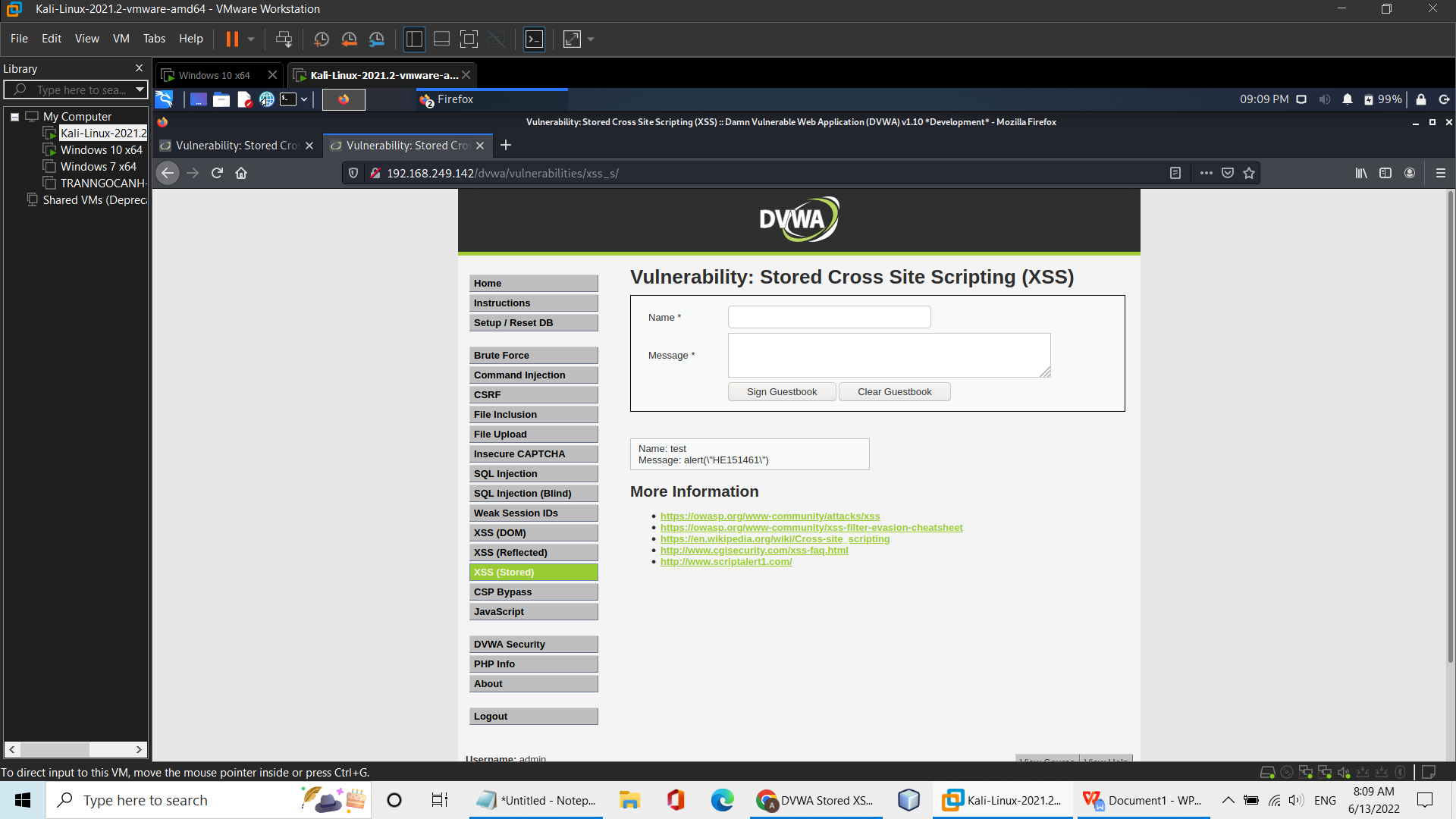




1. **Medium:**

- Đến mức medium thì khi ta thử như mức low thì không chứng minh có lỗi được.

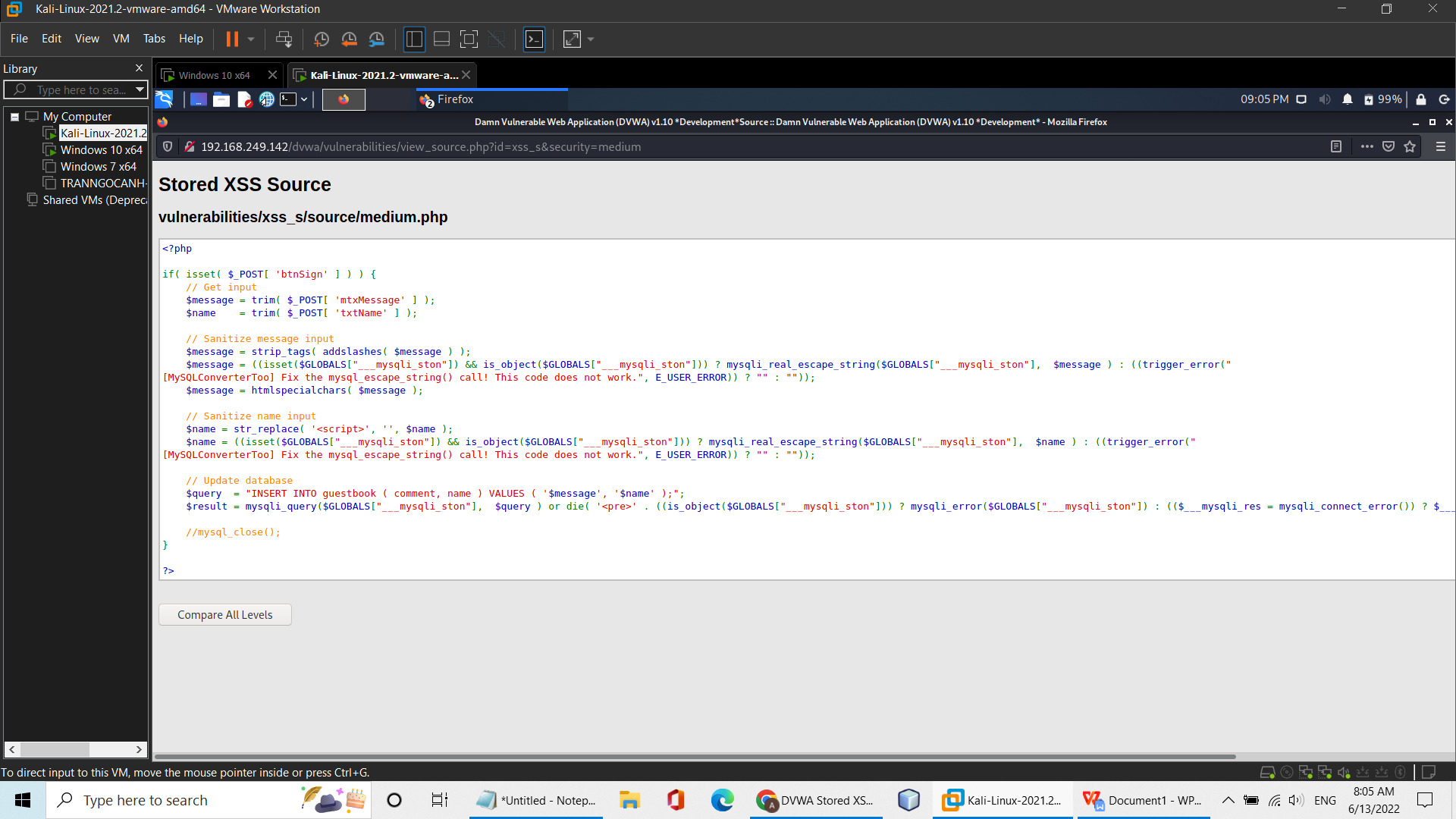




- Đành phải nhìn qua source code để tìm nguyên nhân thì ở đây chúng ta thấy được với :

+ message : có hàm strip\_tags() dùng để loại bỏ tất cả các thẻ html trước khi lưu trữ chúng trong database . Hàm htmlspecialchars() dùng để chuyển đổi tất cả các ký tự không hợp lệ như &, ”, ’, > và < ở dạng mã hóa ký tự html tương đương để chúng không còn ở dạng ban đầu khi phản ánh lại trong trình duyệt.

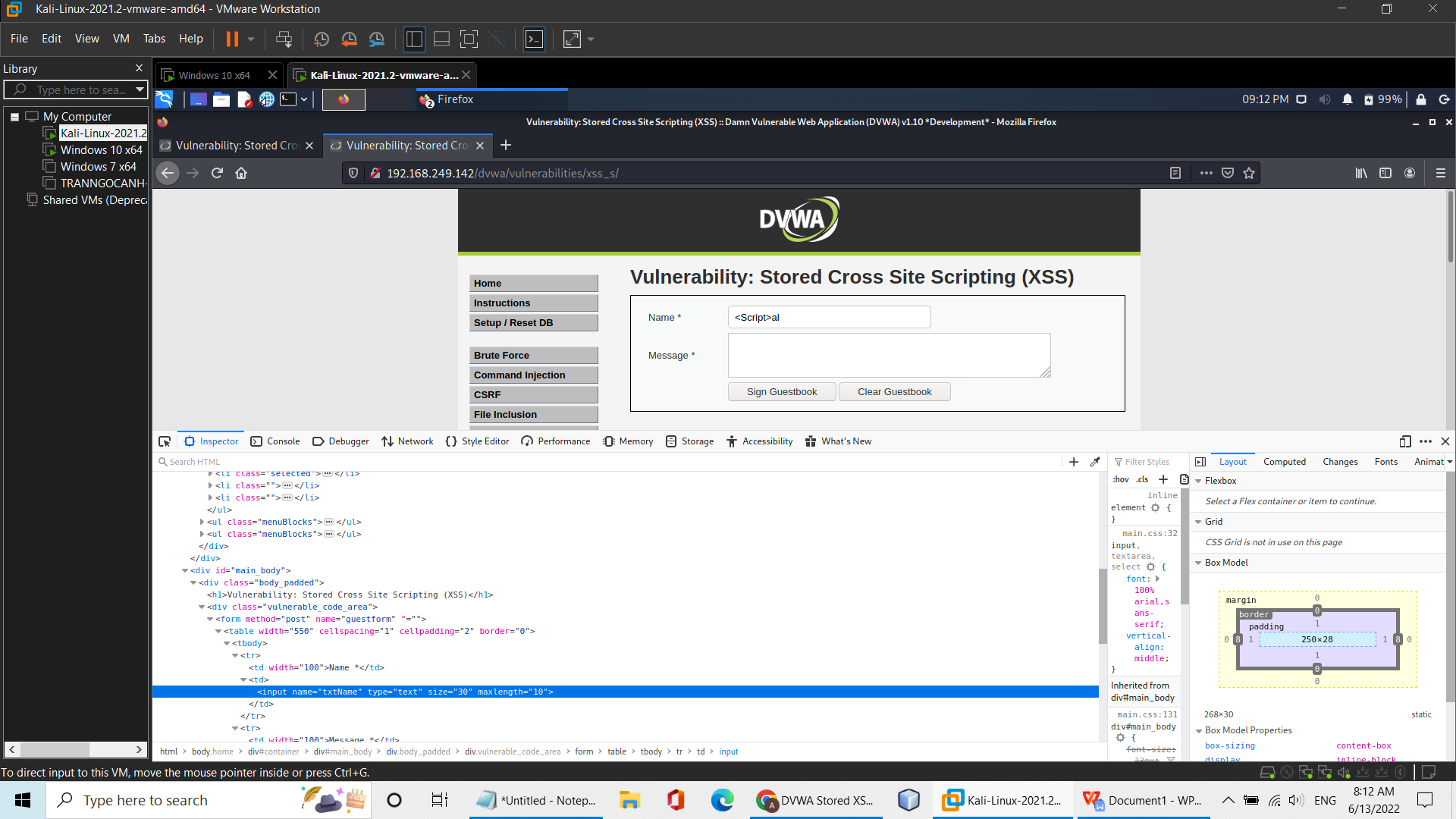
+ name : Hàm str\_replace() với tham số như trong ảnh bên dưới để thay thế thẻ <script> thành kí tự rỗng để đoạn code ta inject không hoạt động.

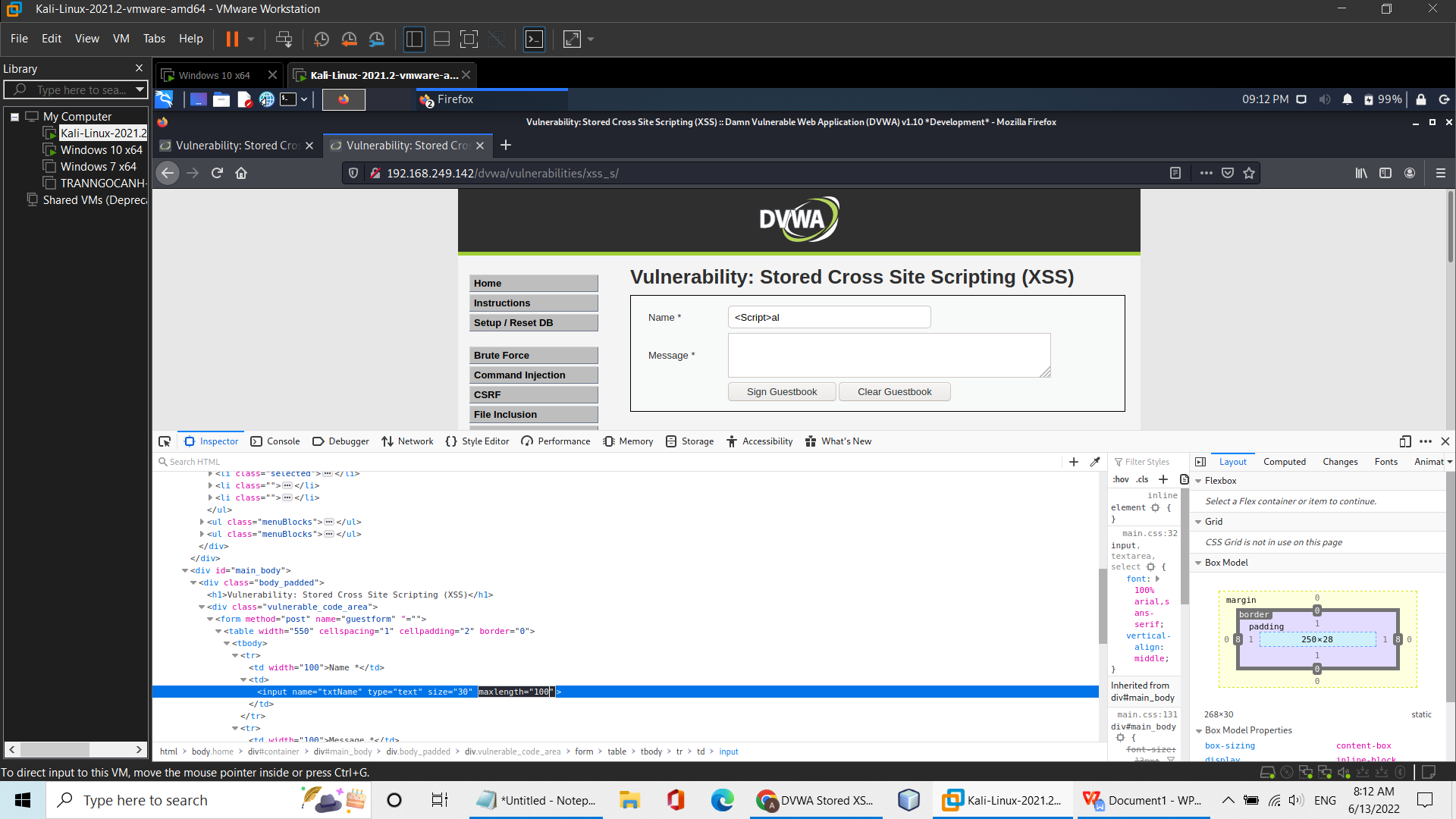


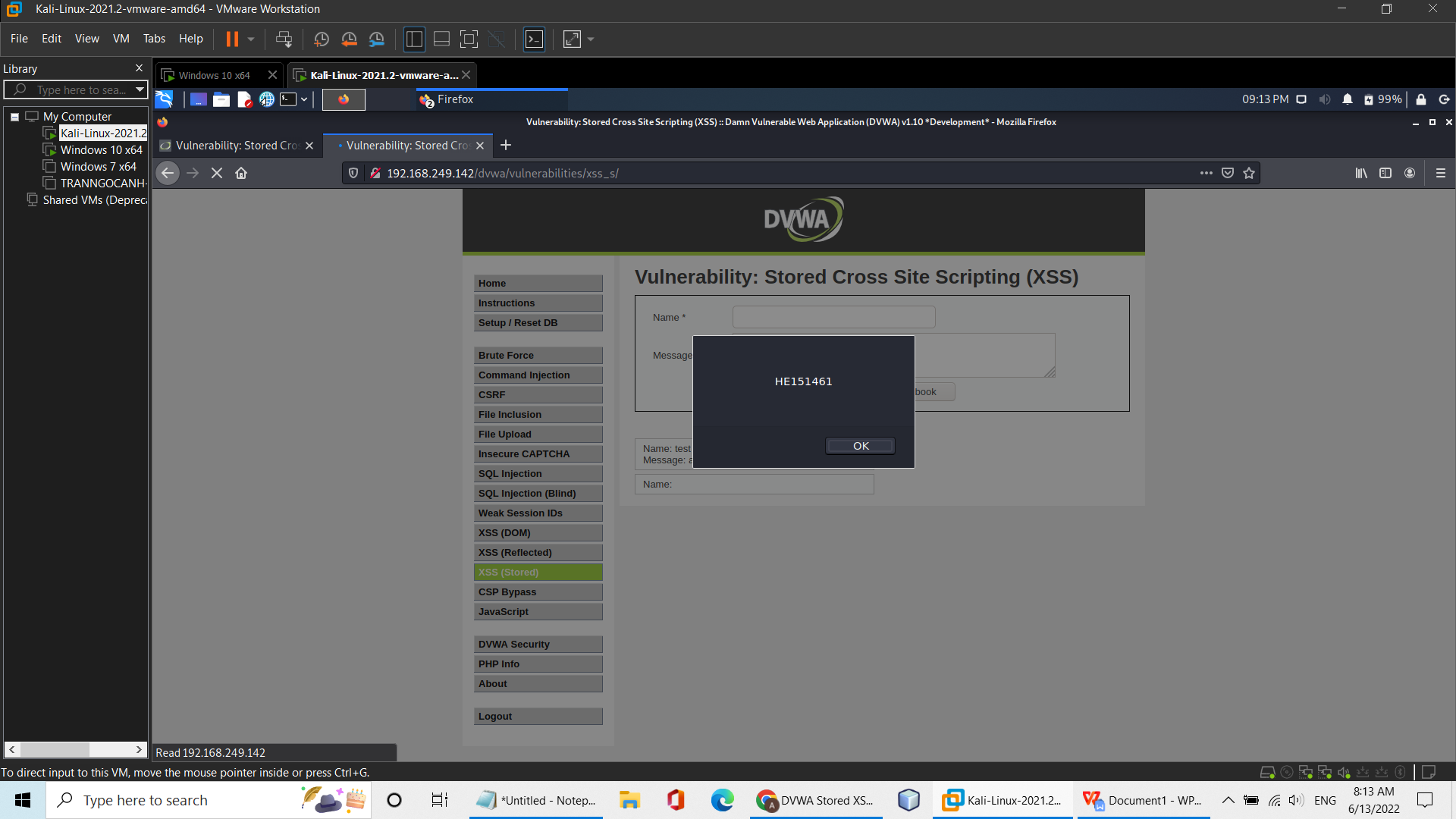
- Nhưng validate như vậy là chưa đủ và ta inject theo cách khác đó là

<Script>alert(“HE151461”)</Script> viết hoa chữ cái đầu của thẻ <script> để bypass hàm thay thế ở trường name.

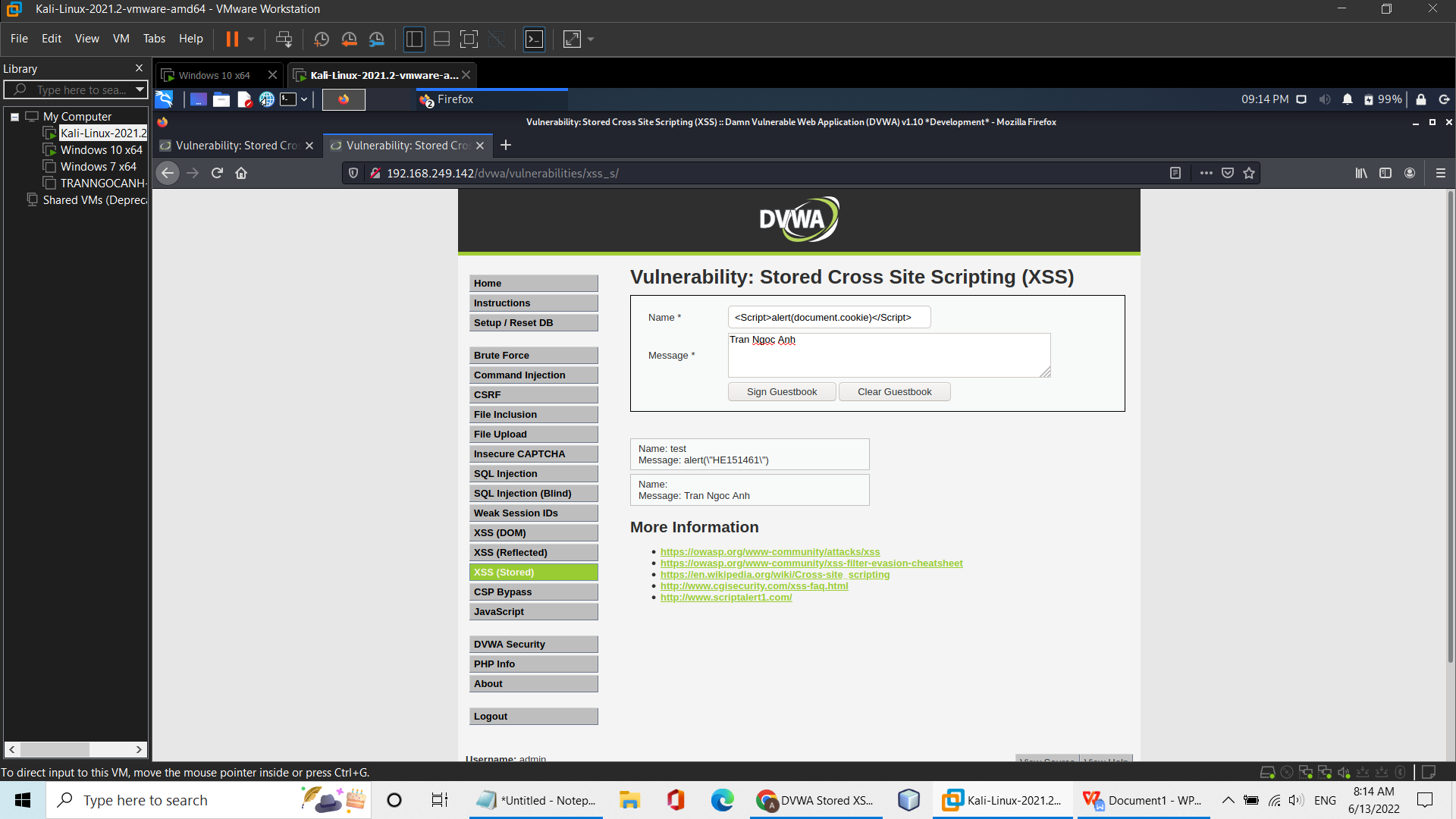
- Ở đây lại có chút vấn đề là ở phía client-side ta thấy bị giới hạn số lượng kí tự nhập vào của trường name , đơn giản chúng ta chỉ cần F12 sửa lại độ dài của trường name từ 10 thành 100 rồi thử lại như trên.

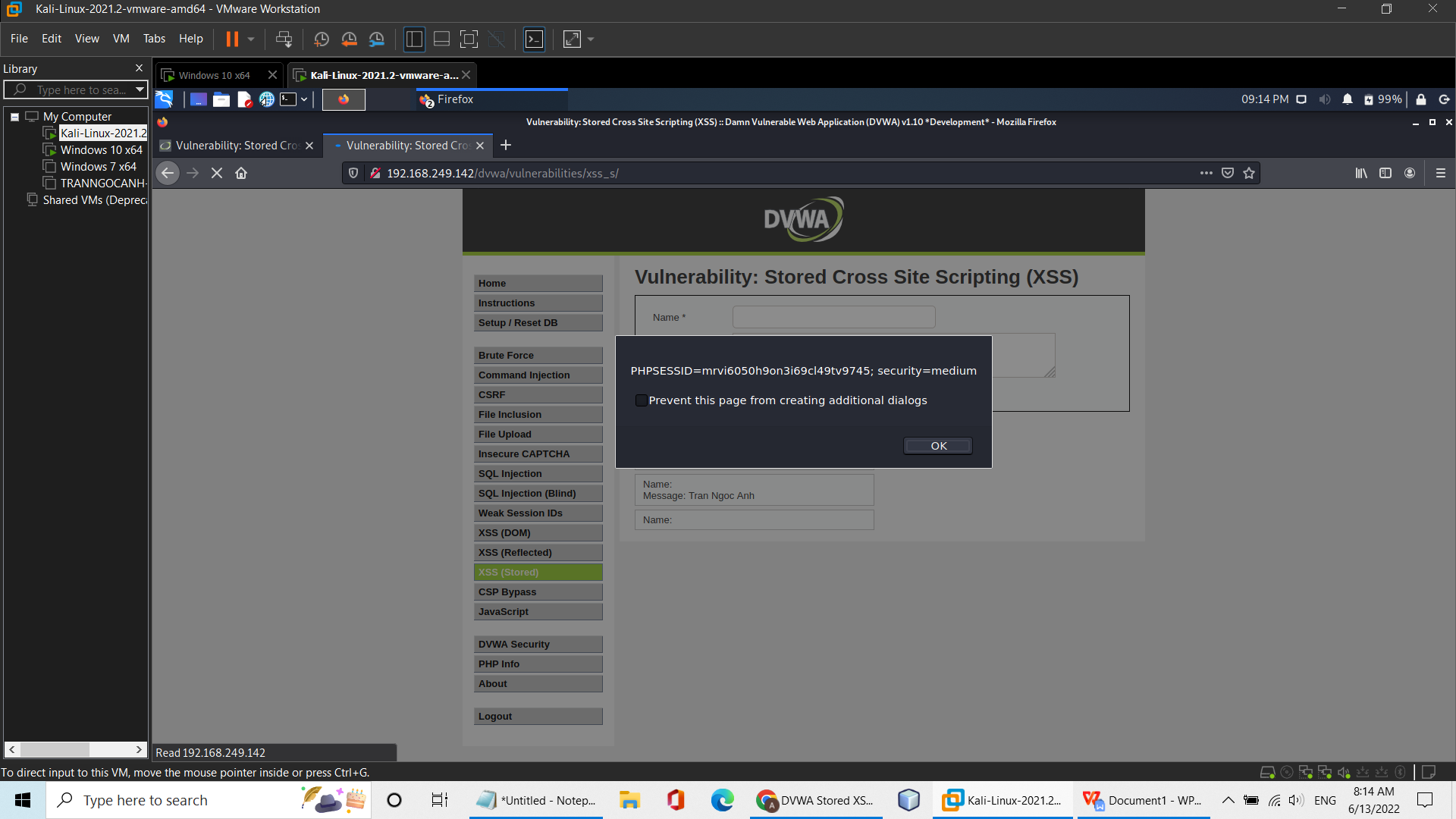






- Cuối cùng chúng ta inject đoạn code <Script>alert(document.cookie)</Script> để lấy được cookie và hoàn thành mức medium.





1. **High:**

- Ở mức high thì các hàm check đầu vào sử dụng cho message vẫn vậy chỉ có name là khác đi chút. Ở đây thì đã loại bỏ tất cả các kiểu của thẻ <script>. Vì vậy muốn bypass mức high chúng ta phải dùng các thẻ khác để khai thác ví dụ như img, svg, input, iframe,…(<svg/onload=alert(document.cookie)>)

