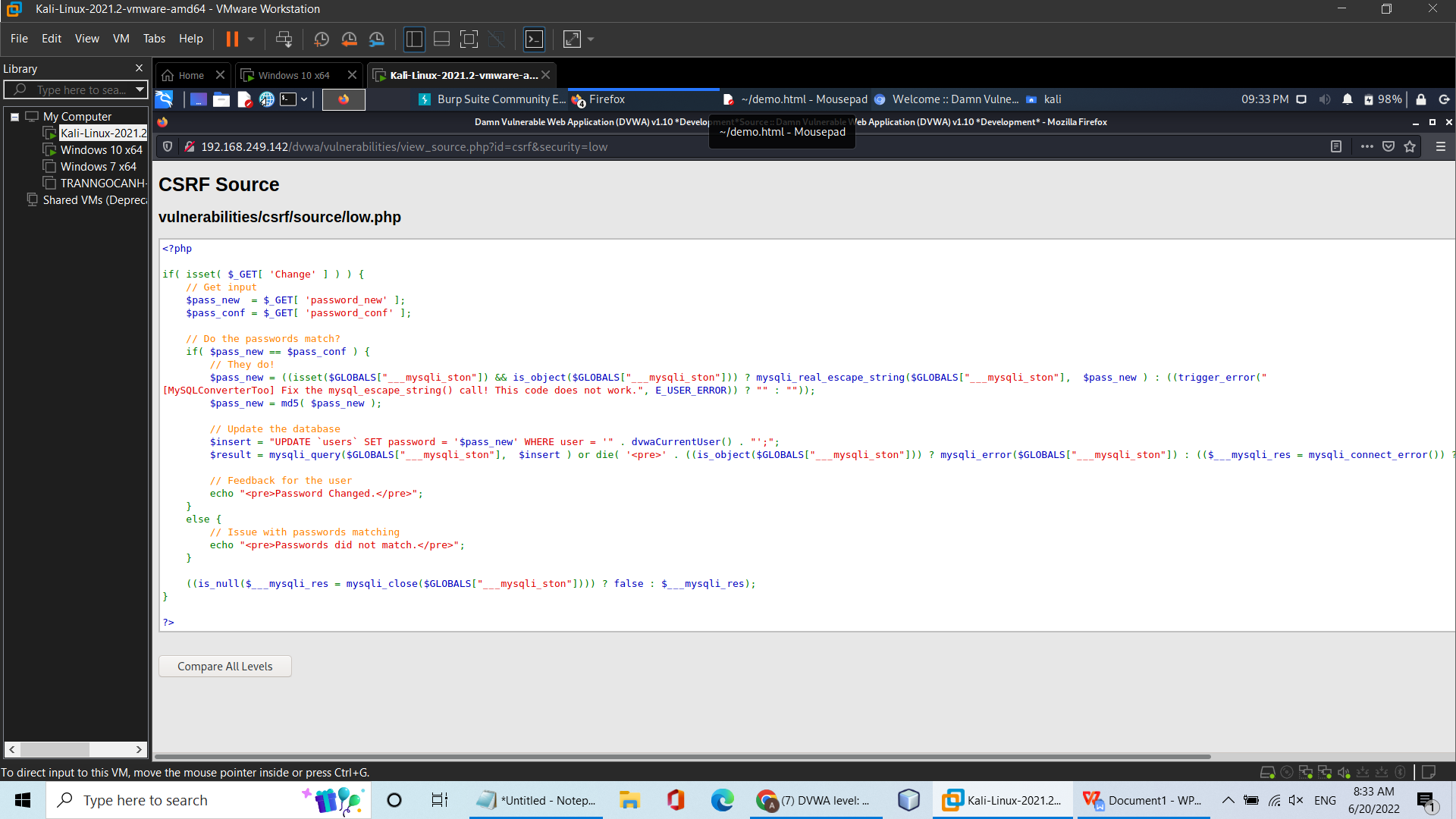
|  |  |
| --- | --- |
| Class | IAW301 |
| Name | Trần Ngọc Anh |
| IC No. | HE151461 |
| Date & Time | 20/6/2022 |

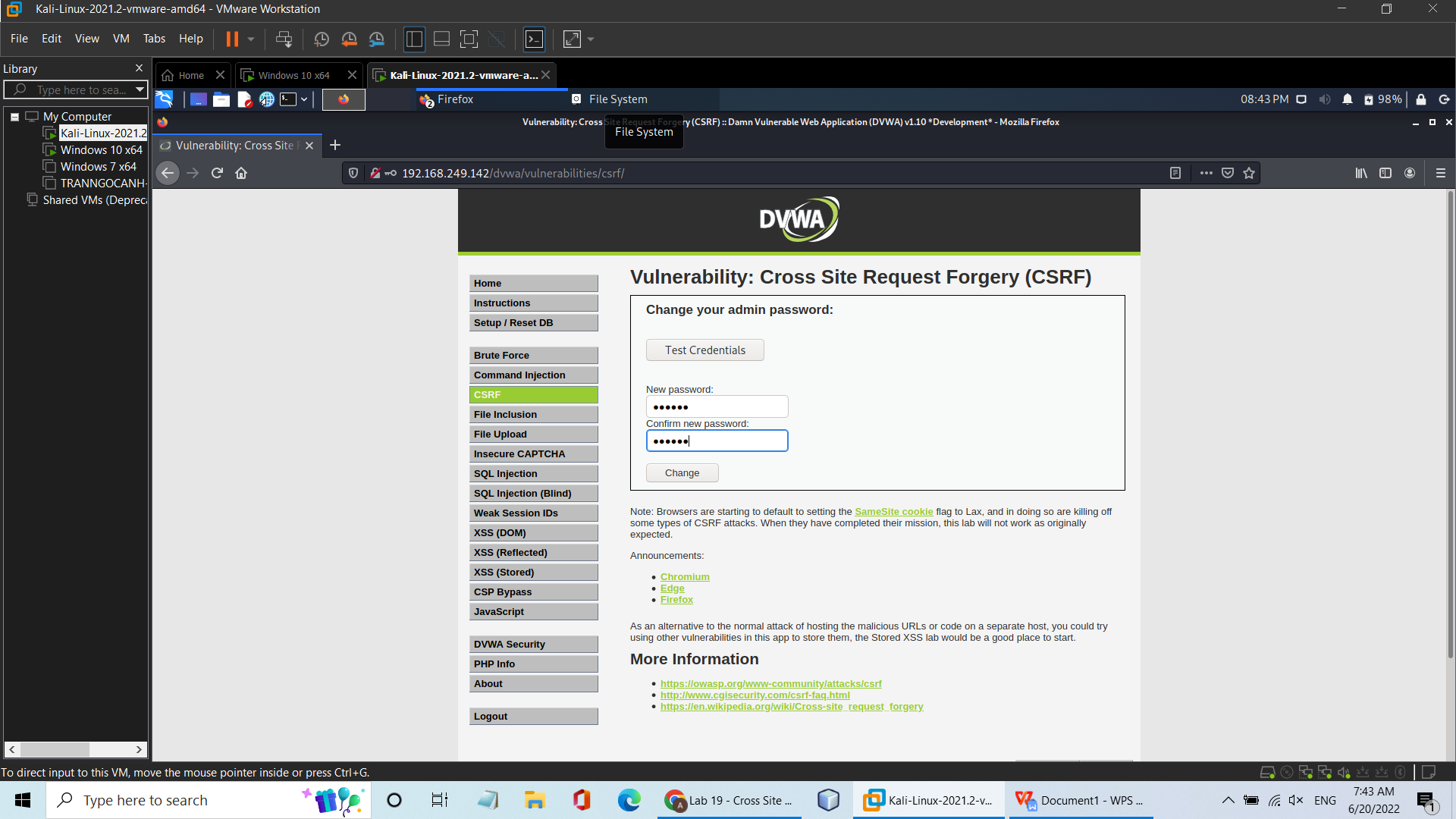
**LAB 19**

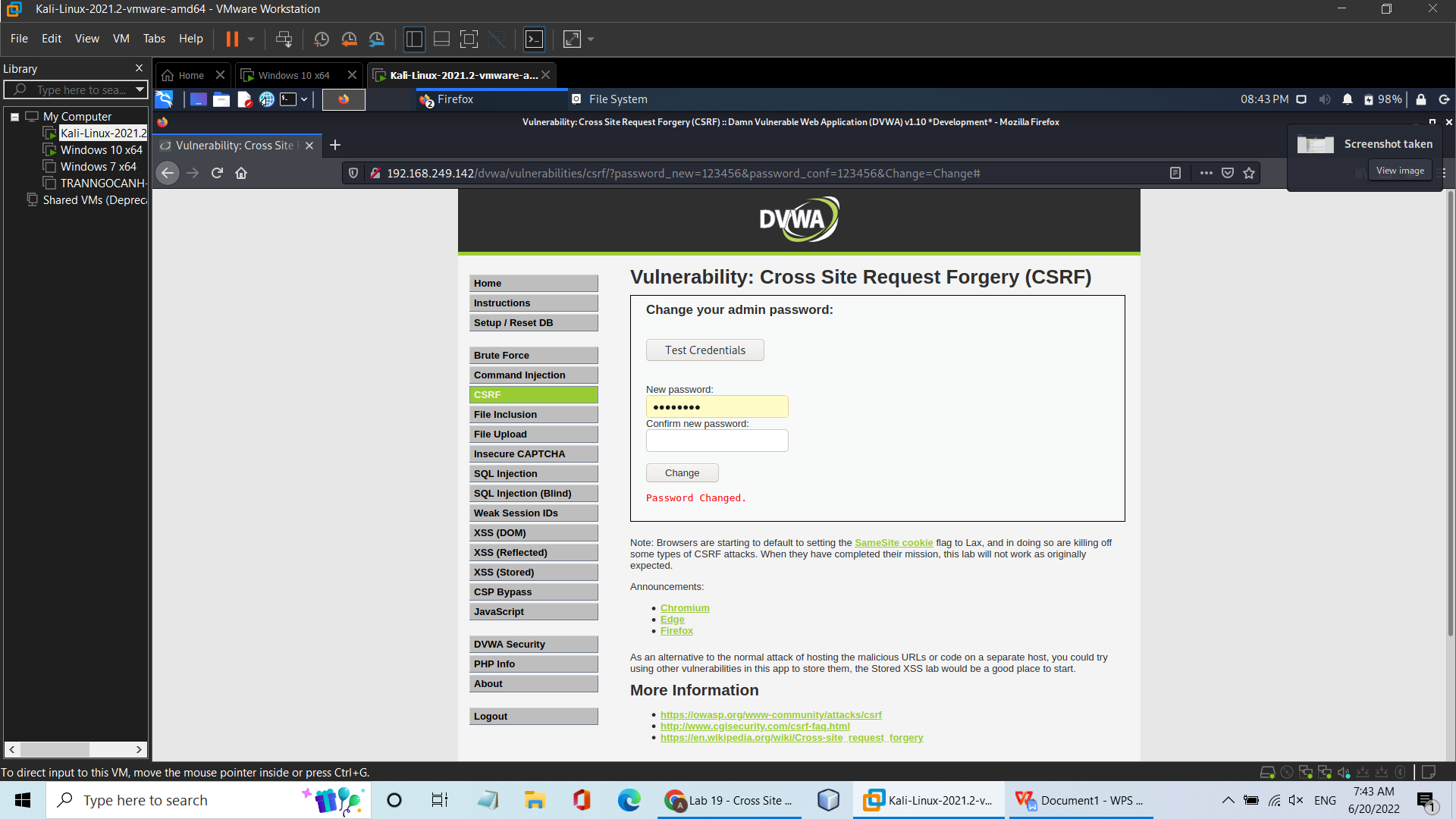
**Cross Site Request Forgery (CSRF)**

1. **Low**

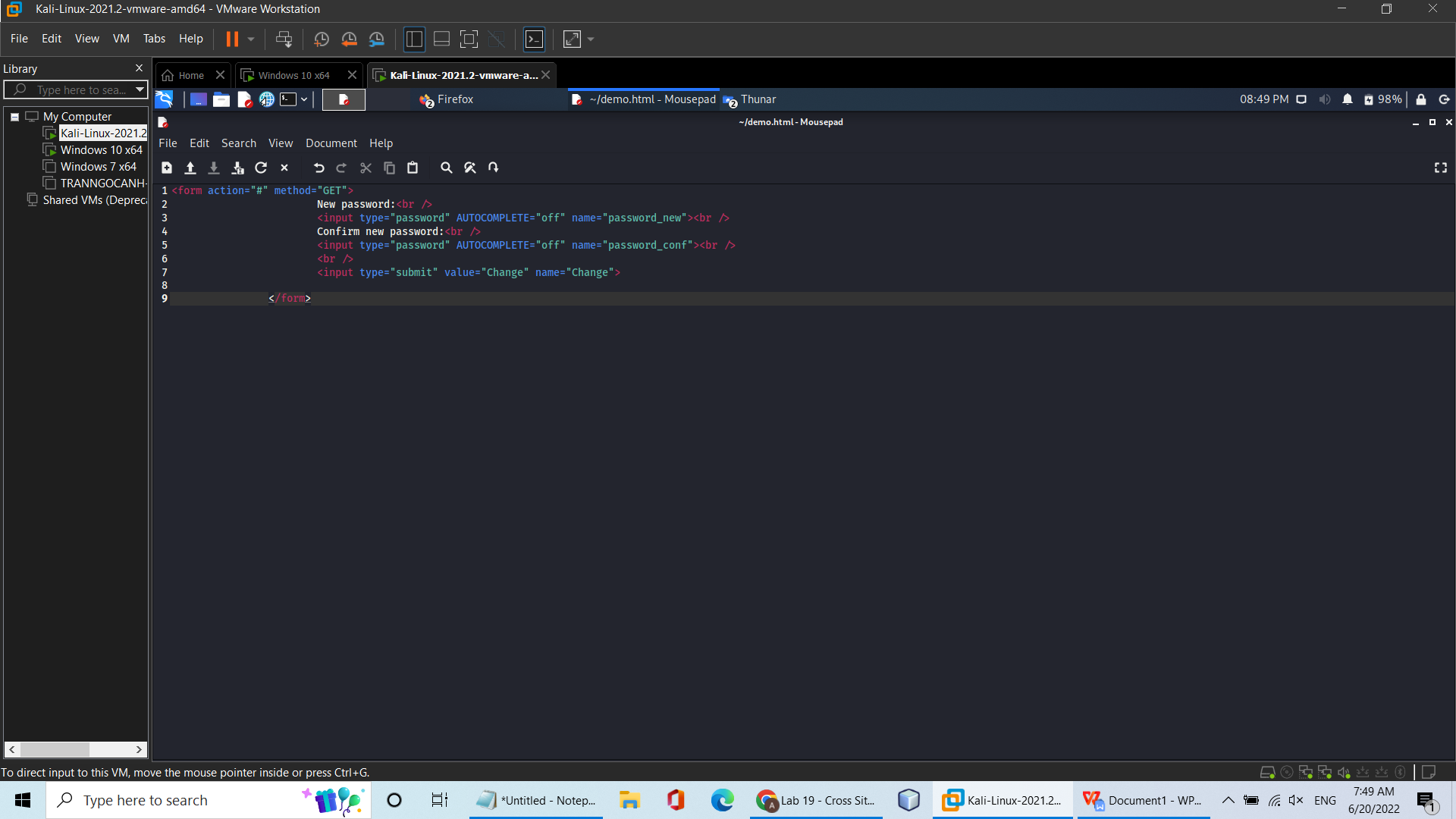
- Đầu tiên ở trang có lỗi CSRF ta thấy có chức năng thay đổi mật khẩu. Tuy nhiên phân tích source code ta thấy việc thay đổi mật khẩu của người dùng hiện tại nhưng lại không có xác thực.





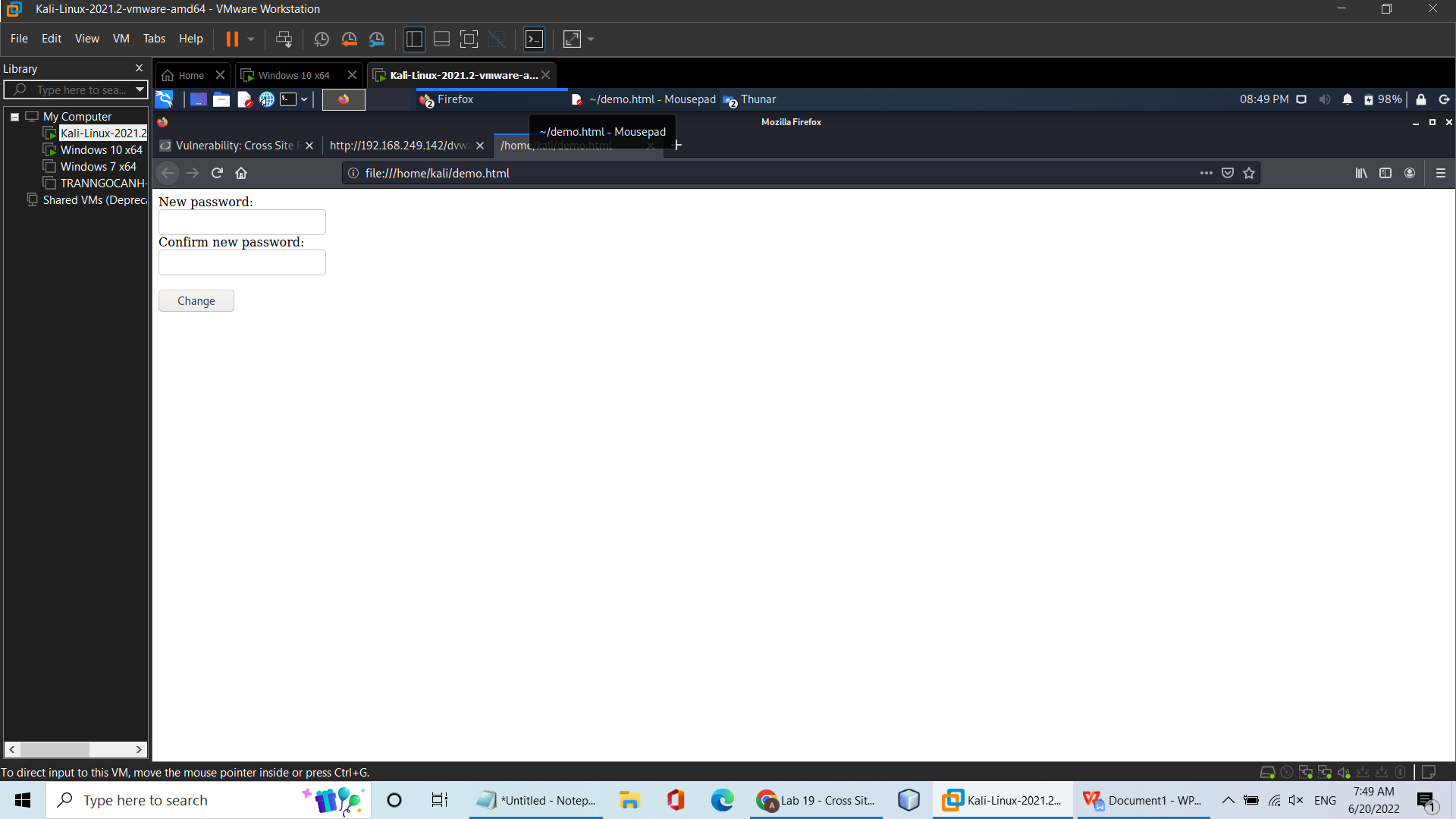


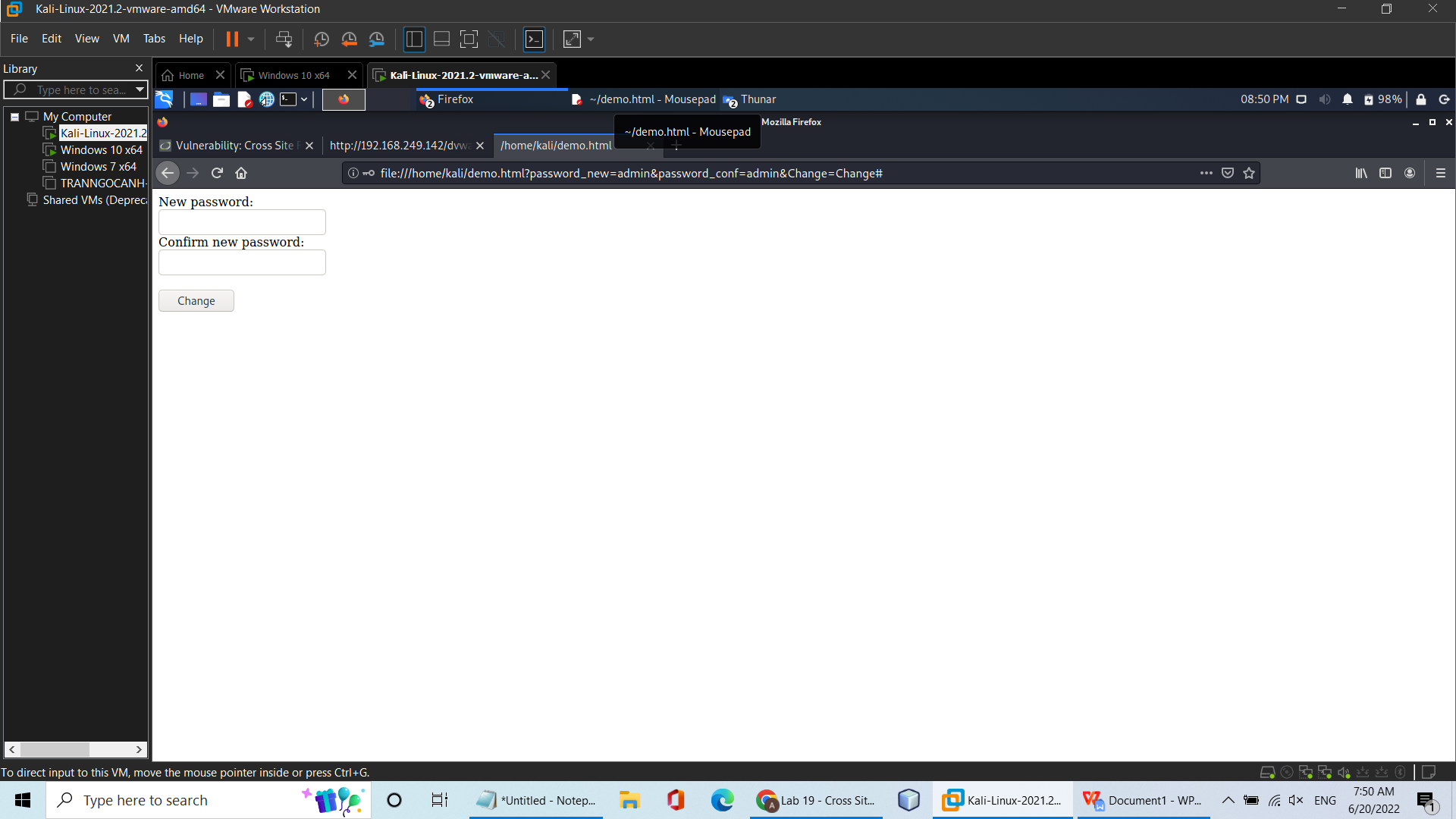
- Ta tạo một file demo.html có một form thay đổi mật khẩu có chứa phương thức GET lấy trong souce code của web để có thể tấn công CSRF.

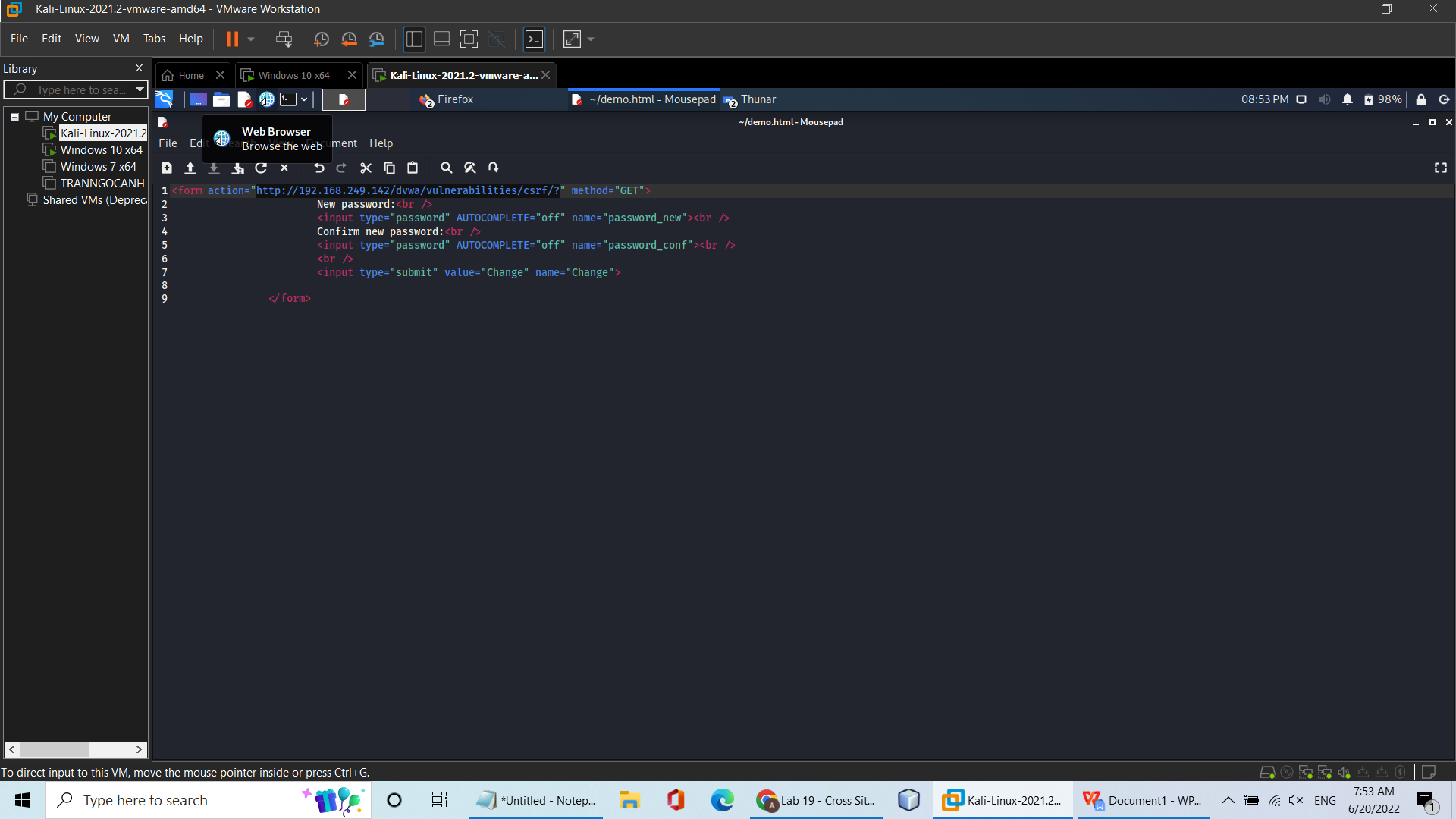


- Sau khi mở file html đó bằng firefox , ta thử đổi mật khẩu thành admin sau khi bấm Change sẽ thấy một đường dẫn URL với các param có sự thay đổi. Nhờ vào sự thay đổi của URL này ta sẽ đổi được đích đến của form đổi mật khẩu trong file demo.html

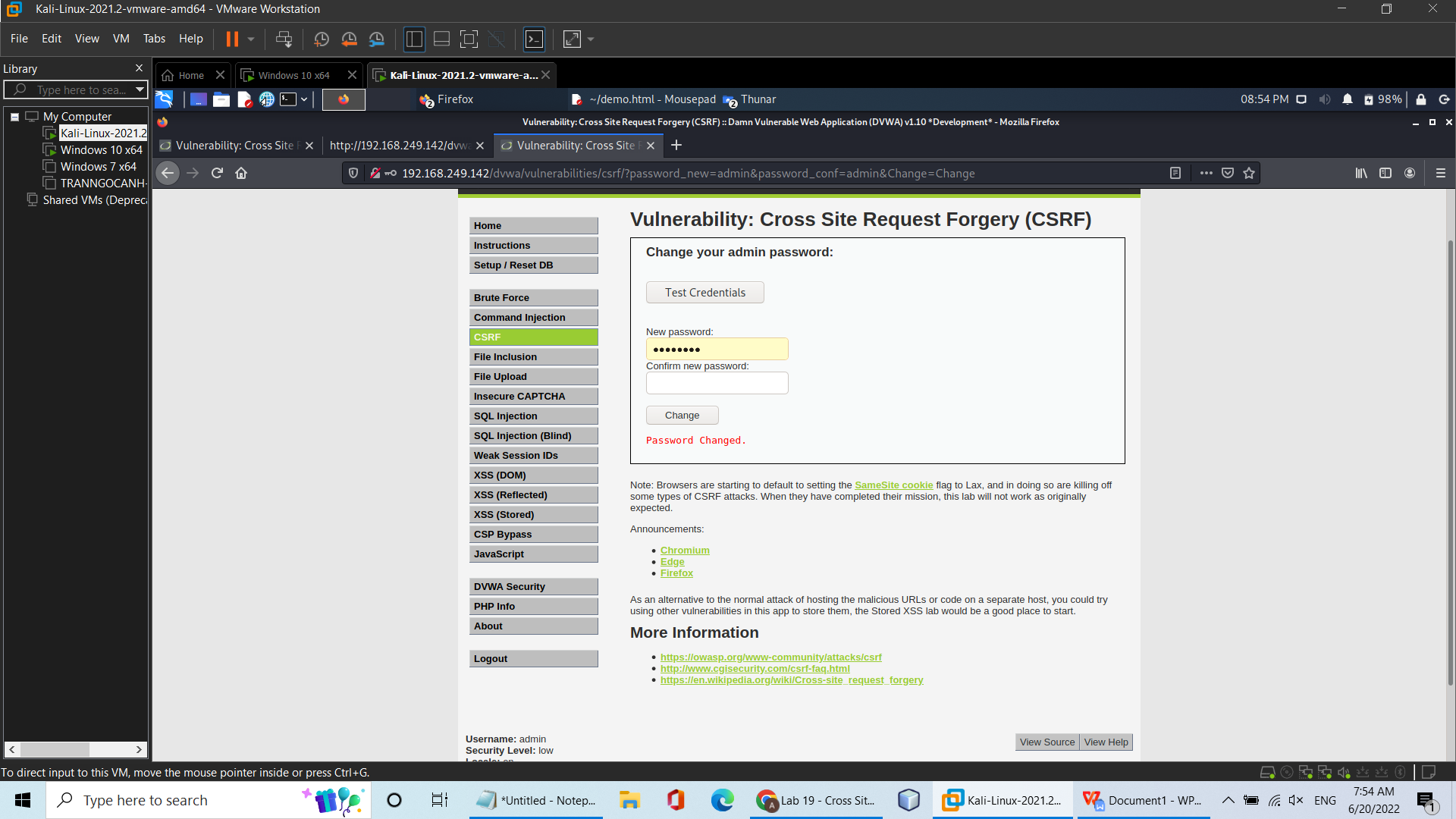
(http:192.168.249.142/dvwa/vulnerabilities/csrf/?)





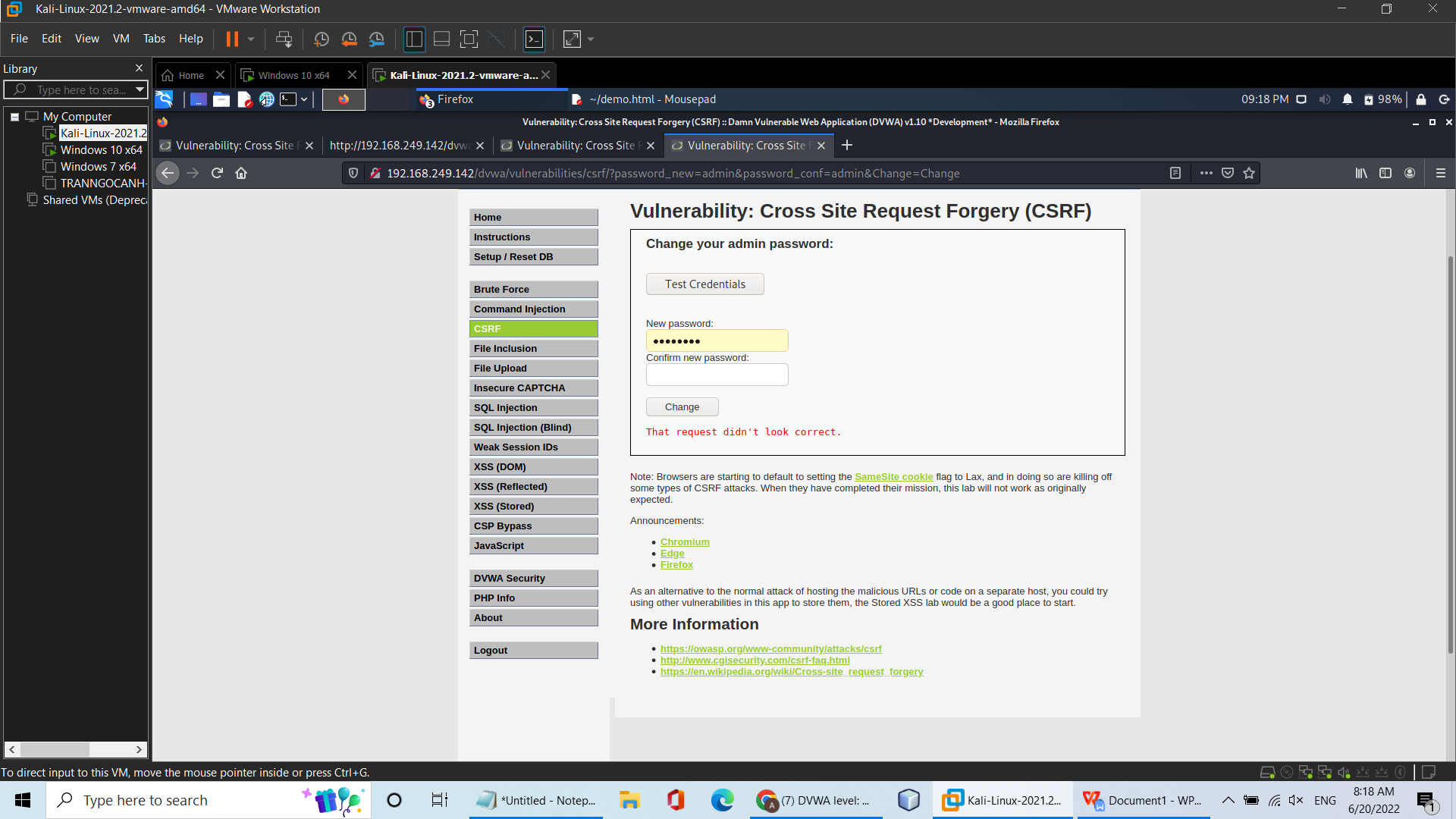


- Sau đó làm như bên trên đổi password thành admin click Change sẽ chuyển hướng đến trang dvwa và sẽ báo đổi mật khẩu thành công.



1. **Medium**

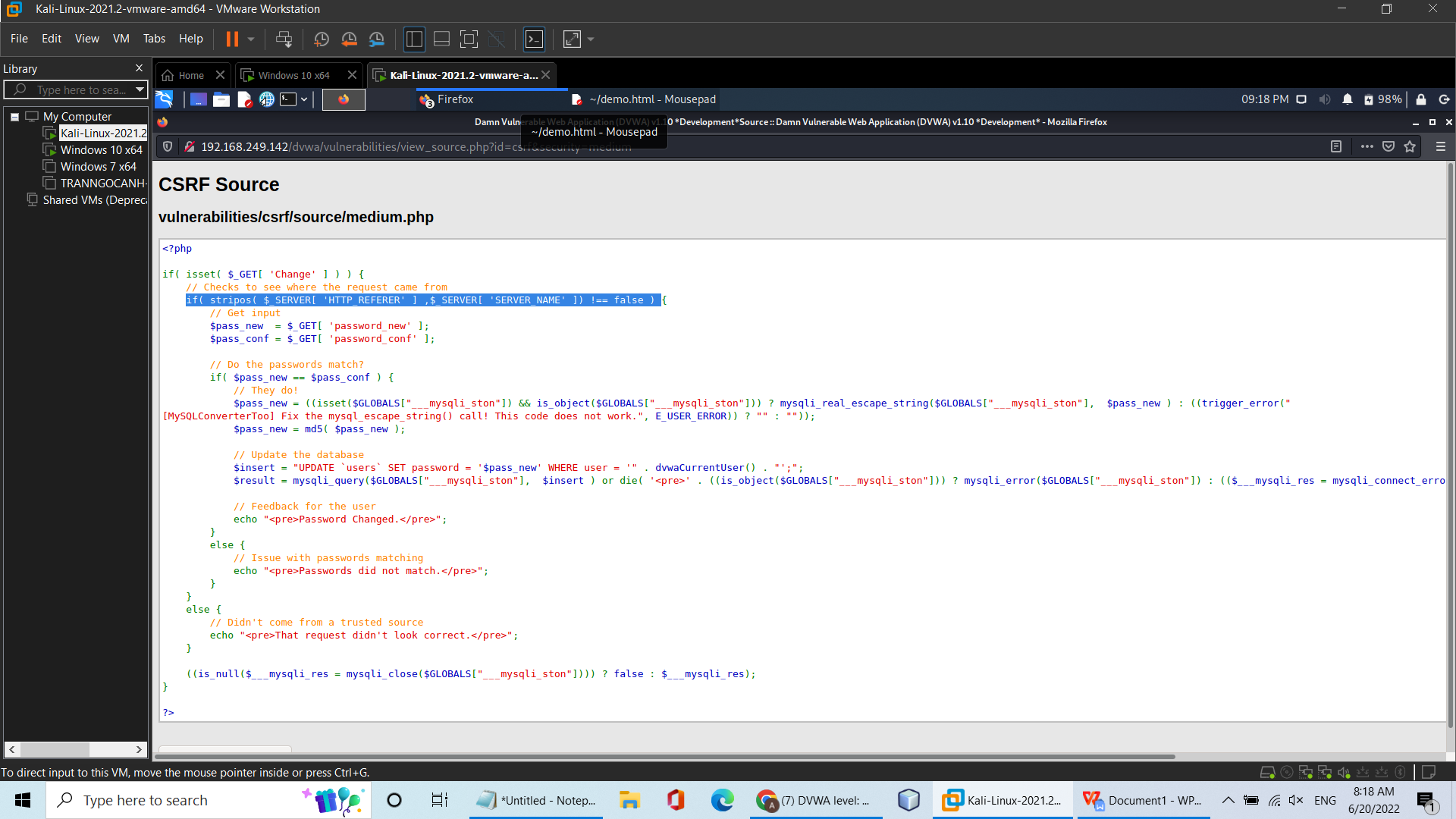
- Đến mức medium thử như mức low thì thấy request không hợp lệ.



- Chúng ta đành phải phân tích source code một chút để xác định nguyên nhân ở đâu. Thì ở đây trước khi mật khẩu được thay đổi đã có xuất hiện một điều kiện check .

+ The Http referer là tên của trường tiêu đề HTTP tùy chọn xác định địa chỉ của trang web (tức là URI hoặc IRI), từ đó tài nguyên được yêu cầu. Bằng cách kiểm tra liên kết giới thiệu, máy chủ cung cấp trang web mới có thể xem yêu cầu bắt nguồn từ đâu.

+ Hàm stripos() ở đây là để xác định xem SERVER\_NAMES có xuất hiện trong HTTP\_REFERER hay không.



- Vì vậy ở đây ta dùng Burp Suite để bắt request từ demo.html đến dvwa khi đổi mật khẩu . Sau đó thêm referer là sẽ by pass được việc check ở bên trên và hoàn thành mức medium.

