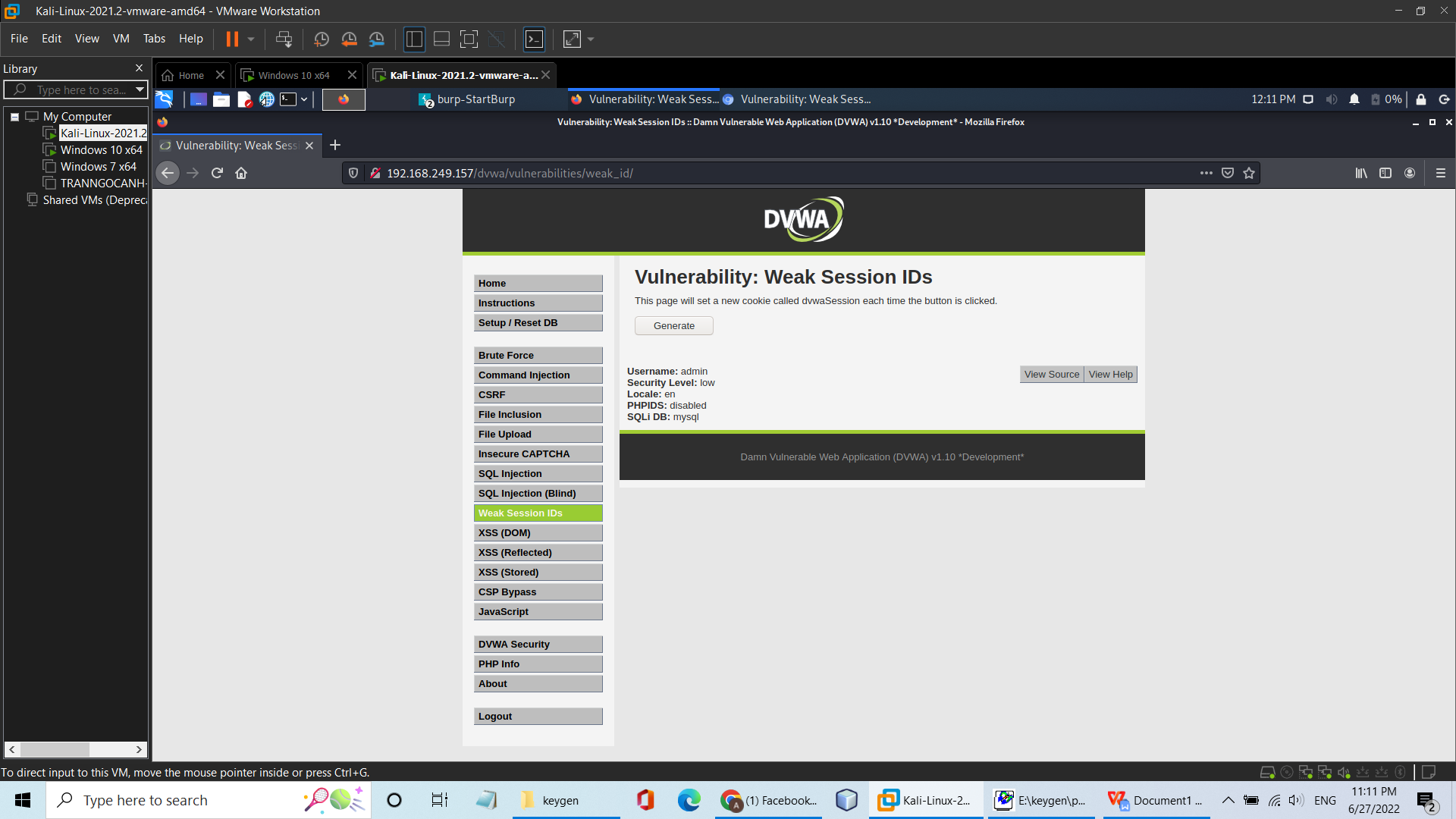
|  |  |
| --- | --- |
| Class | IAW301 |
| Name | Trần Ngọc Anh |
| IC No. | HE151461 |
| Date & Time | 27/6/2022 |

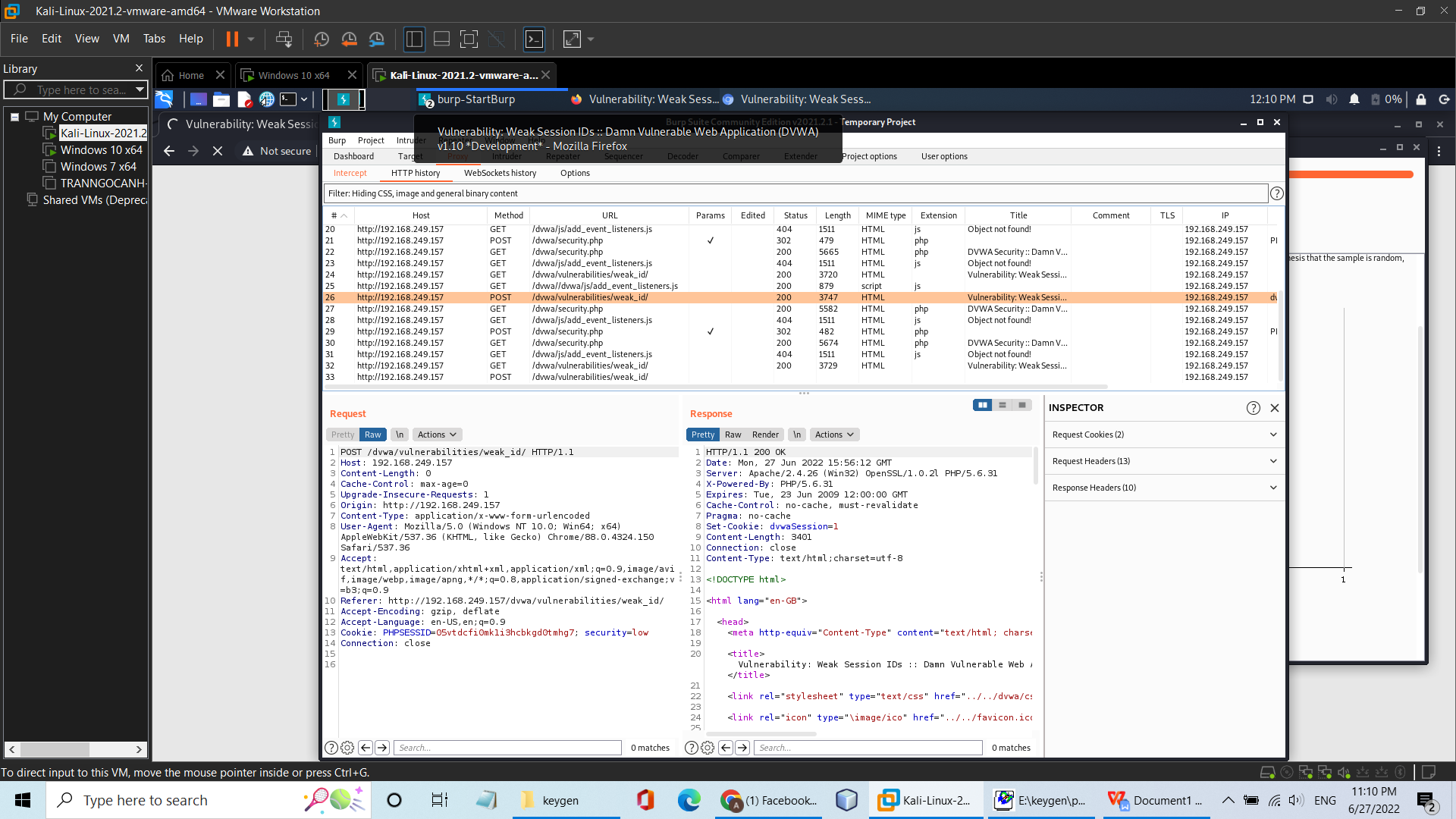
**LAB 22**

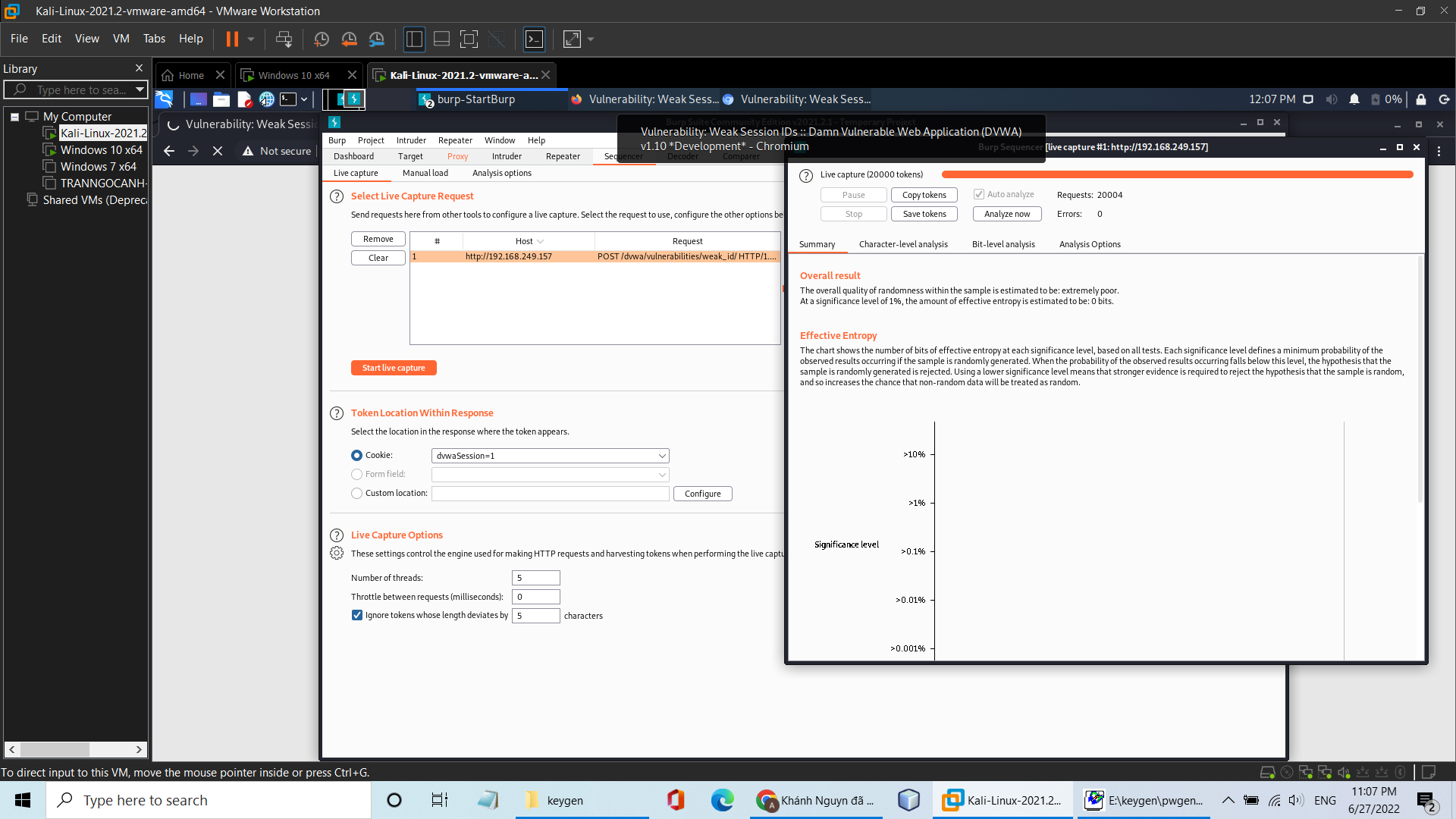
**Weak Session Cookie analysis with Burp Suite**

**1, Thực hiện theo bài viết bên trên 2 mức độ của DVWA (Medium, Impossible). Chụp ảnh với 2 bức cho phần Analyse của Burp.**

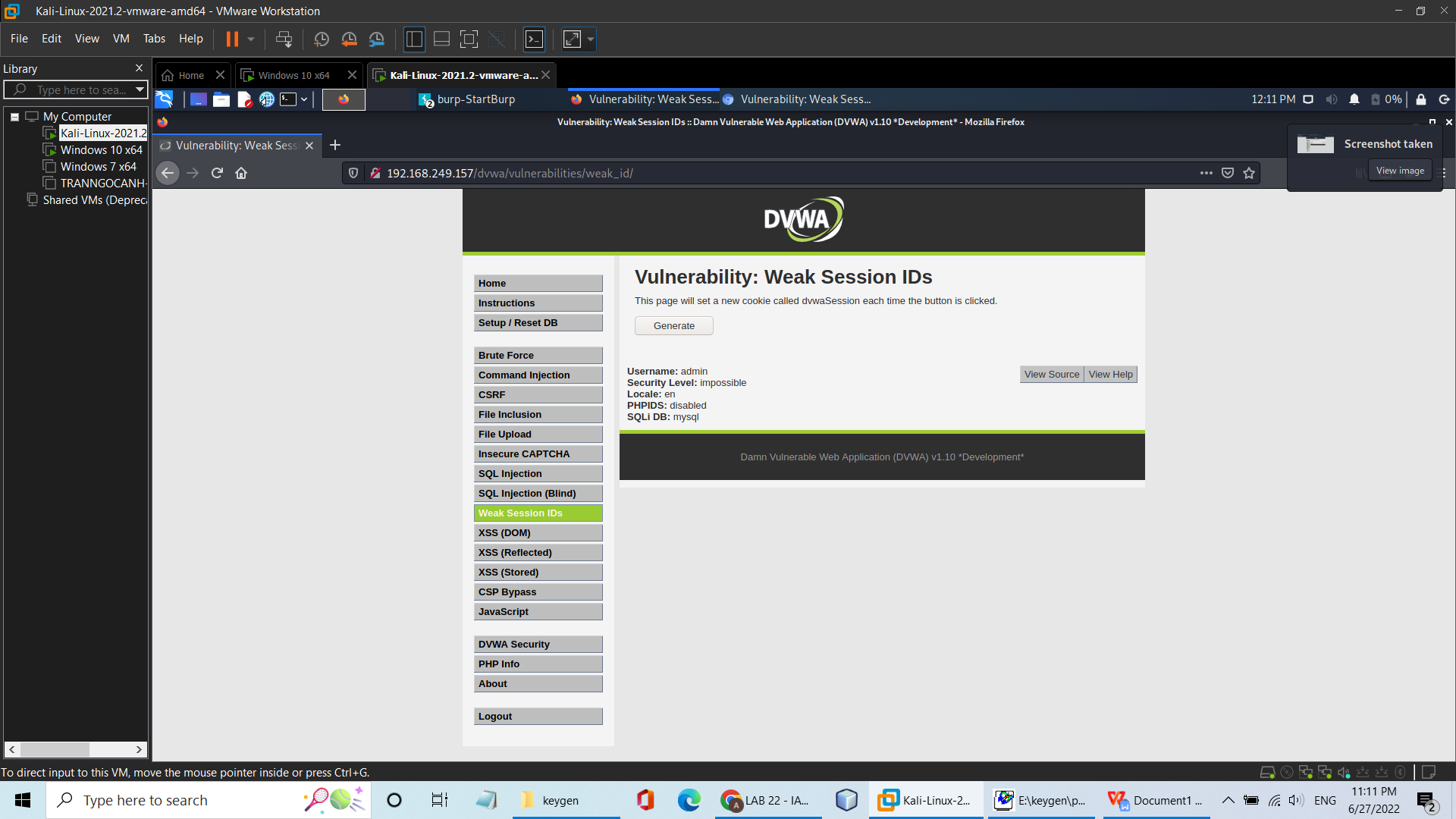
- Medium

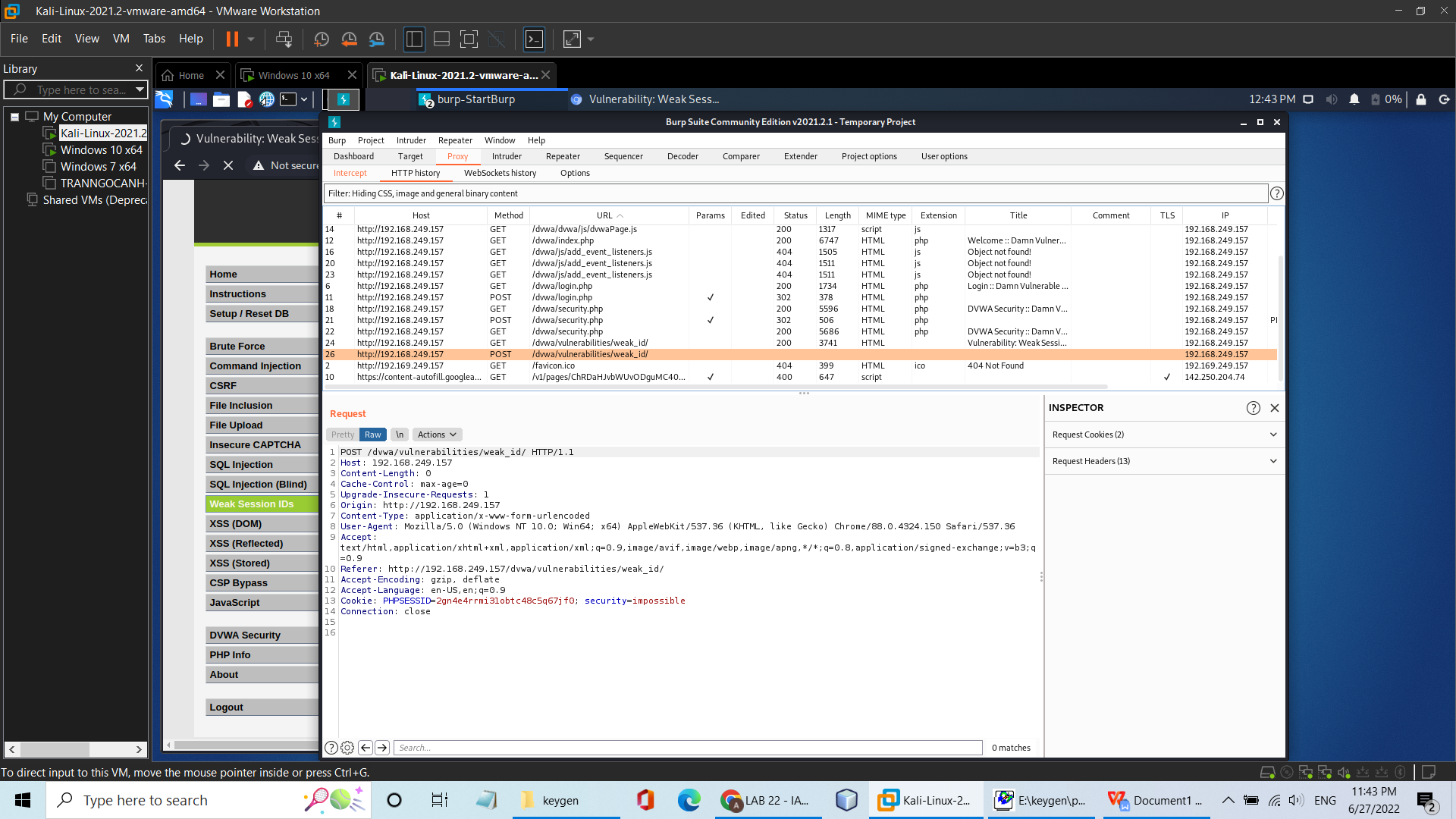


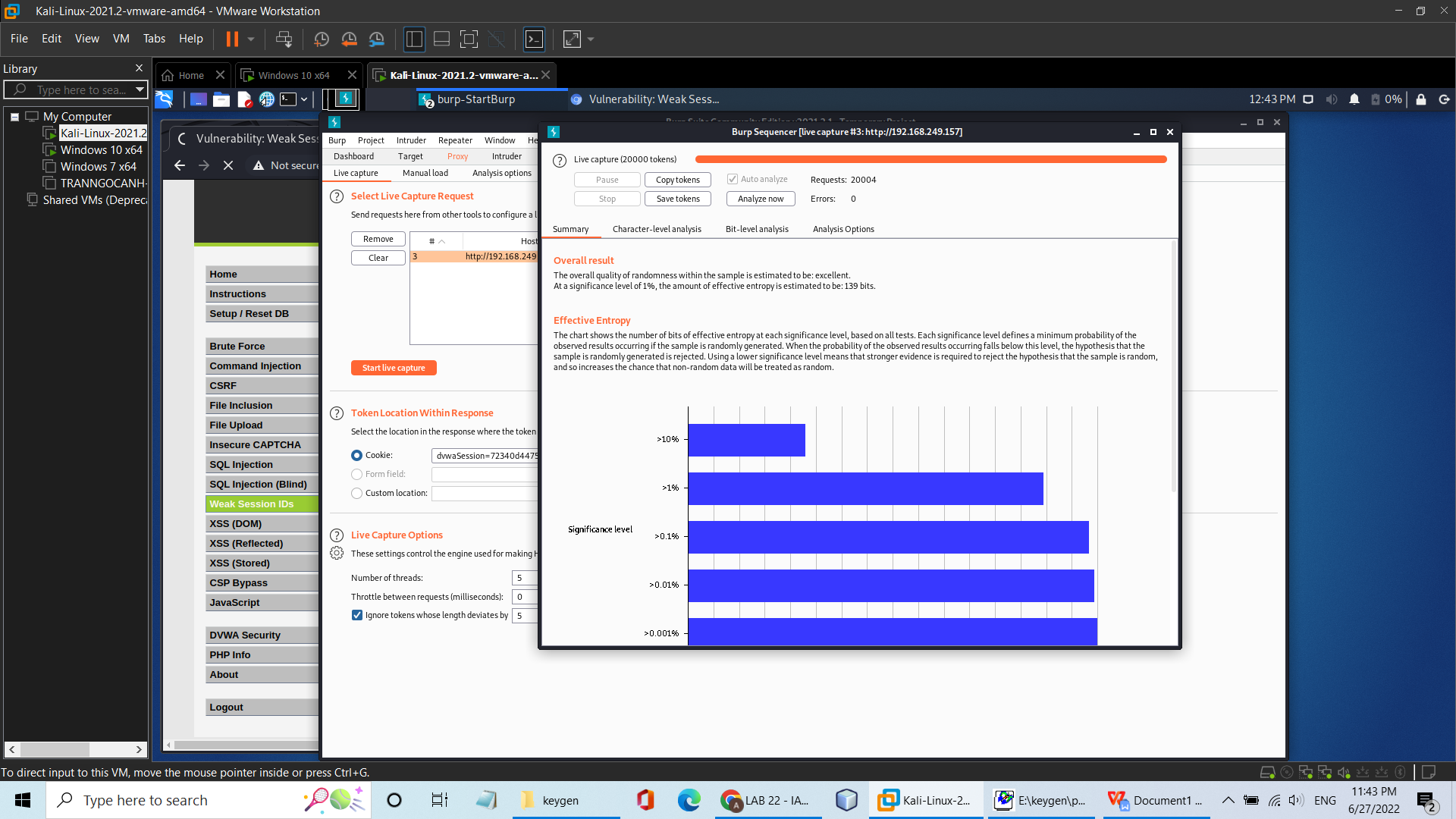




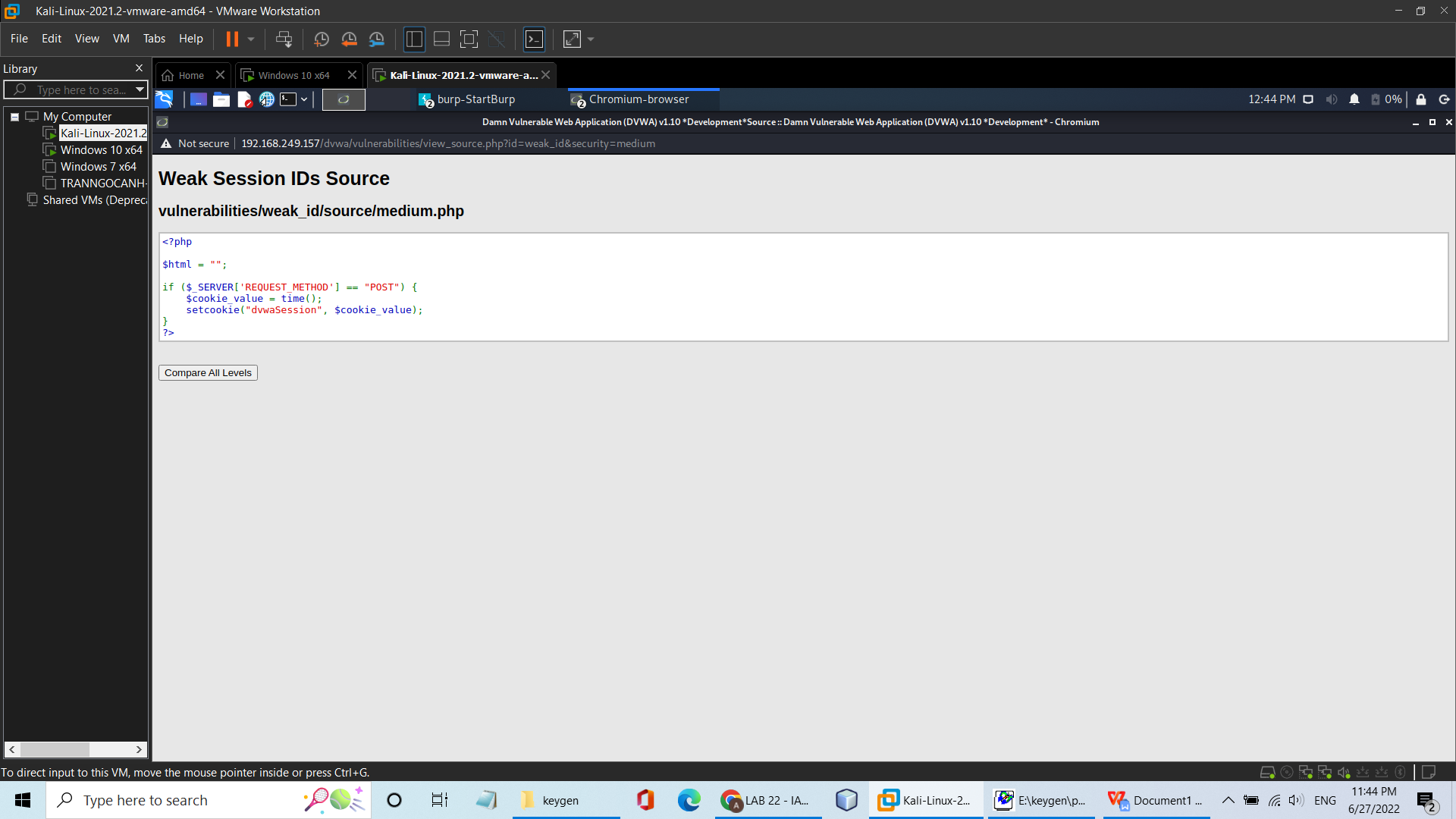
- Impossible



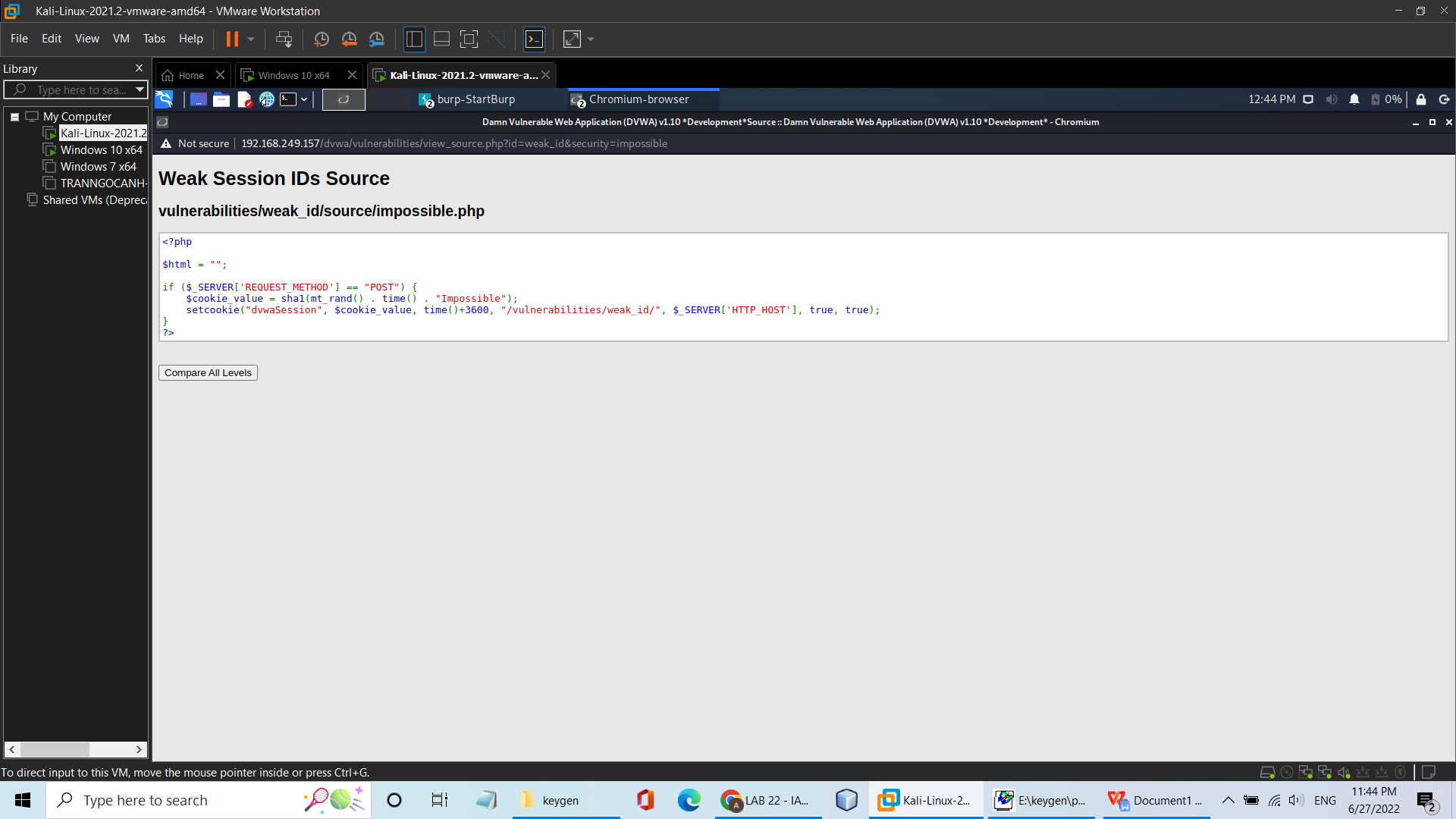




**2, Comment về phương pháp generate dvwaSession của 3 mức độ (Medium, High, Impossible). Và phương pháp đó có đảm bảo tính random hay không.**



- Ở mức medium thì dvwa có generate dvwaSession bằng cách tăng dần các session theo thời gian, nhưng ở đây vẫn là việc tăng tuần sự. Phương pháp này tuy an toàn hơn mức low nhưng chưa đủ để đảm bảo hoàn toàn an toàn.



- Ở mức Impossible thì dvwa đã generate dvwaSession random mã session theo time. Phương pháp này đảm bảo được tính random nên đủ an toàn.

**3, Tại sao Session lại cần phải random.**

- Khi chúng ta đăng nhập vào 1 trang web và xác thực phiên của mình thành công thì đều sẽ có 1 giá trị cookie được random cho phiên đó. Nếu giá trị cookie này không được random thì kẻ tấn công có thể dễ dàng chiếm được quyền phiên tiếp theo của mình và thao tác những hoạt động trái phép trên danh nghĩa của mình. Để giảm thiểu việc kẻ tấn công chiếm được phiên làm việc tiếp theo của mình thì phải random cookie value để gây khó khăn cho kẻ tấn công trong việc tìm ra nó.