**LAB 5**

**Web Attack and Defense (tt)**

|  |
| --- |
| **Họ tên và MSSV:** Phạm Đức Phát  **Lớp: 10\_ĐH\_CNPM2**  **Link youtube:** |

**Câu 1: Khai thác lỗi Cross-site scripting (XSS) trên DVWA**

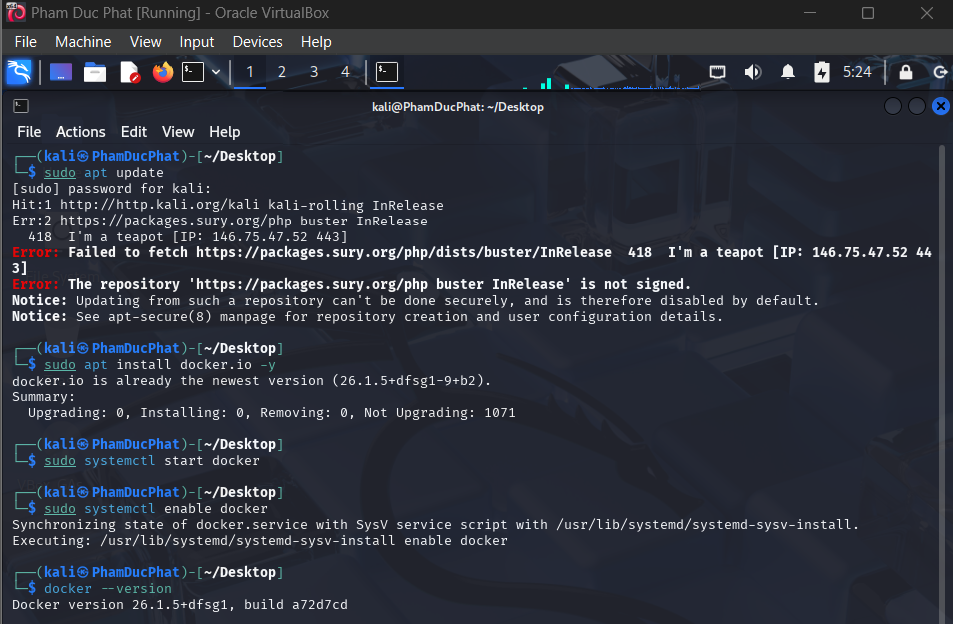
1.1. Tham khảo các tài liệu đính kèm để khai thác lỗi **Dom-based XSS** trên DVWA (security ở mức độ low) để lấy cookie của người dùng đang đăng nhập.

<https://github.com/mrudnitsky/dvwa-guide-2019/blob/master/low/Challenge%2010:%20XSS%20(DOM).md>

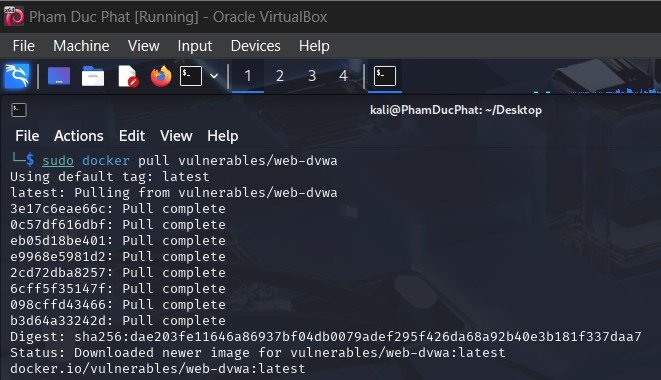
<https://bughacking.com/dvwa-ultimate-guide-first-steps-and-walkthrough/#XSS_DOM>

<https://youtu.be/X87Ubv-qDm4?list=PLHUKi1UlEgOJLPSFZaFKMoexpM6qhOb4Q>

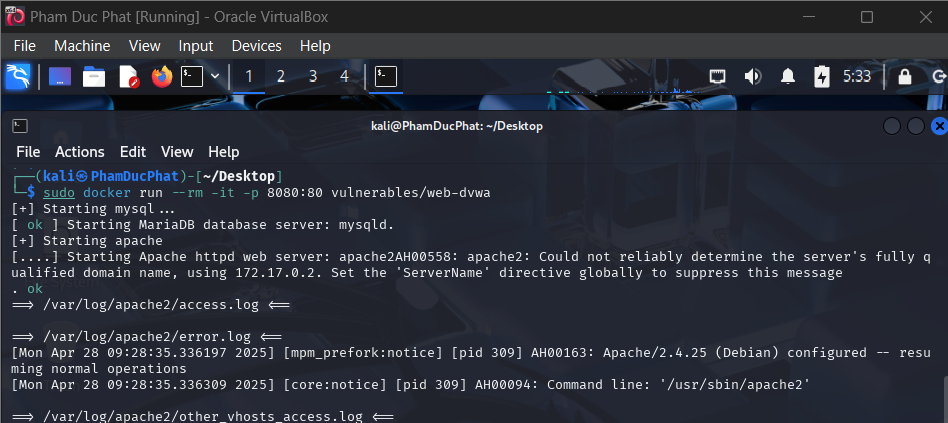
Kiểm tra docker



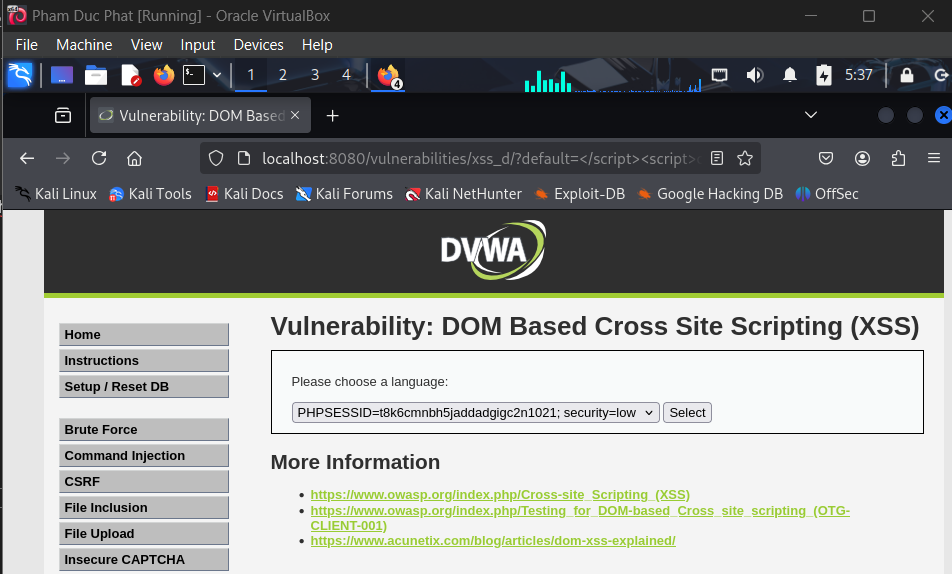
Tải dvwa bằng docker



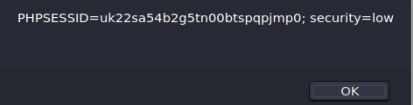
Khởi động container DVWA



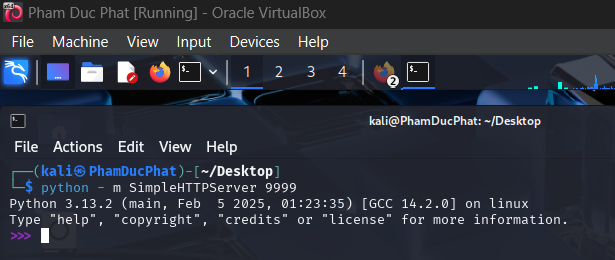
* Mở trang DVWA và chọn XSS, nhập thanh địa chỉ như trong hình bên dưới:



* Kết quả cookie hiện lên:



* Chạy server:



1.2. Tham khảo các tài liệu đính kèm để khai thác lỗi **Stored XSS** trên DVWA (security ở mức độ low) để lấy cookie của người dùng đang đăng nhập. Sau đó dùng công cụ Burp Suite (hoặc chức năng Inspect trên Firefox) để truy cập vào DVWA sử dụng cookie vừa lấy được.

<https://github.com/mrudnitsky/dvwa-guide-2019/blob/master/low/Challenge%2012:%20XSS%20(Stored).md>

<https://bughacking.com/dvwa-ultimate-guide-first-steps-and-walkthrough/#XSS_Stored>

<https://youtu.be/P1I9UGpGdrU?list=PLHUKi1UlEgOJLPSFZaFKMoexpM6qhOb4Q>

(Chụp hình minh họa quá trình thực hiện)

