**LAB 5**

**Web Attack and Defense (tt)**

Họ tên và MSSV: Phan Tân Phước – 1050080070

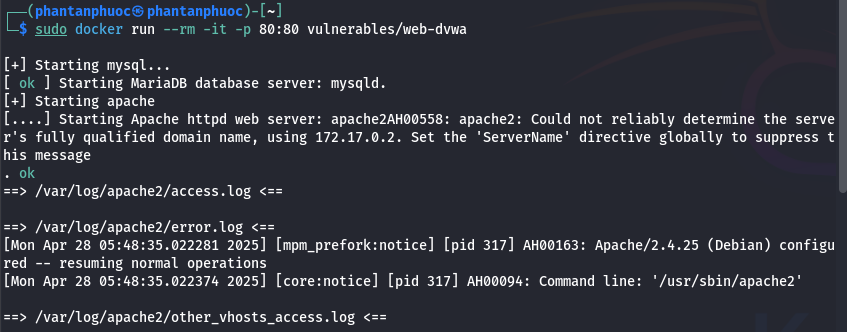
Lớp: 10 – DH – CNPM 1

Link youtube: <https://youtu.be/bs527m-Gb9E>

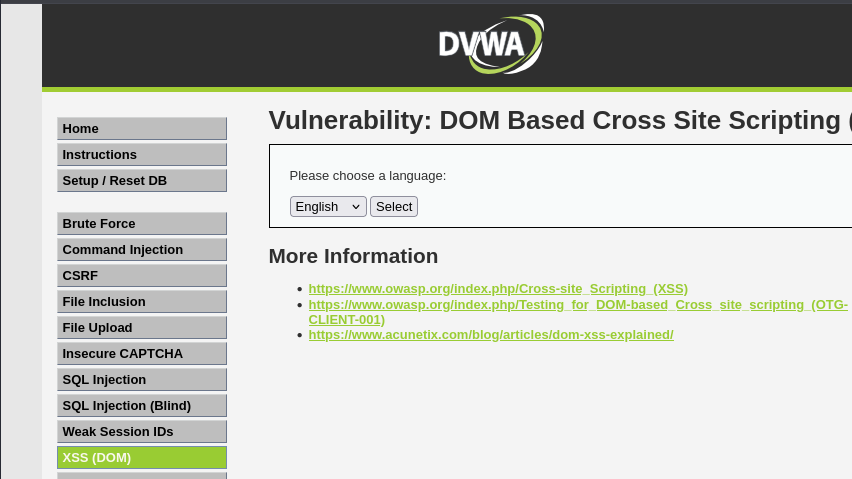
Câu 1: Khai thác lỗi Cross-site scripting (XSS) trên DVWA

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.

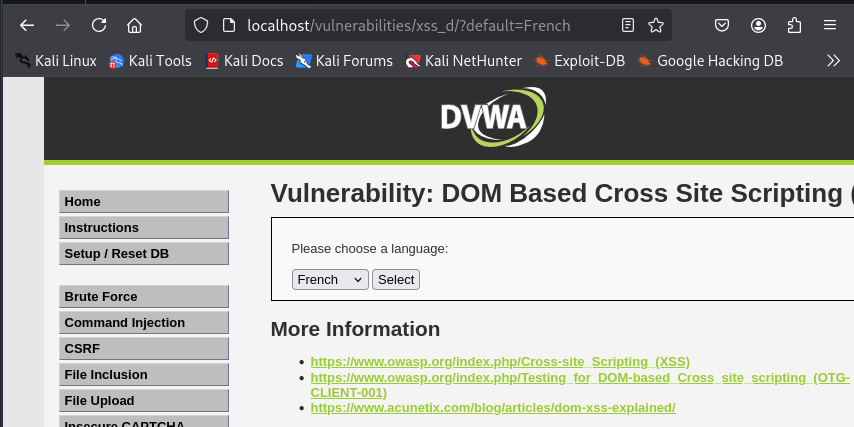
Bước 1: Khởi động dịch vụ DVWA với docker.



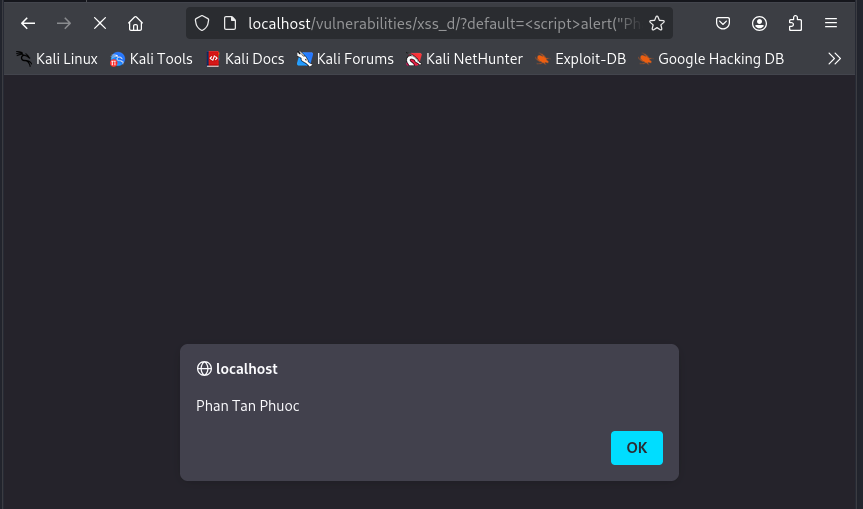
Bước 2: Mở trình duyệt với localhost và tiến thành setup/reset database. Sau đó đăng nhập lại và vào phần XSS DOM.



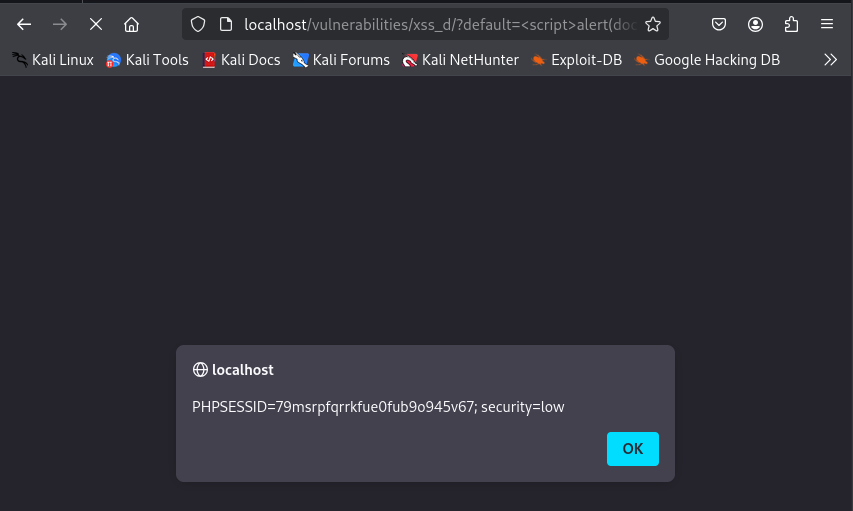
Bước 3: Thực hiện chọn 1 mẩu để kiểm tra phương thức get gọi trên url.



Bước 4: Đổi tên giá trị default thành mã script với alert để kiểm tra mã có thực thi.

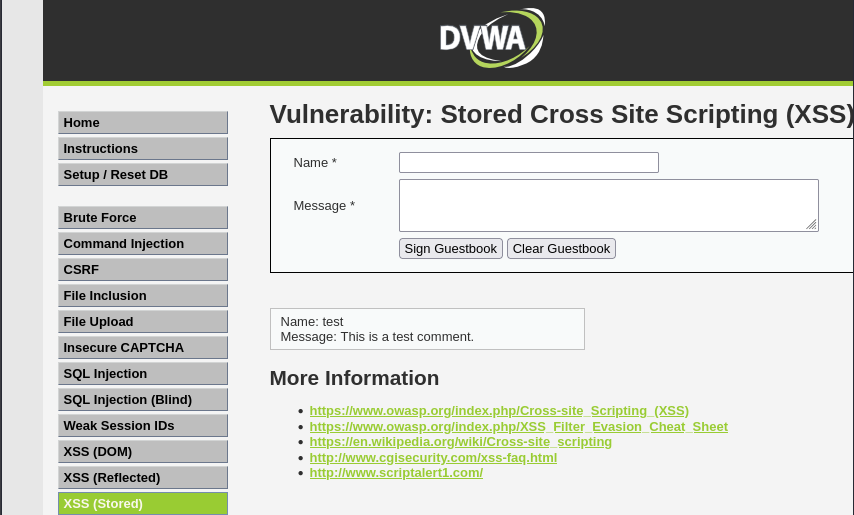


Bước 5: Với mã script có thể thực thi trên url. Tiếp tục viết mã script để thực hiện lấy cookie trang web.

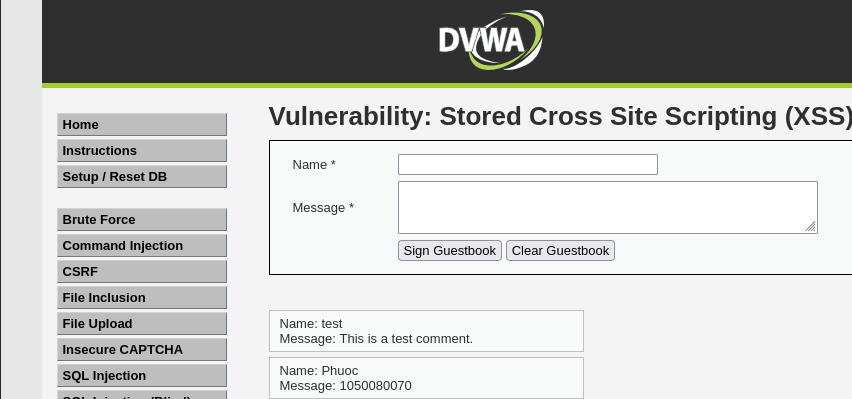


1.2. Tham khảo các tài liệu đính kèm để khai thác lỗi Stored XSS trên DVWA (security ở mức độ low) để lấy cookie của người dùng đang đăng nhập. Sau đó dùng công cụ Burp Suite (hoặc chức năng Inspect trên Firefox) để truy cập vào DVWA sử dụng cookie vừa lấy được.

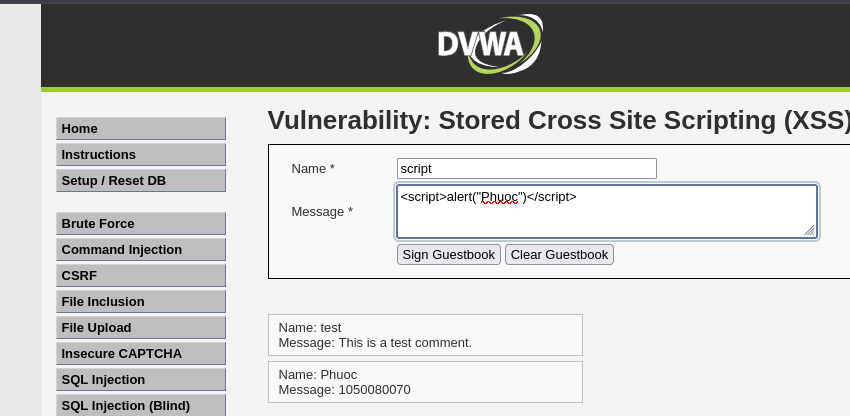
Bước 1: Truy cập XSS Stored trên DVWA.

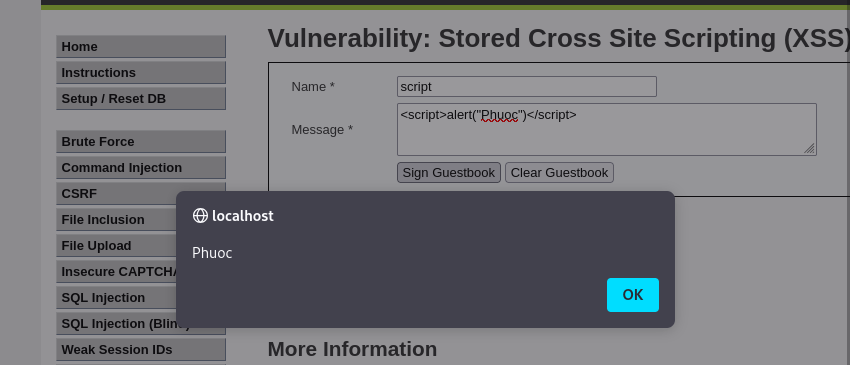


Bước 2: Thực hiện thêm dữ liệu cơ bản.

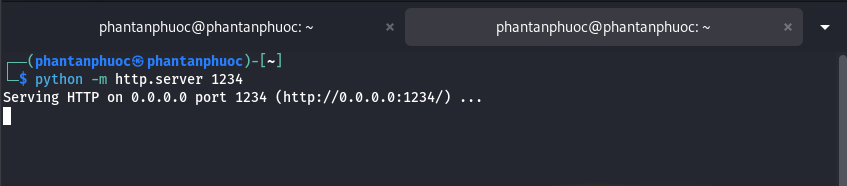


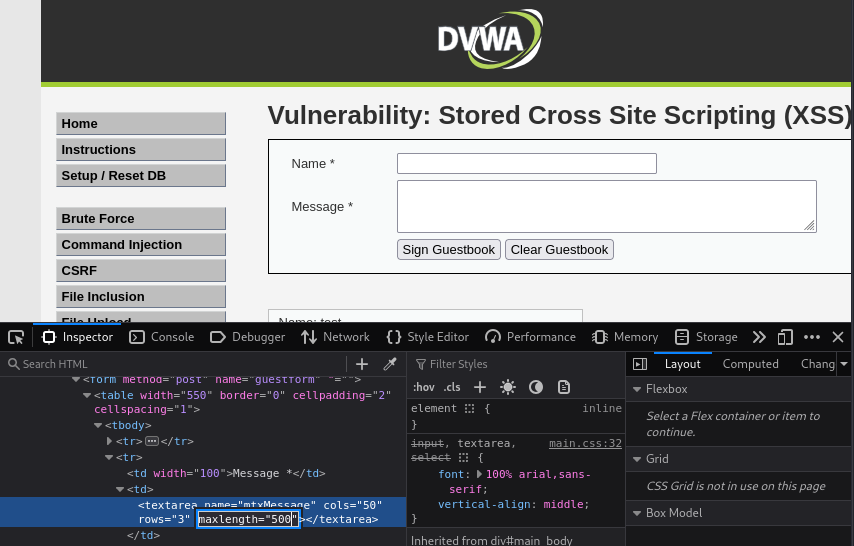
Bước 3: Thực hiện chèn script vào message để xem mã có được thực thi.



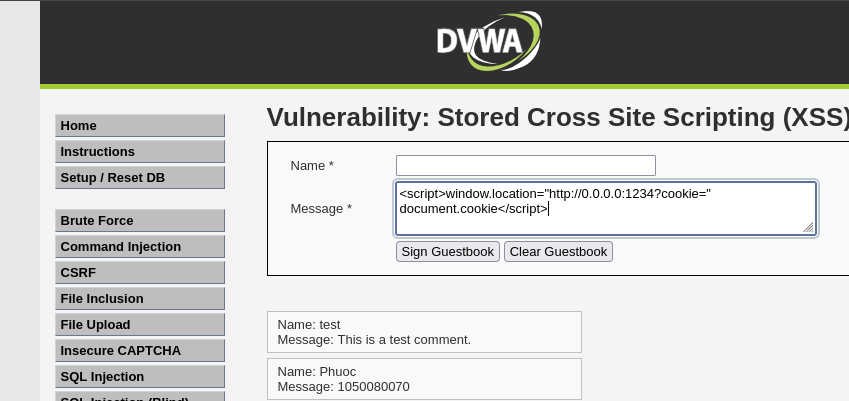


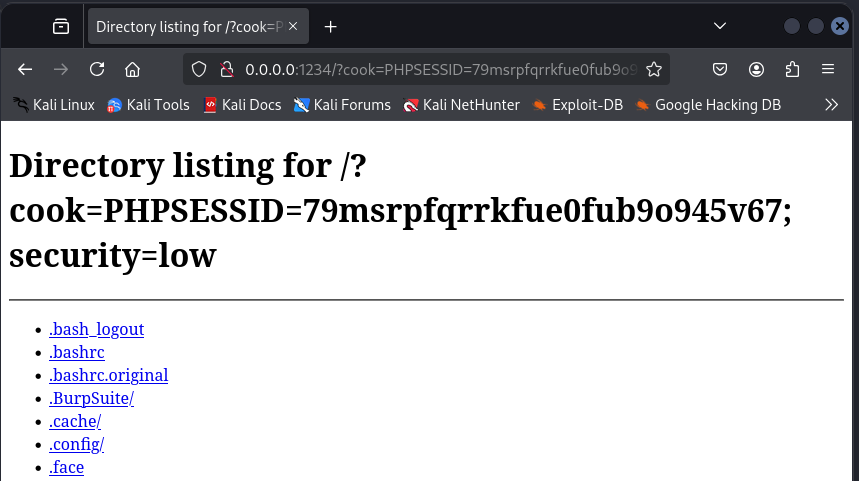
Bước 4: Thực hiện mở 1 host trên máy với python:



Bước 5: Mở chế độ Dev mode (F12) trên web và chuyển kích thước testArea lên 500  


Bước 6: Ghi 1 script vào message trả về cookie gửi đến trang web đã host với python:





1.3. Tham khảo mã nguồn (view source), giải thích ngắn gọn cách DVWA với security ở mức độ medium, high, impossible ngăn chặn tấn công khai thác lỗi Stored XSS.

- Medium: hàm strip\_tags loại bỏ các thẻ HTML và PHP ra khỏi chuỗi và sẽ trả về chuỗi đã loại bỏ hết các thẻ HTML và PHP trong $message. Hàm str\_replace sẽ loại bỏ tất cả &lt;script&gt;trong $name.

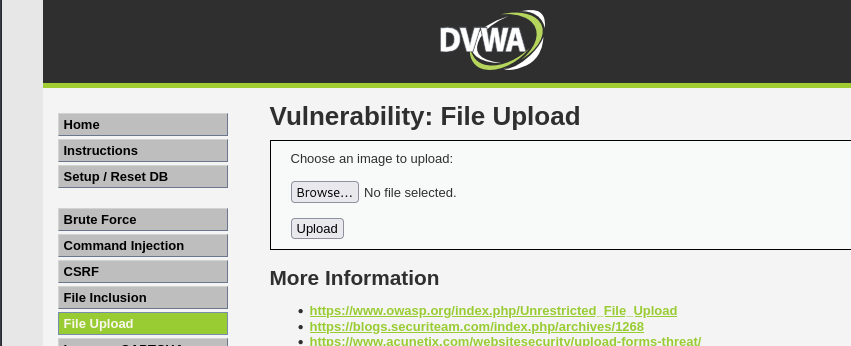
- High: hàm strip\_tags loại bỏ các thẻ HTML và PHP ra khỏi chuỗi và sẽ trả về chuỗi đã loại bỏ hết các thẻ HTML và PHP trong $message. Hàm addslashes() thêm một dấu gạch chéo ngược (\) phía trước ký tự đặc biệt: dấu nháy kép, dấu nháy đơn và dấu gạch chéo ngược trong $message.Loại bỏ tất cả các kí tự mà script có và không cho phép chữ T trong https.

- Impossible: Hàm htmlspecialchars () được triển khai lọc tất cả các ký tự nguy hiểm từ $message và $name.

Câu 2: Khai thác lỗi File upload trên DVWA

2.1 Tham khảo các tài liệu đính kèm để khai thác lỗi File upload trên DVWA (security ở mức độ low) để chiếm shell của máy chạy DVWA.

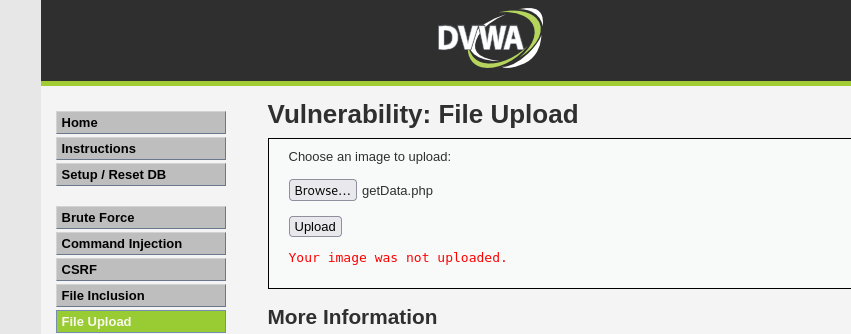
Bước 1: Vào mục File Upload trên DVWA.



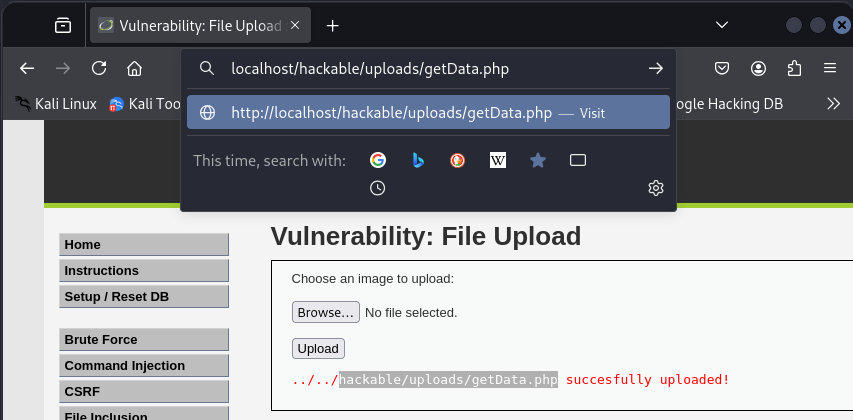
Bước 2: Tạo 1 file php để thực hiện lấy dữ liệu trang web.

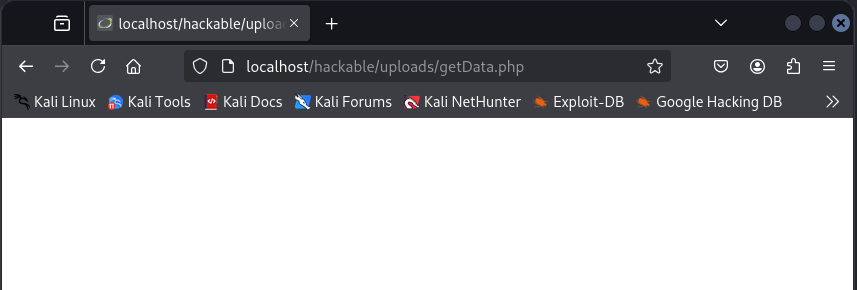


Bước 3: Thực hiện upload file.

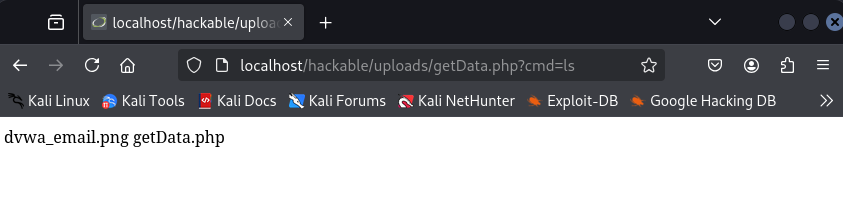


Bước 4: Truy cập đường dẩn sau để sử dụng file getData.php vừa upload.

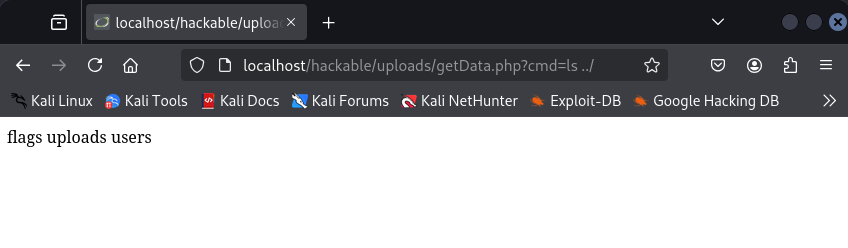


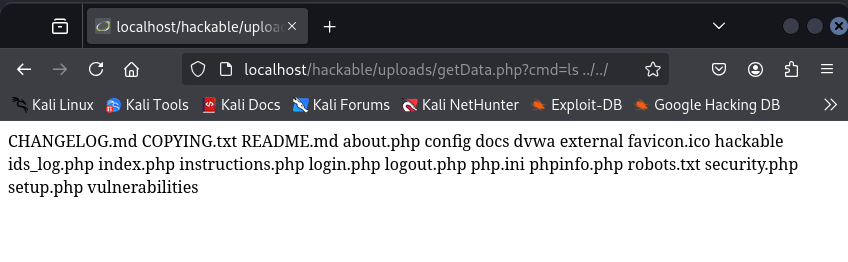


Bước 5: Thực hiện kiểm tra các thư mục hiện có trên web với ls.

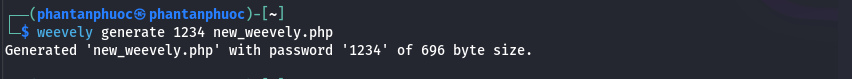


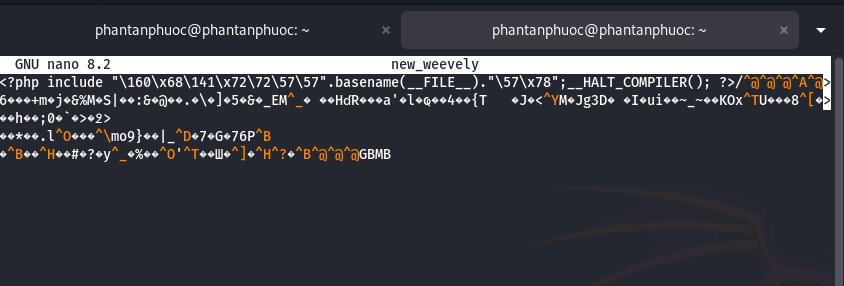
Bước 6: Kiểm tra nhiều thư mục hơn:



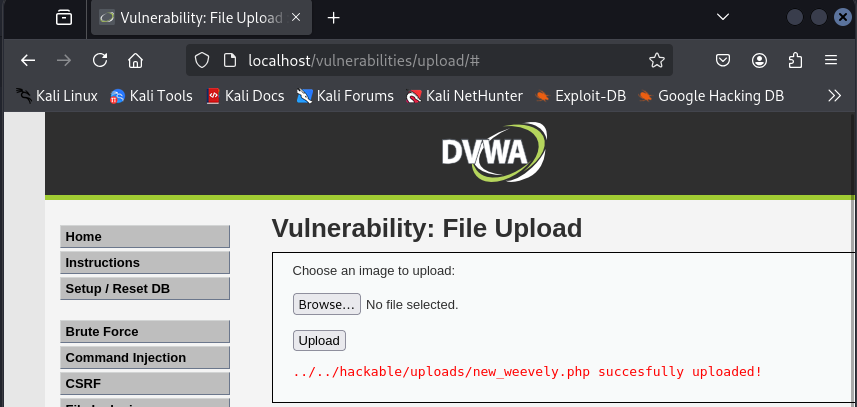


Bước 7: Tạo 1 file weevely.php

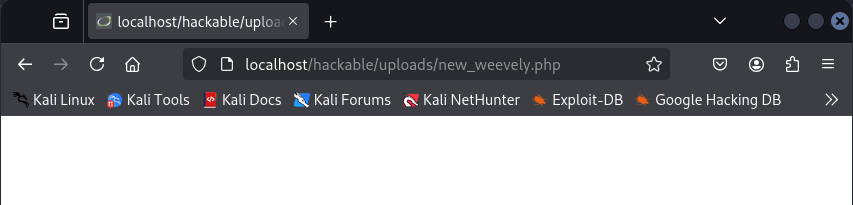




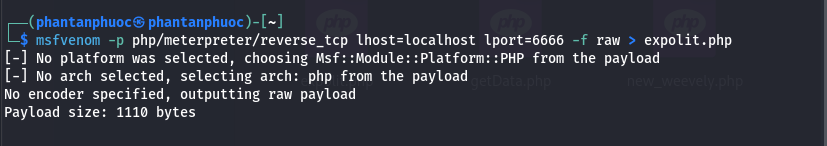
Bước 8: Upload file weevely lên DVWA.



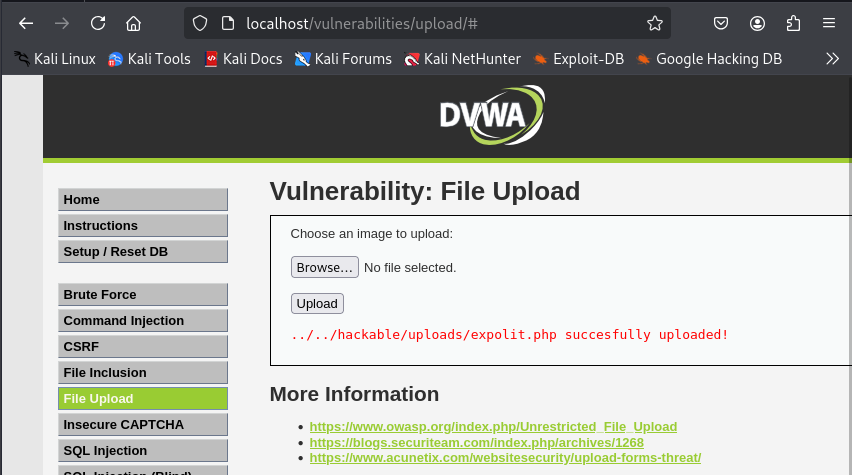
Bước 9: Thực hiện truy cập đến file weevely đã được upload trên DVWA.



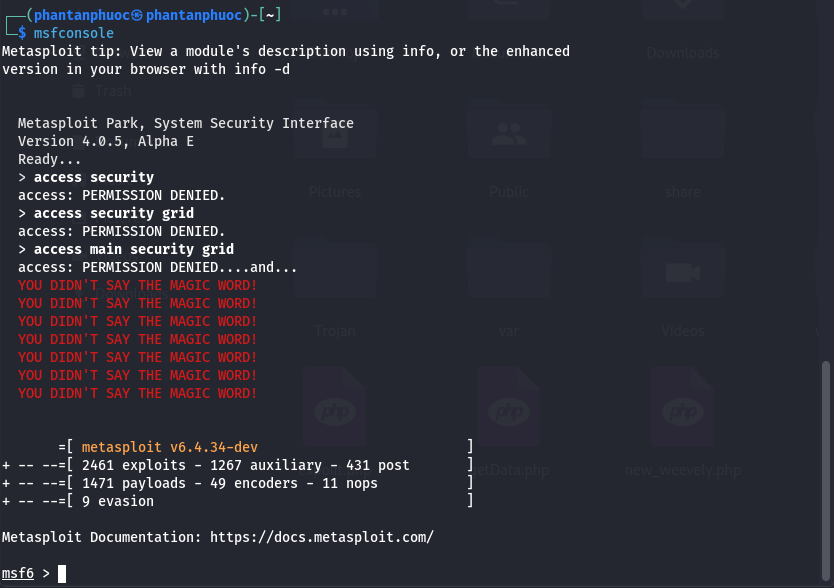
Bước 10: Khởi động host msfvenom sử dụng để khai thác các lỗ hổng PHP trên hệ thống.



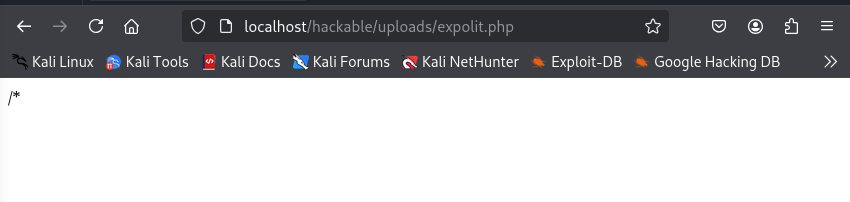
Bước 11: Thực hiện upload file expolit.php.



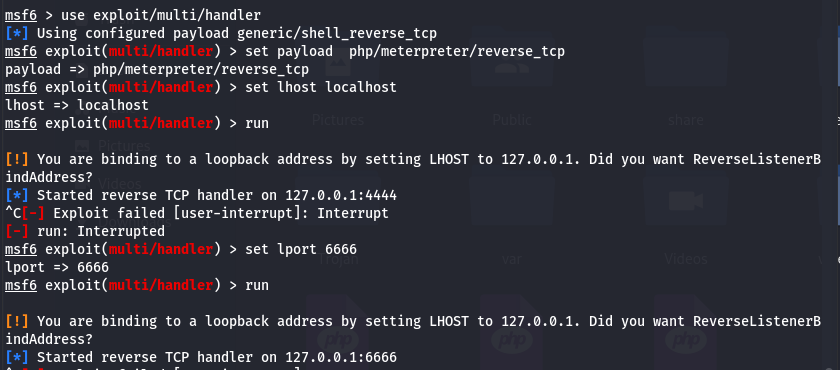
Bước 12: Khởi động msfconsole.



Bước 13: Mở đường dẩn đến file expolit được upload trên trang web.



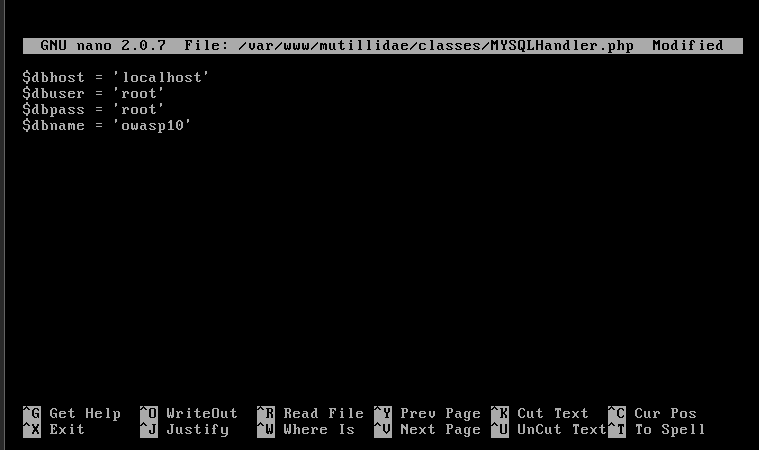
Bước 14: Thực hiện kiểm tra kết nối với msfconsole:

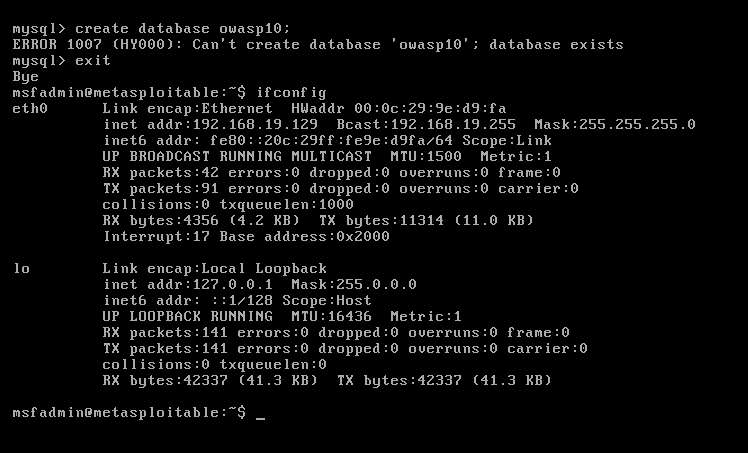


Câu 4: Sử dụng công cụ OWASP ZAP để tìm lỗ hổng bảo mật của ứng dụng web

4.1. Sửa lỗi cấu hình cơ sở dữ liệu của Mutillidae trên máy ảo Metasploitable 2

Bước 1: Cấu hình mySQL:

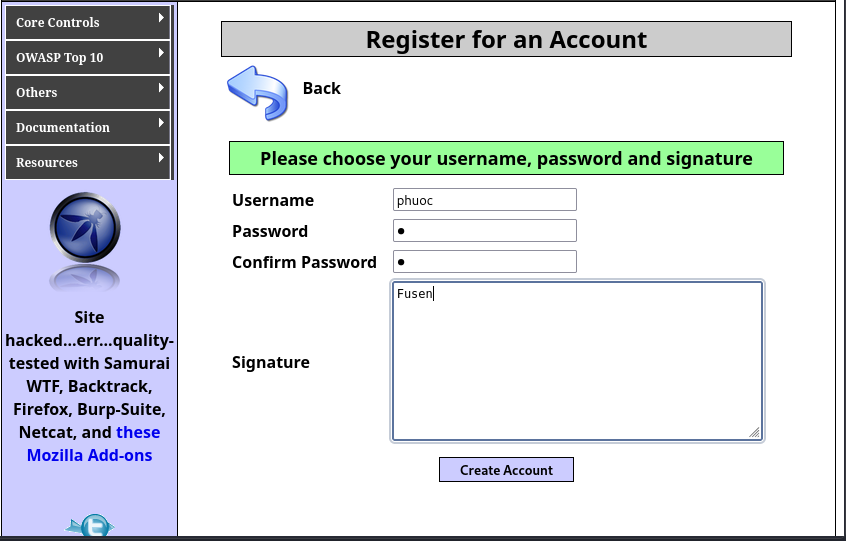




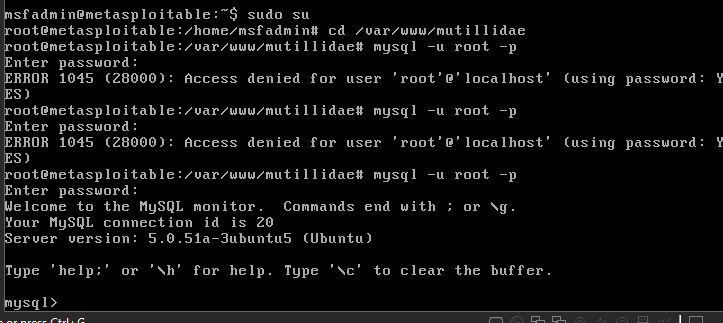
Bước 2: Mở trang web:

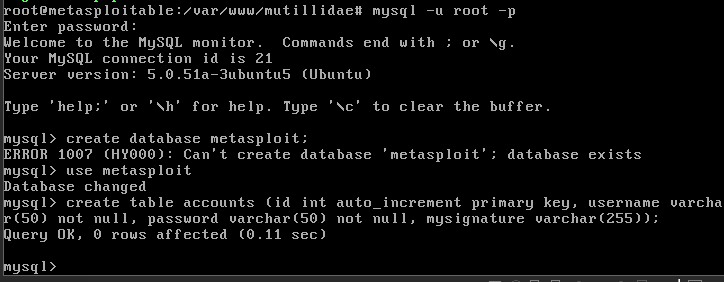


Bước 3: Tién thành đăng ký:

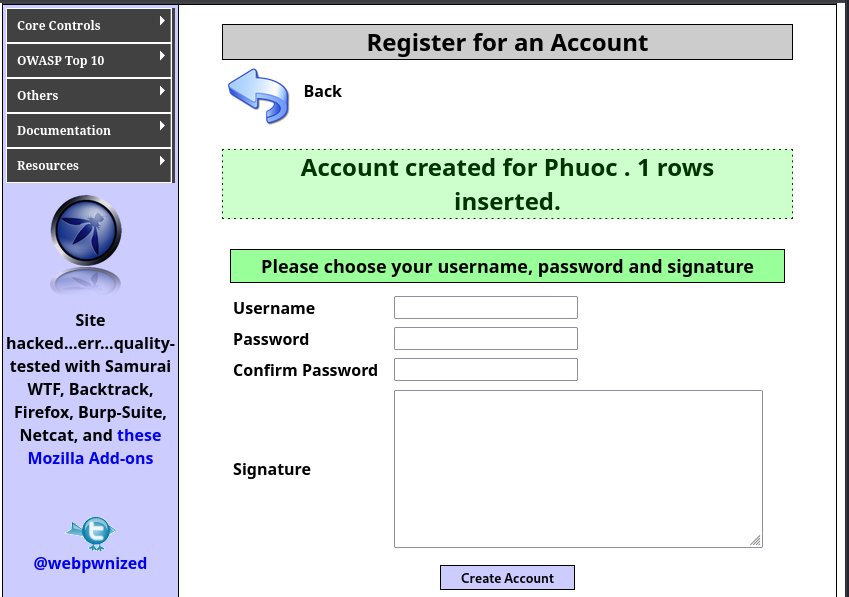


Bước 4: Đăng nhập không thành công tiến thành thêm bảng Account.

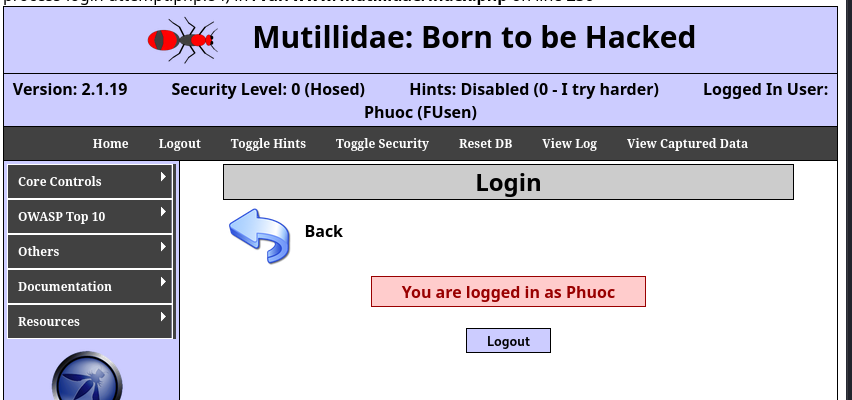




Bước 5: Tạo bảng accounts thành công tiến thành đăng ký lại:

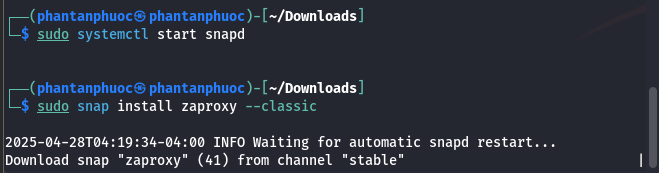


Bước 6: Tiến thành đăng nhập

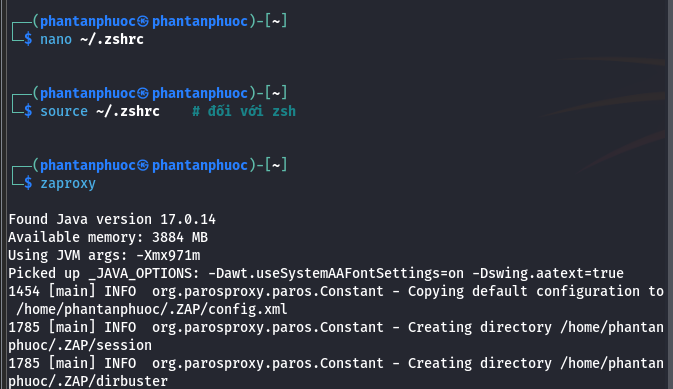


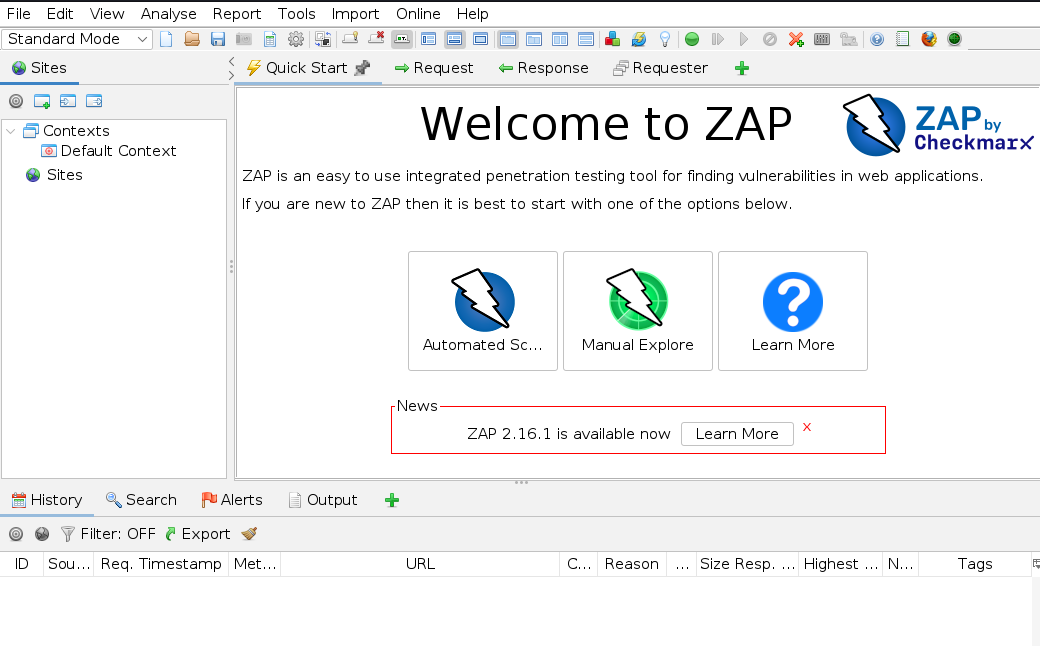
4.2. Khởi động máy ảo Metasploitable 2. Sau đó dùng công cụ OWASP ZAP để tìm các lỗ hổng bảo mật có trên ứng dụng web Mutillidae trên máy ảo Metasploitable 2.

Bước 1: Tải công cụ OWASP ZAP.

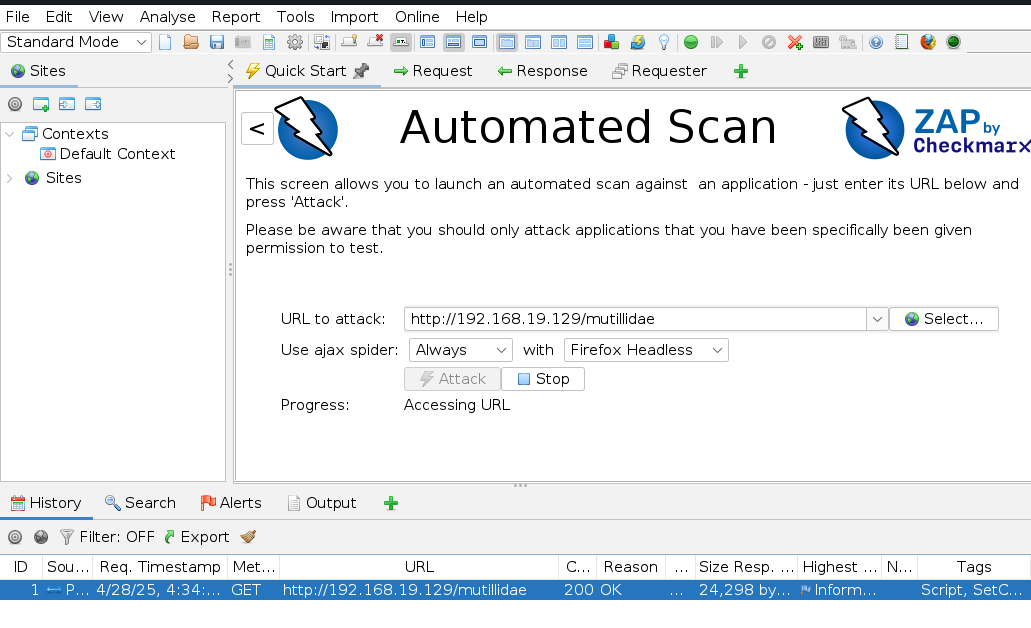


Bước 2: Khởi động ZAP.





Bước 3: Nhập đường dẩn tới trang web mutillidea và thực hiện scan



Bước 4: Kiểm tra alerts

