BÁO CÁO BÀI THỰC HÀNH SỐ 8

KIỂM THỬ LỖ HỔNG SQL INJECTION

Họ và tên:

Yêu cầu kết quả thực hành:

Báo cáo kết quả thực hành có tên theo định dạng HoTenSV\_MSSV\_Lab08.docx

Câu 1(3.5 điểm)

Kiểm thử lỗ hổng SQL Injection trên các trang web :

Xác định các tham số đầu vào và cách thức chúng được gửi tới server (0.25 điểm)

Phân tích và phán đoán kiểu truy vấn (0.25 điểm)

Phân tích và phán đoán vị trí của các giá trị tham số đầu vào được sử dụng trong câu truy vấn (0.5 điểm)

Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào (2.5 điểm)

Lưu ý:

Nói rõ mục đích sử dụng các giá trị kiểm thử

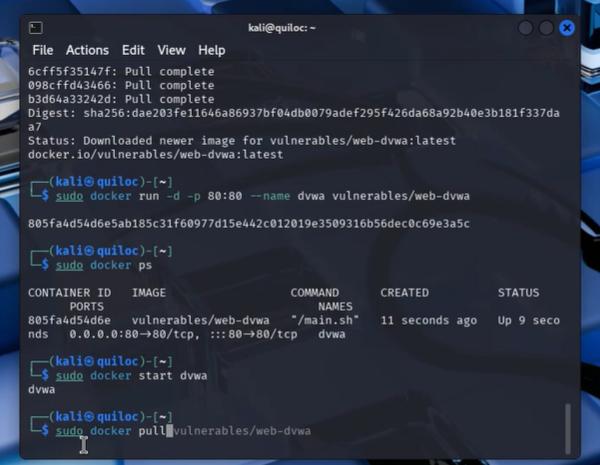
Giải thích rõ các phán đoán và suy luận từ kết quả khi sử dụng mỗi giá trị kiểm thử

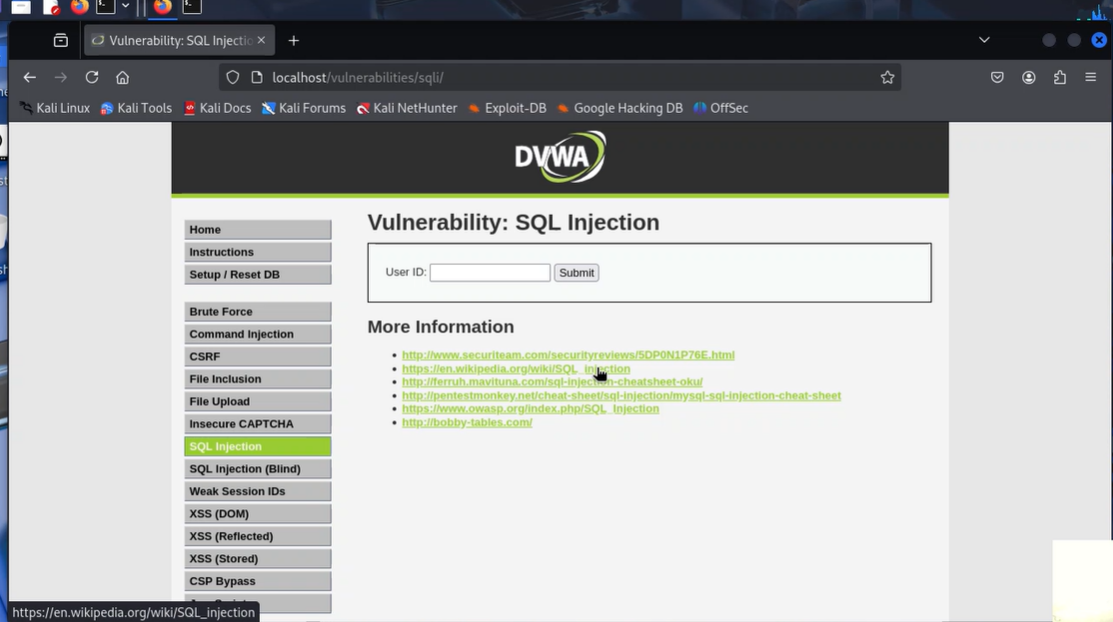
BÁO CÁO KIỂM THỬ LỖ HỔNG SQL INJECTION

1. Mục tiêu kiểm thử:

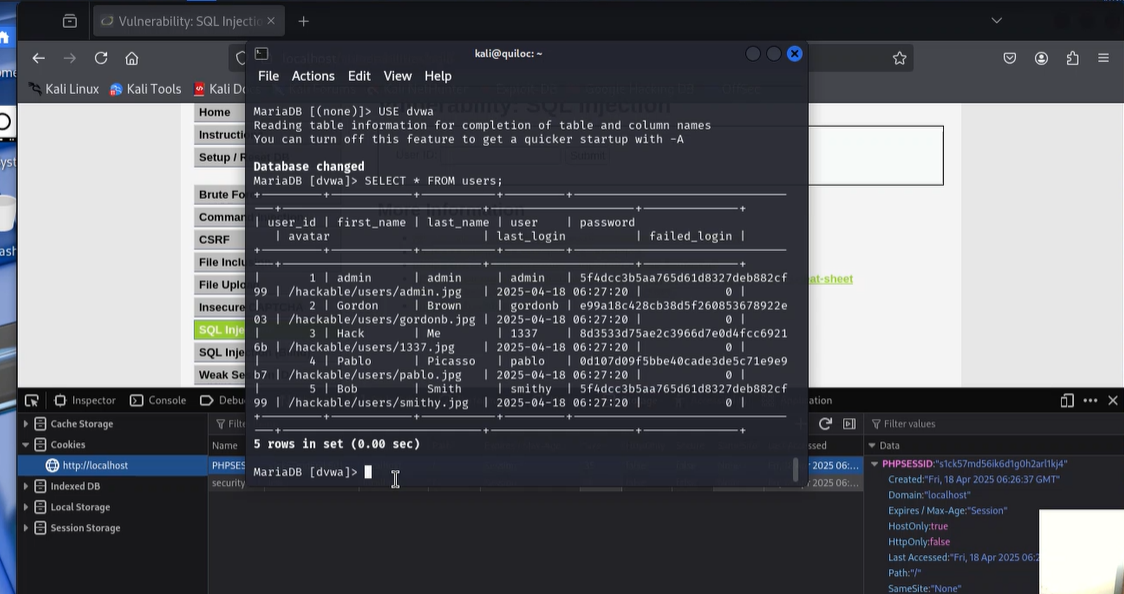
Ứng dụng web: Damn Vulnerable Web Application (DVWA)

URL kiểm thử: <http://localhost/vulnerabilities/sqli/>



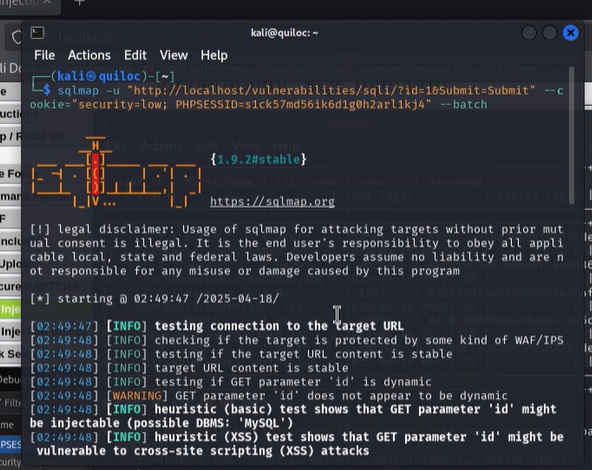


Mục tiêu: Phát hiện và khai thác lỗ hổng SQL Injection trong DVWA.



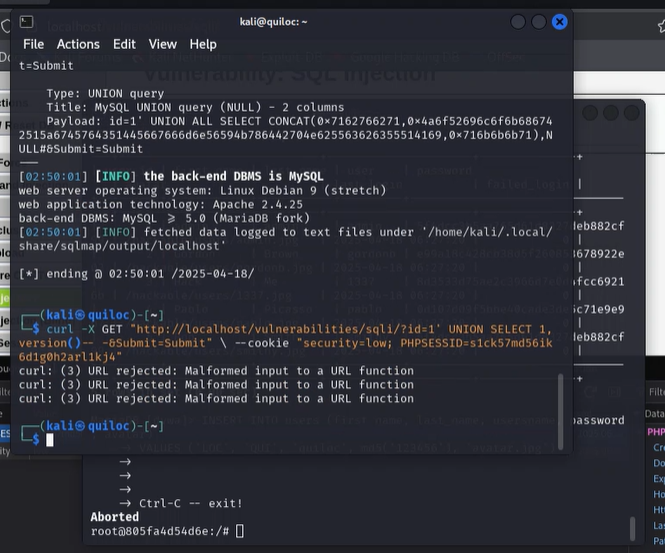
3. Phương pháp kiểm thử:

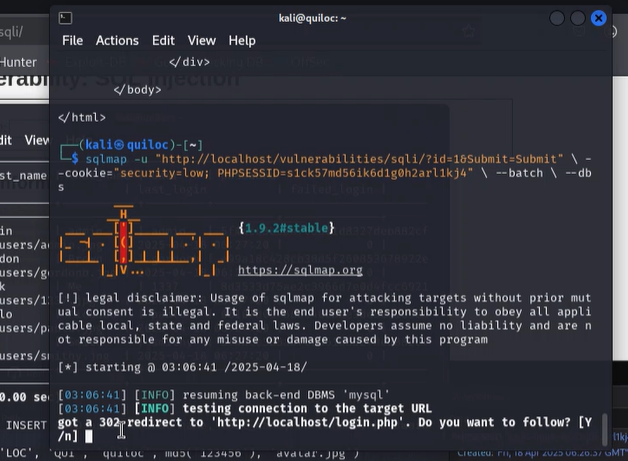
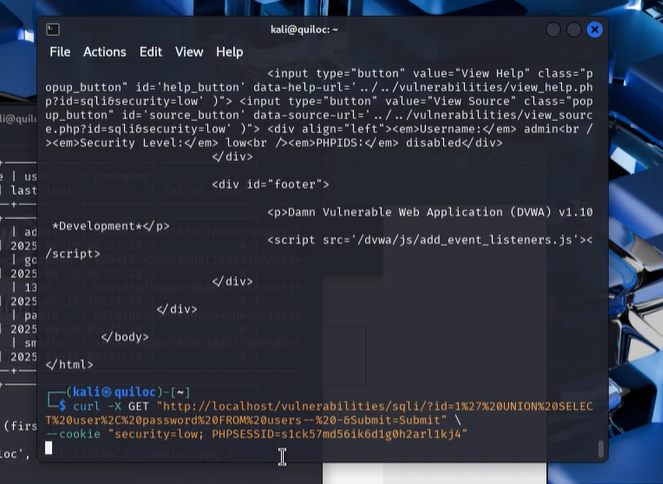
3.1. Xác định điểm tiêm SQL (Injection Point):

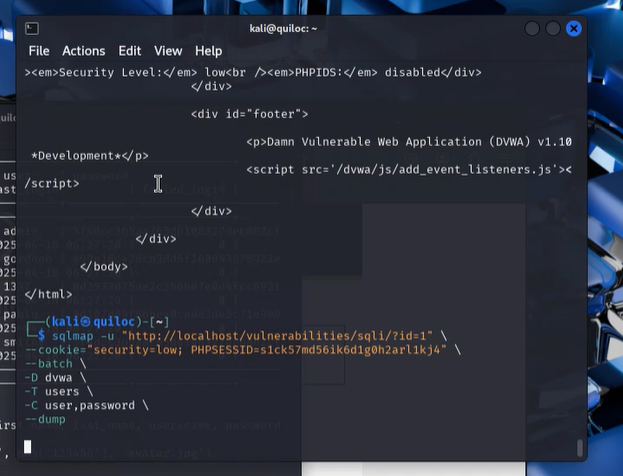


Tham số tiêm: id trên URL GET

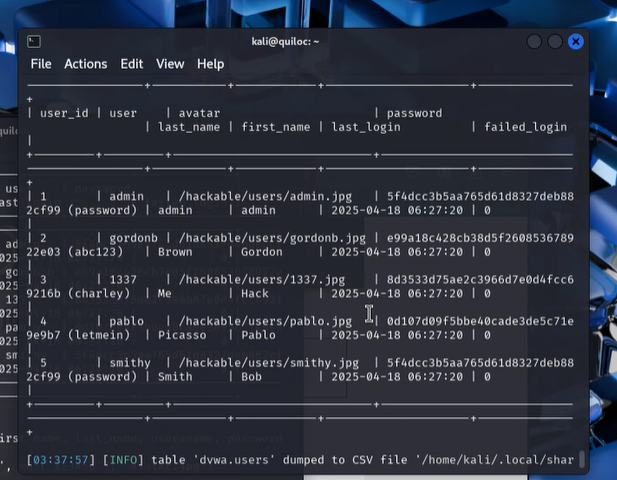
Kiểm thử bằng tay:



3.2. 

3.3.

4. Kết quả kiểm thử:



Phát hiện lỗ hổng SQL Injection tại tham số id

Trích xuất thành công dữ liệu bảng users: tên người dùng, mật khẩu (đã băm MD5), họ tên và avatar.

Một số mật khẩu đã được giải mã bằng tấn công từ điển:

- admin : password

- gordonb : abc123

- charley : letmein