**LAB 4**

**Web Attack and Defense**

Họ tên và MSSV: Phan Tân Phước – 1050080070

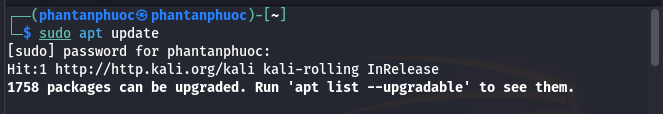
Lớp: 10 – ĐH – CNPM 1

Link youtube: <https://youtu.be/eSlLsSx3WR8>

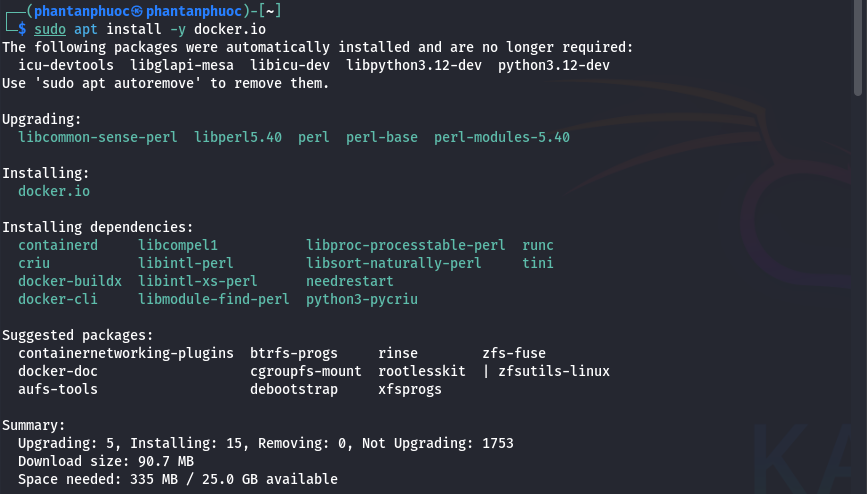
Câu 1: Cài đặt Damn Vulnerable Web Application (DVWA) trên Kali Linux.

Bước 1: Cài đặt docker:

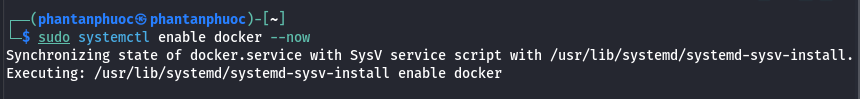
sudo apt update



sudo apt install -y docker.io



sudo systemctl enable docker --now

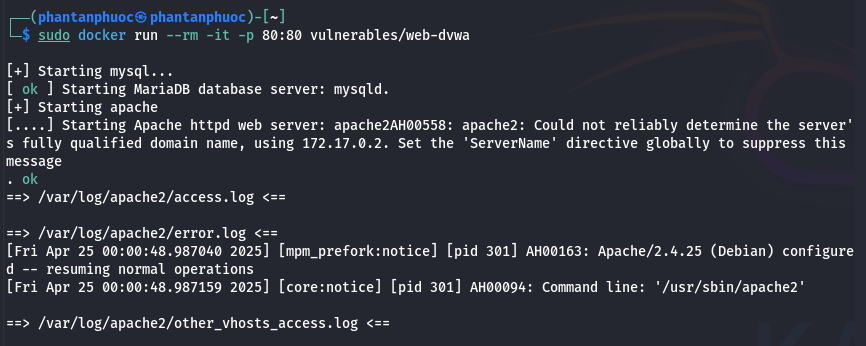


Bước 2: Thêm người dùng vào nhóm docker; log out và log in lại vào kali.

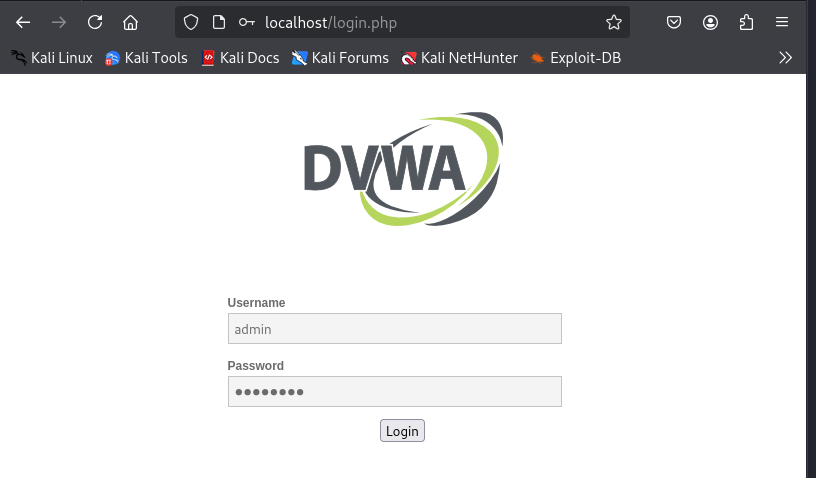
sudo usermod -aG docker $USER



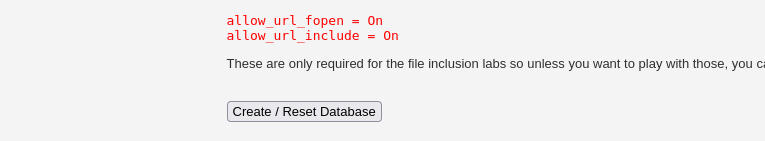
sudo docker run --rm -it -p 80:80 vulnerables/web-dvwa

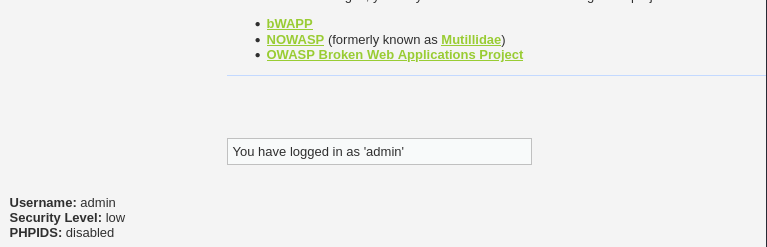


Bước 3: Truy cập vào DVWA ở địa chỉ <http://localhost>.

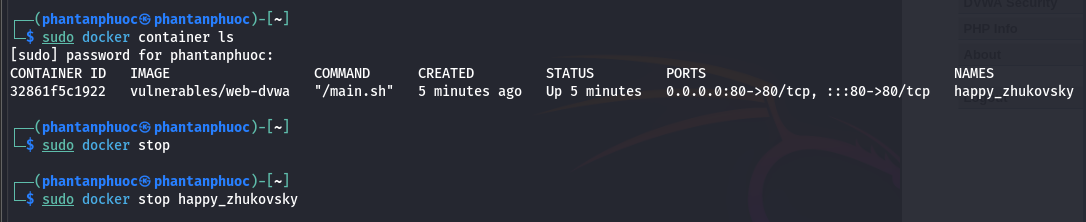


Bước 4: Chọn Create/Reset Database.





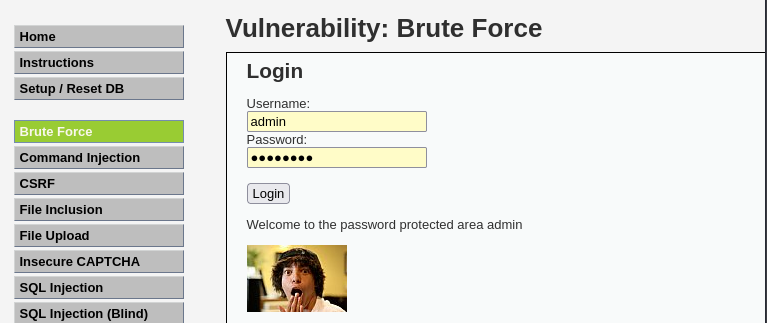
Bước 5: Sau khi hoàn thành bài thực hành dừng container DVWA.



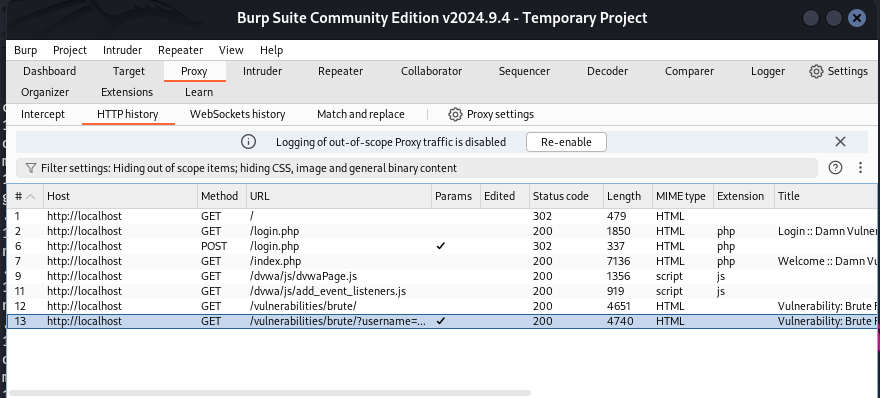
Câu 2: Tấn công dò mật khẩu trên DVWA.

Bài 2.1. Tham khảo các tài liệu đính kèm để thực hiện tấn công dò mật khẩu (Brute force attacks) của một tài khoản trên DVWA (security ở mức độ low) sử dụng công cụ Burp Suite (hoặc Hydra, John The Ripper, v.v.).

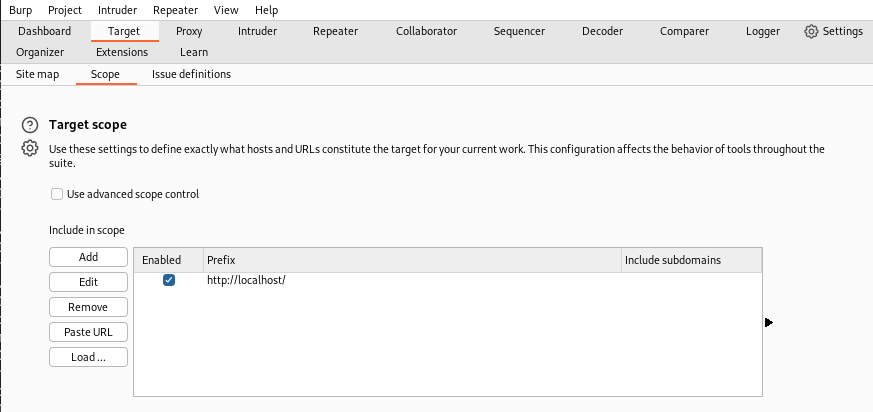
Bước 1: Đăng nhập thông thường và kiểm tra kết quả.

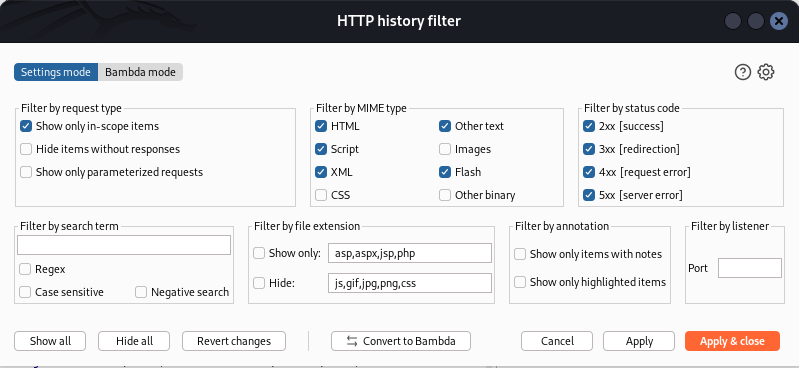


Bước 2: Mở Burp Suite Community Edition

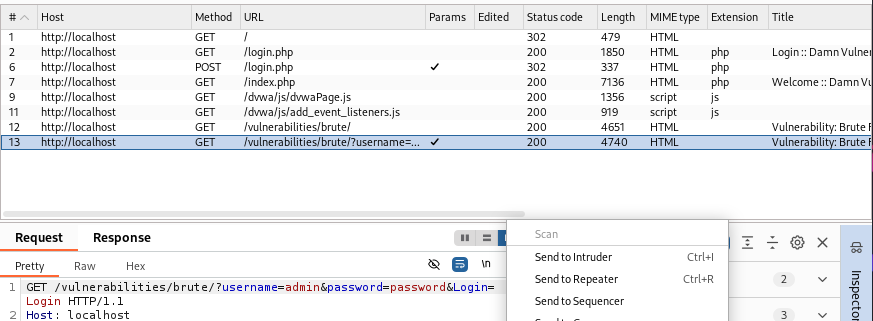


Bước 3: Bật những cài đặt sau.

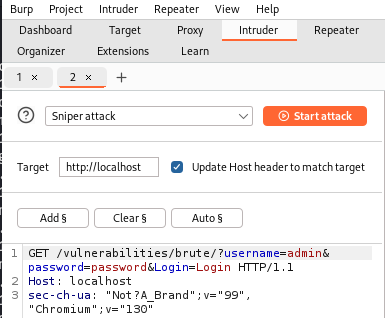


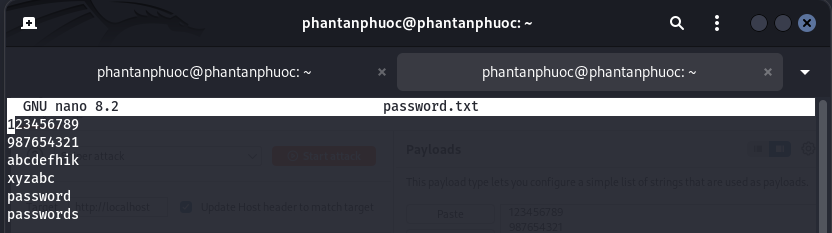


Bước 4: Chọn vào 1 host đã thực hiện đăng nhập trên DVWA. Và chuột phải vào phần Request > Respone.

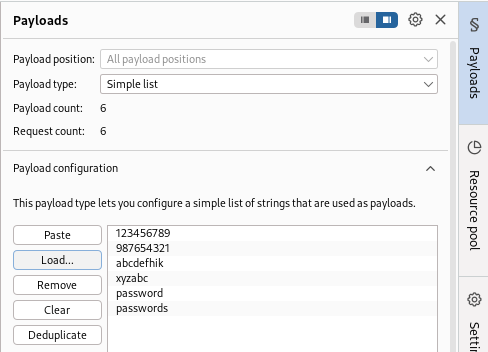


Bước 5: Vào phần Intruder. và kiểm tra name và password.

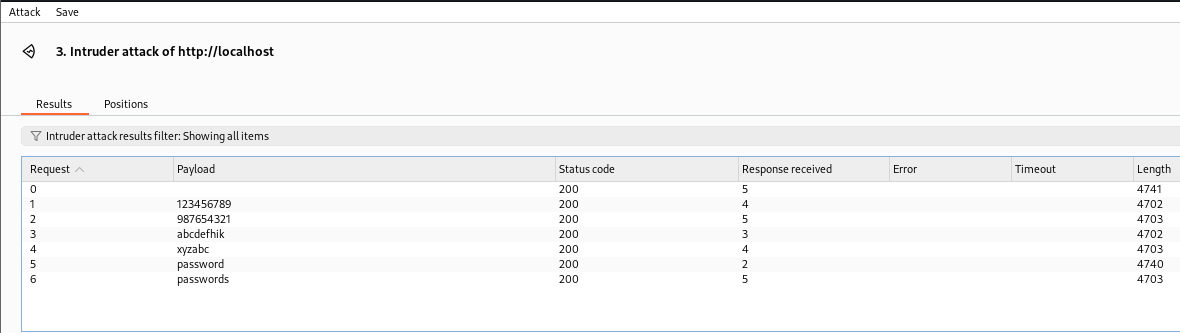


Bước 6: Tạo 1 tệp password.txt chứa các mật khẩu chuẩn bị thăm dò:  


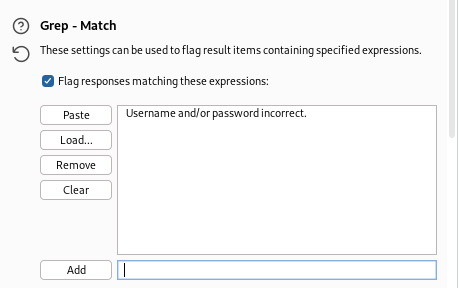
Bước 7: Tải hết các mật khẩu từ tệp mật khẩu lên Burt.



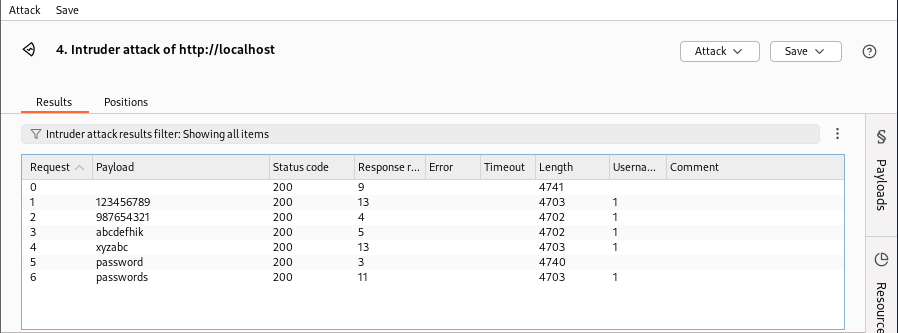
Bước 8: Bắt đầu thăm dò. Nhưng chưa xác định được.



Bước 9: Thêm chuỗi đăng nhập thất bại vào grep – map:



Bước 10: Tiến thành thăm dò lại mật khẩu. Thăm dò thành công vì trường thông báo sai đăng nhập không hiện tại mật khẩu: password



Bài 2.2. Tham khảo mã nguồn (view source), giải thích ngắn gọn cách DVWA với security ở mức độ medium, high, impossible ngăn chặn tấn công dò mật khẩu.

- Medium: Có 2 giây tạm dừng khi đăng nhập sai để hạn chế bị dò mật khẩu.

- High: Có ngẫu nhiên 0 đến 3 giây tạm dừng khi đăng nhập sai. Sinh ra token bí mật và

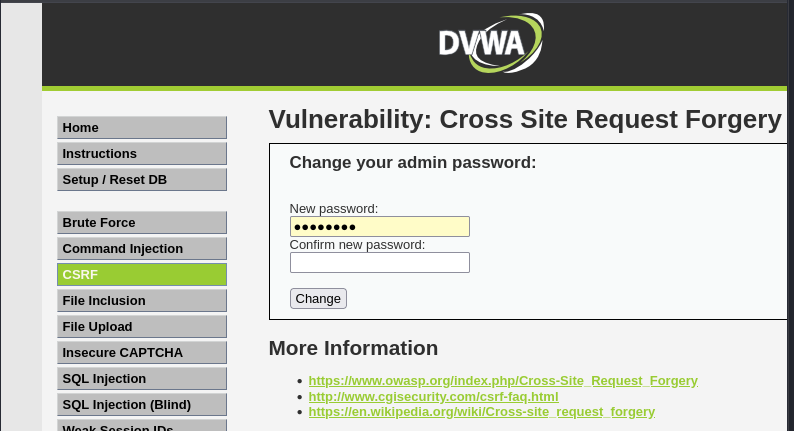
gửi xuống cho người dùng, người dùng khi đăng nhập phải gửi token đó lên.

- Imposible: Nếu mật khẩu sai một số lần nhất định thì khóa tài khoản tạm thời.

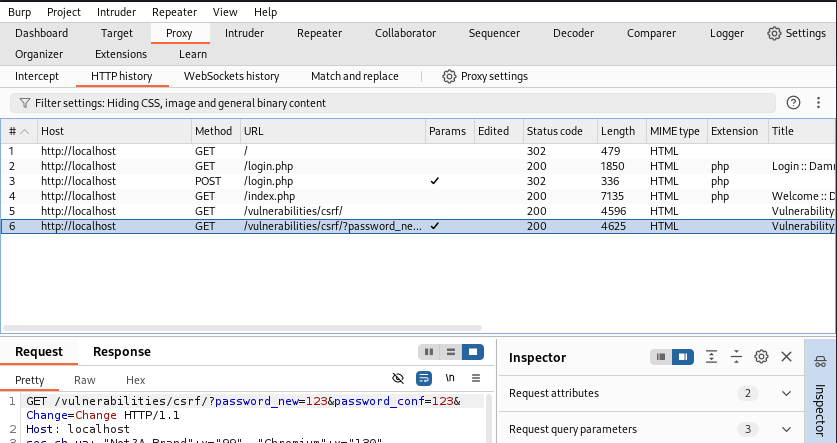
Câu 3: Khai thác lỗi Cross Site Request Forgery (CSRF) trên DVWA

Bài 3.1: Tham khảo các tài liệu đính kèm để khai thác lỗi CSRF của DVWA (security ở mức độ low) để tự động đổi mật khẩu người dùng.

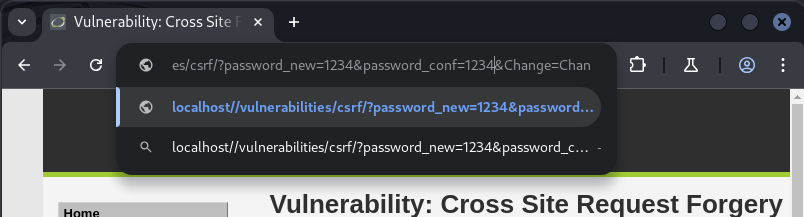
Bước 1: Vào localhost và vào phần CSRF:

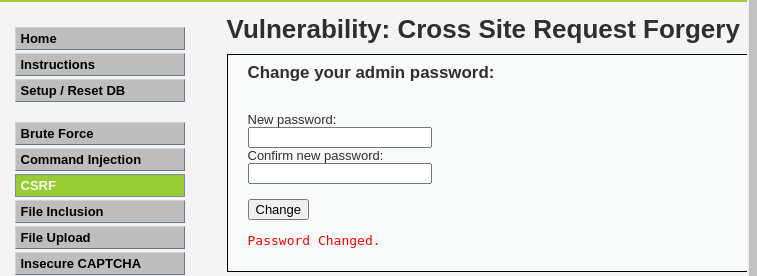


Bước 2: Thực hiện đổi mật khẩu và kiểm tra mã html.



Bước 3: Lấy đường dẩn tại GET và đưa vào trực tiếp trên thanh trình duyệt. Và kiểm tra kết quả có thành công thay đổi không.





Bài 3.2. 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 CSRF. (Chụp hình minh họa quá trình thực hiện)

- Medium: Kiểm tra yêu cầu có phải từ chính bản thân trang web không, kiểm tra lời yêu cầu xuất phát từ đâu.

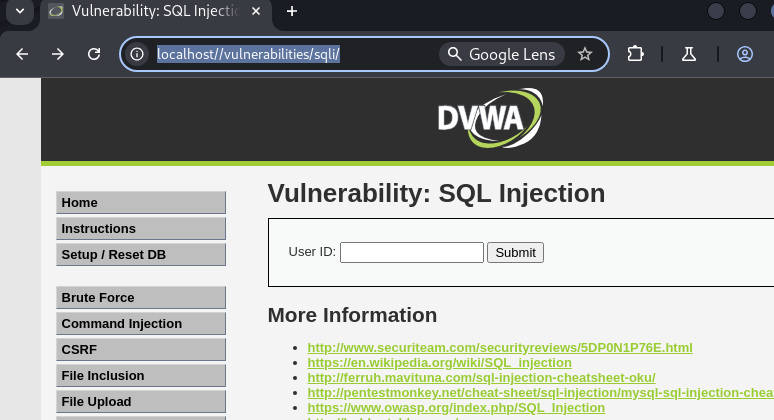
- High: Sinh ra token bí mật và gửi xuống cho người dùng, người dùng khi đổi mật khẩu phải gửi token bí mật đó lên.

- Imopossible: Phải nhập mật khẩu cũ khi muốn đổi mật khẩu.

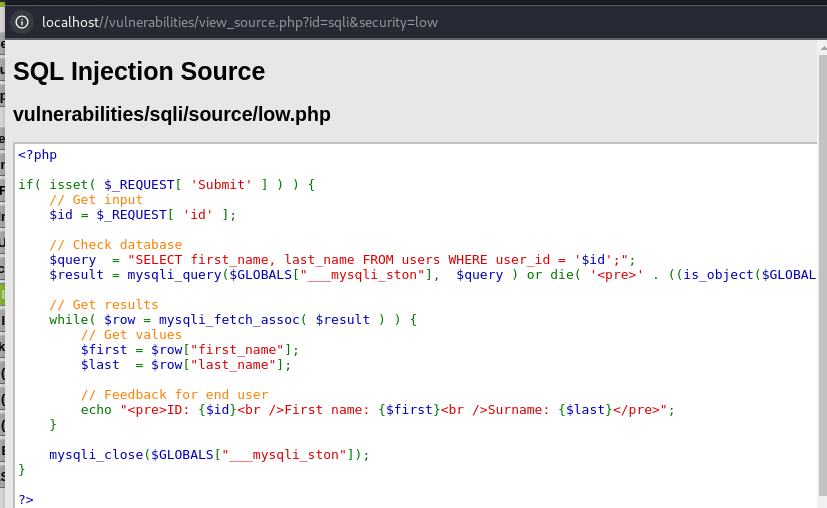
Câu 4: Khai thác lỗi SQL injection trên DVWA

Bài 4.1. Tham khảo các tài liệu đính kèm để khai thác lỗi SQL injection trên DVWA (security ở mức độ low) để lấy mật khẩu người dùng admin.

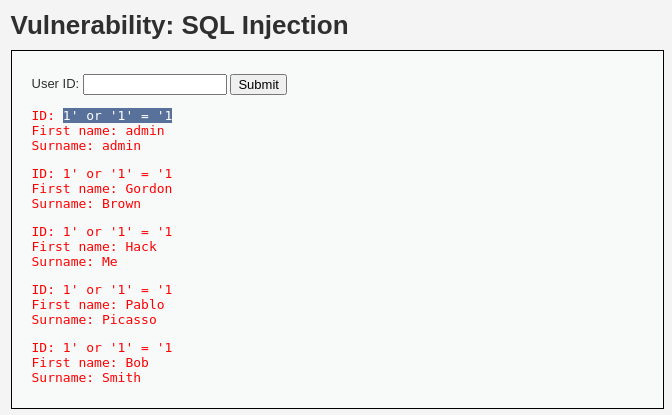
Bước 1: Mở VDWA và vào với đường dẩn sau <http://localhost//vulnerabilities/sqli/>



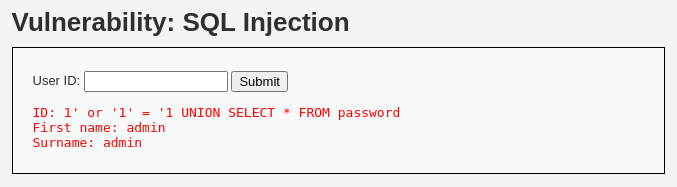
Bước 2: Vào phần View Source và kiểm tra kết quả gửi đi.



Bước 3: Thực hiện tìm kiếm với chuỗi sau để lấy thông tin các người dùng: 1' or '1' = '1

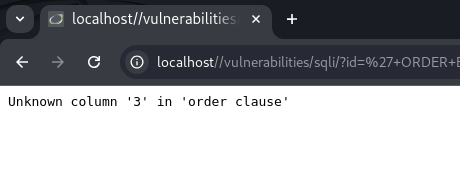


Bước 4: Thực hiện truy vấn sau để lấy tài khoản admin: 1' or '1' = '1 UNION SELECT \* FROM password

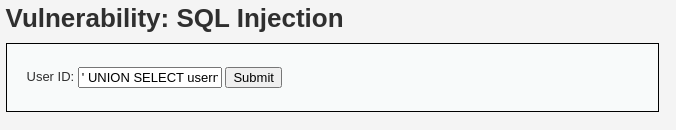


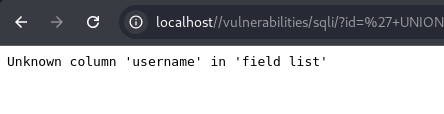
Bước 5: Thực hiện truy vấn sau để kiểm tra tổng dữ liệu: ‘ ORDER BY 3#



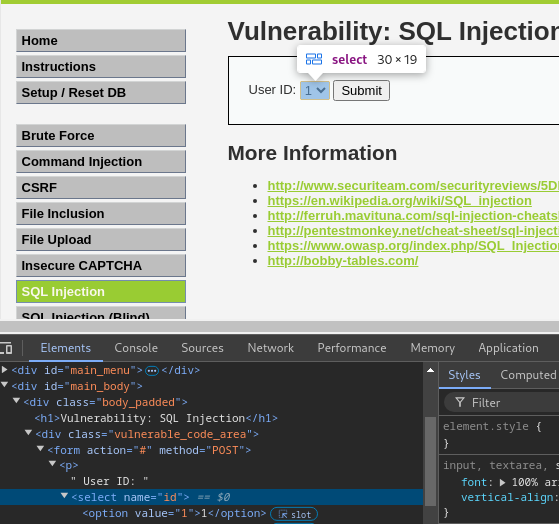


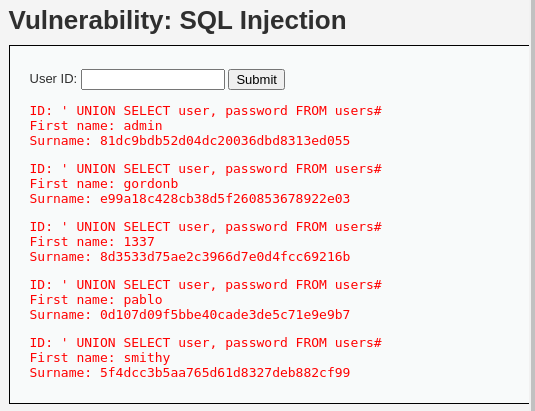
Bước 6: Thực hiện truy vấn sau để kiểm tra tên cột có tồn tại: ' UNION SELECT username, password FROM users#





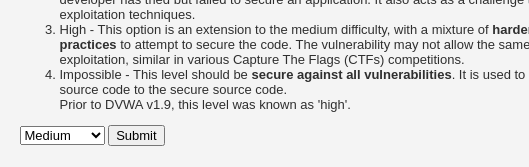
Bước 7: Thực hiện truy vấn sau để lấy thông tin các tài khoản: ' UNION SELECT user, password FROM users#



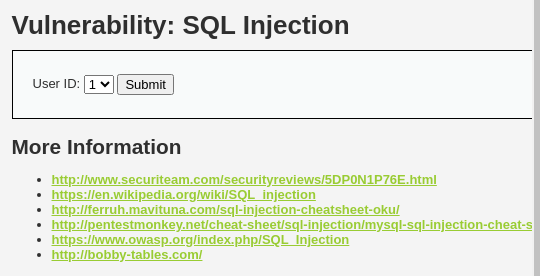


Bài 4.2. Tham khảo các tài liệu đính kèm để khai thác lỗi SQL injection trên DVWA (security ở mức độ medium) để lấy mật khẩu người dùng gordonb.

Bước 1: Chuyển DVWA sang mức medium.



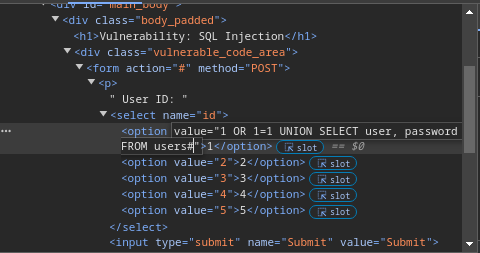
Bước 2: Vào <http://localhost/vulnerabilities/sqli/>. Kiểm tra thay đổi.



Bước 3: Vào view source để kiểm tra source web.

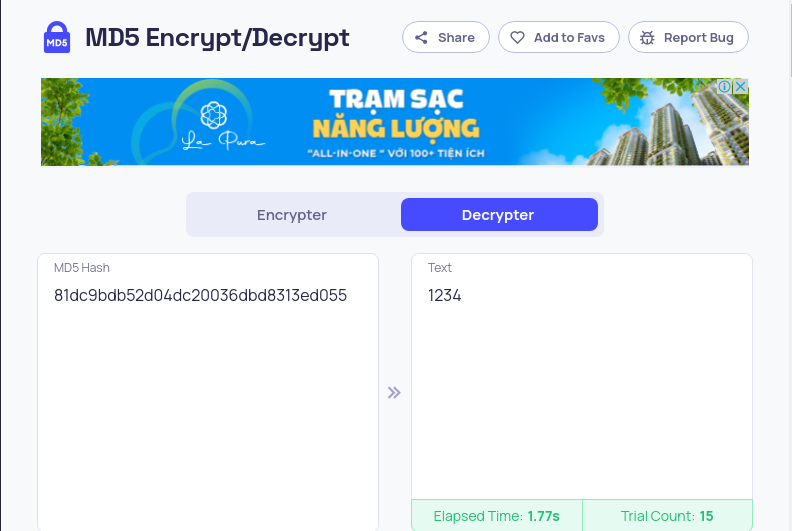


Bước 4: Bật chế độ Kiểm tra và thực hiện truy vấn trực tiếp trên các thẻ HTML với mã sau: 1 OR 1=1 UNION SELECT user, password FROM users#





Bước 5: Lấy 1 mã MD5 trong truy vấn tiến thành giải mã tại trang web : [https://10015.io/tools/md5-encrypt-decrypt](https://10015.io/tools/md5-encrypt-decrypt#google_vignette) với mã 5f4dcc3b5aa765d61d8327deb882cf99



4.3. 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 SQL injection.

- Medium: sử dụng mysql\_real\_escape\_string (). Điều này không cho phép các dấu

ngoặc kép trong giá trị được truyền. Chỉ cho người dùng chọn danh sách chọn để hạn chế bị chèn lệnh.

- High: yêu cầu nhập ID người dùng trên một trang khác nhưng vẫn tồn tại lỗ hổng bảo mật như mức độ Easy.

- Impossible: Kiểm tra xem có phải người dùng nhập số không và đảm bảo chỉ có một kết quả truy vấn được trả về.