BÁO CÁO BÀI THỰC HÀNH SỐ 9

KIỂM THỬ LỖ HỔNG XSS và CSRF

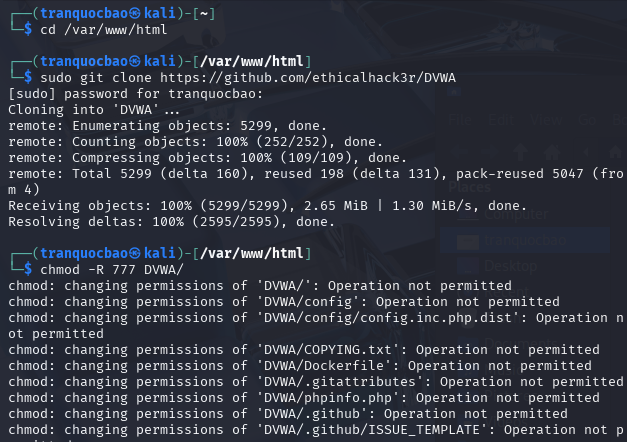
Họ và tên : Trần Quốc Bảo

Lớp 10\_ĐH\_CNPM2

MSSV: 1050080129

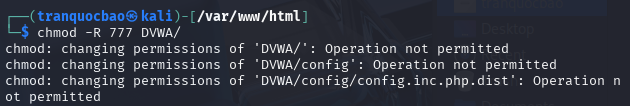
Link YTB: <https://youtu.be/I96N8Rd1RSU>

1. Cài đặt môi trường

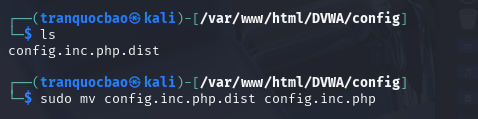


1. Cấu hình DVWA

2.1 Cấu hình một số thông tin, đầu tiên là quyền đọc, ghi và thực thi cho thư mục dvwa:

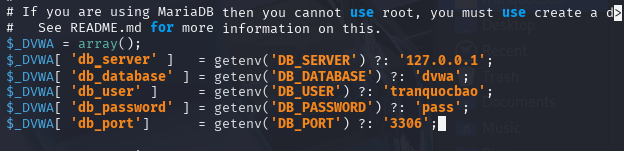


2.2 Tạo một bản sao file mới có tên **config.inc.php**



2.3 Thay đổi các giá trị **db\_user**, **db\_password** thành tên user và mật khẩu tùy chọn:



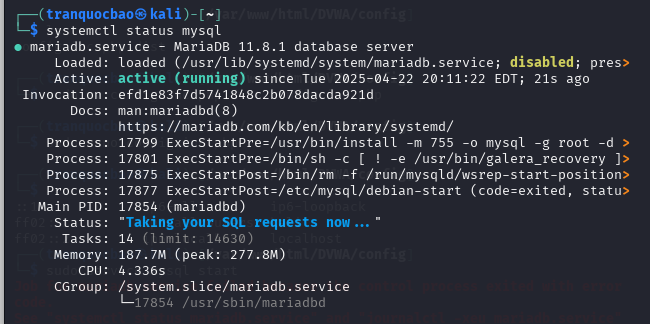


1. **Cấu hình cơ sở dữ liệu MySQL**

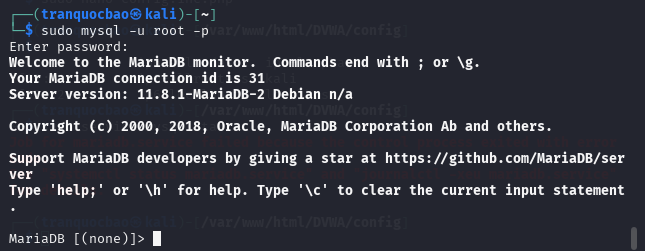
3.1 Để khởi động dịch vụ [MySQL](https://vietnix.vn/mysql-la-gi/)



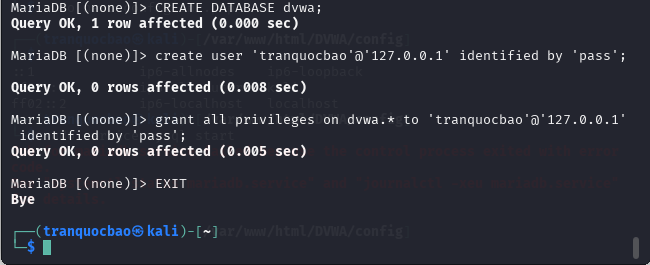
3.2 Kiểm tra trạng thái dịch vụ



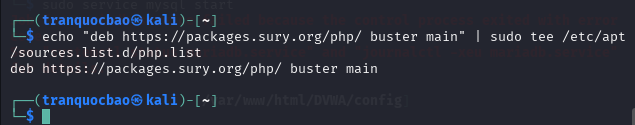
3.3 Đăng nhập vào MySQL với quyền root

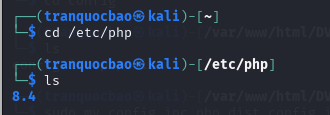


3.4 Tạo user mới với tên người dùng và mật khẩu tương tự như trong file cấu hình DVWA



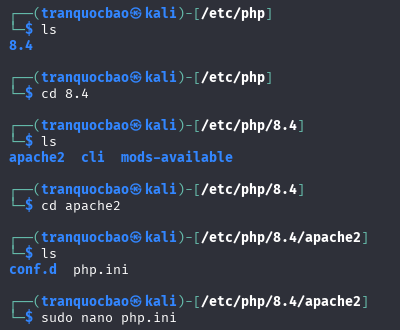
1. **Cài đặt PHP**



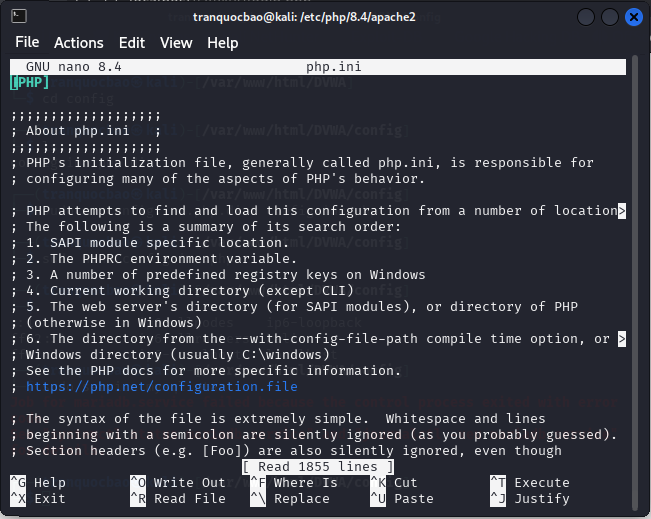


1. **Cấu hình máy chủ Apache**

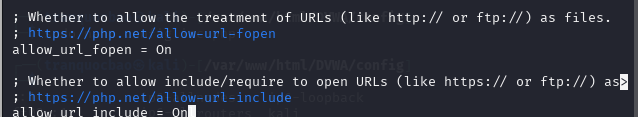
5.1 Chuyển đến thư mục /etc/php/7.4/apache2



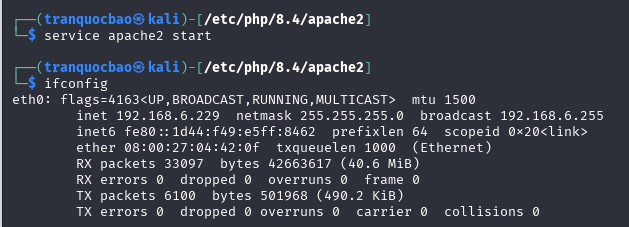
5.2 Chỉnh sửa file php.ini



5.3 Tìm dòng **allow\_url\_fopen** và **allow\_url\_include** rồi thiết lập giá trị thành **On**.

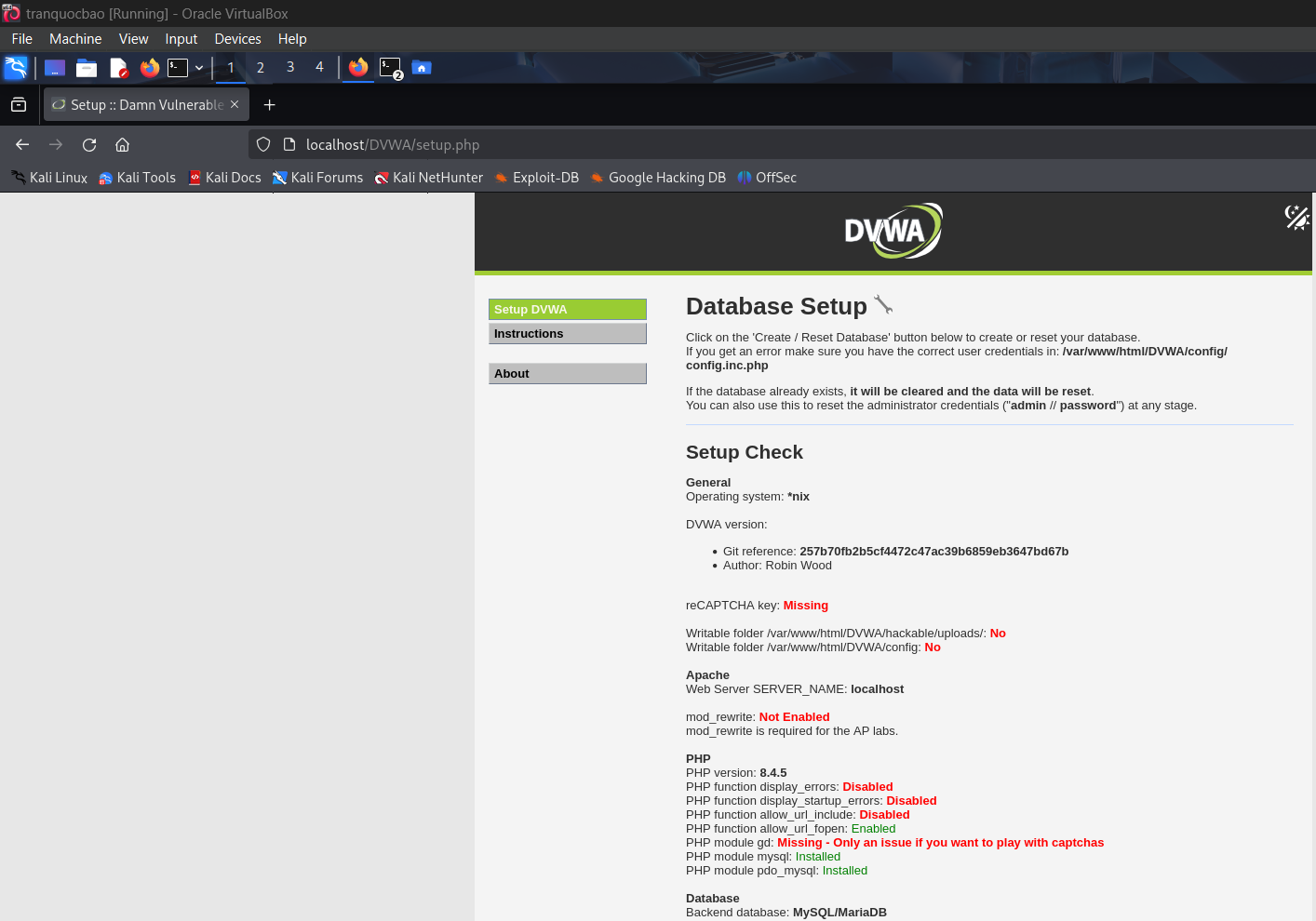


5.4 Khởi động máy chủ apache:



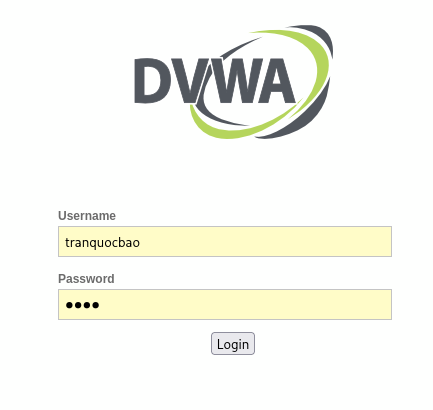
1. **Truy cập DVWA trên trình duyệt**

6.1 Trang **setup.php** sẽ xuất hiện như hình sau

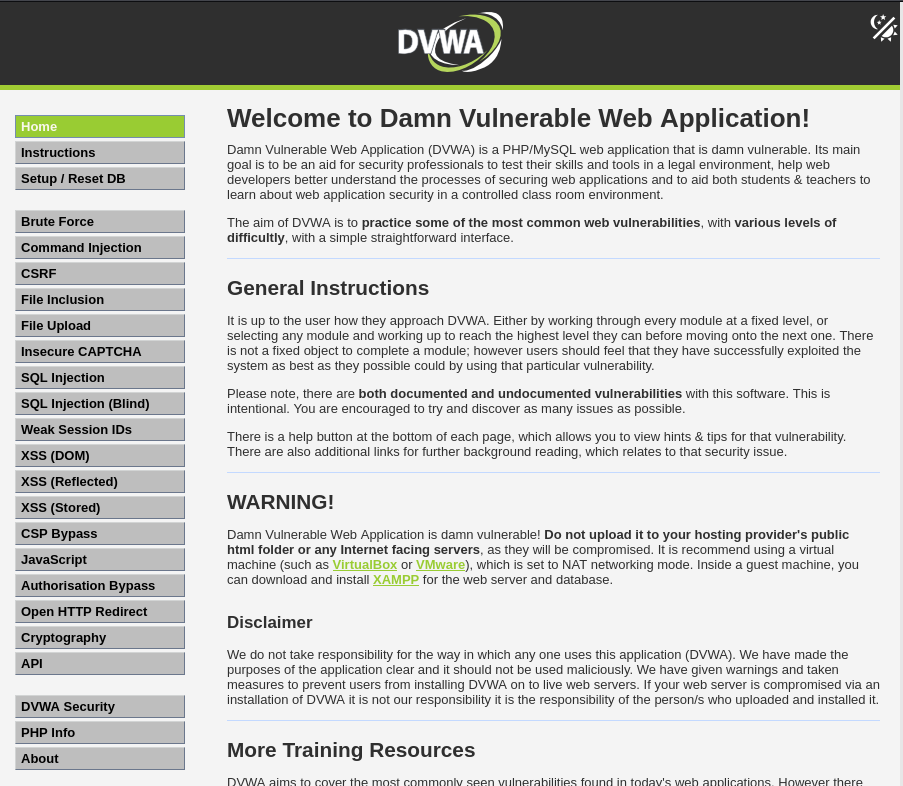


* 1. **Create / Reset Database** để tạo và cấu hình lại database

Bạn sẽ được tự động chuyển hướng đến trang đăng nhập DVWA



Sau khi đăng nhập, bạn sẽ thấy giao diện chính của DVWA



* 1. Thiết lập giá trị cho DVWA Security là “Low” để phần bắt đầu luyện tập dễ dàng hơn



Phần 1: Kiểm thử XSS

Thực hiện kiểm thử lỗ hổng XSS trên website: <http://testphp.vulnweb.com/>

Câu 1: Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa 4 số cuối MSSV: 0129.

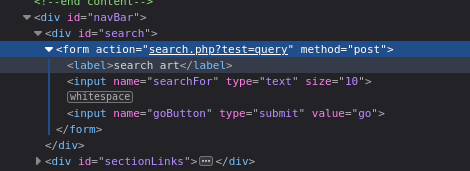
Bước 1: Truy cập vào địa chỉ http: <http://testphp.vulnweb.com/>

- Bước 2: Điền một số giá trị tùy ý vào ô nhập dữ liệu. Kết quả cho thấy chúng ta có thể phán đoán rằng

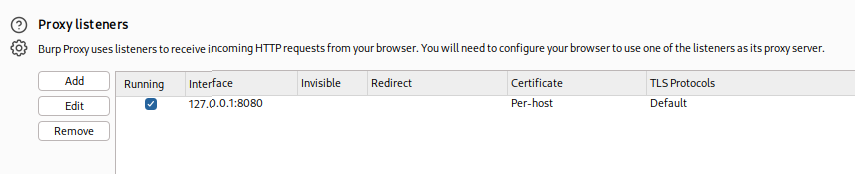
giá trị đầu vào được hiển thị



Nhấn tổ hợp phím Ctrl+U để xem mã nguồn HTML của trang kết quả. Có thể thấy giá trị đầu vào của người dùng nằm trong mã nguồn HTML. Bên cạnh đó, chúng ta có thể thấy một form HTML sử dụng phương thức POST để gửi tham số có tên là searchFor tới website.



Bước 3: Để xác định hết các tham số mà có thể không quan sát được từ mã nguồn HTML, sử dụng phần mềm Burp Suite như hướng dẫn bài thực hành số 5 để quan sát các thông điệp HTTP trao đổi giữa trình duyệt và máy chủ.



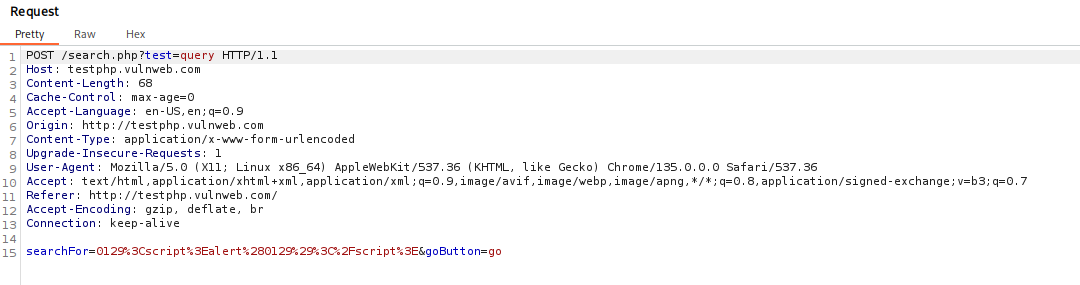
Bước 4: Trên Burp Suite, chọn thẻ Proxy  HTTP Proxy. Chọn thông điệp HTTP Request truy cập

tới địa chỉ ở trên. Ở thẻ Raw chúng ta có thể thấy đây là thông điệp sử dụng phương thức POST để

truy cập. Ở phần thân của thông điệp này có tham số và giá trị mà ta đã truyền.



Bước 1: Thử giá trị 0129<script>alert(0129)</script> Kết quả cho phép phán đoán từ script đã bị lọc.



Bước 2: Để kiểm tra xem bộ lọc có thực hiện đệ quy không, chúng ta sử dụng giá trị

<sscriptcript>alert(0129)</sscriptcript>. Kết quả không thay đổi với bước trên. Như vậy, có thể thấy rằng mọi

từ script sẽ bị lọc khỏi giá trị đầu vào cho tới khi hết.



Bước 3: Để kiểm tra bộ lọc có kiểm tra dạng in hoa hay không, chúng ta sử dụng giá trị

<sCript>alert(1)</sCript>;. Kết quả cho thấy bộ lọc không thực hiện kiểm tra dạng in hoa nên đoạn mã đã

được thực thi.

