BÀI THỰC HÀNH SỐ 9

KIỂM THỬ LỖ HỔNG XSS và CSRF

**Tự học lập trình với PHP, MYSQL, HTML và Javascript cơ bản để có thể hoàn thành bài thực hành này**

1. **Cài đặt môi trường luyện tập**

* Bước 1: Download mã nguồn tại địa chỉ sau:  <http://www.dvwa.co.uk/>

Xem thêm ở đây: <https://vietnix.vn/cai-dat-dvwa-tren-linux/>

Dùng lệnh

wget <https://github.com/digininja/DVWA/archive/refs/heads/master.zip>

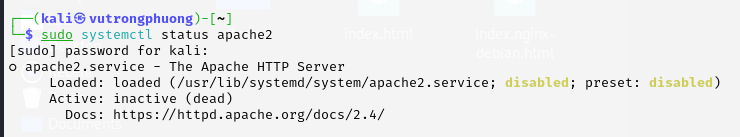


* Bước 2: Giải nén file đã download được và đổi tên thành “dvwa”



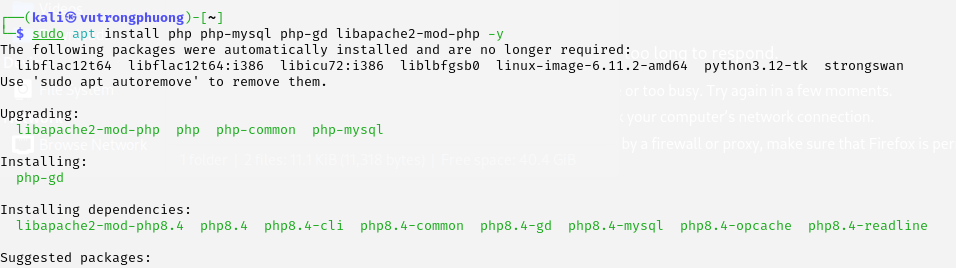
* Bước 3: Sao chép thư mục sau khi đã giải nén vào thư mục webroot của Web Server

Bước 1: **Apache và MariaDB**: Xác minh Apache và MariaDB đã được cài đặt



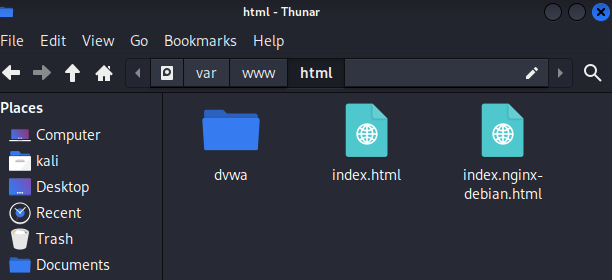






Copy vào thư mực

Di chuyển thư mục DVWA vào thư mục webroot  

* Bước 4: Tạo một CSDL có tên là “dvwa”



**Đăng nhập vào MariaDB**:

mysql -u root -p

đặt lại mật khẩu:

sudo mysqladmin -u root password '123’

**Tạo cơ sở dữ liệu và người dùng**: Trong shell MariaDB, chạy các lệnh SQL sau:

CREATE DATABASE dvwa;

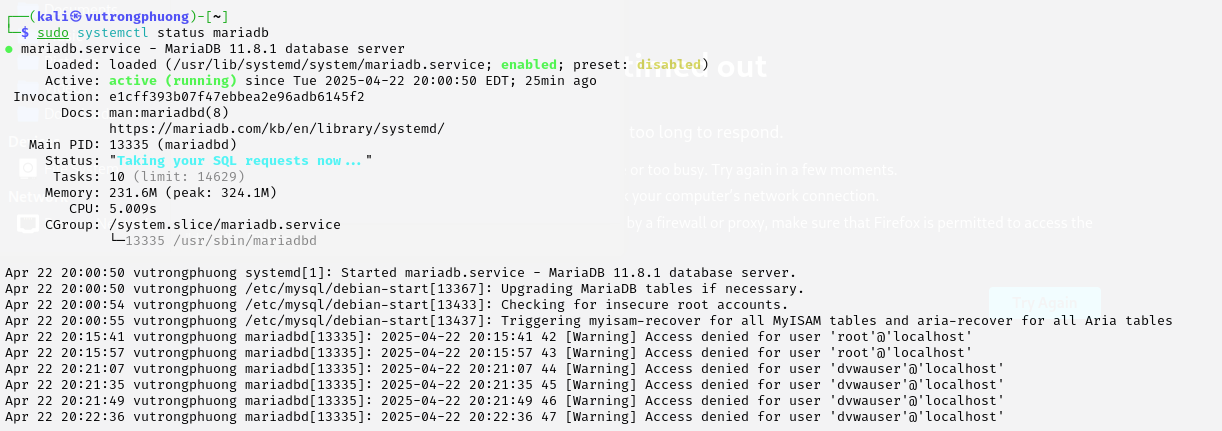
GRANT ALL PRIVILEGES ON dvwa.\* TO 'dvwauser'@'localhost' IDENTIFIED BY 'dvwapassword';

FLUSH PRIVILEGES;

EXIT;

Kiểm tra xem mariadb đã khởi động chưa:

sudo systemctl status mariadb



nhập lệnh

mysql -u root -p

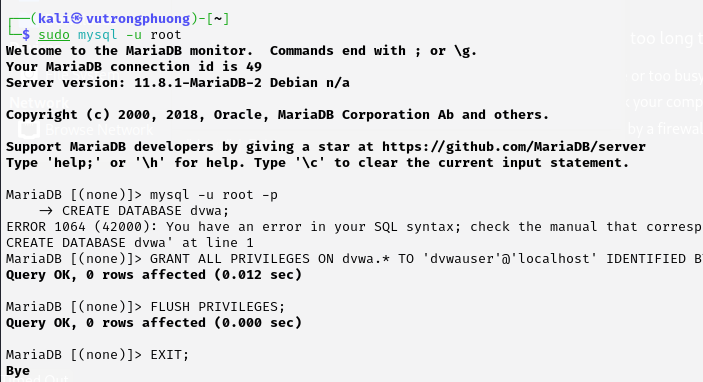
xong chạy từng dòng lệnh

CREATE DATABASE dvwa;

GRANT ALL PRIVILEGES ON dvwa.\* TO 'dvwauser'@'localhost' IDENTIFIED BY 'dvwapassword';

FLUSH PRIVILEGES;

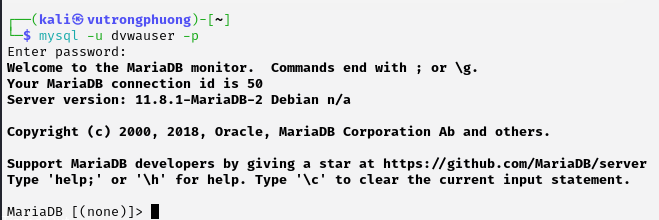
EXIT;



Kiểm tra người dùng dvwauser

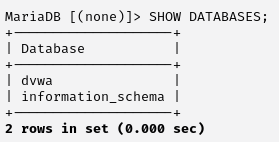
mysql -u dvwauser -p

Nhập mật khẩu: dvwapassword



Trong shell MariaDB, chạy

SHOW DATABASES;



* Bước 5: sửa nội dung file dvwa/config/config.inc.php

sudo nano /var/www/html/dvwa/config/config.inc.php.dist

Sao chép config.inc.php.dist thành config.inc.php:

sudo cp /var/www/html/dvwa/config/config.inc.php.dist /var/www/html/dvwa/config/config.inc.php

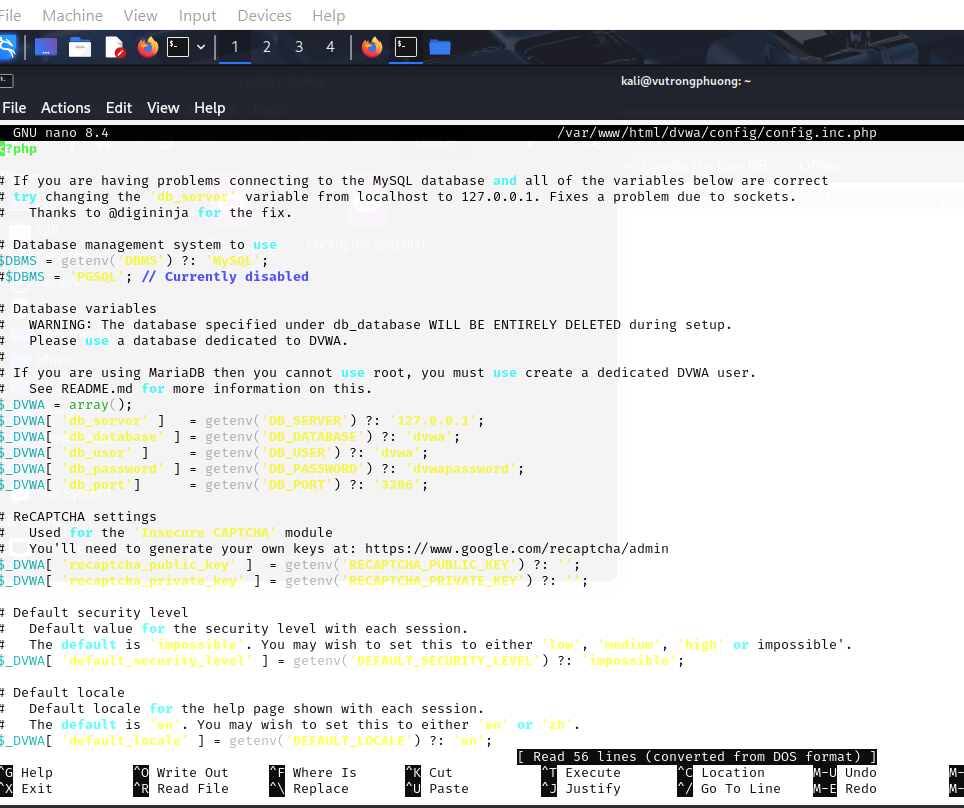
Đảm bảo file config.inc.php có quyền phù hợp:

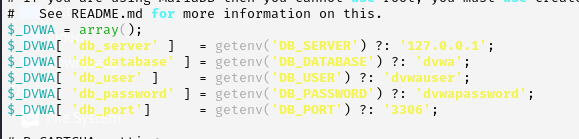
sudo chown www-data:www-data /var/www/html/dvwa/config/config.inc.php

sudo chmod 644 /var/www/html/dvwa/config/config.inc.php



Mở file để chỉnh sửa:  
sudo nano /var/www/html/dvwa/config/config.inc.php

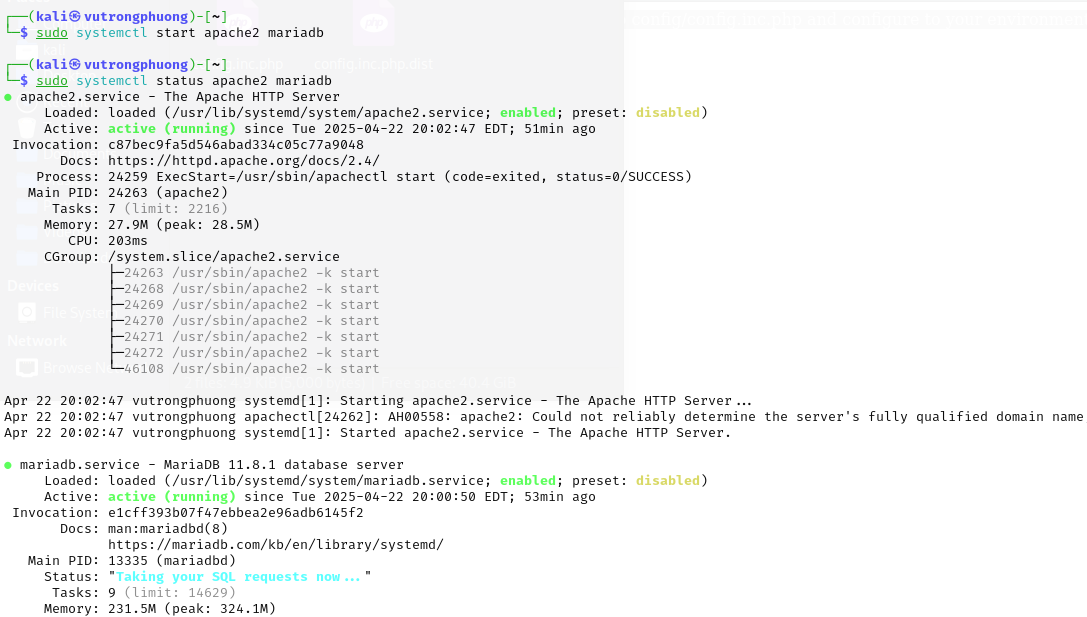




Khởi động marialDB  
với dòng lệnh:

sudo systemctl start apache2 mariadb

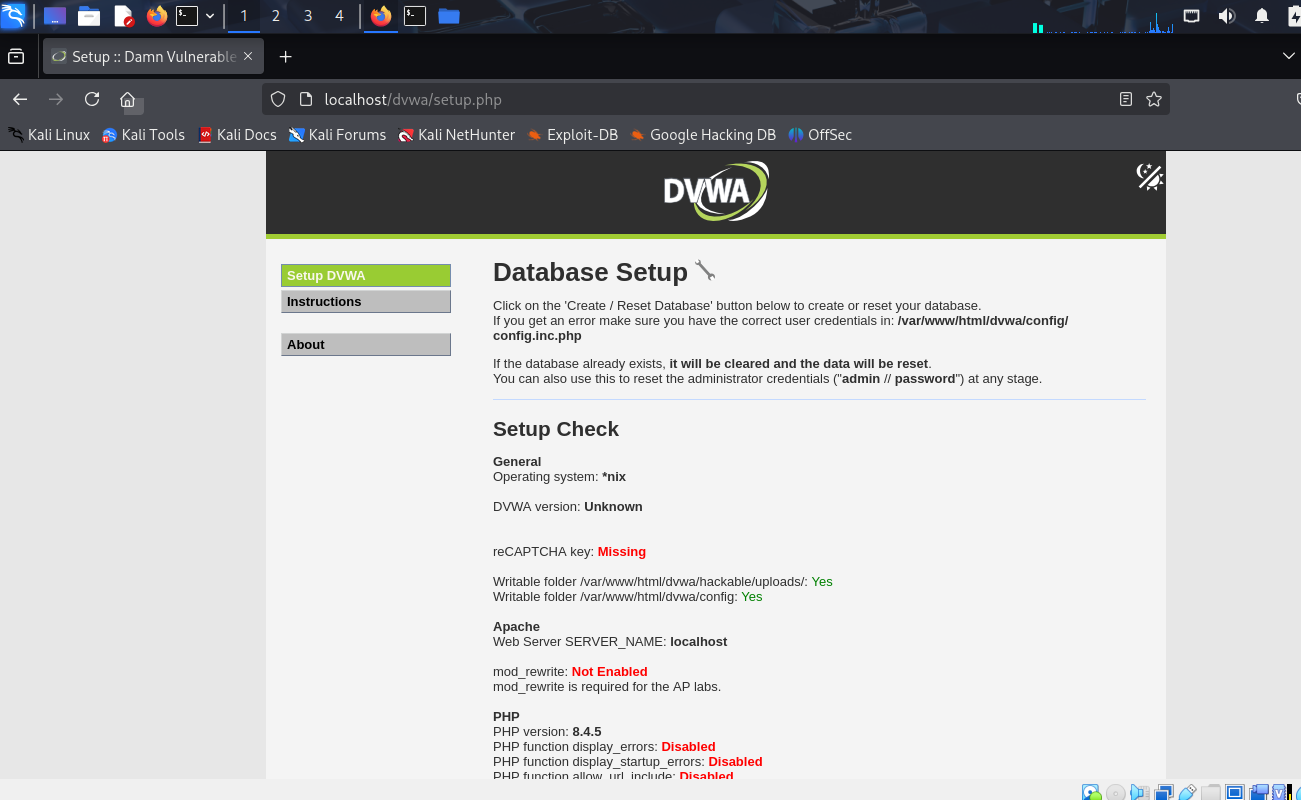
sudo systemctl status apache2 mariadb



Kiểm tra

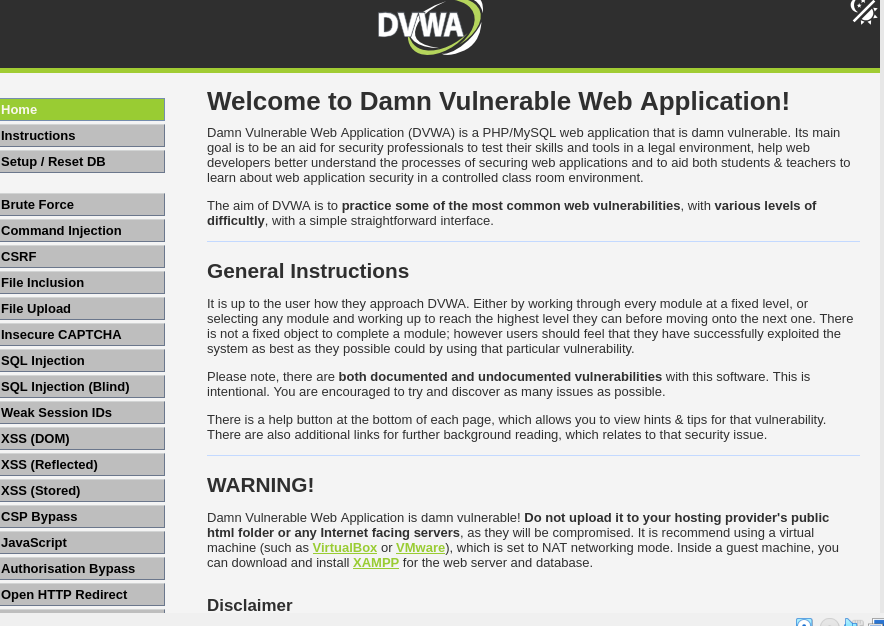
<http://localhost/dvwa/setup.php>

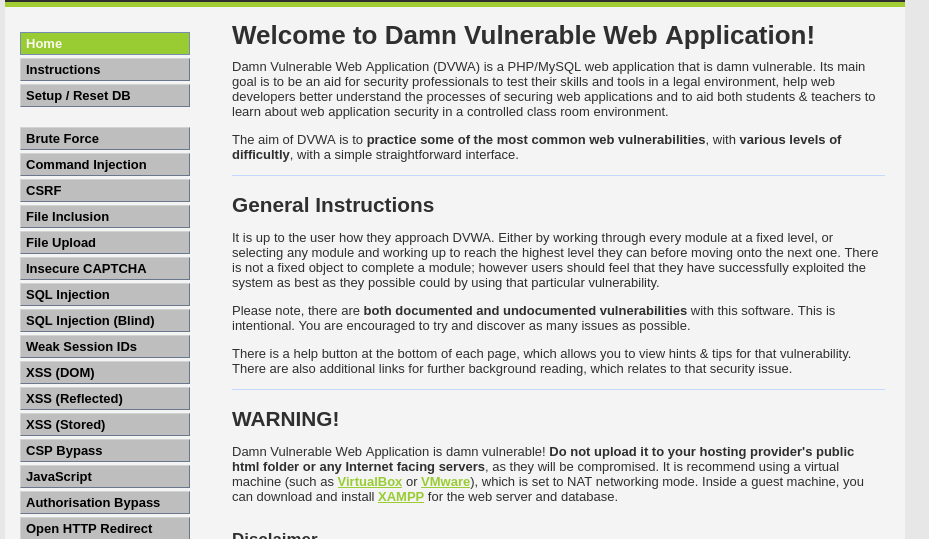
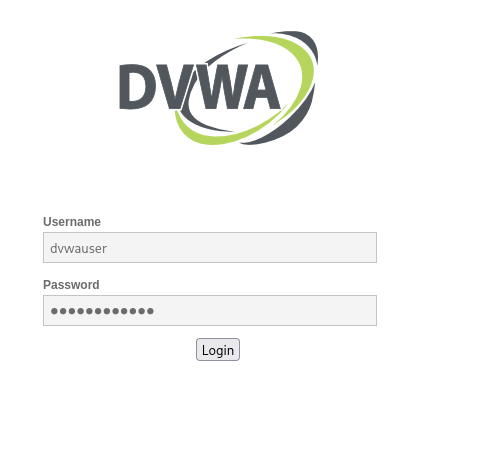
Nhấn nút **Create / Reset Database** để khởi tạo bảng và dữ liệu trong CSDL dvwa



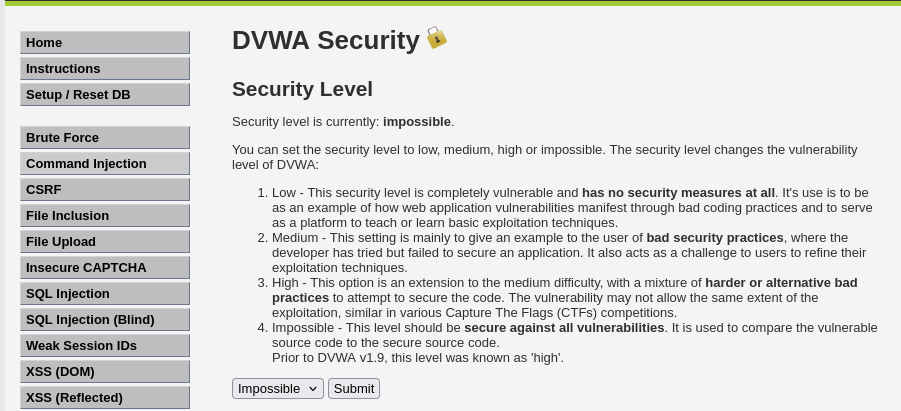
Đăng nhập với:

* **Username**: admin
* **Password**: password





Vào tab **DVWA Security**, chọn mức **Low**.





## **1.5 Kiểm thử lỗ hổng CSRF**

Download và tìm hiểu cách sử dụng công cụ kiểm thử CSRFTester tại địac chỉ: <https://www.owasp.org/index.php/Category:OWASP_CSRFTester_Project>

# **Tấn công XSS**

Truy cập vào website DVWA, chọn mục XSS(Reflected)



Bước 1: Nhập vào ô nhập liệu giá trị An chúng ta được kết quả như sau:



Như vậy có thể đoán được chức năng này hiển thị lời chào với tên người nhập vào

* Bước 2: Nhập vào ô nhập liệu giá trị <b>An</b> chúng ta được kết quả:

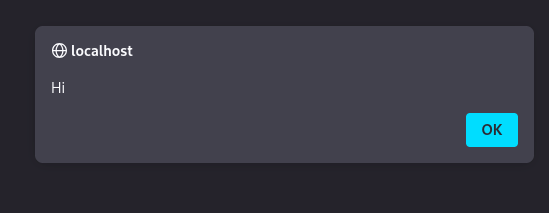


Tên người đã được in đậm cho thấy thẻ <b> đã được xử lý để hiện thị. Đây là cơ sở để nghi ngờ chức năng này có lỗ hổng XSS để khai thác.

* Bước 3: Nhập chuỗi <script> alert(“Hi”)</script> chúng ta sẽ thấy một hộp thoại cảnh báo được bật lên

nhập lệnh:

<script>alert("Hi")</script>



Như vậy có thể thấy, mã Javascript nhúng vào giá trị đầu vào đã được thực thi

Từ ví dụ này có thể kết luận 2 điều.

* Thứ nhất biến name có thể nhận giá trị đầu vào bất kỳ và truyền lên server xử lý.
* Thứ 2, server đã không kiểm soát giá trị đầu vào này trước khi trả về cho trình duyệt. Dẫn đến việc đoạn mã javascript đã bị chèn vào trong source code.

XSS nói chung được chia làm 3 loại chính là **Reflected, Stored và DOM based.**