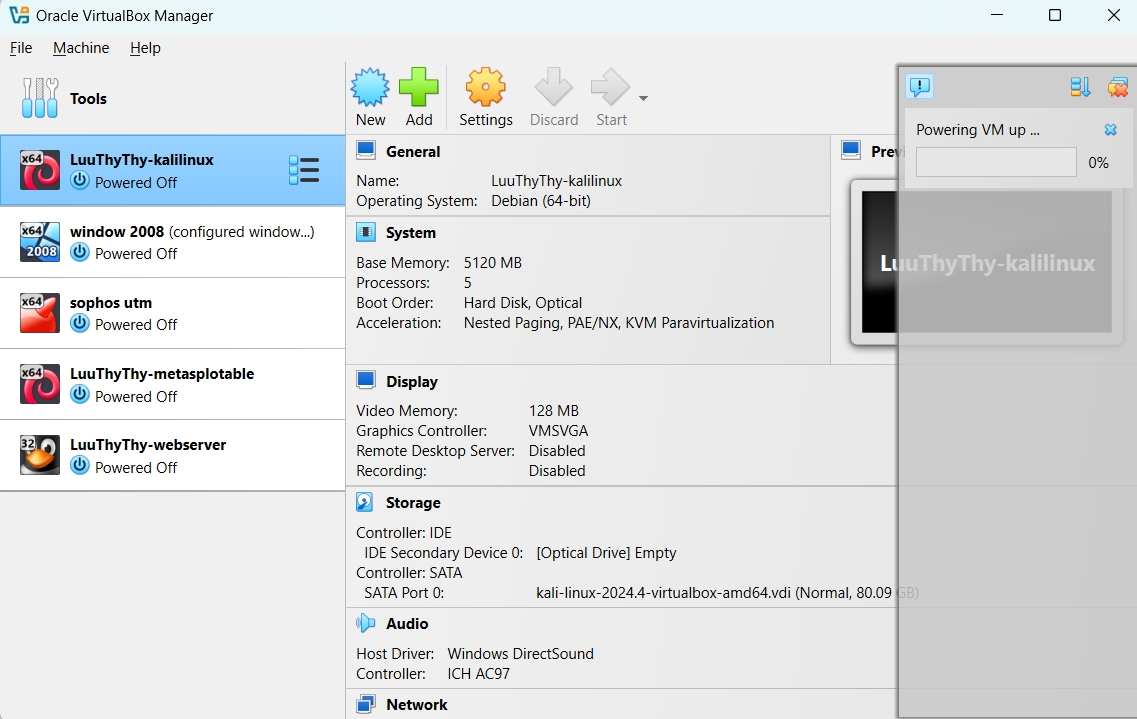
Lưu Thy Thy

1050080078

10ĐH\_CNPM1

**KIỂM THỬ LỖ HỔNG XSS và CSRF**

Khởi động máy ảo Kali linux



Cài đặt môi trường

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/>

Tải xuống DVWA

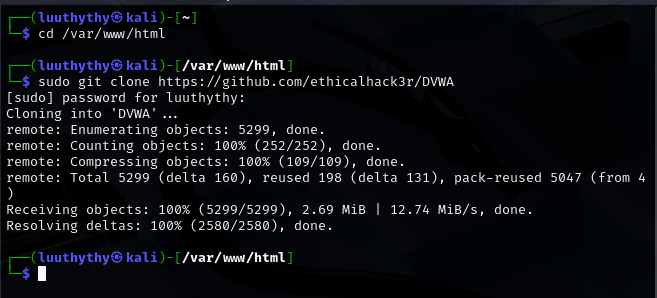
Đầu tiên, bạn cần clone DVWA GitHub vào thư mục /var/www/html, nơi lưu trữ các file Localhost trong hệ thống Linux. Để thực hiện, bạn mở terminal và chuyển đến thư mục /var/www/html bằng lệnh:

cd /var/www/html



Tiếp theo, bạn clone kho lưu trữ DVWA từ GitHub bằng lệnh:

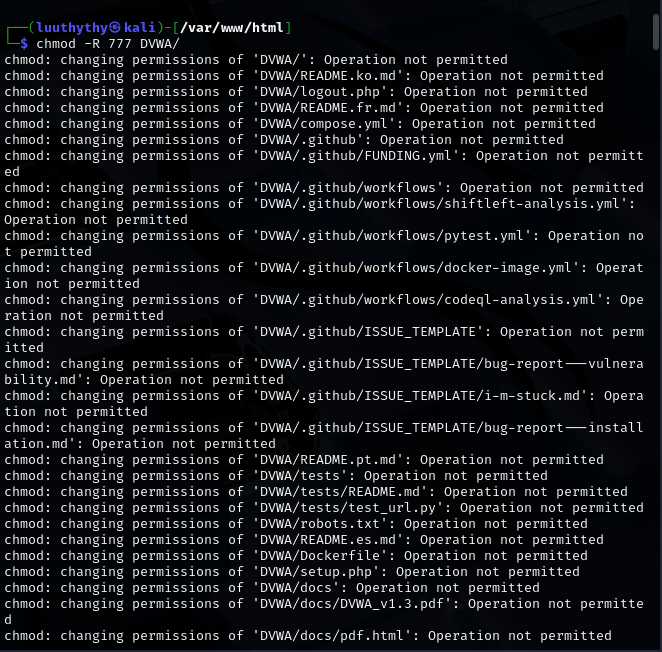
sudo git clone https://github.com/ethicalhack3r/DVWA



Cấu hình DVWA

Sau khi tải DVWA trong thư mục /var/www/html, bạn cần cấu hình một số thông tin, đầu tiên là quyền đọc, ghi và thực thi cho thư mục dvwa:

chmod -R 777 DVWA/

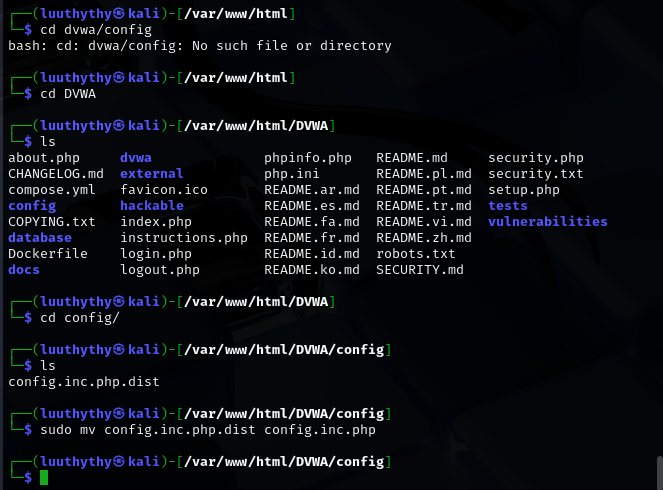


Tiếp theo, bạn cần thiết lập tên người dùng và mật khẩu để truy cập cơ sở dữ liệu. Chuyển đến thư mục **config** bằng lệnh sau:

cd dvwa/config

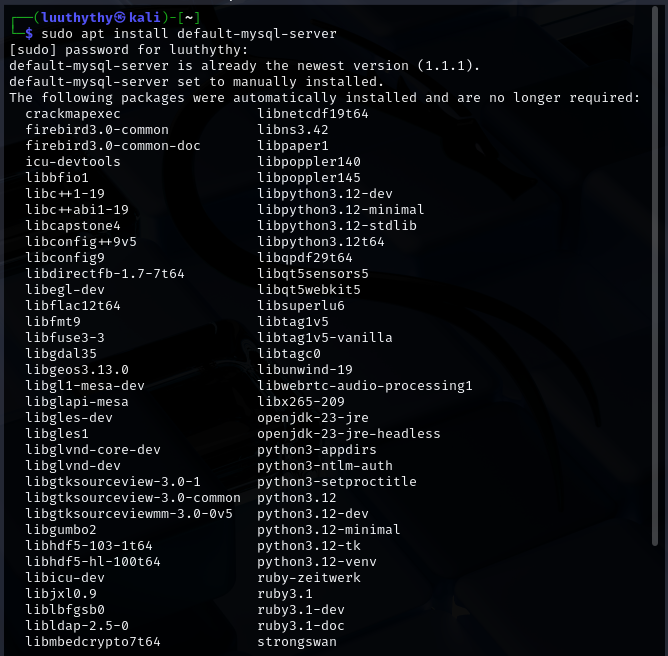
Sau khi chạy [lệnh ls](https://vietnix.vn/lenh-ls-trong-linux/) để xem các file bên trong thư mục, bạn sẽ thấy file gốc **config.inc.php.dist** chứa cấu hình mặc định. Bạn sẽ không chỉnh sửa file này mà giữ lại làm bản backup khi có sự cố, đồng thời tạo một bản sao file mới có tên **config.inc.php**:

sudo mv config.inc.php.dist config.inc.php



Cài đặt MySQL

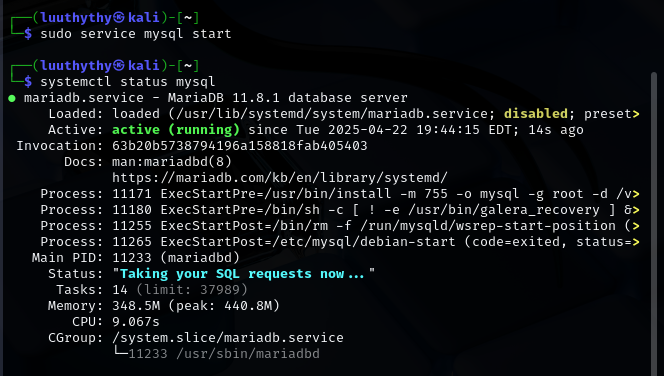
Sử dụng lệnh sau: sudo apt install default-mysql-server



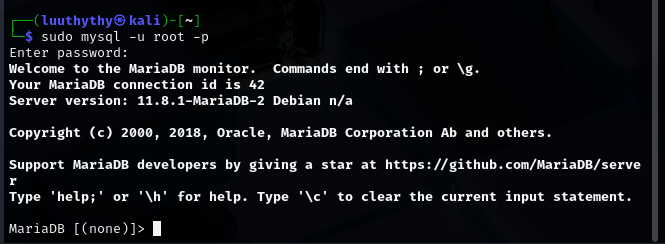
Cấu hình cơ sở dữ liệu MySQL

Để khởi động dịch vụ MySQL, bạn chạy lệnh: sudo service mysql start

Tiếp theo, bạn kiểm tra trạng thái dịch vụ có đang chạy hay không bằng lệnh: systemctl status mysql

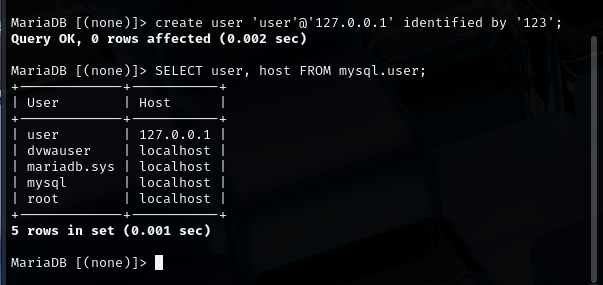


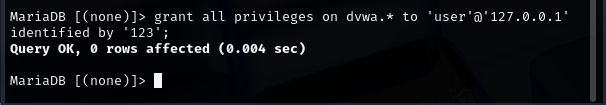
Bạn cần đăng nhập vào MySQL với quyền root (hoặc superuser nếu có) bằng lệnh: sudo mysql -u root -p



Sau đó, bạn cấp quyền cho người dùng mới này trên database dvwa bằng lệnh sau. Cuối cùng, bạn gõ exit để đóng cơ sở dữ liệu:

grant all privileges on dvwa.\* to 'user'@'127.0.0.1' identified by 'pass';





Cài đặt PHP

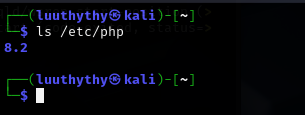
PHP thường được cài đặt sẵn trên Kali Linux, để kiểm tra phiên bản PHP dùng lệnh:

php -v

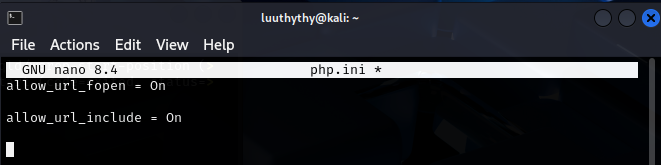


Cấu hình máy chủ Apache

Để cấu hình máy chủ Apache, đầu tiên bạn chạy lệnh sau : ls /etc/php



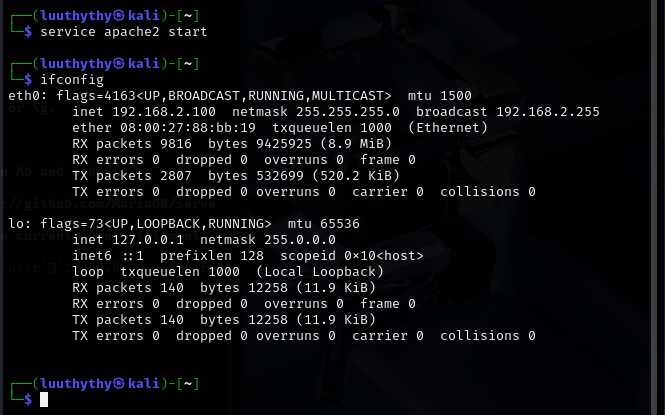
Trong thư mục /etc/php, khi bạn thực thi lệnh ls thì sẽ thấy file có tên php.ini. Bạn sẽ chỉnh sửa file này để cấu hình máy chủ localhost. Đầu tiên, mở file bằng trình soạn thảo nano với lệnh: sudo nano php.ini



Tiếp đó, bạn khởi động máy chủ Apache bằng lệnh:

service apache2 start

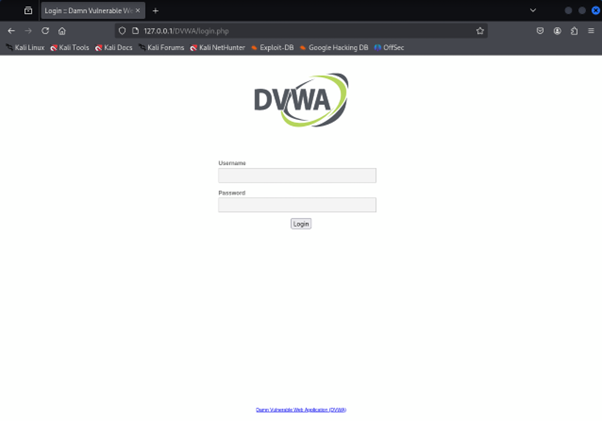
ifconfig



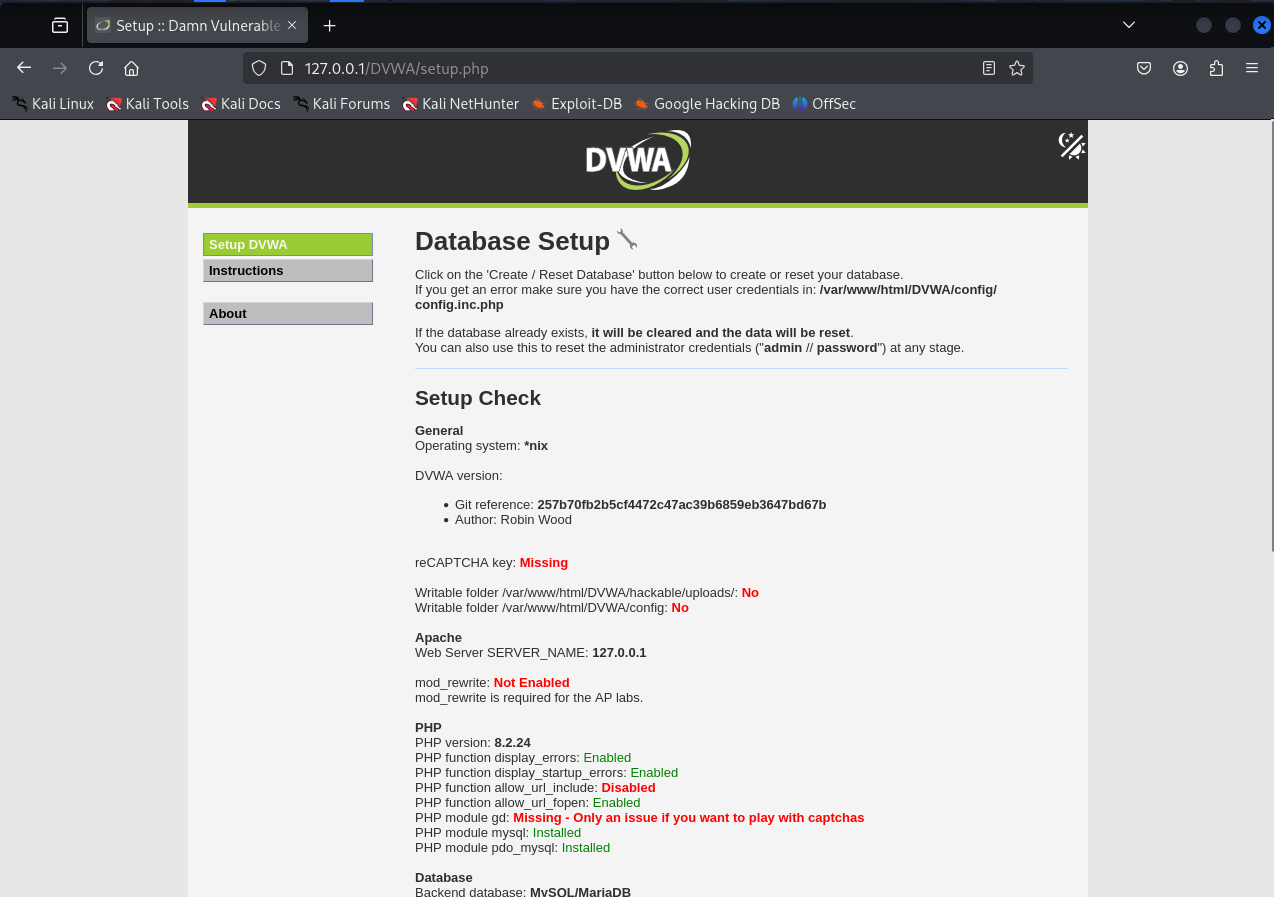
Truy cập DVWA trên trình duyệt

Sau khi hoàn tất cấu hình, bạn hãy mở trình duyệt web và nhập địa chỉ sau:

<http://127.0.0.1/DVWA/>



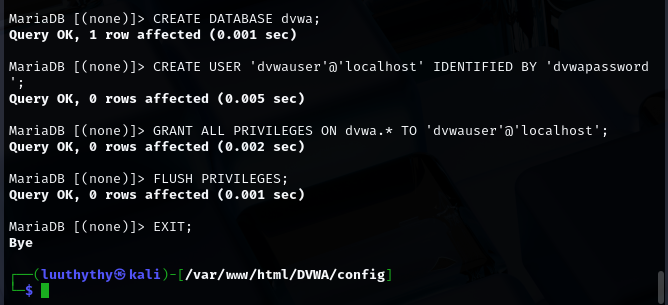
Đăng nhập tài khoản



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

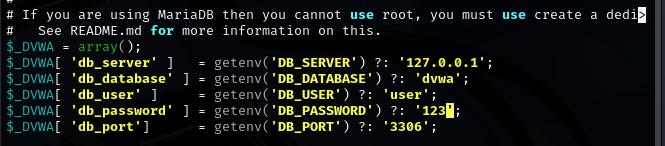
Bước 3: Sao chép thư mục sau khi đã giải nén vào thư mục webroot của Web Server

Bước 4: Tạo một CSDL có tên là “dvwa”

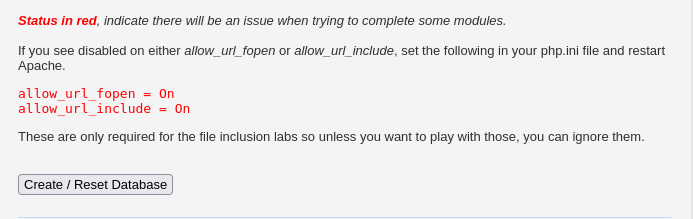


Bước 5: sửa nội dung file dvwa/config/config.inc.php

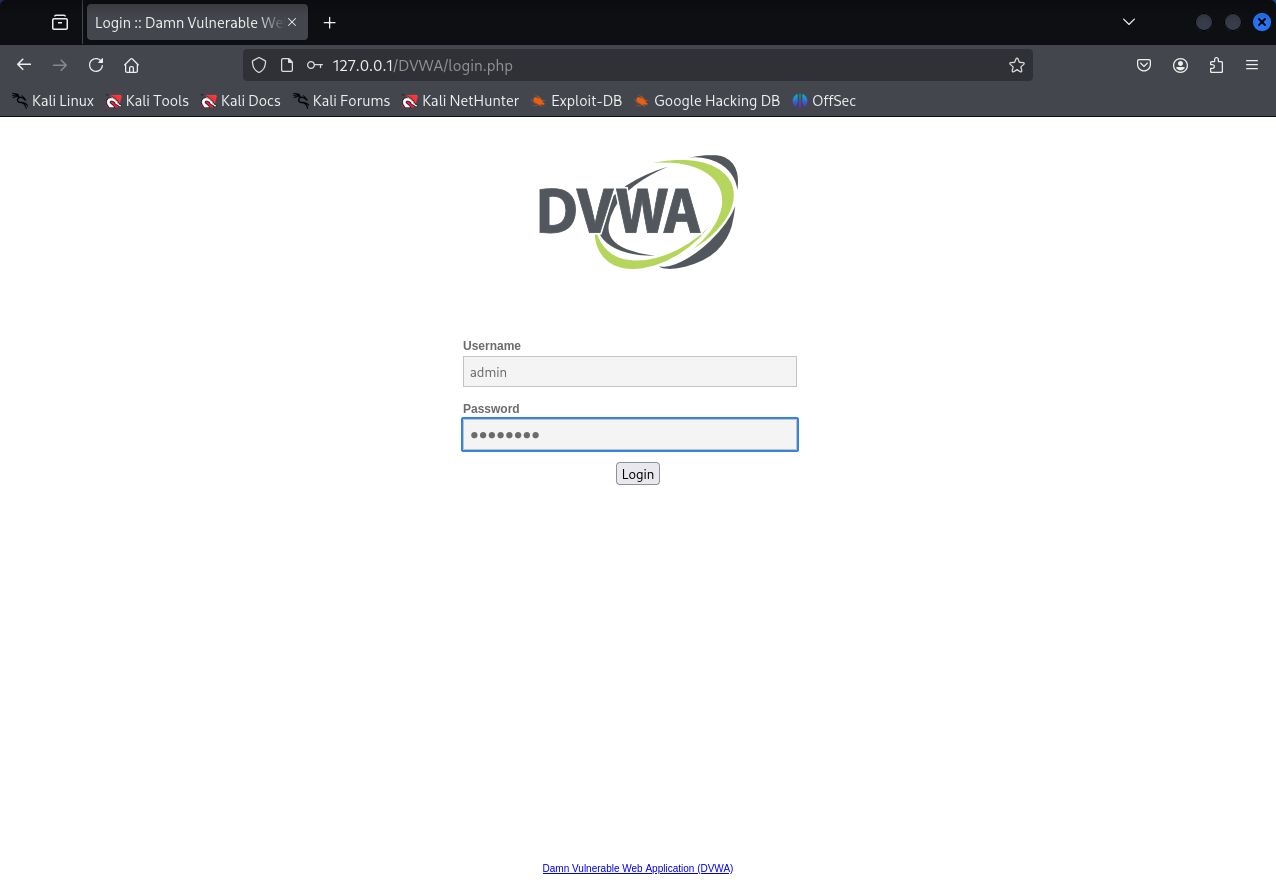




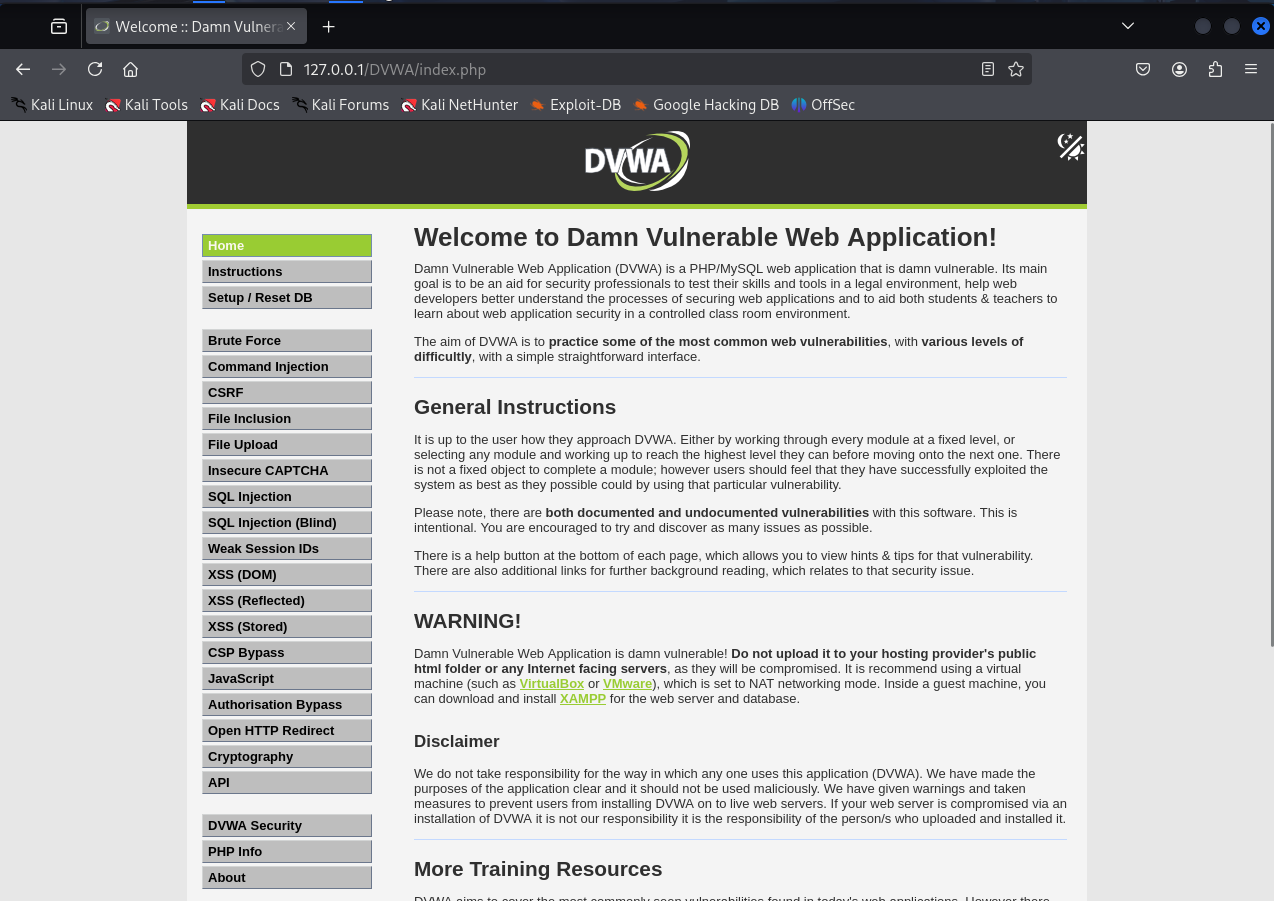
Bước 6: Mở trình duyệt và truy cập vào địa chỉ http://localhost/dvwa/setup.php và nhấp nút Create/Reset database



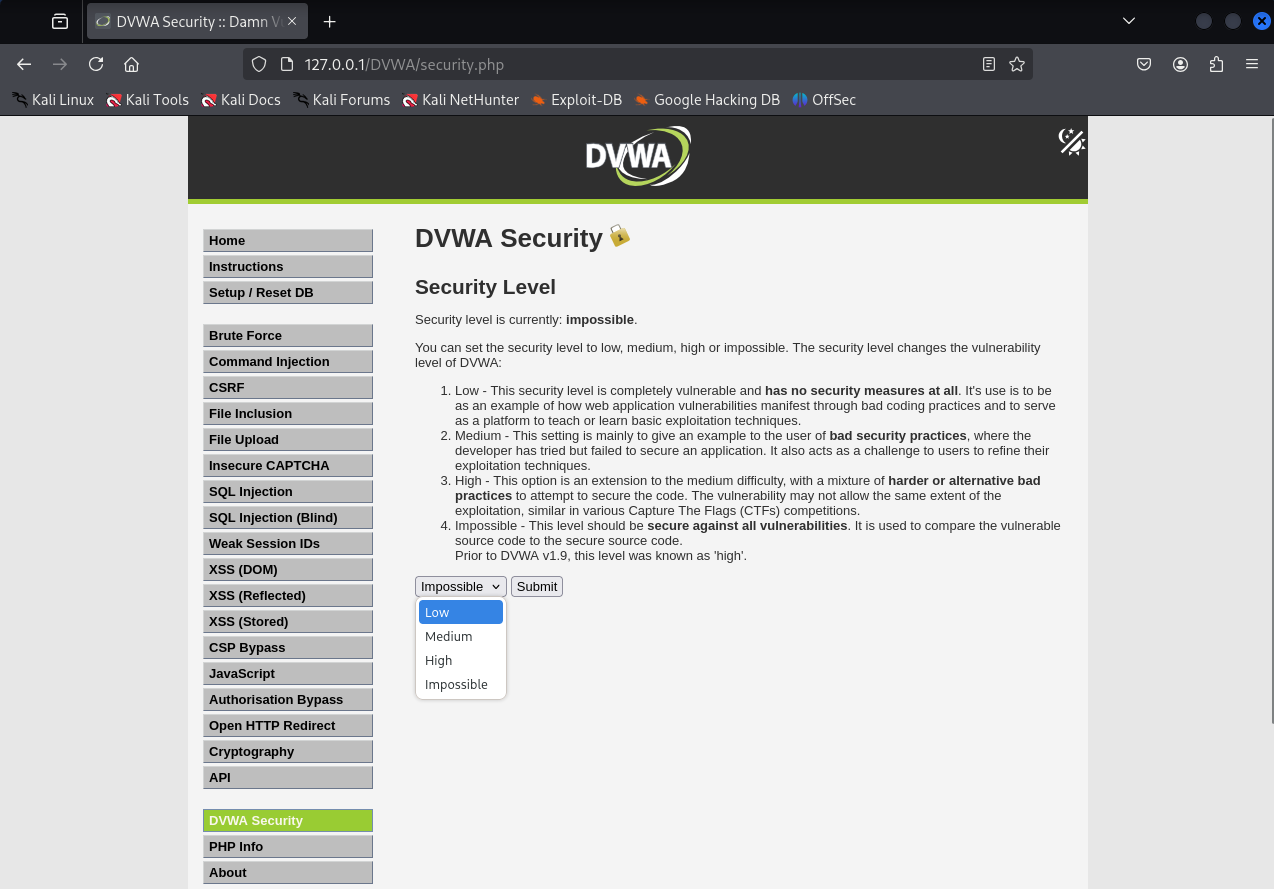
Bước 7: Sau khi cài đặt thành công, truy cập vào website tại địa chỉ http//localhost/dvwa với tài khoản là “admin” và mật khẩu là “password”

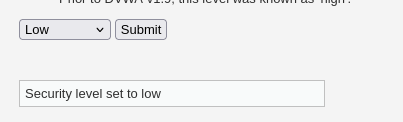


Sau khi đăng nhập, bạn sẽ thấy giao diện chính của DVWA. Tại menu bên trái, bạn có thể lựa chọn các kiểu tấn công khác nhau và tùy chỉnh mức độ bảo mật (Low, Medium, High hoặc Impossible) thông qua nút **DVWA Security**.

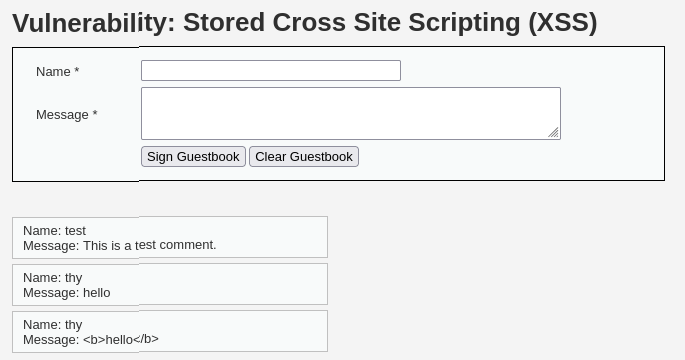


Bước 8: Thiết lập giá trị cho DVWA Security là “Low” để phần bắt đầu luyện tập dễ dàng hơn





Vào XSS (stored)



Nhập vào ô nhập liệu tên người là thy và thông điệp hello. Chúng ta được kết quả như sau:



Nhập vào ô nhập liệu tên người là An và thông <b>hello</b>. Chúng ta được kết quả như sau:

