**Họ và tên: Nguyễn Hữu Anh Vinh**

**Lớp:CNPM2**

**MSSV:1050080168**

**Link youtube:** [**https://www.youtube.com/channel/UCvZTAl1FW3igMEgHxoarqWg**](https://www.youtube.com/channel/UCvZTAl1FW3igMEgHxoarqWg)

**Link github:** [**https://github.com/vinhahihu/java777**](https://github.com/vinhahihu/java777)

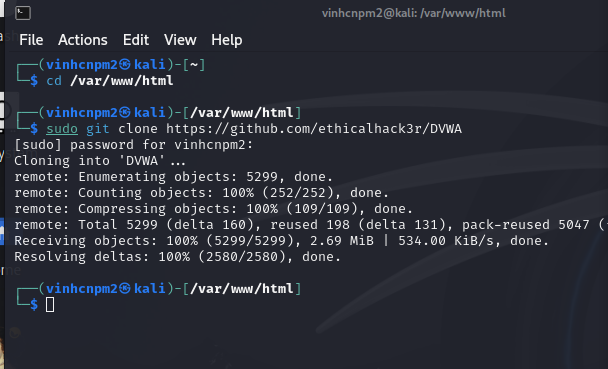
BÀI THỰC HÀNH SỐ 9

KIỂM THỬ LỖ HỔNG XSS và CSRF

1.4 Cài đặt môi trường luyện tập

**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. Để thực hiện, bạn mở terminal và chuyển đến thư mục /var/www/html bằng lệnh:



**Bước 2: Cấu hình DVWA**

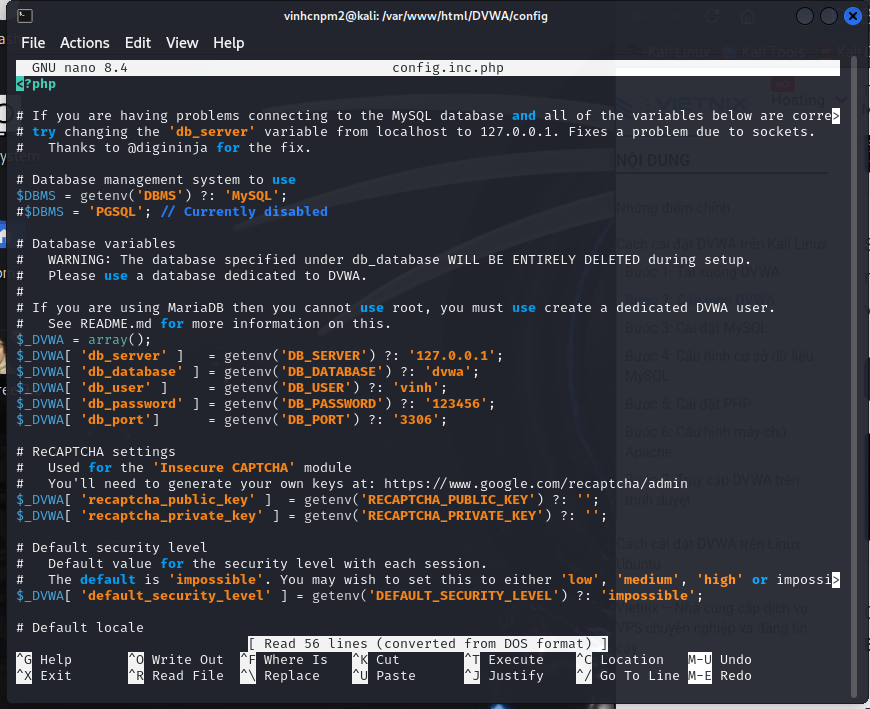
Sau khi tải DVWA trong thư mục /var/www/html, bạn cần cấu hình một số thông tin, đầu tiên là quyền đọc, ghi và thực thi cho thư mục dvwa:

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



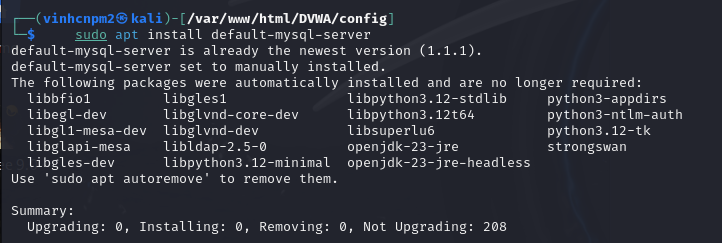
mở file **config.inc.php** mới này bằng trình soạn thảo nano và thay đổi các giá trị **db\_user**, **db\_password** thành tên user và mật khẩu tùy chọn:



**Bước 3: Cài đặt MySQL**

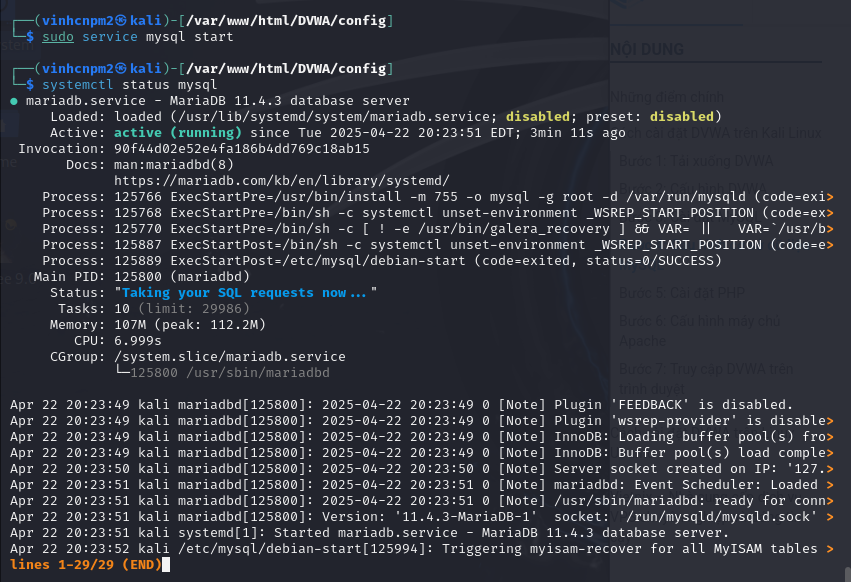
Thông thường, MySQL đã được cài đặt sẵn trên [Kali Linux](https://vietnix.vn/kali-linux-la-gi/). Tuy nhiên nếu chưa cài đặt hoặc gặp sự cố với MySQL, bạn có thể tự cài đặt thủ công. Trên các hệ thống dựa trên Debian có 2 để bạn lựa chọn là: mysql-server và mysql-client. Trong trường hợp này, bạn sẽ cần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

****

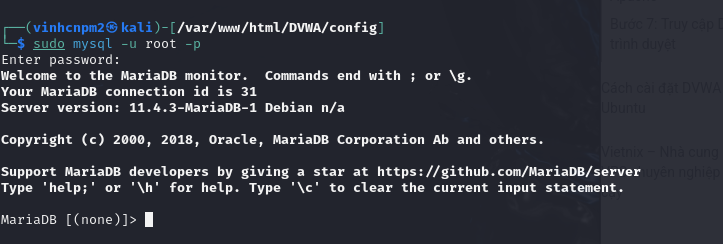
**Bước 4: Cấu hình cơ sở dữ liệu MySQL**

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

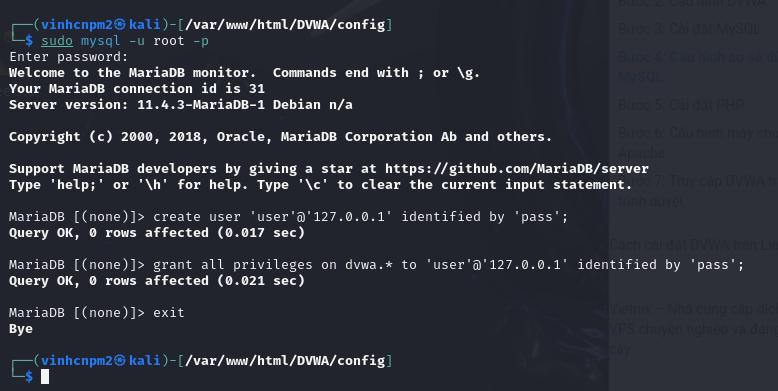
****

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

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:

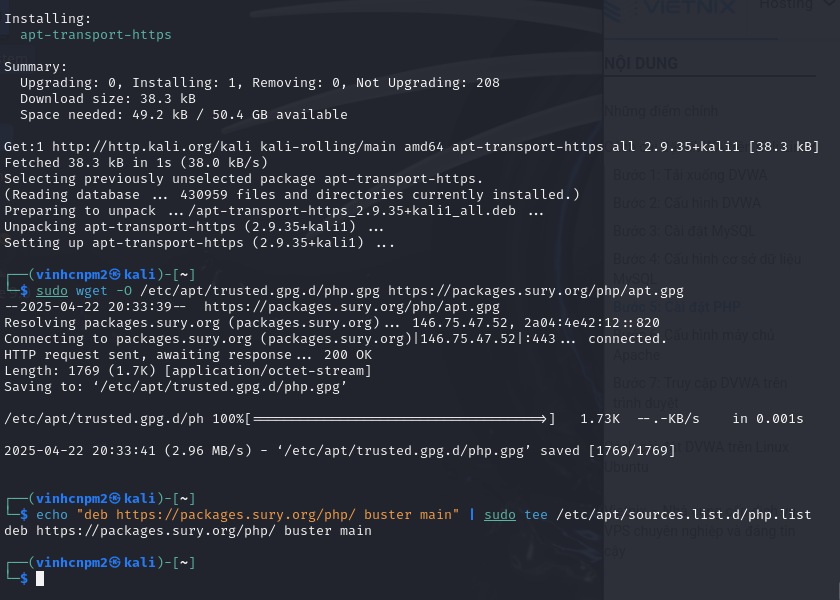
****

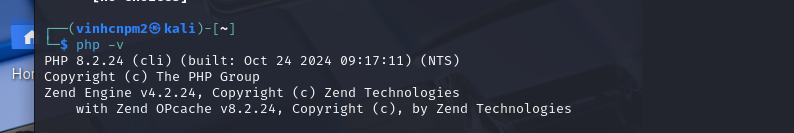
Tiếp theo, bạn tạo user mới với tên người dùng và mật khẩu tương tự như trong file cấu hình DVWA (trong bài viết này mình đặt là user và pass). Máy chủ đang được mình sử dụng là Localhost (127.0.0.1). Lệnh cuối cùng sẽ tương tự như sau:



**Bước 5: Cài đặt PHP**

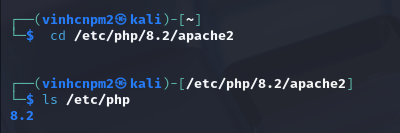
PHP thường được cài đặt sẵn trên Kali Linux. Nếu bạn muốn cài đặt phiên bản cụ thể (ví dụ PHP 7.4), hãy làm theo hướng dẫn sau. Đầu tiên, bạn cần cập nhật hệ thống và thêm kho lưu trữ SURY PHP PPA:





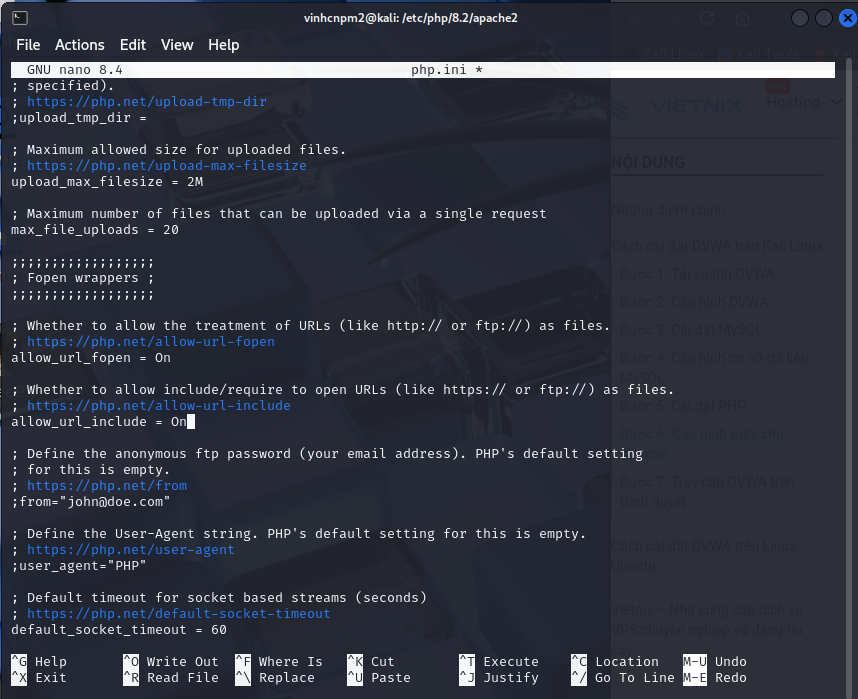
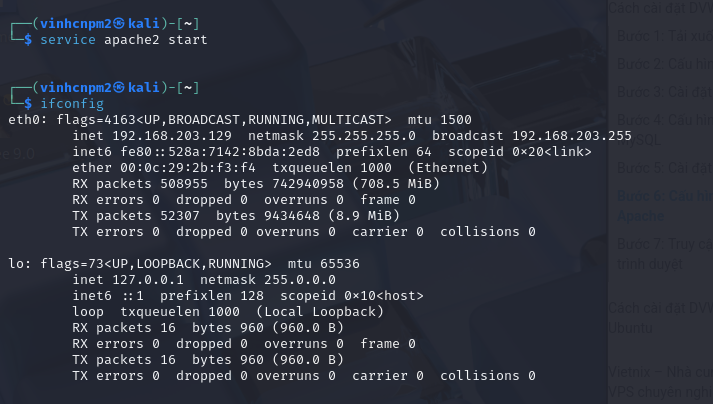
**Bước 6: Cấu hình máy chủ Apache**

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):



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:

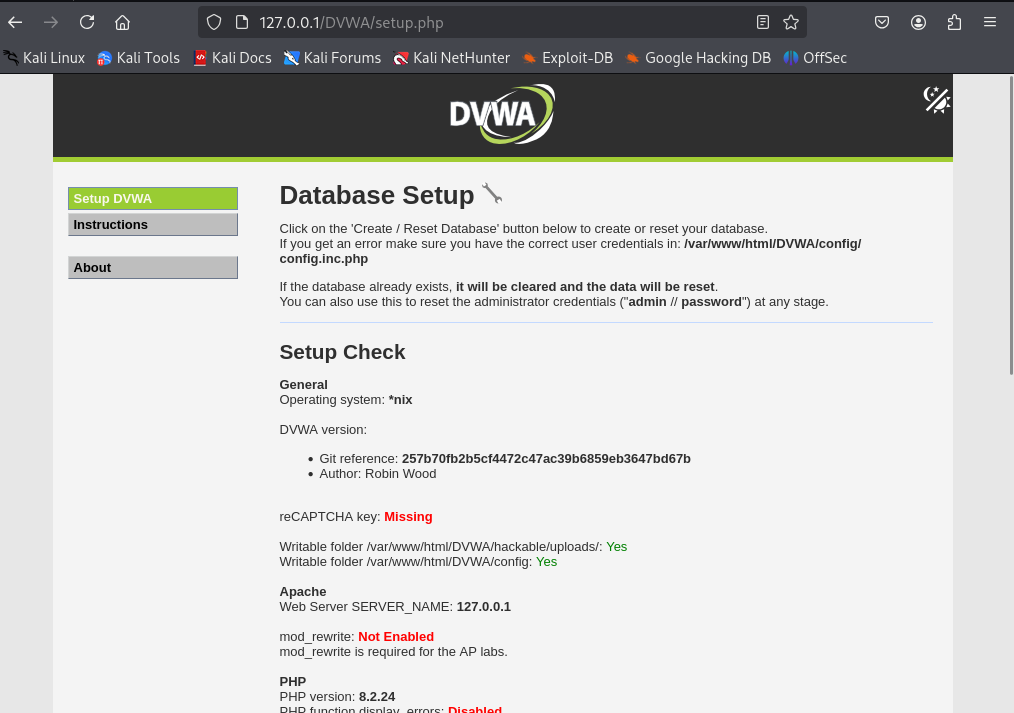
Bạn tìm dòng **allow\_url\_fopen** và **allow\_url\_include** rồi thiết lập giá trị thành **On**. Sau đó, bạn lưu file bằng cách bấm **Ctrl + O** rồi **Enter** và thoát file bằng **Ctrl + X**.

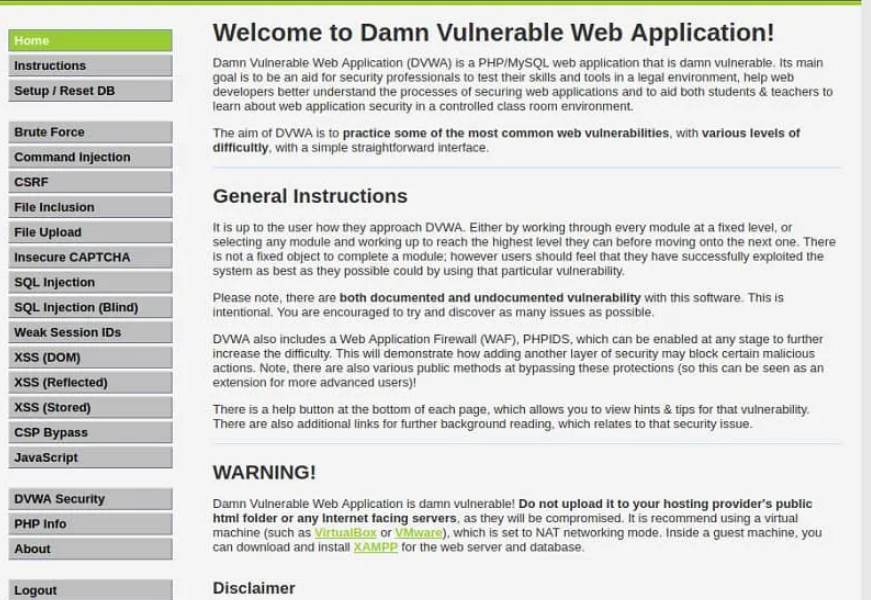
  **Bước 7: Truy cập DVWA trên trình duyệt**

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

<http://127.0.0.1/DVWA/>

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

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**.

2 Tấn công XSS

2.1 Giới thiệu

Cross-Site Scripting (XSS, không gọi là tắt là CSS để tránh nhầm lẫn với khái niệm Cascading Style

Sheet của HTML) là một trong những kĩ thuật tấn công phổ biến nhất hiện nay, được mệnh danh

là Godfather of Attack, và trong nhiều năm liền được liệt vào danh sách những kỹ thuật tấn công nguy hiểm nhất với ứng dụng web.

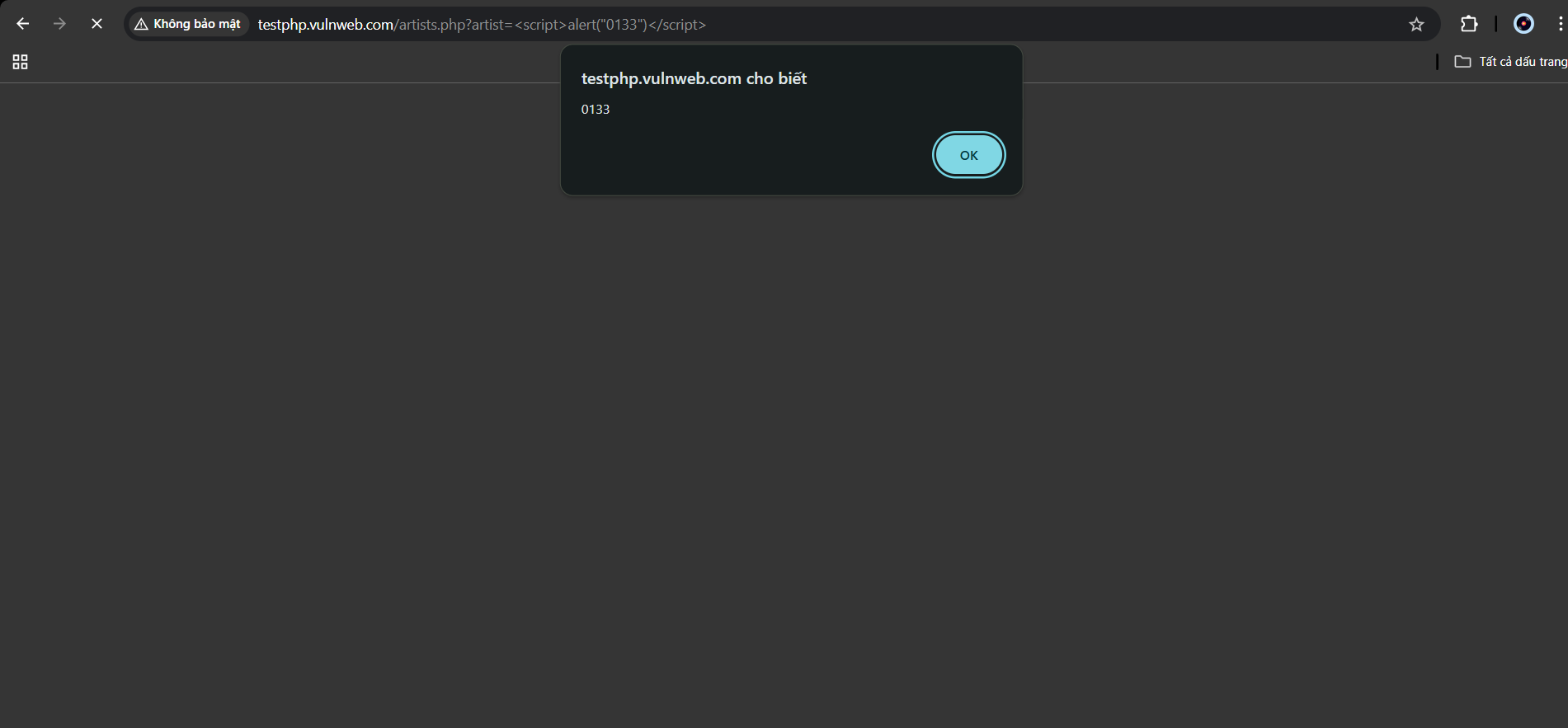
Kỹ thuật XSS được thực hiện dựa trên việc chèn các đoạn script nguy hiểm vào trong source code ứng

dụng web. Nhằm thực thi các đoạn mã độc Javascript để chiếm phiên đăng nhập của người dùng. Để hiểu rõ hơn, chúng ta xét ví dụ sau:

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

**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: **Là artist**

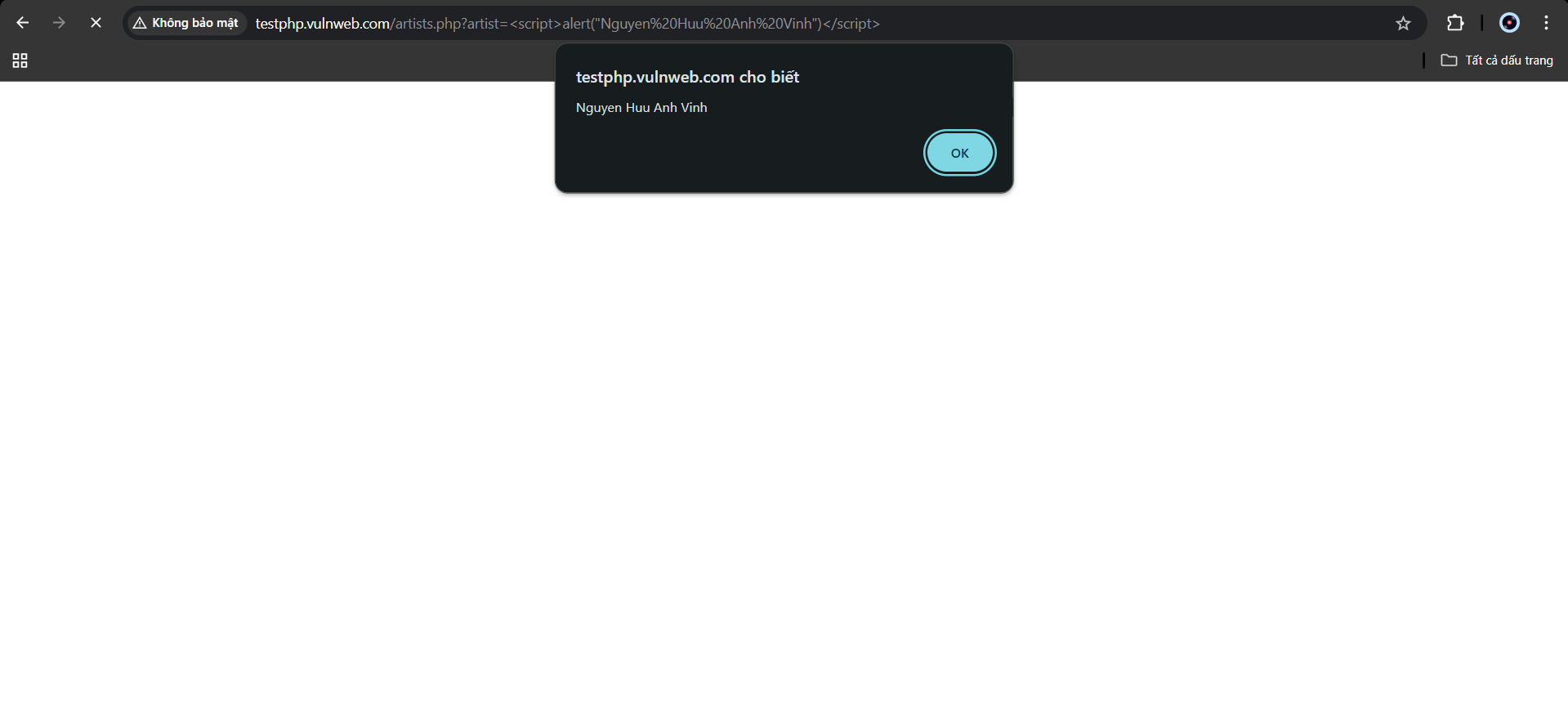
- Xác định giá trị đầu vào xuất hiện trong trang kết quả: **0.25 điểm**

**Là   <script>alert("0133")</script>**

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

* Truy cập trang có tham số artist

**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: **0.25 điểm**
* 
* **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: **0.25 điểm**

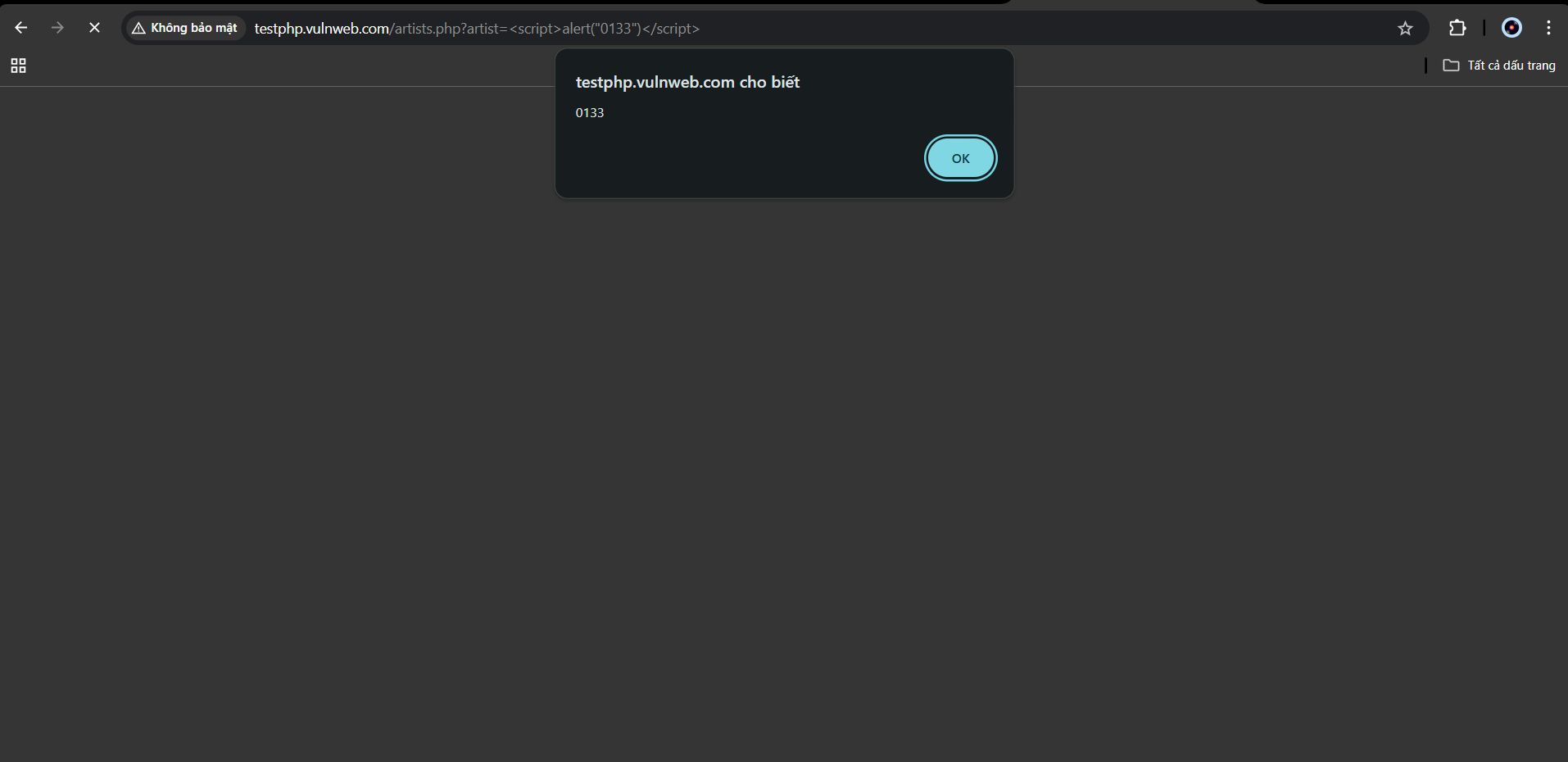
Tham số artist trong URL:

http://testphp.vulnweb.com/artists.php?artist=...

- Xác định giá trị đầu vào xuất hiện trong trang kết quả: **0.25 điểm**

**<script>alert("0133")</script>**

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



1. Truy cập trang:**http://testphp.vulnweb.com/artists.php?artist=1**
2. Thay giá trị artist=1 bằng:**artist=<script>alert("0133")</script>**
3. Trình duyệt hiện popup "0133" → xác nhận server phản hồi lại dữ liệu chưa kiểm soát đầu vào
4. Phán đoán: Do dữ liệu không được lọc → trình duyệt hiểu mã script → lỗi Reflected XSS

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

* Giá trị kiểm thử:

**<script>alert("0133")</script>**

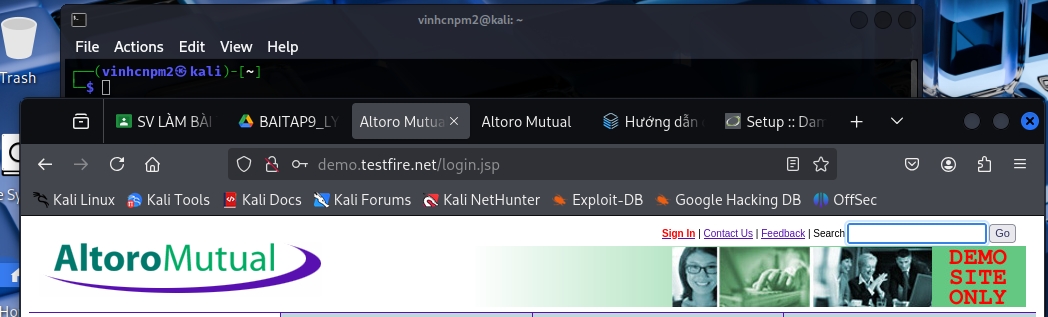
* Giải thích: Đây là đoạn mã JavaScript đơn giản dùng để kiểm tra lỗ hổng XSS. Nếu trình duyệt chạy lệnh alert("0133"), chứng tỏ server không xử lý đúng dữ liệu đầu vào, dẫn tới lỗ hổng Reflected XSS. Hacker có thể thay đoạn alert("0133") bằng các đoạn script độc hại như đánh cắp cookie, chiếm quyền điều khiển tài khoản...

**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/)

Truy cập website kiểm thử:



Đăng nhập vào tài khoản demo

Phân tích hành vi có thể khai thác

