BÀI THỰC HÀNH SỐ 9

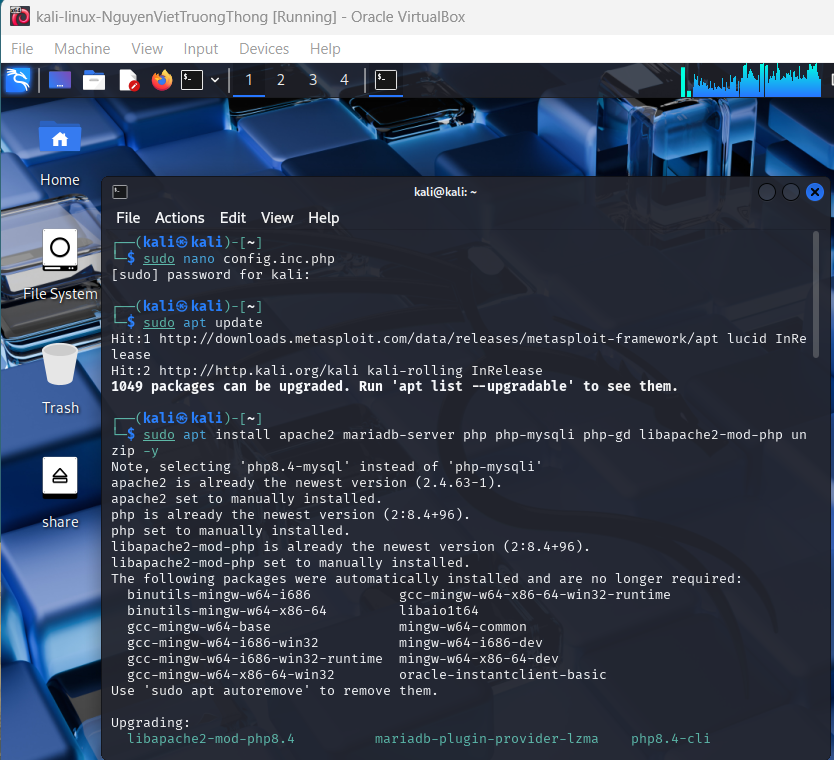
KIỂM THỬ LỖ HỔNG XSS và CSRF

Họ và tên: Nguyễn Việt Trường Thông

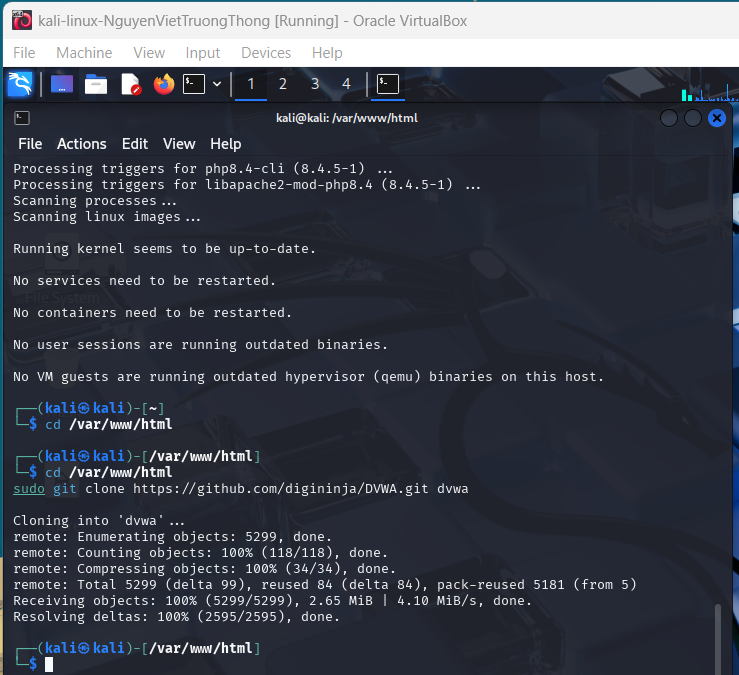
1.Cài đặt Apache, PHP, MySQL

sudo apt update

sudo apt install apache2 mariadb-server php php-mysqli php-gd libapache2-mod-php unzip -y



Cài DVWA

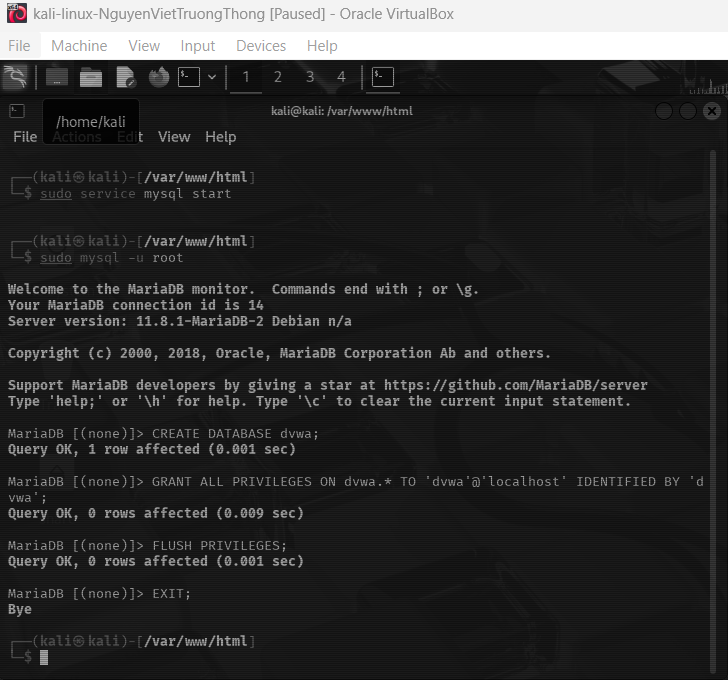


Giải nén thư mục

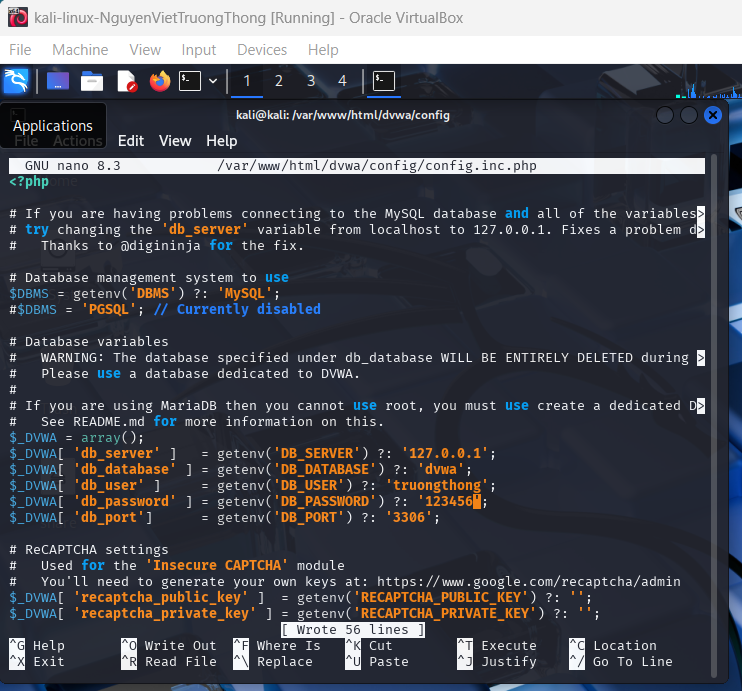
sudo unzip master.zip

sudo mv DVWA-master dvwa

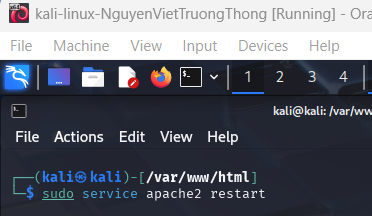
Cấu hình csdl MariaDB



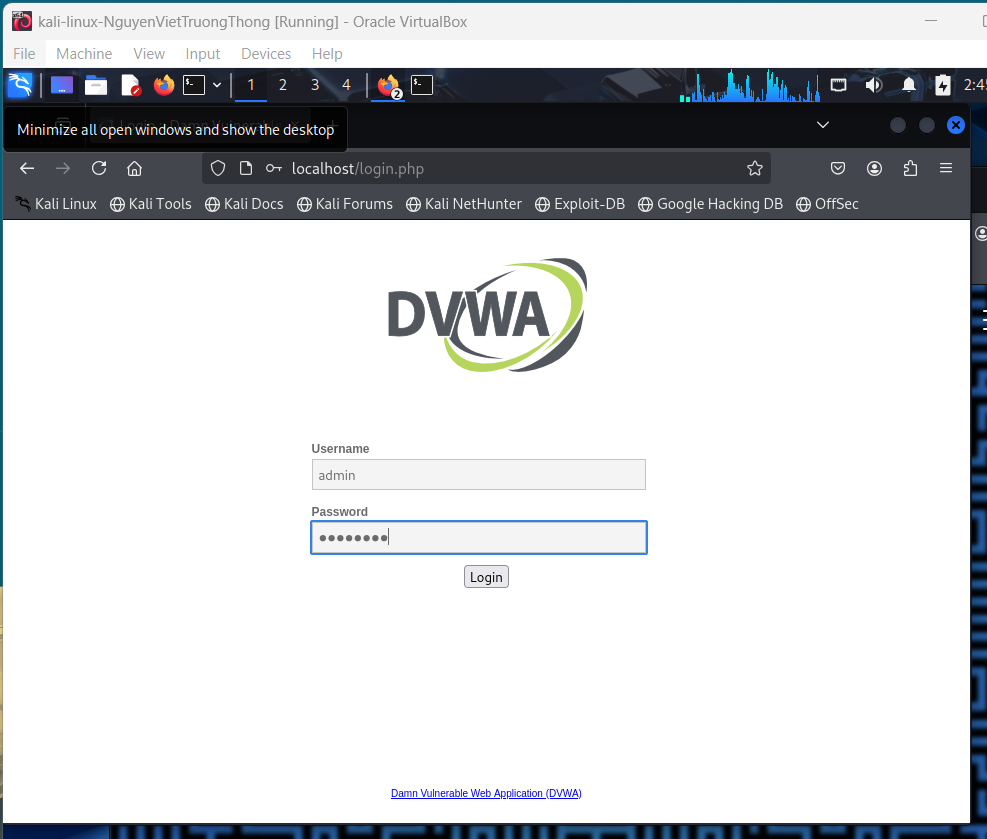
Cấu hình DVWA



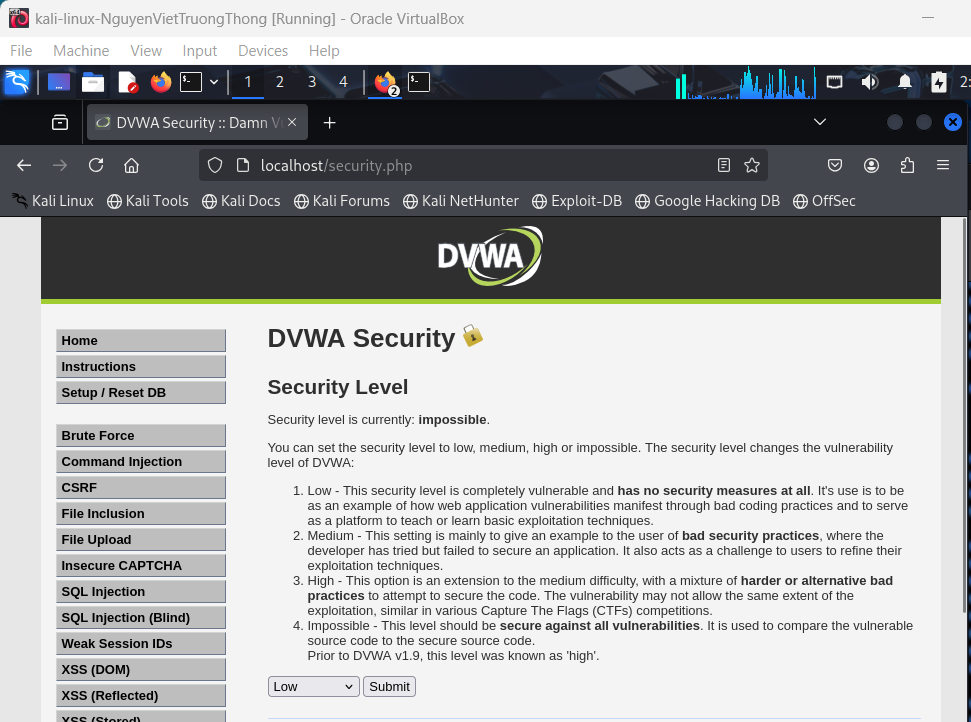
Chạy Apache và cấu hình PHP



Truy cập DVWA



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



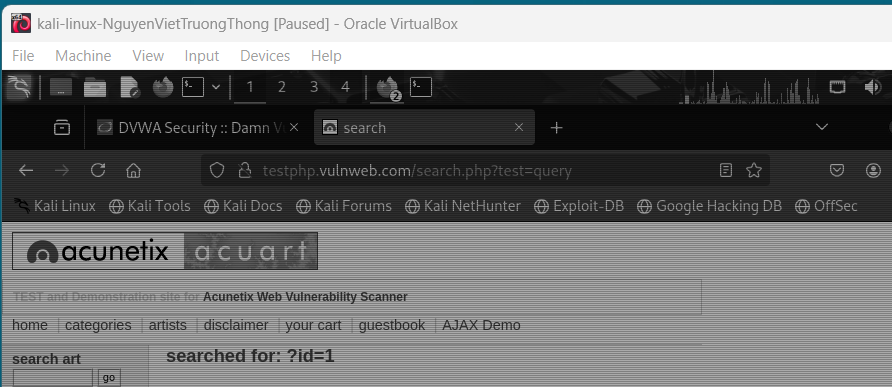
**Câu 1**

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: 0.25 điểm

Tìm kiếm các chức năng có thể nhập dữ liệu, ví dụ: ô tìm kiếm, ô đăng nhập, form liên hệ, URL có tham số GET (?id=1, ?search=abc, v.v.).

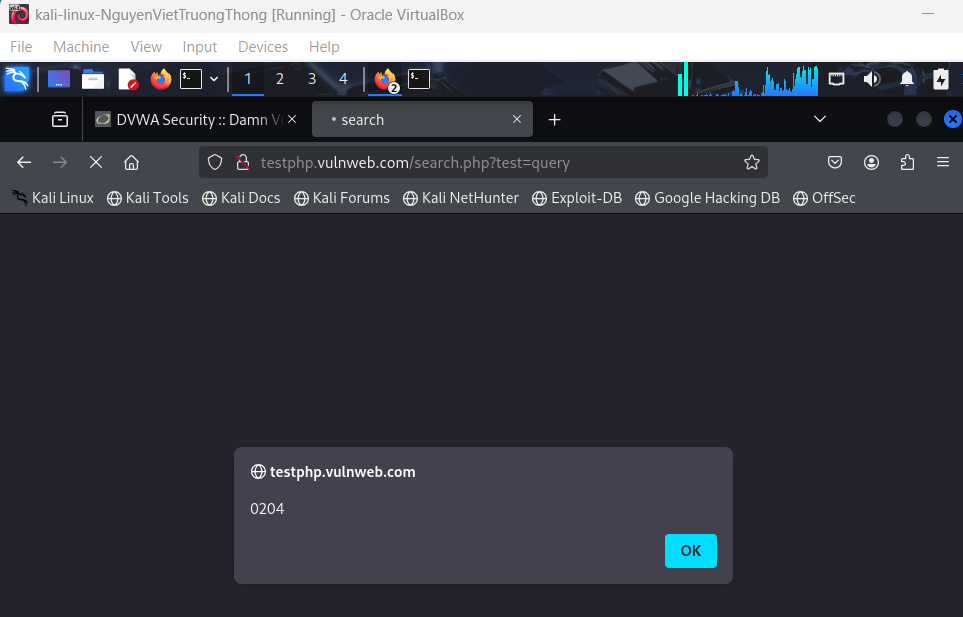


- Xác định giá trị đầu vào xuất hiện trong trang kết quả: 0.25 điểm

Khi nhập giá trị ?id=1 vào form tìm kiếm, kết quả trả về có chứa nội dung nhập > bằng giá trị đầu vào được phản hồi lại trong trang

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

[<script>alert('0204')</script](http://testphp.vulnweb.com/artists.php?artist=%3cscript%3ealert('0204')%3c/script)>



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

Nếu popup alert hiển ra với nội dung 0204 🡪 lỗ hỗng XSS tồn tại

* Chứng tỏ dữ liệu nhập không được lọc trước khi hiển thị lại

**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

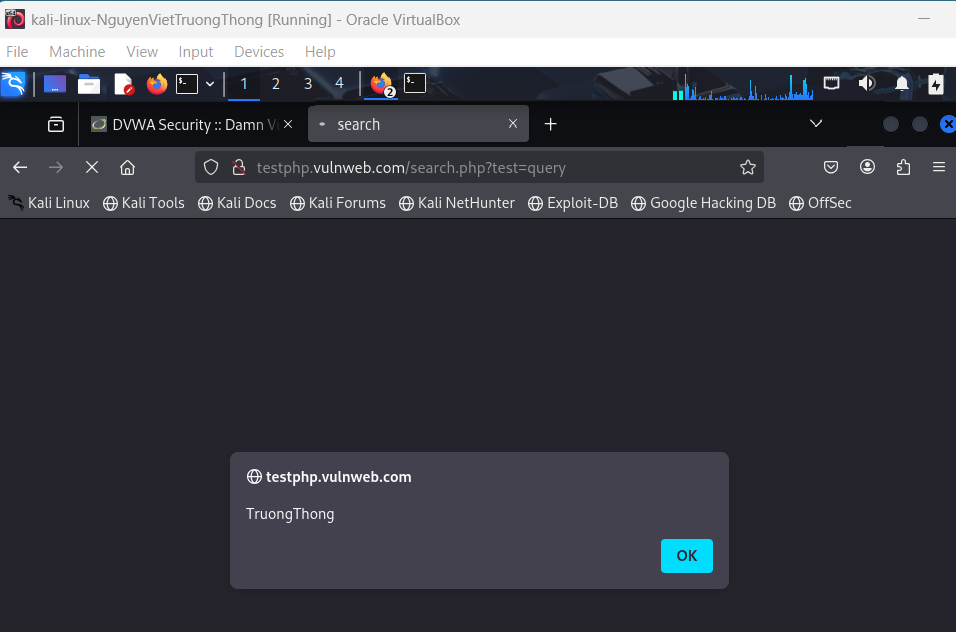
Cũng là trường tìm kiếm ( search ) như trên khi tìm MSSV 0204

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

Nhập vào sẽ hiển thị kết quả

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

[<script>alert('TruongThong')</script](http://testphp.vulnweb.com/artists.php?artist=%3cscript%3ealert('0204')%3c/script)>



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

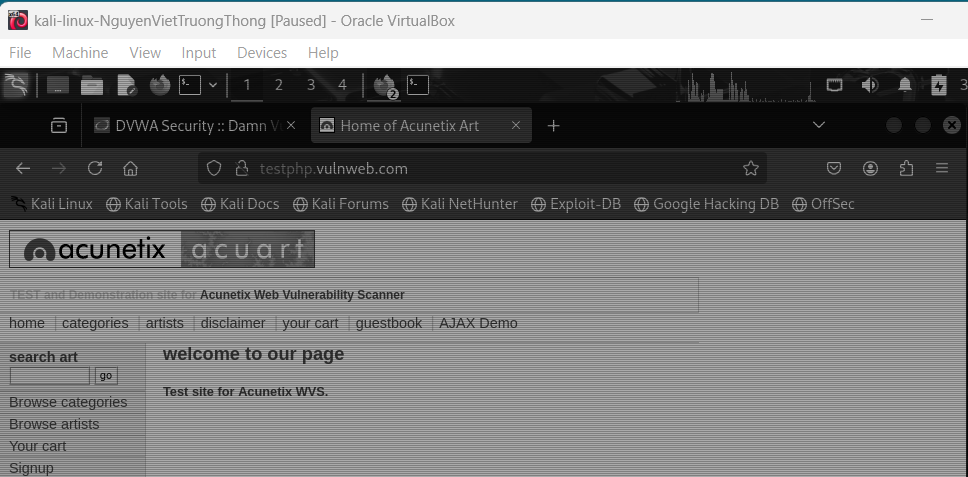
Popup hiển ra với nội dung là TruongThong thì lỗ hỏng tồn tại lỗi XSS

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

Bước 1 : Chọn web <http://testphp.vulnweb.com>

Dò tìm chức năng dễ bị CSRF như: **cập nhật thông tin cá nhân**, **đổi mật khẩu**,...



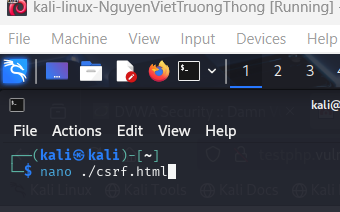
**Bước 2: Kiểm tra request**

Mở chức năng Developer Tools (F12) > Tab **Network**.

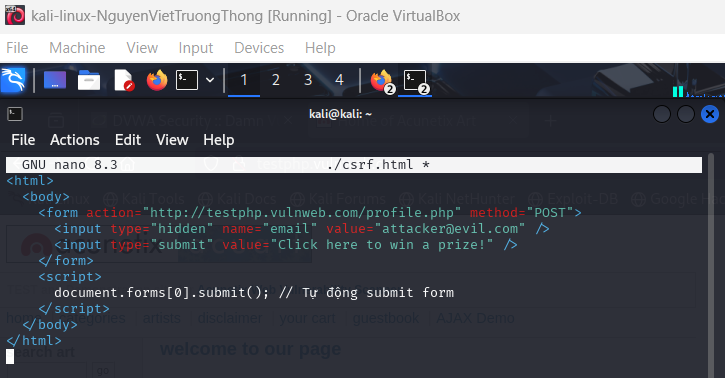
Thực hiện thao tác cần kiểm thử (ví dụ đổi email).

Copy lại request (đặc biệt là POST request có thay đổi dữ liệu).

Bước 3 : Tạo file HTML giả mạo (CSRF PoC)



Có nội dung như sau :



**Bước 4: Mở file để kiểm thử**

