**BÁO CÁO BÀI THỰC HÀNH SỐ 9**

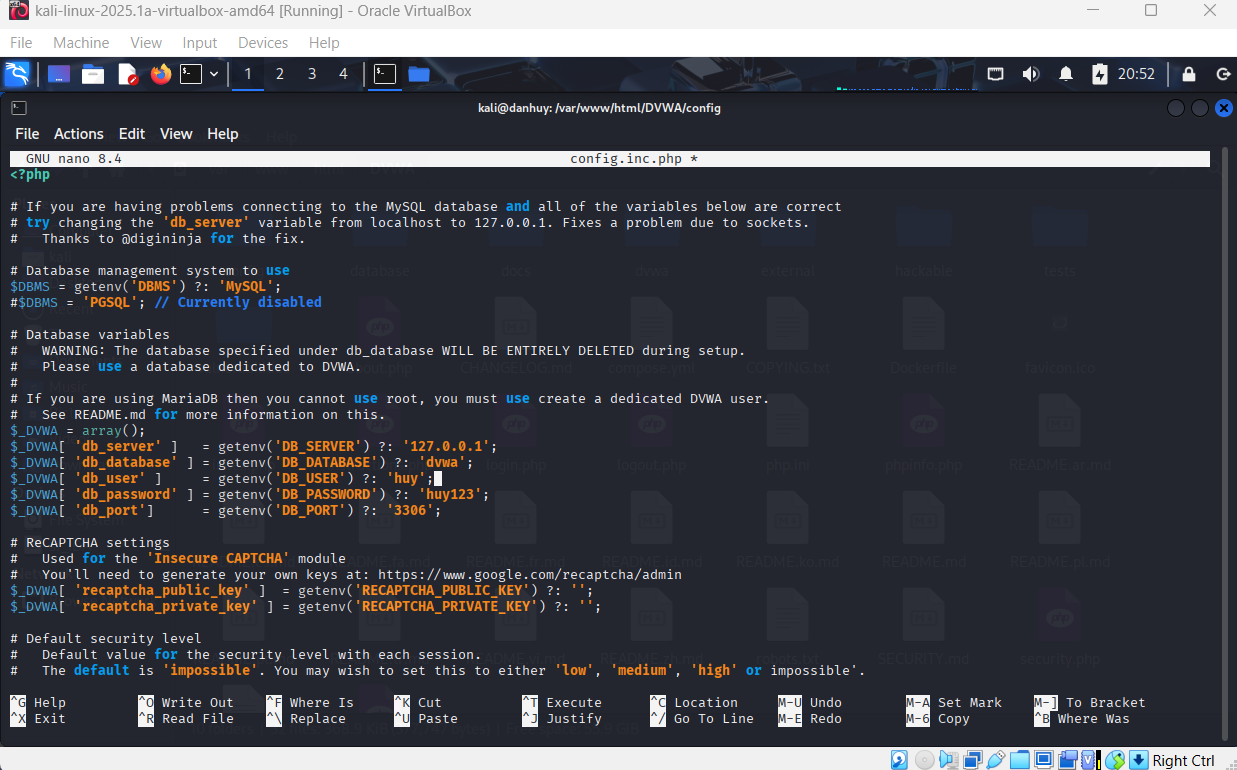
**KIỂM THỬ LỖ HỔNG XSS và CSRF**

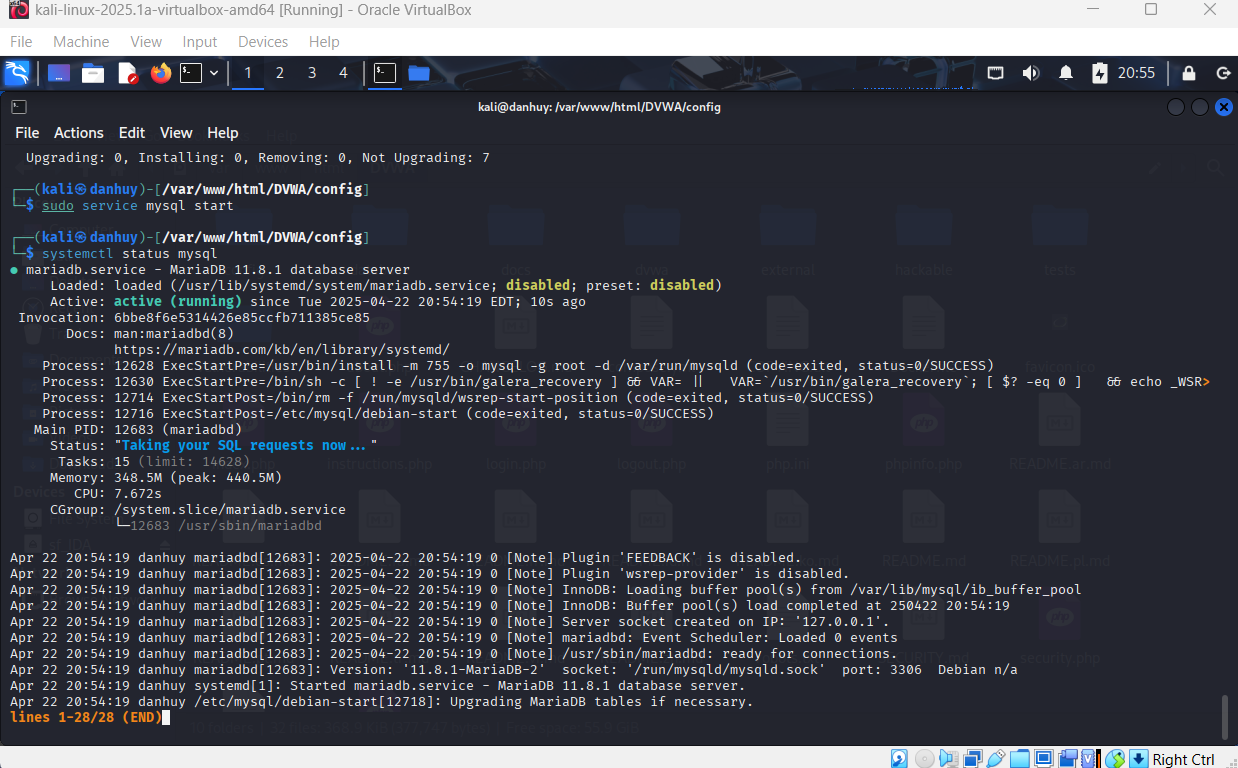
Họ và tên: Trương Đan Huy

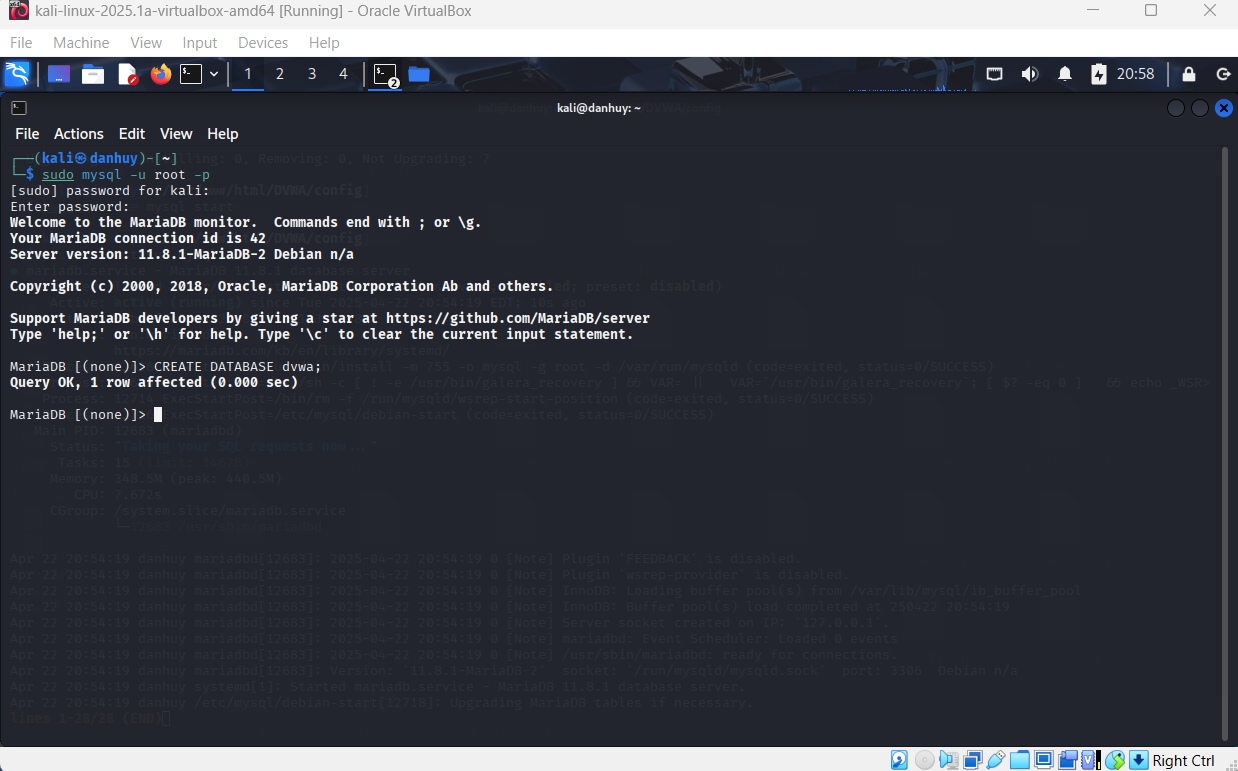
Bài làm

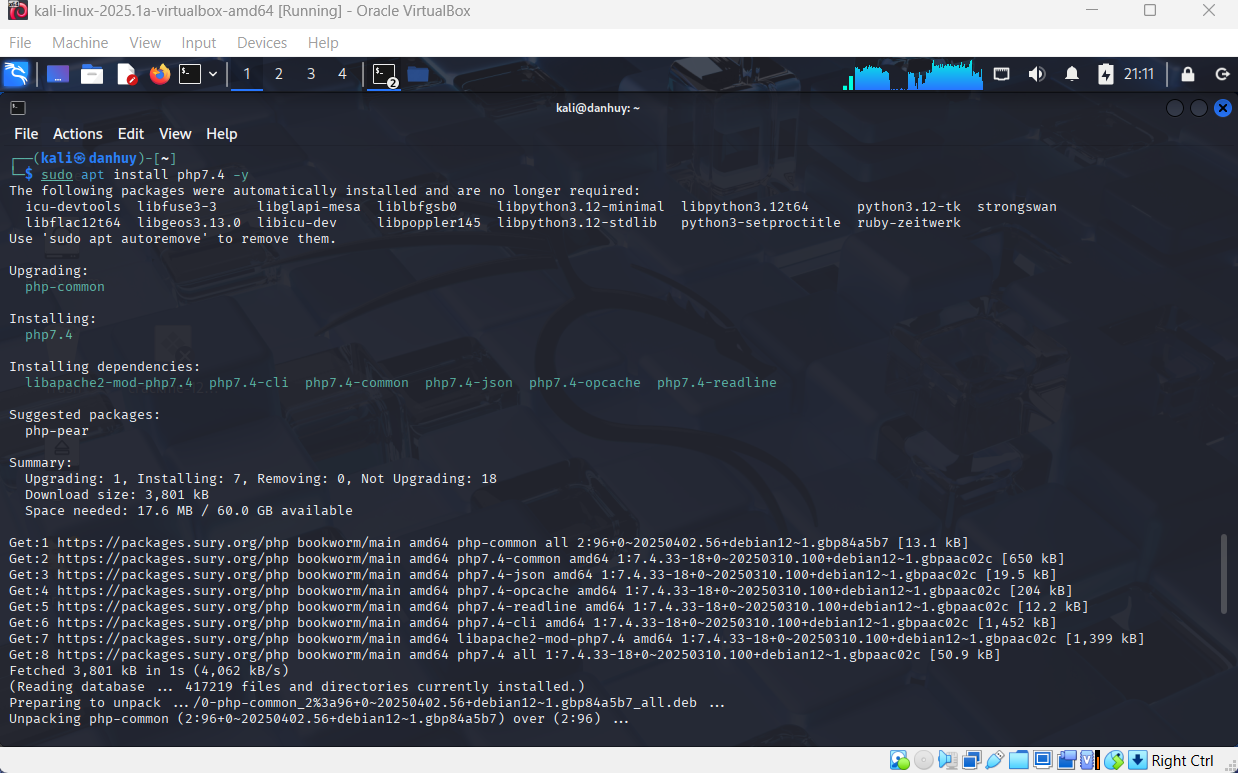
**Câu 1:**

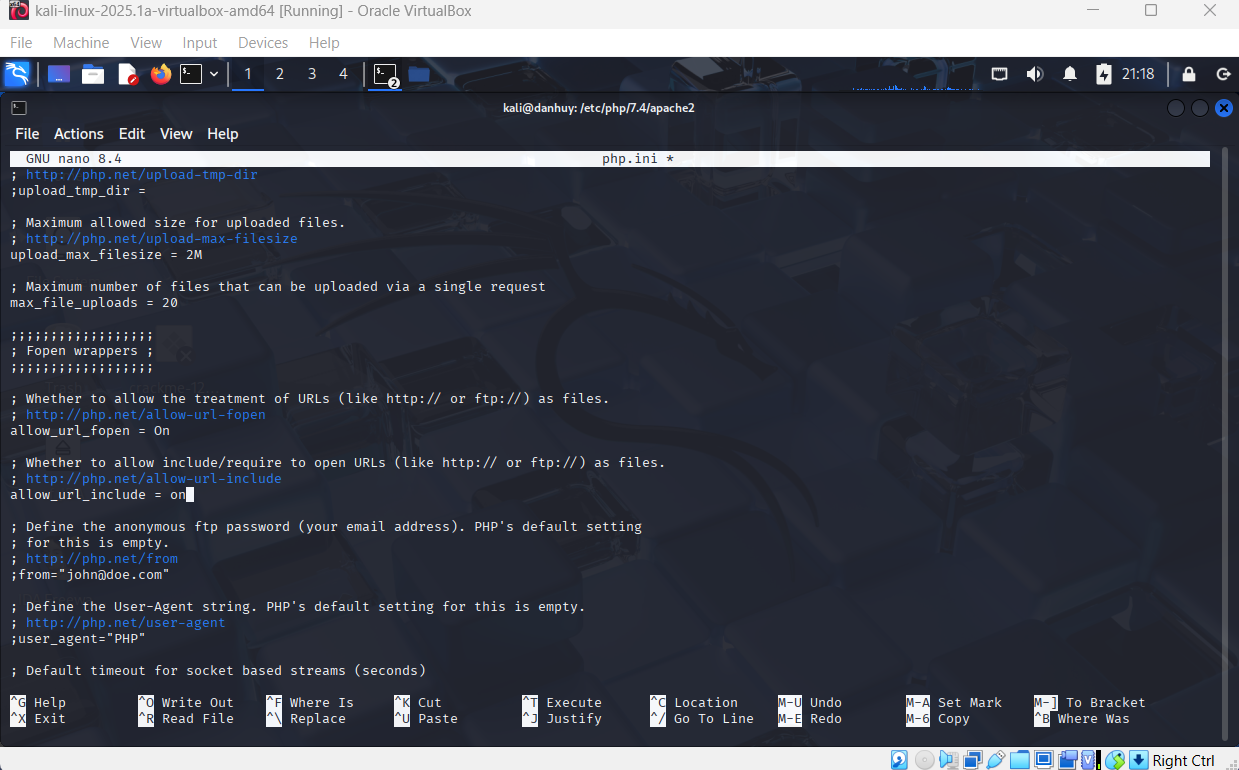
Các bước cài đặt:



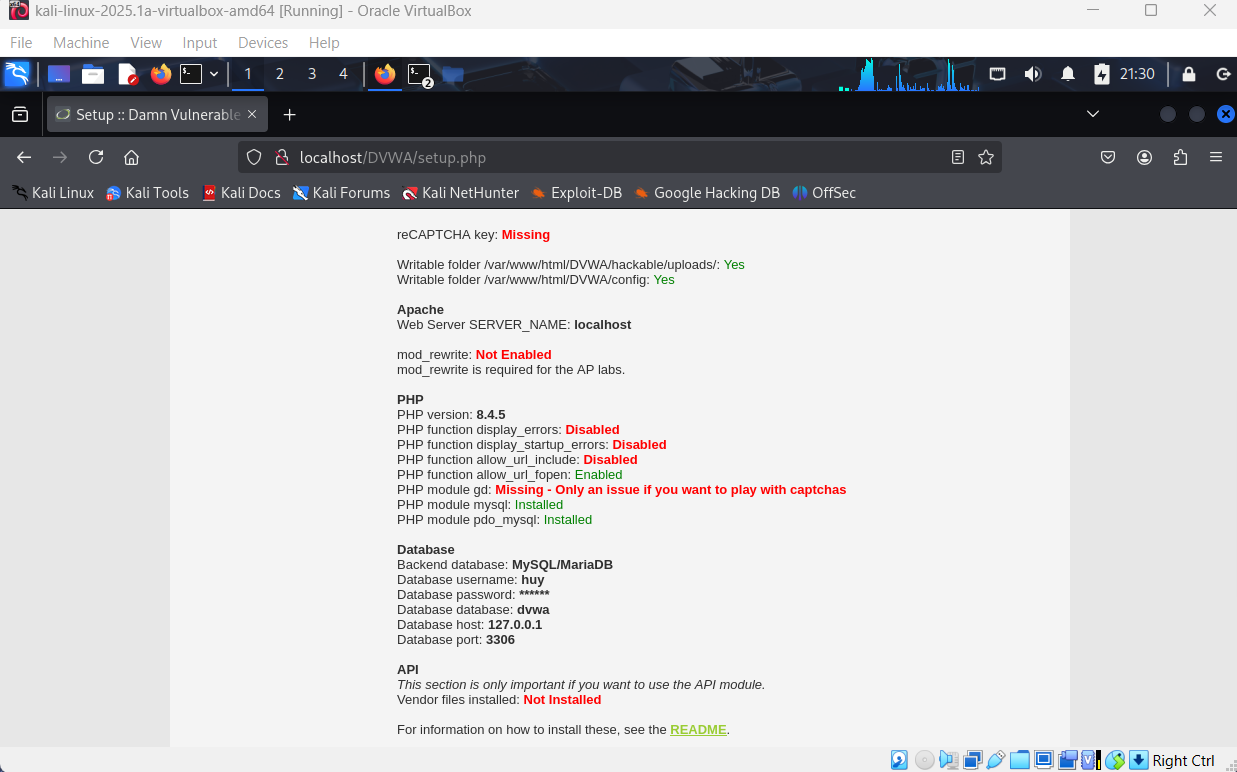












**Câu 1: Thực thi đoạn mã hiển thị thông báo chứa 4 số cuối MSSV**

**Trang web chọn kiểm thử:** http://testphp.vulnweb.com  
**URL kiểm thử:** http://testphp.vulnweb.com/artists.php?artist=1

**1. Xác định tham số đầu vào:**

* Tham số: artist trong URL artists.php?artist=1

**2. Xác định giá trị đầu vào xuất hiện trong trang kết quả:**

* Khi nhập artist=1, nội dung trang sẽ thay đổi theo ID artist → có phản hồi hiển thị từ giá trị đó.

**3. Các bước kiểm thử:**

* Truy cập URL trên và thử gán payload như sau: http://localhost/dvwa/setup.php

**Câu 2: Hiển thị thông báo chứa tên sinh viên**

Giả sử tên sinh viên là **Nguyen Van A**

**1. Tham số đầu vào:**

* Vẫn dùng artist trên testphp.vulnweb.com

**2. Giá trị xuất hiện trong trang:**

* Payload được chèn hiển thị trong kết quả trang web.

**3. Các bước kiểm thử:**

* URL kiểm thử: http://testphp.vulnweb.com/.

**Phần 2: Kiểm thử CSRF**

**Chọn trang:** http://demo.testfire.net

http://demo.testfire.net/bank/change-password.aspx

Đăng nhập tài khoản (ví dụ user: jdoe / password: demo)

**Kết luận:**

* Nếu không có token xác thực hoặc xác minh lại mật khẩu → trang dễ bị CSRF.