BÁO CÁO BÀI THỰC HÀNH SỐ 9

KIỂM THỬ LỖ HỔNG XSS và CSRF

Họ và tên:Hồ ĐÌnh Nguyên

Link youtube:<https://www.youtube.com/channel/UCEPuvFCAI79ySOkCeCdgRyw>

lonk githup:https://github.com/Dinh-nguyen16122003/BaoMatMangMayTinhVaHeThong.git

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

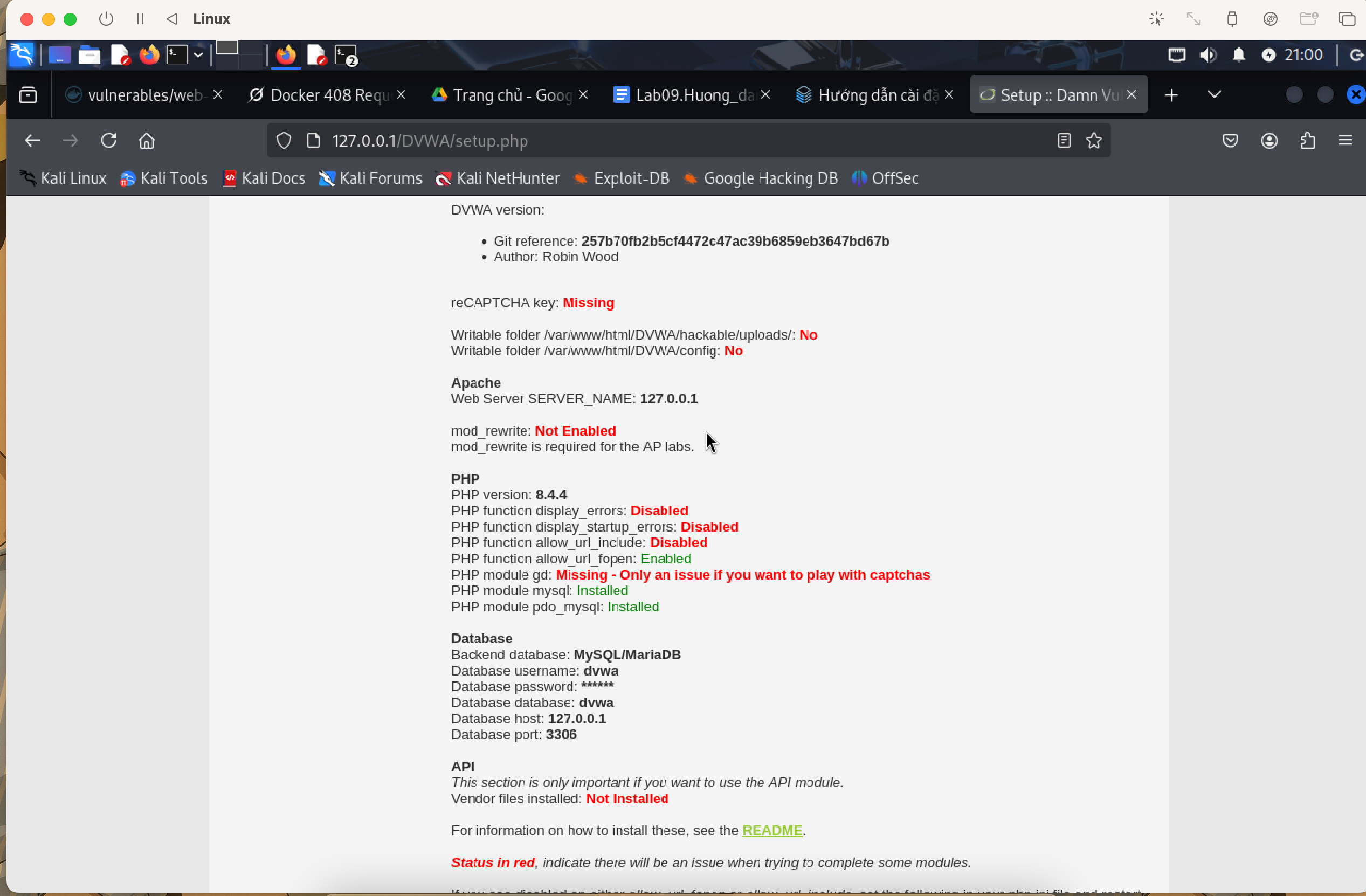
Phần 1: Kiểm thử XSS

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

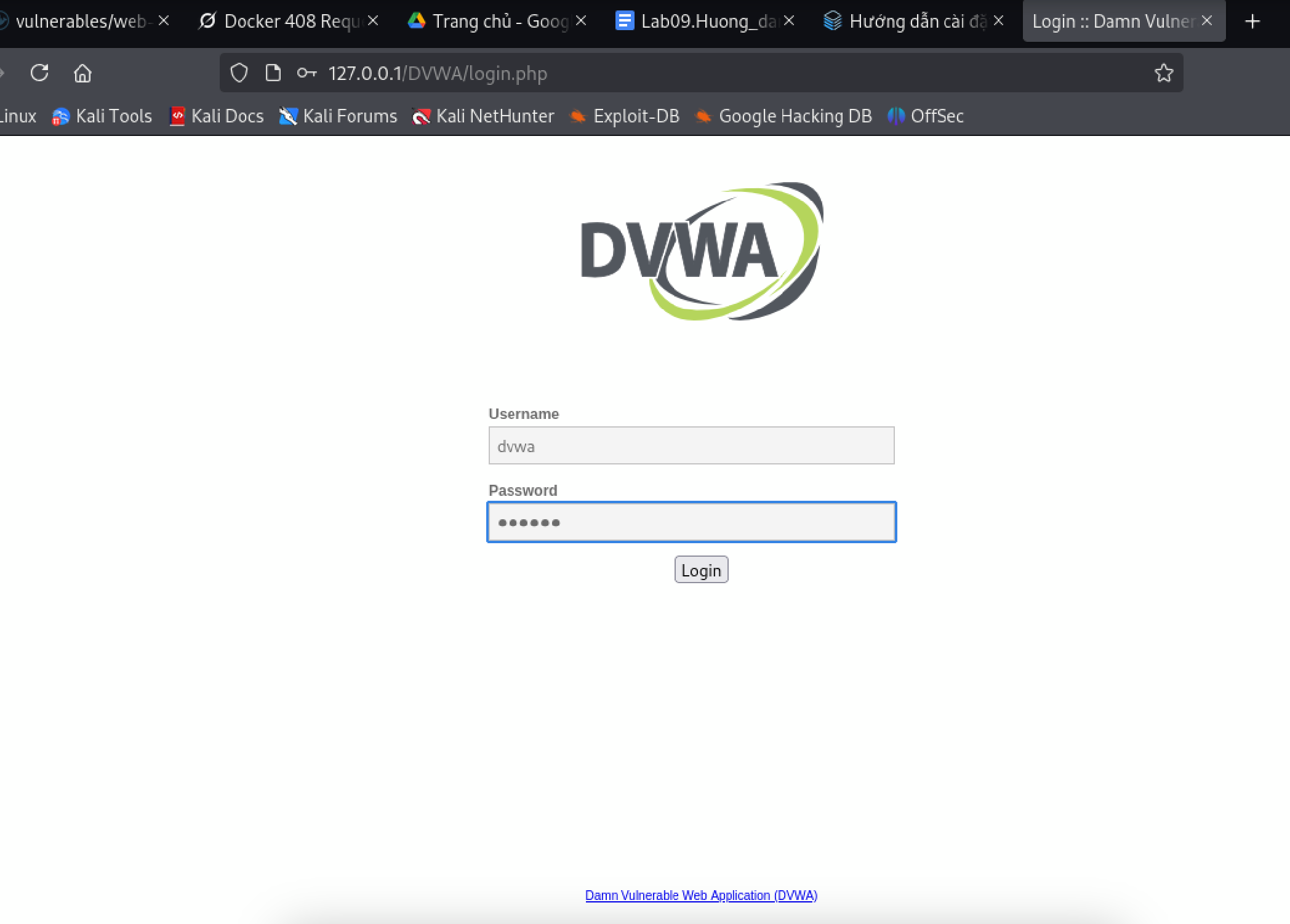
1. <http://demo.testfire.net`>

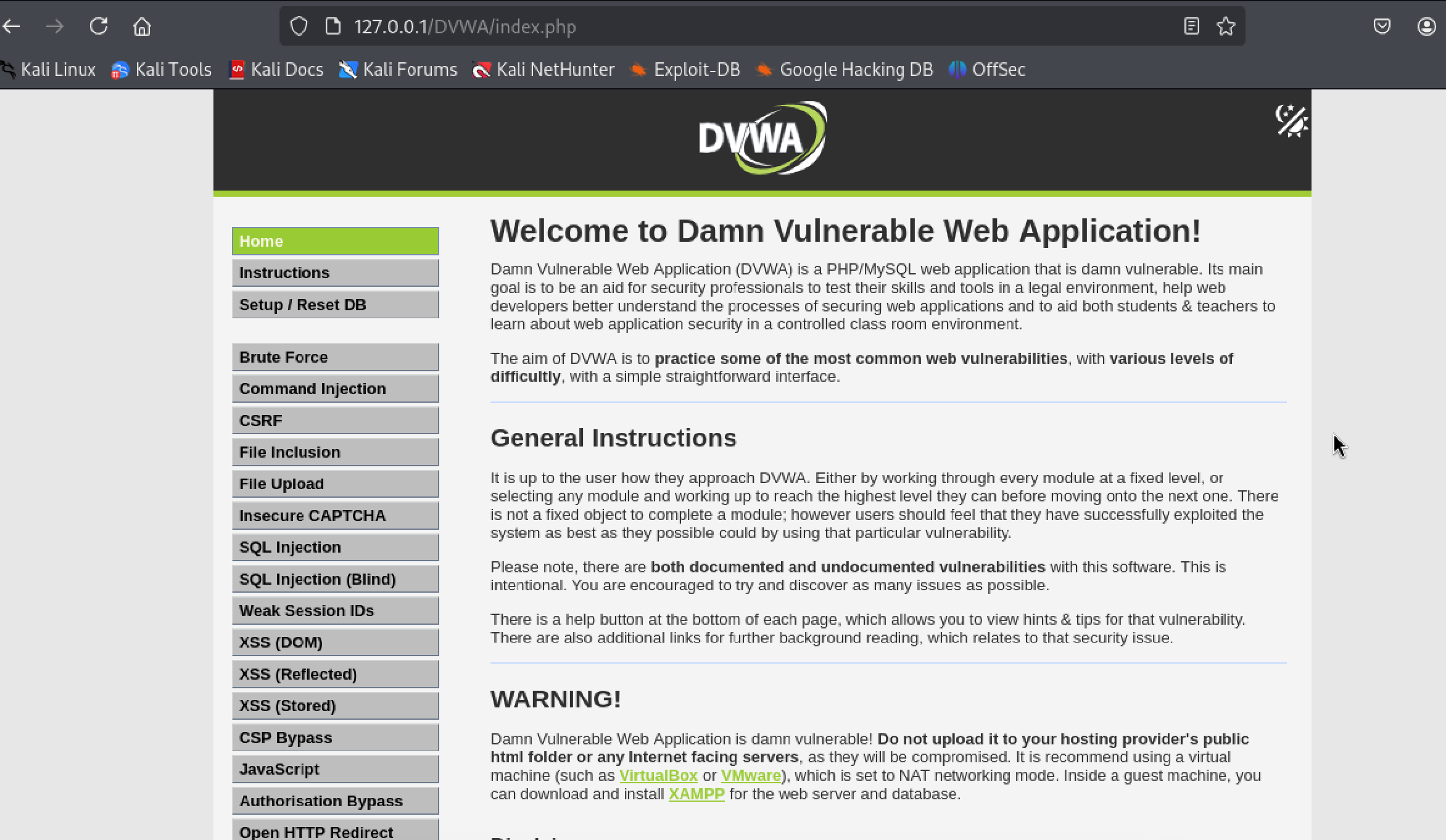
câu 1:

tạo sql và



đăng nhập vào

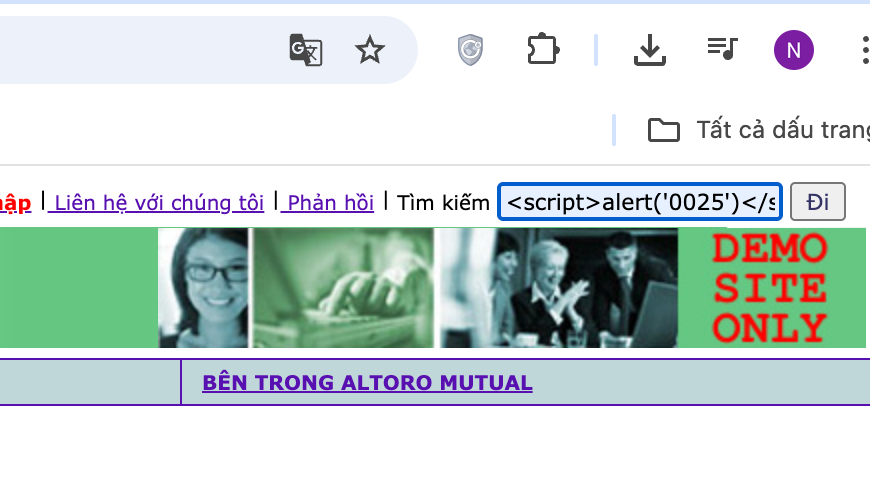


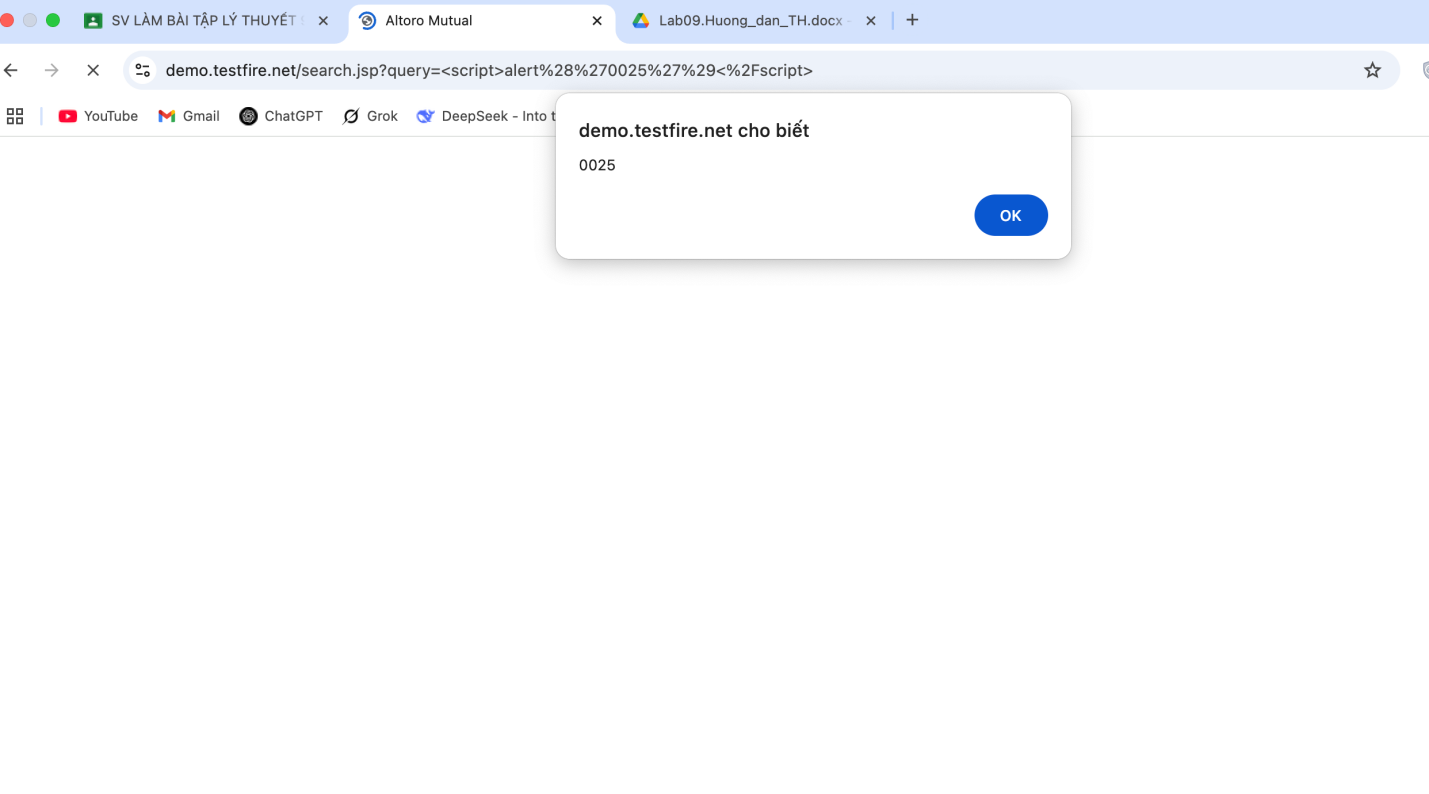


Tham số đầu vào lả1: query

Giá trị đầu vào là: 0025

Các bước kiểm thử và phán đoán:





→ **lỗ hổng XSS tồn tại**.

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

<script>alert("0025")</script>

**Giải thích:**  
Khi giá trị trên được nhập và kết quả hiển thị ra thông báo chứa 0025, điều này chứng minh rằng **đoạn mã JavaScript được thực thi từ phía người dùng**, cho thấy website có lỗ hổng **Reflected XSS**.

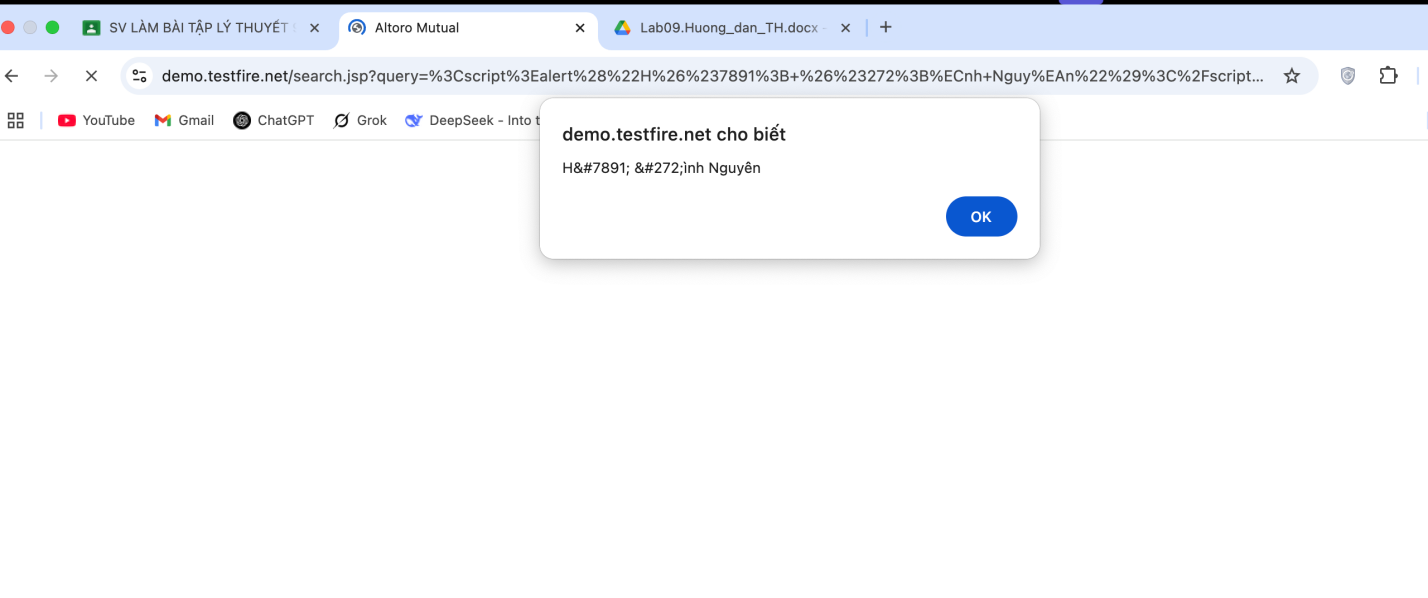
Câu 2:

Tham số đầu vào lả1: query

Giá trị đầu vào là: Hồ Đình Nguyên

Các bước kiểm thử và phán đoán:





→ **lỗ hổng XSS tồn tại**.

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

<script>alert("Hồ Đình Nguyên")</script>

**Giải thích:**  
Khi giá trị trên được nhập và kết quả hiển thị ra thông báo chứa “Hồ Đình Nguyên”, điều này chứng minh rằng **đoạn mã JavaScript được thực thi từ phía người dùng**, cho thấy website có lỗ hổng **Reflected XSS**.

Câu 3:

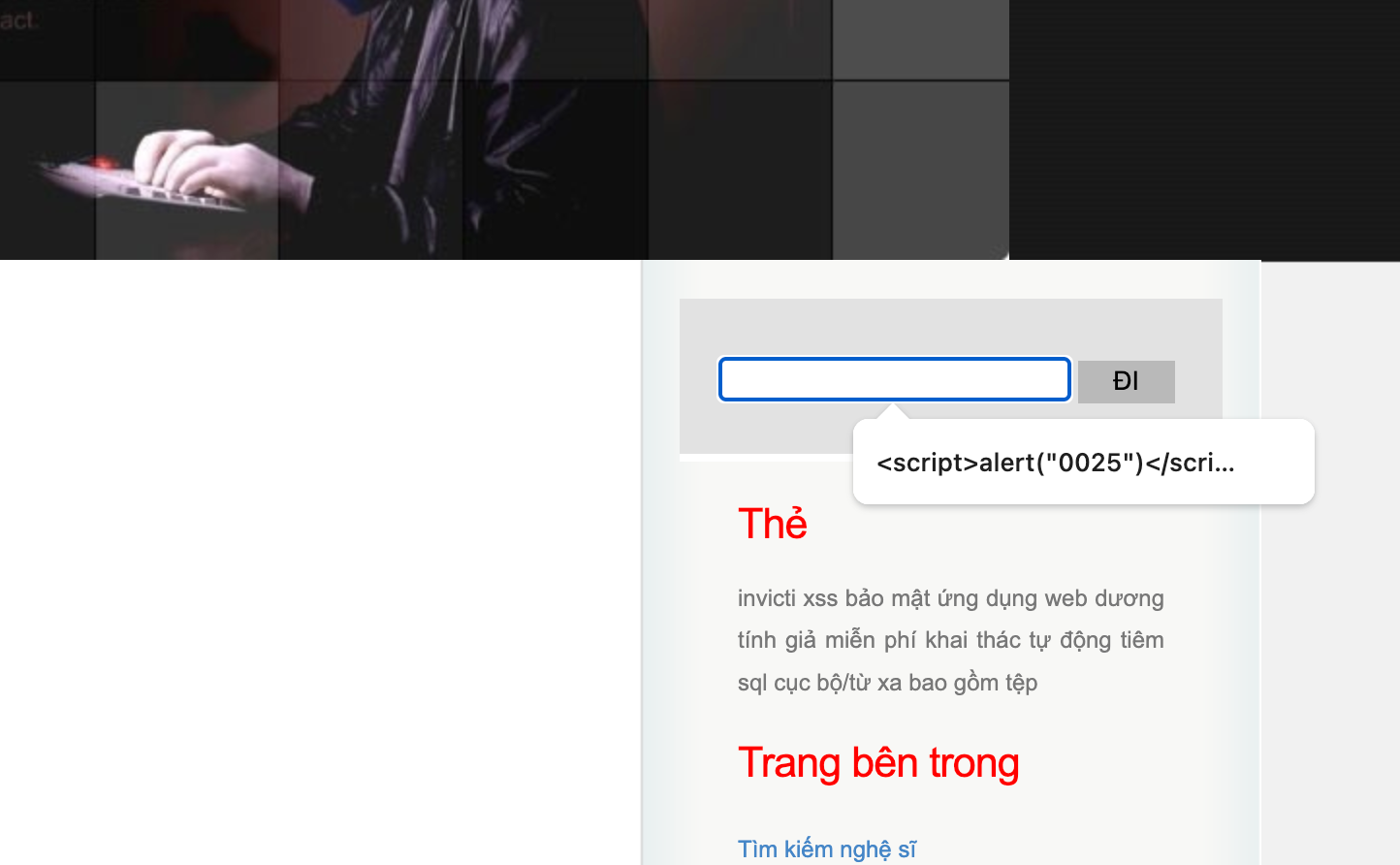
sử dụng trang web này:

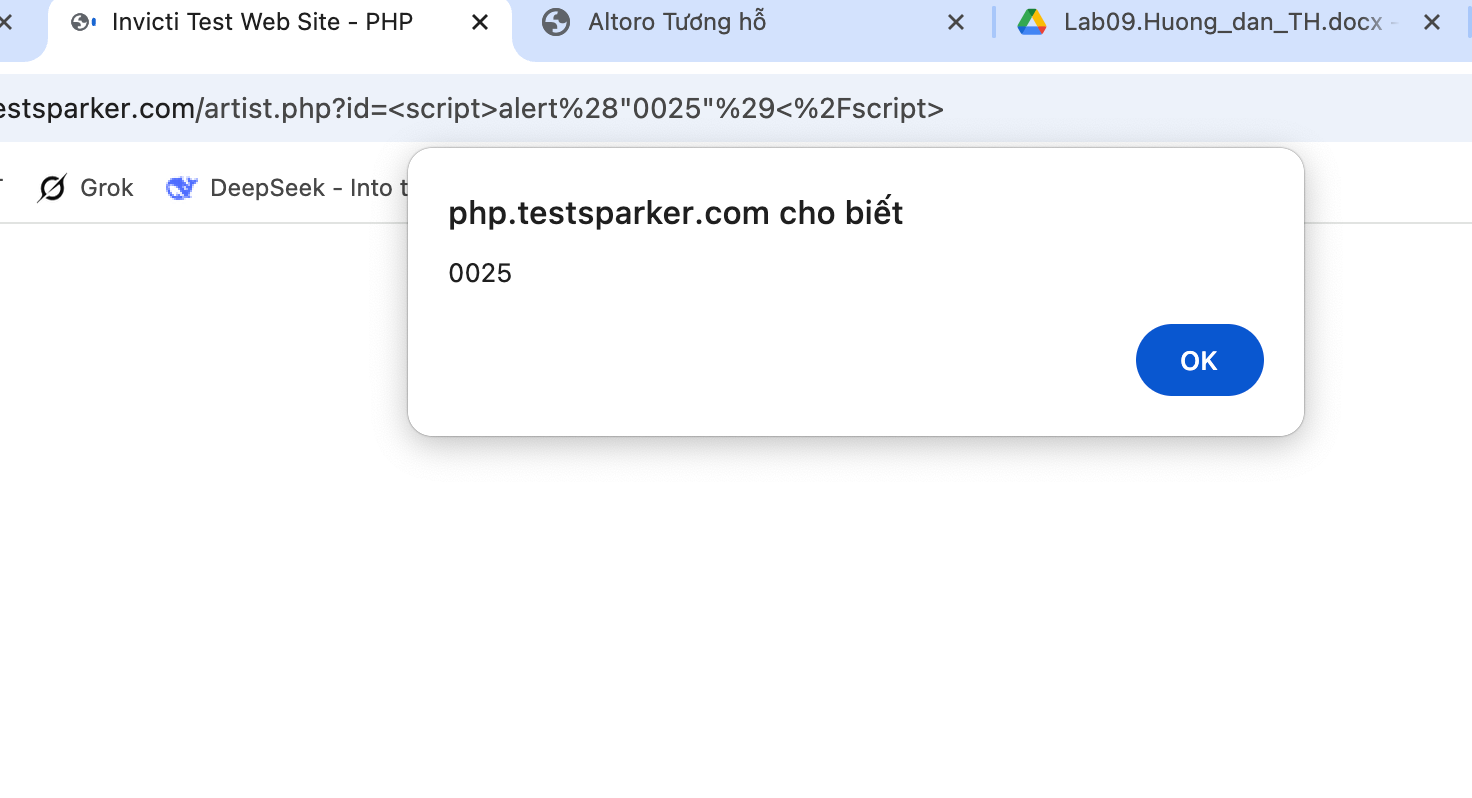
<http://php.testsparker.com>

Tham số đầu vào lả1: query

Giá trị đầu vào là: 0025

Các bước kiểm thử và phán đoán:





→ **lỗ hổng XSS tồn tại**.

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

<script>alert("0025")</script>

**Giải thích:**  
Khi giá trị trên được nhập và kết quả hiển thị ra thông báo chứa 0025, điều này chứng minh rằng **đoạn mã JavaScript được thực thi từ phía người dùng**, cho thấy website có lỗ hổng **Reflected XSS**.

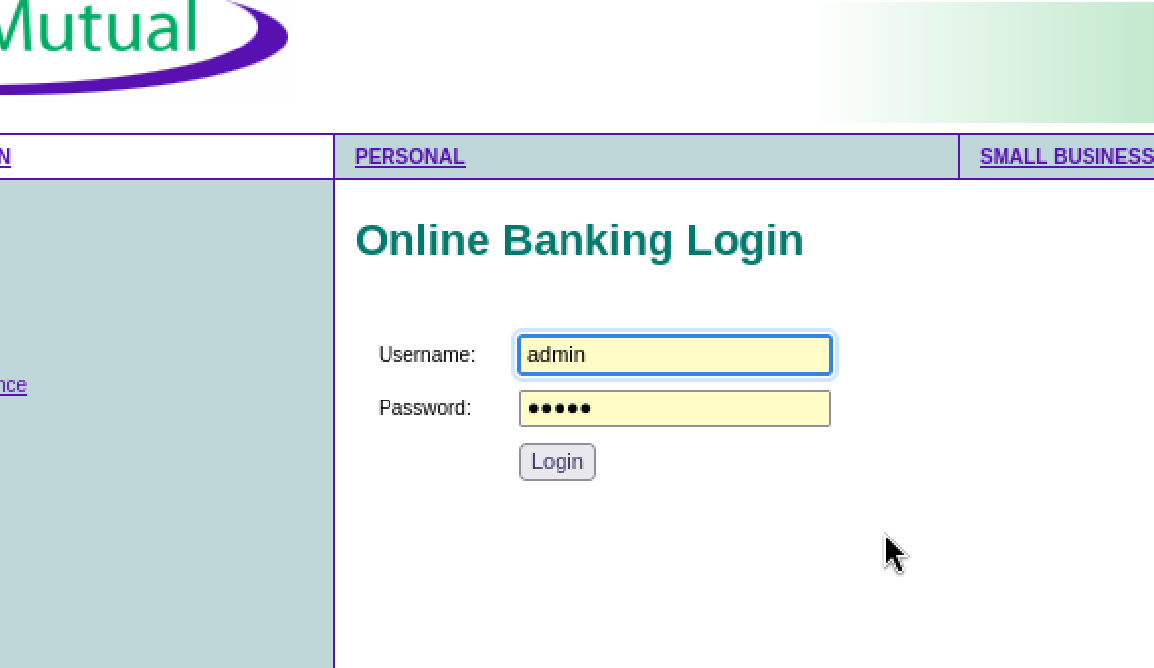
Phần 2: Kiểm thử CSRF (2 điểm)

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

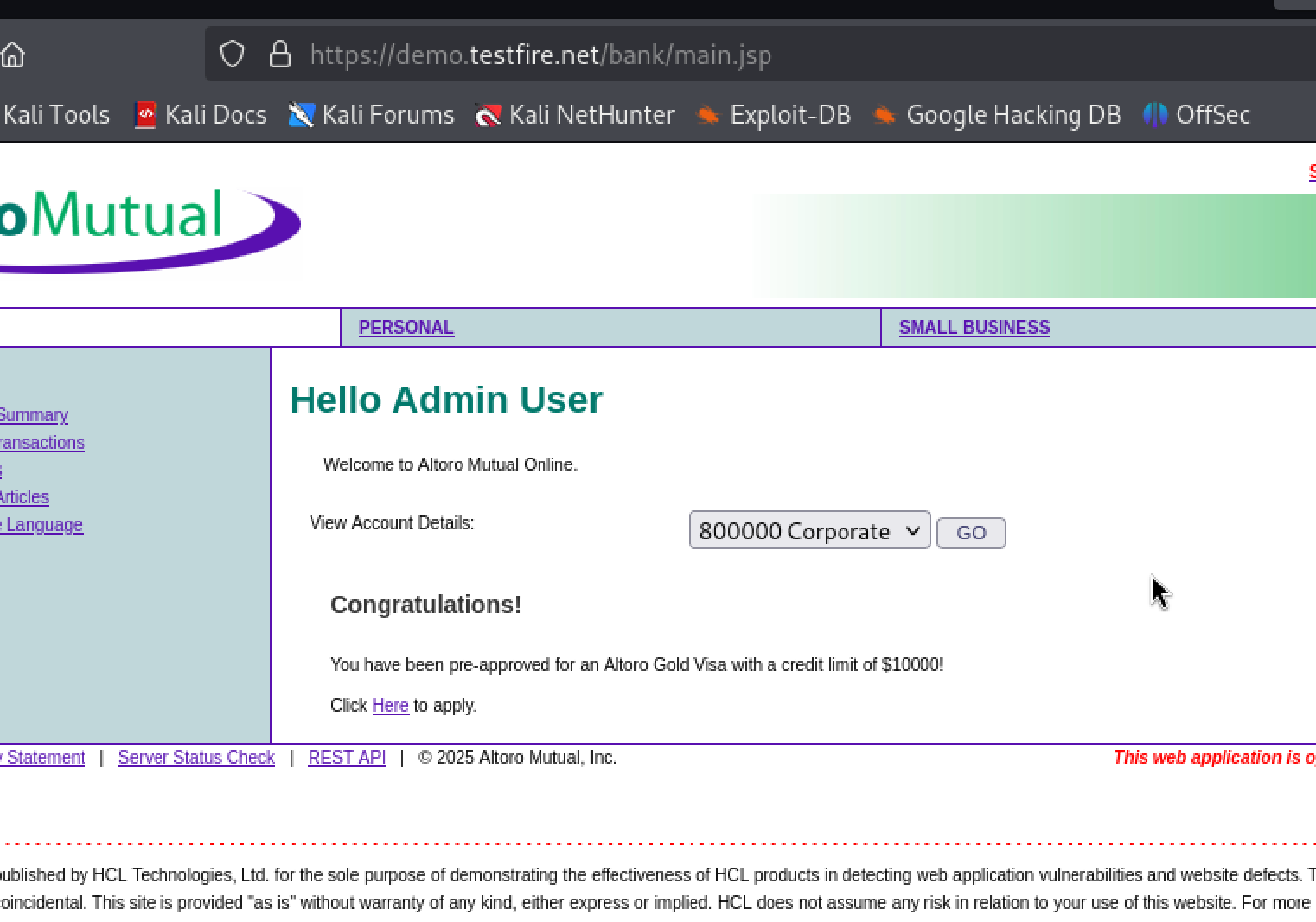
sau để thử nghiệm

<http://demo.testfire.net/login.jsp>

Đăng nhập:



Đăng nhập thành công



vào transter funds

