**BÁO CÁO BÀI THỰC HÀNH SỐ 9**

**KIỂM THỬ LỖ HỔNG XSS và CSRF**

Họ và tên: Phạm Hồ Bình An - MSSV: 1050080127

Link youtube: https://youtu.be/pFkZDdkSvo8

***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: **0.25 điểm**

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

**-** 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: **0.5 điểm**

**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**

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

**-** 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: **0.5 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**

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

**-** 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: **0.5 điểm**

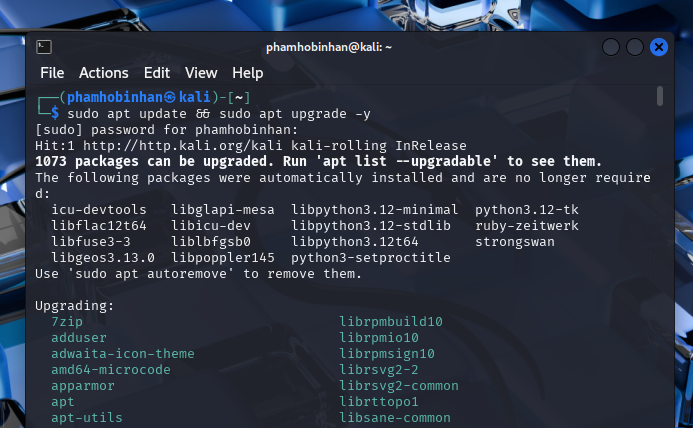
**Phần 2: Kiểm thử CSRF (2 điểm)**

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/)

Cài đặt ứng dụng web DVWA để luyện tập

Đầu tiên cần cập nhật máy áo Linux:



**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/).

Ảnh có chứa văn bản, ảnh chụp màn hình

Nội dung do AI tạo ra có thể không chính xác.  
  
Bước 2

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:

Ảnh có chứa văn bản, ảnh chụp màn hình

Nội dung do AI tạo ra có thể không chính xác.

Bước 3: Sao chép thư mục sau khi đã giải nén vào thư mục webroot của Web Server

Ảnh có chứa văn bản, ảnh chụp màn hình, máy tính

Nội dung do AI tạo ra có thể không chính xác.

Bước 4: Tạo một CSDL có tên là “dvwa”

Bước 5: sửa nội dung file dvwa/config/config.inc.php

Ảnh có chứa văn bản, ảnh chụp màn hình, máy tính, phần mềm

Nội dung do AI tạo ra có thể không chính xác.

Cài đặt MySQL

Ảnh có chứa văn bản, ảnh chụp màn hình, máy tính, phần mềm

Nội dung do AI tạo ra có thể không chính xác.

Cấu hình MySQL

Ảnh có chứa văn bản, ảnh chụp màn hình

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, công nghệ

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

Câu1  
- Tham số đầu vào: `name` (hoặc input tương tự trên trang http://testphp.vulnweb.com hoặc DVWA).  
- Xuất hiện trong trang kết quả: Chuỗi nhập vào được phản hồi trực tiếp trong HTML.  
- Các bước kiểm thử:  
 1. Truy cập trang nhập liệu (ví dụ mục XSS(Reflected) trong DVWA).  
 2. Nhập `<script>alert('0127')</script>` vào ô nhập liệu.  
 3. Quan sát nếu popup xuất hiện thì chứng minh tồn tại XSS.  
- Kết luận: Trang không kiểm soát đầu vào, thực thi JavaScript => tồn tại lỗ hổng XSS Reflected.

- Tham số đầu vào: `name` (trong URL hoặc form).  
- Xuất hiện trong trang kết quả: Hiển thị tên người dùng.  
- Các bước kiểm thử:  
 1. Nhập `<script>alert(Pham Ho Binh An')</script>` vào ô tên.  
 2. Nếu trình duyệt bật popup thì chứng minh mã JavaScript đã được thực thi.  
- Kết luận: Tồn tại lỗ hổng XSS khi dữ liệu không được encode trước khi phản hồi.

- Tham số đầu vào: `message` (trong mục XSS Stored DVWA).  
- Xuất hiện trong trang kết quả: Tin nhắn được lưu và hiển thị cho mọi người.  
- Các bước kiểm thử:  
 1. Nhập `<script>alert('0127')</script>` vào ô 'message' trong XSS Stored.  
 2. Truy cập lại trang, popup vẫn bật => Stored XSS.  
- Kết luận: Trang lưu trữ và thực thi script => nguy cơ cao bị tấn công hàng loạt.

- Trang kiểm thử: http://testasp.vulnweb.com hoặc DVWA mục CSRF.  
- Bước 1: Đăng nhập DVWA với admin/password.  
- Bước 2: Tạo một form HTML giả thực hiện hành động như đổi mật khẩu.  
- Bước 3: Lưu file HTML và mở trong khi đang đăng nhập.  
```html  
<form action="http://localhost/dvwa/vulnerabilities/csrf/" method="POST">  
 <input type="hidden" name="password\_new" value="newpass123">  
 <input type="hidden" name="password\_conf" value="newpass123">  
 <input type="submit" value="Submit request">  
</form>  
```  
- Quan sát: Nếu mật khẩu bị thay đổi mà không yêu cầu xác thực lại => tồn tại CSRF.