BÁO CÁO BÀI THỰC HÀNH SỐ 9

KIỂM THỬ LỖ HỔNG XSS và CSRF

Họ và tên: Nguyễn Phương Sinh

Phần 1: Kiểm thử XSS

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

<http://testasp.vulnweb.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

A screenshot of a computer

AI-generated content may be incorrect.

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

Sau khi thay đổi giá trị id, nội dung của trang thay đổi theo.

Giá trị id được sử dụng để truy vấn dữ liệu và hiển thị nội dung — nếu bị chèn script, sẽ xuất hiện trong trang HTML → đây là **vị trí phản chiếu đầu vào → dễ bị XSS**.

- 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