**BÁO CÁO BÀI THỰC HÀNH SỐ 9**

**KIỂM THỬ LỖ HỔNG XSS và CSRF**

***Họ và tên: Đào Ngọc Qúi***

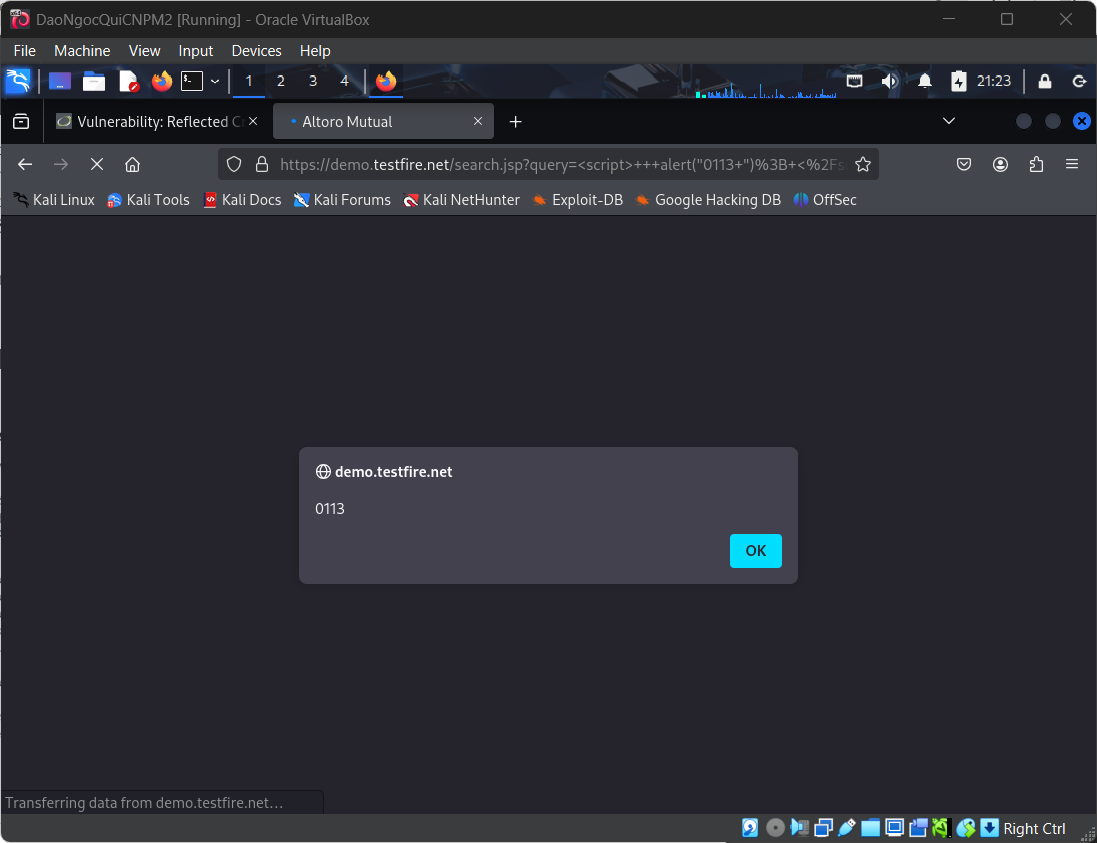
***Yêu cầu kết quả thực hành:***

**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/)`

**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: <script> alert("0113 "); </script>

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

https://demo.testfire.net/search.jsp?query=%3Cscript%3E+++alert%28%220113+%22%29%3B+%3C%2Fscript%3E

Các bước kiểm thử

Bước 1 Nhập script

<script> alert(“0113”); </script>

Bước 2: Gửi

Nhấn nút go

Bước 3: Phản hồi

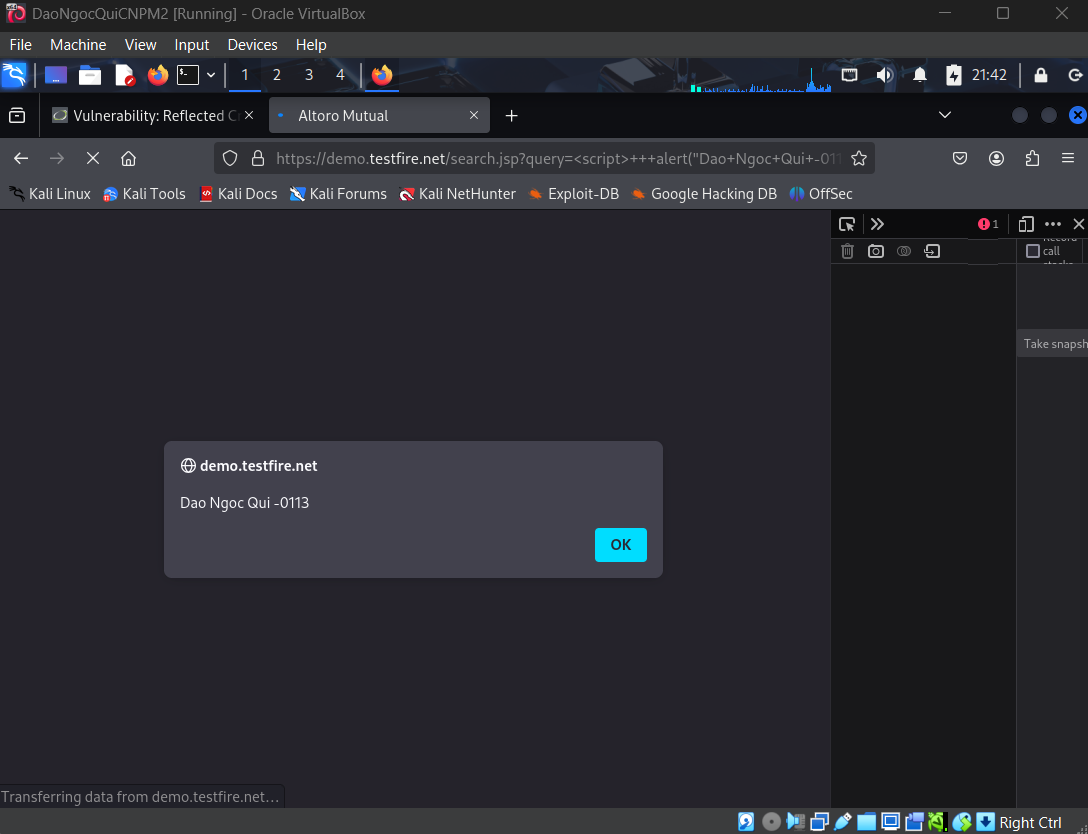
Xem thông báo

Phán đoán

Nếu alert hiện -> có lỗ hỏng XSS

Không có -> đã được mã hóa

**Câu 2**



\

<scrip> alert(“Dao Ngoc Qui – 0113”); </scrip>

Các bước kiểm thử

Bước 1: nhập <scrip> alert(“Dao Ngoc Qui – 0113”); </scrip>

Bước 2 gửi

Bước 3 phản hồi

Phán đoán

Nếu alert hiện -> có lỗ hỏng XSS

Không có -> đã được mã hóa

**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/)

