**BÁO CÁO BÀI THỰC HÀNH SỐ 9**

**KIỂM THỬ LỖ HỔNG XSS và CSRF**

Họ và tên: Lê Hoàng Phúc

Lớp: 10 CNPM2

**Cài đặt môi trường luyện tập**

Cài đặt ứng dụng web DVWA để luyện tập

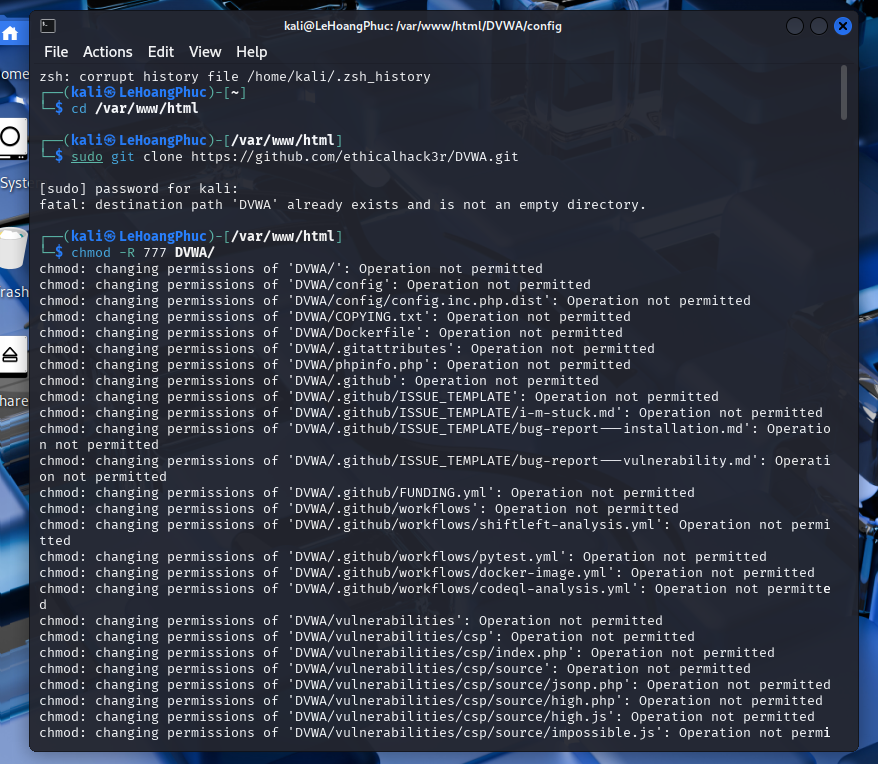
Bước 1: Download mã nguồn tại địa chỉ sau: http://www.dvwa.co.uk/

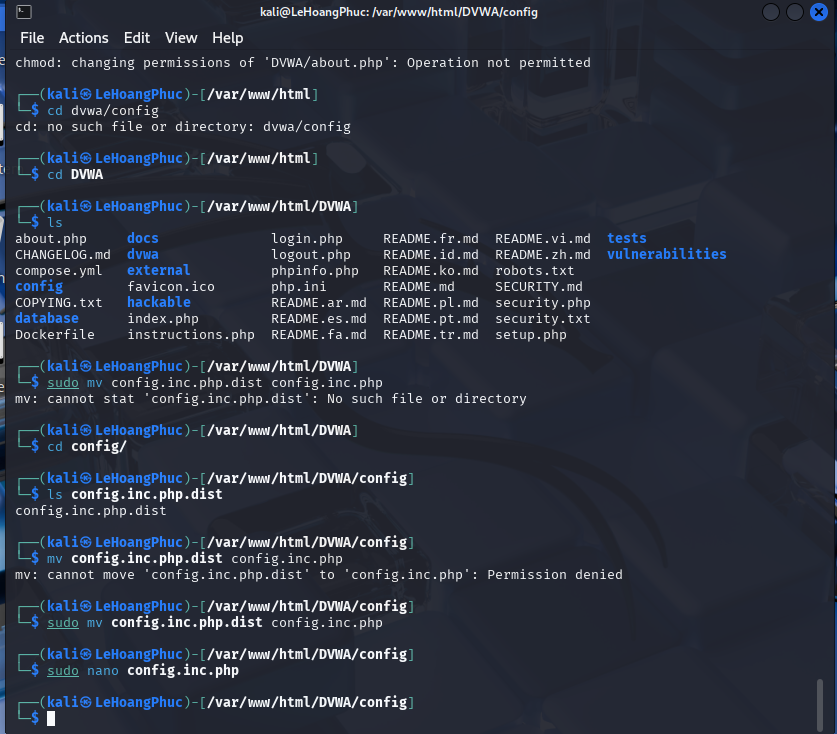
- Xem thêm ở đây: <https://vietnix.vn/cai-dat-dvwa-tren-linux/>

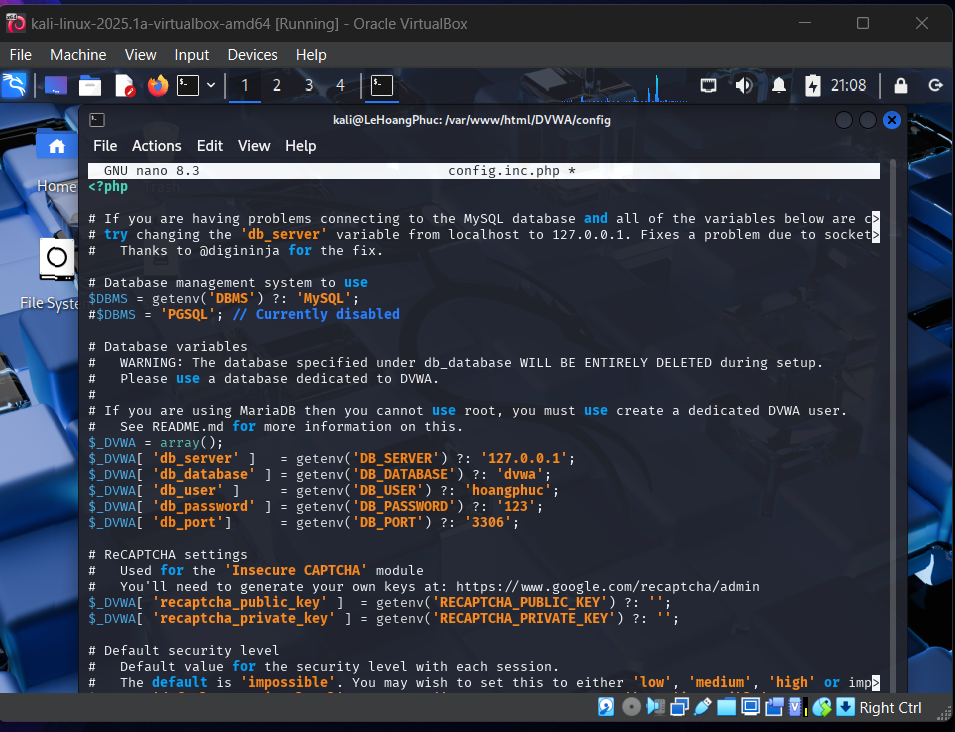
Bước 2: Giải nén file đã download được và đổi tên thành “dvwa”

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

- Bước 4: Tạo một CSDL có tên là “dvwa”

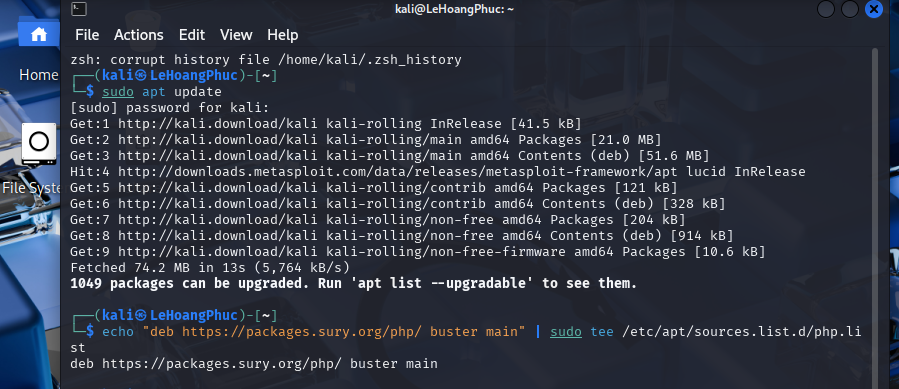


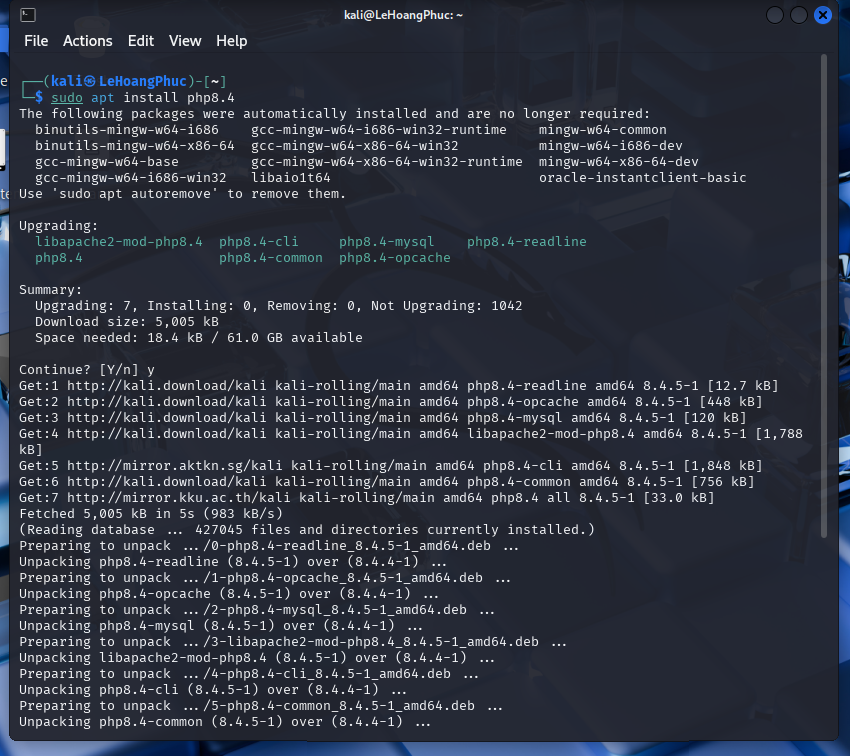


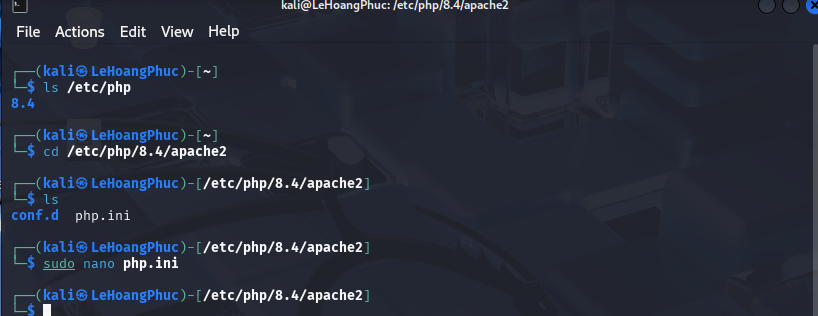


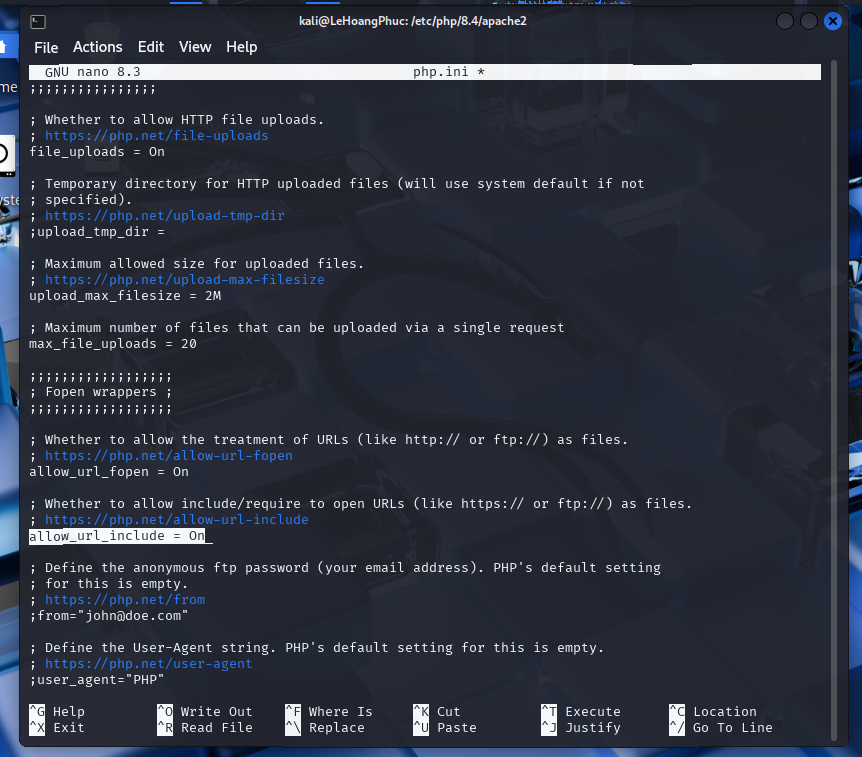
A screenshot of a computer

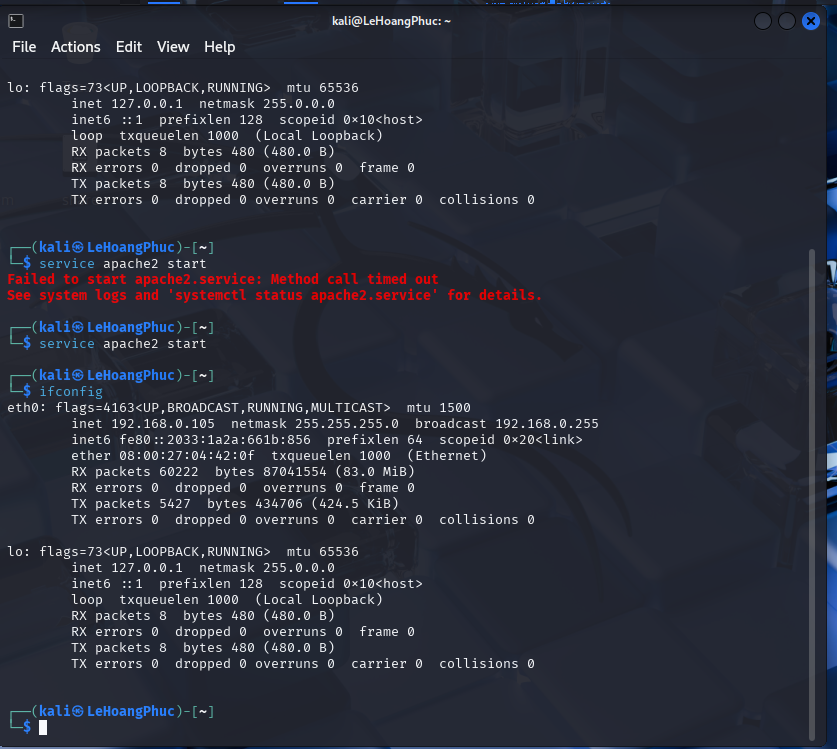
AI-generated content may be incorrect.

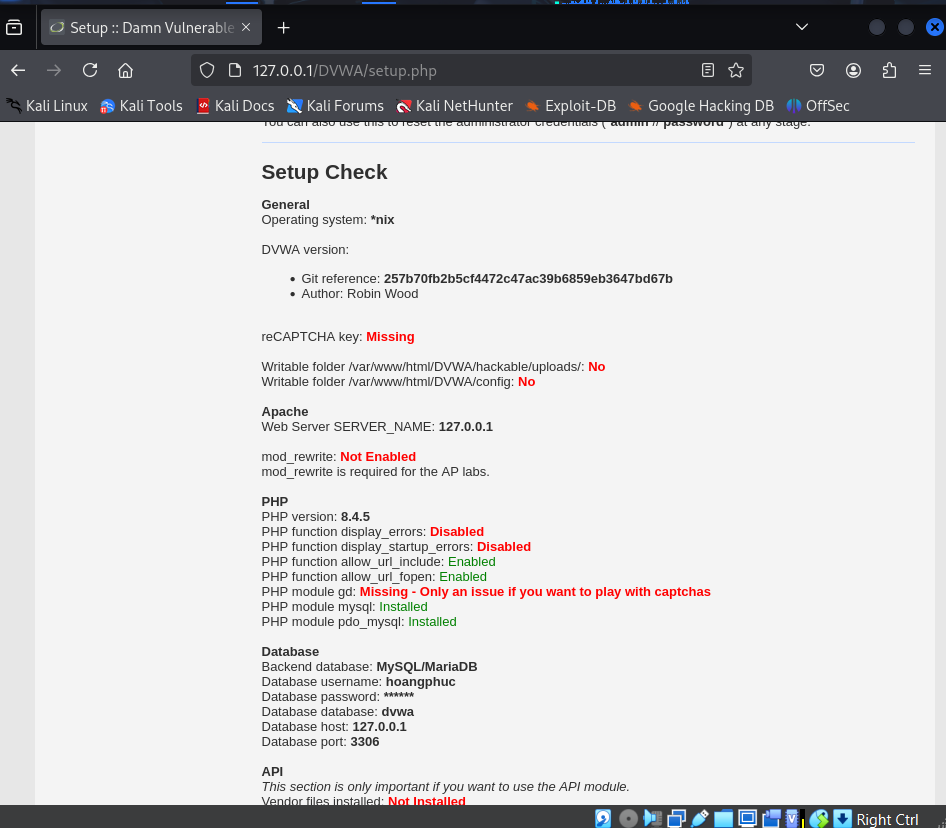








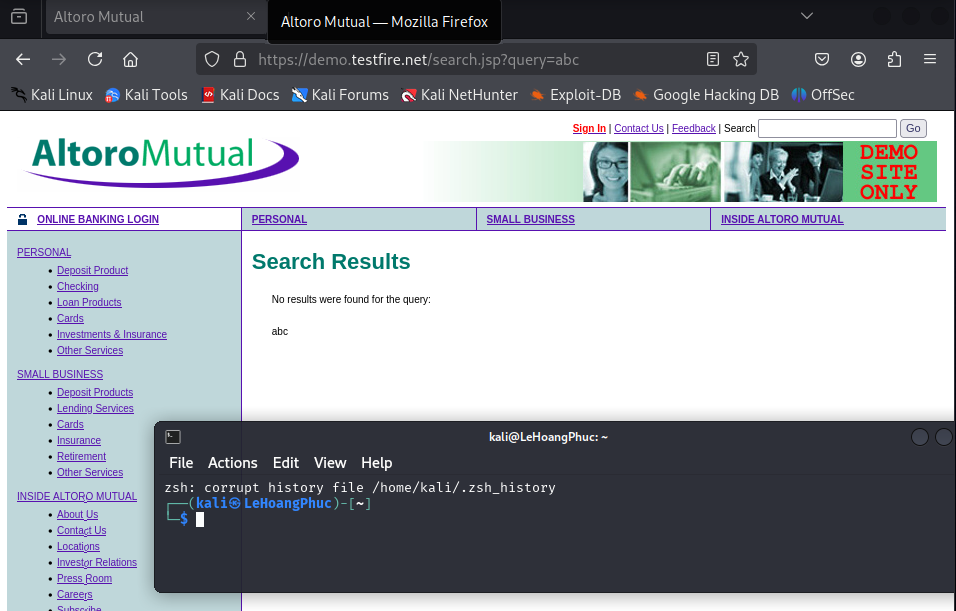




Câu 1

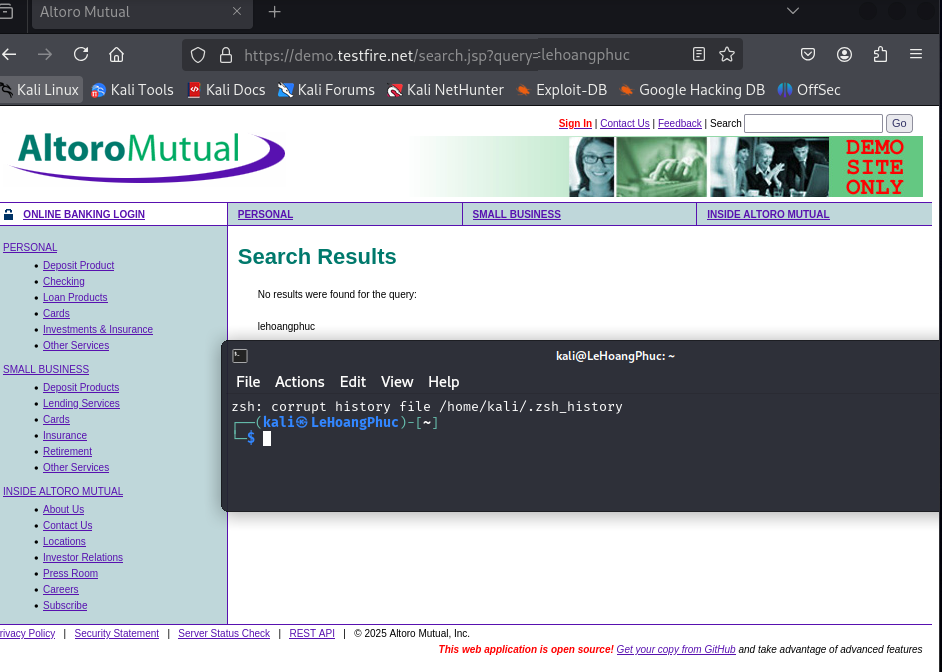
Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa 4 số cuối MSSV.





Tham số đầu vào là: query: **search.jsp?query=abc**

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

Truy cập:

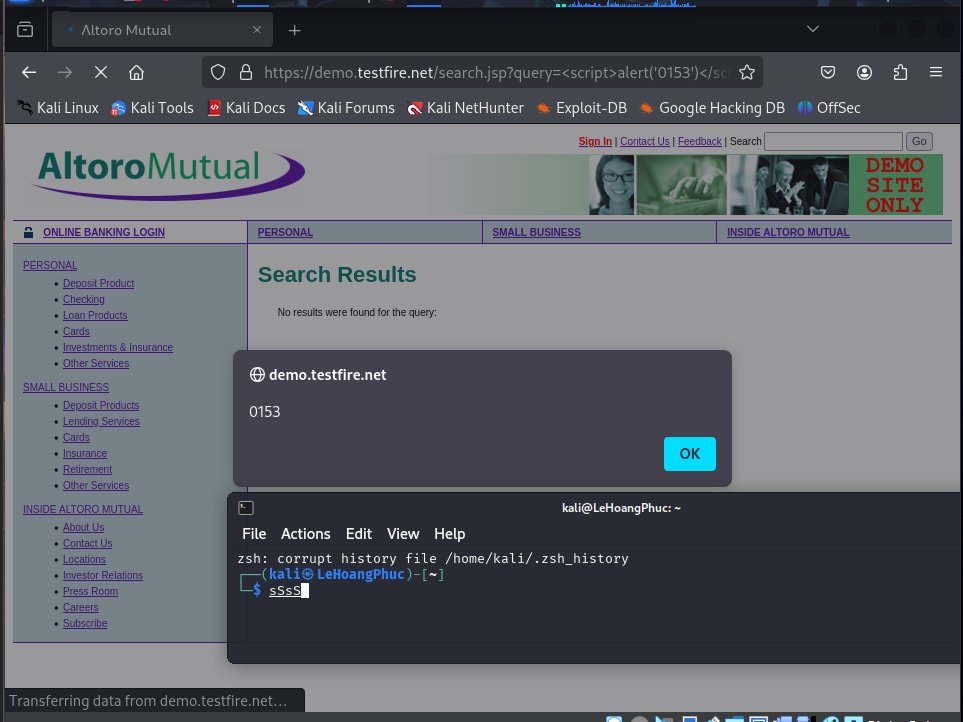
[http://demo.testfire.net/search.jsp?query=<script>alert('0153')</script](http://demo.testfire.net/search.jsp?query=%3cscript%3ealert('0153')%3c/script)>

Giá trị kiểm thử cho thấy lỗ hổng và giải thích: 0.5 điểm

<script>alert('1234')</script>

Kết quả hiện thị là

[http://demo.testfire.net/search.jsp?query=<script>alert('0153')</script>](http://demo.testfire.net/search.jsp?query=%3cscript%3ealert('0153')%3c/script%3e)



cho thấy giá trị đầu vào không được mã hóa gây lỗ hổng XSS.