**BÁO CÁO BÀI THỰC HÀNH SỐ 4**

**KIỂM THỬ LỖ HỔNG XSS và CSRF**

***Họ và tên: Nguyễn Thanh Ý***

***MSSV: 0850080056***

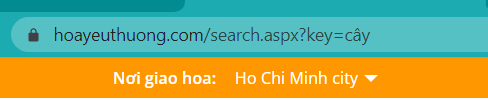
**Phần 1: Kiểm thử XSS**

Thực hiện kiểm thử lỗ hổng XSS trên một trang website: https://hoayeuthuong.com/

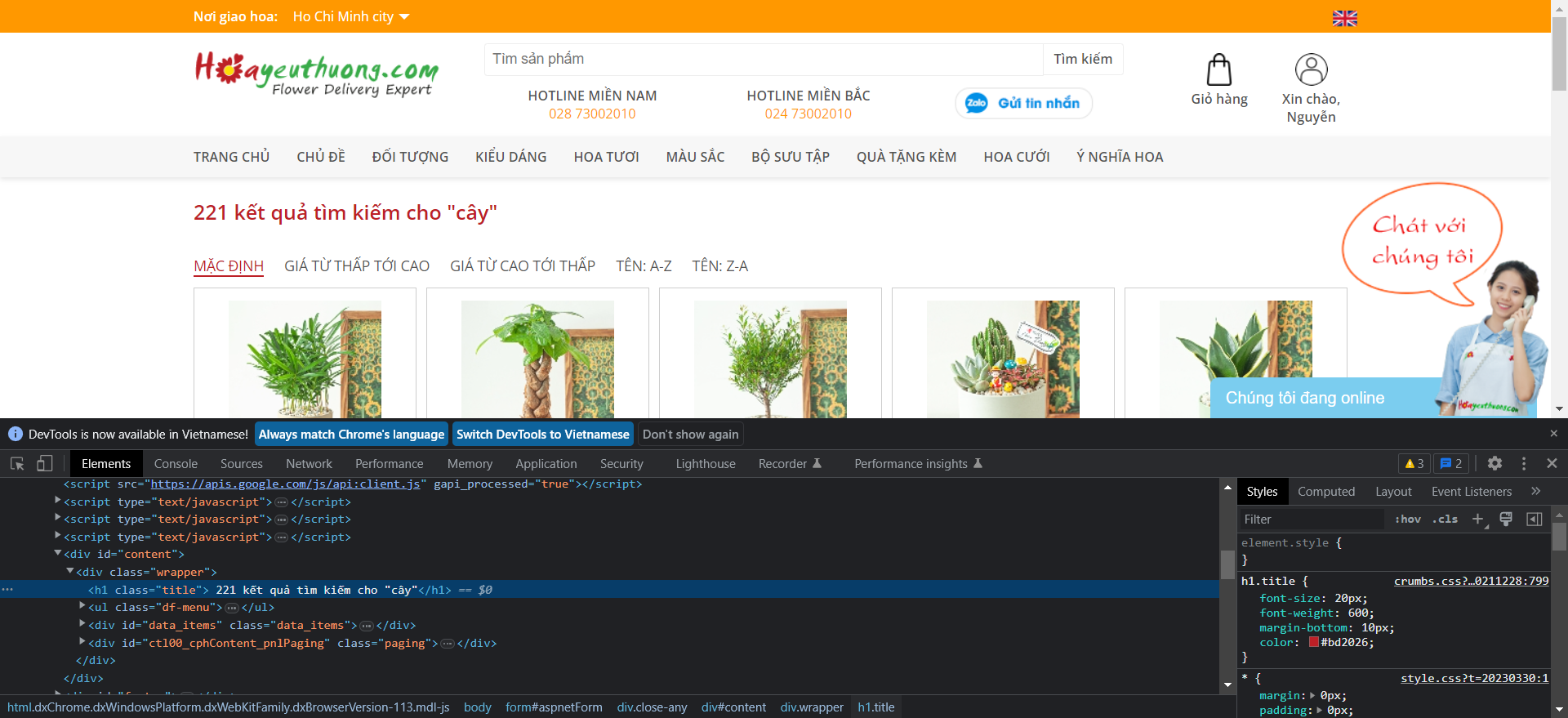
**Câu 1**

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: **Tham số đầu vào `key=`**

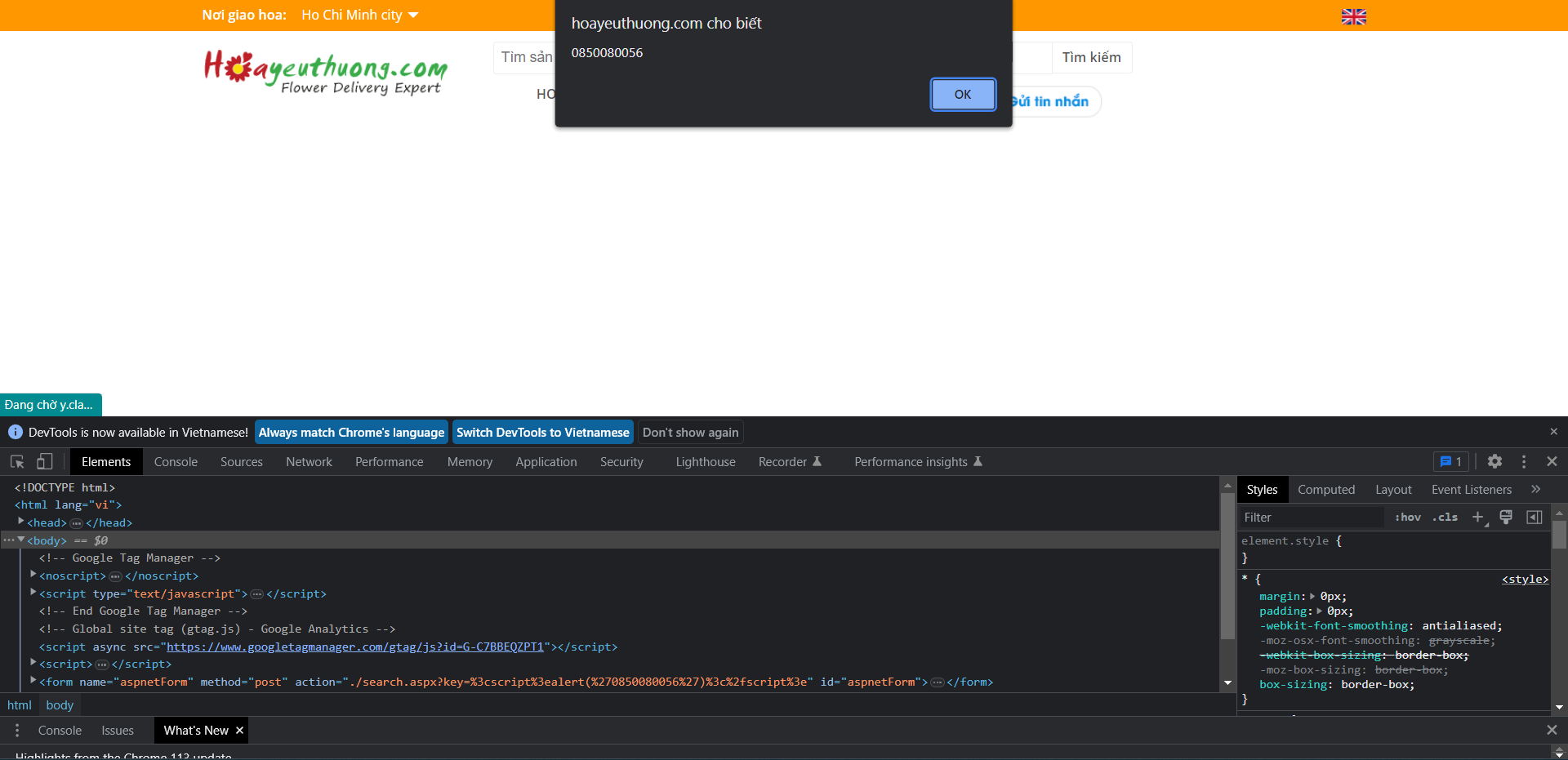


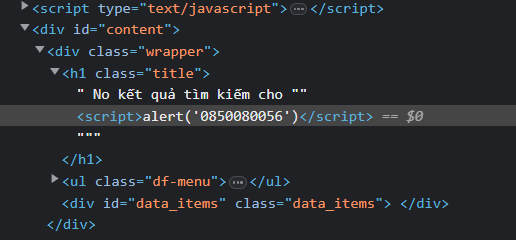
- Xác định giá trị đầu vào xuất hiện trong trang kết quả:

****

**-** Có thể chèn đoạn javascript ở tham số kết quả “cây”:

- Chèn giá trị alert(‘0850080056’):

**

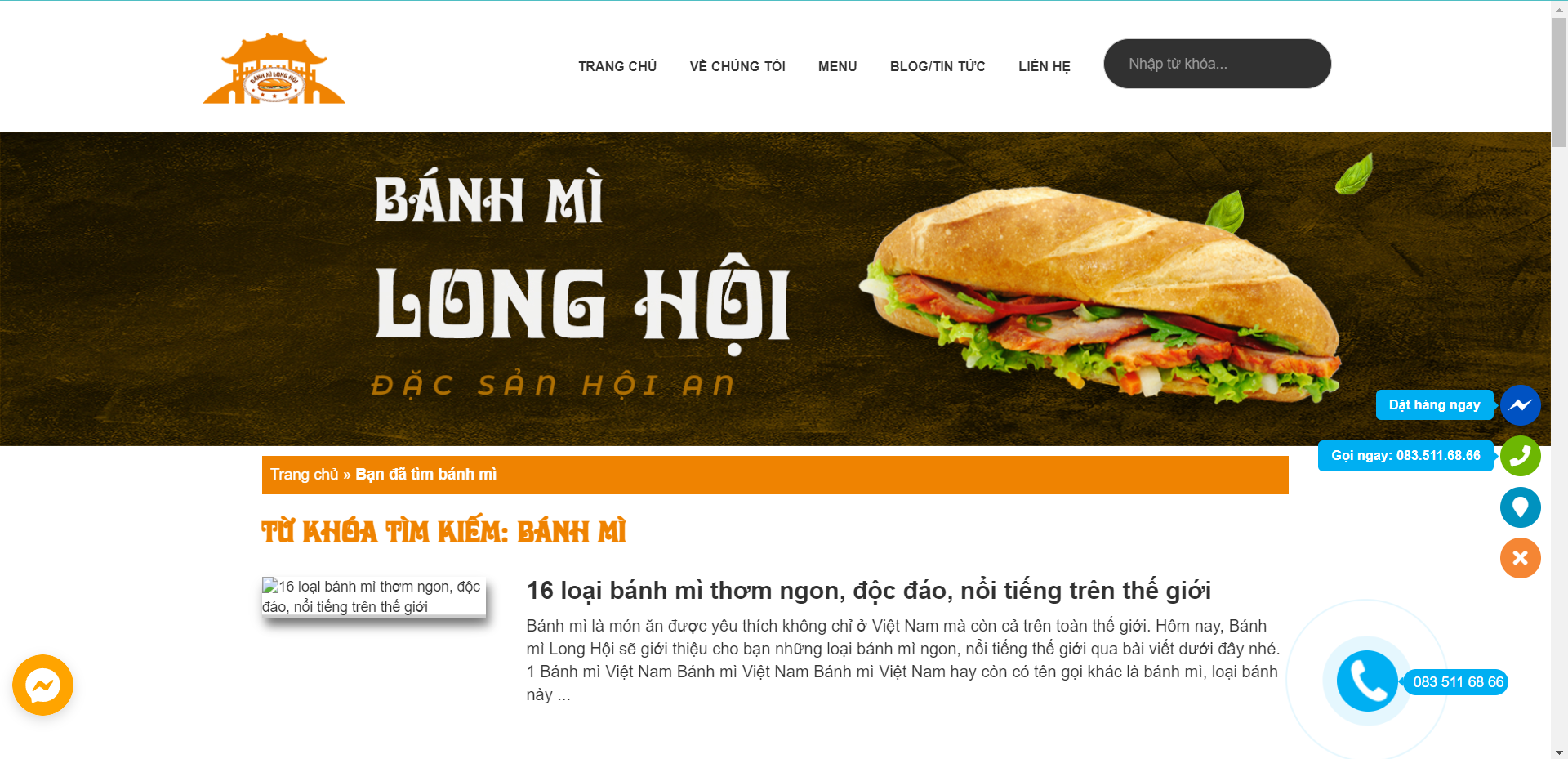


**Câu 2: https://banhmilonghoi.vn/**

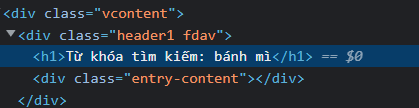
Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa tên của sinh viên. Điểm cho mỗi tham số đầu vào đã kiểm thử được:

**-** Xác định các tham số đầu vào: `**s=`**

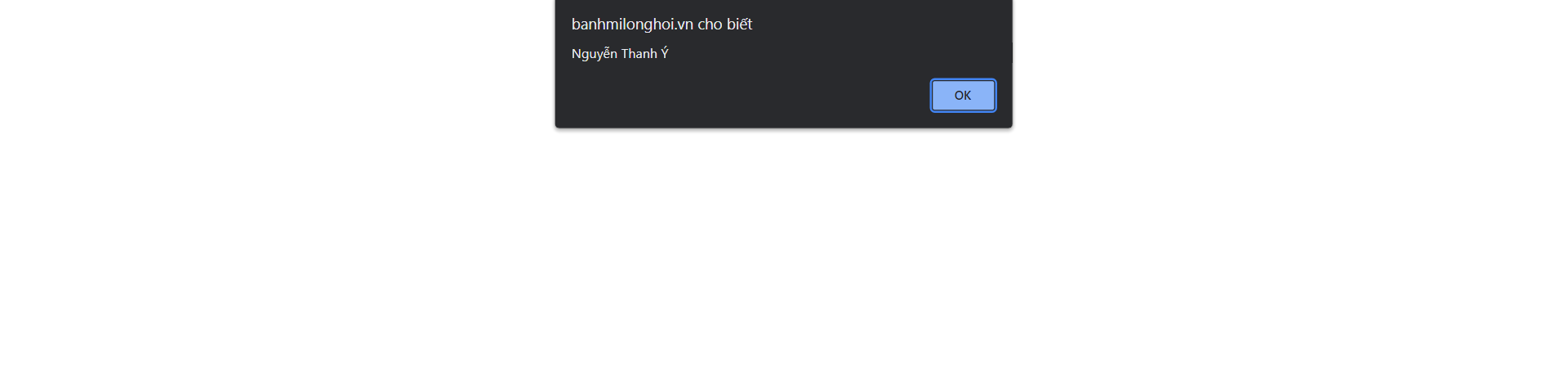
- Xác định giá trị đầu vào xuất hiện trong trang kết quả:

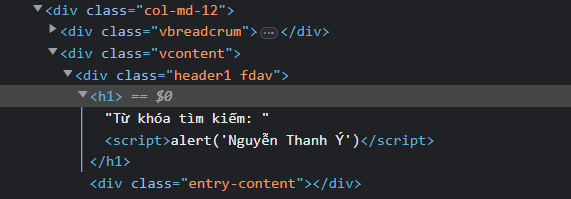
****

**-** Trang web sẽ nhận dữ liệu từ khoá và cho vào thẻ h1



Nên chúng ta sẽ chèn 1 đoạn javascript vào đây

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

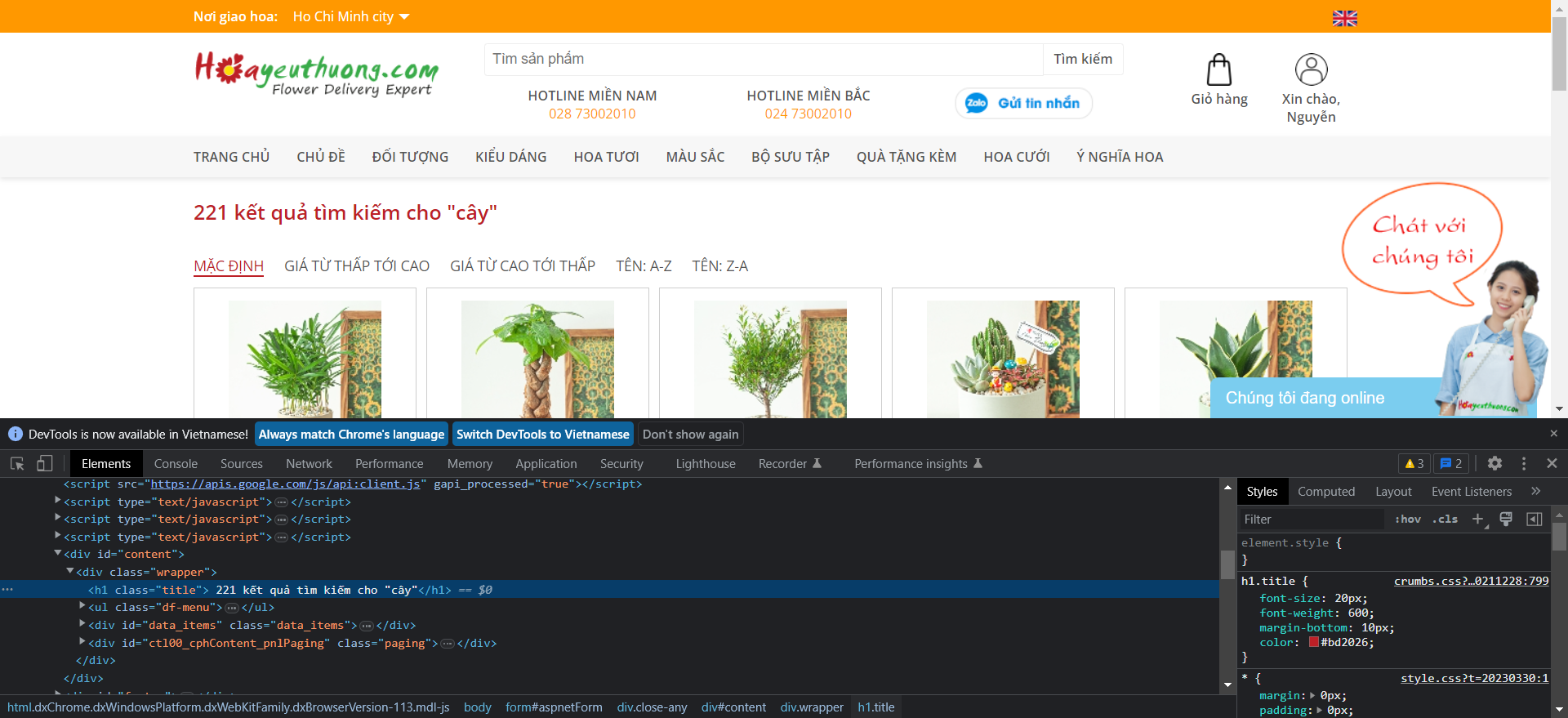
**

**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:

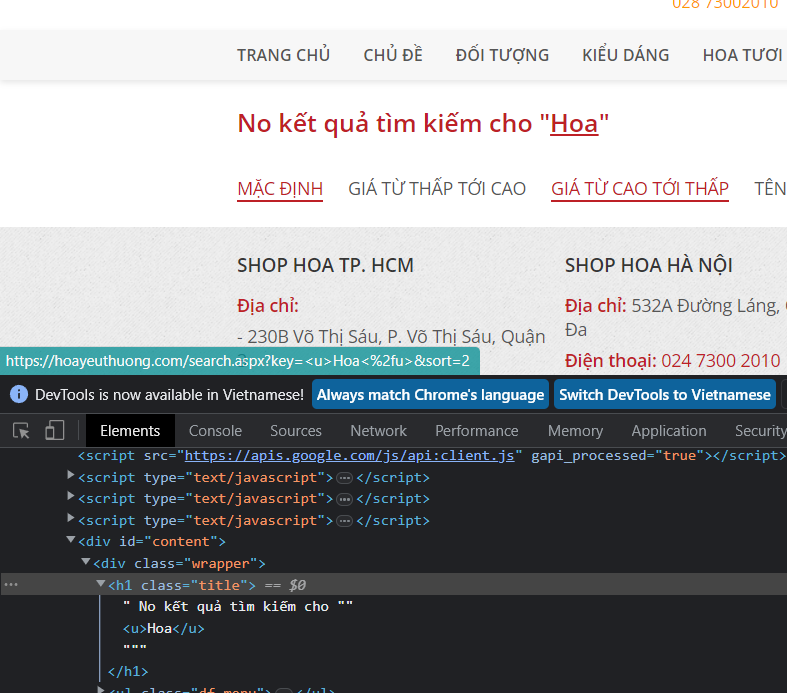
**-** Xác định các tham số đầu vào: **`key=`**

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

****

**-** Thử gạch chân từ khoá tìm kiếm bằng lệnh <u>hoa</u>

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



**Phần 2: Kiểm thử CSRF (2 điểm)**