**BÁO CÁO BÀI THỰC HÀNH SỐ 4**

**KIỂM THỬ LỖ HỔNG XSS và CSRF**

Họ và tên: Phạm Lê Nhật Quang

Link Youtube: https://youtu.be/hQQ-LEQYTmw/

Yêu cầu kết quả thực hành:

Báo cáo kết quả thực hành có tên theo định dạng HoTenSV\_MSSV\_Lab04.docx

Trình bày quá trình kiểm thử theo mẫu sau

Phần 1: Kiểm thử XSS

Thực hiện kiểm thử lỗ hổng XSS trên một trang website: http://testphp.vulnweb.com/

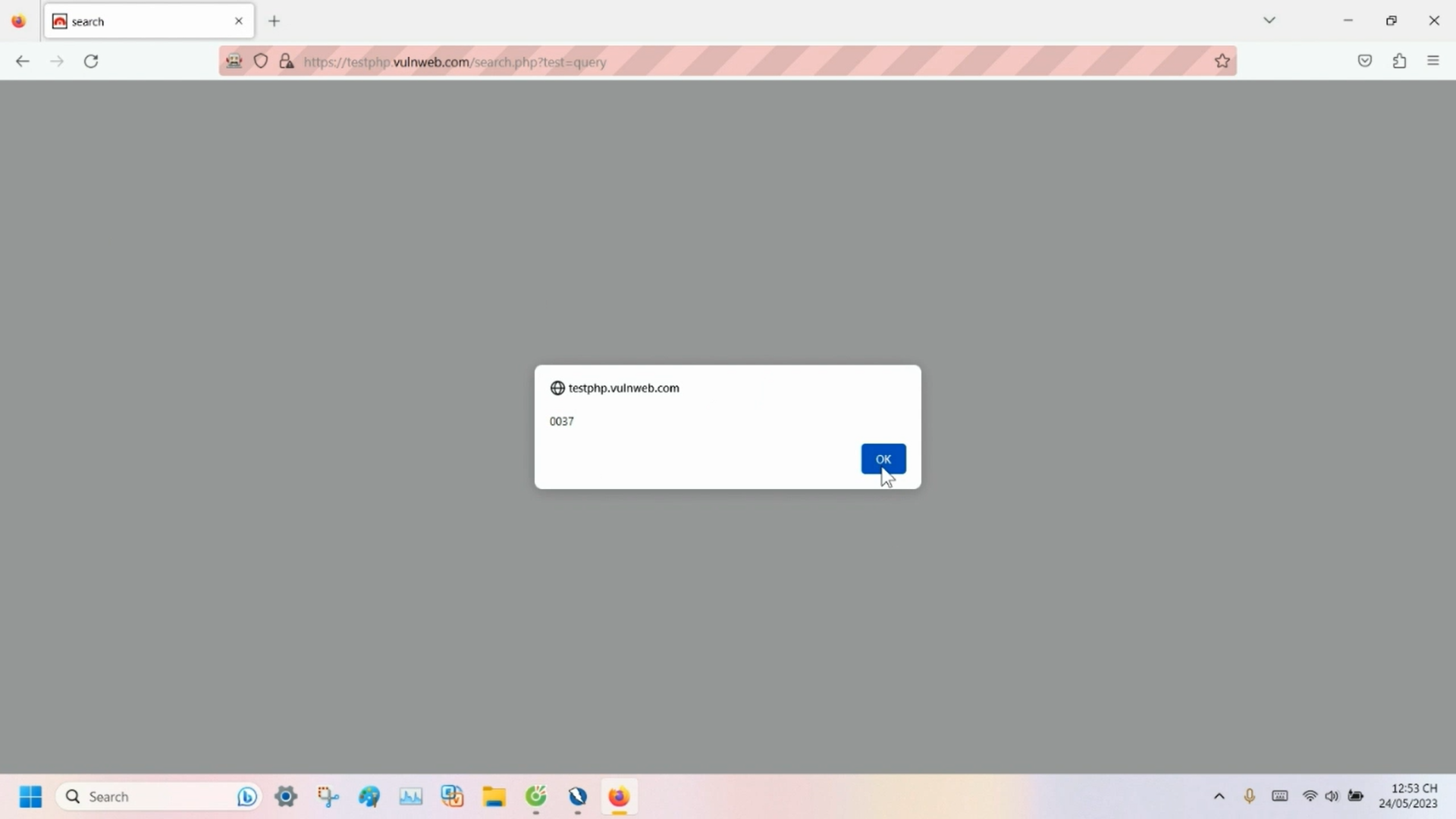
Câu 1

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:

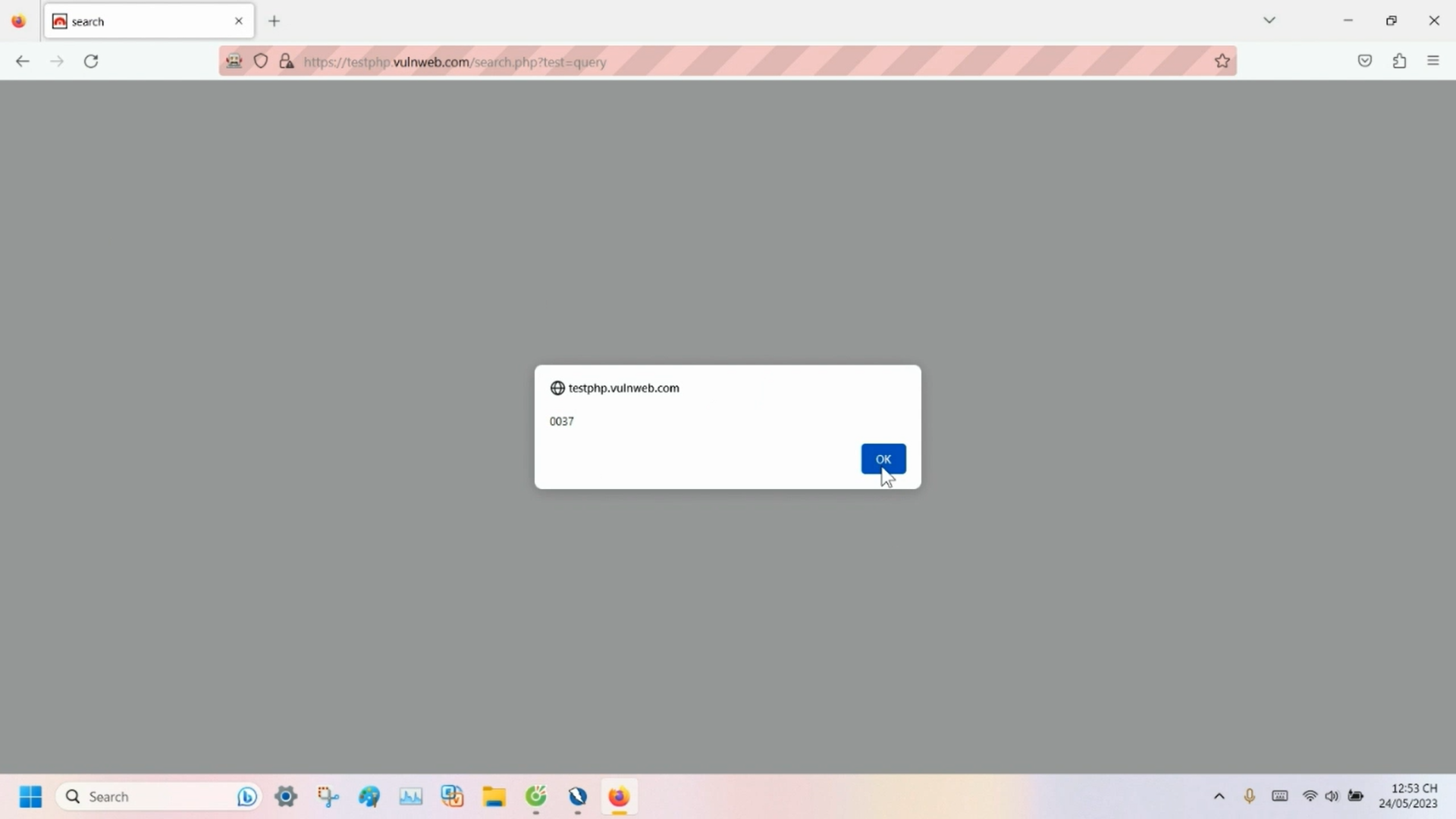
- Xác định các tham số đầu vào: 0.25 điểm

Trả lời: **<script>alert(‘0037’)</script>**



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

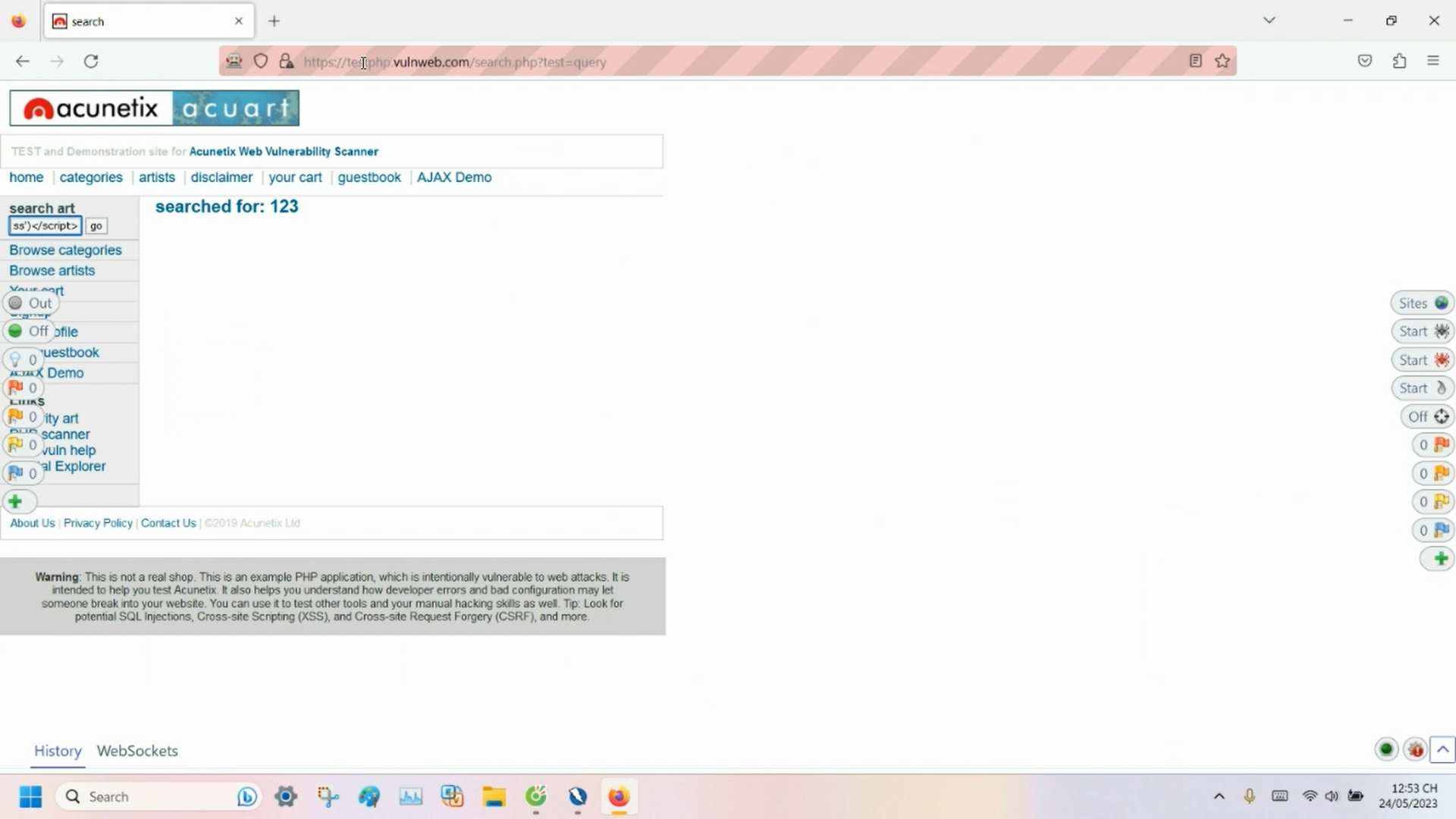
**Trả lời: 0037**



- Các bước kiểm thử và phán đoán: 0-1 điểm theo các bước kiểm thử và logic trong phán đoán

**Trả lời: Chèn thẻ <b> 0037 </b> cho kết quả in đậm**

**Suy đoán trang Web bị lỗi XXS**



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

Trả lời:

* Nếu thông báo hiển thị "0037", điều này cho thấy rằng giá trị đầu vào của bạn không được xử lý một cách an toàn và lỗ hổng XSS đã được khai thác thành công.
* Lỗ hổng XSS xảy ra khi trang web không chặn hoặc không mã hóa đúng các ký tự đặc biệt như "<", ">", "'", """ và "&", từ đó cho phép mã độc chèn vào trang và được thực thi trên trình duyệt của người dùng.
* Khi lỗ hổng XSS được khai thác, mã <script>alert('0037')</script> sẽ được chèn và thực thi, và một thông báo xuất hiện với nội dung là "0037".

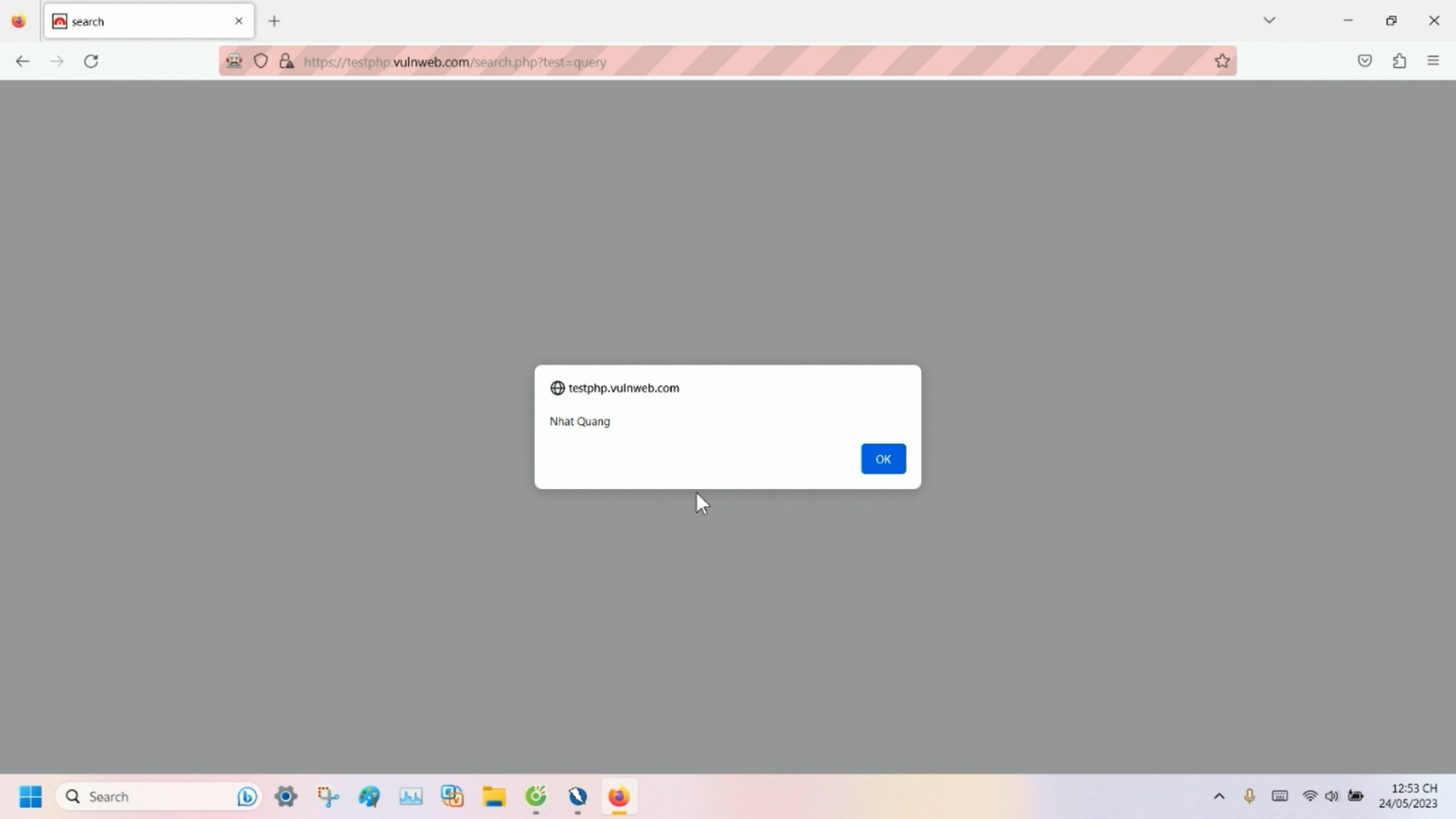
Câu 2

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:

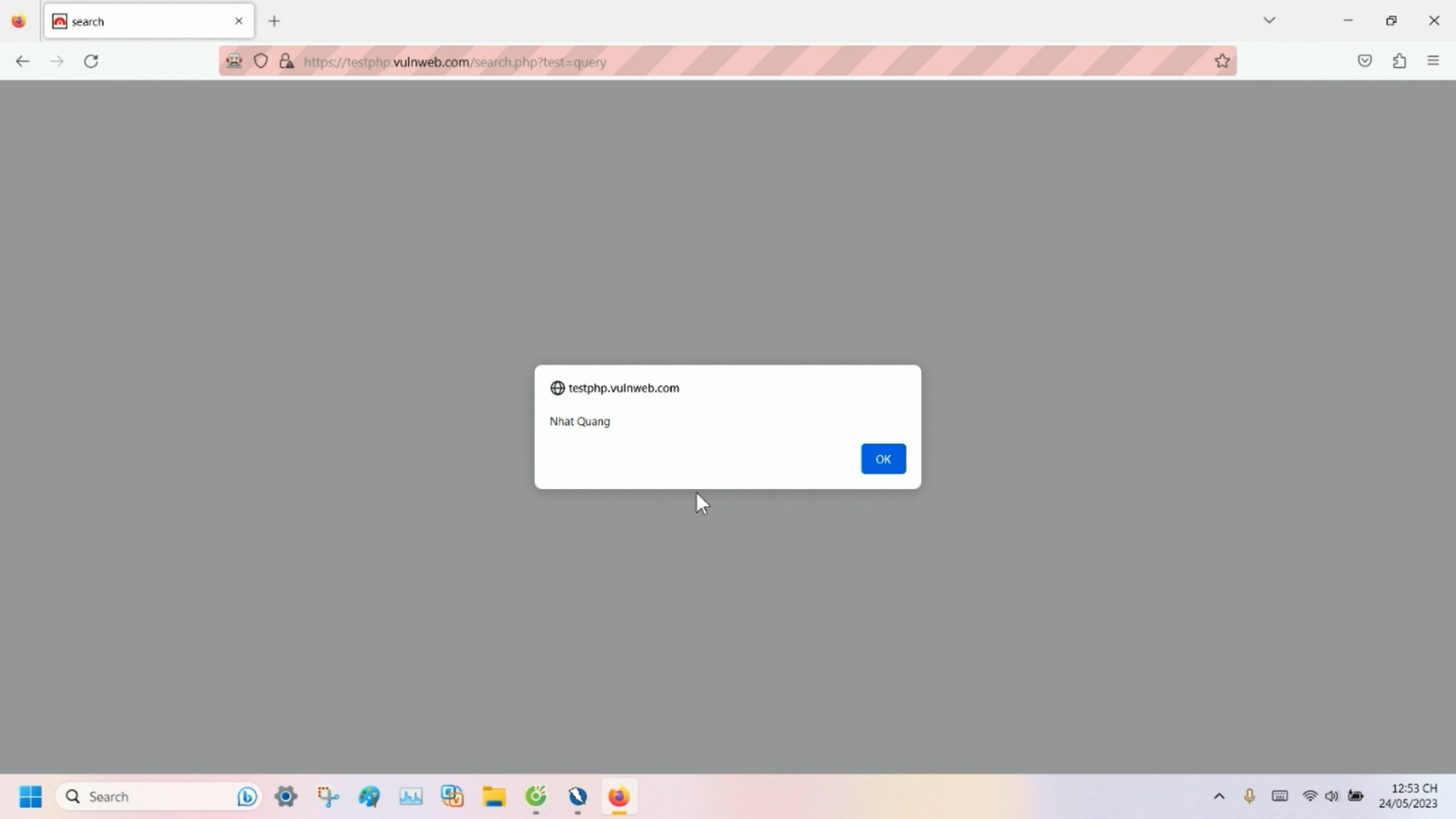
- Xác định các tham số đầu vào: 0.25 điểm

Trả lời: **<script>alert(‘quang’)</script>**



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

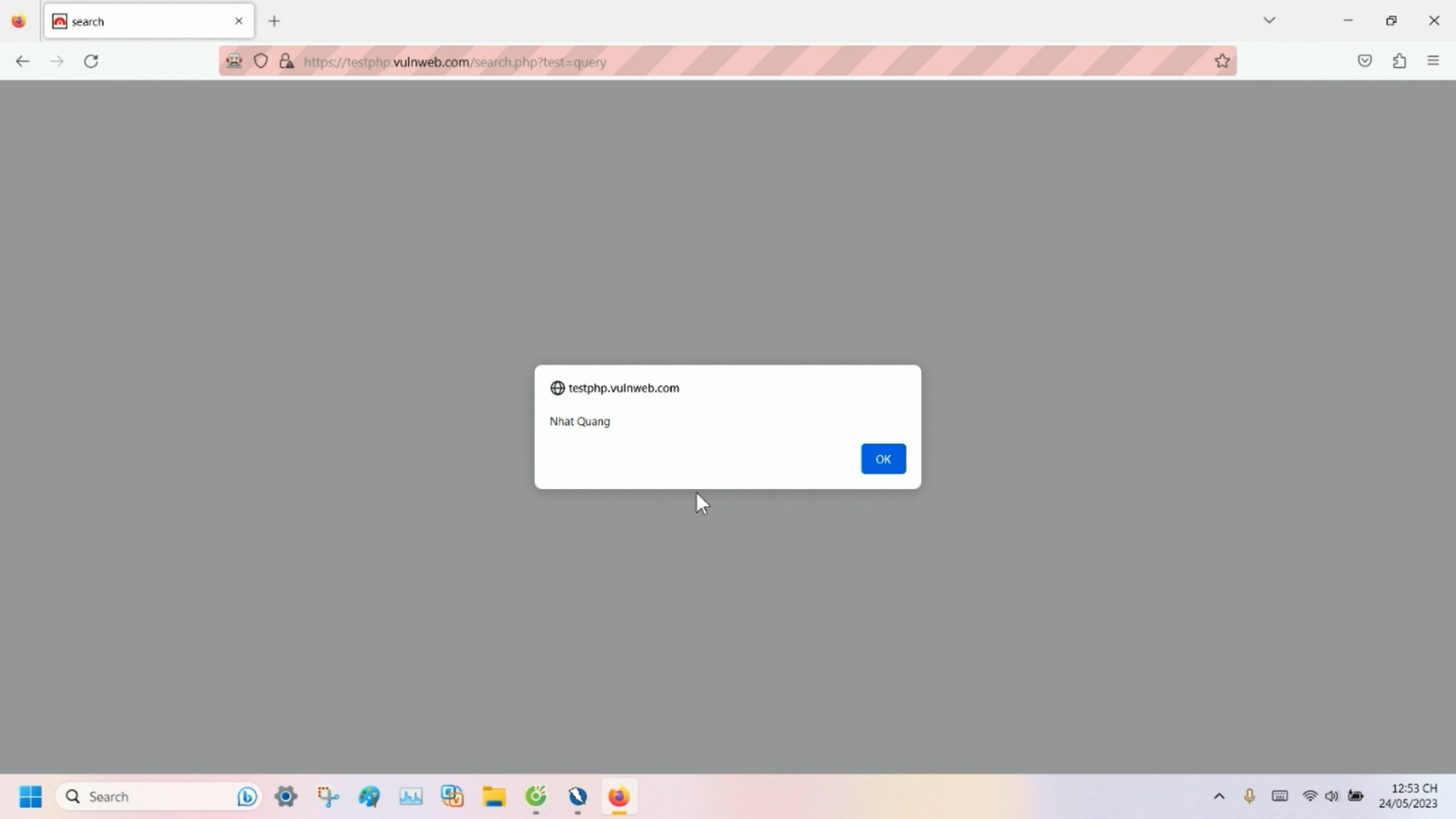
**Trả lời: quang**



- Các bước kiểm thử và phán đoán: 0-1 điểm theo các bước kiểm thử và logic trong phán đoán

**Chèn thẻ <b> quang </b> cho kết quả in đậm**

**Suy đoán trang Web bị lỗi XXS**



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

Trả lời:

* Nếu thông báo hiển thị "quang", điều này cho thấy rằng giá trị đầu vào của bạn không được xử lý một cách an toàn và lỗ hổng XSS đã được khai thác thành công.
* Lỗ hổng XSS xảy ra khi trang web không chặn hoặc không mã hóa đúng các ký tự đặc biệt như "<", ">", "'", """ và "&", từ đó cho phép mã độc chèn vào trang và được thực thi trên trình duyệt của người dùng.
* Khi lỗ hổng XSS được khai thác, mã <script>alert('quang')</script> sẽ được chèn và thực thi, và một thông báo xuất hiện với nội dung là "quang".

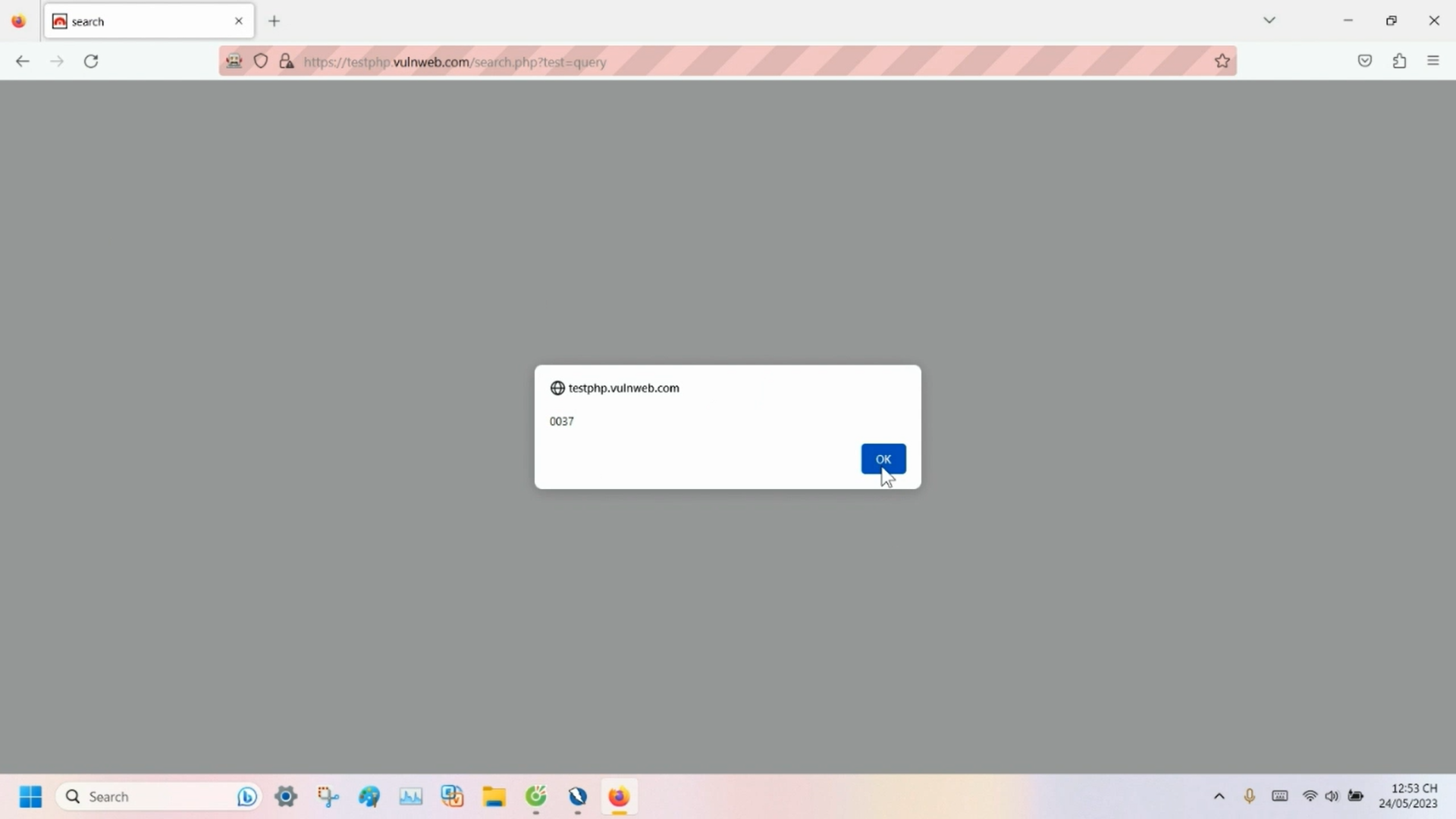
Câu 3

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:

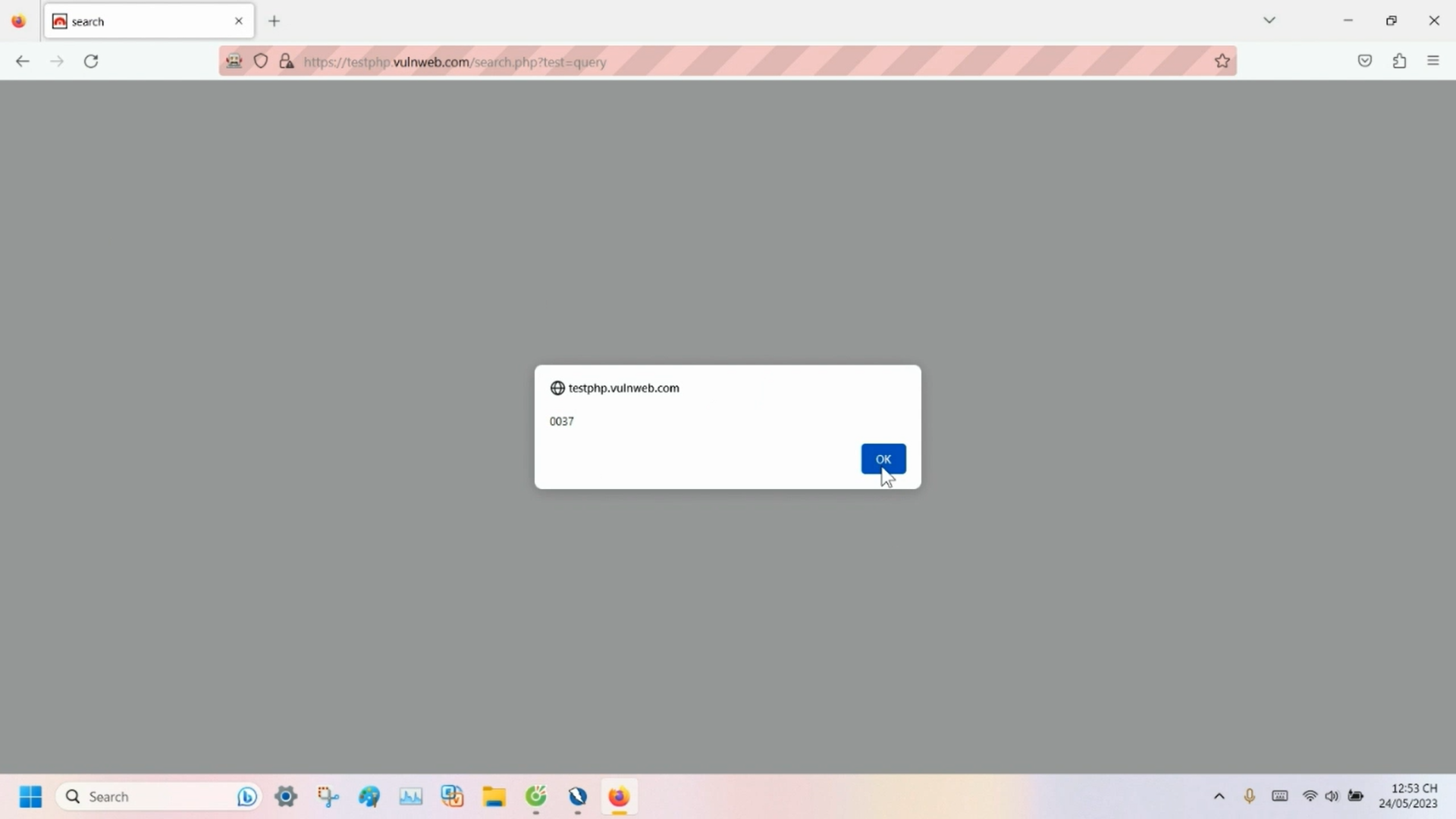
- Xác định các tham số đầu vào: 0.25 điểm

Trả lời: **<script>alert(‘0037’)</script>**



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

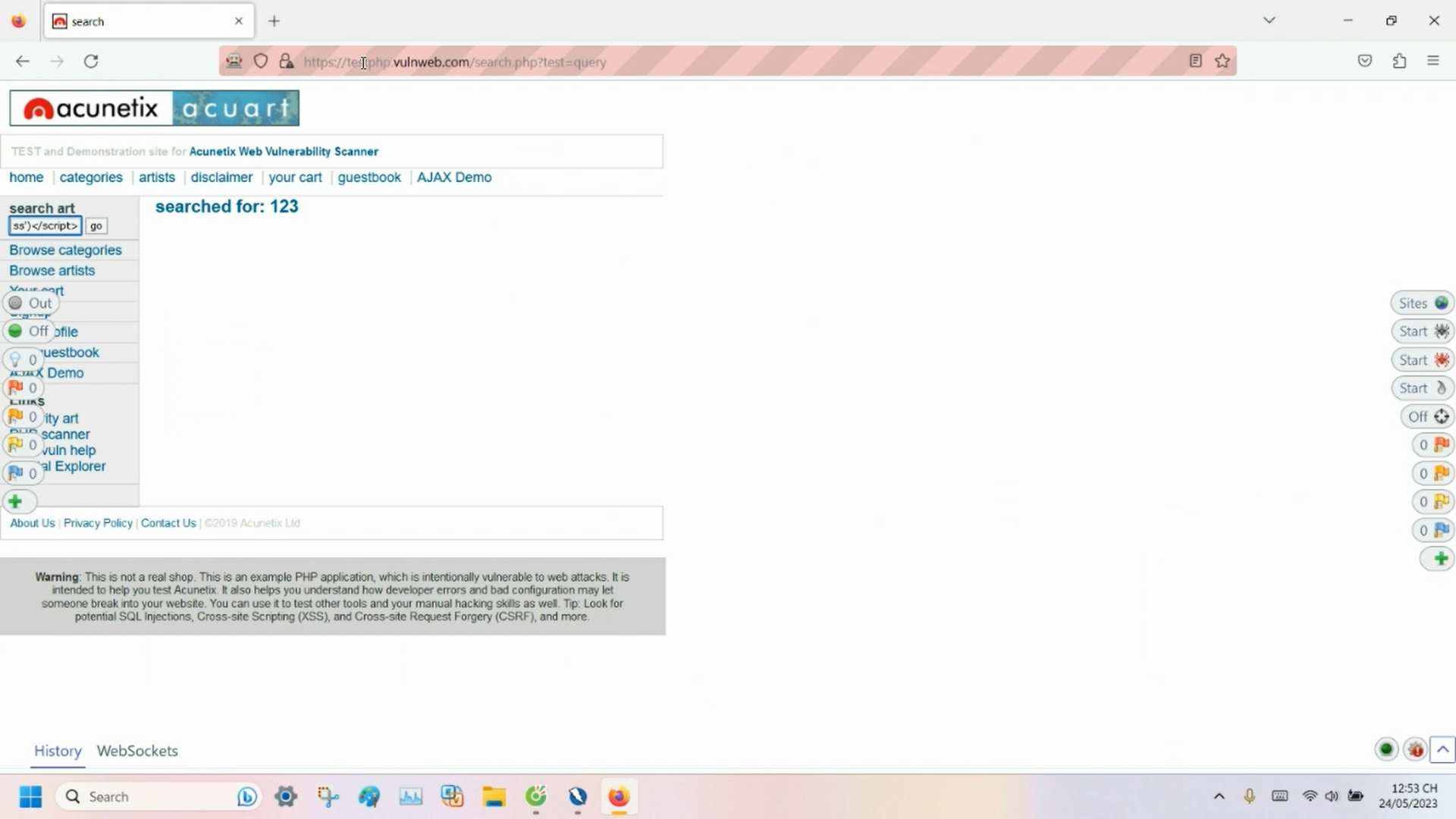
**Trả lời: 0037**



- Các bước kiểm thử và phán đoán: 0-1 điểm theo các bước kiểm thử và logic trong phán đoán

**Trả lời: Chèn thẻ <b> 0037 </b> cho kết quả in đậm**

**Suy đoán trang Web bị lỗi XXS**



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

Trả lời:

* Nếu thông báo hiển thị "0037", điều này cho thấy rằng giá trị đầu vào của bạn không được xử lý một cách an toàn và lỗ hổng XSS đã được khai thác thành công.
* Lỗ hổng XSS xảy ra khi trang web không chặn hoặc không mã hóa đúng các ký tự đặc biệt như "<", ">", "'", """ và "&", từ đó cho phép mã độc chèn vào trang và được thực thi trên trình duyệt của người dùng.
* Khi lỗ hổng XSS được khai thác, mã <script>alert('0037')</script> sẽ được chèn và thực thi, và một thông báo xuất hiện với nội dung là "0037".

Phần 2: Kiểm thử CSRF (2 điểm)

Trình bày các bước thực hiện và kết quả kiểm thử lỗ hổng CSRF trên một trang website

Bước 1: Xác định yêu cầu đích

Phân tích trang web http://testphp.vulnweb.com/để xác định yêu cầu cần tấn công CSRF. Trong trường hợp này, yêu cầu cần tấn công là thay đổi địa chỉ giao hàng thông qua yêu cầu POST đến http://testphp.vulnweb.com/update-address.

Bước 2: Tạo trang web độc hại

Tạo một trang web độc lập, được kiểm soát bởi kẻ tấn công, có chứa mã độc thực hiện yêu cầu CSRF. Ví dụ, tạo một trang web độc hại tại http://evil.com/csrf.html.

Bước 3: Tạo yêu cầu giả mạo

Trên trang web độc hại http://evil.com/csrf.html, tạo một biểu mẫu HTML để tạo yêu cầu giả mạo.

Ví dụ, tạo một biểu mẫu có phương thức POST và hành động (action) là http://testphp.vulnweb.com//update-address, với các trường (input fields) chứa thông tin cần thiết như địa chỉ giao hàng mới.

Bước 4: Tấn công trang web mục tiêu

Gửi yêu cầu giả mạo từ trang web độc hại http://evil.com/csrf.html đến trang web http://testphp.vulnweb.com//update-address.

Đảm bảo rằng yêu cầu được thực hiện tự động khi người dùng truy cập trang web độc hại, ví dụ: bằng cách đưa liên kết độc hại trong một email.

Bước 5: Kiểm tra kết quả

Kiểm tra kết quả của yêu cầu giả mạo. Nếu thành công, địa chỉ giao hàng trên trang web http://testphp.vulnweb.com/sẽ bị thay đổi thành địa chỉ mới được định nghĩa trong yêu cầu giả mạo.

Để kiểm tra, bạn có thể thử đăng nhập vào tài khoản của người dùng và kiểm tra xem địa chỉ giao hàng đã thay đổi hay không.

Lưu ý rằng kết quả kiểm thử CSRF sẽ phụ thuộc vào việc trang web http://testphp.vulnweb.com/đã áp dụng biện pháp bảo mật chống CSRF hay không. Nếu trang web không áp dụng các biện pháp bảo mật phù hợp, kiểm thử CSRF có thể thành công và địa chỉ giao hàng sẽ bị thay đổi không mong muốn.