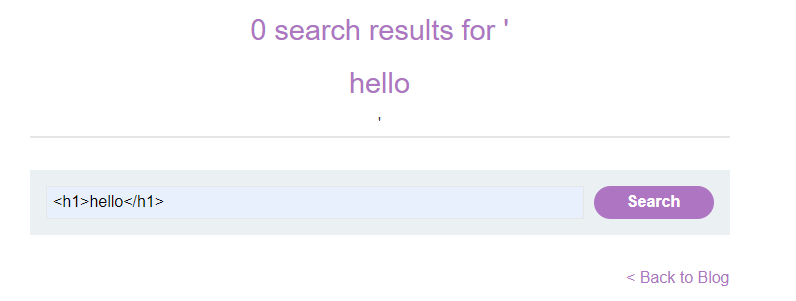
Mai Quốc Việt – 21IT595 – Bài 1 - XSS

Trong bài tập này, ta đang tương tác với chức năng tìm kiếm của trang web. Khi em nhập một từ khóa vào ô tìm kiếm và nhấn "Search", trang web sẽ trả lại kết quả tương ứng với từ khóa đó. Nếu từ khóa bạn nhập vào được đưa trực tiếp vào trang HTML mà không qua quá trình kiểm tra hoặc mã hóa đặc biệt, nó có thể dẫn đến lỗ hổng Reflected XSS.

Nên em đã thử tìm kiếm trên thanh tìm kiếm là <h1>hello</h1> để kiểm thử



ở đây ta có thể thấy, thay vì trang web tìm kiếm kí tự em nhập vào là <h1>hello</h1> thì nó lại chỉ tìm mỗi chữ hello. về lý thuyết, trang web phải xử lý an toàn đầu vào này. Cụ thể, trang web nên hiển thị từ khóa tìm kiếm theo đúng ngữ cảnh mà nó được nhập vào, nhưng đồng thời không cho phép các thẻ HTML hoặc JavaScript được thực thi.

Điều này cho thấy trang web không an toàn và dễ bị tấn công XSS, vì nó cho phép các đoạn mã HTML và JavaScript do người dùng nhập vào được thực thi trên trình duyệt.

* Trang web không an toàn (có lỗ hổng XSS): Sẽ không mã hóa các ký tự đặc biệt, và dẫn đến việc các thẻ HTML hoặc JavaScript được thực thi, tạo ra rủi ro bảo mật như tấn công XSS

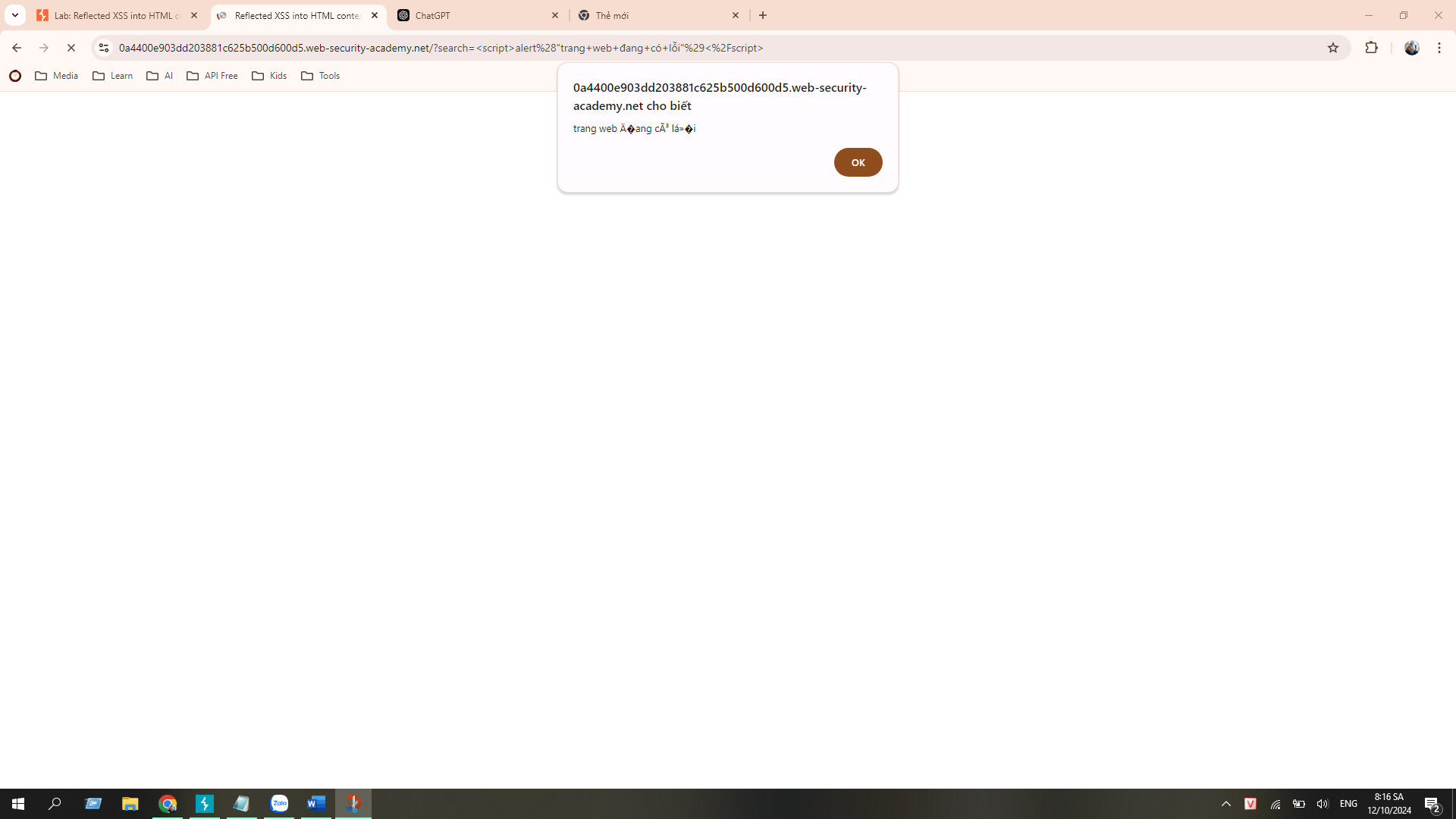
payload là đoạn mã hoặc dữ liệu được chèn vào một ứng dụng web để kiểm tra xem lỗ hổng có tồn tại hay không. Khi nói đến XSS payload, nó thường là một đoạn mã JavaScript được thiết kế để thực thi trên trình duyệt của người dùng nếu lỗ hổng tồn tại.

Với bài tập này, yêu cầu là thực hiện một cuộc tấn công Reflected XSS bằng cách hiển thị một hộp thoại cảnh báo (alert box). Vì vậy, payload bạn cần sử dụng để khai thác lỗ hổng XSS của trang web là:

<script>alert("trang web đang có lỗi")script>

Sau đó em sẽ dán đoạn code trên vào thanh tìm kiếm và searrch

Kết quả nhật được



Như vậy em đã chứng tỏ được

Trang web không mã hóa đầu vào: Thay vì hiển thị an toàn chuỗi ký tự bạn đã nhập, trang web đã cho phép trình duyệt thực thi đoạn mã JavaScript này. Điều này cho thấy trang web không áp dụng biện pháp bảo mật như mã hóa hoặc lọc các ký tự đặc biệt như <script>. Reflected XSS: Đây là một ví dụ điển hình của lỗ hổng

Reflected XSS. Lỗ hổng này cho phép kẻ tấn công chèn mã độc (JavaScript) vào một trang web, và mã này sẽ được thực thi ngay lập tức trên trình duyệt của người dùng.