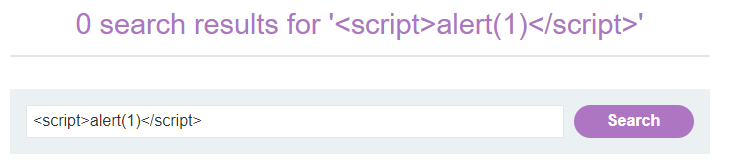
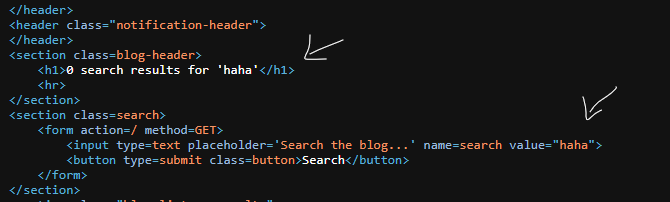
các dấu ngoặc nhọn (<, >) được HTML-encoded (tức là chúng được chuyển thành các ký tự an toàn như &lt;, &gt;) để ngăn việc chèn thẻ HTML thông thường



Thử tìm kiếm với một đoạn ký tự bất kỳ và xem source



Kết quả trên ta thấy đượcc

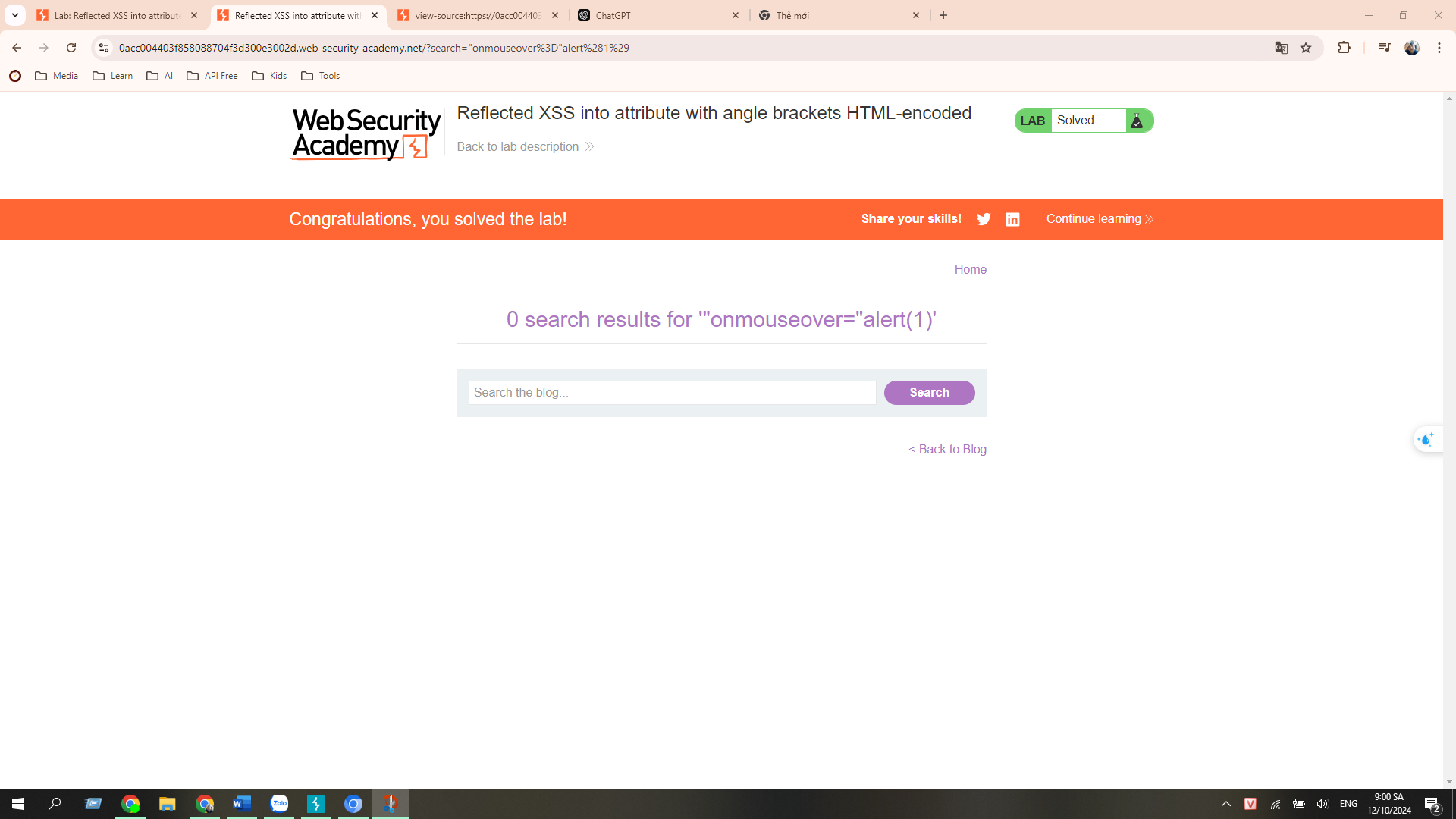
Trong phản hồi từ server, ta sẽ thấy rằng chuỗi bạn vừa nhập xuất hiện bên trong một thuộc tính của thẻ HTML <input value="haha"> . Điều này cho thấy chuỗi đầu vào của ta đã được phản hồi lại trong trang web dưới dạng giá trị của một thuộc tính HTML.

Mục tiêu của em là thoát khỏi dấu ngoặc kép của thuộc tính hiện tại và chèn một sự kiện JavaScript như onmouseover để thực thi mã JavaScript khi di chuột qua phần tử đó.

Payload : " onmouseover="alert(1)

sẽ thoát ra khỏi thuộc tính hiện tại và chèn sự kiện onmouseover, khiến trình duyệt thực thi lệnh alert(1) khi người dùng di chuột qua phần tử này.

Kết quả



Khi di chuột vào thanh input

