SCENARIO

The application contains a reflected cross site scripting vulnerability in the search box functionality where angle brackets are HTML-encoded. We will try to trigger an alert message by injecting a payload into the search box.

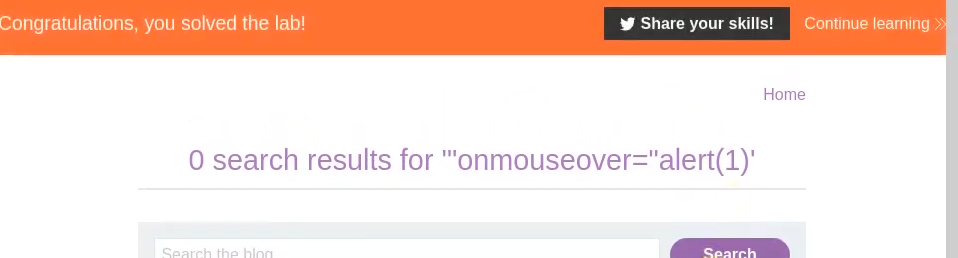
**PROCEDURE**

1. Go to the vulnerable application and try searching for anything.
2. Get the request in BurpSuite’s Interceptor and we see that the string is reflected inside a single quoted attribute.
3. In order to break out of that attribute and execute our malicious script we will try to inject an event handler payload into the BurpSuite’s Repeater and then to solve the lab we will do the same in the browser itself.

**PAYLOAD**

onmouseover='alert(1)

**PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Encode All Characters:** Ensure that all characters, not just angle brackets, are HTML-encoded when reflected back into the webpage. This means converting characters like <, >, ', " and & into their HTML-encoded equivalents (&lt;, &gt;, &apos;, &quot;, and &amp;). This will prevent attackers from breaking out of HTML attributes.
2. **Attribute Value Quoting:** Always use double quotes around attribute values, as this will reduce the chances of attackers breaking out of attributes using a single quote.
3. **Content Security Policy (CSP):** Implement a strong CSP. This will add an extra layer of security by restricting where scripts can be loaded from and disallowing the use of inline scripts.
4. **User Input Validation:** Always validate user input. Even though encoding is critical, validating the input ensures that unexpected values are not processed. Utilize strict input validation methods like regular expressions to ensure only valid input is accepted.