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)

**REMEDIATION**