SCENARIO

The application contains a reflected cross site scripting vulnerability in the search query tracking functionality because it encodes angle brackets before processing. We will try to trigger an alert message by injecting a payload into the application.

**PROCEDURE**

1. Go to the vulnerable application and search for anything.
2. Inspect the source of the HTML page and we can see that our provided string was provided into a javascript string.
3. At the end, we will create a payload to inject into the search.

**PAYLOAD**

';-alert("HACKED!");’

**REMEDIATION**