SCENARIO

The application contains a reflected cross site scripting vulnerability in the search query tracking functionality because angle brackets and double quotes are HTML encoded and single quotes are escaped. 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 in our provided string the single quotes are back slashed and angle brackets are encoded.
3. At the end, we will create a payload to inject into the search to trigger an alert.

**PAYLOAD**

'\';alert(“HACKED!”)//

**REMEDIATION**