SCENARIO

The application contains a stored cross site scripting vulnerability in the comment box functionality, website input field to be specific but inside a template string with angle brackets, single, and double quotes HTML encoded, and backticks escaped. We will try to trigger an alert message by injecting a payload into the application.

**PROCEDURE**

1. Go to the vulnerable application and comment anything in any blog with all fields filled.
2. As we know that the input is enclosed within a JavaScript template literal so we will create the payload accordingly.
3. It will force the application to trigger an alert whenever clicked on the commentor’s name.

**PAYLOAD**

${alert(1)}

**REMEDIATION**