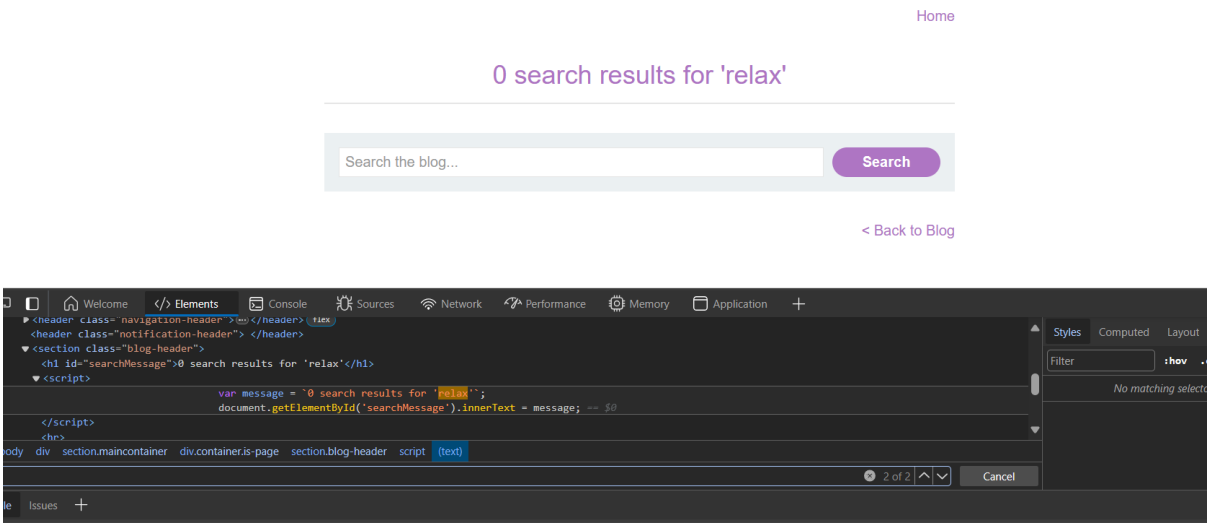
Lab: Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped

S. Giridharan
CB.SC.P2CYS23006

This lab contains a reflected cross-site scripting vulnerability in the search blog functionality. The reflection occurs inside a template string with angle brackets, single, and double quotes HTML encoded, and backticks escaped. To solve this lab, perform a cross-site scripting attack that calls the alert function inside the template string.

Enter your string in the search bar and click ‘Search’.



You can use the search bar in the DOM to easily find your string. It appears two times.Our DOM-browser shows two results for our string: the first within an <h1> tag, and the second below within the <script> tag.

There is the template literal the lab title was telling us about. It is being defined as the variable ‘message’.

The Payload to trigger an Alert is,

${alert()}

Lab: Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped

S. Giridharan
CB.SC.P2CYS23006