Lab: DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded

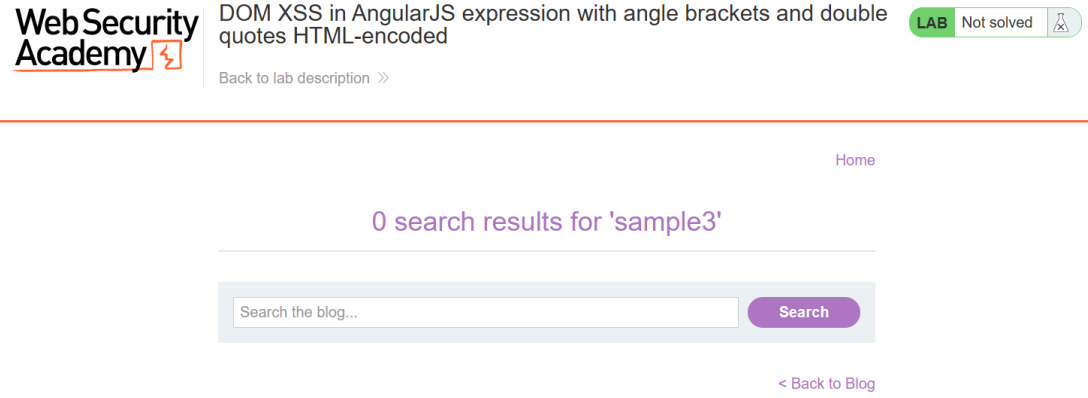
S. Giridharan
CB.SC.P2CYS23006

This lab contains a DOM-based cross-site scripting vulnerability in a AngularJS expression within the search functionality.

AngularJS is a popular JavaScript library, which scans the contents of HTML nodes containing the ng-app attribute (also known as an AngularJS directive). When a directive is added to the HTML code, you can execute JavaScript expressions within double curly braces. This technique is useful when angle brackets are being encoded.

To solve this lab, perform a cross-site scripting attack that executes an AngularJS expression and calls the alert function.

The most trivial example given at the documentation linked above is a simple addition with {{1+2}}. So using sample{{1+2}} as search term, the search term is displayed as:



We can use this vulnerability to trigger an alert event,

hello{{$on.constructor('alert(1)')()}}

Lab: DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded

S. Giridharan
CB.SC.P2CYS23006