SCENARIO

The application contains a simple DOM based cross site scripting vulnerability in the search box functionality which uses **AngularJS** expression in it to search for something, 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.

**PROCEDURE**

1. Go to the vulnerable web application’s home page and search for any string.
2. Open the element inspector tab and got to the page’s source.
3. In there we can see that our searched string is enclosed into an **ng-app directive**.
4. So, now enter the given payload into the search box and we’ll be able to see an alert.

**PAYOAD**

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

**REMEDIATION**