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.

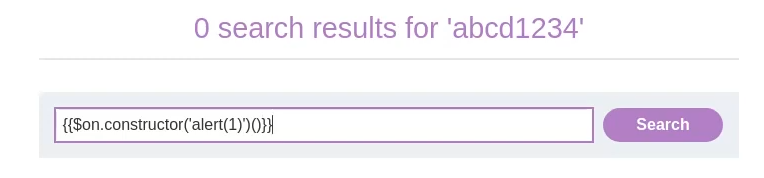
**PROCEDURE**

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)')()}}

**PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Update AngularJS:** Older versions of AngularJS (before 1.6.0) are more susceptible to sandbox escape vulnerabilities. Always keep AngularJS updated to the latest stable version to ensure you have all the security patches.
2. **Avoid User-Controlled Data in AngularJS Expressions:** Never put user-controlled data into AngularJS expressions. Doing so exposes the application to potential expression injection. If user input must be processed, ensure it's handled safely without passing it directly into AngularJS bindings or expressions.
3. **Use AngularJS Strict Contextual Escaping (SCE):** SCE is a mode in which AngularJS requires explicit trust for binding certain types of strings, thus preventing inadvertent execution of content that isn’t intended to be executable.