SCENARIO

The application contains a reflected DOM based cross site scripting vulnerability. Reflected DOM vulnerabilities occur when the server-side application processes data from a request and echoes the data in the response. A script on the page then processes the reflected data in an unsafe way, ultimately writing it to a dangerous sink.

**PROCEDURE**

1. Go to the vulnerable application and search for some random string.
2. Use BurpSuite’s Target page’s Site Map tab.
3. We can see that there is a page named **searchresults.js** which contains all the JavaScript logic code and there’s no code in the page’s source.
4. Study the search requests and try sending different strings to see that we are getting the response as a JSON object.
5. Now we will try to break out of that JSON object by creating a payload based on the response we are getting.
6. In the end, enter the payload into the search box in order to trigger an alert.

**PAYOAD**

\"-alert(1)}//

**REMEDIATION**