SCENARIO

The application implements a Content Security Policy and contains a reflected cross site scripting vulnerability in the search box functionality. We will try to bypass the CSP and exploit the vulnerability to make the application trigger an alert.

**PROCEDURE**

1. Go the vulnerable web applications inject the first payload in the search box.
2. Observe the request in BurpSuite’s Interceptor to find out that we control the CSP’s token/directive value and can change it accordingly.
3. Based on the observations we will create our second payload to inject into the URL which will force the application to generate and alert.
4. The injection uses the script-src-elem directive in CSP. This directive allows you to target just script elements. Using this directive, you can overwrite existing script-src rules enabling you to inject unsafe-inline, which allows you to use inline scripts.

**PAYLOAD**

1. <img src=1 onerror=alert(1)>
2. https://YOUR-LAB-ID.web-security-academy.net/?search=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&token=;script-src-elem%20%27unsafe-inline%27

**REMEDIATION**