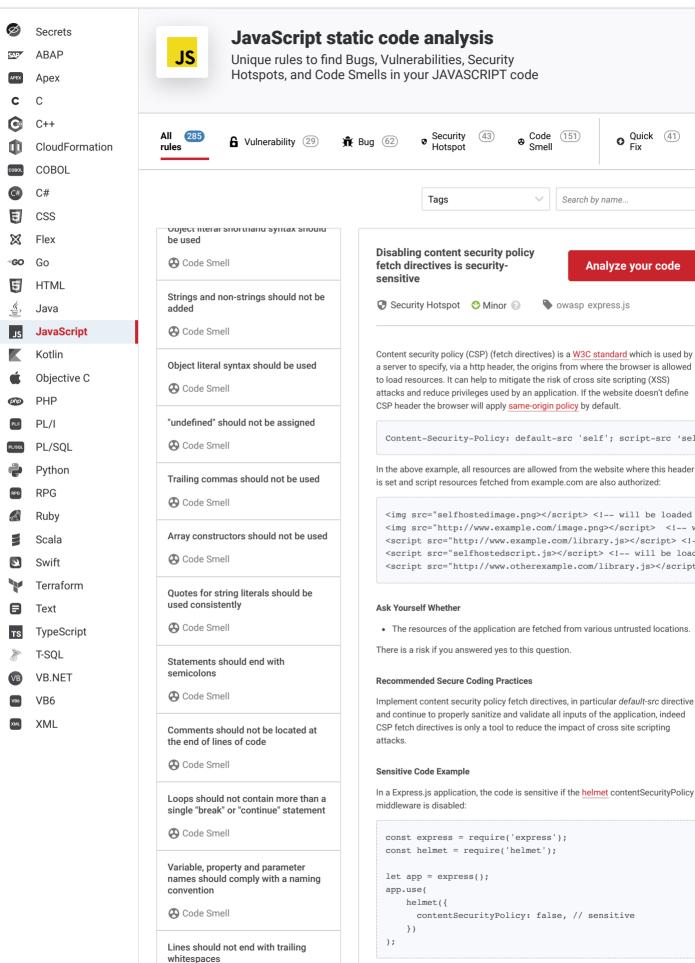


Products ✓

O Quick 41 Fix

(151)

Search by name.



Analyze your code owasp express.js Content security policy (CSP) (fetch directives) is a W3C standard which is used by a server to specify, via a http header, the origins from where the browser is allowed to load resources. It can help to mitigate the risk of cross site scripting (XSS) attacks and reduce privileges used by an application. If the website doesn't define CSP header the browser will apply same-origin policy by default. Content-Security-Policy: default-src 'self'; script-src 'sel In the above example, all resources are allowed from the website where this header is set and script resources fetched from example.com are also authorized: </script> <!-- will be loaded</pre> </script> <!-- w</pre> <script src="http://www.example.com/library.js></script> <!-</pre> <script src="selfhostedscript.js></script> <!-- will be load</pre> <script src="http://www.otherexample.com/library.js></script</pre> • The resources of the application are fetched from various untrusted locations. There is a risk if you answered yes to this question. Implement content security policy fetch directives, in particular default-src directive and continue to properly sanitize and validate all inputs of the application, indeed

Code Smell

JavaScript static code analysis: Disabling content security policy fetch directives is security-sensitive

Files should contain an empty newline at the end

Code Smell

An open curly brace should be located at the end of a line

Code Smell

Tabulation characters should not be used

Code Smell

Function and method names should comply with a naming convention

Code Smell

In a Express.js application, a standard way to implement CSP is the helmet contentSecurityPolicy middleware:

```
const express = require('express');
const helmet = require('helmet');

let app = express();
app.use(helmet.contentSecurityPolicy()); // Compliant
```

See

- OWASP Top 10 2021 Category A5 Security Misconfiguration
- w3.org Content Security Policy Level 3
- OWASP Top 10 2017 Category A6 Security Misconfiguration
- developer.mozilla.org Content Security Policy (CSP)

Available In:

sonarcloud 👌 | sonarqube

© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD are trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved.

Privacy Policy