Security

Hotspot

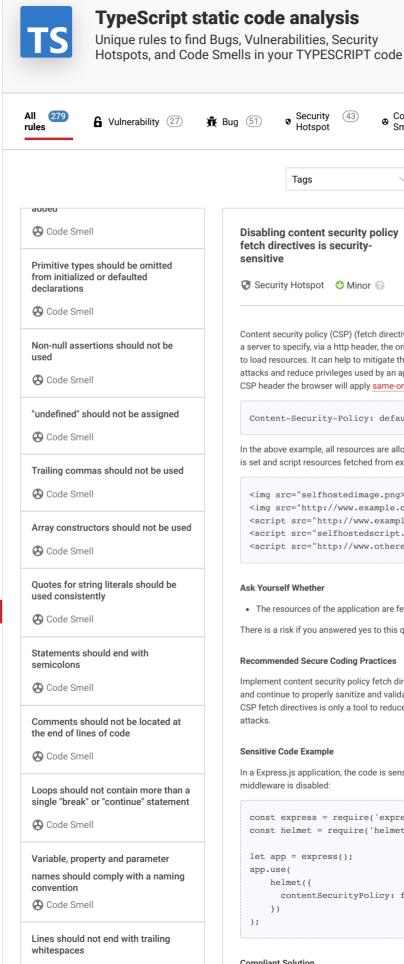
(43)

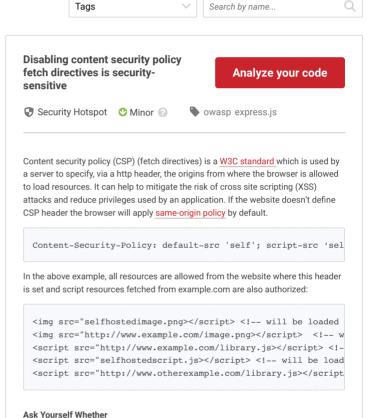


Products ✓

O Quick 50 Fix







⊗ Code

Smell

(158)

## Recommended Secure Coding Practices

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 CSP fetch directives is only a tool to reduce the impact of cross site scripting attacks

• The resources of the application are fetched from various untrusted locations.

## Sensitive Code Example

In a Express.js application, the code is sensitive if the helmet contentSecurityPolicy middleware is disabled:

```
const express = require('express');
const helmet = require('helmet');
let app = express();
app.use(
    helmet({
      contentSecurityPolicy: false, // sensitive
);
```

## **Compliant Solution**

Code Smell

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 <a href="helmet contentSecurityPolicy middleware">helmet contentSecurityPolicy middleware</a>:

```
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