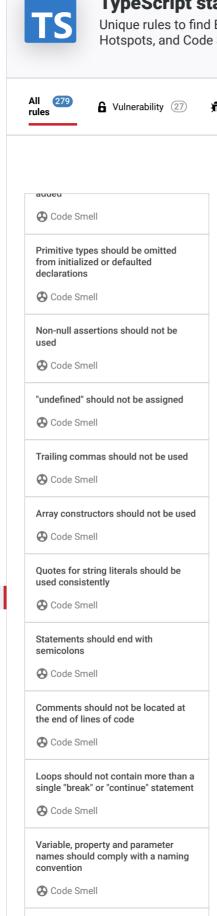


Products >

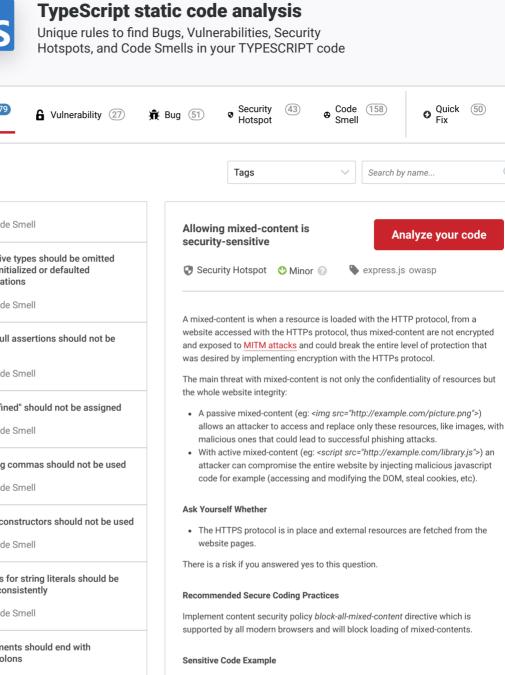




Lines should not end with trailing

whitespaces

Code Smell



supported by all modern browsers and will block loading of mixed-contents.

In Express.js application the code is sensitive if the helmet-csp or helmet middleware is used without the blockAllMixedContent directive

```
const express = require('express');
const helmet = require('helmet');
let app = express();
 helmet.contentSecurityPolicy({
      "default-src": ["'self'", 'example.com', 'code.jquery.
    } // Sensitive: blockAllMixedContent directive is missin
 })
);
```

Compliant Solution

In Express.js application a standard way to block mixed-content is to put in place the **helmet-csp** or **helmet** middleware with the blockAllMixedContent directive: 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

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

let app = express();

app.use(
  helmet.contentSecurityPolicy({
    directives: {
      "default-src": ["'self'", 'example.com', 'code.jquery.
      blockAllMixedContent: [] // Compliant
    }
  })
);
```

See

- OWASP Top 10 2021 Category A5 Security Misconfiguration
- OWASP Top 10 2017 Category A3 Sensitive Data Exposure
- developer.mozilla.org Mixed-content
- developer.mozilla.org Content Security Policy (CSP)
- w3.org Content Security Policy Level 3

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