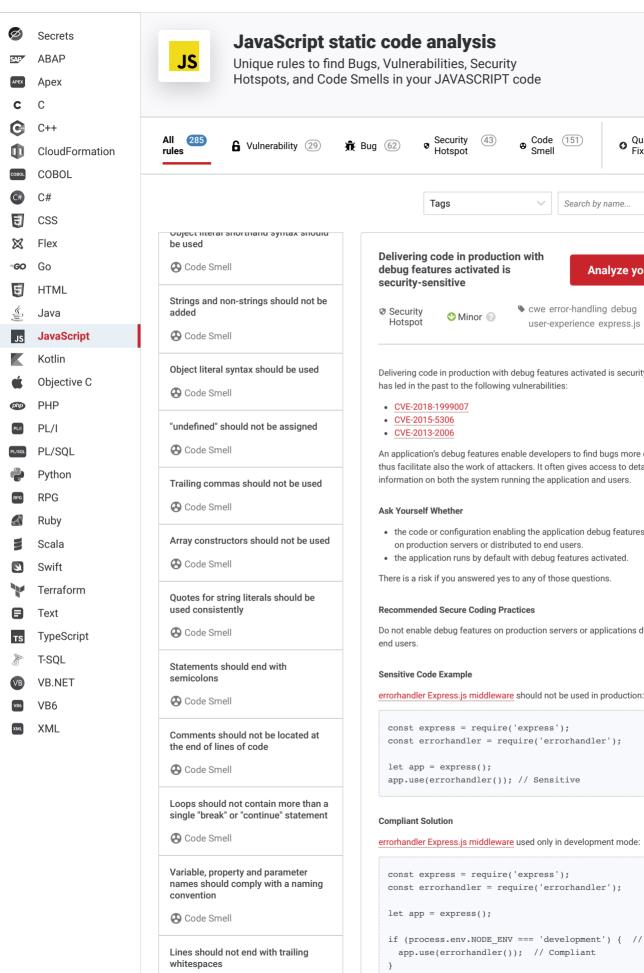


Products >

O Quick 41 Fix

(151)



Search by name. Delivering code in production with Analyze your code cwe error-handling debug user-experience express.js owasp Delivering code in production with debug features activated is security-sensitive. It has led in the past to the following vulnerabilities: An application's debug features enable developers to find bugs more easily and thus facilitate also the work of attackers. It often gives access to detailed information on both the system running the application and users. • the code or configuration enabling the application debug features is deployed on production servers or distributed to end users the application runs by default with debug features activated. There is a risk if you answered yes to any of those questions. **Recommended Secure Coding Practices** Do not enable debug features on production servers or applications distributed to

errorhandler Express.js middleware used only in development mode:

```
const express = require('express');
const errorhandler = require('errorhandler');
if (process.env.NODE ENV === 'development') { // Compliant
  app.use(errorhandler()); // Compliant
```

See

Code Smell

JavaScript static code analysis: Delivering code in production with debug features activated is security-sensitive

Files should contain an empty newline

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

- OWASP Top 10 2021 Category A5 Security Misconfiguration
- OWASP Top 10 2017 Category A3 Sensitive Data Exposure
- MITRE, CWE-489 Active Debug Code
- MITRE, CWE-215 Information Exposure Through Debug Information

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