Security

Hotspot

Tags

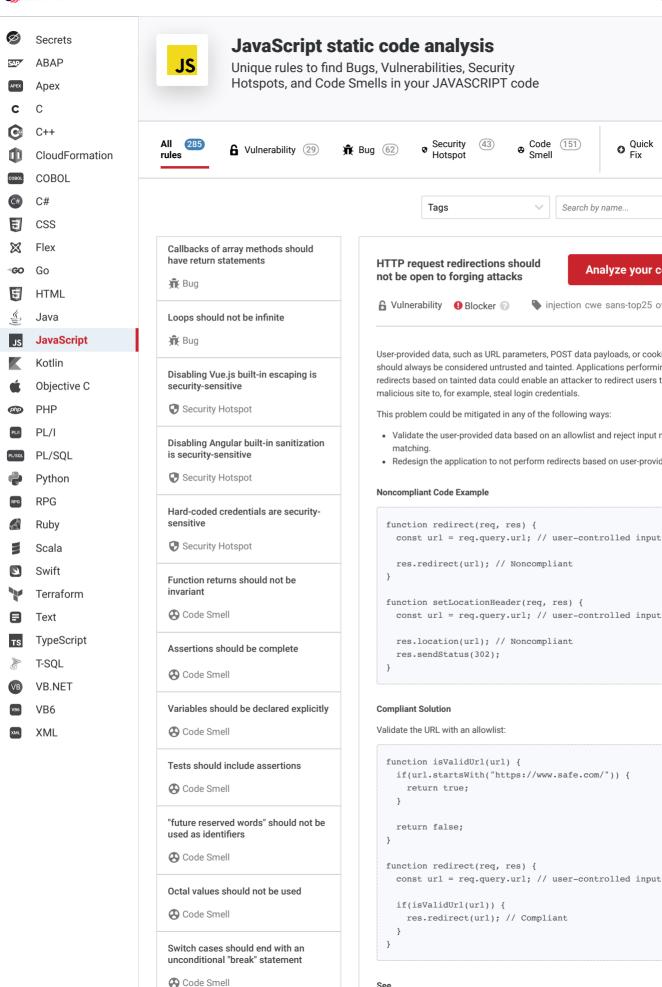
(43)

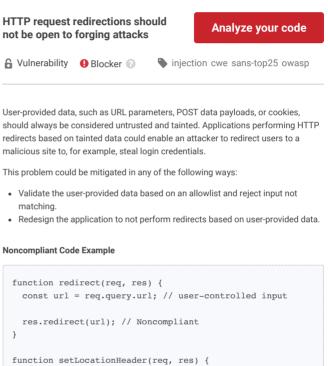


Products >

O Quick 41 Fix

Q





(151)

Search by name.

Compliant Solution

Validate the URL with an allowlist:

```
function isValidUrl(url) {
 if(url.startsWith("https://www.safe.com/")) {
    return true;
 return false;
function redirect(req, res) {
 const url = req.query.url; // user-controlled input
 if(isValidUrl(url)) {
    res.redirect(url); // Compliant
```

• OWASP Top 10 2021 Category A1 - Broken Access Control

"switch" statements should not

JavaScript static code analysis contain non-case labels

Code Smell

A new session should be created during user authentication

Vulnerability

JWT should be signed and verified with strong cipher algorithms

Vulnerability

Cipher algorithms should be robust

Vulnerability

Encryption algorithms should be used with secure mode and padding

OWASP Top 10 2017 Category A5 - Broken Access Control
MITRE, CWE-20 - Improper Input Validation
MITRE, CWE-601 - URL Redirection to Untrusted Site ('Open Redirect')
SANS Top 25 - Risky Resource Management

Available In:

Sonarcloud Sonarqube

Developer
Edition

© 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