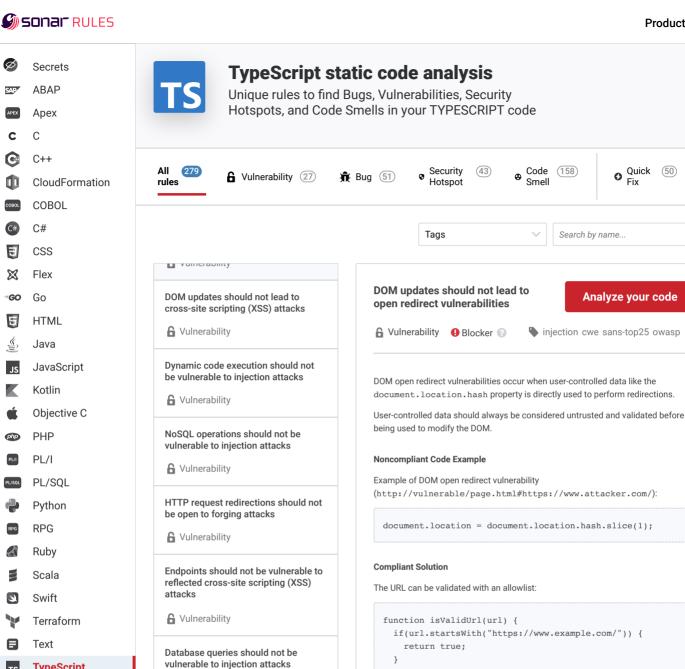


Products >

(50)

O Quick Fix

Analyze your code



if(url.startsWith("https://www.example.com/")) { return false;

document.location = document.location.hash.slice(1);

if(isValidUrl(document.location.hash.slice(1))) {

See

- OWASP Top 10 2021 Category A1 Broken Access Control
- 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



TypeScript T-SQL **VB.NET** VB6 XML

Vulnerability Disabling Vue.js built-in escaping is security-sensitive

XML parsers should not be vulnerable

I/O function calls should not be

OS commands should not be

vulnerable to command injection

vulnerable to path injection attacks

Security Hotspot

Vulnerability

to XXE attacks

Vulnerability

6 Vulnerability

attacks

Disabling Angular built-in sanitization is security-sensitive

Security Hotspot

© 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

Hard-coded credentials are security- sensitive Security Hotspot
Function returns should not be invariant Code Smell
Assertions should be complete Code Smell
Tests should include assertions Code Smell