

Products ∨

O Quick Fix

(435)

Code

Smell

Security

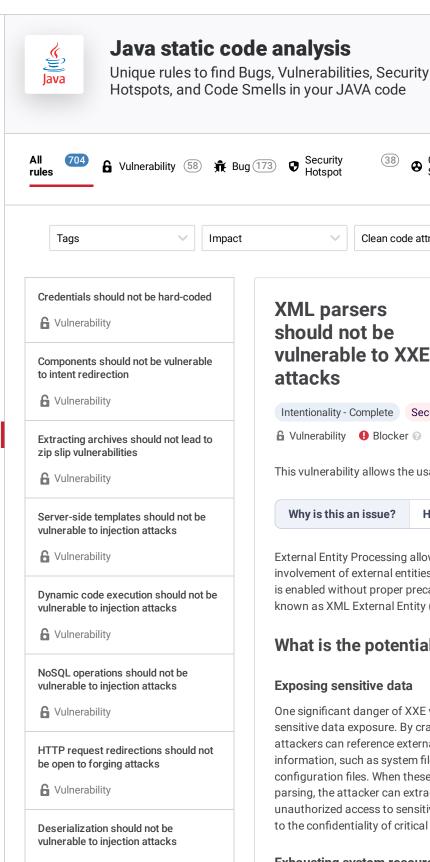


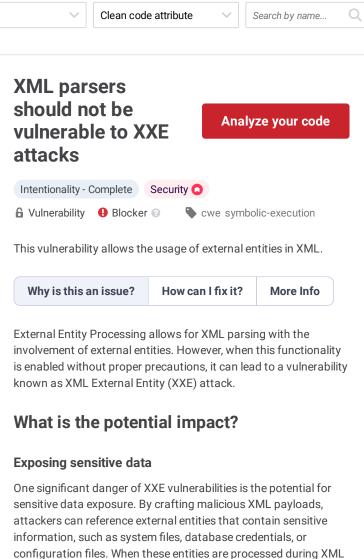
Swift

Text

Terraform

TypeScript





parsing, the attacker can extract the contents and gain

to the confidentiality of critical information.

Exhausting system resources

unauthorized access to sensitive data. This poses a severe threat

T-SOL

VB.NET

VB6

XML

Vulnerability

Endpoints should not be vulnerable to reflected cross-site scripting (XSS) attacks

■ Vulnerability

Database queries should not be vulnerable to injection attacks

■ Vulnerability

A secure password should be used when connecting to a database

6 Vulnerability

XPath expressions should not be vulnerable to injection attacks

♠ Vulnerability

I/O function calls should not be vulnerable to path injection attacks

Vulnerability

LDAP queries should not be vulnerable to injection attacks

6 Vulnerability

OS commands should not be vulnerable to command injection attacks

♠ Vulnerability

"@SpringBootApplication" and "@ComponentScan" should not be used in the default package

📆 Bug

Another consequence of XXE vulnerabilities is the potential for denial-of-service attacks. By exploiting the ability to include external entities, attackers can construct XML payloads that cause resource exhaustion. This can overwhelm the system's memory, CPU, or other critical resources, leading to system unresponsiveness or crashes. A successful DoS attack can disrupt the availability of services and negatively impact the user experience.

Forging requests

XXE vulnerabilities can also enable Server-Side Request Forgery (SSRF) attacks. By leveraging the ability to include external entities, an attacker can make the vulnerable application send arbitrary requests to other internal or external systems. This can result in unintended actions, such as retrieving data from internal resources, scanning internal networks, or attacking other systems. SSRF attacks can lead to severe consequences, including unauthorized data access, system compromise, or even further exploitation within the network infrastructure.

Available In:

sonarlint ⊕ | sonarcloud 🐼 | sonarqube 🕽



© 2008-2024 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.

> Sonar helps developers write Clean Code. Privacy Policy | Cookie Policy