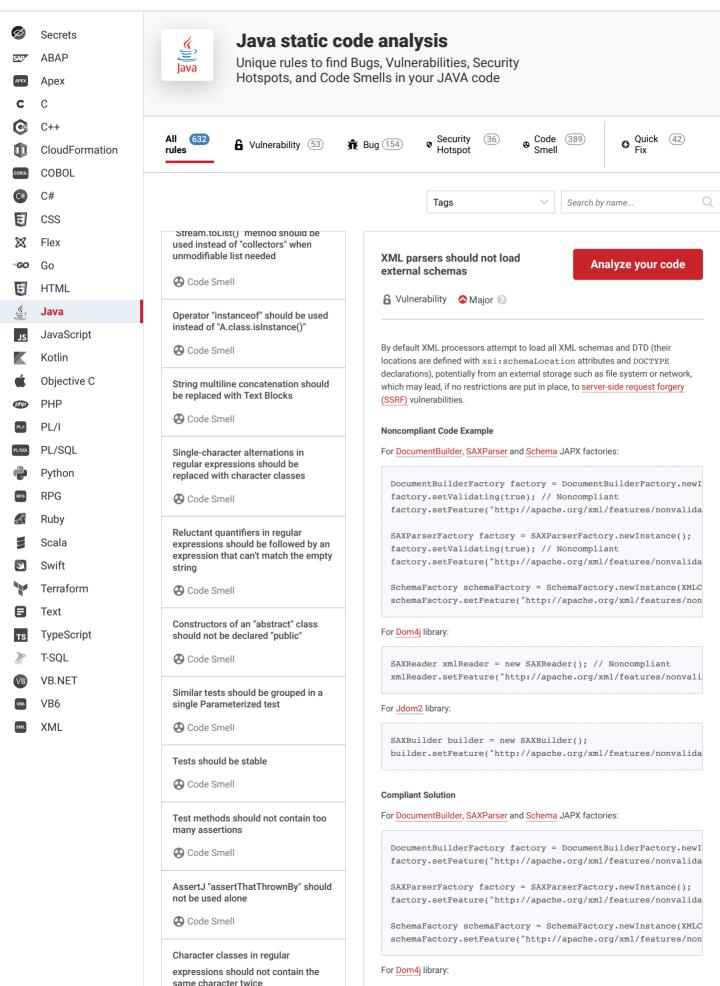


Products ✓



Code Smell

Names of regular expressions named groups should be used

Code Smell

Regexes containing characters subject to normalization should use the CANON_EQ flag

Code Smell

Regular expressions should not be too complicated

Code Smell

JUnit assertTrue/assertFalse should be simplified to the corresponding dedicated assertion SAXReader xmlReader = new SAXReader(); // Noncompliant xmlReader.setFeature("http://apache.org/xml/features/nonvali

For Jdom2 library:

SAXBuilder builder = new SAXBuilder(); builder.setFeature("http://apache.org/xml/features/nonvalida

Exceptions

This rules does not raise an issue when an EntityResolver is set.

DocumentBuilderFactory factory = DocumentBuilderFactory.newI
factory.setValidating(true);
DocumentBuilder builder = factory.newDocumentBuilder();
builder.setEntityResolver(new MyEntityResolver());

SAXBuilder builder = new SAXBuilder();
builder.setFeature("http://apache.org/xml/features/nonvalida builder.setEntityResolver(new EntityResolver());

See

- Oracle Java Documentation XML External Entity Injection Attack
- OWASP Top 10 2017 Category A4 XML External Entities (XXE)
- OWASP XXE Prevention Cheat Sheet
- MITRE, CWE-611 Information Exposure Through XML External Entity Reference
- MITRE, CWE-827 Improper Control of Document Type Definition

Available In:

sonarlint ⊜ 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