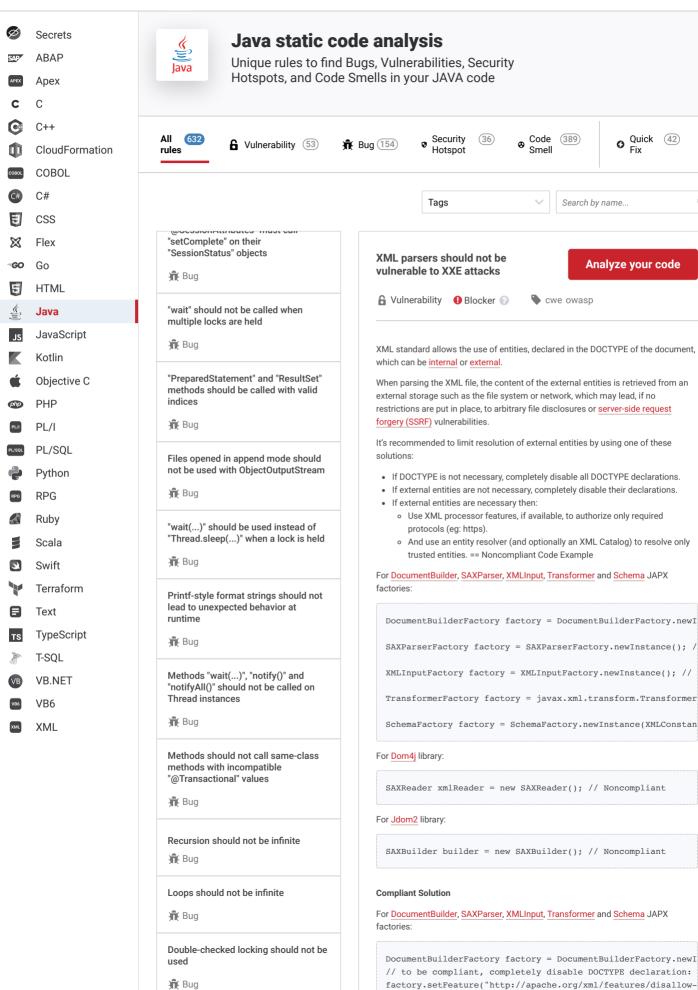


Products ∨



// or completely disable external entities declarations:
factory.setFeature("http://xml.org/sax/features/external-gen

kesources snoula de closea

₩ Bug

Hard-coded credentials are securitysensitive

Security Hotspot

Methods returns should not be invariant

Code Smell

"ThreadGroup" should not be used

Code Smell

"clone" should not be overridden

factory.setFeature("http://xml.org/sax/features/external-par
// or prohibit the use of all protocols by external entities
factory.setAttribute(XMLConstants.ACCESS_EXTERNAL_DTD, "");
factory.setAttribute(XMLConstants.ACCESS_EXTERNAL_SCHEMA, ""
// or disable entity expansion but keep in mind that this do
// and this solution is not correct for OpenJDK < 13 due to
factory.setExpandEntityReferences(false);</pre>

SAXParserFactory factory = SAXParserFactory.newInstance();
// to be compliant, completely disable DOCTYPE declaration:
factory.setFeature("http://apache.org/xml/features/disallow// or completely disable external entities declarations:
factory.setFeature("http://xml.org/sax/features/external-gen
factory.setFeature("http://xml.org/sax/features/external-par
// or prohibit the use of all protocols by external entities
SAXParser parser = factory.newSAXParser(); // Noncompliant
parser.setProperty(XMLConstants.ACCESS_EXTERNAL_DTD, "");
parser.setProperty(XMLConstants.ACCESS_EXTERNAL_SCHEMA, "");

XMLInputFactory factory = XMLInputFactory.newInstance();
// to be compliant, completely disable DOCTYPE declaration:
factory.setProperty(XMLInputFactory.SUPPORT_DTD, false);
// or completely disable external entities declarations:
factory.setProperty(XMLInputFactory.IS_SUPPORTING_EXTERNAL_E
// or prohibit the use of all protocols by external entities
factory.setProperty(XMLConstants.ACCESS_EXTERNAL_DTD, "");
factory.setProperty(XMLConstants.ACCESS_EXTERNAL_SCHEMA, "")

TransformerFactory factory = javax.xml.transform.Transformer // to be compliant, prohibit the use of all protocols by ext factory.setAttribute(XMLConstants.ACCESS_EXTERNAL_DTD, ""); factory.setAttribute(XMLConstants.ACCESS_EXTERNAL_STYLESHEET

SchemaFactory factory = SchemaFactory.newInstance(XMLConstan // to be compliant, completely disable DOCTYPE declaration: factory.setFeature("http://apache.org/xml/features/disallow-// or prohibit the use of all protocols by external entities factory.setProperty(XMLConstants.ACCESS_EXTERNAL_DTD, ""); factory.setProperty(XMLConstants.ACCESS_EXTERNAL_SCHEMA, "")

For <u>Dom4j</u> library:

SAXReader xmlReader = new SAXReader(); xmlReader.setFeature("http://apache.org/xml/features/disallo

For Jdom2 library:

SAXBuilder builder = new SAXBuilder(); builder.setProperty(XMLConstants.ACCESS_EXTERNAL_DTD, ""); builder.setProperty(XMLConstants.ACCESS_EXTERNAL_SCHEMA, "")

See

- OWASP Top 10 2021 Category A5 Security Misconfiguration
- 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