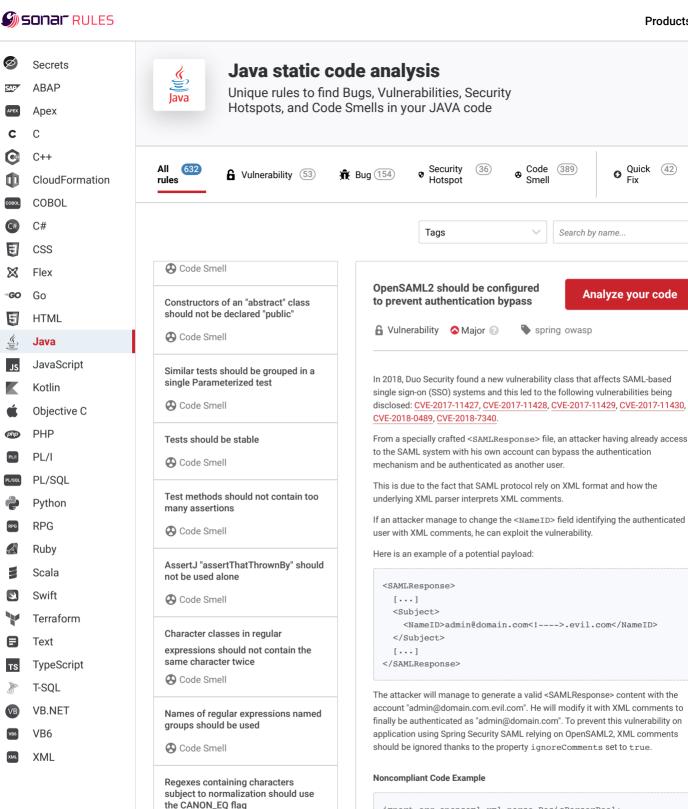


Products ✓



The attacker will manage to generate a valid <SAMLResponse> content with the account "admin@domain.com.evil.com". He will modify it with XML comments to finally be authenticated as "admin@domain.com". To prevent this vulnerability on application using Spring Security SAML relying on OpenSAML2, XML comments should be ignored thanks to the property ignoreComments set to true.

```
import org.opensaml.xml.parse.BasicParserPool;
import org.opensaml.xml.parse.ParserPool;
import org.opensaml.xml.parse.StaticBasicParserPool;
public ParserPool parserPool() {
  StaticBasicParserPool staticBasicParserPool = new StaticBa
  staticBasicParserPool.setIgnoreComments(false); // Noncomp
  return staticBasicParserPool;
public ParserPool parserPool() {
  BasicParserPool basicParserPool = new BasicParserPool();
  basicParserPool.setIgnoreComments(false); // Noncompliant
  return basicParserPool:
```

Code Smell

complicated

Code Smell

dedicated assertion

Code Smell

exceptions

Regular expressions should not be too

JUnit assertTrue/assertFalse should be simplified to the corresponding

Only one method invocation is expected when testing runtime Exception testing via JUnit
ExpectedException rule should not be
mixed with other assertions

Code Smell

"@Deprecated" code marked for
removal should never be used

Code Smell

Vararg method arguments should not
be confusing

Code Smell

Whitespace for text block indent

## **Compliant Solution**

```
public ParserPool parserPool() {
  return new StaticBasicParserPool(); // Compliant: "ignoreC
}
```

```
public ParserPool parserPool() {
  return new BasicParserPool(); // Compliant: "ignoreCommen
}
```

## See

- OWASP Top 10 2021 Category A6 Vulnerable and Outdated Components
- OWASP Top 10 2021 Category A7 Identification and Authentication Failures
- OWASP Top 10 2017 Category A2 Broken Authentication
- OWASP Top 10 2017 Category A9
   Using Components with Known Vulnerabilities
- Duo Finds SAML Vulnerabilities Affecting Multiple Implementations
- Spring Security SAML and this week's SAML Vulnerability
- Spring Security SAML: Issue #228

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