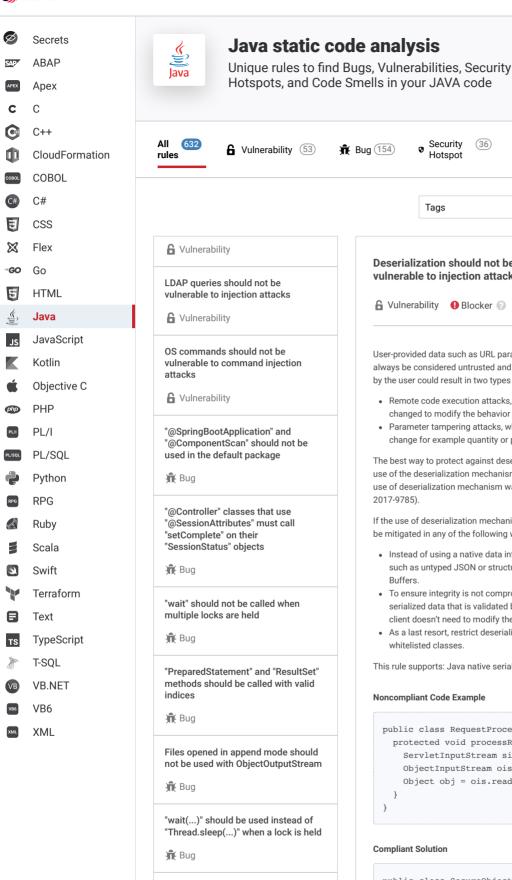
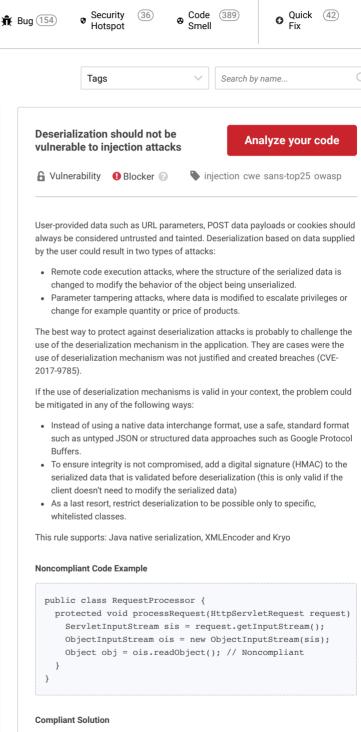


Products ✓



```
6 Vulnerability (53)
vulnerable to command injection
"@ComponentScan" should not be
"PreparedStatement" and "ResultSet"
methods should be called with valid
Files opened in append mode should
not be used with ObjectOutputStream
"wait(...)" should be used instead of
"Thread.sleep(...)" when a lock is held
Printf-style format strings should not
lead to unexpected behavior at
runtime
₩ Bug
Methods "wait(...)", "notify()" and
"notifyAll()" should not be called on
Thread instances
```



public class SecureObjectInputStream extends ObjectInputStre

protected Class<?> resolveClass(ObjectStreamClass osc) thr

if (!osc.getName().equals(AllowedClass.class.getName()))

throw new InvalidClassException("Unauthorized deserial

// Only descrialize instances of AllowedClass

return super.resolveClass(osc);

// Constructor here

@Override

- Bug

Methods should not call same-class methods with incompatible "@Transactional" values

∰ Bug

Recursion should not be infinite

👚 Bug

Loops should not be infinite

📆 Bug

Double-checked locking should not be used

📆 Bug

```
public class RequestProcessor {
  protected void processRequest(HttpServletRequest request)
    ServletInputStream sis = request.getInputStream();
    SecureObjectInputStream sois = new SecureObjectInputStre
    Object obj = sois.readObject();
  }
}
```

See

- OWASP Top 10 2021 Category A8 Software and Data Integrity Failures
- OWASP Top 10 2017 Category A8 Insecure Deserialization
- MITRE, CWE-20 Improper Input Validation
- MITRE, CWE-502 Deserialization of Untrusted Data
- SANS Top 25 Risky Resource Management

Available In:

sonarcloud 🐼 | sonarqube | Develope Edition

© 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