




 Secrets


 ABAP


 Apex


 C


 C++


 CloudFormation


 COBOL


 C#


 CSS


 Flex


 Go


 HTML


 **Java**


 JavaScript


 Kotlin


 Objective C


 PHP


 PL/I


 PL/SQL


 Python


 RPG


 Ruby


 Scala


 Swift


 Terraform


 Text


 TypeScript

 T-SQL

 VB.NET

 VB6

 XML



Java static code analysis

Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your JAVA code

All rules 632

Vulnerability 53

Bug 154


Security Hotspot 36

Code Smell 389


Quick Fix 42

Tags ▾


Search by name... 🔍

 Bug


Only one method invocation is expected when testing checked exceptions

 Bug


Assertion methods should not be used within the try block of a try-catch catching an Error

 Bug


Getters and setters should access the expected fields

 Bug


Zero should not be a possible denominator

 Bug


Locks should be released

 Bug


"runFinalizersOnExit" should not be called

 Bug


"ScheduledThreadPoolExecutor" should not have 0 core threads

 Bug


"Random" objects should be reused

 Bug


The signature of "finalize()" should match that of "Object.finalize()"

 Bug

Jump statements should not occur in "finally" blocks

 Bug

"super.finalize()" should be called at the end of "Object.finalize()" implementations

 Bug

Thread suspensions should not be vulnerable to Denial of Service attacks

Analyze your code

Vulnerability

Critical

injection cwe owasp denial-of-service

User-provided data, such as URL parameters, POST data payloads, or cookies, are tainted with user-controlled inputs. Therefore, they should always be considered untrusted.

Using user-controlled data to define the suspension time of threads execution could allow attackers to suspend thread execution for a long period of time.

Web servers generally have a limited amount of threads that can run in parallel. With a few requests, attackers can cause a Denial of Service, making the application unavailable for all users.

Recommended Secure Coding Practices

- Avoid using user-controlled data to define thread execution suspension time.
- Define a maximum suspension time.

Noncompliant Code Example

```
protected void doGet(HttpServletRequest req, HttpServletResponse res) {
    Long time = Long.parseLong(req.getParameter("time"));
    Thread.sleep(time); // Noncompliant
    // ...
}
```

Compliant Solution

```
protected void doGet(HttpServletRequest req, HttpServletResponse res) {
    Long time = Long.parseLong(req.getParameter("time"));
    Thread.sleep(Math.min(inputTime, 1000));
    // ...
}
```

See

- [OWASP Top 10 2021 Category A3](#) - Injection
- [OWASP Top 10 2017 Category A1](#) - Injection
- [MITRE, CWE-400](#) - Uncontrolled Resource Consumption

Available In:

sonarcloud





sonarqube

Developer Edition

https://rules.sonarsource.com/java/RSPEC-6390

© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD are trademarks of

1/2

<div>Using slow regular expressions is security-sensitive</div> <div> Security Hotspot</div>
<div>Using publicly writable directories is security-sensitive</div> <div> Security Hotspot</div>
<div>Using clear-text protocols is security-sensitive</div> <div> Security Hotspot</div>
<div>Accessing Android external storage is security-sensitive</div> <div> Security Hotspot</div>