




 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... 🔍

Parentheses should be removed from a single lambda input parameter when its type is inferred

Code Smell

Abstract classes without fields should be converted to interfaces

Code Smell

Lambdas containing only one statement should not nest this statement in a block

Code Smell

"Collections.EMPTY\_LIST", "EMPTY\_MAP", and "EMPTY\_SET" should not be used

Code Smell

Local variables should not be declared and then immediately returned or thrown

Code Smell

Unused local variables should be removed

Code Smell

Private fields only used as local variables in methods should become local variables

Code Smell

"public static" fields should be constant

Code Smell

Loops should not contain more than a single "break" or "continue" statement

Code Smell

Declarations should use Java collection interfaces such as "List" rather than specific implementation classes such as "LinkedList"

Code Smell

### Allowing deserialization of LDAP objects is security-sensitive

Analyze your code

Security Hotspot Major cwe owasp

JNDI supports the deserialization of objects from LDAP directories, which can lead to remote code execution.

This rule raises an issue when an LDAP search query is executed with SearchControls configured to allow deserialization.

#### Ask Yourself Whether

- The application connects to an untrusted LDAP directory.
- User-controlled objects can be stored in the LDAP directory.

There is a risk if you answered yes to any of those questions.

#### Recommended Secure Coding Practices

It is recommended to disable deserialization of LDAP objects.

#### Sensitive Code Example

```
DirContext ctx = new InitialDirContext();
// ...
ctx.search(query, filter,
    new SearchControls(scope, countLimit, timeLimit, att
        true, // Noncompliant; allows deserialization
        deref));
```

#### Compliant Solution

```
DirContext ctx = new InitialDirContext();
// ...
ctx.search(query, filter,
    new SearchControls(scope, countLimit, timeLimit, att
        false, // Compliant
        deref));
```

#### See




- [OWASP Top 10 2021 Category A8](#) - Software and Data Integrity Failures
- [MITRE, CWE-502](#) - Deserialization of Untrusted Data
- [OWASP Top 10 2017 Category A8](#) - Insecure Deserialization
- [BlackHat presentation](#)
- Derived from FindSecBugs rule [LDAP\\_ENTRY\\_POISONING](#)

Available In:

sonarcloud | sonarqube

https://rules.sonarsource.com/java/RSPEC-4434

1/2


<b>"switch" statements should have at least 3 "case" clauses</b>
 Code Smell
<b>A "while" loop should be used instead of a "for" loop</b>
 Code Smell
<b>The default unnamed package should not be used</b>
 Code Smell
<b>"equals(Object obj)" should be overridden along with the "compareTo(T obj)" method</b>

© 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](#)