sonar

RULES

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

# Java static code analysis

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

All rules632

Vulnerability53

Bug154

Security Hotspot36

Code Smell389

Quick Fix42

Tags

Search by name...

security-sensitive

Security Hotspot

Using unsafe Jackson deserialization configuration is security-sensitive

Security Hotspot

Setting JavaBean properties is security-sensitive

Security Hotspot

Disabling CSRF protections is security-sensitive

Security Hotspot

Using non-standard cryptographic algorithms is security-sensitive

Security Hotspot

Using pseudorandom number generators (PRNGs) is security-sensitive

Security Hotspot

Mocking all non-private methods of a class should be avoided

Code Smell

Empty lines should not be tested with regex MULTILINE flag

Code Smell

Methods setUp() and tearDown() should be correctly annotated starting with JUnit4

Code Smell

Class members annotated with "@VisibleForTesting" should not be accessed from production code

Code Smell

"String#replace" should be preferred to "String#replaceAll"

Code Smell

Derived exceptions should not hide

LDAP connections should be authenticated

Analyze your code

Vulnerability

Critical

cwe owasp

An LDAP client authenticates to an LDAP server with a "bind request" which provides, among other, a [simple authentication method](#).

Simple authentication in LDAP can be used with three different mechanisms:

- Anonymous Authentication Mechanism by performing a bind request with a username and password value of zero length.
- Unauthenticated Authentication Mechanism by performing a bind request with a password value of zero length.
- Name/Password Authentication Mechanism by performing a bind request with a password value of non-zero length.

Anonymous binds and unauthenticated binds allow access to information in the LDAP directory without providing a password, their use is therefore strongly discouraged.

### Noncompliant Code Example

This rule raises an issue when an LDAP connection is created with Context.SECURITY\_AUTHENTICATION set to "none".

```
// Set up the environment for creating the initial context
Hashtable<String, Object> env = new Hashtable<String, Object>
env.put(Context.INITIAL_CONTEXT_FACTORY, "com.sun.jndi.ldap.
env.put(Context.PROVIDER_URL, "ldap://localhost:389/o=JNDITu

// Use anonymous authentication
env.put(Context.SECURITY_AUTHENTICATION, "none"); // Noncomp

// Create the initial context
DirContext ctx = new InitialDirContext(env);
```

### Compliant Solution

```
// Set up the environment for creating the initial context
Hashtable<String, Object> env = new Hashtable<String, Object>
env.put(Context.INITIAL_CONTEXT_FACTORY, "com.sun.jndi.ldap.
env.put(Context.PROVIDER_URL, "ldap://localhost:389/o=JNDITu

// Use simple authentication
env.put(Context.SECURITY_AUTHENTICATION, "simple");
env.put(Context.SECURITY_PRINCIPAL, "cn=S. User, ou=NewHires
env.put(Context.SECURITY_CREDENTIALS, getLDAPPassword());








// Create the initial context
DirContext ctx = new InitialDirContext(env);
```

See

- OWASP Top 10 2021 Category A7 - Identification and Authentication Failures

https://rules.sonarsource.com/java/RSPEC-4433

1/2

<div>their parents' catch blocks</div> <div> Code Smell</div>	<div><ul style="list-style-type: none"><li>OWASP Top 10 2017 Category A2 - Broken Authentication</li><li>MITRE, CWE-521 - Weak Password Requirements</li><li>Idapwiki.com- Simple Authentication</li></ul></div> <div>Available In:</div> <div>      </div>
<div>String offset-based methods should be preferred for finding substrings from offsets</div> <div> Code Smell</div>	
<div>"default" clauses should be last</div> <div> Code Smell</div>	
<div>"equals" method parameters should not be marked "@Nonnull"</div> <div> Code Smell</div>	
<div>A conditionally executed single line</div>	

© 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](#)