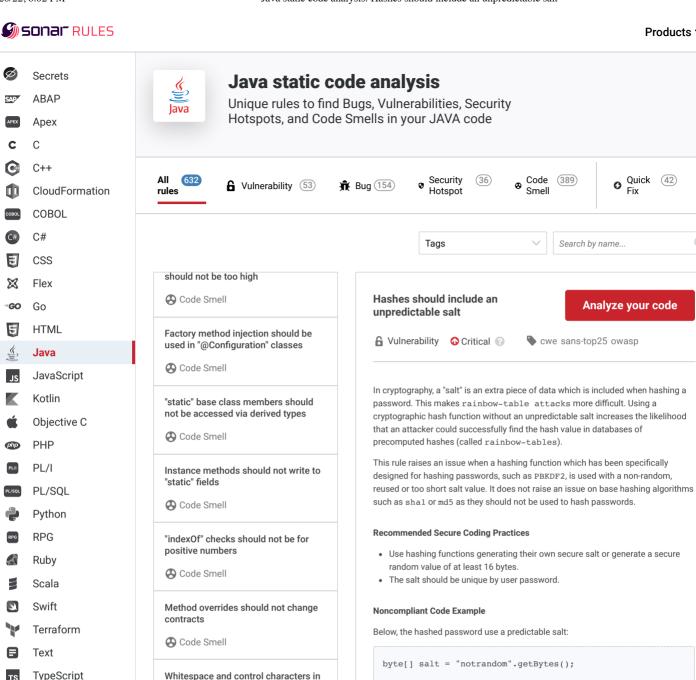


Products ✓

O Quick 42 Fix



literals should be explicit

Null should not be returned from a

Classes should not access their own

"Condition.await(...)" should be called

 $Illegal Monitor State Exception\ should$

JUnit assertions should not be used in

subclasses during initialization

Code Smell

"Roolean" method

Code Smell

Code Smell

"Object.wait(...)" and

inside a "while" loop

Code Smell

not be caught

Code Smell

```
PBEParameterSpec cipherSpec = new PBEParameterSpec(salt, 100
PBEKeySpec spec = new PBEKeySpec(chars, salt, 10000, 256); /
```

Compliant Solution

Use java.security.SecureRandom to generate an unpredictable salt:

```
SecureRandom random = new SecureRandom();
byte[] salt = new byte[16];
random.nextBytes(salt);
PBEParameterSpec cipherSpec = new PBEParameterSpec(salt, 100
PBEKeySpec spec = new PBEKeySpec(chars, salt, 10000, 256); /
```

See

- OWASP Top 10 2021 Category A2 Cryptographic Failures
- OWASP Top 10 2017 Category A3 Sensitive Data Exposure
- MITRE, CWE-759 Use of a One-Way Hash without a Salt
- MITRE, CWE-760 Use of a One-Way Hash with a Predictable Salt
- SANS Top 25 Porous Defenses

Available In:

sonarlint ⊕ | sonarcloud ↔ | sonarqube

T-SQL

VB.NET

VB₆

XML

Class names should not shadow interfaces or superclasses
Code Smell

"Cloneables" should implement "clone"
Code Smell

Try-with-resources should be used
Code Smell

"readResolve" methods should be inheritable
Code Smell

© 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