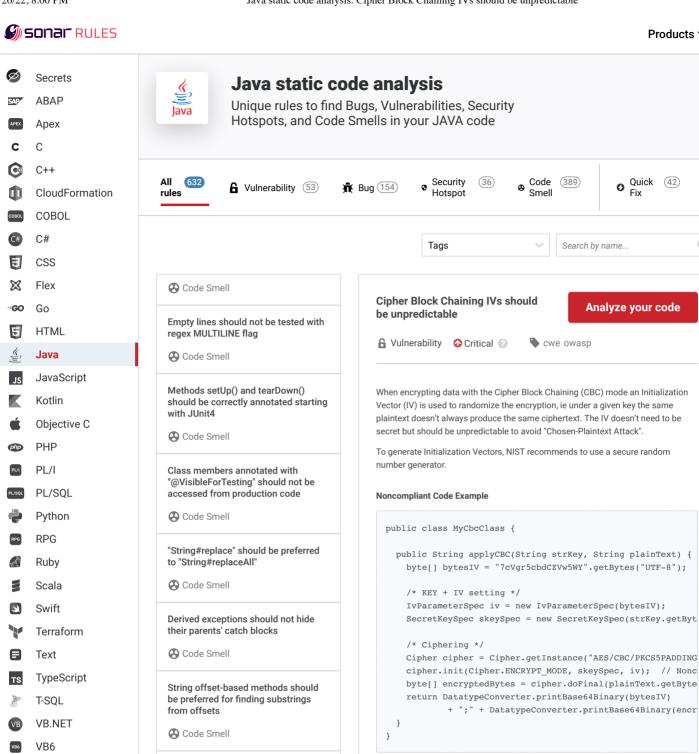
Products ✓

O Quick 42 Fix



"default" clauses should be last

"equals" method parameters should

A conditionally executed single line should be denoted by indentation

Conditionals should start on new lines

Cognitive Complexity of methods

not be marked "@Nonnull'

A Code Smell

Code Smell

Code Smell

Code Smell

Code Smell

should not be too high

Compliant Solution

```
public class MvCbcClass {
 SecureRandom random = new SecureRandom():
 public String applyCBC(String strKey, String plainText) {
   byte[] bytesIV = new byte[16];
   random.nextBytes(bytesIV);
    /* KEY + IV setting */
   IvParameterSpec iv = new IvParameterSpec(bytesIV);
   SecretKeySpec skeySpec = new SecretKeySpec(strKey.getByt
    /* Ciphering */
   Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5PADDING
   cipher.init(Cipher.ENCRYPT_MODE, skeySpec, iv); // Compl
   byte[] encryptedBytes = cipher.doFinal(plainText.getByte
    return DatatypeConverter.printBase64Binary(bytesIV)
            + ";" + DatatypeConverter.printBase64Binary(encr
```

XML

Available In:

Factory method injection should be used in "@Configuration" classes

Code Smell

"static" base class members should not be accessed via derived types

Code Smell

Instance methods should not write to "static" fields

Code Smell

"indexOf" checks should not be for positive numbers

A Code Smell

See

OWASP Top 10 2021 Category A2 - Cryptographic Failures
OWASP Top 10 2017 Category A6 - Security Misconfiguration
MITRE, CWE-329 - CWE-329: Not Using an Unpredictable IV with CBC Mode
MITRE, CWE-330 - Use of Insufficiently Random Values
NIST, SP-800-38A - Recommendation for Block Cipher Modes of Operation
Derived from FindSecBugs rule STATIC_IV

© 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

sonarlint - sonarcloud - sonarqube