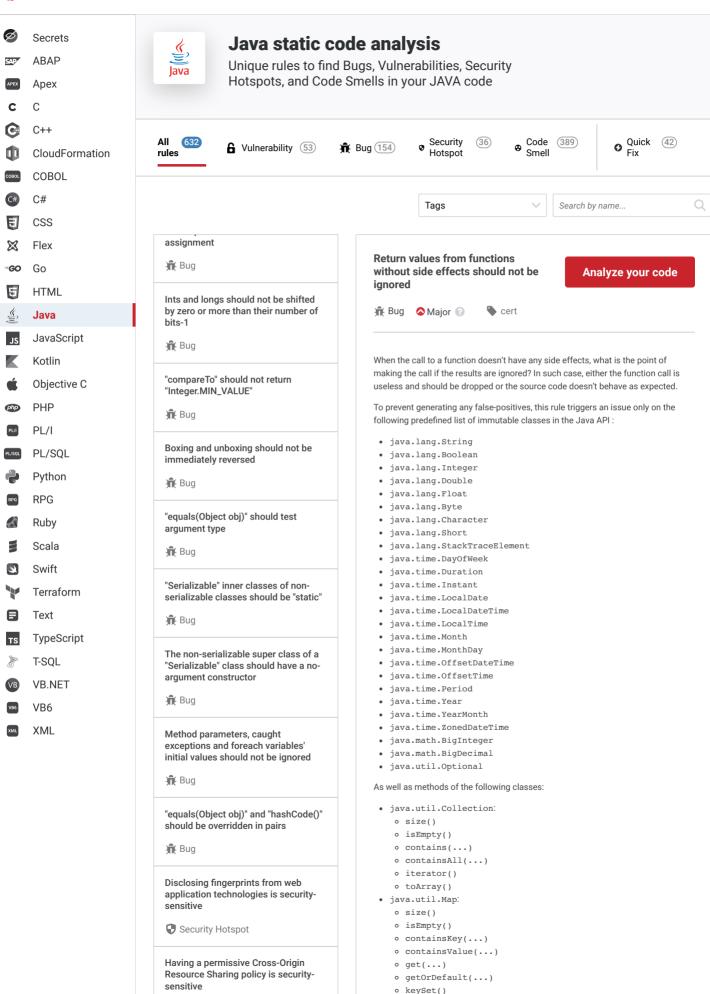


Products ∨



o entrySet()

Security Hotspot

Delivering code in production with debug features activated is securitysensitive

Security Hotspot

Searching OS commands in PATH is security-sensitive

Security Hotspot

Allowing both safe and unsafe HTTP methods is security-sensitive

Security Hotspot

Creating cookies without the "HttpOnly" flag is security-sensitive

- o values()
- java.util.stream.Stream
  - o toArray
  - o reduce
  - o collect
  - o min
  - o max
  - o count
  - o anyMatch
  - o allMatch
  - o noneMatch
  - o findFirst o findAnv
  - o toList

## Noncompliant Code Example

```
public void handle(String command){
 command.toLowerCase(); // Noncompliant; result of method t
```

## **Compliant Solution**

```
public void handle(String command){
 String formattedCommand = command.toLowerCase();
}
```

## Exceptions

This rule will not raise an issue when both these conditions are met:

- The method call is in a try block with an associated catch clause.
- The method name starts with "parse", "format", "decode" or "valueOf" or the  $method \ is \ String.get Bytes (Charset).$

```
private boolean textIsInteger(String textToCheck) {
    try {
        Integer.parseInt(textToCheck, 10); // OK
        return true;
    } catch (NumberFormatException ignored) {
        return false;
}
```

• CERT, EXP00-J. - Do not ignore values returned by methods

Available In:

sonarlint ⊕ | sonarcloud 👌 | sonarqube

© 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