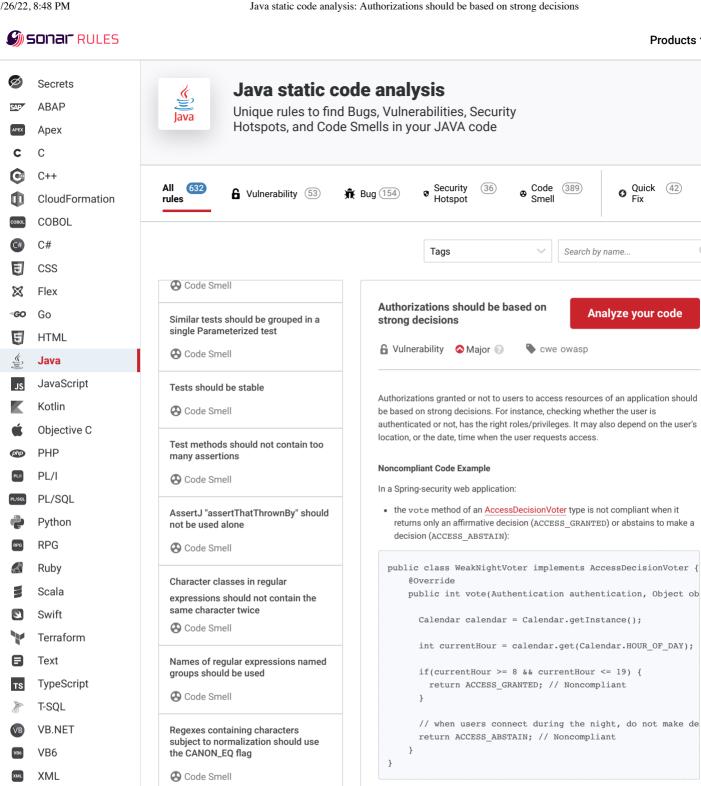
Products ✓

O Quick 42 Fix



Regular expressions should not be too

JUnit assertTrue/assertFalse should

be simplified to the corresponding

Only one method invocation is

expected when testing runtime

**Exception testing via JUnit** ExpectedException rule should not be

complicated

Code Smell

dedicated assertion

Code Smell

exceptions Code Smell - the hasPermission method of a  $\underline{\text{PermissionEvaluator}}$  type is not compliant when it doesn't return false:

```
public class MyPermissionEvaluator implements PermissionEval
   @Override
   public boolean hasPermission(Authentication authenticati
       //Getting subject
       Object user = authentication.getPrincipal();
       if(user.getRole().equals(permission)) {
              return true; // Noncompliant
       return true; // Noncompliant
```

## Compliant Solution

In a Spring-security web application:

A Code Smell

"@Deprecated" code marked for removal should never be used

Code Smell

Vararg method arguments should not be confusing

Code Smell

Whitespace for text block indent should be consistent

Code Smell

'List.remove()' should not be used in

• the vote method of an AccessDecisionVoter type should return a negative decision (ACCESS DENIED):

```
public class StrongNightVoter implements AccessDecisionVoter
   @Override
   public int vote(Authentication authentication, Object ob
     Calendar calendar = Calendar.getInstance();
     int currentHour = calendar.get(Calendar.HOUR OF DAY);
     if(currentHour >= 8 && currentHour <= 19) {</pre>
        return ACCESS_GRANTED;
      // users are not allowed to connect during the night
      return ACCESS_DENIED; // Compliant
```

• the hasPermission method of a PermissionEvaluator type should return

```
public class MyPermissionEvaluator implements PermissionEval
    @Override
    public boolean hasPermission(Authentication authenticati
        //Getting subject
        Object user = authentication.getPrincipal();
        if(user.getRole().equals(permission)) {
             return true:
        return false; // Compliant
   }
}
```

## Exceptions

No issue is reported when the method throws an exception as it might be used to indicate a strong decision.

- OWASP Top 10 2021 Category A1 Broken Access Control
- OWASP Top 10 2017 Category A5 Broken Access Control
- MITRE, CWE-285 Improper Authorization

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