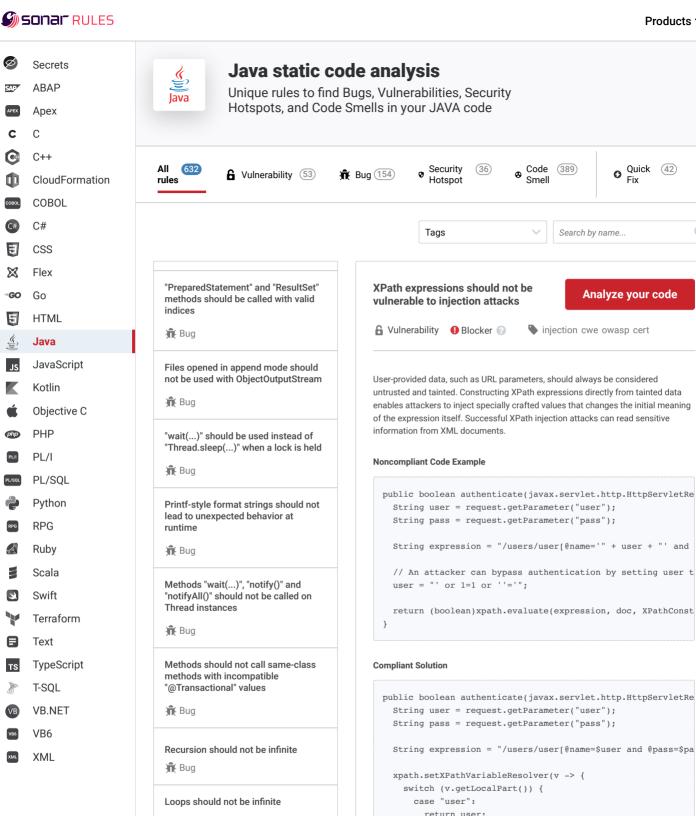


Products ✓



```
public boolean authenticate(javax.servlet.http.HttpServletRe
  String user = request.getParameter("user");
  String pass = request.getParameter("pass");
  String expression = "/users/user[@name=$user and @pass=$pa
       return user;
      case "pass":
       return pass;
      default:
        throw new IllegalArgumentException();
  });
  return (boolean)xpath.evaluate(expression, doc, XPathConst
```

See

- OWASP Top 10 2021 Category A3 Injection
- OWASP Top 10 2017 Category A1 Injection
- MITRE, CWE-643 Improper Neutralization of Data within XPath Expressions
- CERT, IDS53-J. Prevent XPath Injection

₩ Bug

₩ Bug

R Bug

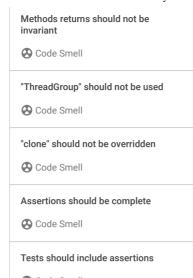
sensitive

Security Hotspot

Double-checked locking should not be

Resources should be closed

Hard-coded credentials are security-





© 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