Security

Hotspot

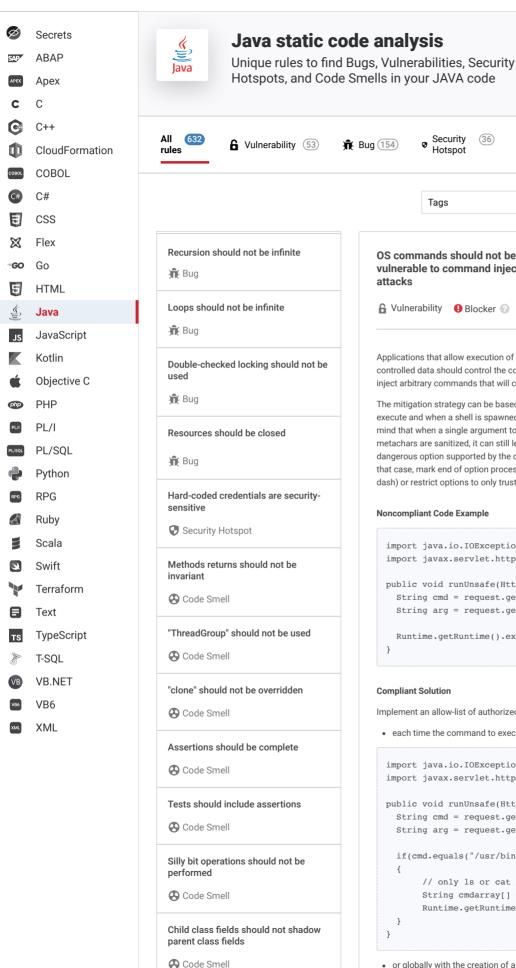
(36)

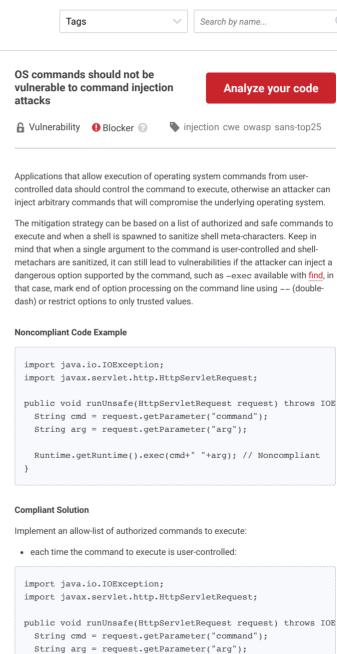


Products >

(42)

O Quick Fix





if(cmd.equals("/usr/bin/ls") || cmd.equals("/usr/bin/cat")

String cmdarray[] = new String[] { cmd, arg }; Runtime.getRuntime().exec(cmdarray); // Compliant

// only ls or cat command are authorized

• or globally with the creation of a SecurityManager overriding checkExec()

method

⊗ Code

Smell

(389)

JUnit test cases should call super

methods

Code Smell TestCases should contain tests A Code Smell Short-circuit logic should be used in boolean contexts Code Smell Methods and field names should not be the same or differ only by

capitalization

Code Smell

Switch cases should end with an unconditional "break" statement

```
class MySecurityManager extends SecurityManager {
 MySecurityManager() {
    super();
  public void checkExec(String cmd) {
    if(!(cmd.equals("/usr/bin/ls") || cmd.equals("/usr/bin/c
      throw new SecurityException("Unauthorized command: "+c
}
```

```
MySecurityManager sm = new MySecurityManager();
System.setSecurityManager(sm);
```

## See

- OWASP Top 10 2021 Category A3 Injection
- OWASP OS Command Injection Defense Cheat Sheet
- OWASP Top 10 2017 Category A1 Injection
- MITRE, CWE-20 Improper Input Validation
- MITRE, CWE-78 Improper Neutralization of Special Elements used in an OS
- SANS Top 25 Insecure Interaction Between Components

Available In:

sonarcloud color sonarqube Edition

© 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