Security

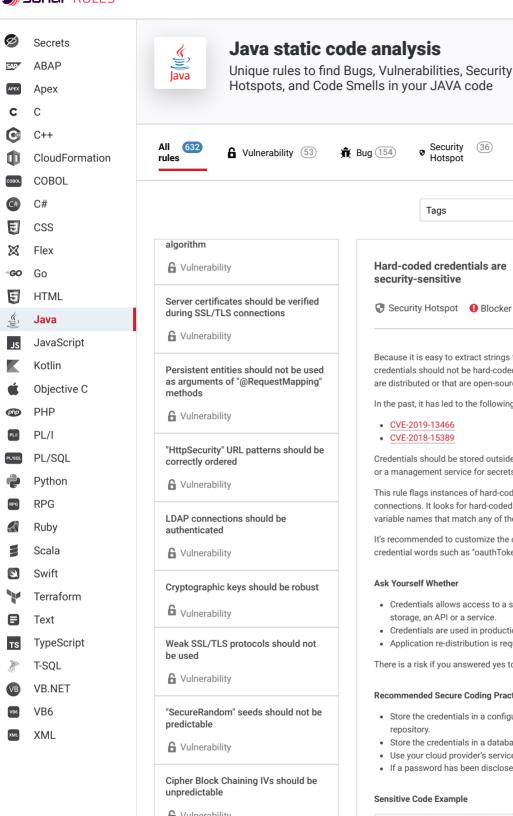
Hotspot

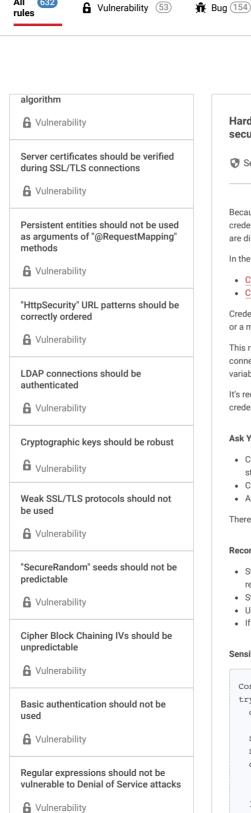
(36)



Products ✓

O Quick 42

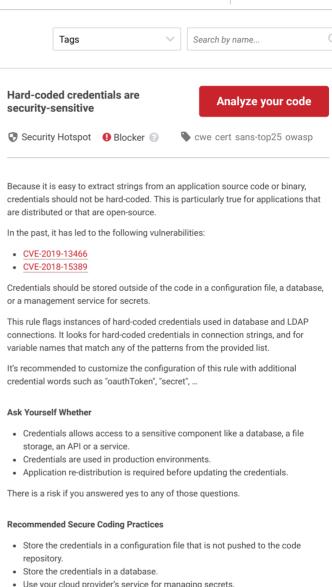




"HttpServletRequest.getRequestedSession

should not be used 6 Vulnerability





• If a password has been disclosed through the source code: change it.

conn = DriverManager.getConnection("jdbc:mysql://localhost

conn = DriverManager.getConnection("jdbc:mysql://localhost

java.net.PasswordAuthentication pa = new java.net.Password

"user=" + uname + "&password=" + password); // Sensi

"user=steve&password=blue"); // Sensitive

⊗ Code

Smell

(389)

Compliant Solution

Sensitive Code Example

try {

Connection conn = null:

String uname = "steve";

String password = "blue";

Hashes should include an unpredictable salt

6 Vulnerability

Calls to methods should not trigger an IllegalArgumentException



Unsupported methods should not be called on some collection implementations



Cast operations should not trigger a ClassCastException



See

- OWASP Top 10 2021 Category A7 Identification and Authentication Failures
- OWASP Top 10 2017 Category A2 Broken Authentication
- MITRE, CWE-798 Use of Hard-coded Credentials
- MITRE, CWE-259 Use of Hard-coded Password
- CERT, MSC03-J. Never hard code sensitive information
- SANS Top 25 Porous Defenses
- Derived from FindSecBugs rule Hard Coded Password

Available In:

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