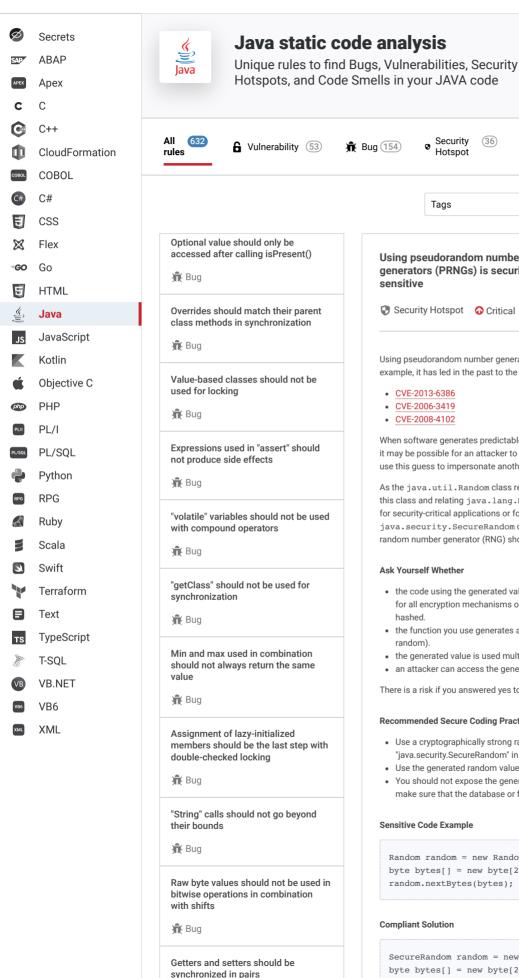
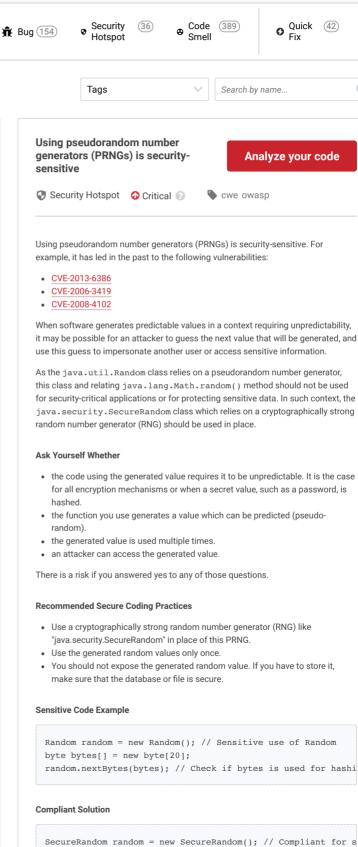


Products >

(42)





byte bytes[] = new byte[20];

random.nextBytes(bytes);

₩ Bug

Java static code analysis: Usin

Non-thread-safe fields should not be static

Bug

"null" should not be used with
"Optional"

Bug

Unary prefix operators should not be repeated

Bug

"=+" should not be used instead of "+="

Rug Bug

Se

- OWASP Top 10 2021 Category A2 Cryptographic Failures
- OWASP Top 10 2017 Category A3 Sensitive Data Exposure
- Mobile AppSec Verification Standard Cryptography Requirements
- OWASP Mobile Top 10 2016 Category M5 Insufficient Cryptography
- MITRE, CWE-338 Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
- MITRE, CWE-330 Use of Insufficiently Random Values
- MITRE, CWE-326 Inadequate Encryption Strength
- MITRE, CWE-1241 Use of Predictable Algorithm in Random Number Generator
- CERT, MSC02-J. Generate strong random numbers
- CERT, MSC30-C. Do not use the rand() function for generating pseudorandom numbers
- <u>CERT, MSC50-CPP.</u> Do not use std::rand() for generating pseudorandom numbers
- Derived from FindSecBugs rule Predictable Pseudo Random Number Generator

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