Code Smell (56)





All rules 98

Kotlin static code analysis

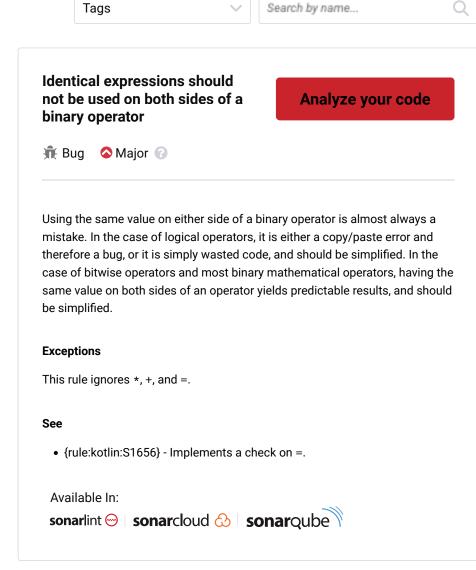
6 Vulnerability (10)

Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your KOTLIN code

R Bug (17)

	ard-coded credentials are security-
	ensitive
•	Security Hotspot
Ci	pher algorithms should be robust
6	Vulnerability
wi	ncryption algorithms should be used th secure mode and padding theme
6	Vulnerability
	erver hostnames should be verified uring SSL/TLS connections
6	Vulnerability
	erver certificates should be verified iring SSL/TLS connections
	Vulnerability
Cr	yptographic keys should be robust
6	Vulnerability
	eak SSL/TLS protocols should not
6	Vulnerability
	ecureRandom" seeds should not be edictable
6	Vulnerability
	pher Block Chaining IVs should be predictable
6	Vulnerability
	ashes should include an apredictable salt
6	Vulnerability
	egular expressions should be entactically valid
ìĵî	E Bug

📆 Bug



Security Hotspot (15)

© 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

"ScheduledThreadPoolExecutor" should not have 0 core threads
Jump statements should not occur in "finally" blocks
Using clear-text protocols is security-sensitive Security Hotspot
Accessing Android external storage is security-sensitive Security Hotspot
Receiving intents is security-sensitive Security Hotspot
Broadcasting intents is security- sensitive Security Hotspot
Using weak hashing algorithms is security-sensitive Security Hotspot
Using pseudorandom number generators (PRNGs) is security-sensitive Security Hotspot
Empty lines should not be tested with regex MULTILINE flag Code Smell
Cognitive Complexity of functions should not be too high Code Smell