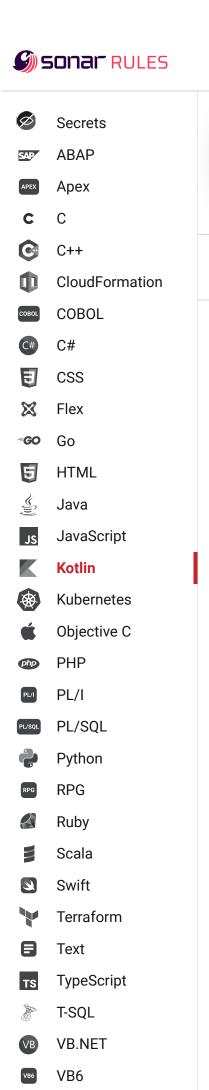
Code Smell (56)



XML



All rules 98

Kotlin static code analysis

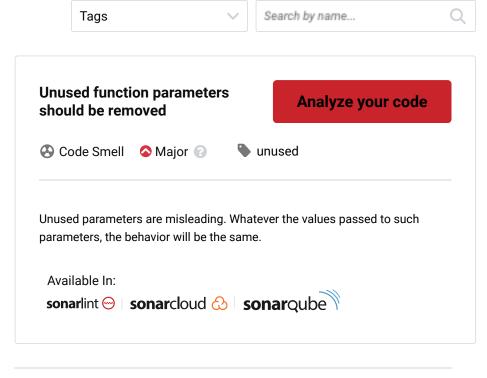
6 Vulnerability (10)

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

R Bug 17

Hard-coded	credentials are security-
sensitive	referencials are security
Security	Hotspot
Cipher algo	rithms should be robust
6 Vulnerab	pility
	algorithms should be used mode and padding
	oility
	names should be verified TLS connections
6 Vulnerab	pility
	ficates should be verified TLS connections
6 Vulnerab	pility
Cryptograph	nic keys should be robust
6 Vulnerab	oility
Weak SSL/T be used	FLS protocols should not
6 Vulnerab	oility
"SecureRand predictable	dom" seeds should not be
읍 Vulnerab	pility
Cipher Block unpredictab	k Chaining IVs should be lle
읍 Vulnerab	pility
Hashes sho unpredictab	ould include an ole salt
6 Vulnerab	pility
Regular exp syntactically	ressions should be y valid
Rug	
	rsOnExit" should not be

Rug 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