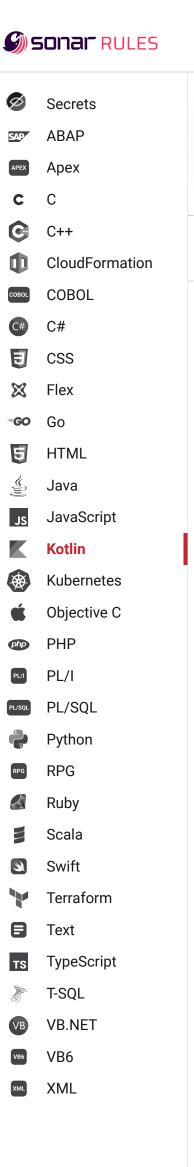
Q





Kotlin static code analysis

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

	Tags Search by name
Hard-coded credentials are security- sensitive	Control flow statements "if", "for", "while", "when" and "try"
Security Hotspot	should not be nested too deeply Analyze your of
Cipher algorithms should be robust	Code Smell
■ Vulnerability	
Encryption algorithms should be used with secure mode and padding scheme	Nested if, for, while, when, and try statements are key ingredier making what's known as "Spaghetti code". Such code is hard to read, refactor and therefore maintain.
☆ Vulnerability	Available In:
Server hostnames should be verified during SSL/TLS connections	sonarlint ⊕ sonarcloud む sonarqube
읍 Vulnerability	
Server certificates should be verified during SSL/TLS connections	© 2008-2022 SonarSource S.A., Switzerland. All content is copyright prote SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD trademarks of SonarSource S.A. All other trademarks and copyrights are
읍 Vulnerability	property of their respective owners. All rights are expressly reserved <u>Privacy Policy</u>
Cryptographic keys should be robust	
备 Vulnerability	
Weak SSL/TLS protocols should not be used	
备 Vulnerability	
"SecureRandom" seeds should not be predictable	
备 Vulnerability	
Cipher Block Chaining IVs should be unpredictable	
备 Vulnerability	
Hashes should include an unpredictable salt	
읍 Vulnerability	
Regular expressions should be syntactically valid	
∰ Bug	

"runFinalizersOnExit" should not be

called

📆 Bug

"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	