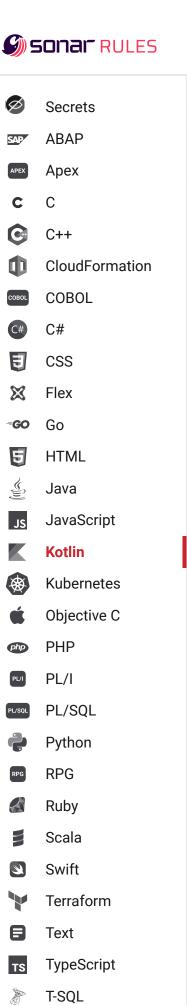
Code Smell (56)





**VB.NET** 

VB6

XML



## **Kotlin static code analysis**

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

**♣** Bug 17

All rules 98
Hard-coded credentials are security-
sensitive
Security Hotspot
Cipher algorithms should be robust
Encryption algorithms should be used with secure mode and padding scheme
❸ Vulnerability
Server hostnames should be verified during SSL/TLS connections
<b>☆</b> Vulnerability
Server certificates should be verified during SSL/TLS connections
❸ Vulnerability
Cryptographic keys should be robust
❸ Vulnerability
Weak SSL/TLS protocols should not be used
❸ Vulnerability
"SecureRandom" seeds should not be predictable
❸ Vulnerability
Cipher Block Chaining IVs should be unpredictable
❸ Vulnerability
Hashes should include an unpredictable salt
❸ Vulnerability
Regular expressions should be syntactically valid
🖟 Bug
"runFinalizersOnExit" should not be called

📆 Bug

	Tags			Search	by name	
	ements sl arate lines	hould be on			Analyze y	our code
<b>3</b> C	ode Smell	<b>△</b> Major ②	•	convent	ion	
For b	etter readab	ility, do not put r	nore th	an one st	atement on	a single line.
Nonc	ompliant Co	de Example				
	ompliant Co					
fo		);				
fo Comp	o(); bar(	);				
for for ba	o(); bar(  oliant Solution	);				

Security Hotspot 15

@ 2008-2022 Sonar Source 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