Secrets
ABAP
Apex
C
C++
CloudFormation
COBOL
C#
CSS
Flex
Go
HTML
Java
JavaScript
Kotlin
Kubernetes
Objective C
PHP
PL/I
PL/SQL
Python
RPG
Ruby
Scala
Swift
Terraform
Text
TypeScript
T-SQL
VB.NET
VB6
XML

Kotlin static code analysis

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

| All rules 98 | 🔓 Vulnerability 10 | 🐛 Bug 17 | 🛡 Security Hotspot 15 | ☢ Code Smell 56 |

Tags ⌄   Search by name... 🔍

Hard-coded credentials are security-sensitive

🛡 Security Hotspot

Cipher algorithms should be robust

🔓 Vulnerability

Encryption algorithms should be used with secure mode and padding scheme

🔓 Vulnerability

Server hostnames should be verified during SSL/TLS connections

🔓 Vulnerability

Server certificates should be verified during SSL/TLS connections

🔓 Vulnerability

Cryptographic keys should be robust

🔓 Vulnerability

Weak SSL/TLS protocols should not be used

🔓 Vulnerability

"SecureRandom" seeds should not be predictable

🔓 Vulnerability

Cipher Block Chaining IVs should be unpredictable

🔓 Vulnerability

Hashes should include an unpredictable salt

🔓 Vulnerability

Regular expressions should be syntactically valid

🐛 Bug

"runFinalizersOnExit" should not be called

🐛 Bug

Functions should not have too many lines of code

Analyze your code

☢ Code Smell   ⊗ Major ?   🏷 brain-overload

A function that grows too large tends to aggregate too many responsibilities.

Such functions inevitably become harder to understand and therefore harder to maintain.

Above a specific threshold, it is strongly advised to refactor into smaller functions which focus on well-defined tasks.

Those smaller functions will not only be easier to understand, but also probably easier to test.

Available In:

sonarlint ⊙⊙ | **sonar**cloud ☁ | **sonar**qube 〃

"ScheduledThreadPoolExecutor" should not have 0 core threads

🐞 Bug

Jump statements should not occur in "finally" blocks

🐞 Bug

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