

-  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 ▾  

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

### Track uses of "TODO" tags

Analyze your code

 Code Smell    Info       cwe

TODO tags are commonly used to mark places where some more code is required, but which the developer wants to implement later.

Sometimes the developer will not have the time or will simply forget to get back to that tag.

This rule is meant to track those tags and to ensure that they do not go unnoticed.

#### Noncompliant Code Example

```
fun doSomething() {  
    // TODO  
}
```

#### See

- MITRE, CWE-546 - Suspicious Comment

Available In:

sonarlint  | sonarcloud  | sonarqube 

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