

-  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

## Regular expressions should be syntactically valid

Analyze your code

-  Bug
-  Critical
- 
-  regex

Regular expressions have their own syntax that is understood by regular expression engines. Those engines will throw an exception at runtime if they are given a regular expression that does not conform to that syntax.

To avoid syntax errors, special characters should be escaped with backslashes when they are intended to be matched literally and references to capturing groups should use the correctly spelled name or number of the group.

To match a literal string instead of a regular expression, either all special characters should be escaped, the `RegexOption.LITERAL` flag or functions that don't use regular expressions should be used.

### Noncompliant Code Example

```
Regex(" ( [ ")
"( [ ".toRegex()
```

### Compliant Solution

```
Regex("\\(\\[ ")
Regex("\"\"\\(\\[ \"\"")
"\\(\\[ ".toRegex()
"\"\"\\(\\[ \"\"".toRegex()

Regex("( [ ", RegexOptions.LITERAL)
"( [ ".toRegex(RegexOptions.LITERAL)
```

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>