



Flex

Go =GO

HTML 5

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** 



## **Objective C static code analysis**

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

}

**Compliant Solution** 

return num;

Available In:

int pow(int num, int exponent) {

sonarcloud **⊘** | sonarqube )

num = num \* pow(num, exponent-1);

All 315 6 Vulnerability 10 rules

**R** Bug (75)

• Security Hotspot ⊗ Code (212)

O Quick 13 Fix

Tags

Search by name...

"memset" should not be used to delete sensitive data

Vulnerability

POSIX functions should not be called with arguments that trigger buffer overflows

■ Vulnerability

Function-like macros should not be invoked without all of their arguments

📆 Bug

The address of an automatic object should not be assigned to another object that may persist after the first object has ceased to exist

📆 Bug

"pthread\_mutex\_t" should be unlocked in the reverse order they were locked

🖷 Bug

"pthread\_mutex\_t" should be properly initialized and destroyed

📆 Bug

"pthread\_mutex\_t" should not be consecutively locked or unlocked twice

📆 Bug

Functions with "noreturn" attribute should not return

📆 Bug

"memcmp" should only be called with pointers to trivially copyable types with no padding

🖷 Bug

Stack allocated memory and nonowned memory should not be freed

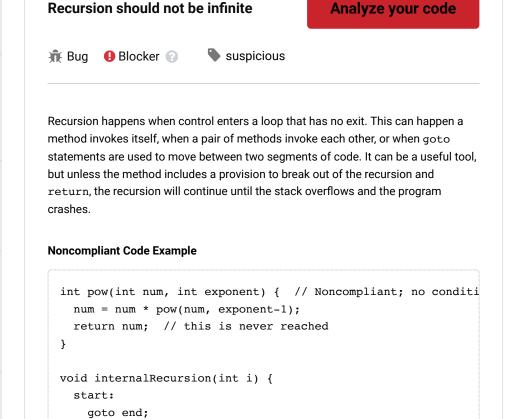
📆 Bug

Closed resources should not be accessed

📆 Bug

Dynamically allocated memory should be released

📆 Bug



goto start; // Noncompliant; there's no way to break out

if (exponent > 1) { // recursion now conditional and stop-

© 2008-2022 SonarSource 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

Freed memory should not be used
Rug
Memory locations should not be released more than once
Rug
Memory access should be explicitly bounded to prevent buffer overflows
<b>∰</b> Bug
Printf-style format strings should not lead to unexpected behavior at runtime
Rug
Recursion should not be infinite
Rug
Resources should be closed
Rug
Hard-coded credentials are security- sensitive
Security Hotspot
"goto" should jump to labels declared later in the same function
☼ Code Smell
Only standard forms of the "defined" directive should be used
Code Smell
Switch labels should not be nested inside non-switch blocks