





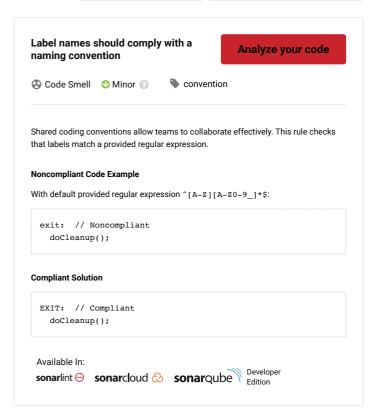
C static code analysis

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

All 311 rules	6 Vulnerability 13	∰ Bug 74	Security Hotspot	T8 Code (206) Smell	Quick 14 Fix
---------------	---------------------------	------------------------	------------------	---------------------	--------------

Tags

"memset" should not be used to del sensitive data	lete
■ Vulnerability	
POSIX functions should not be calle with arguments that trigger buffer overflows	ed
XML parsers should not be vulneral to XXE attacks	ble
Function-like macros should not be invoked without all of their argumen	
∰ 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 unlock in the reverse order they were locke	
∄ Bug	
"pthread_mutex_t" should be proper initialized and destroyed	rly
∰ 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 wi	ith
pointers to trivially copyable types with no padding	



Search by name.

© 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

Stack allocated memory and nonowned memory should not be freed

R
Bug

Closed resources should not be
accessed
Bug

Dynamically allocated memory should
be released
Bug

Freed memory should not be used