





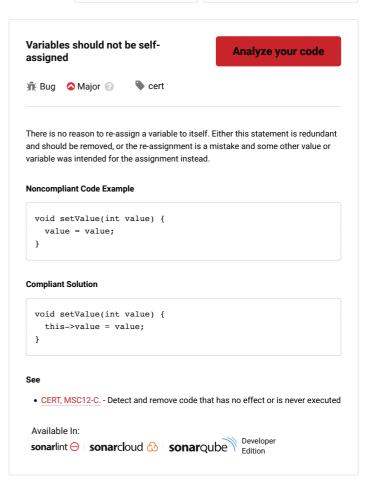
C static code analysis

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

All 311 rules	6 Vulnerability 13	∰ Bug 74	Security 18 Hotspot	Code 206 Smell	Quick 14 Fix
---------------	---------------------------	------------------------	---------------------	----------------	-----------------

Tags

	memset" should not be used to delete ensitive data
ĺ	G Vulnerability
٧	POSIX functions should not be called with arguments that trigger buffer overflows
ĺ	G Vulnerability
	(ML parsers should not be vulnerable o XXE attacks
ĺ	G Vulnerability
	Function-like macros should not be nvoked without all of their arguments
}	n Bug
s	The address of an automatic object should not be assigned to another object that may persist after the first object has ceased to exist
}	f Bug
	pthread_mutex_t" should be unlocked n the reverse order they were locked
}	n Bug
	pthread_mutex_t" should be properly nitialized and destroyed
}	n ̃ Bug
С	pthread_mutex_t" should not be consecutively locked or unlocked wice
}	n Bug
	unctions with "noreturn" attribute
}	n Bug
p	memcmp" should only be called with pointers to trivially copyable types with no padding
	n Bug



Search by name...

© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARI,INT, 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