Code Smell 144



VB6 XML



PHP static code analysis

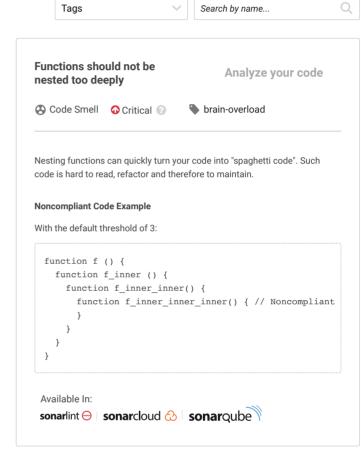
Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your PHP code

R Bug (51)

	JordPress theme and plugin editors re security-sensitive
(Security Hotspot
	llowing requests with excessive ontent length is security-sensitive
6	Security Hotspot
	fanual generation of session ID is ecurity-sensitive
(Security Hotspot
	etting loose POSIX file permissions security-sensitive
Ç	Security Hotspot
	ormatting SQL queries is security- ensitive
(Security Hotspot
"(goto" statement should not be used
Q	Code Smell
е	haracter classes in regular xpressions should not contain only ne character
Q	Code Smell
	uperfluous curly brace quantifiers hould be avoided
Q	Code Smell
	on-capturing groups without uantifier should not be used
Q	Code Smell
	ordPress option names should not e misspelled
	Code Smell

WordPress options should not be defined at the end of "wp-config.php"

Code Smell



Security Hotspot 33

© 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

Constants should not be redefined

Code Smell

Regular expressions should not contain empty groups

Code Smell

Regular expressions should not contain multiple spaces

Code Smell

Single-character alternations in regular expressions should be replaced with character classes

Code Smell

Reluctant quantifiers in regular