Code Smell (144)





VB6 XML



PHP static code analysis

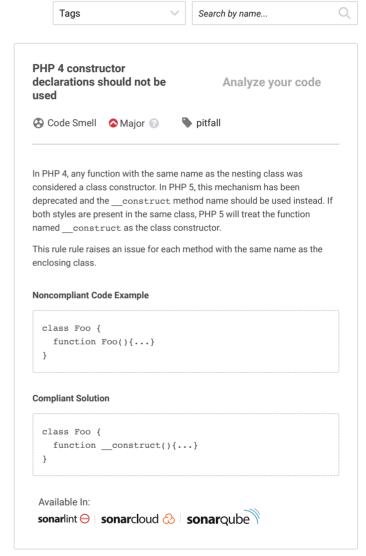
Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your PHP code

₩ Bug (51)

A	Il rules 268 Vulnerability 40
	vulnerable to injection attacks
	 G Vulnerability
	"sleep" should not be called
	Static members should be referenced with "static::"
	n Bug
	"require_once" and "include_once" should be used instead of "require" and "include"
	👬 Bug
	Errors should not be silenced
	🐧 Bug
	Files should not contain characters before " php"</td
	👬 Bug
	Method visibility should be explicitly declared
	n Bug
	Controlling permissions is security- sensitive
	Security Hotspot
	Writing cookies is security-sensitive
	Security Hotspot
	Framework-provided functions should be used to test exceptions
	☼ Code Smell
	Unicode-aware versions of character classes should be preferred
	Code Smell

Alias functions should not be used

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

Perl-style comments should not be used

Code Smell

Superglobals should not be accessed directly
Code Smell

Colors should be defined in upper case
Code Smell

String literals should not be concatenated
Code Smell