Code Smell (144)

Search by name...







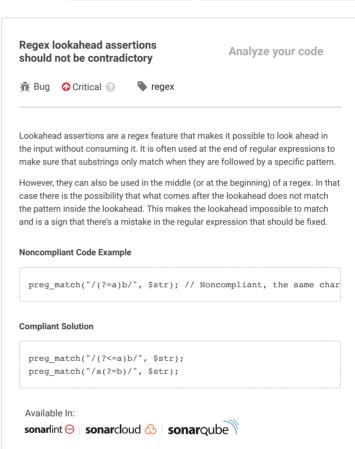
## PHP static code analysis

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

O Vulnerability	
Server-side requests should not be vulnerable to forging attacks	Rege shoul
	∰ Bu
The number of arguments passed to a function should match the number of parameters	Lookal the inp
₩ Bug	make s
Non-empty statements should change control flow or have at least one side-effect	case the the para
<b>⋒</b> Bug	Nonco
Variables should be initialized before use	pre
<b>⋒</b> Bug	Compl
Replacement strings should reference existing regular expression groups	pre
n Bug	pre
Alternation in regular expressions should not contain empty alternatives	Avail <b>son</b> a
n Bug	
Unicode Grapheme Clusters should be avoided inside regex character classes	© 2008 SON SonarSo
n Bug	
Assertions should not compare an object to itself	
<b>∰</b> Bug	
Regex alternatives should not be redundant	
₩ Bug	
Alternatives in regular expressions should be grouped when used with anchors	
₩ Bug	

Array values should not be replaced

unconditionally



Security Hotspot 33

Tags

© 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

Exceptions should not be created without being thrown

Bug

Array or Countable object count comparisons should make sense

👬 Bug

All branches in a conditional structure should not have exactly the same implementation

👬 Bug

The output of functions that don't