Code Smell (144)







All rules (268)

PHP static code analysis

6 Vulnerability (40)

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

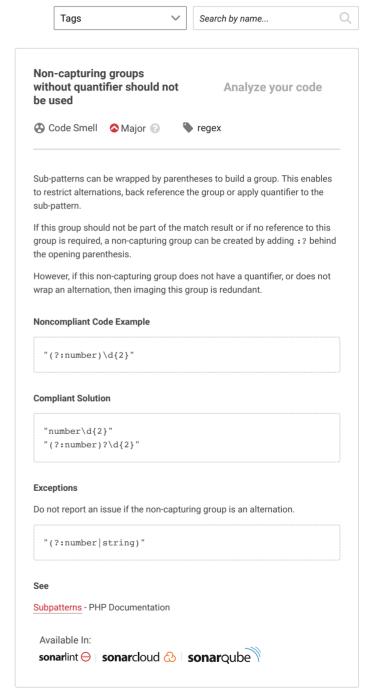
₩ Bug (51)

SHA-1 and Message-Digest ha algorithms should not be used secure contexts	
■ Vulnerability	
Assertions should not be mad end of blocks expecting an ex	
👚 Bug	
Regular expressions should be syntactically valid	е
∰ Bug	
Only one method invocation is expected when testing except	
👬 Bug	
Reading the Standard Input is security-sensitive	
Security Hotspot	
Using command line argumen security-sensitive	ts is
Security Hotspot	
Using Sockets is security-sens	sitive
Security Hotspot	
Encrypting data is security-se	nsitive
Security Hotspot	
Using regular expressions is s sensitive	ecurity-
Security Hotspot	
Deserializing objects from an untrusted source is security-s	ensitive
Security Hotspot	

Literal boolean values and nulls should not be used in equality

assertions

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

"global" should not be used

Code Smell

"switch" statements should not be nested

Code Smell

Cyclomatic Complexity of functions should not be too high

Code Smell

Control flow statements "if", "for", "while", "switch" and "try" should not be nested too deeply

Code Smell

Cyclomatic Complexity of classes