Code Smell (144)







PHP static code analysis

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

∰ Bug (51)

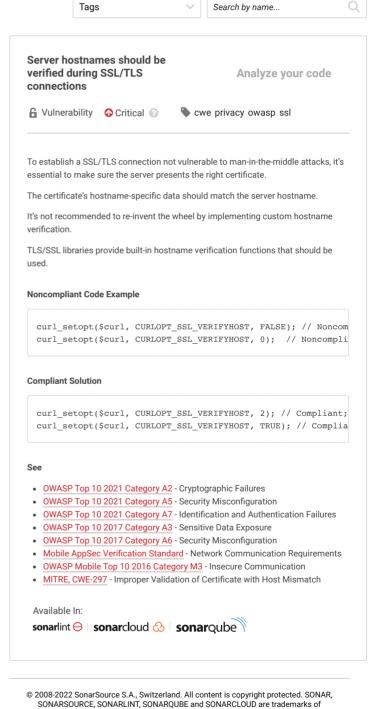
Security Hotspot 33

All rules (268)
Dynamically executing code is security-sensitive
Security Hotspot
`str_replace` should be preferred to `preg_replace`
Code Smell
"default" clauses should be first or las
☼ Code Smell
A conditionally executed single line should be denoted by indentation
☼ Code Smell
Conditionals should start on new lines
Code Smell
Cognitive Complexity of functions should not be too high
☼ Code Smell
Parentheses should not be used for calls to "echo"
Code Smell
Functions should not be nested too deeply
Code Smell
References should not be passed to function calls
Code Smell
"switch" statements should have "default" clauses
Code Smell

Code Smell

Code Smell

String literals should not be duplicated



SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved.

Privacy Policy

Methods should not be empty Code Smell
Constant names should comply with a naming convention Code Smell
Secret keys and salt values should be robust • Vulnerability
Authorizations should be based on strong decisions • Vulnerability