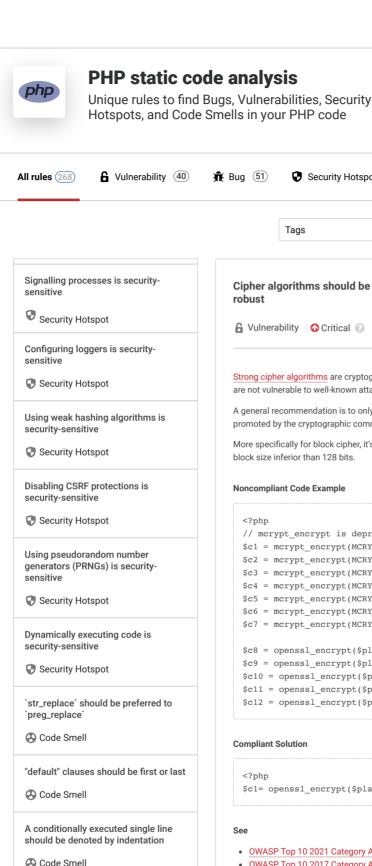
Code Smell (144)

Search by name...







Conditionals should start on new lines

Cognitive Complexity of functions should not be too high

Parentheses should not be used for

Code Smell

A Code Smell

calls to "echo"

n Bug (51)

Security Hotspot 33

Tags

Cipher algorithms should be Analyze your code robust we privacy owasp sans-top25 Strong cipher algorithms are cryptographic systems resistant to cryptanalysis, they are not vulnerable to well-known attacks like brute force attacks for example. A general recommendation is to only use cipher algorithms intensively tested and promoted by the cryptographic community. More specifically for block cipher, it's not recommended to use algorithm with a block size inferior than 128 bits. **Noncompliant Code Example** <?php // mcrypt encrypt is deprecated since PHP 7.1 \$c1 = mcrypt_encrypt(MCRYPT_DES, \$key, \$plaintext, \$mode); \$c2 = mcrypt encrypt(MCRYPT DES COMPAT, \$key, \$plaintext, \$m \$c3 = mcrypt_encrypt(MCRYPT_TRIPLEDES, \$key, \$plaintext, \$mo \$c4 = mcrypt encrypt(MCRYPT 3DES, \$key, \$plaintext, \$mode); \$c5 = mcrypt_encrypt(MCRYPT_BLOWFISH, \$key, \$plaintext, \$mod \$c6 = mcrypt_encrypt(MCRYPT_RC2, \$key, \$plaintext, \$mode); \$c7 = mcrypt_encrypt(MCRYPT_RC4, \$key, \$plaintext, \$mode); \$c8 = openssl_encrypt(\$plaintext, "bf-ecb", \$key, \$options=0 \$c9 = openssl_encrypt(\$plaintext, "des-ede3", \$key, \$options \$c10 = openssl_encrypt(\$plaintext, "des-ofb", \$key, \$options \$c11 = openssl_encrypt(\$plaintext, "rc2-cbc", \$key, \$options \$c12 = openssl encrypt(\$plaintext, "rc4", \$key, \$options=OPE Compliant Solution \$c1= openssl_encrypt(\$plaintext, "aes-256-gcm", \$key, \$optio OWASP Top 10 2021 Category A2 - Cryptographic Failures OWASP Top 10 2017 Category A3 - Sensitive Data Exposure MITRE, CWE-327 - Use of a Broken or Risky Cryptographic Algorithm • SANS Top 25 - Porous Defenses Available In: sonarlint ⊕ | sonarcloud ♦ | sonarqube

© 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

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

Control structures should use curly

Control structures should use curly braces