

- Secrets
- ABAP
- Apex
- C
- C++
- CloudFormation
- COBOL
- C#
- CSS
- Flex
- Go
- HTML
- Java
- JavaScript
- Kotlin
- Objective C
- PHP
- PL/I
- PL/SQL
- Python
- RPG
- Ruby
- Scala
- Swift
- Terraform
- Text
- TypeScript
- T-SQL
- VB.NET
- VB6
- XML



PHP static code analysis

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

All rules 268 Vulnerability 40 Bug 51 Security Hotspot 33 Code Smell 144

Tags Search by name...

Code Smell

More than one property should not be declared per statement

Code Smell

The "var" keyword should not be used

Code Smell

"<?php" and "<?=" tags should be used

Code Smell

File names should comply with a naming convention

Code Smell

Comments should not be located at the end of lines of code

Code Smell

Local variable and function parameter names should comply with a naming convention

Code Smell

Field names should comply with a naming convention

Code Smell

Lines should not end with trailing whitespaces

Code Smell

Files should contain an empty newline at the end

Code Smell

Modifiers should be declared in the correct order

Code Smell

An open curly brace should be located at the beginning of a line

Cryptographic RSA algorithms should always incorporate OAEP (Optimal Asymmetric Encryption Padding)

Analyze your code

Vulnerability Critical cwe owasp sans-top25

Without OAEP in RSA encryption, it takes less work for an attacker to decrypt the data or infer patterns from the ciphertext. This rule logs an issue when openssl_public_encrypt is used with one the following padding constants: OPENSSL_NO_PADDING or OPENSSL_PKCS1_PADDING or OPENSSL_SSLV23_PADDING.

Noncompliant Code Example

```
function encrypt($data, $key) {
    $encrypted='';
    openssl_public_encrypt($data, $encrypted, $key, OPENSSL_
    return $encrypted;
}
```

Compliant Solution

```
function encrypt($data, $key) {
    $encrypted='';
    openssl_public_encrypt($data, $encrypted, $key, OPENSSL_
    return $encrypted;
}
```

See






- OWASP Top 10 2021 Category A2 - Cryptographic Failures
- OWASP Top 10 2017 Category A3 - Sensitive Data Exposure
- OWASP Top 10 2017 Category A6 - Security Misconfiguration
- MITRE, CWE-780 - Use of RSA Algorithm without OAEP
- MITRE, CWE-327 - Use of a Broken or Risky Cryptographic Algorithm
- SANS Top 25 - Porous Defenses
- Derived from FindSecBugs rule RSA NoPadding Unsafe

Deprecated

This rule is deprecated; use {rule:php:S5542} instead.

Available In:

sonarlint sonarcloud sonarqube

 Code Smell
An open curly brace should be located at the end of a line  Code Smell
Tabulation characters should not be used  Code Smell
Method and function names should comply with a naming convention  Code Smell
Creating cookies with broadly defined "domain" flags is security-sensitive  Security Hotspot

SONAR, SONARSOURCE, SONARLIN1, 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](#)