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...

be used to end lines
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
Code Smell

Neither DES (Data Encryption Standard) nor DESede (3DES) should be used

Analyze your code

Vulnerability ❗ Blocker ? cwe owasp sans-top25

According to the US National Institute of Standards and Technology (NIST), the Data Encryption Standard (DES) is no longer considered secure:

> Adopted in 1977 for federal agencies to use in protecting sensitive, unclassified information, the DES is being withdrawn because it no longer provides the security that is needed to protect federal government information.
> Federal agencies are encouraged to use the Advanced Encryption Standard, a faster and stronger algorithm approved as FIPS 197 in 2001.

For similar reasons, RC2 should also be avoided.

Noncompliant Code Example

```
<?php
  $ciphertext = mcrypt_encrypt(MCRYPT_DES, $key, $plaintex
  // ...
  $ciphertext = mcrypt_encrypt(MCRYPT_DES_COMPAT, $key, $p
  // ...
  $ciphertext = mcrypt_encrypt(MCRYPT_TRIPLEDES, $key, $pl
  // ...
  $ciphertext = mcrypt_encrypt(MCRYPT_3DES, $key, $plainte

  $cipher = "des-ede3-cfb";  // Noncompliant
  $ciphertext_raw = openssl_encrypt($plaintext, $cipher, $
?>
```

Compliant Solution

```
<?php
  $ciphertext = mcrypt_encrypt(MCRYPT_RIJNDAEL_128, $key,
?>
```

See

- OWASP Top 10 2021 Category A2 - Cryptographic Failures
- OWASP Top 10 2017 Category A6 - Security Misconfiguration
- MITRE, CWE-326 - Inadequate Encryption Strength
- MITRE, CWE-327 - Use of a Broken or Risky Cryptographic Algorithm
- SANS Top 25 - Porous Defenses
- Derived from FindSecBugs rule DES / DESede Unsafe

Deprecated

This rule is deprecated; use {rule:php:S5547} instead.

Available In:

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

sonarlint | sonarcloud | sonarqube

Privacy Policy