

- Secrets
- ABAP
- Apex
- C
- C++
- CloudFormation
- COBOL
- 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... 🔍

Variables should not be self-assigned	Bug
Useless "if(true) {...}" and "if(false){...}" blocks should be removed	Bug
All "catch" blocks should be able to catch exceptions	Bug
Constructing arguments of system commands from user input is security-sensitive	Security Hotspot
Allowing unfiltered HTML content in WordPress is security-sensitive	Security Hotspot
Allowing unauthenticated database repair in WordPress is security-sensitive	Security Hotspot
Allowing all external requests from a WordPress server is security-sensitive	Security Hotspot
Disabling automatic updates is security-sensitive	Security Hotspot
WordPress theme and plugin editors are security-sensitive	Security Hotspot
Allowing requests with excessive content length is security-sensitive	Security Hotspot
Manual generation of session ID is security-sensitive	

Conditionals should start on new lines

Analyze your code

Code Smell

Critical ?

suspicious

Code is clearest when each statement has its own line. Nonetheless, it is a common pattern to combine on the same line an `if` and its resulting `then` statement. However, when an `if` is placed on the same line as the closing `}` from a preceding `else` or `elseif`, it is either an error - `else` is missing - or the invitation to a future error as maintainers fail to understand that the two statements are unconnected.

Noncompliant Code Example

```
if ($condition1) {
    // ...
} if ($condition2) { // Noncompliant
    //...
}
```

Compliant Solution

```
if ($condition1) {
    // ...
} elseif ($condition2) {
    //...
}
```


Or

```
if ($condition1) {
    // ...
}


if ($condition2) {
    //...
}
```

Available In:


sonarlint | sonarcloud | sonarqube

 Security Hotspot


Setting loose POSIX file permissions
is security-sensitive

 Security Hotspot


Formatting SQL queries is security-
sensitive

 Security Hotspot

"goto" statement should not be used

 Code Smell

Character classes in regular
expressions should not contain only
one character

 Code Smell