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

## "session.use_trans_sid" should not be enabled

Analyze your code

Vulnerability | Blocker | owasp php-ini

PHP's `session.use_trans_sid` automatically appends the user's session id to urls when cookies are disabled. On the face of it, this seems like a nice way to let uncookie-able users use your site anyway. In reality, it makes those users vulnerable to having their sessions hijacked by anyone who might:

- see the URL over the user's shoulder
- be sent the URL by the user
- retrieve the URL from browser history
- ...

For that reason, it's better to practice a little "tough love" with your users and force them to turn on cookies.

Since `session.use_trans_sid` is off by default, this rule raises an issue when it is explicitly enabled.

### Noncompliant Code Example

```
; php.ini
session.use_trans_sid=1   ; Noncompliant
```

### See

- OWASP Top 10 2021 Category A5 - Security Misconfiguration
- OWASP Top 10 2017 Category A6 - Security Misconfiguration

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