

- 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...



Empty statements should be removed

Code Smell

A close curly brace should be located at the beginning of a line

Code Smell

URLs should not be hardcoded

Code Smell

Class names should comply with a naming convention

Code Smell

Track uses of "TODO" tags

Code Smell

"file\_uploads" should be disabled

Vulnerability

"enable\_dl" should be disabled

Vulnerability

"session.use\_trans\_sid" should not be enabled

Vulnerability

"allow\_url\_fopen" and "allow\_url\_include" should be disabled

Vulnerability

"open\_basedir" should limit file access

Vulnerability

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

Vulnerability

"exit(...)" and "die(...)" statements should not be used

Bug

### Disabling automatic updates is security-sensitive

Analyze your code

Security Hotspot Major owasp

Automatic updates are a great way of making sure your application gets security updates as soon as they are available. Once a vendor releases a security update, it is crucial to apply it in a timely manner before malicious actors exploit the vulnerability. Relying on manual updates is usually too late, especially if the application is publicly accessible on the internet.

#### Ask Yourself Whether

- there is no specific reason for deactivating all automatic updates.
- you meant to deactivate only automatic major updates.

There is a risk if you answered yes to any of those questions.

#### Recommended Secure Coding Practices

Don't deactivate automatic updates unless you have a good reason to do so. This way, you'll be sure to receive security updates as soon as they are available. If you are worried about an automatic update breaking something, check if it is possible to only activate automatic updates for minor or security updates.

#### Noncompliant Code Example

```
define( 'WP_AUTO_UPDATE_CORE', false ); // Sensitive
define( 'AUTOMATIC_UPDATER_DISABLED', true ); // Sensitive
```

#### Compliant Solution

```
define( 'WP_AUTO_UPDATE_CORE', true ); // Minor and major
define( 'WP_AUTO_UPDATE_CORE', 'minor' ); // Only minor
define( 'AUTOMATIC_UPDATER_DISABLED', false );
```

#### See

- [OWASP Top 10 2021 Category A5](#) - Security Misconfiguration
- [Wordpress.org](#) - Disable WordPress Auto Updates
- [OWASP Top 10 2017 Category A6](#) - Security Misconfiguration


Available In:

sonarcloud | sonarqube

Functions and variables should not be defined outside of classes

 Code Smell

Track lack of copyright and license headers

 Code Smell

Octal values should not be used

 Code Smell

Switch cases should end with an unconditional "break" statement

 Code Smell

Session-management cookies should not be persistent

trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved.  
[Privacy Policy](#)