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...

Values should not be uselessly incremented
Bug

Related "if/else if" statements and "cases" in a "switch" should not have the same condition
Bug

Objects should not be created to be dropped immediately without being used
Bug

Identical expressions should not be used on both sides of a binary operator
Bug

All code should be reachable
Bug

Loops with at most one iteration should be refactored
Bug

Short-circuit logic should be used to prevent null pointer dereferences in conditionals
Bug

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

Dynamically executing code is security-sensitive

Analyze your code

Security Hotspot | Critical | cwe owasp

Executing code dynamically is security-sensitive. It has led in the past to the following vulnerabilities:

- CVE-2017-9807
- CVE-2017-9802

Some APIs enable the execution of dynamic code by providing it as strings at runtime. These APIs might be useful in some very specific meta-programming use-cases. However most of the time their use is frowned upon as they also increase the risk of Injected Code. Such attacks can either run on the server or in the client (exemple: XSS attack) and have a huge impact on an application's security.

This rule marks for review each occurrence of the `eval` function. This rule does not detect code injections. It only highlights the use of APIs which should be used sparingly and very carefully. The goal is to guide security code reviews.

Ask Yourself Whether

- the executed code may come from an untrusted source and hasn't been sanitized.
- you really need to run code dynamically.

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

Recommended Secure Coding Practices

Regarding the execution of unknown code, the best solution is to not run code provided by an untrusted source. If you really need to do it, run the code in a sandboxed environment. Use jails, firewalls and whatever means your operating system and programming language provide (example: Security Managers in java, iframes and same-origin policy for javascript in a web browser).

Do not try to create a blacklist of dangerous code. It is impossible to cover all attacks that way.

Avoid using dynamic code APIs whenever possible. Hard-coded code is always safer.

Noncompliant Code Example

```
eval($code_to_be_dynamically_executed)
```

See

- OWASP Top 10 2021 Category A3 - Injection
- OWASP Top 10 2017 Category A1 - Injection

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

- MITRE, CWE-95 - Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')

Available In:

sonarcloud | sonarqube