



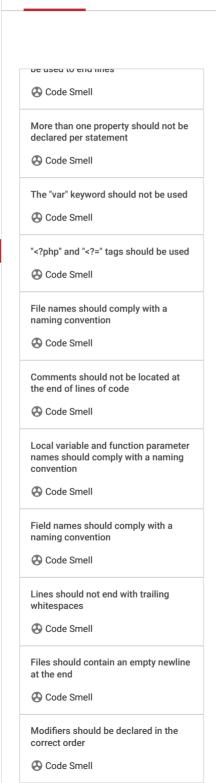


# PHP static code analysis

Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your PHP code



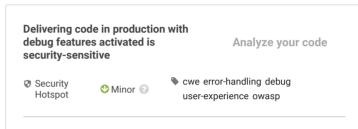
Tags



An open curly brace should be located

at the beginning of a line

Code Smell



Search by name...

Delivering code in production with debug features activated is security-sensitive. It has led in the past to the following vulnerabilities:

- CVE-2018-1999007
- CVE-2015-5306
- CVE-2013-2006

An application's debug features enable developers to find bugs more easily and thus facilitate also the work of attackers. It often gives access to detailed information on both the system running the application and users.

## Ask Yourself Whether

- the code or configuration enabling the application debug features is deployed on production servers or distributed to end users.
- the application runs by default with debug features activated.

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

### Recommended Secure Coding Practices

Do not enable debug features on production servers or applications distributed to end users.

### Sensitive Code Example

CakePHP 1.x, 2.x:

```
Configure::write('debug', 1); // Sensitive: development mode or Configure::write('debug', 2); // Sensitive: development mode or Configure::write('debug', 3); // Sensitive: development mode
```

### CakePHP 3.0:

use Cake\Core\Configure;
Configure::config('debug', true); // Sensitive: development

## WordPress:

define(  $\mbox{'WP\_DEBUG'}, \mbox{ true });$  // Sensitive: development mode

### Compliant Solution

CakePHP 1.2:

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

Configure::write('debug', 0); // Compliant; this is the prod

### CakePHP 3.0:

```
use Cake\Core\Configure;
Configure::config('debug', false); // Compliant: "0" or "fa
```

### WordPress:

```
define( 'WP_DEBUG', false ); // Compliant
```

#### See

- OWASP Top 10 2021 Category A5 Security Misconfiguration
- OWASP Top 10 2017 Category A3 Sensitive Data Exposure
- MITRE, CWE-489 Active Debug Code
- MITRE, CWE-215 Information Exposure Through Debug Information

### Available In:



© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD are trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved.

Privacy Policy