



D

月

TS

Swift

Text

T-SQL

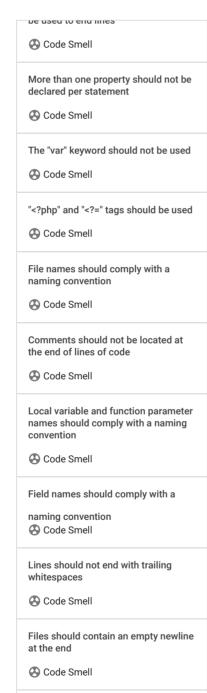
**VB.NET** 

VB6

XML

Terraform

**TypeScript** 



Modifiers should be declared in the

An open curly brace should be located

at the beginning of a line

correct order Code Smell

All rules (268)

PHP static code analysis

Unique rules to find Bugs, Vulnerabilities, Security

Hotspots, and Code Smells in your PHP code 6 Vulnerability (40) **R** Bug (51) Security Hotspot 33 Code Smell (144) Tags Search by name... "open\_basedir" should limit Analyze your code file access ■ Vulnerability Blocker cwe owasp php-ini The open\_basedir configuration in *php.ini* limits the files the script can access using, for example, include and fopen(). Leave it out, and there is no default limit, meaning that any file can be accessed. Include it, and PHP will refuse to access files outside the allowed path. open basedir should be configured with a directory, which will then be accessible recursively. However, the use of . (current directory) as an open\_basedir value should be avoided since it's resolved dynamically during script execution, so a  $\mathtt{chdir}('/')$  command could lay the whole server open to the script. This is not a fool-proof configuration; it can be reset or overridden at the script level. But its use should be seen as a minimum due diligence step. This rule raises an issue when open basedir is not present in php.ini, and when open\_basedir contains root, or the current directory (.) symbol. **Noncompliant Code Example** ; php.ini try 1 ; open\_basedir="\${USER}/scripts/data" Noncompliant; co ; php.ini try 2 open\_basedir="/:\${USER}/scripts/data" ; Noncompliant; **Compliant Solution** ; php.ini try 1 open\_basedir="\${USER}/scripts/data" • OWASP Top 10 2021 Category A1 - Broken Access Control OWASP Top 10 2021 Category A5 - Security Misconfiguration

> © 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.

• OWASP Top 10 2017 Category A6 - Security Misconfiguration

MITRE, CWE-23 - Relative Path Traversal

MITRE, CWE-36 - Absolute Path Traversal

sonarlint ⊕ | sonarcloud ♦ | sonarqube

Available In:

Privacy Policy

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