

- 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



Python static code analysis

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

All rules 216 Vulnerability 29 Bug 55 Security Hotspot 31 Code Smell 101

Tags

Search by name...

Unused class-private methods should be removed
Code Smell
Track uses of "FIXME" tags
Code Smell
"Exception" and "BaseException" should not be raised
Code Smell
Redundant pairs of parentheses should be removed
Code Smell
Nested blocks of code should not be left empty
Code Smell
Functions, methods and lambdas should not have too many parameters
Code Smell
Collapsible "if" statements should be merged
Code Smell
Logging should not be vulnerable to injection attacks
Vulnerability
Repeated patterns in regular expressions should not match the empty string
Bug
Function parameters initial values should not be ignored
Bug
Disabling versioning of S3 buckets is security-sensitive
Security Hotspot

Cognitive Complexity of functions should not be too high

Analyze your code high

Code Smell Critical ? brain-overload

Cognitive Complexity is a measure of how hard the control flow of a function is to understand. Functions with high Cognitive Complexity will be difficult to maintain.

See


- Cognitive Complexity

Available In:

sonarlint sonarcloud sonarqube

© 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


Disabling server-side encryption of S3 buckets is security-sensitive

 Security Hotspot

Having a permissive Cross-Origin Resource Sharing policy is security-sensitive

 Security Hotspot

Delivering code in production with debug features activated is security-sensitive

 Security Hotspot

Allowing both safe and unsafe HTTP methods is security-sensitive

 Security Hotspot