



Secrets



_{АРЕХ} Арех

C C

C+-

CloudFormation

COBOL COBOL

C# C#

E CSS

X Flex

-GO Go

5 HTML

🗐 Java

JS JavaScript

Kotlin

Objective C

PHP

PL/I

PL/SQL PL/SQL

Python

RPG RPG

Ruby

■ Scala

Swift

Terraform

■ Text

Ts TypeScript

T-SQL

VB VB.NET

VB6 VB6

ML XML



Python static code analysis

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

All rules 216

6 Vulnerability 29



Security Hotspot 31



Code Smell (101)

Code Smell

Local variable and function parameter names should comply with a naming convention

Code Smell

Field names should comply with a naming convention

Code Smell

Class names should comply with a naming convention

Code Smell

Method names should comply with a naming convention

Code Smell

Track uses of "TODO" tags

Code Smell

HTML autoescape mechanism should not be globally disabled

Vulnerability

Variables, classes and functions should be either defined or imported

👚 Bug

"__exit__" should accept type, value, and traceback arguments

👬 Bug

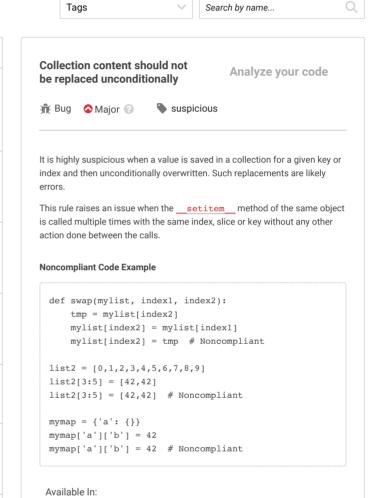
"return" and "yield" should not be used in the same function

🖟 Bug

Track lack of copyright and license headers

Code Smell

HTTP response headers should not be vulnerable to injection attacks



© 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

sonarlint ⊕ | sonarcloud ₺ | sonarqube

Regular expressions should be syntactically valid

Bug

Sending emails is security-sensitive

Security Hotspot

Reading the Standard Input is security-sensitive

Security Hotspot

Using command line arguments is security-sensitive

Security Hotspot