

- 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... 🔍

Bug
Exceptions' "__cause__" should be either an Exception or None
Bug
"break" and "continue" should not be used outside a loop
Bug
Break, continue and return statements should not occur in "finally" blocks
Bug
Allowing public ACLs or policies on a S3 bucket is security-sensitive
Security Hotspot
Using publicly writable directories is security-sensitive
Security Hotspot
Using clear-text protocols is security-sensitive
Security Hotspot
Expanding archive files without controlling resource consumption is security-sensitive
Security Hotspot
Signalling processes is security-sensitive
Security Hotspot
Configuring loggers is security-sensitive
Security Hotspot
Using weak hashing algorithms is security-sensitive
Security Hotspot
Disabling CSRF protections is

"__init__" should not return a value

Analyze your code

Bug

Blocker

?

By contract, every Python function returns something, even if it's the `None` value, which can be returned implicitly by omitting the `return` statement, or explicitly.

The `__init__` method is required to return `None`. A `TypeError` will be raised if the `__init__` method either yields or returns any expression other than `None`. Returning some expression that evaluates to `None` will not raise an error, but is considered bad practice.

Noncompliant Code Example

```
class MyClass(object):
    def __init__(self):
        self.message = 'Hello'
        return self # Noncompliant
```


Compliant Solution

```
class MyClass(object):
    def __init__(self):
        self.message = 'Hello'
```


Available In:

sonarlint | sonarcloud | sonarqube


security-sensitive

 Security Hotspot


Using non-standard cryptographic algorithms is security-sensitive

 Security Hotspot

Using pseudorandom number generators (PRNGs) is security-sensitive

 Security Hotspot

Constants should not be used as conditions

 Code Smell

"SystemExit" should be re-raised

 Code Smell