

- 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... 🔍

unpredictable
Vulnerability
Regular expressions should not be vulnerable to Denial of Service attacks
Vulnerability
Hashes should include an unpredictable salt
Vulnerability
Regex lookahead assertions should not be contradictory
Bug
Regex boundaries should not be used in a way that can never be matched
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

Variables, classes and functions should be defined before being used

Analyze your code

Bug Blocker ?

Variables, Classes and functions should be defined before they are used, otherwise the code will fail.

Noncompliant Code Example

```
def noncompliant():
    foo() # Noncompliant
    foo = sum

    func() # Noncompliant
    def func():
        pass

    MyClass() # Noncompliant
    class MyClass:
        pass
```

Compliant Solution


```
def compliant():
    foo = sum
    foo()

    def func():
        pass
    func()

    class MyClass:
        pass
    MyClass()
```

Available In:
sonarlint sonarcloud sonarqube

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 security-sensitive