

- Secrets
- ABAP
- Apex
- C
- C++
- CloudFormation
- COBOL
- 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... 🔍

Only strings should be listed in <code>"__all__"</code>
🐞 Bug
<code>"__init__"</code> should not return a value
🐞 Bug
<code>"yield"</code> and <code>"return"</code> should not be used outside functions
🐞 Bug
String formatting should not lead to runtime errors
🐞 Bug
Recursion should not be infinite
🐞 Bug
Silly equality checks should not be made
🐞 Bug
Granting access to S3 buckets to all or authenticated users is security-sensitive
🛡️ Security Hotspot
Hard-coded credentials are security-sensitive
🛡️ Security Hotspot
Functions returns should not be invariant
💩 Code Smell
The <code>"exec"</code> statement should not be used
💩 Code Smell
Backticks should not be used
💩 Code Smell

Only defined names should be listed in `"__all__"`

Analyze your code

🐞 Bug 🚫 Blocker ?

Developers may define a list named `__all__` in a module to limit the names imported from it by wildcard imports (`from mymodule import *`). This list can only reference defined names, otherwise an `AttributeError` will be raised when the module is imported.

Noncompliant Code Example

```
from mymodule import my_func

__all__ = ["unknown_func"] # Noncompliant. "unknown_fu
```

Compliant Solution

```
from mymodule import my_func

__all__ = ["my_func"]
```

See

- Python documentation - Importing \* From a Package

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](#)


Methods and field names should not differ only by capitalization

 Code Smell

JWT should be signed and verified

 Vulnerability

Cipher algorithms should be robust

 Vulnerability

Encryption algorithms should be used with secure mode and padding scheme

 Vulnerability

Server hostnames should be verified during SSL/TLS connections

 Vulnerability