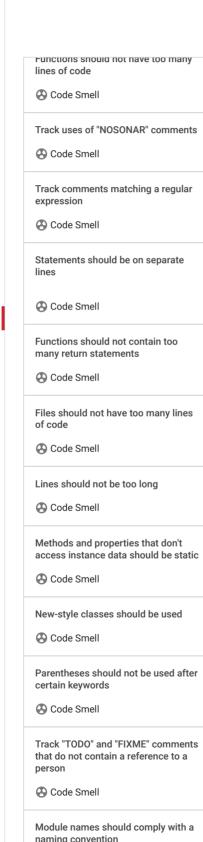




VB.NET

VB6

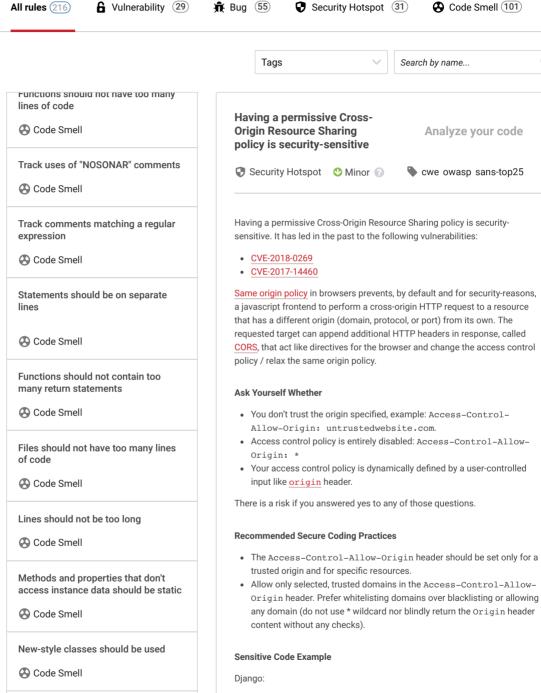
XML





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





CORS ORIGIN ALLOW ALL = True # Sensitive Flask from flask import Flask from flask_cors import CORS app = Flask(__name__) CORS(app, resources={r"/*": {"origins": "*", "send_wild

User-controlled origin:

Code Smell

Comments should not be located at the end of lines of code

Code Smell

Lines should not end with trailing whitespaces

Code Smell

Files should contain an empty newline at the end

Code Smell

Long suffix "L" should be upper case

Code Smell

```
origin = request.headers['ORIGIN']
resp = Response()
resp.headers['Access-Control-Allow-Origin'] = origin #
```

Compliant Solution

Django:

```
CORS_ORIGIN_ALLOW_ALL = False # Compliant
```

Flask:

```
from flask import Flask
from flask_cors import CORS

app = Flask(__name__)
CORS(app, resources={r"/*": {"origins": "*", "send_wild"}
```

User-controlled origin validated with an allow-list:

```
origin = request.headers['ORIGIN']
resp = Response()
if origin in TRUSTED_ORIGINS:
    resp.headers['Access-Control-Allow-Origin'] = origin
```

See

- OWASP Top 10 2021 Category A5 Security Misconfiguration
- OWASP Top 10 2021 Category A7 Identification and Authentication
 Failures
- developer.mozilla.org CORS
- <u>developer.mozilla.org</u> Same origin policy
- OWASP Top 10 2017 Category A6 Security Misconfiguration
- OWASP HTML5 Security Cheat Sheet Cross Origin Resource Sharing
- MITRE, CWE-346 Origin Validation Error
- MITRE, CWE-942 Overly Permissive Cross-domain Whitelist
- SANS Top 25 Porous Defenses

Available In:

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