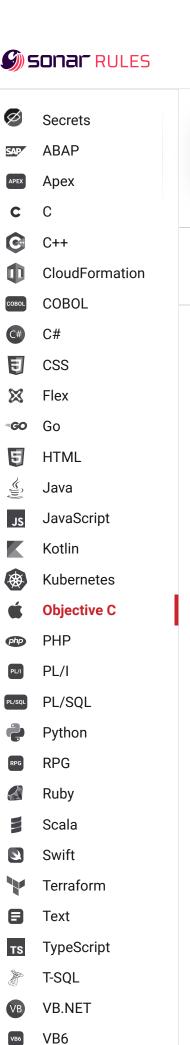
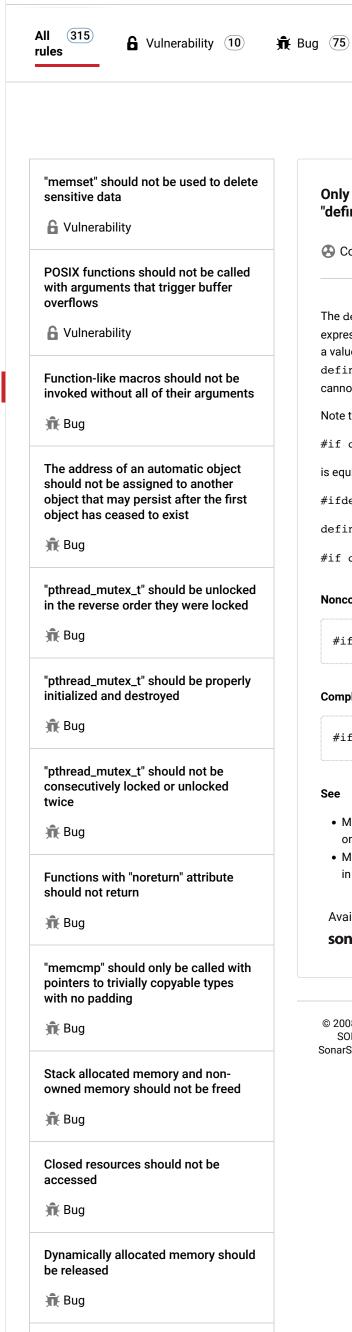
O Quick 13 Fix





XML



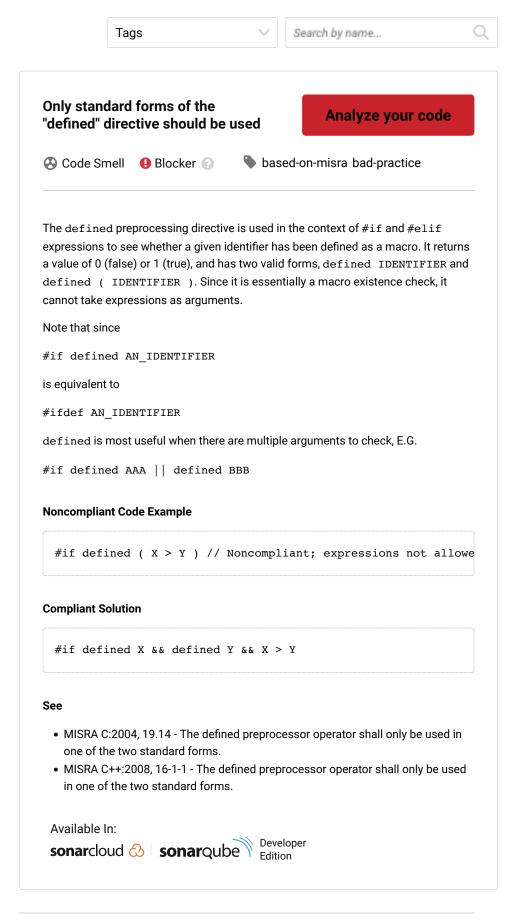
Objective C static code analysis

Unique rules to find Bugs, Vulnerabilities, Security

Hotspots, and Code Smells in your OBJECTIVE C code

o Security

Hotspot



⊗ Code (212)

© 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**

Freed memory should not be used
∰ Bug
Memory locations should not be released more than once
∰ Bug
Memory access should be explicitly bounded to prevent buffer overflows
Rug
Printf-style format strings should not lead to unexpected behavior at runtime
Rug
Recursion should not be infinite
∰ Bug
Resources should be closed
∰ Bug
Hard-coded credentials are security- sensitive
Security Hotspot
"goto" should jump to labels declared later in the same function
Code Smell
Only standard forms of the "defined" directive should be used
Switch labels should not be nested inside non-switch blocks