

- Secrets
- ABAP
- Apex
- C
- C++
- CloudFormation
- COBOL
- C# 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



C# static code analysis

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

All rules 409

Vulnerability 34

Bug 76

Security Hotspot 28

Code Smell 271

Quick Fix 52

Tags ▾

Search by name... 🔍

Bug

Collections should not be passed as arguments to their own methods

Bug

Related "if/else if" statements should not have the same condition

Bug

Objects should not be created to be dropped immediately without being used

Bug

Identical expressions should not be used on both sides of a binary operator

Bug

Loops with at most one iteration should be refactored

Bug

Variables should not be self-assigned

Bug

Constructing arguments of system commands from user input is security-sensitive

Security Hotspot

Deserializing objects without performing data validation is security-sensitive

Security Hotspot

Disabling ASP.NET "Request Validation" feature is security-sensitive

Security Hotspot

Allowing requests with excessive content length is security-sensitive

Security Hotspot

Setting loose file permissions is

Cognitive Complexity of methods should not be too high

Analyze your code

Code Smell Critical ? brain-overload

Cognitive Complexity is a measure of how hard the control flow of a method is to understand. Methods with high Cognitive Complexity will be difficult to maintain.





See

- Cognitive Complexity

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](#)

security-sensitive  Security Hotspot
Formatting SQL queries is security-sensitive  Security Hotspot
Using hardcoded IP addresses is security-sensitive  Security Hotspot
"goto" statement should not be used  Code Smell
"new Guid()" should not be used