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

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...

move the counter in the right direction
Bug

"ToString()" method should not return null
Bug

Return values from functions without side effects should not be ignored
Bug

Values should not be uselessly incremented
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

Assemblies should have version information

Analyze your code

Code Smell | Critical | pitfall

If no `AssemblyVersionAttribute` is provided, the same default version will be used for every build. Since the version number is used by The .NET Framework to uniquely identify an assembly this can lead to broken dependencies.

Noncompliant Code Example

```
using System.Reflection;

[assembly: AssemblyTitle("MyAssembly")] // Noncompliant

namespace MyLibrary
{
}
```

Compliant Solution

```
using System.Reflection;

[assembly: AssemblyTitle("MyAssembly")]
[assembly: AssemblyVersion("1.2.125.0")]

namespace MyLibrary
{
}
```

See

Microsoft documentation - Assembly Versioning

Available In:

sonarlint | sonarcloud | sonarqube

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 security-sensitive

Security Hotspot