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...

"protected" members
Code Smell

Underscores should be used to make large numbers readable
Code Smell

"ToString()" calls should not be redundant
Code Smell

"==" should not be used when "Equals" is overridden
Code Smell

An abstract class should have both abstract and concrete methods
Code Smell

Multiple variables should not be declared on the same line
Code Smell

Culture should be specified for "string" operations
Code Smell

"switch" statements should have at least 3 "case" clauses
Code Smell

break statements should not be used except for switch cases
Code Smell

String literals should not be duplicated
Code Smell

Files should contain an empty newline at the end
Code Smell

Unused "using" should be removed
Code Smell

Searching OS commands in PATH is security-sensitive

Analyze your code

Security Hotspot | Minor | cwe owasp

When executing an OS command and unless you specify the full path to the executable, then the locations in your application's `PATH` environment variable will be searched for the executable. That search could leave an opening for an attacker if one of the elements in `PATH` is a directory under his control.

Ask Yourself Whether

- The directories in the PATH environment variable may be defined by not trusted entities.

There is a risk if you answered yes to this question.

Recommended Secure Coding Practices

Fully qualified/absolute path should be used to specify the OS command to execute.

Sensitive Code Example

```
Process p = new Process();
p.StartInfo.FileName = "binary"; // Sensitive
```

Compliant Solution

```
Process p = new Process();
p.StartInfo.FileName = @"C:\Apps\binary.exe"; // Compliant
```

See

- OWASP Top 10 2021 Category A8 - Software and Data Integrity Failures
- OWASP Top 10 2017 Category A1 - Injection
- MITRE, CWE-426 - Untrusted Search Path
- MITRE, CWE-427 - Uncontrolled Search Path Element

Available In:

sonarcloud | sonarqube

A close curly brace should be located at the beginning of a line

Code Smell

Tabulation characters should not be used

Code Smell

Methods and properties should be named in PascalCase

Code Smell

Track uses of in-source issue suppressions

Code Smell