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...

Code Smell

Cognitive Complexity of methods should not be too high

Code Smell

"params" should not be introduced on overrides

Code Smell

"[DefaultValue]" should not be used when "[DefaultParameterValue]" is meant

Code Smell

"[Optional]" should not be used on "ref" or "out" parameters

Code Smell

Non-flags enums should not be used in bitwise operations

Code Smell

Inner class members should not shadow outer class "static" or type members

Code Smell

"Explicit" conversions of "foreach" loops should not be used

Code Smell

Instance members should not write to "static" fields

Code Smell

"IndexOf" checks should not be for positive numbers

Code Smell

Whitespace and control characters in string literals should be explicit

Code Smell

Properties should not make collection or array copies

Code Smell

Server certificates should be verified during SSL/TLS connections

Analyze your code

Vulnerability | Critical | cwe privacy owasp ssl

Validation of X.509 certificates is essential to create secure SSL/TLS sessions not vulnerable to man-in-the-middle attacks.

The certificate chain validation includes these steps:

- The certificate is issued by its parent Certificate Authority or the root CA trusted by the system.
- Each CA is allowed to issue certificates.
- Each certificate in the chain is not expired.

It's not recommended to reinvent the wheel by implementing custom certificate chain validation.

TLS libraries provide built-in certificate validation functions that should be used.

Noncompliant Code Example

```
ServicePointManager.ServerCertificateValidationCallback +=
    (sender, certificate, chain, errors) => {
        return true; // Noncompliant: trust all certificates
    };
```

Compliant Solution

```
ServicePointManager.ServerCertificateValidationCallback +=
    (sender, certificate, chain, errors) =>
    {
        if (development) return true; // for development, tr
        return errors == SslPolicyErrors.None
            && validCerts.Contains(certificate.GetCertHashSt
    };
```

See

- OWASP Top 10 2021 Category A2 - Cryptographic Failures
- OWASP Top 10 2021 Category A5 - Security Misconfiguration
- OWASP Top 10 2021 Category A7 - Identification and Authentication Failures
- OWASP Top 10 2017 Category A3 - Sensitive Data Exposure
- OWASP Top 10 2017 Category A6 - Security Misconfiguration
- Mobile AppSec Verification Standard - Network Communication Requirements
- OWASP Mobile Top 10 2016 Category M3 - Insecure Communication
- MITRE, CWE-295 - Improper Certificate Validation

Available In:

sonarlint | sonarcloud | sonarqube

Flags enumerations zero-value members should be named "None"

Code Smell

Overflow checking should not be disabled for "Enumerable.Sum"

Code Smell

Field-like events should not be virtual

Code Smell

Non-constant static fields should not be visible

Code Smell