

- 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...

Unread "private" fields should be removed

Code Smell

Base class methods should not be hidden

Code Smell

Inherited member visibility should not be decreased

Code Smell

Threads should not lock on objects with weak identity

Code Smell

A conditionally executed single line should be denoted by indentation

Code Smell

Conditionals should start on new lines

Code Smell

Assemblies should have version information

Code Smell

Exception types should be "public"

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

JWT should be signed and verified with strong cipher algorithms

Analyze your code

Vulnerability Critical cwe privacy owasp

If a JSON Web Token (JWT) is not signed with a strong cipher algorithm (or not signed at all) an attacker can forge it and impersonate user identities.

- Don't use none algorithm to sign or verify the validity of a token.
- Don't use a token without verifying its signature before.

### Noncompliant Code Example

[jwt-dotnet](#) library:

```
var decodedtoken1 = decoder.Decode(token, secret, verify: false);

var decodedtoken2 = new JwtBuilder()
    .WithSecret(secret)
    .Decode(forgedtoken1); // Noncompliant: signature should be verified
```

### Compliant Solution

[jwt-dotnet](#) library:

```
var decodedtoken1 = decoder.Decode(forgedtoken1, secret, verify: true);





var decodedtoken2 = new JwtBuilder()
    .WithSecret(secret)
    .MustVerifySignature()
    .Decode(token); // Compliant
```

### See

- [OWASP Top 10 2021 Category A2](#) - Cryptographic Failures
- [OWASP Top 10 2017 Category A3](#) - Sensitive Data Exposure
- [MITRE, CWE-347](#) - Improper Verification of Cryptographic Signature

Available In:

sonarlint | sonarcloud | sonarqube

 Code Smell
<b>Non-flags enums should not be used in bitwise operations</b>  Code Smell
<b>Inner class members should not shadow outer class "static" or type members</b>  Code Smell
<b>"Explicit" conversions of "foreach" loops should not be used</b>  Code Smell
<b>Instance members should not write to</b>