

- 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...



"[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

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

Code Smell

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

Code Smell

### LDAP connections should be authenticated

Analyze your code

Vulnerability Critical cwe owasp

An LDAP client authenticates to an LDAP server with a "bind request" which provides, among other, a [simple authentication method](#).

Simple authentication in LDAP can be used with three different mechanisms:

- Anonymous Authentication Mechanism* by performing a bind request with a username and password value of zero length.
- Unauthenticated Authentication Mechanism* by performing a bind request with a password value of zero length.
- Name/Password Authentication Mechanism* by performing a bind request with a password value of non-zero length.

Anonymous binds and unauthenticated binds allow access to information in the LDAP directory without providing a password, their use is therefore strongly discouraged.

#### Noncompliant Code Example

This rule raises an issue when an LDAP connection is created with `AuthenticationTypes.Anonymous` or `AuthenticationTypes.None`.

```
DirectoryEntry myDirectoryEntry = new DirectoryEntry(adPath)
myDirectoryEntry.AuthenticationType = AuthenticationTypes.No

DirectoryEntry myDirectoryEntry = new DirectoryEntry(adPath,
```

#### Compliant Solution

```
DirectoryEntry myDirectoryEntry = new DirectoryEntry(myADSPa





DirectoryEntry myDirectoryEntry = new DirectoryEntry(myADSPa
```

#### See

- [OWASP Top 10 2021 Category A7](#) - Identification and Authentication Failures
- [OWASP Top 10 2017 Category A2](#) - Broken Authentication
- [MITRE, CWE-521](#) - Weak Password Requirements
- [ldapwiki.com](#) - Simple Authentication

Available In:

sonarlint | sonarcloud | sonarqube

<b>Field-like events should not be virtual</b>  Code Smell
<b>Non-constant static fields should not be visible</b>  Code Smell
<b>Inappropriate casts should not be made</b>  Code Smell
<b>Constructors should only call non-overridable methods</b>  Code Smell