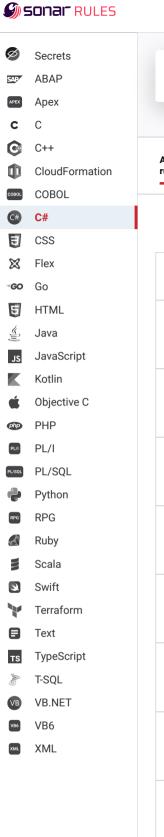
Analyze your code

serialization owasp



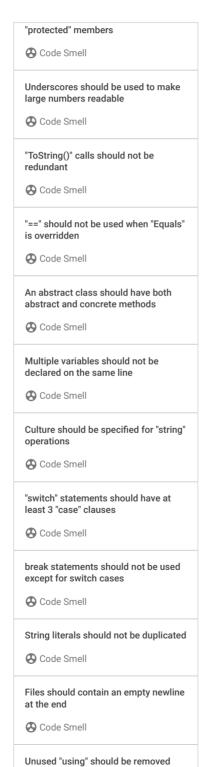




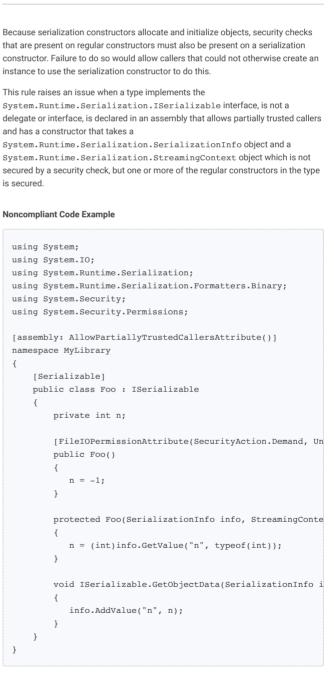
be secured

♠ Vulnerability

Serialization constructors should



Code Smell



Compliant Solution

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

Code Smell

Tabulation characters should not be

Code Smell

Methods and properties should be named in PascalCase

Code Smell

Track uses of in-source issue suppressions

Code Smell

```
using System;
using System.IO;
using System.Runtime.Serialization;
using System.Runtime.Serialization.Formatters.Binary;
using System.Security;
using System.Security.Permissions;
[assembly: AllowPartiallyTrustedCallersAttribute()]
namespace MyLibrary
    [Serializable]
   public class Foo : ISerializable
        private int n;
        [FileIOPermissionAttribute(SecurityAction.Demand, Un
        public Foo()
           n = -1;
        [FileIOPermissionAttribute(SecurityAction.Demand, Un
        protected Foo(SerializationInfo info, StreamingConte
           n = (int)info.GetValue("n", typeof(int));
        void ISerializable.GetObjectData(SerializationInfo i
           info.AddValue("n", n);
}
```

- OWASP Top 10 2021 Category A8 Software and Data Integrity Failures
- OWASP Top 10 2017 Category A8 Insecure Deserialization

Available In:

sonarlint ⊕ | sonarcloud ♦ | sonarqube



© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD are trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved. Privacy Policy