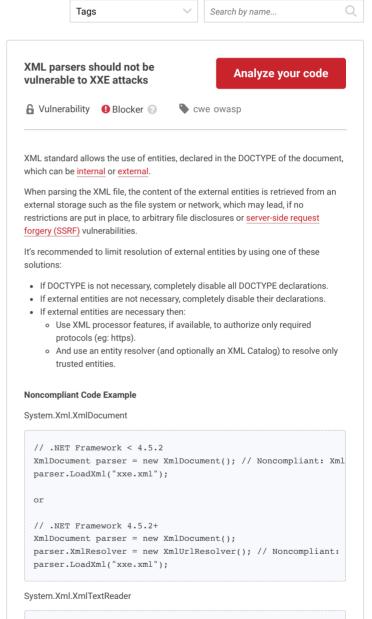


Code Smell



// .NET Framework < 4.5.2 XmlTextReader reader = new XmlTextReader("xxe.xml"); // Nonc while (reader.Read()) // .NET Framework 4.5.2+ XmlTextReader reader = new XmlTextReader("xxe.xml"); reader.XmlResolver = new XmlUrlResolver(); // Noncompliant: while (reader.Read()) { ... }

System.Xml.XmlReader

"operator==" should not be overloaded on reference types

Code Smell

Type should not be examined on "System.Type" instances

Code Smell

Test method signatures should be correct

Code Smell

Method overloads with default parameter values should not overlap

Code Smell

```
// .NET Framework 4.5.2+
XmlReaderSettings settings = new XmlReaderSettings();
settings.DtdProcessing = DtdProcessing.Parse;
settings.XmlResolver = new XmlUrlResolver();
XmlReader reader = XmlReader.Create("xxe.xml", settings); //
while (reader.Read())
{ ... }
```

System.Xml.XPath.XPathDocument

```
// prior to .NET 4.5.2
XPathDocument doc = new XPathDocument("example.xml"); // Non
XPathNavigator nav = doc.CreateNavigator();
string xml = nav.InnerXml.ToString();
```

Compliant Solution

System.Xml.XmlDocument

```
XmlDocument parser = new XmlDocument();
parser.XmlResolver = null; // Compliant: XmlResolver has bee
parser.LoadXml("xxe.xml");
or

XmlDocument parser = new XmlDocument(); // Compliant: XmlDoc
parser.LoadXml("xxe.xml");
```

System.Xml.XmlTextReader

```
// .NET 4.5.2+
XmlTextReader reader = new XmlTextReader("xxe.xml"); // Comp
while (reader.Read())
{ ... }

// .NET 4.0 to .NET 4.5.1
XmlTextReader reader = new XmlTextReader("xxe.xml");
reader.DtdProcessing = DtdProcessing.Prohibit; // Compliant:

// < .NET 4.0
XmlTextReader reader = new XmlTextReader(stream);
reader.ProhibitDtd = true; // Compliant: default is false</pre>
```

System.Xml.XmlReader

```
XmlReader reader = XmlReader.Create("xxe.xml"); // Compliant
while (reader.Read())
{ ... }
```

System.Xml.XPath.XPathDocument

```
// prior to .NET 4.5.2
XmlReader reader = XmlReader.Create("example.xml");
XPathDocument doc = new XPathDocument(reader); // Compliant:
XPathNavigator nav = doc.CreateNavigator();
string xml = nav.InnerXml.ToString();
```

See

- OWASP Top 10 2021 Category A5 Security Misconfiguration
- OWASP Top 10 2017 Category A4 XML External Entities (XXE)
- OWASP XXE Prevention Cheat Sheet
- MITRE, CWE-611 Information Exposure Through XML External Entity Reference
- MITRE, CWE-827 Improper Control of Document Type Definition

Available In:

sonarlint ⊖ | sonarcloud 🐼 | sonarqube

owners. All rights are expressly reserved.

<u>Privacy Policy</u>