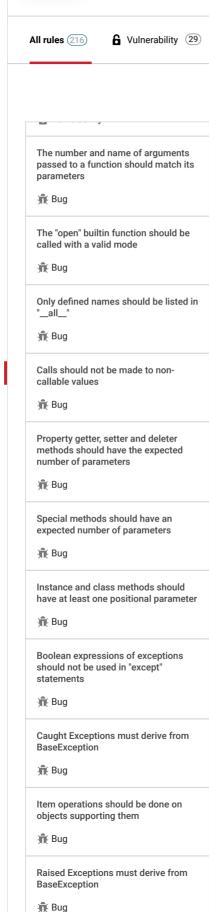


T-SQL

VB.NET

VB₆

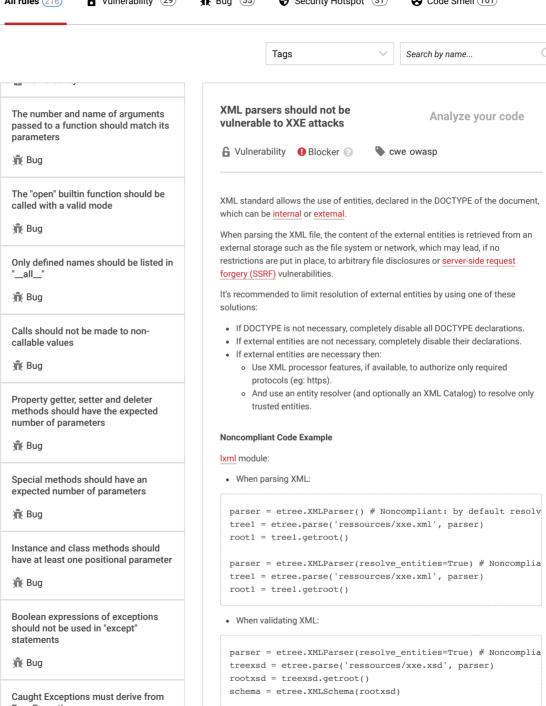
XML





Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your PYTHON code





ac = etree.XSLTAccessControl(read network=True, write networ transform = etree.XSLT(rootxsl, access_control=ac)

xml.sax module:

· When transforming XML:

```
parser = xml.sax.make parser()
mvHandler = MvHandler()
parser.setContentHandler(myHandler)
```

Operators should be used on compatible types



Function arguments should be passed only once



Iterable unpacking, "for-in" loops and "yield from" should use an Iterable object



Variables, classes and functions should be defined before being used

```
parser.setFeature(feature_external_ges, True) # Noncompliant
parser.parse("ressources/xxe.xml")
```

Compliant Solution

Ixml module:

• When parsing XML, disable resolve_entities and network access:

```
parser = etree.XMLParser(resolve_entities=False, no_network=
tree1 = etree.parse('ressources/xxe.xml', parser)
root1 = tree1.getroot()
```

 When validating XML (note that network access cannot be completely disabled when calling XMLSchema):

```
parser = etree.XMLParser(resolve_entities=False) # Compliant
treexsd = etree.parse('ressources/xxe.xsd', parser)
rootxsd = treexsd.getroot()
schema = etree.XMLSchema(rootxsd) # Compliant
```

• When transforming XML, disable access to network and file system:

```
parser = etree.XMLParser(resolve_entities=False) # Compliant
treexsl = etree.parse('ressources/xxe.xsl', parser)
rootxsl = treexsl.getroot()

ac = etree.XSLTAccessControl.DENY_ALL # Compliant
transform = etree.XSLT(rootxsl, access_control=ac) # Complia
```

To prevent xxe attacks with xml.sax module (for other security reasons than XXE, xml.sax is not recommended):

```
parser = xml.sax.make_parser()
myHandler = MyHandler()
parser.setContentHandler(myHandler)
parser.parse("ressources/xxe.xml") # Compliant: in version 3
parser.setFeature(feature_external_ges, False) # Compliant
parser.parse("ressources/xxe.xml")
```

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

© 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