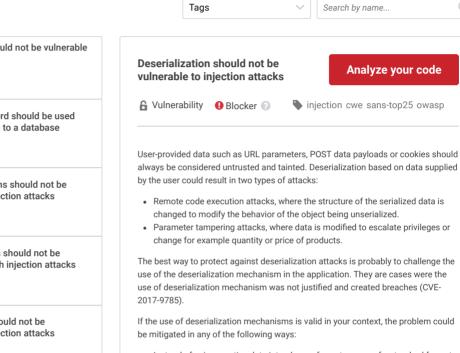


₩ Bug

whitespace

SQL keywords should be delimited by





• Instead of using a native data interchange format, use a safe, standard format such as untyped JSON or structured data approaches such as Google Protocol

- To ensure integrity is not compromised, add a digital signature (HMAC) to the serialized data that is validated before deserialization (this is only valid if the client doesn't need to modify the serialized data)
- As a last resort, restrict descrialization to be possible only to specific, whitelisted classes

Noncompliant Code Example

For XmlSerializer serializer, the expected type should not come from user-controlled input:

```
public class XmlSerializerTestCase : Controller
  public ActionResult unsecuredeserialization(string typeNa
  {
    ExpectedType obj = null;
    Type t = Type.GetType(typeName); // typeName is user-co
     XmlSerializer serializer = new XmlSerializer(t); // Non
    obj = (ExpectedType) serializer.Deserialize(fs);
     // ....
}
```

Compliant Solution

For XmlSerializer serializer:

```
public class XmlSerializerTestCase : Controller
  public ActionResult securedeserialization()
```



Composite format strings should not lead to unexpected behavior at runtime

Rug

Recursion should not be infinite

👬 Bug

Destructors should not throw exceptions

🖟 Bug

Hard-coded credentials are securitysensitive

```
ExpectedType obj = null;
    XmlSerializer serializer = new XmlSerializer(typeof(Exp
    obj = (ExpectedType) serializer.Deserialize(fs);
    // ....
  }
}
```

See

- OWASP Top 10 2021 Category A8 Software and Data Integrity Failures
- OWASP Top 10 2017 Category A8 Insecure Deserialization
- MITRE, CWE-134 Use of Externally-Controlled Format String
- MITRE, CWE-502 Deserialization of Untrusted Data
- SANS Top 25 Risky Resource Management

Available In:

sonarcloud 🕙 sonarqube Developer Edition

© 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