Test.php

* **总漏洞数**: 1

1. **漏洞类型**: XML 外部实体注入 (XML External Entity Injection, XXE)
   * **CWE 标号**: CWE-611
   * **描述**: 使用 libxml\_disable\_entity\_loader(false) 重新启用了实体加载，并且在解析用户输入的 XML 时未禁用外部实体引用，可能导致 XXE 攻击。
   * **修复建议**: 禁用外部实体加载，确保在解析用户输入的 XML 时不加载外部实体。

Test2.php

* **总漏洞数**: 1

1. **漏洞类型**: XML 外部实体注入 (XML External Entity Injection, XXE)
   * **CWE 标号**: CWE-611
   * **描述**: 使用 libxml\_disable\_entity\_loader(false) 重新启用了实体加载，并且在解析用户输入的 XML 时未禁用外部实体引用，可能导致 XXE 攻击。
   * **修复建议**: 禁用外部实体加载，确保在解析用户输入的 XML 时不加载外部实体。

Xmlreader\_tests.cs

* **总漏洞数**: 1

1. **漏洞类型**: XML 外部实体注入 (XML External Entity Injection, XXE)
   * **CWE 标号**: CWE-611
   * **描述**: 在 XMLReader\_WithDTDProcessingParseAndXmlResolverSet\_NotSafe 测试方法中，启用了 DTD 处理和设置了 XmlResolver，可能导致 XXE 攻击。
   * **修复建议**: 禁用外部实体解析，通过设置 DtdProcessing 为 Ignore 或 Prohibit，并禁用 XmlResolver。

Xxe.js

* **总漏洞数**: 1

1. **漏洞类型**: XML 外部实体注入 (XML External Entity Injection, XXE)
   * **CWE 标号**: CWE-611
   * **描述**: 使用 libxmljs.parseXmlString 解析用户上传的 XML 文件时启用了 noent 选项，可能导致 XXE 攻击。
   * **修复建议**: 禁用外部实体加载，确保在解析用户输入的 XML 时不加载外部实体。

Xxe1.cs

* **总漏洞数**: 1

1. **漏洞类型**: XML 外部实体注入 (XML External Entity Injection, XXE)
   * **CWE 标号**: CWE-611
   * **描述**: 使用 XmlDocument.LoadXml 解析用户输入的 XML 字符串时未禁用外部实体加载，可能导致 XXE 攻击。
   * **修复建议**: 禁用外部实体加载，确保在解析用户输入的 XML 时不加载外部实体。