CWE-611 : XML External Entity Reference (XXE)

This guide explains XML Eternal Entity Reference (XXE) in more detail.

Contents:

XML External Entity Reference (XXE) (CWE-611)

CWE-611 describes **XXE injection** as follows:

> "The software processes an XML document that can contain **XML entities** with URIs that resolves to documents outside of the intended sphere of control, causing the product to embed incorrect documents into its output."

An XML External Entity attack is a type of attack against an application that parses XML input.

This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser.This attack may lead to the disclosure of confidential data, denial of service, server side request forgery and other system impacts.

The XML standard defines the structure of an XML document. The standard defines a concept called an *entity*, which is a storage unit of some type.

There are a few different types of entities (external entity), that can access local or remote content via a declared system identifier. The system identifier is assumed to be a URI that can be dereferenced (accessed) by the XML processor when processing the entity.

The XML processor then replaces occurrences of the named external entity with the contents dereferenced by the system identifier. If the system identifier contains tainted data and the XML processor dereferences this tainted data, the XML processor may disclose confidential information normally not accessible by the application. Similar attack vectors apply the usage of external DTDs, external stylesheets, external schemas, etc. which, when included, allow similar external resource inclusion style attacks.

Attacks can include disclosing local files, which may contain sensitive data such as passwords or private user data.

Since the attack occurs relative to the application processing the XML document, an attacker may use this trusted application to pivot to other internal systems, possibly disclosing other internal content via http (s) requests or launching a CSRF attack to any unprotected internal services.

In some situations, an XML processor library that is vulnerable to client-side memory corruption issues may be exploited by dereferencing a malicious URI, possibly allowing arbitrary code execution under the application account. Other attacks can access local resources that may not stop returning data, possibly impacting application availability if too many threads or processes are not released.

XXE (CWE-611) coverage by Kiuwan

In Kiuwan, you can search rules covering XXE (CWE-611) filtering by

- Vulnerability Type = **Injection**, and/or
- CWE tag = **CWE:611**

Kiuwan incorporates the following rules for XXE (CWE-611) for the following languages.

To obtain detailed information on functionality, coverage, parameterization, remediation, example codes, etc., follow the same steps as described in SQL Injection.

Language	Rule code
C#	OPT.CSHARP.SEC.XMLEntityInjection
Java	OPT.JAVA.SEC_JAVA.XmlEntityInjectionRule
Javascript	OPT.JAVASCRIPT.XmlEntityInjection
Objective-C	OPT.OBJECTIVEC.XMLEntityInjection

PHP	**CUS.PHP.XmlEntityInjection**
	OPT.PHP.XmlEntityInjection
Python	**OPT.PYTHON.SECURITY.XmlEntityInjection**
Swift	**OPT.SWIFT.SECURITY.XMLEntityInjection**