CWE-643 : XPath Injection

This page will describe XPath injection in more detail.

Contents:

XPath Injection (CWE-643)

> **CWE-643** describes **XPath Injection** as follows:
>
> "The software uses external input to dynamically construct an **XPath expression** used to retrieve data from an XML database, but it does not neutralize or incorrectly neutralizes that input. This allows an attacker to control the structure of the query."

Similar to SQL Injection, XPath Injection attacks occur when a web site uses user-supplied information to construct an XPath query for XML data.

By sending intentionally malformed information into the web site, an attacker can find out how the XML data is structured, or access data that he may not normally have access to. He may even be able to elevate his privileges on the web site if the XML data is being used for authentication (such as an XML based user file).

> The net effect is that the attacker will have control over the information selected from the XML database and may use that ability to control application flow, modify logic, retrieve unauthorized data, or bypass important checks (e.g. authentication).

Querying XML is done with XPath, a type of simple descriptive statement that allows the XML query to locate a piece of information. Like SQL, you can specify certain attributes to find, and patterns to match. When using XML for a web site it is common to accept some form of input on the query string to identify the content to locate and display on the page.

This input must be sanitized to verify that it doesn't mess up the XPath query and return the wrong data.

XPath Injection (CWE-643) coverage by Kiuwan

> In Kiuwan, you can search rules covering XPath-Injection (CWE-643) filtering by
>
> - Vulnerability Type = **Injection,** and/or
> - CWE tag = **CWE:643**

Kiuwan incorporates the following rules for XPath-Injection (CWE-643) 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.XPathInjection
Java	OPT.JAVA.SEC_JAVA.XPathInjectionRule
Javascript	OPT.JAVASCRIPT.XPathInjection
Objective-C	OPT.OBJECTIVEC.XPathInjection
PHP	OPT.PHP.XPathInjection
Python	OPT.PYTHON.SECURITY.XpathInjection
Swift	OPT.SWIFT.SECURITY.XpathInjection