# CWE Detail – CWE-112

## Description

The product accepts XML from an untrusted source but does not validate the XML against the proper schema.

## Extended Description

Most successful attacks begin with a violation of the programmer's assumptions. By accepting an XML document without validating it against a DTD or XML schema, the programmer leaves a door open for attackers to provide unexpected, unreasonable, or malicious input.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Related Attack Patterns (CAPEC)

* CAPEC-230
* CAPEC-231

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Unexpected State — Notes:

## Potential Mitigations

**•** Architecture and Design: Always validate XML input against a known XML Schema or DTD. It is not possible for an XML parser to validate all aspects of a document's content because a parser cannot understand the complete semantics of the data. However, a parser can do a complete and thorough job of checking the document's structure and therefore guarantee to the code that processes the document that the content is well-formed. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)

## Demonstrative Examples

**•** The XML file is loaded without validating it against a known XML Schema or DTD.

**•** The DocumentBuilder object does not validate an XML document against a schema, making it possible to create an invalid XML document.