# CWE Detail – CWE-1336

## Description

The product uses a template engine to insert or process externally-influenced input, but it does not neutralize or incorrectly neutralizes special elements or syntax that can be interpreted as template expressions or other code directives when processed by the engine.

## Extended Description

Many web applications use template engines that allow developers to insert externally-influenced values into free text or messages in order to generate a full web page, document, message, etc. Such engines include Twig, Jinja2, Pug, Java Server Pages, FreeMarker, Velocity, ColdFusion, Smarty, and many others - including PHP itself. Some CMS (Content Management Systems) also use templates. Template engines often have their own custom command or expression language. If an attacker can influence input into a template before it is processed, then the attacker can invoke arbitrary expressions, i.e. perform injection attacks. For example, in some template languages, an attacker could inject the expression "{{7\*7}}" and determine if the output returns "49" instead. The syntax varies depending on the language. In some cases, XSS-style attacks can work, which can obscure the root cause if the developer does not closely investigate the root cause of the error. Template engines can be used on the server or client, so both "sides" could be affected by injection. The mechanisms of attack or the affected technologies might be different, but the mistake is fundamentally the same.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2024-34359: Chain: Python bindings for LLM
 library do not use a sandboxed environment when
 parsing a template and constructing a prompt,
 allowing jinja2 Server Side Template Injection and
 code execution - one variant of a "prompt
 injection" attack.

**•** CVE-2017-16783: server-side template injection in content management server

**•** CVE-2020-9437: authentication / identity management product has client-side template injection

**•** CVE-2020-12790: Server-Side Template Injection using a Twig template

**•** CVE-2021-21244: devops platform allows SSTI

**•** CVE-2020-4027: bypass of Server-Side Template Injection protection mechanism with macros in Velocity templates

**•** CVE-2020-26282: web browser proxy server allows Java EL expressions from Server-Side Template Injection

**•** CVE-2020-1961: SSTI involving mail templates and JEXL expressions

**•** CVE-2019-19999: product does not use a "safe" setting for a FreeMarker configuration, allowing SSTI

**•** CVE-2018-20465: product allows read of sensitive database username/password variables using server-side template injection

## Modes of Introduction

**•** Architecture and Design: The developer might choose a template engine that makes it easier for programmers to write vulnerable code.

**•** Implementation: The programmer might not use engine's built-in sandboxes or other capabilities to escape or otherwise prevent template injection from untrusted input.

## Common Consequences

**•** Impact: Execute Unauthorized Code or Commands — Notes:

## Potential Mitigations

**•** Architecture and Design: Choose a template engine that offers a sandbox or restricted mode, or at least limits the power of any available expressions, function calls, or commands. (Effectiveness: N/A)

**•** Implementation: Use the template engine's sandbox or restricted mode, if available. (Effectiveness: N/A)

## Applicable Platforms

**•** Java (Class: None, Prevalence: Undetermined)

**•** PHP (Class: None, Prevalence: Undetermined)

**•** Python (Class: None, Prevalence: Undetermined)

**•** JavaScript (Class: None, Prevalence: Undetermined)

**•** None (Class: Interpreted, Prevalence: Undetermined)

## Notes

**•** Relationship: Since expression languages are often used in templating languages, there may be some overlap with CWE-917 (Expression Language Injection). XSS (CWE-79) is also co-located with template injection.

**•** Maintenance: The interrelationships and differences between CWE-917 and CWE-1336 need to be further clarified.