# CWE Detail – CWE-917

## Description

The product constructs all or part of an expression language (EL) statement in a framework such as a Java Server Page (JSP) using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended EL statement before it is executed.

## Extended Description

Frameworks such as Java Server Page (JSP) allow a developer to insert executable expressions within otherwise-static content. When the developer is not aware of the executable nature of these expressions and/or does not disable them, then if an attacker can inject expressions, this could lead to code execution or other unexpected behaviors.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2021-44228: Product does not neutralize ${xyz} style expressions, allowing remote code execution. (log4shell vulnerability in log4j) (KEV)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Application Data — Notes:

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

## Potential Mitigations

**•** Architecture and Design: Avoid adding user-controlled data into an expression interpreter when possible. (Effectiveness: N/A)

**•** Implementation: If user-controlled data must be added to an expression interpreter, one or more of the following should be performed: Validate that the user input will not evaluate as an expression Encode the user input in a way that ensures it is not evaluated as an expression (Effectiveness: N/A)

**•** System Configuration: The framework or tooling might allow the developer to disable or deactivate the processing of EL expressions, such as setting the isELIgnored attribute for a JSP page to "true". (Effectiveness: N/A)

## Applicable Platforms

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

## Notes

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

**•** Relationship: In certain versions of Spring 3.0.5 and earlier, there was a vulnerability (CVE-2011-2730) in which Expression Language tags would be evaluated twice, which effectively exposed any application to EL injection. However, even for later versions, this weakness is still possible depending on configuration.