CWE-917 : Expression Language (EL) Injection

Expression Language (EL) Injection (CWE-917)

CWE-917 describes **Expression Language (EL) Injection** as follows:

> *“The software constructs all or part of an* ***expression language (EL) statement in 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.”*

Another interpreter suitable to be attacked by injection is Expression Language (EL) in JSPs. Expression Language (EL) Injection happens when attacker controlled data enters an EL interpreter.

In frameworks like *Spring MVC*, EL tags are evaluated twice (one by the application server and the result is evaluated as EL expression again by the Spring tag implementation), which allows an attacker to pass in the HTTP request message a value (header, cookie, message parameter) containing EL expression that could be executed.

Depending on the context, this may allow execution of arbitrary code, modification of unintended session or application attributes, or even downloading remote malicious Java classes with custom classloaders.

Other frameworks, like *Struts*, use a similar expression language (OGNL) that in certain cases allow double execution of OGNL.

EL Injection (CWE-917) coverage by Kiuwan

In Kiuwan, you can search rules covering EL Injection (CWE-917) filtering

- by Vulnerability Type (“Injection”) and/or
- by CWE tag (“CWE:917”).

Kiuwan incorporates the next rules for EL Injection (CWE-917) 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
JSP	OPT.JSP.SEC_JSP.ExpressionLanguageInjection