# CWE Detail – CWE-106

## Description

When an application does not use an input validation framework such as the Struts Validator, there is a greater risk of introducing weaknesses related to insufficient input validation.

## Extended Description

Unchecked input is the leading cause of vulnerabilities in J2EE applications. Unchecked input leads to cross-site scripting, process control, and SQL injection vulnerabilities, among others. Although J2EE applications are not generally susceptible to memory corruption attacks, if a J2EE application interfaces with native code that does not perform array bounds checking, an attacker may be able to use an input validation mistake in the J2EE application to launch a buffer overflow attack.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

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

## Potential Mitigations

**•** Architecture and Design: Use an input validation framework such as Struts. (Effectiveness: N/A)

**•** Architecture and Design: Use an input validation framework such as Struts. (Effectiveness: N/A)

**•** Implementation: Use the Struts Validator to validate all program input before it is processed by the application. Ensure that there are no holes in the configuration of the Struts Validator. Example uses of the validator include checking to ensure that: Phone number fields contain only valid characters in phone numbers Boolean values are only "T" or "F" Free-form strings are of a reasonable length and composition (Effectiveness: N/A)

**•** Implementation: Use the Struts Validator to validate all program input before it is processed by the application. Ensure that there are no holes in the configuration of the Struts Validator. Example uses of the validator include checking to ensure that: Phone number fields contain only valid characters in phone numbers Boolean values are only "T" or "F" Free-form strings are of a reasonable length and composition (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** However, the RegistrationForm class extends the Struts ActionForm class which does use the Struts validator plug-in to provide validator capabilities. In the following example, the RegistrationForm Java class extends the ValidatorForm and Struts configuration XML file, struts-config.xml, instructs the application to use the Struts validator plug-in.