# CWE Detail – CWE-105

## Description

The product has a form field that is not validated by a corresponding validation form, which can introduce other weaknesses related to insufficient input validation.

## Extended Description

Omitting validation for even a single input field may give attackers the leeway they need to compromise the product. 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: Some products use the same ActionForm for more than one purpose. In situations like this, some fields may go unused under some action mappings.

## Common Consequences

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

**•** Impact: Bypass Protection Mechanism — Notes: If unused fields are not validated, shared business logic in an action may allow attackers to bypass the validation checks that are performed for other uses of the form.

## Potential Mitigations

**•** Implementation: Validate all form fields. If a field is unused, it is still important to constrain it so that it is empty or undefined. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** The validator XML file, validator.xml, provides the validation for the form fields of the RegistrationForm.