# CWE Detail – CWE-1173

## Description

The product does not use, or incorrectly uses, an input validation framework that is provided by the source language or an independent library.

## Extended Description

Many modern coding languages provide developers with input validation frameworks to make the task of input validation easier and less error-prone. These frameworks will automatically check all input against specified criteria and direct execution to error handlers when invalid input is received. The improper use (i.e., an incorrect implementation or missing altogether) of these frameworks is not directly exploitable, but can lead to an exploitable condition if proper input validation is not performed later in the product. Not using provided input validation frameworks can also hurt the maintainability of code as future developers may not recognize the downstream input validation being used in the place of the validation framework.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Modes of Introduction

**•** Architecture and Design: This weakness may occur when software designers choose to not leverage input validation frameworks provided by the source language.

**•** Implementation: This weakness may occur when developers do not correctly use a provided input validation framework.

## Common Consequences

**•** Impact: Unexpected State — Notes: Unchecked input leads to cross-site scripting, process control, and SQL injection vulnerabilities, among others.

## Potential Mitigations

**•** Implementation: Properly use provided input validation frameworks. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)