# CWE Detail – CWE-75

## Description

The product does not adequately filter user-controlled input for special elements with control implications.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-81
* CAPEC-93

## Modes of Introduction

**•** Implementation: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Common Consequences

**•** Impact: Modify Application Data, Execute Unauthorized Code or Commands — Notes:

## Potential Mitigations

**•** Requirements: Programming languages and supporting technologies might be chosen which are not subject to these issues. (Effectiveness: N/A)

**•** Implementation: Utilize an appropriate mix of allowlist and denylist parsing to filter special element syntax from all input. (Effectiveness: N/A)

## Applicable Platforms

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