# CWE Detail – CWE-914

## Description

The product does not properly restrict reading from or writing to dynamically-identified variables.

## Extended Description

Many languages offer powerful features that allow the programmer to access arbitrary variables that are specified by an input string. While these features can offer significant flexibility and reduce development time, they can be extremely dangerous if attackers can modify unintended variables that have security implications.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2006-7135: extract issue enables file inclusion

**•** CVE-2006-7079: Chain: extract used for register\_globals compatibility layer, enables path traversal (CWE-22)

**•** CVE-2007-0649: extract() buried in include files makes post-disclosure analysis confusing; original report had seemed incorrect.

**•** CVE-2006-6661: extract() enables static code injection

**•** CVE-2006-2828: import\_request\_variables() buried in include files makes post-disclosure analysis confusing

**•** CVE-2009-0422: Chain: Dynamic variable evaluation allows resultant remote file inclusion and path traversal.

**•** CVE-2007-2431: Chain: dynamic variable evaluation in PHP program used to modify critical, unexpected $\_SERVER variable for resultant XSS.

**•** CVE-2006-4904: Chain: dynamic variable evaluation in PHP program used to conduct remote file inclusion.

**•** CVE-2006-4019: Dynamic variable evaluation in mail program allows reading and modifying attachments and preferences of other users.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Modify Application Data — Notes: An attacker could modify sensitive data or program variables.

**•** Impact: Execute Unauthorized Code or Commands — Notes:

**•** Impact: Varies by Context, Alter Execution Logic — Notes:

## Potential Mitigations

**•** Implementation: For any externally-influenced input, check the input against an allowlist of internal program variables that are allowed to be modified. (Effectiveness: N/A)

**•** Implementation: Refactor the code so that internal program variables do not need to be dynamically identified. (Effectiveness: N/A)

## Demonstrative Examples

**•** The call to extract() will overwrite the existing values of any variables defined previously, in this case $isAdmin. An attacker can send a POST request with an unexpected third value "isAdmin" equal to "true", thus gaining Admin privileges.