# CWE Detail – CWE-627

## Description

In a language where the user can influence the name of a variable at runtime, if the variable names are not controlled, an attacker can read or write to arbitrary variables, or access arbitrary functions.

## Extended Description

The resultant vulnerabilities depend on the behavior of the application, both at the crossover point and in any control/data flow that is reachable by the related variables or functions.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** 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, Execute Unauthorized Code or Commands — Notes: An attacker could gain unauthorized access to internal program variables and execute arbitrary code.

## Potential Mitigations

**•** Implementation: Refactor the code to avoid dynamic variable evaluation whenever possible. (Effectiveness: N/A)

**•** Implementation: Use only allowlists of acceptable variable or function names. (Effectiveness: N/A)

**•** Implementation: For function names, ensure that you are only calling functions that accept the proper number of arguments, to avoid unexpected null arguments. (Effectiveness: N/A)

## Applicable Platforms

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

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

## Notes

**•** Research Gap: Under-studied, probably under-reported. Few researchers look for this issue; most public reports are for PHP, although other languages are affected. This issue is likely to grow in PHP as developers begin to implement functionality in place of register\_globals.