# CWE Detail – CWE-621

## Description

The product uses external input to determine the names of variables into which information is extracted, without verifying that the names of the specified variables are valid. This could cause the program to overwrite unintended variables.

## Extended Description

For example, in PHP, extraction can be used to provide functionality similar to register\_globals, a dangerous functionality that is frequently disabled in production systems. Calling extract() or import\_request\_variables() without the proper arguments could allow arbitrary global variables to be overwritten, including superglobals. Similar functionality is possible in other interpreted languages, including custom languages.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

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

**•** CVE-2006-7079: Chain: PHP app uses extract for register\_globals compatibility layer (CWE-621), enabling 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

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

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

## Potential Mitigations

**•** Implementation: Use allowlists of variable names that can be extracted. (Effectiveness: N/A)

**•** Implementation: Consider refactoring your code to avoid extraction routines altogether. (Effectiveness: N/A)

**•** Implementation: In PHP, call extract() with options such as EXTR\_SKIP and EXTR\_PREFIX\_ALL; call import\_request\_variables() with a prefix argument. Note that these capabilities are not present in all PHP versions. (Effectiveness: N/A)

## Applicable Platforms

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

## 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.

## Notes

**•** Research Gap: Probably under-reported for PHP. Seems under-studied for other interpreted languages.