# CWE Detail – CWE-616

## Description

The PHP application uses an old method for processing uploaded files by referencing the four global variables that are set for each file (e.g. $varname, $varname\_size, $varname\_name, $varname\_type). These variables could be overwritten by attackers, causing the application to process unauthorized files.

## Extended Description

These global variables could be overwritten by POST requests, cookies, or other methods of populating or overwriting these variables. This could be used to read or process arbitrary files by providing values such as "/etc/passwd".

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2002-1460: Forum does not properly verify whether a file was uploaded or if the associated variables were set by POST, allowing remote attackers to read arbitrary files.

**•** CVE-2002-1759: Product doesn't check if the variables for an upload were set by uploading the file, or other methods such as $\_POST.

**•** CVE-2002-1710: Product does not distinguish uploaded file from other files.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Files or Directories, Modify Files or Directories — Notes:

## Potential Mitigations

**•** Architecture and Design: Use PHP 4 or later. (Effectiveness: N/A)

**•** Architecture and Design: If you must support older PHP versions, write your own version of is\_uploaded\_file() and run it against $HTTP\_POST\_FILES['userfile'])) (Effectiveness: N/A)

**•** Implementation: For later PHP versions, reference uploaded files using the $HTTP\_POST\_FILES or $\_FILES variables, and use is\_uploaded\_file() or move\_uploaded\_file() to ensure that you are dealing with an uploaded file. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** In the "four globals" method, PHP sets the following 4 global variables (where "varname" is application-dependent):

**•** \*\* note: 'userfile' is the field name from the web form; this can vary.