# CWE Detail – CWE-471

## Description

The product does not properly protect an assumed-immutable element from being modified by an attacker.

## Extended Description

This occurs when a particular input is critical enough to the functioning of the application that it should not be modifiable at all, but it is. Certain resources are often assumed to be immutable when they are not, such as hidden form fields in web applications, cookies, and reverse DNS lookups.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2002-1757: Relies on $PHP\_SELF variable for authentication.

**•** CVE-2005-1905: Gain privileges by modifying assumed-immutable code addresses that are accessed by a driver.

## Related Attack Patterns (CAPEC)

* CAPEC-384
* CAPEC-385
* CAPEC-386
* CAPEC-387
* CAPEC-388

## Modes of Introduction

**•** Implementation: N/A

**•** Architecture and Design: N/A

## Common Consequences

**•** Impact: Modify Application Data — Notes: Common data types that are attacked are environment variables, web application parameters, and HTTP headers.

**•** Impact: Unexpected State — Notes:

## Potential Mitigations

**•** Architecture and Design: When the data is stored or transmitted through untrusted sources that could modify the data, implement integrity checks to detect unauthorized modification, or store/transmit the data in a trusted location that is free from external influence. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A

## Notes

**•** Relationship: MAID issues can be primary to many other weaknesses, and they are a major factor in languages that provide easy access to internal program constructs, such as PHP's register\_globals and similar features. However, MAID issues can also be resultant from weaknesses that modify internal state; for example, a program might validate some data and store it in memory, but a buffer overflow could overwrite that validated data, leading to a change in program logic.

**•** Theoretical: There are many examples where the MUTABILITY property is a major factor in a vulnerability.