# CWE Detail – CWE-302

## Description

The authentication scheme or implementation uses key data elements that are assumed to be immutable, but can be controlled or modified by the attacker.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2002-0367: DebPloit (KEV)

**•** CVE-2004-0261: Web auth

**•** CVE-2002-1730: Authentication bypass by setting certain cookies to "true".

**•** CVE-2002-1734: Authentication bypass by setting certain cookies to "true".

**•** CVE-2002-2064: Admin access by setting a cookie.

**•** CVE-2002-2054: Gain privileges by setting cookie.

**•** CVE-2004-1611: Product trusts authentication information in cookie.

**•** CVE-2005-1708: Authentication bypass by setting admin-testing variable to true.

**•** CVE-2005-1787: Bypass auth and gain privileges by setting a variable.

## Related Attack Patterns (CAPEC)

* CAPEC-10
* CAPEC-13
* CAPEC-21
* CAPEC-274
* CAPEC-31
* CAPEC-39
* CAPEC-45
* CAPEC-77

## Attack TTPs

**•** T1574.007: Path Interception by PATH Environment Variable (Tactics: persistence, privilege-escalation, defense-evasion)

**•** T1539: Steal Web Session Cookie (Tactics: credential-access)

**•** T1574.006: Dynamic Linker Hijacking (Tactics: persistence, privilege-escalation, defense-evasion)

**•** T1528: Steal Application Access Token (Tactics: credential-access)

**•** T1562.003: Impair Command History Logging (Tactics: defense-evasion)

**•** T1134: Access Token Manipulation (Tactics: defense-evasion, privilege-escalation)

## Modes of Introduction

**•** Architecture and Design: COMMISSION: This weakness refers to an incorrect design related to an architectural security tactic.

**•** Implementation: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Architecture and Design: Implement proper protection for immutable data (e.g. environment variable, hidden form fields, etc.) (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** Modifying the value of a cookie on the client-side is trivial, but many developers assume that cookies are essentially immutable.