# CWE Detail – CWE-784

## Description

The product uses a protection mechanism that relies on the existence or values of a cookie, but it does not properly ensure that the cookie is valid for the associated user.

## Extended Description

Attackers can easily modify cookies, within the browser or by implementing the client-side code outside of the browser. Attackers can bypass protection mechanisms such as authorization and authentication by modifying the cookie to contain an expected value.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2009-1549: Attacker can bypass authentication by setting a cookie to a specific value.

**•** CVE-2009-1619: Attacker can bypass authentication and gain admin privileges by setting an "admin" cookie to 1.

**•** CVE-2009-0864: Content management system allows admin privileges by setting a "login" cookie to "OK."

**•** CVE-2008-5784: e-dating application allows admin privileges by setting the admin cookie to 1.

**•** CVE-2008-6291: Web-based email list manager allows attackers to gain admin privileges by setting a login cookie to "admin."

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism, Gain Privileges or Assume Identity — Notes: It is dangerous to use cookies to set a user's privileges. The cookie can be manipulated to claim a high level of authorization, or to claim that successful authentication has occurred.

## Potential Mitigations

**•** Architecture and Design: Avoid using cookie data for a security-related decision. (Effectiveness: N/A)

**•** Implementation: Perform thorough input validation (i.e.: server side validation) on the cookie data if you're going to use it for a security related decision. (Effectiveness: N/A)

**•** Architecture and Design: Add integrity checks to detect tampering. (Effectiveness: N/A)

**•** Architecture and Design: Protect critical cookies from replay attacks, since cross-site scripting or other attacks may allow attackers to steal a strongly-encrypted cookie that also passes integrity checks. This mitigation applies to cookies that should only be valid during a single transaction or session. By enforcing timeouts, you may limit the scope of an attack. As part of your integrity check, use an unpredictable, server-side value that is not exposed to the client. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A

**•** The programmer expects that the AuthenticateUser() check will always be applied, and the "authenticated" cookie will only be set when authentication succeeds. The programmer even diligently specifies a 2-hour expiration for the cookie.

**•** N/A

## Notes

**•** Maintenance: A new parent might need to be defined for this entry. This entry is specific to cookies, which reflects the significant number of vulnerabilities being reported for cookie-based authentication in CVE during 2008 and 2009. However, other types of inputs - such as parameters or headers - could also be used for similar authentication or authorization. Similar issues (under the Research view) include CWE-247 and CWE-472.