# CWE Detail – CWE-348

## Description

The product has two different sources of the same data or information, but it uses the source that has less support for verification, is less trusted, or is less resistant to attack.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2001-0860: Product uses IP address provided by a client, instead of obtaining it from the packet headers, allowing easier spoofing.

**•** CVE-2004-1950: Web product uses the IP address in the X-Forwarded-For HTTP header instead of a server variable that uses the connecting IP address, allowing filter bypass.

**•** CVE-2001-0908: Product logs IP address specified by the client instead of obtaining it from the packet headers, allowing information hiding.

**•** CVE-2006-1126: PHP application uses IP address from X-Forwarded-For HTTP header, instead of REMOTE\_ADDR.

## Related Attack Patterns (CAPEC)

* CAPEC-141
* CAPEC-142
* CAPEC-73
* CAPEC-76
* CAPEC-85

## Attack TTPs

**•** T1584.002: DNS Server (Tactics: resource-development)

**•** T1557.002: ARP Cache Poisoning (Tactics: credential-access, collection)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism, Gain Privileges or Assume Identity — Notes: An attacker could utilize the untrusted data source to bypass protection mechanisms and gain access to sensitive data.

## Applicable Platforms

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

## Demonstrative Examples

**•** The 'HTTP\_X\_FORWARDED\_FOR' header can be user controlled and so should never be trusted. An attacker can falsify the header to gain access to the page.