# CWE Detail – CWE-697

## Description

The product compares two entities in a security-relevant context, but the comparison is incorrect, which may lead to resultant weaknesses.

## Extended Description

This Pillar covers several possibilities: the comparison checks one factor incorrectly; the comparison should consider multiple factors, but it does not check at least one of those factors at all; the comparison checks the wrong factor.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2021-3116: Chain: Python-based HTTP Proxy server uses the wrong boolean operators (CWE-480) causing an incorrect comparison (CWE-697) that identifies an authN failure if all three conditions are met instead of only one, allowing bypass of the proxy authentication (CWE-1390)

**•** CVE-2020-15811: Chain: Proxy uses a substring search instead of parsing the Transfer-Encoding header (CWE-697), allowing request splitting (CWE-113) and cache poisoning

**•** CVE-2016-10003: Proxy performs incorrect comparison of request headers, leading to infoleak

## Related Attack Patterns (CAPEC)

* CAPEC-10
* CAPEC-120
* CAPEC-14
* CAPEC-15
* CAPEC-182
* CAPEC-24
* CAPEC-267
* CAPEC-3
* CAPEC-41
* CAPEC-43
* CAPEC-44
* CAPEC-45
* CAPEC-46
* CAPEC-47
* CAPEC-52
* CAPEC-53
* CAPEC-6
* CAPEC-64
* CAPEC-67
* CAPEC-7
* CAPEC-71
* CAPEC-73
* CAPEC-78
* CAPEC-79
* CAPEC-8
* CAPEC-80
* CAPEC-88
* CAPEC-9
* CAPEC-92

## Attack TTPs

**•** T1027: Obfuscated Files or Information (Tactics: defense-evasion)

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Varies by Context — Notes:

## Applicable Platforms

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

## Demonstrative Examples

**•** Here, the equals() method only checks the make and model of the Truck objects, but the year of manufacture is not included.

**•** In AuthenticateUser(), the strncmp() call uses the string length of an attacker-provided inPass parameter in order to determine how many characters to check in the password. So, if the attacker only provides a password of length 1, the check will only examine the first byte of the application's password before determining success.

## Notes

**•** Research Gap: Weaknesses related to this Pillar appear to be under-studied, especially with respect to classification schemes. Input from academic and other communities could help identify and resolve gaps or organizational difficulties within CWE.

**•** Maintenance: This entry likely has some relationships with case sensitivity (CWE-178), but case sensitivity is a factor in other types of weaknesses besides comparison. Also, in cryptography, certain attacks are possible when certain comparison operations do not take place in constant time, causing a timing-related information leak (CWE-208).