# CWE Detail – CWE-187

## Description

The product performs a comparison that only examines a portion of a factor before determining whether there is a match, such as a substring, leading to resultant weaknesses.

## Extended Description

For example, an attacker might succeed in authentication by providing a small password that matches the associated portion of the larger, correct password.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2014-6394: Product does not prevent access to restricted directories due to partial string comparison with a public directory

**•** CVE-2004-1012: Argument parser of an IMAP server treats a partial command "body[p" as if it is "body.peek", leading to index error and out-of-bounds corruption.

**•** CVE-2004-0765: Web browser only checks the hostname portion of a certificate when the hostname portion of the URI is not a fully qualified domain name (FQDN), which allows remote attackers to spoof trusted certificates.

**•** CVE-2002-1374: One-character password by attacker checks only against first character of real password.

**•** CVE-2000-0979: One-character password by attacker checks only against first character of real password.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Alter Execution Logic, Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Testing: Thoroughly test the comparison scheme before deploying code into production. Perform positive testing as well as negative testing. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** 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

**•** Relationship: This is conceptually similar to other weaknesses, such as insufficient verification and regular expression errors. It is primary to some weaknesses.