# CWE Detail – CWE-315

## Description

The product stores sensitive information in cleartext in a cookie.

## Extended Description

Attackers can use widely-available tools to view the cookie and read the sensitive information. Even if the information is encoded in a way that is not human-readable, certain techniques could determine which encoding is being used, then decode the information.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2002-1800: Admin password in cleartext in a cookie.

**•** CVE-2001-1537: Default configuration has cleartext usernames/passwords in cookie.

**•** CVE-2001-1536: Usernames/passwords in cleartext in cookies.

**•** CVE-2005-2160: Authentication information stored in cleartext in a cookie.

## Related Attack Patterns (CAPEC)

* CAPEC-31
* CAPEC-37
* CAPEC-39
* CAPEC-74

## Attack TTPs

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

**•** T1005: Data from Local System (Tactics: collection)

**•** T1552.004: Private Keys (Tactics: credential-access)

## Modes of Introduction

**•** Architecture and Design: OMISSION: This weakness is caused by missing a security tactic during the architecture and design phase.

## Common Consequences

**•** Impact: Read Application Data — Notes:

## Applicable Platforms

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

## Demonstrative Examples

**•** Because the account ID is in plaintext, the user's account information is exposed if their computer is compromised by an attacker.

## Notes

**•** Terminology: Different people use "cleartext" and "plaintext" to mean the same thing: the lack of encryption. However, within cryptography, these have more precise meanings. Plaintext is the information just before it is fed into a cryptographic algorithm, including already-encrypted text. Cleartext is any information that is unencrypted, although it might be in an encoded form that is not easily human-readable (such as base64 encoding).