# CWE Detail – CWE-525

## Description

The web application does not use an appropriate caching policy that specifies the extent to which each web page and associated form fields should be cached.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-37

## Attack TTPs

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

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

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Application Data — Notes: Browsers often store information in a client-side cache, which can leave behind sensitive information for other users to find and exploit, such as passwords or credit card numbers. The locations at most risk include public terminals, such as those in libraries and Internet cafes.

## Potential Mitigations

**•** Architecture and Design: Protect information stored in cache. (Effectiveness: N/A)

**•** Architecture and Design: Use a restrictive caching policy for forms and web pages that potentially contain sensitive information. (Effectiveness: N/A)

**•** Architecture and Design: Do not store unnecessarily sensitive information in the cache. (Effectiveness: N/A)

**•** Architecture and Design: Consider using encryption in the cache. (Effectiveness: N/A)