# CWE Detail – CWE-13

## Description

Storing a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource making them an easy target for attackers.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity — Notes:

## Potential Mitigations

**•** Implementation: Credentials stored in configuration files should be encrypted, Use standard APIs and industry accepted algorithms to encrypt the credentials stored in configuration files. (Effectiveness: N/A)

## Demonstrative Examples

**•** Username and password information should not be included in a configuration file or a properties file in plaintext as this will allow anyone who can read the file access to the resource. If possible, encrypt this information.