# CWE Detail – CWE-555

## Description

The J2EE application stores a plaintext password in a configuration file.

## Extended Description

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

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Architecture and Design: Do not hardwire passwords into your software. (Effectiveness: N/A)

**•** Architecture and Design: Use industry standard libraries to encrypt passwords before storage in configuration files. (Effectiveness: N/A)

## Demonstrative Examples

**•** N/A