# CWE Detail – CWE-520

## Description

Allowing a .NET application to run at potentially escalated levels of access to the underlying operating and file systems can be dangerous and result in various forms of attacks.

## Extended Description

.NET server applications can optionally execute using the identity of the user authenticated to the client. The intention of this functionality is to bypass authentication and access control checks within the .NET application code. Authentication is done by the underlying web server (Microsoft Internet Information Service IIS), which passes the authenticated token, or unauthenticated anonymous token, to the .NET application. Using the token to impersonate the client, the application then relies on the settings within the NTFS directories and files to control access. Impersonation enables the application, on the server running the .NET application, to both execute code and access resources in the context of the authenticated and authorized user.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

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

## Potential Mitigations

**•** Operation: Run the application with limited privilege to the underlying operating and file system. (Effectiveness: N/A)