# CWE Detail – CWE-11

## Description

Debugging messages help attackers learn about the system and plan a form of attack.

## Extended Description

ASP .NET applications can be configured to produce debug binaries. These binaries give detailed debugging messages and should not be used in production environments. Debug binaries are meant to be used in a development or testing environment and can pose a security risk if they are deployed to production.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Implementation: N/A

**•** Build and Compilation: N/A

## Common Consequences

**•** Impact: Read Application Data — Notes: Attackers can leverage the additional information they gain from debugging output to mount attacks targeted on the framework, database, or other resources used by the application.

## Potential Mitigations

**•** System Configuration: Avoid releasing debug binaries into the production environment. Change the debug mode to false when the application is deployed into production. (Effectiveness: N/A)

## Applicable Platforms

**•** ASP.NET (Class: None, Prevalence: Undetermined)

## Demonstrative Examples

**•** Change the debug mode to false when the application is deployed into production.