# CWE Detail – CWE-12

## Description

An ASP .NET application must enable custom error pages in order to prevent attackers from mining information from the framework's built-in responses.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: Read Application Data — Notes: Default error pages gives detailed information about the error that occurred, and should not be used in production environments. Attackers can leverage the additional information provided by a default error page to mount attacks targeted on the framework, database, or other resources used by the application.

## Potential Mitigations

**•** System Configuration: Handle exceptions appropriately in source code. ASP .NET applications should be configured to use custom error pages instead of the framework default page. (Effectiveness: N/A)

**•** Architecture and Design: Do not attempt to process an error or attempt to mask it. (Effectiveness: N/A)

**•** Implementation: Verify return values are correct and do not supply sensitive information about the system. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** In the following insecure ASP.NET application setting, custom error message mode is turned off. An ASP.NET error message with detailed stack trace and platform versions will be returned.