# CWE Detail – CWE-7

## Description

The default error page of a web application should not display sensitive information about the product.

## Extended Description

A Web application must define a default error page for 4xx errors (e.g. 404), 5xx (e.g. 500) errors and catch java.lang.Throwable exceptions to prevent attackers from mining information from the application container's built-in error response. When an attacker explores a web site looking for vulnerabilities, the amount of information that the site provides is crucial to the eventual success or failure of any attempted attacks.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Application Data — Notes: A stack trace might show the attacker a malformed SQL query string, the type of database being used, and the version of the application container. This information enables the attacker to target known vulnerabilities in these components.

## Potential Mitigations

**•** Implementation: Handle exceptions appropriately in source code. (Effectiveness: N/A)

**•** Implementation: Always define appropriate error pages. The application configuration should specify a default error page in order to guarantee that the application will never leak error messages to an attacker. Handling standard HTTP error codes is useful and user-friendly in addition to being a good security practice, and a good configuration will also define a last-chance error handler that catches any exception that could possibly be thrown by the application. (Effectiveness: N/A)

**•** Implementation: 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

**•** Java (Class: None, Prevalence: Undetermined)

## Demonstrative Examples

**•** N/A