# CWE Detail – CWE-382

## Description

A J2EE application uses System.exit(), which also shuts down its container.

## Extended Description

It is never a good idea for a web application to attempt to shut down the application container. Access to a function that can shut down the application is an avenue for Denial of Service (DoS) attacks.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## Modes of Introduction

**•** Implementation: A call to System.exit() is probably part of leftover debug code or code imported from a non-J2EE application.

## Common Consequences

**•** Impact: DoS: Crash, Exit, or Restart — Notes:

## Potential Mitigations

**•** Architecture and Design: The shutdown function should be a privileged function available only to a properly authorized administrative user (Effectiveness: N/A)

**•** Implementation: Web applications should not call methods that cause the virtual machine to exit, such as System.exit() (Effectiveness: N/A)

**•** Implementation: Web applications should also not throw any Throwables to the application server as this may adversely affect the container. (Effectiveness: N/A)

**•** Implementation: Non-web applications may have a main() method that contains a System.exit(), but generally should not call System.exit() from other locations in the code (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A