# CWE Detail – CWE-55

## Description

The product accepts path input in the form of single dot directory exploit ('/./') without appropriate validation, which can lead to ambiguous path resolution and allow an attacker to traverse the file system to unintended locations or access arbitrary files.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2000-0004: Server allows remote attackers to read source code for executable files by inserting a . (dot) into the URL.

**•** CVE-2002-0304: Server allows remote attackers to read password-protected files via a /./ in the HTTP request.

**•** CVE-1999-1083: Possibly (could be a cleansing error)

**•** CVE-2004-0815: "/./////etc" cleansed to ".///etc" then "/etc"

**•** CVE-2002-0112: Server allows remote attackers to view password protected files via /./ in the URL.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Files or Directories, Modify Files or Directories — Notes:

## Potential Mitigations

**•** Implementation: Inputs should be decoded and canonicalized to the application's current internal representation before being validated (CWE-180). Make sure that the application does not decode the same input twice (CWE-174). Such errors could be used to bypass allowlist validation schemes by introducing dangerous inputs after they have been checked. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)