# CWE Detail – CWE-430

## Description

The wrong "handler" is assigned to process an object.

## Extended Description

An example of deploying the wrong handler would be calling a servlet to reveal source code of a .JSP file, or automatically "determining" type of the object even if it is contradictory to an explicitly specified type.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2001-0004: Source code disclosure via manipulated file extension that causes parsing by wrong DLL.

**•** CVE-2002-0025: Web browser does not properly handle the Content-Type header field, causing a different application to process the document.

**•** CVE-2000-1052: Source code disclosure by directly invoking a servlet.

**•** CVE-2002-1742: Arbitrary Perl functions can be loaded by calling a non-existent function that activates a handler.

## Related Attack Patterns (CAPEC)

* CAPEC-11

## Attack TTPs

**•** T1036.006: Space after Filename (Tactics: defense-evasion)

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Varies by Context, Unexpected State — Notes:

## Potential Mitigations

**•** Architecture and Design: Perform a type check before interpreting an object. (Effectiveness: N/A)

**•** Architecture and Design: Reject any inconsistent types, such as a file with a .GIF extension that appears to consist of PHP code. (Effectiveness: N/A)

## Applicable Platforms

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