# CWE Detail – CWE-433

## Description

The product stores raw content or supporting code under the web document root with an extension that is not specifically handled by the server.

## Extended Description

If code is stored in a file with an extension such as ".inc" or ".pl", and the web server does not have a handler for that extension, then the server will likely send the contents of the file directly to the requester without the pre-processing that was expected. When that file contains sensitive information such as database credentials, this may allow the attacker to compromise the application or associated components.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2002-1886: ".inc" file stored under web document root and returned unparsed by the server

**•** CVE-2002-2065: ".inc" file stored under web document root and returned unparsed by the server

**•** CVE-2005-2029: ".inc" file stored under web document root and returned unparsed by the server

**•** CVE-2001-0330: direct request to .pl file leaves it unparsed

**•** CVE-2002-0614: .inc file

**•** CVE-2004-2353: unparsed config.conf file

**•** CVE-2007-3365: Chain: uppercase file extensions causes web server to return script source code instead of executing the script.

## Modes of Introduction

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: Read Application Data — Notes:

## Potential Mitigations

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

**•** Architecture and Design: Do not store sensitive information in files which may be misinterpreted. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** database.inc

## Notes

**•** Relationship: This overlaps direct requests (CWE-425), alternate path (CWE-424), permissions (CWE-275), and sensitive file under web root (CWE-219).