# CWE Detail – CWE-646

## Description

The product allows a file to be uploaded, but it relies on the file name or extension of the file to determine the appropriate behaviors. This could be used by attackers to cause the file to be misclassified and processed in a dangerous fashion.

## Extended Description

An application might use the file name or extension of a user-supplied file to determine the proper course of action, such as selecting the correct process to which control should be passed, deciding what data should be made available, or what resources should be allocated. If the attacker can cause the code to misclassify the supplied file, then the wrong action could occur. For example, an attacker could supply a file that ends in a ".php.gif" extension that appears to be a GIF image, but would be processed as PHP code. In extreme cases, code execution is possible, but the attacker could also cause exhaustion of resources, denial of service, exposure of debug or system data (including application source code), or being bound to a particular server side process. This weakness may be due to a vulnerability in any of the technologies used by the web and application servers, due to misconfiguration, or resultant from another flaw in the application itself.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## Related Attack Patterns (CAPEC)

* CAPEC-209

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: Read Application Data — Notes: An attacker may be able to read sensitive data.

**•** Impact: DoS: Crash, Exit, or Restart — Notes: An attacker may be able to cause a denial of service.

**•** Impact: Gain Privileges or Assume Identity — Notes: An attacker may be able to gain privileges.

## Potential Mitigations

**•** Architecture and Design: Make decisions on the server side based on file content and not on file name or extension. (Effectiveness: N/A)

## Applicable Platforms

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