# CWE Detail – CWE-698

## Description

The web application sends a redirect to another location, but instead of exiting, it executes additional code.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2013-1402: Execution-after-redirect allows access to application configuration details.

**•** CVE-2009-1936: chain: library file sends a redirect if it is directly requested but continues to execute, allowing remote file inclusion and path traversal.

**•** CVE-2007-2713: Remote attackers can obtain access to administrator functionality through EAR.

**•** CVE-2007-4932: Remote attackers can obtain access to administrator functionality through EAR.

**•** CVE-2007-5578: Bypass of authentication step through EAR.

**•** CVE-2007-2713: Chain: Execution after redirect triggers eval injection.

**•** CVE-2007-6652: chain: execution after redirect allows non-administrator to perform static code injection.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Alter Execution Logic, Execute Unauthorized Code or Commands — Notes: This weakness could affect the control flow of the application and allow execution of untrusted code.

## Demonstrative Examples

**•** This code redirects unauthorized users, but continues to execute code after calling http\_redirect(). This means even unauthorized users may be able to access the contents of the page or perform a DoS attack on the server being queried. Also, note that this code is vulnerable to an IP address spoofing attack (CWE-212).