# CWE Detail – CWE-644

## Description

The product does not neutralize or incorrectly neutralizes web scripting syntax in HTTP headers that can be used by web browser components that can process raw headers, such as Flash.

## Extended Description

An attacker may be able to conduct cross-site scripting and other attacks against users who have these components enabled. If a product does not neutralize user controlled data being placed in the header of an HTTP response coming from the server, the header may contain a script that will get executed in the client's browser context, potentially resulting in a cross site scripting vulnerability or possibly an HTTP response splitting attack. It is important to carefully control data that is being placed both in HTTP response header and in the HTTP response body to ensure that no scripting syntax is present, taking various encodings into account.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2006-3918: Web server does not remove the Expect header from an HTTP request when it is reflected back in an error message, allowing a Flash SWF file to perform XSS attacks.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Execute Unauthorized Code or Commands — Notes: Run arbitrary code.

**•** Impact: Read Application Data — Notes: Attackers may be able to obtain sensitive information.

## Potential Mitigations

**•** Architecture and Design: Perform output validation in order to filter/escape/encode unsafe data that is being passed from the server in an HTTP response header. (Effectiveness: N/A)

**•** Architecture and Design: Disable script execution functionality in the clients' browser. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A