# CWE Detail – CWE-93

## Description

The product uses CRLF (carriage return line feeds) as a special element, e.g. to separate lines or records, but it does not neutralize or incorrectly neutralizes CRLF sequences from inputs.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2002-1771: CRLF injection enables spam proxy (add mail headers) using email address or name.

**•** CVE-2002-1783: CRLF injection in API function arguments modify headers for outgoing requests.

**•** CVE-2004-1513: Spoofed entries in web server log file via carriage returns

**•** CVE-2006-4624: Chain: inject fake log entries with fake timestamps using CRLF injection

**•** CVE-2005-1951: Chain: Application accepts CRLF in an object ID, allowing HTTP response splitting.

**•** CVE-2004-1687: Chain: HTTP response splitting via CRLF in parameter related to URL.

## Related Attack Patterns (CAPEC)

* CAPEC-15
* CAPEC-81

## Modes of Introduction

**•** Implementation: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Common Consequences

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

## Potential Mitigations

**•** Implementation: Avoid using CRLF as a special sequence. (Effectiveness: N/A)

**•** Implementation: Appropriately filter or quote CRLF sequences in user-controlled input. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** Assuming a string consisting of standard alpha-numeric characters, such as "Jane Smith", is submitted in the request the HTTP response including this cookie might take the following form:

**•** N/A