# CWE Detail – CWE-615

## Description

While adding general comments is very useful, some programmers tend to leave important data, such as: filenames related to the web application, old links or links which were not meant to be browsed by users, old code fragments, etc.

## Extended Description

An attacker who finds these comments can map the application's structure and files, expose hidden parts of the site, and study the fragments of code to reverse engineer the application, which may help develop further attacks against the site.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2007-6197: Version numbers and internal hostnames leaked in HTML comments.

**•** CVE-2007-4072: CMS places full pathname of server in HTML comment.

**•** CVE-2009-2431: blog software leaks real username in HTML comment.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

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

## Potential Mitigations

**•** Distribution: Remove comments which have sensitive information about the design/implementation of the application. Some of the comments may be exposed to the user and affect the security posture of the application. (Effectiveness: N/A)

## Demonstrative Examples

**•** N/A