# CWE Detail – CWE-219

## Description

The product stores sensitive data under the web document root with insufficient access control, which might make it accessible to untrusted parties.

## Extended Description

Besides public-facing web pages and code, products may store sensitive data, code that is not directly invoked, or other files under the web document root of the web server. If the server is not configured or otherwise used to prevent direct access to those files, then attackers may obtain this sensitive data.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2005-1835: Data file under web root.

**•** CVE-2005-2217: Data file under web root.

**•** CVE-2002-1449: Username/password in data file under web root.

**•** CVE-2002-0943: Database file under web root.

**•** CVE-2005-1645: database file under web root.

## Modes of Introduction

**•** Operation: COMMISSION: This weakness refers to an incorrect design related to an architectural security tactic.

**•** Implementation: COMMISSION: This weakness refers to an incorrect design related to an architectural security tactic.

## Common Consequences

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

## Potential Mitigations

**•** Implementation: Avoid storing information under the web root directory. (Effectiveness: N/A)

**•** System Configuration: Access control permissions should be set to prevent reading/writing of sensitive files inside/outside of the web directory. (Effectiveness: N/A)

## Applicable Platforms

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