# CWE Detail – CWE-213

## Description

The product's intended functionality exposes information to certain actors in accordance with the developer's security policy, but this information is regarded as sensitive according to the intended security policies of other stakeholders such as the product's administrator, users, or others whose information is being processed.

## Extended Description

When handling information, the developer must consider whether the information is regarded as sensitive by different stakeholders, such as users or administrators. Each stakeholder effectively has its own intended security policy that the product is expected to uphold. When a developer does not treat that information as sensitive, this can introduce a vulnerability that violates the expectations of the product's users.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2002-1725: Script calls phpinfo()

**•** CVE-2004-0033: Script calls phpinfo()

**•** CVE-2003-1181: Script calls phpinfo()

**•** CVE-2004-1422: Script calls phpinfo()

**•** CVE-2004-1590: Script calls phpinfo()

**•** CVE-2003-1038: Product lists DLLs and full pathnames.

**•** CVE-2005-1205: Telnet protocol allows servers to obtain sensitive environment information from clients.

**•** CVE-2005-0488: Telnet protocol allows servers to obtain sensitive environment information from clients.

## Modes of Introduction

**•** Policy: This can occur when the product's policy does not account for all relevant stakeholders, or when the policies of other stakeholders are not interpreted properly.

**•** Requirements: This can occur when requirements do not explicitly account for all relevant stakeholders.

**•** Architecture and Design: Communications or data exchange frameworks may be chosen that exchange or provide access to more information than strictly needed.

**•** Implementation: This can occur when the developer does not properly track the flow of sensitive information and how it is exposed, e.g., via an API.

## Common Consequences

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

## Applicable Platforms

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

## Demonstrative Examples

**•** The code displays a user's credit card and social security numbers, even though they aren't absolutely necessary.

## Notes

**•** Maintenance: This entry is being considered for deprecation. It overlaps many other entries related to information exposures. It might not be essential to preserve this entry, since other key stakeholder policies are covered elsewhere, e.g. personal privacy leaks (CWE-359) and system-level exposures that are important to system administrators (CWE-497).

**•** Theoretical: In vulnerability theory terms, this covers cases in which the developer's Intended Policy allows the information to be made available, but the information might be in violation of a Universal Policy in which the product's administrator should have control over which information is considered sensitive and therefore should not be exposed.