# CWE Detail – CWE-359

## Description

The product does not properly prevent a person's private, personal information from being accessed by actors who either (1) are not explicitly authorized to access the information or (2) do not have the implicit consent of the person about whom the information is collected.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-464
* CAPEC-467
* CAPEC-498
* CAPEC-508

## Attack TTPs

**•** T1606.001: Web Cookies (Tactics: credential-access)

## Modes of Introduction

**•** Architecture and Design: OMISSION: This weakness is caused by missing a security tactic during the architecture and design phase.

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

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

## Potential Mitigations

**•** Requirements: Identify and consult all relevant regulations for personal privacy. An organization may be required to comply with certain federal and state regulations, depending on its location, the type of business it conducts, and the nature of any private data it handles. Regulations may include Safe Harbor Privacy Framework [REF-340], Gramm-Leach Bliley Act (GLBA) [REF-341], Health Insurance Portability and Accountability Act (HIPAA) [REF-342], General Data Protection Regulation (GDPR) [REF-1047], California Consumer Privacy Act (CCPA) [REF-1048], and others. (Effectiveness: N/A)

**•** Architecture and Design: Carefully evaluate how secure design may interfere with privacy, and vice versa. Security and privacy concerns often seem to compete with each other. From a security perspective, all important operations should be recorded so that any anomalous activity can later be identified. However, when private data is involved, this practice can in fact create risk. Although there are many ways in which private data can be handled unsafely, a common risk stems from misplaced trust. Programmers often trust the operating environment in which a program runs, and therefore believe that it is acceptable store private information on the file system, in the registry, or in other locally-controlled resources. However, even if access to certain resources is restricted, this does not guarantee that the individuals who do have access can be trusted. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** The code in the example above logs a plaintext password to the filesystem. Although many developers trust the filesystem as a safe storage location for data, it should not be trusted implicitly, particularly when privacy is a concern.

**•** First the application must declare that it requires the ACCESS\_FINE\_LOCATION permission in the application's manifest.xml:

**•** N/A

## Notes

**•** Maintenance: This entry overlaps many other entries that are not organized around the kind of sensitive information that is exposed. However, because privacy is treated with such importance due to regulations and other factors, and it may be useful for weakness-finding tools to highlight capabilities that detect personal private information instead of system information, it is not clear whether - and how - this entry should be deprecated.

**•** Other: There are many types of sensitive information that products must protect from attackers, including system data, communications, configuration, business secrets, intellectual property, and an individual's personal (private) information. Private personal information may include a password, phone number, geographic location, personal messages, credit card number, etc. Private information is important to consider whether the person is a user of the product, or part of a data set that is processed by the product. An exposure of private information does not necessarily prevent the product from working properly, and in fact the exposure might be intended by the developer, e.g. as part of data sharing with other organizations. However, the exposure of personal private information can still be undesirable or explicitly prohibited by law or regulation. Some types of private information include: Government identifiers, such as Social Security Numbers Contact information, such as home addresses and telephone numbers Geographic location - where the user is (or was) Employment history Financial data - such as credit card numbers, salary, bank accounts, and debts Pictures, video, or audio Behavioral patterns - such as web surfing history, when certain activities are performed, etc. Relationships (and types of relationships) with others - family, friends, contacts, etc. Communications - e-mail addresses, private messages, text messages, chat logs, etc. Health - medical conditions, insurance status, prescription records Account passwords and other credentials Some of this information may be characterized as PII (Personally Identifiable Information), Protected Health Information (PHI), etc. Categories of private information may overlap or vary based on the intended usage or the policies and practices of a particular industry. Sometimes data that is not labeled as private can have a privacy implication in a different context. For example, student identification numbers are usually not considered private because there is no explicit and publicly-available mapping to an individual student's personal information. However, if a school generates identification numbers based on student social security numbers, then the identification numbers should be considered private.