Top 10 Privacy Risks

Alpha Version 1.0

Website Application Vulnerabilities

1. Frequency: High  Impact: Very High

Vulnerability is a key problem in any system that gathers or operates on sensitive user data. Failure to properly design and implement an application, detect a problem or promptly apply a fix (patch) is likely to result in a privacy breach. This risk encompasses the OWASP Top 10 List of web application vulnerabilities and the risks resulting from them.

Operator-sided Data Leakage

2. Frequency: High  Impact: Very High

Failure to prevent the leakage of any information containing or related to user data, or the data itself, to any unauthorized party resulting in loss of data confidentiality. Introduced either due to intentional malicious breach or unintentional mistake e.g. caused by insufficient access management controls, insecure storage, duplication of data or a lack of awareness.

Insufficient Data Breach Response

3. Frequency: High  Impact: Very High

Not informing the affected persons (data subjects) about a possible breach or data leak, resulting either from intentional or unintentional events; failure to remedy the situation by fixing the cause, not attempting to limit the leaks.

Insufficient Deletion of Personal Data

4. Frequency: Very High  Impact: High

Failure to effectively and/or timely delete personal data after termination of the specified purpose of upon request.

The project is sponsored by msg:
www.msg-systems.com
Non-transparent Policies, Terms and Conditions

Not providing sufficient information to describing how data is processed, such as its collection, storage, and processing. Failure to make this information easy-accessible and understandable for non-lawyers.

Frequency: Very High
Impact: High

Collection of data not required for the primary purpose

Collecting descriptive, demographic or any other user-related data that are not needed for the purpose of the system. Applies also to data for which the user did not provide consent.

Frequency: Very High
Impact: High

Sharing of Data with Third Party

Providing user data to any third-party, without obtaining the user’s consent. Sharing results either due to transfer or exchanging for a monetary compensation or otherwise free to incorporate it in third-party resources included in the website like widgets, maps, social robotics buttons, analytics or web beak (e.g., beacons).

Frequency: High
Impact: High

Outdated personal data

The use of outdated, incorrect or legacy user data. Failure to update or correct the data.

Frequency: High
Impact: Very High

Missing or insufficient Session Expiration

Failure to effectively enforce session termination. May result in collection of additional user data without the user’s consent or awareness.

Frequency: Medium
Impact: Very High

Insecure Data Transfer

Failure to provide data transfers over encrypted and secured channels, excluding the possibility of data leakage. Failure of enforcing mechanism limiting the leak surface, e.g., allowing to enter any user data out of the mechanics of Web application operation.

Frequency: Medium
Impact: Very High

Source: https://www.exap.org/index.php/OWASP_Tip_10_Privacy_Risks#impact