OWASP Top 10 Privacy Risks

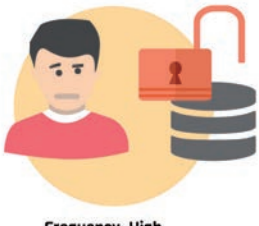
Alpha Version 1.0

#1 Website Application Vulnerabilities

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

Frequency: High
Impact: Very High

#2 Operator-sided Data Leakage



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.

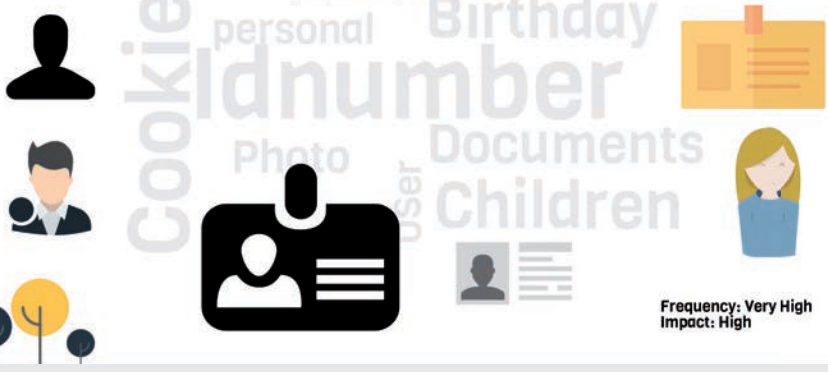
#3 Insufficient Data Breach Response

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.

Frequency: High
Impact: Very High

#4 Insufficient Deletion of Personal Data

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



Frequency: Very High
Impact: High

The project is sponsored by msg:
www.msg-systems.com

Non-transparent Policies, Terms and Conditions

#5

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

Frequency: Very High
Impact: High

#6

Collection of data not required for the primary purpose

Collecting descriptive, demographic or any other user-related data that are not needed for the purposes 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

#7

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 due to inappropriate use of third-party resources included in the web site like widgets (e.g. maps, social networks buttons), analytics or web bugs (e.g. beacons).

Frequency: High
Impact: High

#8

Outdated personal data

The use of outdated, incorrect or bogus user data.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

Frequency: High
Impact: Very High

Missing or insufficient Session Expiration

#9

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

#10

Insecure Data Transfer

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

Frequency: Medium
Impact: Very High

Source: https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project