P1 Web 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.

How to check?

- Are regular penetration tests performed with a focus on privacy?
- Are developers trained regarding web application security?
- Are secure coding guidelines applied?
- Is any of the used software out of date (server, database, frameworks, other infrastructure components)?

Countermeasures

- Perform a penetration test by trusted and approved independent (3rd party) cyber-security experts.
- Perform regular vulnerability and web privacy scans e.g. with automated tools (SAST, IAST, DAST).
- Track remediation of findings.
- Train application developers and architects in secure development.
- Apply procedures for secure development (e.g. Security Development Lifecycle - SDL) and DevSecOps
- Patch in compliance with existing standards (install updates, patches and hotfixes on a regular basis).

Example

- Injection Flaws allow attackers among others to copy or manipulate data by attacks like SQL injection.
- Sensitive Data Exposure allows attackers to gather sensitive information e.g. due to missing or weak encryption.
- Use of Insecure Direct Object References allows attackers to guess and access sensitive information, especially if access control is missing or weak.
- Usage of Components with Known Vulnerabilities, e.g. unpatched software flaws, and Security Misconfigurations, e.g. unhardened application platform.
- It is possible for attackers to gain access to, manipulate or delete personal data that the application is processing e.g. by abusing rights or entering malicious code.

References

- OWASP Top 10 Project
- OWASP ASVS
- Open SAMM
- OWASP Proactive Controls
- Security Development Lifecycle (SDL)
- OWASP Secure Application Design Project
- Lists of known vulnerabilities can be found at CVE and NVD
- ISMS of the German Federal Office for Information Security (BSI)

P2 Operator-sided Data Leakage	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.

How to check?
--- 	
• Research the reputation and reliability of the operator:
  ○ Have there been former breaches related to the operator?
  ○ Does the provider proactively prove privacy and security and if yes, how?
  ○ Is there a bug bounty program to report vulnerabilities?
  ○ Is the provider certified according to ISO/IEC 27001/2 or ISO/IEC 27017/18 (cloud providers) and ISO/IEC 27701 (privacy information management)?
  ○ Is the operator located in a country with high privacy standards?
• Audit the operator:
  ○ Are privacy best practices in place?
  ○ Is awareness training mandatory for all employees?
  ○ Is there a privacy engineering team?
  ○ How is personal data anonymized?
  ○ Is personal data encrypted?
  ○ Who has access to the data (need-to-know-principle) and encryption keys?
• Audit methods:
  ○ Paper-based audit (fair)
  ○ Interview-based audit (good)
  ○ On-site audit and system-checks (best)
	Countermeasures
	--- 	
	• Usage of proper Authentication, Authorization and Access Management (physical as well as logical) considering:
	  ○ Principle of least privilege
	  ○ Multi-Factor Authentication
	  ○ Privileged Account Management
	  ○ Avoidance of local accounts
	• Use strong encryption for all personal data stored (data at rest) especially on mobile media (e.g. USB memory sticks, laptop hard disks, tablet and phone local storage, backup tapes, portable hard disk drives).
	• Awareness training for all employees regarding handling of personal data.
	• Implementation of a data classification and information handling policy.
	• Monitor and detect classified data when it leaks from endpoints, web portals and cloud services (e.g. by DLP, SIEM).
	• Implement Privacy by Design
	• Anonymisation of personal data:
	It is common practice to anonymise personal data and use it for other purposes e.g. testing or marketing. Anonymisation is not easy (e.g. aol search data leak) and there are many anonymisation theories which can be very complex.
	• Use pseudonymisation which means that data can only be connected to a person with the help of a third party.

Example --- • Handbook for Safeguarding Sensitive PII • Article 29 Working Party on Anonymization	References --- • ISO 2700x, 27701 and 29100 series • IT-Grundschutz-Catalogues

P3 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.
How to check? General questions: ● Is an incident response plan for privacy incidents in place? ● Is this plan tested regularly (provide evidence e.g. a test protocol)? ● Do you have a Computer Emergency Response Team (CERT) and / or a Privacy Team? ● Do you have monitoring for incidents (e.g. SIEM) in place? If there was a privacy incident, did you: ● detect it (timeously)? ● notify relevant parties, including the individuals themselves, in a timely manner? ● protect evidence, remaining data during response / investigation? Is your incident response: ● Timely - information is disclosed to affected parties soon enough for them to avoid additional harm? ● Honest, accurate and understandable? Organizations that experience a privacy breach have a responsibility to clearly communicate the nature and scope of the breach to those affected. ● Established company wide for security breach notifications (policy)?	Countermeasures Countermeasures (in advance): ● Create and maintain an incident response plan and an incident team with relevant members from across the organization. ● Test incident response plan regularly (at minimum tabletop exercise bi-annually). ● Include privacy-related incidents in test. ● Establish a qualified Computer Emergency Response Team (CERT). ● Establish a Privacy Team. ● Continuously monitor for personal data leakage and loss. Responding to the breach: ● Validate the breach. ● Immediately assign / notify the incident manager responsible for investigation. ● Inform CERT and Privacy Team ● Assemble an incident response team ● Determine the scope and composition of the breach (e.g. legislation, confidentiality). ● Notify the data owners. ● Determine whether to notify the authorities (situation dependent). ● Decide how to investigate to ensure that the evidence is appropriately handled. ● Determine whether notification of affected individuals is needed and when and how. ● Collect and review any breach response documentation and analyze reports.
Example AICPA Privacy Incident Response Plan Template Data Breach Response Checklist (PTAC)	References Key Steps for Organizations in Responding to Privacy Breaches (Privacy Commissioner of Canada) Data Breach Notification Pattern - Privacy Patterns

P4 Consent on Everything	Aggregation or inappropriate use of consent to legitimate processing. Consent is "on everything" and not collected separately for each purpose (e.g. use of website and profiling for advertising). Note: “Problems with getting consent” has been merged with this topic. Non-transparent policies, terms & conditions (P5) support this issue.
How to check? ● Is consent aggregated or inappropriately used to legitimate processing? ● Are data flow restrictions rather than consent used? ● Is the default setting for consent “on” (opt-out) for those purposes not absolutely necessary for the service.	Countermeasures ● Collect consent separately for each purpose (e.g. use of website and profiling for advertising). ● Consent should be voluntarily
Example Personal data purchases from elsewhere are imported into the application where the provenance and consent is unknown or inadequately verifiable.	References ● Helen Nissenbaum on Post-Consent Privacy - YouTube ● https://hbr.org/2018/09/stop-thinking-about-consent-it-isnt-possible-and-it-isnt-right

P5 Non-transparent Policies, Terms and Conditions	Not providing sufficient information to describe how data is processed, such as its collection, storage, processing and deletion. Failure to make this information easily-accessible and understandable for non-lawyers.

How to check?

Check if policies, terms and conditions:

- Are easy to find
- Fully describe data processing:
  - Who are you / who is processing the data
  - Including data transfers
  - Analysis performed
  - Retention time
  - Metadata used
  - What are the rights
  - …
- Understandable for non-lawyers
- Complete, but KISS (Keep it short and simple)
- Include a process for obtaining user consent if the terms, policies or conditions change.
- Are available in the user's language
- Explain which data are collected
- Explain the purposes for which personal data is collected
- Use a readability score tester like https://readable.com/ to check whether a text is hard to read or not.
- Are privacy rules actively communicated or does the user have to take action

Countermeasures

- Terms & Conditions (T&Cs) should be specifically for the use and data processing of the website.
- They should be easy to understand for non-lawyers and not too long.
- Provide an easily readable summary of the terms and conditions as well as a long version.
- Pictograms can be used for visual aid.
- Use separate T&Cs for use and data processing.
- Use release notes to identify change history of T&Cs and policies/notices over time.
- Keep track of which users consented to which version and any other time at which they may opt in to newer versions.
- Deploy Do Not Track on the server side.
- When collecting information it should be clear why it is needed. You should also try to predict whether you will be likely to do other things with it in the future and tell the users if you have such plans.
- Provide a list of cookies, widgets etc. used with an explanation of the use e.g. sharing data or advertising.
- Provide an opt-out-button for the users.

Example

- Easily readable summaries:
  - http://www.avg.com/privacy
  - 500px.com
- Explanation of cookies, widgets etc. including an opt-out-button if existing:
  - http://www.kaspersky.com/third-party-tracking

References

- Guidance on writing a privacy notice | Data Protection - UCL – University College London
- HTTPA (HTTP with Accountability)
- Appropriate Privacy Icons - Privacy Patterns
- Paper: The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services

P6 Insufficient Deletion of Personal Data	Failure to effectively and / or timeously delete personal data after termination of the specified purpose or upon request.
How to check? ● Inspect the data retention / deletion policies and/or agreements. ● Evaluate their appropriateness. ● Request deletion protocols. ● Test processes for deletion requests. ● Check if transparency is provided (which data is deleted when and which data is not deleted and why).	Countermeasures ● Establish a data deletion concept. Data retention, archival and deletion policies and processes have to be implemented and documented. ● Personal data has to be deleted after termination of the specified purpose and after an appropriate time frame (e.g. one month). ● Personal data has to be deleted on rightful user request. ● Secure locking (with very limited access to the data) might be an option if deletion is not possible due to technical restrictions. ● Real deletion is preferable though and minimizes the risk. ● Evidence should be collected to verify the deletion as per policy. ● Any data in backups, other copies or shared with third parties has to be considered. ● Exceptions are possible in case of retention required by law. Access should be very limited and protocolled for this case. ● For cloud services also consider degaussing / cryptographic wiping of archived and backed-up data. ● Deletion of user profiles after longer periods of inactivity. ● Deploy systems with good privacy practices, in this case minimization.
Example Customer data is deleted automatically after a certain period of inactivity (Hotmail removes user profiles in case they are not used for one year) or after termination of contract (it is not required by law to keep all customer information for accounting or other purposes).	References ● How to write a GDPR data retention policy – free template (itgovernance.co.uk) ● German Standard DIN 66398 on retention and deletion of personal data

P7 Insufficient Data Quality	The use of outdated, incorrect or bogus user data. Failure to update or correct the data. Incorrect data can be a result of ambiguous instructions during data collection (e.g., imprecise form fields), technical errors (e.g., saving process, login process), or incorrect data linking (e.g., cookie errors, or during the inclusion of a contact list or social network account).
How to check? ● Ask the operator how it is ensured that personal data is up-to-date. ● Check for possibilities to update personal data in the application. ● Are there regular checks to validate that data is up-to-date (e.g. “please verify your shipping address”)? ● Question how long it is likely that data is up to date and how often it usually changes.	Countermeasures ● Put a procedure in place to validate user data ● Implement a procedure to update the user’s personal data by obtaining inputs from them after a certain time period. ● The user should approve data if he or she is triggering a “critical” action. ● Provide a form to enable users to update their data. ● In case of an update make sure to forward the information to any third parties / subsystems that received the user’s data before (if there are any). ● Consistency checks help against typographical and copy & paste errors.
Example An update form is provided on the website so that the user can update his or her data when needed. A leading webshop is asking whether your address and account data is correct before you can finish your order (CRM clearing).	References UK ICO on keeping personal data up to date Art. 16 GDPR - Right to rectification

P8 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.
How to check? • Is the logout button easy to find and promoted? • Is there an automatic session timeout < 1 week (for critical applications < 1 day). • Are session timeout lengths appropriate to the length required to complete a transaction (long enough) but also to the sensitivity of the data that the session accesses (shorter for higher sensitivity)? • A single service can support several combinations of session sensitivity and length. Each such available session type should be evaluated.	Countermeasures • Automatic session expiration should be set. Expiration time could differ widely depending on the criticality of the application and data. • Session timeout should be no longer than a week and much shorter for critical use cases. A best practice for medium criticality (e.g. webmailer, web shop, social network) is one day as default setting. • Session timeout should be configurable by the user according to his or her needs. • If a user has not used the logout-button to finish his session the last time, the user should see a reminder message at next login. • If the user is unable to logout, or the logout does not terminate the session completely, data may continue to be collected (e.g. tracking sites the user visits elsewhere).
Example When a user forgets to logout from web.de (German mail provider) a popup tells the users at next login that logging out is important for security reasons. Facebook does not implement automatic session expiration. The user has to logout manually. In case the user does not actively log out and someone else uses the device he or she can access or manipulate the user's profile. Amazon implements security without logout button by partitioning the content into different sensitivity levels, and tracking the x-main and session-id cookies. Amazon ensures that only the authenticated user can access personal details, but provides personalized content to a returning user without login.	References OWASP Session Management Cheat Sheet Carnegie Mellon Guidelines for Data Protection recommends automatic session timeout besides other controls

P9 Inability of users to access and modify data	Users do not have the ability to access, change or delete data related to them.
How to check? ● Is there a possibility to view own data ● Is there a possibility to request updates, or change data? ● Are updates forwarded and considered by relevant third parties?	Countermeasures ● Allow to directly access, modify and delete data via the user account ● If this is not fully possible, provide other means to access, modify and delete user data e.g. via form or email request ● Perform user requests in a timely manner and consider third parties ● Track user requests ● For further countermeasures see also P7
Example Information degrades over time leading to inaccuracies that might adversely affect an individual.	References CNIL Developer's Guide Sheet n°13: Prepare for the exercise of people's rights

P10 Collection of data not required for the user-consented 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.
How to check? ● List personal data collected by the application. ● Request description of purpose. ● Check if collected data is required to fulfill the purpose. ● If data is collected that is not required for the primary purpose(s), check if consent to collect and process this data was given and is documented. ● Are individuals notified and asked if purpose or processing is changed? ● Are regular compliance checks regarding the collection of personal data and user consent in place?	Countermeasures ● Define the purpose of the collection of personal data. ● Only collect personal data required to fulfill the purpose. ● Default is to collect as little data as possible unless the user chooses otherwise (data reduction / minimization). ● Provide the data subject the option to provide additional data voluntarily to improve the service (e.g. product recommendation, personalized advertisement) with possibility to opt-out. ● The purpose for collection of personal data collected is specified no later than at the time of data collection. ● Conditioned collection: Collect personal data only if they are really required for a used feature.
Example Positive: ● A webshop collects Email addresses to send an order confirmation to the buyer. This email address is not used to send news about products (another purpose) unless the user actively chooses this option (opt-in). Negative: ● A leading webshop provides personalized advertisement to its users. This can be disabled, but the default setting is on. From a privacy point of view it should be disabled by default and the user should opt-in to receive personalized product recommendations.	References Purpose limitation under the GDPR: can Article 6(4) be automated? Privacy Design Strategies: ● M. Colesky, J.-H. Hoepman, and C. Hillen. **A Critical Analysis of Privacy Design Strategies**. In *2016 International Workshop on Privacy Engineering – IWPE'16*, San Jose, CA, USA, May 26 2016. (to appear). ● J.-H. Hoepman. **Privacy Design Strategies**. In *IFIP TC11 29th Int. Conf. on Information Security (IFIP SEC 2014)*, pages 446-459, June 2-4 2014.

Generic countermeasures

Some countermeasure and privacy best practices do not only address a single risk. The following countermeasures apply to “all of the above”:

- Privacy Impact Assessment as part of change control processes
- Privacy threat assessment e.g. Linddun privacy threat analysis framework
- Undertake a privacy risk assessment of all current application portfolio
- Define privacy requirements early in projects
- Review privacy throughout process development
- Privacy awareness training (managers, staff, volunteers, contractors)
- Organizational Privacy Policy
- Instrument processes to automatically detect that privacy requirements are in place
- Track changes to legislation, guidance and any privacy-related clauses in other mandates such as contracts
- Ask local DPA to audit you
- Map (or create a process flow for) the data in order to understand what is collected, why it is needed, how it is used, and what protections are in place
- Use anonymization, pseudonymization and data minimisation/avoidance where possible
- Implement metrics to measure privacy performance in applications/data
- Specifically for GDPR: CNIL GDPR Developers Guide