Data Masking for Logging Systems

Double Good Technologies, LP

January 2024

Contents

1 Purpose: **2**

2 Scope: **2**

3 Key Objectives: **2**
3.1 Current Logging State: 2
3.2 PII (Personally Identifiable Information) and Sensitive Fields: . . 2
3.3 Priority of Masking PII/Sensitive Data: 3
3.4 Recommended Technical Solutions: 3

4 Responsibilities: **3**

5 Training and Awareness: **3**

6 Enforcement: **4**

7 Compliance **4**

8 Revision **4**

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC7.2

Table 2: Document history

Date	Comment
Jan 4 2024	Initial document

Security Policy: Data Masking for Logging Systems

1 Purpose:

The purpose of this security policy is to establish guidelines and practices for implementing data masking in various logging systems across web and mobile applications. The policy aims to mitigate the risk of exposing sensitive user information in logs while maintaining effective logging capabilities.

2 Scope:

This policy applies to all development and operations teams involved in the implementation and maintenance of logging systems for both web and mobile applications.

3 Key Objectives:

Implement robust data masking techniques to safeguard sensitive user information within logs. Ensure that logging in various systems continues to be effective for debugging purposes without compromising user data privacy. Adhere to recommended technical solutions and best practices for data masking, aligning with industry standards. # Key Practices:

3.1 Current Logging State:

Regularly assess and review the criticality of the current logging state. Ensure that all necessary information is being tracked for effective issue resolution and debugging.

3.2 PII (Personally Identifiable Information) and Sensitive Fields:

Maintain an updated and well-documented list of Personally Identifiable Information (PII) and sensitive fields. Regularly review and update the list as applications evolve. Examples of PII Fields:

- Name
- Surname
- Patronymic
- Date of birth
- Email address
- Phone number
  - **Exception**: Not masked unless required by law or regulation
- Address

- Government-Issued Documents:
  - Passport numbers
  - Social security numbers
  - etc

Examples of Sensitive Fields:

- **Third-party Identifiers.** Examples: Social media user IDs, bank account numbers, credit card numbers, etc.
- **Medical Information.** Examples: Diagnoses, test results, medical history, etc.
- **Financial Information.** Examples: Transaction amounts, account balances, etc.
- **Client Information.** Examples: Names, addresses, phone numbers, etc.
- **Confidential Information.** Examples: Passwords, API keys, etc.

3.3 Priority of Masking PII/Sensitive Data:

Establish a clear prioritization framework for masking user PII/sensitive data based on severity. Ensure that high-priority data is always fully masked, while allowing for limited masking of lower-priority data for specific debugging needs.

3.4 Recommended Technical Solutions:

Adhere to recommended technical solutions for data masking, aligning with industry best practices. Regularly review documentation for updates and new recommendations. Implement and maintain these solutions consistently across all relevant logging systems. Specific Examples of How to Implement Recommended Technical Solutions:

Redaction: Replace sensitive data with a placeholder, such as "****". Anonymization: Replace sensitive data with a random or pseudorandom value. Pseudonymization: Replace sensitive data with a unique identifier that does not reveal the identity of the user.

4 Responsibilities:

Development and operations teams are collectively responsible for implementing and maintaining data masking practices as per this policy. Security teams are responsible for conducting periodic reviews to ensure compliance with the policy.

5 Training and Awareness:

Conduct training sessions for development and operations teams to raise awareness about the importance of data masking and its impact on user data privacy.

Ensure that team members are familiar with the guidelines outlined in this policy.

6 Enforcement:

Non-compliance with data masking practices outlined in this policy may result in corrective actions, including but not limited to code reviews, retraining, and, if necessary, escalation to higher management.

7 Compliance

Non-compliance with this policy may result in corrective action, as per the organization's policies and procedures.

8 Revision

This policy will be reviewed periodically and updated to reflect changing training needs and best practices in professional development.