BabiEat Secure Authentication Report

Prepared by: Marie Claude Hayfa

Internship Role: Cybersecurity Intern

Advisor: Ibrahim Fleifel

Company: BabiEat

Date: February 26, 2025

1. Introduction

This report outlines best practices for secure authentication at BabiEat, focusing on token management, safeguarding user and payment data, and API security.
The goal is to:
- Enhance application security
- Protect sensitive information
- Build and maintain user trust

2. Secure Authentication

- Strong Password Policies: Enforce minimum length, complexity, and apply rate limiting.
- Multi-Factor Authentication (MFA): Add extra layers of protection via SMS, email codes, or authenticator apps.
- Account Lockout Mechanisms: Temporarily lock accounts after multiple failed attempts to prevent brute-force attacks.

3. Token Management

Definition: Token management ensures the secure creation, storage, usage, and revocation of authentication tokens that control access to APIs and systems.

Best Practices:
- Session Tokens / JWTs: Use random, secure tokens for user sessions; store them in HttpOnly cookies or secure storage.
- Expiration & Rotation: Set expiration times and rotate tokens after sensitive actions (e.g., password changes).
- Revocation: Allow tokens to be invalidated if a device is lost or compromised.

Example for BabiEat: Implement OAuth 2.0 with JWT (JSON Web Tokens) for customer login and API authentication.

4. Safeguarding User and Payment Data

User credentials, delivery addresses, and payment details are sensitive assets. Breaches could result in fraud, financial loss, or damaged trust.

Techniques:
- Encryption: Encrypt all sensitive data (AES for storage, TLS 1.3 for transmission).
- Tokenization: Replace credit card numbers with secure tokens (PCI-DSS compliance).
- Access Control: Restrict database access using role-based permissions (RBAC).
- Monitoring: Detect unusual patterns, such as repeated failed payment attempts.

Example for BabiEat: Use trusted payment gateways (e.g., Stripe or PayPal) with built-in fraud detection and tokenization.

5. API Security Best Practices

BabiEat uses APIs to connect restaurants, drivers, and customers. APIs are high-value targets for attackers.

Best Practices:
- Enforce strong authentication (OAuth 2.0 / OpenID Connect)
- Always use HTTPS (TLS 1.3)
- Apply rate limiting to prevent brute-force/DDoS attacks
- Validate inputs to prevent SQL injection or XSS attacks
- Use an API Gateway to centralize security policies
- Log and monitor API traffic for anomalies

Example for BabiEat: Deploy an API Gateway (e.g., AWS API Gateway, Kong) for centralized authentication and monitoring.

6. Conclusion

By adopting strong authentication policies, effective token management, secure handling of user/payment data, and robust API security measures, BabiEat can:
- Protect sensitive customer and business data
- Maintain system integrity
- Increase resilience against cyber threats
- Strengthen user trust and brand reputation