## **PASTA Threat Model Analysis for Sneaker Company Mobile App**

|  |  |
| --- | --- |
| **Stages** | **Sneaker company** |
| **I. Define business and security objectives** | Make 2-3 notes of specific business requirements that will be analyzed.   * *Users can create member profiles internally or by connecting external accounts.* * *The app must process financial transactions.* * *The app should be in compliance with PCI-DSS.*   The business objectives for the new mobile app include enabling users to create member profiles either directly or through external accounts, processing financial transactions, and ensuring compliance with PCI-DSS (Payment Card Industry Data Security Standard) and GDPR (General Data Protection Regulation) standards. Security objectives focus on implementing robust authentication for all user accounts, safeguarding financial transactions, and maintaining adherence to PCI-DSS to protect sensitive payment information and the GDPR regulations to ensure customer trust. |
| **II. Define the technical scope** | List oftechnologies used by the application:   * Application programming interface (API) * Public key infrastructure (PKI) * Advanced encryption system (AES) * SHA-256 * SQL   APIs are crucial for data exchange between customers, partners, and employees, and thus should be given priority. They handle significant amounts of sensitive data while connecting various users and systems. However, it's important to identify which specific APIs are being used before prioritizing one technology over another. Due to their extensive use and wide attack surface, APIs are more vulnerable to security vulnerabilities. |
| **III. Decompose application** | D[ata flow diagram](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview) |
| **IV. Threat analysis** | * Injection * Session hijacking |
| **V. Vulnerability analysis** | * *Absence of prepared statements* * *Compromised or broken API token* |
| **VI. Attack modeling** | [A](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?usp=sharing&resourcekey=0-zYPY7AhPJdcClXamlAfOag)ttack Modeling Tree |
| **VII. Risk analysis and impact** | - Implement SHA-256 for secure hashing  - Establish comprehensive incident response procedures  - Enforce a robust password policy  - Apply managerial controls  - Adhere to the principle of least privilege |