## PASTA worksheet

|  |  |
| --- | --- |
| **Stages** | **Sneaker company** |
| **I. Define business and security objectives** | * Ensure secure user authentication for member profiles (internal/external account linking). * Guarantee PCI-DSS compliance for financial transaction processing. * Protect customer data integrity and confidentiality during storage and transmission. |
| **II. Define the technical scope** | * **Technologies**: APIs (for data exchange), PKI (certificate management), AES (data encryption), SHA-256 (hashing), SQL (database). * **Prioritization**: APIs are critical due to their role in connecting systems and handling sensitive data (e.g., payment details). However, their broad attack surface (e.g., unsecured endpoints) requires strict input validation and rate limiting. |
| **III. Decompose application** | [Sample data flow diagram](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview) |
| **IV. Threat analysis** | * **Injection** (e.g., SQLi via unfiltered user inputs). * **Session Hijacking** (e.g., stolen cookies to impersonate users). |
| **V. Vulnerability analysis** | * **Lack of Prepared Statements**: Exposes SQL databases to injection. * **Broken API Tokens**: Allows unauthorized access to sensitive endpoints. |
| **VI. Attack modeling** | [Sample attack tree diagram](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?usp=sharing&resourcekey=0-zYPY7AhPJdcClXamlAfOag) |
| **VII. Risk analysis and impact** | 1. **SHA-256**: Securely hash stored passwords and sensitive data. 2. **Incident Response Procedures**: Rapid containment of breaches (e.g., API token revocation). 3. **Password Policy**: Enforce complexity and MFA to prevent credential stuffing. 4. **Principle of Least Privilege**: Limit database/user access to minimize attack impact. |