## PASTA worksheet

|  |  |
| --- | --- |
| **Stages** | **Sneaker company** |
| **I. Define business and security objectives** | * Users should be able to create profiles by either signing in or connecting their linked accounts. * It must be capable of making financial transactions. * Information must be kept private and secure in compliant with PCI-DSS. |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *API* * *PKI* * *AES* * *SHA-256* * *SQL*   *Since transactions and data exchange between customers, partners and employees are the most important parts, API must be prioritized. Yet, API should be picked considering there will be sensitive information transmitted and received. An insecure API would enlarge the attack surface.* |
| **III. Decompose application** | [Sample data flow diagram](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview?resourcekey=0-DZAkf7Vzh2PXsP-j3oXV-g) |
| **IV. Threat analysis** | * *SQL Injection* * *Session Hijacking* |
| **V. Vulnerability analysis** | * *Not using prepared statements for SQL queries.* * *Mishandled cookies can make session hijacking possible.* |
| **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** | * SHA-256 * Implementing Incident response procedures * Implementing a Password Policy * Applying principle of least privilege |