## PASTA worksheet

| **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 comply with PCI-DSS.*** |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *Application programming interface (API)* * *Public key infrastructure (PKI)* * *SHA-256* * *SQL*   *APIs facilitate the exchange of data between customers, partners, and employees, so they should be prioritized. They handle a lot of sensitive data while connecting various users and systems. However, details such as which APIs are being used should be considered before prioritizing one technology over another. APIs can be more prone to security vulnerabilities because there’s a larger 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** | List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application.   * *Injection* * *Session hijacking* |
| **V. Vulnerability analysis** | List **2 vulnerabilities** in the PASTA worksheet that could be exploited.   * *Lack of prepared statements* * *Broken API token* |
| **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** | List **4 security controls** that can reduce risk.  ***SHA-256*** *for hashing sensitive data such as passwords to ensure data integrity.*  ***Incident response procedures*** *to quickly identify and mitigate security incidents.*  ***Password policy*** *to enforce strong password creation and management practices.*  ***Principle of least privilege*** *to ensure users and systems have the minimum level of access necessary.* |