## PASTA worksheet

|  |  |
| --- | --- |
| **Stages** | **Sneaker company** |
| **I. Define business and security objectives** | asking broad questions about the purpose of the application.  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.* |
| **II. Define the technical scope** | understand the attack surface by identifying the technologies being used by the application and understanding their dependencies.  List oftechnologies used by the application:   * *Application programming interface (API)* * *Public key infrastructure (PKI)* * *Advanced encryption system (AES)* * *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 they connect various users and systems together. However, details such as which APIs are being used should be considered before prioritizing one technology over another. So, they can be more prone to security vulnerabilities because there’s a larger attack surface.* |
| **III. Decompose application** | builds upon the previous stage by investigating how the application's components communicate together. The objective here is to review how the application works and how security controls are currently implemented.  [Sample data flow diagram](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview) |
| **IV. Threat analysis** | consider the types of threats that might affect your application. This relates to the technologies you've already scoped. Another thing to consider is the types of data your application will be processing.  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** | associating asset vulnerabilities with potential threats. The objective here is to identify what is wrong with the design of the app or its codebase based on your security testing.  List **2 vulnerabilities** in the PASTA worksheet that could be exploited.   * *Lack of prepared statements* * *Broken API token* |
| **VI. Attack modeling** | threats and vulnerabilities identified in the previous steps using attack trees. The purpose of using attack trees here is to show that the potential threats that you've identified are actually viable.  Resources like MITRE ATT&CK and the CVE® list are useful references to find evidence that validates the information that you've modeled in your attack tree.  [Sample attack tree diagram](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?usp=sharing&resourcekey=0-zYPY7AhPJdcClXamlAfOag) |
| **VII. Risk analysis and impact** | identify ways to mitigate the risks that were identified from stages IV - VI and plan for any remaining risks that can't be remediated.  List **4 security controls** that can reduce risk.  *SHA-256, incident response procedures, password policy, principle of least privilege* |