## PASTA worksheet

|  |  |
| --- | --- |
| **Stages** | **Sneaker company** |
| **I. Define business and security objectives** | Make **2-3 notes** of specific business requirements that will be analyzed.   * *Will the app process transactions?* * *Does it do a lot of back-end processing?* * *Are there industry regulations that need to be considered?*   *This Finance app is developed for simple and seamlessly connects sellers and buyers (Traders). Where the sellers can buy cryptocurrencies by their accounts by using login credentials and others.*  *The process of the transaction seamlessly throws a big security concern.*  *Yes, this app is doing a lot of back-end processes. In this app, users just interact with the application interface and choose the sneakers they want to buy further listing the available items and processing transactions and many other functions are performed by the back-end.*  *Industries need to focus on securing the PII of users because they use their accounts for purchasing the company products so, the company needs to focus on security threats and conduct threat modeling techniques to find out proactive vulnerabilities which cause risk to user personal data.* |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *Application programming interface (API)* * *Public key infrastructure (PKI)* * *SHA-256* * *SQL*   Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others.  The technologies that are mentioned above are the best suited for this application.  An API is a set of rules that define how software components interact with each other. By using API we don’t need to perform functionality of n application from scratch.  PKI is an encryption framework that secures the exchange of online information. We can secure user login credentials more efficiently by using symmetric and asymmetric techniques.  SHA-256 is a commonly used hash function that takes an input of any length and produces a digest of 256 bits. By using the hashing function and salting technique we can secure users passwords and prevent threat attacks from users accounts.  SQL is a programming language used to create, interact with, and request information from a database. For example, the mobile app uses SQL to store information about the sneakers that are for sale, as well as the sellers who are selling them. It also uses SQL to access that data during a purchase. |
| **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.   * *What are the internal threats?* * *What are the external threats?*   *The internal threats could be application users who use weak passwords for accessing their accounts making is easy for attackers to access their accounts.*  *The external threat could be SQL injection which is exploited by threat actors in the database. This database is performing flawful operations.* |
| **V. Vulnerability analysis** | List **2 vulnerabilities** in the PASTA worksheet that could be exploited.   * *Could there be things wrong with the codebase?* * *Could there be weaknesses in the database?* * *Could there be flaws in the network?*   *There could be a wrong use of PKI in applications which will be vulnerable in the future for organizations.*  *Yes, there could be a weakness in the database. The malicious actor uses SQL injection in the database which will be a risk for organizations.*  *If there any vulnerability in API and organizations aren’t focused on hashing techniques, It will be a cause for flaws in the network.* |
| **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 you’ve learned about that can reduce risk.  When performing threat modeling, multiple methods can be used, such as  STRIDE  PASTA  Trike  VAST |