## 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?; Yes, the app will process transactions for buying and selling shoes* * *Does it do a lot of back-end processing?:*   *It should do a lot of back end processing if there are going to be algorithms to get more buyers and sell more shoes.*   * *Are there industry regulations that need to be considered?:*   *Yes, everything to secure all PII and SPII* |
| **2** | List oftechnologies used by the application:   * *Application programming interface (API)* * *Public key infrastructure (PKI)* * *SHA-256* * *SQL*   *The API should be the first, because if the code isn't secure, it would be vulnerable to injection attacks. PKI is the most secure infrastructure for keys for this type of website, especially if there are going to be sellers and buyers who need their own keys. SHA-256 needs to be used to cypher data to prevent attack, and SQL for search simplicity.* |
| **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?*   *Anyone who has access to the database, and competitors*   * *What are the external threats?*   *Anyone who is looking to steal data in the database like passwords* |
| **V. Vulnerability analysis** | List **2 vulnerabilities** in the PASTA worksheet that could be  exploited.   * *Could there be things wrong with the codebase?*   *Potential data leaks, and vulnerabilities for remote code execution*   * *Could there be weaknesses in the database?*   *Could be vulnerable to SQL injection in any type*   * *Could there be flaws in the network?*   *Yes, like specific port numbers that are not used, or DoS/DDoS protection* |
| **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.  Import password policies  Use SHA-256 encryption to make it harder to decrypt the database  Use asymmetric encryption for most security  Block unused network ports |