## 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?*   The mobile app has a feature that will let the sellers and shoppers conduct different transactions. The app includes payment options, log-in and out to the customers’ accounts, and direct messages, requiring it to have a lot of back-end processing. The company aims to make their customers confident on the confidentiality and security of the information they are providing. |
| **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.  On the list of these technologies, I decided to prioritize public key infrastructure or PKI in evaluation. This technology is responsible for all the online transactions, particularly credit card information.  Second is the API wherein it is utilize to make the development of the software and adding feature to the application faster and easier than starting from the scratch. Having a secured API must be implemented in the mobile app since this will control the user experience and functionality of the app. Next is the SHA-256 that uses hash functions to encrypt all the details of the customer, especially the sensitive ones such as passwords and credit card information. Last is the SQL connected to the database where customer data is being stored. SQL injection risk can be easier to be mitigated compared to the above technologies since a parameterized SQL code is a key for mitigation of the risk. |
| **III. Decompose application** | [Sample data flow diagram](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview?resourcekey=0-DZAkf7Vzh2PXsP-j3oXV-g)  After logging-in where their information are encrypted and hidden through public key infrastructure, when a user is finding an available sneaker of their type, a product search process will happen where the request of the customer will be released by the database, in which SQL commands are connected. The APIs used will produce the functionality that wil be helpful to the customers. |
| **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?*   Internal threats - employees, system administrator  External threat - bruteforce attackers, man-in-the-middle attacks (unsecured session due to HTTPS absence) |
| **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?*  1. Not closing the database connection properly 2. Lack of input validation on user input |
| **VI. Attack modeling** | [Sample attack tree diagram](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?usp=sharing&resourcekey=0-zYPY7AhPJdcClXamlAfOag)  The two types of threats against the user data are SQL injection due to lack of prepared statements, and session hijacking due to weak log-in credentials. |
| **VII. Risk analysis and impact** | List **4 security controls** that you’ve learned about that can reduce risk.   1. Secured Coding Practices 2. Encryption of data at rest 3. Least Privilege 4. Multi-factor authentication |