## 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 application is expected to accept, process and store customer personal information and financial data. Hence the application security will have to comply with applicable laws and standard that concerns PII and SPII e.g. GERD, CFAA, PIPEDA, ECPA, etc. |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *API* * *PKI* * *AES* * *SHA-256* * *SQL*   Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others.  PKI would be my priority as it concerns the basic security of the whole application. Next will be hashing method \*SHA256); it is essential to design a solid integrity mechanism for the data exchanged within and without the network. Also, ensuring the integrity of the data stored in the database is equally important. Thus, preparing the database against SQL injection and other database exploits is important. Finally, API must be designed to maintain an uninterrupted exchange of data between the app and thedatabase. |
| **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?* * *Internal threats for the application include specific XSS attacks.* * *External attacks include SQL injection and DoS.* |
| **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?* * *Lack of Prepared statements against SQL injections* * *Broken API* |
| **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.   * Hashing * Authentication and MFA * Authorization * Accountability |