## 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 app will be used to process transactions between sellers and shoppers, so data privacy and security are the priority in the mobile application.  The back-end process should be streamlined as much as possible, with functionalities like a messaging system between buyers and sellers, the ability to rate sellers to encourage good service, and the implementation of different payment options. Users must feel confident with the treatment of their information.  There are several industry regulations that need to be considered to avoid legal issues in the future, like: -   * GDPR, or General Data Protection Regulation, * PCI DSS, or Payment Card Industry Data Security Standard |
| **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.  API (Application Programming Interface) will be the method used to connect with the different shops or sellers that will be present in the application for the shoppers or buyers.  PKI (Public Key Infrastructure) will be the encryption framework used to secure the exchange of online information and establish trust by using a system of digital certificates.  AES (Advanced Encryption Standard) will be the symmetric algorithm used to encrypt or cipher sensitive data in transactions, giving different options to do it, from 128 bits to 256 bits.  SHA-256 (Secure Hashing Algorithms) will be the hash function used to protect sensitive user data by using secure digests of 256 bits, which are collision-resistant.  SQL (Structured Query Language) will be the programming language used to create, interact with, and request information from the database management system. |
| **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?*   Threats to consider in the development of the application that are risks to the information being handled by the application:   * SQL injection. * Session hijacking. |
| **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?*   Vulnerabilities that could be exploited:   * Lack of prepared statements. * Weak login credentials. |
| **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.  To reduce risk, there are several security controls that can be implemented from the NIST’s Digital Identity Guidelines (NIST SP 800-63B) like:   * Multi-factor authentication. * Password policies.   Other security controls must also be implemented to prevent SQL injection:   * Prepared statements, a coding technique that executes SQL statements before passing them on to the database. * Input sanitization, programming that removes user input that could be interpreted as code. * Input validation, programming that ensures user input meets a system’s expectations. |