## 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 main purpose of the application is to facilitate the process of*  *buying / selling shoes between sellers and shopper, usrs can authenticate via a login process, the platform contains information about customers and sellers. Buyers are able to ommunicate with sellers asking questions about the shoes they are interested inand rate the service provided.* |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *API* * *PKI* * *AES* * *SHA-256* * *SQL*   [*SQL tends to have the most vulnrabilities when it comes to an attack and in particular SQL injecion where code can be run by attackers to manipulate get or delete data from the database.*](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview?resourcekey=0-DZAkf7Vzh2PXsP-j3oXV-g)  Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others. |
| **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 would be SQL injection where an*  *attacker can execute malicious code gaining acess to the data but*  *with the potential thrat of using this as a backdoor to gain access to*  *other platforms and cause harm.* |
| **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?*   *The concern could be that login information could be stored withn the*  *database, if an attaker has access to user credrntials they have system*  *control.* |
| **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.  MFA should be implmntd within th ntwork to add an extra layer of secuity in case of a password breach.  Sanitizing fields within a web application to avoid character escaping  Enforce strong password mixture of upper and lowrcase as well as special characters minimum 12 characters and change every 30 days.  If not already implemnted introduce HTTPS which will enrypt session data during web application queries where th transmissions would be encrypted with SSL / TLS. |