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?*   *1) Sneaker company new app have a different types of payment process for the users for the the proper payment handlings to the seller and the shopers for that they wants there payment methods to be secure.*  *2) This new app required a lot of back-end programming for keeping track of the products, as well as all the users account in the secure database, so that servers can fetch data securely from the database as mentioned that data privacy is a big concern*  *3) There are industry regulations that need to be considered related to the diffrent types of payment methods that should be secured* |
| **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.  1) SQL querries that run on database is a very high priority sql querries need to be sanitized for and using prepared statement so that it is protected by SQL injections  2) API interfaces which connect the user with the server needed to be secure so that threat actor not able to hack the API  3) SHA-256: hashing algorithm should use to protect the user, seller and shoppers passwords and there credentials.  4) AES and PKI: is also considered for encrypting user logins information. |
| **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?*   *-) The internal threat to the Sneaker company new app could be use of social engineering( phising attack) by sending the emails to the users using the company brand, name and domain for fake sales or deals*  *-) The external threats could be done by the threat actors by using the SQL injectionon on the database to collect the users PII and SII* |
| **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?*   *-) It could be possible if the web app developer have flaws in the codebase and threat actor use to exploit it by puting the malicious code in the middle of the connection between the user and the server or using the malicious script to control the server as a part of a stored injection attack.*  *-) It could be possible if database is not configured securely and taking all types of sql querries as a input when user trying to login using there credentials could result in SQL injection tnat could led the user, seller, and shopper data be at risk.*  *-) There could be flaws in the network if the threat actor flooded the servers with the network traffic like DOS or DDOS attack which slows the process of transaction as well as taking more time to showing the item listing on the user browsers which creates overall bad user experience to the new app* |
| **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.  1) As a part of the technical security control configure the database in such a way that it would accept sanitized querries and prepared statements so that database is protected by SQL injection.  2) Another tecnical security control of using MFA for the users, sellers, and shopers as a part of there login credentials  3) Other technical securtiy control like monitoring and configure the server by using SIEM tools like Wireshark for packet analyzing for protecting the network.  4) As a part of operational security control app should follow the industry regulations for the transcation that could be done securely. |