## PASTA worksheet

|  |  |
| --- | --- |
| **Stages** | **Sneaker company** |
| **I. Define business and security objectives** | * *Users should be able to easily create and update their accounts* * *Buyers and sellers should be able to easily send messages to each other* * *Buyers should be given several options for payment* |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *API* * *PKI* * *AES* * *SHA-256* * *SQL*   We would look into PKI first because of the likelihood an attacker can use unencrypted data when communicating between the user’s client and the website. Other technologies listed will be utilized in further down given a defense in depth strategy. |
| **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** | * *Unencrypted data can be subject to packet sniffing, leading to attacks such as IP spoofing and session hijacking* * *Not using prepared statements in the application code may allow attackers to use SQL injection* |
| **V. Vulnerability analysis** | * *If the payment data is unencrypted, packet sniffing can discover sensitive information like credit card numbers* * *Search and text submissions can include code used in SQL injection attacks and fields should be validiated* |
| **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.   * Install an SSL certificate and leverage communication over HTTPS for data encryption for data in transit * Use prepared statements to minimize risk from SQL injection attacks. * RBAC should be used for API requests so the users would not call the server with requests they do not have the privileges of running * Enforce a strong password rule to make brute force or dictionary attacks more difficult |