## PASTA Worksheet

| **Stages** | **Sneaker company** |
| --- | --- |
| **I. Define business and security objectives** | * The app will process transactions * The app will accept user login credentials * The app will allow communication between two parties |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *Application programming interface (API)* * *Public key infrastructure (PKI)* * *SHA-256* * *SQL* * SQL   + SQL is used to communicate between the app and a central database. Since the database will contain sensitive data to a multitude of users ensuring it’s security is paramount. |
| **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** | * SQL injection   + A type of external threat where a malicious actor manipulates the query to return sensitive information from the database * Weak credentials   + Weak login credentials could result in unauthorized access to a user account |
| **V. Vulnerability analysis** | * Payment Form   + Methods used to collect payment information could be vulnerable to exploit * Search Queries   + The method of querying for product listings could be vulnerable to injection attacks. |
| **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** | * Strong password policies   + Strong passwords could reduce the likelihood of brute force attacks, session hijacking or rainbow table attacks * Include “salting” practices   + Salting hash values generated by SHA256 add an extra layer of security to the encryption * Prepared statements   + Prepared statements can protect against SQL injection attacks by running the query before sending it to the database * Input sanitization/validation   + Ensure user input is sanitized and validated |