## PASTA worksheet

| **Stages** | **Sneaker company** |
| --- | --- |
| **I. Define business and security objectives** | 1. *Both buyers and sellers should be able to create and manage accounts.* 2. *The app will support direct messaging between users.* 3. *The app must handle customers’ data safely and securely in compliance with PCI-DSS.* |
| **II. Define the technical scope** | *A lot of users will be interacting with the application by performing actions like signingup, logging-in and so on. So I think the first port of call should be evaluating if customers are connecting through the secure protocol HTTPS. Failure to use this protocol might expose users’ network traffic to IP spoofing or packet sniffing attacks which might expose sensitive information such as login credentials. Evaluating PKI will help to discover if network packets are encrypted in transit.*  *Users generally start communication with the database from the login page of the server. Failure to write code that sanitises input might lead to the execution of maliciously injected SQL queries. Hence, developers must write code that is able to filter out unwanted texts using certain key characters. They can achieve this by using prepared statements. With this, the code will execute the SQL before passing them on to the database.*  *It is also very important to make sure that customer data such as usernames and passwords are encrypted properly at rest. If data at rest aren’t hashed before storage, threat actors who successfully bypass the perimeter defenses could gain administrative access to network systems and the database. Using the SHA-256 algorithm will reduce the chances of compromising information that is stored in the DBs.* |
| **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** | *An SQL injection attack is an external threat*  *Weak security credentials such as a username and passwords is an internal threat.* |
| **V. Vulnerability analysis** | *Lack of prepared statements to sanitise inputs is a serious vulnerability. This can lead to easy injection of malicious code allowing a threat actor to retrieve information easily from the database.*  *Misconfigured firewalls which allow unrestricted access to certain ports and protocols can pose grave dangers to network systems.*  *Storing sensitive information such as credit card details and passwords iin plaintext is another critical vulnerability in application infrastructure.* |
| **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** | 1. Implementing multi-factor authentication can reduce TCP session hijacking attempts. 2. Introducing strong password policies like ensuring password rotation. 3. Enabling encryption at rest and transit is vital for data security. 4. Implementing salting and hashing will add an additional layer of security for data stored at rest. |