## PASTA worksheet

| **Stages** | **Sneaker company** |
| --- | --- |
| **I. Define business and security objectives** | There are payments happening on the app to give customers a seamless payment experience. Customers can also connect with sellers through the app. The customer has the ability to rate the seller. |
| **II. Define the technical scope** | Making sure the PKI is airtight should be prioritized. The exchange of payment information is highly sensitive, so its encryption should be important to the app. Other information, such as address will also be encrypted. |
| **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 * Session Hijacking |
| **V. Vulnerability analysis** | The payment processing system could be vulnerable to attack if it does not encrypt data properly. A session could be hijacked if proper protocols are not used in establishing a connection between the user and seller. |
| **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** | Input validation could help prevent SQL injection. This would ensure that code is not being put into entry fields to access databases.  Using the HTTPS protocol would ensure that sessions when connecting to the app are secure and info is properly encrypted.  Having secure password policies would help prevent brute force attacks from threat actors.  Least privilege would ensure that employees have access to only the information they need to complete their jobs. It would also make sure sensitive data is only used when it is needed. |