## PASTA worksheet

| **Stages** | **Sneaker company** |
| --- | --- |
| **I. Define business and security objectives** | Make **2-3 notes** of specific business requirements that will be analyzed.   * *The app will handle payment information for buyers and sellers.* * *Messaging between buyers and sellers.* * *Payment transfer security is a regulated space with pre existing standards.* |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *API uses a GUI to navigate, buy and sell products.* * *PKI uses both asymmetric and symmetric keys with AES for payment information and RSA to exchange keys.* * *SHA-256 is used to protect passwords and payment information* * *SQL is used to access listed item catalogs as well as during payment resolution.*   Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others. |
| **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.   * *Session hijacking* * *SQL injection* |
| **V. Vulnerability analysis** | List **2 vulnerabilities** in the PASTA worksheet that could be exploited.   * *Broken API token* * *Any location where a user inputs data that is accessed by an SQL query needs to be treated as a prepared statement. This even includes things like using the username or password as part of a query to prevent secondary injections.* * *Could there be flaws in the network?* |
| **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.  SHA-256, password policies, least privilege, incident response procedures |