## PASTA worksheet

|  |  |
| --- | --- |
| **Stages** | **Sneaker company** |
| **I. Define business and security objectives** | * *The app should facilitate seamless connection between sellers and shoppers.* * *User sign-up, login, and account management should be easy.* * *Data privacy is a major concern, ensuring responsible handling of user information.* |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *API* * *PKI* * *AES* * *SHA-256* * *SQL*   APIs serve as the backbone of interactions between different components of the application, making them essential to evaluate first. PKI, AES, SHA-256, and SQL are crucial for securing data transmission, encryption, and storage, aligning with the app's focus on data privacy and secure transactions. |
| **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** | * *Internal threats such as unauthorized access by employees or contractors.* * *External threats like SQL injection attacks or unauthorized access by hackers.* |
| **V. Vulnerability analysis** | * *Potential vulnerabilities in the application codebase, such as injection flaws or insecure deserialization.* * *Database vulnerabilities like weak authentication or inadequate access controls.* |
| **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** | * *Implementing secure coding practices and regular code reviews to mitigate application vulnerabilities.* * *Enforcing strong authentication mechanisms like multi-factor authentication (MFA) to prevent unauthorized access.* * *Implementing encryption at rest and in transit to protect sensitive data from interception or unauthorized access.* * *Regular security assessments, penetration testing, and monitoring to proactively detect and respond to security threats.* |