You’re part of the growing security team at a company for sneaker enthusiasts and collectors. The business is preparing to launch a mobile app that makes it easy for their customers to buy and sell shoes.

You are performing a threat model of the application using the PASTA framework. You will go through each of the seven stages of the framework to identify security requirements for the new sneaker company app.

## PASTA worksheet

|  |  |
| --- | --- |
| **Stages** | **Sneaker company** |
| **I. Define business and security objectives** | Make **2-3 notes** of specific business requirements that will be analyzed.   * *App will process transactions* * *App have a lot of back-end processing, it was developed to have extended functions and customer services.* * *Organization wants to avoid legal issues with improper payment handling ex. PCI-DSS* |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *API* * *PKI* * *AES* * *SHA-256* * *SQL*   We recommend prioritizing analyzing of API and SQL. Other technologies are checked secure methods of protecting data. SQL is sensitive on development mistakes which must be addressed immediately to improve app security. API handle a lot of sensitive data and is large attack surface. |
| **III. Decompose application** | Sample data flow diagram – w materiałach pomocniczych |
| **IV. Threat analysis** | * *Weak login credentials* * *Broken API authentication* |
| **V. Vulnerability analysis** | * *Injection* * *Session hijacking* |
| **VI. Attack modeling** | [Sample attack tree diagram](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?usp=sharing&resourcekey=0-zYPY7AhPJdcClXamlAfOag) – w materiałach pomocniczych |
| **VII. Risk analysis and impact** | **List 4 security controls that can reduce risk.**   * Implementation of prepared statements * Implementation of MFA * Implementation of input validation * Strong password policies |