Threat Modeling using PASTA

Scenario:
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.

Threat Modeling:

1) **Define business and security objectives:**

   - Complaints with PCI-DSS and GDPR
   - Users can create member profiles internally or by connecting external accounts.
   - Protecting the Customer Information(PII,SPII)

2) **Define the technical scope:**

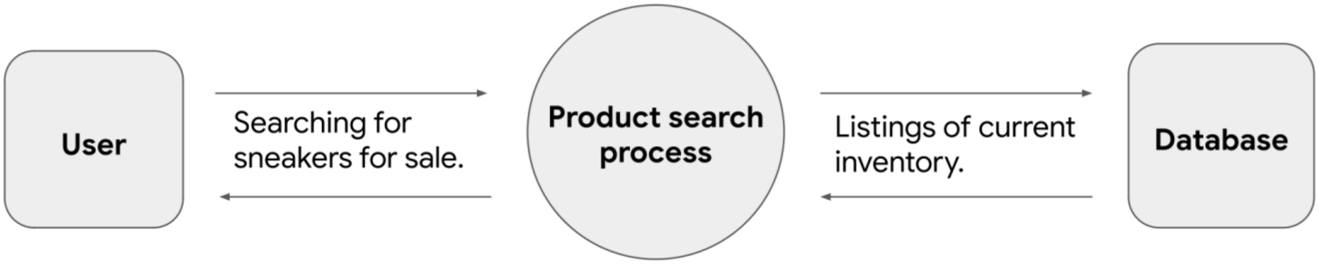
   List of Technologies used by Application:

   - API
   - PKI
   - AES
   - SHA-256
   - SQL

The user information must be encrypted while data in transit and perform hashing while data at rest to avoid data leakages. SQL is used to store the information in databases and is prone to SQL Injection attacks which needs to protected as well.

3) **Decompose application**

   Data flow diagram:


User
Searching for sneakers for sale.
Product search process
Listings of current inventory.
Database

4) **Threat analysis:**

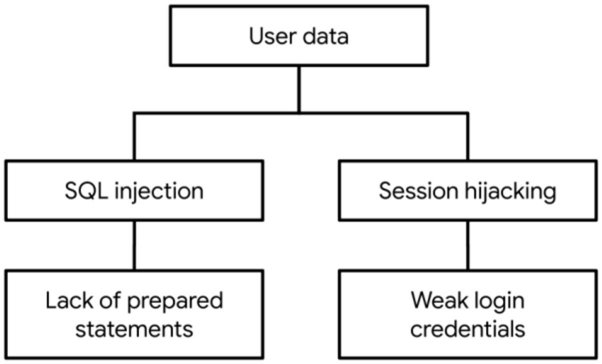
   Internal Threats: Employees clicking phishing emails, Leaving laptops /computers unattended with sensitive information open, Coding without best practices that can prone to cross site scripting or sql injection attacks

   External Threats : *Social Engineering , SQL Injection , Cross-site scripting*

5) **Vulnerability analysis:**

   - Lack of prepared statements
   - Broken API token
   - Lack of Employee training
   - Lack of monitoring and password policies

6) **Attack modeling**



7) **Risk analysis and impact:**

- Hashing Using SHA-256
- Implementing the principle of least privilege
- Implementing defense in-depth
- SIEM and IDS/IPS Tools
- Code Reviews
- Incident Response procedures
- Implementing security controls