PASTA Model Framework

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.

Components of PASTA

- Define Business and Security Objectives
- Define the Technical Scope
- Decompose Application (Data flow diagram)
- Threat analysis
- Vulnerability analysis
- Attack modeling (Attack tree)
- Risk anaylsis and impact

1. Define Business and Security Objectives

Requirements

Description: *Our application should seamlessly connect sellers and shoppers. It should be easy for users to sign-up, log in, and manage their accounts. Data privacy is a big concern for us. We want users to feel confident that we're being responsible with their information.*

Buyers should be able to directly message sellers with questions. They should also have the ability to rate sellers to encourage good service. Sales should be clear and quick to process. Users should have several payment options for a smooth checkout process. Proper payment handling is really important because we want to avoid legal issues.

Business	Security
Process Transactions/ Payments	Compliance with PCI-DSS
Users can create profiles and manage account	Protected by passwords and Multi-factor Authentication, Encryption
Database Utilization	Multifactor authentication, validate inputs, stored procedures
Secure Messaging	Encryption

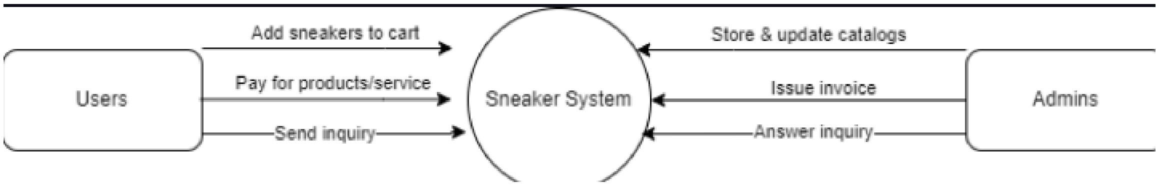
Context Diagram:

Users	Admins
Add item to cart	Store and update catalogs
Pay for products/service	Issue Invoice
Send Inquiry	Answer Inquiry

2. Define the Technical Scope

- API to connect the exchange of data between customers, employees and customers.
- Public key infrastructure (PKI)
- SHA-256 (Hash functions to protect the sensitive data from being viewed by administrators or anyone)
- SQL

3. Decompose Application



4. Threat Analysis

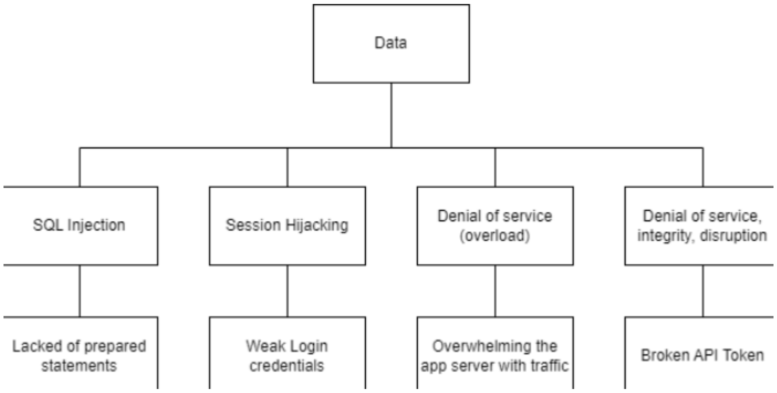
- SQL Injection
- Session Hijacking
- Denial-of-service
- Denial of service, integration issues, service disruptions

5. Vulnerability Analysis

- Lack of prepared statements (parameterized query, is a powerful tool in SQL that helps prevent SQL injection attacks and improve database performance.)
- Weak credential logins
- Overloaded app server
- Broken API Token

6. Attack Modelling

Attack tree diagram:


Data
SQL Injection
Session Hijacking
Denial of service (overload)
Denial of service, integrity, disruption
Lacked of prepared statements
Weak Login credentials
Overwhelming the app server with traffic
Broken API Token

7. Risk Analysis and Impact

- SHA-256 Hashing
- Incident response procedures
- Playbook (security policy)
- Password policy
- Principle of least privilege
- Zero-trust