ASTA Model Framework

Processs of Attack Simulation and Threat Analysis

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

Implementation

Define Business and Security Objectives

Business	Security
Process transactions	One account, one payment method
Users can create profiles	Protected by passwords and Multi-Factor Authentication
Accept multiple payment methods	The app should be in compliance with PCI-DSS
Database utilization	Provide multi-factor authentication

Context Diagram:

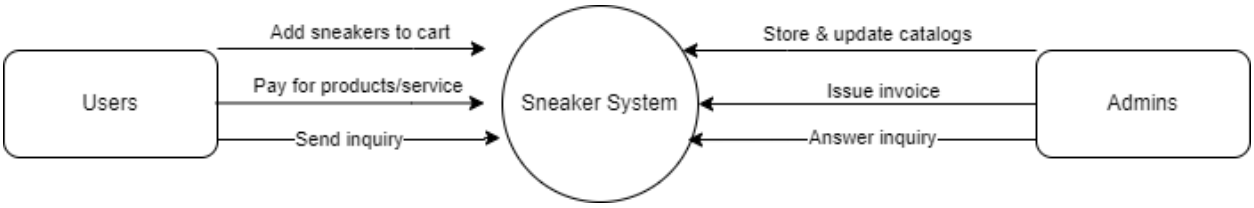
Users	Admins
Add sneakers to cart	Store & update catalogs
Pay for products/service	Issue invoice
Send inquiry	Answer inquiry

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

Decompose Application

Data Flow Diagram Level 0 or Context Diagram: In this case, I did not include level 1 and 2 as it might be way more complex.



Threat Analysis

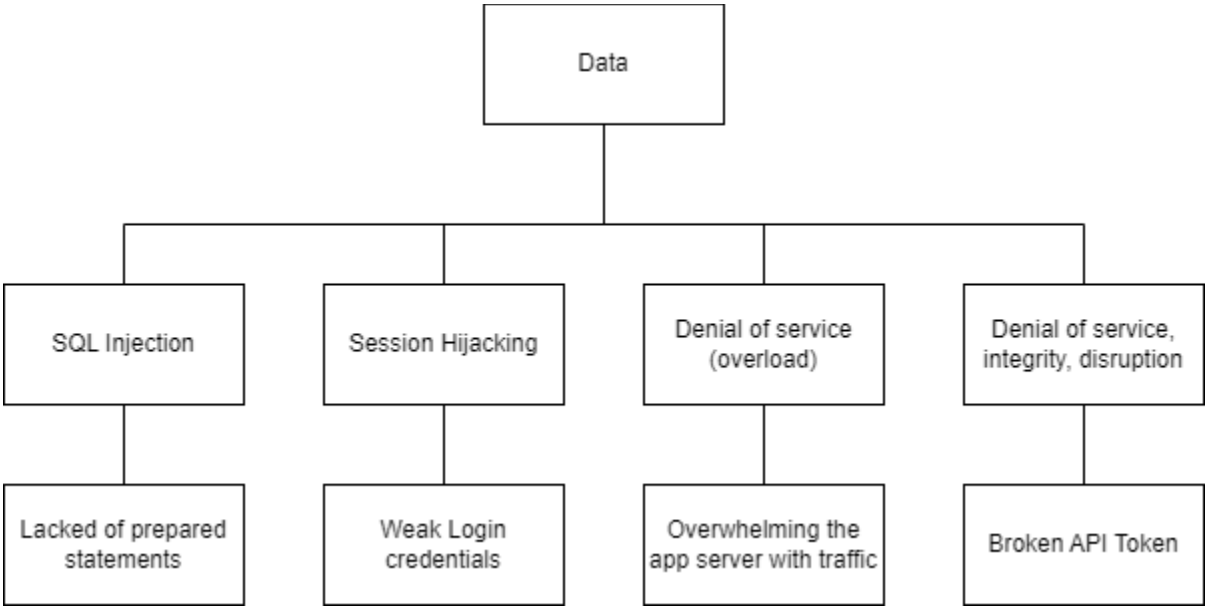
- SQL Injection
- Session Hijacking
- Denial-of-service
- Denial of service, integration issues, service disruptions

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

Attack Modelling

Attack tree diagram:



Risk Analysis and Impact

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