Cybersecurity Threat Modeling Activity

Activity Overview

In this exercise, I utilized the **Process of Attack Simulation and Threat Analysis (PASTA)** framework to evaluate the security risks associated with a new mobile shopping application. The goal was to conduct a thorough **threat model** to pinpoint potential vulnerabilities prior to the application's launch, ensuring a secure experience for users.

Threat modeling plays a vital role in secure software development, enabling security teams to **proactively identify, assess, and mitigate threats** before they can be exploited. PASTA, a well-regarded threat modeling framework, assists in evaluating an application's risk profile and formulating suitable security controls.

Scenario

I took on the role of a security analyst for a company focused on sneaker resale. The business aimed to introduce a **mobile marketplace app** that allows users to **buy and sell sneakers** in a secure manner.

My responsibility was to perform a **threat model** using the **PASTA framework**, systematically identifying risks through all seven stages:

1. **Defining Business & Security Objectives**
2. **Defining the Technical Scope**
3. **Decomposing the Application**
4. **Threat Analysis**
5. **Vulnerability Analysis**
6. **Attack Modeling**
7. **Risk Analysis & Impact Assessment**

Threat Modeling Breakdown

Stage I - Business & Security Objectives

The following **business and security objectives** were established for the sneaker marketplace app:

- **Secure Transactions:** The app must **safely process payments** while adhering to industry security standards (e.g., PCI DSS).

- **User Data Protection:** Customer information, including **login credentials, payment details, and purchase history**, must be encrypted and stored securely.
- **Fraud Prevention:** The platform must implement **authentication and anti-fraud mechanisms** to safeguard against unauthorized transactions and activities.