🛡️ PASTA Threat Modeling – Sneaker Marketplace App by Jordan Butler

📱 Scenario Overview

The company is launching a mobile app that allows sneaker collectors to buy and sell rare and high-demand shoes. As part of the security team, you're performing a threat model using the **PASTA** (Process for Attack Simulation and Threat Analysis) framework to evaluate the app's risk profile before launch.

🧩 PASTA – 7 Stages

---

1. Define Business Objectives

- **Enable secure in-app transactions** for buying and selling sneakers.
- **Protect user data**, including payment details, shipping addresses, and login credentials.
- **Maintain high availability** of the app to support global users 24/7 during product launches and limited drops.

---

2. Define the Technical Scope

- **Frontend (mobile app):** iOS and Android clients built using React Native.
- **Backend:** REST API hosted on AWS using Node.js and MongoDB.
- **Authentication:** OAuth2.0 with multi-factor authentication (MFA) and JWT for session management.

---

3. Application Decomposition (Data Flow Diagram Concepts)

- **User Registration/Login → Authentication Service → Database**
- **Product Upload → API Gateway → Cloud Storage**
- **Payment Processing → Payment API (e.g., Stripe) → Banking Provider**
- **Notifications → Push Notification Service**

---

4. Threat Analysis (Attacker Mindset)

- **Threat 1:** A threat actor attempts **credential stuffing** to gain access to high-profile reseller accounts.
- **Threat 2:** An attacker injects a **malicious script** into image metadata (sneaker photo) to exploit the upload API and compromise the backend.

---

5. Vulnerability Identification

- **Vulnerability 1:** Weak rate-limiting on login endpoints may allow brute-force attacks.
- **Vulnerability 2:** File upload endpoint doesn’t validate or sanitize image metadata, leaving the API open to injection attacks.

---

6. Attack Tree Mapping (Assets → Threats → Vulnerabilities)

- **Asset:** User account
  → **Threat:** Credential stuffing
  → **Vulnerability:** Missing rate limit
  → **Impact:** Account takeover, data theft
- **Asset:** Backend API
  → **Threat:** Code injection via image upload
  → **Vulnerability:** Unsanitized metadata
  → **Impact:** Server compromise, lateral movement

---

7. Risk Mitigation & Security Controls

- **Defense 1:** Enforce **rate limiting** and lockout mechanisms on login attempts.
- **Defense 2:** Require **multi-factor authentication (MFA)** for all user accounts.
- **Defense 3:** Implement **file type validation** and strip all metadata from uploaded files.
- **Defense 4:** Use **WAF (Web Application Firewall)** to filter and block malicious requests.

✅ Summary

This PASTA threat model identified key risks in the sneaker marketplace app, including account takeover and backend API compromise. Implementing targeted controls like rate limiting, MFA, and secure upload handling will significantly reduce the attack surface. This proactive security planning ensures the app can launch with stronger resilience and user trust.