PASTA Threat Modeling Exercise

# Stage I: Business Objectives

- Enable seamless interaction between buyers and sellers.  
- Ensure easy account management and strong data privacy.  
- Support secure and fast payment processing to avoid legal issues.

# Stage II: Technology Requirements

I would prioritize evaluating the API first because it serves as the communication channel between various components of the app, including third-party services. If improperly secured, APIs can expose sensitive endpoints and data. Given its central role in data exchange, it presents a higher initial risk than other technologies.

# Stage IV: Potential Threats

- API exploitation through injection or parameter tampering.  
- Social engineering targeting support staff to gain unauthorized access.

# Stage V: System Vulnerabilities

- SQL injection vulnerabilities due to improper input validation.  
- Weak encryption configurations or insecure key exchanges in PKI.

# Stage VII: Security Controls

- Implement input validation and sanitization to prevent SQL injection.  
- Use HTTPS and secure cipher suites for encrypted communication.  
- Require multi-factor authentication for user and admin logins.  
- Regularly update and patch third-party libraries and APIs.