Mobile App Details

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.

PASTA worksheet

Stages	**Sneaker company**
I. Define business and security objectives *Stage I typically requires gathering input from many individuals at a business.* Make **2-3 notes** of specific business requirements that will be analyzed. ● *Will the app process transactions?* ● *Does it do a lot of back-end processing?* ● *Are there industry regulations that need to be considered?*	*Business Requirements:* - *Easy for **users to sign-up, log in, and manage** their **accounts**.* - ***Data privacy** / **safe data handling** is a important* - *In app **Messaging*** - *Making the **selling process** easy and quick.* - *Several **payment options** for a smooth **checkout process**.* - ***Proper payment handling** to avoid legal issues.*
II. Define the technical scope List of technologies used by the application: ● *Application programming interface (API)* ● *Public key infrastructure (PKI)* ● *SHA-256* ● *SQL* Write **2-3 sentences** (40-60 words) that	**Data** at **rest**: - Database server OS must be kept updated - Use encryption algorithms like AES-256 to protect stored data. - Encrypt sensitive fields (e.g., passwords, payment info). - Never store passwords as plain text! - Use hashing (SHA-256) to store passwords securely. - Vulnerabilities in unpatched DB engines (MySQL, PostgreSQL, MongoDB, etc.) can be exploited. - Role Based Access controls

describe why you choose to prioritize that technology over the other	- Least Access Principle **APIs** (Data in transit) are used for : - Login purposes - Browsing the products or buyers - Searching items - Viewing buyer or product details - Adding item to cart - Checkout process - Retrieve order history - To send updates All APIs must **use HTTPS/TLS** requests to encrypt data in transit **SQL queries** are used (data creation and updation): - Sign up new user - Fetching search results - Fetching User Information - Updating User Information **PKI is used:** - When a user opens the app and connects to the server: - The server sends its digital certificate. - The app uses PKI to verify the server's identity. - If trusted, a secure HTTPS connection is established. - This ensures that: - User data like login info and credit card details are encrypted in transit. - The app is talking to the real server — not a fake one (prevents MITM attacks). The above technologies ensure that data is safe when it's at rest, in transit or in use.
III. Decompose application	The data flow diagram
IV. Threat analysis List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application. • *What are the internal threats?* • *What are the external threats?*	Internal Threats: - Physical - Lack of security in the building - No physical access control for employees - Open files - Unshredded papers or designs or manuals - Technical - No firewall on server - Outdated softwares - Human - Unintentional by Employees - Intentional by disgruntled Employees External Threats: - Competitors - For getting sensitive info - Hackers - For monetary gains - Users - Unintentionally disclose sensitive information
V. Vulnerability analysis List **2 vulnerabilities** in the PASTA	- Lack of validation in forms - Not using secure HTTPS for API requests

worksheet that could be exploited. ● *Could there be things wrong with the codebase?* ● *Could there be weaknesses in the database?* ● *Could there be flaws in the network?*	- Sensitive information stored in plain text in the database - No firewalls
VI. Attack modeling	Attack Tree Diagram
VII. Risk analysis and impact List **4 security controls** that you’ve learned about that can reduce risk.	Physical Controls: - Strong walls - Security guards - Surveillance cameras - Access control systems Technical Controls: - Firewalls - Antivirus software - Intrusion detection systems - Access control mechanisms (e.g., passwords, biometrics) Administrative Controls: - Password policies and training, - Training regarding Social Engineering attacks - Training to deal with user data and buyer data - Data classification policies - Access control procedures.