PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	• *Seamless connection between customers and sellers* • *User info should be stored and handled securely* • *Smooth and faster checkouts with multiple payment methods*
II. Define the technical scope	• *Application programming interface (API) is a way of communication between softwares. Third party APIs allow you to add different functionalities in your app without hard coding them* • *Public key infrastructure (PKI) will use both symmetric and asymmetric encryption e.g. AES and RES to encrypt sensitive information such as credit card info and the interaction between app and the user* • *SHA-256 will hash sensitive data such credit card info and user passwords* • *SQL will be used for data handling. It helps in structured interaction such as creating and requesting data.*
III. Decompose application	Sample data flow diagram
IV. Threat analysis	• *Social engineering is a threat that can't be ruled out. It can be used to get access to all sorts of information e.g. an employee could be tricked in giving important credentials.* • *Encryption methods can also be compromised* • *DoS attack is another threat that can affect communication between the app and users thus rendering the service useless* • *APIs are also prone to attacks and hence API security should not be overlooked*

V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. ● *Broken Access Control* ● *Insecure Design* ● *Injections e.g. Cross-Site Scripting* ● *Cryptographic Failures* ● *Identification and Authentic Failures*
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	The security controls can be divided into four categories: 1. Physical Security: Securing the infrastructure, such as access to buildings or the perimeter. 2. Digital Security: 2FA, or MFA can be used to reduce the attack surface from the end-user 3. Cybersecurity Controls: Encryptions and firewalls in place to prevent unauthorized access. Security the client side. 4. Cloud Security: In case the company uses any cloud-service for the app, it should also have prevention measures.