PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	***Data Privacy and Security****: Implement robust measures to protect user data and ensure privacy.* ***Transaction Processing****: Handle payments securely, supporting multiple options and complying with legal and industry standards.* ***Regulatory Compliance****: Adhere to data protection and payment processing regulations to avoid legal issues.*
II. Define the technical scope	In evaluating the technologies used by the application, prioritizing **SQL** is crucial because it handles the storage and retrieval of sensitive data, including user information and transaction details. Misconfigured databases or SQL injection vulnerabilities could lead to significant data breaches. Ensuring robust SQL security practices is essential to protect user data and prevent unauthorized access.
III. Decompose application	Sample data flow diagram In Stage III of PASTA, the app's data flow, such as a product search process, is analyzed for security risks. Key protections include encrypting data in transit and at rest, enforcing access controls, preventing SQL injection via input validation, and monitoring for anomalies, ensuring secure handling of user data and database interactions.
IV. Threat analysis	*In Stage IV of PASTA, potential threats to the sneaker app include:* *- External Threats: SQL injection attacks on the product search process and MITM attacks on data in transit.* *- Internal Threats: Insider misuse of database access and insufficient logging, which could allow undetected malicious activity within the application.*
V. Vulnerability analysis	In Stage V of PASTA, two potential vulnerabilities that could be exploited in the sneaker app include: 1. Codebase Vulnerability: Improper input validation in the product

	search function could leave the application susceptible to SQL injection attacks. 2. Database Weakness: Lack of encryption for sensitive data stored in the database could expose user information to attackers if the database is breached.
VI. Attack modeling	Sample attack tree diagram In Stage VI of PASTA, the attack tree outlines potential ways threat actors could exploit vulnerabilities. Two key attack vectors include SQL injection due to a lack of prepared statements and session hijacking via weak login credentials. These attack paths help security teams prioritize mitigation strategies to safeguard user data.
VII. Risk analysis and impact	In Stage VII of PASTA, four security controls that can reduce risks include: 1. Encryption: Protect data in transit and at rest by using strong encryption protocols. 2. Input Validation: Mitigate SQL injection by validating and sanitizing user inputs. 3. Multi-Factor Authentication (MFA): Strengthen login security to prevent session hijacking. 4. Prepared Statements: Safeguard against database attacks by using prepared SQL queries instead of dynamic ones.