PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	Secure user authentication and account management. Protection of user data privacy. Compliance with payment processing regulations.
II. Define the technical scope	I prioritize evaluating the SQL database interactions because SQL injection is a common and high-impact vulnerability that could compromise user data and payment information.
III. Decompose application	Reviewed the data flow diagram showing data moving from the user to the product search process, querying the database, and returning sneaker listings. Sample data flow diagram
IV. Threat analysis	1. SQL injection attacks targeting the database via the product search process. 2. Social engineering attacks targeting employees to gain system access.
V. Vulnerability analysis	1. Inadequate input validation in SQL queries. 2. Poor security training increasing susceptibility to social engineering.
VI. Attack modeling	Reviewed the sample attack tree showing SQL injection (due to lack of prepared statements) and session hijacking (due to weak login credentials) targeting user data. Sample attack tree diagram
VII. Risk analysis and impact	1. Implement input validation and prepared statements for SQL queries. 2. Use multi-factor authentication to strengthen login security. 3. Encrypt sensitive data both in transit and at rest. 4. Provide security awareness training to employees.