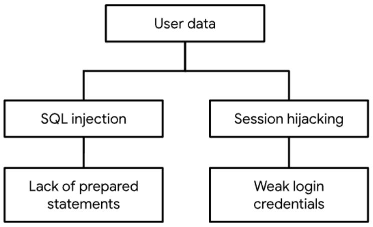
PASTA worksheet

Scenario

You're part of the growing security team at a company for sneaker enthusiasts and collectors. The business is preparing to launch a mobile app that makes it easy for their customers to buy and sell shoes.

You are performing a threat model of the application using the PASTA framework. You will go through each of the seven stages of the framework to identify security requirements for the new sneaker company app.

Stages	Sneaker company
I. Define business and security objectives	Make 2-3 notes of specific business requirements that will be analyzed. ● *Users can create member profiles internally or by connecting external accounts.* ● *The app must process financial transactions.* ● *The app should be in compliance with PCI-DSS.*
II. Define the technical scope	List of technologies used by the application: ● *Application programming interface (API)* ● *Public key infrastructure (PKI)* ● *Advanced encryption system (AES)* ● *Public-key cryptosystem (RSA)* ● *SHA-256* ● *SQL* *APIs play a crucial role in data exchange among customers, partners, and employees. Prioritizing them is essential, yet understanding which APIs are in use is vital before favoring one technology over another. Due to their expansive reach, APIs managing sensitive data can be more susceptible to security vulnerabilities, given the broader attack surface they present.*

III. Decompose application	Sample data flow diagram **Sample attack tree** **Note:** Applications like this normally have large, complex attack trees with many branches.  User data SQL injection Session hijacking Lack of prepared statements Weak login credentials
IV. Threat analysis	List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application. - *Injection* - *Session hijacking* - *Cross-Site-Scripting (XSS)*
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. - *Lack of prepared statements* - *Broken API token*
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	List **4 security controls** that can reduce risk. *SHA-256, incident response procedures, password policy, principle of least privilege, network segmentation, encryption,*