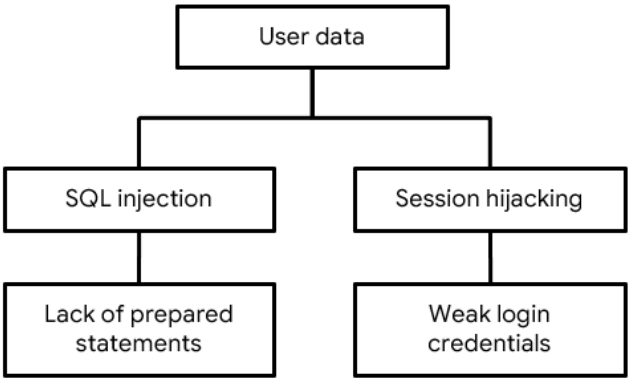
Applying the PASTA Threat Model Framework

Stages	Sneaker Company
I. Define business and security objectives	• *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	Technologies used by the application: • *Application programming interface (API)* • *Public key infrastructure (PKI)* • *Advanced encryption system (AES)* • *SHA-256* • *SQL* *APIs facilitate data exchange and should be prioritized due to their role in connecting users and systems. They handle sensitive data, which increases the attack surface and potential vulnerabilities.*
III. Decompose application	Basic data flow diagram for process breakdown: 
IV. Threat analysis	• *Injection* • *Session hijacking*
V. Vulnerability analysis	• *Lack of prepared statements* • *Broken API token*
VI. Attack modeling	Basic attack tree diagram for potential attack vectors 
VII. Risk analysis and impact	**Security controls** that can reduce risk. • *SHA-256 encryption* • *Incident response procedures* • *Password policy* • *Principle of least privilege*

Lab Summary:

- I carefully reviewed the description of the sneaker company app to understand the specific business objectives and security requirements.
- I prioritized the evaluation of technologies used in the app and decided to focus on APIs due to their critical role in data exchange and potential vulnerabilities.
- I analyzed the application's processes by decomposing them and examining the data flow (data flow diagram).
- I identified potential threats to the application, including injection attacks and session hijacking, which could compromise the security of the handled information.
- I explored vulnerabilities such as the lack of prepared statements and broken API tokens that could be exploited by malicious actors.
- Drafted basic attack tree diagram, which would have provided insights into potential attack vectors.
- To mitigate risks and improve security, I identified four important security controls: SHA-256 encryption, incident response procedures, implementing a strong password policy, and following the principle of least privilege.

Key Learnings:

- Understanding the importance of aligning business objectives and security requirements in threat modeling.
- Prioritizing technology evaluation based on its criticality, sensitivity, and potential attack surface.
- Analyzing application processes to identify potential threats and vulnerabilities.
- Recognizing common types of threats like injection attacks and session hijacking.
- Familiarity with vulnerabilities such as the lack of prepared statements and broken API tokens.
- Considering security controls as proactive measures to minimize risks and strengthen overall security posture.