Process for Attack Simulation and Threat Analysis (PASTA)

Stages	**Sneaker company**
I. Define business and security objectives	Make **2-3 notes** of specific business requirements that will be analyzed. ● *Users have the capability to establish member profiles either internally or through linking external accounts.* ● *The application is responsible for handling financial transactions.* ● *Ensuring compliance with PCI-DSS standards is a requirement for the application.*
II. Define the technical scope	List of technologies used by the application: ● *Application programming interface (API)* ● *Public key infrastructure (PKI)* ● *SHA-256* ● *SQL* *APIs play a crucial role in enabling the exchange of data among customers, partners, and employees, thus warranting prioritization. They manage a significant volume of sensitive information while connecting diverse users and systems. However, before prioritizing one technology over another, factors such as the specific APIs in use should be carefully evaluated. It's important to recognize that APIs can be more susceptible to security vulnerabilities due to their extensive attack surface.*
III. Decompose application	Sample data flow diagram
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*
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. ● *Unprepared statements* ● *Broken API token*

VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	List **security controls** that you've learned about that can reduce risk. *Access Control: Implementing strict access control measures to ensure that only authorized individuals can access sensitive data and resources.* *Encryption: Encrypting data both at rest and in transit to protect it from unauthorized access or interception.* *Patch Management: Regularly updating and patching software and systems to address known vulnerabilities and mitigate potential risks.* *Intrusion Detection and Prevention Systems (IDPS): Deploying IDPS to monitor network traffic and detect and prevent potential security breaches or unauthorized activities.* *Multi-Factor Authentication (MFA): Requiring multiple forms of authentication (e.g., passwords, biometrics, tokens) to verify the identity of users and enhance security.* *Security Awareness Training: Providing regular training and education to employees to raise awareness about security threats and best practices.* *Firewall Configuration: Configuring firewalls to filter incoming and outgoing network traffic based on predetermined security rules to prevent unauthorized access.* *Data Loss Prevention (DLP): Implementing DLP solutions to monitor, detect, and prevent the unauthorized transmission or exfiltration of sensitive data.* *Incident Response Plan: Developing and maintaining an incident response plan to effectively respond to security incidents, minimize their impact, and facilitate recovery.* *Security Auditing and Logging: Implementing auditing and logging mechanisms to track user activities and facilitate forensic analysis in the event of a security breach.*
