

PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	<ul style="list-style-type: none"> • <i>Users can create member profiles internally or by connecting external accounts.</i> • <i>The app must process financial transactions.</i> • <i>The app should be in compliance with PCI-DSS.</i>
II. Define the technical scope	<ul style="list-style-type: none"> • <i>Application programming interface (API)</i> • <i>Public key infrastructure (PKI)</i> • <i>SHA-256</i> • <i>SQL</i> <p><i>APIs facilitate the exchange of data between customers, partners, and employees, so they should be prioritized. They handle a lot of sensitive data while they connect various users and systems. However, details such as which APIs are being used should be considered before prioritizing one technology over another. So, they can be more prone to security vulnerabilities because there's a larger attack surface.</i></p>
III. Decompose application	<u>Data flow diagram</u>
IV. Threat analysis	<ul style="list-style-type: none"> • <i>SQL Injection</i> • <i>Session hijacking</i>
V. Vulnerability analysis	<ul style="list-style-type: none"> • <i>Lack of prepared statements</i> • <i>Broken API token</i> • <i>Weak Login Credentials</i>
VI. Attack modelling	<u>Attack tree diagram</u>
VII. Risk analysis and impact	<ul style="list-style-type: none"> • <i>SHA-256</i> • <i>Separation of Duties</i> • <i>Strong password policy</i> • <i>Principle of least privilege</i>