

Process for Attack Simulation and Threat Analysis (PASTA)

Stages	Sneaker company
I. Define business and security objectives	<p>Make 2-3 notes of specific business requirements that will be analyzed.</p> <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	<p>List of technologies used by the application:</p> <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 together. 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	Data flow diagram (see Supplements)
IV. Threat analysis	<p>List 2 types of threats in the PASTA worksheet that are risks to the information being handled by the application.</p> <ul style="list-style-type: none"> • <i>Injection</i> • <i>Session hijacking</i>
V. Vulnerability analysis	<p>List 2 vulnerabilities in the PASTA worksheet that could be exploited.</p> <ul style="list-style-type: none"> • <i>Lack of prepared statements</i> • <i>Broken API token</i>
VI. Attack modeling	Sample attack tree (see Supplements)
VII. Risk analysis and impact	<p>List 4 security controls that can reduce risk.</p> <p><i>SHA-256, incident response procedures, password policy, principle of least privilege</i></p>

SUPPLEMENTS:

Data flow diagram

Note: This data flow diagram represents a single process. Data flow diagrams for an application like this are normally much more complex.



Sample attack tree

Note: Applications like this normally have large, complex attack trees with many branches.

