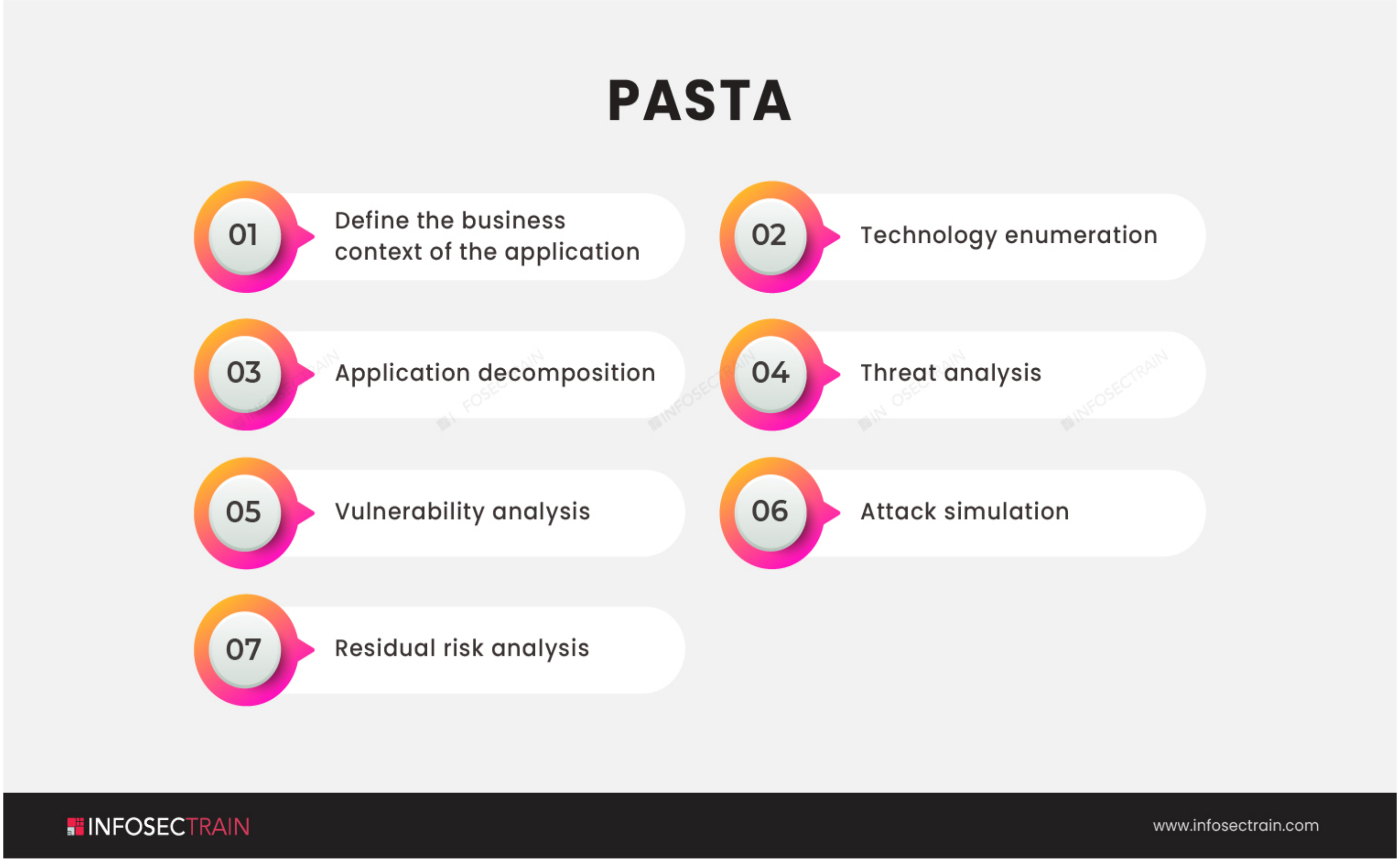
Scenario :: Threat Modeling using PASTA framework

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.

PASTA THREAT MODELING - INFODIAGRAM



PASTA

01 Define the business context of the application

02 Technology enumeration

03 Application decomposition

04 Threat analysis

05 Vulnerability analysis

06 Attack simulation

07 Residual risk analysis

INFOSECTRAIN www.infosectrain.com

Brief on PASTA threat modeling Stages

Stage - 1 : Identify the mobile app business objective

Business Objective : Our application should seamlessly connect sellers and shoppers. It should be easy for users to sign-up, log in, and manage their accounts. Data privacy is a big concern for us. We want users to feel confident that we're being responsible with their information.

Buyers should be able to directly message sellers with questions. They should also have the ability to rate sellers to encourage good service. Sales should be clear and quick to process. Users should have several payment options for a smooth checkout process. Proper payment handling is really important because we want to avoid legal issues.

Stage - 2 : Evaluate the app's components

Component : Since the app will handle the data exchange and storing, it would be necessary to have robust security, these technologies will be used ,

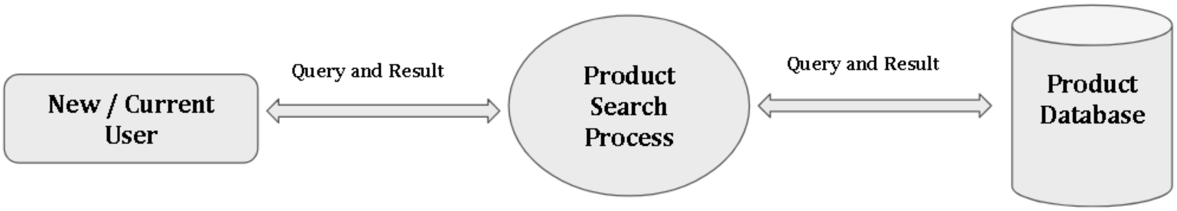
- *Application programming interface (API):* An API is a set of rules that define how software components interact with each other. In application development, third-party APIs are commonly used to add functionality without having to program it from scratch.
- *Public key infrastructure (PKI):* PKI is an encryption framework that secures the exchange of online information. The mobile app uses a combination of symmetric and asymmetric encryption algorithms: AES and RSA. AES encryption is used to encrypt sensitive data, such as credit card information. RSA encryption is used to exchange keys between the app and a user's device.
- *SHA-256*: SHA-256 is a commonly used hash function that takes an input of any length and produces a digest of 256 bits. The sneaker app will use SHA-256 to protect sensitive user data, like passwords and credit card numbers.
- *Structured query language (SQL):* SQL is a programming language used to create, interact with, and request information from a database. For example, the mobile

app uses SQL to store information about the sneakers that are for sale, as well as the sellers who are selling them. It also uses SQL to access that data during a purchase.

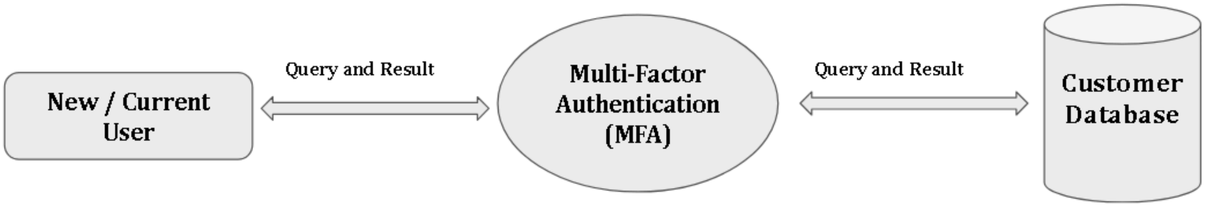
Stage - 3 : Review the data flow diagram

Data flow Diagram **-** An example would of the app's processes might be to allow buyers to search the database for shoes that are for sale.

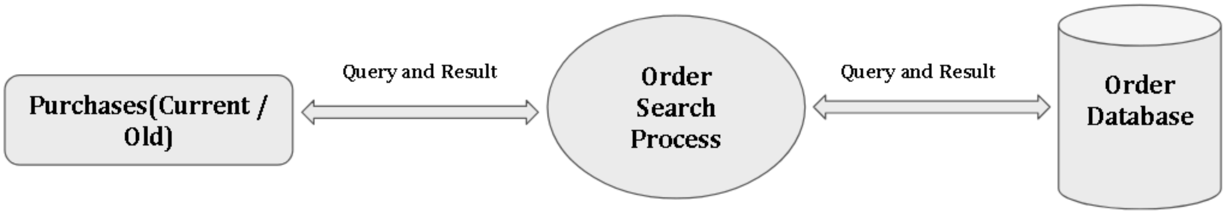
USER SIDE VIEW



LOGIN / SIGN UP SIDE VIEW



ORDER SIDE VIEW



Stage - 4 : Use an attacker mindset to analyze potential threats

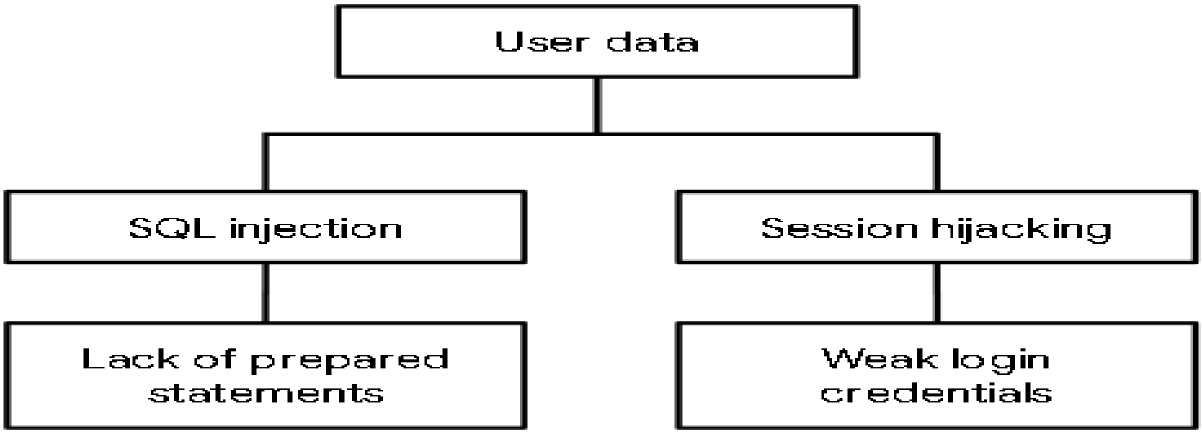
Potential Threat : The attacker could target the app's authentication system and use a virus. Authentication could also be attacked if a threat actor social engineers an employee. Best way to understand the potential threats would be to analyze the Internal system logs that you will use as a security analyst are good sources of threat intel.

Stage - 5 : List Vulnerabilities that can be exploited by those threats

List of Vulnerabilities : The most helpful website to access the software current and legacy vulnerabilities can be accessed in these pages like CVE (Provides a detailed list of flagged vulnerabilities and remediation) and OWASP (Refer OWASP Top 10 Projects)

Stage - 6 : Map assets, threats, and vulnerabilities to an attack tree.

Attack Tree : A flow diagram on threats and vulnerabilities used to attack the sneaker app.



Stage - 7 : Identify new security controls that can reduce risk

Control : An action in place if and when a vulnerability is exploited by a malicious actor.

Reports

STAGES	TITLE	SNEAKER COMPANY REPORTS
1	**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.*
2	**Define the technical scope**	List of technologies used by the application: - *Application programming interface (API)* - *Public key infrastructure (PKI)* - *SHA-256* - *SQL* *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.*
3	**Decompose application**	***See the Briefs***
4	**Threat analysis**	- *Injection* - *Session hijacking*

5	**Vulnerability analysis**	● *Lack of prepared statements* ● *Broken API token*
6	**Attack modeling**	***See the Briefs***
7	**Risk analysis and impact**	**6 security controls** that can reduce risk. *SHA-256, incident response procedures, password policy, principle of least privilege, Multi Factor Authentication(MFA) and regulatory compliance.*