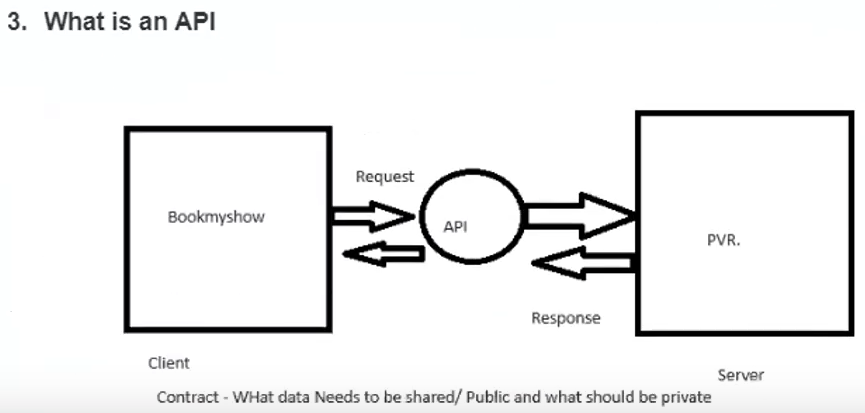
A diagram of a software development

Description automatically generated



API – Application Programming Interface – interface between 2 Application:

1. Bookmyshow and PVR
2. Zomato and Google Maps
3. Ola/uber with Google Maps
4. Swiggy with Banks
5. Dominos with Maps
6. Dominoes with Zomato
7. PhonePe with Banks

# Security Testing

Security testing is an integral part of software testing, Which is used to **discover the weaknesses, risks, or threats in the software application** and also help us to stop the nasty attack from the outsiders and make sure the security of our software applications.

The primary objective of security testing is to find all the potential ambiguities and vulnerabilities of the application so that the software does not stop working. If we perform security testing, then it helps us to identify all the possible security threats and also help the programmer to fix those errors.

It is a testing procedure, which is used to define that the data will be safe and also continue the working process of the software.

Examples of Security Breach:

1. Citizens data loss from government Official Vaccine Website.
2. WazirX Data loss.
3. Hackers stole 2 million Customers data from Dominos.
4. JW Marriott – Customers data lost – how ? – They used login Credentials of employees.

The goal of security testing is to:

* To identify the threats in the system
* To measure the potential vulnerabilities of the system
* To help in detecting every possible security risk in the system
* To help developers fix security problems through coding

In Depth explanation:

* **Evaluate the system’s ability to withstand an attack:** Security testing evaluates the system’s ability to withstand different types of attacks, such as network attacks, social engineering attacks, and application-level attacks.
* **Social Engineering attack:**  Involves Psychological Manipulation that tricks victims into sharing sensitive data.
* **Phishing:** Mails, Login website – Impersonating login and will compromise your credentials.

They will make it look like it’s okay, but it will be redirecting you to a malicious website and it can attack your system, it can copy your credentials, it can make your banking info to be compromised.

1. UI – will be an imposter
2. Mail imposter

* **Ensure compliance:** Security testing helps ensure that the system meets relevant security standards and regulations, such as HIPAA, PCI DSS, and SOC2
* **Provide a comprehensive security assessment:** Security testing provides a comprehensive assessment of the sytem’s security posture, including the identification of vulnerabilities, the evaluation of the system’s ability to withstand an attack, and compliance with relevant security standards.
* **Help organizations prepare for potential security incidents:** Security testing helps organizations understand the potential risks and vulnerabilities that they face, enabling them to prepare for and respond to potential security incidents.
* **Identify and fix potential security issues before deployment to production:** Security testing helps identify and fix security issues before the system is deployed to production. This helps reduce the risk of a security incident occurring in a production environment

## Explain the term vulnerability:

Vulnerability is a weakness or flaw in an IT system, network, or other resources that can be exploited to gain unauthorized access. Any intruder or bug can quickly attack the system due to its vulnerability. Using the vulnerability, an attacker can run malicious code, set up malware, or steal confidential information.

**Phishing:** In most cases, hackers send out fake emails that look as if they’re coming from legitimate sources, such as financial institutions, eBay, PayPal – and even friends and colleagues.

## Distributed denial-of-service attacks

In a distributed denial-of-service(DDoS) attack, multiple compromised machines attack a target, such as a server, website or other network resource, making the target totally inoperable.

The flood of connection requests, incoming messages or malformed packets forces the target system to slow down or to crash and shut down, denying service to legitimate users or systems.

## How to prevent DDoS attacks(or any attacks)

To help prevent DDoS attacks, companies should take the following steps:

* Implement technology and tools to monitor networks visually and know how much bandwidth a site uses on average. DDoS attacks offer visual clues so administrators who understand the normal behaviors of their networks will be better able to catch these attacks.
* Ensure servers have the capacity to handle heavy traffic spikes and the necessary mitigation tools necessary to address security problems.
* Update and patch firewalls and network security programs.
* Set up protocols outlining the steps to take in the event of a DDoS attack occurring

## Principle of Security Testing:

Below are the six basic principles of security testing:

* **Confidentiality –** it is a security process that prevents the leak of the data from the outsider’s because it is the only way where we can ensure the security of our data.

Example – Bank details when making a transaction/ or at any other time, especially PIN, passwords.

* **Integrity –** In this, we will secure those data which have been changed by unofficial person. The primary objective of integrity is to permit the receiver to control the data that is given by the system.
* **Authentication-** The authentication process comprises confirming the **individuality of a person**, tracing the source of a product that is necessary to allow access to the private information or the system.

**Example:** Login – Username and Password

**Presentation:** Pointers on how an organization has implemented security in their or in terms of authentication, authorization, encryption, etc.

* **Authorization –** It is the process of defining that a client is permitted to perform an action and also receive the services. The example of authorization is Access control.
* I am having authorization to edit the document, and trainees are not authorized to ed this document.
* Trainees oly have authorization to view only access.
* **Availability –** In this, the data must be retained by an official person, and they also gurantee that the data and statement services will be ready to use whenever we need it.

How easily I can get information about ICICI bank customer details?