<u>Assignment 1</u>: Study different types of Manual testing and prepare small description about each manual testing types

Manual Testing is a type of software testing in which test cases are executed manually by a tester without using any automated tools. The purpose of Manual Testing is to identify the bugs, issues, and defects in the software application.

Types of Manual Testing:

- Black Box Testing
- White Box Testing
- Unit Testing
- System Testing
- Integration Testing
- Acceptance Testing

White-box testing

The white box testing is done by Developer, where they check every line of a code before giving it to the Test Engineer. Since the code is visible for the Developer during the testing, that is why it is also known as White box testing.

Black box testing

The black box testing is done by the Test Engineer, where they can check the functionality of an application or the software according to the customer /client's needs. In this, the code is not visible while performing the testing; that is why it is known as black-box testing.

Gray Box testing

Gray box testing is a combination of white box and Black box testing. It can be performed by a person who knew both coding and testing. And if the single person performs white box, as well as black-box testing for the application, is known as Gray box testing.

<u>Assignment 2:</u> Different types of the Cyber Attacks

A cyber attack refers to an action designed to target a computer or any element of a computerized information system to change, destroy, or steal data, as well as exploit or harm a network.

Few types of cyber attacks are as follows:

- DoS and DDoS Attacks
- MITM Attacks
- Phishing Attacks
- Whale-phishing Attacks

- Spear-phishing Attacks

DoS and DDoS Attacks

A denial-of-service attack is designed to overwhelm the resources of a system to the point where it is unable to reply to legitimate service requests. A distributed denial-of-service attack is similar in that it also seeks to drain the resources of a system. A DDoS attack is initiated by a vast array of malware-infected host machines controlled by the attacker. These are referred to as "denial of service" attacks because the victim site is unable to provide service to those who want to access it.

MITM Attacks

Man-in-the-middle (MITM) types of cyber attacks refer to breaches in cybersecurity that make it possible for an attacker to eavesdrop on the data sent back and forth between two people, networks, or computers. It is called a "man in the middle" attack because the attacker positions themselves in the "middle" or between the two parties trying to communicate. In effect, the attacker is spying on the interaction between the two parties.

Phishing Attacks

A phishing attack occurs when a malicious actor sends emails that seem to be coming from trusted, legitimate sources in an attempt to grab sensitive information from the target. Phishing attacks combine social engineering and technology and are so-called because the attacker is, in effect, "fishing" for access to a forbidden area by using the "bait" of a seemingly trustworthy sender.

Whale-phishing Attacks

A whale-phishing attack is so-named because it goes after the "big fish" or whales of an organization, which typically include those in the C-suite or others in charge of the organization. These individuals are likely to possess information that can be valuable to attackers, such as proprietary information about the business or its operations.

Spear-phishing Attacks

Spear phishing refers to a specific type of targeted phishing attack. The attacker takes the time to research their intended targets and then write messages the target is likely to find personally relevant. These types of attacks are aptly called "spear" phishing because of the way the attacker hones in on one specific target. The message will seem legitimate, which is why it can be difficult to spot a spear-phishing attack.

<u>Assignment 3</u>: Define Microservices and Monolithic, difference between REST and SOAP

Monolithic: A monolithic architecture is a traditional model of a software program, which is built as a unified unit that is self-contained and independent from other applications.

A monolithic architecture is a singular, large computing network with one code base that couples all the business concerns together.

Organizations can benefit from either a monolithic or microservices architecture, depending on several different factors.

- Easy
- Development
- Performance
- Simplified testing

  Easy debugging

The disadvantages of a monolith include:

- Slower development speed
- Scalability
- Reliability
- Barrier to technology adoption
- Lack of flexibility
- Deployment

Microservices: A microservices architecture, also simply known as microservices, is an architectural method that relies on a series of independently deployable services. These services have their own business logic and database with a specific goal. Updating, testing, deployment, and scaling occur within each service.

The advantages of microservices are:

- Agility
- Flexible scaling
- Continuous deployment
- Highly maintainable and testable
- Independently deployable
- Technology flexibility
- High reliability
- Happier teams

The disadvantages of microservices can include:

- Development sprawl
- Exponential infrastructure costs
- Added organizational overhead
- Debugging challenges
- Lack of standardization
- Lack of clear ownership

REST: **representational state transfer**

REST is a set of architectural principles attuned to the needs of lightweight web services and mobile applications. Because it is a set of guidelines, it leaves the implementation of these recommendations to developers.

An application is said to be RESTful if it follows 6 architectural guidelines.

- A client-server architecture composed of clients, servers, and resources.
- Stateless client-server communication, meaning no client content is stored on the server between requests. Information about the session's state is instead held with the client.
- Cacheable data to eliminate the need for some client-server interactions.
- A uniform interface between components so that information is transferred in a standardized form instead of specific to an application's needs.
- A layered system constraint, where client-server interactions can be mediated by hierarchical layers.
- Code on demand, allowing servers to extend the functionality of a client by transferring executable code

SOAP: simple object access protocol

SOAP is a standard protocol that was first designed so that applications built with different languages and on different platforms could communicate. Because it is a protocol, it imposes built-in rules that increase its complexity and overhead, which can lead to longer page load times.

Common web service specifications include:

- **Web services security (WS-security)**: Standardizes how messages are secured and transferred through unique identifiers called tokens.
- **WS-Reliable Messaging**: Standardizes error handling between messages transferred across unreliable IT infrastructure.
- **Web services addressing (WS-addressing)**: Packages routing information as metadata within SOAP headers, instead of maintaining such information deeper within the network.
- **Web services description language (WSDL)**: Describes what a web service does, and where that service begins and ends.

SOAP vs REST

Many legacy systems may still adhere to SOAP, while REST came later and is often viewed as a faster alternative in web-based scenarios. REST is a set of guidelines that offers flexible implementation, whereas SOAP is a protocol with specific requirements like XML messaging.