**Assignment 1: Study different types of Manual testing and prepare small description about each manual testing types**

Manual testing is a software testing process in which test cases are executed manually without using any automated tool. All test cases executed by the tester manually according to the end user's perspective. It ensures whether the application is working, as mentioned in the requirement document or not. Test cases are planned and implemented to complete almost 100 percent of the software application. Test case reports are also generated manually.

**Types of Manual Testing**

* Acceptance Testing
* Black Box Testing- Integration testing, System Testing, Unit Testing
* White Box Testing
* Gray Box Testing

**Acceptance Testing:** User Acceptance Testing (UAT) is performed by the client or end-user, to confirm that the software meets the agreed requirements. Sometimes called pre-production testing, it takes place during the final phase before releasing the product to market.

UAT is an example of functional testing and types of acceptance testing include Alpha (executed within the organization) and Beta (where the[application](https://www.globalapptesting.com/blog/perfect-app) is released to a limited market to generate user feedback).

**Black Box Testing:** Also known as behavioral testing, this method aims to analyze an application’s functionality from the end-user’s perspective. The internal code structure is not visible during testing (hence the name “Black Box”), so testers are only aware of the inputs and expected outputs of the software.

Black Box Testing has several subdivisions, including functional testing for requirement compliance, smoke testing to assess basic functionality, and partitioning (dividing software into groups that are expected to exhibit similar behavior).

**Integration Testing:** Integration Testing is the process of testing an application with two or more integrating components. It is performed once the individual components have been unit-tested, and aims to identify problems with the interfaces and the interactions between them.

The two main methods are the Bottom-Up Approach (moving steadily from the bottom module to the top module) and Top-Down Approach (the opposite).

**System Testing:** System Testing means testing the system as a whole, once all its components have been unit-tested and integrated. It checks that the complete application works as intended, by comparing it against the original requirements.

Also called end-to-end testing, it typically involves installability testing (does the software install correctly?) and recovery testing (can the application recover from hardware crashes and network failures?).

**Unit Testing:** This is when the individual units or components of an application’s source code are tested, to make sure each function performs as expected. It is usually carried out by developers rather than engineers, as it requires detailed knowledge of the internal program design and code.

Also known as module testing or component testing, it simplifies the debugging system and helps to detect and protect against bugs in the future.

**White Box Testing:** Sometimes called transparent box testing or structural testing, this is a method of testing the internal structures or workings of an application. It is performed by the developer, who checks the software’s internal codes before passing it to a test engineer.

The main focus of White Box Testing is on strengthening security and improving the software’s design and usability. A combination of Black Box and White Box testing is known as Gray 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.

**Assignment 2: Different types of cyber attacks**

**Malware Attack:** A malware attack is a common cyberattack where malware executes unauthorized actions on the victim’s system. The malicious software encompasses many specific types of attacks such as ransomware, spyware, command and control, and more.

**Eavesdropping Attack:** Eavesdropping attacks involve the bad actor intercepting traffic as it is sent through the network. In this way, an attacker can collect usernames, passwords, and other confidential information like credit cards. Eavesdropping can be active or passive.

With active eavesdropping, the hacker inserts a piece of software within the network traffic path to collect information that the hacker analyzes for useful data. Passive eavesdropping attacks are different in that the hacker “listens in,” or eavesdrops, on the transmissions, looking for useful data they can steal.

Both active and passive eavesdropping are types of MITM attacks. One of the best ways of preventing them is by encrypting your data, which prevents it from being used by a hacker, regardless of whether they use active or passive eavesdropping.

**Brute Force Attack:** A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. Hackers work through all possible combinations hoping to guess correctly. These attacks are done by ‘brute force’ meaning they use excessive forceful attempts to try and force their way into your private accounts.

**Ransomware:** With ransomware, the victim’s system is held hostage until they agree to pay a ransom to the attacker. After the payment has been sent, the attacker then provided instructions regarding how the target can regain control of their computer. The name ransomware is appropriate because the malware demands a ransom from the victim.

In a ransomware attack, the target downloads ransomware, either from a website or from within an email attachment. The malware is written to exploit vulnerabilities that have not been addressed by either the system’s manufacturer or the IT team.

**DoS and DDoS Attacks:** A DOS 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 (DDoS) 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.

With a DoS attack, the target site gets flooded with illegitimate requests. Because the site has to respond to each request, its resources get consumed by all the responses. This makes it impossible for the site to serve users as it normally does and often results in a complete shutdown of the site.

**Assignment 3: Define Microservices and Monolithic, difference between REST and SOAP**

**Microservices:** It is an architectural development style in which the application is made up of smaller services that handle a small portion of the functionality and data by communicating with each other directly using lightweight protocols like HTTP. According to Sam Newman, “Microservices are the small services that work together.”

The Microservice architecture has a significant impact on the relationship between the application and the database. Instead of sharing a single database with other microservices, each microservice has its own database. It often results in duplication of some data, but having a database per microservice is essential if you want to benefit from this architecture, as it ensures loose coupling. Another advantage of having a separate database per microservice is that each microservice can use the type of database best suited for its needs. Each service offers a secure module boundary so that different services can be written in different programming languages. There are many patterns involved in microservice architecture like service discovery & registry, caching, API gateway & communication, observability, security, etc.

**Advantages of microservices:**

* It is easy to manage as it is relatively smaller.
* If there’s any update in one of the microservices, then we need to redeploy only that microservice.

**Disadvantages of microservices:**

* Being a distributed system, it is much more complex than monolithic applications. Its complexity increases with the increase in a number of microservices.
* Skilled developers are required to work with microservices architecture, which can identify the microservices and manage their inter-communications.

**Monolithic:** If all the functionalities of a project exist in a single codebase, then that application is known as a monolithic application. We all must have designed a monolithic application in our lives in which we were given a problem statement and were asked to design a system with various functionalities. We design our application in various layers like presentation, service, and persistence and then deploy that codebase as a single jar/war file. This is nothing but a monolithic application, where **“mono”**represents the single codebase containing all the required functionalities.

**Advantages of monolithic applications:**

* Simple to develop relative to microservices, where skilled developers are required in order to identify and develop the services.
* Easier to deploy as only a single jar/war file is deployed.

**Disadvantages of Monolithic applications:**

* It becomes too large with time and hence, difficult to manage.
* We need to redeploy the whole application, even for a small change.

**SOAP VS REST**

|  |  |  |
| --- | --- | --- |
| **No.** | **SOAP** | **REST** |
| 1) | SOAP is a protocol. | REST is an architectural style. |
| 2) | SOAP stands for Simple Object Access Protocol. | REST stands for REpresentational State Transfer. |
| 3) | SOAP can't use REST because it is a protocol. | REST can use SOAP web services because it is a concept and can use any protocol like HTTP, SOAP. |
| 4) | SOAP uses services interfaces to expose the business logic. | REST uses URI to expose business logic. |
| 5) | JAX-WS is the java API for SOAP web services. | JAX-RS is the java API for RESTful web services. |
| 6) | SOAP defines standardsto be strictly followed. | REST does not define too much standards like SOAP. |
| 7) | SOAP requires more bandwidth and resource than REST. | REST requires less bandwidth and resource than SOAP. |
| 8) | SOAP defines its own security. | RESTful web services inherits security measures from the underlying transport. |
| 9) | SOAP permits XML data format only. | REST permits different data format such as Plain text, HTML, XML, JSON etc. |
| 10) | SOAP is less preferred than REST. | REST more preferred than SOAP. |