

Software testing

- **Introduction:-**
- Testing is a process of executing a program with the aim of finding error. To make our software perform well it should be error free.If testing is done successfully it will remove all the errors from the software.

(a) Black Box testing:- It is used for validation. In this we ignores internal working mechanism and focuses on **what is the output?**.

(b) White Box testing:- It is used for verification. In this we focus on internal mechanism i.e. **how the output is achieved?**

- **Principles of Testing:-**

- (i) All the test should meet the customer requirements
- (ii) To make our software ,testing should be performed by third party
- (iii) Exhaustive testing is not possible. As we need the optimal amount of testing based on the risk assessment of the application.
- (iv) All the test to be conducted should be planned before implementing it.
- (v) It follows parento rule(80/20 rule) which states that 80% of errors comes from 20% of program components.
- (vi) Start testing with small parts and extend it to large parts.

Types of Testing:-

1. Unit Testing

It focuses on smallest unit of software design. In this we test an individual unit or group of inter related units. It is often done by programmer by using sample input and observing its corresponding outputs.

Example:

- a) In a program we are checking if loop, method or function is working fine
- b) Misunderstood or incorrect, arithmetic precedence.
- c) Incorrect initialization

2. Integration Testing

The objective is to take unit tested components and build a program structure that has been dictated by design. Integration testing is testing in which a group of components are combined to produce output.

Integration testing are of two types: (i) Top down (ii) Bottom up

3. Regression Testing

Every time new module is added leads to changes in program. This type of testing make sure that whole component works properly even after adding components to the complete program.

Example

In school record suppose we have module staff, students and finance combining these modules and checking if on integration these module works fine is regression testing

4. Smoke Testing

This test is done to make sure that software under testing is ready or stable for further testing

It is called smoke test as testing initial pass is done to check if it did not catch the fire or smoked in the initial switch on.

Example:

If project has 2 modules so before going to module make sure that module 1 works properly

5. Alpha Testing

This is a type of validation testing. It is a type of *acceptance testing* which is done before the product is released to customers.

Example:

When software testing is performed internally within the organization

6. Beta Testing

The beta test is conducted at one or more customer sites by the end-user of the software. This version is released for the limited number of users for testing in real time environment

Example:

When software testing is performed for the limited number of people

7. System Testing

In this software is tested such that it works fine for different operating system. It is covered under the black box testing technique. In this we just focus on required input and output without focusing on internal working.

In this we have security testing, recovery testing, stress testing and performance testing

Example:

This include functional as well as non functional testing

8. Stress Testing

In this we give unfavorable conditions to the system and check how they perform in those conditions.

Example:

- (a) Test cases that require maximum memory or other resources are executed
- (b) Test cases that may cause thrashing in a virtual operating system
- (c) Test cases that may cause excessive disk requirement

9. Performance Testing

It is designed to test the run-time performance of software within the context of an integrated system. It is used to test speed and effectiveness of program.

Example:

Checking number of processor cycles.

Security testing

What is Security Testing?

- Security Testing is defined as a type of Software Testing that ensures software systems and applications are free from any vulnerabilities, threats, risks that may cause a big loss.
- Security testing of any system is about finding all possible loopholes and weaknesses of the system which might result into a loss of information, revenue, reputation at the hands of the employees or outsiders of the Organization.
- The goal of security testing is to identify the threats in the system and measure its potential vulnerabilities, so the system does not stop functioning or is exploited. It also helps in detecting all possible security risks in the system and help developers in fixing these problems through coding.


- **Types of Security Testing:**
- There are seven main types of security testing as per Open Source Security Testing methodology manual. They are explained as follows:




Vulnerability Scanning



Security Scanning




Penetration testing



Risk Assessment



Security Auditing



Posture Assessment

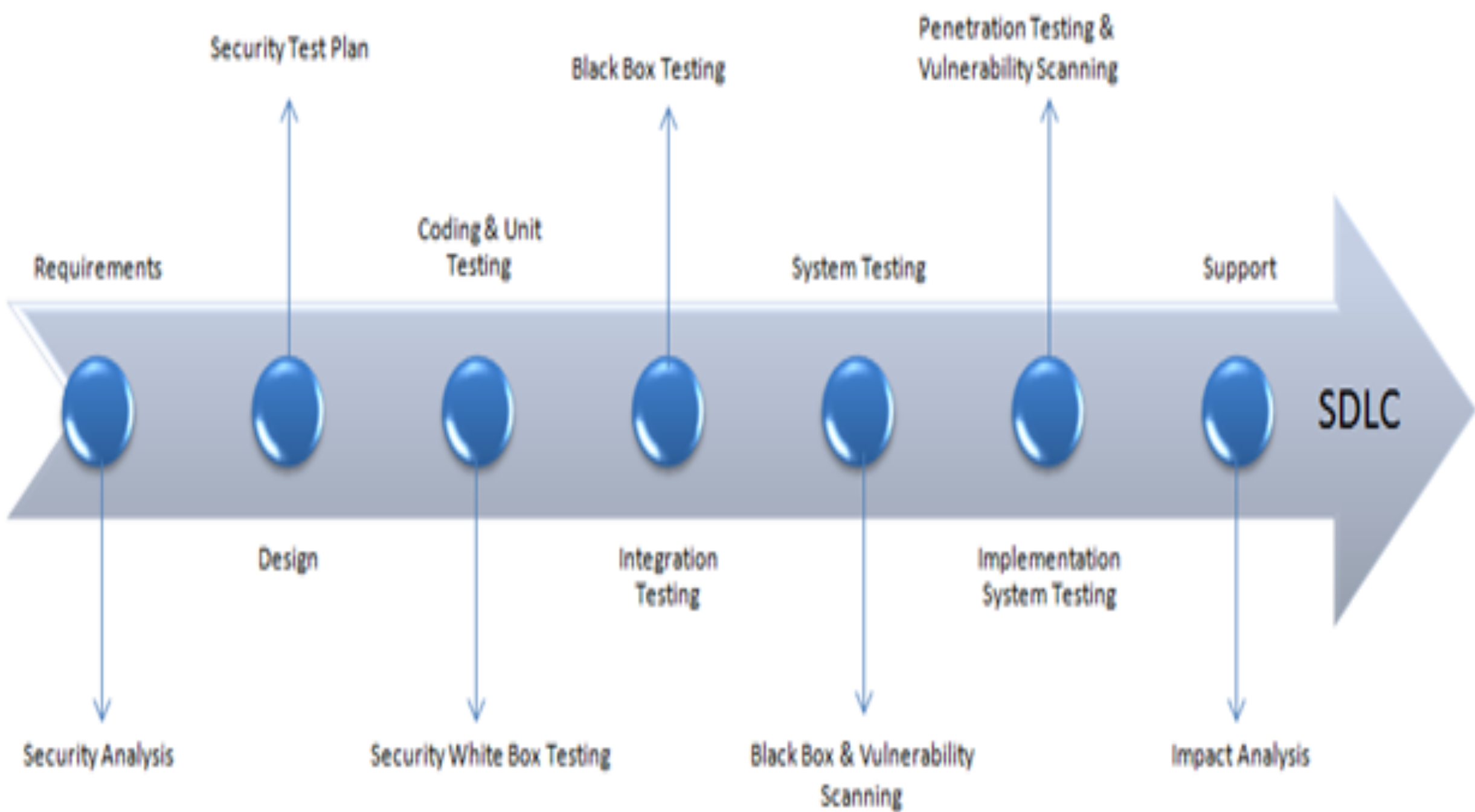


Ethical hacking

- **Vulnerability Scanning:** This is done through automated software to scan a system against known vulnerability signatures.
- **Security Scanning:** It involves identifying network and system weaknesses, and later provides solutions for reducing these risks. This scanning can be performed for both Manual and Automated scanning.
- **Penetration testing:** This kind of testing simulates an attack from a malicious hacker. This testing involves analysis of a particular system to check for potential vulnerabilities to an external hacking attempt.
- **Risk Assessment:** This testing involves analysis of security risks observed in the organization. Risks are classified as Low, Medium and High. This testing recommends controls and measures to reduce the risk.
- **Security Auditing:** This is an internal inspection of Applications and Operating systems for security flaws. An audit can also be done via line by line inspection of code
- **Ethical hacking:** It's hacking an Organization Software systems. Unlike malicious hackers, who steal for their own gains, **the intent is to expose security flaws in the system.**
- **Posture Assessment:** This combines Security scanning, [Ethical Hacking](#) and Risk Assessments to show an overall security posture of an organization.

- **How to do Security Testing**

- It is always agreed, that cost will be more if we postpone security testing after software implementation phase or after deployment. So, it is necessary to involve security testing in the SDLC life cycle in the earlier phases.
- Let's look into the corresponding Security processes to be adopted for every phase in SDLC



SDLC Phases	Security Processes
Requirements	Security analysis for requirements and check abuse/misuse cases
Design	Security risks analysis for designing. Development of Test Plan including security tests
Coding and Unit Testing	Static and Dynamic Testing and Security White Box Testing
Integration Testing	Black Box Testing
System Testing	Black Box Testing and Vulnerability scanning
Implementation	Penetration Testing , Vulnerability Scanning
Support	Impact analysis of Patches

- The test plan should include
- Security-related test cases or scenarios
- Test Data related to security testing
- Test Tools required for security testing
- Analysis of various tests outputs from different security tools

- **Example Test Scenarios for Security Testing:**
- Sample Test scenarios to give you a glimpse of security test cases -
- A password should be in encrypted format
- Application or System should not allow invalid users
- Check cookies and session time for application
- For financial sites, the Browser back button should not work.

- **Methodologies/ Approach / Techniques for Security Testing**
- In security testing, different methodologies are followed, and they are as follows:
- **Tiger Box:** This hacking is usually done on a laptop which has a collection of OSs and hacking tools. This testing helps penetration testers and security testers to conduct vulnerabilities assessment and attacks.
- **Black Box:** Tester is authorized to do testing on everything about the network topology and the technology.
- **Grey Box:** Partial information is given to the tester about the system, and it is a hybrid of white and black box models.

- **Roles:**

- Hackers - Access computer system or network without authorization
- Crackers - Break into the systems to steal or destroy data
- Ethical Hacker - Performs most of the breaking activities but with permission from the owner
- Script Kiddies or packet monkeys - Inexperienced Hackers with programming language skill

- **Conclusion:**
- Security testing is the most important testing for an application and checks whether confidential data stays confidential.
- In this type of testing, tester plays a role of the attacker and play around the system to find security-related bugs.
- Security Testing is very important in Software Engineering to protect data by all means.