## Performance Testing

In this section, we will learn about performance testing, why we need it, types of performance testing, and the performance testing process.

## What is performance testing?

It is the most important part of non-functional testing.

“Checking the behavior of an application by applying some load is known as performance testing.”

### Speed

 Determines whether the application responds quickly

### Scalability Testing

Checking the performance of an application by increasing or decreasing the load in particular scales (no of a user) is known as **scalability testing**. Upward scalability and downward scalability testing are called scalability testing.

Scalability testing is divided into two parts which are as follows:

* **Upward scalability testing**
* **Downward scalability testing**

### Stability Testing

Checking the performance of an application by **applying the load for a particular duration of time** is known as **Stability Testing**.

## Reliability

**Reliability Testing** is a software testing process that checks whether the software can perform a failure-free operation in a particular environment for a specified time period. The purpose of Reliability testing is to assure that the software product is bug-free and reliable enough for its expected purpose.

## Types of Performance Testing

Following are the types of performance testing:

* **Load testing**
* **Stress testing**
* **Spike testing**
* **Volume testing**
* **Soak testing**

### Load testing

The load testing is used to check the performance of an application by applying some load which is either less than or equal to the desired load is known as load testing.

Tools:

* LoadRunner[HP]
* LoadNinja
* WebLOAD
* LoadComplete

**Stress Testing**

The stress testing is testing, which checks the behavior of an application by applying load greater than the desired load.

Tools:

* Apache JMeter
* NeoLoad
* Stress tester
* LoadRunner

**Spike Testing**

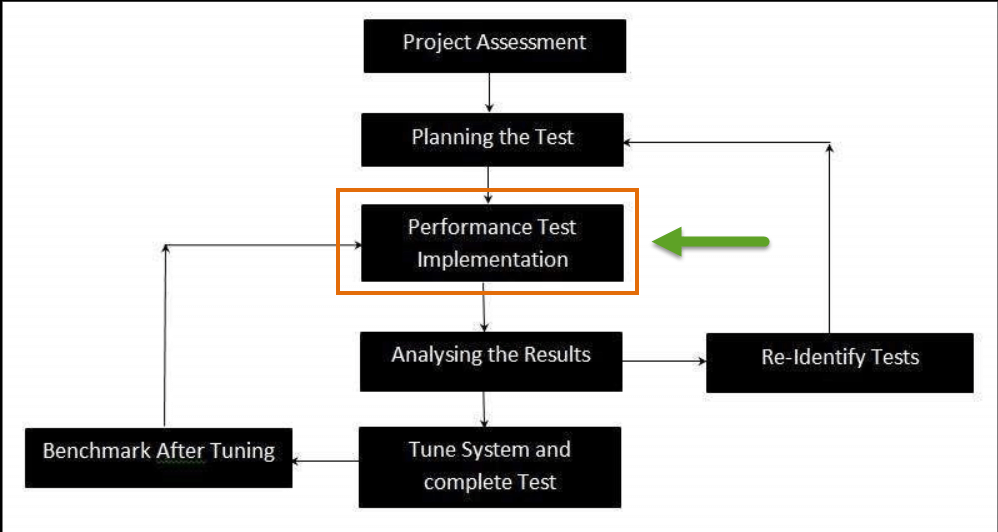
Tests the software’s reaction to sudden large spikes in the load generated by users.

**Volume Testing**

Under Volume Testing large no. of. Data is populated in a database, and the overall software system’s behavior is monitored. The objective is to check software application’s performance under varying database volumes.

**Soak Testing**

**Soak Testing** is a type of non functional testing that is used to measure performance of a software application under a huge volume of load for an extended period of time.



## SECURITY TESTING

## What is Security Testing?

**Security Testing** is a type of Software Testing that uncovers vulnerabilities, threats, risks in a software application and prevents malicious attacks from intruders. The purpose of Security Tests is to identify all possible loopholes and weaknesses of the software system which might result in a loss of information, revenue, repute at the hands of the employees or outsiders of the Organization.

## Types of Security Testing:

There are seven main types of security testing:

* Vulnerability Scanning
* Security Scanning
* Penetration Testing
* Risk Assessement
* Security Auditing
* Posture Assessement
* 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.

|  |  |
| --- | --- |
| **SDLC Phases** | **Security Processes** |
| **Requirement** | Security analysis for requirements and check abuse/misuse cases |
| **Design** | Security risks analysis for designing. Development of testplan 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 |

## Security Testing Tools:

* Acunetix
* Intruder
* Owasp
* Wireshark
* W3af
* ZAP
* SonarQube
* Arachini

**Key Terms used in Security Testing:**

**Vulnerability:**

This is the weakness of the web application. The cause of such “weakness” can be due to the bugs in the application, an injection (SQL/ script code), or the presence of viruses.

**URL Manipulation:**

Some web applications have an additional feature to communicate between the browser and the server in the URL. Changing some information in the URL may sometimes lead to unintended behavior by the server and this termed URL Manipulation.

**SQL injection:**

This is the process of inserting SQL statements through the web application user interface into some query that is then executed by the server.

**XSS (Cross-Site Scripting):**

When a user inserts HTML/client-side script in the user interface of a web application, this insertion is visible to other users and it is termed as XSS.

**Security Testing 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

**Six Basic Security Concepts:**

**• Confidentiality** – Information should be accessible to only those with authorized access.

**• Integrity** – A measure intended to allow the receiver to determine that the information which it is providing is correct.

**• Authentication** – Establish the identity of the user.

**• Authorization** – The user should receive a service or perform an action for which he has permission

**. • Availability** – Information and communication services should be ready at any time, as needed.

**• Non-repudiation** – Prevent later denial that an action happened.