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.**

WHY SECURITY TESTING IS IMPORTANT?

- **The main goal of Security Testing is to identify the threats in the system and measure its potential vulnerabilities, so the threats can be encountered and the system does not stop functioning or can not be exploited.**
- **It also helps in detecting all possible security risks in the system and helps developers to fix the problems through coding.**

TYPES:

1. Vulnerability Scanning:

This is done through automated software to scan a system against known vulnerability signatures.

2.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.

3.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.

4.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.

5.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

6.Ethical hacking:

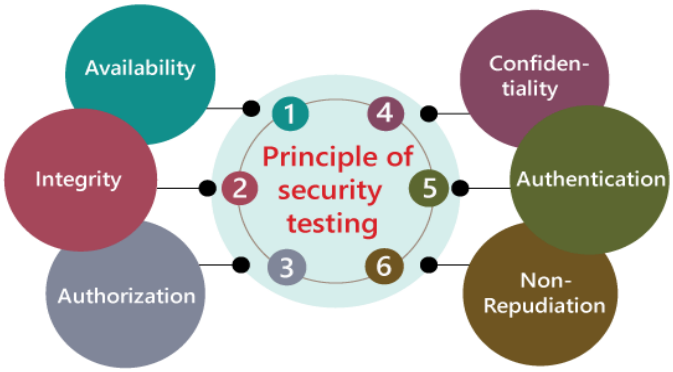
It's hacking an Organization Software systems. Unlike malicious hackers, who steal for their own gains, the intent is to expose security flaws in the system.

7.Posture Assessment:

This combines Security scanning, Ethical Hacking and Risk Assessments to show an overall security posture of an organization.

PRINCIPLES:

- **Availability**
- **Integrity**
- **Authorization**
- **Confidentiality**
- **Authentication**
- **Non-repudiation**



1.AVAILABILITY:

In this, the data must be retained by an official person, and they also guarantee that the data and statement services will be ready to use whenever we need it.

2.INTEGRITY:

In this, we will secure those data which have been changed by the unofficial person. The primary objective of integrity is to permit the receiver to control the data that is given by the system.

The integrity systems regularly use some of the similar fundamental approaches as confidentiality structures. Still, they generally include the data for the communication to create the source of an algorithmic check rather than encrypting all of the communication. And also verify that correct data is conveyed from one application to another.

3.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.

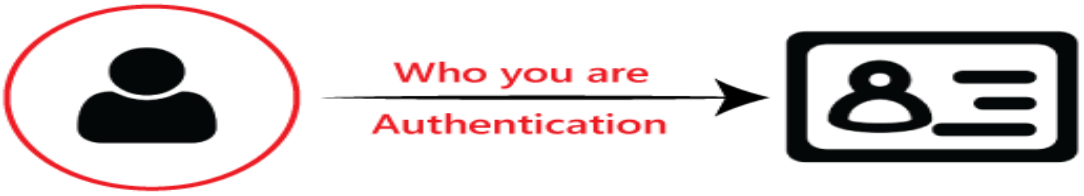
4.CONFIDENTIALITY:

It is a security process that protracts the leak of the data from the outsider's because it is the only way where we can make sure the security of our data.

5.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.

T
h
e



a

6.NON-REPUDIATION:

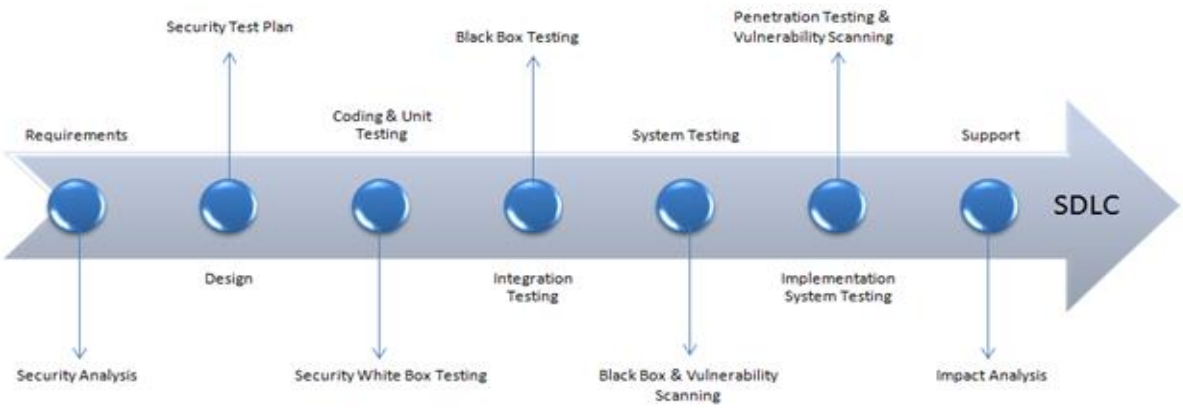
It is used as a reference to the digital security, and it a way of assurance that the sender of a message cannot disagree with having sent the message and that the recipient cannot repudiate having received the message.

The non-repudiation is used to ensure that a conveyed message has been sent and received by the person who claims to have sent and received the message.

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

EXAMPLE:

- 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.

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.

TOOLS:

1. Acunetix

2. Intruder

3. Owasp

4. WireShark

5. W3af