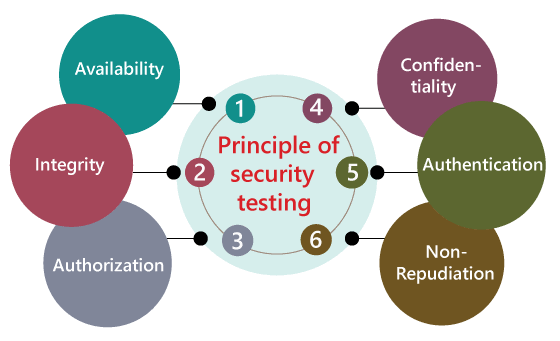
**Security testing:**

It’s happened during the all stages of development.

* Security testing checks whether software is vulnerable to cyber attacks, and tests the impact of malicious or unexpected inputs on its operations. Security testing provides evidence that systems and information are safe and reliable, and that they do not accept unauthorized inputs.
* Security testing is a type of non-functional testing.

**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.



**Principal of security testing:**

**1.Confidentiality**: it should be maintaining secret.& Information only get authorized person.

**2.integrity** :providing correct information to the user in a right way.

**3.Authentication:** it’s giving rights to the correct/Identity user.

**4.Availability:** whenever we want to access in right time.

**5.Non- repudiation:** we have to prevent the Denial of service that an action happened.



**Types of Security Testing:**

There are seven different kinds of security testing that can be conducted, with varying degrees of involvement from internal and external teams.

**1. Vulnerability Scanning** – involves use of an automated software tool to scan systems against predetermined vulnerabilities.

**2. Risk Assessment** – consists of an analysis of security risks in the application, software, or network. Once identified, they are classified as low, medium, high, or critical and mitigation measures can be enacted based on priority.

**3. Security Scanning** – can be done with manual or automated testing and serves as a means for locating network or system weaknesses.

**4. Penetration Testing** – simulates an attack from a malicious party or hacker and helps to clearly identify critical vulnerabilities in the system, software, or application.

**5. Security Auditing** – an internal inspection of all the operating systems and applications with the intent of finding security flaws. The results from the audit can then be passed to the applicable teams for follow up and correction.

**6. Ethical Hacking** – hired experts attempt to hack into a system or network with the goal of exposing flaws and gaps in the existing security measures.

**7. Posture Assessment** – a combination of ethical hacking, security scanning, and risk assessments to give a snapshot of the overall security within the organization.

**How to Perform Security Testing:**

Certain security testing processes correspond to different phases of the SDLC. Within the requirements phase, security analysis is necessary to check for any misuse cases. From there, when design begins, security risk analysis can be implemented.

A combination of black box and vulnerability scanning is recommended during system testing

Once the implementation phase begins, those two can be repeated with the addition of penetration testing to get the best picture of the strength of the security measures currently in place. In the instance of black box testing for security purposes, using crowd testers can yield more comprehensive results.