### **Pre-notes on Security Testing**

#### **Introduction to Security Testing**

**Definition:** Security testing is a type of software testing that aims to identify vulnerabilities and weaknesses in software applications, networks, or systems. The main goal is to ensure that data and resources are protected from potential intruders.

**Purpose:**

* To protect data from unauthorized access and breaches.
* To ensure the integrity, confidentiality, and availability of data.
* To prevent security threats and risks.

**Key Aspects:**

* Authentication: Ensures that only authorized users can access the system.
* Authorization: Ensures that users have the correct permissions.
* Confidentiality: Ensures that data is protected from unauthorized access.
* Integrity: Ensures that data is accurate and has not been tampered with.
* Availability: Ensures that systems and data are available when needed.

#### **Security Testing Types**

1. **Vulnerability Scanning:**
   * Automated tools scan the system to identify known vulnerabilities.
2. **Penetration Testing:**
   * Ethical hackers simulate attacks to identify vulnerabilities that could be exploited.
3. **Security Auditing:**
   * Manual or automated review of the code, design, and architecture to ensure compliance with security standards.
4. **Risk Assessment:**
   * Identifying, evaluating, and prioritizing risks followed by applying resources to minimize and control the probability of the event.
5. **Ethical Hacking:**
   * Authorized hacking to uncover security flaws in the system.
6. **Posture Assessment:**
   * Combination of security scanning, ethical hacking, and risk assessments to provide an overall security posture of an organization.
7. **Dynamic Application Security Testing (DAST):**
   * Testing the running application to identify vulnerabilities through external interfaces.
8. **Static Application Security Testing (SAST):**
   * Analysis of the source code to find vulnerabilities without executing the program.

#### **Security Testing with Burp Suite**

**Introduction:** Burp Suite is an integrated platform for performing security testing of web applications. It contains various tools that work seamlessly together to support the entire testing process.

**Key Features:**

* **Spider:** Crawls the application to map the content.
* **Scanner:** Automatically scans for numerous vulnerabilities.
* **Intruder:** Allows manual and automated customized attacks.
* **Repeater:** Sends individual requests repeatedly to test for vulnerabilities.
* **Sequencer:** Analyzes the randomness of tokens.
* **Decoder:** Decodes and encodes data.
* **Comparer:** Compares two pieces of data to identify differences.
* **Extender:** Allows the addition of third-party or custom extensions.

**Steps to Use Burp Suite:**

1. **Setup:**
   * Download and install Burp Suite.
   * Configure the browser to use Burp Suite as a proxy.
2. **Spidering:**
   * Use the Spider tool to crawl and map the application.
   * Identify all the pages and functionalities.
3. **Scanning:**
   * Use the Scanner to automatically identify common vulnerabilities such as SQL injection, cross-site scripting (XSS), and others.
4. **Manual Testing:**
   * Use tools like Repeater and Intruder for manual and semi-automated testing.
   * Test for vulnerabilities like CSRF, broken authentication, and session management issues.