**SECURITY TESTING TYPES:**

1.Vulnerability scanning

2.Security scanning

3.Penetration testing

4.Risk assessment

5.Security auditing

6.Ethical hacking

7.Posture assessment

**1.Vulnerability scanning**

This type of security testing involves the detection of system vulnerabilities through automated software. Vulnerability scanners examine web apps from the outside to identify cross-site scripting, SQL injections, command injections, insecure server configuration, etc.

The drawback of vulnerability scanning is that it can accidentally cause a system crash if mistakes for an invasive activity.

**2.Security scanning**

Security scanning aims to assess the general security level of the system by detecting weak points and loopholes. The more intricate the system or network is, the more complicated the security scan has to be. It can be done as a one-time check, but most software development companies prefer performing security scanning on a regular basis.

**3.Penetration testing**

Penetrating is the imitation of a cyberattack to check for exploitable vulnerabilities. The two most common forms of penetration testing are application penetration testing that aims to detect technical vulnerabilities and infrastructure penetration testing which examines servers, firewalls, and other hardware.

**4.Risk assessment**

A security risk assessment is a process of identifying and implementing key security controls in software. It also focuses on preventing security defects and vulnerabilities. A comprehensive security assessment allows organizations to create risk profiles for networks, servers, applications, etc., assess their criticality regarding business operations, and apply mitigating controls based on assessment results.

**5.Security auditing**

Security auditing is the process of testing and assessing the security of the company’s information system. A security audit allows verifying the adequacy of the implemented security strategy, uncovering extraneous software, and confirming the company’s compliance with regulations.

**6.Ethical hacking**

The term “ethical hacking” stands for the act of intruding into the system to detect vulnerabilities before a malicious attacker could find and exploit them. Ethical hackers may apply the same methods and tools used by their malicious counterparts but with the permission of the authorized person – they are also expected to report all the vulnerabilities found during the process to the management.

**7.Posture assessment**

A cybersecurity posture indicates how resilient the information security environment is when it comes to cybersecurity, and how well the enterprise can defend itself against cyberattacks.

Posture assessment provides an overall view of the organization’s security posture, what gaps currently exist, and what steps need to be taken to for improvement.