1. Security requirements analysis:

1. Configuration and Deployment Management.
2. Test File Extensions Handling for Sensitive Information.
3. HTTP method.
4. HTTP Strict Transport Security.
5. File Permission.
6. Identity Management.
7. Authentication Schema.
8. Strong password policy and CAPTCHA.
9. Authorization.
10. Session Management.
11. Input Validation.
12. Cryptography and end-to-end encryption.
13. Client-side protection.

2. Penetration testing

Penetration testing is going to be done in two ways: automatically and manually.

Penetration testing is done:

• Manually using the procedures developed for a particular application and type of threat

or

• Automatically using:

- o web application vulnerability scanners,
- o binary analysis tools,
- o proxy tools.

The main attacks performed during penetration testing are listed below:

- • Cross site scripting;
- • SQL injection;

- Server misconfiguration;
- Form manipulation;
- Cookies poisoning;
- Platforms vulnerabilities;
- Weak session management;
- Buffer overflows;
- Command injection.

Metrics that are collected on the dynamic testing stage:

- Number of vulnerabilities found (by features, lines of code, etc.)

3. Toolset

- NMAP: NMAP is short for Network Mapper. It is an open-source tool that helps you map a network by scanning ports, discovering operating systems, and creating an inventory of devices and the services running on them.
- WireShark: WireShark is another famous open-source tool that you can use for protocol analysis. It allows you to monitor network activities at a microscopic level. It is a growing platform with thousands of developers contributing from across the world.
- Burp Suite: Burp Suite is a set of penetration testing tools by Portswigger Web Security. It is used by ethical hackers, pen-testers, and security engineers. It is like a one-stop-shop for bug bounty hunters and security researchers. Let us take a look at a few tools included in Burp Suite.
- Nessus: Nessus is a vulnerability scanner by Tenable. It has been used by security professionals for vulnerability assessment since 1998. Their aim is to make vulnerability assessments simple and remediations quick. You can deploy it on a variety of platforms.
- Metasploit: Metasploit is a Ruby-based open-source framework, used by both ethical hackers and malicious actors to probe systematic vulnerabilities on networks and servers. The Metasploit framework also contains portions of fuzzing, anti-forensic, and evasion tools.