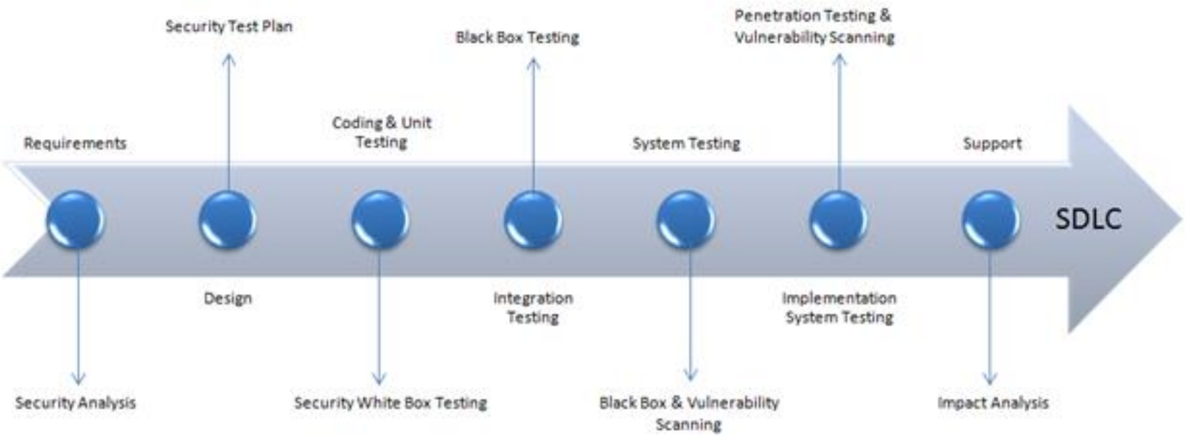
Security Testing

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.

It helps in detecting all possible security risks in the system and helps developers to fix the problems through coding.



Tools of Security Testing

1) **Acunetix**

   Acunetix, with its vulnerability scanner, pioneered automated web application security testing. The Acunetix Vulnerability Scanner features innovative black-box scanning and SPA crawling techniques in the form of AcuSensor and DeepScan respectively. The multi-threaded, DeepScan crawler has the capability to run an uninterrupted scan of WordPress installation for over a thousand vulnerabilities. A Login Sequence Recorder enables the tool to scan password-protected fields, whereas an in-built vulnerability management system helps with generation of various technical and compliance reports.

2) **Intruder**

   Intruder is a powerful, automated penetration testing tool that discovers security weaknesses across your IT environment. Offering industry-leading security checks, continuous monitoring and an easy-to-use platform, Intruder keeps businesses of all sizes safe from hackers.

3) Owasp -Open Web Application Security Project

The Open Web Application Security Project (OWASP) is a worldwide non-profit organization focused on improving the security of software. The project has multiple tools to pen test various software environments and protocols. Flagship tools of the project include

1. Zed Attack Proxy (ZAP – an integrated penetration testing tool)
2. OWASP Dependency Check (it scans for project dependencies and checks against know vulnerabilities)
3. OWASP Web Testing Environment Project (collection of security tools and documentation)

4) WireShark

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark can be used to capture and interactively browse the contents of network traffic.

Wireshark is also commonly used to analyze data from a trace file, generally in the form of a pcap (the file format of libpcap). Wireshark has a GUI and comes in both 32-bit and 64-bit versions.

5) W3af- web application attack and audit framework

It is a web application audit and attack framework that is effective against over 200 vulnerabilities. By identifying vulnerabilities such as SQL Injection, Cross-site scripting, Guessable credentials, unhandled application errors, and PHP misconfigurations, it assists in limiting the total exposure of a website to malicious elements. With both graphical and console-based interface, W3af promises the possibility of audit a web app’s security in less than five clicks. It can be used to send HTTP request and cluster HTTP responses. If a website is protected, it can use authentication modules to scan them. Output can be logged into a console, a file or sent via email.

6) Google Nogotofail

It is a network traffic security testing tool. It checks application for known TLS/SSL vulnerabilities and misconfigurations. Nogotofail provides a flexible and scalable way of scanning, identifying, and fixing weak SSL/TLS connections. It checks whether or not they are vulnerable to man-in-the-middle (MiTM) attacks. It can be set up as a router, VPN server or proxy server and works for Android, iOS, Linux, Windows, Chrome, OS, OSX, and any other device that is used to connect to the internet.

7) SQLMap

SQLMap is a penetration testing tool, powered by a detection engine for automating identification and exploitation of SQL injection flaws. Encompassing support for a broad spectrum of database management systems and SQL injection techniques, SQLMap automatically recognizes hash-based passwords and supports orchestration of a dictionary-based attack to crack them. With seven levels of verbosity support, it offers ETA support for each query and brings granularity and flexibility for both users' switches and features. Its fingerprint and enumeration features are valuable in streamlining an effective penetration test run.

8)Metasploit

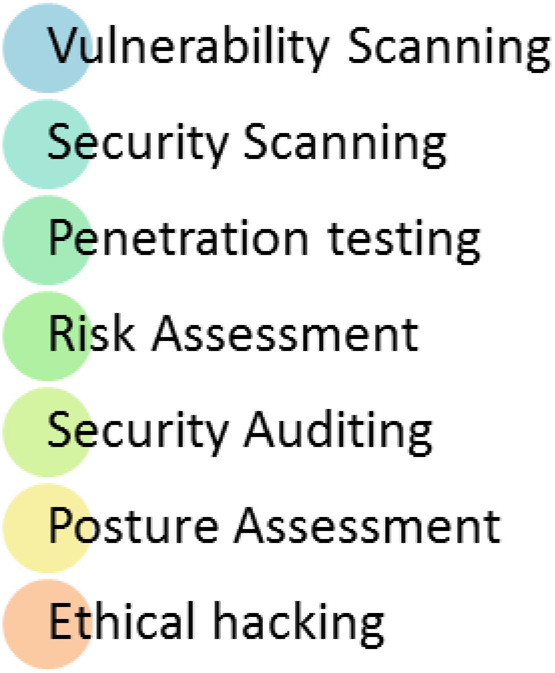
The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is open-source, free, and available to the public.

The project provides information about security vulnerabilities used by penetration testers during security audits and network administrators to ensure the correct configuration of the network's devices.

9)**NetSparker(Austin)**

NetSparker acts as a one-stop shop for all the web security needs. Available as both hosted as well as self-hosted solution, this platform can be easily integrated completely in any type of test and dev environment. NetSparker has a trade-marked Proof-Based-Scanning technology that uses automation to identify vulnerabilities and verify false positives, thus eliminating the need for unnecessary investment of huge man hours.

Types of Security Testing:



Vulnerability Scanning

Security Scanning

Penetration testing

Risk Assessment

Security Auditing

Posture Assessment

Ethical hacking

- **Vulnerability Scanning**: This is done through automated software to scan a system against known vulnerability signatures.
- **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.
- **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.
- **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.
- **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
- **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.

- **Posture Assessment:** This combines Security scanning, Ethical Hacking and Risk Assessments to show an overall security posture of an organization.

Keyterms

Vulnerability

Vulnerability is **the inability to resist a hazard or to respond when a disaster has occurred**

URL Manipulation

URL manipulation, also called URL rewriting, is **the process of altering (often automatically by means of a program written for that purpose) the parameters in a URL (Uniform Resource Locator)**. URL manipulation can be employed as a convenience by a Web server administrator, or for nefarious purposes by a hacker.

SQL Injection

SQL injection (SQLi) is **a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database**. It generally allows an attacker to view data that they are not normally able to retrieve.

Cross-site scripting attacks, also called XSS attacks, are a type of injection attack that injects malicious code into otherwise safe websites. An attacker will use a flaw in a target web application to send some kind of malicious code, most commonly client-side JavaScript, to an end user.