1A. Introduction

What is Web Application Security Testing?

A security test is a method of evaluating the security of a computer system or network by methodically validating and verifying the effectiveness of application security controls. A web application security test focuses only on evaluating the security of a web application. The process involves an active analysis of the application for any **weaknesses, technical flaws, or vulnerabilities**. Any security issues that are found will be presented to the system owner, together with an assessment of the impact, a proposal for mitigation or a technical solution.

What is a Vulnerability ?

A vulnerability is a flaw or weakness in a system's design, implementation, operation or management that could be exploited to compromise the system's security objectives.**(You are residing in a structurally fragile building with potential risks)**

Note: If you encounter any problems, please notify the system owner, conduct a joint investigation, and work together to identify a solution.

What is a Threat ?

A threat is anything (a malicious external attacker, an internal user, a system instability, etc) that may harm the assets owned by an application (resources of value, such as the data in a database or in the file system) by exploiting a vulnerability. **(Earthquake is a threat for your building)**

Vulnerability Assessment

- Vulnerability Testing also called Vulnerability Assessment is a process of evaluating security risks in software systems to reduce the probability of threats
- The purpose of vulnerability testing is reducing the possibility for intruders/hackers to get unauthorized access of systems. It depends on the mechanism named Vulnerability Assessment and Penetration Testing(VAPT) or VAPT testing.

Why do Vulnerability Assessment?

- It is important for the security of the organization.
- The process of locating and reporting the vulnerabilities, which provide a way to detect and resolve security problems by ranking the vulnerabilities before someone or something can exploit them.
- In this process Operating systems, Application Software and Network are scanned in order to identify the occurrence of vulnerabilities, which include inappropriate software design, insecure authentication, etc.

Penetration Testing

- Penetration Testing or Pen Testing is a type of Security Testing used to uncover vulnerabilities, threats and risks that an attacker could exploit in software applications, networks or web applications.
- The purpose of penetration testing is to identify and test all possible security vulnerabilities that are present in the software application. Penetration testing is also called Pen Test.

Why Penetration Testing?

- Financial sectors like Banks, Investment Banking, Stock Trading Exchanges want their data to be secured, and penetration testing is essential to ensure security
- In case if the software system is already hacked and the organization wants to determine whether any threats are still present in the system to avoid future hacks.
- Proactive Penetration Testing is the best safeguard against hackers

Penetration Testing Strategies

Based on the amount of information available to the tester

Strategies	Descriptions

Black Box	• Testers have no knowledge about the test target. • They have to figure out the loopholes of the system on their own from scratch. This is similar to the blind test strategy in, which simulates the actions and procedures of a real attacker who has no information concerning the test target
White Box	• Testers are provided with all the necessary information about the test target. • This strategy is referred to in as targeted testing where the testing team and the organization work together to do the test, with all the information provided to the tester prior to test
Grey Box	• Partial disclosure of information about the test target leads to gray box penetration testing. • Testers need to gather further information before conducting the test

Based on the specific objectives to be achieved

Strategies	Descriptions
External testing	• Any attacks on the test target using procedures performed from outside the organization that owns the test target . • The objective of external testing is to find out if an outside attacker can get in and how far he can get in once he has gained access.
Internal testing	• Penetration is performed from within the organization that owns the test target. • The strategy is useful for estimating how much damage a disgruntled employee could cause. • Internal testing is centered on understanding what could happen if the test target was successfully penetrated by an authorized user with standard access privileges.

Penetration Testing Types

Title	Descriptions
Network penetration testing	• An ethical and safe way to identify security gaps or flaws in the design, implementation or operation of the organization’s network. • The testers perform analysis and exploits to assess whether modems, remote access devices and maintenance connections can be used to penetrate the test target.
Application penetration testing	• An attack simulation intended to expose the effectiveness of an application's security controls by highlighting risks posed by actual exploitable vulnerabilities • Organizations use firewall and monitoring systems to protect information, security can still be compromised since traffic can be allowed to pass through the firewall.

Social engineering	• Preys on human interaction to obtain or compromise information about an organization and its computer systems [• It is used to determine the level of security awareness among the employees in the organization that owns the target system. • This is useful to test the ability of the organization to prevent unauthorized access to its information and information systems