What is Security Testing? Types with Example

What is Security Testing?

SECURITY TESTING is a type of Software Testing that uncovers vulnerabilities, threats, risks in a software application and prevents malicious attacks from intruders. 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.

Why Security Testing is Important?

The main goal of **Security Testing** is to identify the threats in the system and measure its potential vulnerabilities, so the threats can be encountered and the system does not stop functioning or can not be exploited. It also helps in detecting all possible security risks in the system and helps developers to fix the problems through coding.

In this tutorial, you will learn-

Types of Security Testing:

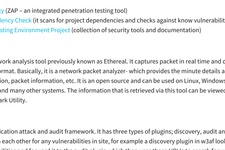
There are seven main types of security testing as per Open Source Security Testing methodology manual. They are explained as follows:

- **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.

How to do Security Testing

It is always agreed, that cost will be more if we postpone security testing after software implementation phase or after deployment. So, it is necessary to involve security testing in the SDLC life cycle in the earlier phases.

Let's look into the corresponding Security processes to be adopted for every phase in SDLC



SDLC Phases	Security Processes
Requirements	Security analysis for requirements and check abuse/misuse cases
Design	Security risks analysis for designing. Development of Test Plan including security tests
Coding and Unit Testing	Static and Dynamic Testing and Security White Box Testing
Integration Testing	Black Box Testing
System Testing	Black Box Testing and Vulnerability scanning
Implementation	Penetration Testing, Vulnerability Scanning
Support	Impact analysis of Patches

The test plan should include

- Security-related test cases or scenarios
- Test Data related to security testing
- Test Tools required for security testing
- Analysis of various tests outputs from different security tools

Example Test Scenarios for Security Testing:

Sample Test scenarios to give you a glimpse of security test cases -

- A password should be in encrypted format
- Application or System should not allow invalid users
- Check cookies and session time for application
- For financial sites, the Browser back button should not work.

Methodologies/ Approach / Techniques for Security Testing

In security testing, different methodologies are followed, and they are as follows:

- **Tiger Box**: This hacking is usually done on a laptop which has a collection of OSs and hacking tools. This testing helps penetration testers and security testers to conduct vulnerabilities assessment and attacks.
- **Black Box**: Tester is authorized to do testing on everything about the network topology and the technology.
- **Grey Box**: Partial information is given to the tester about the system, and it is a hybrid of white and black box models.

Security Testing Roles

- Hackers - Access computer system or network without authorization
- Crackers - Break into the systems to steal or destroy data
- Ethical Hacker - Performs most of the breaking activities but with permission from the owner
- Script Kiddies or packet monkeys - Inexperienced Hackers with programming language skill

Security Testing Tool

1) Owasp

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)

2) WireShark

Wireshark is a network analysis tool previously known as Ethereal. It captures packet in real time and display them in human readable format. Basically, it is a network packet analyzer- which provides the minute details about your network protocols, decryption, packet information, etc. It is an open source and can be used on Linux, Windows, OS X, Solaris, NetBSD, FreeBSD and many other systems. The information that is retrieved via this tool can be viewed through a GUI or the TTY mode TShark Utility.

3) W3af

w3af is a web application attack and audit framework. It has three types of plugins; discovery, audit and attack that communicate with each other for any vulnerabilities in site, for example a discovery plugin in w3af looks for different url's to test for vulnerabilities and forward it to the audit plugin which then uses these URL's to search for vulnerabilities.

Myths and Facts of Security testing:

Let's talk about an interesting topic on Myths and facts of security testing:

Myth #1: We don't need a security policy as we have a small business

Fact: Everyone and every company need a security policy

Myth #2: There is no return on investment in security testing

Fact: Security Testing can point out areas for improvement that can improve efficiency and reduce downtime, enabling maximum throughput.

Myth #3: Only way to secure is to unplug it.

Fact: The only and the best way to secure an organization is to find "Perfect Security". Perfect security can be achieved by performing a posture assessment and compare with business, legal and industry justifications.

Myth #4: The Internet isn't safe. I will purchase software or hardware to safeguard the system and save the business.

Fact: One of the biggest problems is to purchase software and hardware for security. Instead, the organization should understand security first and then apply it.

Conclusion:

Security testing is the most important testing for an application and checks whether confidential data stays confidential. In this type of testing, tester plays a role of the attacker and play a person to find security-related bugs. Security Testing is very important in Software Engineering to protect data by all means.

Prev
Report a Bug
Next

YOU MIGHT LIKE:

SOFTWARE TESTING
What is Regression Testing? Definition, Test Cases (Example)
What is Regression Testing? REGRESSION TESTING is defined as a type of software testing to confirm...
Read more »

SOFTWARE TESTING
Do Testers have to Write Code?
A very common question that a software Testing aspirant has is... Do testers have to write code??...
Read more »

SOFTWARE TESTING
What is SDET? Full Form, Meaning, Role and Responsibilities
SDET SDET (Software Development Engineer in Test) in testing is an IT professional who can work equally...
Read more »

SOFTWARE TESTING
What is Interface Testing? Types & Example
What is Interface Testing? Interface Testing is defined as a software testing type which verifies...
Read more »

SOFTWARE TESTING
20 Best Bug Tracking Tools (Defect Tracking Tools) in 2021
(loadpositon top-ads-automation-testing-tools) A bug tracking tool can help record, report,...
Read more »

SOFTWARE TESTING
7 Principles of Software Testing: Learn with Examples
This tutorial introduces the seven basic Software Testing Principles that every Software tester...
Read more »

Testing Tutorials
REST Client Testing
REST Assured
Security Testing
GUI Testing
Testing Methodology