ISSN: 2454-4248
04 – 07

Analysis of Different Software Security Testing Techniques, Benefits, Challenges and Life Cycle

Dr. Satpal Singh
Assistant Professor
Punjabi University Patiala, India
satpal.singh@pbi.ac.in

Abstract: - Security testing is the software testing technique which makes sure that the system or application software which is developed is free from security threats and cannot be hacked by the hacker. Once an application or software us developed, once the final product is tested for all its functions, components etc it is also important to test for its privacy and security. If the system is not secure enough, then it can easily be attacked and hacked and all the sensitive data and information will be exploited by the hacker and use them in their favour. There are variety of security testing which will be discussed in this paper. The security testing has few requirements like testing the integrity, confidentiality, authorisation, availability etc. The security elements of the system depend upon the security features being implemented in the system so the testing process will also be different for each system. The various techniques and approaches can be explained by Security taxonomy. The paper will discuss elements of security testing, methodologies, pros and cons of security testing, etc.

***Keywords:* -** Security testing, Techniques of Security testing, Advantages of security testing, Challenges of security testing, Elements of security testing, Life cycle of security testing.

*****

Introduction: -

There are few stages of the software development life cycle for any project. A software development or application development goes through various stages like requirement gathering and documentation, design phase, coding phase, testing phase, and finally implementation and maintenance phase. Each step is carried out cautiously and one after the other. The output of one stage serves as the input for the other stage. Therefore, it is necessary that each phase should be completed carefully with the help of skilled professionals. Testing is also one of the important stages of the SDLC cycle. It is done thoroughly before delivering the final product to the end sure. It is carried out to validate that the final product is working as per the user requirements. In testing phase various functionality is tested for the system like performance of the system, unit testing, integration testing, security testing etc. Security testing is done to make sure that security attacks from hackers are prevented and to identify the risks and threats for the system. It is important to perform security testing of the system as it contains critical and sensitive personnel data and information which could be at risk to be attacked or hijacked by the cyber-attack. The objective of security testing is to find out all the possible loopholes and weakness of the system which could be at risk to get attacked. Security attack might result in loss of revenue, important information, etc. It also helps to identify possible vulnerabilities so that the system does not stops functioning or cannot be exploited by the hackers. Once all the loopholes are identified by the testers, the code is fixed with the help of developers. They will use enhanced algorithms and try to implement efficient security protocols which will help to increase the security of the system. For each system, security elements will be different and hence the type of security testing will also be different. Following are few security elements which should be kept in mind to perform the security testing of the application or software: - [1]

1. Availability: -
    - It is to make sure that data and information will be available to the authorised users whenever they need it.
    - To make sure that all the services used for communication and information will be made available whenever it is expected to be available for use.

2. Authentication: -
    - It is used to check the authentication use of the application It is to make sure that only it is used by authorised user.
    - It is to make sure that the user has authorised identity, it is also responsible to trace the origin of the artifact, and also to make sure that the computer has trusted programs.

3. Authorisation: -
    - The aim of this element is to make sure that the request generated by the user or the requestor is a genuine request and it is allowed to be used by the user.

- For example, access control could be an example of authorisation where access can be given to only authorised users of that particular service.

4. Integrity: -
   - The goal of this element is to make sure that modifications could never be done by unauthorised user.
   - It is also used to make sure that correct data is transferred between the two applications.

5. Confidentiality: -
   - A safety effort which safeguards against the revelation of data to parties other than the planned beneficiary is in no way, shape or form the main approach to guaranteeing the security.

6. Non-disavowal: -
   - It is used in digital security to make sure that the sender has sent the message and the receiver has received the message. In both cases, the sender as well as receiver can never deny that they have sent and received the message.

Life cycle of Security testing: - [2]

It is very important to include security testing in each phase of the software development life cycle which will make sure that there is no loophole left in any component of the software being developed. Each phase will have corresponding security testing phase and it will be conducted simultaneously along with the development of the software. Following are the stages: -

1. Requirement gathering : Security analysis
2. Designing: - Security test plan
3. Coding and unit testing: Security white box testing
4. Integration testing: Black box testing
5. System Testing: Vulnerability testing
6. Implementation: Penetration testing

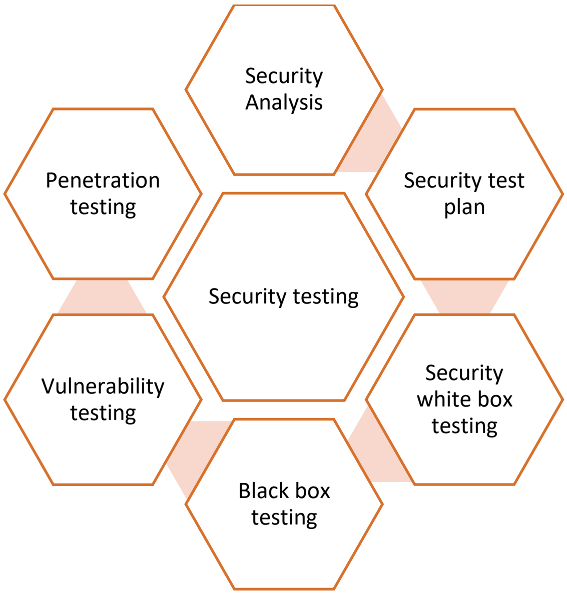

Figure 1. Various phases of Security testing.

1. Security Analysis: -
   This security analysis is conducted during first stage which is information gathering. Once all the information is gathered and documented, then it is used for analyses of security in terms of any misuse of cases.
2. Security test Plan: -
   Once all the requirements of the user are documented, then designing of the system starts in second stage where it is also important to perform Security test plan. The security test plan contains following elements: -
   - Security-related experiments or situations.
   - Test Data connected with security testing.
   - Test Tools expected for security testing.
   - Examination of different tests yields from various security apparatus.

3. Security White box testing: -
   - The coding and unit testing stage of SDLC is related to the conversion of designing into coding and then testing for its functionality. In this phase, to make sure the security of the system is ensured, security white box testing is performed. This is used to test the internal structure of the system being coded is secure. This will also test the internal design, code structure and working of the software..

4. Security Black box testing: -
   - Once all the components of the software are developed, it is integrated into one single unit and then tested whether it is working as per the desired expectations. To make sure the security of the system, black box testing is conducted in this phase.
   - Black box security tests are led to recognize and determine potential security weaknesses before

arrangement or to intermittently distinguish and determine security issues inside sent frameworks.

5. Vulnerability testing: -

- This is conducted during the system testing of the system developed. Once the system is ready it is tested for its functionality, and the final product is as per expectations or not. T
- his is done before delivering the final product to the end user. In the same phase, the system is tested for all the possible risks and threats related to its security.
    - For this the system is tested for possible vulnerable points from where it could be attacked. Once these loopholes are identified, the code is made more secure with the help of the coders of the system.

6. Penetration testing: -

- Once software is ready it is delivered to the end user for use. Entrance Testing or Pen Testing is a kind of Security Testing used to cover weaknesses, dangers and dangers that an aggressor could take advantage of in programming applications, organizations or web applications.
- The motivation behind entrance testing is to recognize and test all conceivable security weaknesses that are available in the product application.

Security testing techniques: - [3]

There are following 7 main variety of security testing: -

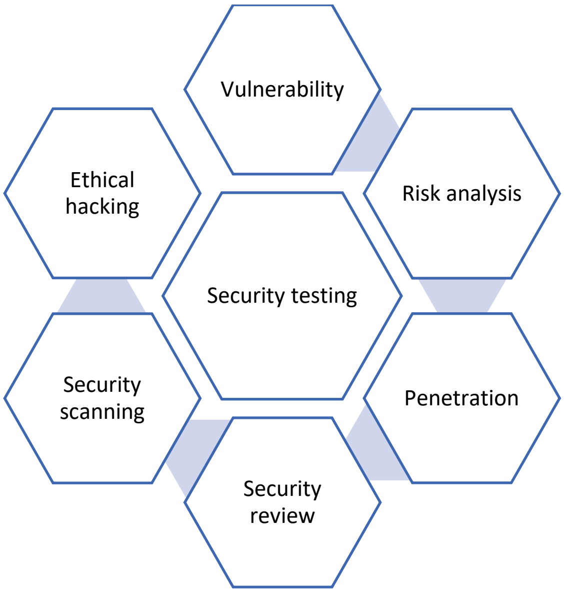

Figure 2 Types of Security testing.

1. Vulnerability testing: - It is used to identify the major vulnerable points for threat and attacks by the intruder. It is the first step in the security testing of any software or application.
2. Penetration testing: - It is used to test the security strength of the software by making an attack by an expert engineer to test for its capability to tolerate the attack. It is used to test whether if in real there is attack by an intruder, then the system is able to identify and report that attack or not.
3. Security scanning: - Security examining is the most common way of recognizing weaknesses and misconfigurations in the application/programming, organization, and frameworks. Both manual and robotized apparatuses are utilized for this test type. The experiences from these tests are recorded, broke down top to bottom, and arrangements gave to fix the issue.
4. Ethical Hacking: - This is also similar to penetration testing, in this type of security testing, various cyber like attacks will be conducted on the system in a simulator environment to test the tolerance of the system to deal with the cyber-attacks in real.
5. Risk Analysis: - All the risks related to network, security, application etc are identified and then categorised into high, medium, low. Once it is labelled then the measures will be taken based upon the priority of the risks.
6. Security review and audit: - It is a structured way of identifying and test whether all the security standards are implemented using the documented standards of the software.

Advantages of security testing: - [4]

Following are few benefits of performing security testing of the application or software: -

1. Reduced cost: - It helps to reduce the cost of the testing process. As if after delivering the software, there are issues identified by the customer then the testing and fixing of the issues will be more costly as compared to the security testing being conducting simultaneously during the development of the software.
2. Time and effort: - Since the issues are identified during the development phase only, then it will be easy for the developers to identify then in the code and fix them. This saves a lot of time and efforts as the developers are aware of the code and are able to fix the issues as soon as they are located and identified.
3. Insurance from outer assaults: - Security testing lessens the gamble of assaults by showing every one of the blunders during the testing system. With the development of innovation, the security of the application is similarly significant. It becomes required in the event that there is any course of exchange and clients' very own information.

4. Enhanced quality of the delivered software: - The security testing make sure that the quality of the final product is efficient and improved due to the fact that the testers reports bugs and developers fixes them then and there only.

Challenges of Security testing: - [5]

Following are few challenges of security testing: -

1. Code vulnerability: - Due to the weakness and vulnerability of programming languages, the security of the application will still be at risk.
2. Open-source components: - Utilizing open-source parts with no/little discernment about inner understanding of the parts might prompt weaknesses, undesirable intricacy, what's more, irregularities in the general item.
3. Lack of planning: - The improper planning of the development of the software leads to many vulnerabilities and security threats to the system.
4. Speed issue: - If the development of the software is done very fast by not keeping in mind various security protocol then for sure the system will have many entry points which can be easily attacked by the intruders.

Conclusion: - Security testing is the product testing method which ensures that the framework or application programming which is created is liberated from security dangers and can't be hacked by the programmer. When an application or programming us grew, when the eventual outcome is tried for every one of its capabilities, parts and so on it means quite a bit to test for its protection and security. On the off chance that the framework isn't adequately secure, then, at that point, it can without much of a stretch be gone after and hacked and every one of the delicate information and data will be taken advantage of by the programmer and use them in support of themselves. There are assortment of safety testing which will be talked about in this paper. The security testing has not many necessities like testing the trustworthiness, classification, authorisation, accessibility and so on. The security components of the framework rely on the security highlights being executed in the framework so the testing system will likewise be different for every framework. The different strategies and approaches can be made sense of by Security scientific classification.

References: -

[1]. https://en.wikipedia.org/wiki/Security_testing#:~:text.
[2]. https://www.guru99.com/what-is-security-testing.html#3.
[3]. https://www.indusface.com/blog/attributes-and-types-of-security-testing/
[4]. https://www.qable.io/7-benefits-of-security-testing-in-software-development-life-cycle-sdlc/
[5]. https://www.360logica.com/blog/major-challenges-faced-by-testers-while-performing-security-testing/