Software Testing Methodologies for Finding Errors

Khawar Iqbal Malik, Hina Khalid, Sidra Hassan, Kalsum Fatima
Students of MSCS, Department of Computer Sciences,
University of Lahore, Sargodha Campus-Pakistan

Abstract

Software testing is an action which is intended for estimating an attribute or competence of a program and guarantee that it convenes the desired result. There are many techniques to software testing, but efficient testing of difficult product is fundamentally a process of study, not simply a matter of creating and following itinerary methods. It is often impractical to locate all the errors and problems in the program. This basic problem in testing thus put open issue, as to what would be the policy that we should accept for testing. Thus, the choice of right approach at the right time will formulate the software testing proficient and useful. In this paper we have illustrated software testing methodologies which are classified by principle.

Keywords: Correctness Testing, Performance Testing, Reliability Testing, Security Testing

1- Introduction

Software testing is a collection of actions carry out with the aim of locating errors in software. It also validates and authenticate whether the program is functioning properly with no errors or not. It evaluates the software for verdict errors.

Software testing is not only used for locating and repairing of errors but it also guarantees that the system works according to client satisfaction. Software testing is a chain of method which is intended to confirm that the computer code or program should perform what it was planned to do. Software testing is a critical process to locate errors. The key function of testing can be quality assurance, reliability estimation, validation or verification. The other objectives or software testing includes. [6][7][8]

- The better it workings the more professionally it could be checked.
- As much the software controlled more the testing could be programmed and optimized
- As much fewer the alteration, the fewer the troubles to testing
- A successful test is the one that expose a concealed error.
- Testing is a method to recognize the accuracy of software.
- The common purpose of software testing is to establish the quality of software system by methodically implementing the software in cautiously controlled situations.

Classified by purpose software testing can be divided into [4]
1. Correctness Testing
2. Performance Testing
3. Reliability Testing
4. Security Testing

2- Software Testing Techniques

Software testing is a technique which is used to evaluate the quality of software developed. It is also a method of locating errors in software and makes it a possible task. It is functional procedure of
running program with the aim of locating errors. The diagram signifies some of the most common practices of software testing which are classified by purpose. [4]

![Diagram of software testing techniques](image)

**Fig. 1** signify different software testing techniques which are classified by purpose

### 2.1 Correctness Testing

The most important reason of testing is accuracy and correctness which is also the minimum obligation of software. Accuracy of testing tells the right performance of system from the incorrect one for which it will need some type of vision. Either a white box point of view or black box point of view can be taken in testing software as a tester may or may not know the inside detail of the software module under test. For e.g. Data flow, Control flow etc. The ideas of white box, black box or grey box testing are not limited to correctness testing only. [4]

![Diagram of correctness testing](image)

**Fig. 2** Represent various form of correctness testing
2.1.1 White Box Testing

White box testing provides a study of inside working and construction of a piece of software. White box testing is the method of giving the input to the system and examining how the system processes that input to produce the desire output. It is compulsory for a tester to have the full information of the source code. White box testing is appropriate at integration, unit and system levels of the software testing process. In white box testing one can be sure that all parts through the test objects are properly executed. [2][10]

![Fig. 3 Represent working process of White Box Testing](image)

Some synonyms of white box testing are [5]
- Logic Driven Testing
- Design Based Testing
- Open Box Testing
- Transparent Box Testing
- Clear Box Testing
- Glass Box Testing
- Structural Testing

Some important types of white box testing techniques are:
- Control Flow Testing
- Branch Testing
- Path Testing
- Data flow Testing
- Loop Testing

There are some advantages & disadvantages of white box testing -

**Advantages**
1. Side effects are useful.
2. Bugs in hidden codes are exposed.
3. Estimated the division done by execution uniformity.
4. Developer carefully gives reason about implementation.

**Disadvantages**
1. It is very costly.
2. Missed out the cases not available in the code.

2.1.2 Black Box Testing

Principally Black box testing is a primary part of ‘Correctness testing’ but its thoughts are not limited to correctness testing only. Correctness testing is a technique which is classified by reason in software testing.

Black box testing provides the study of the provision of a piece of software without reference to its internal working. The objective is to test how well the module matches to the published requirement for the unit. Black box testing have no concern the internal logical arrangement of the system, it only check the basic feature of the system. It certain that input is correctly accepted and output is properly formed. Other types of Black box testing methods includes graph based testing method, equivalence partitioning, boundary value analysis, comparison testing, orthogonal array testing, specialized testing, fuzz testing, and traceability metrics. [2]
Advantages
1. Black box tester has no “bond” with the code.
2. Tester perspicacity is very simple.
3. Programmer and tester both are independent of each other.
4. More efficient on larger component than clear box testing.

Disadvantages
1. Test cases are difficult to intend without clear provision.
2. Only small numbers of possible input can actually be tested.

2.1.3 Grey Box Testing

Grey box testing techniques combination of two previous techniques i.e white box and black box. Grey box testing method is used for testing a piece of software against its condition but using some knowledge of its internal working as well. [2] Grey box testing may also include reverse engineering to conclude, for instance, boundary values or error messages. Grey box testing is methods which occupy testing software while already include some knowledge of its highlight code or logic. The understanding of internals of the program in grey box testing is more than black box testing, but less than clear box testing. [11]

2.2 Performance Testing

‘Performance Testing’ include all the different phases as the conventional testing life cycle as a sovereign discipline which involve approach such as plan, design, execution, analysis and reporting. This testing is performed to estimate the conformity of a system or module with specified performance requirement. [2] Estimation of a performance of any software system contains resource usage, throughput and stimulus response time.

By performance testing we can measure the distinctiveness of performance of any software. One of the most important objectives of performance testing is to maintain a low latency of a website, high throughput and low utilization. [5]

Some of the main goals of performance testing are: [5]
- Measuring response time of end to end transactions.
- Measurement of the delay of network between client and server.
- Monitoring of system resources which are under various loads.

Some of the common mistakes which happen during performance testing are: [5]
- Ignoring of errors in input.
- Analysis is too complex.
- Erroneous analysis.
- Level of details is inappropriate.
- Ignore significant factors.
- Incorrect Performance matrix.
- Important parameter is overlooked.
- Approach is not systematic.

There are seven different phases in performance testing process: [5]

Phase 1 – Requirement Study
Phase 2 – Test plan
Phase 3 – Test Design
Phase 4 – Scripting
Phase 5 – Test Execution
Phase 6 – Phase
Phase 7 -Preparation of Report  Test Analysis

There are two kinds of performance testing:

2.2.1 Load Testing
Load Testing is a term for the attempt of performance testing. The main feature of the load testing is to establish whether the certain system is able to knob the predictable no. of users or not. This can be done by making the effective user to display as real user so that it will be easy to achieve load testing. It is conceded only to check whether the system is performing well or not. The main objective of load testing is to check whether the system can perform well for specified user or not. Load testing is also used for checking an application against heavy load or inputs such as testing of website in order to find out at what point the website or applications fails or at what point its performance degrades. [2][5]

Two ways for implementing load testing are
1. Manual Testing: It is not a very practical option as it is very iterative in nature and it involves [5]
   ➢ Measure response time
   ➢ Compare results
2. Automated Testing: As compared to manual load testing the automated load testing tools provide more efficient and cost effective solution. Because with automated load testing, tools test can easily be rerun any number of times and decreases the chances of human error during testing. [5]

2.2.2 Stress Testing
We can identify stress testing as performing random operational sequence, at larger than normal volume, at faster than normal speed and for longer than normal periods of time, as a method to pick up the pace the rate of finding errors and verify the strength of our product, or we can say this is a testing, which is accomplish to estimate a system or module at or beyond the limits of its particular requirements to establish the load under which it fails and how. Stress testing also establishes the performance of the system as user base raise. In stress testing the application is tested against heavy loads such as large no. of inputs, large no. of queries, etc. [2] [5]

There are some weak and strong points of stress testing.
Weak Points
1. Defects are reproducible
2. Not able to test the correctness of a system.
3. Not representing real world situation.
Strong Points
1. Very helpful in finding deadlocks.
2. No other type of test can find defect as stress testing.
3. Robustness of application is tested.

2.3 Reliability Testing

Fig. 5 Represent Reliability testing
‘Reliability Testing’ is very important, as it determine all the crashes of a system and eliminate them before the system is installed. Reliability testing is associated to many feature of software in which testing procedure is incorporated; this testing procedure is an effective variety method to measure software reliability. Estimation model is prepared in reliability testing which is used to analyze the data to guesstimate the present and foresee future reliability of software. [4][2]

According to estimation, the developers can chose whether to release the software or not and the end user will decide whether to accept that software or not.

Based on reliability information, the hazard of using software can also be evaluated. Robustness testing and stress testing are the variances of reliability testing. By Robustness we mean how software component works under stressful environmental conditions. Robustness testing only watches the robustness problem such as machine crashes, abnormal terminations etc. Robustness testing is very portable and scalable. [4]

2.4 Security Testing
Security Testing: ‘Security testing’ assures that only the allowed personnel can have right of entry the program and only the certified personnel can access the functions accessible to their security level. Security testing of any developed or underdeveloped system is all about locating the major ambiguities and weaknesses of a system which can damage to the system by an authorized user. [1][2]

Security testing is very supportive for the tester for locating and removing of problems. It guarantees that the system will execute for a long time without any issue. It also guarantees that the systems used by any clients are safe from any illegal attack. In this way, security testing is beneficial for the organization in all aspects. [1][2]

Five major concepts which are covered by security testing are

Confidentiality: no expose of the information to the unknown party other than projected beneficiary.

Integrity: Here we will retain the reliability of the system by permit the receiver to decide that the information which he is obtaining is right.

Authentication: It keep the authentications of the system and WPA, WPA2, WEP are several forms of authentication.

Availability: Information should be available to authenticated person when and where is required.

Authorization: Security testing ensures that only the authorized user can access the information or particular service. Access control is an example of authorization.

Different types of security testing in any organization are as follows: [3]
1. Security Auditing and Scanning: Security Auditing includes direct examination of the operating system and of the system on which it is developed. In Security Scanning the auditor scan the operating system and then tries to find out the weaknesses in the operating and network.
2. Vulnerability Scanning: Various vulnerability scanning software performs Vulnerability Scanning, which involves the scanning of the program for all known vulnerability.
3. Risk Assessment: Risk Assessment is a method in which the auditors analyze the risk involved with any system and all the probability of loss which occurs because of that risk. It is analyzed through interviews, discussions, etc.
Fig. 6 Represent various type of security testing

4. Posture Assessment and Security Testing: Posture Assessment and Security Testing help the organization to know where it stands in context of security by combining the features of security scanning, risk assessment and ethical hacking.

5. Penetration Testing: Penetration Testing is an effective way to find out the potential loopholes in system and it is done by a tester which forcibly enters into the application under test. A tester enters into the system with the help of combination of loopholes that the application has kept open unknowingly.

6. Ethical Hacking: Ethical Hacking involves large no. of penetration test on a system under test. To stop the forced entry of any external elements into a system this is under security.

3. Conclusion

Software testing is an important procedure for the perfection and extent of a software system quality. But it is actually not possible to find out all the errors in the program. So, the fundamental question arises, which technique we adopt to test. In our paper, we have expressed some of the most common and frequently used approach of software testing which are classified by purpose and they are classified into [5]

1. Correctness testing, which is used to test the right performance of the system and it is additionally separated into black box, white box and grey box testing techniques (combines the features of black box and white box testing).

2. Performance testing, which is a separate restraint and entail all the phases as the main stream testing life cycle i.e. strategy, plan, design, execution, analysis and reporting. Performance testing is further divided into load testing and stress testing.

3. Reliability testing, which evolve all the collapse of the system and eliminate them prior to the system installed?
4. Security testing persuaded that only the allowed personnel have right of entry the system and is further separated into Security Auditing and Scanning, Vulnerability Scanning, Risk Assessment, Posture Assessment and Security Testing, Penetration Testing and Ethical Hacking. The successful use of these techniques in industrial software development will validate the results of the research and drive future research. [8]

References:

[3] Open source security testing methodology manual of PETE HERZOG and the institute for security and open methodology-ISECOM.
[10] White box testing from Wikipedia, the free encyclopedia.