

Different Forms of Software Testing Techniques for Finding Errors

Mohd. Ehmer Khan

Department of Information Technology
Al Musanna College of Technology, Sultanate of Oman

Abstract

Software testing is an activity which is aimed for evaluating an attribute or capability of a program and ensures that it meets the required result. There are many approaches to software testing, but effective testing of complex product is essentially a process of investigation, not merely a matter of creating and following route procedure. It is often impossible to find all the errors in the program. This fundamental problem in testing thus throws open question, as to what would be the strategy that we should adopt for testing. Thus, the selection of right strategy at the right time will make the software testing efficient and effective. In this paper I have described software testing techniques which are classified by purpose.

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

1. Introduction

Software testing is a set of activities conducted with the intent of finding errors in software. It also verifies and validate whether the program is working correctly with no bugs or not. It analyzes the software for finding bugs. Software testing is not just used for finding and fixing of bugs but it also ensures that the system is working according to the specifications. Software testing is a series of process which is designed to make sure that the computer code does what it was designed to do. Software testing is a destructive process of trying to find the errors. The main purpose of testing can be quality assurance, reliability estimation, validation or verification. The other objectives or software testing includes. [6][7][8]

- The better it works the more efficiently it can be tested.
- Better the software can be controlled more the testing can be automated and optimized.
- The fewer the changes, the fewer the disruption to testing.
- A successful test is the one that uncovers an undiscovered error.

- Testing is a process to identify the correctness and completeness of the software.
- The general objective of software testing is to affirm the quality of software system by systematically exercising the software in carefully controlled circumstances.

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 process which is used to measure the quality of software developed. It is also a process of uncovering errors in a program and makes it a feasible task. It is useful process of executing program with the intent of finding bugs. The diagram below represents some of the most prevalent techniques of software testing which are classified by purpose. [4]

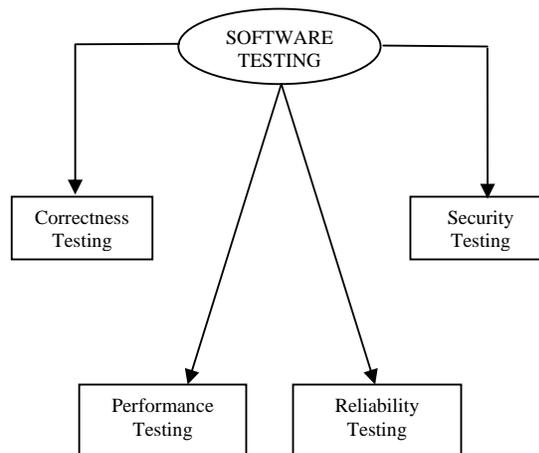


Fig. 1 Represent different software testing techniques which are classified by purpose

2.1 Correctness Testing

The most essential purpose of testing is correctness which is also the minimum requirement of software. Correctness testing tells the right behavior of system from the wrong one for which it will need some type of Oracle. 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]

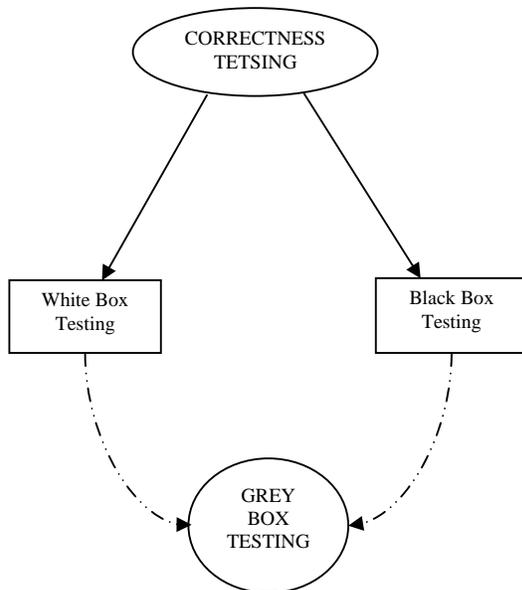


Fig. 2 Represent various form of correctness testing

2.1.1 White Box Testing

White box testing based on an analysis of internal working and structure of a piece of software. White box testing is the process of giving the input to the system and checking how the system processes that input to generate the required output. It is necessary for a tester to have the full knowledge of the source code. White box testing is applicable 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

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:

1. Control Flow Testing
2. Branch Testing
3. Path Testing
4. Data flow Testing
5. Loop Testing

There are some pros & cons of white box testing-

Pros-

1. Side effects are beneficial.
2. Errors in hidden codes are revealed.
3. Approximate the partitioning done by execution equivalence.
4. Developer carefully gives reason about implementation.

Cons-

1. It is very expensive.
2. Missed out the cases omitted in the code.

2.1.2 Black Box Testing

Basically Black box testing is an integral part of 'Correctness testing' but its ideas are not limited to correctness testing only. Correctness testing is a method which is classified by purpose in software testing.

Black box testing is based on the analysis of the specifications of a piece of software without reference to its internal working. The goal is to test how well the component conforms to the published requirement for the component. Black box testing have little or no regard to the internal logical structure of the system, it only examines the fundamental aspect of the system. It makes sure that input is properly accepted and output is correctly produced. In black box testing, the integrity of external information is maintained. The black box testing methods in which user involvement is not required are functional testing, stress testing, load testing, ad-hoc testing, exploratory testing, usability testing, smoke testing, recovery testing and volume testing, and the black box testing techniques where user involvement is required are user acceptance testing,

alpha testing and beta testing. 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]



Fig. 4 Represent working process of Black Box Testing

There are various pros and cons of black box testing- [5]

Pros-

1. Black box tester has no “bond” with the code.
2. Tester perception is very simple.
3. Programmer and tester both are independent of each other.
4. More effective on larger units of code than clear box testing.

Cons-

1. Test cases are hard to design without clear specifications.
2. Only small numbers of possible input can actually be tested.
3. Some parts of the back end are not tested at all.

2.1.3 Grey Box Testing

Grey box testing techniques combined the testing methodology of white box and black box. Grey box testing technique is used for testing a piece of software against its specifications but using some knowledge of its internal working as well. [2]

Grey box testing may also include reverse engineering to determine, for instance, boundary values or error messages. Grey box testing is a process which involves testing software while already having some knowledge of its underline 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' involve all the phases as the mainstream testing life cycle as an independent discipline which involve strategy such as plan, design,

execution, analysis and reporting. This testing is conducted to evaluate the compliance of a system or component with specified performance requirement. [2] Evaluation of a performance of any software system includes resource usage, throughput and stimulus response time.

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

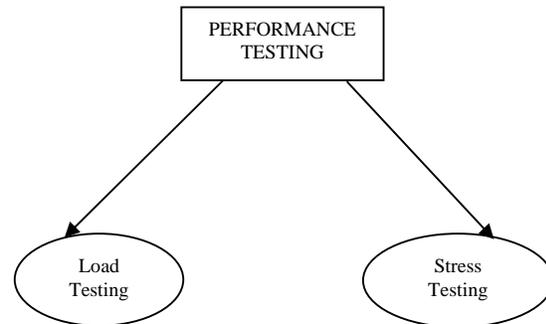


Fig. 5 Represent two types of performance testing

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 – Test Analysis

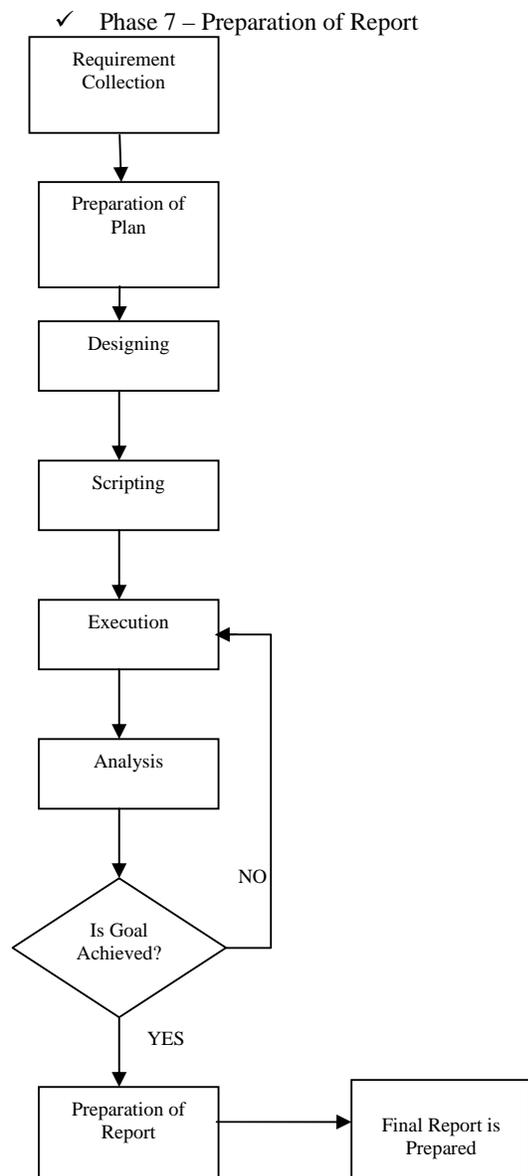


Fig. 6 Represent Performance Testing Process

Typically to debug applications, developers would execute their applications using different execution stream. Which are completely exercised the applications in an attempt to find errors. Performance testing is secondary issue when looking for errors in the applications but, however, it is still an issue.

There are two kinds of performance testing:

2.2.1 Load Testing

Load Testing is an industry term for the effort of performance testing. The main feature of the load testing is to determine whether the given system is able to

handle the anticipated no. of users or not. This can be done by making the virtual user to exhibit as real user so that it will be easy to perform load testing. It is carried 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 increases the up time for critical web applications by helping us to spot the bottle necks in the system which is under large user stress.

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 solutions. 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 define 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 accelerate the rate of finding defects and verify the robustness of our product, or we can say stress testing is a testing, which is conducted to evaluate a system or component at or beyond the limits of its specified requirements to determine the load under which it fails and how. Stress testing also determines the behaviour of the system as user base increases. 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. Not able to test the correctness of a system.
2. Defects are reproducible.
3. Not representing real world situation.

Strong Points

1. No other type of test can find defect as stress testing.
2. Robustness of application is tested.

3. Very helpful in finding deadlocks.

2.3 Reliability Testing

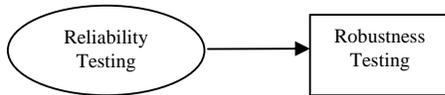


Fig. 7 Represent Reliability testing

'Reliability Testing' is very important, as it discover all the failures of a system and removes them before the system is deployed. Reliability testing is related to many aspects of software in which testing process is included; this testing process is an effective sampling method to measure software reliability. Estimation model is prepared in reliability testing which is used to analyze the data to estimate the present and predict future reliability of software. [4][2]

Depending on that estimation, the developers can decide whether to release the software or not and the end user will decide whether to adopt that software or not.

Based on reliability information, the risk of using software can also be assessed. 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' makes sure that only the authorized personnel can access the program and only the authorized personnel can access the functions available to their security level. Security testing of any developed system or (system under development) is all about finding the major loopholes and weaknesses of a system which can cause major harm to the system by an authorized user. [1][2]

Security testing is very helpful for the tester for finding and fixing of problems. It ensures that the system will run for a long time without any major problem. It also ensures that the systems used by any organization are secured from any unauthorized 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: By security testing, we will ensure the confidentiality of the system i.e. no disclosure of the information to the unknown party other than intended recipient.
- Integrity: By security testing, we will maintain the integrity of the system by allowing the receiver to determine that the information which he is getting is correct.
- Authentication: Security testing maintains the authentications of the system and WPA, WPA2, WEP are several forms of authentication.
- Availability: Information is always kept available for the authorized personnel whenever they needed and assures that information services will be ready for use whenever expected.
- Authorization: Security testing ensures that only the authorized user can access the information or particular service. Access control is an example of authorization.

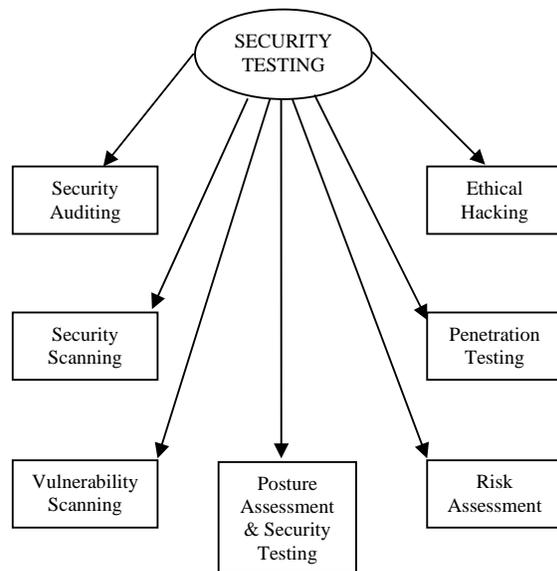


Fig. 8 Represent various type of security testing

Different types of security testing in any organization are as follows: [3]

1. Security Auditing and Scanning: Security Auditing includes direct inspection 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.
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 which is under security testing.

3. Conclusion

Software testing is an important technique for the improvement and measurement of a software system quality. But it is really not possible to find out all the errors in the program. So, the fundamental question arises, which strategy we would adopt to test. In my paper, I have described some of the most prevalent and commonly used strategies of software testing which are classified by purpose and they are classified into [5]

1. Correctness testing, which is used to test the right behavior of the system and it is further divided 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 an independent discipline and involves 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 discovers all the failure of the system and removes them before the system deployed.
4. Security testing makes sure that only the authorized personnel can access the system and is further divided 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:

- [1] Software testing-Brief introduction to security testing by Nilesh Parekh published on 14-07-2006 available at <http://www.buzzle.com/editorial/7-14-2006-102344.asp>
- [2] Software testing glossary available at http://www.aptest.com/glossary.html#performance_testing
- [3] Open source security testing methodology manual of PETE HERZOG and the institute for security and open methodology-ISECOM.
- [4] Software testing by Jiantao Pan available at http://www.ece.cmu.edu/~roopman/des-899/sw_testing/
- [5] Software Testing by Cognizant Technology Solution.
- [6] Introduction to software testing available at <http://www.onestoptesting.com/introduction/>
- [7] Software testing techniques available at <http://pesona.mmu.edu.my/~wruslan/SE3/Readings/GB1/pdf/ch14-GB1>
- [8] Paper by Lu Luo available at <http://www.cs.cmu.edu/~luluo/Courses/17939Report.pdf>
- [9] Security testing-wikipedia the free encyclopedia available at <http://en.wikipedia.org/wiki/security-testing>.
- [10] White box testing from wikipedia, the free encyclopedia.
- [11] Software testing for wikipedia available at http://en.wikipedia.org/wiki/grey_box_testing#grey_box_testing

Mohd. Ehmer Khan

I completed my B.Sc in 1997 and M.C.A. in 2001 from Aligarh Muslim University, Aligarh, India, and pursuing Ph.D (Computer Science) from Singhania University, Jhunjhunu, India. I have worked as a lecturer at Aligarh College Engineering & Management, Aligarh, India from 1999 to 2003. From 2003 to 2005 worked as a lecturer at Institute of Foreign Trade & Management, Moradabad, India. From 2006 to present working as a lecturer in the Department of Information Technology, Al Musanna College of Technology, Ministry of Manpower, Sultanate of Oman. I am recipient of PG Merit Scholarship in MCA. My research area is software engineering with special interest in driving and monitoring program executions to find bugs, using various software testing techniques.