GSJ: Volume 10, Issue 12, December 2022
ISSN 2320-9186

Global Scientific JOURNALS

GSJ: Volume 10, Issue 12, December 2022, Online: ISSN 2320-9186
www.globalscientificjournal.com

SECURITY TESTING TYPES FOR SOFTWARE TOOLS

Afsheen Gull

Department of Computer Science & Information Technology, Univerity of Engineering & Techology Peshawar, Pakistan
Email: afshegul@gmail.com

KeyWords
Security; Assets; Classifications; web-based systems; Information Technology; Hacking; Protection.

ABSTRACT

Software systems have become the necessity of most of the organizations and testing their security and integrity has become crucial. However, attacks on the online systems have been increased over the last decades. This research caters to these aspects with the objectives to determine and evaluate the security testing techniques for different test cases and test strategies in testing security of software systems and the security vulnerabilities which exist in those systems.

GSJ: Volume 10, Issue 12, December 2022
ISSN 2320-9186

INTRODUCTION

Attacks on online systems have increased significantly over the last few years. This is evident from the list of most successful companies in the world i.e. most of them are related to 'IT' and 'IS' [1]. With the digital transformation of businesses, there comes a need for the integrated securities of the business because the businesses related to IT and IS are vulnerable to security threats. The companies have to devise and implement security systems for their 'IT' and 'IS' infrastructure [2]. These infrastructures consist of various hardware systems and software systems. While developing software to run the hardware or manage any other business activity, the developers in this technological era have to cater to the security requirements of the software systems to avoid vulnerabilities and threats [3]. The problem regarding the software security testing is the selection, design and implementation of the testing technique that is most suitable and cost effective.

LITERATURE REVIEW

Due to increase in website application security issues, security testing is becoming important and critical activity of web application development. Purpose of security testing is to provide the confidentiality of the data, to check about the data leakage and maintain the functionality as intended [4]. It checks whether the security requirements are fulfilled by the web applications when they are subject to malicious input data [5]. Due to the rising explosion in the security vulnerabilities, there occurs a need to understand its unique challenges and issues which will eventually serve as a useful input for the security testing tool developers and test managers for their relative projects [6].

Software Security Testing

Software security testing is a process of determining on regular basis the potential of installed programs to safeguard data and maintain the functionality of business information systems by averting the vulnerabilities and threats [7].

The services under software security testing help in several ways:

- Identification of errors, threats and vulnerabilities that are not otherwise visible during code reviews
- Discover security issues that exist out of boundary or results from incorrect development of products
- Constant risk analysis at all levels of software from design level to the implementation and operation phase
- Proactive approach of designing by simulating different types of intruder and understanding the attackers' approaches

As shown in Figure 1, following are the types of software security testing.

1. *Formal Security Testing*
2. *Model based Security Testing*
3. *Fault Injection based Security Testing*

GSJ: Volume 10, Issue 12, December 2022
ISSN 2320-9186

4. *Fuzzy Testing*
5. *Vulnerability Scanning Testing*
6. *Property based Testing*
7. *White Box based Security Testing*
8. *Risk based Security Testing*

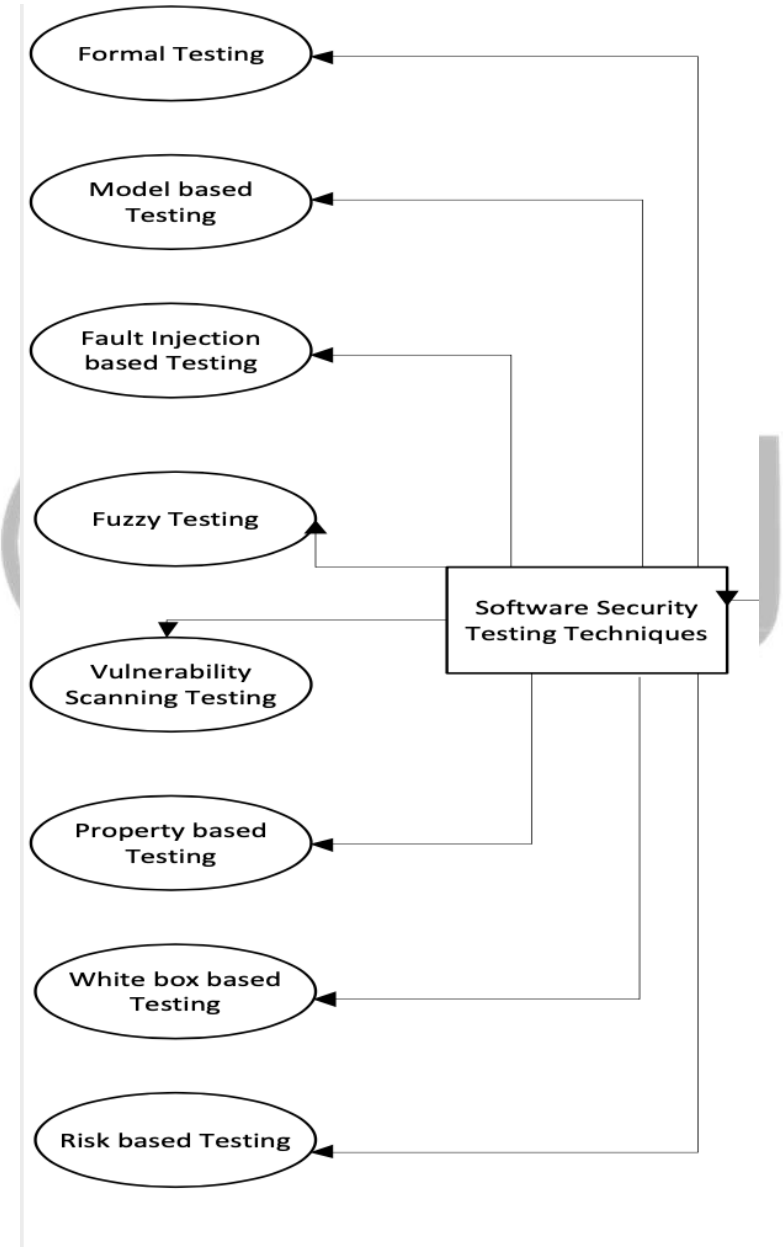

Figure 1: Software Security Testing Types

GSJ: Volume 10, Issue 12, December 2022
ISSN 2320-9186

The details of each type of security testing is as follows:

1. ***Formal Security Testing***

The method completely opens up a software program first, analyzes all its equations and then sets its own mathematical model and formal specifications with own in-coded language [8].

1. ***Model based Security Testing***

On the positive side, model based security testing constructs a security plan depending on the structure and behavior of the software.

1. ***Fault Injection based Security Testing***

This testing method according to the research of focuses on identifying the interaction points of systems and applications such as network interface, file systems, user inputs and other environmental variables.

1. ***Fuzzy Testing***

In order to discover security vulnerabilities in systems, fuzzy testing comes as an effective strategy. In this method, random data is injected into the program to test whether the program can run under clustered environment [9].

1. ***Vulnerability Scanning Testing***

It is one of the important methods to identify the potential security risks reflect from the software. The method involves two schemes; first testing space scanning that deals with procedure data, network data, and string and network port.

1. ***Property based Testing***

Property based testing is a unique security software as it is capable of transforming the security properties of software's into its own specified systems with predefined language such as TASPEC [10]. It instantly discovers the violation that is done by intruders against the code set by this system against its security properties so can successful deals with large inputs of data.

1. ***White Box based Security Testing***

It is static analysis based method and is most widely used in testing the security of the software's and systems. White box based security technique is capable to find security bugs especially buffer overflows which can easily harm the systems [11].

1. ***Risk based Security Testing***

As the name represents, risk based testing is associated with risk analysis for analyzing security concerns that may occur at any part of the software development cycle [27].

GSJ: Volume 10, Issue 12, December 2022
ISSN 2320-9186

Conclusion

In this paper, we have explained various types of testing techniaus that can be used for testing the security of a software system. The need for each type of testing is described. In addition, the advantages and disadvantages of each type of testing is also given. In future, a detailed analysis of each technique on various case studies can be applied.

References

[1] O. Juwita and F. N. Arifin, "Design of information system development strategy based on the conditions of the organization," 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), Kuta Bali, 2017, pp. 1-5, doi: 10.1109/CAIPT.2017.8320732.

[2] A. Yasin, L. Liu, T. Li, R. Fatima and W. Jianmin, "Improving software security awareness using a serious game", IET Software, vol. 13, no. 2, pp. 159-169, 2019. Available: 10.1049/iet-sen.2018.5095 [Accessed 2 September 2020].

[3] A. A. U. Rahman and L. Williams, "Software Security in DevOps: Synthesizing Practitioners' Perceptions and Practices," 2016 IEEE/ACM International Workshop on Continuous Software Evolution and Delivery (CSED), Austin, TX, 2016, pp. 70-76, doi: 10.1109/CSED.2016.021.

[4] S. Rafique, M. Humayun, Z. Gul, A. Abbas and H. Javed, "Systematic Review of Web Application Security Vulnerabilities Detection Methods," Journal of Computer and Communications, vol. 3, p. 28, 2015.

[5] A. Jaiswal, G. Raj and D. Singh, "Security Testing of Web Applications: Issues and Challenges," International Journal of Computer Applications, vol. 88, 1 2014.

[6] G. A. Di Lucca, A. R. Fasolino, F. Faralli and U. De Carlini, "Testing web applications," in International Conference on Software Maintenance, 2002. Proceedings., 2002.

GSJ: Volume 10, Issue 12, December 2022
ISSN 2320-9186
[7] S. de Vries, "Software Testing for security", Network Security, vol. 2007, no. 3, pp. 11-15, 2007

He and Y. Liu, "Research on Software Testing to Ensure Web Application Usability, Reliability and Security", Advanced

[8] Materials Research, vol. 1049-1050, pp. 1972-1976, 2014. Available: 10.4028/www.scientific.net/amr.1049-1050.1972.

[9] Almendros-Jiménez and A. Becerra-Terón, "Automatic property-based testing and path validation of XQuery programs", Software Testing, Verification and Reliability, vol. 27, no. 1-2, p. e1625, 2017 Available: 10.1002/stvr.1625.

[10] "White Box Testing with Object Oriented programming", International Journal of Recent Trends in Engineering and Research, vol. 3, no. 11, pp. 156-160, 2017. Available: 10.23883/ijrter.2017.3505.xkmqq.

[11] Y. Kim and S. Cha, "Threat scenario-based security risk analysis using use case modeling in information systems", Security and Communication Networks, vol. 5, no. 3, pp. 293-300, 2011. Available: 10.1002/sec.321.