IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 8, August 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

Attack System and Vulnerability Discovery in Penetration Testing using SQL Injection

Mahmoud Abedi*, Ali Zaghian

Department of mathematics and cryptography, Malek-Ashtar university of technology, Esfahan, Iran.

*Corresponding author's mail: abedimahmood405@yahoo.com

Abstract: The SQL Injection attack is a popular way of attack in terms of document structure and common threats now a day. There are several ways of attack detection as per our study and also prevention methods had been discussed in several research papers. So the main motivation of our paper to penetrate the attack. One of the hacking technique is commonly occur in banking sector is sql injection. Security testing can be done by two ways i.e static analysis which is otherwise known as white box testing and by dynamic analysis which is known as black box testing.In this paper we have shown the penetration testing of web application to detect the sql injection vulnerability. This paper describes the penetration testing processes and mainly focuses on vulnerability discovery, attack generation and obtain the test cases and maintaining a pentester database which store all the attack responses. We have taken an internet banking transaction case study.

Keywords

SQL injection attack, attack detection, attack prevention, Restricted IP, Testing, Security Testing , Penetration Testing

1. Introduction

There are lot of attacks with different intension can be happen in the internet world. The challenging and most threating attack is SQL Injection attack [1]. In this attack the attacker can gain access the data, by fooling authentication mechanisms, for the purpose of alteration and to execute arbitrary code [2]. There is several methodologies and algorithm are suggested in [3], [4], [5], [6], [7], [8], [9], but there is need of enhancement in the said field. In [10] author suggested that instantaneously a dissonant and host level entry point is fully secured; the depose interface uncovered by a fascination becomes the only source of Feign. SQL Injection Attack can be used by kindred who scarcity to carry out access to the

database and steal, change or delete data for which they do not have permission. In [11] different techniques was proposed to provide a solution for SQLIAs (SQL Injection Attacks), but many of these solutions have limitations that affect their effectiveness and practicability.

Encryption and decryption of the data in the communication channel are also helpful for protecting the data. For encryption and decryption we can use DES, RSA, RC4 and RC5 algorithms [12]. Block based division can be possible with subset superset mining or partitioning techniques [13][14] It is also useful in the scene where the sending data and the wrapper will be different so that confusion will be increases and the security in the receiving side will be more imposed. In cryptography we perform encryption on the original text to create the cipher text and decryption is just an opposite mechanism to form the plaintext. In steganography we hide the original plaintext within any other, text, PDF, images etc. The mechanism of reading the original text will be separately sent to the receiver for data reading. Cryptography is used to change the original plain text to encode or make unreadable form of

text [15]. The excruciating materials are clandestine on the sender comrade in order to have them secluded and spellbound from illicit access and then sent via the network. When the data are received then the opposite process will be employed for decryption depending on an algorithm. Decryption is the process of converting data from encrypted format back to their original format [16][17][18].

In the SQL attack the attacker can apply the insertion or "injection" of either a partial or complete SQL query via the data input or transmitted from the client (browser) to the web application. If it will be successful then insertion in the unauthorized area, deletion, and updation can be possible without the permission of the legitimate user. So it is a serious threat and we need some solution in this regard to prevent it. For prevention we first need proper detection so that we get the timely alert and recognize the attack. SQL statements can be constructed in various ways and the string form data will be prevented a encryption technique with proper SQL parser to retrieve it and find it suitable in the case of matching the SQL parser. Then after the short analysis we have to plan a log file to maintain it so that exact comparison will be possible and we find the malicious content.

We provide here a brief survey and efficient penetration technique. Other sections are arranged in the following manner: Section 2 describes about Literature Review; Section 3 discusses about proposed work; section 4 shows the result analysis; Section 5 describes Conclusions.

2 .RELATED WORK

Halfond et al[19] presented a technique for penetration testing which involves static and dynamic analysis to increase the efficiency both the information gathering and the response analysis phase. The author implemented static and dynamic analysis to improve penetration testing.For discovering input vectors the static analysis technique are used and for automatic the response analysis the dynamic analysis technique is used. The main objective of dynamic analysis is to find error while running the program. To measure the effectiveness of these techniques, an experiment was conducted for static and dynamic analysis based penetration testing on nine web applications.

Xiong et al [20] presented an approach of model driven frame work which integrates the software developement life cycle phases with penetration testing process . So the vulnerability can be easily detected and testing can be done repeatable manner and by the expert personnel. To measure the cost effectiveness, systematic and fully integrated into a systematic and fully integrated into a security oriented software developement life cycle,security experts are still required to maintain knowledge. In this paper the test cases are derived from models.

Stepien et al[21] presented an approach to penetration testing for inherent to penetration testing of web pplication hich consists inherent features of TTCN-3 languages. This paper derives the functional test cases and has taken an example of a malicious bank website. This paper has described a message sequence diagram of a malicious bank website to show the XSS attacks. It generate the functional test cases.

Pietraszek et al[22] presented an approach of Taint based Technique in which the author modified a PHP nterpreter to track taint information at the character level.Contextsensitive analysis is used in this technique to eject sql queries if an untrusted input has been used to

create certain types of sql tokens. The advantages of this approach is that they require modifications to the run time environment, which decreases the portability.

Halfond et al.[23] developed Amnesia(Analysis For Monitoring and Neutralizing Sql Injection Attack). In this paper the author proposed a model based technique that combines the static and dynamic analyses. In this paper the tool first identifies hotspot, where sql queries are issued to database engines. Non-deterministic finite automata is used at each hot spot to develop query model.

In this paper we have used UML 2.0 because UML 2.0 is given the detailed and more explanation .It contains activity diagram which shows the dynamic characterists of a system. In this paper activity diagram is used as modelling diagram as it shows the flow between various activities.

3. Proposed Methodology

In this paper, we propose an effective and flexible SQL Injection detection mechanism which is control from the admin. Our proposed methodology provides secure centralized control system with blocking of data system on the restricted IP. Our approach achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving clients and it can be control by the Admin. It can provide data accessing on the fly if the IP is in unblock list. This flexibility is archived by remote consistency through Java Remote Method Invocation (RMI). The data status is changed runtime and the instance is changed automatically. If the data accessing is stopped from the admin then any remote SQL injection will be failed as the used tokens from SQL server is topped and the penetration system will start working. The working procedure is better understand by figure 1.

4. CONCLUSION AND FUTURE WORK

In this paper we presented an approach of penetration testing process to detect sql injection. Here we presented an activity diagram to model system functions. The result indicate that our method is better effective to solve all these problems simultaneously. The case study represented in this paper is relatively small. In the future research, we plan to apply this approach on a comparatively large application to review the scalability of the proposed approach and generate test cases and implement the tools. In our future work we will implement the tool in a testing environment and will give better result and giving protection to the system for various attacks. Our research outcomes help: to measure the security level of Web Applications using proposed tools to find or

detect vulnerabilities of online applications and to protect the application through proper coding. In the future, we will improve the performance of the current system.

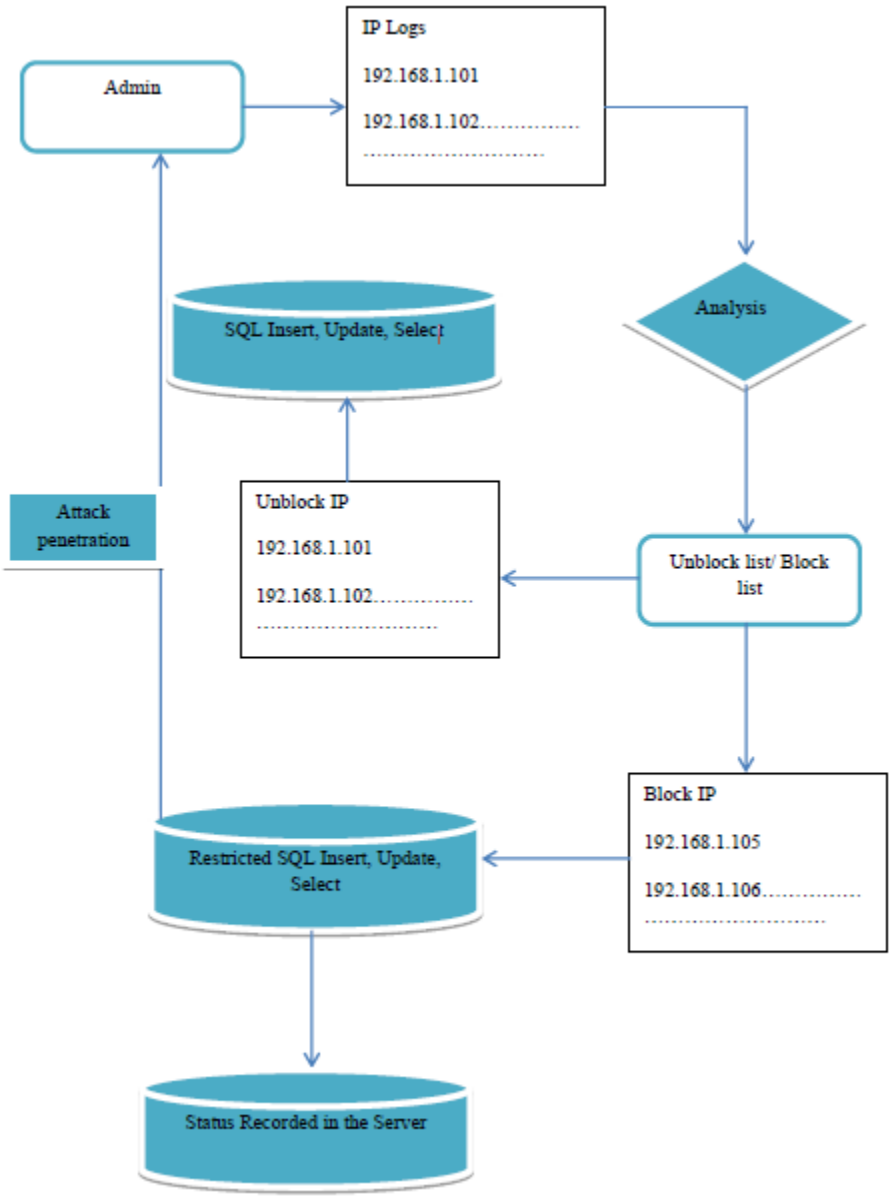

Figure 1: Attack Penetration System

References

[1] W. G. J. Halfond, et al., "A Classification of SQL-Injection Attacks and Countermeasures," in Proceedings of the IEEE International Symposium on Secure Software Engineering, Arlington, VA, USA,2006.

[2] A. Asmawi, Sidek Zailani Mohamed Razak Shukor Abd, "System architecture for SQL injection and insider misuse detection system for DBMS," in International Symposium on Information Technology (ITSim'2008), 2008, pp. 1 -6.

[3] C. Bockermann, et al., "Learning SQL for Database Intrusion Dete ction Using Context-Sensitive Modelling (Extended Abstract)," in 6th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA '09), Berlin, Heidelberg, 2009, pp. 196--205.

[4] K. Kemalis and T. Tzouramanis, "SQL-IDS: a specification-based approach for SQL-injection detection," in Proceedings of the 2008 ACM symposium on Applied computing (SAC'2008), New York, NY,USA, 2008, pp. 2153--2158.

[5] M. Kiani, et al., "Evaluation of Anomaly Based Character Distribution Models in the Detection of SQL Injection Attacks," in Third International Conference on Availability, Reliability and Security (ARES'2008), Washington, DC, USA, 2008, pp. 47--55.

[6] E. Bertino, et al., "Profiling Database Applications to Detect SQL Injection Attacks," in Proceedings of the Performance, Computing, and Communications Conference (IPCCC'2007), 2007, pp. 449-458.

[7] W. Robertson, et al., "Using Generalization and Characterization Techniques in the Anomaly-Based Detection of Web Attacks," in 13th Annual Network and Distributed System Security Symposium (NDSS'2006), 2006.

[8] V. H. García, et al., "Web Attack Detection Using ID3," in International Federation for Information Processing 2006, pp. 323- 332.

[9] F. Valeur, et al., "A Learning-Based Approach to the Detection of SQL Attacks," in Proceedings of the Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), Vienna, Austria, 2005, pp. 123--140.

[10] R. Ezumalai and G. Aghila. Combinatorial Approach for Preventing SQL Injection Attacks. IACC, 2009.

[11] Junjin, Mei. "An approach for SQL injection vulnerability detection." In Information Technology: New Generations, 2009. ITNG'09. Sixth International Conference on, pp. 1411-1414. IEEE, 2009 .

[12] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava,"Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", CONSEG 2012.

[13] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Vipul Agarwal, Yogeshver Khandagre, "Knowledge Discovery with a Subset-Superset Approach for Mining Heterogeneous Data with Dynamic Support",Conseg-2012.

[14] Preeti Khare, Hitesh Gupta, "Finding Frequent Pattern with Transaction and Occurrences based on Density Minimum Support Distribution", International Journal of Advanced Computer Research (IJACR), Volume-2 Number-3 Issue-5 September-2012.

[15] Lakhtaria, Kamaljit I. "Protecting computer network with encryption technique: A Study." In Ubiquitous Computing and Multimedia Applications, pp. 381-390. Springer Berlin Heidelberg, 2011.

[16] Chan, Aldar CF, and Claude Castelluccia. "A security framework for privacy-preserving data aggregation in wireless sensor networks." ACM Transactions on Sensor Networks (TOSN) 7, no. 4 (2011): 29.

[17] Stalling, W.,Cryptography and network security principles and practices ,4th edition Prentice Hall,2005.

[18] Shannon, Claude E. "Communication Theory of Secrecy Systems*." Bell system technical journal 28, no. 4 (1949): 656-715.

[19] Halfond WGJ, Orso , Improving penetration testing through static and dynamic analysis, Software Testing, Verification, And Reliability(2011).

[20] Pulei Xiong, Liam Peyton, A Model-Driven Penetration Test Framework for Web Applications, 2010 Eighth Annual International Conference on Privacy, Security and Trust.

[21] Halfond WGJ, Orso A. AMNESIA: Analysis and Monitoring for NEutralizing SQL-Injection Attacks, Proceedings of the International Conference on Automated Software Engineering, Long Beach, CA, U.S.A., November 2005;174183.

[22] T. Pietraszek and C. V. Berghe , Defending Against Injection Attacks through Context-Sensitive String Evaluation, In Proceedings of Recent Advances in Intrusion Detection (RAID2005), 2005.

[23] Bernard Stepien, Liam Peyton, Pulei Xiong , Using TTCN-3 as a Modeling Language for Web Penetration.