Methodology and Analysis for Various SQL Injection Techniques

Antveer Kaur
Department of computer science
Banasthali University Jaipur, Rajasthan, India (302001)
bntsnghbrr940@gmail.com

Abstract— Now day's online transaction is done by most of web applications. These applications have vulnerabilities which make its security weak. Every application has provided authentication and authorization functionality, security remains an issues. SQL injection is a technique which gives access to backend database without valid credentials. SQL injection technique has been discovered with new innovative method. This paper presents analysis of various new methodologies of SQL injection, their preventions and its vulnerabilities. We experimented on various methodology of this attack with various applications and analyzed its prevention strategies for programmer of web applications.

Keywords- SQL injection techniques; Backend database; Web applications;

I. INTRODUCTION

In recent days, Web applications have been developed for fulfill various purpose in overall world. Thus, Web applications store large amount of data in its database. Even, Sensitive information of users is stored by its database. Users can interact with application backend database using application design for such tasks like as extracting information from database, made queries on database and more. In less secure web applications have much vulnerability which provides access of user's sensitive information to unauthorized user? Sometime, unauthorized user can damage web application and destroy complete database of system. This is called as SQL Injection which thefts data of trusted users of web application [7]. Today, Government and defense department are affected by this vulnerability of SQL injection.

In this paper, we have experimented on new SQL injection attack, vulnerabilities and generate its prevention techniques for developers. The objective of this paper has to aware to users and developers also. It is also useful for readers and researchers. SQL injection has SQL vulnerability which provides access to unauthorized users without validation as client side. There have need to developer about understanding of these vulnerabilities. In paper, we have studied about the aspect of coding method to implement the web applications.

The reminder has following sections: Section 2 described about SQL injection aspects. Section 3 provides information about various different types of attacks in past and present. Section 4 have experimented experience with analysis of these techniques along with its prevention. Section 5 concludes about it and its future work.

II. SQL INJECTION

SQL is high level language for relational database management. It was developed in 1970 by F. Codd at IBM. SQL Injection is mechanism which takes to benefit of flaw or weakness of SQL database management system.SQL Injection is technique which attacker adds malicious keyword and operators with SQL query and injects it into textbox of designing interface of web applications. Thus, it gives access to attacker on backend database as admin or unauthorized users. Formal definition of SQL injection is given by (Su et al., 2006) [1]. [2] It represents various types of vulnerabilities in web programming which are follows: validation for users input is not defined properly. Users input are not checked at client side as server side. Lack of data types accepted in web programming language. [4]They have described about problem formulation and architecture of SQL injection. The architecture of SQL injection technique is given in following diagram which have shown in figure 1.

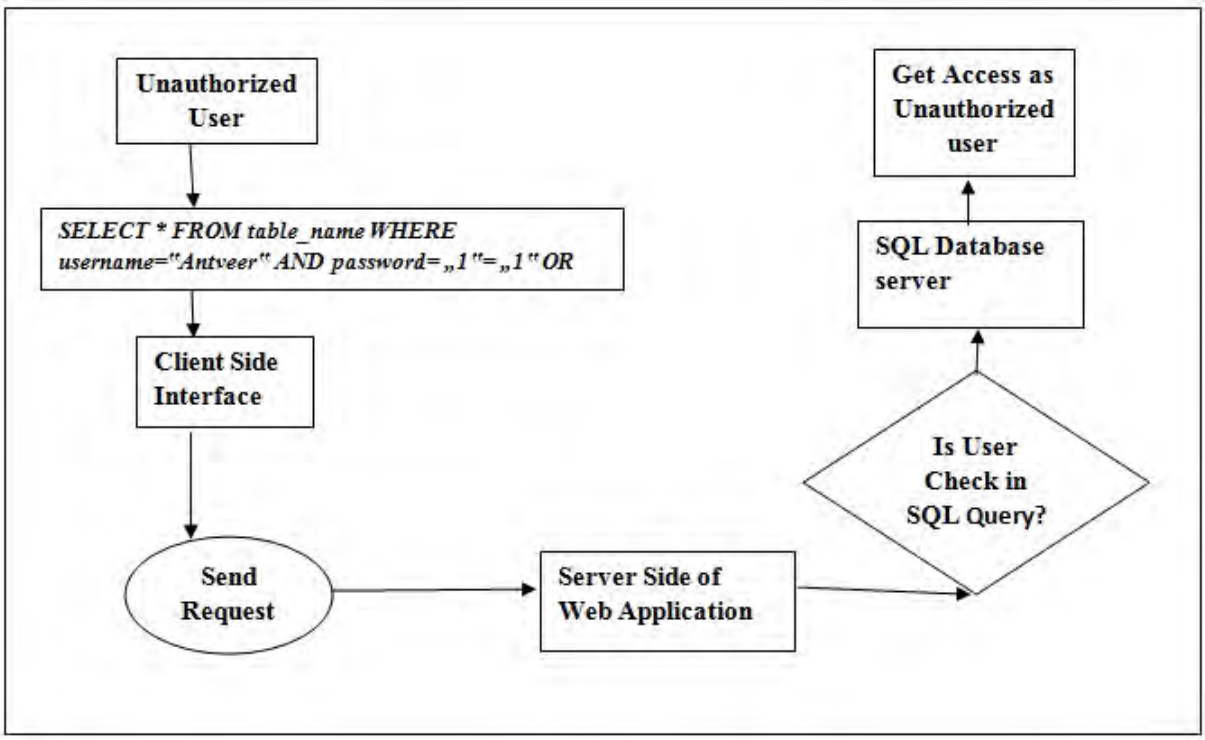

Figure 1. Architecture of SQL injection technique

System Architecture describes about SQL injection technique where unauthorized user able to access the authorized user resource on web application.

III. SQL INJECTION TECHNIQUE WITH DIFFERENT METHODOLOGIES

SQL injection techniques have been developed with new innovative methods. We have categorized SQL injection technique in various types as follows.

A. *String Tautology based SQL Injection Method*

Unauthorized user input SQL string as conditional query statement that executes a true condition. This conditional statement takes input of malicious code in login page interface. This method is also referred by AND/OR tautology conditions. This method is successful on login interface .It may be returned all data rows of targeted table which is used by bypass authentication. (Preveen Kumar, 2013) He has presented the scenario for this method. For example

We write an injected statement like as*" SELECT * FROM tb_USERS WHERE USER_NAME='antveer' OR '1'='1' "*. The output of this query which will return all rows of antveer user related. The condition is also true, so that it will return all rows of table.

B. *Numeric Tautology based SQL Injection Method*

This method is similar to above tautology it gives result based on numeric condition. The unauthorized user would input numeric values in conditional query statement that would give result as true condition. We write an injected statement like as *" " SELECT * FROM tb_USERS WHERE USER_ID=101 OR '1'='1' "*.The output will return row which id have 101 and also return all the row of table.

C. *Blind SQL Injection Method*

This technique collects important information of data by sending request to server. This technique uses URL for exploiting information from page. It is similar to normal SQL Injection ***(***Amirtahmasebi et al., 2009***).*** It can retrieve sensitive information from server using true or false statement on this query. For example, we write an injected code statement like as" *http://www.banasthali.org/librarydetail.asp?catgory=book OR' 1'='*1' ". This statement will return the result related to book category and will also return all row using true condition.

D. *Database Backdoor Method*

Database has malicious trigger activity code which known as backdoor. In this method, hacker can set trigger in order to get input information on his/her e-mail. For Example, attacker can set trigger like this" *Create trigger*

backdoor before insert on student for each row, update student set email='bntsnghbrr940@gmail.com' where user_id=NEW.user_id;"

E. SQL Injection with Shell Uploading

Shell is like as a program routine which can access service of operating system kernel. Attacker attach shell script with browse button .It can take access of admin data and its resource. It can also change the content of web on server. Attacker can take over server without authentication or authorization details [8].

IV. IMPLEMENTATION AND ANALYSIS

We have experimented on system using prevention techniques and analysis of this method. We can secure our website using following method.

A. Using function mysql_real_escape_string ()

Developer can make web application secure at time of coding. Programmer can use this function in server side coding to prevent from unauthorized users like as.

Using function mysql_real_escape_string ($_POST ['USERNAME']);

B. Using Auto complete Enabled

Auto complete is tag of html form which used to disable auto completion of browser. For example

<form name="form1" method="post" action="Index.aspx" autocomplete="disabled">

C. Using Encryption Technique with strong password

Encryption is an important key of security. Programmer can use encryption to store the password in SQL database .It has ability to secure from blind SQL injection. Web application URL can also convert into encrypted form where attacker cannot perform Conditional SQL query statement.

D. Using Multitier architecture of web application

Web application has multitier architecture which has many layers. Attacker need to breaks security of multitier architecture to exploit information from backend database. For example-Three multitiers have three layers such a User interface layer; business logic layer and database layer.

We have worked on above methods to implement the website .We have generated these result after or before applying security method.

Figure 2. Demo before Security Method Using Vulnerability Tool.

Figure 3. Demo after Security method Using Vulnerability Tool

Here we are trying to comparative analysis of SQL injection methods and another vulnerability attacks. We have analyzed about prevention technique which can stop SQL injection. We will study using formula which has shown in equation 1.Formula has calculated the percentage of technique which can stop SQL injection [5].

$$Percentage\ of\ Prevention\ Technique\ (\%) = \frac{\text{Total no. of Technique which can stop SQL injection}}{\text{Total no. of technique}} \quad (1)$$

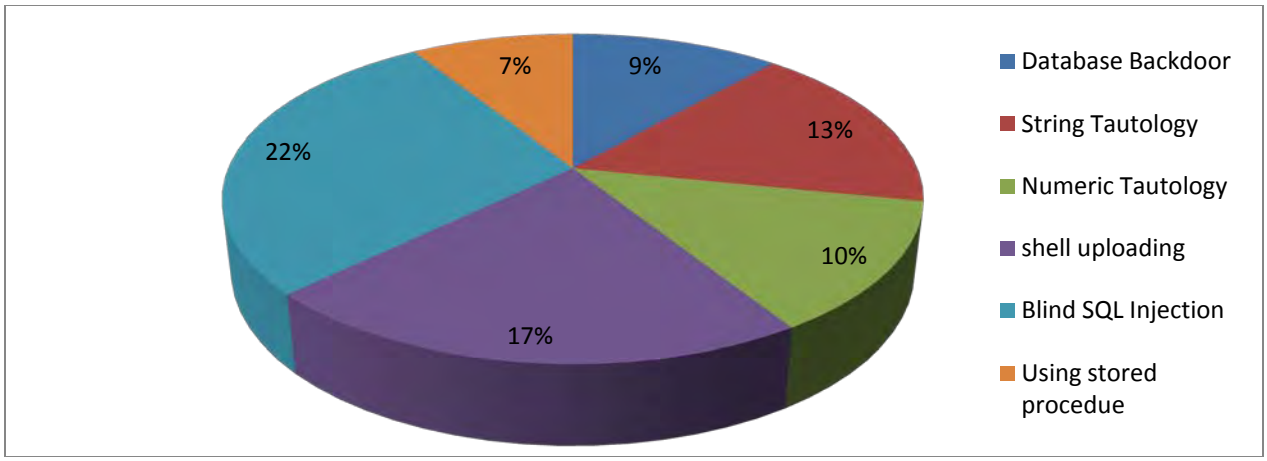

Figure 4. Percentage of SQL injection methodologies used to perform attack in 2011-2014

Currently, OWASP have analyzed about these methods which have performed in 2011-2014.

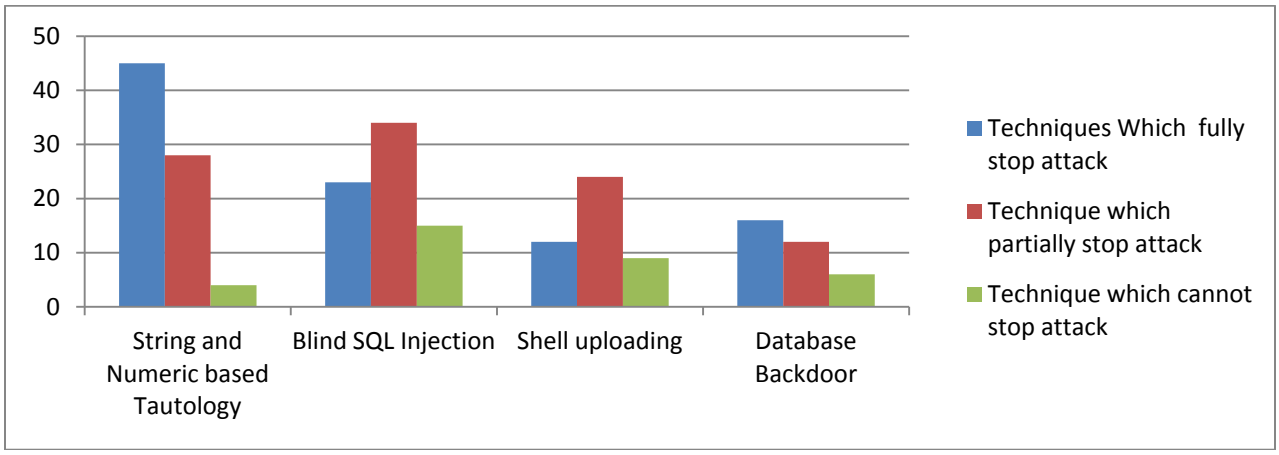

Figure 5. Percentage of SQL injection Prevention and detection techniques.

V. CONCLUSION

The main objective of this work has to aware programmer and readers from SQL injection techniques .We have explained security method to secure development of web application .Today, many techniques have came to prevent from SQL injection. But, these days it remains a big issue in development area. Because Black hat always busy to find out new techniques and applying it in new way. Our work is beneficial for researchers and developers of websites. New Techniques will be required to handle new SQL injection method. We need to survey continuously to this attack.

REFERENCES

[1] A Tajpour, A., Masrom, M., Heydari, M.Z., and Ibrahim, S.," SQL injection detection and prevention tools assessment". Proc. 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT"10) 9-11 July (2010), 518-522

[2] A. Tajpour, S. Ibrahim, M. Masrom, "SQL Injection Detection and Prevention Techniques" International Journal of Advancements in Computing Technology Volume 3, Number 7, August 201110.4156/ijact.vol3.issue7.11

[3] A. Masebi, K. Jalalinia, and S. Khadem, "A survey of SQL injection defense mechanisms". International Conference for Internet Technology and Secured Transactions (ICITST 2009), 9-12 Nov. (2009), pp. 1-8.

[4] Priyanka, Vijay B., "Detection of SQL Injection Attack and Various Prevention Strategies". International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.

[5] C. Dougherty (2012) "Practical Identification of SQL Injection Vulnerabilities" United States Computer Emergency Readiness Team (US-CERT October 25, 2012).

[6] P. Kumar (2013) "The Multi-Tier Architecture for Developing Secure Website with Detection and Prevention of SQL-Injection Attacks" International Journal of Computer Applications (0975 – 8887) Volume 62– No.9, January 2013 .

[7] N. Seixas, J. Fonseca, M. Vieira, and H. Madeira, "Looking at Web Security Vulnerabilities from the Programming Language Perspective": A Field Study. Proc. of 20th International Symposium on Software Reliability Engineering 2009 (ISSRE, 09), 16-19 Nov.2009, pp. 129-135.

[8] S. Shrivastava, R. Ranjan, K. Tripathi, "Attacks Due to SQL injection & their Prevention Method for Web-Application", International Journal of Computer Science and information technologies, Vol 3 (2), pp.3615-3618, 2012.

[9] Z. Su and G. Wassermann. "The Essence of Command Injection Attacks in Web Application". In the 33rd Annual Symposium on Principles of Programming languages, pages 372-382, Jan. 2006.