ISSN No. 0976-5697

Volume 4, No. 8, May-June 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Web Application Vulnerabilities Monitoring & Avoiding Techniques

Neeraj Sharma, Mohammad Arshad, Anurag Jain
Department of Computer Science
RITS Bhopal, India
neerajsharmans12@gmail.com, arshad10uk@gmail.com, anurag.akjain@gmail.com

Abstract: In recent years the great advances have occurred in the field of Information & Technology, there are several services provided by the I.T. to an ordinary user some of them may possibly depend on each other, as we know the critical aspect is Information on which everything depends. As the globalization increases the information regarding every prospective is also get increased ,so it is very necessary to secure that information which may be present in any form on world wide web .In this paper we have provided the study of various SQL-Injection web vulnerabilities detection & prevention techniques with their characteristics, and also provided our approach for authentication process to avoid such attacks ,we will implement our procedure for preventing SQL-Injection attacks in stored procedures using Regular Expression.

Keywords: vulnerability, SQLIAs, Authentication

I. INTRODUCTION

In today's world internet had occupied a tremendous growth which impacts the commerce and culture hugely .This great network to which we call World Wide Web(WWW) is the series of interconnected servers works combine to form the internet, the E-commerce applications of internet provide wide range of applications(services)to the internet users .With the great evolution of technology ,present users can do anything on his finger-tips while sitting at the home .Information on the World wide Web can be present in several forms for e.g. this information may be related to the bank account details of an internet buyers ,it may be some secure information of an enterprise, information may be in the form of databases etc. As it provides several benefits it have some drawbacks also, the information in any form may be vulnerable to various security threats from which SQL-Injection attacks is the one.

Internet workstations can be feared by several SQL-Injection vulnerabilities. SQL-Injection Attacks (SQLIAs) provides un-authorized persons the direct access to the database store of the web applications, and with the power to insert, delete or modify the information stored on these applications. In recent there are many SQLIAs with several consequences and have several victims which includes high-profile companies and associations such as Travelocity , on the basis of one of the study performed by the Gartner Group on over 300 websites about 97% of the audited sites were found to be vulnerable to these kind of web attacks [1].

SQL Injection attacks will performed by changing the overall execution behavior of the SQL query in such a way that the result of the query will always evaluated to be true by using some malicious keywords or commands before the input validation phenomena ,we can say that these attacks takes the advantage of various flaws present in the SQL dynamics(evaluation functionality) .In 2010 the two attacks namely SQL Injection and Cross Site Scripting(XSS) attacks are enlisted in the list of top-10 web application vulnerabilities according to OWASP(open web application security project) project [4]. The most famous SQL-Injection incident has occurred probably in the beginning of 2005 in which the card systems solutions database security get leaked due to such attacks [5]. There may be several SQL Injection attacks with their different prospective, but in our solution we found that there are many research papers have been proposed for handling SQL Injection in stored procedures, but most of them have used the concept of encryption or hashing to prevent them but using extra fields for hash values increases the space requirement .In this survey we will proposed a simple framework based on regular expression to prevent SQLIAs inside the stored procedures.

All the validation or authentication rules (steps) will be stored in the secure manner inside database .At the time of request arrival it will be granted on the basis of validation rules stored the only difference between this approach and the other ones is that in this mechanism the validation steps will be stored in the database server also and not just inside the web hosting server ,in this way the rules are protected by the two levels of security both at the web hosting server and database security.

A. *Objective of our work:*

In this study, several types of SQLIAs are evaluated with their behavior such as their syntax, way of execution, target platform etc. and also with their prevention techniques.

B. *Structure of This paper:*

After providing the initial information , the organization of this paper can be classified as : the section 2 will give the introduction about the types of SQLIAs ,and then after the section 3 will provide the information regarding our proposal to avoid such attacks, then section 4 will provide the comparative analysis of various techniques on the basis of detection & prevention capabilities , and then after section 5 will concludes the paper noting the contribution of our work and future enhancements.

II. VARIOUS CATEGORIES OF SQL INJECTION ATTACKS (SQLIAS)

SQLIAs can be of various types which provide threats to web applications, each SQLIAs exhibits different syntax, behavior and different way of evaluation with each one

targeting the different or same web application platform. The following are the types:

A. Tautologies:

In this malicious codes (SQL Injection codes) were inserted inside various conditional statements such that those conditional statements were always evaluated to be true. It may have the following types:

a. String SQL Injection:

These attacks are also referred as the AND/OR Attacks [19] [20] these attacks are always evaluated to be true if used properly by the intruders.

b. Numeric SQL Injection:

They are quite similar to the above attacks, but the only difference is that the numerical values are used instead of strings such that the conditional statements were always evaluates to be true [1].

c. Comment Attacks:

These attacks take the benefit of inline commenting which is allowed by SQL syntax [21].

B. Logical incorrect queries:

Information collected on the basis of generated error messages from the target database which will provide necessary data to the intruder to target the database.

C. Union Query:

In this the malicious query will be combined with the safe query using the UNION keyword for fetching the information regarding the various tables of the database to hire attacks.

D. Stored procedures:

These are the set of rules (steps) which are stored inside the accessing database **and** any request will be granted on the basis of these steps, but they can also be violated using malicious keywords or statements by the unauthorized persons.

E. Piggy-Backed Queries:

In this scheme various malicious queries will be nested inside the original injected(infected) query.

F. Inference:

In this the conclusions will be evaluated by the intruders on the basis of true/false questions regarding the database. It will be of following types:

a. Blind Injection:

Summary information useful to hire attacks will be collected as per the replies after asking the true/false questions from the target web application.

b. Timing Attacks:

In this the necessary information will be collected as per the response overhead of the web databases, which is used by the attacker to launch attacks.

G. Alternate Encodings:

It aims to remains unidentified by the secure and defensive programming used to secure the web applications because it may contain several backtracking mechanisms which will easily open the identity of the unauthorized person(Intruder) trying to destruct the security of the given database application.

III. DETECTION & PREVENTION SURVEY

Simple table's representing the characteristics of various approaches:

A. SQL Injection detection schemes:

S.No	Name of detection technique	Provide security for	Working Methodology
(i)	SAFELI [3]	ASP.NET web applications	Static Analysis Framework
(ii)	Thomas et al.'s scheme [6]	Open source projects	Automated Prepared Statement Generation Algorithm
(iii)	Ruse et al.'s scheme [7]	This experiment is basically not done on Real-Life existing database(but on sample)	Automatic Test Case Generation
(iv)	Haxia and Zhihong's Scheme [8]	Web applications	Secure Database Testing Design
(v)	Roichman & Guides Scheme [9]	Web applications	Fine –grained Access control Mechanism
(vi)	Shin et al.'s Approach[10]	Web applications	A Specification Based Methodology

B. Some SQL-Injection Detection & prevention techniques:

S.No	Name of technique	Experiment conducted mainly with
(i)	AMNESIA [11]	My SQL,IV5.0.21,JAVA based DBMS
(ii)	SQLrand [12]	Common Gateway Interface(CGI)applications
(iii)	SQL DOM [13]	Relational databases from the OOP(Object Oriented Programming)Languages point of view
(iv)	SQL-IDs [5]	JAVA based Real -time applications

C. Some more SQL-Injection Detection techniques:

S.No	Name of technique	Experiment conducted mainly with
(i)	SQL –Guard [14]	Web applications
(ii)	SQLIPA [15]	Web applications
(iii)	CSSE [18]	Real world PHP applications
(iv)	Swaddler [17]	Web applications(prototype of this approach for the PHP language)
(v)	SQL Check [16]	Web applications

IV. OUR PROPOSAL (PREVENTING SQL INJECTION ATTACKS IN STORED PROCEDURES USING REGULAR EXPRESSION SQL-CURE)

A. Problem Statement:

Recently many papers have been proposed for handling SQL injection in stored procedure. Most of the papers used the concept of encryption or hashing to prevent SQL injection attacks. But using extra fields for hash values increases the space requirement. In this project we will proposed a simple framework based on regular expression to prevent SQL injections inside the stored procedure.

B. Proposed Solution:

The data based will store all the validation rules in a secure way. Whenever any request come, the database will validate the request with the validation rules stored. The basic difference between this idea and the other SQL injection prevention technique is that in this technique the validation rules will be stored inside the database and not just inside the web hosting server. So the rules are protected by two levels of security a) Web hosting server security b) Database security. Even if a hacker hacks the web application it will not be possible for him to collect information because both the validation rules and stored procedure will be stored inside the Database and database will have its own security.

A simple working model of our work proposal:

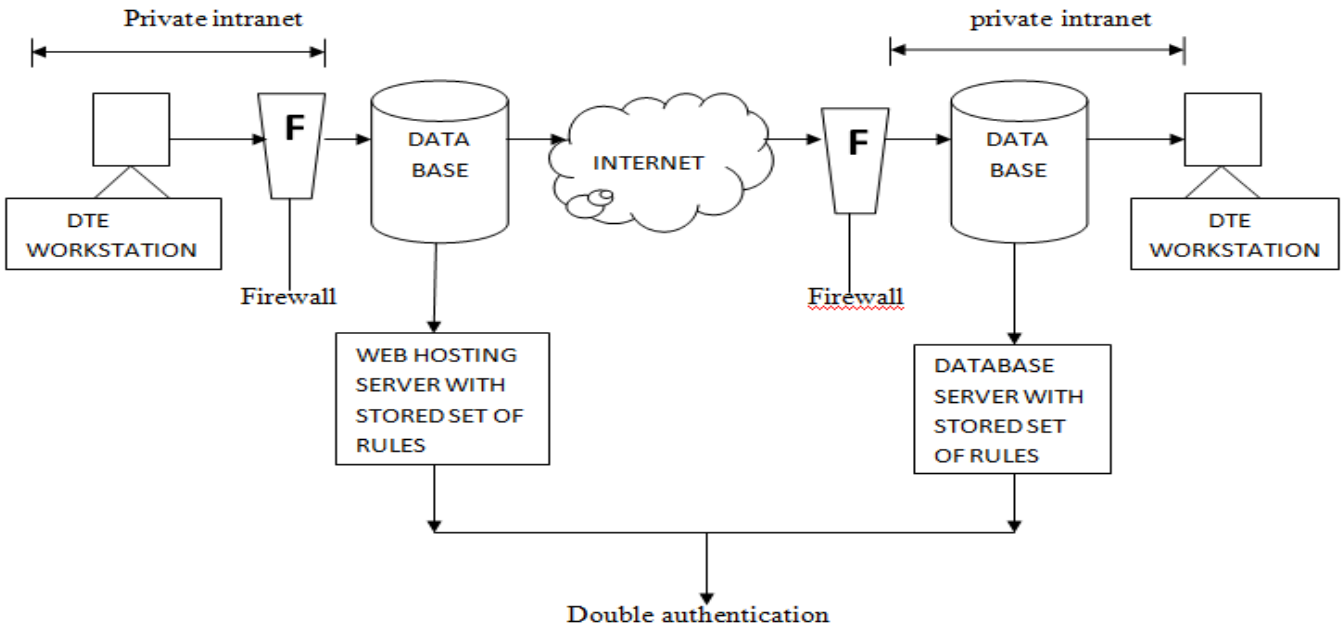

Figure: 1

The above figure is representing the diagrammatical representation for our work which will increase the reliability level and can avoid various illegal (un-authorized) accesses.

C. Benefits & flaws:

In our procedure we have provided the two way authentication to avoid unauthorized access, if somehow the breach of security will be occurs at the web hosting server it will be quickly identified by the check point at the database server again. As our technique provides advantages it has some drawbacks to, because as the check points increases the working and time overhead also increases.

V. CONCLUSION

In this paper we have explained about the information which will be stored in any form on the World Wide Web (WWW) and about the types of intrusion attacks(SQLIA's) with their simple description which are threat to web applications ,also the snapshot of various mechanisms which can destruct the security of the web application is given in the discussion. In this survey the characteristics of various SQLIA's (SQL Injection Attacks) attacks detection and prevention techniques are provided on the basis of comparative analysis. After reading this one will get the

quick view of available web vulnerabilities .The SQL Injection attacks were prevails as one of the Top 10 vulnerabilities and threats to the online business targeting web databases, so we have also provided our proposal to avoid such attacks for increasing the authentication level.

VI. REFERENCES

[1]. Combining Static Analysis and Runtime Monitoring to Counter SQL Injection Attacks William G.J. Halfond and Alessandro Orso College of Computing Georgia Institute of Technology {whalfond|orso}@cc.gatech.edu.

[2]. A Detailed Survey on Various Aspects of SQL Injection: Vulnerabilities, Innovative Attacks, and Remedies Diallo Abdoulaye Kindy and Al-Sakib Khan Pathan Department of Computer Science, International Islamic University Malaysia, Malaysia E-mail: diallo14@gmail.com and sakib@iium.edu.my.

[3]. Fu, X., Lu, X., Peltsverger, B., Chen, S., Qian, K., and Tao, L., A Static Analysis Framework For Detecting SQL Injection Vulnerabilities. Proc. 31st Annual International Computer Software and Applications Conference 2007 (COMPSAC 2007), 24-27 July (2007), 87-96

[4]. http://www.owasp.org/index.php/Top_10_2010-A1-Injection, retrieved on 13/01/2010.

[5]. Kemalis, K. and T. Tzouramanis. SQL-IDS: A Specification-based Approach for SQLinjection Detection. SAC'08. Fortaleza, Ceará, Brazil, ACM (2008), 2153 2158.

[6]. Thomas, S., Williams, L., and Xie, T., on automated prepared statement generation to Remove SQL injection vulnerabilities. Information and Software Technology, Volume 51 Issue 3, March (2009), 589–598.

[7]. Ruse, M., Sarkar, T., and Basu. S., Analysis & Detection of SQL Injection Vulnerabilities Via Automatic Test Case Generation of Programs. Proc. 10th Annual International 21 Symposium on Applications and the Internet (2010), 31-37.

[8]. Haixia, Y. and Zhihong, N., A database security testing scheme of web application. Proc. of 4th International Conference on Computer Science & Education 2009 (ICCSE '09), 25-28 July (2009), 953-955.

[9]. Roichman, A., Gudes, E., Fine-grained Access Control to Web Databases. Proceedings of 12th SACMAT Symposium, France (2007).

[10]. Shin, Y., Williams, L., and Xie, T., SQLUnitGen: Test Case Generation for SQL Injection Detection. North Carolina State University, Raleigh Technical report, NCSU CSC TR 2006-21 (2006).

[11]. Junjin, M., an Approach for SQL Injection Vulnerability Detection. Proc. of the 6th International Conference on Information Technology: New Generations, Las Vegas, Nevada, April (2009), 1411-1414.

[12]. Boyd S.W. and Keromytis, A.D., SQLrand: Preventing SQL Injection Attacks. Proceedings Of the 2nd Applied Cryptography and Network Security (ACNS'04) Conference, June (2004), 292–302.

[13]. McClure, R.A. and Kruger, I.H., SQL DOM: compile time checking of dynamic SQL Statements. 27th International Conference on Software Engineering (ICSE 2005), 15-21 May (2005), 88- 96.

[14]. Buehrer, G., Weide, B.W., and Sivilotti, P.A.G., Using Parse Tree Validation to Prevent SQL Injection Attacks. Proc. of 5th International Workshop on Software Engineering and Middleware, Lisbon, Portugal (2005) 106–113.

[15]. Ali, S., Shahzad, S.K., and Javed, H., SQLIPA: An Authentication Mechanism Against SQL Injection. European Journal of Scientific Research, Vol. 38, No. 4 (2009), 604-611.

[16]. Su, Z. and Wassermann, G., The essence of command injection attacks in web Applications. In ACM Symposium on Principles of Programming Languages (POPL'2006), January (2006).

[17]. Swaddler: An Approach for the Anomaly-based Detection of State Violations in Web Applications Marco Cova, Davide Balzarotti, Viktoria Felmetsger, and Giovanni Vigna Department of Computer Science, University of California Santa Barbara Santa Barbara, CA 93106-5110, USA {Marco, balzarot,rusvika,vigna}@cs.ucsb.edu.

[18]. Defending against Injection Attacks through Context-Sensitive String Evaluation? Tadeusz Pietraszek1 and Chris Vanden Berghe1;2 1 IBM Zurich Research Laboratory S□aumerstrasse 4, CH-8803 R□uschlikon, Switzerland 2 Katholieke Universiteit Leuven Celestijnenlaan 200A, B-3001 Leuven, Belgium fpie|vbcg@zurich.ibm.com.

[19]. McClure, R.A. and Kruger, I.H., SQL DOM: compile time checking of dynamic SQL Statements. 27th International Conference on Software Engineering (ICSE 2005), 15-21 May (2005), 88- 96.

[20]. Amirtahmasebi, K., Jalalinia, S.R., and Khadem, S., A survey of SQL injection defense Mechanisms. International Conference for Internet Technology and Secured Transactions (ICITST 2009), 9-12 Nov. (2009), 1-8.

[21]. Luong, V., Intrusion Detection and Prevention System: SQL-Injection Attacks. Master's Projects. Paper 16. (2010), available at:

http://scholarworks.sjsu.edu/etd_projects/16.