 ISSN: 2321-8169
22 – 26

Analysis of SQL Injection Attack Detection Techniques for Web-Based Application

Aniruddha S. Holey
P. G. Department of CST
H.V.P.M., Amravati
Amravati, Maharashtra, India
Email: aniruddha.holey@gmail.com

Prof. S. S. Sherekar
Department of CSE,
SGB Amravati University,
Amravati, Maharashtra, India
Email:ss_sherekar@rediffmail.com

Prof. V. M. Thakare
Department of CSE,
D.C.P.E.,
SGB Amravati university,
Amravati, Maharashtra,India
Email:vilthakare@yahoo.co.in

Abstract:In the world of digitization, web applications are widely used. SQL injection attack is most used by attacker that's why it's very dangerous attack. The interaction between the web application and Database through Structure query language (SQL). The malicious code is injected into string and then passes into database backend for parsing and execution. Structure query language injection attack is ranked first position in the open web application security project (OWASP). Impact of SQL injection attack is losses confidentiality, integrity, authentication and authorization.This paper focuses on the consequences, comparison and analysis of SQL injection attack detection techniques to check the effectiveness and evaluation is based on the resources needed to implements the SQLIA detection techniques and helps other researchers to choose the right techniques for further studies.

Keywords- *SQL Injection attack, SQLI attack types and categories, Detection techniques*

_____ ***** _____

I. INTRODUCTION

In SQL injection attack the attacker posts specially crafted structure query language statements which are executed in the database server and produce malicious outcomes [1]. The web application confidentially, integrity and availability may be compromised to many types of attacks and could be easily hacked [2]. Hackers could implement some simple methods to get access to the database system through the web application to obtain, delete or update the existing data, and this is known as SQL Injection Attack. Structured Query Language Injection (SQLI) attack is a code injection technique in which malicious SQL statements are inserted into the SQL database by simply using web browsers. SQLI attack can cause severe damages on a given SQL database such as losing data, disclosing confidential information or even changing the values of data.

SQL injection attack stands among top ten most threatening attacks to database security. Various techniques have been developed to curb SQLIA but still the rate of such attacks is increasing day by day.SQL injection attacks are most highly distributed attack techniques constituting nearly 49% of all attacks. The SQL Injection attack is very pervasive because stagnated data, No distributed security, Known hierarchy of privileges, easiest attack ever, unsafe underline architecture, blind trust on user input, Double edge sward, Inherent code, Difficult detection, cost and vigilance while creating error message [3].

SQLI attack is a technology vulnerability that comes from dynamic script language such as Hypertext Processor (PHP), Active Server Pages (ASP), Java Server pages (JSP) and Common Gateway Interface (CGI).The development of web application is very fast because some new technologies are introducing i.e. Ruby-on-rails, Word press and different frameworks are available for fast development [4].

SQL Injection Attacks (SQLIAs) are attacks that pose a security threats to web applications by manipulating, modifying, retrieving or destructing sensitive information underlying database server through web applications. This type of attacks could compromise data confidentiality, integrity and availability of database systems of the online applications. The classification of order injection attack contains First order attacks, Second order attack and last lateral attack [5]. SQL injection is an active attack that poses threat to web application that uses database by injecting SQL queries into data-plane input. The SQLI attacks focus on the component of the e-learning system such as web services and database systems [6].

Vast use of SQL based databases makes it the center of attention of hackers. SQL injection attack is a well-known security threat to database driven web applications. A successful SQL injection attack reveals critical confidential information to the hacker [7]. The features of SQL injection attack are Normal accessibility, extensive use, simple injection, high danger and forms of SQL injection attacks are to bypass the authentication, the key operations to database system and perform database system command. SQL Injection could be very dangerous in many cases depending on the platform where the attack is launched and its gets success in injecting rogue users to the target system [8].

Categories of SQL Injection attacks:
SQL injection attack are categorized into four category [9].

 ISSN: 2321-8169
22 – 26

(i) *SQL Manipulation:* These method is by changing the where clause or union of the SQL statement.

(ii) *Code Injection:* It is the process of inserting SQL command and possible when multiple SQL statement per database request is supported.

(iii) *Function call Injection:* It is the process of inserting various database function call into a vulnerable SQL statement and make an operating system call or manipulate data in database.

(iv) *Buffer overflow:* It is caused by using function call Injection.

Types of SQL Injection attack:

Following TABLE I show the types of SQL Injection attack with brief description [9].

TABLE I: TYPES OF SQL INJECTION ATTACK

Sr. No	Types of attacks	Description
1	Tautologies	SQL injection queries are injected into one or more conditional statements so that they are always evaluated to be true.
2	Logically Incorrect Queries	Using error messages rejected by the database to find useful data facilitating injection of the backend database.
3	Union Query	Injected query is joined with a safe query using the keyword UNION in order to get information related to other tables from the application.
4	Alternate Encodings	It aims to avoid being identified by secure defensive coding and automated prevention mechanisms. Hence, it helps the attackers to evade detection. It is usually combined with other attack techniques.
5	Stored Procedure	Many databases have built-in stored procedures. The attacker executes these built-in functions using malicious SQL Injection codes.
6	Inference Blind Injection Timing Attacks	An attacker derives logical conclusions from the answer to a true/false question concerning the database. Information is collected by inferring from the replies of the page after questioning the server true/false questions. An attacker collects information by observing the response time (behavior) of the database.
7	Piggy-Backed Queries	Additional malicious queries are inserted into an original injected query.

The remainder of this paper is organized as follows. In Section II, the SQL Injection attack type and their categorization. The detection techniques of SQL Injection attack is discussed in Section III. Sections IV and V include the consequence, comparison, analysis and discussion respectively, also section VI include conclusion and finally references.

II. SQL INJECTION ATTACK TYPE AND THEIR CATEGORIZATION:

Table-II shows a chart of the SQLI attacks and their categories. Can be categories the SQLI attacks with their supporting category.

TABLE-II: CATEGORIZATION OF SQL INJECTION ATTACK TYPE.

Categories / SQLI Attacks	SQL Manipulation	Code Injection	Function call Injection	Buffer Overflow
Tautologies	√	X	X	X
Union Query	√	√	X	X
Stored Procedure	X	X	√	X
Piggy Backed Queries	X	√	X	X
Alternate Encoding	√	X	X	X
Interface based attack	X	√	X	√

SQL injection attacks are categorization as SQL Manipulation, Code Injection, Function call Injection and Buffer overflow. Tautologies and Alternate Encoding are considered in SQL Manipulation. Union Query is considering not only in SQL Manipulation but also Code Injection. Stord procedure considers in Function call Injection and Piggy backed Queries consider in Code Injection. Interface based attack is considering not only code injection but also Buffer Overflow.

III .DETECTION TECHNIQUES

In order to protect a web application from SQL Injection attack, we require basic concept detection of SQL injection attack. Here, mention the working of method in brief.

NN based model – In [10], Sherykhkanloo et al., proposes a new approach based on Artificial Intelligence (AI) and Neural network (NNs) for the detection of Structure Query Language Injection (SQLI) attack. The model includes three main elements of a URL generator, a URL classifier and an NN model. The URL generator and the URL classifier are in order to provide required malicious and benign URLs for three phases of testing, Validating and training of the NN model. The implementation scenario of experiment contains 1000 selected URLs are scattered in three phases of training, validating and testing with distribution rate of 70%, 15% and 15% respectively. The receiver operating characteristic (ROC) curves for training, validating and testing and also capture the ROC curve for all three types of data are combined. The capture result for NN based model for the detection of SQLI attack show a good performance in accuracy, perform correctly, and true positive rate as well as false positive rate.

Dynamic and static analysis technology (DSAT) - In [11], Wang et. al., targeting PHP oriented and Application SQL Vulnerability detection method based on the Injection analysis technology. This method perform a detailed analysis on the one time injection in the aspects of data flow and program behavior based on the combination of static and dynamic analysis technology. Its implements the SQL vulnerability detection algorithm based on Lexical features comparison. Also combines alias analysis technology behavior model and SQL which is based on Lexical features comparison. In a result section some test website that selects from the open source web project of OWASP. There are Pixy, RIPS and lastly propose system tools used. The Missing report rate, False alarm rate and performance of propose system is good.

SQL Injection attack detection proposed model (SQLIADM) – Buja et. al., in [12] propose a detection model for detecting and recognizing the web vulnerability and also generate a report regarding the vulnerability level of the web application. The proposed model is based on the main detection module. The main detection module process is executed by employing the Boyer Moore string. In the process of proposed model firstly, inserting the input string and secondly main detection module based on Boyer Moore string matching algorithms with four panel reference models, which consists the crawler panel, parameter testing panel, exploit panel and report panel. This model detects the vulnerable web application with the specified criteria of the SQL injection attack with efficiency and accuracy.

Removing SQL query attributes value (RSQLQAV) - Lee et al. in [13] suggest a novel method for SQL injection attack detection based on removing SQL query attribute values. This method removes the value of an SQL query attribute of web pages when parameters are submitted and then compare it with a predetermined one. For implementation of this method used static and dynamic analysis. The web application architecture contains three parts presentation tier, CGI tier and Database tier. The SQL injection vulnerabilities are between presentation and CGI tier. Multiple methods available for protection of SQL injection attack web framework, static analysis, Dynamic analysis, combined method of static and dynamic analysis, Instruction set randomization, SQL query profiling, Machine learning method. This method use to detect Static and Dynamic analysis. The novel method remove the attribute values of SQL queries at runtime and compare them with the SQL queries analyzed in advance (Dynamic and Static method respectively.). the detection method proposed in this article uses the function f which deletes the attribute values in the SQL queries. The function is shown in formula (1). The attribute values of the static SQL queries in the web application and those of the SQL queries generated at runtime will be deleted.

$$FDQ = f(FQ),\ DDQ = f(DQ). \qquad (1)$$

Here, $\oplus$ is the symbol representing the exclusive OR operator. That is, two strings are logically exclusively ORed.

$$FDQ \oplus DDQ \begin{cases} = 0 \text{ Normal}, \\ \neq 0 \text{ Abnormal} \end{cases}$$

If we apply this formula to the above example, the following two results are obtained:

$$FDQ \oplus DDQ1 = 0 : \text{Normal}$$

$$FDQ \oplus DDQ2 \neq 0 : \text{Abnormal}$$

µ4SQLi (Mutation Operators) – Appelt et al in [14] suggest automated testing for SQL injection vulnerabilities based on Input mutation operator. This technique rests on a set of mutation operators that manipulates inputs to create new test inputs to trigger SQLI attack. This method produces effective inputs that lead to executable and harmful SQL statements. Mutation operators are classified into three classes behavior-changing, syntax repairing, obfuscation and Test Generation algorithm. This method uses two parameter for getting results SugarCRM and HotelIRS. There are total 108 input parameter for all their web services. A result without the WAF indicates that both approaches can detect vulnerabilities in the subject. Results with the WAF are even more dramatic. When testing many services with many input parameters, µ4SQLi is more effective and less costly techniques to detect exploitable vulnerabilities.

IV.CONSEQUENCES AND COMPARISON OF SQLI DETECTION TECHNIQUES

Table IV show a chart consequence of the SQLI detection techniques in brief. In Table V, show a chart of the

approaches and their detection capability against various SQLIAs.

TABLE-IV: CONSEQUENCES OF SQLI DETECTION TECHNIQUES

Approach	Overview
NN based model[10]	Its shows a good performance in terms of accuracy, true positive rate and false positive rate. The NN model performs correctly.
DSAT[11]	The missing report rate, false alarm rate and performance of system is good.
SQLIADM[12]	The model is decrease the possibility of the SQL Injection attack that can be launch onto the web application.
RSQLQAV[13]	This method is efficient and can't be implemented on web application but also used on any application connected to database.
µ4SQLi[14]	The techniques and tools performed much better than state of practice standard attack pattern. The probability of detecting SQL injection vulnerabilities is high.

TABLE- V: DETECTION APPROCHES AND SQL INJECTION ATTACK TYPE

Attack / Approaches	Tautology	Logically Incorrect Query	Union Query	Stored Procedure	Piggy Backed Query	Inference	Alternate Encodin
NN based Model [10]	X	X	√	X	√	√	X
DSAT [11]	√	√	√	√	√	√	√
SQLIADM[12]	√	√	√	√	√	√	√
RSQLQAV [13]	√	√	√	√	√	√	√
µ4SQLi [14]	√	X	X	X	X	X	X

V.ANALYSIS AND DISCUSSION

Following analysis Table –VI shows comparison of various detection techniques with respect to Techniques based on, Resources needed, Advantages and Disadvantages.

TABLE VI: ANALYSIS OF DETECTION TECHNIQUES

Detection techniques	Techniques based on	Resources needed	Advantages	Disadvantages
NN Model [10]	Artificial Intelligence (AI) and particularly Neural Network (NN).	Uniform resource locator (URL) generator, URL Classifier and NN model.	Good performance in accuracy, true positive rate and false Positive rate.	
DSAT[11]	Lexical Feature comparison	Alias analysis techniques, Behavior model, SQL Vulnerability detection algorithms	This system can test more injection points and improve the test rate of SQL vulnerabilities.	It has relatively poor performance in the single performance and cross platform test ability.
SQLIADM[12]	Boyer Moore string Matching algorithm.	Four Panel reference detection.	It is more efficient and Accurate.	The time and speed is depending on the speed Of internet.
RSQLQAV[13]	Static and Dynamic analysis	Remove the attribute values of SQL queries at runtime and compare them with SQL queries.	It's Very effective and Simple. It's Implemented Any type of database.	
u4SQLi [14]	Input Mutation operator	Behavior-changing operator, syntax repairing and obfuscation, Test Generation algorithm.	More effective, Less Costly And faster technique.	Little Bit fluctuations Between result when web application Firewall Activates or deactivate.

The analysis of various detection techniques of SQL Injection attack, Started from the NN based model [10] that perform accurately and correctly but check only Union Query, Piggy-Backed query and Inference attack then DSAT [11] that can test more injection points but relatively poor performance in single performance and cross platform test ability then SQLIADM [12] by using Boyer Moore String matching

algorithm it made possible to detect all types of attack and time and speed of detection is depending on the speed of Internet but detects more attack, then RSQLQAV

[13] Which is based on Static and Dynamic analysis that very effective and simple and also implemented in any type of DBMS but checks all type of SQLI attack.

Lastly, u4SQLi [14] which is based on Input mutation operator, when testing many services with many input parameter is more effective, faster technique and less costly and only check tautology attack.

VI. CONCLUSION

SQL injection attack is most popular in web applications. Various tools have been developed for detection. In this paper a study and analysis of various detection techniques of SQL Injection Attack is enlist. The comparison is done on the basis of detection techniques based on, resources needed for techniques implementation, advantages and disadvantages of techniques. This Consequence is useful for the evaluation of the detection techniques effectiveness.

The research is focus on the removal of SQL injection attack from top ten most dangerous attack lists. It's required to detect the SQL injection attack in database and application at same time. SQL injection attack is pervasive, so this is broad area where innovative measures needed to be taken for detection of SQL Injection Attacks.

REFERENCES

[1] Puspendra Kumar, R.K. Pateriya , "A Survey on SQL Injection Attacks, Detection and Prevention Techniques" ICCCNT'12 26th _28th July 2012, Coimbatore, India, 2012.

[2] Harish Dehariy , Piyush Kumar Shukla , Manish Ahirwar ," A Survey on Detection and Prevention Techniques of SQL Injection Attacks", International Journal of Computer Applications (0975 – 8887) Volume 137 – No.5, March 2016.

[3] Pankajdeep Kaur,Kanwal Preet Kour,"SQL Injection: Study and Augmentation", International Conference on Signal Processing, Computing and Control (2015 ISPCC), 2015.

[4] Aniruddha Holey, Prof. S. S. Sherekar, Prof. V. M. Thakare, "Analysis of web application vulnerabilities", Satellite Conference ICSTSD 2016 International Conference on Science and Technology for Sustainable Development, Kuala Lumpur, MALAYSIA, May 24-26, 2016.

[5] Chandershekhar Sharma, Dr. S.c. Jain, "Analysis and Classification of SQL Injection Vulnerabilities and Attacks on Web Applications", IEEE International Conference on Advances in Engineering & Technology Research (ICAETR - 2014) Dr. Virendra Swarup Group of institutions, Unnao, India, ,August 01-02,2014.

[6] Sum Keng Chung1, Ow Chee Yee2 , Manmeet Mahinderjit Singh3 , Rohail Hassan," SQL Injections Attack and Session Hijacking on E-Learning Systems" , IEEE International Conference on Computer,Communication and Control Technology (I4CT 2014), September 2-4, 2014 – Langkawi, Kedah, Malaysia, 2014.

[7] Amirmohammad Sadeghian, Mazdak Zamani, Shahidan M. Abdullah," A taxonomy of SQL Injection Attacks", 2013 International Conference on Informatics and Creative Multimedia Universiti Teknologi Malaysia ,Kuala Lumpur, Malaysia, IEEE, 2013.

[8] Diallo Abdoulaye kindy and Al-Sakib Khan Pathan, "A Survey on SQL Injection : Vulnerabilities, Attacks and Prevention Techniques", 2011 IEEE 15th International Symposium on Consumer Electronics (ISCE), 14-17 June 2011, Singapore, IEEE, 2011.

[9] Shubham Mukherjee,Sudeshna Bora, Pritam Sen, Chittaranjan Pradhan", SQL Injection: A Sample Review",6th ICCCNT 2015 July 13 - 15, 2015, Denton, U.S.A, 2015.

[10] Naghmeh Moradpoor Sheykhkanloo, " Employing Neural Networks for the Detection of SQL Injection Attack", SIN '14, September 09 - 11 2014, Glasgow, Scotland Uk , 2014.

[11] Yaohui Wang, Dan Wang, Wenbing Zhao, Yuan Liu," Detecting SQL Vulnerability Attack based on the Dynamic and Static Analysis Technology", IEEE 39th Annual International Computers, Software & Applications Conference, 2015.

[12] Geogiana Buja, Dr. Kamarularifin Bin Abd Jalil, Dr. Fakariah Bt. Hj Mohd Ali, Teh Faradilla Abdul Rahman," Detection Model for SQL Injection Attack: An Approach for Preventing a Web Application from the SQL Injection Attack", IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE) , April 7 - 8, 2014, Penang, Malaysia, 2014.

[13] Inyong Lee a, Soonki Jeong b, Sangsoo Yeoc, Jongsub Moon, "A novel method for SQL injection attack detection based on removing SQL query attribute values", Mathematical and computer modeling 55, 2012.

[14] Dennis Appelt, Cu Duy Nguyen, and Lionel C. Briand, Nadia Alshahwan, "Automated Testing for SQL Injection Vulnerabilities: An Input Mutation Approach "ISSTA'14, July 21–25, 2014, San Jose, CA, USA, 2014.