A Novel 3 Stage Hybrid Framework For SQLIA Detection, Prevention Using Pattern Based And Supervised Machine Learning Model

[1]Mr. B.R.Thakare, [2]Prof.D.S.Thosar

[1] *Student, Computer Engineering Department, Sir Visvesvaraya Institute of Technology, Chincholi, Nashik, Maharashtra, India*
[2] *Assistant Professor, Computer Engineering Department, Sir Visvesvaraya Institute of Technology, Chincholi, Nashik, Maharashtra, India*

ABSTRACT

Internet plays a very important role in our day to day life. Web application provides various services. As usage of web application increased, security become major concern.
Security experts from SANS, a major SQL injection threat affected 160000 websites which are using IIS , Apache and MYSQL frameworks due to lack of proper validation and security holes SQL injection.

This paper introduces two level framework for detection and prevention of SQLIA using patterns based and machine learning models. Despite of the abundance of techniques available for preventing SQL injection, issues, recently vulnerability database reported new major SQL injection threats. So it is necessary.

In proposed framework query will pass through two stages scanning for SQLIA detection and prevention. The two stages are pattern based and machine learning based. As well database firewall will be there for monitoring incoming SQL queries. If query passes all this stages, then only query is valid otherwise there is attack. The approach usage a patterns and machine learning models in which value is entered for every field is checked for SQL injection attack by parsing it.

Keyword: - *SQLIA, Internet, Machine learning, SQL Injection, web application*

1. INTRODUCTION

With the rapid development of internet, web applications are becoming increasingly popular and web application database gaining more and more value. Preventing attacks become a crucial for developers to protect database. Here, the important point is what was attacked or from where and find a way to prevent it.

The SQL injection attack bypasses traditional security mechanism such as firewall and intrusion detection system. They performed through ports normal web page. As more and more usage of web application increases security risk as well.

These online services use web applications and web services. Most web attacks target the vulnerabilities of web applications. The SQL Injection Attack (SQLIA) does not waste system resources as other attacks do. However, because of its ability to obtain/insert information from/to databases, it is a strong threat to servers like military or banking systems. SQL injection attack is a code injection technique which is commonly used to attack the confidential data by injecting malicious SQL queries as input in entry field for execution. Typical usage of SQL injection is to leak information from database bypass authentication logic or add unauthorized accounts.

There are numerous techniques are available for SQL injection detection like malicious text detection and text based key generation. In this paper, we are introducing a novel two stage framework for SQLIA detection and prevention using patterns and machine learning. As well database firewall used. If query matched all constraints, it will allow executing otherwise it will be prevented.

First we introduced the SQL injection, then related work where we describe SQL injection types, different tools, and various systems. Next the actual proposed framework with its design and implementation. Then we present the conclusion of above work with future scope.

1.1 DEFINITION OF SQL INJECTION

SQL injection is method of abusing web application that use client supplied data in SQL queries. It uses to insert SQL Meta characters and commands into web degraded inputs fields. In order to operate the accomplishment of the back end SQL queries.
An intruder, who wants to perform an injection, enters malicious query input in place of original query structure. SQLIA method that attack the data driven applications. There are two types of attacks:

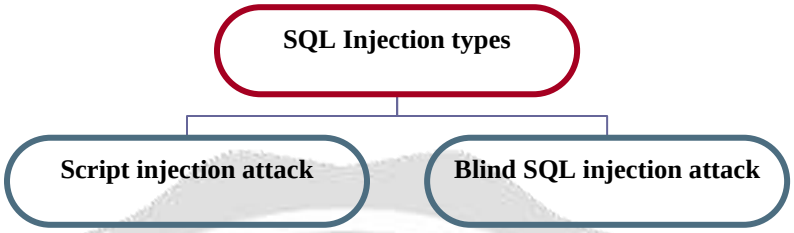

Fig - : SQL Injection types

Example:
Original query:
Select * from users where uid='admin' and password='admin@123', if the attacker's input uid=' or '1 '=' 1', then SQL query string will be
select * from users where the uid = " or '1' ='1' and Password=", we can see that the query conditions are always true, that is, there are some records as the results of the query, so the user certification is success, which contrary to the original intention of the program.

The attacker did not enter the correct user name and password and can still login the system, the attacker exploit the system by SQL injection through the careful construction of the special SQL statements. The web application build on the technology of Active/java server pages, ASP, PHP, Perl and SQL server, Mysql, Oracle, DB2, Sybase, etc. are likely to have this vulnerability. Because some database servers provide powerful access to the command line shell and registry functions, the attacker can not only query, modify, insert the database but also even control the entire database server.

1.2 SQL INJECTION TYPES

There are different types of SQL injection attacks.

A. Logically Incorrect Queries :- Beneficial information are retrieved when unwanted queries arise which helps the intruder for attack Then the attacker injects junk input to the SQL query such as type mismatches, logical errors etc.

B. Piggy-Backed Queries: In piggy-backed queries the attacker endeavors to piggy-back additional queries to the original query. Here the attack is performed by injecting query delimiter like ";".

C. Timing Attacks: In timing attacks, the database interruption response leads to information gain. This technique uses IF-THEN clause for SQL injection.

D. Stored Procedure: The attacker uses stored procedure in database system. It is a code which is susceptible as program code.

E. Blind Injection: In some cases the programmers while preparing code hides some errors which later on helps the attackers to get into the confidential areas.

F. Tautologies: This attack helps to inject SQL tokens to conditional query statement which when evaluated give true always.

1.3 PURPOSE OF SQL INJECTION ATTACK

Sr. No.	Parameter For Classification	Attack Type
1	Purpose of attack	▪ Database finger printing ▪ Analyzing schema ▪ Extracting data ▪ Amending data ▪ Executing dos ▪ Equivocating detection ▪ Bypassing authentication ▪ Remote control
2	Input Source	▪ Cookies ▪ Server variable ▪ Second order injection
3	Technical difference	▪ Classical SQLIA ▪ Out of band SQLIA
4	Technique based	▪ Tautology ▪ Illegal queries ▪ Union query ▪ Piggyback query ▪ Stored procedure ▪ Alternate encoding

2. LITERATURE SURVEY

Literature survey is very paramount for gaining and understanding much more erudition about concrete area of a subject. It is unfeasible to produce complex applications without defects, and even when this occurs, it is impossible to know it, prove it, and repeat it systematically. Software developers cannot assure code scalability and sustainability with excellence and security, even when security is defined from the ground up. One of the aspects that contribute to security quandaries seems to be cognate to how lamentable different programming languages are in terms of propensity for mistakes Clowes[5] discussed common security problems associated to the easiness in programming with PHP and its features, but this affects many other programming languages. The choice of the type system (strong or weak) and the type checking (static or dynamic) of the programming language also affects the robustness of the software. For example, a strong typed language with a static type checking can help deliver a safer application without affecting its performance. Scholte et al.[6] presented an empirical study on a large set of input validation vulnerabilities developed in six programming languages. However, that work focused on the relationship between the specific programming language used and the vulnerabilities that are commonly reported, not going into details in what concerns the typical software faults that originate vulnerabilities, like we do in the present work.

3. DESIGN AND IMPLEMENTION OF PROPOSED FRAMEWORK

Before presenting the new method, let's look at the architectural layers of web applications as shown in Figure 1 below.

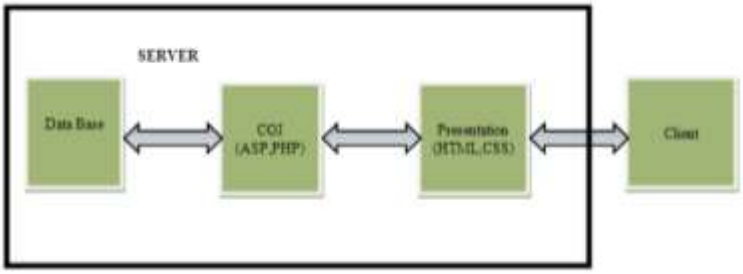

Fig. 1 Different layers of Web Applications

The presentation layer is the graphical user interface (GUI) which shows the results of the user request. The CGI layer is responsible for processing tasks at the server. As we discussed above, methods of detecting and preventing SQLIAs are either static which happens at the Database layer or dynamic which happens at the CGI layer or machine learning or combined method.

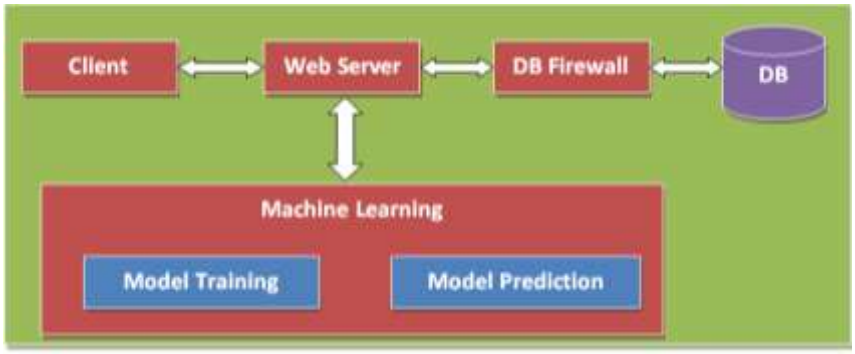

Fig .2 Proposed Framework block diagram

The Proposed framework is basically divided in to following entities and modules

1) Client- The Client layer represents the user's web browser which communicates with the server.
2) Web Server- The languages which are used in this layer are the server-based languages like ASP, PHP, etc. At the Database layer, the data related to the web application are saved and in case a request from CGI is received, the proper result will be sent to the client.
3) DB Firewall- For increasing security of database, the firewall will be installed and used to prevent the SQLIA. It will helpful for detecting invalid queries.
4) Machine Learning- the supervised machine learning models are used for sql injection detection and prevention. The supervised machine learning models will be used.

4. CONCLUSION

This paper presents a novel framework for detection and prevention of SQLIA attacks. As the popularity of web application increasing, the security of web application is major concern. SQL Injection attacks are the costly and dangerous attacks on web applications: it is a code injection technique that allows attackers to obtain unrestricted access to the databases and potentially delicate information like usernames, passwords, email ids, credit card details present in them. It covers the broad introduction to SQL injection attacks and their types. As well the literature review present the various concepts proposed by various researchers in the field of SQL injection. Then the various purposes of SQL injection attack are elaborated. The proposed framework is using machine learning approach for prevention and detection of SQLIA attack as the day by day, the way of attack is changing. The framework also usage the pattern based detection and prevention of SQLIA attack.

5. ACKNOWLEDGEMENT

I am colossally gratifying to Dr. K. T. V. Reddy, Principal, Sir Visvesvaraya Institute of Technology (SVIT), Nashik for inspiring me towards this and for implausible backing and leadership too. As well we prolong obligations towards Prof. Shedge K. N. (Asst.Professor), HOD M. Tech (CSE) of Computer Engineering Department, Prof. Thosar D. S., Assistant Professor and M.E Coordinator and Staff Members for their appreciated Assistance and Provision.

.

6. REFERENCES

[1]. Yakkala V Naga Manikanta ,Protecting Web Applications from SQL Injection Attacks by using Framework and Database Firewall International Conference on Advances in Computing, Communications and Informatics (ICACCI-2012)

[2]. Lwin Khin Shar and Hee Beng Kuan Tan- Defeating SQL Injection

[3]. Jose´ Fonseca, Nuno Seixas, Marco Vieira, and Henrique Madeira Analysis of Field Data on Web Security Vulnerabilities, IEEE Transactions On Dependable And Secure Computing, Vol. 11, No. 2, March/April 2014

[4]. Chen Ping, Wang Jinshuang, Pan Lin, Yu Han Research and Implementation of SQL Injection Prevention Method Based on ISR 2016 2nd IEEE International Conference on Computer and Communications

[5]. S. Clowes, ―A Study in Scarlet, Exploiting Common Vulnerabilities in PHP Applications,‖ http://www. secureреality. com.au/studyinscarlet.txt, 2013.

[6]. T. Scholte et al., ―An Empirical Analysis of Input Validation Mechanisms,‖ Proc. ACM Symp. Applied Computing, pp. 1419-1426, 2012.

[7]. https://www.owasp.org

[8]. Detection of SQL Injection Attacks by Removing the Parameter Values of SQL Query Rajashree A. Katole SGBAU, Amravati, Maharashtra, India. 978-1-5386-0807-4/18/©2018 IEEE