iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4060

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Prevention of SQL Injection Attack by Checking the given Input Strings

Reetik Mathankar[1], S V Athawale[2]
[1, 2]*Department of Computer Engineering, AISSMS-COE, Pune*

Abstract: ***Today, the internet has become a very important place, whenever it comes to sharing of information the first thing that comes to mind is the great "Internet". But as technology advances, the threats become even greater. Hackers always have their eyes over the databases that are stored in the servers of respective websites. SQL injection is the most lethal technique to compromise a database. It fools the database by executing some malicious code and thus gains the access. SQL Injection also stands first in the list of top ten web application vulnerabilities published by OWASP(Open Web Application Security Project). This paper discusses the way of dealing with such SQL Injection attacks by checking or comparing the input string given to the database.***

Keywords: **SQL Injection, String Compare, SQL Injection Attack Prevention, SQL Database**

I. INTRODUCTION

In today's world internet has become as important as electricity in our day to day lives. If the internet goes down for a day not only commercial but also social work will get affected. On the internet there exists the World Wide Web a.k.a WWW, which is nothing but an information space that stores resources and documents that can be shared around the world. There are many websites available on the internet that can be accessed by the people. Databases are used to store the documents, images, videos, etc that are to be displayed on the website. Websites using SQL databases can be compromised by hackers using SQL Injection attacks which tops the OWASP list.

SQL is a standard language used to access and manipulate databases. It is quite an irony and shameful as well since prevention of SQL Injection attack is really easy but still it is the most used attack to compromise the database. SQL Injection also known as SQLi in short, is an attack that executes some malicious SQL statement to gain access or manipulate the database in an unauthentic way. An SQL Injection attack if successful can result in unauthorized viewing of database. Here checking and validating the input string plays an important role in the prevention of attack. It becomes easy for a hacker when the coding of the web application is poor.

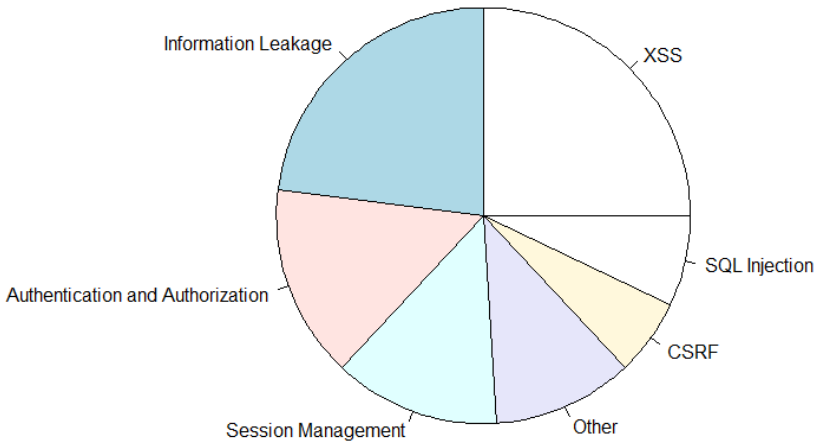


Fig. 1 Web Application Vulnerabilities

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

II. LITERATURE SURVEY

A. Padma N Joshi. [1] discussed the method of preventing SQL Injection by performing the following steps: Getting the input from User-Interface, then by checking the pattern to avoid SQL Injection, next step is to check user database with id and password, and the final step is if user is not valid then failure otherwise login would be successful.

B. S. Parveen. [3] briefly discussed the different types of SQL Injection attacks along with their brief explanation. They have proposed three main techniques for SQL Injection Prevention: Static, Dynamic and Hybrid and also when these methods are suitable to use are explained.

C. Benjamin Appiah. [2], proposed a unique method to prevent injection has been discussed by using fingerprints and pattern matching. In this method, the whole string is tokenized and is checked for single quotes (‘), double quotes (“), and backslashes (\) if any as they are not included in structure from the query.

D. Yi Wang. [4], has given an approach using three vector kernel using SVM to prevent SQL Injection. It brings more accuracy since it classifies more information than using syntax or context analysis by itself.

III. TYPES OF SQL INJECTION

To prevent an SQL Injection attack we must know about the types of SQL Injection. Some basic types of SQL Injection attacks are:

A. Union-Based SQLi

Union-based SQLi as the name suggests makes use of UNION operator to join results of two or more statements in a single result. It is crafted such that two queries can return the result at once.

B. Error-Based SQLi

An Error-based SQLi gives the hacker the data by giving out the error messages. It is so dangerous that a hacker can even get the whole structure of database using Error-based SQLi.

C. Blind SQLi

This is a type of attack that asks the database true or false questions. The attacker steals the data by asking a series of questions to the database.

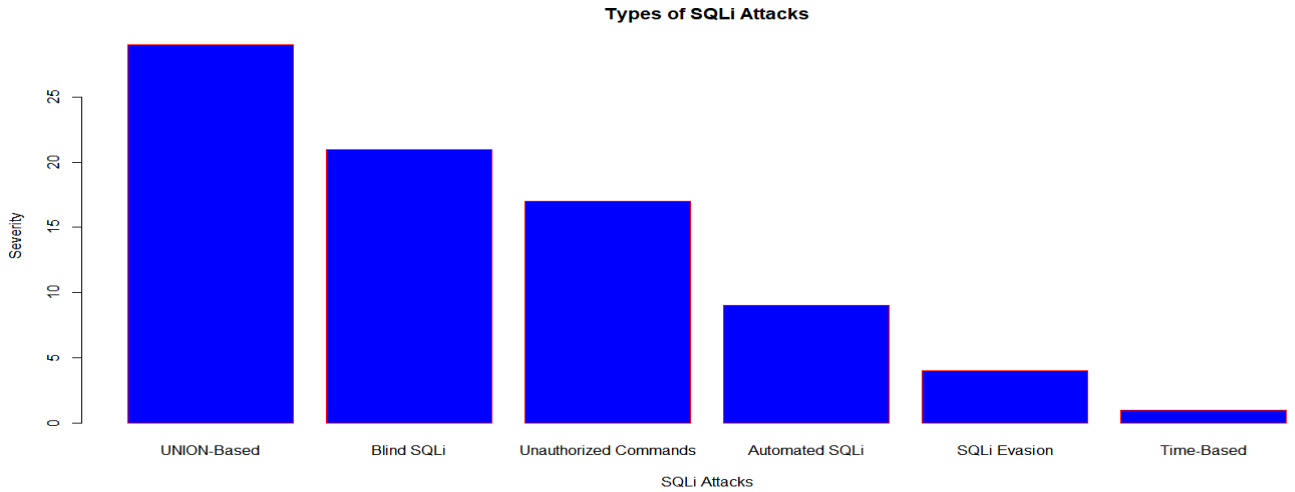


Fig. 2 Different types of SQLi

IV. PREVENTION METHOD FOR SQLI

Firstly it is important to understand what SQL queries are, in SQL, queries are formal question used to either retrieve data or update, insert data in tables of database. It is a string which consists of keywords, identifier, operators, and constant values. To detect an SQL Injection attack, the web application should determine whether the query is genuine or not. The basic idea is to store all the possible malicious queries and compare them with the given input query. For comparison, we will be creating a small framework which will store the malicious queries and compare them with the input queries.

This framework needs to be updated with the new emerging queries. An efficient algorithm to search the query can be implemented to produce the result faster. The following flowchart will display the methodology:

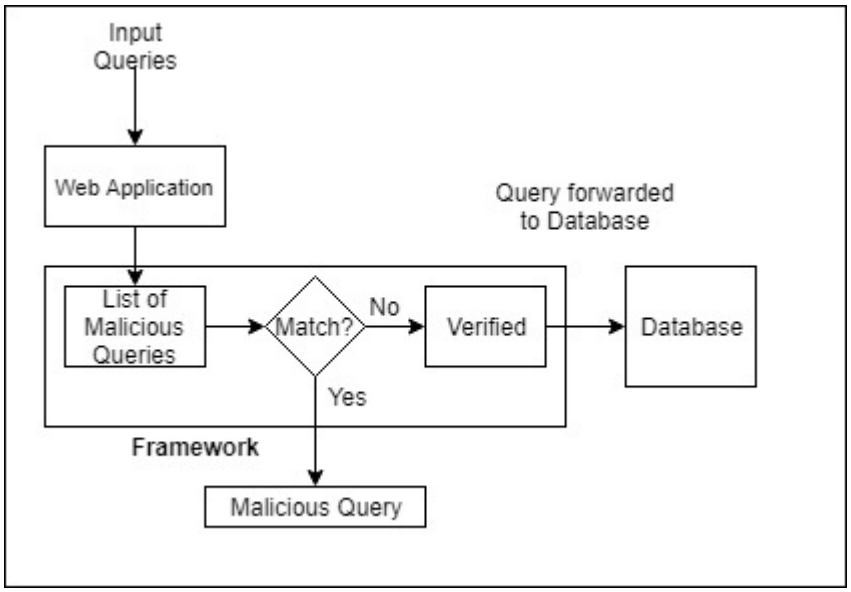


Fig. 3 Structure of Framework

Though this method will prevent most of the common basic SQL Injection attacks, this isn't a foolproof prevention technique. There are tools available to find out the SQL Injection vulnerabilities in a web application. Some of the best tools are mentioned below:

1) *BSQL Hacker:* This tool is for those who want an automated attack on the web application. This tool is mainly used for blind SQL injection attack. It performs multi-threaded attack for faster results.
2) *Safe3 SQL Injector:* This tools also makes the process of Injection automatic and helps the hacker to gain access to the database.
3) *SQLMap:* This is an open injection tool and the most popular among SQL Injection tools. It also provides a detection engine which can be used to prevent an intrusion.

V. CONCLUSIONS

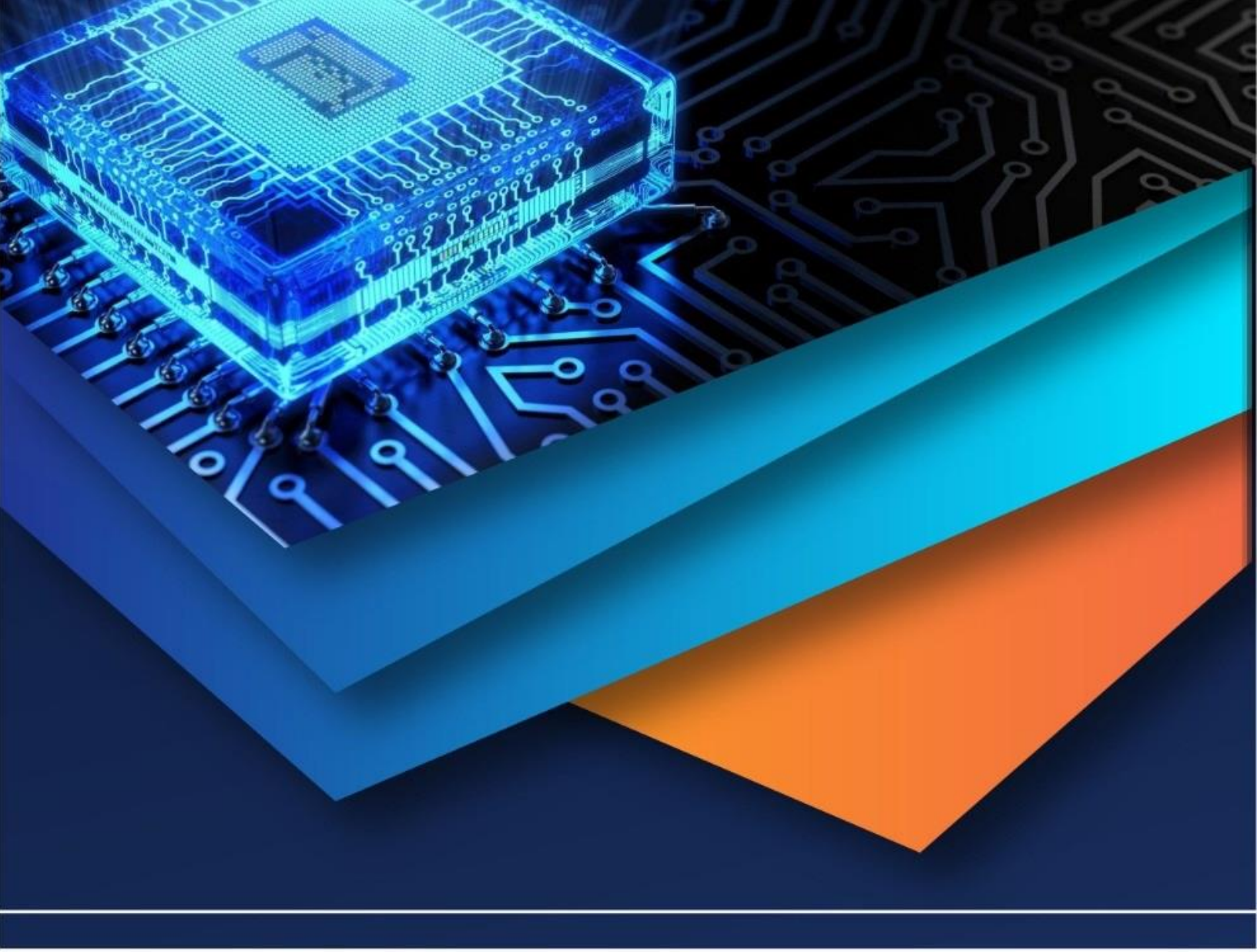
SQL Injection attacks are easy to prevent if web applications are properly coded. There must be an awareness amongst the developers about different vulnerabilities as well. Our framework is easy to implement but must be regularly updated. Hence we conclude SQL Injection Attacks which will be using some malicious string if matched with the strings in our framework will block the attack.

VI. ACKNOWLEDGEMENT

I would like to thank Prof. Mr S. V. Athawale Sir, under whose guidance I was able to come up with this method to prevent SQL Injection Attacks. I would also like to thank my family members and my friends who helped me throughout.

REFERENCES

[1] Padma N Joshi, N. Ravishankar, M. B. Raju and N.CH. Ravi, "Encountering SQL Injection in Web Applications", 2018 Second International Conference on Computing Methodologies and Communication(ICCMC), Year: 2018, Pages: 257-261.
[2] Benjamin Appiah, Eugene Opaku-Mensah and Zhiguang Qin, "SQL Injection Attack Detection Using Fingerprints and Pattern Matching Technique", 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), Year: 2017, Pages: 583-587.
[3] S. Parveen, "SQL Injection Impact on Web Server & Their Risk Mitigation Policy Implementation Techniques An Ultimate solution to Prevent Computer Network from Illegal Intrusion", International Journal of Advanced Research in Computer Science Volume 8, No. 3, March – April 2017.
[4] Yi Wang and Zhoujun Li, "SQL Injection Detection via Program Tracing and Machine Learning", Internet and Distributed Computing Systems, Year: 2012, Pages: 264-274
[5] Testing for SQL Injection. Retrieved 28 March 2019, from https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005)
[6] Best free and Open Source SQL Injection Tools [Updated 2019]. Retrieved 28 March 2019, from https://resources.infosecinstitute.com/best-free-and-open-source-sql-injection-tools/#gref
[7] Types of SQL Injection. Retrieved 26 March 2019, from https://latesthackingnews.com/2017/10/31/types-of-sql-injection/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY