Septic: Detecting Injection Attacks and Vulnerabilities inside the DBMS

Pratiksha Garkar[1], Varad Arthmwar[2], Ganesh Gaikwad[3], Mohini Chavan[4], S.K.Patil[5]
[1234]BE Students, [5]Professor,
[12345]Department of Computer Engineering, Marathwada Mitramandal's Institute of Technology, Lohgaon, Pune -411047.

Abstract- Now day's database attacks are increase rapidly. Database continue to be the most commonly used backend storage in enterprise, but they are often integrated with vulnerable application, such as web frontends, which allow injection attacks to be performed. The effectiveness of such attacks we lose our confidential data in fraction of second. This leads to subtitle vulnerabilities in the way input validation is done in application. In this paper, we propose SEPTIC (Self-Protecting Databases from Attacks), a mechanism for DBMS attack prevention, which can also assist on the identification of the vulnerabilities in the applications.

Keywords- SQL injection, Attack Detection, Attack Prevention, DBMS, Machine Learning.

I. INTRODUCTION

Our project deals with detection of SQL injection attack. SQL injection nothing but code injection technique that break a security of database layer of an application. Our project deals with detection of SQL injection attack and block that user who try to break the database security. SQL Injections can manipulate data (delete, update, add etc.) and corrupt or delete tables of the database. It is used to attack data-driven application. Lack of input validation is a major vulnerability behind dangerous database attacks. By taking advantage of this, attacker scan injects their code into applications to perform malicious tasks. In which malicious SQL statements are into an entry field for execution. The attacker send a specially encoded SQL statement that is designed to break the database security and access the confidential data. Incorrectly validated or non-validated string literals are concatenated into a dynamic SOL statement and interpreted as code by the SQL engine. We propose DBMS system to detect and block attacks in runtime without programmer intervention. To implement SEPTIC mechanism, we develop an online shopping application that consists of list of cloths displayed in various materials and designs. The user may view these products as per categories. If the user likes a product, user can easily add it to user shopping cart.

Once user dam wishes to buy product now, user must register on the site first. Once the user makes a successful transaction then admin will get report of his bought products which is display at order list. The objective of this project is providing security for transaction done by the user. Using AES (Advanced Encryption Standard) encryption technique. We use ASE technique to transaction and user account details can be made secured. AES encryption is also used to encrypt the user's card and password information while transaction.

II. MOTIVATION

Preventing the web and business application databases by attackers.
Detecting the attack inside the DBMS.

III. LITERATURE REVIEW

In [1] paper presents a Some of the most dangerous web attacks, such as Cross-Site Scripting and SQL injection, exploit vulnerabilities in web applications that may accept and process data of uncertain origin without proper validation or filtering, allowing the injection and execution of dynamic or domain-specific language code. Propose a model that highlights the key weaknesses enabling these attacks, and that provides a common perspective for studying the available defences. We then categorize and analyse a set of 41 previously proposed defences based on their accuracy, performance, deployment, security, and availability characteristics. Detection accuracy is of importance, as our findings show that many defence mechanisms have been tested in a poor manner. In addition, we observe that some mechanisms can be bypassed by attackers with knowledge of how the mechanisms work.

In [2] paper an attempt has been made to develop an online shop that allows users to check for different cloths for women's available at the online store and can purchase cloths online. The project consists of list of cloths displayed in various materials and designs. The user may browse through these products as per categories. If the user likes a product, he/she can add it to his/her shopping cart. Once user wishes to checkout he must register on the site first. Once the user makes a successful transaction admin will get report of his bought products. The objective of this project is to develop a secure path for transaction done by the user. Using AES (Advanced Encryption Standard) encryption technique, the transaction and user account details can be made secured.

In [3] In this paper, we studied the scenario of the different types of attacks with descriptions and examples of how attacks of that type could be performed and their detection & prevention schemes. It also contains strengths and weaknesses of various SQL injection attacks. It is known to all that SQL injection attacks easily prevented by applying more secure schemes in login phase and after login phase. Therefore, we implement our proposed scheme called SQLENCP, the SQL injection prevention by encryption & hashing techniques, to handle the SQLIA and prevent them. Although, the proposed implemented system is unable to handle all the SQL injection attacks, but it can prevent tautology attacks, union based query attacks & illegal structured query attacks. A proposed a new approach that is completely based on the hash method of using the SQL queries in the web-based environment, which is much secure and provide the prevention from the attackers SQL. But, our proposed strategy requires the alterations in the design of existing schema database and a new guideline for the database user before writing any new database. Through these guidelines, we found the effective outcomes in SQL injections Preventions. After that we compared these techniques in terms of their ability to stop SQLIA.

IV. PROPOSED SYSTEM

As we are developing an online application in which the work of both user and admin is mandatory and the essential factor is that as the user select the product it is put into the cart for further process but before that we need to have an account on that web online shopping based application so that in future we can access that account again. Here the work of the user is to shop or can say buy a product and admin work is to display the product in terms of many categories. The purpose to developed is the prevention in two aspects. While accessing the account that is in running time online prevention and second one is when we store our personal details.

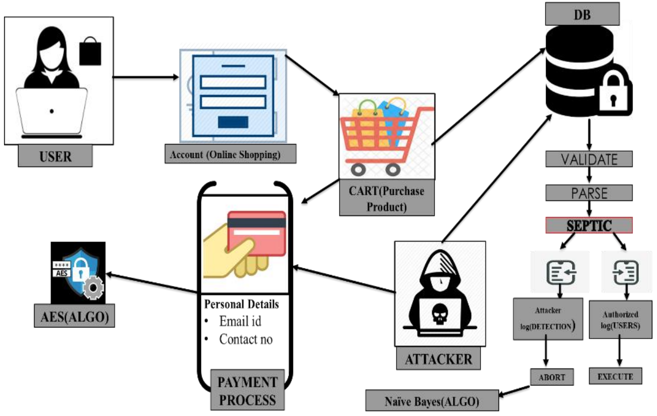

Fig.1: System Architecture

The main contributions of this paper are:
(1) Detect the SQL injection attacks.
(2) stop the databases attack and provide security to database.

V. SYSTEM ARCHITECTURE

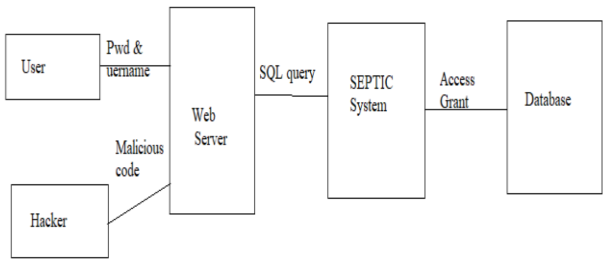

Fig.2: System Architecture

- **Naïve Bayes:**

Detection of SQL Injection attacks using a machine learning algorithm called Naïve Bayes Naïve Bayes is a classification machine learning algorithm that assumes that an incident is unrelated to and is independent of other all other incidents. Naïve Bayes classifier is used to classify between malicious and non-malicious SQL queries.

- **ASE Algorithm:**

AES stands for Advanced Encryption Standard used to protect the confidential data from attacker. The AES is more secure than DES. In AES encryption divided into three phase 1] Initial Round 2] Main Round 3] final Round. These three phase contain different operations To decrypt cipher text by using AES (Advanced Encryption Standard) perform three operation on cipher text.

1] Inverse Final Round 2] Inverse Main Round 3] Inverse Initial round. AES is based on different keys size like 128, 192, and 256 bits

- **SEPTIC:**

In this we are using SEPTIC methods for prevention of database system from different type of attacks from attacker by following three modes.

1] Training Mode
2] Detection Mode
3] Prevention Mode

VI. ADVANTAGES

- To keeping confidential data secure.
- Availability.
- Reduces the man-effort.
- Reduce data redundancy.

VII. CONCLUSION

This System define the way provide protection from attacks against web and business application databases. It defines the idea of catching attacks inside the database, protected from attacks. The top threat related to databases are SQL injection can be prevented by system.

VIII. REFERENCES

[1]. Dimitris Mitropoulos, Panos Louridas,† Michalis Polychronakis,‡ and Angelos D. Keromytis, “Defending Against Web Application Attacks: Approaches, Challenges and Implications”, IEEE_Transactions on Dependable andvSecure Computing Volume: 16 , Issue 2 , 2019.

[2]. Karan Ray, Nitish Pol, Suraj Singh Guided by Prof. SUVARNA ARANJO, “Detecting Data Leaks via SQL Injection Prevention on an E-Commerce”, International Journal of Scientific & Engineering Research Volume 9, Issue 3, March-2018.

[3]. Anamika Joshi, Geetha V “SQL Injection detection using machine learning”, 2014 International Conference onControl, Instrumentation, Communication and Computational Technologies (ICCICCT)Vijin P, Suhail Basheer V, Shaab Mon PK, Sabin MK, “Advanced Vehicle Over Speed Detection and Billing System (AVODABS)” , International Conference on Green Engineering and Technologies,IEEE 2015

[4]. Mayank Namdev , Fehreen Hasan, Gaurav Shrivastav, “A Novel Approach for SQL Injection Prevention Using Hashing & Encryption (SQL-ENCP)”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3, 2012.

[5]. Ammar Alazab Al-Balqa, Ansam Khresiat, "New Strategy for Mitigating of SQL Injection Attack", International Journal of Computer Applications Volume 11, November 2016.

[6]. Aniruddh Ladole , Mrs. D. A. Phalke,"SQL Injection Attack and User Behavior Detection by Using Query Tree, Fisher Score and SVM Classification", International Research Journal of Engineering and Technology Volume: 03 June-2016

[7]. Ib´eria Medeiros1 Miguel Beatriz2 Nuno Neves1 Miguel Correia2, "Demonstrating a Tool for Injection Attack Prevention in MySQL", 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks 2017