



e-ISSN: 2319-8753 | p-ISSN: 2320-6710

IJRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH


IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 3, March 2021

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.512

 9940 572 462

 6381 907 438

 ijirset@gmail.com

 www.ijirset.com



Identification Methodology for SQL Injection Attacks

Sahil Nadaf, H.A.Hingoliwala

PG Student, Department of Computer Engineering, JSPM's Jayawantrao Sawant College of Engineering,

Hadapsar, India

Professor, Department of Computer Engineering, JSPM's Jayawantrao Sawant College of Engineering, Hadapsar, India

ABSTRACT: Structured query language (SQL) may be a text language that permits manipulating the information hold on within the info through the commands like INSERT, UPDATE and DELETE etc. Code injection technique within which hacker manipulates the logic of SQL command to get access on the info and different sensitive info. Most common vulnerability gift on the network. SQL injection could be a code injection technique, accustomed attack data-driven applications, during which malicious SQL statements area unit inserted into associate entry field for execution (e.g., to dump the info contents to the attacker). The foremost common reason for info vulnerabilities could be a lack of reasonable care at the instant they're deployed. During this paper, we tend to propose a novel approach Self-Protecting databases from attacks, a mechanism for software system attack bar, which may conjointly assist on the identification of the vulnerabilities within the applications. To develop a secure path for group action done by the user AES algorithm which is an (Advanced Encryption Standard) cryptography technique, the group action and user account details is created secured.

KEYWORDS: Novel Approach, AES algorithm, Machine learning algorithm, Naïve Bayes Algorithm[1].

I. INTRODUCTION

SQL Injection is "a code injection technique that exploits a security vulnerability occurring in the database layer of an application". SQL Injection is "a code injection technique that exploits a security vulnerability occurring within the info layer of Associate in nursing application". In alternative words, its SQL code injected in as user input within a question. SQL Injections will manipulate knowledge (delete, update, add etc.) and corrupt or delete tables of the info. It's accustomed attack data-driven application. Lack of input validation may be a major vulnerability behind dangerous net application attacks. By taking advantage of this, assailant scan injects their code into applications to perform malicious tasks. Within which malicious SQL statements square measure into Associate in nursing entry field for execution. This is often a technique to attack net applications that have an information repository. The assailant would send a specially crafted SQL statement that's designed to cause some malicious action. Incorrectly valid or non-Statement and understood as code by the SQL engine. 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. He can then login using same id password next time. Frontend The middle tier or code behind model is designed in JAVA and SQL Serves as a backend to store product data thus the online shopping project brings an entire clothing shop online and makes it easy for both buyer and seller to make deals. Admin can add data about their subscribers and it will be viewed by user. The highlighted part here is encryption of card data using AES (Advanced Encryption Standard) technique. The Online Shop secures the card payment and won't let the card data to get hacked. While user doing a card payment, all the card data is encrypted and then stored into database

II. REVIEW OF LITERATURE

1. This 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 code. Propose a model that highlights the key weaknesses enabling these attacks, and that provides a common perspective for studying the available defences. Availability of source code enhances basic scientific tasks like verification and reproducibility. Secure methods can form the basis for developing methods with more extensive coverage.[1]



2. This 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 user may browse through these products as per categories. If the user likes a product, he/she can add it to his/hers 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. AES encryption is also used to encrypt the user's card and password information while transaction.[2]

3. The web is the firmest and most common medium of communication and business interchange. The attackers make use of these loopholes to gain unauthorized access by performing various illegal activities this may result in theft, leak of personal data or loss of property. The proposed classifier uses combination of Naïve Bayes machine learning algorithm and Role Based Access Control mechanism for detection our approach detects malicious queries with the help of classifier. The addition of another parameter for RBAC has increased the accuracy of detection.[3]

4. 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. 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[4]

5. In this paper, a successful SQLIAs can have serious consequences to the victimized organization that include financial lose, reputation lose, compliance and regulatory breach. To this end, we propose an approach based on negative tainting along with SQL keyword analysis for detecting and preventing SQLIA. We were able to successfully distinguish between legitimate SQL queries and malicious ones that had adopted various evasion methods such as encoding, comments and white space evasion methods as well as logical expressions and string techniques that were not captured by commercially available detection engines.[5]

6. This paper a system is proposed to detect the SQL Injection attacks by using SVM classification and Fisher Score. A lot of research is done to detect and prevent the SQL Injection attacks. To reveal data from database users with valid login id can also enter the malicious queries. Proposed System can also classify the users in to normal users or attackers according to the query submitted by them[6]

7. In this paper, every SQL Query that allows the inputs from the attacker sides can defect our real web application. Uses which are immune to SQL injection attacks validate and sanitize all user input, never use dynamic SQL injection, perform using an account with few privileges, hash or encrypt their secrets, and present error messages that reveal little if no useful information to the hacker. For information on testing your application for injection vulnerabilities, see the sidebar "Injection Testing".[7]

III. SYSTEM OVERVIEW

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 develop 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 into the database

IV. SYSTEM ARCHITECTURE

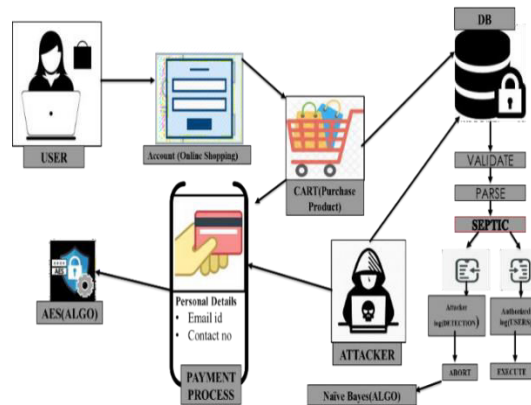


Fig. 01 System architecture

V. ALGORITHMS

- **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 a particular 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. [3]

- **AES algorithm:**

This algorithm is used for security purposes i.e., to enter the data into an encrypted form into a database.

Input: Generate an Initialization Vector (IV)

1. Generating or Loading a Secret Key.
2. Creating the Cipher.
3. Encrypting a String.
4. Decrypting Back to a String.

Output: Inserting the data into the database into an encrypted format [5]

- **Novel Approach:**

In this we are using novel approach methods for prevention of database system from different types of attacks from an attacker by following three modes:

- Training (The type of Strings that will be used by attacker) mode
- Detection (The type of attack is detected) mode
- Prevention (novel approach mechanism to detect and prevent itself) mode

VI. CONCLUSION

According to technology seller application security, the highest threat associated with databases is SQL injection. SQL injection attacks are often prevented by the new style of mechanism of SEPTIC. It jointly provides a concept of catching attacks within the software and characteristic vulnerabilities in an application code, once attacks were detected. In



future we will be able to use the mechanism to stop business connected confidential knowledge so nobody can try and gain credentials of others and exploit the victim

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 and Secure 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 on Control, Instrumentation, Communication and Computational Technologies (ICCICCT).
- [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]niruddh Ladole, Mrs. D. A. Phalke, “SQL Injection Attack and User Behaviour Detection by Using Query Tree, Fisher Score and SVM Classification”, International Research Journal of Engineering and Technology Volume: 03 June-2016
- [7]Sanchit Narang, Shivam Sharma, Rajendra Prasad Mahapatra, “Prevention of SQL injection in E -Commerce”, International Journal of Computational Engineering Research September –2015 Beach, California, USA



INNO  **SPACE**
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 **9940 572 462**  **6381 907 438**  **ijirset@gmail.com**



www.ijirset.com

Scan to save the contact details