IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

|DOI:10.15680/IJIRSET.2021.1006175|

SQL (Structured Query Language) Injection Attack inside DBMS with Novel Methodologies

Miss.Risha Jilhawar[1], Mr.Rahul Deore[2], Mr.Mandar Tribhuwan[3], Mr.Ashutosh Kelkar[4], Prof.Priyanka Nanaware[5]

B.E Students, Department of Computer Engineering, Sinhgad Academy of Engineering, Kondhwa, Pune, India[1,2,3,4]

Department of Computer Engineering, Sinhgad Academy of Engineering, Kondhwa, Pune, India[5]

ABSTRACT: Databases are utilized in many facets of your everyday life because they allow data to be saved fast and conveniently. SQL injection is a code injection approach for attacking data-driven systems that involves inserting sql Queries into an entry field for implementation (e.g., to dump the database contents to the attacker). Sql vulnerability are most commonly caused by a lack of due diligence when they are implemented. In this research, we present SQL injection prevention method, a DBMS detection and mitigation technique that can also aid in the detection of attackers. We create an online shopping application to apply the SQL injection prevention method. The most typical source of database problems is a lack of due diligence at the time when the database was created. The customer has the option of browsing these items by category. A user can add a purchase to his or her shopping basket if he or she likes it. If a person wants to check out, he must first register on the site. After the user completes a successful transaction, the admin will receive a summary on the things he purchased. To create a safe way for user transactions, the AES algorithm (Advanced Encryption Standard) encryption technology may be used to safeguard the transactions and user account credentials. They've been dispatched.

.

KEYWORDS: SQL injection, Attack Detection, Attack Prevention, DBMS, Machine Learning.

I. INTRODUCTION

SQL Injection is defined as "a script injector that leverages a security flaw in an application's data layer." To put it differently, its SQL code injected as users enter into a query. Injection Attacks can destroy or remove table data as well as change data (delete, update, add, etc.). It's a kind of malware that targets content applications. A fundamental flaw in harmful web app assaults is the unavailability of access control. An attacker scan exploits this by injecting their malware into programmed to execute malicious actions. Injecting Malicious queries are entered into an input field and executed. The intruder would transmit a specially constructed SQL declaration that would induce a certain harmful behavior. Incorrectly validated or unvalidated bridged are combined in a dynamically SOL declaration and evaluated as the SQL engine code. In order to identify and stop assaults in operation without programming effort, we present modification – hacking – DBMS prevention measures. An online shop that enables customers of the e - commerce website to look for various clothes for ladies, and to buy clothes online. The project includes a collection of textiles presented in different materials and styles. These goods can be seen by the user according to the classifications. The next time you log in, you may also use the same password. Users can now pay via card. Once the user successfully manages the transaction, his purchased items will be reported. This way you'll create the whole frontend with HTML, CSS, JSP and JavaScript. In JAVA and SQL Server, the intermediate stage or code underlying the model is intended as a background for stocking product data, making online shopping easier for both buyer and seller to place deals.Admin may add information about your customers and the visitor will see it. The most important aspect is the encryption of card data via the AES technology. The Ecommerce Website valid contract for the account and does not accept tapping of the card data. All card information is secure and then saved on the database when the user makes a card payment

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

|DOI:10.15680/IJIRSET.2021.1006175|

II. REVIEW OF LITERATURE

A presentation of this paper Some of the most severe online attacks, for example Cross-Site Scripting and SQL injection, use vulnerability in online applications, allowing the insertion and execution of dynamic or domain-specific language code to accept and handle unsure origin data without sufficient validation or filtering. Suggest a model that emphasises the principal flaws that allow such assaults and that offers a shared view of the potential defences. Source code accessibility improves key scientific activities such as testing and reproductivity. The development of approaches with a broader scope can be based on safe procedures. [1]This article attempts to create an online shop that enables customers to check on the various clothing for women in the online shop and may buy clothes online. These goods can be seen by the user according to the categories. You may add it to your shopping cart when the consumer loves a product. Upon check-out, the user must first register on the website. Once the user successfully manages the transaction, his purchased items will be reported. The goal of this project is to establish a safe user transaction path. The transaction and user account credentials may be safeguarded with the use of AES (Advanced Encryption Standard) encryption technology.[2] The Internet is the most prevalent and corporate communication and exchange media. These loop holes are used by attackers to get unauthorized access by carrying out different illicit actions It can lead to robbery, personal information leakage or property loss. The classifier presented employs the combination of the machine learn algorithm and role-based access detection mechanism Naïve Bayes Our solution uses the classifier to detect malicious requests. Adding additional RBAC parameter increases detection accuracy. [3]We explored in this work the many sorts of assaults with descriptions and examples of how such assaults may be carried out and how their systems for detecting and preventing them have been identified. It also has the strengths and limitations of other SQL attacks. A proposed new solution which is entirely based on the hash technique for the use of Web-based SQL queries, which is safe and offers SQL attacker avoidance. [4]

In this article, successful SQLIAs may have substantial effects, including financial loss, reputation loss, conformance and regulatory violations, for the afflicted firm. We suggest a negative spot-based technique to identify and prevent SQLIA, together with SQL keyword testing. We were able to distinguish successfully between legitimate SQL queries and malicious ones which had used different methods of evasion such as encoding, commenting and white space avoidance, as well as logical expressions and stringing techniques not captured by commercially available sensing devices.[5]This document proposes a solution to identify assaults from SQL Injection using the Fisher Score and the SVM classification. Much research has been undertaken to identify and mitigate attacks from the SQL Injection. Malicious queries can also be entered in order to disclose data from database users with a valid login id. The system suggested may also categorise people according to the inquiry made in normal users or assailants. [6].Every SQL query that enables an attacker to get inputs potentially fault our actual web application in this article. Any application that is SQL-immune validates and purges the user input, never uses the dynamic SQL injection, does not utilise a few privileges account, hash or encrypt secrets, and displays error messages that provide little or no relevant information to hackers. See the sidebar "Injection Testing" for details on testing your application for injection vulnerabilities. [7]

III. SYSTEM OVERVIEW

When we develop an online application, where both user and admin work are mandatory, it is vital to place it in the cart for further processing as the user selects the product but, before doing so, we have to have a shopping online web application account to ensure that this account is accessible in the future again. Their use is essential. Here the user's job is to shop or can tell him to purchase a product and the admin work will show the product in various categories. The aim to be developed is two-fold prevention. When we visit the on-line preventive account in due course and when we store our personal data in the database, secondly.Here we are using two algorithms for prevention one is for encrypting the user’s mandatory data and second is the detection of sql injection string from which attack can be occurred at user login page we use Naive Bayes Algorithm for detection of string

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

|DOI:10.15680/IJIRSET.2021.1006175|

IV. SYSTEM ARCHITECTURE

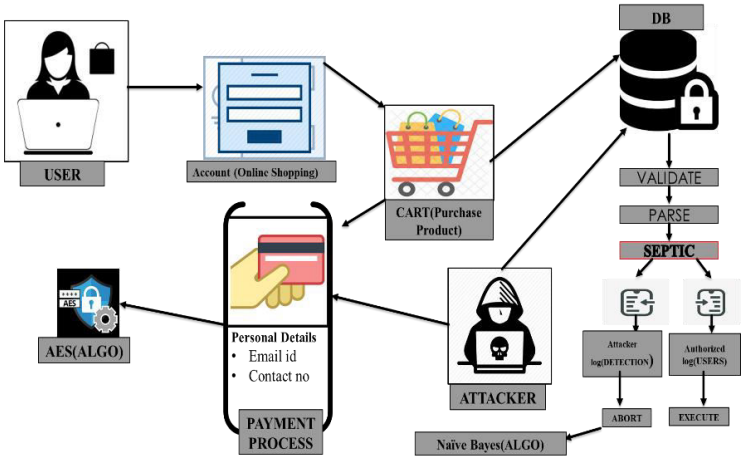

Fig. 01 System architecture

V. ALGORITHMS

- **Naïve Bayes:**
  SQL Detection Attack utilizing a Naïve Bayes machine learning technique Naïve Bayes is a method for classifying machines, which assumes that one occurrence does not link to or is independent of prior episodes. Classification Naïve Bayes is used to categories dangerous SQL queries between non harmful and malignant.[11]
  This article identifies SQL threats with a Naïve Bayes master learning method. Naïve Bayes is a method for classifying machines, which assumes that one occurrence does not link to or is independent of prior episodes. In this article, the classification of Naïve Bayes is utilized to categories harmful or non-malicious SQL queries. They've utilized a training dataset that contains malicious and non-malicious SQL queries to train the model and additionally each query is marked with this training data. [1]
  Data labelling helps the model understand what is harmful and what is not harmful. Such a model is referred to as a supervised machine model. Once the model has been trained, the test dataset uses it to check if the model appropriately categorizes the SQL queries.[4]

Flow of the Code:

1. Read each test file, remove stop words, perform stemming and load in to objects.

2. Read each training file, remove stop words, perform stemming and load in to objects.

3. For each test file, for each class name, for each word; check if the probability already exists in cache.

4. Else compute the probability of each word and multiply them to get overall probability for the test file.

5. Check which probability has maximum among the classes for the test file which gives the class value of the file

- **AES algorithm:**

This technique is used to input data in a database in encrypted format for security purposes. When a registered user wishes to login, the username and password can be encrypted using the secret user key AES encryption method. A query is then generated automatically You will use the encoded username and password. You ought then to have a look at it. Rabin query encryption is used to encrypt public server key and delivered to the server when encryptedInput:

1. Generate an Initialization Vector (IV)
2. Generating or loading a Secret Key.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

|DOI:10.15680/IJIRSET.2021.1006175|

3. Creating the Cipher.
4. Encrypting a String.
5. Decrypting Back to a String.

Output: Inserting the data into the database into an encrypted format

- **Sql Injection Attack Detection and Prevention:**

In this we are using Sql Injection Attack Detection and Preventionmethods for prevention of database system from different type of attacks from attacker by following three modes:

- Training mode
- Detection mode
- Prevention mode

VI. RESULT AND DISCUSSIONS

Experiments are done by a personal computer with a configuration: Intel (R) Core (TM) i3-2120 CPU @ 3.30GHz, 4GB memory, Windows 7, MySQL 5.1 backend database and jdk 1.8. The application is web application used tool for design code in Eclipse and execute on Tomcatserver. According to technology vendor application security the top threat related to databases are SQL injection can be prevented by the new form of mechanism of Sql injection detection and prevention it also gives an idea of catching attacks inside the DBMS and identifying the vulnerabilities in an application code, when attacks were detected. In future we can use the mechanism to prevent business related confidential data so that no one can try to gain credentials of others and exploit the victim

1. Database: Attacks detected and stored into the database according to the type of attack

BiD	BlindString	ip
1	ruchikakamble@gmail.com' or '1'='1	LAPTOP-IMRFCHES/192.168.43.115
2	' or '1'='1	LAPTOP-IMRFCHES/192.168.43.115

Fig 2: Attacks detected and type of attack

2. Data is also stored into the log file and tells which type of attack it is
3.

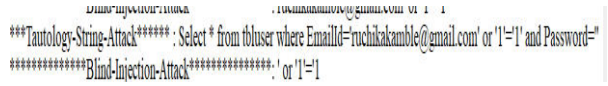

Fig 2: Attacks detected and Data is also stored into the log file

4. Database store users password in encrypted format using AES Algorithm

Password
2L3ZxmMyejmh8spjLxgERw==
Ru@123
/ESTDy1wiCFYAgyZ4raAtQ==
ralMAPktD7BTSnqBq2nIIw==

Fig 3 users password in encrypted format is been stored in database for security

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

|DOI:10.15680/IJIRSET.2021.1006175|

	Algorithm	Accuracy
Existing Algorithm	DES	69%
Proposed Algorithm	AES	93%

Fig. 4 Accuracy associated with algorithm for encrypting data

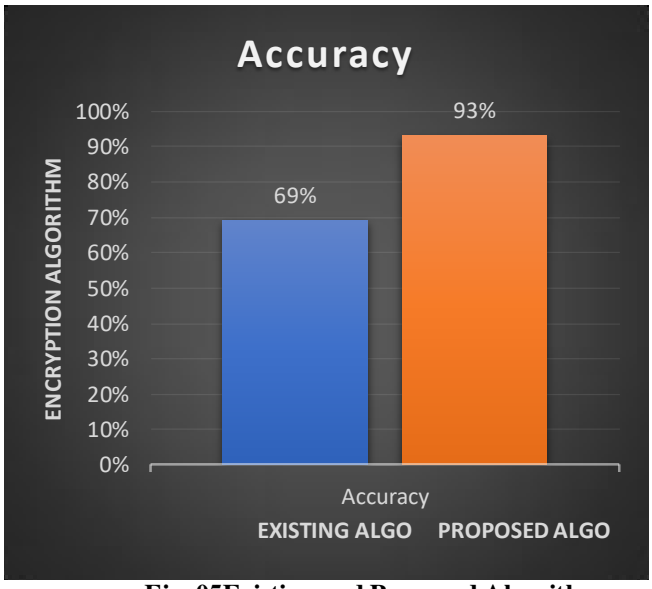

Fig. 05Existing and Proposed Algorithm

REFERENCES

[1]. Dan. Boneh, In Proceedings of the Third Algorithmic Number Theory Symposium, Lecture Notes in Computer Science, Vol. 1423, Springer-Verlag, pp. 48--63, 1998 Full paper:

[2]. Husna Tariq, Dr. Parul Agarwal*," Secure Keyword Search Using Dual Encryption in Cloud: An Approach", International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 5

[3]. Chi Harold Liu, Senior Member, IEEE, Qiuxia Lin, Shilin Wen. "Blockchain-enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning", IEEE Transaction on Industrial Volume: 15, Issue: 6 , June 2019.

[4]. Shangping Wang, Dongyi Li, Yaling Zhang, Juanjuan Chen, "Smart Contract-Based Product Traceability System in the Supply Chain Scenario", IEEE Access, 2019.

[5]. M. Nakasumi, "Information Sharing for Supply Chain Management Based on Block Chain Technology," in 2017 IEEE 19th Conference on Business Informatics (CBI), Thessaloniki, Greece, Jul. 2017.

[6]. Kui Ren, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing‖ in IEEE transactions on parallel and distributed systems, Vol. No. 22, Issue 5, MAY 2011.

[7]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data,"Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

[8]. Jing L, Xiong L, Licheng W ,Debiao H, Haseeb A, Xinxin N(2017) "Fuzzy encryption in cloud computation: efficient verifiable outsourced attribute-based encryption"

[9]. Priyanka Kumari, Raj Kumar Paul, "A Study for Authentication and Integrity of Data Files in Cloud Computing", IJOSCIENCE,Volume2,Issue 9 December 2016.

[10]. Arshi Jabbar and P. U. Lilhore, "Design and Implementation of Hybrid EC-RSA Security Algorithm Based on TPA for Cloud Storage", International Journal Online Of Science, vol. 3, no. 11, p. 6, Nov. 2017.

[11]. Emura, K., Miyaji, A., Nomura, A., Omote, K., and Soshi, M. (2010) 'A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length', Int. J. Applied Cryptography.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

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