IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

SQL INJECTION ATTACKS DETECTION USING MACHINE LEARNING

[1]Mohana Ragini pursuing M.Tech (CSE)

[2]Banda Avinash Assistant Professor

Universal college of engineering and Technology,Perecharla,Guntur.

ABSTRACT

Users’ crucial data is stored in databases by the web-based applications that collect it. Due to their Internet accessibility, these applications and the databases that are connected to are exposed to a variety of information security risks. The threats include cyber attacks like Cross Site Scripting (CSS), Denial of Service Attack (DoS), and SQL Injection Attacks. When considering web-based applications, the top ten vulnerabilities includes SQL Injection attacks. An organization or corporation may suffer harm as a consequence of this kind of attack since the attacker can obtain or steal sensitive information. In order to classifying and recognize SQL Injection attacks, we are considering utilizing an algorithm from machine learning approaches. Any web system mustinclude a robust SQL injection detection to counteract this risk. In this project, machinelearning is applied to provide using training data, which is then analyzed against testing data. The outcomes of the detection demonstrates that the proposed approach generates high accuracy in differentiating between malicious and harmless web requests.

Keywords: CROSS SITE SCRIPTING(CSS), DENIAL OF SERVICES(DOS), SQLINJECTION....

1.INTRODUCTION

In section 1.1 of the project, SQL Injection Attacks Detection Using Machine Learningon Hospital Web, an overview of the context is covered in this chapter. The motivationsare addressed in section 1.2. The project’s objectives are then described in section 1.3.Finally, a research work flow is introduced step by step in section 1.4 as a result of themotivations that have been presented

1.1 Context

The most important resource for all organisations is data. Organizations must take action to secure and monitor their data. In the current climate, cyber threats and cy- ber attacks against databases used by web apps or by enterprises are on the rise. The perpetrator and threat to data privacy is hackers, who, as one example, could target weak websites with a SQL Injection Attack (SQLIA). Additionally, there are numeroustools available that may be used to automatically carry out bugging operations and as-sess a website’s vulnerabilities. These tools, which can be fully or semi-automated, areused to identify flaws and defects in online applications. With these tools, an attacker has a greater possibility of accessing the web system database while being aware of theflaws the web contains and how to exploit them. By inserting malicious SQL queries into the database, a type of attack known as SQL injection manipulates a website to reveal sensitive data. Hence, if the SQL injection can be recognized earlier, it can helpthe security officer or security analyst to terminate the attack. (9)

1.2 Problem/Motivation

According to OWASP's list of the top 10 online attacks from 2018 to 2022, SQL injection continues to be the most common attack against websites. According to reports, SQL injection is a hazardous form of cyber attack that necessitates ongoing study for a better web system defiance. We can protect the data from being taken by those attackers by incorporating an effective detection mechanism into a web system. Due to its capacity to make decisions similar to those made by humans but with more accuracy, capacity, and durability, machine learning and artificial intelligence are attracting the attention of many researchers. Future detection of SQL injection protection mechanismswill be improved by the application of machine learning. (2)

1.3 Objectives

In this Project We are exploiting databases and manipulating them via SQL. By injecting code and going to take advantage of SQL vulnerabilities, an attack known as SQL Injection attempts to obtain unauthorized access to a database. We are using a web server(KHIRE'S HOSPITAL) as our target and perform SQL injection attacks on the web server. We are employing the Navies Bayes algorithm's proposed classificationstrategy to categories, detect SQL injected payloads or codes, and distinguish them from typically generated user queries. We also highlighting how well our machine can discriminate between dangerous and benign queries. We are developing a machinelearning algorithm to differentiate between these attacks and determine how accuratelyour machine can identify them.

1.3.1 WEBSERVER (KHIRE'S HOSPITAL

Consider a hospital website where users can enroll in by entering a username and pass-word. The authentication will succeed when the user enters a legitimate user- name and password, and they'll be able to log in. We use SQL injection tools to test the vulnerabilities of that web server and perform the attacks , the logs of these attacks are presented as a data set to the machine and let it decide the differences between thenormally generated queries and SQL injected codes. The Navies Bayes machine learning classification algorithm is used for the detection of malicious SQL injection attacksaccurately.

1.4 Research work flow

The following work flow will be described in the report in accordance with the study'sobjectives:

Step 1: Users were able to schedule appointments on the relevant accessible datesby using a hospital web server built using react.js and a users login page. For the web

server administrator to keep track of patient visits and electronic health records, a track-ing table was created. For the electronic health record, which can only be accessed by the web server administrator, arbitrary data was collected. Using MySQL, databases of users and passwords, electronic health records, and a server hosted on the Free MySQL hosting.com website were constructed. A frontend interface for the hospital's website was also created.

Step 2: Once the target web server had been installed, SQL injection tools like theBurp suite and SQL Map were used to see if the server was vulnerable to such assaults..

Step 3: creating and analyzing machine learning classification algorithms to distinguish between typical user requests and harmful codes imposed by an attacker.

Step 4: Utilizing this approach, we can determine how well our trained systempredicts the responding outcome (accuracy : 0.98)

2.LITERATURE REVIEW

2.1 SQL INJECTION:

By manipulating the data entered into an application, a hacker can insert a SQL queryinto such a database to retrieve records from an information system. There are many different types of SQL injection techniques, including blind SQL injection, union-based SQL injection, and error-based SQL injection.

2.1.1 Blind SQL Injection Attacks:

Blind SQL injection occurs when an attacker attacks a website without first determining whether it is susceptible to SQL injection. Since the administrator has added security mechanisms to the website, no data are displayed on the page. As a result, the attackermust transmit a payload to be able to reconstruct the database structure while watchingthe web application's response to determine how the database server behaves. There are two types of blind SQL injections, which are Boolean and Time-based.

- **Boolean-based:** Boolean-based SQLIA is a type of blind SQL injection an in- stance of blind SQL injection where the website will only display the outcome when the right query has been supplied as the parameter of the request statements.
'Cm

- **Time-based:** Blind SQL injections, such as time-based SQLIA, work by sendingSQL queries to the database and afterwards awaiting for some time for a response. The attacker could therefore draw any conclusions from this result whether the HTTP response suggests a direct or delayed response.

2.1.2 Union SQL Injection Attacks:

One of the in-band SQL injection attacks, the union-based attack utilizes the UNION SQL query to combine the outcomes of two or more SQL statements into a single resultfor the HTTP response. An application system can potentially be manipulated by the attacker by making union statements like UNION SELECT.

2.1.3 Error SQL Injection Attacks:

Error-based In a SQLI attack, the attacker examines the error message which appears onthe web application site to obtain data from the database. The server's whole databaseis possible to access through this type of SQL injection attack. Error messages areinitially intended to make it simpler for engineers to troubleshoot and discover bugs. (8)

2.2 Related SQL Injection Tools:

Tools for SQL injection testing are beneficial since they allows penetration testers to assess the level of security of an industry's websites. Using automated tools simplifiesthe process for security professionals to conduct out SQL injection attacks than beginning from scratch.

- **BURP SUITE -** A semi-automated tool for attempting SQL Injection attacks, Burp Suite is an integrated graphical tool for performing security testing of web applications.

- **SQL Map** – Database takeover and automatic SQL injection tool

2.3 Machine Learning:

Algorithms that can learn from data without using rules-based programming are the foundation of machine learning. This indicates that machine learning is a method for enabling a machine to make a decision on its own through the application of machine- learning algorithms without the use of programmable codes.

2.4 Supervised Learning:

By carefully monitoring the incoming information, this kind of machine learning trainsitself. In order for the machine to learn and make predictions in the future, it needs sufficiently labelled data with the reasonable response during training. This type of machine learning will be used in this project to examine the predictions it makes re- grading the detection of SQL injections. Supervised learning can be distinguished into two:

- **Regression –**Based on the statistic of the previously obtained data, regression analysis forecasts the following value. By examining the sample, the regression approach assesses the test data a0 and a1 (X, Y). The purpose of training the data and dispersing it across the linear graph is to determine a threshold value that will assist characterize the outcomes(12)
- **Classification** – In order to classify an attribute for the subsequent decision, the classification technique is a type of supervised learning approach that determines the attribute of data during the training phase. Researchers utilize this methodology frequently since it is well-known. This approach is being utilized in this project to characterise the logs in order to determine whether or not they are malicious.

3.METHODOLOGY

3.1 Proposed hypothesis

SQL Injection works in the following format, When a user of KHIRE’s HOSPITAL submits his username and password during the authentication process, the query con- structed in the result of an approved login attempt will appear such as this one where:

Username = AJAYPassword = 123456

SQL Query: SELECT * FROM users WHERE name = ‘AJAY’ andpassword = ‘123456’

The following input, however, might also potentially be entered into the website’susername and password entries by a person with sinister intentions where:

Username = AJAY Password = ’ or ‘1’ = ‘1’

In this scenario, a SQL query will be executed.

SQL Query: SELECT * FROM users WHERE name = ‘AJAY’ andpassword = ‘’ or ‘1’ = ‘1’

This user will always be able to access the website because 1=1 is a perpetual.The user acquires unauthorized access to some other person’s account information, andpossessing this knowledge could have very damaging consequences. (10)

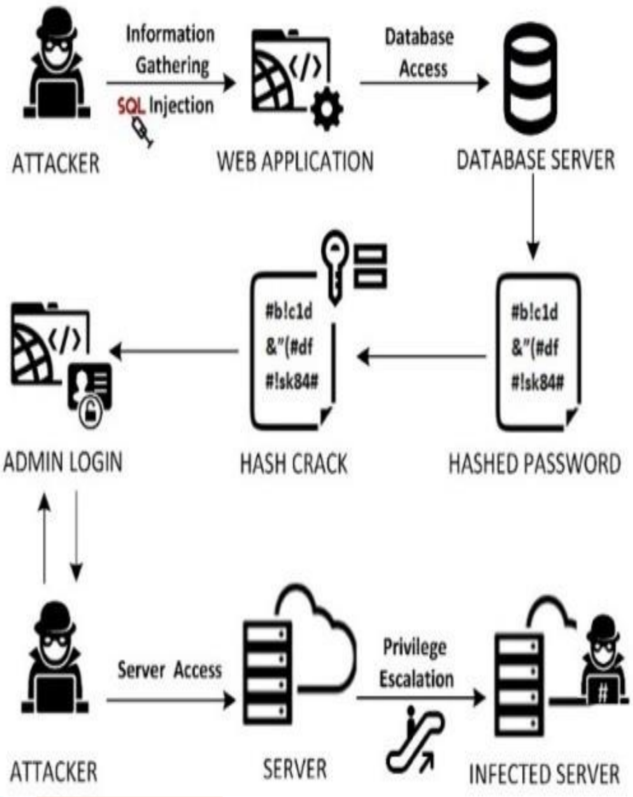


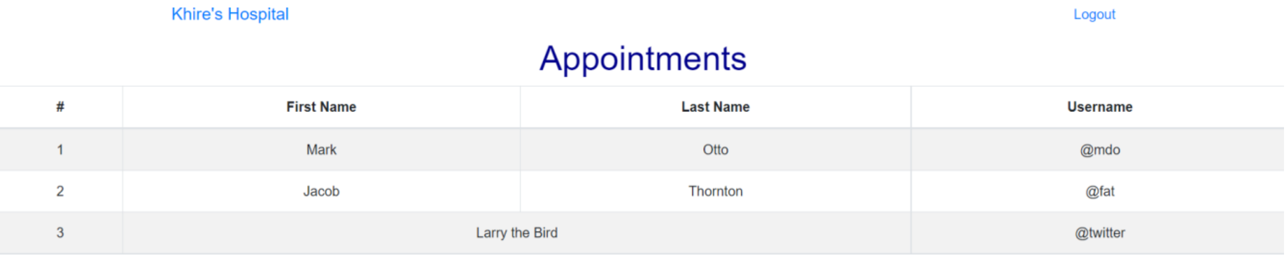
Figure 3.1: circular flow of the attack

- **About the Webserver:** We made a webserver of a medical hospital as our targetand initiated the following things

1.)During a user login , the user is directed to the appointment booking session.

2.)The administrator of the webserver contains all the access to the secure data of

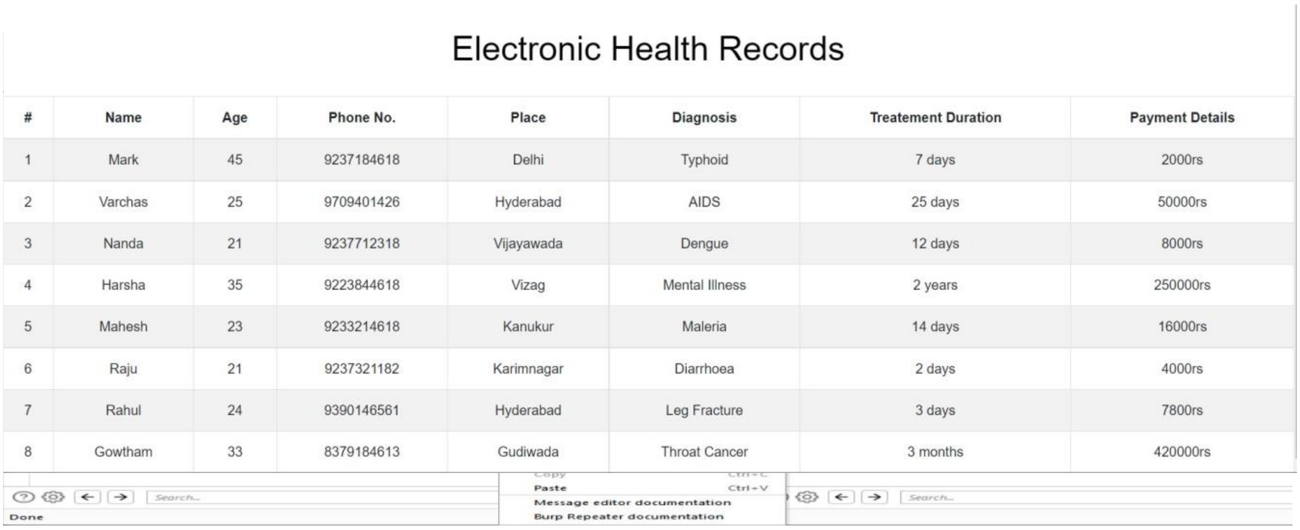
the patients or users , the important data of patients like their Name, address, phone number , their diagnosis, and payment details is presented into the ELECTRONIC HEALTH RECORD(EHR) that every hospital web server needs to maintain and protect. The admin has also access to the number of appointments scheduled by the users.(3)



Appointments

#	First Name	Last Name	Username
1	Mark	Otto	@mdo
2	Jacob	Thornton	@fat
3	Larry the Bird		@twitter

Figure 3.2: Showing all Appointments



Electronic Health Records

#	Name	Age	Phone No.	Place	Diagnosis	Treatement Duration	Payment Details
1	Mark	45	9237184618	Delhi	Typhoid	7 days	2000rs
2	Varchas	25	9709401426	Hyderabad	AIDS	25 days	50000rs
3	Nanda	21	9237712318	Vijayawada	Dengue	12 days	8000rs
4	Harsha	35	9223844618	Vizag	Mental Illness	2 years	250000rs
5	Mahesh	23	9233214618	Kanukur	Maleria	14 days	16000rs
6	Raju	21	9237321182	Karimnagar	Diarrhoea	2 days	4000rs
7	Rahul	24	9390146561	Hyderabad	Leg Fracture	3 days	7800rs
8	Gowtham	33	8379184613	Gudiwada	Throat Cancer	3 months	420000rs

Figure 3.3: Showing Electronic Health Record of patients.

3.1.1 TOOLS:

- **Python:** Python is a popular programming language that can be used on servers to create web applications.
- **Numpy:** Numpy is a python library used for working with arrays, domain in algebra

, and matrices.

- **Pandas:** Working with "relational or labelled data" is made easier with the help of this Python module that offers quick, versatile, and expressive data structure. It servesas an advanced building component for data analysis in the actual world.
- **TensorFlow:** It is an open-source software library for machine learning and artificialintelligence with such a focus on deep neural networks.
- **Keras:** It is a public library that functions with a variety of backends, including TensorFlow.
- **Burp Suite (semi automatic):**We employ a Chrome-based browser that has alreadyset up to function with the target or web server. We find the HTTP request history and response. We put the URL of our target into the Burp suite chromium and if we try to use a random username and the password , of course its access is denied but the response is monitored. Now we send the request to the repeater which is a tab in burp

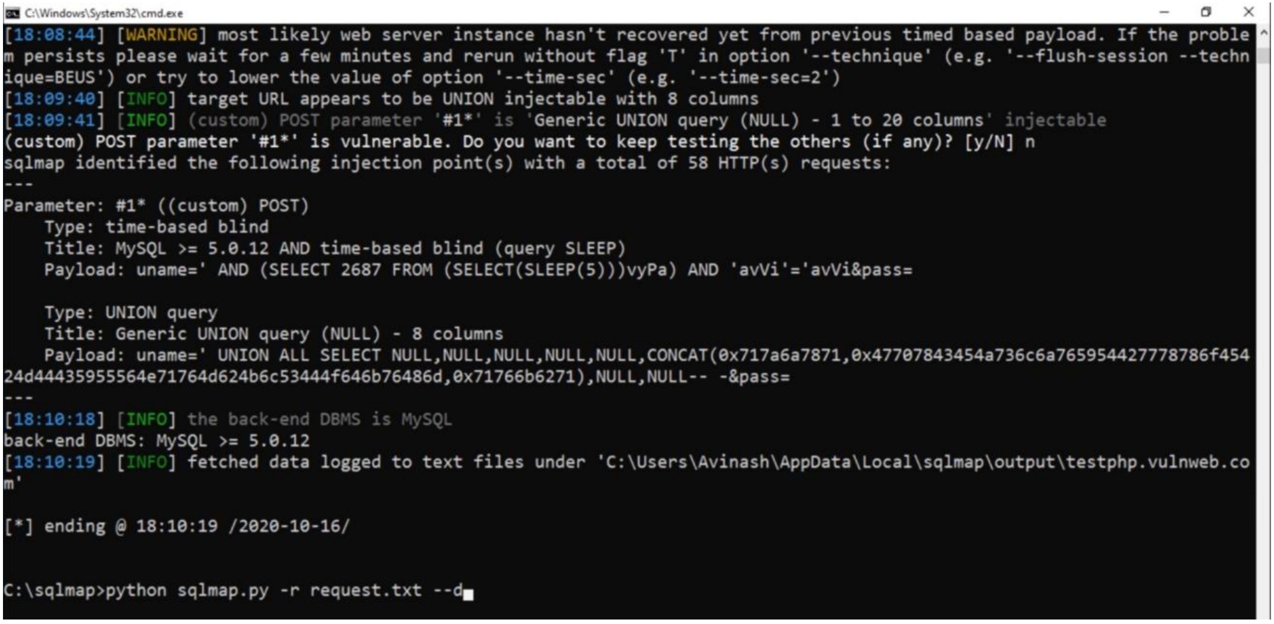
suite where we can modify the request to see different responses. Here we send the rawrequest to the intruder tab, its the actual place where we set the payloads and do all of the attacks. Based on the requested payload length, the request gets rendered and gets bypassed. (6)

Figure 3.4: Using Burp Suite.

- **SQL Map(fully automated):**An open source software tool SQL Map is used inpenetration testing to identify and take the advantage of SQL injection flows. It auto- mates the detecting and exploitation of SQL injection.

Python sqlmap.py -u URL http://localhost:3000/login (assigning the target)

In SQL Map we have levels while performing the tests starting with default level-1and upto level-5 . After connecting to the target URL, SQL Map is going to retry the request and find to what kind of SQL injection attacks does the server is vulnerablefor SQL MAP uses automated payloads which are complex to crack. Upon requesting“Python sqlmap.py -r request.txt –dbs” provides the available databases of the target and retrieve the schemas , provide the tables available in the database.



```
[18:08:44] [WARNING] most likely web server instance hasn't recovered yet from previous timed based payload. If the proble
m persists please wait for a few minutes and rerun without flag 'T' in option '--technique' (e.g. '--flush-session --techn
ique=BEUS') or try to lower the value of option '--time-sec' (e.g. '--time-sec=2')
[18:09:40] [INFO] target URL appears to be UNION injectable with 8 columns
[18:09:41] [INFO] (custom) POST parameter '#1*' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 58 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: uname=' AND (SELECT 2687 FROM (SELECT(SLEEP(5)))vyPa) AND 'avVi'='avVi&pass=

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: uname=' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x717a6a7871,0x47707843454a736c6a765954427778786f454
24d44435955564e71764d624b6c53444f646b76486d,0x71766b6271),NULL,NULL-- -&pass=
---
[18:10:18] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[18:10:19] [INFO] fetched data logged to text files under 'C:\Users\Avinash\AppData\Local\sqlmap\output\testphp.vulnweb.co
m'

[*] ending @ 18:10:19 /2020-10-16/


C:\sqlmap>python sqlmap.py -r request.txt --d
```

Figure 3.5: Using SQL Map.

3.2 Count Vectorizer:

Scikit-learn’s Count Vectorizer is used to convert a collection of text documents that maybe converted into a vector of term/token counts using the vectorizer programme. Additionally, it makes it possible to pre-process text data before creating the vector representation.

3.3 Stopwords:

A stop word is a frequently used term that a search engine has been configured to ignore, both while indexing items for searching and when retrieving them as the resultof a search query. Examples of stop words include "the," "are," and "and." Its used forcleaning and filtering the data set, the stop words removes the words which does not addany value to the sentence.

3.4 Mechanism/Algorithm:

3.4.1 How ML helps in detecting those attacks:

A classification approach to machine learning called Nave Bayes makes the assumption that each encounter is unconnected to and independent of every other incident. SQL queries are separated among malicious and non-malicious categories using the Nave Bayes classifier. In order to train the model, we typically employ a training data set thatcomprises both malicious and harmless SQL queries. Furthermore, each query in this training data set is labeled.(5)
The model can determine what is malicious and harmless by categorizing the data.A supervised machine-learning model is the name for this kind of model. After the model has been trained it is tested against the test data set to determine whether it accurately characterizes the SQL queries. This model indicates to even be capableof recognizing recently discovered and unidentified SQL Injection attacks.. We are training our machine to classify the data, identify the indifferent or strange queries compared to normal ones, and test how accurate the machine detects the SQL injectionattacks.

3.4.1.1 Navies Bayes Algorithm

Uncertainty and probability are hard to bear for human beings. But in machine learning,there are certain algorithms that help to find your way around this limitation. The NaiveBayes machine learning algorithm is one of the tools to deal with uncertainty with thehelp of probabilistic methods.

- Conditional probability is defined: The probability of a given b is specified as thecombination probability of both a and b happening, divided by that of the probability of b. If another event happens, we're focused in how feasible it is that it will happen.

$$P(A \mid B) = \frac{P(A \wedge B)}{P(B)} \qquad (3.1)$$

The algorithm simply takes for granted that all input variables are independent. Understanding the data set and classifying the data with multiple features in records. In
order to evaluate the proposed naive Bayes-based pattern recognition model for SQL
injection attack, 4201 instances of vulnerable and non-vulnerable variables in web applications were included in the data set. For each fold test, 80 of the data set was used
for training and 20 for testing. We are using Naive Bayes to classify the differences
between the normally generated queries during logging in and malicious SQL injecting
codes or syntaxes. The machine learning approach is used to detect and classify what
has normally generated queries and what the SQL exploited codes.(?)

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)} \qquad (3.2)$$

Where:
P (A|B) = Probability of A being true given that B is true
P (B|A) = Probability of B being true given that A is true
P (A) = Probability of A regardless of the other data
P (B) = Probability of B regardless of other data

3.5 Analytical validation:

3.5.1 DATA SET

Due to the limited number of SQL injection attacks data sets accessible, we were only
able to discover one dataset with something like a small number of samples. Discovering the data set that comprises malicious SQL injecting codes as well as some regular
ones was a huge setback. Given that there are no other accessible datasets, we opted to
utilize this one. We decided to utilize the dataset as there's none other available.

3.5.2 TRAINING THE DATASET

Machine learning methodologies for data pre-processing were applied to produce the dataset for this study. The dataset undergone clean filtration to eradicate all noise. In order to accurately evaluate the proposed approach, 80 percent of the total of the datasetwas utilized for training while 20 percent for testing. (11)

3.5.3 WEBSERVER(target)

A webserver (KHIRE'S HOSPITAL) was made as a target and assigned the databases to the web, with the users' login page. The users logged in will be able to book an appointment online on a specific date and the administrator of the webserver has accessto the number of appointments and the user details.

3.5.4 ELECTRONIC HEALTH RECORD

It's a collection of medical information of a patient that is stored on a computer whichconsists of information about the patient's contact details, address, diagnosis, treatmentduration, and payment details . . . ..For the purpose of this project, arbitrary data was provided to the EHR which is only accessible by the webserver administrator.

3.5.5 SQL INJECTION

Semi-automatic and fully-automatic tools were used to exploit the vulnerabilities of thetarget web server and perform SQL Injection attacks.

3.5.6 MACHINE LEARNING

Navies Bayes classification algorithm was used to detect the SQL injection attacks between the normally generated user queries and the malicious SQL syntax commandsand was able to classify between them. (13)

4.Results and discussion

In this project, a code was built based on navies Bayes classification so as mentionedto detect and classify between the general or normal user queries during user login andunusual syntaxes that diff from the normal user queries like malicious SQL exploits Eg " or ""=" , " OR 1 = 1 – -,

A target web server was made using react.js, MySQL, HTML, and CSS for the purposeof performing these attacks and made arbitrary data into the electronic health record which can only be accessible by the system administrator.

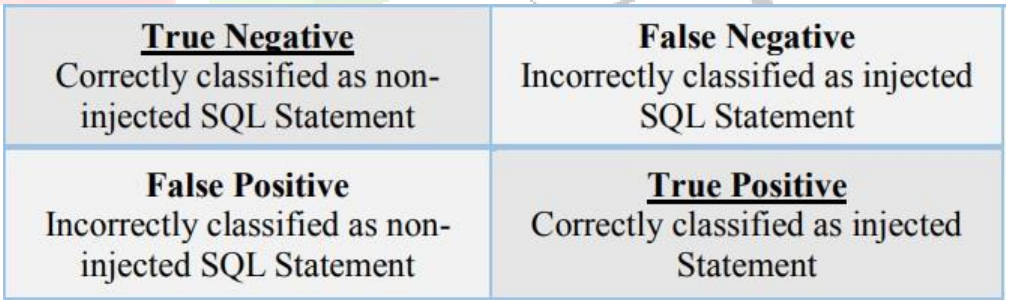
We have successfully built the code to detect these sorts of attacks, our main aim throughout this project has been to detect the SQL injection attacks using machine learning classification algorithms like navies Bayes.

4.1 Evaluation Metrics :

A predictive model's effectiveness is measured by an evaluation metric. This often entails building a model on a dataset, testing it on a holdout dataset that wasn't used during training, and comparing the predictions to the holdout dataset's anticipated values. Metrics for classification issues require comparing the expected and predicted classlabels or interpreting the anticipated probability for the problem's class labels.

4.2 Confusion Matrix :

Confusion matrices are used to visualize important predictive analytics like recall, specificity, accuracy, and precision. Confusion matrices are useful because they give direct comparisons of values like True Positives, False Positives, True Negatives and False Negatives. In our example, the TP and TN stand for the proportion of properly categorized SQL statements, whereas the FP and FN stand for wrongly classified SQLstatements. As illustrated in Fig 1, a matrix known as the confusion matrix may be created by combining the values of TP, FP, TN, and FN.



True Negative Correctly classified as non-injected SQL Statement	**False Negative** Incorrectly classified as injected SQL Statement
False Positive Incorrectly classified as non-injected SQL Statement	**True Positive** Correctly classified as injected Statement

Figure 4.1: fig:Guide to read confusion matrix

4.3 Specificity:

The capacity of the algorithm or model to predict a true negative of each accessiblecategory may be used to describe specificity.

$$\text{Specificity} = \frac{\text{True Negatives}}{\text{True Negatives} + \text{False Positives}} \qquad (4.1)$$

4.4 Sensitivity:

The parameter used to assess a model’s capacity to forecast the true positives of eachaccessible category is known as sensitivity in machine learning.

$$\text{Sensitivity} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Negatives}} \tag{4.2}$$

4.5 Precision:

When we want the forecast of 1 to be as accurate as possible, we employ precision. Precision is determined by dividing the total number of true positives and false positivesby the number of true positives in a classification issue with two classes.

$$\text{Precision} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}} \tag{4.3}$$

4.6 Recall:

When you need to appropriately categories an event that has already happened, recall comes in handy. For instance, for SQL Injection detection algorithms to be effective, recall must be high. In these circumstances, we don’t care about the genuine 0s becauseour main goal is to identify the true 1s as frequently as feasible

$$\text{Recall} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Negative}} \tag{4.4}$$

5.CONCLUSION

Accuracy: The machine learning model, based on the Naive Bayes classification, achieved an accuracy of 0.98 in distinguishing between normal user queries and malicious SQL injection codes.
Effectiveness: The model demonstrated high effectiveness with a sensitivity of 1.0 and specificity of 0.97, indicating its strong ability to correctly identify true positives and true negatives.
Precision & Recall: The precision of the model was 0.94, and it had a perfect recall score of 1.0, showing its proficiency in classifying SQL injection attacks accurately.
F1 Score: The F1 score, which balances precision and recall, was 0.97, reflecting the model's overall reliability in detecting SQL injection attacks.
The project successfully developed a machine learning approach to detect SQL injection attacks, highlighting the potential of such models in enhancing web application security . The future scope suggests further optimization and integration of the model with web applications for real-time attack prevention and alerting.

REFERENCES

[1] Ciampa(2010)]10]A. Ciampa, C.A. Visaggio, M. P.: 2010, A heuristic-based approach for detecting sql-injection, *Proceedings of the ICSE* **15**(3), 321–387.

[2] Ding Chen*, Qiseng Yan, C. W. J. Z.: 2020 June, Sql injection attack detection and prevention techniques, *Using Deep Learning.School of Cyberspace Security, Chengdu University of Information Technology, Chengdu* **15**(3), 321–387.

[3] F. Valeur, D. M. and Vigna, G.: 2005, A learning-based approach to the detectionof sql attacks, **15**(3), 321–387.

[4] Kamtuo, K. and Soomlek, C.: 2016 December 17, Machine learning for sql injec-tion prevention on server-side scripting, **15**(3), 321–387.

[5] Mishra, S.: 2019 May 23, Sql injection detection using machine learning, *San Jose State University* **15**(3), 321–387.

[6] M.N.Kavitha, V.Vennila, G. A. K.: 2021 March, Prevention of sql injection attackusing unsupervised machine learning approach, *2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA)* **15**(3), 321–387.

[7] Morufu Olalere, Abdullahi Egigogo Raji, I. I. J. R. G.: 2018 July, A naïve bayes based pattern recognition model for detection and categorization of structured query language injection attack, *International Journal of Cyber-Security and Dig-ital Forensics* **15**(3), 321–387.

[8] Muhammad Amirulluqman Azman, M. F. M. and Sulaiman, R.: 2021 Febru- ary 05, Machine learning-based technique to detect sql injection