ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 2 Issue 1, January 2022 / Page No: 5-11
Paper Id: JETA-V2I1P102 / Doi: 10.56472/25832646/JETA-V2I1P102

Original Article

SQL Injection Attack Detection in Websites

V. Saranya[1], Havisha Monal. A[2]
[1,2]*PG Teacher in Computer Science, Krishna International School, Ramanathapuram, India*

Received Date: 18 November 2021 Revised Date: 21 December 2021 Accepted Date: 09 January 2022

Abstract: *Web applications are broadly used in nowadays. The demand of e-commerce websites are also increase today and it fully depends on cash exchange services like on-line banking, e-shopping, on-line charge installment, Currency exchange, and more. SQL is defined as the midstream of mesh server and database server scripting languages which is used for execution processes. Mesh server waits to catch request from users and it helps to answers back through web browser HTTP response. So it is indispensable to maintain their records confidentiality from intruders. SQL Infusion assault is one of the top most attacks which are done by intruders to hack database records without web admin knowledge. Detection of SQL Infusion Assault is quite different from other attacks because intruders changed SQL query behavior by inserting some inputs through input forms. This work completely focused to discover and avoid SQL Infusion Assault in E- Commerce websites. The research work identifies the SQL assault infusion by proposing the methodology which includes validation process and encryption process to adopt information security principles. In the first module, projected experiments holds sample dataset not real dataset for particular ecommerce sites. It contains user login details such as userid, username, secret key and so forth. This login details helps to investigate unauthenticated client in their sites by using exposure tool. In the second module, every client is given a client name and secret word, utilizing structure based verification is given, when the client name and secret word matches, they are offered access to different modules and they can see the products.Third module is Input validation is validated automatically when user enter their login details intothe input form. Information approval keeps dishonorably shaped information from entering a data framework .Finally, Anomaly Detection module focus on the request which have been received by the web server, users can see that the request which just incorporate words or digits or a mix of these two, can never contain assaults against the web server.*

Keywords: *SQL Injection, Security.*

INTRODUCTION

In this Chapter**,** the work briefly describes about Domain, Assaults, E-commerce Websites and what the foremost challenges, problems faced by web application users and provides a concrete solution to avoid these issues in an effective way. It also holds small introduction about the process of SQL Infusion Assault and described about standing techniques which was followed by many researchers. In addition the projected techniques followed by web users in future to enhance security and describes about modules description. The proposed detection tool effectively validates user‟s input and provides quick response to users. It protects databank from evaders by using validation techniques and get quick response from webserver to user.

Information Security Definition

Information is a resource for all people and organizations. Data Security alludes tothe assurance of these advantages with a specific end goal to accomplish C - I - A as the accompanying graph:

Information security (IS) is intended to ensure the secrecy, honesty and accessibility of PC framework information from those with malignant expectations. Classification, respectability and accessibility are now and again alluded to as the CIA Triad of data security. This group of three has advanced into what is normally named the Parkerianhexad, which incorporates classification, ownership (or control), trustworthiness, credibility, accessibility and utility.
Information security handles hazard administration. Anything can go about as a hazard or a risk to the CIA set of three or Parkerianhexad. Delicate data must be kept - it can't be changed, modified or exchanged without consent. For instance, a message could be altered amid transmission by somebody capturing it before it achieves the proposed beneficiary. Great cryptography apparatuses can help alleviate this security risk.

Advanced marks can enhance data security by upgrading validness procedures andprovoking people.

RELATED WORK

In this chapter various explanation by researchers are proposed to detect and prevent data from SQL Infusion Assault and also describes about what are the problems are faced by researchers and how they clarify their work are valid to used by web users and how to enhance their research in future. This part demonstrates a variety of analysis and research complete in the field of your attention and the outcome previously published.

Kuisheng Wang ,VanHouv et al proposes a sort of SQL recognition strategy which joined with dynamic corrupt examination and information sifting. What's more, it is insertedin the cloud condition to accomplish the assurance of the Web applications in cloud arrangement. To start with, the technique gets the SQL[15] watchwords through the investigation of lexical control for SQL explanation.
DEBABRATA KAR, KHUSHBOO AGARWAL, AJIT KUMAR SAHOO, AND SUVASINI PANIGRAHI et al proposed a novel technique to identify pernicious inquiries utilizing a twin Hidden Markov Model (HMM) group and approve it with extensive arrangement of kindhearted and vindictive questions gathered from five test web applications written in PHP and MySQL.

ED PEARSON, CINDY L. BETHEL et al considered SQL infusion assaults (SQLIA) [9]have been the guilty party of most hierarchical digital security breaks. This type of assault could detrimentally affect a business or then again association.

DR. AHMAD GHAFARIAN et al represents a genuine security risk to the database driven web applications. This kind of assault gives assailants effectively access to the application's fundamental database and to the possibly touchy data these databases contain. A programmer through particularly planned input, can get to substance of the database that cannot something else have the capacity to do as such. This is generally done by modifying SQL proclamations that are utilized inside web applications. Because of significance of security of web applications, specialists have contemplated SQLIA discovery and counteractive action widely and have created different techniques. In this examination, in the wake of inspecting the current research in this field, we display another half breed strategy

VAMSHI KRISHNA GUDIPATI et al comprehend the dangers and the seriousness of endeavors conveyed, the research work provides verification of ideas to abuses completed to trade off web applications and how the databases are isused utilizing the SQL infusion philosophies. Progressed techniques on the most proficient method to safeguard SQL infusions are quickly advocated.

RAJASHREE et al utilizing SQL infusion assailants can take secret data. In this research, the SQL infusion assault recognition technique by expelling the parameter estimations of the SQL inquiry is talked about and comes about are introduced.

AJIT PATIL, et al distinguish diverse assaults and discover the answers for distinctive sort of assaults, for example, DDOS, SQL infusion and Brute constrain assault. For this situation, we utilize customer server design. To execute this we keep up profile of client and based on this we discover ordinary client or aggressor when framework find that assault is available then it straightforwardly obstruct the assault.

SOLOMON OGBOMON UWAGBOLE et al presents an application setting design driven corpus to prepare a administered learning model. The model is prepared with ML calculations of Two-Class Support Vector Machine (TC SVM) and Two-Class Logistic Regression (TC LR) executed on Microsoft Azure Machine Learning (MAML) studio to relieve SQLIA. This conspire exhibited here, at that point shapes the subject of the observational assessment in Receiver Operating Characteristic (ROC) bend.PROBLEM DEFINITION

The infusion without a doubt is considered as a standout amongst the most genuine dangers to web application security. Various assaults are completed utilizing this helplessness and a great many sites are imperiled each day. For whatever length of time that the web applications are inadequately planned, the SQL infusion systems will win. Accordingly web designers need to take after standards with a specific end goal to anticipate SQL infusions on their sites as our research has proposed.

Each occurrence of SQL infusion, the imperfection is the same: a programmer sends SQL code in way the site's specialists did not imagine, allowing the programmer to perform unanticipated and unapproved exercises. By following thepreventive philosophies and fixing every one of the locales which are powerless ought to be finished. A progression of entrance tests ought to be completed and every one of the sites which are unstable coded ought to be fixed and looked after deliberately.

Problem statement

The present framework gives more security than existing procedures in view of exposure tool. The proposed Exposure tool excellently approves client's information and gives speedy reaction to clients. It guards database from intruders by utilizing approval strategies and get fast reaction from web server to client. Exposure tool gives protective setting so client feels safe to work in this condition. The necessary modules are identified as an approach to detect the SQL

Assault and their names are such as Dataset, User Entry, Input Validation, and Anomaly Detection.It contains user login details such as userid, username, secret key and so forth.Every client is given a client name and secret word, utilizing structure based verification is given, when the client name and secret word matches, they are offered access to different modules and they can see the products and post the feedback.Input is validated automatically when user enter their login details into the input form.The working strategy for this module is additionally in light of precisely the same. This module helps to detect SQL injection attack.
Finally the total number of users allowed to register in the database and number of transactions, number of encryption sessions undergone by the process.

As a whole, the problem describes a novel method to detect SQL Assault and provides a different enhancement solution to the existing work by enriching the information security principles.

PROPOSED SYSTEM

This chapter provides the detailed study about the proposed algorithm performance which is used to detect SQL Infusion Assault and how to prevent user from assault. The proposed algorithm has a set of rules to resolve a SQLIA and this chapter expresses step by step performance of proposed algorithm. Also holds detailed explanation about validation process and encryption process.

PROPOSED ALGORITHM

PARAMETERS

i: Input
n: Length of input string c: Compare with sql queryv: Valid data
u: User Entry m: Invalid data
d: Display error messagee: Encrypted Data

Algorithm 1: (Validation Process)

```
STEP1: SQL PROCEDURE (i,n)
STEP 2: START()
STEP 3: Get input data from user ( i )
STEP 4: Evaluate with generalized sql query(c)
STEP 5: Check length of input string of data (n)
STEP 6: if( i ==c) && ( i ==n) // check length of input data and compare withsql query.
STEP 7: Condition true // v= valid data
STEP 8: THEN v [ i]=v[n] // if valid data then allow user
STEP 9: THEN print u //authenticated user
STEP 10: ELSE
STEP 11: Condition false
STEP 12: Then m[ i]=m[n] // if invalid data
STEP 13:Then print d // display error message
STEP 14:Then e // data encrypted for security
STEP 15: return // return to initial statement
STEP 16: END
```

ALGORITHM EXPLANATION (Validation Process)

Input is validated automatically when user enter their login details into the input form. Input validation is the correct testing of any input provided by a client or application. Information approval keeps dishonorably shaped information from entering a data framework.

Flow Chart for Validation Process

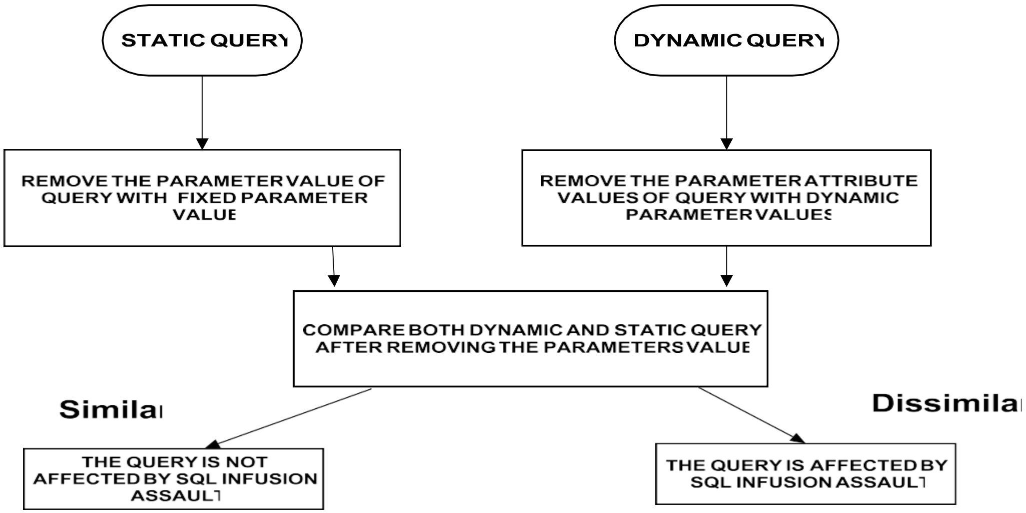

STATIC QUERY
DYNAMIC QUERY
REMOVE THE PARAMETER VALUE OF QUERY WITH FIXED PARAMETER VALUE
REMOVE THE PARAMETER ATTRIBUTE VALUES OF QUERY WITH DYNAMIC PARAMETER VALUES
COMPARE BOTH DYNAMIC AND STATIC QUERY AFTER REMOVING THE PARAMETERS VALUE
Similar
Dissimilar
THE QUERY IS NOT AFFECTED BY SQL INFUSION ASSAULT
THE QUERY IS AFFECTED BY SQL INFUSION ASSAULT

Fig. 1 Validation Process

ALGORITHM EXPLANATION(Encryption Process)

This section holds the in depth explanation of [1] [11] validation performance through this algorithm. This process splits into two parts, one is static query andanother one is dynamic query. Both query removes remove the parameter attribute values based on query type.

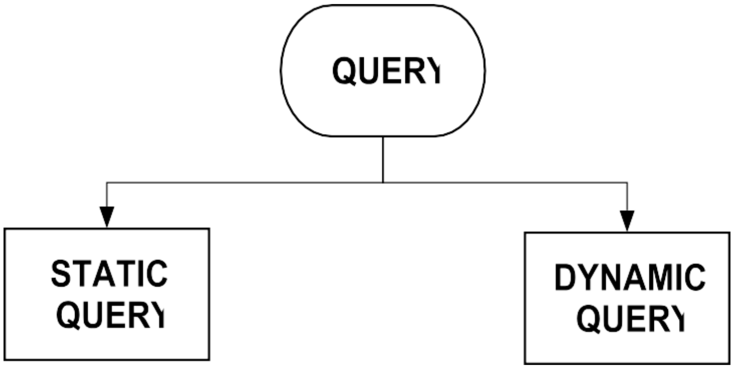


Fig. 2 Types of Query

```
Algorithm 2: (Encryption Process)
SQLI Avoidance (Query)
{
$Inputquery= Query;
$Dbconnection =mysql_connect("host","username","password);
$Selectdatabase =mysql_selectdb("databasename");
$username = md5($username);
$password = md5($password);
$result = mysql_query("select * from tablename where un=‟$username‟ andpswd=‟$password‟”");
While($row=mysql_fetch_assoc($result))
{
Echo $row[„un‟]; Echo  $row[„pswd‟];
}}
```

MD5 ALGORITHM EXPLANATION

This algorithm generates secret key to secure data from intruders. By using thistechnique it blocks intruders from web application. It creates a bridge between databank server and mesh server. The cryptographic algorithm MD5 allows input of arbitrary length and produces as secret key 128 bits long and also known as the “hash”.MD5 hashing is the one way process and it does not allow user / intruder to decrypt data. So the projected system handles technique to block intruder permanently.

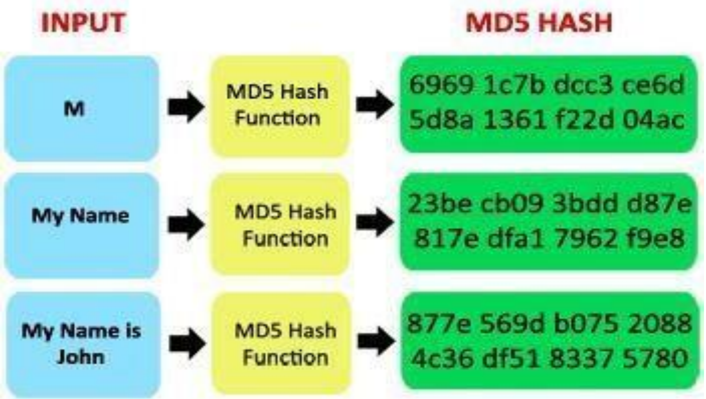
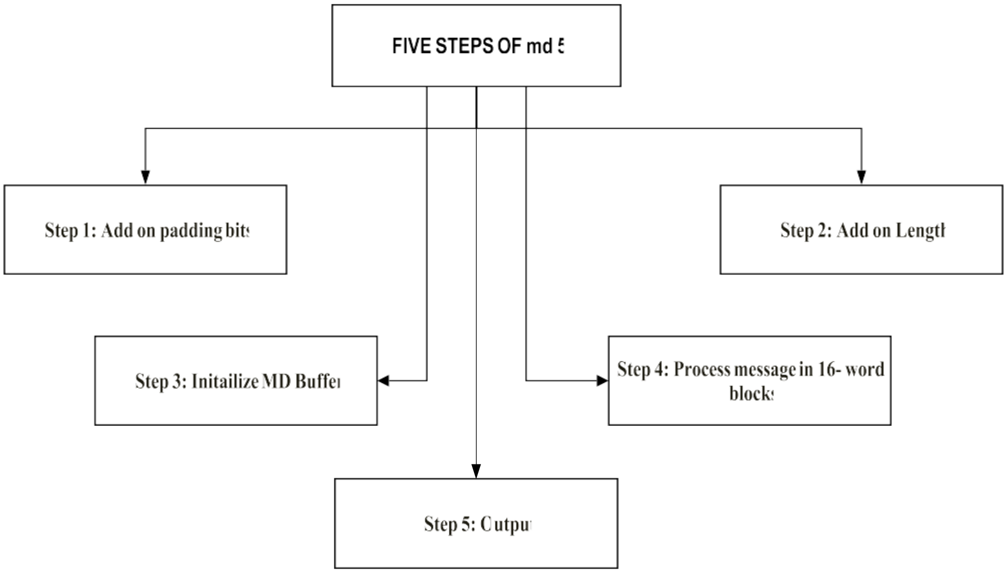

INPUT
MD5 HASH
M
MD5 Hash Function
6969 1c7b dcc3 ce6d 5d8a 1361 f22d 04ac
My Name
MD5 Hash Function
23be cb09 3bdd d87e 817e dfa1 7962 f9e8
My Name is John
MD5 Hash Function
877e 569d b075 2088 4c36 df51 8337 5780

Fig. 3 MD5 Encryption Process

The following steps are followed by MD5 Algorithm:


FIVE STEPS OF md 5
Step 1: Add on padding bits
Step 2: Add on Length
Step 3: Initailize MD Buffer
Step 4: Process message in 16- word blocks
Step 5: Output

The proposed system includes the mix of two calculations[4] Blowfish and MD5. Blowfish calculation is utilized at the customer side and other on the cloud side. The outlined system scrambles the content documents by partitioning them into little pieces. For the most part, the capacity of scrambled records expands the measure of room use which restricts down the work of cloud condition. So the proposed system defeats this issue and furthermore decreases the encryption and also the unscrambling time.The point is to diminish the capacity necessity of the scrambled data and lessen the splitting likelihood of any information section by utilizing the strategy for encryption by blowfish calculation. This is realized that recreation based methodologies in Cloud figuring frameworks and application practices offer numerous huge advantages jump at the chance to test the recently created strategies and arrangements. In this research work, different parameters of the proposed calculation are assessed and test comes about acquired demonstrates that the proposed calculation has lesser encryption and unscrambling time and needs less capacity limit in contrast with EDS-AES calculation. Future noticeable quality is given to the proposed structure execution contrasting with some other distinctive calculations with demonstrates their viability. The work can likewise be reached out by including an improvement system alongside this half breed way to deal with make it as immaculate, successful and practical as could be allowed. An improvement system can be utilized to pack the encoded record size to a more noteworthy degree. Further, advancement system can likewise recognize assaults like measurements like deduplication productivity increment and change in security. In CDC component veiling is utilized to produce high deduplication proportion. To actualize malware and spam both of which are most prominent security dangers.

Chunking[13] is a procedure that parts an entire document or information into isolated pieces. Piecing is connected to recognize duplication in any remote procedures, for example, information deduplication and information pressure. Content characterized lumping is a procedure of part the record into variable length pieces according to the cut focuses characterized at first. Likewise these are additionally testing as byte moving is included which results to be required tobuild the deduplication procedure. While at the same time preparing out substance characterized Chunking onto cloud based Dedup App for the scrambled information put away in cloud brings about change in proficiency.

A procedure which incorporates applying Rabin CDC for reason for making variable size lumps and further preparing that information pieces for scrambled information on cloud. This deals with same information being transferred byvarious clients on same distributed storage a safe deduplication instrument in light of CDC and MD5 has been actualized. In this system genuine dataset is gathered and after that CDC calculation is connected on that information to make irregular pieces. MD5 calculation is utilized for making hash estimation of theories pieces made by CDC which is additionally contributed as an arranged lumped document into our past model.DeDup came about into lessening in transferring and downloading. Execution proposed instrument hadoop record appropriated framework is utilized at back end which helps enhancing system data transmission. DeDup application is made to give better GUI of lumping instrument helps working less demanding for the scrambled information being worked on distributed storage.

RESULT AND DISCUSSION

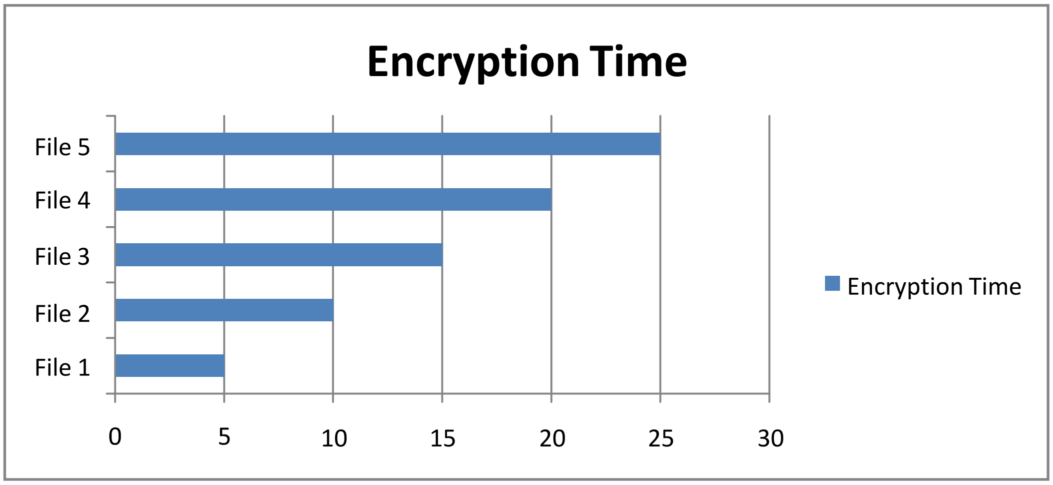
This chapter discusses about final results of proposed system and it shows the speed of encrypted time in microseconds depends on file size. The following files such as file1, file2, file3, file4, file 5 are vary based in file size such as 10 MB, 20 MB, 30 MB, 50 MB, 60 MB so the file encryption time also different. But MD5 hash function has high speed capacity to digest message and the results shown as graph and table

The below table 1 is the experimental results which determines number of files, file size and time taken to encrypt file. The bar graph is created for better understanding.

The speed of secure hash function is shown in Figure 9. This one way technique facilitates to block intruders from web application permanently. MD5 is an effective technique to digest message the speed of encryption is very important so this work used MD5 technique that to helps web admin to feel safe from intruders or vulnerability.

Table 1. Comparison of Encrypted File Depends on FileSize

Sl.No	File Name	File Size forEncryption	Time per ms
1	File 1	10 MB	5
2	File 2	20 MB	10
3	File 3	30 MB	15
4	File 4	50 MB	20
5	File 5	60 MB	30



Graph 1. Comparison graph for encrypted file depends on file size

This tool approves client inputs naturally. Initially the client sends the http demand to web application and it checks information coordinating from database server at that point gets its information not straightforwardly send to Web server. Detection tool validates user inputs thoroughly and then send response to client.

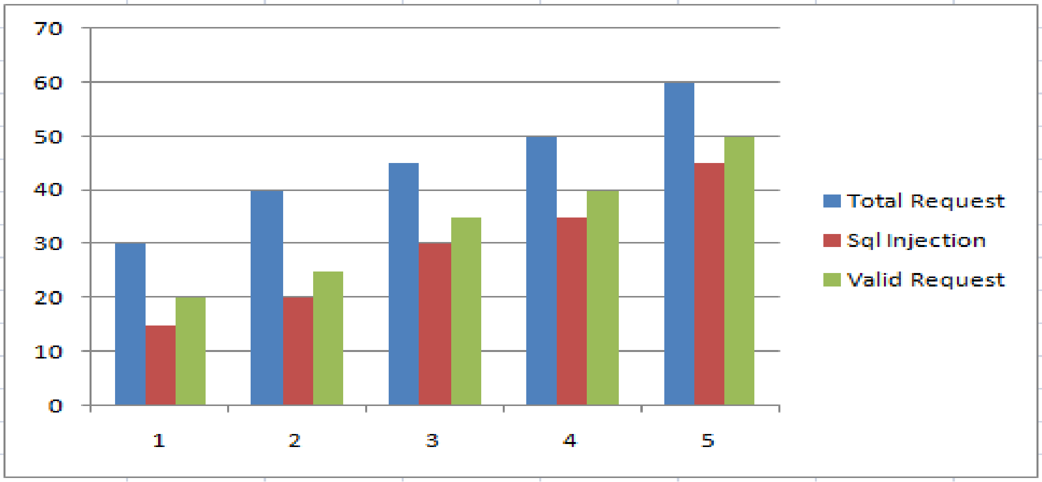


Fig. 4 SQL Infusion Assault Detection Tool Report

SUMMARY

In this research work, a challenge is made to solve all the previous work issues. The detection tool is extremely proficient and quickly analyzes assault when comparing to previous work.Above experimental results, proved projected system has more efficiency to detect SQL Infusion Assault and to prevent web applications from intruders. These results also tackle all the issues which were made by standing work techniques. By generating graphs and tables to make quick investigation about projected and standing work techniques.

REFERENCE

[1] Abdelhamid, Youcef, Ahmed, "Improving web application firewalls to detect advanced sql injection attacks", *Information Assurance and Security*, 2014.

[2] Ahmad Ghafarian, "A Hybrid Method for Detection and Prevention of SQL Injection Attacks", *Computing Conference* 2017, 18-20 July 2017.

[3] Ajit Patil, Aishwarya Laturkar, Prof. S. V. Athawale, RutujaTakale, PriyaTathawade, "A Multilevel System to Mitigate DDoS, Brute forceand SQL Injection Attack for Cloud Security", *International Conference on Information, Communication, Instrumentation and Control*, 2017.

[4] Anushka Gaur, "Analyzing Storage and Time Delay by Hybrid Blowfish-Md5 Technique" *International Conference on Energy, Communication, Data Analytics and Soft Computing* (ICECDS-2017).

[5] Ashwini S Afre, Mrs. Manisha Bharati "DeyPos: For Multi-Users Environments Using MD" 978-1-5090-4264-7/17/$31.00 ©2017 *IEEE.*

[6] Bhale Pradeepkumar Gajendra, "Achieving Cloud Security using Third Party Auditor, MD5 and Identity-Based Encryption" *International Conference on Computing, Communication and Automation (ICCCA2016).*

[7] B.Hanmanthu, B.Raghu Ram, Dr.P.Niranjan, "SQL injection attack prevention based on decision tree classification", *International Conference on Intelligent Systems and Control*, 2015.

[8] Debabrata Kar_, Khushboo Agarwal_, Ajit Kumar Sahoo_, and Suvasini Panigrahi, "Detection of SQL Injection Attacksusing Hidden Markov Model", *IEEE International Conference on Engineering and Technology*, 2016.

[9] Ed Pearson, Cindy L. Bethel, "A Design Review: Concepts for Mitigating SQLInjection Attacks", 4TH International Journal for forensics and security, 25-27 April 2016.

[10] Evans Dogbe, Richard Millham, Prenitha Singh, " A Combined Approach to Prevent SQL Injection Attacks", *Science and Information Conference 2013*.