5

Database Security Attacks

Deepali Kamthania
Vivekananda School of Information Technology
VIPS, Delhi, India
deepali102@gmail.com

Anilesh Kumar
Vivekananda School of Information Technology
VIPS, Delhi, India
anilesh196@gmail.com

ABSTRACT

The data is individual units of information and it is an integral part of every organization. The data is generated very rapidly therefore comes the need for storing this data into a database for efficient management. After storing the data several operations have to performed like data manipulation, data maintenance which can be done by using database management system. As the data is crucial for the organization it is essential to secure the data present in the database. A secure database is the one that is retaliated from different possible database attacks. In an order to make these database secure different types of security models are needed to be implemented. Ensuring security for the database is a very critical issue for the organizations. As the complexity of the database increases, much complex security measures needs to be incorporated. This paper covers different types of attacks that databases faces along with SQL injection attack demonstration on a vulnerable PHP and MySQL based website with possible security attacks control methods.

Keywords: *SQL, DBMS, Injection, AES, MD5.*

1. INTRODUCTION

A database can be defined as a collection of data that is saved on a computer system's hard drive. Databases allow any authorized user to access, enter and analyze data quickly and easily. It's a collection of queries, tables, and views [1]. When a database is created it needs to be managed thus, comes the role of the database management system. DBMS is a software that is managed by an authorized user and can be accessed by other applications to retrieve and analyze the data. The organizations store their day to day transactions and sensitive information to the database and spend a huge capital in securing their databases from intruders. One of the major issues is that many of the database security professionals do not have a full understanding of risk and security issues related to different databases. According to many IT experts, many enterprise DBA's are not aware of which databases, tables, and columns contain sensitive data because they are either handling legacy applications or there are no records or documentation of the data models [2].

In this paper, the MySQL DBMS is taken as the major focus as it is the current market leader and its user base is 32.97%. The paper covers the logical architecture of the MySQL, database security concerns, threats, and possible attacks along with prevention techniques. The recent security attacks are also mentioned which is categorized by different sectors. The demonstration of a SQL injection attack is also performed on a vulnerable PHP based website having MySQL as backend.

2 MYSQL FRAMEWORK

MySQL, the most popular Open Source SQL database management system, is developed, distributed, and supported by Oracle Corporation. MySQL is free and open-source software under the terms of the GNU General Public License, and is also available under a variety of proprietary licenses [3].

2.1.1 MySQL Logical Architecture

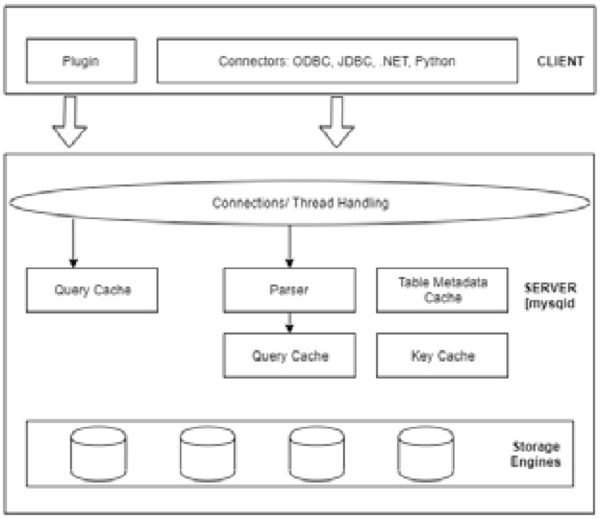


Figure 1: MySQL Logical Architecture [3]

Fig. 1 shows the different layers of MySQL logical architecture.

The MySQL Logical Architecture has different layers:

1. **Client:** Tool to connect and communicate to MySQL server.
2. **Server:** MySQL instance where actual data getting stored and data processing is happening.
   - i. **Mysqld:** It is the MySQL Server and it manages access to the MySQL data directory that contains databases and tables.
   - ii. **Connection/Thread Handling:** Manages client connections/sessions, Task like Authentication (user credentials) and Authorization (User access privileges).
   - iii. **Parser:** Check for SQL syntax by checking every character in SQL query and generate a SQL ID for each SQL query.
   - iv. **Metadata cache:** Cache for object metadata information and DB objects stats.
   - v. **Key cache:** Cache table indexes.
   - vi. **Query cache:** Shared identical queries from memory. If an identical query from client found in a query cache then, MySQL server retrieves the result from the query cache for that query rather than parsing and executing it again [3].
3. **Storage Engines:** Storage engine responsible for SQL statement execution and fetching data from data files.

3. CLASSICAL SECURITY CONCERNS

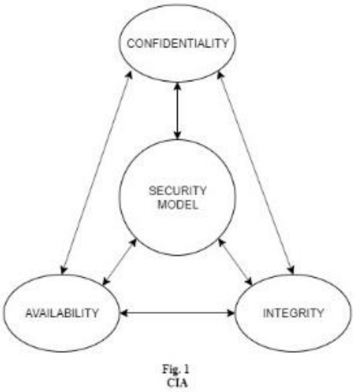


Figure 2. CIA Triad [4]

Fig. 2 shows the CIA Triad of security concerns. **Confidentiality**, **Integrity**, and **Availability**, also known as the **CIA triad**, is a model designed to guide policies for information security within an organization [4]. Confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people.

4. SECURITY THREATS AND POSSIBLE ATTACKS

4.1 Database Security Threats

The threats identified over the last couple of years are the same that continue to plague businesses today, the most common database security threats can be characterized as shown in Fig.3. These attacks are elaborated in the following sections:

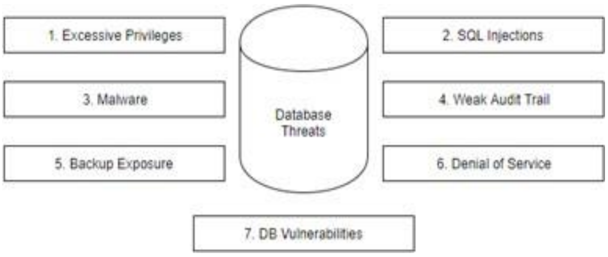


Figure 3. Database Threats

Fig. 3 shows the various database threats as discussed below.

4.1.1 *Excessive Privileges*

When personnel of an organization are granted default database privileges that exceed the requirements of their job functions, these privileges can be abused.

Database rights can be exploited in many ways. Users can misuse privileges for an unauthorized reason. This type of threat is most dangerous due to the abuse of information by authorized users. Such rights can be exploited and create unnecessary risks [5].

4.1.2 *SQL Injections*

SQL Injections are dynamically built SQL statements which are supplied by the intruders via web page input to manipulate the database. It is one of the common database attack technique and this type of attack may lead to the destruction of a database.

4.1.3 *Malware*

Cybercriminals, state-sponsored hackers, and spies use advanced attacks that combine multiple tactics – such as spear-phishing emails and malware – to penetrate organizations and steal sensitive data [5]. Malware is often used to steal sensitive data via legitimate users using infected devices.

4.1.4 *Weak Audit Trail*

DBA's should maintain a record of all database transactions, if they are not auditing the database it represents serious organizational risks on many levels [5]. After a database breach, you don't want to be in a position where you can only say something bad happened, but you can't get detailed information about exactly what happened.

4.1.5 *Backup Exposure*

Backup database storage media is often not safe from an attack and exposure to high risk as well as a natural disaster like flood, earthquake, etc. As a result, many high-profile security breaches have involved the theft of database backup tapes and hard disks.

4.1.6 *Denial of Service*

Denial of Service (DoS) is a type of Database threat in which an intruder attacks a device that leads to a database in which they shut down the whole system or network making it inaccessible to authorized users.

4.1.7 *DB Vulnerabilities*

Finding vulnerable and unpatched databases or finding databases that still have default accounts and parameters for configuration is common. Attackers are able to exploit these vulnerabilities which leads to access of the data in the database.

4.2 Segments of Database Attacks

There are several security layers in a database. These layers are as following: database administrator, system admin, security officer, developers and employee [6] and security can be violated at any of these layers by an attacker.

An attacker can be classified into three classes:

4.2.1 *Intruder*

An intruder is considered an unauthorized user who inordinately accesses a computer system and attempts to obtain beneficial data.

4.2.2 *Insider*

An insider is known as a person who is one of the representatives of trusted users and his / her authority's misconduct and attempts to obtain information beyond his / her allowance.

4.2.3 *Administrator*

An administrator is an authorized user who has privileges to operate a computer system or databases, but who unlawfully uses the rights of his / her administration as per the security policy of an entity to monitor on DBMS activities and obtain important information.

4.3 Types of Database Attacks

The attacks performed on database are basically classified into three types [7]:

4.3.1 *Passive Attacks*

Passive attacks focus on observation. The attacker will observe the data in the database here. A passive attack is dangerous but less problematic than active attacks. Passive attacks are generally carried out without any modification of the data. Passive attacks can be carried out in three ways:

i. **Static Leakage**

   The snapshot of the database is observed in this form of passive attack in the sense of extracting the plain text values at a specified time. Static leakage is only concerned with observing the data in the database for a specified period of time, but after a time the intruder ceases observing the data.

ii. **Linkage Leakage**

   In this type of passive attack, to obtain the plain text value, a link is established between the database value and the position of that specified value in index. Some steps are taken in connection leakage to actually perform the connection attack.

First step in this leakage is to find the index value of the database and find a particular data on which attack is to be performed. And in second step, when the required data value is found in an index of the database, the data get linked with the database value.

iii. **Dynamic Leakage**

In this type of passive attack, the plain text value can be generated by observing the continuous changes performed in database for a particular time. Then after observing the changes the data is analyzed that help the attacker to get the related data about the plain text value [7].

4.3.2 *Active Attacks*

Contrary to the passive attack, the active attack is much more troublesome because passive attack is based on the findings and there can be no shift in information in passive attack [7]. But in active attack, the modification of data is done. Active attacks can be carried out in three ways:

i. **Spoofing**

In spoofing a value is generated by using some algorithm and the original value is then replaced with the newly generated value.

ii. **Splicing**

In this active attack, two cipher text values are there and one cipher text value is then replaced by another cipher text value.

iii. **Replay**

In this active attack, a single cipher text value is replaced with its old version or previously updated value of the cipher text.

4.3.3 *SQL Injections*

SQL Injection is a type of attack in which an intruder passes an unauthorized set of SQL statements via web page input which leads to access of information from a database. SQL injection is one of the most common web hacking techniques. SQL injection is a code injection technique that might destroy a database.

4.4 Recent Attacks

According to Risk Based Security research newly published in the 2019 MidYear QuickView Data Breach Report [8], the first six months of 2019 have seen more than 3,800 publicly disclosed breaches exposing an incredible 4.1 billion compromised records. Perhaps even more remarkable is the fact that 3.2 billion of those records were exposed by just eight breaches. As for the exposed data itself, the report has email (contained in 70% of breaches) and passwords (65%) at the top of the pile. Some of the highlights of data breaches in Q1 2019 [9]:

Table 1: Data Breached in the First Quarter of the Yzear 2019.

Sector	Organization Name	Attack Date	No. of records exposed	Information exposed
Financial	Capital One	22-03-2019 to 23-03-2019	106 Million	Social security number, names, addresses, ZIP codes, phone numbers, email addresses, birthdates, and self-reported income.
Entertainment	Evite	22/02/2019	100 Million	Names, email addresses, passwords, and IP addresses of customers.
Healthcare	American Medical Collection Agency	01-08-2018 to 30/03/2019	>20 Million	Social Security numbers, dates of birth, payment card data, and credit card information.
Education	Georgia Tech	14-12-2018 to 22-03-2019	1.3 Million	Names, addresses, Social Security numbers and birth dates.
Public	Federal Emergency Management Agency (FEMA)	15-03-2019	2.3 Million	Street addresses, financial institution names, electronic funds transfer numbers, and bank transit numbers of survivors of hurricanes Harvey, Irma, and Maria, and the California wildfires.

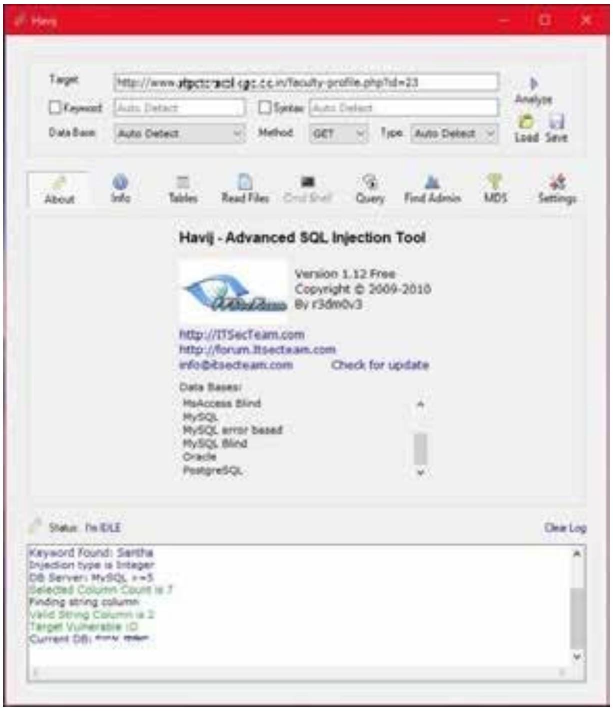
5. DEMONSTRATION ON SQL INJECTION ATTACK

There are different database attacks mentioned in the paper and one of them is SQL Injections (4.3.3 SQL Injections) which is a common attack method used. Given below is a demonstration of a simple SQL injection attack performed on a live website based on PHP and MySQL which is vulnerable and no security layer is present on the website.

In the following Figures, (Fig. 4,5,6,7,8) some of the crucial information of the website have been deliberately omitted for security reasons. With the help of a freeware software "havij" SQL Injection is performed, which is an automated tool SQL injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page.

It is a fully automated SQL Injection tool and it is distributed by ITSecTeam, an Iranian security company. The tool is designed with a user-friendly GUI that makes it easy for an operator to retrieve the desired data.

Step 1: Find a vulnerable website and copy its URL to havij's Target column.



```
Target: http://www.stpctc... .c.in/faculty-profile.php?id=23
□ Keyword: Auto Detect    □ Syntax: Auto Detect
Data Base: Auto Detect    Method: GET    Type: Auto Detect
```

Havij - Advanced SQL Injection Tool

Version 1.12 Free
Copyright © 2009-2010
By r3dm0v3

http://ITSecTeam.com
http://forum.itsecteam.com
info@itsecteam.com   Check for update

Data Bases:
MsAccess Blind
MySQL
MySQL error based
MySQL Blind
Oracle
PostgreSQL

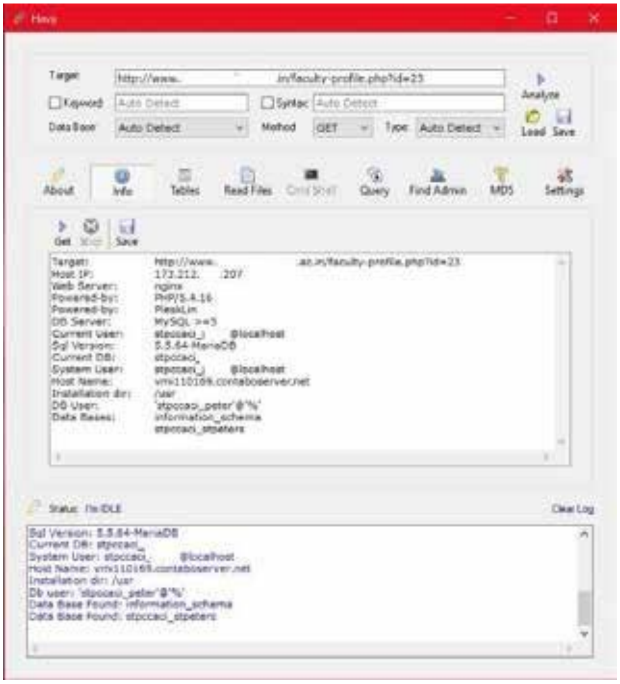
Status: I'm IDLE

```
Keyword Found: Santha
Injection type is Integer
DB Server: MySQL >=5
Selected Column Count is 7
Finding string column
Valid String Column is 2
Target Vulnerable :D
Current DB:
```

Figure 4

Fig. 4 shows the URL of the webpage is loaded to the application.

Step 2: Analyze the vulnerable website by clicking analyze button and the status section shows relevant information about the database linked to that website.



```
Target:            http://www.            .ac.in/faculty-profile.php?id=23
Host IP:           173.212.    .207
Web Server:        nginx
Powered-by:        PHP/5.4.16
Powered-by:        PleskLin
DB Server:         MySQL >=5
Current User:      stpccaci_j      @localhost
Sql Version:       5.5.64-MariaDB
Current DB:        stpccaci_
System User:       stpccaci_j      @localhost
Host Name:         vmi110169.contaboserver.net
Installation dir:  /usr
DB User:           'stpccaci_peter'@'%'
Data Bases:        information_schema
                   stpccaci_stpeters
```

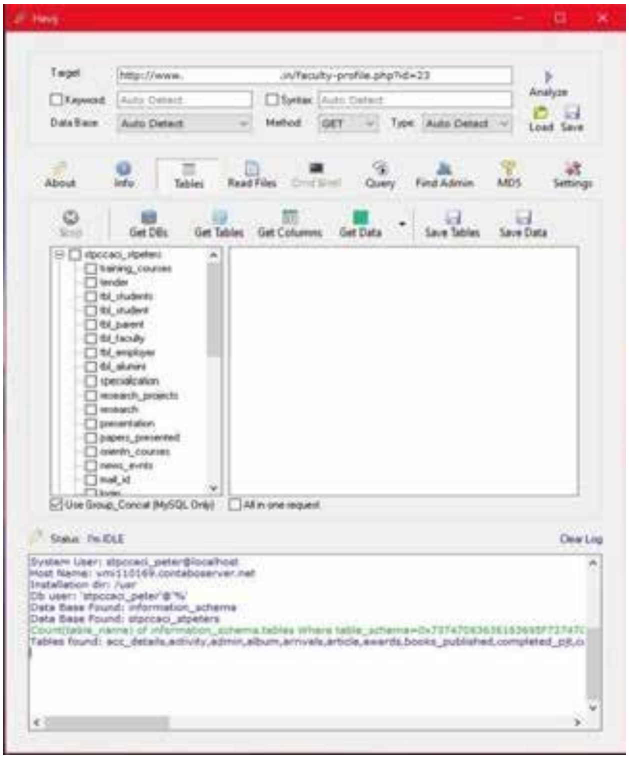
Status: I'm IDLE

```
Sql Version: 5.5.64-MariaDB
Current DB: stpccaci_
System User: stpccaci_      @localhost
Host Name: vmi110169.contaboserver.net
Installation dir: /usr
Db user: 'stpccaci_peter'@'%'
Data Base Found: information_schema
Data Base Found: stpccaci_stpeters
```

Figure 5

Fig. 5 shows the MySQL database details, version number and user of the database.

Step 3: After inspecting the database it lists the number of databases and table present in the server and the data present in the tables can be viewed.

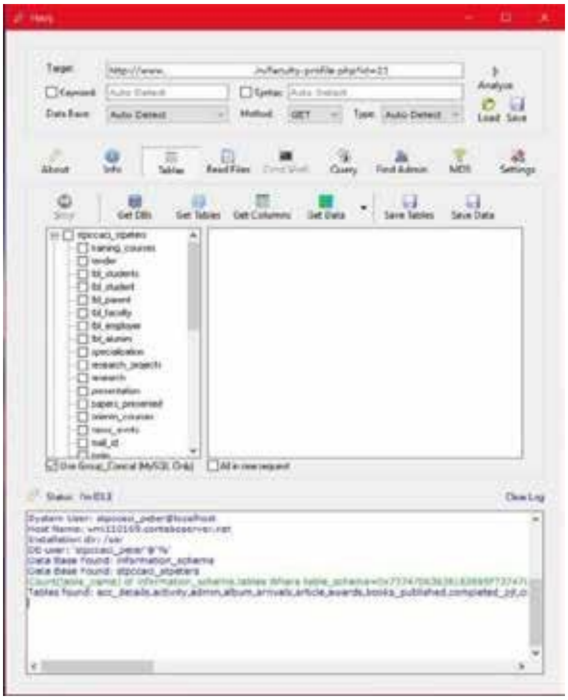


```
⊟ □ stpccaci_stpeters
    □ training_courses
    □ tender
    □ tbl_students
    □ tbl_student
    □ tbl_parent
    □ tbl_faculty
    □ tbl_employee
    □ tbl_alumni
    □ specialization
    □ research_projects
    □ research
    □ presentation
    □ papers_presented
    □ orientn_courses
    □ news_events
    □ mail_id
    □ login
☑ Use Group_Concat (MySQL Only)    □ All in one request
```

Status: I'm IDLE

```
System User: stpccaci_peter@localhost
Host Name: vmi110169.contaboserver.net
Installation dir: /usr
Db user: 'stpccaci_peter'@'%'
Data Base Found: information_schema
Data Base Found: stpccaci_stpeters
Count(table_name) of information_schema.tables where table_schema=0x737470636361636935F73747
Tables found: acc_details,activity,admin,album,arrivals,article,awards,books_published,completed_pjt,c
```

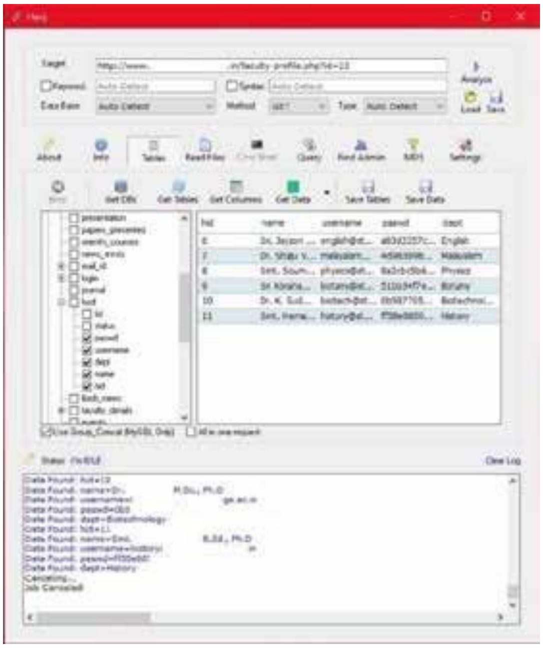
Figure 6 (a)



```
Target: http://www.          .in/faculty-profile.php?id=23
Data Base: Auto Detect   Method: GET   Type: Auto Detect
☑ Use Group_Concat (MySQL Only)   □ All in one request
Status: I'm IDLE

System User: stpccaci_peter@localhost
Host Name: wm110169.contaboserver.net
Installation dir: /usr/
DB user: 'stpccaci_peter'@'%'
Data Base found: information_schema
Data Base found: stpccaci_stpeters
Count(table_name) of information_schema.tables where table_schema=0x7374706363616369...
Tables found: acc_details,activity,admin,album,arrivals,article,awards,books_published,completed_ph_c
```

Figure 6 (b)



fid	name	username	pswd	dept
6	Dr. Jaison ...	english@st...	a83d2257c...	English
7	Dr. Shibu V....	malayalam...	45463998...	Malayalam
8	Smt. Soum...	physics@st...	8a2cb5b4...	Physics
9	Sr. Koraha...	botany@st...	51093f7e...	Botany
10	Dr. K. Sud...	biotech@st...	0b587705...	Biotechnol...
11	Smt. Hema...	history@st...	f55be8850...	History

```
Status: I'm IDLE

Data Found: fid=10
Data Found: name=Dr.                M.Sc., Ph.D
Data Found: username=                    ge.ac.in
Data Found: pswd=0b5
Data Found: dept=Biotechnology
Data Found: fid=11
Data Found: name=Smt.                   B.Ed., Ph.D
Data Found: username=history@              in
Data Found: pswd=f55be85
Data Found: dept=History
Canceling...
Job Canceled!
```

Figure 6 (c)

Figure 6 (a)(b)(c) shows the various table records of the MySQL database.

From the following figures (Fig. 4-6) shows the entire information of the MySQL database. This attack could have been avoided if the owner of the website has deployed any security layer like incorporating SSL certificate etc. and used sessions in their website as the URL was clearly showing the PHP ID which gives clear access to deploy SQL injection attack. While adding data to the database the DBA should have used any encryption method to secure the data.

6. ATTACK CONTROL METHODS

To remove the security threats every organization must consist of a security policy that should be implemented for sure. A strong security policy must contain well-defined security features [10].

i. Access Control

Accesscontrolmakessure that allcommunications between databases and other system objects are as per the policies and controls defined [10]. Even if the intruder tries to manipulate the database, with the help of access control it will not allow to make any changes to the database.

ii. Inference Policy:

The aim of the inference control is to avoid indirect disclosure of information [7]. Generally, there are three ways to unauthorized data disclosure: Corelated Data, Missing Data and Statistical Inference.

iii. User Identification /Authentication:

A basic requirement for security is that you need to know your users. Before you can evaluate their permissions and access rights, you need to recognize them so that you can review their conduct on the information.

Database authentication includes identification and authentication of users. External authentication can be performed by the operating system or network service [7].

iv. Accountability and Auditing:

Accountability and audit checks are needed to ensure the physical integrity of the data which requires defined access to the databases and that is handled through auditing and for keeping the records. The data puts on servers for authentication, accounting and access of a user can be analyzed with the help of auditing and accountability [10].

v. Encryption:

Encryption is the process of converting information into a cipher or a code so that it cannot be readable to all other people except those who hold a key for the ciphertext [10]. The ciphertext or encoded text is called as encrypted data. This can be achieved by using different types of encryption methods such as, MD5 SQL encryption, Asymmetric public key encryption, Advanced Encryption Standard (AES), Cryptography etc.

7. CONCLUSION

Database security is essential for every organization as the database contain their crucial data. As per Norton data breach report around 3800 data breaches have been already reported publicly in 2019, and SQL injection attacks have a major role in it. The attack prevention techniques are mentioned in this paper such as data encryption, database access control, inference policy, etc. Ensuring database security should be a priority for all organizations and cryptography is the key. Security measures should be involved at all levels, starting from the physical level and ending with the data level (physical, network, host, applications, and data).

REFERENCES

1. Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin, Review of Attacks on Databases and Database Security Techniques, Facility International Journal of Engineering Technology and Database Security Techniques Research, Volume 2, Issue 11, November-2012.
2. Sohail IMRAN, Dr Irfan Hyder, Security Issues in Database, Second International Conference on Future Information Technology and Management Engineering, 2009.
3. MySQL Reference Manual https://dev.mysql.com/doc/refman/8.0/en/
4. Ayyub Ali, Dr. Mohammad Mazhar Afzal, Database Security: Threats and Solutions, International Journal of Engineering Inventions, Volume 6, Issue 2, February 2017.
5. Mubina Malik, Trisha Patel, Database Security: Attacks and Control Methods, International Journal of Information Sciences and Techniques, Volume 6, Issue No. 1/2, March 2016.
6. Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar, Database Security and Encryption: A Survey Study, International Journal of Computer Applications (0975 – 888) Volume 47– No.12, June 2012.
7. Preeti Sharma, Monika, Database Security: Attacks and Techniques, International Journal of Scientific & Engineering Research, ISSN 2229-5518, Volume 7, Dec- 2016.
8. https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report
9. https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html
10. Deepika, Nitasha Soni, Database Security: Threats and Security Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 5-Issue 5, May 2015.