*DATABASE SECURITY* : A discuss on the problems involved in keeping a database secure and the possible solutions.

By John Idogun

Student No: 2061190

**7CIO17/UM1 IS/IT Management**

**Department of Information Technology Management, University of Wolverhampton.**

*Table of Content*

1.0*. What is Database Security …………………………………………………………..…3*

1.1. *Authentication……………………………………………………………………………..3*

1.2*. Authorization…………………………………………………………………………….…4*

## *1.2.1 Overview of database authorization (Privilege and roles)……5*

2.0 *Problems with Database security and their solutions………………………6*

3.0 *References ………………………………………………………………………………………..9*

1.0 What is Database Security:

Database security refers to the various means or measures that is use to secure database management systems from vicious, dangerous cyber-attacks. We can also say that database security includes the various tools, measures, and controls designed to preserve or protect data integrity, data confidentiality and data availability. (IBM Cloud Education, Imperva 2018).

Database Security was primarily initiated to protect and address the following

* The data in the database
* The database management system(DBMS)
* Any applications associated or connected to the database
* The network platform used to interact with the database
* The underlying hardware, the physical database server or virtual database server.

Furthermore, database security is a sophisticated and intriguing phenomenon that has to do with various sections of information security technologies and techniques, it is also naturally in disagreement with the usability of the database, i.e. the more usable and accessible a database is the more likely it is to be attacked, Also, the more secured a database is to threats and malicious attack the more difficult it is to access and use. This phenomenom is called Anderson’s Rule.

Basically, Database security can be managed by these two modes of security controls i.e *Authentication and Authorization*

* 1. Authentication:

This has to do with the process of affirming that the logs of a user are in accordance with its rights to perform the activities he/she is authorized to perform. User authentication can be performed at operating system level or the database level itself.

In this present generation, a lot of us are familiar with the idea of authentication, while some of us aren’t, some of us are aware , some may know it, and some may not know it.

For example, when a mobile phone asks for a PIN it is simply doing its job of authentication

Likewise, when a computer asks for a second re-entering of a password it is simply trying to authenticate the user of that account

But when it has to do with databases, the authentication requires one or more dimensions because it happens at different levels, these levels are initiated by the database, or the setup changes to allow either the operating system or some outside methods to be done in authenticating users this can be seen in the Microsoft SQL server, the authentication used by the users is either database authentication, operating system authentication or a mixture of both this is also called the so-called mixed-mode authentication. Techopedia(2022).

Examples of authentication activities or authentication tools are Phone numbers and email confirmation messages, QR code scanners, retinas and finger-prints. The latter two can be called biometrics.

All these examples of authentication stated above are created to assist in keeping the database safe from hackers or malicious users.

In securing a database ,the database security can be managed externally from the database system.

Here are some types of security authentication process:

* Based on Operating System authentications.
* Lightweight Directory Access Protocol (LDAP)

For Database, the security service is a part of the operating system. For Authentication, it requires two different credentials, these are userid or username, and password.

*1.2. Authorization*

This is the process whereby a database management system gets information about an already authenticated user, the information determines the role the user is going to get and privileges-what kind of accessibility would be given to him or her IBM (2021).

## *1.2.1 Overview of database authorization (Privilege and roles).*

For a user to be authorized a *privilege* is given to that individual. A *privilege* is permission given to an authorized user to perform an action or a task. The privilege allows a user to create or access database resources. *Privileges* are stored in the database catalogs. Authorized users can pass on privileges on their own objects to other users by using the GRANT statement. Privileges can be granted to individual users, to groups, or to PUBLIC. PUBLIC is a special group that consists of all users, including future users. Users that are members of a group will indirectly take advantage of the privileges granted to the group, where groups are supported.

A *Role* is a database object that groups one or more privileges. Roles can be assigned to users or groups or other roles by using the GRANT statement. Users that are members of roles have the privileges that are defined for the role with which to access data.

The forms of authorization, such as administrative authority, privileges, and Row and column access (RCAC) access, are discussed in [Authorization of Big SQL objects](https://www.ibm.com/docs/en/SSCRJT_5.0.2/com.ibm.swg.im.bigsql.doc/doc/bi_admin_biga_enable_authorization.html#reference_b1x_pxx_b4). In addition, ownership of objects brings with it a degree of authorization on the objects created.

Here are different ways of permissions available for authorization:

*Primary permission*: Grants the authorization ID directly.

*Secondary permission*: Grants to the groups and roles if the user is a member

*Public permission*: Grants to all users publicly.

*Context-sensitive permission*: Grants to the trusted context role.

*2.0 Problems with Database security and their solution*

## *A) Before deployment security testing must be done.*

Most times, When it comes to the deployment of databases and their websites, software programmers are quick to deploy it without undergoing some form of software testing. Although a series of functionality tests are conducted to ensure its maximum performance this test doesn’t show if they are in tandem with what they are meant to do. So therefore it is necessary that we test the security of the website with different types of tests before we deploy

## *B)Poor Encryption and Data Breaches Come Together.*

In this digital age, a lot of documents are shared and sent online, there are network interfaces that can be tracked by people with malicious intent, this is due to poor software security of a database.

*Solution:* In order to alienate this scenario it is important that one uses TLS or SSL-encrypted communication platforms

## *C) Feeble Cybersecurity Software = Broken Database*

Weak cybersecurity software can result in a feeble database, A Case study of this scenario is the Equifax Data breach of 2017 which affected about 147 million customers of the firm. Upon investigation and findings, they concluded that the cybersecurity software was outdated and weak. This case showed to the general populace how important good cybersecurity software is to defending the database

*Solution:* The Technical department of each firm should conduct user data security testing, regular updating of software, most especially internet security, and at least twice a year an external auditor should audit the software available.

## *D)Stolen Database Backups*

In any organization there are two kinds of threats available that is internal and external, the internal threats is perpetuated by staff, workers, and generally people with internal access to an organization.

No matter the sophistication and complexity of software the loyalty of staff can be questioned, times without numbers there are times companies contend with internal threats more than external. Any individual who has access to sensitive data can sell it to a third party for gains this in turn will affect the company’s reputation.

*Solution:* Access should be restricted for all except the keyworkers. The database should be encrypted, strict security standards executed and a fine should be given if there is a violation of any of these.

## *E) Flaws in Features.*

Databases are hacked when a weakness in the features is noticed. Hackers input some code into the system to break it.

*Solution*: The best way to protect this is by undergoing security testing from a third party, the chances of ensuring good protection of each database is by making the functional structure simpler and better.

## *F) Weak and complex database infrastructure*

Hackers don’t successfully hack into an establishment or company’s database in one go, it takes time and constant monitoring of the site. They opt for playing the hopscotch game where they look for weaknesses within and then use it to their advantage. Until they get access to the database they keep on launching series of attacks. *Wishdeck( 2018).*

A complex database is very easy to attack because there are chances that one will neglect and fix its weaknesses, most times security softwares are not capable of mitigating and protecting the system from attacks.

*Solution*: It is important that every department in the organization has a controlled access to its database and the organization should use a decentralized approach to database designing this makes security better.

## *G) Poor data protection as a result of limitless administration access*

Access should be restricted to certain people this will assist in a smart division of duties and curb data breach, if a lot of persons has an access to a database there is a likelihood that data could be stolen.

*Solution:* users won’t be given administrative access this way users that are not involved in administration process will experience difficulties in stealing data. Another possible solution will be to limit the number of user accounts so that if hackers gain access to these accounts they are only able access few accounts.

## *H) Website Security should be tested to avoid SQL Injections*

SQL injections has been an age long way of breaching the security of data. SQL injection attacks the database and front end. The codes are inserted as strings forcing admin officers of the database to wipe out the malicious codes. Also, studies have shown that one of the greatest and simple way to effect data breach is through SQL injections.

*Solution:* The solution to this will be web application security and the implementation of firewalls.

## *I) Adequate Management of Encryption Keys*

Sensitive data are best protected when we encrypt them and we have to assign the keys to various competent individuals, this is paramount because these information can be targeted by hackers.

Important keys like encryption keys are meant to be guarded meticulously.

## *J) Irregularities in Data*

Inconsistencies in data can result in an inconsistent database, and oftentimes this lead to vulnerabilities in the security of the websites.

*Solution :* The data input into the database should be consistent

*References*

Impeva (2018) . *Database Security*, Available at <https://www.imperva.com/learn/data-security/database-security/>- Accessed on 19/12/2022

IBM Cloud Education (2019). *Database Security* , Available at <https://www.ibm.com/cloud/learn/database-security>. Accessed on 19/12/2022

Tutorialspoint (2021) Database Available at https://www.tutorialspoint.com/db2/db2\_database\_security.htm#. Accessed on 19/12/2022

Techopedia (2022), *Database authentication*. Available at [https://www.techopedia.com/definition/27388/database-authentication Accessed on 19/12/2022](https://www.techopedia.com/definition/27388/database-authentication%20Accessed%20on%2019/12/2022)

IBM Db2 SQL(2021*). Database Authorization*. Available at https://www.ibm.com/docs/en/db2-big-sql/5.0.2?topic=authorization-database Accessed on 19/12/2022

WishDesk(2018), *Most Common Database Security Issues and how to solve them*. Available at- <https://wishdesk.com/blog/database-security-issues#:~:text=Database%20security%20issues%20and%20what%20to%20do%20with,Outdated%20software%20...%208%20Logging%20not%20configured%20>. Accessed on 19/12/2022