International Journal of Computer Applications Technology and Research
Volume 13–Issue 07, 35 – 38, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1307.1005

Database Security: Navigating Threat Landscapes and Defense Mechanisms

Aliyu Umar
Department of Information Technology
Taraba State University
Jalingo Taraba State, Nigeria

Yahaya Saidu
Department of Computer Sciences
Taraba State University
Jalingo Taraba State, Nigeria

Tirmizi Mohammed
Department of Computer Science
Taraba State University
Jalingo Taraba State, Nigeria

Ahmed Musa Iliyasu
Department of Computer Sciences
Taraba State University
Jalingo Taraba State, Nigeria

Abstract: In today's interconnected world, databases serve as the backbone of virtually every organization, handling vast amounts of sensitive information. However, with this reliance comes a host of security threats that can jeopardize the integrity and confidentiality of data. This paper presents a comprehensive review of ten prominent threats to databases, ranging from SQL injection attacks to insider threats and data breaches. Each threat is analyzed in detail, highlighting its potential impact and offering effective solutions for mitigating risks. By understanding these threats and implementing robust security measures, organizations can safeguard their databases against malicious actors and ensure the continued integrity and availability of their data assets.

Keywords: Database security; Threats; Solutions; Defense mechanisms; Denial of Service (DoS) attack

1. INTRODUCTION

Databases are integral to daily activities, whether in government, private, or individual use, as they store sensitive information. A database comprises related records, and each record contains related fields. There are two main types of databases: manual-based systems, also known as traditional databases, and computerized database systems. Traditional databases, often found in offices, store records in files kept in cabinets. Computerized or modern database systems can be further categorized into flat databases and relational databases. Flat databases store records in a single table, while relational databases store records in multiple tables with relationships between them. Relational databases are widely preferred due to advantages such as reducing redundancy. The Database Management System (DBMS) is the program responsible for managing and monitoring access to the database, allowing authorized individuals to access it. Finally, the Database Administrator controls access, ensuring that only authorized users access the database.

3. THREATS OF DATABASE

SQL injection attacks occur when attackers insert unwanted or malicious database statements into Structured Query Language (SQL) queries, exploiting vulnerabilities in the system to access sensitive information from the database. Here are the sources of SQL injection attacks: Web forms: Attackers can insert malicious SQL statements into web forms, which are graphical user interfaces (GUIs) used by authorized users to access information or data. These web forms contain detailed information needed by authorized users, such as employee identification numbers, names, salary grades, addresses, departments, and more. Attackers exploit vulnerabilities in web forms by injecting malicious SQL statements to gain access to sensitive information. Server variables: SQL injection can also be inserted into server variables, which are used to retrieve server-related information, such as AUH-TYPE used for user authentication or validation. Attackers inject server variables to access authorized users' passwords and usernames, enabling them to perform malicious activities [5]

Operating system vulnerabilities pose significant risks to the security of databases, including popular systems like Linux and Windows, as well as associated services linked to databases. Exploiting vulnerabilities in the operating system can lead to unauthorized access to the database. For instance, an attacker could exploit vulnerabilities to launch a Denial of Service (DoS) attack. By flooding the network with excessive traffic, legitimate users may be unable to access the database, effectively denying them service. This creates an opportunity for the attacker to gain unauthorized entry into the organizational database while the legitimate users are unable to connect. [5].

Privilege abuse occurs when a legitimate database user, who is authorized, misuses their privileges to carry out unwanted or unlawful activities within the database. For instance, an authorized user with access rights to view and edit employee records might abuse this privilege by increasing an employee's salary without proper authorization. Such actions can be detrimental to an organization. [6]

Excessive privilege abuse occurs when authorized users are granted database privileges that surpass their legitimate needs. This grants them access to sensitive data or functionalities they shouldn't have, which could be exploited for unlawful or malicious purposes. For instance, consider an authorized user with access to view employee details in a Human Resource Management System database. If this user is granted privileges beyond what is necessary—such as access to salary information or employee performance records—they may abuse this excess privilege. This could involve unauthorized viewing, manipulation, or dissemination of sensitive data, compromising the confidentiality and integrity of the system [5] [2]

Administrative abuse refers to situations where a database administrator misuses their authority to carry out malicious activities within the database. For instance, an administrator might change employee records, such as their salary or grade level, for personal gain or other malicious purposes. This abuse of privilege can have significant consequences within an organization's database system [7]

Denial of Service (DoS) attacks can be launched by attackers to disrupt the functionality of a system or network, particularly targeting the organization's network. This can be achieved through various means such as generating excessive traffic, causing data corruption, flooding the network, or enforcing heavy traffic on the organizational network. The objective is to prevent authorized users from accessing the database [2]

Following a successful DoS attack, the attacker may proceed to carry out unlawful activities on the database. For instance, if the attacker aims to access financial transactions to steal money, they might crash the server to deny access to authorized users and then proceed to steal money from the database. Such actions result in significant losses for organizations that rely on database systems to store important or sensitive information [2]

Privilege elevation poses a significant threat to database systems. An ordinary user within an organization could exploit vulnerabilities in the software to gain additional privileges, elevating their status from a normal user to a system administrator. Once elevated to a system administrator, they may then use their newfound privileges to carry out malicious or unlawful activities, gaining unauthorized access to important information stored in the organizational database [8]

For instance, the perpetrator of such malicious activity might manipulate financial records for an employee by increasing their salary without authorization. This issue can lead to setbacks for the organization, as it compromises the integrity and security of its database system.

Backup exposure occurs when unauthorized users gain access to database backups with the intention of obtaining vital information. This exposure can occur through connections with insiders, such as having a friend who is an authorized user within the organization. In such cases, unauthorized individuals may exploit these connections to obtain access to the database backup [2]

Additionally, authorized users or insiders themselves may also be perpetrators of database backup theft. These individuals, who have legitimate access to the database, may steal the backup for the purpose of accessing sensitive information stored within the organizational database. The theft of database backups poses a significant risk of database exposure, which can be highly detrimental to organizations relying on their database systems to safeguard sensitive information.

Weak authentication poses a serious threat to database security, as it can provide attackers with the means to identify legitimate users and gain unauthorized access to the database. Attackers may employ various methods to steal login credentials for authorized users. One method is direct credential theft, where unauthorized users obtain or steal login credentials belonging to legitimate database users. Social engineering is another technique attacker may use. In this scenario, the attacker takes advantage of being in proximity to a legitimate database user, perhaps posing as a computer engineer tasked with maintaining the organization's computers. Through this ruse, the attacker may obtain the login credentials or username and password of an authorized database user. Additionally, attackers may resort to brute force methods, systematically trying different combinations of letters and numbers to crack passwords and access sensitive information stored in the organizational database. Addressing weak authentication is crucial for safeguarding database security and protecting sensitive organizational data [10]

Weak audit trails present a significant risk to database security. Deploying a robust database audit mechanism to track all activities and transactions within the database is crucial. Failure to implement such mechanisms can lead to substantial losses for organizations [11]

For example, both insiders and outsiders could act as attackers. Without proper audit mechanisms to capture comprehensive information about both authorized and unauthorized users, including usernames, passwords, the source and location of operations, and even images of attackers, an organization remains vulnerable to various threats [9]

Failure to address this issue constitutes a serious problem for organizations, as it compromises their ability to monitor and respond effectively to security incidents.

4. SOLUTIONS TO THREATS

To prevent SQL injection attacks, implementing the following methods is advisable: Virtual Patching or Web Application Firewall (WAF): This technology is utilized to control and monitor any malicious activities targeting the database. A WAF acts as a protective barrier between the web application and the internet, filtering and blocking potentially harmful traffic, including SQL injection attempts. Green SQL: Developed by Microsoft, Green SQL is software designed to control database access by blocking SQL injection attacks. For instance, if an unwanted or attacker is detected, Green SQL captures detailed information about the attacker, such as their source internet protocol (IP) address, operating environment, and username. By deploying these methods, organizations can significantly enhance their defenses against

SQL injection attacks and mitigate the associated risks to their databases [1][5]

Operating System (OS) vulnerabilities can be mitigated through two primary methods: regular updates of the database and the implementation of intrusion prevention systems (IPS). Regular updates help prevent attacks or unauthorized access to the database by addressing any known vulnerabilities in the OS. However, continuous updates may not always be sufficient, especially in the presence of new vulnerabilities. In such cases, intrusion prevention systems become necessary. IPS monitors the application and identifies any attackers attempting to gain unlawful access to the database through network traffic. The combination of these two methods can significantly improve the organization's security posture [12]

To prevent privilege abuse in a database, implementing access control methods is essential. These methods not only control access to database queries but also manage access to the database context itself. Access control provides detailed information about legitimate database users, including their usernames, passwords, and the source of application names. By deploying access control mechanisms, organizations can effectively restrict access to sensitive data and prevent unauthorized users from abusing their privileges within the database environment.

To address the issue of excessive privilege abuse, one effective solution is the implementation of query-level access control. This control mechanism restricts database privileges to only the necessary level required for normal operations. With query-level access control in place, if an authorized user attempts to exceed their designated privileges by executing a query that accesses unauthorized data or functionality, the system triggers an alert. This alert notifies the system administrators of the attempted breach, allowing them to intervene and prevent potential malicious activities from occurring within the database. By employing query-level access control, organizations can enforce granular access permissions, ensuring that users are only granted the precise privileges required for their specific tasks. This proactive approach enhances database security and helps mitigate the risks associated with excessive privilege abuse. [7]

The solution to addressing Administrator Abuse involves implementing access control measures. These measures aim to capture detailed login information about legitimate administrators, including their username, password, system used, timestamp of access, and location. With access control in place, it becomes possible to detect any misuse of database privileges by administrators who engage in malicious activities. By implementing access control, organizations can enhance their security posture and minimize the risks associated with Administrator Abuse [13]

To prevent a Denial of Service (DoS) attack, one method is to configure the firewall to block unauthorized users or attackers from accessing sensitive information. The firewall can filter packets from attackers and block their access attempts, allowing only authorized users to access information from the database. Another approach is to disable all unnecessary or unused network services, as attackers might exploit these services to gain access to the database through the network. Implementing both methods can significantly enhance the organization's operational security. [9]

The solution to privilege elevation involves implementing both traditional intrusion prevention systems (IPS) and access control measures. The traditional IPS is designed to capture or detect any unauthorized attempts to access a database. Access control, on the other hand, is geared towards identifying any individuals attempting to use abnormal Structured Query Language (SQL) to access vital information within the database [4]

To prevent exposure of database backups, the organization needs to employ several strategies. First, encrypting sensitive information stored on backup devices is crucial. This ensures that even if attackers steal the backup device, they won't be able to access any sensitive information since it's encrypted. Secondly, implementing an audit mechanism is essential. This mechanism tracks attackers by recording their movements, and it can even capture their picture or face. This allows the organization to trace the attacker and take appropriate actions. By utilizing these methods, the organization can effectively prevent database backup exposure [2]

To mitigate unauthorized access due to weak authentication, implementing a restriction where users can only access the database from specific Internet Protocol (IP) addresses is advisable. By defining access permissions based on IP addresses, users would be restricted from accessing the database from locations outside of the defined IPs. This measure effectively prevents unwanted or unauthorized users from gaining access to the database [2]

Improving weak audit trails requires enhancing the audit mechanism to operate at higher speeds. This can be achieved by offloading audit mechanisms or appliances onto the network, which can significantly enhance an organization's capabilities. Universal user tracking software is utilized to capture comprehensive login details about users, including usernames and passwords.

Grand Transaction tracking software is an advanced tool designed to capture any unauthorized access to the database, including details such as the source operating system and hostname [6]

5. CONCLUSION

Investing in database security is crucial for organizations to safeguard their valuable information assets and uphold stakeholder trust. By implementing robust security measures, organizations can confidently protect their databases from potential threats and vulnerabilities, ensuring the integrity, confidentiality, and availability of their data. Prioritizing database security not only fortifies an organization's defenses but also enhances its overall resilience against cyber threats, thereby supporting sustained operational success and stakeholder confidence.

6. ACKNOWLEDGMENTS

We extend our heartfelt appreciation to the reviewers for their constructive comments, which have greatly enhanced the quality of this paper..

7. REFERENCES

[1] Anjaligupta, R., & Ramya, R. (2022). *Descriptive analysis on database security techniques.* International

Journal of Novel Research and Development, 7(10), 1-5. https://doi.org/10.2456/4184

[2] Teimoor, R. A. (2021). *A review of database security concepts, risks, and problems*. *UHD Journal of Science and Technology*, 5*(2)*, 38-46.

[3] Ali, A., & Mazhar, M. (2017). *Database Security: Threats and Solutions*. *International Journal of Engineering Inventions*, 6*(2), 25-27*

[4] Rekha Ahirwar, Rashi Saxena, Pankaj Yadav (2016, March). Challenges to Data Base Security – A Futuristic View. IOSR Journal of Computer Engineering. Vol. 18 . issue.2 pp.01-04

[5] Shulman, A n.d, Top Ten Database Security Threats How to Mitigate the Most Significant Database Vulnerabilities. Available from:<http://www.schell.com/Top_Ten_Database_Threats.pdf>. [5 March 2016].

[6] Tejashri R. Gaikwad1, A. B. Raut2 (2014, April). A Review on Database Security. International Journal of Science and Research (IJSR) Vol.3 issue.4,pp.372-374 IEEE

[7] Top Ten Database Security Threats (2014). White Paper. Available from :< http://www.imperva.com/docs/wp_topten_database_threats.pdf>. [4 March 2016]

[8] P. K. Rai (2015, June). *An overview of different database security approaches for distributed environment*. IJISET - International Journal of Innovative Science, Engineering & Technology. Vol. 2. Issue. 6 pp. 2348 – 7968

[9] T.Gunasekhar, K.Thirupathi Rao, P.Saikiran3 and P.V.S Lakshmi(2014). *A Survey on Denial-of-Service Attacks. International* Journal of Computer Science and Information Technologies. Vol. 5 (2) 2014, 2373-2376

[10] Malik, M, & Petel,T, " Database Security - Attacks And Control Methods" in Cmpica, Charotar University of Science & Technology (CHARUSAT), Changa. 2006 Available from:< http://charusat.net/NCSCA2016/NCSCA-2016_Conference-proceeding/>.[2 March 201 6].

[11] Singh A, Singh. P, Nath. U (2015, May). Enforcing Database Security in Un-trusted Environment by using Multisession and Biometrics based Authentication. International Journal of Emerging Research in Management &Technology. Vol.4, issue.5 pp. 207-2011

[12] Mittal, K& Rohilla, S. (2013, *May). Database Security: Threats And Challenges*, International Journal Of Advance Research In Computer Science And Software Engineering,vol.3, no.5, pp.810-813.

[13] Mou Shen, Mengdong Chen, Min Li and Lianzhong Liu(2013) . Research of Least Privilege for Database Administrators. International Journal of Database Theory and Application Vol.6, No.6 . pp.39-50

[14] Al-sayid, A. and Aldlaeen, D(2012).Database Security Threats: Survey Study. , 2013 5th International Conference on Computer Science And Information Technology (CSIT), Applied Science University, Amman, Jordan, pp.60-64. IEEE