DATABASE SECURITY BEST PRACTICES

Group 2

AGENDA

- INTRODUCTION
- DB SECURITY THREATS
- WHY IT IS IMPORTANT
- BEST PRACTICES
- CONCLUSION

INTRODUCTION

Database security means establishing and preserving database confidentiality, integrity, and availability (CIA) using tools, controls, and measures.[1]

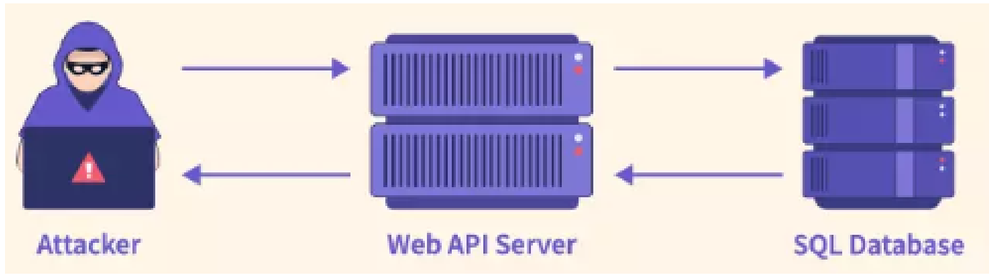
Database security addresses:

- The data in database
- DBMS
- The computing and/or network infrastructure used to access the database

DB SECURITY THREATS

1 sql injection attacks

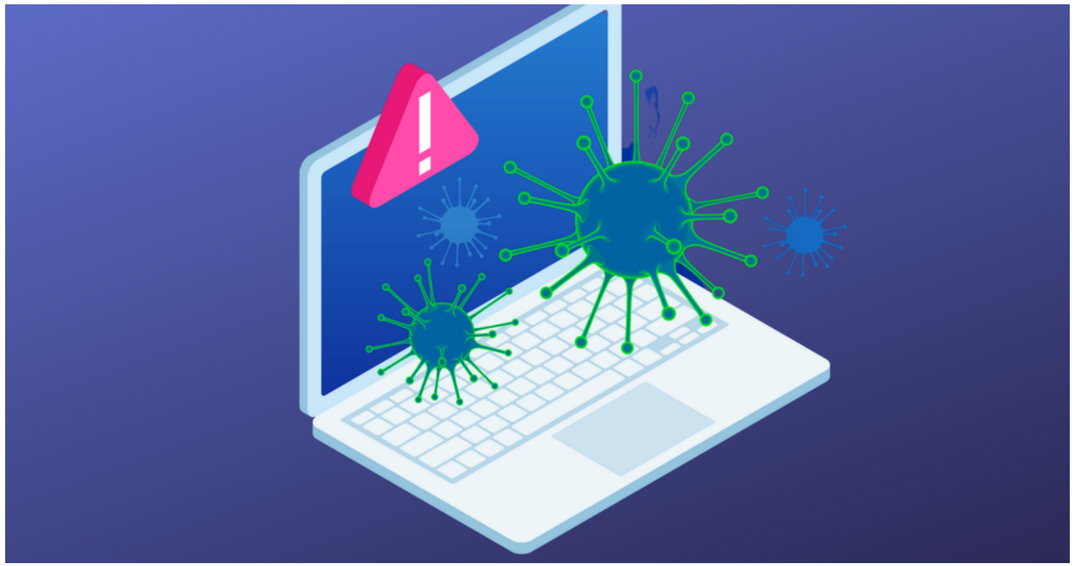
SQL injection is the most common threat. This attack is performed by entering a query into a SQL form, and if the database interprets the result as “true” it enables access to the database.



DB SECURITY THREATS

2 Malware attacks

Malware is designed to target vulnerabilities on a network, granting access to a database, or causing damage to it. These vulnerabilities relate to unprotected endpoints on a network that can be exploited via a range of different attacks.



DB SECURITY THREATS

3 Denial of Service attacks

A Denial of Service (DoS) attack occurs when a database server receives more requests than it can process, causing the system to become unstable or crash. These erroneous requests can be created by an attacker and directed at a specific target. The volume of fake requests overwhelms the system, resulting in downtime for the victim.

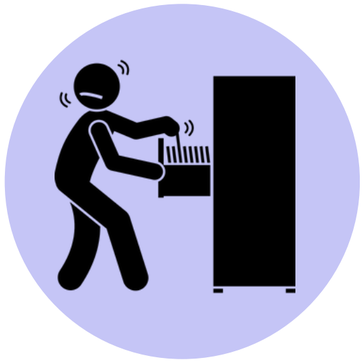
DB SECURITY THREATS

4

Database Backup Exposures

Backing up a database regularly is obviously recommended, but often, many of these backups are left unprotected, making them a common target for attackers. Securing backups is especially vital for industries that hold vital customer information, such as healthcare providers or banks and financial institutions.

WHY IT IS IMPORTANT



Protecting Sensitive Information

Maintaining Business Continuity

Preventing Cyber Attacks

WHY IT IS IMPORTANT

Protect the Organization's Customers

Conserve the Organization's Reputation

Complying with Government Regulations

BEST PRACTICES

In today's digital age, where data has become the lifeblood of organizations, the security of databases is of paramount importance.

Database security best practices are a set of guidelines and measures aimed at safeguarding databases from unauthorized access, data breaches, and other security threats.

BEST PRACTICES

Access Control

Implement strong access control mechanisms to ensure that only authorized individuals can access the database.

Encryption

Encryption serves as a vital security measure to protect data both at rest and in transit.

Patching and Updates

Staying up to date with patches and updates provided by database vendors is critical to address security vulnerabilities.

BEST PRACTICES

Database Auditing

Monitor and log database activities, track who accessed the database, what actions were performed, and detect any suspicious behavior.

Secure Configuration

Follow the principle of least privilege by granting users only the necessary privileges required for their tasks.

Backup and Recovery

Implementing a robust backup and recovery strategy ensures business continuity and protection against data loss.

BEST PRACTICES

Regular Security Testing

Conduct regular security assessments, vulnerability scanning, and penetration testing on the database systems.

Training and Awareness

Provide regular training and awareness programs for the employees to educate them about database security best practices.

Incident Response Plan

Develop an incident response plan that outlines the steps to be taken in the event of a security breach.

CONCLUSION

Database security best practices serve as a critical defense mechanism in an era of escalating cyber threats.

Thank you for listening ♡

Do you have any questions?

REFRENCES

1 “Database Security: An Essential Guide | IBM,” Ibm.com, 2022. https://www.ibm.com/topics/database-security#:~:text=the%20next%20step-,What%20is%20database%20security%3F,compromised%20in%20most%20data%20breaches. (accessed May 21, 2023).