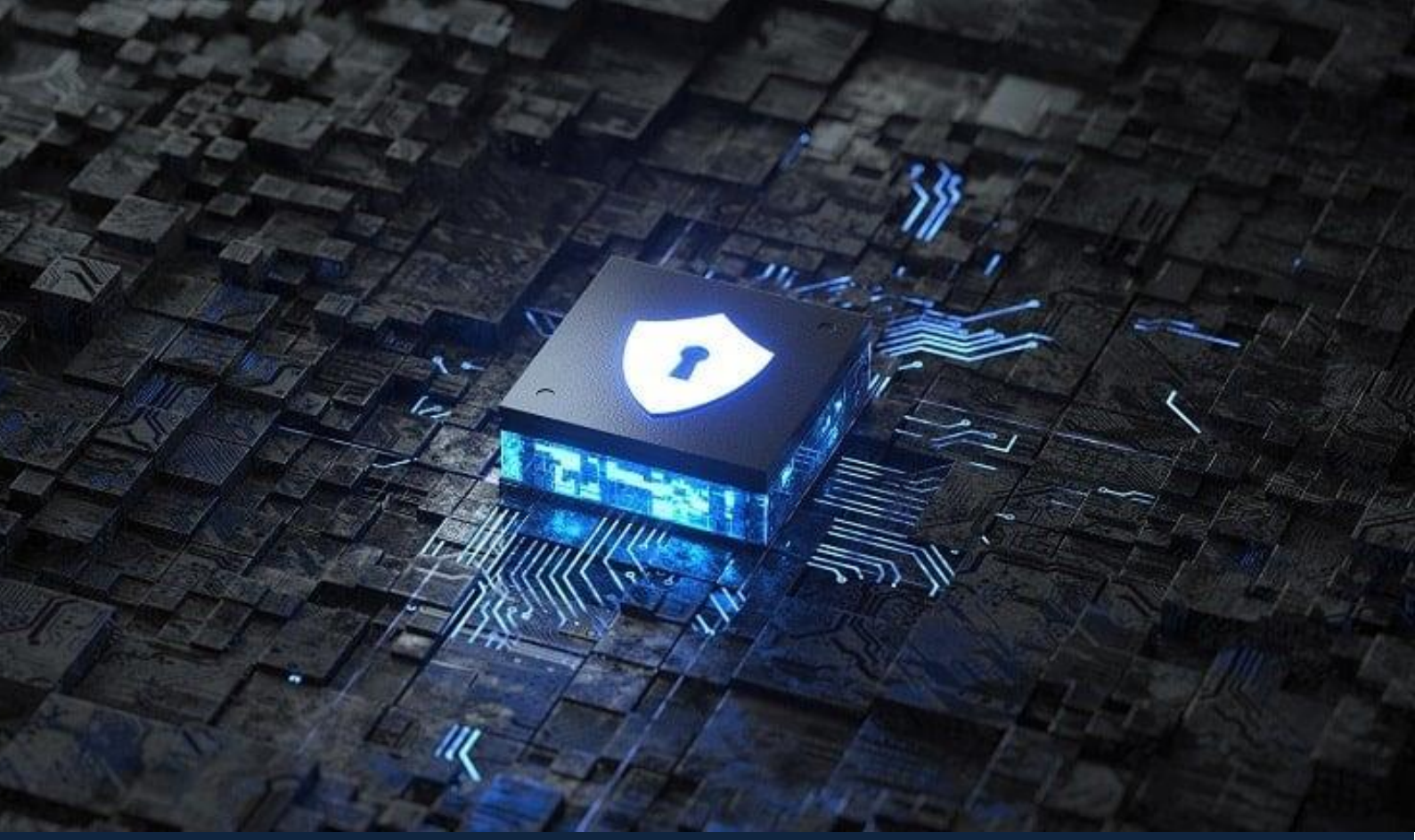

Theoretical essay

Database Security

Author: Ketheeswaran Ammar Syed
January 15, 2023

UNIVERSITAS STUDIORUM FLUMINENSIS · SVEUČILIŠTE U RIJECI ·

uniri

1. Introduction

Database security refers to the protection of the database against illegal access, usage, disclosure, disruption, alteration, or destruction. It includes a wide range of measures designed to stop unauthorized users from accessing, using, disclosing, disrupting, altering, or destroying database data. This includes the protection of the database and its infrastructure from intrusions, breaches, and other security-related problems.

The security of databases is essential to the overall security of an organization since databases frequently include sensitive and confidential information, such as financial information, intellectual property, and personal data. Therefore, protecting databases calls for a thorough strategy that incorporates both technical and administrative restrictions. Technical controls include firewalls, intrusion detection and prevention systems, encryption, and security measures incorporated into the database software. To guarantee that the database is correctly configured, maintained, and used in a secure manner, administrative controls include security rules, procedures, and guidelines.

According to the National Institute of Standards and Technology[1] (NIST) in its publication "Guidelines for the Secure Configuration of Databases", it is defined as:

"The protection of the database and the data stored within it from unauthorized access, use, disclosure, disruption, modification, or destruction. Database security includes, but is not limited to, protecting the database software, database servers, database applications, and the data stored in databases."

The Ponemon Institute states that the average cost of a data breach is $3.86 million, and databases are often the primary target of cybercriminals.[2]

As per the OWASP foundation, protecting sensitive and confidential information stored in databases is essential to the overall security of an organization. Unauthorized access, use, disclosure, disruption, modification, or destruction of data can have severe consequences, including loss of reputation, legal liabilities, and financial losses.[3]

In short, protecting the integrity, confidentiality, and availability of the data stored in databases is essential to the overall security of an organization as it prevents unauthorized access and use, breaches or disruptions of sensitive data and can help to avoid costly financial losses and damage to reputation.

[1] https://csrc.nist.gov/publications/detail/sp/800-122/final
[2] https://www.ibm.com/reports/data-breach
[3] https://owasp.org/top10/

2. Threats to Database Security

Due to the large amount of private information they collect and handle, databases are frequently a top target for cybercriminals and other hostile actors. Personal information, financial information, and intellectual property are just a few of the types of data that are kept in databases. This makes them a desirable target for hackers and other bad actors who want to take advantage of flaws in the database or its infrastructure.

Threats to database security can take many various forms, each with its own traits and potential repercussions:

- SQL injection attacks, which take advantage of flaws in the database to access or change data without authorization.
- Insiders with bad intentions who might corrupt or steal data using their access to it.
- Unauthorized access, which happens when an attacker uses a database without authorization.
- Data leaks, which can happen when an attacker steals private information from a database.
- Denial-of-service (DoS) attacks, which can prevent a database from being accessible.
- Advanced persistent threats (APTs), which are complex offenses frequently launched by well-organized and paid groups.

Protecting the integrity, confidentiality, and availability of the data held in databases requires an understanding of the various threats to database security. We will go through these risks in more detail and look at the different methods and approaches that may be utilized to secure databases in the parts that follow.

2.1 SQL Injection

SQL injection is a type of cyber-attack that exploits vulnerabilities in the database to gain unauthorized access or modify data. It occurs when an attacker is able to insert malicious SQL code into a web application, which is then executed by the database. This can allow the attacker to access sensitive data, such as login credentials, personal information, and financial data.

According to OWASP (Open Web Application Security Project) foundation, SQL injection is the number one web application security risk. It's also reported as one of the most common web application attack vector.

Preventing SQL injection attacks requires a combination of input validation, prepared statements, and least privilege principle. Input validation is used to check user input for dangerous characters that can be used to inject SQL code. Prepared statements are used to separate data from SQL code, making it more difficult for attackers to inject malicious SQL code. Least privilege principle is used to limit the access of users and applications to only the data and functionality that they need.

According to the National Institute of Standards and Technology (NIST) in its publication "Guidelines for the Secure Configuration of Databases", it is defined as: