**REPORT CREATED BY:  
ZAINAB ARIF**

# Task: Research different databases available today and find the most secure one with least number of vulnerabilities. Databases:

## Databases are crucial for almost all modern applications, and their different types keep increasing in numbers. In the simplest of terms, a database is an organized collection of data that facilitates efficient storage, retrieval, and management of information. **Types of Databases Available Today**

Databases can be categorized into different types depending on their usage, structure, and storage methods.

Databases can be categorized into the following types:

1. Hierarchical databases
2. Relational or SQL databases
3. Non-relational or NoSQL databases
4. Object-oriented databases
5. Network databases.

### Hierarchical Databases: This type structures data using a parent-child relationship. **Examples:**Windows Registry, IBM Information Management System (IMS), Navigation files, Sitemaps, XML, XAML, etc.

### Relational or SQL Databases: In relational databases, data is stored in the form of discrete tables with unique data fields that are identifiable through a primary key. **Examples:**The most popular examples of relational databases include [MySQL](https://www.astera.com/mysql-database-connector/), PostgreSQL, [Microsoft SQL Server](https://www.astera.com/sql-server-connector/), and [Oracle](https://www.astera.com/connect-oracle-database).

### Non-relational or NoSQL Databases: NoSQL databases came to the forefront due to increasingly complex web applications that couldn’t depend on table-based relational models. **Examples: Document databases,** **Column-oriented databases,** **Graph databases,** **Key-value stores.**

### Object-oriented Databases: In an object-oriented database, the system stores information in an object-like manner based on object-oriented programming principles. **Examples:**Some popular examplesinclude**ObjectDB, Db4o, Dbase, Oracle Database,** and [IBM DB2](https://docs.astera.com/projects/centerprise/en/8/connectors/setting-up-ibm-db2iseries-connectivity-in-centerprise.html?_gl=1*1bmt4k7*_gcl_au*MTExMjQxMzU3OC4xNzM2MjMwMzYz).

### Network Databases:

### The database is like a hierarchical database, but it’s different in that it connects the child record with various parent records, allowing two-directional relationships. **Examples:**Integrated Data Store (IDS), EDMS by Xerox, etc.

# ****Overview of Database Security****

# Database security encompasses measures designed to protect the database management system from malicious attacks and unauthorized access. It involves safeguarding the data, the database applications, the database systems, and the associated network infrastructure.

**Common Vulnerabilities in Databases**

Understanding prevalent vulnerabilities is crucial for assessing the security posture of different DBMS options. Common vulnerabilities include:

* **Default, Blank, and Weak Credentials**: Many databases are deployed with default settings, including default usernames and passwords, which attackers can easily exploit.
* **SQL Injection**: This attack involves injecting malicious SQL code into queries, allowing attackers to manipulate the database.
* **Excessive User Privileges**: Granting users more privileges than necessary can lead to unauthorized data exposure or modification.
* **Poorly Managed Sensitive Data**: Inadequate protection of sensitive data can result in data breaches.

***To determine the most secure DBMS with the least number of vulnerabilities, we evaluate several popular systems based on their security features and reported vulnerabilities.***

**PostgreSQL**

PostgreSQL is an open-source relational database known for its robustness and extensibility.

* **Security Features**:
  + **Authentication Methods**: Supports various authentication methods.
  + **Role-Based Access Control**: Offers granular permissions management.
  + **Data Encryption:** PostgreSQL supports encryption for data in transit via SSL/TLS and offers third-party solutions for Transparent Data Encryption (TDE) to secure data at rest.
* **Vulnerabilities**:
  + Historically, PostgreSQL has had a relatively low number of reported vulnerabilities. Regular updates and a proactive security team contribute to its strong security posture.

**Conclusion**  
Based on the evaluation, **PostgreSQL** stands out as a secure DBMS with a relatively low number of reported vulnerabilities. Its robust security features, combined with an active and responsive security team, make it a strong candidate for environments where security is a top priority. PostgreSQL’s security advantages stem from frequent updates, a strong security community, and built-in protections against common database threats, including SQL injection. However, it's essential to note that the security of any database system heavily depends on proper configuration, regular updates, and adherence to security best practices.