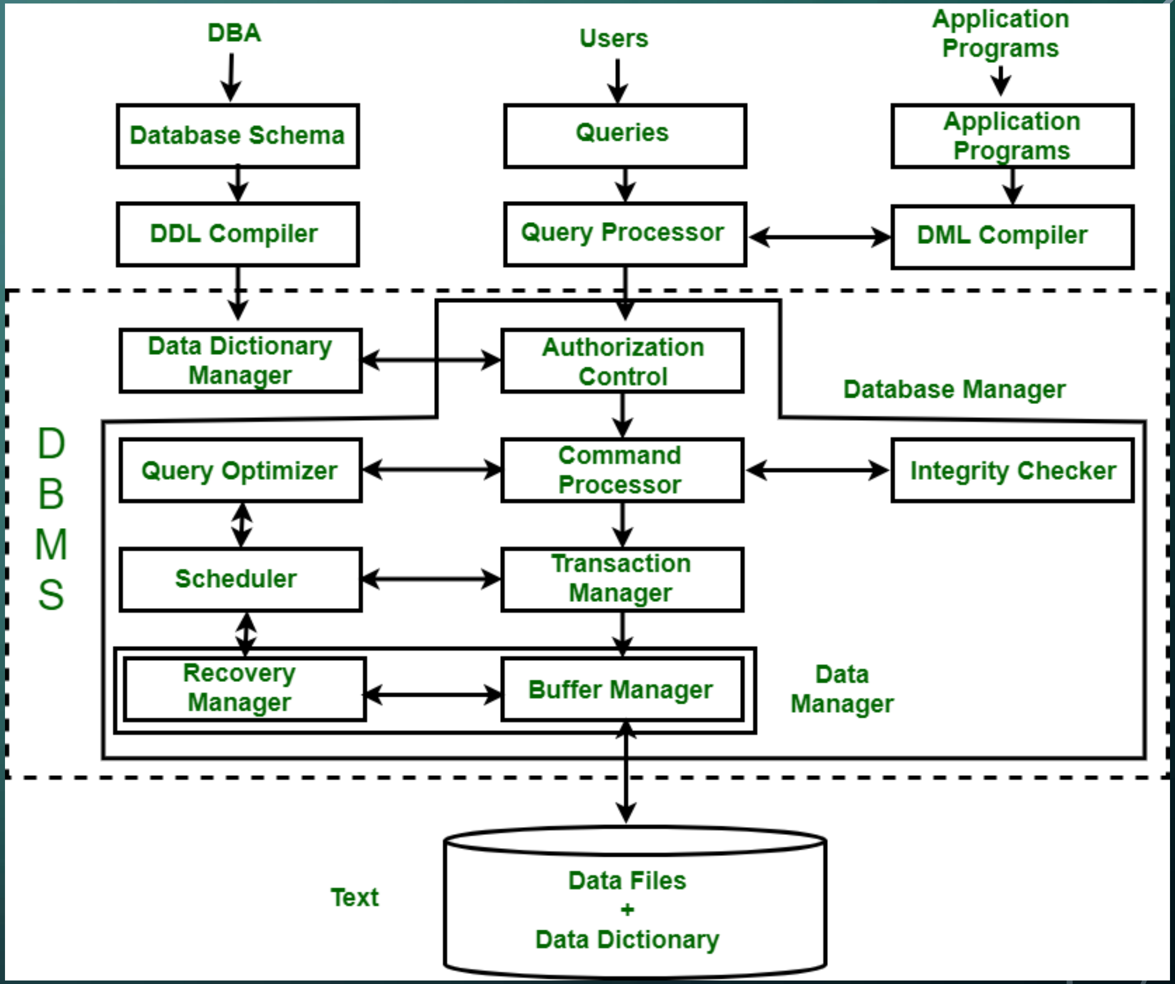
MODULE 4D: AUDITING DATABASES

OBJECTIVES

- Database Auditing
- Operating System Security
- Database Auditing Essentials
- SQL Injection
- Database Vulnerabilities, Integrity

DATABASES

- The term database typically refers to a relational database management system (RDBMS). Database management systems (DBMS) maintain data records and their relationships, or indexes, in tables. Relationships can be created and maintained across and among the data and tables.



https://www.geeksforgeeks.org/structure-of-database-management-system/

DATABASE AUDITING

- Typically, an audit includes a fairly in-depth review of various areas, including the perimeter, the operating system, policies, and so on. If time allows, an audit might cover one or two of the most critical databases.
- Databases are complex beasts requiring patience and technical know-how to audit and secure properly. However, neglecting a database audit is a serious error. Databases are the virtual lockboxes of the information age.

DATABASES

- Databases have some distinct advantages and disadvantages. Because databases are almost always buried deep and far behind the firewall, they are rarely exposed to the types of attacks that your web servers, firewalls, and other systems confront.
- **This is a double edged sword though…**
- Because databases are so far behind the firewall, securing and auditing your databases are often considered afterthoughts, something to be done if you have extra time and maybe just on one or two critical databases. This has led to a situation in which database security typically is left in a shabby condition.

OS SECURITY

- Databases are run on and have some sort of access permissions to their host operating system. So start with the premise that a database which is not properly secured can be used to break into the operating system. Conversely, an unsecured operating system can be used to break into the database. Locking down one but not the other fails to provide proper security to either.

DATABASE AUDITING ESSENTIALS

- Common Database Vendors:
  - Oracle
  - IBM
  - MySQL
  - Microsoft SQL Server

- IT Audit team should have an IT professional, systems admin, or database specialist on hand.

SQL

- Structured Query Language (SQL) is used to access data in a relational database. Technically, SQL should be pronounced as three separate letters “S-Q-L,” but the pronunciation “sequel” has become so commonplace it is also accepted as correct. SQL is a set-based language, meaning that it works on a set of data at a time.

- SQL statements are used to pull data from the database. SQL is built around four core statements:
- • **SELECT** View a subset of data from a table
- • **INSERT** Add new data to a table
- • **UPDATE** Modify existing data in a table
- • **DELETE** Remove a subset of data from a table

SQL STATEMENTS

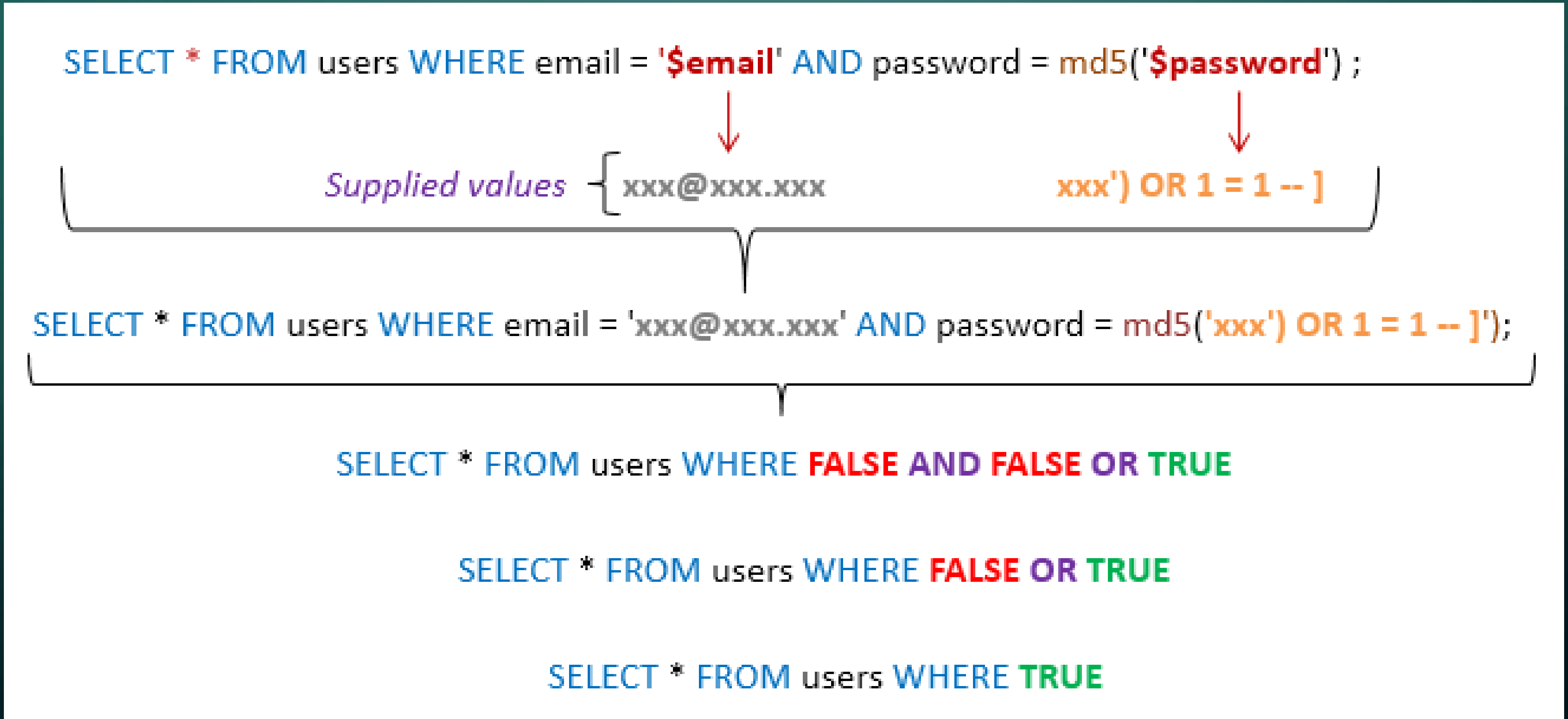
```
SELECT <COLUMN LIST> FROM <TABLE
NAME> WHERE <CONDITION>

SELECT FIRST_NAME, LAST_NAME FROM
EMPLOYEES WHERE SALARY > 2000
```

- SQL Injection

SQL INJECTION

https://www.hacksplaining.com/exercises/sql-injection



```
SELECT * FROM users WHERE email = '$email' AND password = md5('$password') ;
```

Supplied values { xxx@xxx.xxx   xxx') OR 1 = 1 --]

```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx') OR 1 = 1 -- ]');
```

```
SELECT * FROM users WHERE FALSE AND FALSE OR TRUE
```

```
SELECT * FROM users WHERE FALSE OR TRUE
```

```
SELECT * FROM users WHERE TRUE
```

DATABASE INTEGRITY

- Integrity is probably one of the most important concepts when auditing a database.
  Integrity is part of our Cybersecurity CIA triad. Integrity deals with maintain the accuracy and completeness of data.
- It’s highly important that there are integrity controls in place to provide some level of assurance that the data in our databases is not changed maliciously or incidentally.

DATABASE AUDITING

- What are we looking for?
  - What database integrity controls are in place?
  - Access Permissions – Who has access to the database? How is that access granted?
  - Security of the underlying OS & DBMS platform
  - Are sensitive databases encrypted in transit and at rest?
  - Network connections – What ports are open for the database to communicate? How is the DBMS and databases positioned within the network?
  - Database Updating/Patching – Is the database update to date patch-wise?
  - Patch Management – How are patches applied
  - Backup systems – Is there a robust backup system in place for databases