

ONE PAGE SUMMARY

IT & Software > SQL > SQL Security

Introduction to SQL Security

Secure your SQL databases to protect sensitive data.

DEFINITION

SQL Security involves measures to protect databases from unauthorized access and threats. It ensures data integrity, confidentiality, and availability.

KEY CONCEPTS

Authentication

The process of verifying the identity of a user or system accessing the database.

Authorization

Determining what an authenticated user is allowed to do within the database.

Encryption

Transforming data into a secure format to prevent unauthorized access during storage or transmission.

SQL Injection

A common attack where malicious SQL code is inserted into queries to manipulate the database.

Access Control

Policies and mechanisms that restrict access to database resources based on user roles.

EXAMPLES

- Using strong passwords for database accounts.
- Implementing role-based access control for users.
- Encrypting sensitive data like credit card numbers.

MEMORY TIPS

- ★ Remember 'AAA' for Authentication, Authorization, and Access Control.
- ★ Think of 'E' for Encryption as 'Encrypting everything'.
- ★ Use 'SQLI' to recall SQL Injection as a security threat.

COMMON MISTAKES

- ✗ Neglecting to update database security patches.
- ✗ Using default credentials for database accounts.
- ✗ Failing to implement least privilege access.

QUICK RECAP

SQL Security is essential for protecting databases from unauthorized access and threats. Key components include authentication, authorization, and encryption. Always be aware of common vulnerabilities like SQL injection.