

Introduction to Database Security

Introduction to Database Security

Key concepts, threats, and best-practice controls

1. Why Database Security Matters

Reason	Impact
Confidentiality	Prevent unauthorized access to sensitive data (personal, financial, health).
Integrity	Ensure data is accurate, complete, and unaltered.
Availability	Keep data accessible for legitimate users and applications.
Compliance	Meet legal/regulatory requirements (GDPR, HIPAA, PCI-DSS, etc.).
Business Reputation	Avoid costly breaches, loss of customer trust, and legal penalties.

2. Core Security Principles (the “CIA” Triad)

Principle	Goal	Typical Controls
Confidentiality	Only authorized subjects can view data.	Authentication, access control, encryption, masking.
Integrity	Data remains trustworthy and unmodified.	Checksums, digital signatures, audit trails, constraints.
Availability	Data is reachable when needed.	Redundancy, backup & recovery, DDoS mitigation, patch management.

3. Common Threats & Attack Vectors

Threat	Description	Example
SQL Injection	Malicious code inserted into SQL statements.	<code>SELECT * FROM users WHERE name= ' ' OR 1=1-- ' ;</code>
Privilege Escalation	Users gain higher rights than intended.	Exploiting mis-configured roles or stored procedures.

Introduction to Database Security

Threat	Description	Example
Insider Abuse	Authorized users misuse access.	Exporting customer tables to external media.
Brute?Force Authentication	Repeated login attempts to guess credentials.	Automated password spraying.
Backup Theft	Unencrypted backups stolen from storage.	Lost external hard drive containing full dump.
Ransomware	Encryption of database files, demanding payment.	Malware encrypts data files on the DB server.
Misconfiguration	Weak default settings, open ports, excessive privileges.	Default “admin” account left enabled.

4. Security Controls by Layer

4.1. Network & Perimeter

- **Firewalls** – Restrict inbound/outbound traffic to required ports (e.g., 1433 for MSSQL, 5432 for PostgreSQL).
- **VPN / TLS** – Secure remote connections; enforce TLS?1.2+ for client?server traffic.
- **Network Segmentation** – Isolate database servers in a DMZ or dedicated VLAN.

4.2. Host & OS Hardening

- **Patch Management** – Apply OS and DBMS security updates promptly.
- **Least?Privilege Services** – Run DB engine under a non?admin service account.
- **File?System Permissions** – Restrict read/write rights on data, log, and backup directories.

4.3. Database Engine Controls

Control	Purpose	Typical Implementation
Authentication	Verify identity of users/applications.	Local accounts, LDAP/Active Directory, Kerberos, MFA.
Authorization / RBAC	Grant only needed privileges.	Roles, schemas, column?level permissions.

Introduction to Database Security

Control	Purpose	Typical Implementation
Encryption	Protect data at rest & in transit.	Transparent Data Encryption (TDE), column? level encryption, TLS/SSL.
Auditing & Logging	Record who did what, when.	DB?native audit trails, syslog integration, immutable log