Securing Databases: Practical Database Security Skills for Safer Systems (TT8700) Training

Duration: **2 Day**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Overview

As organizations become increasingly dependent on data-driven operations, securing database environments has become a critical business requirement. Threats such as unauthorized access, ransomware, data breaches, and application-based attacks can significantly impact business continuity and regulatory compliance.

This practical course provides database professionals, developers, technical leaders, and stakeholders with the knowledge and skills required to identify vulnerabilities, reduce risk, and strengthen database security controls.

Through expert-led demonstrations and hands-on exercises, participants learn how to assess threats, protect sensitive information, and implement security best practices across database environments.

Prerequisites

Participants should be comfortable with:

- Basic database concepts
- Reading or writing simple SQL queries
- Understanding how applications interact with databases
- General IT and networking fundamentals

Programming experience is not required.

Who Should Attend

This course is ideal for:

- Database Administrators (DBAs)
- Software Developers
- Technical Team Leaders
- Systems and Infrastructure Professionals
- Information Security Specialists
- Risk and Compliance Teams
- Data Protection Stakeholders
- Professionals seeking foundational database security skills

Securing Databases: Practical Database Security Skills for Safer Systems (TT8700) Training

Duration: **2 Day**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

What You Will Learn

By the end of this course, participants will be able to:

- Identify common database security risks
- Assess vulnerabilities using safe and ethical techniques
- Apply core information security principles to database environments
- Protect data both at rest and in transit
- Recognize and mitigate SQL injection and related attacks
- Implement effective access control and privilege management
- Build layered security strategies
- Support compliance and governance requirements
- Improve readiness for security incidents and threats

Outline

Module 1: Foundations of Vulnerability Discovery

Topics Covered

- Why vulnerability discovery matters
- Ethical security testing practices
- Responsible assessment methodologies
- Risk-based security thinking

Module 2: Information Security Fundamentals

Topics Covered

- Confidentiality, Integrity, and Availability (CIA)
- Threats and risk management
- Security controls
- Defense-in-depth strategies

Module 3: Understanding Database Environments

Topics Covered

- Database identification and fingerprinting
- Architecture analysis
- Data flow mapping
- Data validation concepts

Module 4: Database Security Fundamentals

Protecting Data

- Data-at-rest security
- Data-in-transit protection
- Encryption strategies

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Asset Management

- Identifying critical assets
- Asset inventory processes
- Data classification techniques

Privilege Management

- Role-based access control
- Principle of least privilege
- Permission auditing

Boundary Defenses

- Network segmentation
- Security zones
- Access boundaries

Service Continuity

- Business continuity planning
- Disaster recovery considerations
- Service resilience strategies

Module 5: Database Vulnerabilities and Threats

Injection Attacks

- Understanding SQL Injection
- Risk identification
- Mitigation strategies

Authentication and Access Control

- Strong authentication methods
- Authorization weaknesses
- Account security best practices

Data Breaches

- Common causes of data exposure
- Misconfiguration risks
- Data protection strategies

Malware and Ransomware

- Database-focused threats
- Detection and prevention techniques
- Incident response considerations

Insider Threats

- Privileged user risks

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- Misuse of access rights
- Monitoring and auditing practices

Insecure Data Handling

- Sensitive data protection
- Secure data lifecycle management

Third-Party Security Risks

- Vendor security concerns
- External integrations
- Supply chain risk management

Compliance and Governance

- Security standards
- Regulatory requirements
- Compliance considerations

Module 6: Cryptography Essentials

Topics Covered

- Encryption fundamentals
- Key management principles
- Protecting sensitive information
- Secure data exchange practices

Important Note

Databases are rarely attacked in isolation. In many cases, attackers exploit weaknesses in applications that connect to the database. To demonstrate how these attacks occur in real-world environments, the course uses a simple ASP.NET web application as an example platform.

No C# development experience is required. Participants only need a basic understanding of how web applications and database systems interact.