Database Basics and Security

Provider: IBM (Coursera, part of the Cybersecurity Analyst Professional Certificate)
Completion Date: April 17, 2025

Overview

This course introduced the fundamentals of databases and their vulnerabilities, combining core management concepts with security practices. It covered relational and non-relational databases, SQL basics, user management, data protection techniques, and injection vulnerabilities. Hands-on labs provided experience with SQL queries, database administration, and securing systems against common threats.

Key Topics Covered

- Database fundamentals: relational vs. non-relational models, ER diagrams, primary and foreign keys
- SQL operations: SELECT, INSERT, UPDATE, DELETE, COUNT, DISTINCT, LIMIT
- Database management: backups, roles, and permissions
- Data protection: encryption, hashing, masking, tokenization, segmentation
- User management: profiles, password policies, roles, privileges
- Security models: auditing, monitoring, and access control
- Injection vulnerabilities: OS command injection, SQL injection, and prevention methods

Practical Applications

- Querying and modifying databases with SQL
- Designing and managing relational and NoSQL databases
- Securing sensitive information with encryption and access controls
- Implementing auditing models for accountability
- Identifying and mitigating injection vulnerabilities through labs and projects

Personal Reflection

This course gave me a strong foundation in database security by combining theory with practical labs. I learned to query, manage, and protect databases while recognizing and mitigating injection risks. These skills are directly applicable to my focus in cybersecurity, where safeguarding data and ensuring compliance are critical.