Securing Databases | Database Security

Duration: *2 Day(s)*

Course Overview

From ransomware and constant data breaches to state-sponsored attacks, we are under constant and increasing pressure. Retailers, financial institutions, government agencies, high-tech companies, and many others are paying the price for poor application security - financial losses and eroding trust. The developer community must take ownership of these problems and change our perspective of defensive measures and how we design, development, and maintain software applications.

Securing Databases is an essential training course for DBAs and developers who need to produce secure database applications and manage secure databases. Data, databases, and related resources are at the heart of most IT infrastructures. These assets can have high value from a business, regulatory, and liability perspective, and must be protected accordingly. This course showcases demonstrations on how to repeatedly attack and then defend various assets associated with a fully functional database. This approach illustrates the mechanics of how to secure databases in the most practical of terms.

This course introduces the most common security vulnerabilities faced by databases today. Throughout the course, you'll examine each vulnerability from a database perspective through a process of describing the threat and attack mechanisms, recognizing associated vulnerabilities, and then designing, implementing, and testing effective defenses. Multiple practical demonstrations reinforce these concepts with real vulnerabilities and attacks. You'll also learn how to design and implement the layered defenses needed to defend your own databases.

You'll exit this course with the skills required to recognize actual and potential database vulnerabilities, implement defenses for those vulnerabilities, and test those defenses for sufficiency.

Review this course online at https://www.alta3.com/courses/TT8700

Objectives

- Recognize and analyze database vulnerabilities.
- Implement layered defenses and test their effectiveness.
- Design secure database applications with robust authentication.
- Leverage threat modeling and encryption as defense mechanisms.

Who Should Attend

- DBAs
- System Administrators
- Developers
- Enterprise Team Members

Prerequisites

Ideally, students should have approximately 6 months to a year of database working knowledge.

Course Outline

Session: Foundation for Securing Databases

1. Lesson: Why Hunt Bugs?
    - The Language of Cybersecurity

- The Changing Cybersecurity Landscape
- AppSec Dissection of SolarWinds
- The Human Perimeter
- Interpreting the 2021 Verizon Data Breach Investigation Report
- First Axiom in Web Application Security Analysis
- First Axiom in Addressing ALL Security Concerns

2. Lesson: Fingerprinting Databases
   - Fingerprinting Infrastructures and Databases
   - Finding the Databases
   - Scanning Databases for Vulnerabilities
   - Scanning Applications and Operating Systems

3. Lesson: Principles of Information Security
   - Security Is a Lifecycle Issue
   - Minimize Attack Surface Area
   - Layers of Defense: Tenacious D
   - Compartmentalize
   - Consider All Application States
   - Do NOT Trust the Untrusted
   - AppSec Dissection of the Verkada Exploit

Session: Database Security Vulnerabilities

4. Lesson: Database Security Concerns
   - Data at Rest and in Motion
   - Privilege management
   - Boundary Defenses
   - Continuity of Service
   - Trusted Recovery
5. Lesson: Common Vulnerabilities and Databases
   - Unvalidated Input
   - Elevation of Privileges
   - Identifying Protection Needs
   - Evolving Privacy Considerations
   - Options for Protecting Data
   - Transport/Message Level Security
   - SQL Injection Flaws
   - Drill Down on Stored Procedures
   - Quality and Protection of Authentication Data
   - Proper hashing of passwords
   - Handling Passwords on Server Side
   - Managing Updates: Balancing Risk and Timeliness
   - Detecting Threats and Active Attacks
   - Best Practices for Determining What to Log
   - Safe Logging in Support of Forensics
   - System Hardening

- Risks with Internet-Connected Resources (Servers to Cloud)
- Segmentation with Containers and Cloud

6. Lesson: Database Security
    - Design and Configuration
    - Identification and Authentication
    - Computing Environment
    - Database Auditing
    - Boundary Defenses
    - Continuity of Service
    - Vulnerability and Incident Management

Session: Moving Forward with Database Security

7. Lesson: Databases: What Next?
    - Common Vulnerabilities and Exposures
    - Strength Training: Project Teams/Developers
    - Strength Training: IT Organizations

Session: Secure Development Lifecycle (SDL)

8. Lesson: SDL Overview
    - Attack Phases: Offensive Actions and Defensive Controls
    - Secure Software Development Processes
    - Shifting Left
    - Actionable Items Moving Forward
9. Lesson: SDL In Action
    - Risk Escalators
    - Risk Escalator Mitigation
    - SDL Phases
    - Actions for each SDL Phase
    - SDL Best Practices

Session: Taking Action Now for Securing Databases

10. Lesson: Database Asset Analysis
    - Targets: Data/Entity Assets
    - Targets: Functional/Service Assets
    - Classifying Based on Value and Risk Escalation
    - Asset Inventory and Analysis
11. Lesson: Making Application Security Real
    - Cost of Continually Reinventing
    - Leveraging Common AppSec Practices and Control
    - Paralysis by Analysis
    - Actional Application Security

- Additional Tools for the Toolbox

Bonus Topics: Time Permitting

12. Lesson: Cryptography Overview
    - Strong Encryption
    - Message Digests
    - Encryption/Decryption
    - Keys and Key Management
    - NIST Recommendations