skillsoft global knowledge™

SECURING DATABASES (TT8700)

Course Code: 1140

According to research by the National Institute of Standards, 92% of all security vulnerabilities are now considered application vulnerabilities and not network vulnerabilities.

Securing Databases is an intense database security training workshop/seminar essential for DBAs and developers who need to produce secure database applications and manage secure databases. In addition to teaching basic skills, this course digs deep into sound processes and practices that apply to the entire software development lifecycle. Perhaps just as significantly, you will learn about current, real examples that illustrate the potential consequences of not following these best practices.

This course quickly introduces you to the most common security vulnerabilities faced by databases today. You will examine each vulnerability from a database perspective through a process of describing the threat and attack mechanisms, recognizing associated vulnerabilities, and, finally, designing, implementing, and testing effective defenses. Multiple practical demonstrations reinforce these concepts with real vulnerabilities and attacks. You will then be challenged to design and implement the layered defenses you will need in defending your own databases. You will leave the course armed with the skills required to recognize actual and potential database vulnerabilities, implement defenses for those vulnerabilities, and test those defenses for sufficiency.

Security experts agree that the least effective approach to security is "penetrate and patch". It is far more effective to "bake" security into an application throughout its lifecycle. After trying to defend a poorly designed (from a security perspective) database application, you will be ready to build and secure your databases and applications starting at project inception. The final portion of this course builds on the previously learned mechanics for building defenses by exploring how design and analysis can be used to build stronger applications from the beginning of the software lifecycle.

A key component to our ***Best Defense IT Security Training Series***, this workshop is a companion course with several developer-oriented courses and seminars, and it may be customized to suit your team's unique objectives.

What You'll Learn

- Consequences for not properly handling untrusted data such as denial of service, cross-site scripting, and injections
- Test databases with various attack techniques to determine the existence of and effectiveness of layered defenses
- Prevent and defend the many potential vulnerabilities associated with untrusted data
- Concepts and terminology behind supporting, designing, and deploying secure databases
- Problems associated with data security and the potential risks associated with those problems
- Best practices for supporting the many security needs of databases.
- Vulnerabilities associated with authentication and authorization within the context of databases and database applications
- Detect, attack, and implement defenses for authentication and authorization functionality
- Dangers and mechanisms behind Cross-Site Scripting (XSS) and Injection attacks
- Detect, attack, and implement defenses against XSS and Injection attacks
- Concepts and terminology behind defensive, secure coding
- Using Threat Modeling as a tool in identifying software vulnerabilities based on realistic threats against meaningful assets
- Perform both static reviews and dynamic database testing to uncover vulnerabilities
- Design and develop strong, robust authentication and authorization implementations
- Fundamentals of Digital Signatures as well as how they can be used as part of the defensive infrastructure for data
- Fundamentals of Encryption as well as how it can be used as part of the defensive infrastructure for data

Who Needs to Attend

This intermediate-level database course is designed for those who wish to get up and running on developing well-defended database applications.

SECURING DATABASES (TT8700)

Course Code: 1140

VIRTUAL CLASSROOM LIVE	$1,895 USD	2 Day

Virtual Classroom Live Outline

1. Foundation

- Misconceptions
  - Thriving Industry of Identify Theft
  - Dishonor Roll of Data Breaches
  - TJX: Anatomy of a Disaster
  - Heartland: What? Again?
- Security Concepts
  - Terminology and Players
  - Assets, Threats, and Attacks
  - OWASP
  - CWE/SANS Top 25 Programming Errors
  - Categories
  - What They Mean to Your Services
- Defensive Coding Principles
  - Security Is a Lifecycle Issue
  - Minimize Attack Surface
  - Manage Resources
  - Application States
  - Compartmentalize
  - Defense in Depth Layered Defense
  - Consider All Application States
  - Not Trusting the Untrusted
  - Security Defect Mitigation
  - Leverage Experience
- Reality
  - Recent, Relevant Incidents
  - Find Security Defects in Web Application

2. Top Database Security Vulnerabilities

- Security Concerns Common to all DBMSs
  - Authentication
  - Authorization
  - Confidentiality
  - Integrity
  - Auditing
  - Replication, Federation, and Clustering
  - Backup and Recovery
  - OS, Application, and Network Components
- Unvalidated Input
  - Sources of Untrusted Input
  - Trust Boundaries
  - Designing and Implementing Defenses
- Broken Authentication
  - Quality of Passwords
  - Protection of Passwords
  - Hashing Passwords
  - Protecting Authentication Assets
  - System Account Managemen
  - User Account Management
- Broken Access Control
  - Gaining Elevated Privileges
  - Compartmentalization Based on Level of Privilege
  - Special Privileges Provided by Database and Systems
  - Protecting Special Roles
- Cross-Site Scripting (XSS/CSRF) Flaws
  - What and How
  - Role of Databases in Enabling XSS
  - Designing and Implementing Defenses
- Injection Flaws
  - What and How
  - SQL, PL/SQL, XML, and Others
  - Stored Procedures
  - Buffer Overflows
  - Designing and Implementing Defenses
- Error Handling and Information Leakage
  - What and How
  - Four Dimensions of Error Response
  - Proper Error Handling Design
- Insecure Handling
  - Data at Rest
  - Data in Motion
  - Encryption
  - Compartmentalization Based on Level of Privileg
  - Backups and Archives

        - Connection Strings and High Value Server-Side Credentials
        - Designing and Implementing Defenses
    - Insecure Management of Configuration
        - Initial Installation
        - Patch Management
        - Server Hardening
        - Operating System Hardening
        - Connection Hardening
        - Replication Hardening
        - Best Practices
    - Direct Object Access
        - What and How
        - Role of Databases in Enabling Access
        - High Risk Practices to Avoid

3. Database Security
    - Identification and Authentication
        - Group and Individual
        - Key Management Practices
        - Token and Certificates Practices
    - Computing Environment
        - Data Changes and Controls
        - Encryption
        - Privilege Management
        - Additional Controls and Practices
    - Database Auditing
        - Auditing Mechanics and Best Practices
        - Tracking Changes to Code
        - Tracking Changes to Permissions
        - Extending Auditing
    - Boundary Defenses
    - Continuity of Service
        - Defending Backup/Restoration Assets
        - Data and Software Backups
        - Trusted Recovery
    - Vulnerability and Incident Management
4. Cryptography Overview
    - Cryptography defined
    - Strong Encryption
    - Ciphers and algorithms
    - Message digests
    - Types of keys
    - Key management
    - Certificate management
    - Encryption/Decryption

5. Secure Software Development (SSD)
    - SSD Process Overview
        - CLASP Defined
        - CLASP Applied
    - Asset, Boundary, and Vulnerability Identification
    - Vulnerability Response
    - Design and Code Reviews
    - Applying Processes and Practices
    - Risk Analysis
6. Security Testing
    - Testing as Lifecycle Process
    - Testing Planning and Documentation
    - Testing Tools And Processes
        - Principles
        - Reviews
        - Testing
        - Tools
    - Static and Dynamic Analysis
    - Testing Practices
        - Authentication Testing
        - Data Validation Testing
        - Denial Of Service Testing
7. Generic Database Measures
    - Overview, Conventions, and Best Practices
    - Generic Database Checks and Procedures
    - Applying the Measures

Apr 23 - 24, 2025 | 10:00 AM - 6:00 PM EST

Jun 18 - 19, 2025 | 10:00 AM - 6:00 PM EDT

Aug 20 - 21, 2025 | 10:00 AM - 6:00 PM EST

Oct 22 - 23, 2025 | 10:00 AM - 6:00 PM EST

Dec 3 - 4, 2025 | 10:00 AM - 6:00 PM EST

SECURING DATABASES (TT8700)

Course Code: 1140

PRIVATE GROUP TRAINING	2 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 4/7/2025 11:57:55 PM