Securing Databases | Database Security - TT8700

Securing Databases is an essential training course for DBAs and developers who need to produce secure database applications and manage secure databases.

What You'll Learn

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, develop and maintain software applications.
PCI Compliant Developer Training: This secure coding training addresses common coding vulnerabilities in software development processes. This training is used by one of the principal participants in the PCI DSS. Having passed multiple PCI audits, this course has been shown to meet the PCI requirements. The specifications of those training requirements are detailed in 6.5.1 through 6.5.7 on pages 60 through 65 of the PCI DSS Requirements 3.2.1 document.
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 will 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.

Objectives

Throughout the course, you will learn to:

- Establish the first axiom in security analysis of ALL web applications for this course and beyond
- Establish the first axiom in addressing ALL security concerns for this course and beyond
- Understand the 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
- Understand the concepts and terminology behind supporting, designing, and deploying secure databases
- Appreciate the magnitude of the problems associated with data security and the potential risks associated with those problems
- Understand the currently accepted best practices for supporting the many security needs of databases
- Understand the vulnerabilities associated with authentication and authorization within the context of databases and database applications
- Detect, attack, and implement defenses for authentication and authorization functionality
- Understand the dangers and mechanisms behind Injection attacks
- Detect, attack, and implement defenses against Injection attacks
- Understand the concepts and terminology behind defensive, secure database configuration and operation
- Perform both static reviews and dynamic database testing to uncover vulnerabilities
- Design and develop strong, robust authentication and authorization implementations
- Understand the fundamentals of Encryption as well as how it can be used as part of the defensive infrastructure for data

Audience

This is an introduction to database security course for **intermediate skilled team members.** Attendees might include DBAs, system administrators, developers and other

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

Pre-Requisites

{{code}} {{title}}

Agenda

Please note that this list of topics is based on our standard course offering, evolved from typical industry uses and trends. We will work with you to tune this course and level of coverage to target the skills you need most. Course agenda, topics and labs are subject to adjust during live delivery in response to student skill level, interests and participation.

Session: Foundation for Securing Databases

Lesson: Why Hunt Bugs?

- The Language of Cybersecurity
- The Changing Cybersecurity Landscape
- AppSec Dissection of SolarWinds
- The Human Perimeter
- First Axiom in Web Application Security Analysis
- First Axiom in Addressing ALL Security Concerns
- Lab: Case Study in Failure

Lesson: Safe and Appropriate Bug Hunting/Hacking

- Warning to All Bug Hunters
- Working Ethically
- Respecting Privacy
- Bug/Defect Notification
- Bug Hunting Pitfalls

Lesson: Fingerprinting Databases

- Fingerprinting Infrastructures and Databases
- Finding the Databases
- Scanning Databases for Vulnerabilities
- Scanning Applications and Operating Systems

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

Lesson: Database Security Concerns

- Data at Rest and in Motion
- Privilege management
- Boundary Defenses
- Continuity of Service
- Trusted Recovery

Lesson: Vulnerabilities and Databases

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures

Lesson: Database Security

- Design and Configuration
- Identification and Authentication
- Computing Environment
- Database Auditing
- Boundary Defenses
- Continuity of Service
- Vulnerability and Incident Management
- Lab: Database Analysis

Session: Moving Forward with Database Security

Lesson: Databases: What Next?

- Open Web Application Security Project (OWASP)
- OWASP Top Ten Overview
- Web Application Security Consortium
- CERT Secure Coding Standards
- Bug Hunting Mistakes to Avoid
- Tools and Resources
- Lab: Recent Incidents

Session: Secure Development Lifecycle (SDL)

Lesson: SDL Overview

- Attack Phases: Offensive Actions and Defensive Controls
- Secure Software Development Processes
- Shifting Left
- Actionable Items Moving Forward

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

Lesson: Database Asset Analysis

- Targets: Data/Entity Assets
- Targets: Functional/Service Assets
- Classifying Based on Value and Risk Escalation
- Asset Inventory and Analysis

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

Additional Topics: Time Permitting

These topics will be included in your course materials but may or may not be presented during the live class depending on the pace of the course and attendee skill level and participation.

Lesson: Cryptography Overview

- Strong Encryption
- Message Digests
- Encryption/Decryption
- Keys and Key Management
- NIST Recommendations

Follow On Courses

{{code}}	{{title}}

Related Courses

TT8800	Information Assurance (STIG) Overview
TTAI2810	Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp
TTAI2820	Mastering AI Security Boot Camp
TTAI2832	Applying AI to the 2021 OWASP Top Ten
TTAI2835	AI Secure Programming for Web Applications / Technical Overview
TTPS4894	Python Security | Introduction to Python Programming for Security Analysts & Professionals
TT8700	Securing Databases | Database Security
TT8120	Securing Web Applications | 2021 OWASP Top Ten and Beyond
TT8320-J	Java Secure Coding Camp | Attacking and Securing Java Web Applications
TT8320-N	.Net Secure Coding Camp | Attacking and Securing C# / ASP.Net (Core) Web Applications

Attend a Course

Please feel free to Register Online or call 844-475-4559 toll free to connect with our Registrar for assistance. If you ever need additional date options, please contact us for scheduling.