Securing Databases | Database Security (TT8700)

Category: Software Development & Programming | **Vendor:** Trivera Tech

Duration: 16.00 hours (2 days) **13.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

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.®

About This Course

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.

Who Should Attend

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.

Prerequisites & Entry Requirements

General Prerequisites:

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.

Learning Outcomes

Upon successful completion of this course, participants will be able to:

Throughout the course, you will learn to:

- Understand the consequences for not properly handling untrusted data such as denial of service, cross-site scripting, and injections
- 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
- 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
- Understand the concepts and terminology behind defensive, secure database configuration and operation
- Understand the use of 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
- Understand the fundamentals of Digital Signatures as well as how it can be used as part of the defensive infrastructure for data
- Understand the fundamentals of Encryption as well as how it can be used as part of the defensive infrastructure for data
- Identify resources to use for ongoing threat intelligence
- Plan next steps after completion of this training

Detailed Course Outline

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

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: 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

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

Lesson: Databases: What Next

Common Vulnerabilities and Exposures

Strength Training: Project Teams/Developers

Strength Training: IT Organizations

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

Bonus Topics: Time Permitting

Lesson: Cryptography Overview

Strong Encryption

Message Digests

Encryption/Decryption

Keys and Key Management

NIST Recommendations

Additional Course Details

Nexus Humans Securing Databases | Database Security (TT8700) training program is a workshop that presents an invigorating mix of sessions, lessons, and masterclasses meticulously crafted to propel your learning expedition forward.

This immersive bootcamp-style experience boasts interactive lectures, hands-on labs, and collaborative hackathons, all strategically designed to fortify fundamental concepts.

Guided by seasoned coaches, each session offers priceless insights and practical skills crucial for honing your expertise. Whether you're stepping into the realm of professional skills or a seasoned professional, this comprehensive course ensures you're equipped with the knowledge and prowess necessary for success.

While we feel this is the best course for the Securing Databases | Database Security (TT8700) course and one of our Top 10 we encourage you to read the course outline to make sure it is the right content for you.

Additionally, private sessions, closed classes or dedicated events are available both live online and at our training centres in Dublin and London, as well as at your offices anywhere in the UK, Ireland or across EMEA.

Frequently Asked Questions

Q: What delivery options are available for Securing Databases | Database Security (TT8700)?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 2-day Securing Databases | Database Security (TT8700) course provides up to 13.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Securing Databases | Database Security (TT8700) training?

The training takes place over 2 day(s), with each day lasting approximately 16.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Securing Databases | Database Security (TT8700)?

Yes, we provide corporate training, dedicated training, and closed classes for Securing Databases | Database Security (TT8700). Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Databases; Security

Q: Why choose Nexus Human for Securing Databases | Database Security (TT8700)?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Securing Databases | Database Security (TT8700) training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)

© 2026 Nexus Human. All rights reserved. This brochure was generated on 13/11/2026.