Securing Databases | Database Security (TT8700)

Modality: Virtual Classroom

Duration: 2 Days

About this course:

Securing Databases is an extreme training workshop/seminar of database security required for developers and DBAs who need to create secure database applications and oversee secure databases. Notwithstanding showing essential abilities, this course delves profoundly into sound practices and procedures that apply to the whole lifecycle of software advancement. Maybe similarly as fundamentally, understudies find out about current, genuine models that delineate the potential outcomes of not following these great procedures.

Information, databases and related assets are at the core of most IT frameworks. These advantages can have a high incentive from a regulatory, business, and obligation point of view. They should to secured as needs are. In this course, over and over assault and afterward guard different resources related to a completely useful database. This methodology shows the mechanics of how to protect databases in the most functional of terms.

Security specialists concur that the least viable way to deal with security is "infiltrate and fix". Subsequent to investing critical energy attempting to safeguard an ineffectively structured (from a security point of view) application of database, understudies are prepared to figure out how to secure their applications and databases beginning at project origin. The last bit of this course expands on the recently learned mechanics for building protections by investigating how analysis and plan can be utilized to construct more grounded applications from the starting point of the product lifecycle.

The normal compensation of a Data Security Analyst is $64,652 every year.

Course Objective:

Working in an environment of dynamic learning, participants will figure out how to:

- Defend and prevent numerous potential vulnerabilities related to untrusted information
- Test databases with different techniques of assault to decide the presence of and adequacy of layered barriers
- Comprehend the terminology and concepts behind designing, supporting, and deploying secure databases.
- Familiar with the consequences for not appropriately dealing with untrusted information, for example, cross-site scripting, denial of service, and injections.
- Comprehend the presently acknowledged best procedures for supporting the numerous security needs of databases.
- Escalate the size of the issues related to information security and the potential dangers related to those issues
- Recognize, assault, and implement resistances for the functionality of authorization and authentication.

- Comprehend the vulnerabilities related to authorization and authentication inside the context of databases and applications of database
- Recognize, assault, and actualize resistances against XSS and Injection assaults
- Comprehend the risks and components behind Injection attacks and Cross-Site Scripting (XSS).
- Comprehend the utilization of Threat Modeling as an instrument in recognizing programming vulnerabilities dependent on sensible dangers against important resources
- Familiar with the terminology and concepts behind protective, secure, coding.
- Structure and create solid, hearty authorization and authentication and executions
- Perform both dynamic database testing and static audits to reveal vulnerabilities
- Comprehend the basics of Encryption and as to how it may be utilized as a major aspect of the guarded foundation for information
- Understand the basics of Digital Signatures and also how it may be utilized as a major aspect of the guarded foundation for information

Audience:

This is a database course for intermediate -level, intended for the individuals who wish to find a workable pace on growing very much guarded database applications. This course might be tweaked to suit your group's interesting destinations.

Prerequisite:

Real-world experience is highly recommended and Familiarity with databases is required. Preferably, students should have around a half year of working knowledge of the database.

Course Outline:

Module 1: Foundation

Lesson: Who is Safe?

- Assumptions We Make
- Security: The Complete Picture
- Anthem, Sony, Target, Heartland, and TJX Debriefs
- Verizon’s 2017 Data Breach Report
- Attack Patterns and Recommendations

Lesson: Security Concepts

- Motivations: Costs and Standards
- Open Web Application Security Project
- Web Application Security Consortium
- CERT Secure Coding Standards
- Microsoft SDL
- Assets and Trust Boundaries
- Threat Modeling

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

Module 2: Database Security Vulnerabilities

Lesson: Database Security Concerns

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

Lesson: Vulnerabilities

- Unvalidated Input
- Broken Authentication
- Cross Site Scripting (XSS/CSRF)
- Injection Flaws
- Error Handling, Logging, and Information Leakage
- Insecure Storage
- Direct Object Access
- XML Vulnerabilities
- Web Services Vulnerabilities
- Ajax Vulnerabilities

Lesson: Cryptography Overview

- Strong Encryption
- Message digests
- Keys and key management
- Certificate management
- Encryption/Decryption

Lesson: Database Security

- Design and Configuration
- Identification and Authentication
- Computing Environment
- Database Auditing
- Boundary Defenses

- Continuity of Service
- Vulnerability and Incident Management

Lesson: Understanding What's Important

- Common Vulnerabilities and Exposures
- OWASP 2017 Top Ten
- CWE/SANS Top 25 Most Dangerous SW Errors
- Monster Mitigations
- Strength Training: Project Teams/Developers
- Strength Training: IT Organizations

Module 3: Secure Development Lifecycle (SDL)

Lesson: SDL Process Overview

- Types of Security Controls
- Phases of Typical Data-Oriented Attack
- Phases: Offensive Actions and Defensive Controls
- Security Lifecycle Activities

Lesson: Applying Processes and Practices

- Threat Modeling Process
- Modeling Assets and Trust Boundaries
- Modeling Data Flows

Lesson: Risk Analysis

- Identifying Threats
- Relating Threats to Model
- Mitigating Threats
- Reviewing the Application

Module 4: Security Testing

Lesson: Testing Tools and Processes

- Security Testing Principles
- Dynamic Analyzers
- Static Code Analyzers
- Criteria for Selecting Static Analyzers

Lesson: Testing Practices

- OWASP Web App Penetration Testing

- Authentication Testing
- Module Management Testing
- Data Validation Testing
- Denial of Service Testing
- Web Services Testing
- Ajax Testing