DAT101 - DEFENDING DATABASES

Course Learning Objectives

In this course, you'll learn about the vulnerabilities that affect your databases. We'll cover a variety of techniques for securing your databases against such vulnerabilities as SQL injection, buffer overflows, protocol vulnerabilities, and more. We'll also learn some best practices for managing a database to keep it and our data safe.

Description

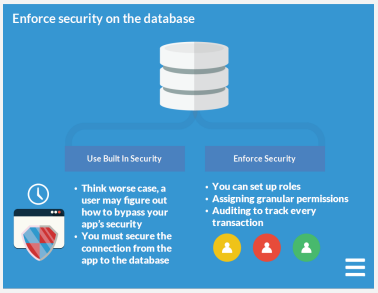
Because databases and their functionality are so diverse, this course is going to focus on important principles and best practices that you can use no matter which product you use. Topics to be covered are about authorizations and authentication, injection attacks, securing sensitive data, logging and auditing, backup and recovery and several attack types such as buffer overflow or protocol vulnerabilities.

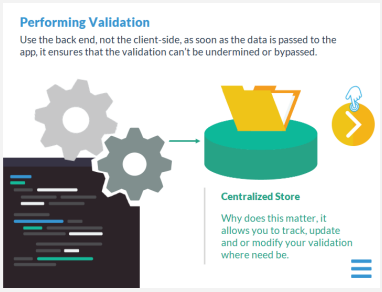
Audience

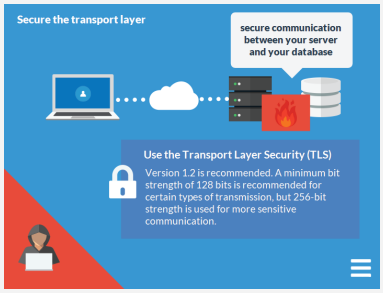
Database Administrators
Database Developers

Time Required

Tailored learning - 60 minutes total







DAT101 - DEFENDING DATABASES

Course Outline

1. Authentication and Authorization

- About the vulnerabilities
- Enforce security on the database
- Use role-based access control with granular permissions
- Granular permissions
- Implement query-level access control
- Enforce a strong password policy
- Don't use hard-coded credentials
- Protect secrets in property and configuration files
- Inactive user accounts
- Restrict host and application access to the database

2. Injection Attacks

- About the vulnerabilities
- SQL injection
- An example of bad input
- Connection string parameter pollution
- Use parameterized queries
- Securing prepared statements
- Securing stored procedures
- Validate input
- Performing validation
- Escaping characters
- Use restrictive access controls
- Control the result set size
- Use secure connection strings
- Best practices

3. Securing Sensitive Data

- Cryptography
- Encryption modes
- Algorithms
- Key management
- Vulnerabilities
- Common attacks
- Store data securely
- Encrypting sensitive data
- Enterprise databases
- Best practices
- Secure the transport layer

4. Logging and Auditing

- Insufficient logging and auditing
- Planning and preparation
- Implement a logging strategy
- Legal, privacy, compliance and regulatory considerations
- Log typical database and server activities
- Audit for signs of suspicious activity
- Protect the logs
- Archive the logs and audit reports

5. Backup, Redundancy & Disaster Recovery

- About the vulnerability
- Disaster recovery and business continuity
- Malware, ransomware and botnets
- Have a business continuity and disaster recovery plan
- Types of backups
- About archive bits
- Comparison of backup types
- Backup techniques
- Backup best practices
- Best practices for restore operations

6. Reducing the Attack Surface

- About the vulnerability
- Denial-of-Service attacks
- Buffer overflow
- Protocol vulnerabilities
- Unnecessary database services
- Patching and updating
- Separate your environments
- Secure the configuration
- Validate database traffic
- Turn off unnecessary services
- Preventing Denial-of-Service attacks

SecurityCompass