DAT101 - DEFENDING DATABASES

Course Learning Objectives

Defending Databases is a course that spans six modules and a range of topics. In the first module, you'll learn why your databases might be prime targets for attackers and how to enforce security policies, restrict database access, and encrypt your database secrets. In module two, you'll consider the impact of injection attacks and learn how to implement the appropriate techniques for defending against injection attacks, and handle input securely. In the third module, we'll discuss securing sensitive data in the database by examining database vulnerabilities that enable an attacker to steal data and cryptography and key management techniques. In the fourth module, we'll discuss logging and auditing and you'll learn how to watch for signs of malicious activity, plan a logging and auditing strategy, and make legal, regulatory, and data protection considerations. In module five, we'll discuss how to be prepared for disasters, malicious attacks, or other kinds of disruption. And finally, in module six, we'll examine security topics that reduce the overall attack surface of your database.

Description

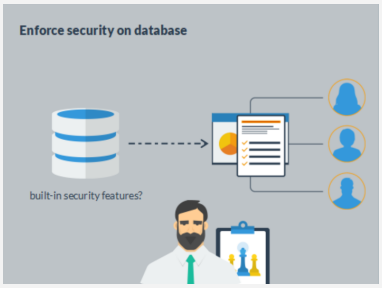
Defending Databases is designed for database administrators, developers, devops engineers, and data analysts working with relational SQL-based databases. This course covers the most common vulnerabilities that affect your databases, techniques for securing your databases, and best practices for managing a database and keeping your data safe.

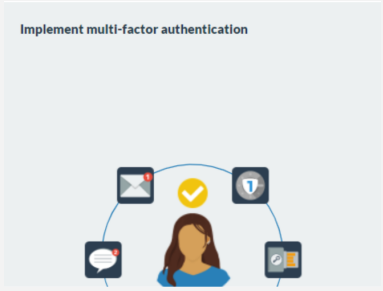
Audience

Database Administrators
Database Developers
DevOps Engineers
Data Analysts

Time Required

Tailored learning - 90 minutes approx.





DAT101 - DEFENDING DATABASES

Course Outline

1. Authentication and Authorization

- Introduction
- Weak authentication
- Weak or default usernames and passwords
- Enforce a strong password policy
- Lock account after unsuccessful login attempts
- Implement multi-factor authentication
- Remove inactive user accounts
- Enforce security on database
- Protect secrets
- Restrict host and application access
- Use of hard-coded credentials
- Avoid use of hard-coded credentials
- RBAC
- Privilege escalation
- Set granular permissions
- Implement query-level access control

2. Injection Attacks

- About
- SQL injection attacks
- Example of a bad input
- Connection string parameter pollution
- Use parameterized queries
- Code: Securing prepared statements
- Code: Securing stored procedures
- Validating input
- Performing validation
- Escaping characters
- Using restricted access controls
- Controling the result set size
- Using secure connection strings
- Best practices

3. Securing Sensitive Data

- About
- Encryption modes
- Encryption algorithms
- Use standard algorithms
- Key management
- Data theft attacks
- Theft of backup data and defense
- Newsflash
- Data modification attacks and defense
- Replay attacks and defense
- Theft of passwords and defense
- On-path attacks and defense
- Rainbow table attacks and defense
- Storing data securely
- Sharing senitive data via VPN
- Using Transparent Data Encryption
- Best practices for protecting data

4. Logging and Auditing

- Introduction
- Reasons to keep logs
- Common flaws
- Right amount of logging and auditing
- Planning and preparation
- Implementing a logging strategy
- Legal and regulatory considerations
- Log database and server activities
- Log activity metadata
- Audit for signs of suspicious activity
- Newsflash
- Archive logs and audit reports

5. Backup, Redundancy and Disaster Planning

- About
- Disaster recovery and business continuity
- Malware, botnets, and ransomware
- Disaster recovery plan
- Types of backups
- Comparison of backup types
- About the archive bit
- Backup storage techniques
- Backup best practices
- Best practices for restoring operations

6. Reducing the Attack Surface

- About
- Denial of service (DoS) attacks
- Buffer overflow
- Protocol vulnerabilities
- Unnecessary database services
- Patching and updating
- Separate your environments
- Secure the configuration
- Validate database traffic
- Use multiple firewalls
- Turn off unnecessary services
- Apply updates and patches
- Prevent DoS attacks

SecurityCompass