Database Security (DISA STIG)

Learn to Attack and Defend Critical Database Assets and How to Build Secure Databases from the Ground Up (within STIGs)

www.triveratech.com

Course Snapshot

- **Course: Database Security (STIG) (TT8820)**
- **Duration:** 3 days
- **Skill-Level & 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.
- **Course Format:** This is a lecture-style event, combining expert presentations with detailed demonstrations and in-depth code walkthroughs. This is not a hands-on course. Students may follow along with demos as desired.
- **Delivery Options**: This course is available for **onsite private classroom presentation**, **live online virtual presentation**, or can be presented in a **flexible blended learning format** for combined onsite and remote attendees. Please also ask about our **Self-Paced / Video** or **QuickSkills / Short Course** options.
- **Customizable**: This course agenda, topics and labs can be further adjusted to target your specific training skills objectives, tools and learning goals. Please inquire for details.

Overview

DISA's Database STIG, in conjunction with both generic and product-specific checklists, provides a comprehensive listing of requirements and needs for improving and maintaining the security of Database Management Systems within the Department of Defense. This course fills in the context, background, and best practices for fulfilling those requirements and needs. As with all of our courses, we maintain tight synchronization between the latest DISA releases and our materials. The close ties between this STIG and the ***Applications Security and Development STIG*** are reflected in the coverage of application issues within the context of this course. A key component to our coverage of **DISA's Security Technical Implementation Guides (STIGS),** this course is a companion course with several developer-oriented courses and seminars

Database Security is an intense database security training course essential for DBAs, QA, Testing, and other personnel who need to deliver secure database applications and manage secure databases within the DoD. In addition to teaching basic skills, this course digs deep into sound processes and practices that apply to the entire software development lifecycle. Perhaps just as significantly, students learn about current, real examples that illustrate the potential consequences of not following these best practices.

Data, databases, and related resources are at the heart of the DoD's IT infrastructures, and must be protected accordingly. In this course, students 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.

Learning Objectives

Students who attend **Database Security (STIG)** will leave the course armed with the skills required to recognize actual and potential database vulnerabilities, implement defenses for those vulnerabilities, and test those defenses for sufficiency. This course quickly introduces students to the most common security vulnerabilities faced by databases today. Each vulnerability is examined from a database perspective through a process of describing the threat and attack mechanisms, recognizing associated vulnerabilities, and, finally, designing, implementing, and testing effective defenses.

Working in a dynamic learning environment attendees will learn to:

- Understand the consequences for not properly handling untrusted data such as denial of service, cross-site scripting, and injections
- Be able to review and test databases to determine the existence of and effectiveness of layered defenses and required checks
- 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
- Understand the dangers and mechanisms behind Cross-Site Scripting (XSS) and Injection attacks
- 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 & Pre-Requisites

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.

Related Courses | STIG Training Suite

- TT8800 Information Assurance (STIG) Overview – 1 day
- TT8810 Application Security and Development (STIG) – 5 days
- TT8820 Database Security (STIG) – 3 days

Enhanced Learning Services: Please also ask about our **Pre-Training Class OnRamp & Prep / Primer** offerings, **Skills Gap Assessment Services**, **Case Studies**, **Knowledge Check Quizzes**, **Skills Immersion Programs & Camps**, **Collaborative Mentoring Services** and **Extended Learning Support** & **Post Training** services.

Course Topics / Agenda

Please note that this list of topics is based on our standard course offering, evolved from typical industry uses and trends. We'll work with you to tune this course and level of coverage to target the skills you need most. Topics, agenda and labs are subject to change, and may adjust during live delivery based on audience interests and skill-level.

Session: Securing Databases Foundation

Lesson: DISA's Security Technical Implementation Guides (STIGS)
- Purpose
- Process
- Areas Covered
- Checklists
- Scripts (SRRs)
- Resources

Lesson: Fingerprinting Databases
- Reconnaissance Goals
- Data Collection Techniques
- Fingerprinting the Environment
- Enumerating Web Applications
- Spidering, Dorks, and Other Tools

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

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
- 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

Session: Moving Forward

Lesson: STIG Database Security Requirements
- Identification and Authentication
  - Group and Individual
  - Key Management Practices
  - Token and Certificates Practices
- Enclave/Computing Environment
  - Auditing Mechanics and Best Practices
  - Data Changes and Controls
  - Encryption
  - Privilege Management

  - Additional Controls and Practices
- Enclave Boundary Defenses
- Continuity of Service
  - Defending Backup/Restoration Assets
  - Data and Software Backups
  - Trusted Recovery
- Vulnerability and Incident Management

Session: Secure Development Lifecycle (SDL)

Lesson: SDL Process Overview
- Revisiting Attack/Defense Basics
- Types of Security Controls
- Attack Phases: Offensive Actions and Defensive Controls
- Secure Software Development Processes
- Shifting Left
- Actionable Items Moving Forward

Session: Taking Action Now

Lesson: Database Checklists
- Checklist Overview, Conventions, and Best Practices
- Generic Database Checks and Procedures
- SQL Server Checks and Procedures (Optional)
  - Installation Checks
  - Database Checks
- Database Checks and Procedures (Optional)
  - Database Automated Checks
  - Database Interview Checks
  - Database Manual Checks
  - Database Verify Checks
  - Home Automated Checks
  - Home Interview Checks
  - Home Manual Checks
  - Home Verify Checks
- Practical Application of the Checklists

Lesson: Design Review
- Asset Inventory and Design
- Assets, Dataflows, and Trust Boundaries
- Risk Escalators in Designs
- Risk Mitigation Options

Lesson: Making Application Security Real
- Cost of Continually Reinventing
- Paralysis by Analysis
- Actional Application Security
- Additional Tools for the Toolbox

Student Materials: Each student will receive a **Student Guide** with course notes, code samples, setp-by-step written lab instructions, software tutorials, diagrams and related reference materials and links (as applicable). Students will also receive related (as applicable) project files, code files, data sets and solutions required for any hands-on work.

Classroom Setup Made Simple: Our dedicated tech team will work with you to **ensure your classroom and lab environment is setup, tested and ready to go** well in advance of the course delivery date, ensuring a smooth start to class and seamless hands-on experience for your students. We offer several flexible student machine setup options including **guided manual set up** for simple installation directly on student machines, or **cloud based / remote hosted lab solutions** where students can log in to a complete separate lab environment minus any installations, or we can supply **complete turn-key, pre-loaded equipment** to bring ready-to-go student machines to your facility. Please inquire for details, options and pricing.

For More Information

Need dedicated training? All courses can be presented **onsite** or **online,** or in a **blended learning format**, tailored to target your specific audience, needs and learning goals. In addition to **full day courses**, we also offer **flex hours, short courses, self-paced options** and more. We train beginner to advanced skills in all areas we cover, and offer **New Hire / Cohort Training**, **Boot Camps**, **Skills Immersion Programs**, **Coaching & Mentoring**, **Reskilling Programs**, **Skills Migration & Transition Programs**, and more. We collaborate with you to ensure all courses are truly targeted to meet your specific needs and learning skills, maximizing your valuable training time, as well as your critical budget. Please visit our extensive **Public Training Schedule** for training for smaller groups or individuals. Please contact us for course details, **Corporate Rates** and **Special Discount Offers**.

For more information about our dedicated training services, collaborative mentoring services, courseware licensing options, courseware development services, public course schedule, training management services, partner and reseller programs, or to see our complete list of course offerings and special offers please visit us at **www.triveratech.com**, email **Info@triveratech.com** or call us toll free at **844-475-4559.** Our pricing and services are always satisfaction guaranteed.
