



## TT8810: Application Security and Development (STIG)

**According to research by the National Institute of Standards, 92% of all security vulnerabilities are now considered application vulnerabilities and not network vulnerabilities**

Trivera Technologies' *Best Defense™ Security Training Series* is a suite of frontline-oriented security courses that provide complete and current coverage of *DISA's Security Technical Implementation Guides (STIGS)* and associated checklists. STIGS are an integral part of the required configuration standards for DoD Information Assurance measures. These measures are focused on preventing cyber espionage and crime as well as denial-of-service attacks. Our comprehensive set of classes address each of the critical issues head-on, as our courses, seminars and workshops explicitly:

- Teach developers, DBAs, and stakeholders what the vulnerabilities are
- Demonstrate, in real terms, the potential impact of each of these vulnerabilities
- Provide experience in how to recognize and properly address these vulnerabilities
- Teach stakeholders how to defend against the potential consequences of security breaches
- Illustrate the value and the process of integrating security into the entire lifecycle of applications, products, and devices

COURSE SNAPSHOT

**Course:** TT8810: Application Security and Development (STIG)

**Duration:** 4 days

**Skill Level:** Intermediate and beyond

**Focus:** Hands-on programming and analysis class covering why and how to integrate security into the entire software development lifecycle

**Audience:** Developers

**Format:** Extensive hands-on programming labs; Expert lecture combined with open discussions and high-level demonstrations. This is a programming course - student machines are required.

**Language / Tools:** Course labs are currently offered in J2EE, .Net C#, and .Net Visual Basic

**Delivery Format:** Available for onsite private classroom presentation, or live online / virtual presentation

**Customizable:** Yes

*DISA's Application Security and Development STIG*, in conjunction with the associated checklist, provides a comprehensive listing of requirements and needs for improving and maintaining the security of software applications and 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. (NOTE: This course will be updated to Version 3 of the *Application Security and Development STIG* that is scheduled for release in September, 2009.)

*Application Security and Development* is a lab-intensive, hands-on application security training course essential for developers, designers, architects, QA, Testing, and other personnel who need to deliver secure applications within the DoD. In addition to teaching basic programming skills, this course digs deep into sound processes and practices that apply to the entire software development lifecycle.

In this course, students thoroughly examine best practices for defensively coding applications, including XML processing and web services. Students will repeatedly attack and then defend various assets associated with a fully-functional application. This hands-on approach drives home the mechanics of how to secure applications in the most practical of terms.

Security experts agree that the least effective approach to security is "penetrate and patch". It is far more effective to "bake" security into an application throughout its lifecycle. After spending significant time trying to defend a poorly designed (from a security perspective) web application, developers are ready to learn how to build secure web applications starting at project inception. The final portion of this course builds on the previously learned mechanics for building defenses by exploring how design and analysis can be used to build stronger applications from the beginning of the software lifecycle.

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.

### ► Course Objectives: What You'll Learn

Students who attend **Application Security and Development** will leave the course armed with the skills required to recognize actual and potential software vulnerabilities, implement defenses for those vulnerabilities, and test those defenses for sufficiency.

This course introduces developers to the most common security vulnerabilities faced by web applications today. Each vulnerability is examined from a programming perspective through a process of describing the threat and attack mechanisms, recognizing associated vulnerabilities, and, finally, designing, implementing, and testing effective defenses.

Multiple practical labs reinforce these concepts with real vulnerabilities and attacks. Students are then challenged to design and implement the layered defenses they will need in defending their own applications.

Working in a lab-intensive, hands-on programming environment, led by our security experts, guided by our expert security team, students will learn to:

- Understand potential sources for untrusted data
- Understand the consequences for not properly handling untrusted data such as denial of service, cross-site scripting, and injections
- Be able to test web applications 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 vulnerabilities of associated with authentication and authorization
- Be able to detect, attack, and implement defenses for authentication and authorization functionality and services
- Understand the dangers and mechanisms behind Cross-Site Scripting (XSS) and Injection attacks
- Be able to detect, attack, and implement defenses against XSS and Injection attacks
- Understand the concepts and terminology behind defensive, secure, coding
- Understand the use of Threat Modeling as a tool in identifying software vulnerabilities based on realistic threats against meaningful assets
- Perform both static code reviews and dynamic application testing to uncover vulnerabilities in Java-based web applications
- Design and develop strong, robust authentication and authorization implementations within the context of application framework
- Understand the fundamentals of Cryptography and Encryption and where they fit in the overall security picture
- Understand the fundamentals of XML Digital Signature and XML Encryption as well as how they are used within the web

services arena

- Be able to detect, attack, and implement defenses for XML-based services and functionality
- Understand techniques and measures that can be used to harden web and application servers as well as other components in your infrastructure
- Understand and implement the processes and measures associated with the Secure Software Development (SSD)
- Acquire the skills, tools, and best practices for design and code reviews as well as testing initiatives
- Understand the basics of security testing and planning
- Work through a comprehensive testing plan for recognized vulnerabilities and weaknesses

This class is “technology-centric”, designed to train attendees in essential secure coding and development skills, coupling the most current, effective techniques with the soundest industry practices. The course provides a solid foundation in basic terminology and concepts, extended and built upon throughout the engagement. Students will examine various recognized attacks against web applications. Processes and best practices are discussed and illustrated through both discussions and group activities.

### ► Audience & Pre-requisites: Who Should Attend

This is an **intermediate-level** programming course, designed for developers who wish to get up and running on developing well defended software applications. This course may be customized to suit your team’s unique objectives.

Familiarity with a programming language is required and real world programming experience is highly recommended. Ideally students should have approximately 6 months to a year of working knowledge.

### ► Related Courses – Suggested Learning Path

**Take Instead:** We offer other courses that provide different levels of knowledge or focus:

- For a high level view of the STIGS and related issues, consider **TT8800 Information Assurance (STIG) Overview**
- For a database orientation, consider: **TT8820 Database Security (STIG)**
- For a high level view of web application security and related issues, consider **TT8020 Understanding Web Application Security**
- For in-depth developer training for web applications with the lifecycle aspect, consider: **TT8325 Securing Web Applications**
- For in-depth developer training with less web application orientation, consider: **TT8200-J Secure Java Coding**

**Take After:** We offer a variety of introductory through advanced security, development, project management, engineering, architecture and design courses. Students may want to consider

the following topics as follow-on to this course.

- **TT8500-J Securing J2EE Web Services**
- **TT8150 Mastering Secure SOA**
- **TT8600 Secure Software Design**
- Additional advanced Security or Secure Programming topics
- Service-Oriented Analysis and Design
- Web Services – Intro through Advanced
- Software Engineering, Design or Project Management tracks

Please note all development courses may also be offered in other programming languages or tailored to suit your unique requirements. Please contact us for details. Please contact us for recommended next steps tailored to your longer term education, project or development objectives.

#### ► **Delivery Environment: Tools to Use**

Although this training is skills-centric, this course can be delivered using a variety of software combinations. Please inquire for details and options.

Our detailed workbooks are complete with software-specific screen shots and step-by-step tutorials for using the software you select. In most cases we can easily port our classes to run in the environment of your choosing.

#### ► **Easy & Secure Set Up! LoadNGo™ Instant Classroom Kit**

For course deliveries or virtual presentation using open-source tools, we'll provide our unique **LoadNGo Instant Classroom Kit**, which enables students to run the entire course off of a DVD that hosts the entire course set up software, labs, and other pertinent useful educational resources, whitepapers and more. You only need to provide the hardware and appropriate O/S, and we'll do the rest. No installation needed. **Great for secure environments.** Minimum set up burden for your team or firm, with maximum results for your students.

No matter which set up option or software your firm requires, we're pleased to provide a detailed set up guide for all private or on-site courses, and as much assistance as you require to prepare your students or classroom for the course. Our support personnel and instructors can be contacted for any advice you may require to prepare your classroom and/or students for attendance.

#### ► **Student Materials: What You'll Receive**

Our robust course materials include much more than a simple slideshow presentation handout. Student materials include a

comprehensive hard-copy course manual, complete with detailed course notes, code samples, diagrams and current reference materials, all directly related to the course at hand, indexed for ease of use. Step-by-step lab instructions and project descriptions are clearly illustrated and commented for maximum learning.

In addition to everything students need for the course, the **LoadNGo Instant Classroom Kit** described above also includes of workshop labs and solutions; non-restricted workshop software, APIs, documentation, technical education papers, and specifications and tutorials pertinent to the training course. Our course kits are designed to serve as an excellent and useful reference set, long after we leave your classroom.

#### ► **Optional Pre / Post-Testing & Skills Assessment**

We work with you to ensure that your resources are well spent. Through our basic course pre-testing and/or post-course assessments, we ensure your team is up to the challenges that this course offers. Our goal is to structure the best solution to ensure your needs are met, whether we customize the material, or devise a different educational path to prepare for this course.

Please contact us for details about our online pre and post test assessment services, custom managed training plans for one student or your entire organization, or our custom online training program management system for monitoring the courses or progress while skilling your students of all experience levels.

#### ► **Bridging the Gap: Collaborative Mentoring Services**

Our team of technical experts is also available for various project assistance services to help your team apply their newly-learned classroom skills to their real-world project in a meaningful, practical way, right after the training ends.

Our custom **collaborative mentoring programs** integrate with or extend your team's classroom training experience, to help bring these skills into existing (or inherited) legacy projects, into new projects, or to simply keep your students sharp them in between projects. Our programs can be highly involved and closely integrated with your project timelines or group development efforts, or can be less involved, serving simply as an overarching educational framework or 'spot check' to keep your group skills moving forward in between projects or waiting for projects to begin.

Please contact us for details about this exciting custom service.

---

**Workshop Topics Covered**


---

**Session: Foundation**

- Misconceptions
  - Thriving Industry of Identify Theft
  - Dishonor Roll of Data Breaches
  - TJX: Anatomy of a Disaster
  - Heartland: What? Again?
- Security Concepts
  - Terminology and Players
  - Assets, Threats, and Attacks
  - OWASP
  - CWE/SANS Top 25 Programming Errors
- DISA's Security Technical Implementation Guides (STIGS)
  - Purpose
  - Process
  - Areas Covered
  - Checklists
  - Scripts (SRRs)
  - Resources
- Defensive Coding Principles
- Reality
  - Recent, Relevant Incidents
  - Find Security Defects In Web Application

**Session: Top Security Vulnerabilities**

- Unvalidated Input
  - Description With Working Example
  - Defenses
  - Identifying Trust Boundaries
  - Qualifying Untrusted Data
  - Implementing An Effect, Layered Defense
  - Designing An Appropriate Response
  - Testing Defenses And Responses
- Overview Of Regular Expressions
  - Regular Expressions
  - Working with Regular Expressions in Java
- Broken Access Control
  - Description With Working Example
  - Defenses
  - Authorization Security Overview
  - Defending Special Privileges Such As Administrative Functions
  - Application Authorization Best Practices
- Broken Authentication And Session Management

- Description With Working Example
- Defenses
- Multi-Layered Defenses Of Authentication Services
- Password Management Strategies
- Password Handling With Hashing Using JCE/JCA
- Mitigating Password Caching
- Testing Defenses And Responses For Weaknesses
- Alternative Authentication Mechanisms
- Best Practices For Session Management in J2EE
- Defending Session Hijacking Attacks
- Best Practices For Single Sign-On (SSO)
- Cross Site Scripting (XSS) Flaws
  - Description With Working Example
  - Defenses
  - Character Encoding Complications
  - Blacklisting
  - Whitelisting
  - HTML/XML Entity Encoding
  - Trust Boundary Definition
  - Implementing An Effective Layered Defense
  - Designing An Appropriate Response
  - Cross-Site Request Forgeries (CSRF)
  - Understanding CSRF
  - Defending Against CSRF
  - Output Encoding – Why
  - Output Encoding – How
  - Output Encoding – Best Practices
- Injection Flaws
  - Description With Working Example
  - Defenses
  - Qualifying Untrusted Data
  - JDBC, PreparedStatement, and StoredProcedures
  - Hibernate Best Practices
  - XML Best Practices
  - Third Party API's
  - Implementing An Effective Layered Defense
  - Designing An Appropriate

- Response
- Error Handling And Information Leakage
  - Description With Working Example
  - Defenses
  - J2EE Application Exception Handling
  - Error Response Best Practices
  - Error, Auditing, And Logging Content Management
  - Error, Auditing, And Logging Service Management
  - Best Practices For Supporting Web Attack Forensics
- Insecure Storage
  - Description With Working Example
  - Defenses
  - Data Leakage
  - Risk Minimization
  - Cryptography Overview
  - JCS/JCE
  - Data Encryption
  - Partial/Complete
  - Property/Deployment/Configuration Files
- Insecure Management Of Configuration
  - Description With Working Example
  - Defenses
  - System Hardening
  - Server Configuration “Gotchas!”
  - Hardening Software Installation
- Direct Object Access
  - Description With Working Example
  - Defenses
  - Java Byte Code Verifier
  - XML/DTD/Schema/XSLT Best Practices
- Spoofing
  - Description With Working Example
  - Defenses
  - Protecting Your Clients
  - Defending Against Cross Site Request Forgeries
  - Phishing Defenses

**Session: Additional Measures**

- Cryptography Overview
  - Cryptography defined
  - Strong Encryption

- Ciphers and algorithms
  - Message digests
  - Types of keys
  - Key management
  - Certificate management
  - Encryption/Decryption
  - Auditing
    - Auditing Mechanics and Best Practices
  - Third Party Software
  - Mobile Code
- Session: Defending XML Processing**
- Defending XML
    - Understanding Common Attacks And How To Defend
    - Operating In Safe Mode
    - Using Standards-Based Security
    - XML-Aware Security Infrastructure
    - JAXP Safe Mode
  - Defending Web Services
    - Security Exposures
    - Transport-Level Security
    - Message-Level Security
    - WS-Security
    - Attacks And Defenses
  - Defending Ajax
    - Ajax Security Exposures
    - Attack Surface Changes
    - Injection Threats And Concerns

- Effective Defenses And Practices

**Session: Secure Software Development (SSD)**

- SSD Process Overview
- Asset, Boundary, and Vulnerability Identification
- Threat Modeling and Analysis
- Process, Design, and Code Reviews
- Applying Processes and Practices
- Configuration Specification and Compliance
- Testing as Lifecycle Process
- Testing Planning and Documentation
- Testing Tools And Processes
  - Principles
  - Reviews
  - Testing
  - Tools
- Static and Dynamic Analysis
- Testing Practices
  - Authentication Testing
  - Data Validation Testing
  - Denial Of Service Testing
  - Web Services Testing
  - Ajax Testing

**Session: Application Deployment**

- Documentation
- Best Practices

- Update and Patch Management
- Incident Response
- Auditing

**Session: Application Security and Development Checklist**

- Checklist Overview, Conventions, and Best Practices
- Generic Application Checks and Procedures
- .Net Framework Checks and Procedures (Optional)
- Web/Java Checks and Procedures (Optional)

---

**Need more info?** Please note that a more detailed outline of the course table of contents, lists of lab exercises and project descriptions is available. Please contact us at [Training@triveratech.com](mailto:Training@triveratech.com) for info.

**Need courseware?** This course is fully customizable, and also available for license with complete support for qualified organizations. Please contact [Courseware@triveratech.com](mailto:Courseware@triveratech.com) for details.

► **Why Work With Trivera Technologies?**

Whether you are a project leader choosing a training provider or course to bring to your team, or an organization or an instructor looking to potentially license or use course materials to train your own team, or a student looking for an exciting, targeted training class to attend or to recommend to your colleagues - **Our single focus is to make YOUR training event or experience a success.** Here's why choosing Trivera Technologies as your IT security education resource takes the risk right out of your decision making process...

- **We provide a solid secure, design, coding and implementation foundation.** Students will learn how to code, use (and reuse!) essential secure Java programming and design skills and concepts properly, using best coding practices, grounding them for advanced curriculum, and will be prepared for designing and implementing solutions. **Students will learn the importance of developing well-defended applications.**
- **Our courses are focused - no "fluff" included.** We offer more than a "laundry list" approach to teaching. All lessons have clear objectives, are fundamental to core secure application development and design practices, and are reinforced by hands-on labs and solid practical examples. Each lesson has performance driven objectives that ensure students will learn technologies and skills core to fundamental server-side application design – nothing more, nothing less.
- **Our materials are comprehensive, and current.** Our comprehensive manuals include not only a hard copy of the course presentation, but also detailed reference notes, pertinent diagrams and charts, current lists of suggested online resources and articles, and often technical tutorials or white papers geared to the topics at hand. Our dedicated course development team keeps everything as current as possible with both industry trends and software editions to ensure your team is getting the most current information available.
- **We foster "Learning by Doing".** Progressive labs are designed in such a way that students get a firm grasp on fundamental skills while they work toward designing a complete application. All labs are take-home, and all solution code is presented in an easy to use self-study format for future use and review.
- **We set you up!** Hands-on courses also include our unique materials for each student, complete with our **LoadNGo Instant Classroom** course set up DVD, software, and a multitude of learning resources that complement the course. Run the course right off the DVD – minimal set up for your company – maximum results for your students.
- **We have to adhere to higher standards.** As a courseware provider to other organizations, training firms and/or independent instructors, our

content and hands-on lab materials are licensed internationally by dozens of firms, and are therefore subject to very stringent quality requirements. Not only will your organization benefit from our own technical team's technical expertise, but also benefit from the feedback of hundreds of students and trainers using these materials, worldwide, on a regular basis. This unique fact guarantees that our materials are not only robust and interesting, but also technically correct, current and of the highest quality and usability.

- **We bring years of practical, current experience into the classroom and content.** Our instructors and course authors are also skilled mentors, Java, JEE/JavaEE, J2EE, .Net, Agile, SOA, and web services developers, architects and security-oriented professionals. We believe that learning, using and maintaining solid software execution and delivery methods are as important as gaining sharp coding skills. Best Practices for software development and execution, beyond technical coding skills, are enforced throughout all of our courses and discussions. Our team brings this extensive experience into every classroom and engagement. Our team has trained thousands of students.
- **We're skills-centric.** Although our team has extensive experience using a variety of tools and solutions, our core content is "technology-centric". Our aim is to teach you the best skills and solutions out there – not to sell you software from any particular vendor.
- **We're Java & JEE / J2EE authors and industry speakers.** Our team was selected to write the online *J2EE, EJB, EJB CMP-CMR and Web Services Tutorial Series for IBM developerWorks®* ([www.ibm.com](http://www.ibm.com)) These are the same instructors who train our classes and author the courseware. Most of our trainers/consultants have also authored additional articles on web services, EJB, Struts, J2EE / JEE and advanced Java topics, and are recognized speakers and presenters on the industry technical seminar circuit. Our team is comprised on several successful published authors. Members of our team have written or contributed to: *Eclipse Kick Start, Mastering Eclipse; Professional Jakarta Struts; Using Java Tools for Extreme Programming; Mastering Resin; Mastering TomCat and others.*
- **Our services are guaranteed.** Whether you're a stakeholder organizing your firm's educational services, a student in our live or virtual classroom or a trainer using our materials to educate your own client or team – **Our core mission is to make YOU a success in the classroom.**

#### ► For Additional Information

**Need dedicated training?** All courses can be brought onsite or run virtually for a **private presentation, anywhere around the world**, customized to suit your unique requirements or goals.

Please contact [Training@triveratech.com](mailto:Training@triveratech.com) for course details, Public Schedule dates and locations, and Special Discount Offers.



Trivera Technologies is a 100%  
Female-Owned Small Business Concern  
GSA Schedule # GS-35F-0188T  
Please contact us for details & pricing.

**Need courseware?** **Let us take the risk out of your classroom delivery!** All materials are also available on a worldwide basis for corporate license with complete instructor support and free corporate branding. Our LoadNGo Set up is available to partners as well! We guarantee our pricing and service. Samples of our course materials, as well as live client references for all of our services are available upon request. Please contact [Courseware@triveratech.com](mailto:Courseware@triveratech.com) for details.

**For more information** about our training, mentoring or courseware development or licensing options, or to see our complete list of course offerings and services, please visit us at [www.triveratech.com](http://www.triveratech.com), email [Training@triveratech.com](mailto:Training@triveratech.com) or call 609.953.1515.