



**BEST
DEFENSE™**

APPLICATION SECURITY
TRAINING SERIES



Collaborative IT Education Services
Training | Mentoring | Courseware
www.triveratech.com

TT8020 Understanding Web Application Security – A Technical Overview (1 day)

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 developer-oriented, application security courses that provide complete coverage of the recently released CWE/SANS *Top 25 Most Dangerous Programming Errors* (<http://cwe.mitre.org/top25/>). These errors, as determined by a consortium of cyber security organizations, enable cyber espionage and crime. Our comprehensive application security and secure coding classes address each of these critical issues head-on, as our courses, seminars and workshops explicitly:

- Teach programmers what these errors are
- Demonstrate, in real terms, the potential impact of each of these errors
- Provide experience in how to recognize and properly address these errors
- Teach stakeholders how to defend against the potential consequences of security breaches in other parts of their IT infrastructure.

COURSE SNAPSHOT

Course: TT8020: Understanding Web Application Security – A Technical Overview (seminar)

Duration: 1 day

Skill Level: Introductory

Focus: Lecture and demonstrations of why and how to integrate security into the entire software development lifecycle for web applications

Audience: Technical managers & stake holders

Format: Seminar / Lecture: Expert lecture combined with open discussions and high-level demonstrations

Language / Tools: This edition is Language Neutral, although we can easily present this in a Java, .Net or other programming language formats.

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

Understanding Web Application Security is an essential application security training course for technical leads, project managers, testing/QA personnel and other stakeholders who need to understand the issues and concepts associated with secure web applications. During this one day dynamic seminar, students learn the best practices for designing, implementing, and deploying secure web applications. Perhaps just as significantly, students learn about current, real examples that illustrate the potential consequences of not following these best practices.

A key component to our *Best Defense Security Training Series*, this workshop is a companion course with several developer-oriented courses and seminars. Although this edition of the course is language-agnostic, it may also be presented using Java, .Net or other programming languages or environments.

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

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. This course builds on the mechanics for building defenses by exploring how design, analysis, testing, and QA can be used to build stronger applications from the beginning of the software lifecycle.

Students who attend **Understanding Web Application Security** will leave this course armed with an understanding of software vulnerabilities, defenses for those vulnerabilities, and testing those defenses for sufficiency. This course quickly introduces the most common security vulnerabilities faced by web

applications today. Each vulnerability is examined through a process of describing the threat and attack mechanisms, the associated vulnerabilities, and, finally, designing, implementing, and testing effective defenses. In many cases, there are demonstrations that reinforce these concepts with real vulnerabilities, attacks, and defenses.

Working in an interactive learning environment, attendees will learn to:

- Understand the concepts and terminology behind defensive, secure, coding
- Appreciate the magnitude of the problems associated with web application security and the potential risks associated with those problems
- Understand the use of Threat Modeling as a tool in

identifying software vulnerabilities based on realistic threats against meaningful assets

- Understand the consequences for not properly handling untrusted data such as denial of service, cross-site scripting, and injections
- Understand the vulnerabilities of associated with authentication and authorization
- Understand techniques and measures that can be used to harden web and application servers as well as other components in your infrastructure
- Relate to the potential vulnerabilities and defenses for the processing of XML in web services and Ajax

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. Attending students will be led through a series of advanced topics comprised of integrated lectures, group discussions and comprehensive demonstrations.

► Audience & Pre-requisites: Who Should Attend

This is a course designed for web application project stakeholders who wish to get up and running on developing well defended web applications. Attendees should have a minimum of 2 years working knowledge in the IT industry, and ideally, students should have a basic understanding of web applications and the associated technologies. Actual development working knowledge is helpful but not necessary.

► Related Courses – Suggested Learning Path

Take Before: Students should have an understanding and a working knowledge in the following topics, or attend these courses as a pre-requisite:

- **TT4000 Understanding Internet Architectures**
- **TT5000 Understanding J2EE**

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

- If you need in-depth developer training for web applications, consider: **TT8320-J Securing J2EE Web Applications** or **TT8320-N Securing .Net Web Applications**
- For a complete focus on web services, please consider **TT8500-J Securing J2EE Web Services** or **TT8500-N Securing .Net Web Services**
- If you need in-depth developer training with less of a web application orientation, consider: **TT8200-J Secure Java Coding** or **TT8200-N Secure .Net Coding**

Please note all development courses may also be offered in other programming languages or tailored to suit your unique requirements.

We will work with you to structure with the best solution to ensure your needs are met, whether we customize the material, or devise a different educational path to help your team best

prepare for this training. Please contact us for recommended next steps tailored to your longer term education, project or development objectives.

► 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 and ease of use.

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 or demonstrations, 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 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.

► 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 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.

Workshop Topics Covered

Session 1: 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
 - Categories
 - What they mean to for web applications
- Defensive Coding Principles
 - Security Is A Lifecycle Issue
 - Minimize Attack Surface
 - Manage Resources
 - Application States
 - Compartmentalize
 - Defense In Depth - Layered Defense
 - Consider All Application States
 - Not Trusting The Untrusted
 - Security Defect Mitigation

- Leverage Experience
- Reality
 - Recent, Relevant Incidents
 - Find Security Defects In Web Application

Session 2: Top Security Vulnerabilities

- Unvalidated Input
- Broken Access Control
- Broken Authentication and Session Management
- Cross Site Scripting (XSS/CSRF) Flaws
- Injection Flaws
- Error Handling and Information Leakage
- Insecure Storage
- Insecure Management of Configuration
- Direct Object Access
- Spoofing

Session3: Defending XML Processing

- Defending XML
- Defending Web Services
- Defending Ajax

Session 4: Secure Software Development (SSD)

- SSD Process Overview
- Applying Processes and Practices
- Risk Analysis

Session 5: Security Testing

- Testing Principles
- Reviews as Form of Testing
- Testing
- Tools
- Testing Practices

***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 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 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 security training 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 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 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 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 have to adhere to higher standards.** As a courseware provider to other organizations, training firms 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 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 technical authors, industry contributors and 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) 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 for course details, Public Schedule dates and locations, and Special Discount Offers.

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 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, email Training@triveratech.com or call 609.953.1515.



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