

## SC GEN 101: APPLICATION SECURITY AWARENESS

After taking this class students will be able to understand the basics of application security and defense. Common application attacks will be demonstrated and dissected. Complete and detailed high level technical explanations on how they work, what they do and the risks posed to your business will be given. Concepts of application security will be discussed in the context of the demonstrated attacks and principles of secure development and risk analysis clearly illustrated. Defensive strategies will be compared and contrasted and reasons for certain security choices will be clearly differentiated. A solid application security roadmap will be discussed focusing on best practices. Web resources for use outside the classroom will be located and evaluated. This class will give you a serious high level appreciation and understanding of the Application Security.

### DURATION & INTENDED AUDIENCE

- Duration: 1 day
- Intended Audience:
  - Information security auditors, analysts, and consultants
  - Web application developers
  - Web application testers and QA staff
  - Project managers
  - Business & requirements analysts

### PRE-REQUISITE KNOWLEDGE

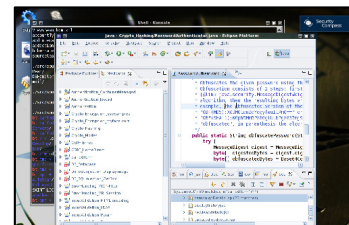
- Basic technical background mandatory
- Knowledge of HTTP and HTML recommended

### LEARNING OBJECTIVES

- Understand major web application security vulnerabilities
- Articulate basic defense mechanisms
- Learn how to further knowledge in particular areas of interest for application security

### LEARNING ENVIRONMENT & TAKEAWAYS

- 4 GB bootable Backtrack Linux flash drive that students keep
- Eclipse, Tomcat, My SQL, and source code from over 30 different **real** open source applications
- Course book containing printouts of each slide along with detailed notes in paragraph form



### CONTACT INFO

- Phone: 1-888-777-2211 x 1
- Email: [training@securitycompass.com](mailto:training@securitycompass.com)

## DETAILED OUTLINE

### Attacks

- Basic auth
- Client certificates
- SSO
- Authentication attacks
- Plaintext passwords
- Authorization tiers
- Authorization attacks and defenses
- Authorization best practices
- Cookie & Session Management
- Session Hijacking
- Session fixation
- Session defense
- PKI
- Crypto attacks
- Rainbow tables and salt

- Parameter manipulation
- XSS
- CSRF
- SQL injection
- Buffer overflow
- Validation Defenses
- Logging & monitoring
- Error Handling

### Application Architecture and Security Principles

- Architecture components and Security
- Security Principles – Good
- Security Principles – Bad
- Secure SDLC