

SC WAS 102: WEB APPLICATION SECURITY FOR PCI COMPLIANCE

This course aims to give developers and security analysts an in-depth understanding of common web application security vulnerabilities. Students perform a deep dive attacking analysis on applications and discuss defense concepts in detail so that they can apply their knowledge to applications of any programming language. Using real examples, the course points out the true risk behind vulnerabilities to help test applications as well understand and triage the results of static analysis tools such as Fortify. The class helps satisfy the PCI DSS objectives of application security training by qualifying students to understand source code review (**PCI DSS 6.3.7**), develop secure code (**PCI DSS 6.5**), and test for common web application vulnerabilities (**PCI DSS 6.6**).

DURATION & INTENDED AUDIENCE

- Duration: 3 days
- Intended Audience:
 - Web application developers
 - Web application testers and QA staff
 - Information security auditors, analysts, and consultants
 - Managers looking for an in-depth understanding of web application attacks

PRE-REQUISITE KNOWLEDGE

- Strong technical background mandatory
- Basic understanding of basic web applications (e.g. tiers in an application, what is HTTP, what is HTML, etc.) mandatory
- Knowledge of a programming language
- General information security OR application development

LEARNING OBJECTIVES

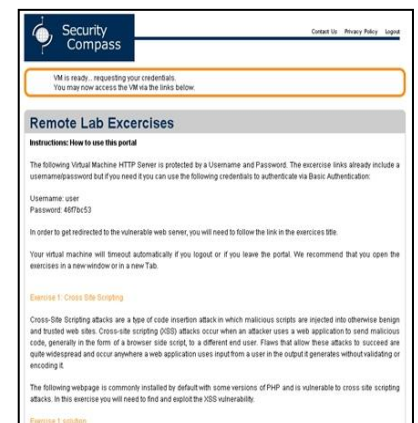
- Understand major web application security vulnerabilities (including OWASP Top 10)
- Get hands-on experience in runtime penetration testing for the most common vulnerabilities
- Understand and use effective tools for evaluating security of web applications
- Produce high-level remediation plans
- Identify security controls at a high level and apply those concepts to source code review
- Identify which vulnerability types are best suited for static analysis, and how to supplement static analysis with manual review

LEARNING ENVIRONMENT & TAKEAWAYS

- 30 days access to Security Compass' remote lab where students can exercise newly acquired penetration testing skills on multiple different **real** open source applications
- Course book containing printouts of each slide along with detailed notes in paragraph form
- 4 GB USB stick with bootable Backtrack

CONTACT INFO

- Phone: 1-888-777-2211 x 1
- Email: training@securitycompass.com



DETAILED OUTLINE

Part 1: Authentication

- Authentication basics
- Factors of authentication
- Authentication mechanisms
- User enumeration
- Brute force
- Network sniffing
- Forgot your password issues

Part 2: Authorization and Access Control

- Authorization basics
- Horizontal and vertical privilege escalation techniques
- Access control: page, functional and content levels

Part 3: Session Management

- Session management basics
- Cookie basics
- Session hijacking
- Session ID weaknesses
- Session fixation
- Cross Site Request Forgery (CSRF)
- Session management best practices

Part 4: Data validation

- Confounding code with data
- Blacklist and whitelist validation
- Cross Site Scripting (XSS), and defense
- Canonicalization/content encoding issues
- SQL Injection and defense
- HTTP Response Splitting, and defense
- LDAP Injection, and defense
- Parameter Manipulation, and defense

Part 5: XML

- XML Basics Review
- Attacks on XML parsers, and defense
- Attacks on XML validation, and defense
- XML Injection, and defense
- XSLT-based attacks

Part 6: Miscellaneous topics

- Info leakage
- Proper error handling
- Logging for intrusion detection
- Accountability
- Third –party code
- File upload/download

Part 7: Cryptography

- Cryptography Basics
- Random numbers
- Symmetric key encryption
- Asymmetric key encryption
- Hashing
- Breaking hashes
- Understanding SSL
- Weak encryption

Part 8: Introduction to Source Code Review

- Automated approaches
- Manual approaches
- The combined approach
- Point of entry review
- Suggested use cases