

SC CBT WAS 101: EXPLOITING AND DEFENDING WEB APPLICATIONS

For this **COMPUTER BASED TRAINING** class you will be given learning material and internet access to fully configured remote lab machines. You will be equipped for compliance with **PCI DSS 6.3.7 and 6.5**. You will learn web application security basics *hands-on*. Learn how attackers penetrate and exploit multiple web applications by executing their attacks *hands-on*. By employing numerous actual attacks, accompanied by detailed and step by step explanations, you will learn their inner workings and be one step closer to getting inside the attackers head. Controlled experimentation will be encouraged. By applying the skills and tools used by attackers you will be better prepared to identify, explain, apply and evaluate defensive measures. A variety of defensive tools and techniques will be discussed, assessed and evaluated. Evaluation of risks based on attacks and defensive tools will be discussed. Good defensive measures and effective preparation depend on knowing the attackers methods.

CBT DURATION & INTENDED AUDIENCE

- Duration: your own pace for class material and hands-on exercises on remote lab machines
- Intended Audience:
 - Information security auditors, analysts, and consultants
 - Web application developers
 - Web application testers and QA staff
 - Managers looking for an in-depth understanding of web application attacks

CBT PRE-REQUISITE KNOWLEDGE

- 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 the OWASP Top 10
- Gain the skills necessary to understand source code review (**PCI DSS 6.3.7**), develop secure code (**PCI DSS 6.5**)
- Get hands-on experience in runtime penetration testing for the most common vulnerabilities
- Understand and use effective tools for evaluating security of web applications

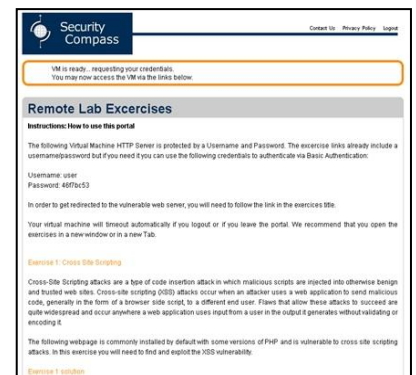
COMPUTER BASED TRAINING LEARNING ENVIRONMENT & TAKEAWAYS

- Dedicated web-accessible remote lab image with multiple **real** vulnerable, open source applications
- Remote access for 200 hours of lab time
- 90 days to use your hours on the lab machines

CONTACT INFO

Phone: 1-888-777-2211 x 1

Email: training@securitycompass.com



The screenshot shows a web portal for "Remote Lab Exercises" under the "Security Compass" logo. It includes a login section with a message: "VM is ready - requesting your credentials. You may now access the VM via the links below." Below this, there are instructions on how to use the portal, including a note that the Virtual Machine HTTP Server is protected by a Username and Password. The provided credentials are: Username: user, Password: 497bc53. There is also a section for "Exercise 1: Cross Site Scripting" which describes the attack and provides a link to a video.

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