

SC WAS 101: EXPLOITING AND DEFENDING WEB APPLICATIONS

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.

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

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
- Produce high-level remediation plans
- Get hands-on experience in runtime penetration testing for the most common vulnerabilities
- Understand and use effective tools for evaluating security of web applications

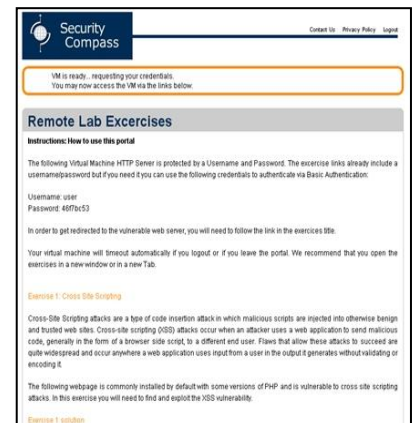
LEARNING ENVIRONMENT & TAKEAWAYS

- 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



The screenshot shows the 'Remote Lab Exercises' page on the Security Compass website. At the top, there is a navigation bar with the Security Compass logo and links for 'Contact Us', 'Privacy Policy', and 'Logout'. Below the navigation bar, a message states: 'VM is ready... requesting your credentials. You may now access the VM via the links below.' The main content area is titled 'Remote Lab Exercises' and includes instructions on how to use the portal. It provides the following credentials: Username: user, Password: 457bc53. It also mentions that the virtual machine will timeout automatically if the user logs out or leaves the portal. The page lists two exercises: 'Exercise 1: Cross Site Scripting' and 'Exercise 2: SQL Injection'. The 'Cross Site Scripting' exercise description explains that it is a type of code injection attack where malicious scripts are injected into otherwise benign and trusted web sites. It also notes that the following webpage is commonly installed by default with some versions of PHP and is vulnerable to cross site scripting attacks.

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