Web Vulnerabilities

9 Module

Module Objectives:

1. Familiarize yourself with Web Vulnerabilities
2. Know what OWASP is
3. Understand how the top ten web vulnerabilities are determined
4. Learn about each of the ten most common web vulnerabilities
5. Discover a little more about each vulnerability
6. Run through the exercises involving OWASP

Module Lesson

Component	Title	Purpose
1. Slideshow (20 minutes)	Web Vulnerabilities	Finding the top ten most common vulnerabilities in web applications
2. Activity 1 (20 minutes)	OWASP Top Ten Part 1	Learn a little bit more about 1-5 of the top ten vulnerabilities and put them to use

IT-ADVENTURES
MAKING IT FUN

3. Activity 2 (20 minutes)	OWASP Top Ten Part 2	Learn a little bit more about 6-10 of the top ten vulnerabilities and put them to use

Note: All activities designed for this module are hands-on. The speed at which the activities can be completed will vary. Each module should approximately take one club or class time to complete.

Additional Resources:

- OWASP Top Ten
  - OWASP Top 10: Injection Attacks
  - OWASP Top 10: Broken Authentication
  - OWASP Top 10: XML External Entities
  - OWASP Top 10: Broken Access Control
  - OWASP Top 10: Security Misconfiguration
  - OWASP Top 10: Cross-Site Scripting (XSS)
  - OWASP Top 10: Insecure Deserialization
  - OWASP Top Ten: Using Components With Known Vulnerabilities
  - OWASP Top Ten: Insufficient Logging and Monitoring
- OWASP Top 10
- Google!
- VMware Glossary