

APPLICATION SECURITY AWARENESS SYLLABUS



Duration

One Day

Audience

Application Developers, Business Analysts, Project Managers, Security Auditors, Application Architects.

Prerequisite Knowledge

A basic understanding of Internet technology is all that is required. The course does not depend on the knowledge of any specific language (ASP, JSP, ColdFusion) or framework (.NET, J2EE); however, it is preferred that students have either application development or information security experience.

Some attack techniques require a working knowledge of HTML and JavaScript. Advanced techniques require a deeper understanding of HTML, JavaScript, SQL, and server-side scripting languages. The instructor will ensure that the course moves at a speed appropriate for the level of student knowledge.

COURSE DESCRIPTION

This course helps students understand the basics of developing secure applications by demonstrating the most commonly exploited vulnerabilities. Students will see examples of each vulnerability and hear real-world examples from FishNet Security's extensive assessment experience.

The course material is augmented with hands-on lab sessions that allow students to explore these attacks on a live example Web site in order to gain a deeper understanding of vulnerabilities. During each vulnerability topic, comprehensive remediation strategies are discussed.

ATTACK TECHNIQUES

- Forceful Browsing
- Client-Side Data Modification
 - Parameter Tampering
 - Hidden Field Manipulation
 - Cookie Poisoning
- Client-Side Logic Subversion
- Exploiting Information Leakage
- Command Injection
- Session Hijacking
- Cross-Site Scripting
- Cross-Site Request Forgery
- Buffer Overflows

REMEDIATION TECHNIQUES

The following remediation techniques will be discussed:

- Input Validation and Output Encoding
- Authentication, Authorization, and Accounting
- Hashing and Encryption
- Error and Exception handling
- Stored Procedures and Parameterized Queries

GENERAL SECURITY TOPICS

- Current Application Security Overview
- Shortcomings of Current Application Security Solutions
- Authentication and Authorization
- Session Management
- Data Validation
- Application Architecture
- Application Security Tools and Frameworks
- Secure Application Development

LAB DETAILS

The lab sessions allow students to gain hands-on experience with application attack techniques as they are covered. FishNet Security has designed a custom Web application (e-commerce) that is vulnerable to the attacks listed above. Students will learn to view applications from the point of view of an attacker by exploiting these vulnerabilities using only a Web browser and a text editor.

CLASSROOM REQUIREMENTS

Classes are typically conducted in the customer's existing training facility. FishNet Security is also able to provide the classroom space if necessary. On-site classrooms require the following:

- Projector with connection for instructor's laptop
- Networked workstations for each student (web browser and text editor)
- LAN connection to the lab network for the instructor's laptop
- Internet connection for the instructor is desirable but not strictly required