

Web Application Security Assessment Using WebInspect 7 and AMP 3.5

Instructor-Led Training



INTENDED AUDIENCE

- Users of WebInspect
- Application Developers
- Quality Assurance Engineers
- Anyone performing Web Application Security Assessments using AMP

DURATION: 4 DAYS

PREREQUISITES

Working knowledge of:

- HTTP Methods
- Encoding (Base64, HEX, URL) techniques used in HTTP/HTTPS
- Basic understanding of web proxies

OVERVIEW

The goal of this course is to create awareness of application security and enable users of Assessment Management Platform (AMP) to manage the security of their web applications across the entire enterprise. Defining specific roles, and assigning permissions to each will allow for segmenting of responsibilities to each group. Scheduling scans, reports and allocating scanning resources through the AMP Console will optimize the efficiency and results of scans. In addition, WebInspect will be explored in depth to perform web application assessments using a myriad of different settings and scenarios. In addition to the basic WebInspect training component, this course addresses manual assessment techniques using WebInspect and the WebInspect Toolkit including the HTTP Editor, Web Proxy, SQL Injector, and the SPI Cookie Cruncher. Appropriate and effective use of these tools is required to validate and test vulnerabilities found in most assessments.

COURSE OBJECTIVES

At the end of the course, you will be able to:

- Identify discrete Web Application vulnerabilities using manual testing techniques
- Validate discrete vulnerabilities found during the automated assessment process
- Manipulate raw http requests using Web Proxy and the HTTP Editor
- Execute automated Web Application Assessments
- Execute authenticated, comprehensive and business logic Web Application Assessments
- Configure scan settings to meet testing requirements
- Create Web Macros using the Web Macro Recorder
- Create Login Macros using the Web Macro Recorder
- Configure scan policies to meet testing requirements
- Generate standard report and documentation
- Evaluate assessment results and identify false-positives
- Validate SQL injection using the SQL Injector
- Analyze session parameters (cookies) using the Cookie Cruncher
- Use the Regular Expression Editor and encoder tools appropriately
- Analyze applications for potential false-negatives
- Identify the components of AMP
- Identify and utilize AMP clients and AMP sensors
- Perform client scans and sensor scans
- Create reports on scan results through AMP
- Use Web Console to initiate scans and view scan results
- Use Windows Console for AMP administration
- Create limited permission roles to restrict sites accessible to pre-defined groups

Day 1	I. Web Application Security Overview
	II. Introduction to Vulnerabilities
	III. Quantifying the Risk
	IV. HTTP 101
	V. Encoding Techniques

Day 2	VI. Regular Expressions
	VII. WebInspect Terminology
	VIII. WebInspect User Interface
	IX. Using the WebInspect Scan Wizard
	X. Using Web Macros

Day 3	XI. Using the WebInspect Home Page
	XII. WebInspect Application Settings
	XIII. WebInspect Scan Settings
	XIV. WebInspect Toolkit

Day 4	XV. Assessment Management Platform (AMP) Overview
	XVI. AMP Devices
	XVII. Running Scans with AMP
	XVIII. AMP Consoles
	XIX. Creating Limited Permission Roles
	XX. AMP Administration