

Introduction to QALinspect 5.1

Instructor-Led Training



INTENDED AUDIENCE

- New users of HP (formerly SPI Dynamics) Application Security Center

DURATION: 2 DAYS

PREREQUISITES

- Working knowledge of HP Quality Center and automated testing procedures

OVERVIEW

This class is targeted at quality assurance professionals responsible for performing the day-to-day tasks associated with evaluating security vulnerabilities in web applications. Students learn how to configure and execute automated web application assessments, create login and web macros, configure scan settings and policies to meet testing requirements, and generate reports using QALinspect. The class consists of lecture and hands-on lab exercises.

COURSE OBJECTIVES

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

- Describe reasons why QA professionals are concerned about security
- Configure and execute automated web application assessments
- Create login macros using the Web Macro Recorder
- Create Tests and Test Sets in Quality Center
- Track Security Vulnerabilities through Defects Module in Quality Center
- Use QALinspect specific settings to manage software defects through SDLC
- Configure scan settings to meet testing requirements
- Create web macros using the Web Macro Recorder
- Configure scan policies to meet testing requirements
- Generate reports

RECOMMENDED FOLLOW-UP COURSES

- Web Application Security Assessment Using WebInspect 7
- Quality Center 9.2 Suite

Day 1	Course Introduction <ul style="list-style-type: none"> • Participant introductions • Administration and Housekeeping • Facilities • Participants' responsibilities • Course objectives • Course outline • Labs • Survey
	I. Overview of Web Application Security <ul style="list-style-type: none"> • Why QA professionals are concerned about security • Security Defects = Functional Defects • Discussion of Common Security Vulnerabilities • Sources of information • Common tools for vulnerability detection • Threat modeling • Overview of Software Development Life Cycle
	III. HTTP 101 <ul style="list-style-type: none"> • HTTP – the stateless protocol • Identify HTTP Methods • Identify state keeping mechanisms • Overview of Requests/Responses • Query and Post Parameters • Using tools to analyze HTTP traffic
	IV. Encoding Techniques and Regular Expressions <ul style="list-style-type: none"> • Recognize Encoding/Hashing techniques used in web applications • Use the Encoder/Decoder tool in the QAInspect Toolkit • Understand Regular Expressions and their application in QAInspect checks • Use the Regular Expression Editor included in the QAInspect Toolkit
	V. Quality Center Setup <ul style="list-style-type: none"> • Identify the modules within Quality Center • Identify the Toolbars within Quality Center • Understand the Test Management Process • Log in to Quality Center

Day 2	<p>VI. Test Planning and Execution</p> <ul style="list-style-type: none"> • Organize Subjects and Tests in a test plan tree • Create QA-INSPECT type tests • Create and organize folders in a test sets tree • Create test sets and add tests to them • Execute automated QA-INSPECT tests • Execute comprehensive scan using QAInspect “staging area”
	<p>VII. QAInspect Terminology and GUI</p> <ul style="list-style-type: none"> • Understand web application scanner terminology • Crawl vs. Audit • Access QAInspect settings and configuration options • Configure and execute a comprehensive scan using QAInspect Auto Status Settings
	<p>VIII. Configure Macros to automate scans</p> <ul style="list-style-type: none"> • Create Login macros to maintain state during scan • Understand logout signatures • Detect logout signatures • Create scan using login macro
	<p>IX. Advanced Scan Settings</p> <ul style="list-style-type: none"> • Learn scan settings and their best usage <ul style="list-style-type: none"> ○ Requestor Thread Counts ○ Create File Not Found custom signature ○ Understand Allowed Hosts ○ Recognize state keeping parameters • Create comprehensive scan with custom settings
	<p>X. Defect Tracking</p> <ul style="list-style-type: none"> • Identify Security Vulnerabilities as Defects • Search and review defects • Track defects throughout their lifecycle • View history of defect
	<p>XI. Start Macros and Policy Manager</p> <ul style="list-style-type: none"> • Create and use Start Macros • Use Policy manager to view check information • Create Custom checks and apply to policy
	<p>XII. Generate Reports</p> <ul style="list-style-type: none"> • Use Report Manager to create reports for scans <ul style="list-style-type: none"> ○ Executive Summary ○ Vulnerability Report ○ Compliance