WebInspect Foundations 19.2

Adoption Readiness Tool (ART)

The Adoption Readiness Tool (ART) provides initial and ongoing enablement to your users to ensure that you get the most out of your software. ART is a cost-effective, comprehensive IT education, documentation and performance support solution. ART provides pre-built simulation-based courses in Micro Focus software that can be accessed by users anytime, anywhere.

ART content provides easy access to self-paced learning content enabling your users to not only dive into an online course, but also to gain direct access to individual components to quickly master specific tasks.

- Access printable job aids targeted towards specific application tasks.
- View or practice a task in a simulated environment.
- Experience full learning with key terms and concepts, product demonstrations and self-assessments by viewing the entire course.

Regardless of which route chosen, users will gain an understanding of the important key concepts, as well as gain competency in both the navigation and functionality of the application.

Course Description

Learn how to dynamically scan Web application, services, and mobile devices to find vulnerabilities, remediate, and report any issues WebInspect discovers. This course is intended to answer application security tester's basic WebInspect usage questions. You will be able to effectively work within WebInspect producing Dynamic Application Security Testing (DAST) to eliminate vulnerabilities and keep up with compliancy before and during your Web application launch. This course includes extensive simulated exercises.

Audience/Job Roles

This course is intended for those whose primary responsibilities include:

- Evaluating your organization's application security posture, quality, and compliance
- Application development and dynamic testing
- Quality Assurance testing

Course Objectives

Upon successful completion of this course, you should be able to:

- Define OWASP Top 10, remediation techniques, DAST and use WebInspect as a DAST tool
- Recognize the WebInspect HTTP protocol to search for vulnerabilities
- Identify the functional characteristics and components of WebInspect
- Create basic, manual, mobile, and work-flow driven scans for a target application
- Recognize settings to specify vulnerability evaluation
- Create Web macros and reports
- Use the Security Toolkit

Prerequisites / Recommended Skills

To be successful in this course, you should have the following prerequisites or knowledge:

- An understanding of basic Web communication protocols.
- Familiarity with some of the most common Web application vulnerabilities (i.e. OWASP Top 10)

Course Topics

Modules	Objectives
Module 1: Introduction to Application Security and DAST	• Introduction • Objectives • Fortify Application Security Solution • Fortify Architecture and Security Management Workflow • Functioning and Secure Applications • Static (SAST) and Dynamic (DAST) Testing • Systems Development Life Cycle (SDLC) • WebInspect and the HTTP Protocol • HTTP(S) Methods • HTTP(S) Authentication Options • Server Response Status Codes • Server Response Fingerprint • WebInspect Fingerprinting • Summary
Module 2: OWASP Top 10 Vulnerabilities and Tools	• Introduction • Objectives • Introduction to OWASP Top 10 • A1 - Injection • A2 - Broken Authentication and Session Management • A3 – Sensitive Data Exposure • A4 - XML External Entities • A5 - Broken Access Control

	• A6 - Security Misconfiguration • A7 - Cross-Site Scripting (XSS) • A8 - Insecure Deserialization • A9 - Using Components with Known Vulnerabilities • A10 - Insufficient Logging & Monitoring • Taxonomy of Software Security Errors • 7 Pernicious Kingdoms and *One Security Defects • The Seven Attack Targets • What the Attacker Sees • DAST Architecture • WebInspect Rules and Procedures • WebInspect Challenges to DAST • OWASP Tools • Guidelines on Securing your System • Hidden Fields • Hidden Fields Source Page View • Hidden Fields Scenario • Exploit the Hidden Fields * • Bypassing HTML Field Restrictions • Exploit Bypassing HTML Field Restrictions * • SQL Injection overview • SQL Injection Scenario • Exploit SQL Injection * • Cross-Site Scripting (XSS) • Cross-Site Scripting (XSS) Attack • Cross-Site Scripting Scenario • Exploit Cross-Site Scripting * • Summary
Module 3: Remediation Methods and Tools for Security	• Introduction • Objectives • Goals of Application Security • Think Like a Security Person • Secure Enough • Fixing Issues Not Exploits • Threat Model and Risk Assessment • Developing a Threat Model • Assets for the Threat Model • STRIDE DREAD Method • STRIDE • DREAD • Assessing a Vulnerability • Performing Risk Assessment • Use DREAD to Explain Vulnerabilities • Summary
Module 4: Basic WebInspect Settings and Scans	• Introduction • Objectives • WebInspect GUI • Get Updates through SmartUpdate * • Specify Application Settings * • Scan Types • Create a Quick (unauthenticated) Guided Scan * • Create a Standard (unauthenticated) Guided Scan *

	• Compare the Scans • Specify Scan Settings * • Create a Basic Manual (Step Mode) Scan * • Summary
Module 5: Macros and Authenticated Scanning	• Introduction • Objectives • Macro Recorder Tool • Login Macros • Workflow Macros • Create a Login Macro * • Create a Workflow Macro * • Run a Basic (Authenticated) Workflow Scan * • Run an (Authenticated) Guided Scan * • Scanning Matrix for WebInspect • Summary
Module 6: Settings for Vulnerability Evaluation	• Introduction • Objectives • Scan Dashboard Initial Review • Search View • Session Info • Attack Information • Working with Vulnerabilities • Review Vulnerability Window • Investigate a Vulnerability * • HTTP Editor Tool • HTTP Editor Tool - Regex Examples • Web Form Editor Tool • Web Form Editor Tool - Backend Server Based on Forms • Create a New Web Form * • Summary
Module 7: Scan Policies and Reports	• Introduction • Objectives • Compliance Manager • Working of Compliance Manager • Policy Manager • Conduct a Policy Inspection * • Build a Custom Attack Groups Policy Check * • Build a Custom Policy * • Generating Reports • Create a Standard Report * • Use Advanced Reporting Features * • Create a Trend Report * • Summary
Module 8: Web Services and Mobile Scanning	• Introduction • Objectives • OWASP Top 10 for Mobile Applications • Mobile Scanning Types • Create a Native Mobile Scan * • Web Services Testing • Design a Test File • Web Services Insights • Swagger REST API for Thorough Scans

	• Perform a Web Services Scan * • Summary
Module 9: WebInspect Security Toolkit	• Introduction • Objectives • Security Toolkit Overview • Server Analyzer Tool • Get a Server Fingerprint * • SQL Injector Tool • Web Proxy Tool • Run the Web Proxy Tool * • Encoders/Decoders Tool • Regular Expression Editor Tool • Summary

❖ Indicates a simulation