Fortify Automated for Static and Dynamic Testing 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

This training takes you through Fortify's automated security solution for protecting your Organization's Web applications through Fortify's static testing, dynamic testing, Security Assistant, Software Security Center (SSC), and WebInspect Enterprise (WIE). You will learn the differences as well as the benefits of both static and dynamic application security testing.

Audience/Job Roles

This course is intended for:

- Application developers, security administrators, penetration testers, and Quality Assurance testers

Course Objectives

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

- Recognize the differences between static and dynamic security testing

- Recognize how applications get attacks based on the OWASP Top 10
- Scan applications thoroughly and correctly both statically and dynamically
- Effectively remediate validated vulnerability findings to issues
- Integrate Projects to the Fortify SSC management platform

Prerequisites / Recommended Skills

There are no prerequisites for this course.

Course Topics

Modules	Objectives
Module 1: Static Application Security Testing (SAST)	• Introduction • Objectives • Layers of Securing Data • Fortify Application Security Solution • Application Security versus Functional Testing • Systems Development Lifecycle (SDLC) • Static (SAST) and Dynamic (DAST) Testing • Static Analysis Advantage • Static vs. Dynamic Analysis Vulnerability Findings • Static Application Analysis Basics • OWASP Top 10 and Fortify • GUIs for Automated Scanning • Fortify Audit Workbench (AWB) • Scan Application Code using Audit Workbench (AWB) * • Audit an Issue using the Analysis Trace * • Audit Workbench Functions Panel • Utilize Functions in Audit Workbench * • SmartView Visualizing Dataflow • Utilize SmartView in Audit Workbench * • Audit an Issue in Audit Workbench * • Plugins Compatible with Fortify • Analyze Scan Results with Visual Studio * • Analyze Scan Results with Eclipse * • Summary • Assessment
Module 2: Dynamic Application Security Testing (DAST)	• Introduction • Objectives • Strengths and Weaknesses to SAST and DAST • Taxonomy of Software Security Errors • 7 Pernicious Kingdoms *Plus One Security Defects • Attacks on an Application • What the Attacker Sees • DAST Architecture • WebInspect Rules and Procedures • WebInspect Challenges to DAST • WebInspect Macros

	• Scan Methods • Simplified API Scanning • Web Proxy Tool • Create a Login Macro * • Run a Guided Authenticated Scan with OWASP Policy and Traffic Monitor Enabled * • Create a Workflow Macro * • Create a Basic Manual (Step Mode) Scan * • Review the WebInspect Scan Results Page * • Run the Web Proxy Tool * • Use the Web Proxy to Create a Workflow Macro * • Summary • Assessment
Module 3: Fortify Security Assistant Plugin	• Introduction • Objectives • Security Assistant Overview • Download Security Assistant from Fortify Marketplace * • Security Assistant Menu Options • Install the Security Assistant Plugin into Eclipse * • Scanning Projects for Issues • Finding Security Issues as you Write Java Code • Inspect the Scan Results using Security Assistant * • Discover Options in Security Assistant * • Summary • Assessment
Module 4: Integrating with Security Software Center (SSC)	• Introduction • Objectives • Fortify SSC Architecture and Security Management Workflow • SSC Browser-Based Platform • Scan Management in SSC • Issue Stats Page • SSC User Accounts • Application and Application Versions in SSC • Creating a New Application Version in SSC • Create New Version Scan Results in the SSC UI * • AWB Options for SSC Collaboration • Integrating Audit Workbench (AWB) to SSC • Verifying a Scan was Successful • Integrate Scan versions from SSC to AWB * • Plugins Compatible for SSC Collaboration • Synchronize Audits to SSC using the Eclipse Plugin * • Uploading your Analysis to SSC • Download a Merged Application File from the SSC * • SSC Application Version Audit • Perform a Basic Remediation in an Application Version with SSC * • SSC Rulepack Updates • Update Rulepacks in SSC * • Summary • Assessment
Module 5: Integrating with WebInspect Enterprise (WIE)	• Introduction • Objectives • Fortify Architecture and Security Management Workflow

	• WebInspect Enterprise (WIE) Consoles • WIE Admin Console Features • WIE Web Console Features • Implementing WIE with SSC • WIE as a Sensor • Create a SSC Application Version and Sync to WIE * • WIE Roles and Users • Create a User from SSC for WIE * • Assign WIE Roles and Permissions * • WIE Scan Management - Scan Status • WIE Scan Management - Scanning • Create a Scan Request * • WIE Scan Management - Templates • WIE Scan Management - Schedules • WIE Scan Management - Blackouts • Create a Scan Template in WIE * • Perform a Web Site Scan in WIE * • Identifying False Positives Results • Vulnerability Rollup • Viewing Scan Results in WIE • Viewing Scan Results in SSC • Analyze Scan Results * • Summary • Assessment

❖ Indicates a simulation