Fortify 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

This course introduces you to the fundamentals of application security and the role of the Fortify Static Code Analyzer (SCA). You will learn how to use Fortify Audit Workbench (AWB), Scan Wizard, Custom Rules Editor, and Software Security Center (SSC) to help you achieve secure applications. With hands-on simulations, you will learn how to find, filter, and group issues, as well as audit those issues. You will learn how to effectively administrate Fortify, produce a custom Data Validation rule, read the analysis trace to remediate issues, integrate the AWB with the SSC and navigate the SSC from a developer's perspective, and finally generate reports.

Audience/Job Roles

This course is intended for all users of the Fortify application.

Course Objectives

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

- Recognize the basic concepts of application security, Threat Models, Risk Assessments, and integrate security into your SDLC
- Navigate through the AWB scan results using filters, searches, and recommendations as well as read, assess, and fix issues using the Analysis Trace
- Apply the appropriate data validation method to remediate given issues
- Integrate the SSC to download and upload scanned applications to the AWB and utilize Audit Assistant
- Create reports from the SSC and the AWB

Prerequisites / Recommended Skills

There are no prerequisites for this course.

Course Topics

Modules	Objectives
Module 1: Introduction to Application Security and OWASP Top 10	• Introduction • Objectives • Application Security in Relation to Computer Security • Types of Application Security • Challenges in Application Security • Challenges in Application Security (Continued) • SQL Injection: Attack • SQL Injection: Remediation • OWASP Top 10: Introduction • OWASP Top 10 Web Application Security Risks • OWASP Top 10 in Fortify's Audit Workbench • Summary
Module 2: Exploring Application Security Attacks	• Introduction • Objectives • OWASP Tools • Guidelines on Securing your System before using WebGoat • Hidden Fields • Hidden Fields Source Page View • Hidden Fields Scenario • Exploit Hidden Fields * • Bypassing HTML Field Restrictions • Exploit Bypassing HTML Field Restrictions * • 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: Data Validation	• Introduction • Objectives

	• Decide Where to Implement Data Validation • Describing the Attack Proxy • Data Validation Types • Data Validation Techniques • Sample Code of Indirect Selection • Indirect Selection • Indirect Selection - Trusting Server-Side Files • Whitelists • Whitelists for Standard Input Types • Data Validation Library - OWASP ESAPI • Blacklists • Examples of Evading Blacklists • Summary
Module 4: Remediation Goals and Activities	• Introduction • Objectives • Main Security Goals • Challenges in Security Goals • Concept of "Secure Enough" • Deciding What to Fix • Dangers of Requiring Exploitability Proof • Remediation Activities • Threat Models • Developing a Threat Model • Assets and Threats Defined • Identifying the Potential Sources of a Breach • Determining Remediation Strategies • Risk Assessment • Classifying Attacks Using STRIDE • Evaluating Attacks Using DREAD • Risk Assessment - Example • Scope of Risk Assessment • Tips on Presenting a Vulnerability • Summary
Module 5: Remediation Security Tools and SDLC Integration	• Introduction • Objectives • Fortify Product Suite Overview • Fortify Architecture and Security Management Workflow • Fortify Scanners • Fortify Server • Fortify Interface Options • Dangers of Misuse • Application Security and Automating Scans • Default Secure Software Development Life Cycle (SDLC) • The Requirements Phase • The Development Phase • The QA-Security Gate Phase • The Deployment Phase • Phased Approach to Securing Applications • Summary
Module 6: Administrating Fortify	• Introduction • Objectives • Typical Fortify Installation

	• Describing Each Fortify Product • Installing the Fortify Desktop Suite • Auditing Preconditions - Before scanning • Auditing Preconditions - Project Information • Auditing Preconditions - Build Information • Auditing Preconditions - Analysis Information • The Different Scan Methods • Scanning Methods with IDE Plugin • Scan using the Eclipse Plugin * • Scanning Methods with AWB Advanced Scan • Scan from AWB using Advanced Scan * • Scanning Methods with Scan Wizard • Scan from the AWB Scan Wizard * • Scanning Methods with Command Line • Scan from Command Line * • Summary
Module 7: Fortify Audit Workbench (AWB)	• Introduction • Objectives • AWB Launch Page • Scan Results Display • Viewing All Issues • Investigating Specific Issues • Investigate Specific Issues * • Viewing All Functions • Audit Guide Two Modes • Audit Guide Wizard Questions • Advanced Audit Guide Questions • Create an Audit Guide * • Search options • Search Modifiers • Advanced Search • Advanced Search (Continued) • Find Issues using Advanced Search * • Issues Auditing Panel • Auditing Issues - Documenting Your Analysis • Analysis Types Icons • Suppressing and Unsuppressing Issues • Practice Auditing and Suppressing Issues * • Practice Finding Suppressed Issues * • Filtering Issues • Practice Filtering Issues * • Practice Hiding Issues * • Moving Issues • Practice Moving Issues * • Grouping Issues • Practice Grouping Issues * • Auditing Cookie Issue • Summary
Module 8: Custom Rules - Data Validation Rule	• Introduction • Objectives • Data Validation Rules • Custom Rule Wizard

	• Import a Rule into AWB • Create a Data Cleanse Rule for Input Validation * • Import Custom Rules * • Summary
Module 9: Reading the Analysis Trace	• Introduction • Objectives • Analysis Trace Overview • The Analysis Evidence Panel • Analysis Trace Icons • Analysis Trace Icons (Continued) • Reading the Analysis Trace - getParameterValues • Reading the Analysis Trace - Path Manipulation • Reading the Analysis Trace - The getRawParameter function • Reading the Analysis Trace - The passthrough function • Reading the Analysis Trace - File(1) • Fixing Issues with the Analysis Trace • Fix an Issue using the Analysis Trace * • Summary

Module 10: Scan Result Folders (Critical, High, Medium, and Low)	• Introduction
	• Objectives
	• Critical Issues Folder
	  • Issues in the Critical Folder
	  • Command Injection
	  • Fixing Command Injection
	  • Auditing a Command Injection Issue
	  • Cross-Site Scripting (XSS)
	  • XSS Remedy - HTML Encoding
	  • XSS Remedy - HTML Encoding (Continued)
	  • XSS Remedy - Other Options
	  • XSS Poor Validation
	  • Password Management - Hardcoded Passwords
	  • Path Manipulation
	  • Privacy Violation
	  • SQL Injection
	  • SQL Injection Remedy - Prepared Statements
	  • SQL Injection Remedy - Data Validation
	  • SQL Injection Remedy - Standardizing
	• High Issues Folder
	  • Access Control Database
	  • Access Control Database Remedy
	  • Access Control Database - Detection
	  • Command Injection
	  • Log Forging
	  • Log Forging Remedy - Wrapper Function
	  • Weak Encryption
	  • Unreleased Resource Database
	• Medium and Low Issues Folders
	  • Medium Category Issues - Misconfiguration
	  • Low Category Issues Folder
	  • Low Category Issues - SQL Injection
	  • Low Category Issues - Cross-Site Request Forgery (CSRF)
	• Summary

Module 11: Integrating AWB with SSC and Running Report	• Introduction
	• Objectives
	• AWB to SSC
	  • AWB Settings for SSC
	  • Downloading from SSC to AWB
	  • Verifying a Scan was Successful
	  • Uploading Your Analysis to SSC
	• SSC Introduction
	  • Scan Management in SSC
	  • Applications in SSC
	  • Creating a New Application Version in SSC
	  • SSC Application Version Audit
	  • Create a Basic Remediation Project *
	  • Sync Application Versions and Upload to the SSC *
	  • Download a Scanned File from SSC *
	  • SSC Rulepack Updates
	  • Update Fortify Rulepacks in SSC *
	  • Introduction to SSC Reports
	  • Creating a Report in SSC
	  • Generate an Issue Trend Report in SSC *
	  • Creating AWB Reports
	  • Generate a Developer Workbook Report in AWB *
	• Generate a Developer Workbook Legacy Report *
	• Summary

Module 12: Utilizing Audit Assistant in SSC	• Introduction • Objectives • Majority of Time Spent Auditing • Too Many 'not an issue' Determinations • The Way Audit Assistant Works • Anonymous Issue Metrics Data • Training Architecture • Leveraging Fortify's Community Intelligence Data • Leveraging a Few Audits to Effect Many • Overview of Scan Analytics • Defining Prediction Policies • Enabling Metadata Sharing • Audit Assistant Workflow • Becoming a Scan Analytics Tenant • Enabling Audit Assistant • Getting an Authentication Token • Training Data Learning • Training your Application Data • Viewing Audit Assistant Results in SSC • Define a Prediction Policy * • Enable Audit Assistant in SSC * • Provide Training Data * • Review your Scan Results with AA * • Audit and Submit Training Data * • Summary

❖ Indicates a simulation

This page is intentionally left blank.