Fortify for Developers using Plugins 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 integrate Fortify with IDE Plugins (Microsoft Visual Studio, Eclipse, Security Assistant, and Fortify on Demand (FoD) through Eclipse) into your software development processes to help you achieve application security. This training will also help you recognize how websites get attacked, define the OWASP Top 10 vulnerabilities, and strategize remediation so you can understand cyber-attacks and their impact on applications.

Audience/Job Roles

This course is intended for developers of the Fortify applications.

Course Objectives

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

- Define application security and its goals to ensure good practices
- Scan applications and remediate validated findings to issues

- Configure Fortify Options within each plugin
- Inspect code with Security Assistant through Eclipse
- Install and utilize Fortify on Demand (FoD) through Eclipse

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, Microsoft Visual Studio)

Course Topics

Modules	Objectives
Module 1: Application Security Overview	• Introduction • Objectives • Fortify Application Security Solution • Compromising Brand and Reputation • Application Security in Relation to Computer Security • Types of Application Security • Application Security vs. Functional Testing • Getting Around Security • Challenges to Online Security • Challenges to Websites Today • Challenges to Automated Systems • Insecure Code • SQL Injection Attack Shuts Down Business • Secure Code • Systems Development Lifecycle (SDLC) • Summary
Module 2: OWASP Top 10 Vulnerabilities	• 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 and Monitoring • Summary
Module 3: Exploring Application Security Attacks	• Introduction • Objectives • OWASP Tools

	• Guidelines on Securing your System • 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 4: Remediation Tools in Application Security	• Introduction • Objectives • Goals of Application Security • Think Like a Security Person • Secure Enough • Fixing Issues Not Exploits • Buffer Overflow Scenario • 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 5: Using Fortify through Visual Studio	• Introduction • Objectives • Visual Studio Plugin Overview • Visual Studio Plugin Solution Screen • Fortify Menu • Solution Scanning Screens • Utilize Fortify Options * • Scan using Fortify * • Investigate the Project Summary * • View Filter Sets * • Create a Group by Option * • Audit Scan Results * • Search Specific Vulnerabilities * • Summary
Module 6: Using Fortify through Eclipse	• Introduction • Objectives • Eclipse Plugin Solution Screen • Fortify Menu • Open a Project in Eclipse to Scan * • Utilize Fortify Options * • Investigate the Project Summary *

	• Create a Customized Group by Listing * • Audit Scan Results * • Search for Specific Vulnerabilities * • Fortify Security Assistant • Utilize Fortify Security Assistant Plugin * • Fortify On Demand (FOD) • Utilize Fortify on Demand within Eclipse * • Summary

❖ Indicates a simulation