Training: Micro Focus
FT120 - Fortify SAST and DAST for Developers

TRAINING GOALS:

Get the Fortify security solution in 2 days. Fortify SAST and DAST for Developers is a two day training that explores how the Fortify product suite Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) scans for security vulnerabilities. As a student you will learn about the threats to applications, as well as the operation and remediation through the Fortify solution. With 70% hands-on activities you will learn how to utilize the Fortify SCA (Static Code Analyzer) and WebInspect.

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

- Identify application security and the Pernicious Kingdoms
- Successfully run static (SAST) and dynamic (DAST) scans
- Analyze the scan results using both Fortify (SAST) and WebInspect (DAST)
- Manage projects and audit issues using Audit Workbench

Audience/Job Roles

- Software/Application Developers, Product Managers, Development Managers, Q/A Managers, Q/A Analysts, and Application Security Analysts

CONSPECT:

- Module 1: Application Security overview
  - Review the OWASP Top 10 2017
  - Recognize layers of Securing Data (whitebox and Blackbox testing)
- Module 2: Fortify Static Scanning
  - Run several different types of scans using Fortify
  - Practice memory tuning to optimize scanning
- Module 3: Scan Results in Audit Workbench (AWB)
  - Identify the findings in the Critical folder
  - Apply the appropriate validation method to remediate a given vulnerability in the Critical folder
  - Audit and suppress findings
- Module 4: Fortify SCA (Static Code Analyzer) Metrics

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Describe the Scanning Process
- Explain the function of each Analyzer
- Recognize how the findings are placed within each risk folder

- Module 5: Fortify IDE Plugins
  - Configure and scan using the Fortify IDE plugins Visual Studio and Eclipse
- Module 6: Analysis Trace and Remediating Vulnerabilities
  - Properly read the analysis trace
  - Learn how to remediate vulnerabilities
- Module 7: WebInspect (WI) Application Exploits
  - Identify characteristics of Web-based application security defects
  - Recognize prevalent software attacks
- Module 8: Dynamic Scanning with WI
  - Produce scans and create macros
  - Evaluate then remediate your scan results
- Module 9: Mobile Scanning with WI
  - Recognize WebInpsect Mobile Templates, Devices and Software
  - Recognize the steps for Native Mobile Scanning
- Module 10: Web Services and API Scanning
  - Describe Web Services (SOAP) scanning capabilities
  - Perform a Web services scan
- Module 11: Application and Scan Settings
  - Review the primary application and default scan setting options in WebInspect

REQUIREMENTS:

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

- Basic programming skills (able to read Java, C/C++, or .NET)
- Basic understanding of web technologies: HTTP Requests and Responses, HTML tags, JavaScript, and server-side dynamic content (JSP, ASP or similar)
- Knowledge of Web Application development and security practices

Difficulty level

CERTIFICATE:

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

The participants will obtain certificates signed by Micro Focus (course completion).

TRAINER:

Authorized Micro Focus Trainer

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007