IBM Security AppScan Enterprise Fundamentals
Information

Length:	2.0 Days
__Ref:	TK300G-X
Delivery method:	Classroom
Price:	EUR

Overview

In this course, you learn how to use IBM Security AppScan Enterprise. The course combines both class lectures and hands-on lab work so that you can learn how to use the product to test for web application security issues. You learn to use best practices in the context of real-world deployments. You gain hands-on experience using Security AppScan Enterprise on a demonstration web application.

Public

The target audience for this basic course is security auditors, security team managers, quality assurance practitioners and web application developers who need to understand web application vulnerability testing reports, run web application security scans on web applications, and administer Security AppScan Enterprise. The audience might also include web developers, managers, or team leaders who are responsible for interacting with testers or who need to ensure that the tools are being implemented fully and appropriately.

Prerequisits

You should have:

- Web application security knowledge
- Completed *Essentials of Web Application Security V2.0 (RT302)*

Objective

- Describe the capabilities of Security AppScan Enterprise
- Explain the potential risks of conducting an automated security scan
- Work with dashboards, jobs, folders, reports, and alerts
- Explain the differences between manual and automatic exploration
- Configure, run, and optimize scans
- Use scan logs and identify messages, export a scan log, and troubleshoot scans
- Describe the process of analyzing scan results and using issue management
- Explain the architecture of IBM Security AppScan Enterprise

- Administer users and groups, and manage access control
- Create scan templates and test policies
- Describe best practices for generating management reports

Topics

- Unit 1: Security AppScan Enterprise overview
- Unit 2: Preparing to scan
- Unit 3: Reports overview
- Unit 4: Managing folders, report packs, and dashboards
- Unit 5: Configuring a basic scan
- Unit 6: Using the manual explore option
- Unit 7: Using recorded login sequences and session management
- Unit 8: Reviewing explore results
- Unit 9: Configuring an advanced scan
- Unit 10: Running a scan and reviwing the reports
- Unit 11: Reading, exporting, and troubleshooting scan logs
- Unit 12: Organizing, verifying, and exporting scan results
- Unit 13: Managing issues
- Unit 14: Managing users, groups and access control
- Unit 15: Creating scan templates
- Unit 16: Test policies
- Unit 17: Reporting the scan results