ProTech
protechtraining.com

"Charting the Course ...

... to Your Success!"

Core IBM Rational AppScan Fundamentals SE (Standard Edition)

Course Summary

Description

This is a lab- intensive, hands- on tool- oriented AppScan / security training course, essential for experienced enterprise developers and security personnel who need to work with AppScan. This course assumes that students already have a solid understanding of web application vulnerabilities and defenses. This course digs deep into sound processes and practices for using the IBM Rational AppScan tool to test, analyze, and evaluate the security and effectiveness of defenses associated with your web applications. Throughout this course, students thoroughly examine the use of AppScan to test and analyze new or existing web applications. Students will repeatedly analyze vulnerable and defended assets associated with fully- functional web applications. This hands- on approach drives home the mechanics of how to secure web applications using AppScan in the most practical of terms. The course then goes into the advanced features and capabilities of AppScan, showing what they are and how to effectively use them. This includes applying AppScan to specific vulnerabilities and application configurations and scenarios. Many of these are accompanied by a hands- on lab that shows the issues as well as how AppScan responds to effective solutions and defenses for these vulnerabilities.

Objectives

At the end of this course, students will be able to:

- Test web applications with various attack techniques to determine the existence of and effectiveness of layered defenses
- Configure AppScan to scan and analyze web applications
- Generate and understand AppScan testing and test results
- Use AppScan in the most effective fashion
- Integrate AppScan into the larger context of secure application development and lifecycles
- Effectively use AppScan to examine web application capabilities such as authentication, sessions, and logout
- Effectively use AppScan to examine web application vulnerabilities such as XSS, SQL Injection, authentication, and many others
- Design, implement, and generate AppScan reports
- Use AppScan to analyze web services
- Schedule AppScan operations
- Extend AppScan

Topics

- Top Security Vulnerabilities
- Working with AppScan
- Advanced AppScan Topics
- Defending XML Processing
- Best Practices

Audience

This is an intermediate - level web application course, designed for students who wish to get up and running on developing well-defended web applications.

Prerequisites

Familiarity with web applications and the web is required and real world programming experience is highly recommended. Ideally students should have approximately 6 months to a year of web development working knowledge.

Duration

Three days

ProTech
protechtraining.com

"Charting the Course ...

... to Your Success!"

Core IBM Rational AppScan Fundamentals SE (Standard Edition)

Course Outline

I. Top Security Vulnerabilities
- A. Unvalidated Input
- B. Broken Access Control
- C. Broken Authentication and Session Management
- D. Cross Site Scripting (XSS/CSRF) Flaws
- E. Injection Flaws
- F. Error Handling and Information Leakage
- G. Insecure Storage
- H. Insecure Management of Configuration
- I. Direct Object Access
- J. Spoofing

II. Working with AppScan
- A. AppScan Overview
  1. What AppScan targets
  2. How AppScan works
  3. AppScan Architecture
- B. Configuring AppScan
- C. Preparing targeted web application
- D. Performing basic scans
  1. What is targeted
  2. Initiating scanning
  3. Terminating scanning operations
- E. AppScan Results
  1. What AppScan generates
  2. Interpreting scanning results
- F. Application Coverage
  1. Understanding application coverage
  2. Increasing application coverage
  3. Testing defenses

III. Advanced AppScan Topics
- A. Static versus Runtime Analysis
- B. Advanced scanning options
- C. Reducing false positives
- D. Scanning for specific features
  1. Sessions
  2. Authentication
  3. Authorization
  4. Logout
- E. Scanning for specific vulnerabilities
  1. Cross-Site Scripting (XSS)
  2. SQL Injection
  3. String Analysis
  4. Buffer Overflows
- F. Compliance analysis
  1. PCI Data Standards and others

IV. Defending XML Processing
- A. AppScan and Web 2.0
  1. Scanning AJAX and JavaScript applications
  2. Analyzing JSON and Adobe Flash
- B. AppScan and Web Services
  1. Scanning web services
  2. Analyzing SOAP messages

V. Best Practices
- A. Defensive Coding Principles Revisited
- B. AppScan usage patterns
- C. What AppScan does not cover
- D. Integrating AppScan into larger security context
- E. Effectively managing AppScan