Web Application Testing: Principles & Practice (Hands-On)

Introduction

Web applications have a different risk profile compared to other computing environments. Typically, Web application developers have to deal with shorter project release timescales, changing technologies, disparate hardware as well as software platforms, and an uncontrolled user base that could run into millions. The combination of these factors ultimately affects the functionality, security and performance of a dynamic, application driven Website.

Web application testing is, therefore, a complex, high-risk process since it requires a thorough understanding of the operating strengths and weaknesses of multiple, interacting hardware and software systems, the collective use of appropriate test cases, and the deployment of specialist Web application testing tools.

The training course addresses fully the issues related to Web application testing. It provides attendees with the knowledge as well as practical skills to identify, plan and carry out different forms of Web application testing, including significant functional, security and performance tests.

Attendees Will Learn About

Web application testing encompassing:

- Threats & Risks
- Test Components
- Testing Strategies
- Test Planning
- Test Cases, Scripts & Suites
- Functional Testing
- Security Testing
- Performance Testing
- Specialist Testing Tools

Who Should Attend

This course is suitable for System Testers, Software Engineers, Security Analysts, Web Auditors and Quality Assurance Managers.

Web Application Testing: Principles & Practice (Hands-On)

Course Content

Web Application Testing: Fundamentals

- Threats & Risks
- Testing Range
- Testing Strategies
- Test Planning
- Test Cases, Scripts, Suites & Scenarios
- Selecting Test Loads
- Manual Testing
- Automated Testing

Web Application Testing: Scope

- Data Testing
- Unit Testing
- Integration Testing
- Functional Testing
- System Testing

Web Application Testing: Security

- Gateway Programs
- Buffer Overflow Handling
- URL Manipulation
- SQL Injection
- Cross-Site Scripting
- Cookie Poisoning
- (In-)Secure Cookies
- AJAX
- Application Logging
- Vulnerability Analysis

Web Application Testing: Performance

- Load Testing
- Stress Testing
- Volume Testing
- Endurance Testing
- Failover Testing