CSP105 – SECURE SOFTWARE TESTING

Course Learning Objectives

Identify the different artifacts of testing and their importance for the process. Describe the importance of testing and its impact on secure software. Describe the types of testing and the benefits and weaknesses of each. Identify impact and assessment and the respective corrective actions for secure software development. Describe the Test Data Lifecycle Management.

Description

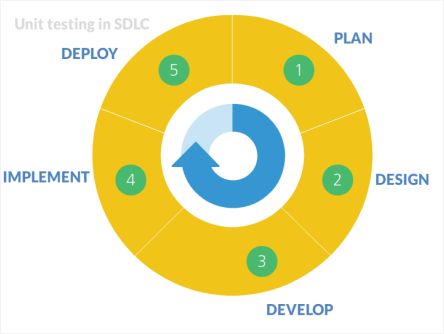
The Security Software Testing domain will address issues pertaining to proper testing of software for security, including the overall strategies and plans. Learners will gain an understanding of the different types of functional and security testing should be performed, what are the criteria for testing, concepts related to impact assessment and corrective actions, and understanding the test data lifecycle.

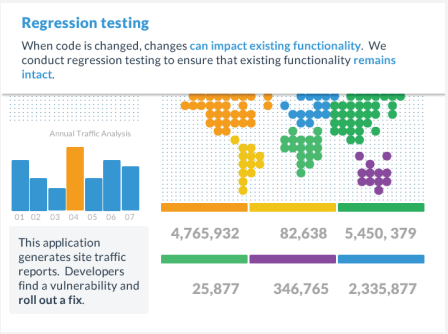
Audience

Certified Secure Software Lifecycle Professional (CSSLP)

Time Required

Tailored learning - 40 minutes total





CSP105 – SECURE SOFTWARE TESTING

Course Outline

1. Components to Testing

- About secure software testing
- Test strategy
- Test plan
- Test cases
- Test scripts
- Putting it all together

2. Testing for Security and Quality Assurance

- Reliability testing
- Unit testing
- Stubs and drivers
- Unit testing in SDLC
- Integration testing
- Regression testing
- Recoverability testing
- Load testing
- Stress testing
- Environment testing
- Interoperability testing
- Simulation testing
- Disaster recovery testing

3. Resiliency and Reporting

- Resiliency testing
- Resiliency testing methodologies
- Blackbox vs. whitebox testing
- Graybox testing
- Cryptographic validation
- Scanning
- Network scanning
- Application scanning
- Penetration testing
- Fuzzing
- Software defects
- Defect reporting
- Tracking defects
- Impact assessments

Security Compass