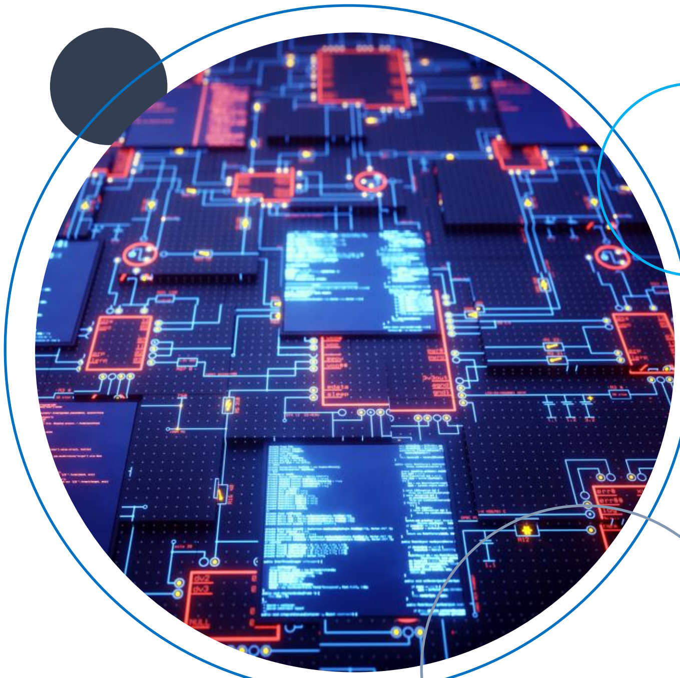
OVERVIEW

The Official (ISC)² CSSLP training provides a comprehensive review of the knowledge required to incorporate security practices – authentication, authorization and auditing – into each phase of the Software Development Lifecycle (SDLC), from software design and implementation to testing and deployment. This training course will help students review and refresh their knowledge and identify areas they need to study for the CSSLP exam.

XTREMELABS



CERTIFIED SECURE SOFTWARE LIFECYCLE PROFESSIONAL (CSSLP)

COURSE OBJECTIVES

After completing this course, the student will be able to:

- Identify the software methodologies needed to develop software that is secure and resilient to attacks.
- Incorporate security requirements in the development of software to produce software that is reliable, resilient and recoverable.
- Understand how to ensure that software security requirements are included in the design of the software, gain knowledge of secure design principles and processes, and gain exposure to different architectures and technologies for securing software.
- Understand the importance of programming concepts that can effectively protect software from vulnerabilities. Learners will touch on topics such as software coding vulnerabilities, defensive coding techniques and processes, code analysis and protection, and environmental security considerations that should be factored into software.
- 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 that should be performed, the criteria for testing, concepts related to impact assessment and corrective actions, and the test data lifecycle.
- Understand the requirements for software acceptance, paying specific attention to compliance, quality, functionality and assurance. Participants will learn about pre- and post-release validation requirements as well as pre-deployment criteria.
- Understand the deployment, operations, maintenance and disposal of software from a secure perspective. This is achieved by identifying processes during installation and deployment, operations and maintenance, and disposal that can affect the ability of the software to remain reliable, resilient and recoverable in its prescribed manner.
- Understand how to perform effective assessments on an organization's cyber-supply chain, and describe how security applies to the supply chain and software acquisition process. Learners will understand the importance of supplier sourcing and being able to validate vendor integrity, from third-party vendors to complete outsourcing. Finally, learners will understand how to manage risk through the adoption of standards and best practices for proper development and testing across the entire lifecycle of products.

TARGET STUDENT

The training seminar is ideal for those working in positions such as but not limited to:

- Software Architect
- Software Engineer
- Software Developer
- Application Security Specialist
- Software Program Manager
- Quality Assurance Tester
- Penetration Tester
- Software Procurement Analyst
- Project Manager
- Security Manager
- IT Director/Manager.

COURSE CONTENT

Lesson 1: Secure Software Concepts

- General Security Concepts
- Risk Management
- Security Policies and Regulations
- Software Development Methodologies

Lesson 2: Secure Software Requirements

- Policy Decomposition
- Data Classification and Categorization
- Requirements

Lesson 3: Secure Software Design

- Design Processes
- Design Considerations

- Securing Commonly Used Architecture
- Technologies

Lesson 4: Secure Software Implementation/Coding

- Common Software Vulnerabilities and Countermeasures
- Defensive Coding Practices
- Secure Software Coding Operations

Lesson 5: Secure Software Testing

- Security Quality Assurance
- Security Testing

Lesson 6: Secure Software Acceptance

Lesson 7: Secure Software Installation, Deployment, Operations Maintenance, and Disposal

- Secure Software Installation and Deployment
- Secure Software Operations and Maintenance
- Supply Chain and Software Acquisition