Secure Programming Foundation

Duration: 2 Days Course Code: S-SPF

Overview:

The S-SPF Secure Programming certificate by SECO demonstrates your ability to understand the logic behind security principles and apply security principles in design and code. The certificate enables you to exhibit your knowledge about web application vulnerabilities and the most effective ways to discover, prevent and eradicate these vulnerabilities.
With a Secure Programming certificate, you will be internationally recognised as a secure software developer.

Target Audience:

The Secure Programming Foundation certification program (S-SPF) is suitable for every programmer or software developer responsible for developing (web) applications. The course is suitable for both novice and experienced developers who wish to acquire a solid grounding in secure software development.

Objectives:

- Secure Programming Foundation equips you with the knowledge and skills you need to lay the foundations of a thriving career as a secure software developer, software engineer or software auditor.
- By passing the SPF certification exam and earning a SECO-Secure Programming Foundation (S-SPF) certificate, you demonstrate your ability to
- Understand the importance of security in the software lifecycle and the logic behind industry-approved secure development principles;
- Understand web application attack surfaces and trust boundaries;
- Understand the workings of HTTP requests and header injection;
- Understand password authentication vulnerabilities and effective countermeasures;
- Understand the security implications of session management and identify effective countermeasures against session fixation;
- Identify countermeasures against cross-site request forgery (CSRF) and clickjacking attacks;
- Identify countermeasures against injection attacks;
- Identify countermeasures against buffer overflows;
- Identify countermeasures against cross-site scripting (XSS);
- Identify countermeasures against file upload attacks;
- Identify countermeasures against character encoding vulnerabilities;
- Understand privilege escalation and list relevant mitigation techniques;
- Secure products by hardening and vulnerability scanning;
- Understand how to prevent side-channel attacks;
- Understand how to prevent DoS attacks;
- Understand the importance of good error handling practices;
- Understand the security risks involved in logging;
- Understand symmetric and asymmetric cryptography, Man-in-the-Middle attacks, and the pitfalls in SSL/TLS and HTTPS certificates.
- Explain how security requirements can/should be identified;
- Perform simple threat modelling exercises and identify security requirements for a system.

Prerequisites:

Experience with at least one programming language is required.

The course and the certificate are ideal for your career advancement if you are a(n)

- (Aspiring) software developer, software engineer or software auditor;
- Aspiring lead developer or architect;
-

Content:

The course covers the following subjects:

- Introduction to Secure Programming
- Secure Programming Awareness
- Authentication and Session Management
- Input Handling
- Authorization
- Configuration, Error Handling and Logging
- Cryptography
- Secure Software Engineering

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/