COURSE OUTLINE

ETHICAL HACKING
Certified Secure Coding for Software Developers (CSCSD)

SPECIALIST-LEVEL COURSE Cost: **£1,300.00** + VAT Duration: **2 days**

This two-day course is for people who want to understand the technical controls used to prevent software vulnerabilities. It focuses on common insecure coding practices and examines how these can be addressed to make secure applications.

"The course was excellent and highly relevant to my work as a web developer. A variety of topics were covered and I thought that a good level of time was dedicated to the most prevalent and serious exploits."
CSCSD Delegate
Falck Safety Services

COURSE OVERVIEW

It is much less expensive to build secure software than to correct security issues after the software has been completed or deal with the costs that may be associated with a security breach.

Securing critical software resources is more important than ever as the focus of attackers has steadily moved to the application layer.

Building secure software requires an understanding of security principles and the goal of software security is to maintain the confidentiality, integrity and availability of information resources in order to enable successful business operations.

During the course, you will have access to a specifically created controlled environment to demonstrate the main areas of vulnerability and mitigation strategies.

THE SKILLS YOU WILL LEARN

- You will learn about the vulnerabilities that arise from insecure coding and the array of hacking techniques that many attackers use to disrupt the way an application's programming/business logic work
- You will find out how to take a 'defence in depth' approach and ensure you consider all the security issues that may arise while developing applications
- You will gain an understanding of the most important principles in secure coding and apply your new knowledge with examples and exercises in Java
- You will learn about the Security Development Lifecycle (SDL), a software development process that will help you build more secure software and address security compliance requirements while reducing development cost.

KEY BENEFITS

With this course, you will:

- Have access to a purpose built controlled environment specifically created to demonstrate the main areas of vulnerability and the key mitigation strategies
- Get the chance to practise techniques to address common insecure coding practices
- Build your skills and confidence in coding secure applications

WHO SHOULD ATTEND

This course is for people who want to learn secure coding, including:

- Penetration testers
- Professional software developers
- Software architects
- Software security auditors
- Security managers

PREREQUISITES

Rather than attempt to cover all languages on one course we focus on the important principles. A basic understanding of web application coding is preferable, ideally in Java (as examples and exercises are in Java), however the course has been developed to be language agnostic

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com

COURSE OUTLINE

ETHICAL HACKING
Certified Secure Coding for Software Developers (CSCSD)

SPECIALIST-LEVEL COURSE | **Cost: £1,300.00 + VAT** | Duration: **2 days**

WHAT QUALIFICATION WILL I RECEIVE?

Those delegates successfully passing the exam at the end of the course will be awarded 7Safe's Certified Secure Coding for Software Developers (CSCSD) qualification.

SYLLABUS

1. **Introduction**
   a. Disclaimer
   b. Trends & Metrics
   c. Lab Environment

2. **Core Security Concepts**
   a. Confidentiality, Integrity, Availability
   b. Authentication and Authorisation
   c. Accounting
   d. Non-repudiation
   e. Privacy
   f. Data Anonymisation
   g. User Consent
   h. Disposition
   i. Test Data Management

3. **Secure Development Lifecycle**
   a. Waterfall vs Agile
   b. Microsoft SDLC
   c. TouchPoints
   d. CLASP
   e. Comparison

4. **Security Design Principles**
   a. Least Privilege
   b. Separation of Duties
   c. Defence in Depth
   d. Fail Safe
   e. Economy of Mechanism
   f. Complete Mediation
   g. Open Design
   h. Least Common Mechanism
   i. Psychological Acceptability
   j. Weakest Link
   k. Leveraging Existing Components

5. **Secure Development Principles**
   a. Input Validation
   b. Canonicalisation
   c. Output Encoding
   d. Error Handling
   e. Authentication & Authorisation
   f. Auditing & Logging
   g. Session Management
   h. Secure Communications
   i. Secure Resource Access
   j. Secure Storage
   k. Cryptography

6. **Best Practices**

7. **Conclusion**

PA Consulting
Global Innovation & Technology Centre Back Lane, Melbourn
Herts, SG8 6DP, United Kingdom
tel: +44(0) 1763 285285
email: cybereducation@paconsulting.com
www: cybereducation.paconsulting.com

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com