How to Write
Secure Code?

About
The Course

Duration
24 Hours/3 Days

This course helps the developers to write more secure code by understating the best practice of writing the code, testing the code and a deep understanding of the hacker's tips and tricks to hack and crack the applications The course is based on the OWASP standards and the SSDLC (Secure Software Development Life Cycle) this will help the software developers, architects and testers to understand the whole life cycle, including the threat modeling, secure by design, secure coding, Static analysis security application, Dynamic analysis security application, Vulnerabilities finding and Secure the services configuration.

Course **outline**

01 Introduction to Secure Coding

02 Secure Coding Techniques

03 Threat modeling STRIDE

04 OWASP top 10 attacks

05 Extra attacks techniques

06 Preventing the attacks techniques

07 Encryption and Hashing Security

Course **outline**

EXPERTS

08   Session Management Security

09   Static analysis security application

10   Dynamic analysis security application

11   Network Security Requirements

12   Web Servers Security

13   Database Secuirty

14   API Secuirty

Course **outline**

Course **Objectives**

How the hacker exploits the vulnerabilities in Web Applications.

OWASP top 10 Attacks Standards .

Secure Coding Techniques.

Threat modeling STRIDE.

How to Prevent the attacks on the Code level.

Encryption and Hashing Security Techniques.

How to Secure the Session Management.

Course **Objectives**

Using the Static analysis security application Standards .

Using the Dynamic analysis security application.

Network Security Requirements .

Web Servers, API and Database Security.

The levels of the Application Security Verification Standards.

The Secure Development and Testing Guide.

Course
Prerequesite

Basics of software development life cycle, basics of coding standards

GET IN TOUCH

www.iExperts.co

info@iExperts.co

Follow @iExperts10 on :