FULLSTACK & SECURECODE PROGRAMMING

(Creating Best of Minds)

Professional Certificate in Full-Stack & Secure Code Programming

Course Code: IT_CT_I_0008/25

Duration: 40 Hours

Target Audience:

- Aspiring **Developers & Programmers**
  Ideal for beginners looking to build a solid foundation in full-stack development with a strong emphasis on secure coding practices.
- IT **Professionals**
  For those who want to enhance their development skills and integrate secure coding standards into their existing workflows.
- **Full-Stack Developers & Software Engineers**
  Perfect for developers looking to strengthen their expertise in building secure, scalable, and efficient applications across front-end and back-end technologies.

Program Objectives:

The primary objective of this course is to provide a comprehensive understanding of full-stack development, while embedding best practices for writing secure code. By the end of the course, participants will:

- Master the fundamentals of front-end and back-end web development.
- Learn to design and implement RESTful APIs.

- Understand how to secure web applications and avoid common security vulnerabilities.
- Be equipped with practical knowledge to implement testing, deployment, and continuous integration practices

Detailed Syllabus

Module 1-Introduction to Full-Stack Development and Secure Coding

- Basics of full-stack development: Front-end, back-end, and databases
- Importance of secure code programming in modern applications
- Overview of software development lifecycle (SDLC)

Module 2- Front-End Development Basics

- Introduction to HTML, CSS, and JavaScript
- Building responsive designs using frameworks (e.g., Bootstrap)
- Basics of front-end libraries like React or Angular

Module 3-Server-Side Programming Fundamentals

- Introduction to back-end programming languages (Node.js, Python, or PHP)
- Basics of server setup and handling requests/responses
- Connecting back-end to front-end

Module 4-Designing and Implementing RESTful APIs

- What are APIs and why are they important?
- Basics of creating RESTful APIs
- Working with HTTP methods and JSON data

Module 5- Secure Code Development Practices

- Principles of secure coding
- Avoiding common vulnerabilities (SQL Injection, XSS, etc.)
- Secure database access and input validation

Module 6-Testing and Quality Assurance

- Basics of testing in software development
- Tools and techniques for testing front-end and back-end
- Writing and running test cases

Module 7- Deployment and Continuous Integration/Continuous Deployment (CI/CD)

- Basics of deployment: Hosting, domains, and servers
- Overview of CI/CD pipelines
- Using tools like GitHub Actions, Jenkins, or GitLab for automation

Module 8-Web Application Security

- Importance of securing web applications
- Introduction to authentication and authorization
- Encryption basics (SSL/TLS, HTTPS)

Module 9-Addressing OWASP Top 10 Vulnerabilities

- Overview of OWASP Top 10 security risks
- Practical strategies to address each risk
- Tools for scanning and improving application security

Passing Criteria: Minimum 50% overall to pass the program.
Assignments: One assignment per module, designed to reinforce key concepts and practical skills.
Project: One **Capstone Project** to demonstrate applied knowledge and integrate learning from all modules.