Course Title: Secure Programming

Duration: Three (3) Days

Class Schedule: 9:00am to 5:00pm

Course Overview:

This course allows students to learn basic and advanced concepts in developing software that adhere to industry approved secure programming practices. Emphasis will be given to: understanding information security concepts, secure programming practices supported by OWASP (OWASP Top 10 Web Application Vulnerabilities), auditing techniques and tools, and common threats to applications and their mitigation strategies.

Topics:

1. Introduction to information Security
2. Secure Coding Principles
3. Introduction to Threat Modeling
4. Web Fundamentals
5. OWASP Top 10
   - Injection
   - Broken Authentication
   - Sensitive Data Exposure
   - XXE
   - Broken Access Control
   - Security Misconfiguration
• XSS
• Insecure Deserialization
• Using Vulnerable Components
• Insufficient Logging and Monitoring

6. Secure Coding Best Practices
• Handling credit card payments
• Authentication
• Password security
• 2FA
• Authorization
• Data Validation
• Session Management
• Cryptography / Encryption
• Auditing and Logging
• Error and Exception Handling
• Denial-of-Service
• Maintenance and Version Control
• Vulnerability Management