Secure Programming Workshop

Duration: 1 day

This comprehensive course equips developers and DevOps professionals with the knowledge and skills to build secure applications using the latest tools and practices. Participants will learn secure programming fundamentals, vulnerability assessment techniques, and advanced security features in GitHub and Azure DevOps. Topics include OWASP standards, CVE databases, secret management with Azure Key Vault, and the integration of Web Application Firewall (WAF) and Azure API Management for enhanced application security. Hands-on sessions will focus on dependency and code scanning, advanced pipeline tasks, and secure coding practices, ensuring attendees can implement robust security measures in real-world scenarios.

Objectives

- Understand the principles of secure programming and the importance of GitHub Advanced Security.
- Explore key secure programming standards, including OWASP, CVE, GHSA, NVD, CERT/CC, and CISA.
- Perform vulnerability audits using tools like NPM Audit and analyze .NET vulnerable packages.
- Leverage static code analysis to identify and mitigate security risks in source code.
- Implement GitHub Advanced Security features, including secret scanning, dependency scanning, and code scanning.
- Integrate Azure DevOps with GitHub Advanced Security for advanced pipeline security.
- Securely manage secrets, keys, and certificates using Azure Key Vault, with a focus on compliance and automation.
- Apply secure coding practices using Azure API Management and Web Application Firewall (WAF).

Outline

- Overview of Secure Programming
  - What is Secure Programming?
  - What is GitHub Advanced Security?
- Secure Programming
  - OWASP
  - CVE, GHSA, NVD, CERT/CC, CISA
  - NPM Audit
  - DotNet Vulnerable Packages
  - Static Code Analysis

- Azure DevOps and GitHub Advanced Security
  - Advanced Security Features
  - Integrations Features
  - Enable GitHub Advanced Security
- Advanced Security in Practice
  - Secret Scanning
  - Dependency Scanning
  - Code Scanning
  - Security Advisories
  - Alerts
- Azure Pipelines
  - Advanced Security Tasks
  - Dependency Scanning Tasks
  - Code Scanning Tasks
  - CodeQL Queries
- Azure Key Vault
  - Why use Key Vault
  - Securely Store Secrets, Keys, and Certificates
  - Integration with Azure & Azure DevOps
  - Security and Compliance
  - Manage Keys in Portal and CLI
  - Access Keys using C#
  - Key Rotation
- Web Application Firewall and Azure API Management
  - Overview of WAF
  - Overview of APIM
  - Integration
  - Security Configuration
  - Secure Coding Practices Leveraging APIM and WAF
- Conclusion
  - Summary of Key Concepts
  - Q&A
  - Further Resources and Next Steps