Attacking and Securing C# / ASP.Net Web Applications

Code: TT8320-N
Length: 4 days
URL: View Online

Discover the cutting-edge of cybersecurity and elevate your skills as a .NET developer with our comprehensive Bug Hunting and Application Security course. Designed specifically for experienced .NET developers, our .Net Secure Coding Camp | Attacking and Securing C# / ASP .Net Web (Core) Applications is an immersive, hands-on training program that delves deep into the world of bug hunting, ethical hacking, and web application security. Through real-world case studies, engaging labs, and expert instruction, you'll gain the knowledge and skills needed to fortify your applications, stay ahead of emerging threats, and protect your organization from costly security breaches.

Upon completing this course, you will not only acquire a profound understanding of application security concepts and best practices but also enhance your problem-solving, debugging, and overall software development prowess. Empowered with these new skills, you'll be well-prepared to identify, address, and prevent security threats in your .NET applications, ensuring a robust and secure digital environment for your organization.

NOTE: PCI Compliant Developer Training: This secure coding training addresses common coding vulnerabilities in software development processes. This training is used by one of the principal participants in the PCI DSS. Having passed multiple PCI audits, this course has been shown to meet the PCI requirements. The specifications of those training requirements are detailed in 6.5.1 through 6.5.7 on pages 60 through 65 of the PCI DSS Requirements 3.2.1 document.

Skills Gained

- Understanding Cybersecurity Concepts: Gain a solid foundation in cybersecurity principles, the evolving threat landscape, and the language of the industry to better identify and address security issues in .NET applications.
- Ethical Bug Hunting Techniques: Learn safe and appropriate methods for hunting bugs, ensuring responsible and ethical practices while working to uncover and address vulnerabilities in your applications.
- Web Application Security: Master the skills required to analyze, identify, and mitigate vulnerabilities in web applications, following best practices and guidelines from organizations such as OWASP, WASC, CWE, and CERT Secure Coding Standard.
- Utilizing Industry-Standard Tools and Frameworks: Acquire hands-on experience with widely used tools and frameworks, such as Visual Studio and .NET Cryptography, to effectively and efficiently secure your applications.
- Improved Problem Solving and Debugging: Enhance your ability to identify, analyze, and resolve security issues in your applications through real-world case studies, labs, and expert instruction.
- Defensive Programming Techniques: Learn and apply defensive programming techniques like securing trust boundaries, input validation, and proper exception handling to create more robust and secure .NET applications.
- Cryptography in .NET: Develop a deep understanding of .NET cryptographic services, hash algorithms, symmetric and asymmetric encryption, and gain hands-on experience with a cryptography wrapper for .NET.
- Secure Software Development Processes: Gain insight into secure software development processes, including the concept of "shifting left" and the implementation of secure design principles, enabling you to create safer and more reliable .NET applications.

Who Can Benefit

This is an intermediate level .Net programming course, designed for experienced .NET developers, software engineers, and architects who are seeking to enhance their knowledge and skills in application security, bug hunting, and secure software development. The course would also be well-suited for IT professionals, such as security analysts, security engineers, and DevOps team members, who are responsible for ensuring the security and integrity of web applications in their organizations.

Prerequisites

Incoming students should have skills equivalent to the topics in, or should have recently attended, this course as a pre-reqisuite:

- TTCN20483 Introduction to Programming in C# | Creating Apps in C# and .Net Core (20483)

Course Details

Session: Bug Hunting Foundation

- Why Hunt Bugs?
- Safe and Appropriate Bug Hunting/Hacking

Session: Scanning Web Applications

- Scanning Applications Overview

Session: Moving Forward from Hunting Bugs

- Removing Bugs

Session: Bug Stomping 101

- Recent, Relevant Incidents
- Finding Security Defects In Web Applications
- Unvalidated Data
- A01: Broken Access Control
- A02: Cryptographic Failures
- A03: Injection
- A04: Insecure Design
- A05: Security Misconfiguration

Session: Bug Stomping 102

- A06: Vulnerable and Outdated Components
- A07: Identification and Authentication Failures
- A08: Software and Data Integrity Failures
- A09: Security Logging and Monitoring Failures
- A10: Server Side Request Forgeries (SSRF)

Session: Moving Forward with Application Security

- Applications: What Next?
- .NET Issues and Best Practices

Session: Exploring .Net Cryptography

- .Net Cryptographic Services

Schedule (as of 3)

Date	Location	
Apr 29, 2024 – May 2, 2024	Virtual	Enroll
Jun 24, 2024 – Jun 27, 2024	Virtual	Enroll
Aug 19, 2024 – Aug 22, 2024	Virtual	Enroll
Oct 15, 2024 – Oct 18, 2024	Virtual	Enroll
Dec 16, 2024 – Dec 19, 2024	Virtual	Enroll
