.Net Secure Coding Camp | Attacking and Securing .Net Web Apps (for .Net Core / Latest Edition)

Duration: *4 Day(s)*

Course Overview

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.

Review this course online at https://www.alta3.com/courses/TT8320-N

Objectives

- Understand cybersecurity concepts and principles relevant to .NET applications.
- Implement ethical bug hunting techniques and web application security best practices.
- Utilize industry-standard tools and frameworks to secure .NET applications.
- Enhance problem-solving skills for identifying and mitigating security threats.

Who Should Attend

- Experienced .NET Developers
- Software Engineers
- Application Architects
- IT Security Analysts
- DevOps Team Members

Prerequisites

Take Before: 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)
```

TT8120 Web Application Security Essentials: Understanding OWASP Risks and Fixes That Really Work TT8700 Securing Databases: Practical Database Security Skills for Safer Systems TTAI2835 AI & Web Application Security: A Practical Guide to Risks & Responses TTCN20483 Programming in C# / Creating Apps in C# and .Net Core TTCN20486 Developing ASP.NET Core 9.x MVC Web Applications (Intermediate C#)

Course Outline

Session: Bug Hunting Foundation

1. Why Hunt Bugs?
2. Safe and Appropriate Bug Hunting/Hacking

Session: Scanning Web Applications

3. Scanning Applications Overview

Session: Moving Forward from Hunting Bugs

4. Removing Bugs

Session: Bug Stomping 101

5. Unvalidated Data
6. Broken Access Control
7. Cryptographic Failures
8. Injection
9. Insecure Design
10. Security Misconfiguration

Session: Bug Stomping 102

11. Vulnerable and Outdated Components
12. Identification and Authentication Failures
13. Software and Data Integrity Failures

14. Security Logging and Monitoring Failures
15. Server Side Request Forgeries (SSRF)

Session: Moving Forward with Application Security

16. Applications: What Next?
17. .NET Issues and Best Practices

Session: Exploring .Net Cryptography

18. .Net Cryptographic Services