.Net Secure Coding Camp | Attacking and Securing .Net Web Apps (for .Net Core / Latest Edition) (TT8320-N)

Category: Software Development & Programming | **Vendor:** Trivera Tech

Duration: 32.00 hours (4 days) **26.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

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.

About This Course

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.

Who Should Attend

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.

Learning Outcomes

Upon successful completion of this course, participants will be able to:

With a strong focus on real-world case studies and labs, this course will sharpen your ability to identify, analyze, and resolve security issues in their applications.
Working in a lab-intensive, hands-on coding environment students will explore:
- 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.

If your team requires different topics or tools, additional skills or custom approach, this course may be further adjusted to accommodate. Our team will collaborate with you to understand your needs and will target the course to focus on your specific learning objectives and goals.

Detailed Course Outline

Why Hunt Bugs

The Language of Cybersecurity

The Changing Cybersecurity Landscape

AppSec Dissection of SolarWinds

The Human Perimeter

First Axiom in Web Application Security Analysis

First Axiom in Addressing ALL Security Concerns

Safe and Appropriate Bug Hunting/Hacking

Warning to All Bug Hunters

Working Ethically

Respecting Privacy

Bug/Defect Notification

Bug Hunting Pitfalls

Session: Scanning Web Applications

Scanning Applications Overview

Scanning Beyond the Applications

Fingerprinting

Vulnerability Scanning: Hunting for Bugs

Reconnaissance Goals

Data Collection Techniques

Fingerprinting the Environment

Enumerating the Web Application

Session: Moving Forward from Hunting Bugs

Removing Bugs

Open Web Application Security Project (OWASP)

OWASP Top Ten Overview

Web Application Security Consortium (WASC)

Common Weaknesses Enumeration (CWE)

CERT Secure Coding Standard

Microsoft Security Response Center

Software-Specific Threat Intelligence

Session: Bug Stomping 101

Unvalidated Data

CWE-787, 125, 20, 416, 434, 190, 476 and 119

Potential Consequences

Defining and Defending Trust Boundaries

Rigorous, Positive Specifications

Allow Listing vs Deny Listing

Challenges: Free-Form Text, Email Addresses, and Uploaded Files

A01: Broken Access Control

CWE-22, 352, 862, 276, and 732

Elevation of Privileges

Insufficient Flow Control

Unprotected URL/Resource Access/Forceful Browsing

Metadata Manipulation (Session Cookies and JWTs)

Understanding and Defending Against CSRF

CORS Misconfiguration Issues

A02: Cryptographic Failures

CWE-200

Identifying Protection Needs

Evolving Privacy Considerations

Options for Protecting Data

Transport/Message Level Security

Weak Cryptographic Processing

Keys and Key Management

NIST Recommendations

A03: Injection

CWE-79, 78, 89, and 77

Pattern for All Injection Flaws

Misconceptions With SQL Injection Defenses

Drill Down on Stored Procedures

Other Forms of Server-Side Injection

Minimizing Server-Side Injection Flaws

Client-side Injection: XSS

Persistent, Reflective, and DOM-Based XSS

Best Practices for Untrusted Data

A04: Insecure Design

Secure Software Development Processes

Shifting Left

Principles for Securing All Designs

Leveraging Common AppSec Practices and Control

Paralysis by Analysis

Actionable Application Security

Additional Tools for the Toolbox

A05: Security Misconfiguration

System Hardening: IA Mitigation

Risks with Internet-Connected Resources

Minimalist Configurations

Application Allow Listing

Secure Baseline

Segmentation with Containers and Cloud

CWE-611

Safe XML Processing

Session: Bug Stomping 102

A06: Vulnerable and Outdated Components

Problems with Vulnerable Components

Software Inventory

Managing Updates: Balancing Risk and Timeliness

Virtual Patching

Dissection of Ongoing Exploits

A07: Identification and Authentication Failures

CWE-306, 287, 798 and 522

Quality and Protection of Authentication Data

Anti-Automation Defenses

Multifactor Authentication

Proper Hashing of Passwords

Handling Passwords on Server Side

A08: Software and Data Integrity Failures

CWE-502

Software Integrity Issues and Defenses

Using Trusted Repositories

CI/CD Pipeline Issues

Protecting Software Development Resources

Serialization/Deserialization

A09: Security Logging and Monitoring Failures

Detecting Threats and Active Attacks

Best Practices for Logging and Logs

Safe Logging in Support of Forensics

A10: Server Side Request Forgeries (SSRF)

CWE-918

Understanding SSRF

Remote Resource Access Scenarios

Complexity of Cloud Services

SSRF Defense in Depth

Positive Allow Lists

Session: Moving Forward with Application Security

Applications: What Next

Common Vulnerabilities and Exposures

CWE Top 25 Most Dangerous SW Errors

Strength Training: Project Teams/Developers

Strength Training: IT Organizations

.NET Issues and Best Practices

Managed Code and Buffer Overflows

.Net Permissions

ActiveX Controls

Proper Exception Handling

Session: Exploring .Net Cryptography

.Net Cryptographic Services

The role of cryptographic services

Hash algorithms and hash codes

Encrypting data symmetrically

Encrypting data asymmetrically

Additional Course Details

Nexus Humans .Net Secure Coding Camp | Attacking and Securing .Net Web Apps (for .Net Core / Latest Edition) (TT8320-N) training program is a workshop that presents an invigorating mix of sessions, lessons, and masterclasses meticulously crafted to propel your learning expedition forward. This immersive bootcamp-style experience boasts interactive lectures, hands-on labs, and collaborative hackathons, all strategically designed to fortify fundamental concepts.

Guided by seasoned coaches, each session offers priceless insights and practical skills crucial for honing your expertise. Whether you're stepping into the realm of professional skills or a seasoned professional, this comprehensive course ensures you're equipped with the knowledge and prowess necessary for success.

While we feel this is the best course for the .Net Secure Coding Camp | Attacking and Securing .Net Web Apps (for .Net Core / Latest Edition) (TT8320-N) course and one of our Top 10 we encourage you to read the course outline to make sure it is the right content for you.

Additionally, private sessions, closed classes or dedicated events are available both live online and at our training centres in Dublin and London, as well as at your offices anywhere in the UK, Ireland or across EMEA.

Frequently Asked Questions

Q: What delivery options are available for .Net Secure Coding Camp | Attacking and Securing .Net Web Apps (for .Net Core / Latest Edition) (TT8320-N)?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 4-day .Net Secure Coding Camp | Attacking and Securing .Net Web Apps (for .Net Core / Latest Edition) (TT8320-N) course provides up to 26.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the .Net Secure Coding Camp | Attacking and Securing .Net Web Apps (for .Net Core / Latest Edition) (TT8320-N) training?

The training takes place over 4 day(s), with each day lasting approximately 32.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for .Net Secure Coding Camp | Attacking and Securing .Net Web Apps (for .Net Core / Latest Edition) (TT8320-N)?

Yes, we provide corporate training, dedicated training, and closed classes for .Net Secure Coding Camp | Attacking and Securing .Net Web Apps (for .Net Core / Latest Edition) (TT8320-N). Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: C# / .Net; Application Security

---

Q: Why choose Nexus Human for .Net Secure Coding Camp | Attacking and Securing .Net Web Apps (for .Net Core / Latest Edition) (TT8320-N)?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your .Net Secure Coding Camp | Attacking and Securing .Net Web Apps (for .Net Core / Latest Edition) (TT8320-N) training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)