Cybersecurity Skills Journey

Java Secure Coding Camp | Attacking and Securing Java Web Applications (TT8320-J)

Learn how to fortify your applications, stay ahead of emerging threats, and protect your organization from costly security breaches

Course Snapshot

- **Course: Java Secure Coding Camp | Attacking and Securing Java Web Applications (TT8320-J)**
- **Duration:** 4 days
- **Audience & Skill-Level:** This is an **intermediate level** secure programming course, designed for experienced Java developers who wish to get up and running on developing well defended software applications.
- **Language:** Coding examples use Java and Eclipse IDE. Visual Studio and .Net edition available. Please inquire for details.
- **Format / Hands-on:** This course combines engaging instructor-led presentations and practical demonstrations with hands-on programming exercises, challenge labs, use case exploration and engaging group activities. Student machines are required.
- **Flexible Delivery Options**: This course can be delivered for your team or organization **online-live (virtual)**, **onsite in-person, self-paced** or across our immersive **blended learning experience platform (LXP).**
- **Public Schedule**: This course is currently available on our Public Open Enrollment Schedule.
- **Customizable**: We're flexible! This course agenda, topics, labs, hours and delivery modalities can be adjusted to target your specific training skills objectives, tools and learning goals. Please ask for details.

Overview

Discover the cutting-edge of cybersecurity and elevate your skills as a Java Web developer with our comprehensive Bug Hunting and Application Security course. Designed specifically for experienced Java web developers, our **Java Secure Coding Camp | Attacking and Securing Java Web 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 Java Web 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.

Learning Objectives

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 you'll:

- Master the fundamentals of secure coding and understand the stages of an exploit, focusing on defensive techniques.
- Establish foundational axioms for analyzing and addressing security in web applications, guiding your approach through this course and future endeavors.
- Learn responsible ethical hacking methods, including defect detection, bug reporting, and ensuring all activities are executed in a safe environment.
- Recognize and sidestep frequent pitfalls in vulnerability testing and bug hunting, leveraging best practices.
- Gain insight into the significance of multilayered defense strategies, evaluating the effectiveness of layered defenses through hands-on testing.
- Identify and handle untrusted data sources, understanding the associated risks like denial of service, cross-site scripting,

and injections.
- Dive deep into authentication and authorization, pinpointing vulnerabilities and learning how to fortify these crucial security areas.
- Understand and counteract web-specific threats such as Cross-Site Scripting (XSS) and Injection attacks, mastering both offensive and defensive techniques.
- Examine risk factors in XML processing, file and software uploads, and deserialization, along with strategies for risk mitigation.
- Get acquainted with key security tools, from code scanners to web application firewalls, while also exploring server and infrastructure hardening techniques.

If your team requires different topics or tools, additional skills or custom approach, this course may be further adjusted to accommodate.

Audience

This is an **intermediate level** Java programming course, designed for experienced Java Web 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.

Pre-Requisites

Practical hands-on Java web development experience. This is java coding class that requires intermediate Java developer skills to complete the lab work.

Related Courses

The following are a subset of our related Cybersecurity courses. Please see our website catalog for the complete list of courses and learning paths.

- TT8120 Introduction to Securing Web Applications (2 days)
- TT8150 2021 OWASP Top Ten Deep Dive (2 days)
- TT8320-J Java secure Coding Camp | Attacking and Securing Java Web Applications (4 days)
- TT8700 Securing Databases (2 days)
- TT8800 Information Assurance (STIG) Overview (2 days)
- TTAI2810 Machine Learning Operations (MLOps) and AI Security Boot Camp (3 days)
- TTAI2820 Mastering AI Security Boot Camp (3 days)
- TTAI2830 AI Security: Applying AI to the OWASP Top Ten (2 days)
- TTAI2835 AI Secure Programming for Web Applications / Technical Overview (1 day)

Enhanced Learning Services: Please also ask about our robust Learning Experience Platform (LXP), Skills Assessment & Skills Prep Services, Skills Immersion Programs & Camps, Coaching and Mentoring Services and Extended Learning Support programs.

Course Topics / Agenda

Bug Hunting Foundation

1. 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

2. Safe and Appropriate Bug Hunting/Hacking
- Warning to All Bug Hunters
- Working Ethically
- Respecting Privacy
- Bug/Defect Notification
- Bug Hunting Pitfalls

Moving Forward From Hunting Bugs

3. 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

Bug Stomping 101

4. 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

5. 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

6. 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

7. 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

8. 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

9. 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

Bug Stomping 102

10. A06: Vulnerable and Outdated Components
- Problems with Vulnerable Components
- Software Inventory
- Managing Updates: Balancing Risk and Timeliness
- Virtual Patching
- Dissection of Ongoing Exploits

11. 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

12. 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

13. A09: Security Logging and Monitoring Failures
- Detecting Threats and Active Attacks
- Best Practices for Logging and Logs
- Safe Logging in Support of Forensics

14. 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

Moving Forward with Application Security

15. Applications: What Next?
- Common Vulnerabilities and Exposures
- CWE Top 25 Most Dangerous SW Errors
- Strength Training: Project Teams/Developers
- Strength Training: IT Organizations

16. Secure Development Lifecycle (SDL)

17. SDL Overview
- Attack Phases: Offensive Actions and Defensive Controls
- Secure Software Development Processes
- Shifting Left
- Actionable Items Moving Forward

18. SDL In Action
- Risk Escalators
- Risk Escalator Mitigation

- SDL Phases
- Actions for each SDL Phase
- SDL Best Practices

Next Steps

- Your Secure Coding Action Plan
- Key Resources

Setup Made Simple! Learning Experience Platform (LXP)

All applicable course software, digital courseware files or course notes, labs, data sets and solutions, live coaching support channels, CodeCoach.AI anytime tutor access, and rich extended learning and post training resources are provided for you in our "easy access, single source, no install required" online **Learning Experience Platform (LXP),** remote lab and content environment. Access periods vary by course. We'll collaborate with you to ensure your team is set up and ready to go well in advance of the class. Please inquire about set up details and options for your specific course of interest.

For More Information

For more information about our training services (instructor-led, self-paced or blended), collaborative coaching services, robust Learning Experience Platform (LXP), Career Experiences, public course schedule, partner programs, courseware licensing options or to see our complete list of course offerings, solutions and special offers, please visit us at **www.triveratech.com**, email **Info@triveratech.com** or call us toll free at **844-475-4559.** Our pricing and services are always satisfaction guaranteed.