Attacking and Securing Java / JEE Web Applications (TT8320-J)

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

This lab-intensive course provides hands-on Java / JEE security training that offers a unique look at Java application security. Beginning with penetration testing and hunting for bugs in Java web applications, you embrace best practices for defensively coding web applications, covering all the OWASP Top Ten as well as several additional prominent vulnerabilities. You will repeatedly attack and then defend various assets associated with fully functional web applications and services, allowing you to experience the mechanics of how to secure JEE web applications in the most practical of terms.

About This Course

This lab-intensive course provides hands-on Java / JEE security training that offers a unique look at Java application security. Beginning with penetration testing and hunting for bugs in Java web applications, you embrace best practices for defensively coding web applications, covering all the OWASP Top Ten as well as several additional prominent vulnerabilities. You will repeatedly attack and then defend various assets associated with fully functional web applications and services, allowing you to experience the mechanics of how to secure JEE web applications in the most practical of terms.

Who Should Attend

This is an intermediate -level programming course, designed for experienced Java developers who wish to get up and running on developing well defended software applications. Familiarity with Java and JEE is required and real world programming experience is highly recommended. Ideally students should have approximately 6 months to a year of Java and JEE working knowledge.

Learning Outcomes

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

Students who attend Attacking and Securing Java Web Applications will leave the course armed with the skills required to recognize actual and potential software vulnerabilities and implement defenses for those vulnerabilities. This course begins by developing the skills required to fingerprint a web application and then scan it for vulnerabilities and bugs. Practical labs using current tools and techniques provide students with the experience needed to begin testing their own applications. Students also gain a deeper understanding of how attackers probe applications to understand the runtime environment as well as find potential weaknesses. This course the introduces developers to the most common security vulnerabilities faced by web applications today. Each vulnerability is examined from a Java/JEE perspective through a process of describing the threat and attack mechanisms, recognizing associated vulnerabilities, and, finally, designing, implementing, and testing effective defenses.

Practical labs reinforce these concepts with real vulnerabilities and attacks. Students are then challenged to design and implement the layered defenses they will need in defending their own applications. There is an emphasis on the underlying vulnerability patterns since the technologies, use cases, and methods of attack as constantly changing. The patterns remain the same through all the change and flux.

This “skills-centric” course is about 50% hands-on lab and 50% lecture, designed to train attendees in secure web application development, coding and design, coupling the most current, effective techniques with the soundest industry practices. Our engaging instructors and mentors are highly experienced practitioners who bring years of current 'on-the-job' experience into every classroom.

Detailed Course Outline

Bug Hunting Foundation

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

Scanning Web Applications

- Scanning Applications Overview

Moving Forward from Hunting Bugs

- Removing Bugs

Foundation for Securing Applications

- Principles of Information Security

Bug Stomping 101

- Unvalidated Data
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control

Bug Stomping 102

- Security Misconfiguration
- Cross Site Scripting (XSS)
- Deserialization/Vulnerable Components
- Insufficient Logging and Monitoring
- Spoofing, CSRF, and Redirects

Moving Forward with Application Security

- Applications: What Next
- Making Application Security Real

Additional Course Details

Nexus Humans Attacking and Securing Java / JEE Web Applications (TT8320-J) 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 Attacking and Securing Java / JEE Web Applications (TT8320-J) 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 Attacking and Securing Java / JEE Web Applications (TT8320-J)?

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 Attacking and Securing Java / JEE Web Applications (TT8320-J) 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 Attacking and Securing Java / JEE Web Applications (TT8320-J) 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 Attacking and Securing Java / JEE Web Applications (TT8320-J)?

Yes, we provide corporate training, dedicated training, and closed classes for Attacking and Securing Java / JEE Web Applications (TT8320-J). 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: Why choose Nexus Human for Attacking and Securing Java / JEE Web Applications (TT8320-J)?

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 Attacking and Securing Java / JEE Web Applications (TT8320-J) 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)