Secure Web Applications / Seminar | Covering OWASP Top Ten, Web Services, Rich Interfaces & More (TT8120)

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

Duration: 16.00 hours (2 days) **13.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

Security experts agree that the least effective approach to security is ''penetrate and patch''. It is far more effective to ''bake'' security into an application throughout its lifecycle. After spending significant time examining a poorly designed (from a security perspective) web application, developers are ready to learn how to build secure web applications starting at project inception. The final portion of this course builds on the previously learned mechanics for building defenses by exploring how design and analysis can be used to build stronger applications from the beginning of the software lifecycle. The Secure Web Application Development Overview is geared for web developers and technical stakeholders who need to produce secure web applications, integrating security measures into the development process from requirements to deployment and maintenance. This overview-level course explores core concepts and challenges in web application security, showcasing current, real world examples that illustrate the potential consequences of not following these best practices. This course is also PCI Compliant.

About This Course

Security experts agree that the least effective approach to security is ''penetrate and patch''. It is far more effective to ''bake'' security into an application throughout its lifecycle. After spending significant time examining a poorly designed (from a security perspective) web application, developers are ready to learn how to build secure web applications starting at project inception. The final portion of this course builds on the previously learned mechanics for building defenses by exploring how design and analysis can be used to build stronger applications from the beginning of the software lifecycle. The Secure Web Application Development Overview is geared for web developers and technical stakeholders who need to produce secure web applications, integrating security measures into the development process from requirements to deployment and maintenance. This overview-level course explores core concepts and challenges in web application security, showcasing current, real world examples that illustrate the potential consequences of not following these best practices. This course is also PCI Compliant.

Who Should Attend

This is an introductory-level course designed for technical application project stakeholders who wish to get up and running on developing well defended web applications. Real-world programming experience is highly recommended for code reviews.

Prerequisites & Entry Requirements

General Prerequisites:

This is not a hands-on course, however its helpful if you have:

- Basic understanding of web development and web architecture
- Some familiarity with basic programming concepts.
- Basic understanding of web security concepts.

Learning Outcomes

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

Students who attend Secure Web Application Development will gain an understanding of how to recognize actual and potential software vulnerabilities, implement defenses for those vulnerabilities, and test those defenses for sufficiency. This course introduces most common security vulnerabilities faced by web applications today. Each vulnerability is examined from a coding perspective through a process of describing the threat and attack mechanisms, recognizing associated vulnerabilities, and, finally, designing, implementing, and testing effective defenses.
Guided by our application security expert, attendees will explore how to:
Ensure that any hacking and bug hunting is performed in a safe and appropriate manner
Identify defect/bug reporting mechanisms within their organizations
Setup and use various tools and techniques to determine a web application’s operational environment
Setup and use various tools and techniques to enumerate all aspects of a web application
Setup and use various tools and techniques to scan a web application for vulnerabilities
Work with specific tools for targeted vulnerabilities
Avoid common mistakes that are made in bug hunting and vulnerability testing
Understand the concepts and terminology behind defensive, secure coding including the phases and goals of a typical exploit
Develop an appreciation for the need and value of a multilayered defense in depth
Understand potential sources for untrusted data
Understand the consequences for not properly handling untrusted data such as denial of service, cross-site scripting, and injections
To test web applications with various attack techniques to determine the existence of and effectiveness of layered defenses
Prevent and defend the many potential vulnerabilities associated with untrusted data
Understand the vulnerabilities of associated with authentication and authorization
Detect, attack, and implement defenses for authentication and authorization functionality and services
Understand the dangers and mechanisms behind Cross-Site Scripting (XSS) and Injection attacks
Detect, attack, and implement defenses against XSS and Injection attacks
Understand the risks associated with XML processing, file uploads, and server-side interpreters and how to best eliminate or mitigate those risks
Learn the strengths, limitations, and use for tools such as code scanners, dynamic scanners, and web

application firewalls (WAFs)

Detailed Course Outline

Introduction: Misconceptions

- Security: The Complete Picture
- Seven Deadly Assumptions
- Anthem, Sony, Target, Heartland, and TJX Debriefs
- Causes of Data Breaches
- Meaning of Being Compliant
- Verizons 2015 Data Breach Report
- 2015 PCI Compliance Report

Lesson: Security Concepts

- Motivations: Costs and Standards
- Open Web Application Security Project
- Web Application Security Consortium
- CERT Secure Coding Standards
- Assets are the Targets
- Security Activities Cost Resources
- Threat Modeling
- System/Trust Boundaries

Lesson: Principles of Information Security

- Security Is a Lifecycle Issue
- Minimize Attack Surface Area
- Layers of Defense: Tenacious D
- Compartmentalize
- Consider All Application States
- Do NOT Trust the Untrusted

Lesson: Unvalidated Input

- Buffer Overflows
- Integer Arithmetic Vulnerabilities
- Unvalidated Input: From the Web
- Defending Trust Boundaries
- Whitelisting vs Blacklisting

Lesson: Overview of Regular Expressions

- Regular Expressions
- Working With Regexes in Java
- Applying Regular Expressions

Lesson: Broken Access Control

- Access Control Issues
- Excessive Privileges
- Insufficient Flow Control
- Unprotected URL/Resource Access
- Examples of Shabby Access Control
- Session and Session Management

Lesson: Broken Authentication

- Broken Quality/DoS
- Authentication Data
- Username/Password Protection
- Exploits Magnify Importance
- Handling Passwords on Server Side
- Single Sign-on (SSO)

Lesson: Cross Site Scripting (XSS)

- Persistent XSS
- Reflective XSS
- Best Practices for Untrusted Data

Lesson: Injection

- Injection Flaws
- SQL Injection Attacks Evolve
- Drill Down on Stored Procedures
- Other Forms of Injection
- Minimizing Injection Flaws

Lesson: Error Handling and Information Leakage

- Fingerprinting a Web Site
- Error-Handling Issues
- Logging In Support of Forensics
- Solving DLP Challenges

Lesson: Insecure Data Handling

- Protecting Data Can Mitigate Impact
- In-Memory Data Handling
- Secure Pipes
- Failures in the SSL Framework Are Appearing

Lesson: Insecure Configuration Management

- System Hardening: IA Mitigation
- Application Whitelisting
- Least Privileges
- Anti-Exploitation
- Secure Baseline

Lesson: Direct Object Access

- Dynamic Loading
- Direct Object References

Lesson: Spoofing and Redirects

- Name Resolution Vulnerabilities
- Fake Certs and Mobile Apps
- Targeted Spoofing Attacks
- Cross Site Request Forgeries (CSRF)
- CSRF Defenses are Entirely Server-Side
- Safe Redirects and Forwards

Lesson: Understanding Whats Important

- Common Vulnerabilities and Exposures
- OWASP Top Ten for 2013
- CWE/SANS Top 25 Most Dangerous SW Errors
- Monster Mitigations
- Strength Training: Project Teams/Developers
- Strength Training: IT Organizations

Lesson: Defending XML

- XML Signature
- XML Encryption
- XML Attacks: Structure
- XML Attacks: Injection
- Safe XML Processing

Lesson: Defending Web Services

- Web Service Security Exposures
- When Transport-Level Alone is NOT Enough
- Message-Level Security
- WS-Security Roadmap
- XWSS Provides Many Functions
- Web Service Attacks
- Web Service Appliance/Gateways

Lesson: Defending Rich Interfaces and REST

- How Attackers See Rich Interfaces
- Attack Surface Changes When Moving to Rich Interfaces
- Bridging and its Potential Problems
- Three Basic Tenets for Safe Rich Interfaces
- OWASP REST Security Recommendations

Lesson: SDL Process Overview

- Software Security Axioms
- Security Lifecycle Phases

Lesson: Applying Processes and Practices

- Awareness
- Application Assessments
- Security Requirements
- Secure Development Practices
- Security Architecture/Design Review
- Security Code Review
- Configuration Management and Deployment
- Vulnerability Remediation Procedures

Lesson: Risk Analysis

- Threat Modeling Process
- 1. Identify Security Objectives
- 2. Describe the System
- 3. List Assets
- 4. Define System/Trust Boundaries
- 5. List and Rank Threats
- 6. List Defenses and Countermeasures

Lesson: Testing Tools and Processes

- Security Testing Principles
- Black Box Analyzers
- Static Code Analyzers
- Criteria for Selecting Static Analyzers

Lesson: Testing Practices

- OWASP Web App Penetration Testing
- Authentication Testing
- Session Management Testing
- Data Validation Testing
- Denial of Service Testing
- Web Services Testing
- Ajax Testing

, Lesson: Why Hunt Bugs

The Language of Cybersecurity

The Changing Cybersecurity Landscape

AppSec Dissection of SolarWinds

The Human Perimeter

Interpreting the Verizon Data Breach Investigation Report

First Axiom in Web Application Security Analysis

First Axiom in Addressing ALL Security Concerns

Lab: Case Study in Failure

Lesson: Safe and Appropriate Bug Hunting/Hacking

Working Ethically

Respecting Privacy

Bug/Defect Notification

Bug Bounty Programs

Bug Hunting Mistakes to Avoid

Session: Moving Forward From Hunting Bugs

Lesson: Removing Bugs

Open Web Application Security Project (OWASP

OWASP Top Ten Overview

Web Application Security Consortium (WASC)

CERT Secure Coding Standards

Microsoft Security Response Center

Software-Specific Threat Intelligence

Session: Foundation for Securing Web Applications

Lesson: Principles of Information Security

Security Is a Lifecycle Issue

Minimize Attack Surface Area

Layers of Defense: Tenacious D

Compartmentalize

Consider All Application States

Do NOT Trust the Untrusted

AppSec Dissection of the Verkada Exploit

Session: Bug Stomping 101

Lesson: Unvalidated Data

Buffer Overflows

Integer Arithmetic Vulnerabilities

Defining and Defending Trust Boundaries

Rigorous., Positive Specifications

Whitelisting vs Blacklisting

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

Lesson: A01: Broken Access Control

Elevation of Privileges

Insufficient Flow Control

Unprotected URL/Resource Access/Forceful Browsing

Metadata Manipulation (JWTs)

CORS Misconfiguration Issues

Cross Site Request Forgeries (CSRF)

CSRF Defenses

Lab: Spotlight: Verizon

Lesson: A02: Cryptographic Failures

Identifying Protection Needs

Evolving Privacy Considerations

Options for Protecting Data

Transport/Message Level Security

Weak Cryptographic Processing

Keys and Key Management

NIST Recommendations

Lesson: A03: Injection

Injection Flaws

SQL Injection Attacks Evolve

Drill Down on Stored Procedures

Other Forms of Server-Side Injection

Minimizing Injection Flaws

Client-side Injection: XSS

Persistent, Reflective, and DOM-Based XSS

Best Practices for Untrusted Data

Lesson: A04: Insecure Design

Secure Software Development Processes

Shifting Left

Cost of Continually Reinventing

Leveraging Common AppSec Practices and Control

Paralysis by Analysis

Actionable Application Security

Additional Tools for the Toolbox

Lab: Actionable AppSec

Lesson: A05: Security Misconfiguration

System Hardening

Risks with Internet-Connected Resources (Servers to Cloud)

Minimalist Configurations

Application Whitelisting

Secure Baseline

Segmentation with Containers and Cloud

Lab: Configuration Guidance

Resolution of External References

Safe XML Processing

Session: Bug Stomping 102

Lesson: A06: Vulnerable and Outdated Components

Vulnerable Components

Software Inventory

Managing Updates: Balancing Risk and Timeliness

AppSec Dissection of Ongoing Microsoft Exchange Exploits

Lab: Spotlight: Equifax

Lesson: A07: Identification and Authentication Failures

Quality and Protection of Authentication Data

Proper hashing of passwords

Handling Passwords on Server Side

Session Management

HttpOnly and Security Headers

Lesson: A08: Software and Data Integrity Failures

Serialization/Deserialization

Issues with Consuming Vulnerable Software

Using Trusted Repositories

CI/CD Pipeline Issues

Protecting Software Development Resources

Lesson: A09: Security Logging and Monitoring Failures

Detecting Threats and Active Attacks

Best Practices for Determining What to Log

Safe Logging in Support of Forensics

Lab: Auditing and Logging Guidance

Lesson: A10: Server-Side Request Forgery (SSRF)

Understanding SSRF

Remote Resource Access Scenarios

Complexity of Cloud Services

SSRF Defense in Depth

Positive Allow Lists

Session: Moving Forward

Lesson: Applications: What Next

Common Vulnerabilities and Exposures

CWE/SANS Top 25 Most Dangerous SW Errors

Strength Training: Project Teams/Developers

Strength Training: IT Organizations

Lab: Spotlight: Capital One

Optional / Bonus Content

Bonus Chapter: Leveraging AI in Web Application Security Development

Introduction to AI in Web Application Security

AI-Powered Threat Detection

AI for Secure Coding

AI in Authentication and Access Control

AI in Incident Response

Challenges and Ethical Considerations in AI for Security

Additional Course Details

Nexus Humans Secure Web Applications / Seminar | Covering OWASP Top Ten, Web Services, Rich Interfaces & More (TT8120) 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 Secure Web Applications / Seminar | Covering OWASP Top Ten, Web Services, Rich Interfaces & More (TT8120) 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 Secure Web Applications / Seminar | Covering OWASP Top Ten, Web Services, Rich Interfaces & More (TT8120)?

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 2-day Secure Web Applications / Seminar | Covering OWASP Top Ten, Web Services, Rich Interfaces & More (TT8120) course provides up to 13.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Secure Web Applications / Seminar | Covering OWASP Top Ten, Web Services, Rich Interfaces & More (TT8120) training?

The training takes place over 2 day(s), with each day lasting approximately 16.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Secure Web Applications / Seminar | Covering OWASP Top Ten, Web Services, Rich Interfaces & More (TT8120)?

Yes, we provide corporate training, dedicated training, and closed classes for Secure Web Applications / Seminar | Covering OWASP Top Ten, Web Services, Rich Interfaces & More (TT8120). 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: OWASP; Security

Q: Why choose Nexus Human for Secure Web Applications / Seminar | Covering OWASP Top Ten, Web Services, Rich Interfaces & More (TT8120)?

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 Secure Web Applications / Seminar | Covering OWASP Top Ten, Web Services, Rich Interfaces & More (TT8120) 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)