Cybersecurity Learning Journey

Securing Web Applications | 2021 OWASP Top Ten and Beyond (TT8120)

Explore Common Web Application Vulnerabilities, How to Implement and Test Attack Defenses & More

Course Snapshot

- **Course: Securing Web Applications | OWASP Top Ten and Beyond (TT8120)**
- **Duration:** 2 days
- **Audience:** This is an **overview-level**, **language neutral** course ideally suited for web developers, software engineers, system administrators, project managers and other technical or security stakeholders who are involved in the design, development, or maintenance of web applications.
- **Format**: This is a lecture style course that combines engaging presentation with lab activities, critical demonstrations and meaningful discussions. Activities and labs are group and discussion based, and not programming based.
- **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**: 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.

From ransomware and constant data breaches to state-sponsored attacks, we are under constant and increasing pressure. Retailers, financial institutions, government agencies, high-tech companies, and many others are paying the price for poor application security - financial losses and eroding trust. The developer community must take ownership of these problems and change our perspective of defensive measures and how we design, develop and maintain software applications.

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.***

Overview

Embark on a comprehensive journey into web application security with our two-day seminar-style course, "**Securing Web Applications / 2021 OWASP Top Ten and Beyond**". Designed for web developers and technical stakeholders, this course equips you with the foundational concepts of defensive and secure coding. You'll learn to move beyond the "penetrate and patch" approach, integrating security into your applications from the get-go, leading to robust, resilient software.

Throughout the engaging course, you'll delve into the best practices for defensively coding web applications, addressing the 2021 OWASP Top Ten and several other vital vulnerabilities. Learn from the mistakes of the past as we dissect real-world examples of poorly designed web applications, providing you with stark illustrations of the potential fallout when security best practices are not adhered to. Our security expert will guide you on the process of integrating security measures into your development lifecycle, ensuring you build secure applications from the ground up.

The course goes beyond theory, offering practical skills directly applicable to your work: ethical hacking, bug hunting, detection, and mitigation of threats to authentication and authorization functionalities. You'll understand the mechanics and threats of Cross-Site Scripting (XSS) and Injection attacks and comprehend the risks and mitigation strategies associated with XML processing, software uploads, and deserialization.

Unlike many courses that are self-guided or delivered by less experienced trainers, this course is led by a seasoned web application security expert who shares practical insights, best practices, and real-life experiences, adding invaluable depth to your learning journey. You'll exit this course well-versed in these technologies, equipped with practical skills, plus the ability to effectively communicate and collaborate in your professional environment. With engaging expert-led lectures, interactive discussions, and insightful demos, this course will provide you with the skills required to begin your journey to building safer, stronger web applications.

Learning Objectives

This course will walk you through how to recognize actual and potential software vulnerabilities and implement defenses for those vulnerabilities. You will explore most common security vulnerabilities faced by web applications today, examining each vulnerability from a coding perspective through a process of describing the threat and attack mechanisms, recognizing associated vulnerabilities, and, finally, designing and implementing effective defenses.

This course combines engaging instructor-led presentations and useful demonstrations with valuable hands-on labs and engaging group activities. Throughout the course you'll:

- Grasp defensive, secure coding concepts and terminology, including the understanding of exploit phases and goals.
- Explore the 2021 OWASP Top Ten (latest edition) as well as several additional prominent vulnerabilities.
- Master the first axioms in security analysis and addressing security concerns across all web applications.
- Learn how to perform ethical hacking and bug hunting in a safe and appropriate manner.
- Identify and utilize effective defect/bug reporting mechanisms within your organization.
- Learn how to avoid common pitfalls in bug hunting and vulnerability testing.
- Develop an appreciation for the value of a multilayered defense strategy.
- Understand potential sources of untrusted data and the consequences of improper handling.
- Comprehend the vulnerabilities associated with authentication and authorization mechanisms.
- Learn how to detect and mitigate threats to authentication and authorization functionalities.
- Understand the mechanics and threats of Cross-Site Scripting (XSS) and Injection attacks, and how to defend against them.
- Comprehend the risks associated with XML processing, software uploads, and deserialization, and learn mitigation strategies.
- Familiarize yourself with security tools, hardening techniques, ongoing threat intelligence resources
- Optional / Bonus: Exploring AI in Web Application Security

If your team requires different topics, additional skills or a custom approach, our team will collaborate with you to adjust the course to focus on your specific learning objectives and goals.

Audience

This is an **overview-level** course ideally suited for web developers, software engineers, system administrators, and other technical stakeholders who are involved in the design, development, or maintenance of web applications. Security professionals looking to deepen their understanding of web application vulnerabilities and defense mechanisms would also greatly benefit. Moreover, project managers and leaders who wish to ensure their teams are following best practices for secure application development will find this course valuable in shaping their strategic direction.

Pre-Requisites

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.

Related Courses

The following is a small subset of our related courses. Please see our full catalog for a complete list.

- TT8120 Securing Web Applications Overview | OWASP Top Ten and Beyond
- TT8150 OWASP Top Ten Deep Dive
- TT8320-J Attacking and Securing Java / Jakarta EE Web Applications
- TT8320-N Attacking and Securing ASP.Net Web Applications
- TT8600 Secure Software Design
- TT8700 Securing Databases
- TT8800 Information Assurance / STIG Overview

- TT8810 Application Security and Development / STIG
- TTPS4894 Introduction to Python for Security Professionals
- TT8170 Exploring AI in Secure Web Application Development
- TT8175 Applying AI to the OWASP Top Ten

Next Steps / Follow-on Courses: We offer a wide variety of courses for application security, secure coding and programming, ethical hacking, AI in application security, database security, STIGs, secure software design and other related topics. Please see our **Cybersecurity / Secure Application Development Courses & Learning Journey Paths** for options based on your specific role and goals.

Course Topics / Agenda

Please note that this list of topics is based on our standard course offering, evolved from typical industry uses and trends. We'll work with you to tune this course and level of coverage to target the skills you need most. Topics, agenda and labs are subject to change, and may adjust during live delivery based on audience skill level, interests and participation.

Session: Bug Hunting Foundation

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

For More Information

For more information about our dedicated skills-focused training services (instructor-led, self-paced or blended), collaborative coaching services, robust Learning Experience Platform (LXP) solutions, Career Experiences, public course schedule, partner programs, courseware licensing options or to see our complete list of course offerings, training 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.