Cybersecurity Learning Journey

2021 OWASP Top Ten Deep Dive (TT8150)

Explore Bug Hunting, Ethical Hacking, Defensive Coding Concepts, Authentication, Authorization, Case Studies & More

Course Snapshot

- **Course: OWASP Top Ten Deep Dive (TT8150)**
- **Duration:** 2 days
- **Audience:** This is an **overview-level**, **language neutral** course ideally suited for software developers, IT professionals, project managers, IT auditors, compliance officers and cybersecurity enthusiasts.
- **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

OWASP 2021 refers to the latest edition of the Open Web Application Security Project (OWASP) Top Ten list, which identifies the most critical web application security risks. It is a valuable resource as it provides organizations with insights into prevalent vulnerabilities, helping them prioritize their security efforts and fortify their applications against potential attacks.

Our **2021 OWASP Top Ten Deep Dive** is a two day engaging course that provides you with the skills to protect data and maintain user trust across various digital projects. From identifying and eliminating bugs to managing unvalidated data, you'll delve into a myriad of vulnerabilities such as Broken Access Control, Cryptographic Failures, and the complexities of Server-Side Request Forgeries (SSRF). Throughout the course you'll explore the realm of software integrity, proper handling of authentication data, and the importance of robust security logging and monitoring systems. You'll also examine the challenges of 'Shifting Left' in software development processes and explore the intricacies of handling software and data integrity failures. These encompass using trusted repositories, protecting software development resources, and issues related to Continuous Integration/Continuous Deployment (CI/CD) pipelines.

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. Through engaging demonstrations and activities, you'll apply your newfound knowledge to real-world scenarios, enhancing your ability to analyze and mitigate security risks while maintaining privacy and ethical standards. You'll also gain practical experience with innovative tools and strategies, working through labs mirroring real-world situations, such as dissecting high-profile case studies like SolarWinds and Capital One.

By the end of this course, you'll have a robust understanding of the OWASP Top Ten, secure software development principles, and a broadened view of web application security. Armed with these skills, you'll be well-prepared to help your organization navigate the challenging landscape of cybersecurity.

Learning Objectives

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

- **Master Safe and Ethical Hacking Practices**: Learn to execute bug hunting and hacking activities in a manner that respects privacy and system integrity, ensuring that all actions align with ethical standards and organizational policies.
- **Identify and Utilize Bug Reporting Mechanisms**: Develop the ability to recognize and effectively utilize defect/bug reporting systems within your organization, facilitating swift response and mitigation.
- **Avoid Common Pitfalls in Vulnerability Testing**: Gain insights into common mistakes made during bug hunting and vulnerability testing and learn strategies to avoid them, enhancing the accuracy and effectiveness of your security assessments.
- **Comprehend Defensive, Secure Coding Concepts**: Delve into the principles and terminology of defensive coding, including understanding the phases and objectives of a typical exploit, to build more secure applications.
- **Appreciate the Multilayered Defense Approach**: Recognize the value of a layered, in-depth defense strategy in cybersecurity, enhancing your capacity to build robust and resilient systems.
- **Identify and Manage Untrusted Data Sources**: Understand the potential origins of untrusted data and the risks they pose, such as denial of service, cross-site scripting, and injections, and develop strategies to properly handle such data.
- **Strengthen Authentication and Authorization Security**: Learn about the vulnerabilities associated with authentication and authorization, and how to detect, attack, and implement defenses to enhance the security of these critical functions.
- **Mitigate Risks of XML Processing, File Uploads, and Server-Side Interpreters**: Familiarize yourself with the risks involved in XML processing, file uploads, and server-side interpreters, and learn how to apply techniques to harden web and application servers, and other infrastructure components to eliminate or mitigate these risks.
- **Optional / Bonus Overview**: Explore applying AI to the OWASP Top Ten

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 software developers, IT professionals, and cybersecurity enthusiasts who are keen to enhance their understanding of web application security. It would also benefit project managers and team leads overseeing digital projects, who require a strong grasp of security principles to manage risks effectively. Furthermore, IT auditors and compliance officers aiming to understand the technical aspects of web application security for better evaluation and enforcement of regulatory standards would find this course invaluable.

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 or cybersecurity concepts
- Awareness of general IT concepts (servers, databases, networks, etc.)

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: Jumping into the OWASP Top 10

Lesson: 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
- Lab: Case Study in Failure

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

Lesson: Removing Bugs
- Open Web Application Security Project (OWASP)
- OWASP Top Ten Overview
- Web Application Security Consortium (WASC)
- CERT Secure Coding Standard
- Microsoft Security Response Center
- Software-Specific Threat Intelligence

Session: Bug Stomping 101

Lesson: Unvalidated Data
- Potential Consequences
- Defining and Defending Trust Boundaries
- Rigorous, Positive Specifications
- Allow Listing vs Deny Listing
- 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 (Session Cookies and JWTs)
- Understanding and Defending Against CSRF
- CORS Misconfiguration Issues
- 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
- 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

Lesson: 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

Lesson: A05: Security Misconfiguration
- System Hardening: IA Mitigation
- Risks with Internet-Connected Resources
- Minimalist Configurations
- Application Allow Listing
- Secure Baseline
- Segmentation with Containers and Cloud
- Safe XML Processing

Session: Bug Stomping 102

Lesson: A06: Vulnerable and Outdated Components
- Problems with Vulnerable Components
- Software Inventory
- Managing Updates: Balancing Risk and Timeliness
- Virtual Patching
- Dissection of Ongoing Exploits
- Lab: Spotlight: Equifax

Lesson: A07: Identification and Authentication Failures
- Quality and Protection of Authentication Data
- Anti-Automation Defenses
- Multifactor Authentication
- Proper Hashing of Passwords
- Handling Passwords on Server Side

Lesson: A08: Software and Data Integrity Failures
- Software Integrity Issues and Defenses
- Using Trusted Repositories
- CI/CD Pipeline Issues
- Protecting Software Development Resources
- Serialization/Deserialization

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

Lesson: A10: Server Side Request Forgeries (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

Optional / Bonus: Leveraging AI in Tackling the OWASP Top Ten
- Introduction to AI in Cybersecurity
- AI for Detecting and Mitigating Security Risks
- AI in Managing OWASP Top Ten Vulnerabilities Detecting XML External Entities (
- AI in Incident Response and Forensics
- The Future of AI in Web Application Security

Setup Made Simple with our robust Learning Experience Platform (LXP)

All applicable course software, digital courseware files or course notes, labs, data sets and solutions, live coaching support channels and rich extended learning and post training resources are provided for you in our "easy access, no install required" high-speed **Learning Experience Platform (LXP),** remote lab and content environment. Course materials, software, resources and post-training platform access periods vary by course.

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.