A tesserent Company

SECURE SOFTWARE DEVELOPMENT OWASP TOP 10

DURATION: 2 DAYS

CYBER SECURITY

The OWASP Top 10 Training Course is designed to arm developers and IT professionals within your organisation with the most current knowledge and skills in web application security. The primary objective is to enhance their understanding and ability to combat the most significant security threats prevalent today, as identified by the Open Web Application Security Project (OWASP) in their widely recognized Top 10 list.

This comprehensive two-day training course offers a balanced mix of theory and practical sessions that will introduce attendees to the latest methodologies, tools, and techniques in the field of web application security. Not only will they learn to identify these critical vulnerabilities, but they will also gain hands-on experience in exploiting and mitigating these risks, using a range of open-source tools.

LEARNING OUTCOMES

The training will empower your developers and IT staff, enabling them to build more secure applications, respond effectively to security incidents, and stay abreast of the rapidly changing landscape of web application security threats. By enhancing their skills, they will contribute to the overall security posture of your organisation, ensuring the integrity, availability, and confidentiality of your data and services

WHO SHOULD ATTEND

This course can be attended by anyone interested in learning about the technical application of OWASP Top 10. Below is just a sample list of those that will most benefit -

- Software Developers
- IT team
- Security engineers
- QA testers
- Technical compliance team
- PCI compliance team

REQUIREMENTS

Standard laptop (Windows 10/Mac/Linux) with sufficient privilege to install software.

COURSE CONTENTS

PHASE 1: INTRODUCTION TO OWASP AND WEB APPLICATION SECURITY

- The importance of web application security
- Introduction to OWASP and the Top 10 project
- Overview of the 2021 Top 10 web application security risks

PHASE 2: IN-DEPTH ANALYSIS OF OWASP TOP 10 RISKS (PART 1)

- A01: Broken Access Control
- A02: Cryptographic Failures
- A03: Injection (including Cross-Site Scripting)

PHASE 3: HANDS-ON WORKSHOP

- Practical exercises on identifying and mitigating risks from Phase 2

PHASE 4: IN-DEPTH ANALYSIS OF OWASP TOP 10 RISKS (PART 2)

- A04: Insecure Design
- A05: Security Misconfiguration (including XML External Entities)
- A06: Vulnerable and Outdated Components

PHASE 5: HANDS-ON WORKSHOP

- Practical exercises on identifying and mitigating risks from Phase 4

PHASE 6: IN-DEPTH ANALYSIS OF OWASP TOP 10 RISKS (PART 3) AND MITIGATION STRATEGIES

- A07: Identification and Authentication Failures
- A08: Software and Data Integrity Failures (including Insecure Deserialization)
- A09: Security Logging and Monitoring Failures
- A10: Server-Side Request Forgery
- Secure coding practices to mitigate risks
- Introduction to security tools and technologies
- Security testing methodologies
  Phase 5: Hands-on Workshop
- Practical exercises on identifying and mitigating risks from Phase 4

PHASE 7: HANDS-ON WORKSHOP

- Practical exercises on identifying and mitigating risks from Phase 6

PHASE 8: CREATING A SECURE DEVELOPMENT LIFECYCLE (SDLC)

- Integrating security into the SDLC
- Ongoing security education for development teams

CYBER SECURITY
WE HAVE YOU COVERED
1300 767 592
customerservice@alc-group.com
alctraining.com.au

f ALC.Training
@alcgroup
in alc-training