OWASP TOP 10 TRAINING

Level - OWASP

Email – contact@DevOpsSchool.com

TRAINING AGENDA

DAY 1

Introduction to OWASP Top 10

- Overview of OWASP Foundation and Top 10 initiative
- Purpose and importance of the OWASP Top 10 in web application security
- Understanding risk exposure and impact on businesses
- How the OWASP Top 10 aligns with secure development

Injection Vulnerabilities

- SQL, NoSQL, OS, and LDAP injection threats
- Common injection patterns and attack scenarios
- Hands-on exercises for detection and mitigation
- Secure coding practices to prevent injection attacks

Broken Authentication & Session Management

- Risks associated with weak authentication mechanisms

- Session management flaws, token vulnerabilities, and hijacking
- Practical examples and lab exercises
- Implementing secure authentication and session controls

Sensitive Data Exposure

- Protecting sensitive data in transit and at rest
- Cryptography best practices for web applications
- Hands-on examples: encrypting sensitive fields and secure storage
- Compliance considerations (e.g., GDPR, PCI DSS)

XML External Entities (XXE) & Security Misconfigurations

- Understanding XXE attacks and prevention
- Detecting and preventing security misconfigurations in servers and frameworks
- Hands-on exercises for configuration review and hardening

Recap & Q&A

- Summary of key vulnerabilities covered
- Q&A session
- Review of hands-on exercises

DAY 2

Broken Access Control

- Horizontal and vertical privilege escalation
- Exploiting insecure direct object references (IDOR)
- Hands-on exercises to test and secure access controls

- Best practices for access control implementation

Cross-Site Scripting (XSS)

- Types of XSS (reflected, stored, DOM-based)
- Input validation and output encoding techniques
- Hands-on exercises to detect and prevent XSS vulnerabilities

Insecure Deserialization & Using Components with Known Vulnerabilities

- Deserialization attacks and mitigation strategies
- Dependency vulnerabilities and using OWASP Dependency-Check
- Hands-on exercises for safe deserialization and component management

Insufficient Logging & Monitoring

- Importance of logging and monitoring for security detection
- Integrating alerts, logging practices, and audit readiness
- Hands-on exercises on log analysis and alerting

Secure SDLC & DevSecOps Integration

- Embedding OWASP Top 10 into software development lifecycle
- DevSecOps pipelines, automated testing, and continuous monitoring
- Practical implementation strategies for enterprise projects

Case Studies & Hands-On Lab

- Real-world breach analysis based on OWASP Top 10 vulnerabilities
- Full-stack web application testing scenario
- Identify, exploit, and remediate vulnerabilities in lab environment

Final Review & Knowledge Assessment

- Recap of all OWASP Top 10 categories and mitigation strategies
- Scenario-based knowledge check
- Recommendations for applying OWASP Top 10 in production
- Q&A and discussion of best practices