OWASP API SECURITY TOP 10 TRAINING

Level - OWASP

Email – contact@DevOpsSchool.com

TRAINING AGENDA

DAY 1

Introduction to API Security

- What are APIs and why they are security-critical
- API architecture (REST, GraphQL, SOAP, gRPC)
- Common API attack surfaces
- Difference between Web Security vs API Security
- Overview of OWASP API Security Top 10

API Authentication & Authorization Basics

- API authentication methods (API keys, OAuth 2.0, JWT, OpenID Connect)
- Authorization models (RBAC, ABAC, scopes)
- Token handling and lifecycle
- Common mistakes in API auth implementations

Broken Object Level Authorization (BOLA)

- Understanding object-level access control
- Real-world BOLA attack examples
- How attackers exploit IDOR in APIs
- Detection and prevention strategies
- Secure coding practices

Broken Authentication

- Weak authentication mechanisms
- Token theft and replay attacks
- Password-based vs token-based auth risks
- Secure authentication design patterns
- Logging and monitoring auth failures

Broken Object Property Level Authorization

- Excessive data exposure
- Mass assignment vulnerabilities
- Over-posting and under-posting issues
- Secure request/response validation

Unrestricted Resource Consumption

- API rate limiting failures
- Denial of Service (DoS) risks
- Pagination, filtering, and query limits
- Protecting APIs from abuse and bots

Broken Function Level Authorization

- Role-based access failures
- Admin vs user endpoint exposure

- Privilege escalation attacks
- Secure API endpoint design

DAY 2

Unrestricted Access to Sensitive Business Flows

- Understanding business logic attacks
- Abuse of workflows and transactions
- Rate abuse in business operations
- API behavioral security controls

Server-Side Request Forgery (SSRF)

- How SSRF impacts APIs
- Internal network exposure risks
- Cloud metadata exploitation
- Input validation and allow-listing

Security Misconfiguration

- Default configurations and exposed endpoints
- Improper CORS configurations
- Missing security headers
- Secure API gateway configurations

Improper Inventory Management

- Shadow APIs and deprecated versions
- API versioning risks
- Documentation vs deployed APIs

- API discovery and inventory tools

Unsafe Consumption of APIs

- Third-party API trust issues
- Data validation from external APIs
- Dependency and supply chain risks
- Secure API integrations

Securing APIs in CI/CD & DevOps Pipelines

- Shift-left API security
- API security testing tools
- OpenAPI/Swagger-based security validation
- Integrating API security into DevSecOps

Logging, Monitoring & Incident Response

- API logging best practices
- Detecting abnormal API behavior
- SIEM integration
- Incident response for API breaches

Best Practices, Compliance & Next Steps

- API security best practices checklist
- Mapping OWASP API Top 10 to compliance standards
- Secure API design principles
- Real-world case studies
- Q&A and certification guidance