Application Security Training- Developer Perspective

Topics

Day 1

1. Securely Implement Microservice Architecture

• Introduction to Microservices Security

• Challenges in Microservice Architectures

• Secure Communication Between Services

• Identity and Access Management in Microservices

• Best Practices for Secure Service Deployment.

2. Securely Integrating Cloud Components into a Web Application

• Overview of Cloud Service Models

• Security Considerations for Cloud Components

• Secure Integration Patterns

• Data Protection in the Cloud

• Monitoring and Logging for Security.

Day 2

3. Front End Security with Modern Scripting Engines

• Scripting Engine Security Models

• Cross-Site Scripting (XSS)Prevention

• Secure Handling of User Input

• Using Content Security Policy (CSP)

• Modern JavaScript Security Features.

4. Infrastructure Security and Secure Configuration

• Infrastructure Security Fundamentals

• Hardening Operating Systems and Networks

• Secure Configuration Management

• Patch Management Strategies

• Automating Compliance Checks.

Day 3

5. Secure Design and Development of Authentication and Authorization Mechanisms, Including Single

Sign-On Patterns

• Authentication vs. Authorization

• Designing Secure Authentication Systems

• Implementing Single Sign-On (SSO) and Social Login

• OAuth and OpenID Connect

• Threats and Mitigations for Authentication Systems.

6. Cross-Domain Web Request Security

• Understanding the Same-Origin Policy

• Cross-Origin Resource Sharing (CORS)

• Secure Design Patterns for Cross-Domain Requests

• JSONP and Other Techniques

• Best Practices for Implementation.

7. Leverage Protective HTTP Headers

• Overview of HTTP Headers for Security

• Configuring Content Security Policy (CSP)

• HTTP Strict Transport Security (HSTS)

• X-Content-Type-Options, X-Frame-Options

• Implementing and Testing Security Headers.

Day 4

8. Defending REST and GraphQL APIs

• Security Challenges with REST and GraphQL

• Authentication and Authorization for APIs

• Input Validation and Sanitization

• Rate Limiting and Throttling

• Monitoring and Logging for Anomaly Detection.

9. Defend Against the Attacks Specified in OWASP Top 10

- Deep Dive into OWASP Top 10 Vulnerabilities
- Practical Defence Techniques
- Advanced Protection Strategies
- Incident Response Planning