Web Application Security Professional

Duration: 3 days (24 hours)

Module 1: Introduction to Web Applications and Security

1.1 Overview of Web Applications

- Fundamentals of Web Applications
- Web Application Components and Architecture
- Evolution of Web Technologies

1.2 Web Application Architectures

- Model-View-Controller (MVC) Framework
- Microservices Architecture
- Serverless Computing and Its Security Implications
- Single Page Applications (SPAs)

1.3 HTTP Protocols and Web Communication

- HTTP Types and Versions
- HTTP Methods and Their Security Considerations
- Cookie Management and Security Implications

1.4 Introduction to Application Security

- Importance of Web Application Security
- Common Security Threats and Attack Vectors
- Overview of Security Tools (Burp Suite, Proxy Tools)
- Lab Environment Setup for Practical Learning

Module 2: Security Frameworks and Industry Standards

2.1 Global Security Standards and Best Practices

- National Institute of Standards and Technology (NIST) Guidelines
- Open Web Application Security Project (OWASP)
- Common Weakness Enumeration (CWE)
- SANS Top 25 Most Dangerous Software Errors

2.2 OWASP Framework and Its Significance

- OWASP Top 10 Overview and Its Importance

- OWASP Testing Guide: Key Concepts and Methodologies

Module 3: OWASP Top 10 Security Risks – Part 1

3.1 Broken Access Control

- Cross-Site Request Forgery (CSRF)
- Path Traversal Attacks
- Authorization Bypass Techniques
- Exposure of Sensitive WSDL Files

3.2 Cryptographic Failures

- Weak Password Storage Mechanisms
- Improper Certificate Chain Validation
- Cryptographic Algorithm Vulnerabilities
- Cleartext Transmission of Sensitive Information
- Key Exchange Without Authentication
- Lack of Secure Transport for Credentials

Module 4: OWASP Top 10 Security Risks – Part 2

4.1 Injection Attacks

- SQL Injection (Error-Based & Blind)
- Command and OS Command Injection
- Cross-Site Scripting (XSS)
    - Client-Side XSS
    - Server-Side XSS
    - DOM-Based XSS

4.2 Insecure Design Principles

- Improper Error Handling Mechanisms
- Unrestricted File Uploads and Their Risks
- HTTP Request Smuggling
- Violation of Secure Design Principles
- Business Logic Vulnerabilities

Module 5: OWASP Top 10 Security Risks – Part 3

5.1 Security Misconfigurations

- XML External Entity (XXE) Attacks
- Absence of Custom Error Pages
- Misconfigured Cookie Attributes (Secure and HttpOnly Flags)

5.2 Risks of Vulnerable and Outdated Components

- Identifying and Mitigating Security Risks in Legacy Systems
- Software Component Inventory and Patch Management

Module 6: OWASP Top 10 Security Risks – Part 4

6.1 Identification and Authentication Failures

- Authentication Weaknesses and Exploitation Techniques
- Session Fixation Attacks
- Weak Password Recovery Mechanisms
- Lockout Mechanism Vulnerabilities
- Unverified Password Change Risks

6.2 Software and Data Integrity Failures

- Insecure Deserialization Attacks
- Lack of Integrity Checks in Software Components

6.3 Security Logging and Monitoring Failures

- Logging of Sensitive Information
- Insufficient Monitoring Leading to Delayed Incident Response

---

Module 7: OWASP Top 10 Security Risks – Part 5

7.1 Server-Side Request Forgery (SSRF) Attacks

- Exploitation of SSRF Vulnerabilities
- Mitigation Strategies

7.2 Security Scanners and Vulnerability Assessment

- Introduction to Automated Security Scanners
- Profiling Security Scans and Understanding Scanner Reports
- Manual vs. Automated Security Assessments

Module 8: Secure Development and DevSecOps Integration

8.1 Secure Software Development Lifecycle (SDLC)

- Common Security Pitfalls in Development
- Security Best Practices for Web Application Development

8.2 Advanced Security Strategies

- Threat Modeling in Secure Development
- Secure Code Reviews and Static Analysis
- Vulnerability Assessment and Penetration Testing (VAPT)

8.3 Introduction to DevSecOps

- What is DevSecOps?
- DevSecOps vs. Traditional Secure SDLC
- DevSecOps Strategies for Web Application Security