CYBER SECURITY PROFESSIONAL

(Web Application Security Engineer)

Module 1: Web Application Security Testing

- Introduction to Security Testing and its importance
- Basic concepts of Security Testing
- CIA Triad
- HTTP Methods
- HTTP Response Code
- HTTP Headers
- Cookie vs Session
- Cryptography - Encryption, Encoding, Hashing
- Symmetric Key Algorithm
- Asymmetric Key Algorithm
- Input Validation
- Output Encoding
- Blacklist Validation
- Whitelist Validation
- Client-Side Validation
- Server-Side Validation
- SDLC and Threat Modelling
- Security Testing Process / Methodology
- SSL Handshaking Process
- SSL vs TLS
- SSL / TLS Versions
- OWASP Top 10 Vulnerabilities

Module 2: Web Application Security Risks & Vulnerability Checks

- SQL Injection
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Insecure Direct Object Reference

- Failure to Restrict URL Access
- Security Misconfiguration
- Unvalidated Redirects and Forwards
- Broken Authentication and Session Management
- Using Components with Known Vulnerabilities
- Sensitive Data Exposure
- XML External Entity (XXE)
- Server-Side Request Forgery (SSRF)
- Insecure Logging and Storage
- Insecure Communication
- Vulnerable SSL/TLS Versions
- Authentication-Related Tests
- Credentials Transport Over Unencrypted Channels

Module 3: Authentication & Authorization Security Testing

- Testing for User Enumeration
- Default or Guessable (Dictionary) User Accounts
- Testing for Brute Force
- Testing for Bypassing Authentication Schema
- Testing for Vulnerable Remember Password and Password Reset
- Testing for Logout and Browser Cache Management
- Testing for CAPTCHA
- Insufficient Password Policy
- Insufficient Password Change Policy
- Passwords Stored in Plain Text
- Password History
- Authorization-Related Tests
- Path Traversals
- Bypassing Authorization Schema
- Privilege Escalation

Module 4: Web Application Security Testing Modules

- Session Management Testing
- Session Hijacking
- Session Fixation
- Session Timeout
- Session Replay
- Session Invalidation
- Exposed Session Variables
- Configuration-Related Tests
- Missing HttpOnly and Secure Flags
- Clickjacking
- HTTP Strict Transport Security Header
- Unsafe CORS Policy (HTML5)
- Cookie Scoped to Parent Domain
- Improper Error Messages
- Malicious File Upload
- Introduction to Various Vulnerability Scanners
- Scanning Application Using BurpSuite and Eliminating False Positives
- Bypassing Client-Side Validations
- Risk Rating and Report Preparation

Module 5: Tools Covered

- BurpSuite
- Acunetix
- Sslyze
- Sqlmap
- Kali Linux - Introduction

Module 6: Network Security Testing

- Basic Concepts of Networking
- TCP vs UDP
- What is an IP

- IP Address Classes
- IPv4 vs IPv6
- Different Ports
- Different Protocols
- Hubs, Switches, Routers, Firewalls
- DMZ
- Network Security Testing Methodology
- Scanning a Network Using Nessus
- Scanning and Evidence Gathering Using Nmap
- Internal vs External Network Security Testing
- Report Preparation
- Network Security Testing Tools: Nmap, Nessus, SSLScan/Sslyze

Module 7: Web Services Security Testing

- Web Services Security Testing

*****Note:** This outline is comprehensive and can be tailored based on course duration, depth of coverage, and the participants expertise levels. As technology continues to evolve, it is crucial to review and update the content regularly to incorporate emerging tools, practices, and industry best standards.