Web Hacking Check Point Certified Pen Testing Expert (CCPE)

Course Duration : 32 Hours **Course code : CCPE-WEB**

1. Course Overview

The **Web Hacking Check Point Certified Pen Testing Expert (CCPE)** course provides advanced knowledge of web application penetration testing. This course focuses on identifying, exploiting, and reporting complex web application vulnerabilities using professional penetration testing methodologies and ethical hacking practices.

2. What you'll learn?

- Advanced web application security concepts
- In-depth OWASP Top 10 exploitation
- Advanced authentication and session attacks
- Business logic vulnerability exploitation
- Web attack automation techniques
- Secure web application defense strategies

3. Target Audience

- Penetration testers
- Ethical hackers
- Bug bounty hunters
- Cybersecurity professionals
- Security researchers

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

4. Pre-Requisites

- Strong knowledge of web application fundamentals
- Experience with ethical hacking tools
- Understanding of HTTP/HTTPS and web technologies

5. Course Content (Modules)

Module 1: Advanced Web Application Architecture

- Modern web frameworks
- Client-server interaction

Module 2: OWASP Top 10 Advanced Attacks

- SQL injection advanced
- Cross-site scripting (XSS) advanced

Module 3: Authentication and Session Attacks

- Session fixation and hijacking
- Authorization bypass

Module 4: Business Logic and API Attacks

- Logic flaws
- API exploitation techniques

Module 5: Automation and Advanced Tools

- Burp Suite advanced
- Custom exploitation scripts

Module 6: Reporting and Defense Strategies

- Professional reporting
- Mitigation and secure coding