Techonquer Certified Web Pentester (TWPT) -

Course Content List

1. Networking & Information Gathering

- Networking Basics
- Information Gathering Techniques
- Website Fundamentals

2. Web Exploitation

- JavaScript Basics
- PHP & XSS Anatomy
- Stored XSS
- DOM XSS
- XSS Exploitation & WAF Bypass

3. SQL Injection

- SQL Fundamentals
- SQL Practical - Error & UNION Based
- Blind SQL Injection - Time Delay
- Boolean-Based SQL Injection - Authentication Bypass

4. File Upload Exploitation

- Content Type & Extension Bypass
- Blacklist & Whitelist Bypass

5. Local File Inclusion (LFI)

- LFI to XSS

6. Network Pentesting

- Host Discovery: ARP, ICMP, TCP/UDP
- Basic & Advanced Port Scanning
- Post Port Scanning Techniques
- Network Enumeration (FTP, SSH, RDP, SMB)
- Vulnerability Scanning

7. Windows Exploitation

- WebDAV Exploitation
- SMB Exploitation

- RDP Exploitation
- WinRM Exploitation

8. Malware Development & Post Exploitation

- Malware Development via MSF (Metasploit Framework)
- Windows Post Exploitation Techniques