

- ▶ Advanced Web Application Penetration Testing
- ▶ Advanced SQL Injection (SQLi)
- ▶ Reflected, Stored and DOM-based Cross Site Scripting (XSS)
- ▶ Cross Site Request Forgery (CSRF) - GET and POST Methods
- ▶ Server-Side Request Forgery (SSRF)
- ▶ Security Misconfigurations
- ▶ Directory Browsing/Bruteforcing
- ▶ CMS Vulnerability Scanning
- ▶ Network Scanning
- ▶ Auth Bypass
- ▶ Web App Enumeration
- ▶ Dictionary Attack
- ▶ Insecure Direct Object Reference Prevention (IDOR)
- ▶ Broken Access Control
- ▶ Local File Inclusion (LFI)
- ▶ Remote File Inclusion (RFI)
- ▶ Arbitrary File Download
- ▶ Arbitrary File Upload
- ▶ Using Components with Known Vulnerabilities
- ▶ Command Injection
- ▶ Remote Code Execution
- ▶ File Tampering
- ▶ Privilege Escalation
- ▶ Log Poisoning
- ▶ Weak SSL Ciphers
- ▶ Cookie Modification
- ▶ Source Code Analysis
- ▶ HTTP Header modification
- ▶ Session Fixation
- ▶ Clickjacking