WEB APPLICATION PENETRATION TESTING CHECKLIST



RECONNAISSANCE

- [ ] Whois lookup (domain registration information)
- [ ] DNS, subdomain enumeration
- [ ] Web server fingerprinting (e.g., server banner, versions, OS detection)
- [ ] Internet archives (wayback URL, wayback machines)
- [ ] Historical DNS data
- [ ] SSL/TLS certificate (e.g., expiry dates, authorities)
- [ ] Google dorking
- [ ] Public repositories (e.g., GitHub, GitLab open directories)
- [ ] Web technologies (e.g, WAF, CDN)
- [ ] Framework, CMS (e.g., Laravel, WordPress, drupal)
- [ ] JavaScript Libraries (e.g jQuery, nodeJS
- [ ] Content Discovery (e.g., robots.txt, sitemap.xml, metadata)
- [ ] Directory, file enumeration (e.g., admin pages, backup, config file)
- [ ] Third-party integration (payment gateway, plugins)
- [ ] Hidden parameters fuzzing

SCANNING

- [ ] Automated scan (e.g, invicti, burpsuite, WPscan, nessus)
- [ ] CVE database (e.g., cve.org, cvedetails.com)
- [ ] Exploit databases (e.g., Exploit-DB, packetstorm)
- [ ] Vendor security releases and advisories

EXPLOITATION

- [ ] HTTP methods enumeration
- [ ] HTTP method overriding
- [ ] Identity management bypass (user enumeration, brute force, guessable user account, weak username policy)
- [ ] Broken link hijacking
- [ ] Metadata analysis
- [ ] Host-header injection
- [ ] OTP bypass

+44 (0) 333 050 9002 info@thecyphere.com www.thecyphere.com

WEB APPLICATION PENETRATION TESTING CHECKLIST

EXPLOITATION

- [ ] Access control bypass (vertical and horizontal privilege escalation, IDOR, OAuth, directory traversal)
- [ ] Authentication bypass (default credentials, weak password policy, weak password change or reset function, account takeover, pre-OAuth takeover, MFA, browser cache)
- [ ] Session management schema (cookie manipulation, session forging)
- [ ] Cookies misconfiguration (unencrypted, leaked, or reusable token)
- [ ] Session timeout
- [ ] Guessable session variables, session hijacking
- [ ] Concurrent session
- [ ] CSRF (Cross-Site Request Forgery)
- [ ] JWT token (exposed or tempered)
- [ ] Input validation (XSS, verb tempering, injection)
- [ ] SQL injection
- [ ] Command injection
- [ ] LDAP injection
- [ ] XML injection
- [ ] SSTI injection
- [ ] CSV injection
- [ ] SSRF (Server-Side Request Forgery)
- [ ] Clickjacking
- [ ] WebSockets
- [ ] Browser/client-side storage
- [ ] Error handling
- [ ] Weak encryption, TLS certificate
- [ ] Business logic (unexpected file type, malicious file, rate limit bypass, OTP bypass, forged request, data injection, bypass payment functions, response manipulation, SMS bombing)
- [ ] HTTP request smuggling
- [ ] Web cache poisoning
- [ ] Missing web security headers
- [ ] File inclusion (LFI, RFI)
- [ ] Parameter tampering
- [ ] Open redirection