WEBSITE PENETRATION TESTING CHECKLIST

RECONNAISSANCE

- Scope Definition: Clear boundaries (URLs, subdomains, data, accounts)
- Technology Fingerprinting: Web servers, CMS, frameworks
- Browse and understand website functions
- HTTP Methods Check: Allowed methods (GET, POST, etc.)

VULNERABILITY SCANNING & EXPLOITATION

- Port Scanning: Open ports, services
- Directory/File Brute-Force
- Input Fuzzing: Unexpected behavior in forms, URLs
- Injection Attacks :SQLi, XSS, OS Command, XML, LDAP, Template
- Session Management
- Authentication: Weak passwords, brute-force resistance, account lockouts
- Access controls, privilege escalation, IDOR
- Open Redirection, File Uploads
- Business Logic Flaws: Bypassing intended flow

RELATED TESTS

- API Testing: REST, SOAP
- Web Server Config: Security headers, error handling, patch levels
- Encryption: Weak ciphers, outdated SSL/TLS, certificate checks

ANALYSIS & REPORTING

- Prioritise: High severity, easy to exploit
- Exploit Attempts: Tools/manual techniques
- Document Steps: For reproducibility & remediation, Reporting

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