# 网络安全渗透测试服务需求

一、服务需求

重保服务需针对保障服务目标门户网站、互联网业务系统（含移动客户端）、第三方外联系统等开展渗透测试工作。

渗透测试服务应综合智能工具扫描结果并结合人工测试和分析的手段，以模拟黑客入侵的方式对服务目标系统进行模拟入侵测试，识别服务目标存在的安全风险，并出具渗透测试报告，实现对保障范围内的网站和信息系统全覆盖。

渗透测试内容主要包括：信息收集类、配置管理类、认证类、会话类、授权类、数据验证类、系统应用漏洞等各类网络安全风险，重点针对操作系统、数据库、应用服务的已知漏洞、不安全配置、Web应用程序的常见漏洞进行测试，以发现网站应用层业务流程和逻辑上的安全漏洞和敏感信息泄露的风险。

二、具体要求

（一）满足原则

1）最小影响要求：渗透工作应尽可能小的影响系统和网络的正常运行，不能对运行和业务产生显著影响。重大系统的测试根据要求开展工作，若出现无法避免的情况（包括系统性能明显下降、网络拥塞、服务中断等），应提供详细的文档说明。

2）可控性要求：检测方法和过程要保证风险可控。

3）整体性要求：渗透内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患。

4）标准性要求：服务方案的设计与实施应依据国内或国际的相关标准进行。

5）规范性要求：检测过程和产生的文档，应具有很好的规范性，可以便于项目的跟踪和控制。

（二）测试要求（人工和工具结合）

1）服务方式包括但不限于：信息收集、端口扫描、漏洞扫描、口令猜测、脚本测试、权限获取等等。模拟黑客的攻击方法需在授权和监督下，方可对系统和网络进行非破坏性质的攻击性测试。

2）系统层安全测试包括且不限于：操作系统漏洞扫描、未授权访问测试、口令猜测等等。

3）应用层安全测试包括且不限于：系统结构分析及测试信息收集、爬网和Googling、应用程序配置管理测试、应用/服务运维配置缺陷检测、业务逻辑缺陷测试（如退款验证、资金交易验证、短信口令攻击等）、程序逻辑缺陷测试（如重放攻击、越权访问、防篡改缺陷等）、登陆验证测试、会话管理测试、SQL注入漏洞挖掘、数据传输安全测试（机密性和完整性）、第三方/开源工具检测、软件、中间件、开发包（如IIS、IHS、WAS、Apache、Struts、SSL、TLS、OpenSSL等）的公开漏洞检测、敏感信息保护、非授权访问测试等。

4）WEB应用独立测试项包括且不限于：WEB应用漏洞扫描、目录遍历、隐藏文件、备份文件、任意文件下载等敏感信息泄露扫描、跨站脚本漏洞、HTTP响应检测、跨站点请求伪造、重定向攻击等脚本攻击测试、文件上传漏洞测试等等。

5）移动端包括且不限于：客户端应用独立测试项、完整性校验、卸载清除检测、动态调试、反编译防范、篡改防范、安装包中敏感信息加密、关键组件访问保护、界面劫持、截屏防范、HOOK测试等等。

（三）服务报告要求

1）实施方必须为测得漏洞的单位编写安全测试报告。

2）测试报告的内容包括：测试目标、测试范围、漏洞复现过程、漏洞危害分析及修复建议。

（四）实施要求

1）实施方应采取有效安全措施，防止因技术检测引发信息安全事件。

2）实施方保证拥有从事本项目服务工作的资质及服务能力，并保证服务成果不会侵犯任何第三方知识产权。

3）实施方参加现场测试服务的人员（如有）须服从统一管理，遵守各项安全规章制度和要求。

4）实施方提供的服务需符合现行法律、法规、规章等规定。

5）实施方所收到的信息只能用于实施方提供渗透性测试及安全风险评估服务工作的目的，而不得用于任何其他目的。

6）如有需要，实施方需协助提供修复指导工作。

**（五）人员要求**

服务提供商提供的安全人员满足招标单位对于安全服务的专业技能要求。

1. 精通使用主流渗透测试和扫描工具，如IBM AppScan、Awvs、burp、nmap、sqlmap、MSF、Fiddler等；"精通OWASP安全测试框架，理解网络、应用、数据等不同层面的安全关注点"
2. 渗透思路清晰，具备独立WEB渗透能力，熟练掌握SQL注入/XSS/CSRF/文件上传/文件包含/命令执行/业务逻辑漏洞等漏洞利用方法，同时能够找出基本的横向越权和垂直越权等经验，可以进行爆破或找出弱口令等能力；
3. 掌握一种或多种编程语言，如：php/java/bash/python；
4. 能够写WebShell，掌握wireshark、MSF等工具，并能够进行主机渗透项目经验；
5. 精通Web端、服务器主机端、移动端APP（安卓、IOS端）、智能IOT端、中间件端\CVE渗透漏洞经验，对溢出、DLL劫持、代码执行、拒绝服务、内核提权、DNS安全漏洞、安全扫描绕过、POC的缓冲区溢出、未授权的访问及权限绕过、路径劫持、内容欺骗等等安全渗透工作经验，能够对各种进行安全评审与测试，并改出有建设性的修复方案；
6. 人员条件：响应供应商投入本项目团队应不少于20人；项目团队中人员应具有注册信息安全专业人员(CISP)证书或注册信息安全运维人员(CISAW安全运维)证书。
7. 供应商能力要求：响应供应商应具有本项目相关的安全测试平台或漏洞管理软件著作权或专利专有技术的；响应供应商应具有中国信息安全测评中心颁布的国家信息安全测评信息安全服务资质证书、具有CCRC中国网络安全审查技术与认证中心颁发信息安全服务资质认证证书。

三、保密要求

要高度重视保密工作：

1）对实施人员及相关文档、数据和载体等进行严格管理，确保服务过程中涉及到的敏感信息得到有效控制；

2）相关文档、数据和载体，不得擅自对外发布或提供给无关机构；

3）服务过程中获知的信息需确保不被泄漏，测试数据和测试结果等不得向其他单位透露。