中国建设银行厦门市分行2024-2026年分行渗透测试服务采购需求工作说明书

一、技术服务目标

渗透测试服务：实施对象为中国建设银行厦门市分行面向互联网的四个应用系统，目前厦门分行互联网资产存在：“厦门分行互联网应用平台”、“厦门房票系统”、“款易得小程序”、“公租房管理信息系统”。若后续系统变动，我行需要更换渗透测试目标系统，供应商应支持我行做渗透测试目标更换。渗透测试服务应包含服务器主机系统漏洞检测。应用系统安全测试，采用渗透性测试手段，全面检测目标系统可能存在的安全风险问题，包括但不限于常见的系统漏洞、中间件漏洞、Web应用漏洞与业务逻辑类漏洞等。

二、范围概述

厦门分行互联网应用平台：该系统由“厦门建行悦理财”公众号、“龙卡信用卡—厦门”公众号、约惠厦门小程序、购车补贴小程序等模块构成。

厦门房票系统：厦门房票小程序。

款易得小程序：款e得小程序。

公租房管理信息系统：公租房APP。

三、采购需求

本次采购四个系统（目标系统如发生更换，供应商应支持我行更换），每个系统预计一年执行2次渗透测试工作，即一年执行8次渗透测试工作，本次计划采购2024-2026年底三年的渗透测试服务，共计采购次数为24次

四、技术服务方式

1.测试方法科学，测试遵循相关安全测试规范；

2.测试过程可控，不可使用对目标系统造成较大恶劣影响的测试行为；

3. 测试所发现的安全风险问题，需详细说明风险影响，风险等级，漏洞利用方法，漏洞修复建议；

4. 测试完成之后，需配合我行人员完成安全风险修复，并进行复查测试，确认风险已修复；

5.根据我行实际需求，提供相应的测试服务，保证测试效果全面有效；

6.测试完成后出具相应的测试结果报告及复查验证报告；

五、项目组织

在我行人员联系供应商进行对应系统渗透测试工作后，开展渗透测试工作之前，供应商应提前两个工作日将渗透测试的源IP地址，及开展渗透测试具体时间段报备给我行联系人。

测试人员具备相关服务资质，拥有2年以上项目实施经验，团队内至少一名人员具有注册信息安全专业人员渗透测试工程师（CISP-PTE）证书，其余团队成员含有信息安全类证书，如：CISP、CISSP、NISP等均可。

六、付款方式

整体项目“2024-2026年分行渗透测试和互联网资产排查服务”合同签订以后，请供应商将渗透测试服务与互联网资产排查服务的发票分别开立增值税专用发票，在收到乙方提供符合要求的发票后三十个工作日内，向乙方支付合同金额40%的费用，整体项目完成后，在收到乙方提供符合要求的发票后三十个工作日内，向乙方支付合同尾款，即合同金额60%的费用。