

# 5G<sup>+</sup>智能银行项目

## 技术安全测试报告

中国建设银行

金融科技部

2019年6月19日



# 1. 测试报告名称

《5G+智能银行项目技术安全测试报告》

# 2. 参照标准及文档依据

《信息安全技术 网络安全等级保护基本要求》

《信息安全管理办法》

《中国建设银行软件开发安全需求规范》

《中国建设银行软件开发安全测试规范》

《中国建设银行 WEB 应用开发常见安全问题汇编》

《5G+智能银行项目需求说明书》

《5G+智能银行项目详细设计说明书》

# 3. 测试保证说明

## 3.1. 参与人员

建设银行金融科技部安全处、建设银行测试中心测试经理、建信金科质控中心测试人员。

## 3.2. 测试方法

本次技术测试分为两个阶段展开, 在项目开发测试过程中采取白盒测试方法进行代码安全性扫描、人工审查及开源软件扫描; 在版本检验环节采取黑盒测试方法开展渗透测试和漏洞扫描。各阶段发现的问题均及时与项目组开发人员确认。测试人员对上述问题进行了复测, 确认整改及时有效。

## 3.3. 测试环境及版本信息

测试环境: 建设银行版本检验环境, 与外联系统调用通过模拟器采用报文模拟方式进行。

表 1 安全测试工具环境

资源类型	资源用途	CPU/内存	台数	软件
X86 服务器	代码静态扫描	16G/256G	1	Fortify
X86 服务器	开源软件扫描	4C/16G	1	龙查
PC 机	代码审核	4C/8G	2	Eclipse 及 SlickEdit
PC 机	渗透测试	4C/8G	4	Metasploit 及 Burpsuite

扫描器	漏洞扫描	2C/4G	1	绿盟 RSAS
-----	------	-------	---	---------

测试版本：5G+智能银行 0621 投产版本，子系统及版本如图 2 所示。

表 2 安全测试软件运行环境

名称	功能用途	硬件配置	软件版本
魔镜	人脸识别	8C/64G*2（集群）	v1.0.2
驾驶舱	沉浸式感应	专用设备	v2.2.0
龙易行渠道	产品签约	2C/8G	V1.6.8
智能银行大脑	智能银行核心	4C/16G	v1.0.2
统一客服	视频及语音交互	2C/8G	V3.0.6

3.4. 测试案例



渗透测试案例集合  
.xlsx

3.5. 评价准则

根据应用缺陷带来的风险危害程度，对发现的各类缺陷分为高、中、低三个级别。针对发现的安全漏洞，在缺陷修复后，经复测通过则认定该缺陷已解决；高危缺陷已全部关闭，且中、低危安全缺陷的修复计划在处置时限要求范围内或有相应缓解措施，可认定为测试通过。

3.6. 限制约束

由于测试环境与生产环境的差异性、外联的真实系统与模拟器差异性，本报告只对本次测试负责。

4. 测试执行情况

在白盒测试阶段，使用 Fortify SCA 扫描工具对全部工程代码进行扫描，涉及 java、javascript、python、html 等四类语言，代码 16 万余行，扫描结果进行人工复核，扫描结果未发现 SQL 注入、文件上传漏洞等问题；使用开源软件代码扫描工具对工程中使用的开源软件进行检测，涉及开源软件使用点 290 处，开源软件类型 60 个，未发现远程命令执行、敏感信息泄露等严重风险告警。

在黑盒测试阶段，采用渗透测试和漏洞扫描方式，设计安全测试案例 16 类 138 项，对 OWASP 的 TOP10 进行重点覆盖。对中间测试发现的问题进行修复后，最终测试运行情况如下：

*测试案例类型	*测试案例名称	*预期结果	*运行结果
AQCS-001	水平越权测试	报错，提示用户身份出错，非法的请求	符合预期
AQCS-002	垂直越权测试	报错，提示用户身份出错，非法的请求	符合预期
AQCS-003	CSRF 攻击	报错，token 无效，非法的请求	符合预期
AQCS-004	SQL 注入测试	报错，提示有非法输入，请输入正确的格式	符合预期
AQCS-005	XSS 注入测试	报错，提示有非法输入，请输入正确的格式	符合预期
AQCS-006	暴力破解测试	报错，用户名或密码错误。第 2 次错误提示时，界面框出现不小于五位的模糊验证码。连续错误出现十次时，该请求 IP 地址将被封禁。	符合预期
AQCS-007	人脸伪装测试	提示，请用户进行眨眼或摇头等操作，验证多维度的面部信息，如不能正确进行上述操作，则提示登录失败。	符合预期
AQCS-008	wifi 入侵检测	报错，连接申请失败，不做进一步的出错提示	符合预期
AQCS-009	路经穿越测试	../.../路经穿越的关键字被过滤掉，正常返回	符合预期
AQCS-010	命令注入攻击测试	阻断来源 ip 地址，禁止访问系统半小时。再次发起后该 ip 将会被封禁 1 天。	符合预期
AQCS-011	批量扫描测试	阻断来源 ip 地址，禁止访问系统半小时。再次发起后该 ip 将会被封禁 1 天。	符合预期
AQCS-012	跨域解析测试	通过报文查看，是进行跳转解析而非建行服务器内解析	符合预期
AQCS-013	文件上传测试	阻断来源 ip 地址，禁止访问系统半小时。再次发起后该 ip 将会被封禁 1 天。	符合预期
AQCS-014	图片验证码专项测试	满足建行的标准要求（验证码的长度最小为 5 位，数字和字母的混合编排，存在一定程度的模糊化）	符合预期
AQCS-015	密码重置测试	满足建行的标准要求（长度最小 6 位，有效时间最长 60 秒）	符合预期

AQCS-016	内部错误暴露	系统对用户输入奇点值进行了正常过滤，即使出现错误，错误信息也不会对用户抛出	符合预期
----------	--------	---------------------------------------	------

测试案例执行率及缺陷修复率如下：

*案例执行率	*执行案例成功率	*缺陷修复率
100%	100%	100%

测试过程中发现 5 个中、低危缺陷，包括跨站脚本、路径穿越、文件上传等等，均得到及时修复。缺陷分析情况如下：

*编号	*缺陷类型	*缺陷描述	*评级	*分析与处理
1	XSS 注入	未对用户的输入提交大小写进行有效过滤， <ScRiT>alert(1)</sCriPt>的 XSS 注入语句成功执行。	低危	已修复
2	XSS 注入	未对用户的输入提交编码格式进行有效过滤， <script>\u0061\u006c\u0065\u0072\u0074(1)</script>的 XSS 注入语句成功执行。	低危	已修复
3	路径穿越	在用户头像自助上传时，可以通过在 post 包中加入../../../../etc/读取操作系统敏感文件	低危	已修复
4	文件上传	在用户身份信息提交时，可以通过修改后缀的方式，将.rar 等特定文件伪装成.jpg 图片绕过检查，但是不能成功进行回连。	中危	已修复
5	内部错误暴露	在用户注册时，用户输入超长昵称，后台返回的错误信息包含内部技术细节。	低危	已修复



## 5. 测试结果

本次安全测试由建设银行金融科技部安全处牵头，由建信金科质控中心测试人员进行具体实施，并经由建设银行测试中心测试人员复核，确保测试流程合规、质量保障活动有效。本次测试共发现 XSS 跨站脚本、目录遍历等问题 5 项，均为中低危缺陷，并且均完成整改修复。

## 6. 结论及建议

本次测试，在白盒测试阶段采用代码扫描工具和开源软件扫描工具，对 5G+ 智能银行项目采用静态检查的方法进行了安全测试；在黑盒测试阶段利用扫描工具和渗透测试采用动态检查的方法对 5G+ 智能银行进行了安全测试。未发现高危缺陷，所有中低危缺陷均已得到解决。牵头方、测试实施方等相关各方，一致同意软件技术安全质量满足建行的规范要求，允许上线。

