



应用服务系统 安全测试的标准化

姓名 张艾俐
职位 安全测试经理

目 录

1 建设背景

2 应用系统标准化安全测试设计与实践

3 后续展望

系统性全面排查 缺陷的能力不足

依托渗透测试方法，以入侵被测系统、控制服务器、获取系统信息为目标，寻找一条可行通路进入系统达到目的即停止，不查找系统所有漏洞。

自主安全技术 能力不足

技术能力不同、关注点不同，则测试结果不同，仅依托个人责任心和工作能力，无法衡量工作量和工作效率。

外部检查合规 缺陷增加

经过历年开发与安全的共同协作，外部检查中发现的高风险漏洞大幅降低，合规类漏洞数量增加。（如软键盘乱序）

安全规范有效 落地不足

2018年，为进一步加强安全管理，部门从各角度颁布多个安全技术规范，但如何落地执行缺乏有效方法和手段。

打造自有安全技术能力

制定统一的安全技术标准和安全测试案例库，将个人技术能力转化为我行安全技术能力并不断发展完善。

提升安全测试效果

制定案例库、改造测试工作流程，实施全面安全测试，提升技术深度和覆盖广度，指导测试工作有序标准化实施，提升安全测试能力。

降低个人技术依赖

标准化测试流程与测试方法，降低因个人能力不同测试结果不同的现状，也为量化考核提供依据。

工作推进思路（标准化规范化）



安全测试 标准化

整合各类安全技术规范；
制定场景化安全测试案例库；
严格实施测试管理流程；
定期追溯测试结果；

1

统一的
技术要求

2

标准的
测试方法

3

规范的
测试管理

目 录

1

建设背景

2

应用系统标准化安全测试设计与实践

3

后续展望

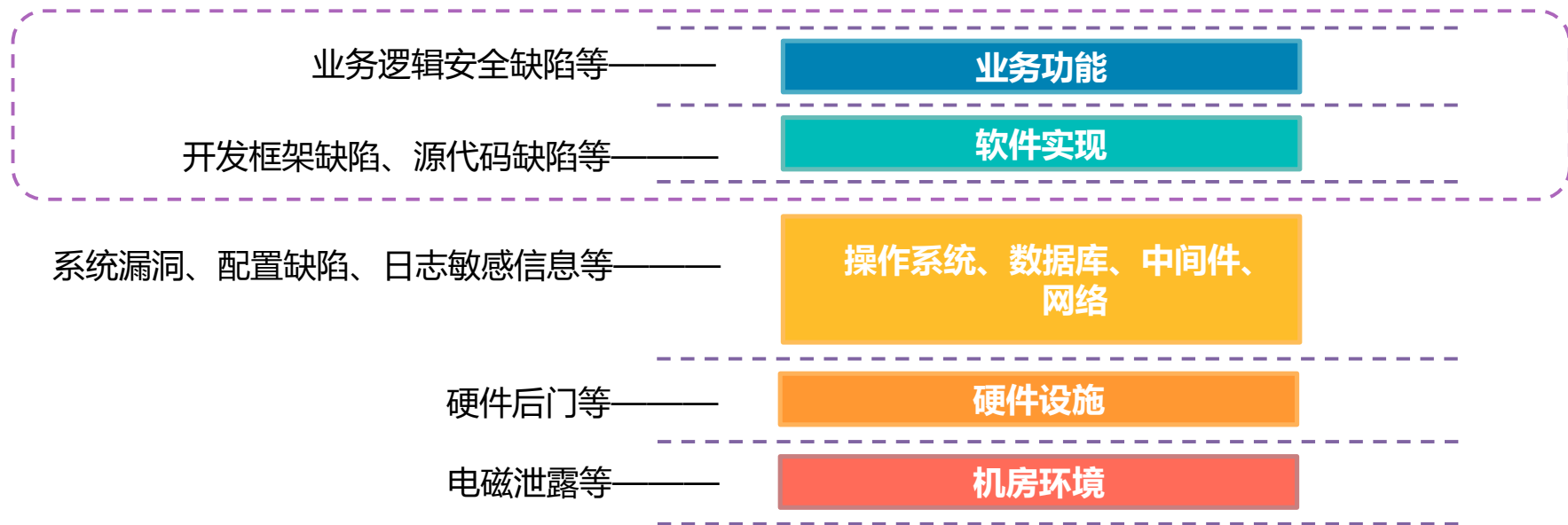
安全测试

通过模拟“**恶意黑客攻击**”的测试手段，来评估系统安全性的一种评估方法，这个过程包括对系统的**任何弱点、技术缺陷或漏洞**的主动分析，是验证应用安全和**识别潜在安全缺陷**的过程。

移动互联系统

在互联网上直接访问，面向客户、行员提供服务的系统，包括APP、WEB、微信，与第三方接口不在测试范围内。

应用安全





需求分析

根据需求内容判断是否需要安全测试



案例选取

根据**场景化安全测试案例库**选取适当的测试案例，制定测试计划（**方案评审**）



案例执行

手工测试：根据**场景化安全测试案例库**中标准化测试步骤开展
自动化测试：依托**自动化测试平台**开展



缺陷修复

对发现缺陷进行跟踪复测，**直至全部修复**



报告审批

形成测试报告（**投产评审**）



业务场景

业务功能：注册与登录、敏感信息查询、金融交易、业务申请、demo测试等
功能组件：身份鉴别、设备标识与认证、页面输入、文件上传下载等



功能场景

访问控制、接口安全、数据安全



系统场景

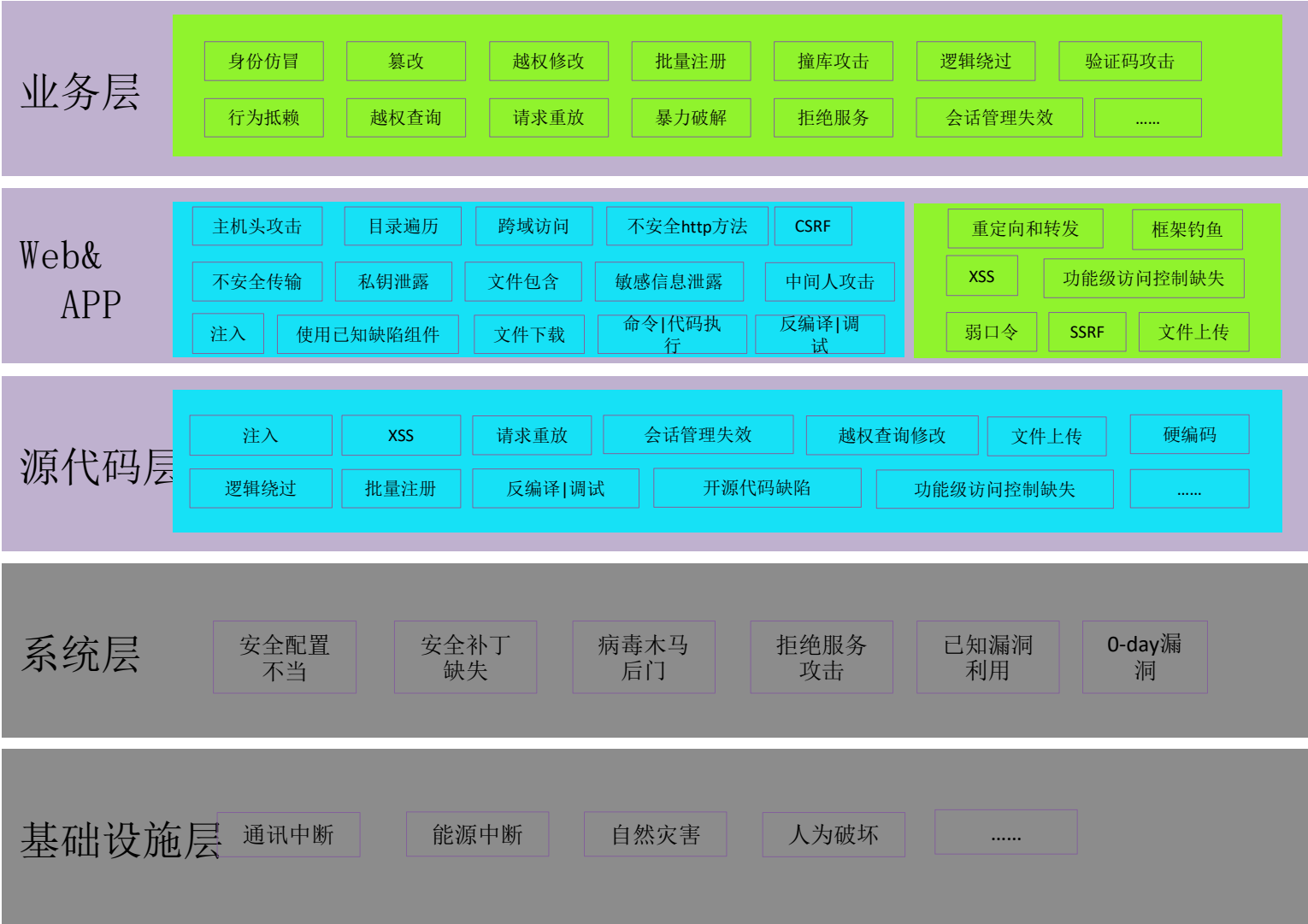
会话管理：会话回退、会话关闭等
配置管理：客户端配置、网络配置、服务器配置、部署管理等
审计管理：日志与审计

场景化安全测试案例库（二）——具体内容

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE

序号	场景类别	子序号	应用场景	风险项	检查点	案例名称	测试方法	适用范围	风险等级	适用类型
1	访问控制	1.1	会话	会话回退	(1)页面后退	会话回退-页面回退	手工	全部	严重	web/app/公众号
					(2)直接输入访问地址	会话回退-直接输入访问地址	手工	全部	严重	web/app/公众号
		1.2	业务管理	会话关闭	(1)会话空闲超时	会话关闭-空闲超时	系统测试	全部	一般	web/app/公众号
					(1)运行状态提醒	会话状态-运行状态提醒	系统测试	全部	一般	web/app/公众号
				账户管理	(1)账户禁用与启用	业务管理-账户管理-账户禁用及启用	访谈	全部	严重	web/app/公众号
					(2)默认账户控制	业务管理-账户管理-默认账户控制	访谈	全部	严重	web/app/公众号
					(3)临时账户管理	业务管理-账户管理-临时账户管理	访谈	全部	严重	web/app/公众号
					(1)多重授权机制	业务管理-账户权限管理-多重授权机制	访谈	全部	严重	web/app/公众号
					(2)账号&权限关系映射	业务管理-账户权限管理-账号与权限关系映射	访谈	全部	严重	web/app/公众号
					(3)手机号&客户号&账户关系映射	业务管理-账户权限管理-手机号客户号账户关系	访谈	全部	严重	web/app/公众号
					(4)转授权功能控制	业务管理-账户权限管理-转授权	访谈	全部	严重	web/app/公众号

案例名称	测试目的 (意图)	测试条件 (数据需求)	测试场景	测试步骤	检查指引	期望结果	测试结果
转账汇款篡改验证转账汇款功能数据完整性保障机制是否存在风险	1.完成开户和电子渠道开通; 2.用户信息 (用户名/手机号、登录密码、关联账号)	转账汇款	1.登录账号, 设置代理抓包, 分别拦截并修改各步骤请求报文: (1)点击"转账汇款", 获得请求报文; (2)输入转账信息, 点击"下一步", 获得请求报文; (3)点击"获取验证码", 输入验证码, 并输入密码, 点击"提交", 获得请求报文。 (4)修改各步骤请求报文中的 "付款账号、转账金额、收款账号、收款人姓名、收款人手机号" ; 2.分别发送修改后的请求报文; 3.拦截各步骤的响应报文; 4.检查是否有成功的响应报文。若存在, 则说明存在数据篡改风险。	1.应用系统通信过程中应使用校验码技术保证通信过程中数据的完整性, 所有涉及资金、账务等敏感信息变动的交易报文必须调用MAC加密类接口进行完整性校验; 2.应对交易数进行数据签名, 签名数据除流水号、交易金额、转入账号、交易日期和时间等要素外, 还应包含由服务器生成的随机数据, 服务器应验证签名的有效性并安全存储签名。	系统提示"报文解析失败"。		



安全测试覆盖

自动化工具实施

人工实施

方案评审

投产评审



经验积累

参与人员：资深安全专家、安全测试经理、开发人员、安全测试人员



通过电子化、精细化管理，加强工作能力、提升工作效率。

目 录

1 建设背景

2 应用系统标准化安全测试设计与实践

3 后续展望



01

对于前沿技术，如生物识别、地理位置等，还需进一步对存在的风险进行深入研究




02

不断提升技术深度



03

不断提升自动化测试

The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid-like structure, possibly representing a network or data flow. The pattern is more dense in some areas and more sparse in others, creating a sense of depth and movement.

THANKS

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE