|  |
| --- |
| XX银行手机银行登录安全设计咨询方案 |
|  |
|  |

目录

[1 简介 4](#_Toc11350733)

[1.1 文档目的 4](#_Toc11350734)

[1.2 文档范围 4](#_Toc11350735)

[1.3 目标对象 4](#_Toc11350736)

[2 手机银行登录场景安全需求 4](#_Toc11350737)

[2.1 输入安全需求 4](#_Toc11350738)

[2.2 认证安全需求 5](#_Toc11350739)

[2.3 通信安全需求 5](#_Toc11350740)

[2.4 日志审计需求 6](#_Toc11350741)

[2.5 错误处理需求 6](#_Toc11350742)

[2.6 会话安全需求 6](#_Toc11350743)

[2.7 APP客户端安全需求 7](#_Toc11350744)

[3 手机银行登录场景安全设计方案 7](#_Toc11350745)

[3.1 输入处理 7](#_Toc11350746)

[3.2 认证管理 8](#_Toc11350747)

[3.2.1 有安全的登录控制措施 8](#_Toc11350748)

[3.2.2 服务间的访问有认证控制措施 8](#_Toc11350749)

[3.3 通信安全 9](#_Toc11350750)

[3.3.1 使用HTTPS协议 9](#_Toc11350751)

[3.3.2 传输的密码进行加密处理 10](#_Toc11350752)

[3.4 日志审计 10](#_Toc11350753)

[3.4.1 关键操作要有日志记录 10](#_Toc11350754)

[3.4.2 不要在日志中记录敏感信息 11](#_Toc11350755)

[3.4.3 日志管理 11](#_Toc11350756)

[3.5 错误处理 11](#_Toc11350757)

[3.6 会话管理 12](#_Toc11350758)

[4 手机银行APP客户端安全设计方案 12](#_Toc11350759)

[4.1 源代码保护 13](#_Toc11350760)

[4.2 安全的数据存储 13](#_Toc11350761)

[4.3 权限最小化 13](#_Toc11350762)

[4.4 三方组件安全 14](#_Toc11350763)

[4.5 使用安全软键盘 14](#_Toc11350764)

[5 附录 14](#_Toc11350765)

[5.1 密码安全要求 14](#_Toc11350766)

[5.2 威胁与对应安全控制措施参考 15](#_Toc11350767)

1. 分发控制

|  |  |  |
| --- | --- | --- |
| **读者** | **文档权限** | **说明** |
| 项目组成员 | 只读 |  |
| 项目经理 | 可修改 |  |

1. 文件版本信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本号** | **变更描述** | **日期** | **作者** | **批准** |
| V0.1 | 创建文档 |  |  |  |
|  |  |  |  |  |

1. 文件版本信息说明

文件版本信息记录本文件提交时的当前有效的版本控制信息，当前版本文件有效期将在新版本文档生效时自动结束。文件版本小于1.0 时，表示该版本文件为草案，仅可作为参照资料之目的。

1. 文档签字确认

安全负责人：

项目经理：

# 简介

## 文档目的

本文档针对XX银行手机银行的登录场景在架构设计阶段可能存在的安全风险及威胁，给出登录的架构安全设计咨询方案。

## 文档范围

本文档只涉及XX银行手机银行的登录场景。

## 目标对象

本文档主要的目标对象有：系统的架构设计人员、开发人员、测试人员、安全人员、以及相关的管理人员等。

# 手机银行登录场景安全需求

根据对手机银行登录场景的威胁分析，并参考相关的规范和要求，我们总结出登录场景的主要安全需求如下。

## 输入安全需求

|  |  |  |
| --- | --- | --- |
| No. | 安全需求 | 规范依据 |
| 1 | 对用户输入的数据要进行合规性检查 | 中国金融移动支付客户端技术规范  中国金融移动支付应用安全规范  网上银行系统信息安全通用规范 |
| 2 | 对用户输入数据的检查要在服务端实施 | 中国金融移动支付客户端技术规范  中国金融移动支付应用安全规范  网上银行系统信息安全通用规范 |

## 认证安全需求

|  |  |  |
| --- | --- | --- |
| No. | 安全需求 | 规范依据 |
| 1 | 当用户输入密码时，密码信息不要明文回显在页面上 | 中国金融移动支付客户端技术规范  网上银行系统信息安全通用规范 |
| 2 | 如有初始密码，首次登录时应强制客户修改初始密码 | 信息安全技术网络安全等级保护测评要求  网上银行系统信息安全通用规范 |
| 3 | 所有的身份认证控制措施都在服务器端执行 | 网上银行系统信息安全通用规范 |
| 4 | 账号的密码要有复杂度的控制 | 信息安全技术网络安全等级保护测评要求  网上银行系统信息安全通用规范 |
| 5 | 用户输入的密码要加密后再传输到服务端认证 | 网上银行系统信息安全通用规范 |
| 6 | 当登录认证失败多次时，增加图像验证码或者短信验证码，或临时锁定用户账号 | 信息安全技术网络安全等级保护测评要求  中国金融移动支付客户端技术规范  中国金融移动支付应用安全规范  网上银行系统信息安全通用规范 |
| 7 | 图像验证码有恰当的安全控制 | 网上银行系统信息安全通用规范 |
| 8 | 短信验证码要有恰当的安全控制 | 网上银行系统信息安全通用规范 |
| 9 | 因登录认证失败多次锁定的账号，在一段时间后要解锁账号 | 网上银行系统信息安全通用规范 |
| 10 | 登录功能中不能有账号信息枚举的可能 | 网上银行系统信息安全通用规范 |
| 11 | 手机银行服务与其它服务要进行双向身份认证 | 网上银行系统信息安全通用规范  银发〔2016〕170号中国人民银行关于进一步加强银行卡风险管理的通知 |
| 12 | 登录过程的所有操作必须使用同一IP地址和MAC地址，否则服务器端应自动终止注册过程 | 网上银行系统信息安全通用规范 |

## 通信安全需求

|  |  |  |
| --- | --- | --- |
| No. | 安全需求 | 规范依据 |
| 1 | 所有Web请求都要使用HTTPS协议 | 中国金融移动支付客户端技术规范  网上银行系统信息安全通用规范  PCI DSS  银发〔2016〕170号中国人民银行关于进一步加强银行卡风险管理的通知 |
| 2 | 使用TLS1.2以上版本协议加密数据 | 中国金融移动支付客户端技术规范  网上银行系统信息安全通用规范 |
| 3 | 证书须使用SHA256以上哈希算法签名，使用RSA2048位或ECC256位以上公钥算法 | 中国金融移动支付客户端技术规范 |
| 4 | 客户端要检查服务端证书的合法性 | 网上银行系统信息安全通用规范 |
| 5 | 用户输入的密码要加密处理后再发送到服务端 | 中国金融移动支付客户端技术规范  网上银行系统信息安全通用规范  PCI DSS  银发〔2016〕170号中国人民银行关于进一步加强银行卡风险管理的通知 |

## 日志审计需求

|  |  |  |
| --- | --- | --- |
| No. | 安全需求 | 规范依据 |
| 1 | 关键操作都要有日志记录 | 信息安全技术网络安全等级保护测评要求  中国金融移动支付客户端技术规范  中国金融移动支付应用安全规范  网上银行系统信息安全通用规范 |
| 2 | 日志中至少要记录操作类型、操作时间、操作者标识、操作对象标识和操作结果 | 信息安全技术网络安全等级保护测评要求  网上银行系统信息安全通用规范 |
| 3 | 不要在日志中记录敏感信息 | 网上银行系统信息安全通用规范 |
| 4 | 对日志进行统一存储和分析处理 | 信息安全技术网络安全等级保护测评要求 |
| 5 | 日志有完整性检查控制措施来防止未授权的修改 | 网上银行系统信息安全通用规范 |
| 6 | 应该只有审计员才能访问日志信息 | 网上银行系统信息安全通用规范 |

## 错误处理需求

|  |  |  |
| --- | --- | --- |
| No. | 安全需求 | 规范依据 |
| 1 | 登录失败时要对错误提示信息模糊化处理 | 网上银行系统信息安全通用规范 |
| 2 | 有恰当的错误处理措施，当错误发生时仅展示通用的页面 | 网上银行系统信息安全通用规范 |
| 3 | 不要在错误提示信息中返回敏感信息 | 网上银行系统信息安全通用规范 |

## 会话安全需求

|  |  |  |
| --- | --- | --- |
| No. | 安全需求 | 规范依据 |
| 1 | 会话ID要足够长、随机，并且要有唯一性 | 中国金融移动支付应用安全规范  网上银行系统信息安全通用规范 |
| 2 | 会话一段时间不活动时，对其进行失效处理 | 中国金融移动支付应用安全规范  网上银行系统信息安全通用规范 |
| 3 | 登录认证成功后要生成新的会话和会话ID | 网上银行系统信息安全通用规范 |
| 4 | 会话ID要存储在Cookie字段中，并要恰当的设置path值，还要添加“httponly”和“secure”属性 | 网上银行系统信息安全通用规范 |
| 5 | 同一账号在同一时间应该只能并发一个会话 | 网上银行系统信息安全通用规范 |
| 6 | 对短时间内的多重并发会话数进行限制 | 中国金融移动支付应用安全规范  网上银行系统信息安全通用规范 |
| 7 | 当系统通信双方中的一方在指定时间内未作任何响应，另一方应能够自动结束会话 | 网上银行系统信息安全通用规范 |
| 8 | 所有的访问请求都要有会话控制 | 中国金融移动支付客户端技术规范  网上银行系统信息安全通用规范 |
| 9 | 会话控制要在服务器端实施 | 网上银行系统信息安全通用规范 |

## APP客户端安全需求

|  |  |  |
| --- | --- | --- |
| No. | 安全需求 | 规范依据 |
| 1 | 客户端程序有防反汇编的安全控制措施，防范攻击者对客户端程序的调试、分析和篡改 | 中国金融移动支付客户端技术规范  网上银行系统信息安全通用规范 |
| 2 | 不要在客户端程序中保存敏感信息 | 中国金融移动支付客户端技术规范  网上银行系统信息安全通用规范  PCI DSS |
| 3 | 若需要在客户端保存敏感信息，则必须加密保存 | 网上银行系统信息安全通用规范  PCI DSS |
| 4 | 在客户端输入敏感信息时要使用安全软键盘 | 中国金融移动支付客户端技术规范  网上银行系统信息安全通用规范 |
| 5 | 只赋予客户端程序业务需要的最低权限 | 信息安全技术网络安全等级保护测评要求 |
| 6 | 确保三方组件的安全性 | 信息安全技术网络安全等级保护测评要求 |

# 手机银行登录场景安全设计方案

在对手机银行登录场景进行业务流程及其威胁分析，并确定登录场景的安全需求后，我们可以得到登录场景的安全设计方案。在此方案中，我们从输入处理、认证管理，通信安全、日志审计、错误处理、会话管理这6方面进行设计，并制定相应的安全控制措施。

## 输入处理

登录时从用户APP提交的手机号、密码、verifycode和验证码等数据要进行有效性验证。检查的具体要求包括：

* 要检查手机号字段必须是纯数字数据，且长度是11位；
* 密码字段必须是数据和字母组合，且长度在6位到20位字符之间；
* 验证码是数据和字母组合，且长度是4位；
* verifycode是数据和字母组合。

并且必须确保所有这些检查控制措施都是在服务器端实施的。若检测到用户输入数据的异常，应对此数据进行抛弃处理并返回登录页面。

## 认证管理

### 有安全的登录控制措施

为了用户体验，一般在用户打开APP首次登录系统时只要求输入手机号和密码进行登录验证，但是在首次登录失败后建议增加图形验证码的校验。如果用户输入密码连续错误6次则应该锁定此账号。由于锁定账号可能导致拒绝服务攻击，因此应该在账号被锁定一段时间后解锁账号，建议锁定时间为1小时。

登录时可检查登录用户手机，若不是之前使用的手机，则增加短信验证码的校验，确保是用户本人进行的操作。图形验证码应由数字和字母组成，具有足够的随机性，长度不应少于4位，具有使用时间限制并仅能使用一次，有效期最多5分钟。

对于短信发送频率也需要控制，一般情况建议间隔为1分钟，避免导致短信轰炸；对于短信有效期也要有安全控制，一般不超过5分钟；短信动态码应随机产生，长度不应少于6位。

### 服务间的访问有认证控制措施

手机银行服务端访问后台数据库服务也要有认证管理，即手机银行需要提交访问数据库的账号密码并在数据库认证成功后才能访问数据库。为了安全考虑，数据库账号应该是一个普通权限的账号，且密码应该满足附录中的密码安全要求。此密码应该保存在单独的配置文件中，并且配置文件只有部署此系统的账号才能访问。

对于手机银行到安保系统的访问也需要有认证控制措施。一般可以通过账号密码、令牌或者证书的方式进行认证控制。

## 通信安全

### 使用HTTPS协议

通常Web访问最常用的就是HTTP协议，但由于HTTP协议是明文传输，因此容易导致登录密码等敏感信息在传输的过程中泄露。为了保证通信的安全，要求在Web访问的通信过程中使用HTTPS协议。具体的就是HTTPS配合SSL/TLS和数字证书来保证通信传输过程的安全。

由于HTTPS是使用SSL/TLS协议来加密数据包，相关的具体安全要求包括：

* 要使用TLS1.2及以上版本的协议来加密数据；
* 其中HTTPS证书必须使用SHA256以上哈希算法签名；
* HTTPS证书必须使用RSA2048位或ECC256位以上公钥算法；
* 应该使用前向加密技术，建议使用ECDHE-RSA或ECDHE-ECDSA。

对于APP到手机银行服务端通信的情况，客户端要检查服务端的数字证书有效性，检查内容至少包括：

* 检查证书的颁发者是否有效；
* 证书是否过期；
* 证书的持有者是否和访问的网站一致。

对于手机银行到安保系统的服务端-服务端通信的情况，互相都应检查对方的证书的有效性，检查内容和前述一致。

为了保证整个通信过程的安全，要求在整个通信过程中都要使用HTTPS协议。

### 传输的密码进行加密处理

基于安全的多重防御思想，应对登录传输的密码进行加密后再发送到服务器端。这需要APP和服务端分别保存公钥和私钥。当用户输入密码后，APP用公钥对密码进行加密并发送到服务器端，服务器端用私钥解密即可得到密码。这里要求使用RSA2048位或ECC256位以上公钥算法。

对于手机银行服务端和安保系统的密码传输，虽然都处于内网中，但是基于安全考虑，建议还是采用上述方案对传输的密码进行加密处理。即手机银行使用公钥加密密码数据并发送给安保系统，安保系统使用私钥解密此密码数据。

## 日志审计

### 关键操作要有日志记录

对于像登录这样的关键操作要有日志记录。应该在服务端实施日志记录动作。记录的内容至少包括：操作分类（登录）、登录手机号、登录时间、手机verifycode、登录结果（成功/失败）。对于像登录手机号、verifycode这样来自用户APP端的数据，在记录到日志前要对数据进行合法性检查，对于非法数据不要记录到日志中。

对于手机银行服务端到数据库的访问，在数据库也要设置进行日志记录。

对于手机银行到安保系统的访问，在手机银行侧也需要记录访问的日志信息，至少也需要包含程序进程、查询的时间、查询的内容、查询的结果等。另外，在安保系统侧也应该记录相应的操作的日志信息。

### 不要在日志中记录敏感信息

不要在日志中记录敏感信息，包括用户的个人信息（比如：姓名、身份证号、银行卡号、密码等），以及系统内部的相关信息（比如：会话id，软件/框架版本等）。

### 日志管理

记录的日志应该统一放在日志服务器进行集中管理和分析审计。对日志要有完整性检查和控制。应只有审计员才能访问日志信息。

## 错误处理

登录失败时应该返回模糊的报错信息，即不管是输入的手机号错误或者是登录密码错误，都应该返回类似“手机号或者登录密码错误”这样模糊的报错信息，不要明确返回类似“手机号不存在”或者“密码错误”这样的报错信息。

对于其它登录过程中的错误或异常情况，要有恰当的错误或异常处理控制措施。当应用程序出错时，只展示给用户通用的错误页面。应使用结构化异常处理机制，捕捉并处理异常现象，避免将应用程序置于不协调的状态，该状态可能会导致信息泄漏或拒绝服务攻击。

错误页面中不能包含系统内部信息或用户个人信息。发生错误时，不要向客户端泄漏信息，不要暴露的内容包括函数名以及调试内部版本时出问题的详细信息。应向客户端返回一般性错误消息。可以将应用程序设置为不向远程用户显示详细错误信息，也可以选择将错误重定向到应用程序页。应捕捉所有未处理异常并将它们发送到一般错误页的页级别或应用程序级别上，创建全局错误处理程序。

## 会话管理

用户登录认证成功后，生成新的会话并设置用户访问的Cookie，其中Cookie值应该有足够的长度，且具有随机性和唯一性，并保证它是不可猜测的。

对于Cookie中的会话id，要恰当的设置path值，还要添加“httponly”和“secure”属性。防止cookie通过跨站攻击被泄露，或者cookie在不安全的http中被传递。

为了提高系统安全性，对会话有效时间进行限制，通常设置为30分钟有效期。若会话在一段时间（如：5分钟）不活动时，对其进行失效处理。

应用系统的同一账号在同一时间应该只能并发一个会话。

对所有的访问请求都要进行会话检查，确保只有有效会话的用户才能访问其相应的业务页面。

在登录过程中，要对用户在短时间内的多重并发会话数进行限制，防止系统被拒绝服务攻击的可能。

另外，在登录过程中，若通信双方中的一方在指定时间内未作任何响应，另一方应能够自动结束会话。

# 手机银行APP客户端安全设计方案

由于APP客户端都是给终端用户使用的，用户对APP拥有完全的控制能力，因此APP很容易被恶意用户分析利用。因此对于APP客户端程序也要进行恰当的安全处理，以增加APP被恶意用户利用的难度。常用的安全控制措施包括：

## 源代码保护

由于APP程序很容易被获取并反编译处理，这样就可以分析源代码，发现其中的漏洞情况，因此要对源代码进行保护，常用的保护控制措施主要有：源代码混淆、NDK保护、程序自校验、加壳等。

## 安全的数据存储

不要在APP客户端中保存用户个人信息、账号密码等敏感信息。如果需要暂时保持敏感信息，应该要对敏感数据进行加密处理，并且要设置数据保存的有效时间。

当应用在后台被挂起时，由于应用数据快照是明文保存在一个目录下的，很容易被恶意程序读取。因此，建议设置登录关键窗口的hidden属性为YES，这样当前在屏幕上显示的内容将被隐藏，返回一个空白的快照来替代任何内容。

由于用户输入的数据可能会被键盘缓存，这可能导致敏感信息泄露。因此当用户在输入敏感信息时，应该禁止键盘缓存功能。

不要在APP的日志中记录或打印敏感信息，并且在正式发布的时候，确保关闭了日志打印开关。

## 权限最小化

程序本身可以在安装时被授予很多权限和功能，如发送短信，手机定位，访问其他应用程序等，这些权限和功能在特定环境下可能被恶意代码所利用。根据软件设计的基本原则“最小特权原则”，在设计应用程序的功能和权限时，只赋予完成操作的必备权限和最少功能。

## 三方组件安全

由于APP程序开发过程中常常会用到一些三方组件，如果这些三方组件存在漏洞，那么也会导致整个APP存在漏洞，从而被攻击的风险。因此APP使用的三方组件需要确保是安全的。

## 使用安全软键盘

敏感数据被通过APP键盘录入系统中。攻击者可通过反编译应用，将键盘钩子（监控程序）捆绑嵌入其中，以监控、窃取用户通过键盘输入的各项数据。因此需要使用安全软键盘，它可以随机分布式虚拟安全键盘，对键盘的数据输入过程、存储过程等进行加密处理，可有效防止数据侦听、键盘劫持、键盘截屏等攻击行为。

# 附录

## 密码安全要求

|  |  |  |
| --- | --- | --- |
| **密码安全基本要求** | | |
| **密码安全策略管理** | **要求概述** | **详细描述** |
| 设置密码时，默认检测密码复杂度 | 系统默认检测密码复杂度，密码至少满足如下要求：  1、密码长度至少6个字符（特权用户至少8个字符）；  2、密码必须包含如下至少两种字符的组合:  －至少一个小写字母；  －至少一个大写字母；  －至少一个数字；  －至少一个特殊字符：`~!@#$%^&\*()-\_=+\|[{}];:'",<.>/?和空格  3、密码不能和账号或者账号的倒写一样；  若设置的密码不符合上述规则，必须进行警告。 |
| 可设置密码出错锁定阈值 | 系统必须提供锁定用户的机制。可选择如下两种方式之一：  方式一：当重复输入错误密码次数（默认3次，次数系统可以设置）超过系统限制时，系统要锁定该用户。  方式二：系统还可以设置下次允许输入密码的间隔时间加倍，采用这种方式时，用户可以不设置自动锁定。 |
| 可设置自动解锁时间（只适用于由于密码尝试被锁定的用户） | 1、对于密码尝试N次失败被锁定的用户，系统要能够设置自动解锁时间，建议默认解锁时间至少为30分钟。  2、用户被锁时间达到预定义时间，应该能自动解锁该用户。  3、在锁定时间内，仅能允许管理员角色所属账号手动解锁该用户。 |
| **密码安全使用规则** | 操作界面中的密码不能明文显示 | 键入密码时不能明文显示出来(操作界面中的输入密码可不显示或用\*代替)，包括在终端上打印或存储在日志中时也不能明文显示密码，即使是内存中的明文密码（如登录期间），也应在使用后立即覆盖。 |
| 密码输入框内容禁止拷贝 | 密码输入框不支持拷贝功能。 |
| 缺省密码符合复杂度要求 | 对于系统内置账号的缺省密码，密码应符合复杂度的要求，并在客户资料中提醒用户修改。 |
| 用户可修改自己的密码 | 1、用户修改自己密码时必须验证旧密码；  2、不允许修改除自身账号以外的账号的密码（管理员除外）。 |
| 密码不能在网络中明文传输 | 密码等认证凭证在传输过程中必须加密，使用高安全等级的加密算法。 |
| 密码在本地存储时必须加密 | 1、密码不能够明文写入日志文件、配置文件以及cookie中；  2、密码文件必须设置访问控制，普通用户不能读取或拷贝加密的内容。 |

## 威胁与对应安全控制措施参考

|  |  |  |
| --- | --- | --- |
| 威胁分类 | 威胁描述 | 安全控制措施 |
| S欺骗身份 | S1使用其他用户的手机号和密码进行登录 | 验证用户手机的短信验证码和密码 |
| S2暴力猜测其他用户的登录手机号和密码并登录 | 验证用户手机的短信验证码或者图形验证码 |
| S3冒充安保系统 | 通过密码、令牌或证书等方式认证安保系统 |
| T篡改数据 | T1篡改APP程序中登录访问的地址 | 对APP程序增加源代码保护措施（如：代码混淆、加密等） |
| T2篡改APP端发送到服务端的登录数据 | 对APP到服务端使用加密协议（如：https）传输数据 |
| T3篡改安保系统发送到手机银行的数据 | 对手机银行到安保系统使用加密协议（如：https）传输数据 |
| R否认 | R1用户否认是其本人登录的手机银行 | 手机银行记录用户登录过程的日志 |
| R2安保系统否认手机银行与其进行交互 | 手机银行记录与安保系统交互过程的日志 |
| I信息泄露 | I1反编译APP程序获得其中的登录相关信息 | 对APP程序增加源代码保护措施（如：代码混淆、加密等） |
| I2恶意程序通过记录键盘操作获得登录手机号和密码信息 | 在输入敏感信息时使用安全的软键盘 |
| I3恶意程序通过截屏获得登录手机号和密码信息 | 对用户输入的密码信息不要明文回显在页面上 |
| I4恶意程序获得APP程序中的其它敏感信息 | 不要在客户端程序中保存敏感信息，若需要在客户端保存敏感信息，则必须加密保存 |
| I5APP程序传输登录信息到服务端过程中信息泄露 | 对APP到服务端使用加密协议（如：https）传输数据 |
| I6手机银行数据库中的登录相关信息泄露 | 数据库敏感信息访问有恰当的权限控制措施 |
| I7服务器端与安保系统传输的登录密码等信息泄露 | 对服务器端到安保系统使用加密协议（如：https）传输数据 |
| I8登录失败提示信息泄露具体错误信息 | 使用模糊化的错误提示信息 |
| I9系统程序异常或错误泄露系统内部信息 | 系统有恰当的错误处理机制，错误发生时只返回通用的错误页面 |
| D拒绝服务 | D1大量的并发登录请求导致登录拒绝服务 | 系统有并发会话数控制措施 |
| D2多次尝试登录导致账号被锁定 | 因多次登录失败被锁的账号有自动解锁机制 |
| D3畸形的数据查询导致系统拒绝服务 | 系统有恰当的错误处理机制 |
| E权限提升 | E1绕过登录认证控制直接访问手机银行业务 | 系统对所有访问都有恰当的认证控制措施 |