Q/GUOSEN

国信证券股份有限公司企业标准

Q/GUOSEN-MAN-SEA 01-2021

国信证券移动应用安全开发规范

2021-08-20 发布 **2021-08-20 实施**

国信证券股份有限公司 发布

前　言

本标准于 2021 年 7 月初次起草发布，8 月首次实施，在编制过程中得到各位同仁的大力支持，在此表示感谢！由于编制时间紧促，难免有遗漏之处，恳请广大参阅者多提高贵意见，以供参考校正。

本标准由国信证券股份有限公司提出。

本标准起草单位：国信证券股份有限公司。

本标准主要起草人：金文佳、朱毅。

本标准于 2021 年 8 月首次发布

引 言

随着移动互联网新兴技术的蓬勃兴起，层出不穷的创新业务，移动应用的使用场景日益广泛，在公司展业与办公管理的使用比重逐渐增大。这种形势下信息系统建设与安全运行的压力越来越大， 所面临的信息安全形势日趋复杂。金融行业的移动互联网应用程序（APP）安全问题尤其严峻。

国信证券移动应用开发安全规范约定了国信证券移动应用在开发阶段应该关注的安全问题，以及解决安全问题需要实现的安全需求，并可对移动应用设计、开发、测试、上线、运营全生命周期进行规范指导，以消减移动应用造成的安全风险。

1 适用范围和对象

本文档主要适用于移动应用的需求、设计、开发阶段，帮助应用开发人员梳理安全需求，提出安全设计规范，并在开发过程中落地，提升系统安全性。

2 引用标准

ISO/IEC 27001 信息安全管理体系-要求

ISO/IEC 27002 信息安全管理实用规则

ISO/IEC 15408 信息技术安全评估通用准则（简称 CC）

OWASP Development Guide

OWASP Code Review Guide

OWASP Testing Guide

OWASP Secure Coding Practices Quick Reference Guide

3 术语与定义

3.1 白名单

白名单是定义用于许可放行的集合。

3.2 黑名单

黑名单是定义用于禁止拒绝的集合。

3.3 重放攻击

重放攻击就是把以前窃听到的数据原封不动地重新发送给接收方，已达到欺骗或者重复操作的效果。

3.4 敏感数据

一旦泄漏、非法提供或者滥用可能危害人身和财产安全，极易导致个人或企业名誉财产受到损害等 的个人及企业信息。

3.5 中间人攻击

中间人攻击（Man-in-the-MiddleAttack，简称“MITM 攻击”）是一种“间接”的入侵攻击，这种攻击模式是通过各种技术手段将受入侵者控制的一台计算机虚拟放置在网络连接中的两台通信计算机之间，这台计算机就称为“中间人”。

4 服务端安全

4.1 框架组件

在使用第三方框架与组件进行移动应用开发时，应遵从以下安全要求：

a. 在选用框架组件时，使用最新版本，在官方渠道下载。

b. 根据应用开发需求，删减或修改框架默认功能。删除不需要使用的功能，并对框架的后台地址和密码等默认配置进行修改。

4.2 输入输出

对于应用程序的输入输出应遵从以下安全要求：

a. 应通过黑名单过滤结合白名单过滤的方式，保证输入数据安全性。建立威胁字符黑名单，统一过滤所有外部输入数据。对于外部输入的富文本数据，需使用特殊的黑名单过滤机制，不能使用通用的黑名单过滤。对于可枚举类型的外部数据，在进行黑名单过滤后，应使用白名单进行二次过滤。

b. 为保证业务系统的安全性，在必要的业务功能中为用户提交的数据或提交数据的频度设置边界值检查机制，例如单笔转账金额限制，单日股票交易量，单日短信验证码发送数量限制等，防止输入负数导致逆向转账、10 元股票 0 元购、超长整数计算结果变负数等不可预知的问题。

c. 对于输出在 APP 应用显示的数据，若数据加载在 HTML5 页面中，则服务器端应对数据进行相应的编码处理。

d. 对于所有在 HTML 上下文中的输出，使用 HtmlEncode（ISO-8859-1）进行编码转换。

e. 对于所有在 JavaScript 上下文中的输出，使用 JavaScript escape 转义，并要求输出的变量在引号内部。

f. 应尽量避免在 CSS 上下文中使用用户可控变量。若有需求，必须对 CSS 输出的用户可控数据进行 CSS escape 转义。

g. 在将客户可控数据插入到 URL 中时，需要对插入的数据进行 URL 编码。

4.3 会话管理

会话的安全管理应该遵守如下安全要求：

a. session id 在服务端创建保存。

b. 为避免会话被识别，session id 需具备随机性。

c. 在未登录情况下，应使用临时 session 来维持会话。

d. 用户登录并建立一个会话时，若发现此用户有旧会话，则注销旧会话。

e. 在身份验证之时，若访问链接从 HTTP 变为 HTTPS，则更新会话标识（一般情况下，不建议从 HTTP 与 HTTPS 中转换）。

f. 当前会话下，如果客户端设备信息（如设备 DeviceId、MAC 地址等）发生变化时，应强制销毁当前会话。

g. 对于重要的请求应防护会话重放攻击，使用请求签名防范会话重放攻击。

4.4 身份认证

身份认证应遵从以下安全要求：

a. 身份认证密码需要有复杂度要求，12 位以上、包含字母数字与特殊字符、不能包含用户名。

b. 身份认证接口使用双因素或者验证码实现防暴力破解的问题。

c. 认证失败时，错误提示模糊处理：不应该出现“用户名不存在、密码错误”的提示，代替为“用户名或密码错误”。制定登陆失败锁定机制。

d. 使用图形验证码时，图形验证码里的字符做扭曲处理，并添加干扰线。图形验证码应该动态生成，不重复，以防止根据图片 hash 进行内容匹配。图形验证码必须是一次性的，每次验证之后必须更新。图形验证码对应的字符内容只能在服务端保存。

e. 使用手机短信验证码时，每条短信认证信息只能使用一次。认证信息在服务器端生成。每条短信认证信息的有效时间不超过 15 分钟。每个手机号在 30 分钟内连续未正常使用的短信验证

码不能超过 4 条。认证码强度要求：保证随机性，至少 6 位。发送短信之前要求经过验证码认证。短信网关要对用户发送的短信内容进行校验，限制用户发送的字符长度，过滤特殊字符。

f. 修改密码策略，应首先验证原口令是否正确，原密码和新密码需要同时提交到服务端。

4.5 权限控制

为了保证权限控制的有效性和安全性，必须遵循：

a. 权限控制标识必须存储在可信数据源中，如 session、数据库、配置文件。

b. 查看用户私有信息应根据 session 中的 user id 来进行查询，而不是根据客户端提交的参数。

c. 检查用户是否具备管理员权限应根据从数据库中查询的权限来判断。

4.6 异常处理

在进行错误处理时需遵从以下要求：

a. 在所有可能出现异常的地方，捕捉程序异常并友好地处理异常。

b. 系统产生的错误信息不能向客户端显示。

c. 自定义友好的错误页面来代替默认的错误页面向客户端展示。

4.7 日志审计

为了保证日志信息真实可靠，不可伪造和篡改，必须满足如下安全要求：

a. 日志真实可靠：写入日志的数据来源必须是用户不可控的，例如业务操作行为应是应用系统定义好的，日志中的操作人用户名应根据当前会话来得到。

b. 内容满足检查要求：能够根据时间或用户名等信息查到操作内容。

c. 日志内容不包含用户密码等不必要的敏感信息。

4.8 隐私保护

为了保护用户隐私，应该采用不完全显示的方式展现用户敏感数据，例如：

数据类型	数据内容	不完全显示方式
真实姓名	张三四	张**
身份证号	352714198007070123	3527**********123
手机号	17033890403	17033****03

邮箱地址	Myemail123@gmail.com	Myemail**@gmail.com
银行账户	6220432568904621	6220*********621
资金账户	620000365409	620******409

要使用星号代替的情况包括但不限于：

1．在页面显示用户信息时。

2．在手机短信中显示用户信息时。

3．在给用户发送的邮件中显示用户信息时。

4.9 加密存储

为了保证数据的完整性、可靠性和机密性，确保只有合法用户才可以访问被加密的数据和文件，需遵从以下安全要求：

a. 应用程序应使用安全的算法储存密码数据，禁止将明文密码直接保存在数据库或配置文件中。

b. 用户密码存储到数据库时，应使用安全的哈希算法（如 sha256、sm3 等），并进行加盐处理。salt 应使用可靠安全的伪随机数生成器生成，保证每个用户密码的 salt 不同。盐和经过哈希处理的密码存储在不同数据表中。

c. 应使用公开的密码算法，禁止随意修改算法和自己设计算法。

d. 应用程序调用密码算法时，应选择安全的算法（AES256、3DES，SM4 等），禁止使用强度较弱的算法：DES、MD5 等。

4.10 文件上传

为了防止攻击者通过文件上传功能上传恶意文件，植入后门，文件上传功能应该满足如下安全要求：

a. 限制允许上传的文件大小，例如要求上传图片不能超过 2M。

b. 在服务端检查文件后缀：取文件名参数中的最后一个.符号之后的扩展名，统一大小写之后进行检查。使用白名单方式进行文件类型检查，如果目标文件的扩展名不在白名单中则拒绝上传。

c. 保存文件路径保密：显示上传的文件时，使用文件 id 进行调用，不要直接显示文件地址。

d. 保存上传文件目录权限，禁止“执行权限”。

e. 对上传的文件进行重命名，例如（日期+6 位的随机数+后缀名）。

f. 上传文件存储到 web 目录以外的位置，禁止用户通过 url 直接访问。

4.11 文件下载

在文件下载和文件引用功能中，应该避免出现任意文件下载引用漏洞。需遵从以下安全要求：

a. 文件定位：禁止直接根据文件位置和文件名来定位下载文件，要下载的文件应该根据一个随机生成的无规律的 id 来定位。

b. 权限检查：文件下载和引用时，应该检查该用户是否具有此文件的下载或引用权限。

4.11 通信安全

服务器端应配合客户端使用加密通信信道或者是报文加密的方式来保证数据传输的安全性。当使用加密信道时，最常见的方式是采用 SSL/TLS 协议对通信信道加密。

5 客户端安全

5.1 客户端保护

客户端保护需遵从以下要求：

a. 应用程序应具备防范内存信息泄漏的功能，避免攻击者使用工具查看内存中用户密码等敏感信息。

b. 应用程序应具备防范键盘记录木马的功能，避免攻击者通过键盘记录截取获得用户密码等敏感信息。

c. 应用程序应具备防范截屏木马的功能，避免攻击者通过屏幕截取获得用户密码等敏感信息。

d. 应用程序应具备防范二次打包的功能，避免攻击者修改应用代码，加入恶意代码，然后重打包发布。

e. 应用程序应具备 Activity 防劫持功能，防止攻击者通过启用后台木马服务，切换给用户钓鱼登录界面，泄漏用户输入的帐号和密码等敏感信息。

f. 应用程序在发布时应进行源代码混淆处理，增加代码阅读难度。

5.2 输入安全

对于客户端用户输入，需遵循以下安全要求：

a. 客户端应配合服务器端对输入的数据进行格式校验，给予用户提示。对于可枚举类型的输入数据，应使用白名单的方式进行检查，若输入内容不符合格式要求则拒绝用户请求。

b. 密码策略

c. 为了保障用户口令安全，输入的密码应该在用户的屏幕上模糊显示。

d. 为了保证用户输入的保密性，系统应提供自主开发的软键盘功能，在输入敏感信息时，使用自定义软键盘而不调用系统默认软键盘。

5.3 数据保护

保障客户端数据安全，需遵从以下安全要求：

a. 客户端应用中禁止以任何形式保存用户密码信息。包括但不局限于 SQLite、文件、SharedPreferences（Android）、NSUserDefaults（iOS）、keyChain（iOS）、LocalStorage（HTML5）。

b. 客户端应用中需要存储用户密码以外的敏感数据时，应进行加密保存，例如：使用 SQLCipher 对 SQLite 数据库进行加密。

c. 防范日志中输出敏感信息

d. 日志记录中不得以任何形式保存或输出密码、密钥等数据，其他敏感性数据仅应在脱敏或加密的前提下保存。

e. 为了保护用户隐私，在客户端显示数据时应对用户敏感信息进行部分遮盖处理，不应在客户端存储或显示明文用户敏感信息。

5.4 防范中间人攻击

为防范中间人攻击，需遵从以下安全要求：

a. 客户端和服务器端通信时，使用加密传输，客户端校验完整的证书链，验证服务端证书是否合法，是否在有效期内，域名信息是否和实际信息一致。

b. 如果服务端使用自签名的证书，应使用公钥锁定等方式确保通信安全，避免受到中间人攻击。

c. 客户端向服务端提交的委托交易等请求，应使用数字签名技术对发送服务端的请求进行签名，发送方使用私钥进行签名，接收方使用发送方的公钥验证签名，保证数据不被篡改。