APP安全评估撰写提交内容

产品名称	APP安全评估撰写提交内容
公司名称	河南刘贵商务服务有限公司
价格	.00/件
规格参数	品牌:融河矩媒 发票:支持/对公
公司地址	河南省南阳市卧龙区卧龙岗街道卧龙路经纬国际1号楼810（注册地址）
联系电话	13323693821 13140513661

产品详情

移动终端APP数据安全存储评估。该评估内容包括如下:

(1) 检查该应用程序的数据可能的本地存放位置，包括但不限于数据文件，日志文件、数据库文件、会话cookie、配置文件、SD卡等;

(2) 检查该数据文件、日志文件、数据库文件、会话cookie、配置文件、SD卡文件是否包含记录敏感信息;

(3) 评估该应用程序是否采取足够的安全措施(如:加密方式、访问权限)保护存放敏感信息的文件。

移动终端APP数据安全传输评估。该项评估内容包括如下:

(1) 检查该应用程序传输敏感信息过程中是否采用SSL/TLS 数据加密传输方式;

(2) 评估SSL加密算法强度(推荐密钥长度为: 2048 位);

(3) 评估客户端是否对SSL证书合法性进行校验。

移动终端APP安全认证与鉴权机制检测。该项评估内容包括如下:

(1) 评估应用程序是否采用适宜的安全认证方式(如“ 口令+验证码 ”“ 口令+短信 ”、“ 口令+令牌 ”、“ 口令+证书 ”等);

(2) 评估应用程序对密钥/密码的安全存储保护方式(推荐哈希算法: SHA-512， 加密算法: RSA-2048、AES-256);

(3) 评估应用程序安全的会话机制(安全cookie方式、session 方式);

(4) 评估应用程序是否过度授权(如管理后台向低权限用户开放)。

移动终端APP数据上传安全检测。该项评估内容包括如下:

(1) 检查管理后台是否关闭非必要上传功能或模块，是否关闭非必要WEB管理方法(put、 move、 delete等);

(2) 检查前端和后端是否严格限制用户侧上传功能(如文件类型、文件格式、文件大小等);

(3) 评估是否对用户，上传数据的合规性(如暴恐、涉黄、政治言论等)进行安全审核(人工或技术)。移动终端APP、Web应用安全检测。例如: SQL 注入、XSS、CSRF、 弱口令和平行越权等。

移动终端APP反编译安全检测。该项评估内容包括如^下:

(1) 评估是否能通过测试工具对应用程序进行反编译得到源代码;

(2) 评估是否可通过测试工具发现应用程序工作流程。

应用程序恶意访问操作检测。该评估内容主要如下:

(1) 评估应用程序的本地执行的配置与权限;

(2) 评估应用程序是否会访问/读取本地其他文件获取用户信息;

(3) 评估应用程序是否会截获/记录/传输应用登录访问的敏感信息;

(4) 评估应用程序在运行时是否会访问非应用外internet访问及执行非许可的动作;

(5) 评估应用程序是否会调用/修改本地其它系统功能(如摄像头、录音、音量调节)

进行非正常应用;

(6) 评估应用程序权限使用知情告知的充分性。

>移动终端软键盘安全性监测。评估涉及用户敏感信息交互是否采用有效的防窃取措施，如软键盘。

>移动终端完整性检测。评估客户端程序是否在启动和更新时存在真实性和完整性校验，防范客户端程序被篡改。

运行阶段安全要求

1、各APP应用开发使用部门，依据电信业务系统安全运维相关管理办法，负责APP应用的日常安全运维工作;保证APP应用持续稳定运行;

2、企信部安全中心，将所有APP下载渠道纳入自建或第三方大数据监测中心进行实时监控，监测内容包

括包括版本、渠道、下载源、下载量等。从而，第一时间发现盗版应用，进行正版盗版APP信息精准对比，使电信安全部门清晰了解APP的正盗版情况及升级情况;做到及时发现、及时处理。

下线阶段安全要求

根据电信业务系统下线相关安全管理规定，进行APP应用下线工作，及时删除销毁敏感数据。