小程序安全

1. **背景**

**1.1金融行业小程序现状及挑战**

小程序因其可以无需安装即可使用，体验接近原生，且可广泛在微信内传播，愈发被金融客户重视。同时，随着金融小程序逐渐规模化，国家在政策上也加强了对移动应用的安全监管，对等级保护和用户隐私安全合规的要求也日渐严格，近日，微信小程序等渠道也被明确纳入监管范畴。加上“业务更迭加速、需求数量提升、业务规模扩大、安全隐患增加”等问题，金融行业的小程序生态需要建立“安全开发、运行监测、营销风控、金融合规”完善的安全体系。

**1.2小程序安全风险**

如今越来越多的微信小程序开发者/运营者正在为品牌商、政府、企业等提供开发/运营服务，帮助其做数字化转型，以及产业化升级等。随之不断涌现出海量一站式小程序技术支持平台，小程序外包化开发和部署成为了大多数客户的选择，快速开发迭代、架构和代码安全性差、缺少深入测试等原因，加之外部越来越多黑客人员、不法工作室涉足小程序蓝海市场，导致小程序数据泄露、业务被攻击等安全问题逐渐增多。

当前金融小程序主要面临的安全风险有：

1. 数据泄露：键盘输入劫持，后台接口暴露，用户隐私泄露
2. 仿冒应用：伪造交易UI，篡改交易信息，盗取用户隐私
3. 交易隐患：交易数据篡改，支付密码泄露，账号信息泄露
4. 恶意攻击：病毒、木马攻击以及植入
5. 安全漏洞：应用存在安全隐患，易被攻击、破解造成损失
6. **产品介绍**

腾讯TMF小程序安全，基于腾讯国内领先安全实验室，十余年安全对抗经验，经过微信小程序大流量安全防护检验，提供行业领先的小程序安全方案，打造“安全检测、代码加固、渗透测试、设备安全”的小程序安全产品矩阵，全面满足监管对互联网应用的安全合规要求。

**2.1 TMF小程序安全产品**

* **小程序安全检测**

安全检测是帮助客户在测试阶段发现小程序安全漏洞，并提供修复建议，帮助客户尽可能避免发生因安全漏洞导致的资产及名誉受损。小程序安全检测具备以下优点：

* 检测能力强，充分保障企业产品安全
* 满足网络安全法、等保2.0、隐私合规等政策要求
* 可私有化独立部署，保障企业数据安全
* **小程序代码加固**

代码加固是针对应用前端代码的加密服务，用户只需将代码(路径或文件)传递给加密工具，即可实现字符串加密、属性加密、调用转换、代码混淆等多项保护措施，提高攻击者分析前端代码逻辑的难度，从而保护代码安全 。小程序代码加固具备以下能力：

* 防逆向：通过对JS文件中的变量名进行无意义混淆，降低代码可读性，使代码不易被逆向分析
* 防篡改：可避免包内被修改后所有代码类文件进行二次打包
* 防调试：实时检测程序调试状态，防止代码逻辑暴露
* 防窃取：对字符串进行加密，防止本地数据文件被窃取
* **小程序渗透测试**

小程序渗透测试，为企业产品提供全面的渗透测试服务，以模拟黑客攻击的形式，提前预知各类业务数据泄露，券币盗刷、资产受损、数据被篡改等各类安全风险。

产品优势：

* 独家支持小程序渗透

小程序内嵌于微信或其他APP内，小程序的代码脚本、本地数据、权限控制都受到微信APP的保护，由于上述小程序技术架构特点，市面所有APP或Web渗透测试服务无法适用于小程序，更无法全面地测试小程序安全性。腾讯TMF小程序渗透测试，在掌握微信小程序系统架构基础上，渗透微信Native层及V8脚本引擎，覆盖从微信用户个人信息授权、小程序本地代码和业务逻辑、本地缓存数据、网络通信数据、后台服务风险，真正做到对小程序安全的全面评测。

* **小程序设备安全**

腾讯移动应用安全设备风险识别产品能力实现假人假机-假人真机-真人真机的全面覆盖，全方位抵御设备欺诈行为 。