Shared Preferences 文件敏感信息保护

测试描述：

App 在处理运行时产生的敏感数据（如账号、密码、手机号、Cookie、Token 等业务相关敏感信息）时，将未经加密的敏感信息以明文的形式保存在文件或者本地数据库中。

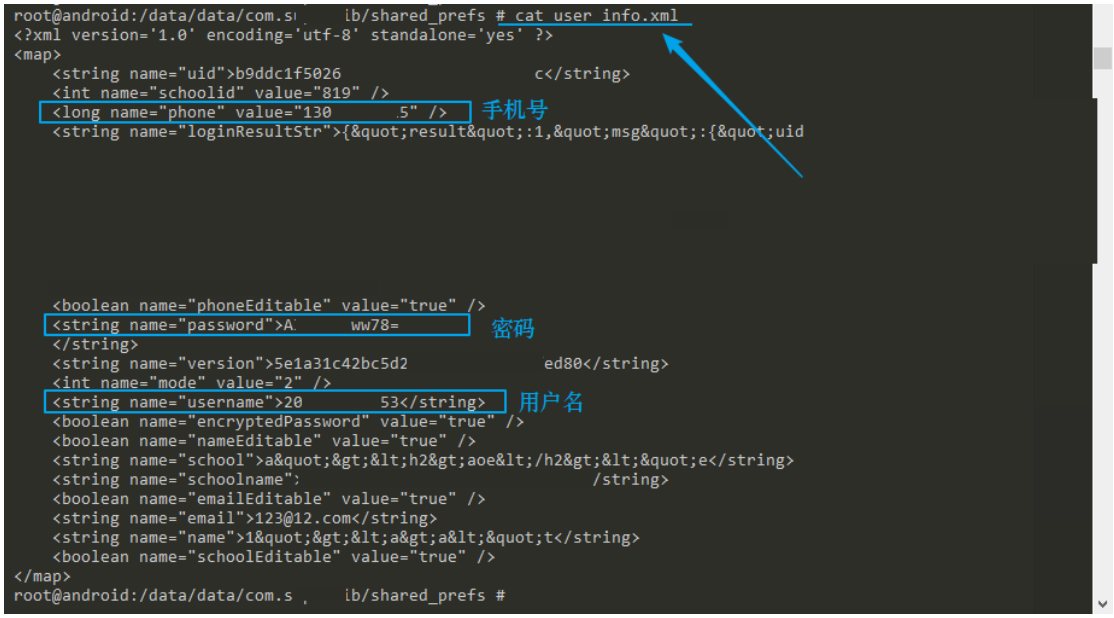
风险危害：

当用户手机失窃或者连接到电脑等情况时，这些明文的敏感数据可能被第三方程序获取，导致用户的账号、密码、手势密码、手机号等个人敏感信息容易泄露。

测试步骤：

1、登录目标 APP，先尽可能多的完善个人信息。

2、使用 adb 工具查看[/data/data/package-name/shared_prefs/]目录下的文件，查找其中是否包含敏感信息，如下图：



修复建议：

1、对敏感信息进行加密保护。

2、根据业务需求确定必需在本地存储的数据，不必要的数据不存储。

参考链接：

a) Android 数据存储之 SharedPreferences 及如何安全存储
https://www.cnblogs.com/whoislcj/p/5494761.html

b) Android 本地数据存储：Shared Preferences 安全风险浅析
http://www.tuicool.com/articles/rqyE3q

c) Android 密钥库系统
https://developer.android.com/training/articles/keystore.html