

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：

```
root@android:/data/data/com.sib/shared_prefs # cat user info.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="uid">b9ddc1f5026                                </string>
  <int name="schoolid" value="819" />
  <long name="phone" value="1305" /> 手机号
  <string name="loginResultStr">{"result":1,"msg":"","uid":
    <boolean name="phoneEditable" value="true" />
    <string name="password">Aww78= 密码
  </string>
  <string name="version">5e1a31c42bc5d2                        ed80</string>
  <int name="mode" value="2" />
  <string name="username">2053</string> 用户名
  <boolean name="encryptedPassword" value="true" />
  <boolean name="nameEditable" value="true" />
  <string name="school">"&lt;h2>";&lt;/h2>"</string>
  <string name="schoolname">                                /string>
  <boolean name="emailEditable" value="true" />
  <string name="email">123@12.com</string>
  <string name="name">"1"&lt;h2>";&lt;/h2>"</string>
  <boolean name="schoolEditable" value="true" />
</map>
root@android:/data/data/com.sib/shared_prefs #
```

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 数据存儲之 SharedPreferences 及如何安全存儲
<https://www.cnblogs.com/whoislcyj/p/5494761.html>
- b) Android 本地数据存儲: 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>