

# IOS客户端通用测试

## 项目范围

适用于IOSAPP安全测试项目基本测试的实施

## 准备工作

一台电脑、一部苹果越狱机 (本次的测试机:iphone 5s version:9.0-9.1完美越狱)系统(Mac、windows 7虚拟机)

Ps:

完美越狱简单地说就是越狱很彻底，破解了操作系统的读写权限，完美越狱完成以后可以自由使用，开关机、下载等。

而不完美越狱，则表示iPhone或iPad不能像越狱之前一样随时可以关机



The background features a dark blue color scheme with a glowing hexagonal grid pattern. Several padlock icons are scattered across the grid, symbolizing security. In the bottom-left corner, a stylized globe is depicted with a network of white dots and lines, representing global connectivity or data flow.

# IOS客户端数据安全

## 1.1 日志信息安全

## 测试项描述

开发者习惯使用日志辅助程序调试，在日志中打印信息，则可能泄露访问链接、收发的数据包甚至身份凭证等内容。



## 0x01使用xcode

Windows->Devices

## 0x02使用iTools

工具箱->实时日志



## 风险评级

视泄露数据的情况而定。

**高风险**——泄露用户身份凭证(如token、cookie)、用户或其他用户隐私信息

**中风险**——泄露关键函数(加解密、校验函数)调用和逻辑信息或者部分隐私信息

**低风险**——非上述两种信息之外的内容泄露评定为这个等级

```
May 25 14:24:22 iPad UMP_Project[8723] <Error>: SecOSStatusWith error:[-25243] The operation couldn't be completed
-25243 - Remote error : The operation couldn't be completed. (OSStatus error -25243 - NoAccessForItem)
May 25 14:24:22 iPad securityd[203] <Error>: securityd_xpc_dictionary_handler UMP_Project[8723] add The operation
completed. (OSStatus error -25243 - NoAccessForItem)
May 25 14:24:22 iPad UMP_Project[8723] <Error>: SecOSStatusWith error:[-25243] The operation couldn't be completed
-25243 - Remote error : The operation couldn't be completed. (OSStatus error -25243 - NoAccessForItem)
May 25 14:24:22 iPad UMP_Project[8723] <Warning>: info={"serviceid":"umCommonService","appcontext":
{"appid":"pmmobile.nc.yonyou.com","tabid":"","funcid":"","funcode":"pmmobile.nc.yonyou.com","userid":"","forcelogin
D5DXdxoE0vZSAdDVnA6YDi0X0pme0SSbMhm%2FtItTpoMsShrTQWLRPk6zhqoBrN9zhIwAkSH%0A9FJE4I702Y%2FeURzYil3uzarqzzaGB6W6U7tOR
3D","pass":"123456","sessionid":"","devid":"0417D6D2-3978-4FE2-88A3-577F92312C04","groupid":"","controllerid":"nc.
ntroller","massotoken":"","user":"pmuser50"},"servicecontext":
{"viewid":"nc.mob.pm.controller.RelateMeController","contextmapping":"ncdata","params":
{"contextmapping":"ncdata","autoDataBinding":"false","error":"initDataNotReady()","callback":"allDataReady()"},"win
troller","controllerid":"nc.mobile.pm.RelateMeController","callback":"","actionid":"","actionname":"fetchAllRelated
{"firmware":"","style":"ios","lang":"en","imsi":"","wfaddress":"0417D6D2-3978-4FE2-88A3-577F92312C04","imei":"","ap
uid":"0417D6D2-3978-4FE2-88A3-577F92312C04","bluetooth":"","rom":"","name":"iPad","resolution":"","wifi":"lmkj","m
4FE2-88A3-577F92312C04","ram":"","model":"iPad","osversion":"8.1.1","devid":"0417D6D2-3978-4FE2-88A3-577F92312C04",
screenSize":{"width":"375 000000","height":"499 000000"},"mode":"iPad AC","touchscreen":"","ll
```



## 修复方法

将所有的NSLog调用去掉再重新编译打包程序



The background features a dark blue color scheme with a glowing hexagonal grid pattern. Several padlock icons are scattered across the grid, and a stylized globe is visible in the lower-left corner. The text is centered in a white, sans-serif font.

# IOS客户端数据安全

## 1.2 程序数据存储安全

## 测试项描述

检设备中程序对应的数据文件夹是否包含敏感数据。由于设备可以进行越狱，且越狱之后数据不会丢失，则导致本地存储敏感信息将造成较大风险。



## SandBox文件存储结构

SubDirectory	Description
AppName.app	存储 app 执行文件和静态资源文件，该文件夹为只读
Documents	App 的配置文件等，该文件夹的内容会被同步到 backup 文件中
Library	Application support files
Library/Preference	应用程序特定的首选项 ( <u>plist</u> 文件)
Library/Caches	缓存数据 (cache file and cookie file)，该文件夹内的内容不会被同步
tmp	在连续启动应用程序时不需要保留的临时文件



## 测试点有哪些？



## 测试步骤

- 1.在设备上安装程序
- 2.运行程序，进行较大量的操作用来填充数据
- 3进入设备文件系统，从数据文件夹中获取所有文件:

在越狱设备中，本测试项需要AppSync(hook内核，绕过程序的签名验证)和A FC2(越狱文件系统)

在iOS7中，相关的程序和数据内容在目录:/var/mobile/Application/<UUID>

在iOS8中，相关的程序内容在目录:/var/mobile/Containers/Bundle/Application/<UUID>

在iOS8中，相关的数据内容在目录/var/mobile/Containers/Data/Application/<UUID>

- 4.检查 plist 文件、slite 文件、binarycookie 文件
- 5.使用keychaindumper 获取 keychaindumper中的信息
- 6.除了上面的文件之外，还有其他存储的文件(如:pdf 文件)



## 文件存储目录

1.plist:全名Property List, 属性列表文件, 它是一种用来存储串行化后的对象的文件。

文件是xml格式的。一般都是存储在各种目录下, 视情况而定

2.Salite:一般在document下, 根据开发者的情况而定

3.Binarycookie:一般在/private/var/mobile/[app directory]/Library/Cookies/

利用BinaryCookieReaderpy工具进行查看



## 风险评级

视信息泄露的严重性而定。

**高风险**——大量用户信息或者泄露了登录密码、支付密码等高敏感度信息

**中风险**——未进行类名混淆以及逻辑混淆

**低风险**——进行了大部分类名混淆，未进行逻辑混淆



## 修复建议:

针对UserDefaults, 建议加密存储, 而且建议使用用户输入数据作为加密密钥(但是可能会影响到自动登录):

- 1.针对salite, 使用SQLCipher进行加密, 密钥使用用户输入数据或者使用服务器相关内容;
- 2.针对binarycookie, 只能清除

```
//Delete previous cookies
NSHTTPCookieStorage *cookieStorage = [NSHTTPCookieStorage sharedHTTPCookieStorage];
for (NSHTTPCookie *each in [[cookieStorage cookiesForURL:YOUR_URL] copy] autorelease) {
    [cookieStorage deleteCookie:each];
}
```

- 3.针对keychain, 加密存储, 密码依然使用用户存输入的数据;另外因为keychain在程序删除仍然存在, 且越狱机子上用keychain 保存完全没有安全可言, 不推荐使用keychain 存储高敏感度数据;
- 4.对于其他文件, 进行独立加密, 并解密读取即可;



The image features a central figure of a person wearing a black hoodie, with their right hand pressed against their forehead in a gesture of stress or contemplation. The background is a vibrant blue digital landscape. It includes a glowing globe on the right side, overlaid with a network of white and blue lines and dots. Scattered throughout the background are several padlock icons, some of which are open, symbolizing digital security or vulnerabilities. The overall aesthetic is high-tech and cyber-themed.

谢谢观赏