**XPOSED(VXP)/FRIDA Report of PoRE**

Student ID 1930xxxxxx

Name your name

* **Tasks List**

Write down the tasks list you finished and the corresponding score

1.贪婪洞窟无限充值

2.

(Or more)

* **Project Demo Video**

**Baidu Netdisk** **share link (and verify code)**

* **Task1**
* **Introduction**

Introduce the task briefly

在贪婪洞窟这款游戏（版本为1.2.0）中免费充值

* **How you find the target function**

Introduce how you reversed the target apk and located the target function you want to hook

**1.用jeb打开apk，由于这款游戏由雷霆工作室制作，进入com.leiting目录**

**2.查看目录下的包，发现在sdk内有一个叫pay的包，应该与支付相关。**

**3.通过查看调用关系可以确定主类是LeitingPay，支付逻辑应该在该类里。**

**4.阅读该类的代码，其逻辑主要是进行各类检查，调用支付宝/微信/银联的支付函数，然后显示支付结果，但未找到与游戏内数据有直接关系的函数。支付宝等公司的支付函数感觉不太好下手，只好另辟蹊径。**

**5.经过一些搜索之后，发现com.leiting.sdk.channel.leiting下的LeitingSdkUser调用了LeitingPay的一个实例。进入该类，发现一个名为doSdkPay的函数，逻辑为：调用LeitingPay，然后根据返回结果调用fail或success。可以确定，fail就是应该hook的函数。**

* **How you hooked the function**

Introduce how you hook the target functions to realize your goal

**1.先尝试hook上fail函数，但日志提示找不到该类，想起助教的提示，可能这个类在另一个dex中。**

**2.根据pj1网页的链接，先hook上attach函数，再load目标类，日志显示hook成功。**

**3.在fail函数调用之前先调用success函数，这样虽然显示购买失败，但充值已经生效。**

* **Task2**
* **Introduction**

Introduce the task briefly

* **How you find the target function**

Introduce how you reversed the target apk and located the target function you want to hook

* **How you hooked the function**

Introduce how you hook the target functions to realize your goal