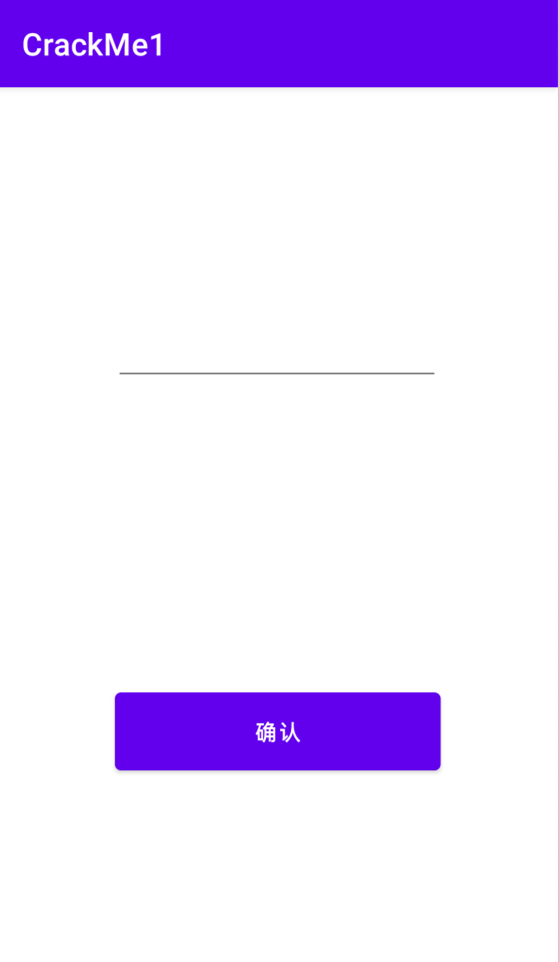
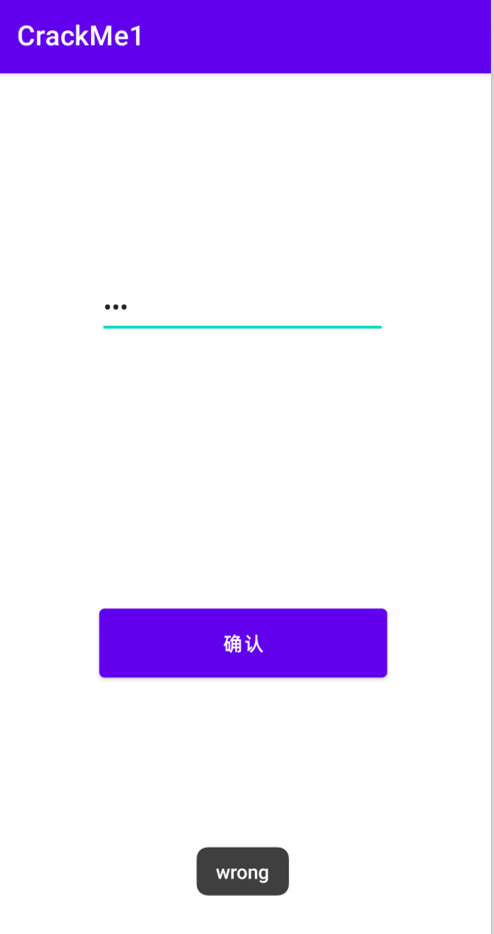
菁英班移动端作业题目说明

一、基本信息

本次作业提供一个Android端可安装的apk文件

|  |  |
| --- | --- |
| 文件名 | SHA1 |
| crackme1.apk | C57EA5B885F28D018A1F949C27F121FAE5B6F143 |

使用 “adb install crackme1.apk”可在手机设备上安装提供的apk文件，在手机设备上打开该apk文件界面如下所示，输入字符串后点击确认会弹出toast消息”wrong”或者”right”。

二、环境要求

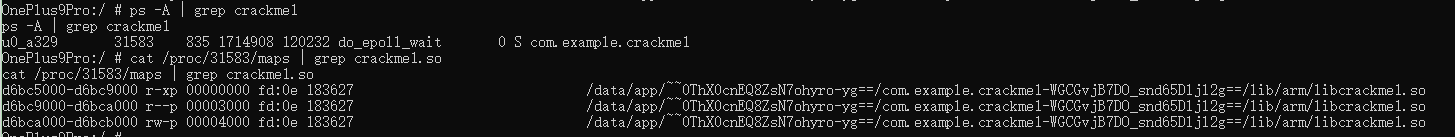
请在root的Android设备上进行测试

三、题目要求

3.1 远程注入模块

使用ptrace技术远程注入模块到crackme1进程中并且不崩溃，然后使用如下命令在远程进程中能够查看注入模块的信息。

|  |
| --- |
| ps -A | grep crackme1 // 查看crackme1.apk进程的pid  cat /proc/$pid/maps | grep $modulename // 在crackme1.apk的maps中需要能看到注入模块的信息 |



3.2 hook

通过hook进程中的函数使得输入任何字符串，点击确认都会弹出toast消息”right”。