1.

Secret1 : flag{e43y_p4ck37_sn1ff1Ng}
Secret2 : flag{a35_15_g00d_f5c533441769fbe027441fcb29c745c6}

2.

Task1：

一开始无论输入什么，服务器的 response 都是一致的：

PMRHEZLTOVWHIIR2GAWCE3LFONZWCZ3FEI5CEV3SN5XGOIDVONSXE3TBNVSSA33SEBYGC43TO5XXEZBOEIWCE2DJNZ2CEORCKRZHSIDUN4QGY33HNFXCAYLTEBDVKRKTKQRH2

利用工具分析安装包，发现包含里 decode 和 encode 函数

尝试用函数解码

获得：

{"result":0,"message":"Wrong username or password.","hint":"Try to login as GUEST"}

使用 GUEST 登录：

得到：

PMRHEZLTOVWHIIR2GAWCE3LFONZWCZ3FEI5CEV3SN5XGOIDVONSXE3TBNVSSA33SEBYGC43TO5XXEZBOEIWCE2DJNZ2CEORCKRCVGVBHOMQHAYLTON3W64TEEBUXGICUIVGVAX2QIFJVGV2EEJ6Q

根据提示

{"result":0,"message":"Wrong username or password.","hint":"TEST's password is TEMP_PASSWD"}

然而，根据提示登录还是不行

发现‘_’会被替换为‘#’

我们发送的登录账户会变成：

username=GUEST&password=TEMP#PASSWD

只有自己修改：

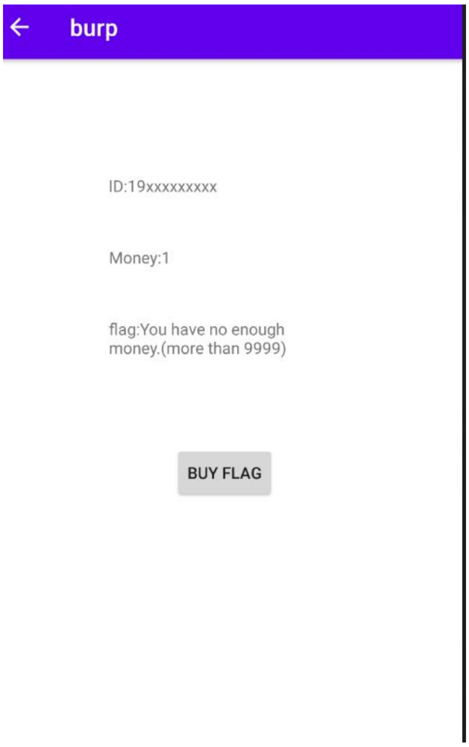
OVZWK4TOMFWWKPKHKVCVGVBGOBQXG43XN5ZGIPKUIVGVAX2QIFJVGV2E

利用 Burp Suite 发送，得到

PMRHEZLTOVWHIIR2GEWCE3LFONZWCZ3FEI5CE43VMNRWK43TEIWCE2LEEI5CEMJZPB4HQ6DYPB4HQ6BCFQRFGZLDOJSXIMJCHIRGM3DBM55WKNBTPFPXANDDNMZTOX3TNYYWMZRRJZTX2IRMEJWW63TFPERDUML5

{"result":1,"message":"success","id":"19xxxxxxxxx","Secret1":"flag{e43y_p4ck37_sn1ff1Ng}","money":1}

同时也进入下一个 activity：



ID:19xxxxxxxxx

Money:1

flag:You have no enough money.(more than 9999)

Task2：

之后点击 buy flag 会自动发送：

OVZWK4S7NFSD2MJZPB4HQ6DYPB4HQ6BGNVXW4ZLZHUYSM2LTL5TGC23FHUYQ

解码后是：

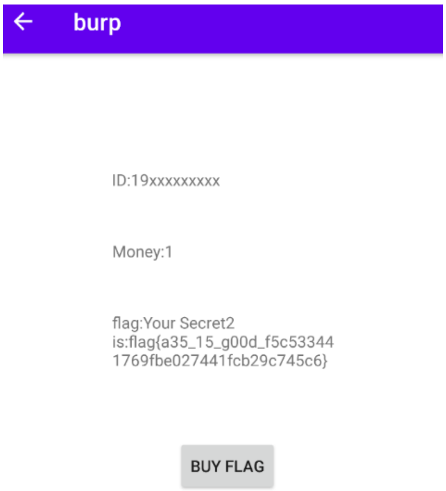
user_id=19xxxxxxxxx&money=1&is_fake=1

修改为：

user_id=19300240012&money=100000000000&is_fake=0

重新编码：

OVZWK4S7NFSD2MJZGMYDAMRUGAYDCMRGNVXW4ZLZHUYTAMBQGAYDAMBQGAYDAJTJONPWMYLLMU6TA



ID:19xxxxxxxxx

Money:1

flag:Your Secret2 is:flag{a35_15_g00d_f5c533441769fbe027441fcb29c745c6}

收到：

PMRG2ZLTONQWOZJCHIRFS33VOIQFGZLDOJSXIMRANFZTUZTMMFTXWYJTGVPTCNK7M4YDAZC7MY2WGNJTGM2DIMJXGY4WMYTFGAZDONBUGFTGGYRSHFRTONBVMM3H2IT5

解码：

{"message":"Your Secret2 is:flag{a35_15_g00d_f5c533441769fbe027441fcb29c745c6}"}

3.

实现 task1、2 的方法都是修改信息，主要是实现显示我们的学号

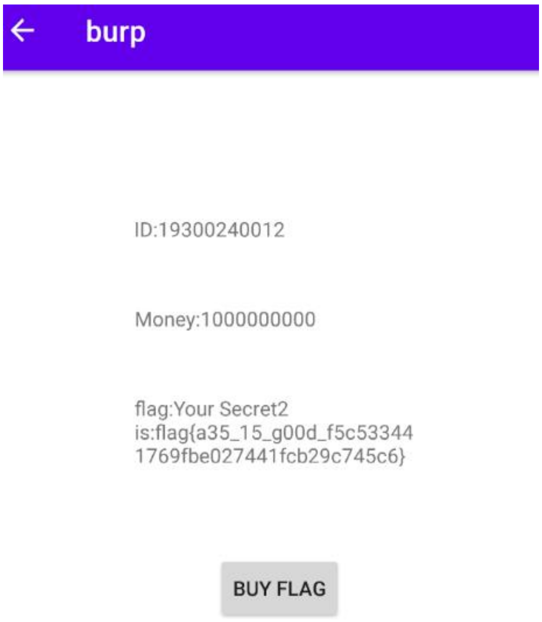
Task1 通过后会返回这个，我们修改

{"result":1,"message":"success","id":"19xxxxxxxxx","Secret1":"flag{e43y_p4ck37_sn1ff1Ng}","money":1}

{"result":1,"message":"success","id":"19300240012","Secret1":"flag{e43y_p4ck37_sn1ff1Ng}","money":1000000000}

编码：

PMRHEZLTOVWHIIR2GEWCE3LFONZWCZ3FEI5CE43VMNRWK43TEIWCE2LEEI5CEMJZGMYDAMRUGAYDCMRCFQRFGZLDOJSXIMJCHIRGM3DBM55WKNBTPFPXANDDNMZTOX3TNYYWMZRRJZTX2IRMEJWW63TFPERDUMJQGAYDAMBQGAYDA7I



ID:19300240012

Money:1000000000

flag:Your Secret2 is:flag{a35_15_g00d_f5c533441769fbe027441fcb29c745c6}

实现 Burp Suite 插件的步骤就是检测是否是要替换的，让后替换成我们希望的。