**Lab 4. Packet Sniffing**

* **Task 1**

(1) Your Answer

secret1: flag{e43y\_p4ck37\_sn1ff1Ng}

secret2: flag{czxv\_1vzx5\_zxd\_71570dadf7656a89fa7cc6018a0a2ef6}

(2) Writeup

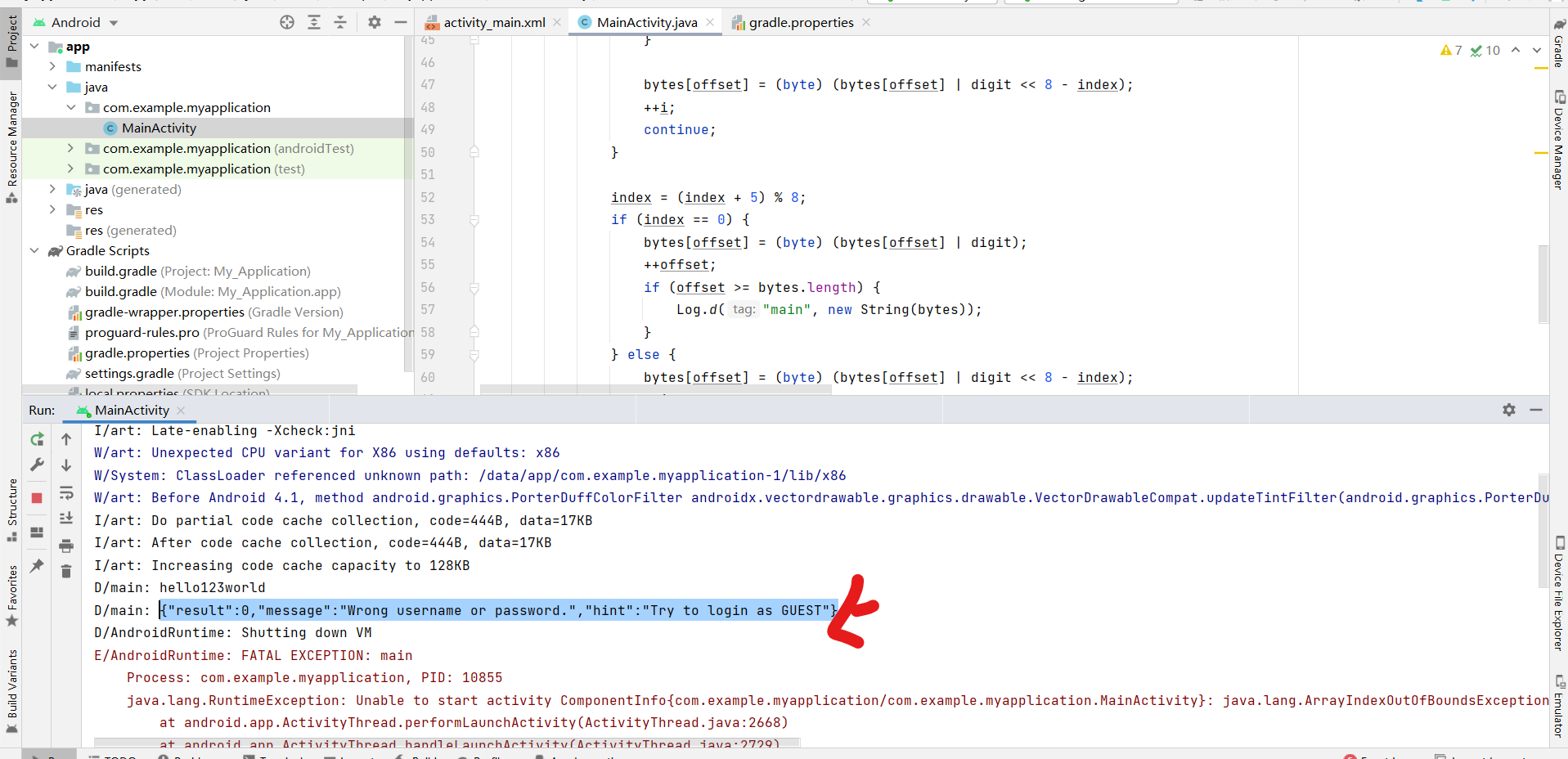
[Record how you solve this task here.]

先访问网站，得到一串字符串

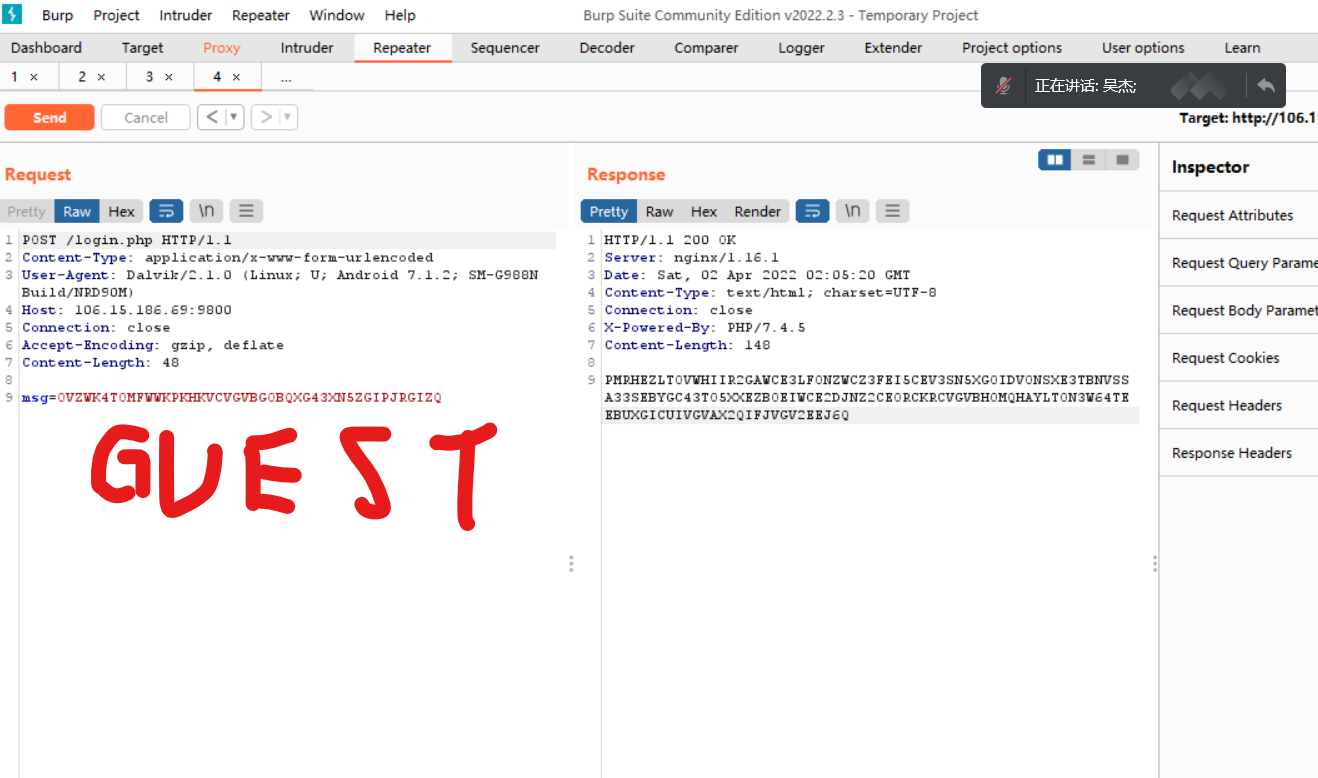


"PMRHEZLTOVWHIIR2GAWCE3LFONZWCZ3FEI5CEV3SN5XGOIDVONSXE3TBNVSSA33SEBYGC43TO5XXEZBOEIWCE2DJNZ2CEORCKRZHSIDUN4QGY33HNFXCAYLTEBDVKRKTKQRH2s"

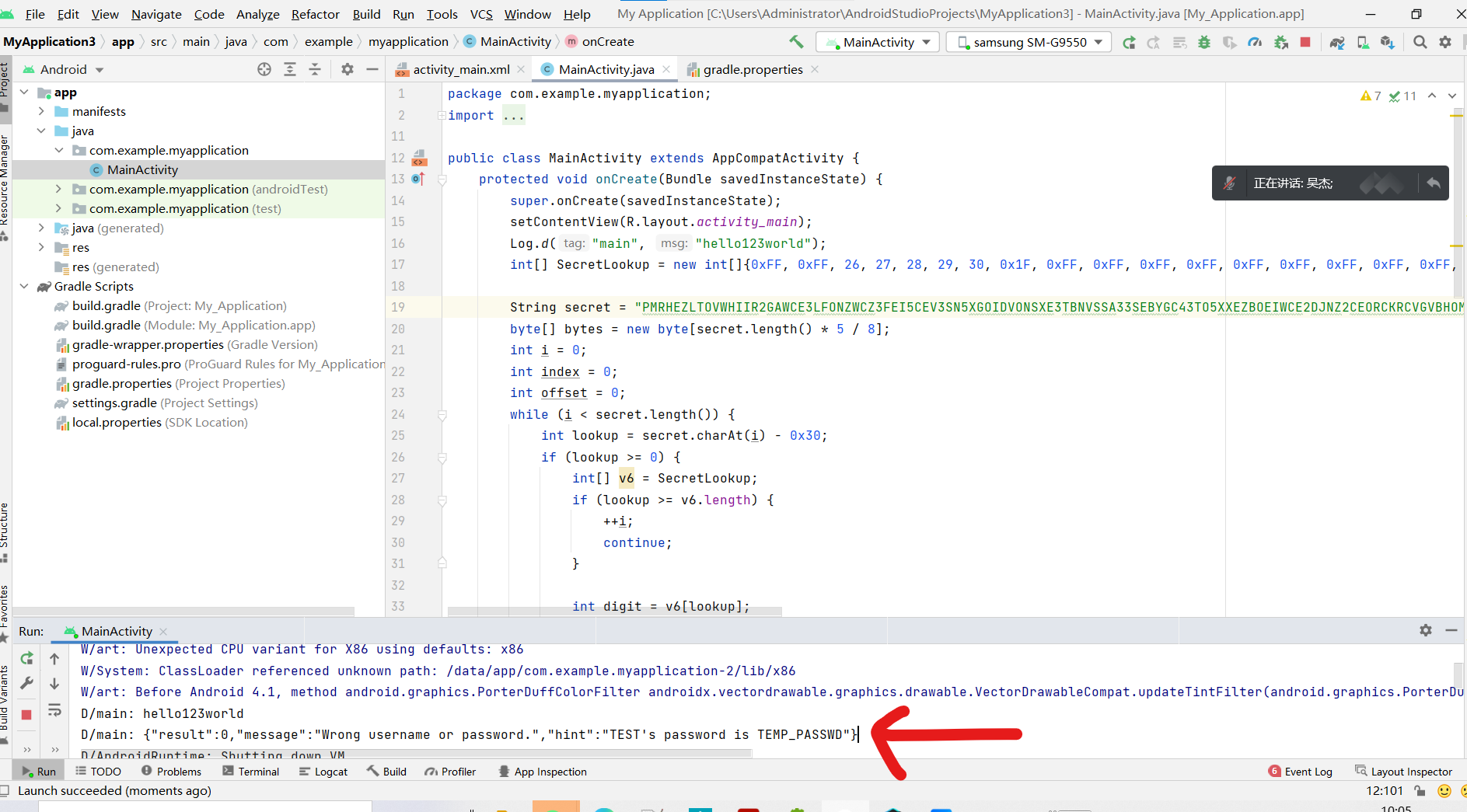
然后按照函数里面的decode一下



用GUEST作为用户名发包



得到的回显消息

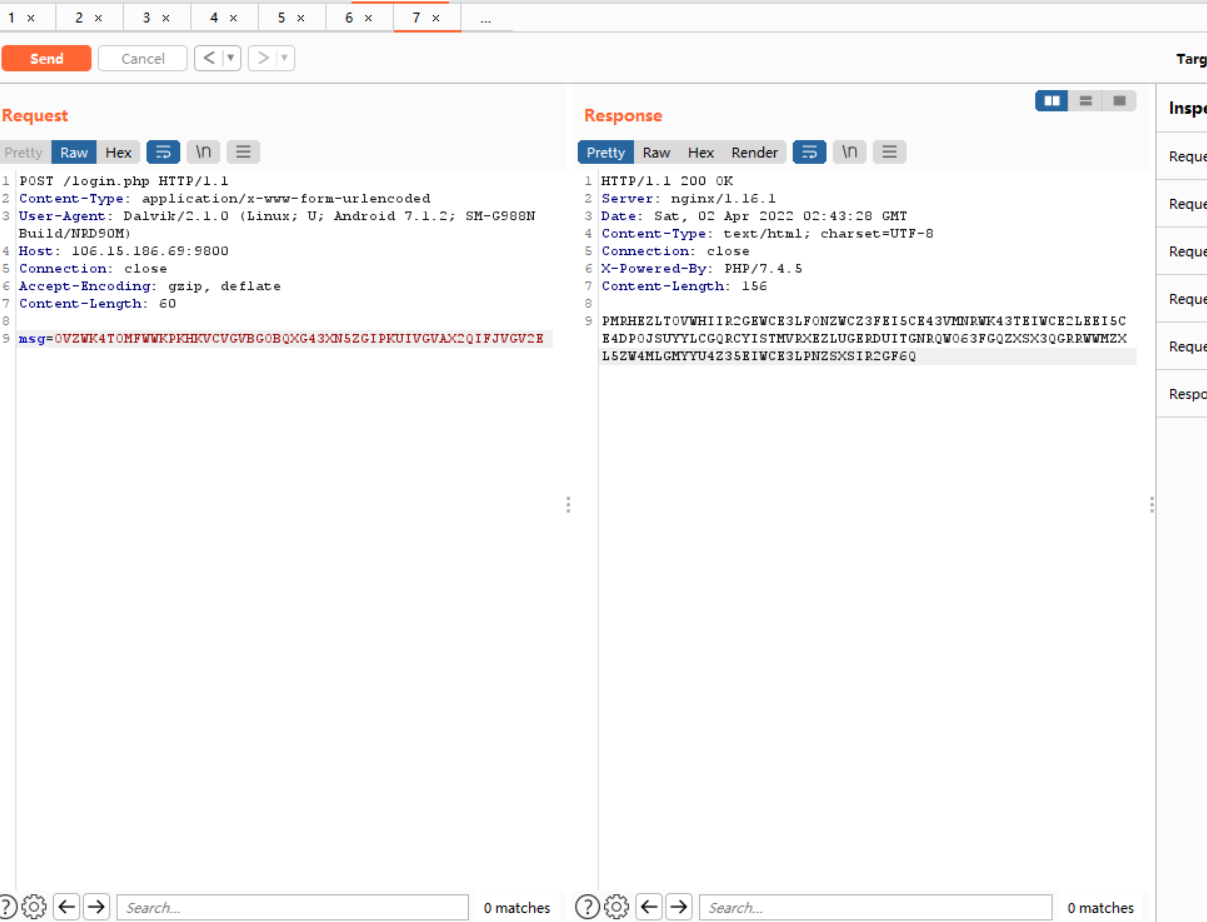


然后我尝试输入payload：username=GUEST&password=TEMP\_PASSWD，结果却还是wrong

原来这里有个小操作，把下划线替换了#，所以我们要用babycipher里的加密对于字符串重新加密，得到PMRHEZLTOVWHIIR2GEWCE3LFONZWCZ3FEI5CE43VMNRWK43TEIWCE2LEEI5CE4DPOJSUYYLCGQRCYISTMVRXEZLUGERDUITGNRQWO63FGQZXSX3QGRRWWMZXL5ZW4MLGMYYU4Z35EIWCE3LPNZSXSIR2GF6Q

然后把这串通过burpsuit再发送，得到字符串后解密得到Secret1

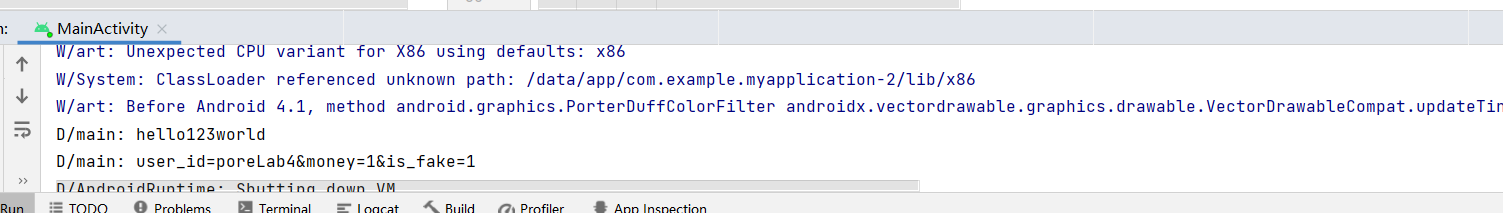




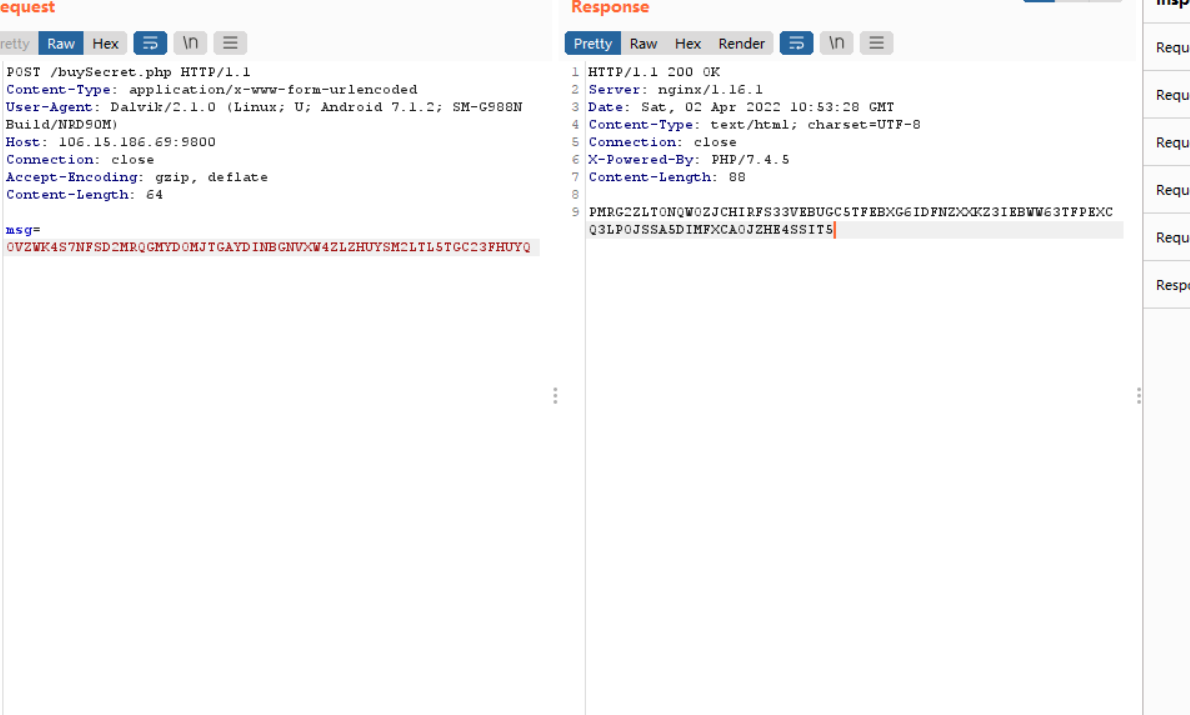


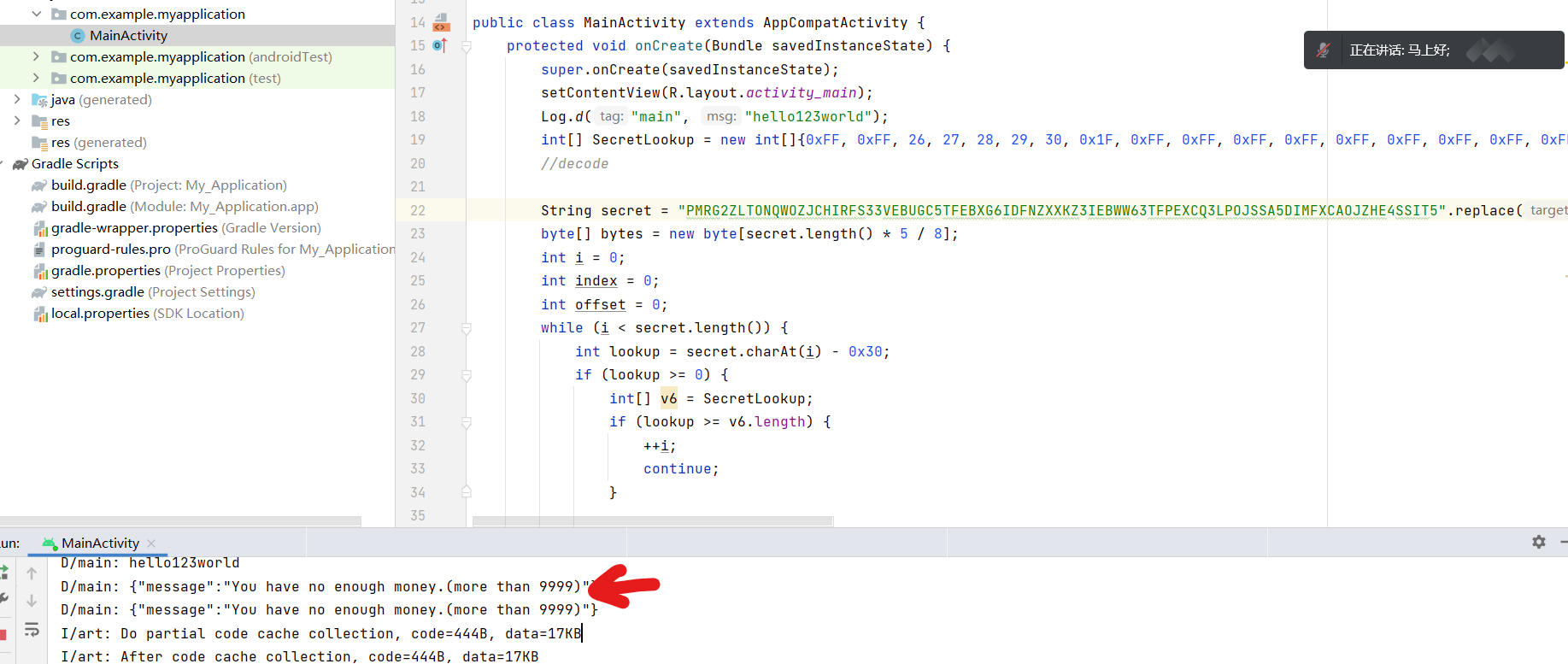
2、

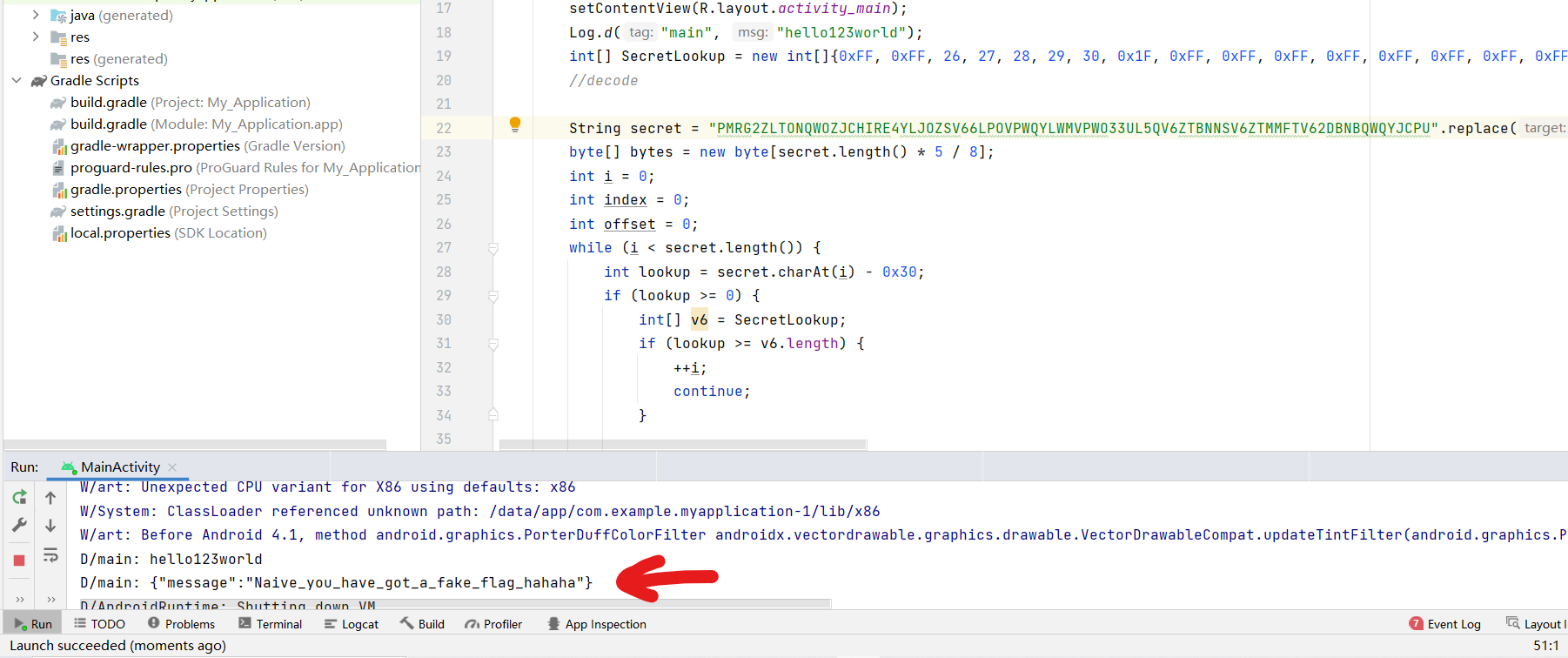
先看一下参数格式



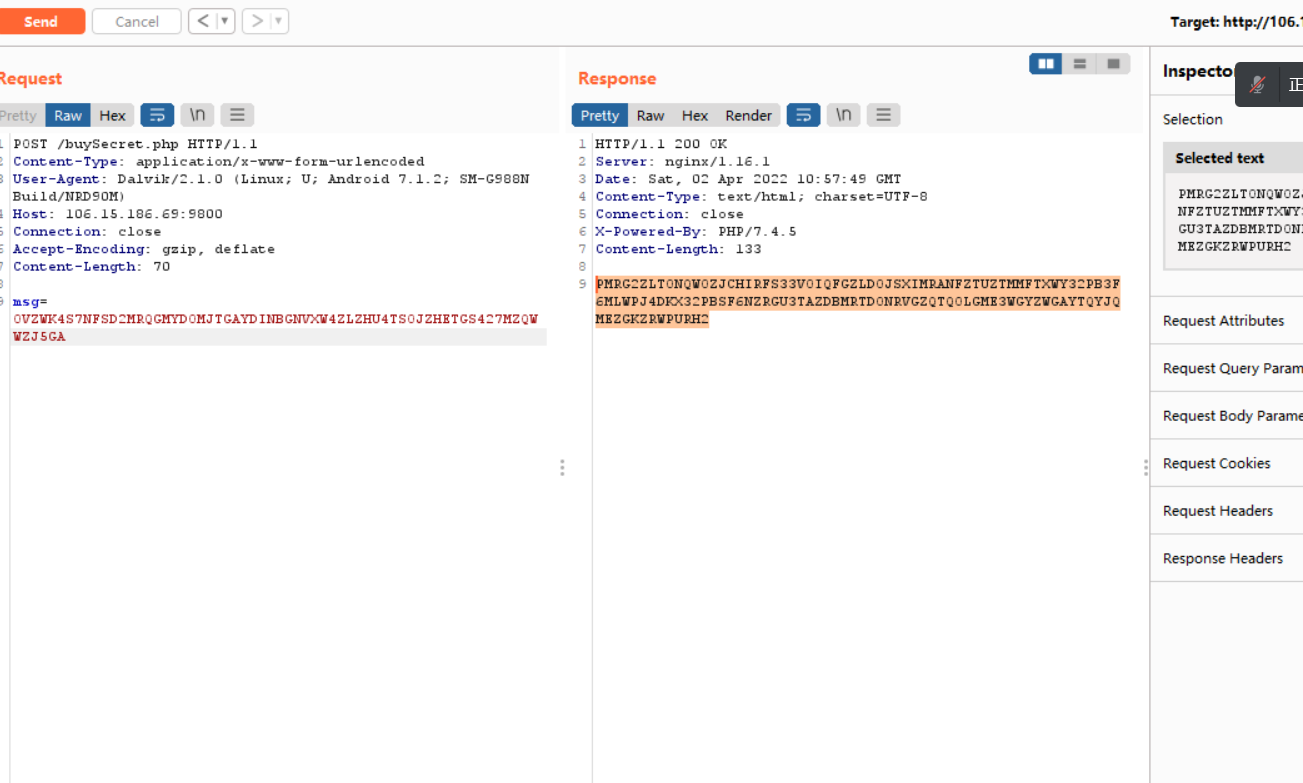
改成学号，得到字符串







payload=*user\_id=20307130044&money=99999&is\_fake=0*



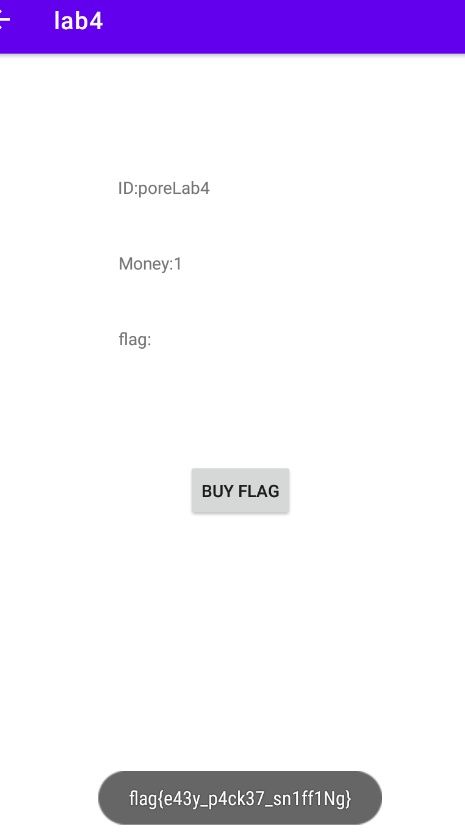
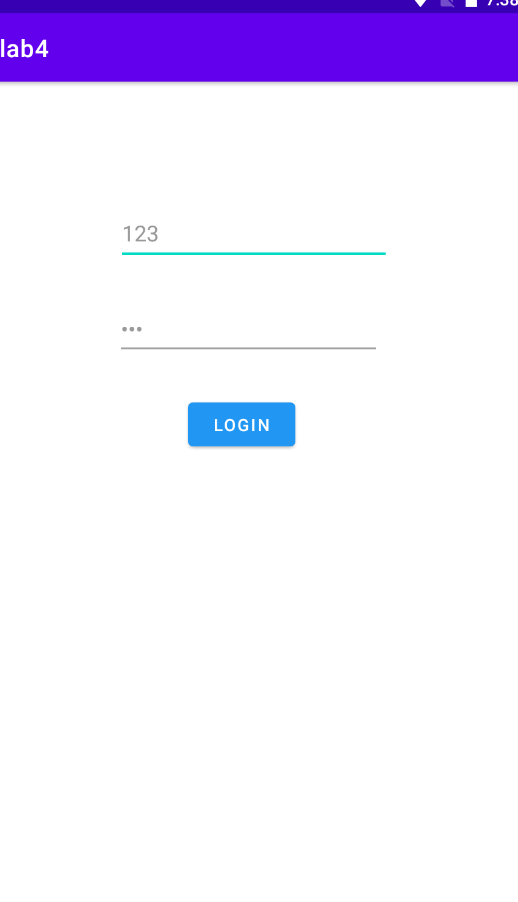


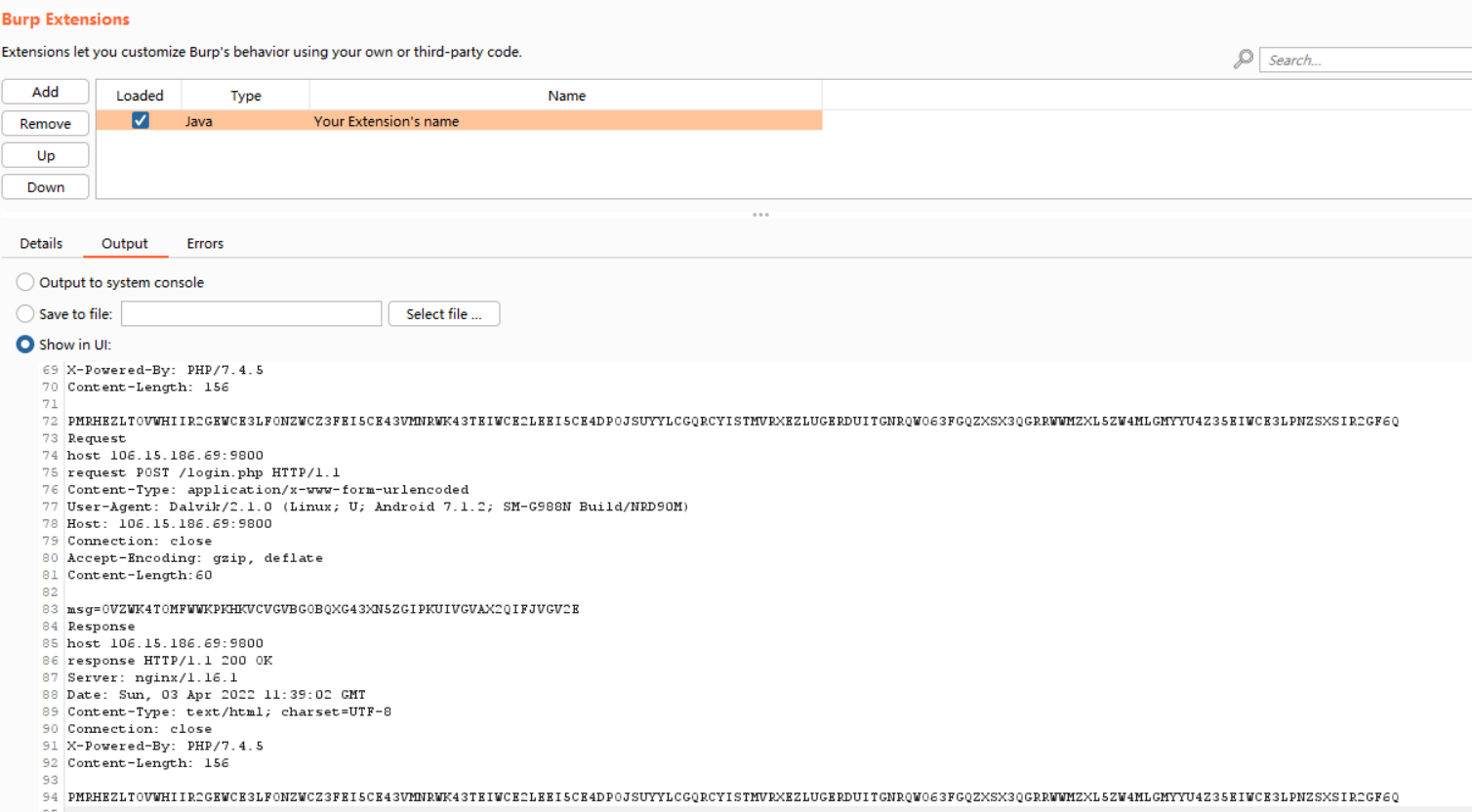
* **Task 2**

(1) Writeup

[Record how you solve this task here.]

第一步，将发送的消息中 Content-Length变为60，然后将msg=后的字符串变成合格的字符串，显示界面如下





第二个也差不多，将Content-Length和数据替换为该有的数据发包就行

