**Lab 4. Packet Sniffing**

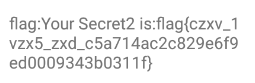
* **Task 1**

(1) Your Answer

secret1: flag{e43\_p4ck37\_sn1ff1Ng}



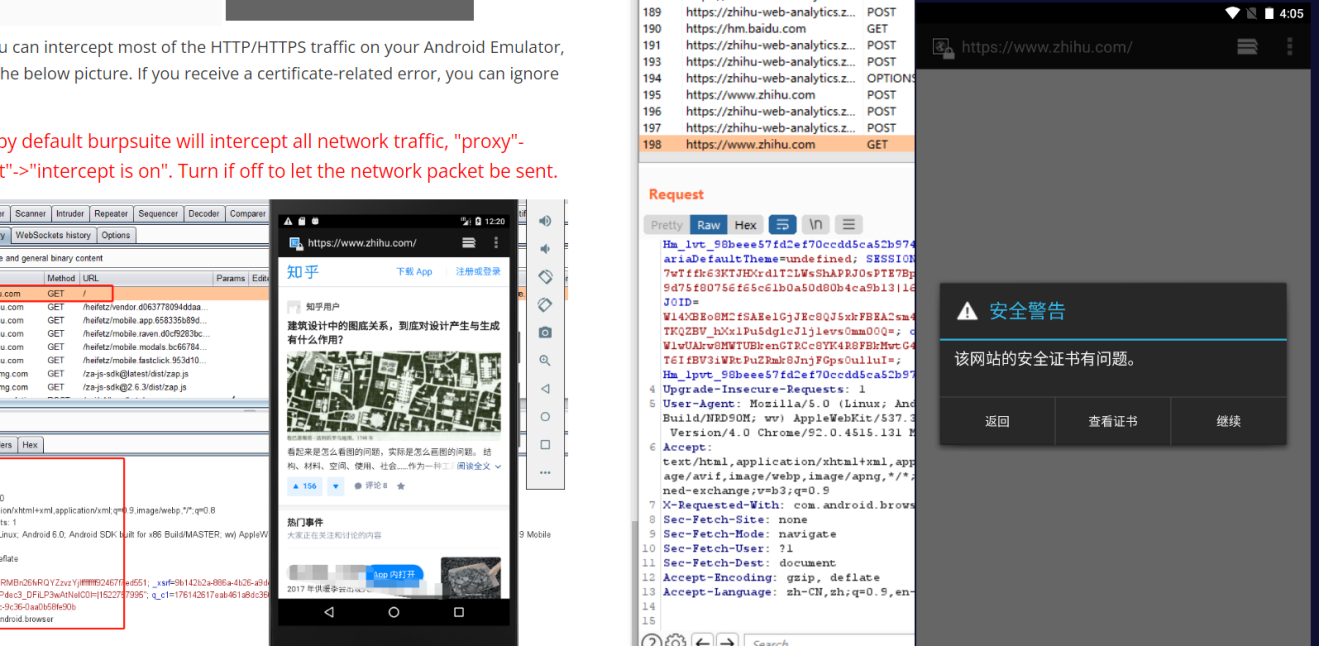
secret2: flag{如下图所示}



(2) Writeup

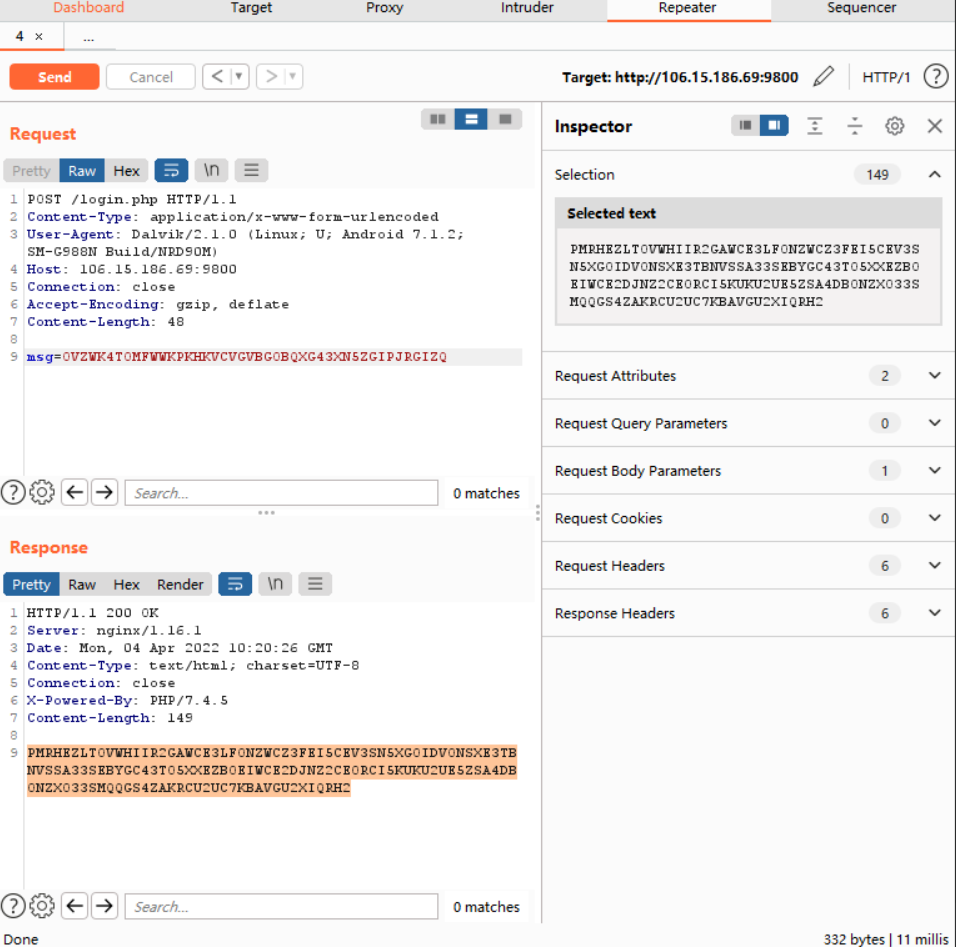
[Record how you solve this task here.]

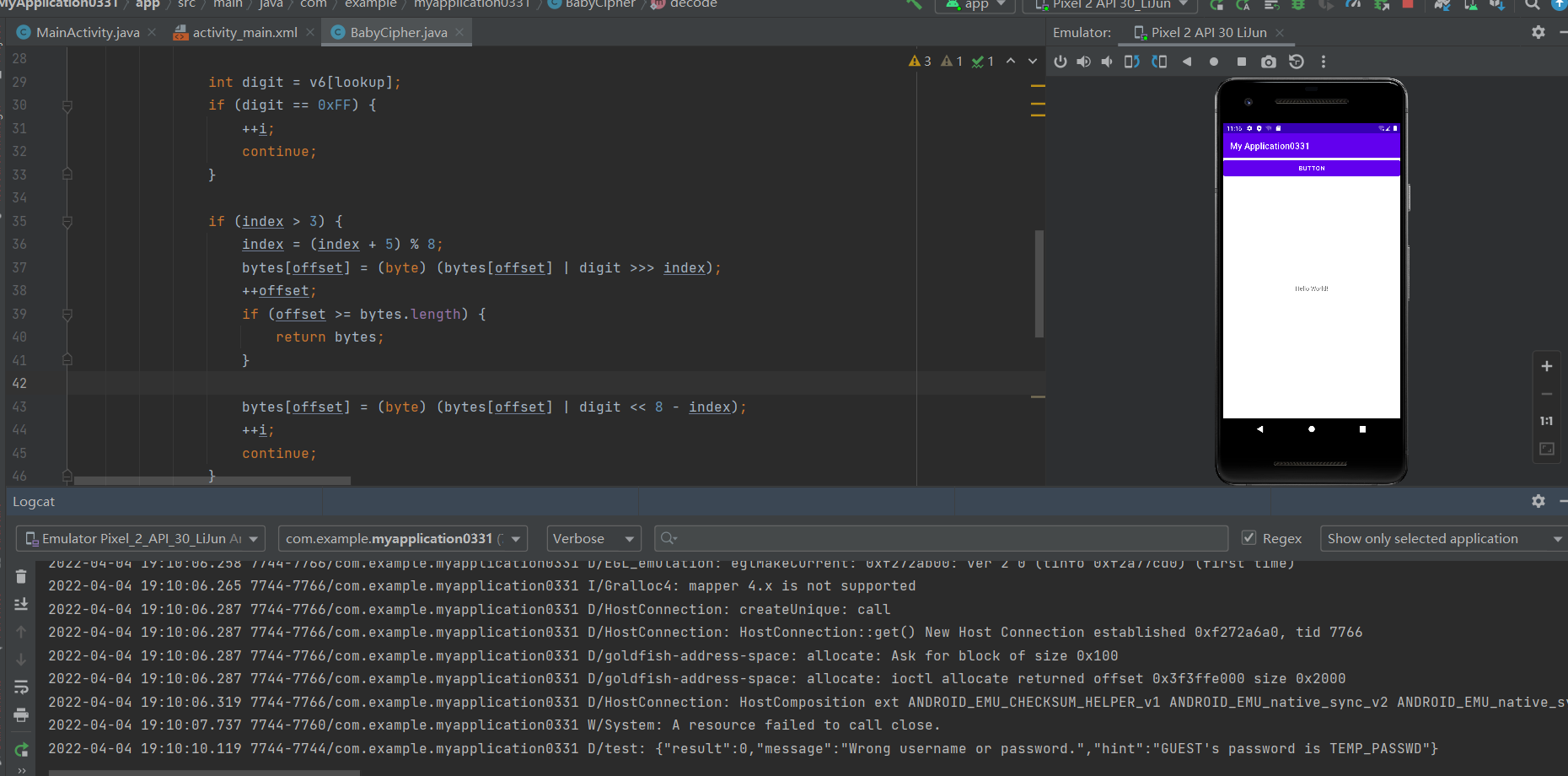
在设置burp的时候出了点问题，和文档所示不同，但是我们要求只要能监听app即可，于是忽略这个小问题。



抓包得到服务器的response，在此之后逆向lab4.apk并得到decode()函数，在模拟器上运行解密函数得到相应信息:

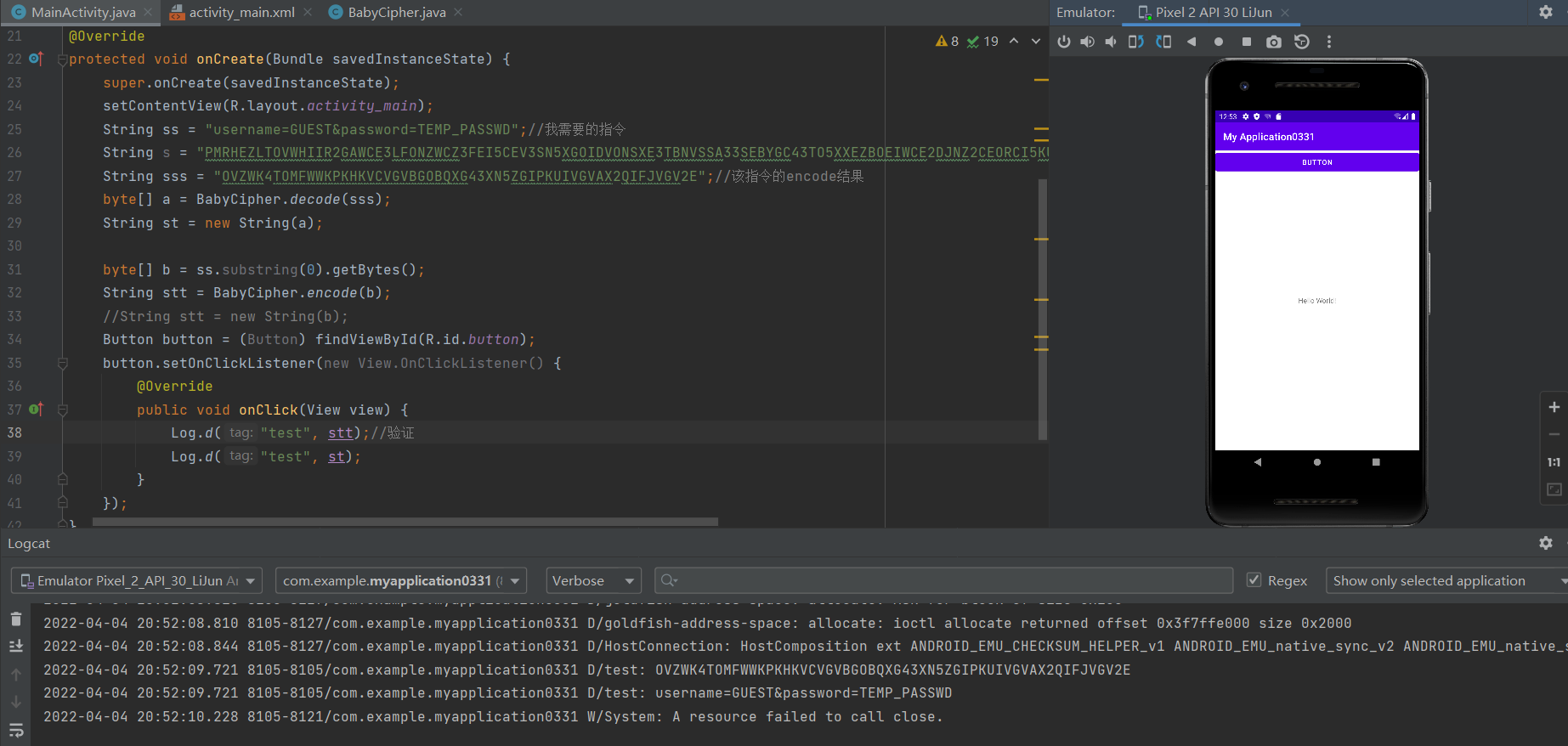
{"result":0,"message":"Wrong username or password.","hint":"GUEST's password is TEMP\_PASSWD"}

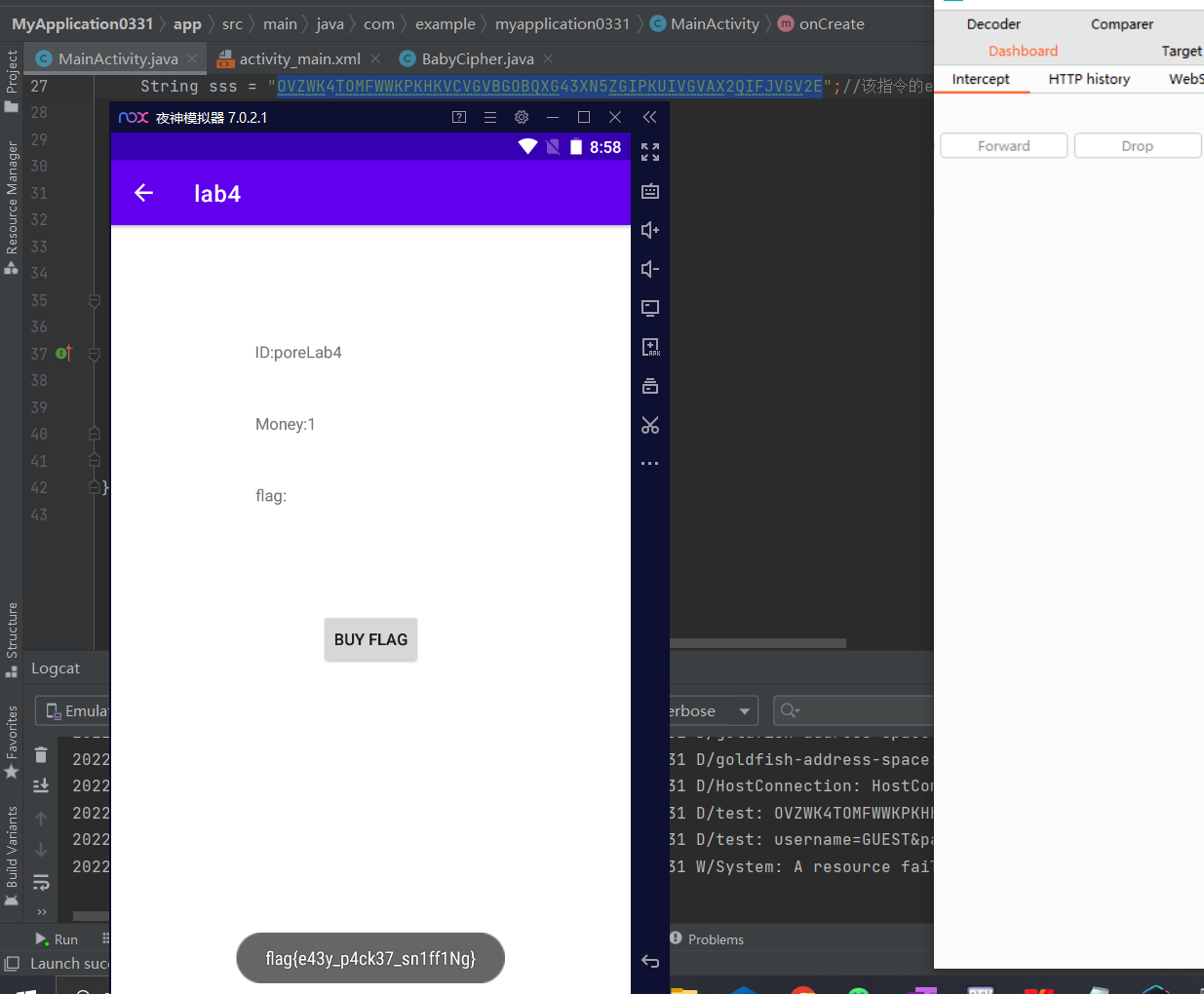




阅读逆向出来的代码可以知道，apk会把我们输入的\_转变成#，我们不允许他这么做，否则服务器收到的指令不正确，我们接下来要做的是将正确的指令进行encode并通过burp修改内容，使得服务器可以返回我们想要的内容：

TEMP\_PASSWD相应的内容进行encode之后是OVZWK4TOMFWWKPKHKVCVGVBGOBQXG43XN5ZGIPKUIVGVAX2QIFJVGV2E

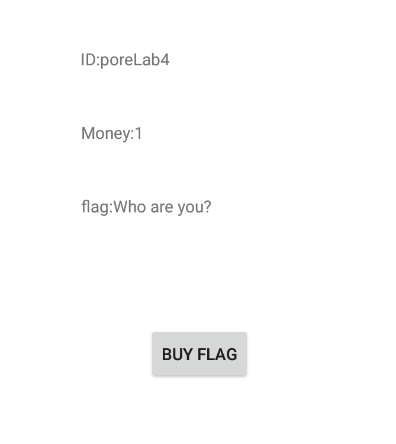




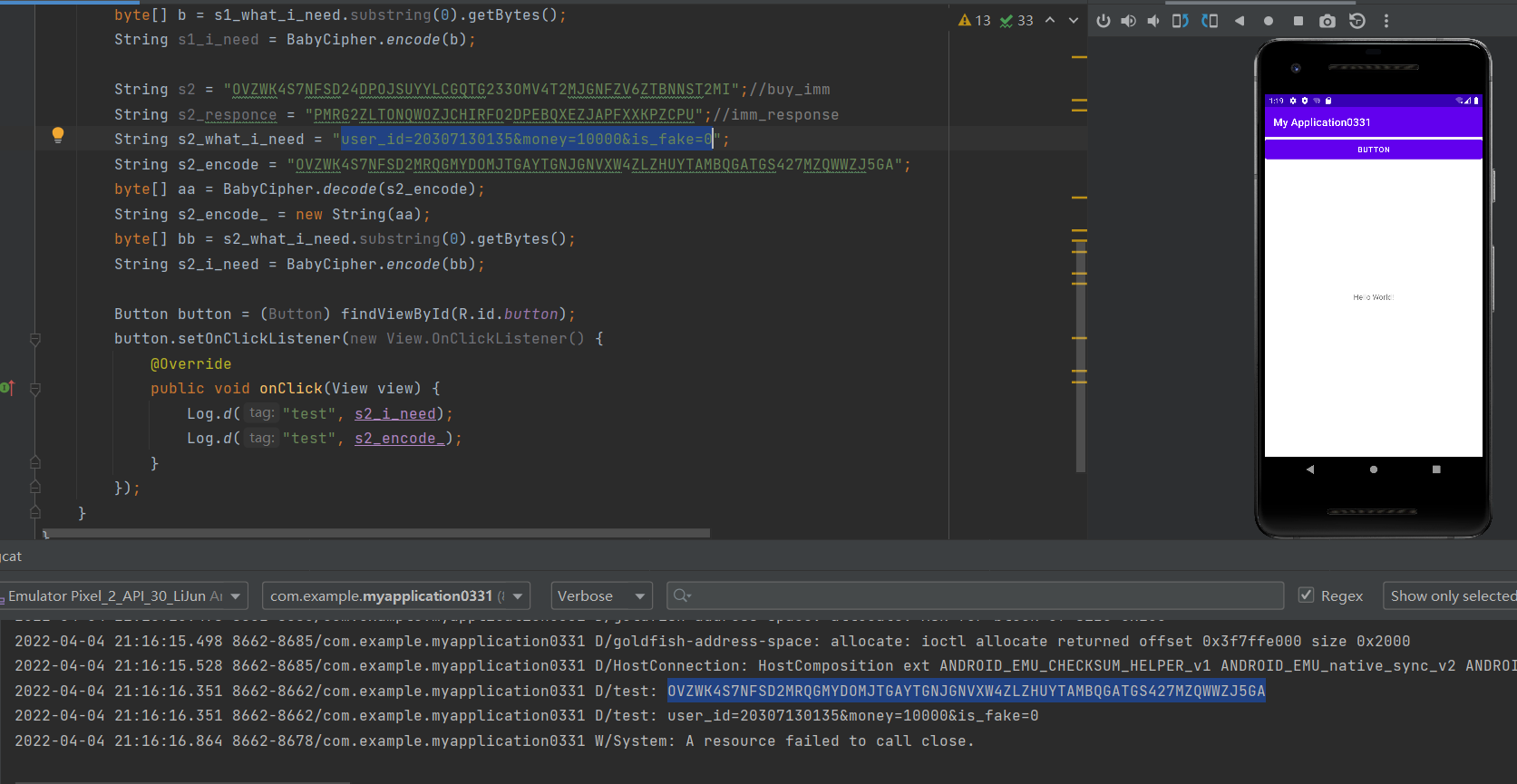
得到第一个secret是：flag{e43\_p4ck37\_sn1ff1Ng}

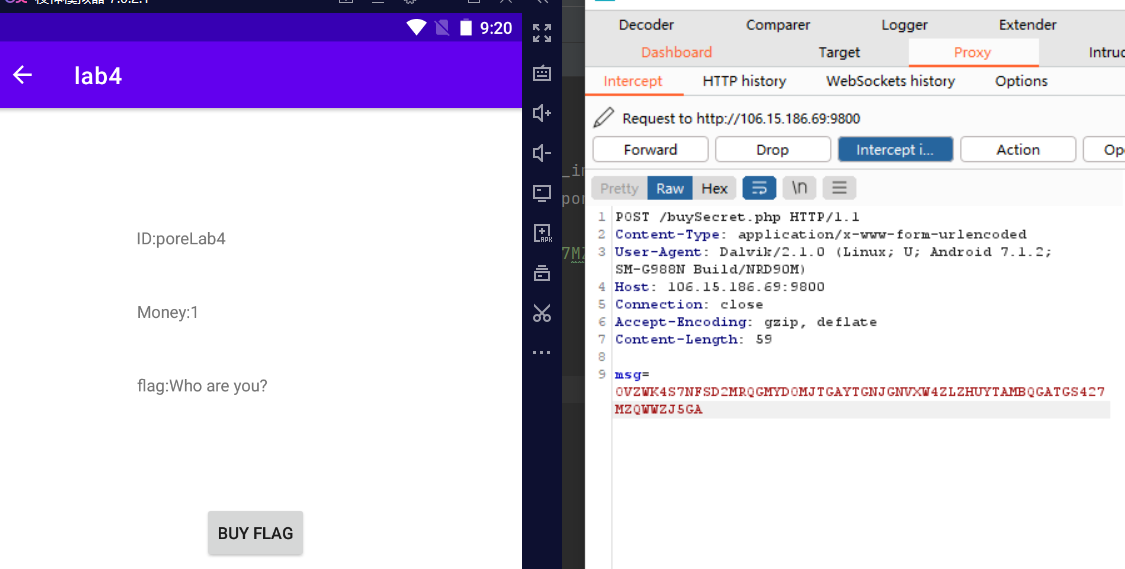
相应报文{"result":1,"message":"success","id":"poreLab4","Secret1":"flag{e43y\_p4ck37\_sn1ff1Ng}","money":1}

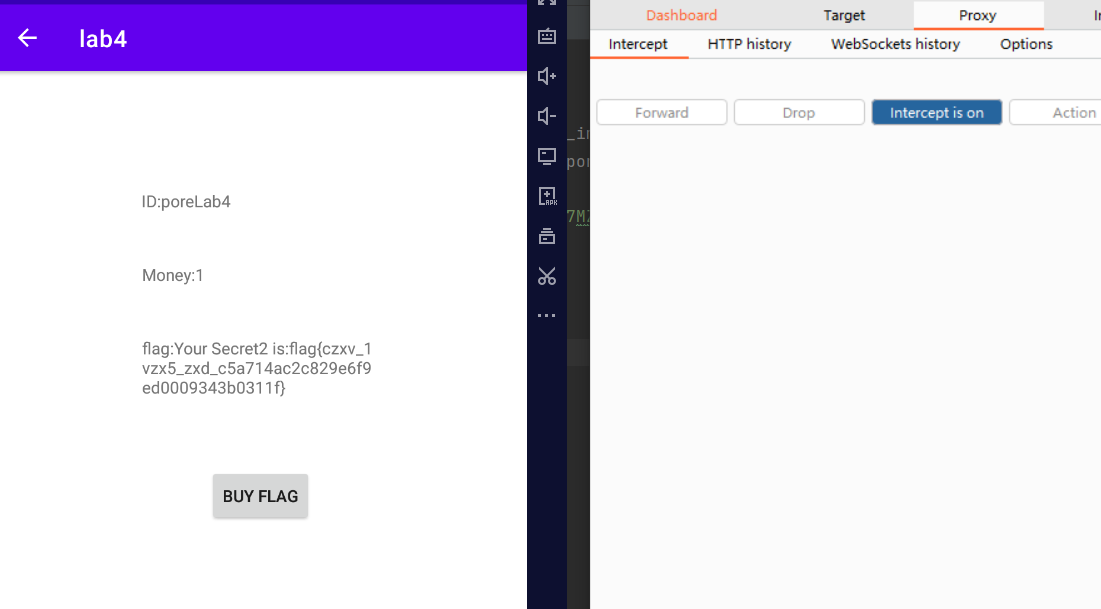
进行第二个secret的时候直接点击按钮发生如下情况：



继续抓包、解码，将我想要发送的信息user\_id=20307130135&money=10000&is\_fake=0进行encode，改变相应内容，让服务器返回flag秘密：





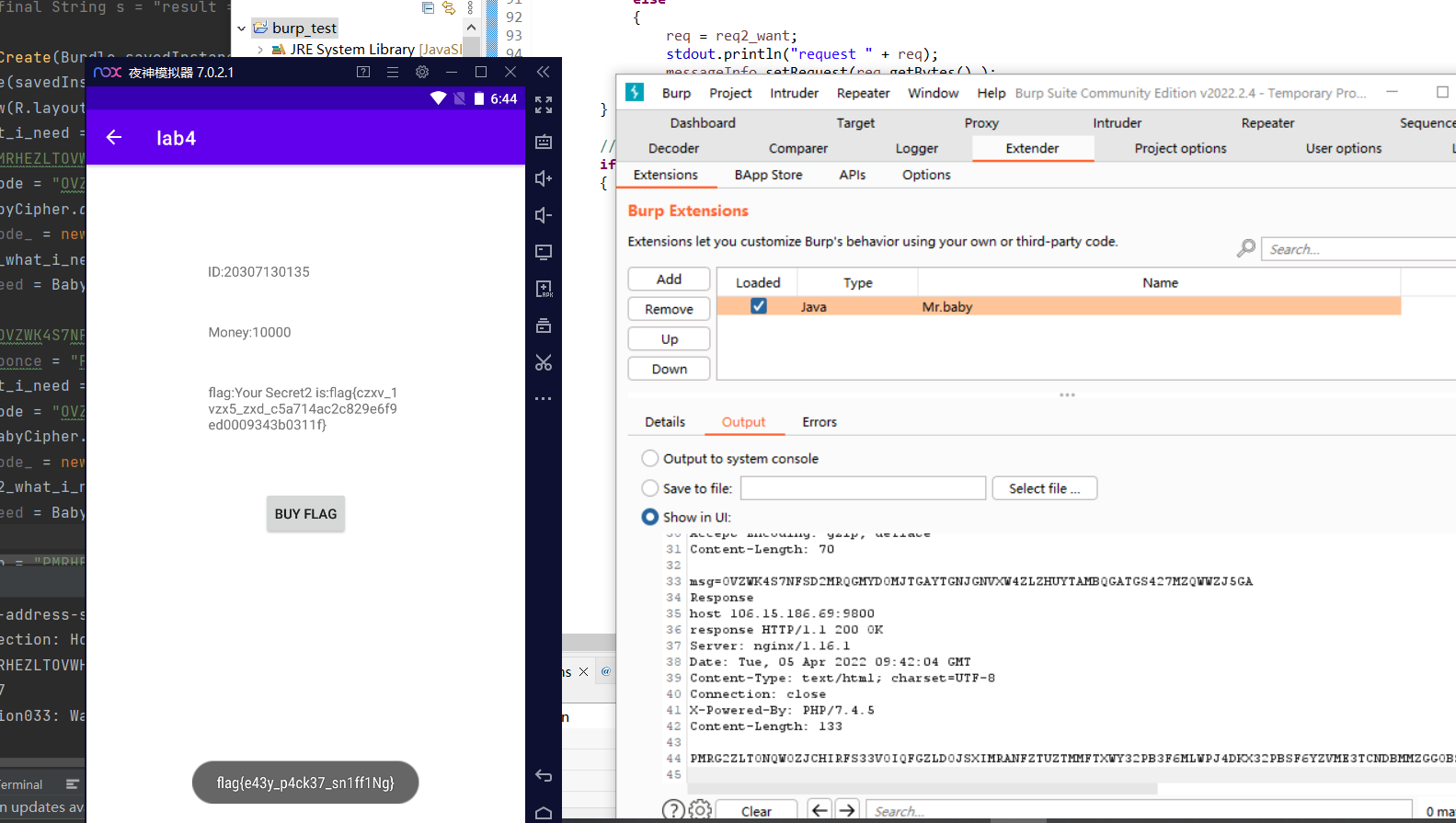


* **Task 2**

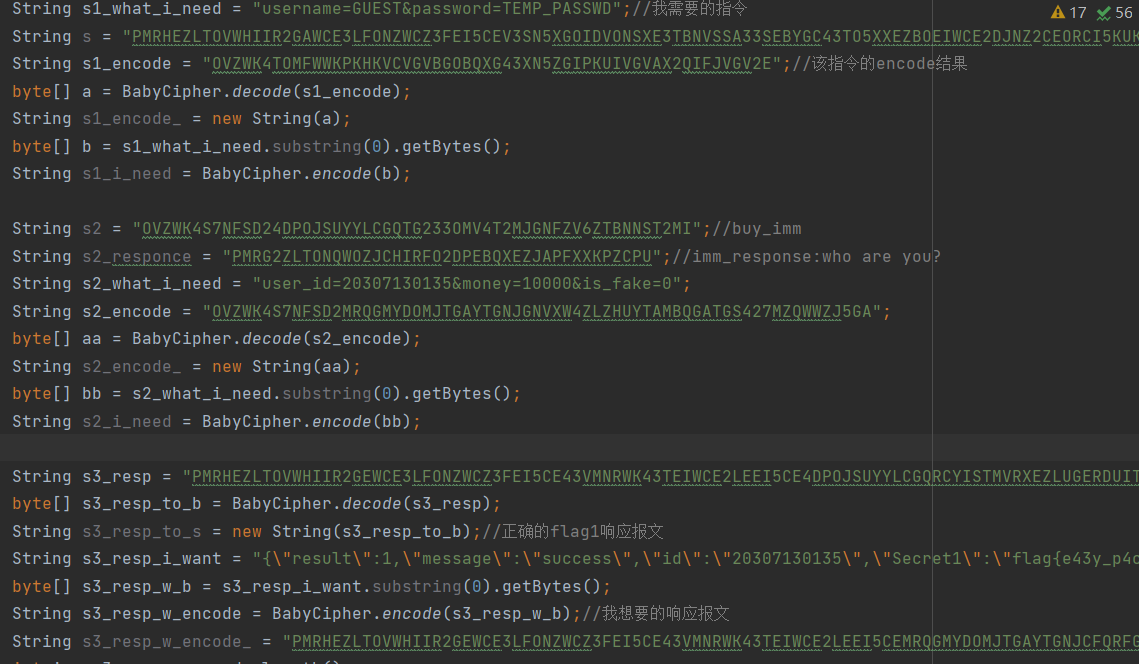
(1) Writeup

[Record how you solve this task here.]

按照提示的代码框架，下载eclipse并导入buep包、将java代码补全，实现直接点击按钮就可以得到两个secret。修改报文内容的时候，由于Length部分没有根据msg长度进行改写，我碰壁一段很撑的时间，好在后来发现了问题所在，及时解决了。效果如下（索性把monny给自己加多点显示出来了）：



为了解决问题而在android studio上做了很多解码的工作，得到相应msg信息：



下面是eclipse中burpextender部分代码截图（完整见其他附件）：



