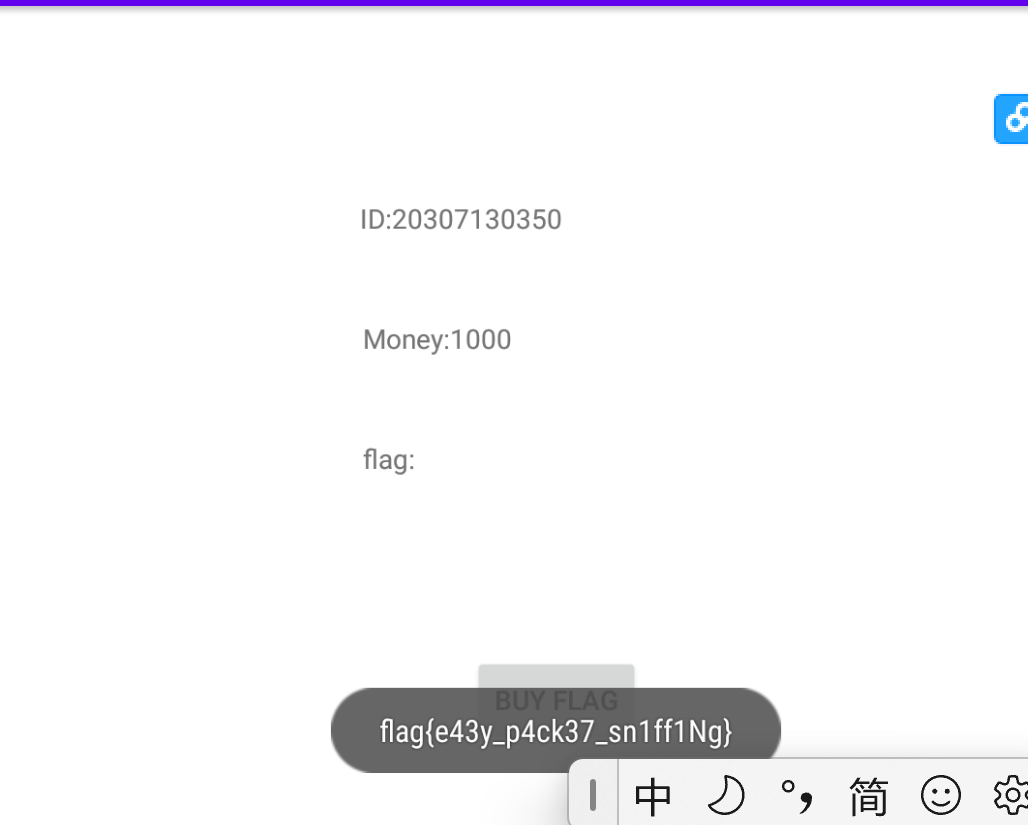
**Lab 4. Packet Sniffing**

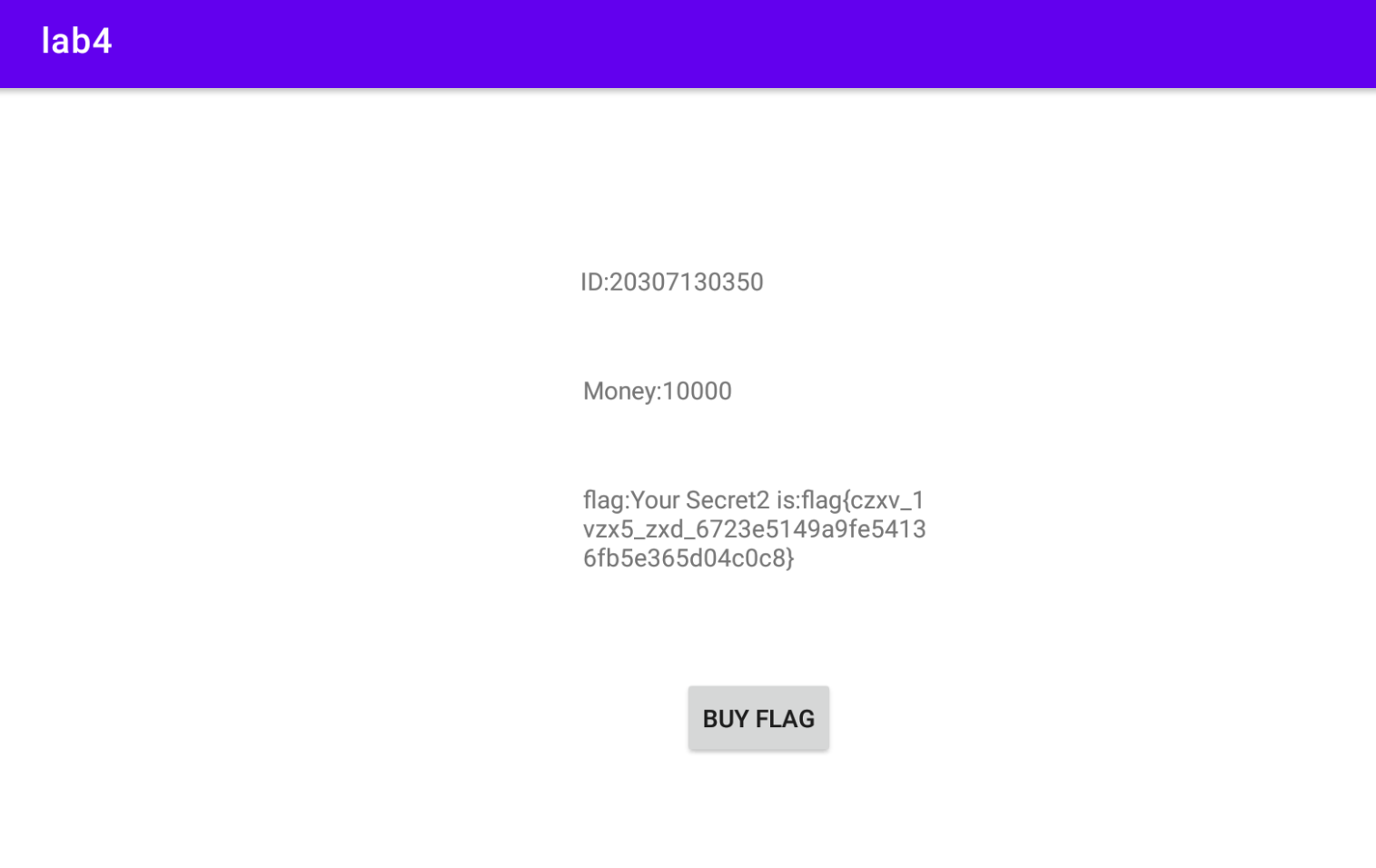
* **Task 1**

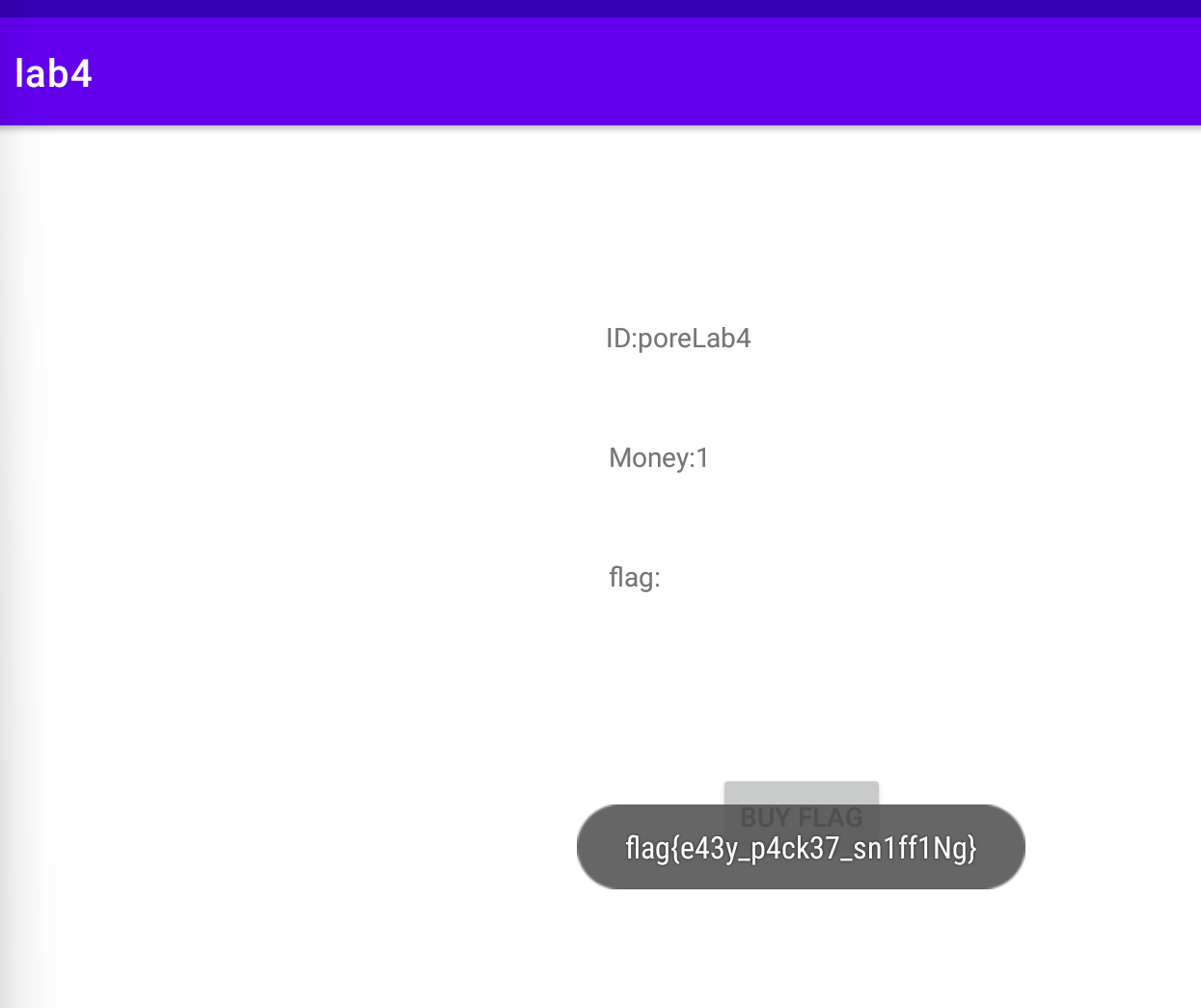
(1) Your Answer

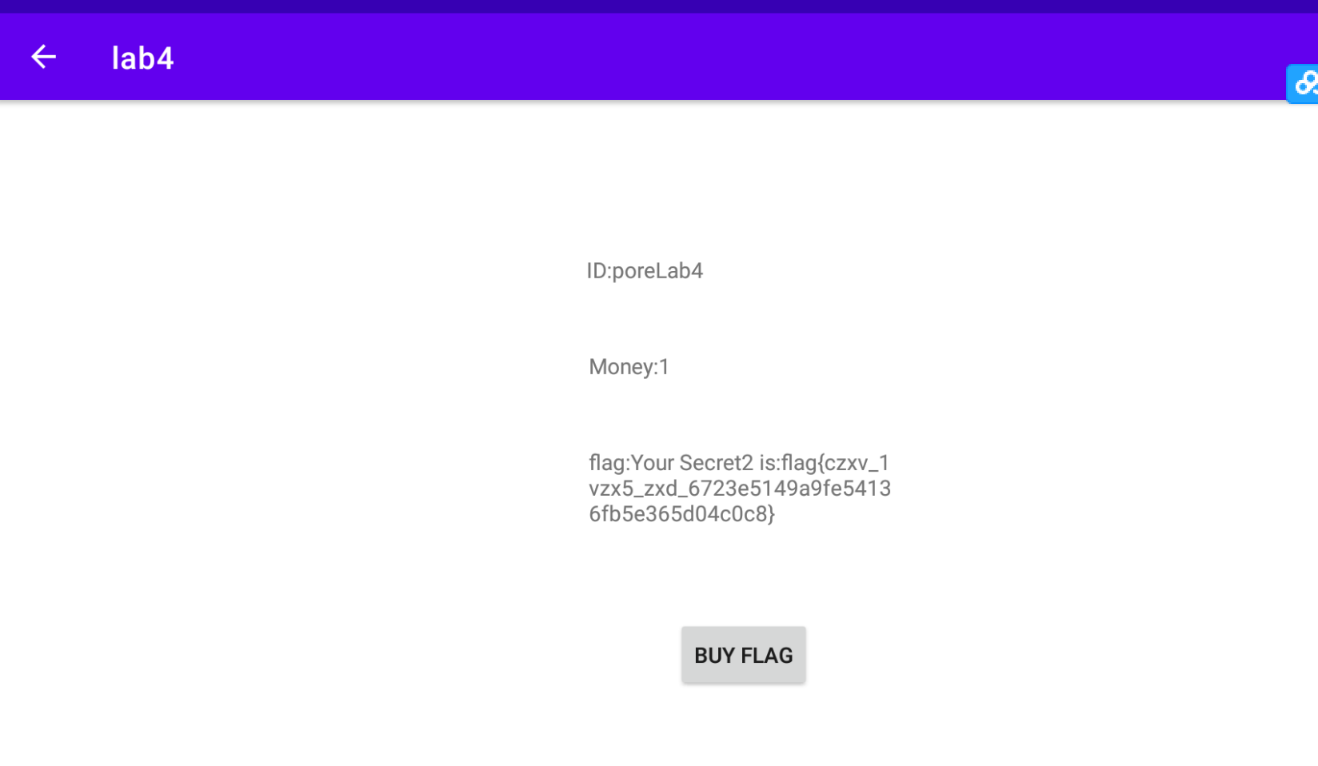
secret1: flag{**e43y\_p4ck37\_sn1ff1Ng**}

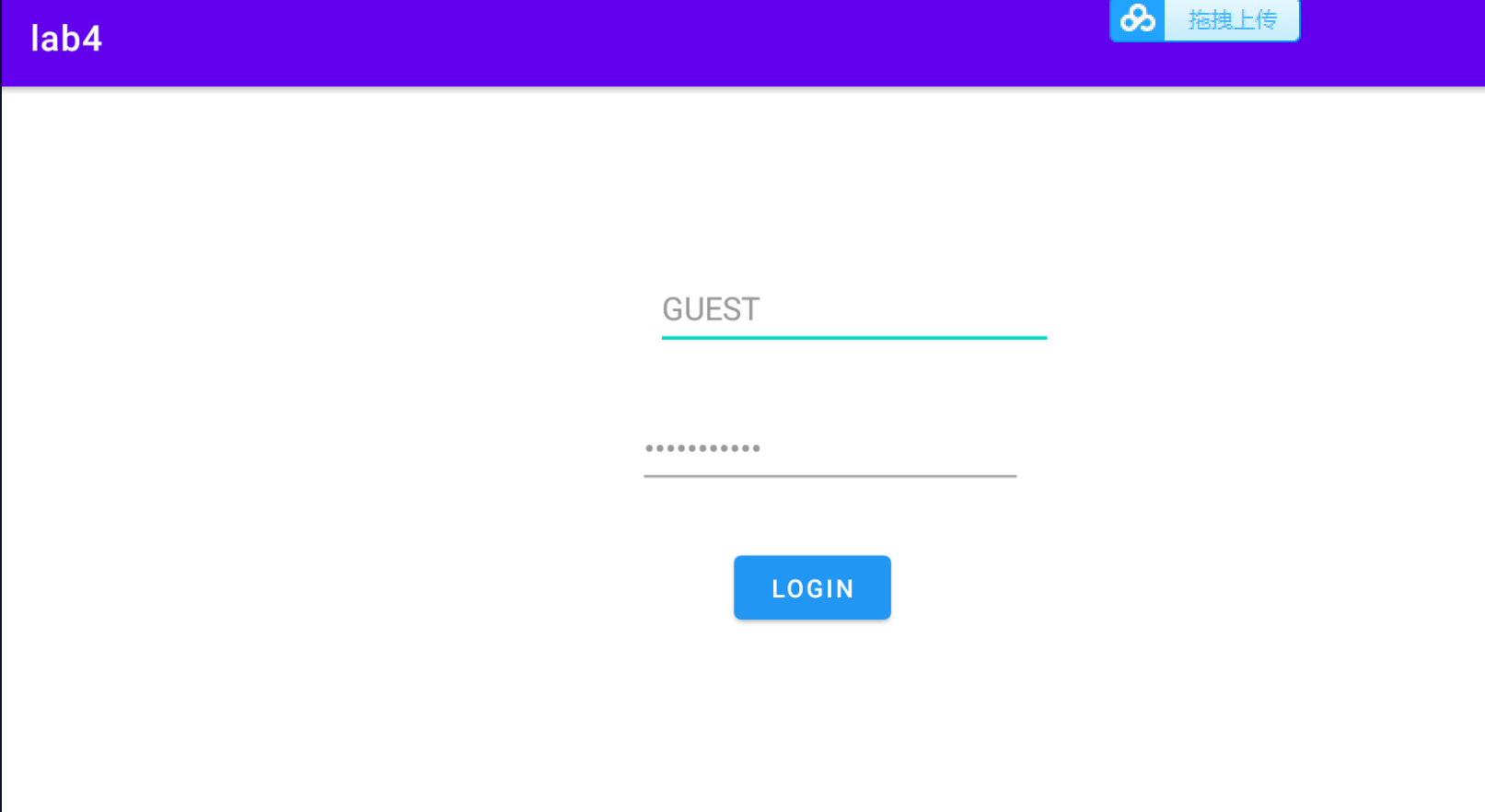
secret2: flag{**czxv\_1vzx5\_zxd\_6723e5149a9fe54136fb5e365d04c0c8**}







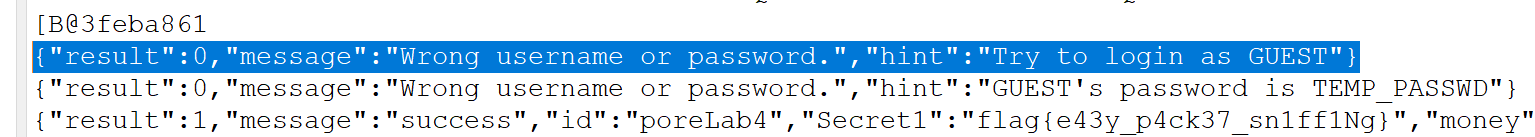




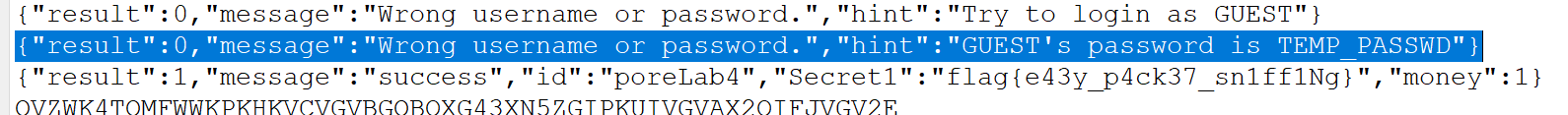
(2) Writeup

[Record how you solve this task here.]

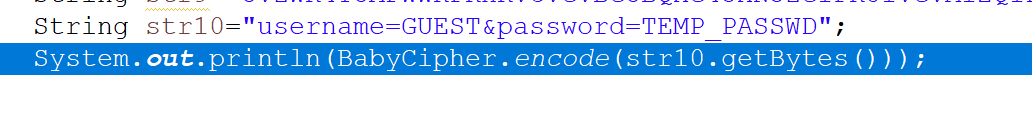
1. Secret1：
   1. Decode第一个网页的返回结果"PMRHEZLTOVWHIIR2GAWCE3LFONZWCZ3FEI5CEV3SN5XGOIDVONSXE3TBNVSSA33SEBYGC43TO5XXEZBOEIWCE2DJNZ2CEORCKRZHSIDUN4QGY33HNFXCAYLTEBDVKRKTKQRH2";

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

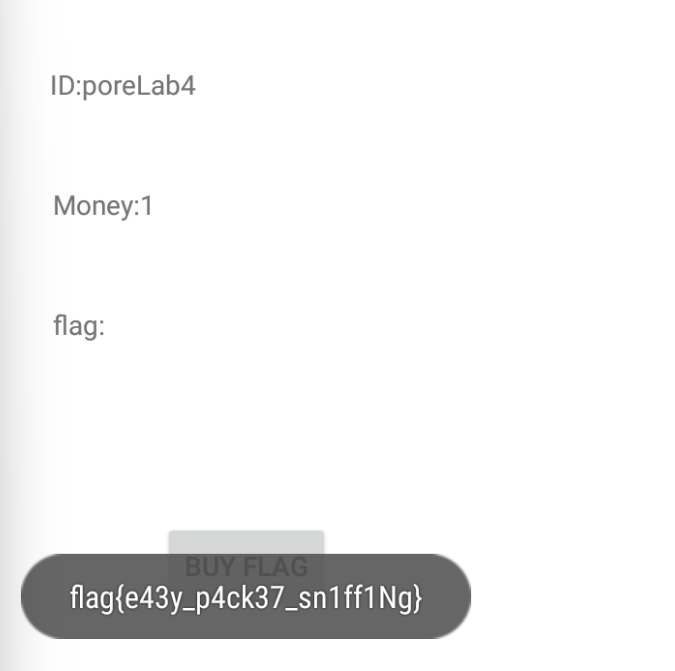
* 1. 根据hint，设置username为Guest,再次用burpsuite得到response的结果是PMRHEZLTOVWHIIR2GAWCE3LFONZWCZ3FEI5CEV3SN5XGOIDVONSXE3TBNVSSA33SEBYGC43TO5XXEZBOEIWCE2DJNZ2CEORCI5KUKU2UE5ZSA4DBONZXO33SMQQGS4ZAKRCU2UC7KBAVGU2XIQRH2

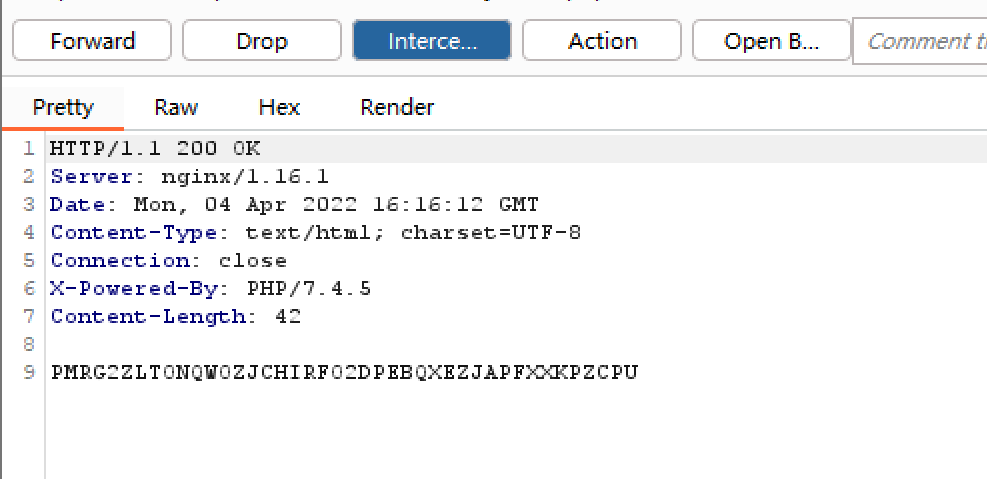
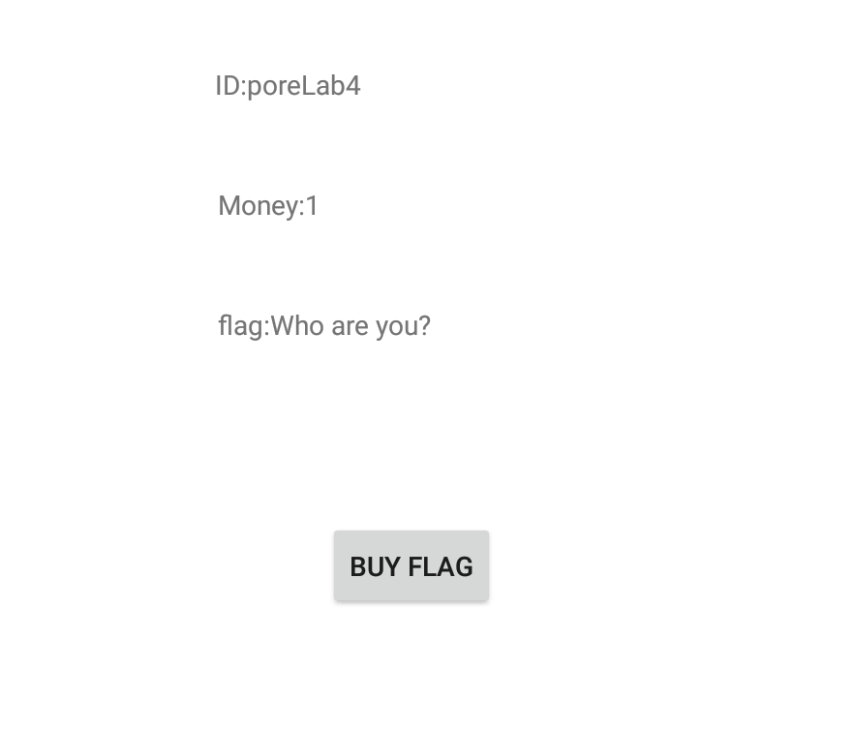
得到：{"result":0,"message":"Wrong username or password.","hint":"GUEST's password is TEMP\_PASSWD"} 。

* 1. 得到password=TEMP\_PASSWD;

对其进行encode，得到

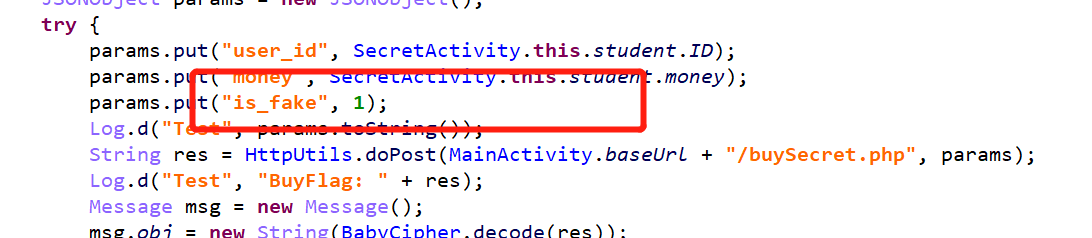


* 1. 将OVZWK4TOMFWWKPKHKVCVGVBGOBQXG43XN5ZGIPKUIVGVAX2QIFJVGV2E放入到burpsuite的proxy-intercept的request包的msg
  2. Forward之后得到结果

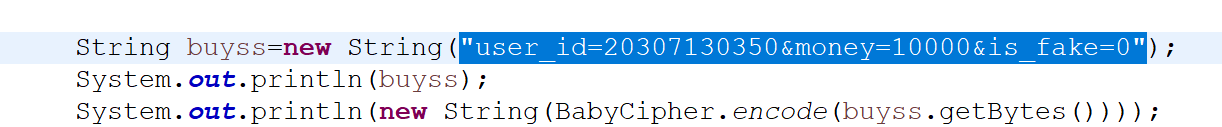
1. Secret2同理：
   1. 不做任何改变得到 

Decode得到的PMRG2ZLTONQWOZJCHIRFO2DPEBQXEZJAPFXXKPZCPU

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

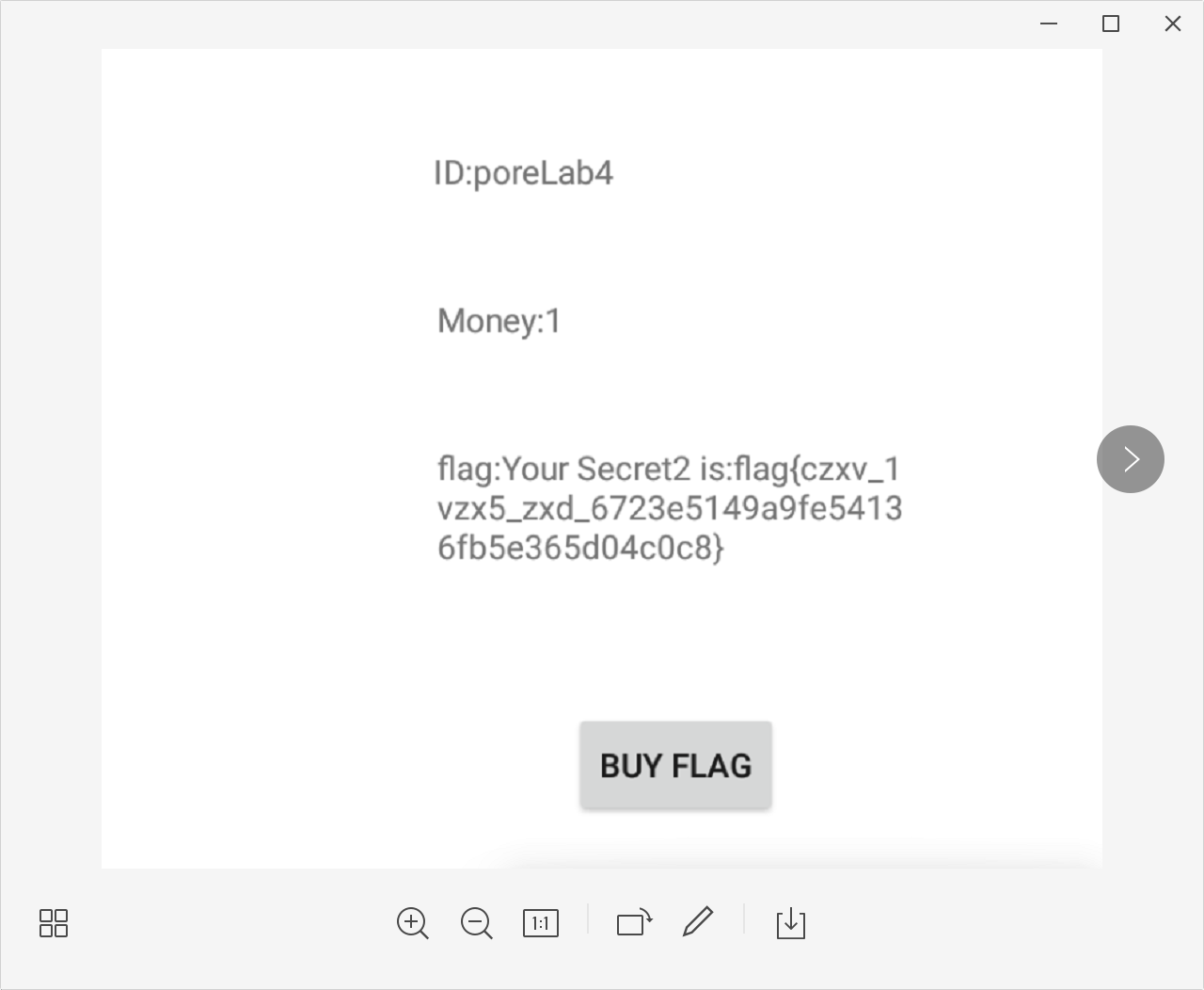
* 1. 根据逆向得到的源码
  2. 设置第二次的paramstr为"user\_id=20307130350&money=10000&is\_fake=1"

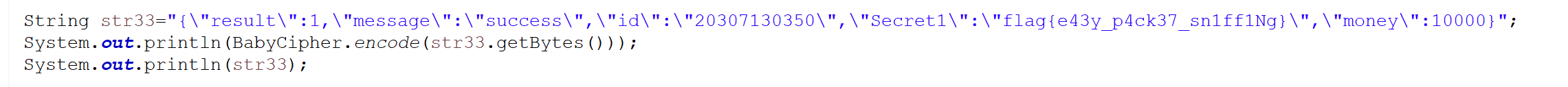
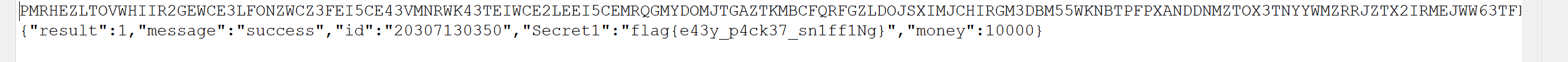
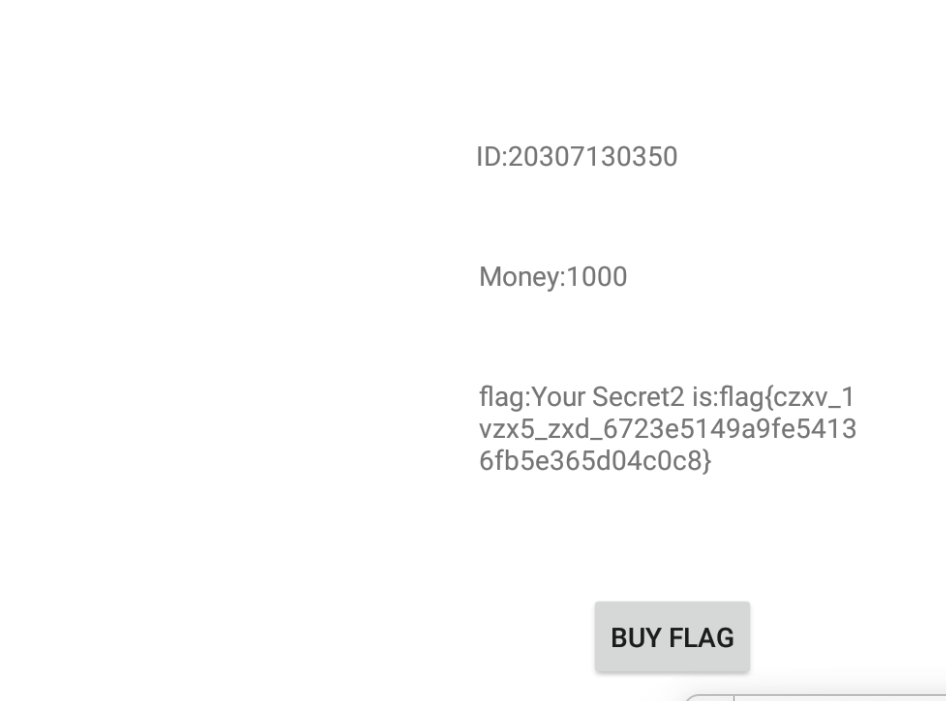
Encode之后得到的结果写入request包中，得到的是naïve…..fake secrect….

因此将is\_fake改为0；



重新encode之后写入request包中，得到

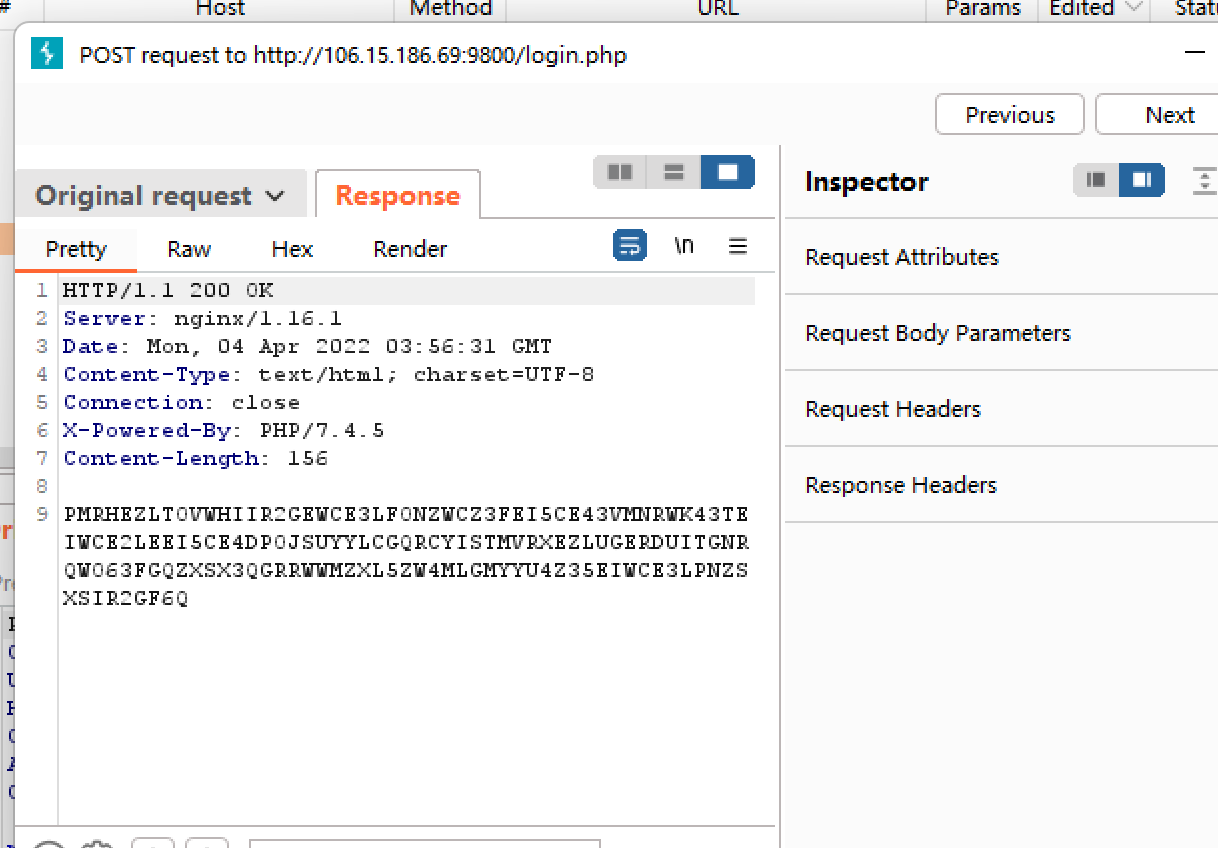
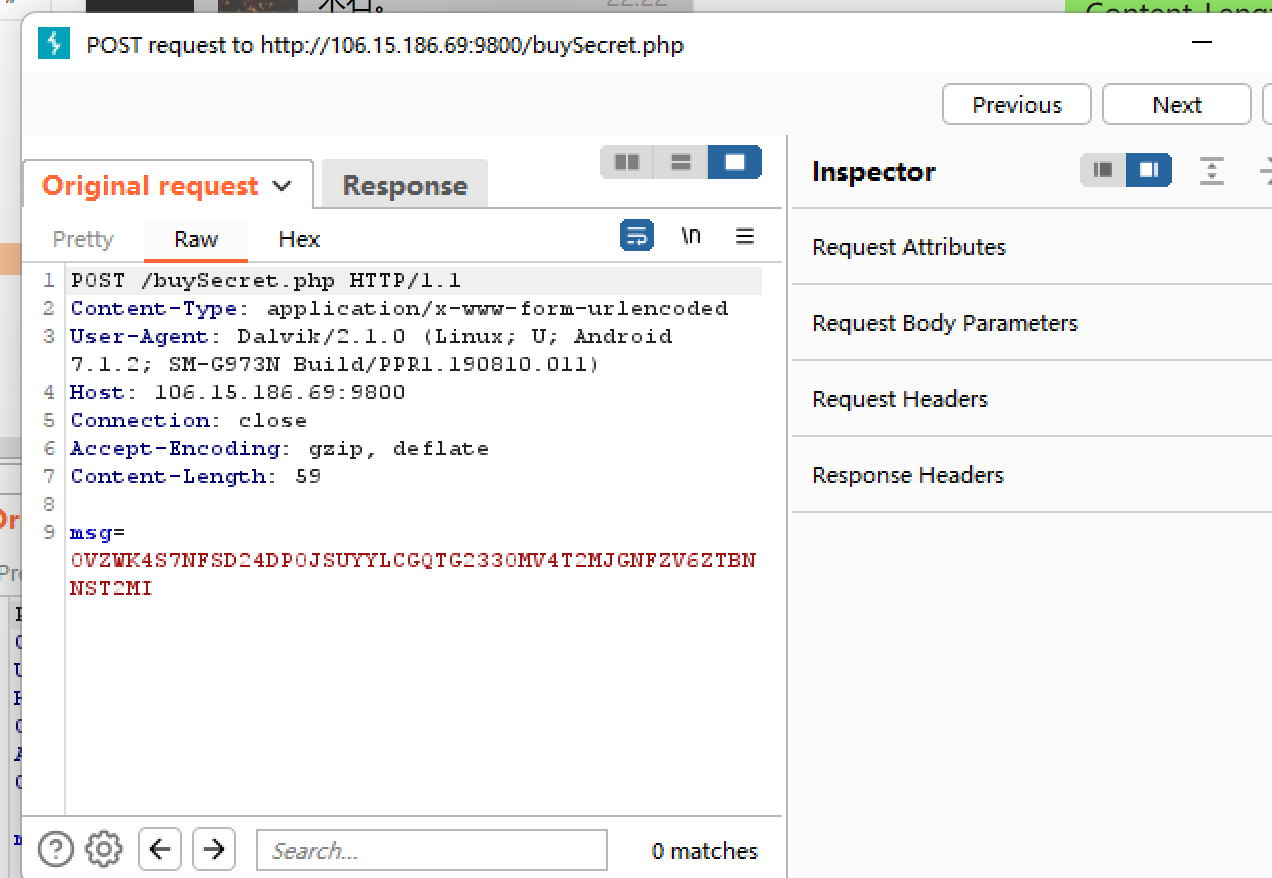
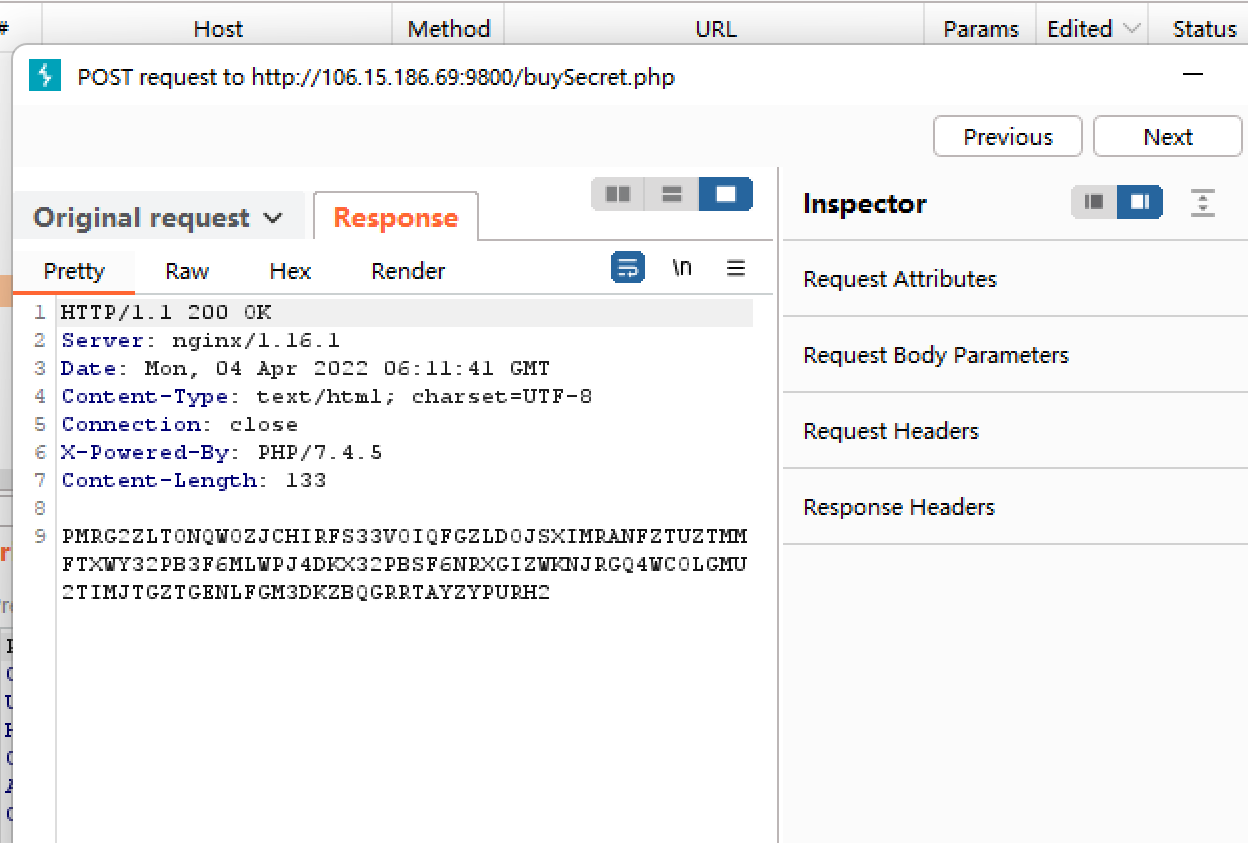
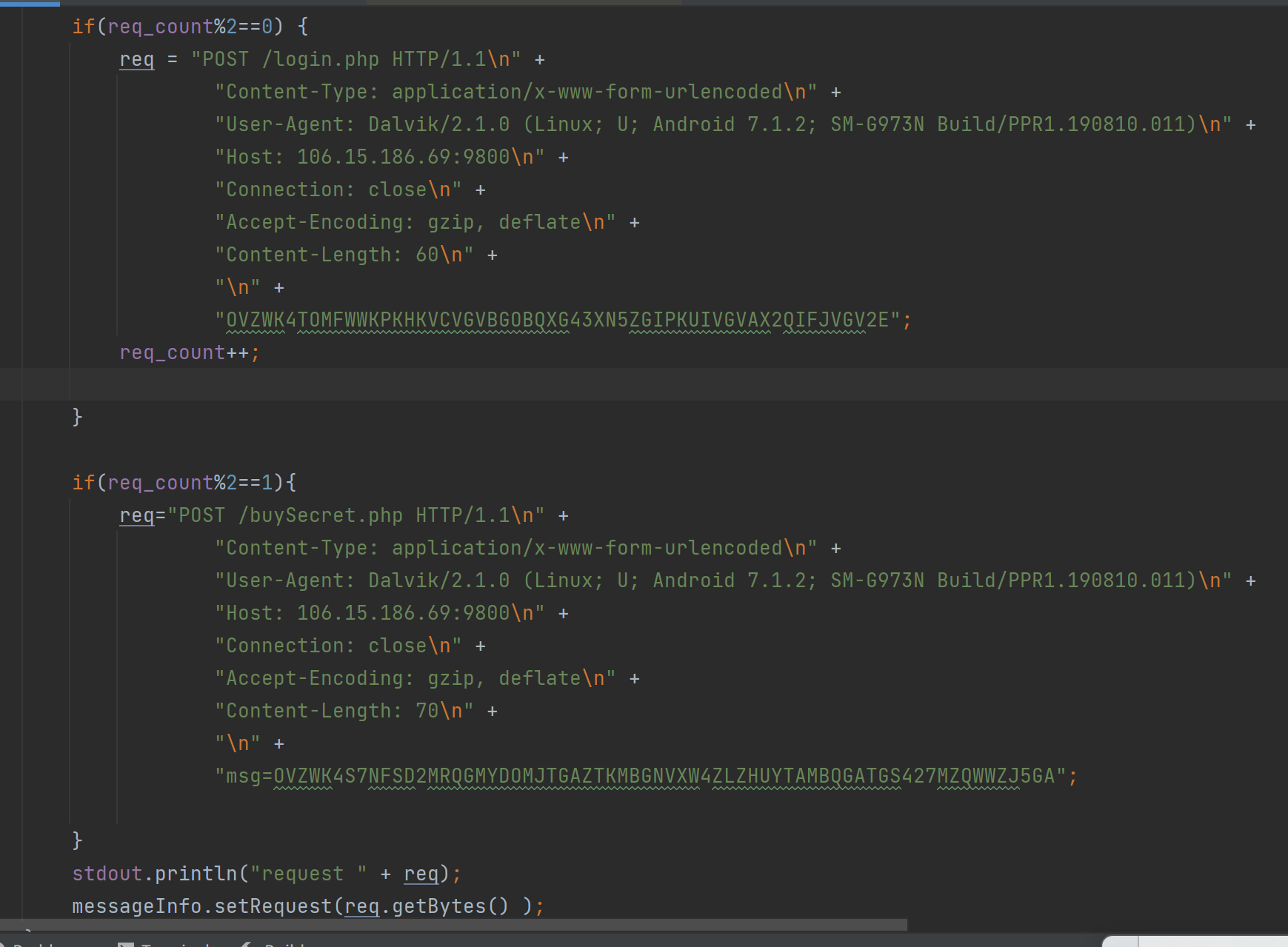
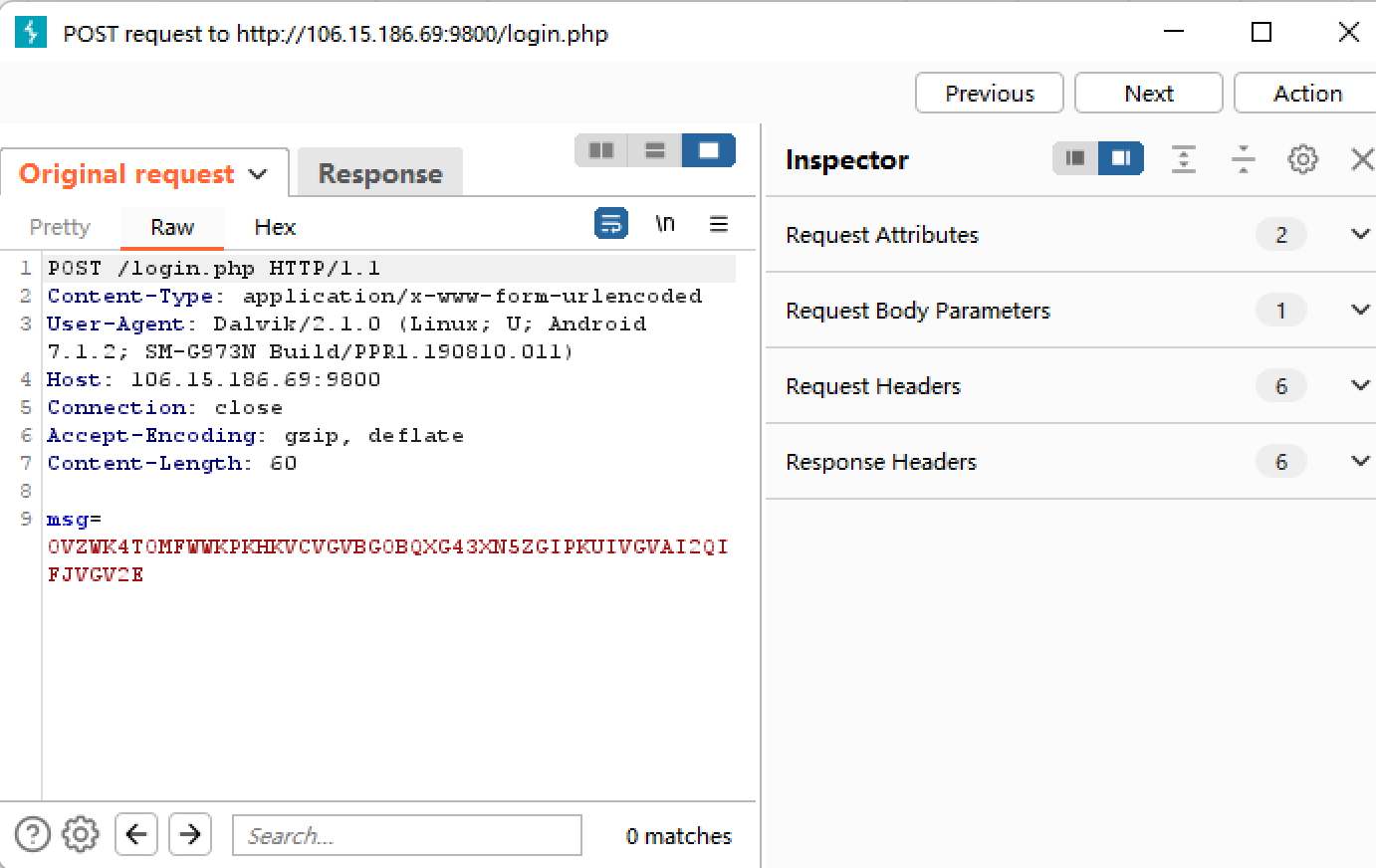


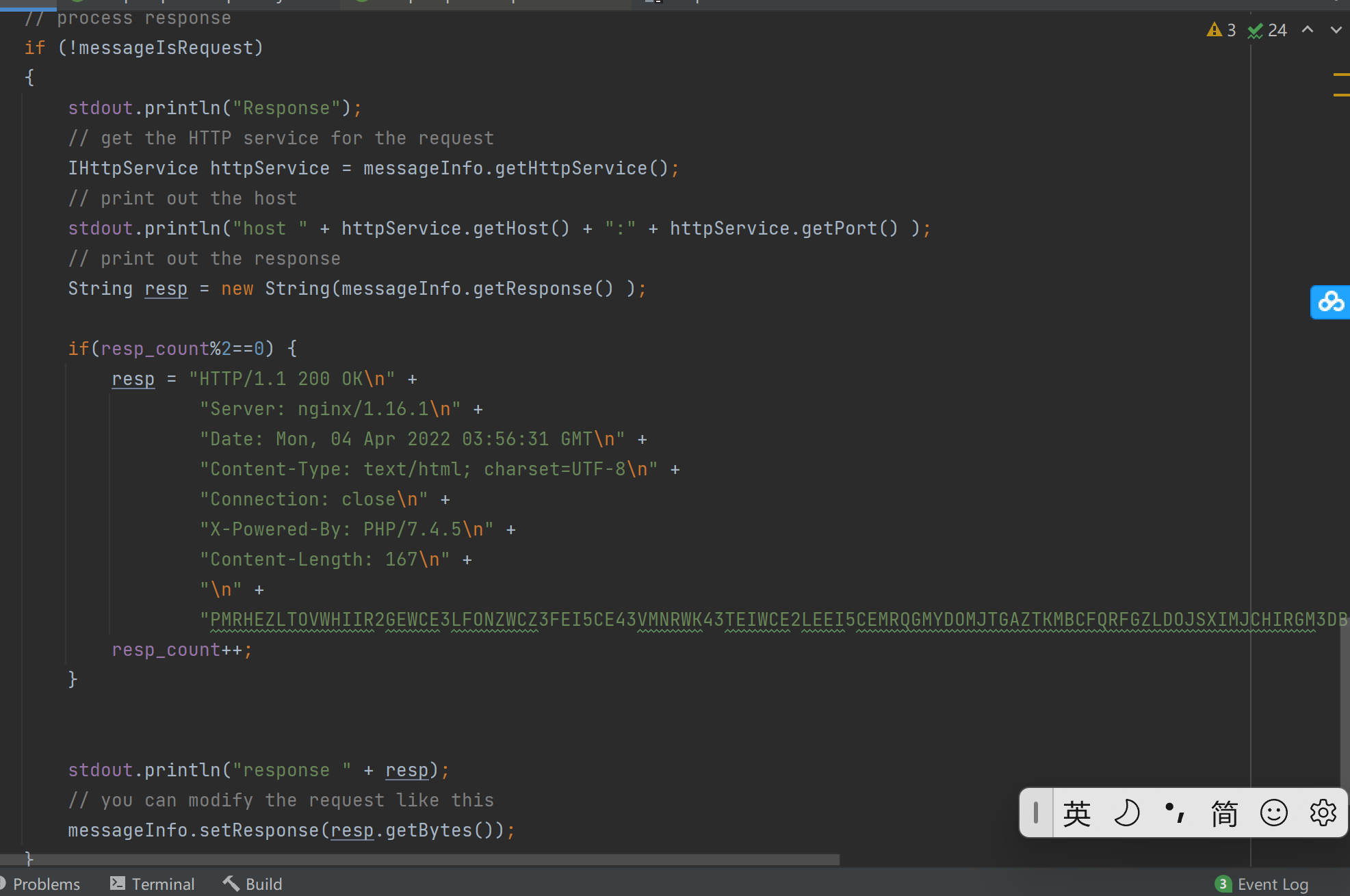
1. 修改id和money：
   1. 对得到的第一个secret1的response 包的结果进行decode，得到
   2. 将其中的”poreLab4”改成20307130350，money改成10000；encode之后的结果写入response包中得到结果
   3. 
   4. 
   5. 根据2.得到flag

* **Task 2**

(1) Writeup

[Record how you solve this task here.]

1. 根据taskA intercept得到的包重写set req和resp，
2. 



1. 注意content-length需要修改到对应的长度。否则无法得到正确的结果。
2. 引入req\_count和resp\_count 变量来确定每次应该返回的request和response包。
3. 优化：引入%来使得可以多次点击buysecret 按钮都能得到正确的secret2；

