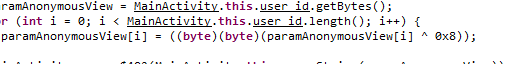
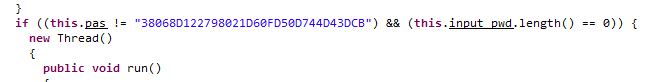
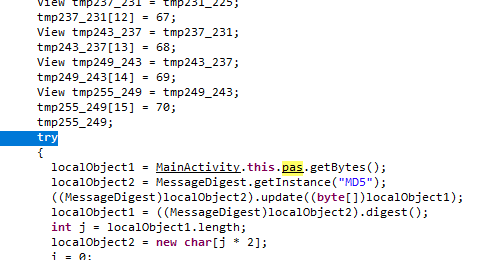
在反编译代码中可以看到这个apk是进行了服务器验证，post用户名和密码，然后返回了两个json数据:status和info

首先要找到密码



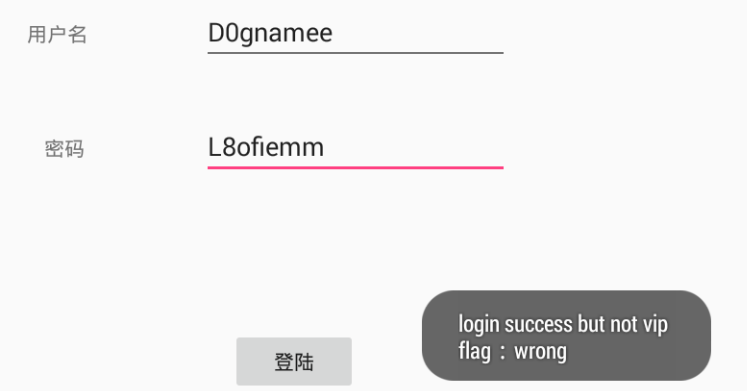


从这里可以看到用户名进行异或算法，然后再进行md5加密然后和一个数据做了比较



将用户名进行异或，得到:L8ofiemm，检验md5加密为38068D122798021D60FD50D744D43DCB,所以L8ofiemm为正确密码

当输入了正确的用户名和密码后，会显示



因为是网络验证，所以进行了抓包，通过抓包可以看到



除了status和info还传回了个table

将table的值进行base64解密，得到 isvip=0 or isvip=7133

试着通过修改post，来上传一个isvip=7133

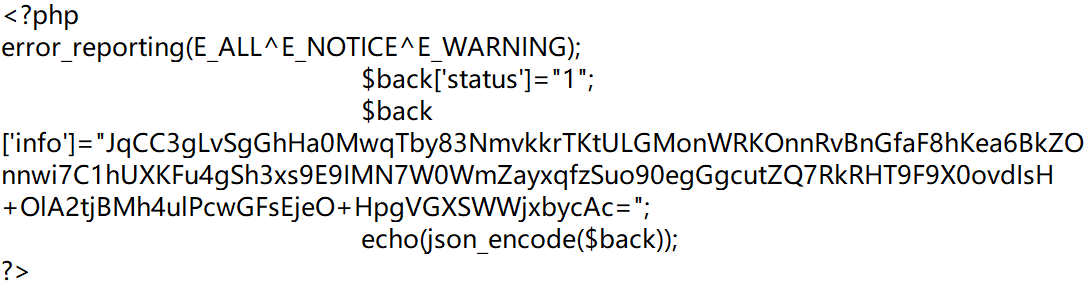


返回了一个数据，通过研究java代码，发现可能是安卓post isvip=7133后用info这个键传回一个数据经过一系列解密，最后弹出flag。

方法一:在本地模拟服务器返回数据

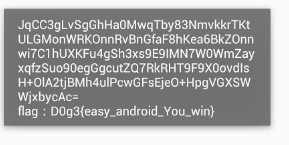
则可以在本地模拟服务器返回值。

构建一个php文件



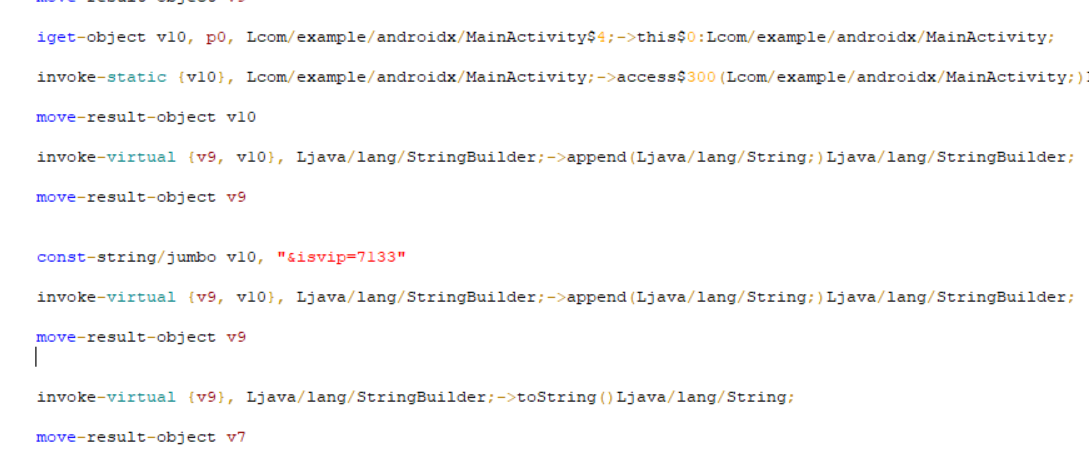
注意要将编码该为UTF-8同时关闭php报错

然后将网址改为模拟器的<http://10.0.2.2/xxx.php>，打包重新编译，再运行就可以得到



方法二:修改smail文件

在smail文件中找到post数据的地方，在传输密码pwd的后面加一句&isvip=7133



同样可以得到

