安卓简单注册器题目writeup

原创

偷一个月亮 于 2019-12-09 01:29:21 发布 240 收藏

分类专栏： android 文章标签： android 逆向

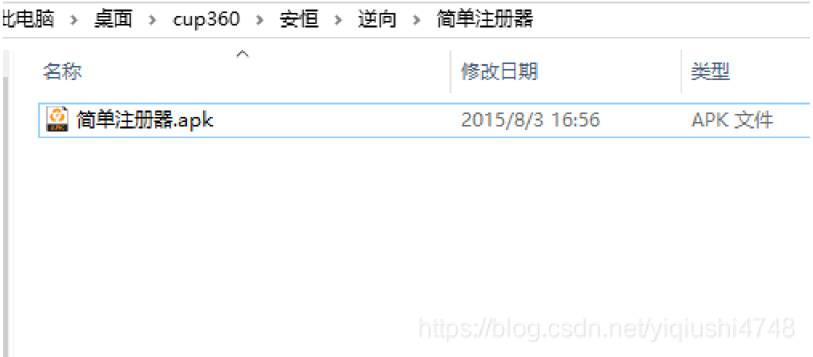
本文链接：https://blog.csdn.net/yiqiushi4748/article/details/103451383

android 专栏收录该内容

0 篇文章 0 订阅

订阅专栏

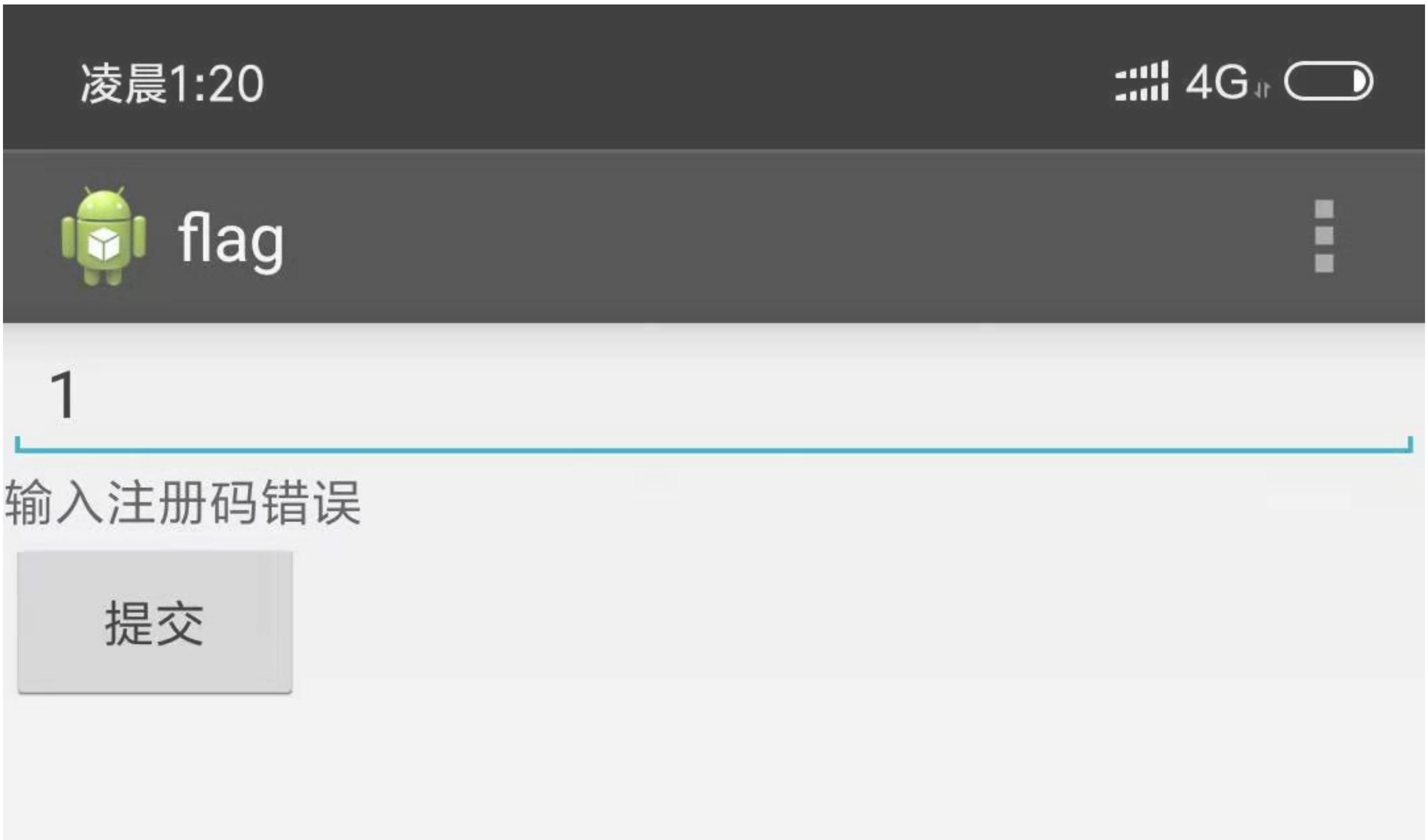
打开题目发现是一个apk，



```
比电脑 › 桌面 › cup360 › 安恒 › 逆向 › 简单注册器

名称                        修改日期            类型
简单注册器.apk              2015/8/3 16:56      APK 文件
```

安装看一下，看到需要输入一个注册码

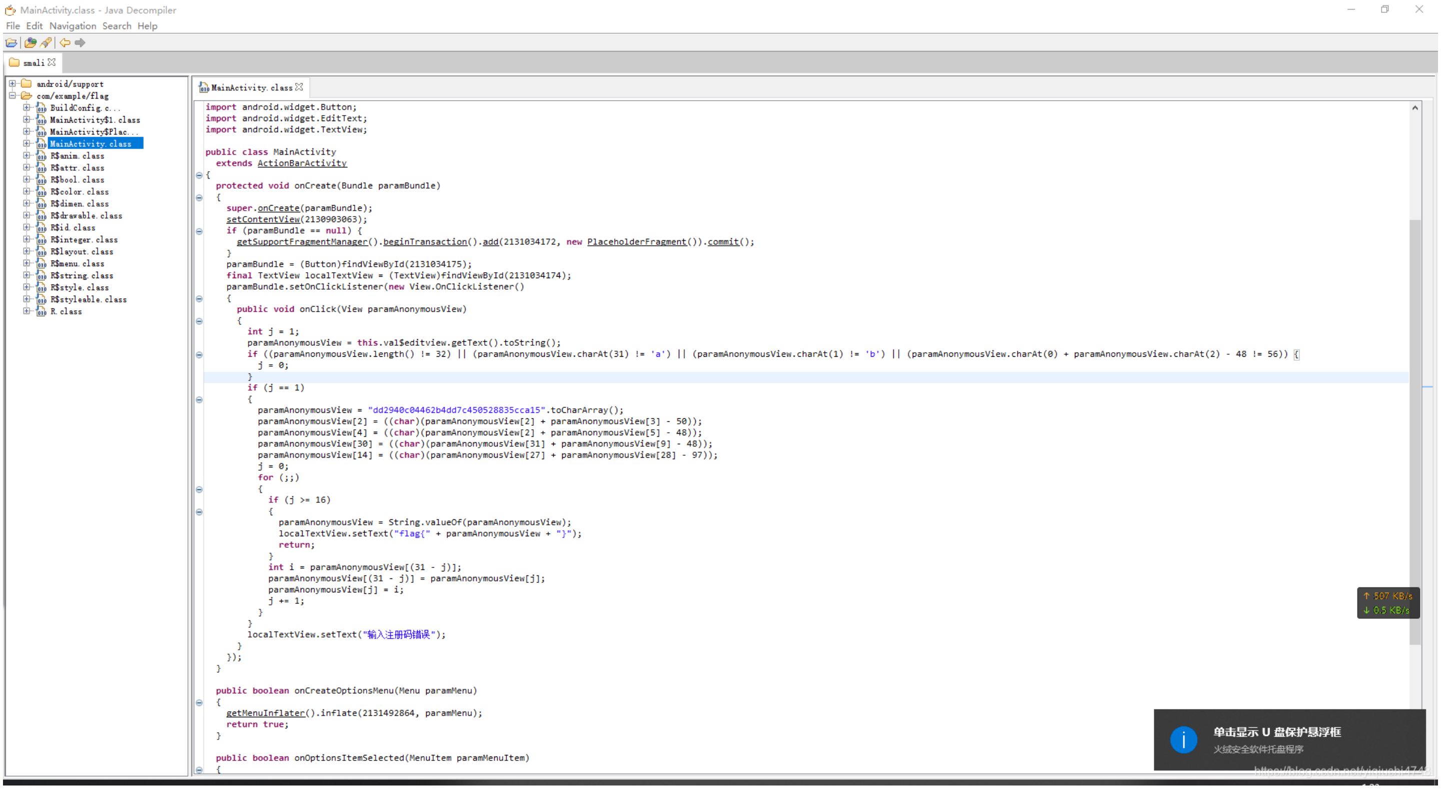
效果如下



输入注册码错误

[redacted]

jd反编译查看源代码



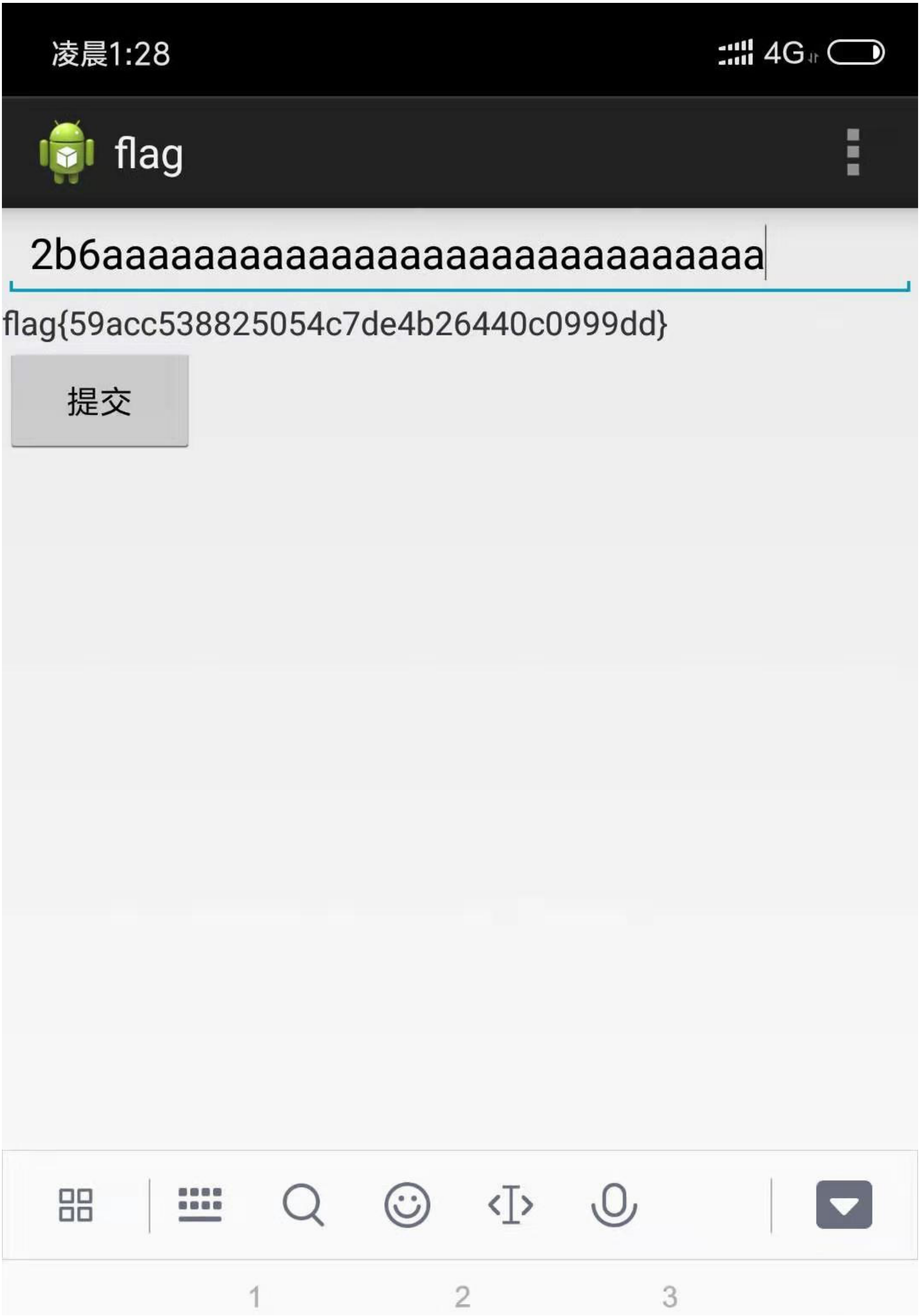
```java
import android.widget.Button;
import android.widget.EditText;
import android.widget.TextView;

public class MainActivity
  extends ActionBarActivity
{
  protected void onCreate(Bundle paramBundle)
  {
    super.onCreate(paramBundle);
    setContentView(2130903063);
    if (paramBundle == null) {
      getSupportFragmentManager().beginTransaction().add(2131034172, new PlaceholderFragment()).commit();
    }
    paramBundle = (Button)findViewById(2131034175);
    final TextView localTextView = (TextView)findViewById(2131034174);
    paramBundle.setOnClickListener(new View.OnClickListener()
    {
      public void onClick(View paramAnonymousView)
      {
        int j = 1;
        paramAnonymousView = this.val$editview.getText().toString();
        if ((paramAnonymousView.length() != 32) || (paramAnonymousView.charAt(31) != 'a') || (paramAnonymousView.charAt(1) != 'b') || (paramAnonymousView.charAt(0) + paramAnonymousView.charAt(2) - 48 != 56)) {
          j = 0;
        }
        if (j == 1)
        {
          paramAnonymousView = "dd2940c04462b4dd7c450528835cca15".toCharArray();
          paramAnonymousView[2] = ((char)(paramAnonymousView[2] + paramAnonymousView[3] - 50));
          paramAnonymousView[4] = ((char)(paramAnonymousView[2] + paramAnonymousView[5] - 48));
          paramAnonymousView[30] = ((char)(paramAnonymousView[31] + paramAnonymousView[9] - 48));
          paramAnonymousView[14] = ((char)(paramAnonymousView[27] + paramAnonymousView[28] - 97));
          j = 0;
          for (;;)
          {
            if (j >= 16)
            {
              paramAnonymousView = String.valueOf(paramAnonymousView);
              localTextView.setText("flag{" + paramAnonymousView + "}");
              return;
            }
            int i = paramAnonymousView[(31 - j)];
            paramAnonymousView[(31 - j)] = paramAnonymousView[j];
            paramAnonymousView[j] = i;
            j += 1;
          }
        }
        localTextView.setText("输入注册码错误");
      }
    });
  }

  public boolean onCreateOptionsMenu(Menu paramMenu)
  {
    getMenuInflater().inflate(2131492864, paramMenu);
    return true;
  }

  public boolean onOptionsItemSelected(MenuItem paramMenuItem)
  {
```

查看器有个if函数进行判断，我们需要让j==1，此时我们要不满足if条件
关键代码如下

```java
paramAnonymousView = this.val$editview.getText().toString();
        if ((paramAnonymousView.length() != 32) || (paramAnonymousView.charAt(31) != 'a') || (paramAnonymousView.charAt(1) != 'b') || (paramAnonymousView.charAt(0) + paramAnonymousView.charAt(2) - 48 != 56)) {
          j = 0;
        }
        if (j == 1)
        {
          paramAnonymousView = "dd2940c04462b4dd7c450528835cca15".toCharArray();
          paramAnonymousView[2] = ((char)(paramAnonymousView[2] + paramAnonymousView[3] - 50));
          paramAnonymousView[4] = ((char)(paramAnonymousView[2] + paramAnonymousView[5] - 48));
          paramAnonymousView[30] = ((char)(paramAnonymousView[31] + paramAnonymousView[9] - 48));
          paramAnonymousView[14] = ((char)(paramAnonymousView[27] + paramAnonymousView[28] - 97));
          j = 0;
          for (;;)
          {
            if (j >= 16)
            {
              paramAnonymousView = String.valueOf(paramAnonymousView);
              localTextView.setText("flag{" + paramAnonymousView + "}");
              return;
            }
```

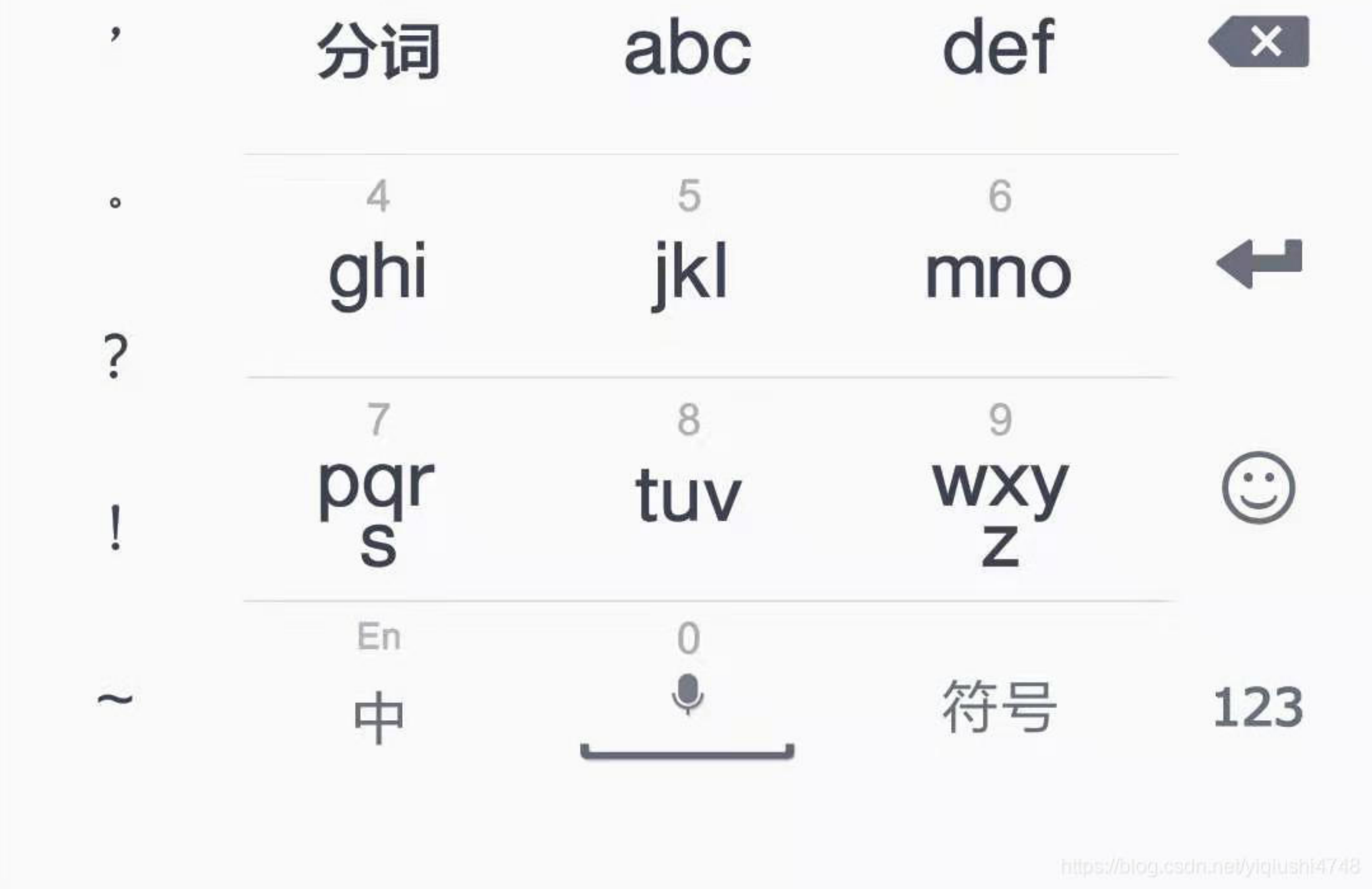
所以需要输入的注册码长度位32且最后一位为a且第二位为b且第一位和第三位的ascii编码和为104，就会输出flag

所以我们构造符合条件的注册码为 `2b6aaaaaaaaaaaaaaaaaaaaaaaaaaaaa` ,提交getflag



2b6aaaaaaaaaaaaaaaaaaaaaaaaaaaaa

flag{59acc538825054c7de4b26440c0999dd}


，
分词
abc
def
。
4
ghi
5
jkl
6
mno
？
7
pqrs
8
tuv
9
wxyz
！
～
En
中
0
符号
123