

# XCTF app1

原创

[pipixia233333](#) 于 2019-01-22 12:52:31 发布 976 收藏

分类专栏: [逆向之旅](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_41071646/article/details/86592704](https://blog.csdn.net/qq_41071646/article/details/86592704)

版权



[逆向之旅](#) 专栏收录该内容

128 篇文章 2 订阅

订阅专栏

本来还想撸驱动的。。。。但是实在撸不下去了 编译原理 打算的是下学期看 所以只能没有什么事来刷刷XCTF的题了

刷刷mobile 还是挺好的~~~~~

然后 这个是入门的题 应该算是简单的

直接反编译的 源代码。。

```
this.btn.setOnClickListener(new View.OnClickListener()
{
    public void onClick(View paramAnonymousView)
    {
        for (;;)
        {
            try
            {
                paramAnonymousView = MainActivity.this.text.getText().toString();
                PackageInfo localPackageInfo = MainActivity.this.getPackageManager().getPackageInfo("com.example.yaphetshan.tencentgreat", 16384);
                str = localPackageInfo.versionName;
                int j = localPackageInfo.versionCode;
                i = 0;
                if ((i >= paramAnonymousView.length()) || (i >= str.length())) {
                    continue;
                }
                if (paramAnonymousView.charAt(i) != (str.charAt(i) ^ j))
                {
                    Toast.makeText(MainActivity.this, "再接再厉, 加油~", 1).show();
                    return;
                }
            }
            catch (PackageManager.NameNotFoundException paramAnonymousView)
            {
                String str;
                int i;
                Toast.makeText(MainActivity.this, "年轻人不要耍小聪明噢", 1).show();
                continue;
            }
            i++;
            continue;
            if (paramAnonymousView.length() != str.length()) {
                continue;
            }
            Toast.makeText(MainActivity.this, "恭喜开启闯关之门!", 1).show();
        }
    }
}
```

然后感觉0。。。。emmmmmmmmmmm

一目了然啊 if (paramAnonymousView.charAt(i) != (str.charAt(i) ^ j))

这个就是判断 条件了 然后 他这个是拿我们输入的字符串看的 我们去看 另一个是什么

PackageInfo localPackageInfo =

MainActivity.this.getPackageManager().getPackageInfo("com.example.yaphetshan.tencentgreat", 16384);

str = localPackageInfo.versionName;

str= 这个包里面的 versionName 成员 我们直接去找这个成员就好了

```
package com.example.yaphetshan.tencentgreat;

public final class BuildConfig
{
    public static final String APPLICATION_ID = "com.example.yaphetshan.tencentgreat";
    public static final String BUILD_TYPE = "debug";
    public static final boolean DEBUG = Boolean.parseBoolean("true");
    public static final String FLAVOR = "";
    public static final int VERSION_CODE = 15;
    public static final String VERSION_NAME = "X<cP[?PHNB<P?aj";
}
```

[https://blog.csdn.net/qq\\_41071646](https://blog.csdn.net/qq_41071646)

然后 写出脚本就好了

```
#include <iostream>
#include <algorithm>
#include <stdio.h>
#include <math.h>
#include <string.h>
#include <queue>
#include <vector>
#include <algorithm>
#include <map>
using namespace std;
char s[]="X<cP[?PHNB<P?aj";
int code=15;
int main()
{
    for(int i=0;i<strlen(s);i++)
    {
        printf("%c",s[i]^code);
    }
    return 0;
}
```

得出答案

W3l\_T0\_GAM3\_One