BUUCTF 简单题

原创

mUn0s 于 2021-05-14 22:37:34 发布 163 收藏
分类专栏： CTF

本文链接：https://blog.csdn.net/ciudadcaa/article/details/116808015

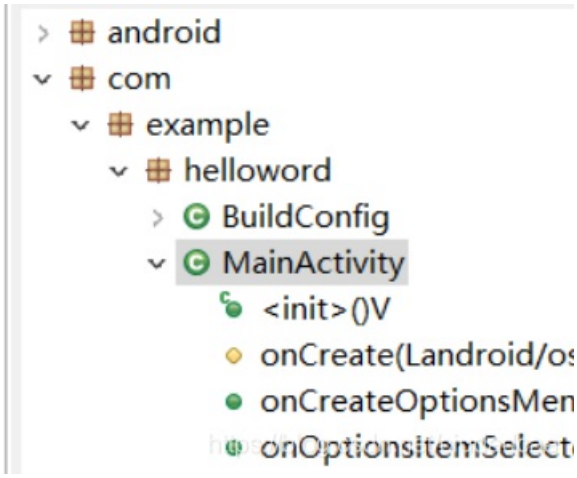
py不动了来做简单题学知识：

BUUCTF:

helloword:

下载下来是APK文件，应该是Mobile题型，

拿jed打开找到主函数



点进去，就看到了flag

```
.method public constructor <init>()V
          .registers 1
00000000  invoke-direct       ActionBarActivity-><init>()V, p0
00000006  return-void
.end method

.method protected onCreate(Bundle)V
          .registers 6
00000000  invoke-super        ActionBarActivity->onCreate(Bundle)V, p0, p1
00000006  const               v3, 0x7F030018
0000000C  invoke-virtual      MainActivity->setContentView(I)V, p0, v3
00000012  const-string        v0, "flag{7631a988259a00816deda84afb29430a}"
00000016  const-string        v1, "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
0000001A  invoke-virtual      String->compareTo(String)I, v0, v1
00000020  move-result         v2
00000022  return-void
.end method
```


XOR:

典型的逆向，IDA打开进入主函数F5反编译

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int i; // [rsp+2Ch] [rbp-124h]
  char __b[264]; // [rsp+40h] [rbp-110h] BYREF

  memset(__b, 0, 0x100uLL);
  printf("Input your flag:\n");
  get_line(__b, 256LL);
  if ( strlen(__b) != 33 )
    goto LABEL_7;
  for ( i = 1; i < 33; ++i )
    __b[i] ^= __b[i - 1];
  if ( !strncmp(__b, global, 0x21uLL) )
    printf("Success");
  else
LABEL_7:
    printf("Failed");
  return 0;
}
```


可以看到我们要输入一串字符串，长度为33，然后前一位和后一位作XOR运算，与global变量比较相等则输出成功

点进global查看

```
segment byte public 'DATA' use64
assume cs:__cstring
;org 100000F6Eh
db 'f',0Ah              ; DATA XREF: __data:_global↓o
db 'k',0Ch,'w&O.@',11h,'x',0Dh,'Z;U',11h,'p',19h,'F',1Fh,'v"M#D',0Eh,'g'
db 6,'h',0Fh,'G2O',0
db 'Input your flag:',0Ah,0
                        ; DATA XREF: _main+B↑o
ccess[]
db 'Success',0          ; DATA XREF: _main+122↑o
iled[]
db 'Failed',0           ; DATA XREF: _main:loc_100000EB0↑o
align 4
ends
```


是一串字符串，只需要逆着回去就行了，编写py程序，这里我懒得写直接搬的，第一位f不用动,本来就是相等的

```
s = ['f',0xA,'k',0xC,'w','&','O','.','@',0x11,'x',0xD,'Z',';','U',0x11,'p',0x19,'F',0x1F,'v','"','M','#','D
flag = 'f'#第一个字符不用进行异或运算
for i in range(1,len(s)):
    if(isinstance(s[i],int)):#将数字转化为字符
        s[i] = chr(s[i])
for i in range(1,len(s)):
    flag += chr(ord(s[i]) ^ ord(s[i-1]))#a^b=c 等于 a^c=b

print(flag)
```

这里isinstance() 函数就是来判断一个对象是否是一个已知的类型，类似 type()。

> isinstance() 与 type() 区别：
>
> type() 不会认为子类是一种父类类型，不考虑继承关系。
>
> isinstance() 会认为子类是一种父类类型，考虑继承关系。
>
> 如果要判断两个类型是否相同推荐使用 isinstance()。

ord()函数主要用来返回对应字符的ascii码； chr()主要用来表示ascii码对应的字符，可以用十进制，也可以用十六进制。

基础知识点说多了有点~，然后运行，得flag

flag{QianQiuWanDai_YiTongJiangHu}