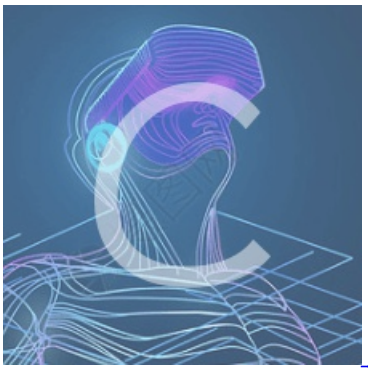
BUUCTF_xor

原创

ZYen12138 于 2020-10-16 13:05:30 发布

分类专栏： # BUUCTF CTF

本文链接：https://blog.csdn.net/weixin_46009088/article/details/109114316



BUUCTF 同时被 2 个专栏收录

17 篇文章 2 订阅

订阅专栏

CTF

17 篇文章 0 订阅

订阅专栏

BUUCTF_xor

用IDA载入，按F5打开_main函数，如下：

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char *v3; // rsi
  int result; // eax
  signed int i; // [rsp+2Ch] [rbp-124h]
  char v6[264]; // [rsp+40h] [rbp-110h]
  __int64 v7; // [rsp+148h] [rbp-8h]

  memset(v6, 0, 0x100uLL);
  v3 = (char *)256;
  printf("Input your flag:\n", 0LL);
  get_line(v6, 256LL);
  if ( strlen(v6) != 33 )
    goto LABEL_12;
  for ( i = 1; i < 33; ++i )
    v6[i] ^= v6[i - 1];
  v3 = global;
  if ( !strncmp(v6, global, 0x21uLL) )
    printf("Success", v3);
  else
LABEL_12:
    printf("Failed", v3);
  result = __stack_chk_guard;
  if ( __stack_chk_guard == v7 )
    result = 0;
  return result;
}
```


有两个关键函数strlen和strncmp，strlen指出该字符串长度是33，strncmp将v6和global进行对比，上面对v6进行修改，所以global是xor后的结果，点击global来到字符串的位置，看到下面的字符串,一看好像没有33个字符。

```
; DATA XREF: _main+10D↑r
; "f\nk\fw&O.@\x11x\rZ;U\x11p\x19F\x1Fv\"M"...
```

再点击进去找到最终的字符串：

```
(WOXZUPFVMDGH db 'f',0Ah      ; DATA XREF: __data:global↓o
 'k',0Ch,'w&O.@',11h,'x',0Dh,'Z;U',11h,'p',19h,'F',1Fh,'v"M#D',0Eh,'g',6,'h',0Fh,'G2O',0
```

用python写出脚本：

```
s = ['f',0xA,'k',0xC,'w','&','O','.','@',0x11,'x',0xD,'Z',';','U',0x11,'p',0x19,'F',0x1F,'v','"','M','#','D',0xE
,'g',6,'h',0xF,'G','2','O']
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)
```

运行等到下图：

```
flag{QianQiuWanDai_YiTongJiangHu}
```