BUUCTF Reverse xor WriteUp

原创

PlumpBoy 于 2021-09-10 18:40:36 发布 316 收藏

分类专栏： BUUCTF 逆向题解 文章标签： 系统安全 安全

本文链接：https://blog.csdn.net/weixin_45723661/article/details/120227871

xor-WP

首先吧xor文件扔进IDA里面

```
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 )//注意此处i是从1开始的
    __b[i] ^= __b[i - 1];
  if ( !strncmp(__b, global, 0x21uLL) )
    printf("Success");
  else
LABEL_7:
    printf("Failed");
  return 0;
}
```

通过分析源码得出，此处为输入的33位，每一位与其前一位进行异或后的值再与global进行比较。

global的值为

```
0000F6E                 assume cs:__cstring
0000F6E                 ;org 100000F6Eh
0000F6E aFKWOXZUPFVMDGH db 'f',0Ah              ; DATA XREF: __data:_global↓o
0000F6E                 db 'k',0Ch,'w&O.@',11h,'x',0Dh,'Z;U',11h,'p',19h,'F',1Fh,'v"M#D',0Eh,'g'
0000F6E                 db 6,'h',0Fh,'G2O',0
```

将这些字符全部转换为十六进制，注意最后一位0是字符串结尾，不需要写。

python写出解密脚本为：

```
a = [0x00, 0x66, 0x0A, 0x6b, 0x0c, 0x77, 0x26, 0x4f, 0x2e, 0x40,
     0x11, 0x78, 0x0d, 0x5a, 0x3b, 0x55, 0x11, 0x70, 0x19, 0x46,
     0x1f, 0x76, 0x22, 0x4d, 0x23, 0x44, 0x0e, 0x67, 0x06, 0x68,
     0x0f, 0x47, 0x32, 0x4f]
flag = ""
for i in range(1, len(a)):
    flag += chr(a[i] ^ a[i-1])
print(flag)
```

flag为`flag{QianQiuWanDai_YiTongJiangHu}`