

buuctf-xor

原创

bygwys 于 2022-01-18 16:04:41 发布 105 收藏

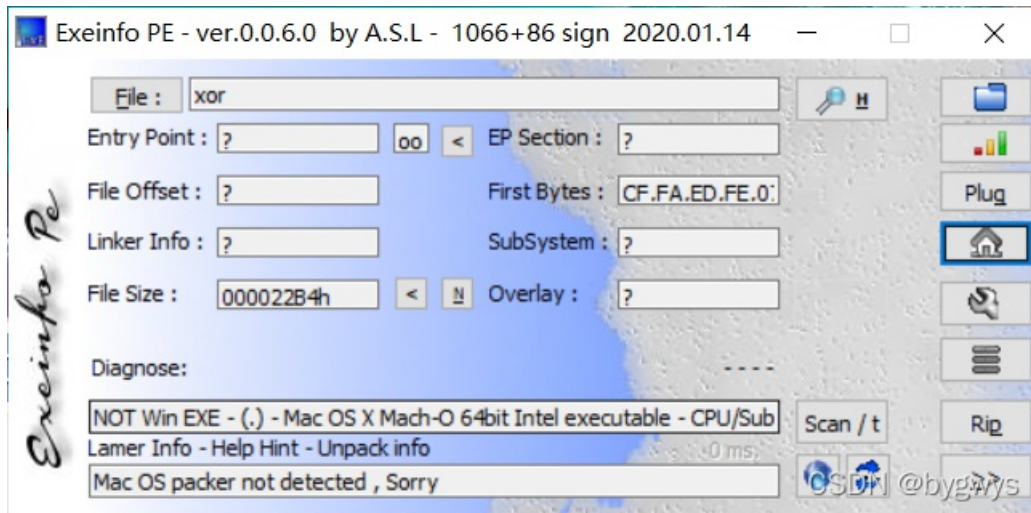
文章标签: [p2p](#) [linux](#) [gnu](#)

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/bygwys/article/details/122562089>

版权

先查壳64位



找到主函数

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     int i; // [rsp+2Ch] [rbp-124h]
4     char __b[264]; // [rsp+40h] [rbp-110h] BYREF
5
6     memset(__b, 0, 0x100uLL);
7     printf("Input your flag:\n");
8     get_line(__b, 256LL);
9     if ( strlen(__b) != 33 )
10        goto LABEL_7;
11    for ( i = 1; i < 33; ++i )
12        __b[i] ^= __b[i - 1];
13    if ( !strncmp(__b, global, 0x21uLL) )
14        printf("Success");
15    else
16 LABEL_7:
17        printf("Failed");
18    return 0;
19 }
```

CSDN @bygwys

字符串显示

```
0E ;org 100000F0E11
6E aFKWOXZUPFVMDGH db 'f',0Ah ; DATA XREF: __data:_global↓
6E db 'k',0Ch,'w&0.@',11h,'x',0Dh,'Z;U',11h,'p',19h,'F',1Fh,'v"M#D',0Eh,'g'
6E db 6,'h',0Fh,'G20',0
90 aInputYourFlag db 'Input your flag:',0Ah,0
90 ; DATA XREF: _main+B↑
A2 ; const char aSuccess[]
A2 aSuccess db 'Success',0 ; DATA XREF: _main+122↑
AA ; const char aFailed[]
AA aFailed db 'Failed',0 ; DATA XREF: _main:loc_100000EB0↑
B1 align 4
B1 __cstring ends
B1
000FB4 ; =====
```

CSDN @bygwys

写脚本

The screenshot shows the Dev-C++ 5.11 IDE. The main window displays a C++ program named 1.cpp. The code is as follows:

```
1 #include <stdio.h>
2 int main()
3 {
4     int i;
5     char b[264]={'f',0x0A,'k',0x0C,'w','&','0','.', '@',0x11,'x',0x0D,
6     char a[264]={0};
7     for ( i = 1; i < 33; ++i )
8         a[i] = b[i]^b[i - 1];
9     for ( i = 1; i < 33; ++i )
10        printf("%c",a[i]);
11        public int __cdecl printf (const char * __restrict__ _Format, ...)
12 }
```

The output window shows the execution of the program. The output is:

```
lag{QianQiuWanDai_YiTongJiangHu}
-----
Process exited after 0.2359 seconds with return value 0
请按任意键继续. . .
```

The status bar at the bottom of the IDE shows the current cursor position: 行: 10 列: 16.

CSDN @bygwys

因为第一位不参与所以加个f

flag{QianQiuWanDai_YiTongJiangHu}