

BUUCTF Reverse reverse2 WriteUp

原创

PlumpBoy



于 2021-09-10 18:35:53 发布



24



收藏

分类专栏: [BUUCTF 逆向题解](#) 文章标签: [linux](#) [系统安全](#) [安全](#) [经验分享](#)

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/weixin_45723661/article/details/120227810

版权



[BUUCTF 逆向题解 专栏收录该内容](#)

18 篇文章 1 订阅

订阅专栏

reverse_2

拖入HxD中看见ELF, linux平台的程序, 但是懒得开虚拟机了, 顺手搜索了一下, 看见了一个很像flag的字符串, 结果提交试了下, 错误的, 那么应该是程序对这个字符串做了一些操作。

```
00001030 26 06 40 00 00 00 00 00 36 06 40 00 00 00 00 00 &.@.....6.@.....
00001040 46 06 40 00 00 00 00 00 56 06 40 00 00 00 00 00 F.@.....V.@.....
00001050 66 06 40 00 00 00 00 00 76 06 40 00 00 00 00 00 f.@.....v.@.....
00001060 86 06 40 00 00 00 00 00 00 00 00 00 00 00 00 00 t.@.....
00001070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00001080 7B 68 61 63 6B 69 6E 67 5F 66 6F 72 5F 66 75 6E {hacking_for_fun
00001090 7D 00 47 43 43 3A 20 28 55 62 75 6E 74 75 20 34 }.GCC: (Ubuntu 4
000010A0 2E 38 2E 34 2D 32 75 62 75 6E 74 75 31 7E 31 34 .8.4-2ubuntu1~14
000010B0 2E 30 34 2E 33 29 20 34 2E 38 2E 34 00 00 2E 73 .04.3) 4.8.4...s
000010C0 79 6D 74 61 62 00 2E 73 74 72 74 61 62 00 2E 73 ymtab..strtab..s
000010D0 68 73 74 72 74 61 62 00 2E 69 6E 74 65 72 70 00 hstrtab..interp.
000010E0 2E 6E 6F 74 65 2E 41 42 49 2D 74 61 67 00 2E 6E .note.ABI-tag..n
000010F0 6F 74 65 2E 67 6E 75 2E 62 75 69 6C 64 2D 69 64 ote.gnu.build-id
00001100 00 2E 67 6E 75 2E 68 61 73 68 00 2E 64 79 6E 73 ..gnu.hash..dys
```



CSDN @PlumpBoy

拖入IDA

```

v8 = __readfsqword(0x28u);
pid = fork();
if ( pid )
{
    waitpid(pid, &stat_loc, 0);
}
else
{
    for ( i = 0; i <= strlen(&flag); ++i )
    {
        if ( *(&flag + i) == 'i' || *(&flag + i) == 'r' )
            *(&flag + i) = '1';
    }
}
printf("input the flag:");
__isoc99_scanf("%20s", s2);
if ( !strcmp(&flag, s2) )
    result = puts("this is the right flag!");
else
    result = puts("wrong flag!");
return result;
}

```

核心就是for循环，它对flag字符串进行了转换，再与输入进行比较。通过查询发现flag就是我们上面找到的字符串。写个程序将其输出就可以了。

```

#include<iostream>
#include<stdio.h>
using namespace std;

int main()
{
    char a[] = "hacking_for_fun";
    for (int i = 0; i <= 15; ++i)
    {
        if ( a[i] == 'i' || a[i] == 'r' )
            a[i] = '1';
        cout << a[i];
    }
    return 0;
}

```

```

hacking_for_fun
D:\C++\20210522\Project1\Debug\Project1.exe (进程 16136)已退出, 代码为 0。
按任意键关闭此窗口. . .

```