

实验吧CTF逆向题目逆向观察题解

原创

iqiqiya 于 2017-12-26 20:12:47 发布 2068 收藏

分类专栏: [-----实验吧CTF 我的CTF进阶之路](#) 文章标签: [逆向](#) [writeup](#) [逆向观察](#) [实验吧CTF](#) [reverse](#)

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/xiangshangbashaonian/article/details/78906020>

版权



[-----实验吧CTF 同时被 2 个专栏收录](#)

6 篇文章 0 订阅

订阅专栏

[我的CTF进阶之路](#)

108 篇文章 18 订阅

订阅专栏

附上题目链接

<http://ctf5.shiyanbar.com/reverse/rev50/rev50>

IDA调试

```
sub_4004F0 .plt
puts .plt
__stack_chk_fail .plt
__libc_start_main .plt
strcap .plt
__gaon_start__ .plt
memcpy .plt
_start .text
deregister_tm_clones .text
register_tm_clones .text
__do_global_ctors_aux .text
frame_dummy .text
main .text
__libc_csu_init .text
__libc_csu_fini .text
_tera_proc .fini
puts .exte
__stack_chk_fail .exte
__libc_start_main .exte
strcap .exte
memcpy .exte
3 signed int i; // [rsp+1Ch] [rbp-64h]
4 __int64 src; // [rsp+20h] [rbp-60h]
5 int v6; // [rsp+28h] [rbp-58h]
6 __int16 v7; // [rsp+2Ch] [rbp-54h]
7 char v8; // [rsp+2Eh] [rbp-52h]
8 char dest; // [rsp+30h] [rbp-50h]
9 unsigned __int64 v10; // [rsp+68h] [rbp-18h]
10
11 v10 = __readfsqword(0x28u);
12 if ( argc <= 1 )
13 {
14     puts("usage ./rev50 password");
15 }
16 else
17 {
18     src = 'sedecrem';
19     v6 = 0;
20     v7 = 0;
21     v8 = 0;
22     memcpy(&dest, &src, '\t');
23     for ( i = 0; i <= 999; ++i )
24     {
25         if ( !strcmp(argv[1], (&dict)[i]) && !str
26         {
27             puts("Good password ! ");
28             goto LABEL_10;
29         }
30     }
```

可知只要先按R转成字符串 再将sedecrem逆序即可

Linux下调试:

首先放到Ubuntu里, chmod +x 附上执行权限

但发现程序需要后挂参数运行 rev50 123456

`gdb -q rev50 #gdb挂载调试此程序`

然后disas main 显示所有的函数，发现有2个比较函数，此时断点下哪个都行

然后set args 123456设置挂载参数

直接r跑起来得到mercedes