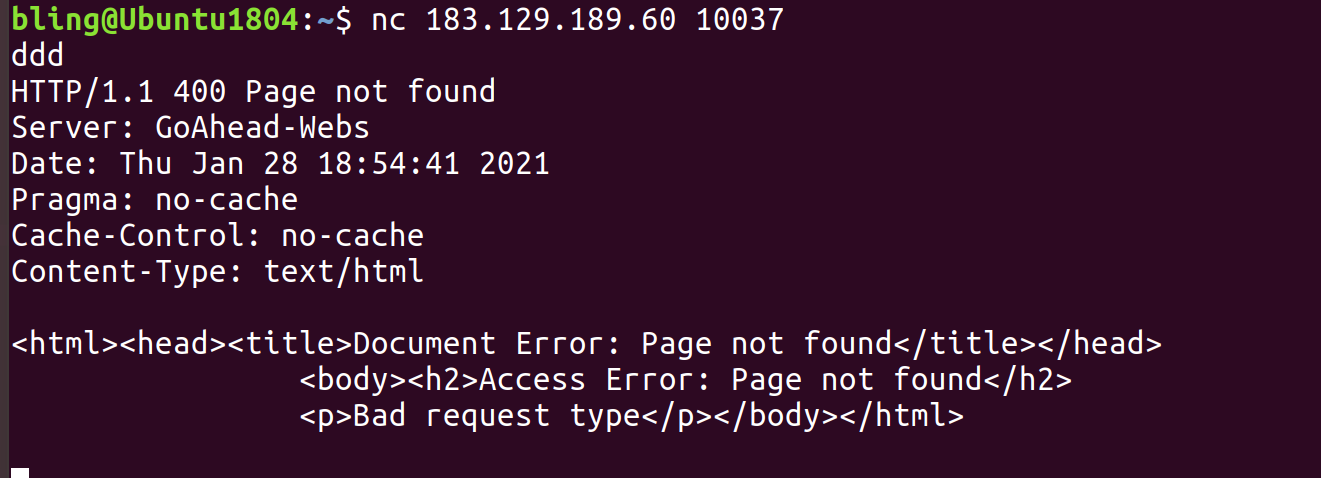
# blinkblink题解

## 1 尝试访问

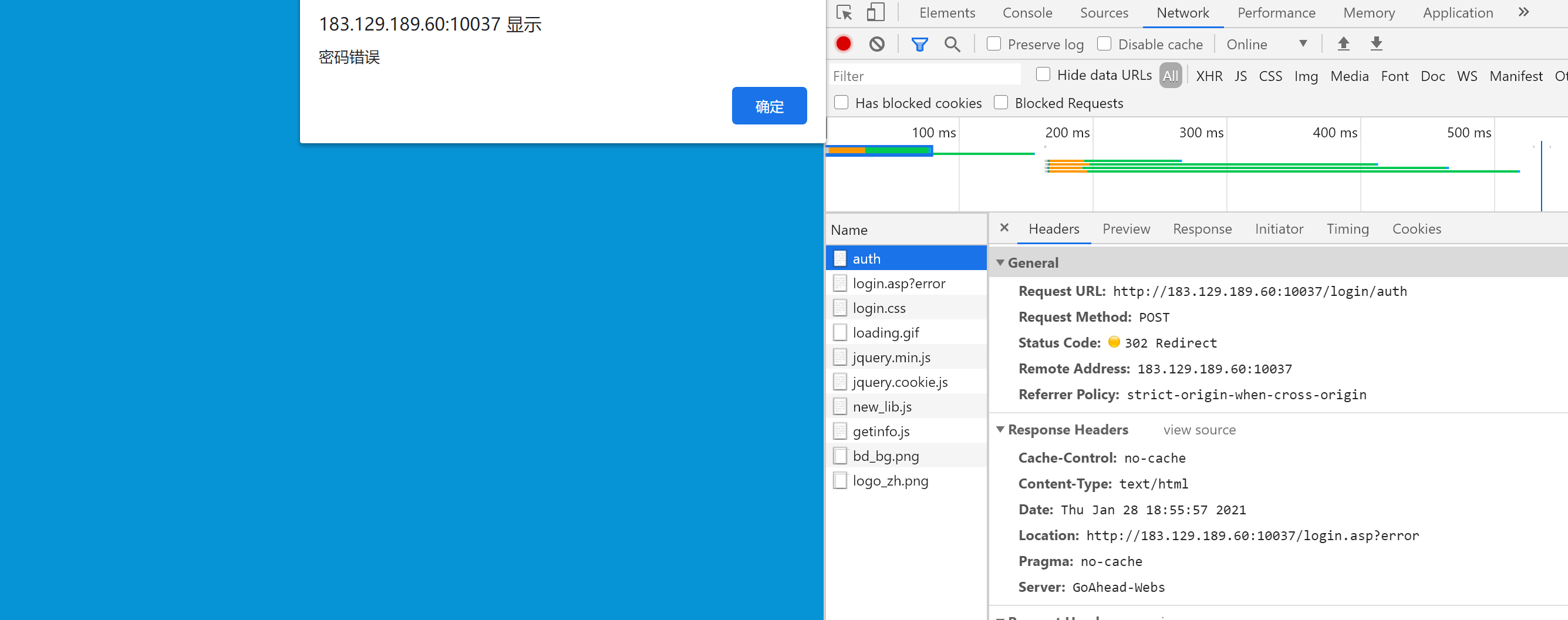
nc连上给的ip



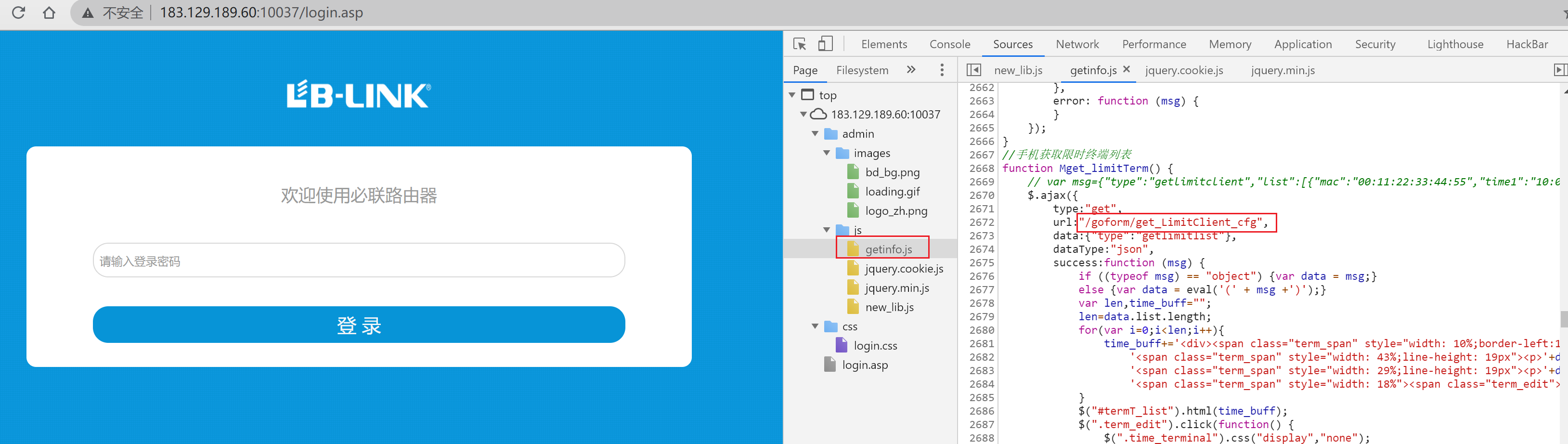
浏览器打开



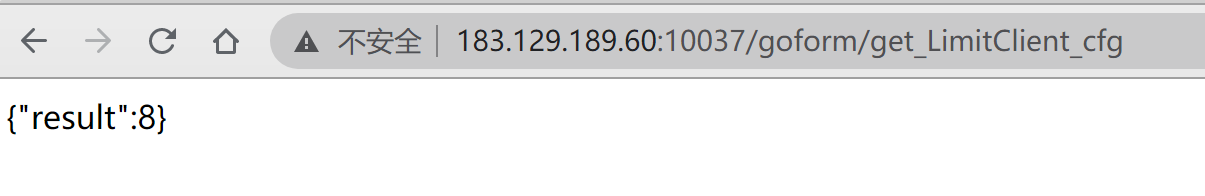
尝试登陆，查看网页文件源码



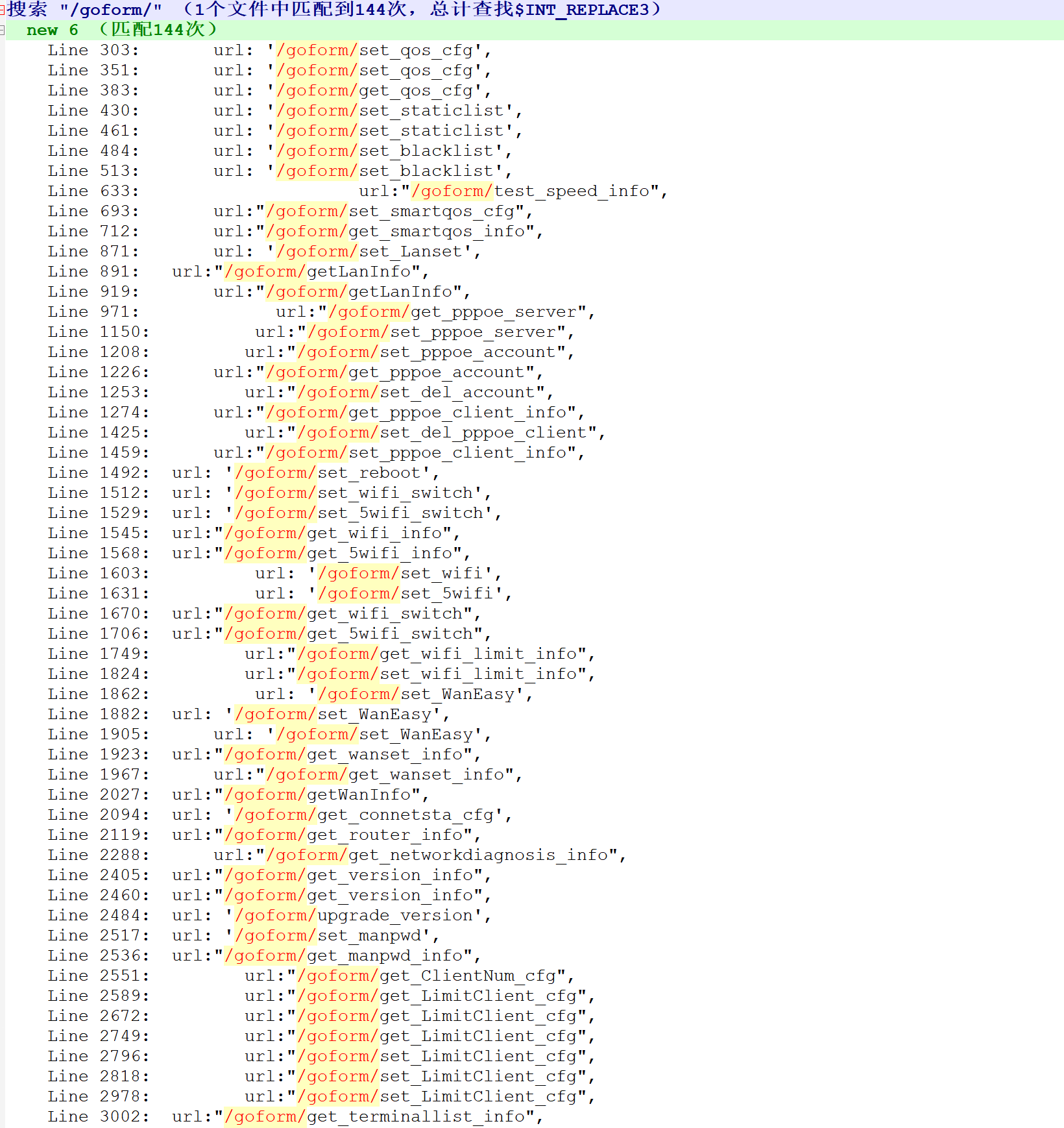
发现getinfo.js中有url，尝试访问



有返回值

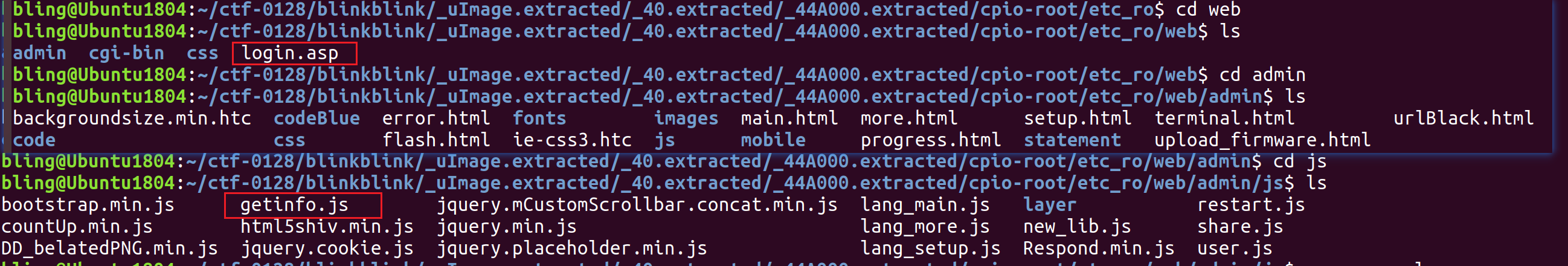


该js中有144个url

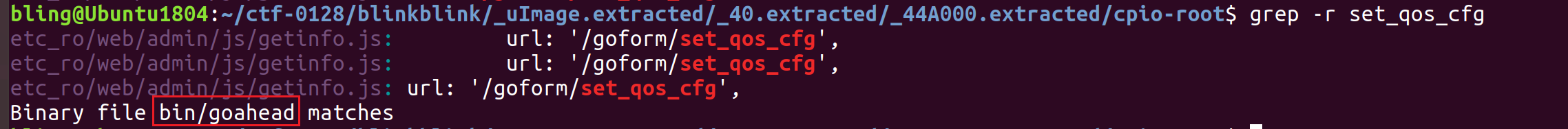


## 2 分析本地固件包

下载下来的固件包用binwalk解包，找到了login.asp以及getinfo.js

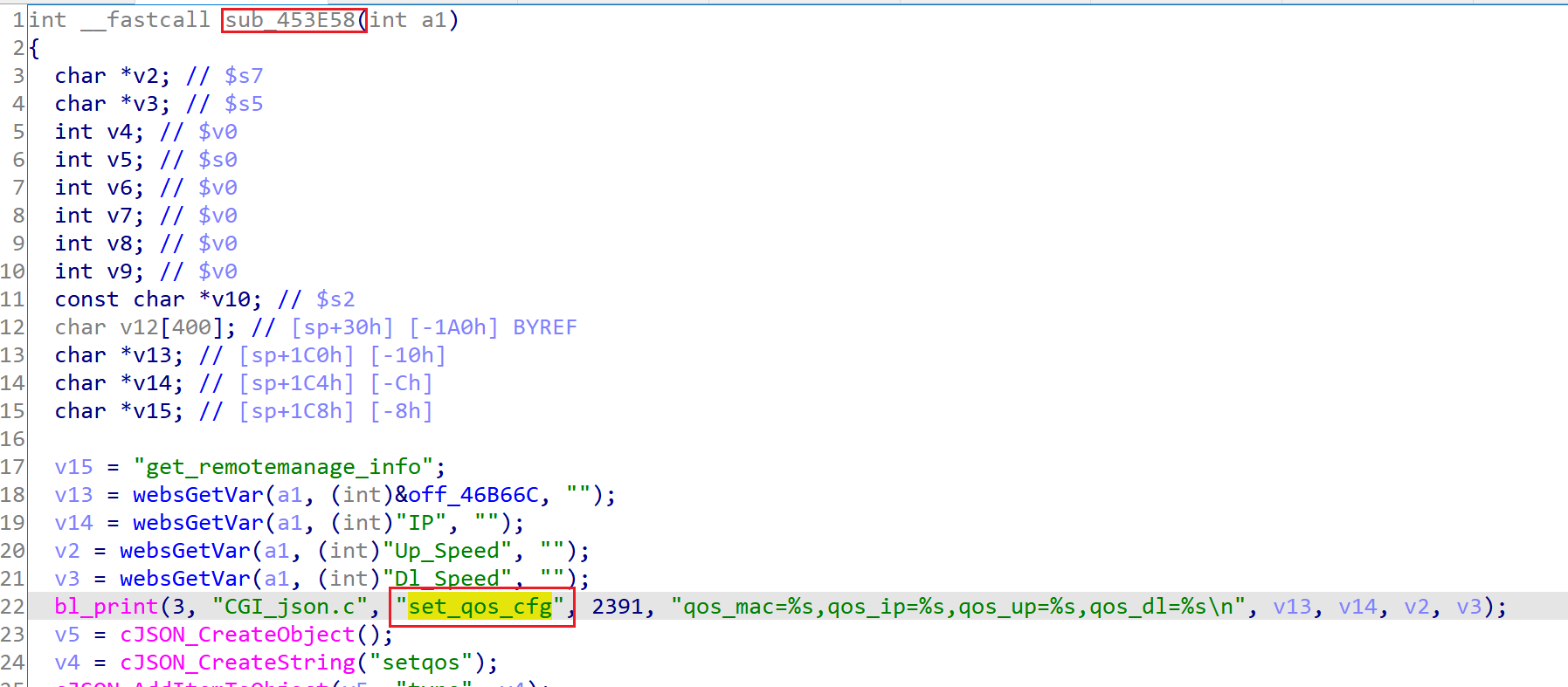


除了getinfo.js，还在goahead中找到有

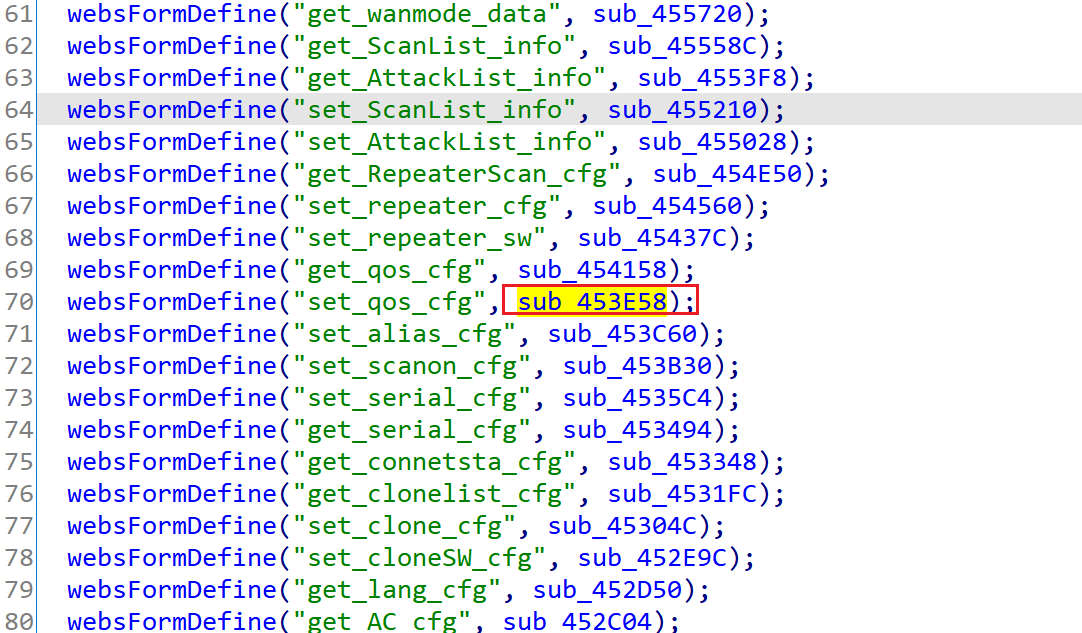


goahead是一个嵌入式web服务器：https://www.embedthis.com/goahead/

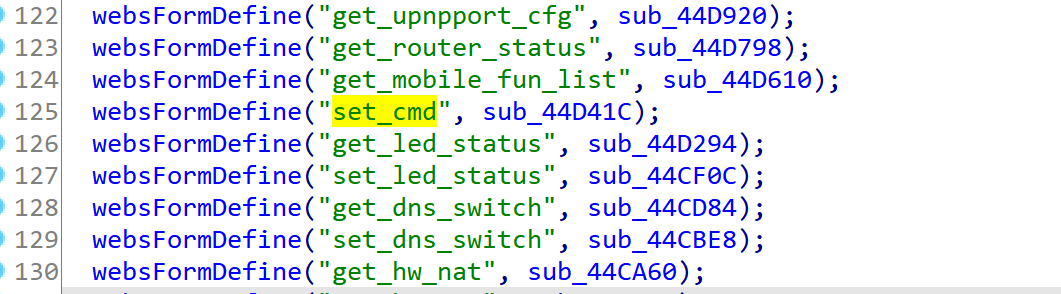
IDA分析goahead，查找字符串’set\_qos\_cfg’，找到如下引用



继续查看对该函数的引用



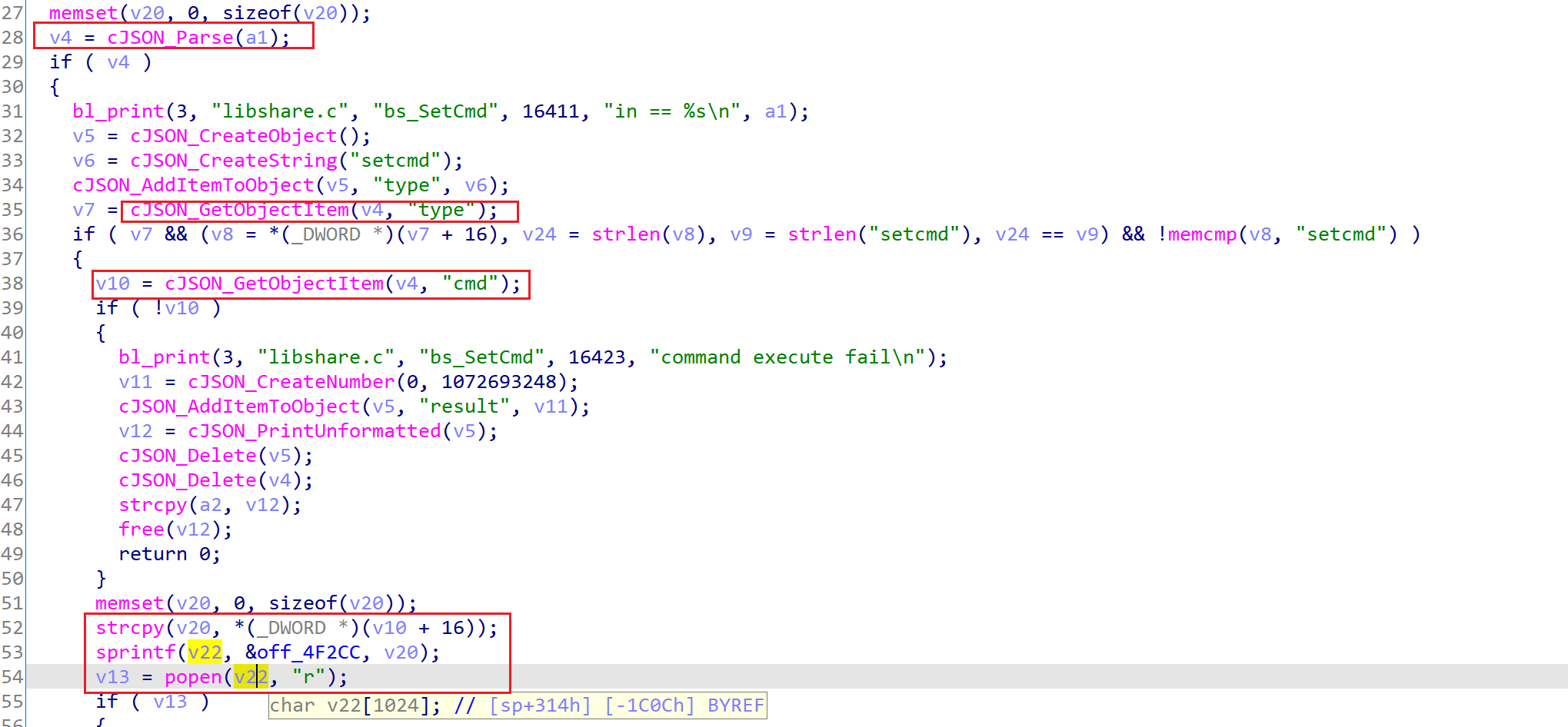
这里的接口比getinfo.js中的要多，发现一个cmd，很可疑：



跟进sub\_44d41c



经过查找，bs\_SetCmd函数的定义在libshare-0.0.26.so中。该函数将cmd键对应的值直接执行，



尝试访问

