BUUCTF-web-[ACTF2020 新生赛]Upload 1

原创

chujhss 于 2021-06-22 11:20:21 发布 119 收藏 2

分类专栏： 练习

本文链接：https://blog.csdn.net/qq_47271638/article/details/118102746

练习 专栏收录该内容

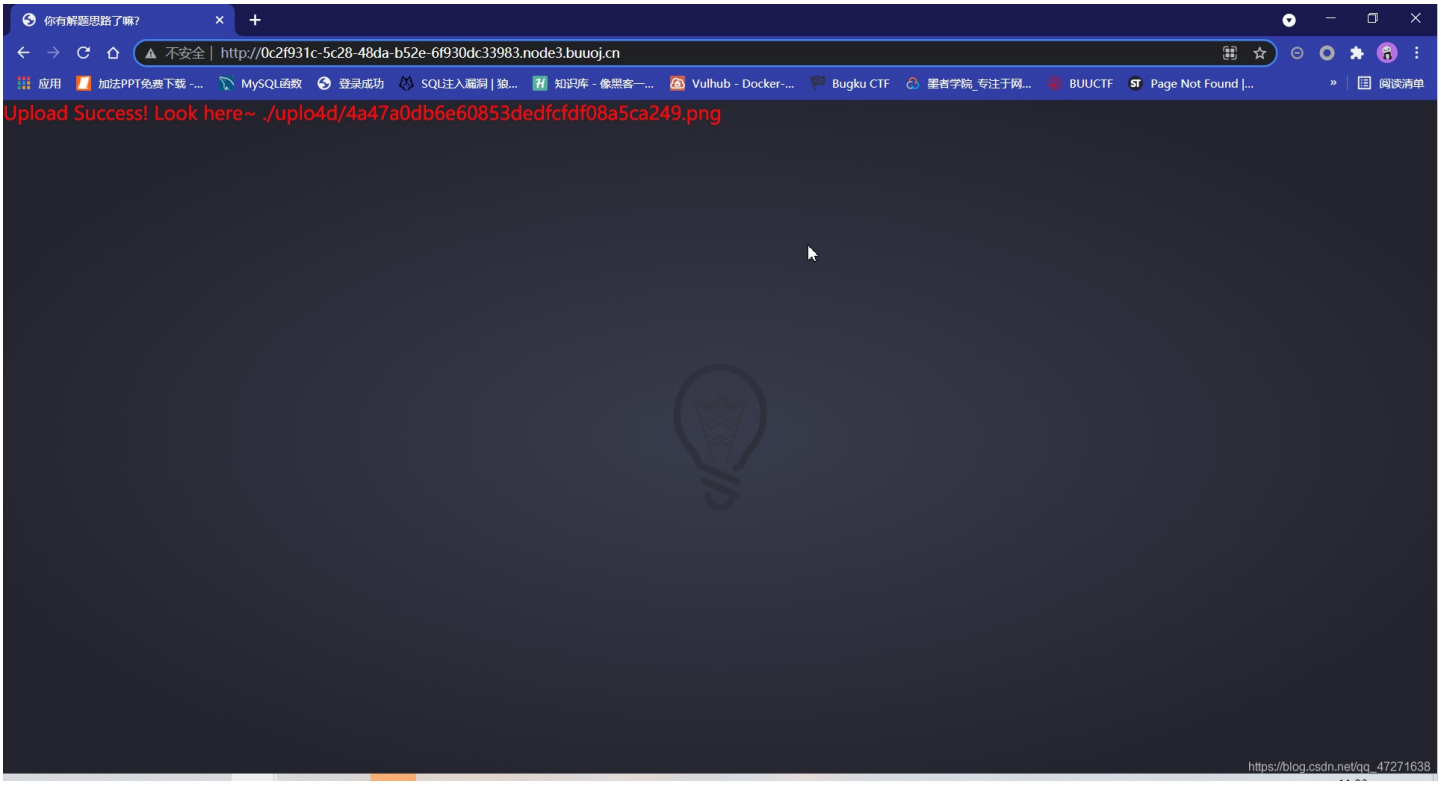
6 篇文章 0 订阅

订阅专栏

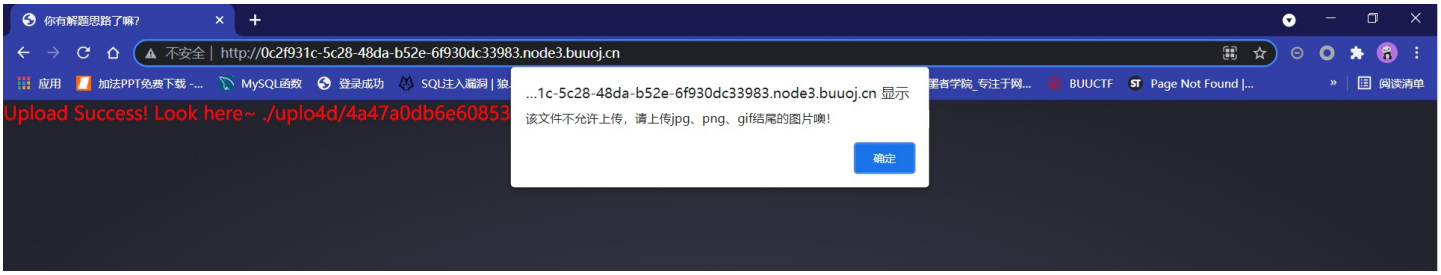
打开靶场

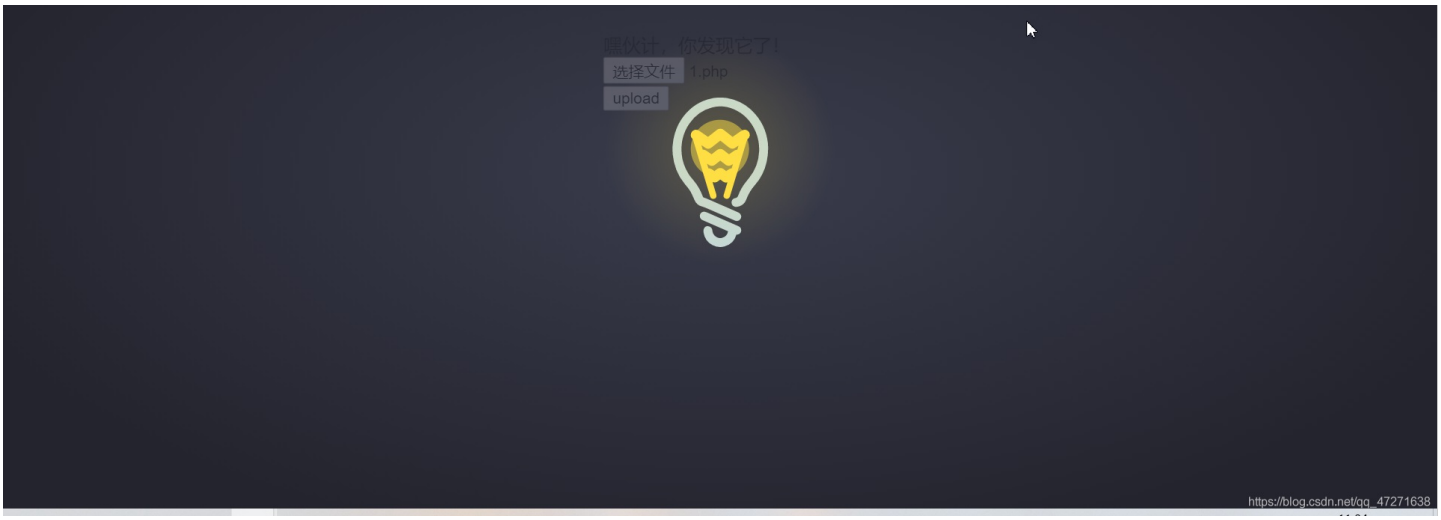
发现网页设计很好看突然就觉得今天挺不错的这可能就是有感而生吧

尝试着上传png文件和php文件

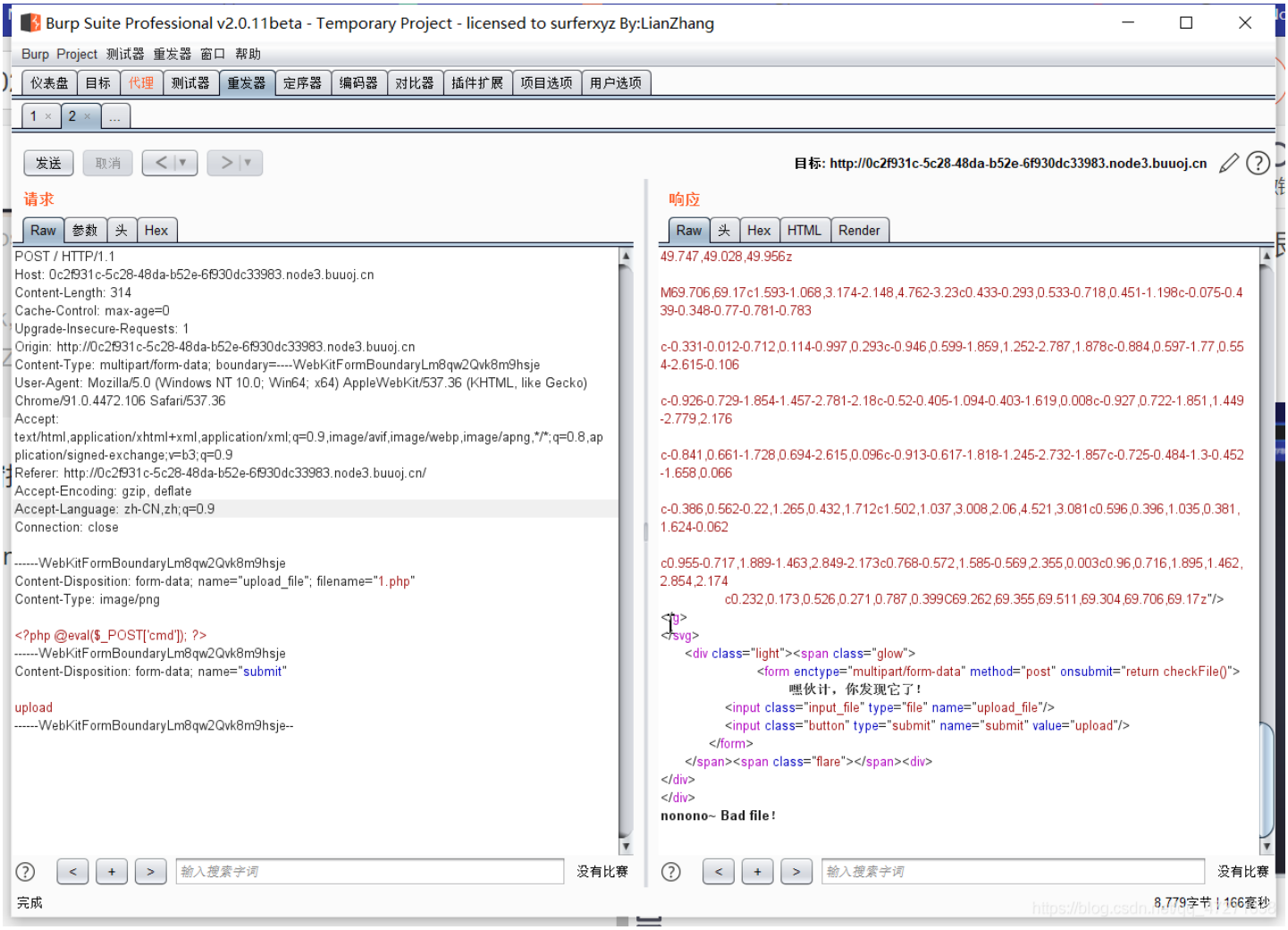


发现png文件上传成功；开始上传php文件

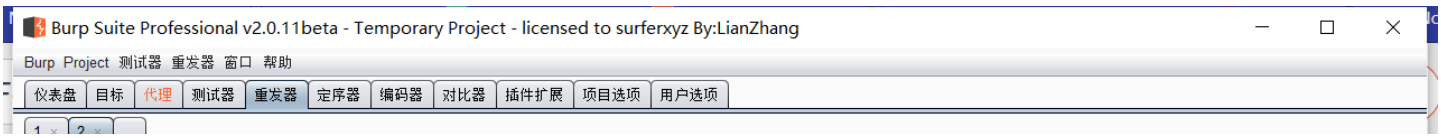


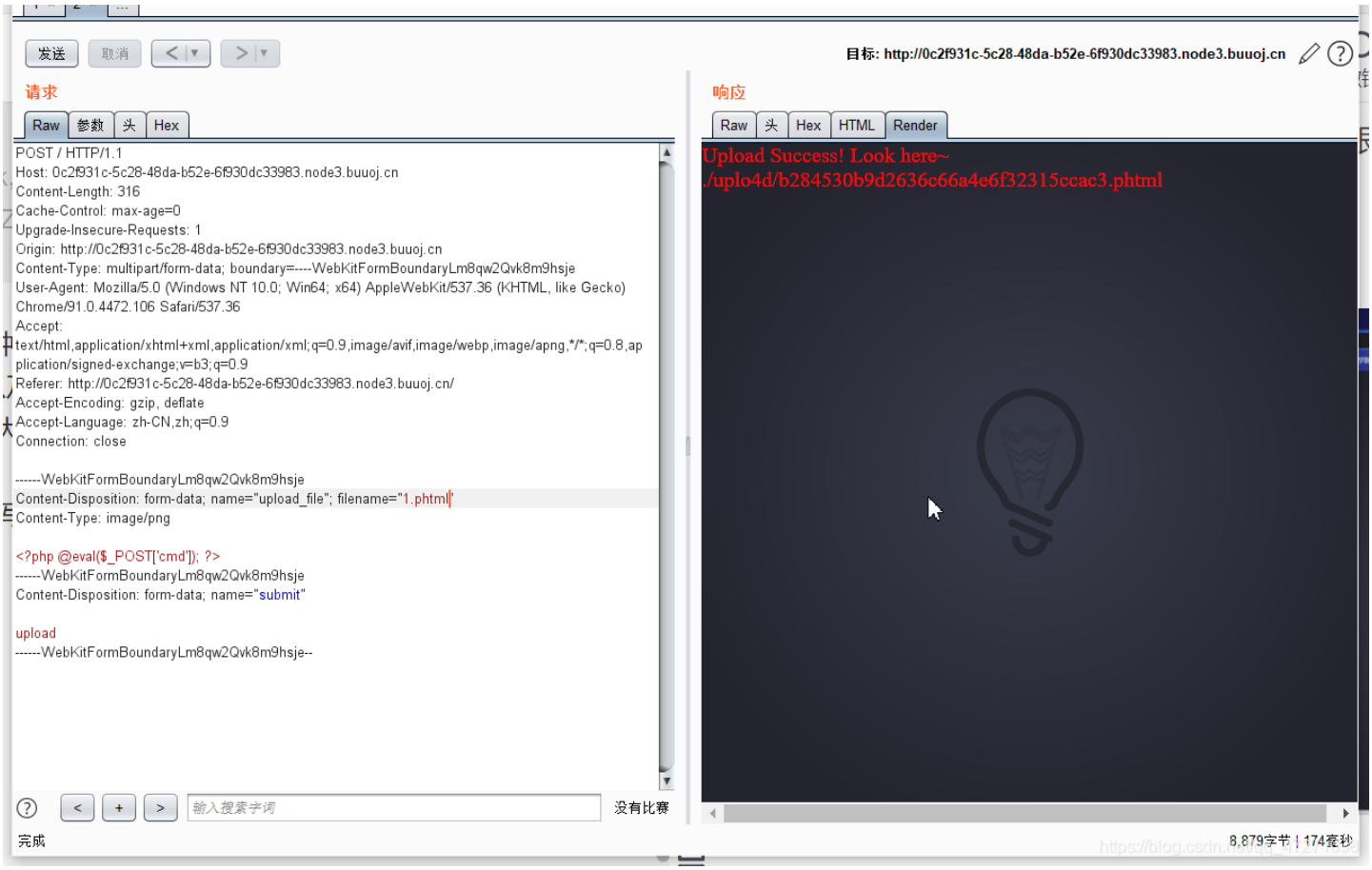


php文件被拦截而且是弹窗拦截初步估计是被前端代码给拦截了前端代码设计了白名单吧
接着用burp抓包然后修改png文件为php文件绕过前端的白名单

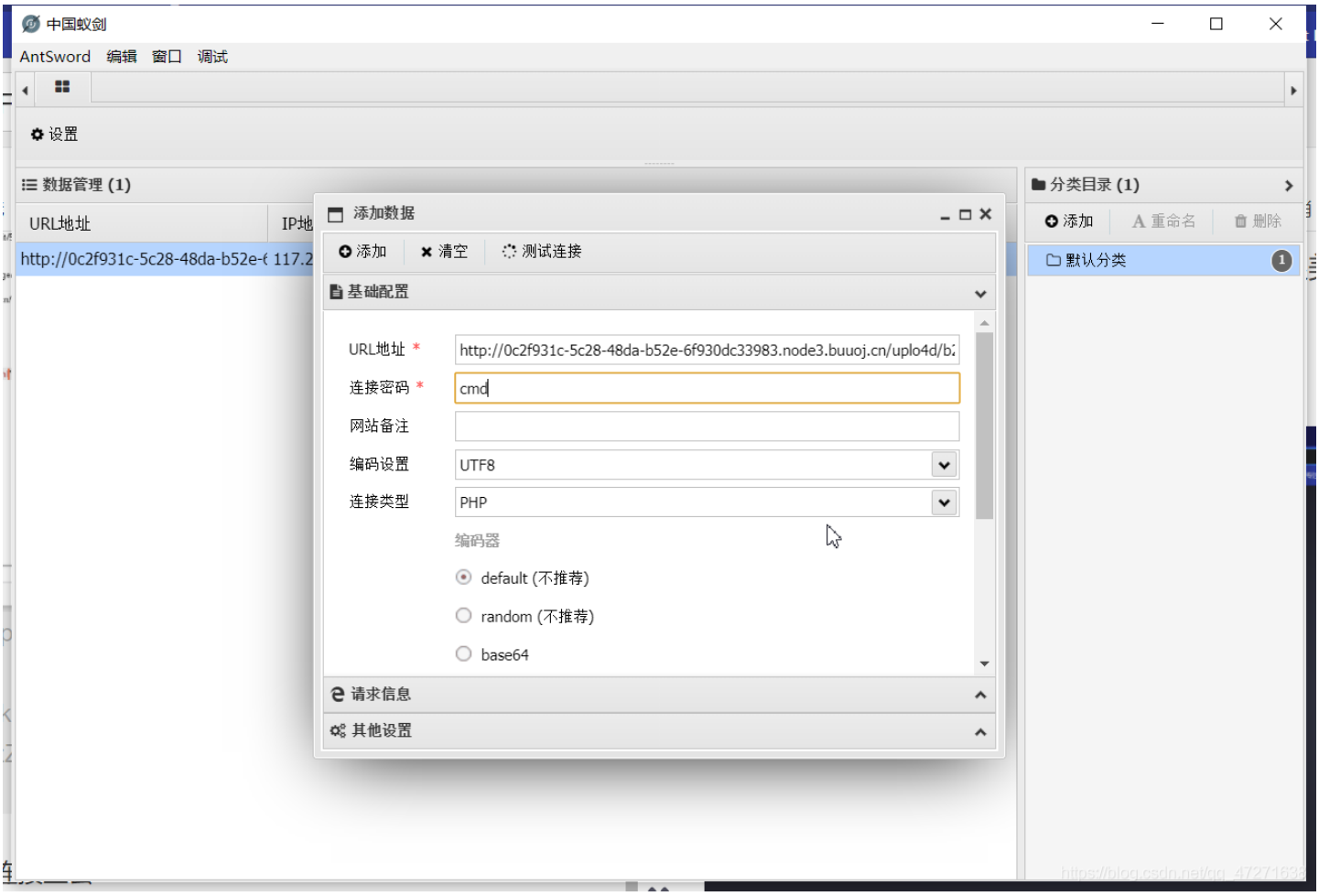


同样被检测到了尝试是哪种检测
上传php3，php4，php5以及phtml文件后缀或者在php文件后面加上“ ”空格符绕过检查 或者“.”加点绕过和大小写绕过或者上.htaccess文件将png格式当做php形式执行
发现phtml和加“.”以及大小写都能绕过但是大写不行无法被解析为PHP文件

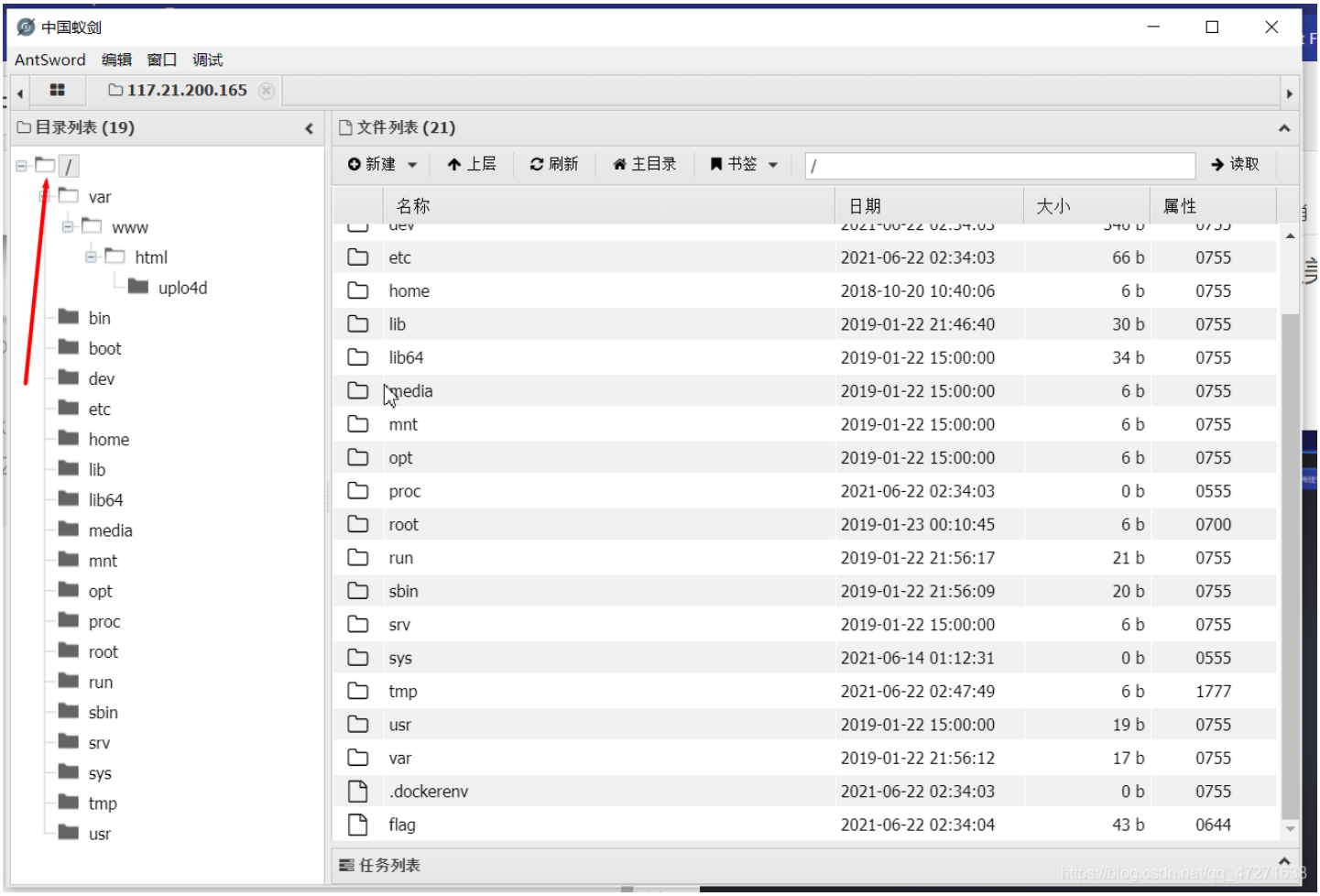




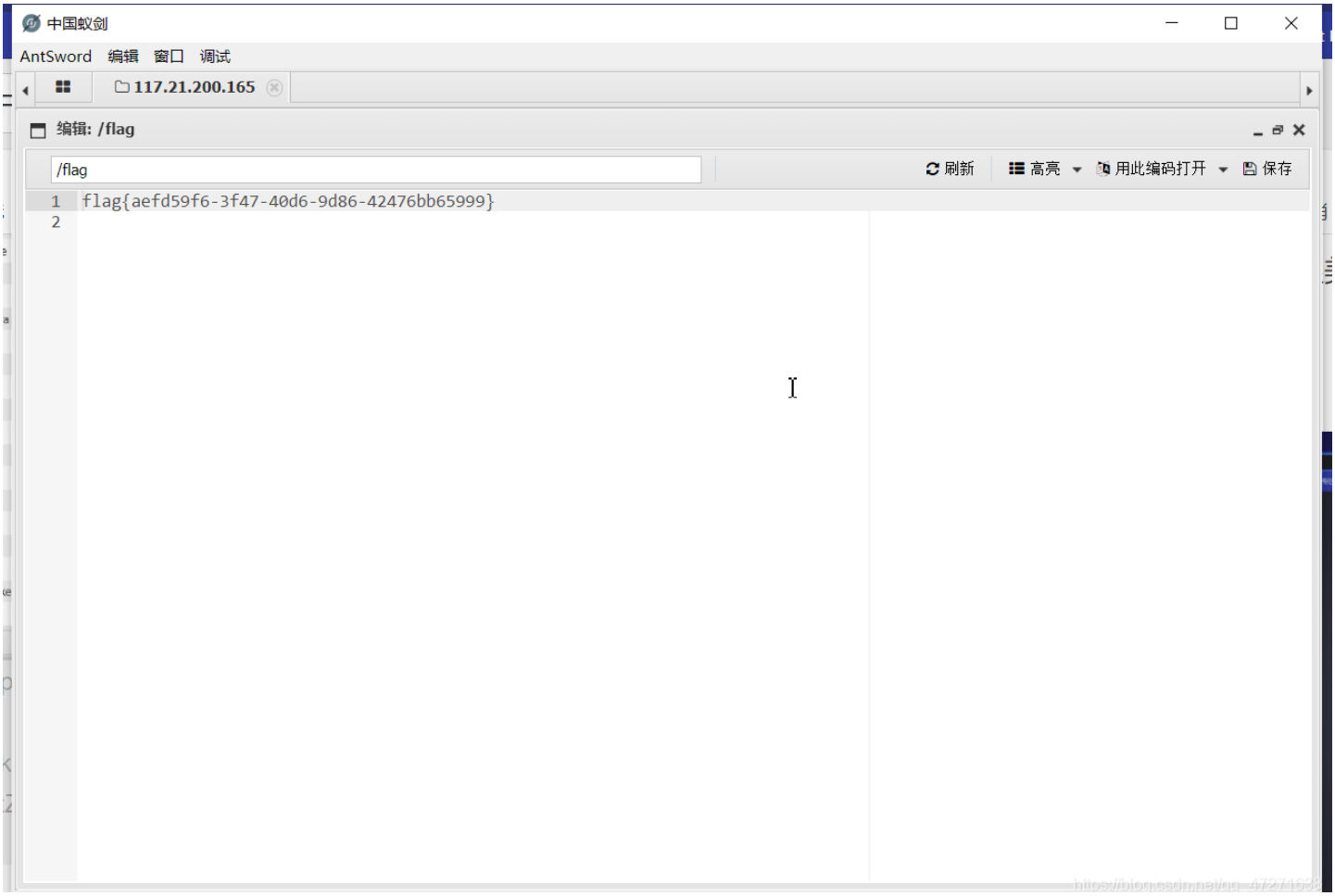
再找到文件的位置用蚁剑连接上去



发现flag在根目录里面


中国蚁剑
AntSword 编辑 窗口 调试
117.21.200.165
目录列表 (19)
/
var
www
html
uplo4d
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
文件列表 (21)
新建
上层
刷新
主目录
书签
/
读取
名称
日期
大小
属性
etc 2021-06-22 02:34:03 66 b 0755
home 2018-10-20 10:40:06 6 b 0755
lib 2019-01-22 21:46:40 30 b 0755
lib64 2019-01-22 15:00:00 34 b 0755
media 2019-01-22 15:00:00 6 b 0755
mnt 2019-01-22 15:00:00 6 b 0755
opt 2019-01-22 15:00:00 6 b 0755
proc 2021-06-22 02:34:03 0 b 0555
root 2019-01-23 00:10:45 6 b 0700
run 2019-01-22 21:56:17 21 b 0755
sbin 2019-01-22 21:56:09 20 b 0755
srv 2019-01-22 15:00:00 6 b 0755
sys 2021-06-14 01:12:31 0 b 0555
tmp 2021-06-22 02:47:49 6 b 1777
usr 2019-01-22 15:00:00 19 b 0755
var 2019-01-22 21:56:12 17 b 0755
.dockerenv 2021-06-22 02:34:03 0 b 0755
flag 2021-06-22 02:34:04 43 b 0644
任务列表

打开提交就行


中国蚁剑
AntSword 编辑 窗口 调试
117.21.200.165
编辑: /flag
/flag
刷新
高亮
用此编码打开
保存
1 flag{aefd59f6-3f47-40d6-9d86-42476bb65999}
2