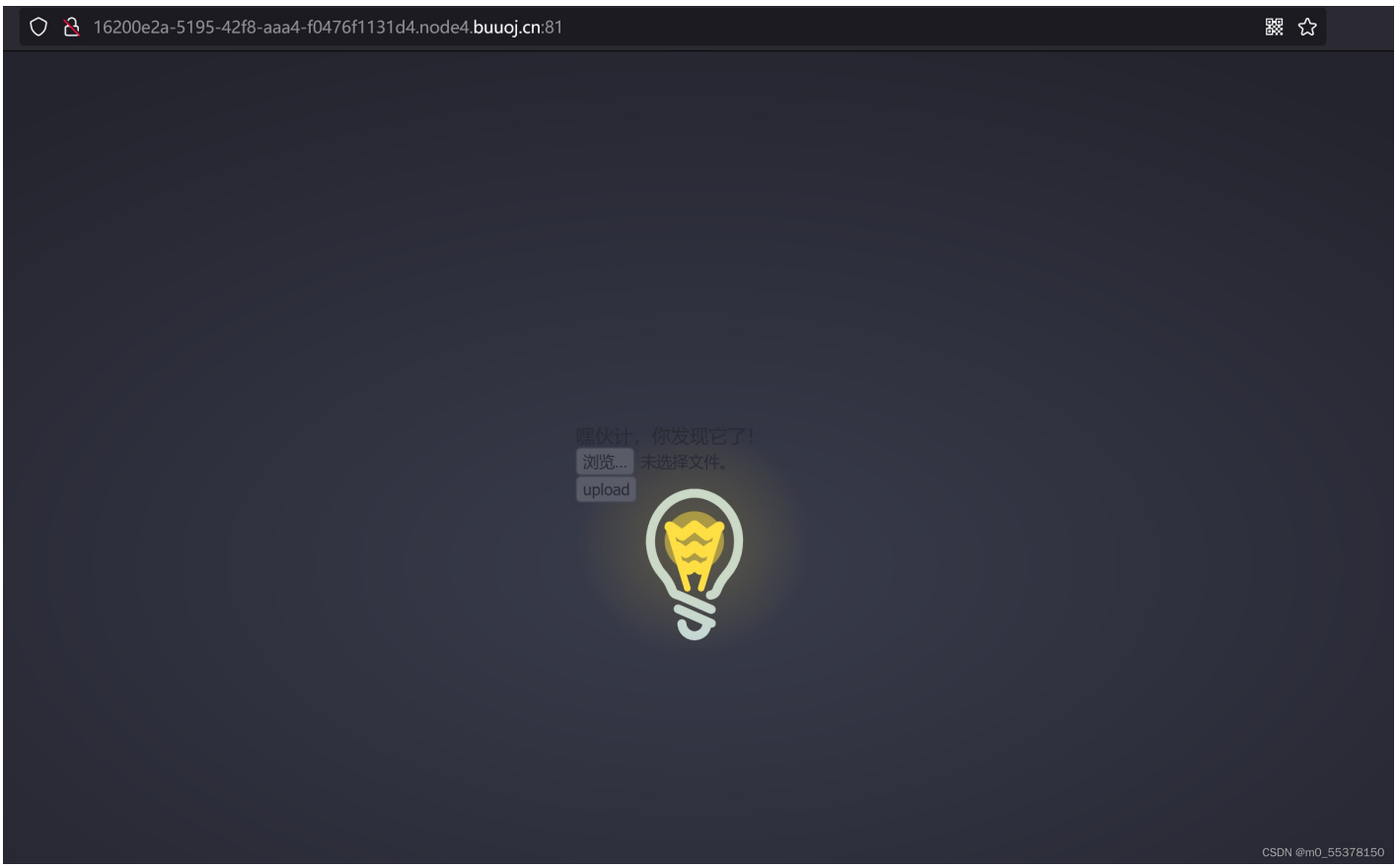
buu web：[ACTF2020 新生赛]Upload

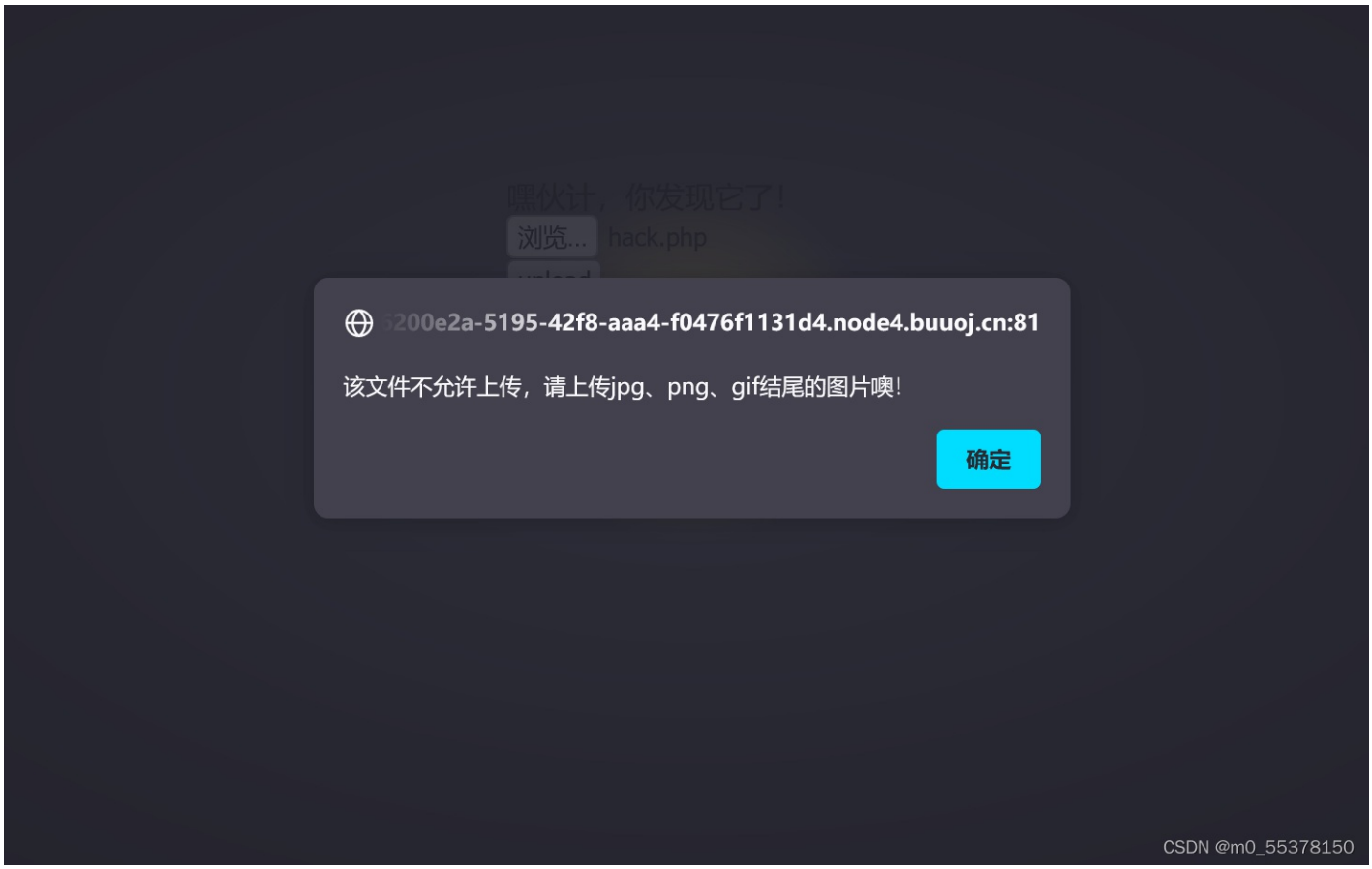
原创

m0_55378150 于 2022-04-10 18:41:30 发布 601 收藏
分类专栏： buuctf 文章标签： web安全

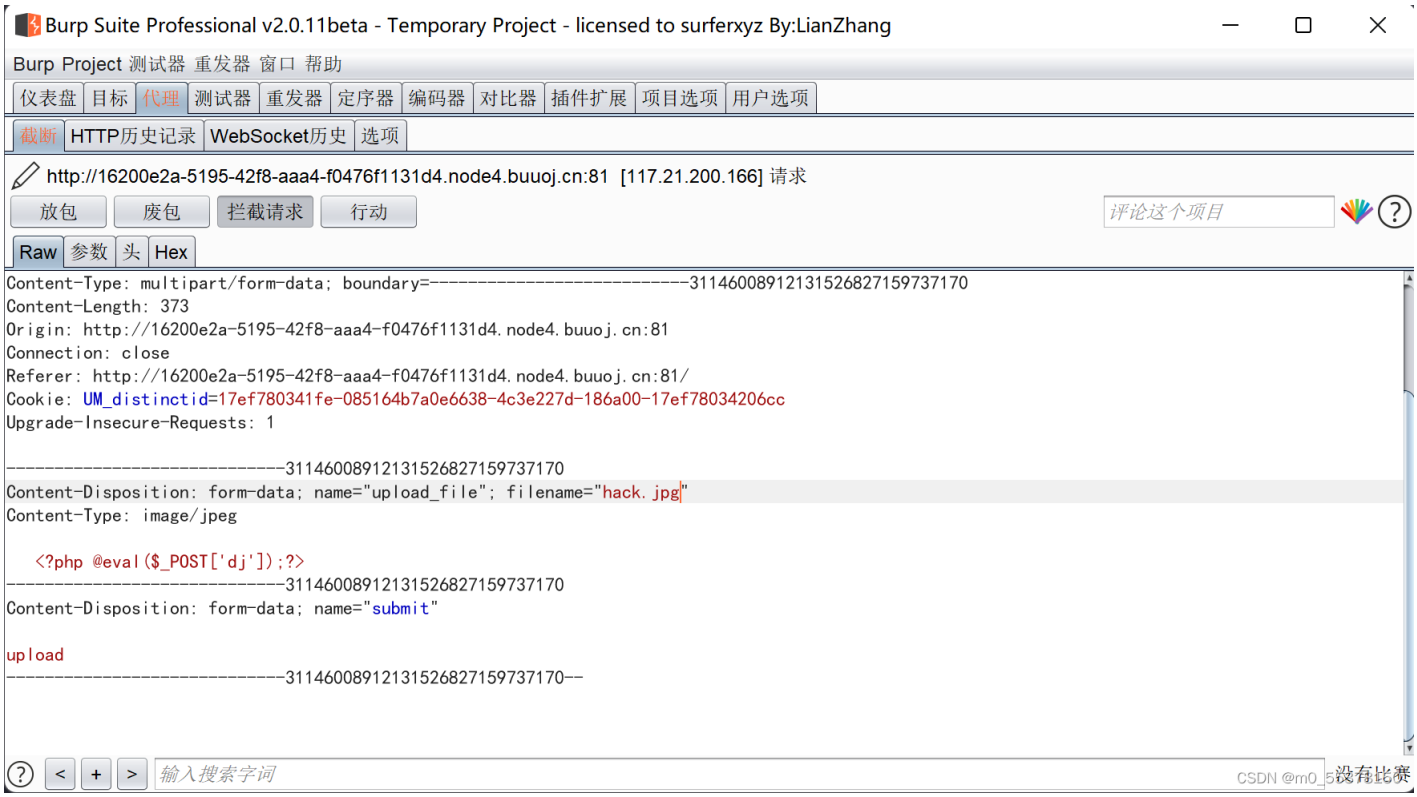
打开靶机，发现是一个文件上传窗口



老规矩，先上传一句话木马



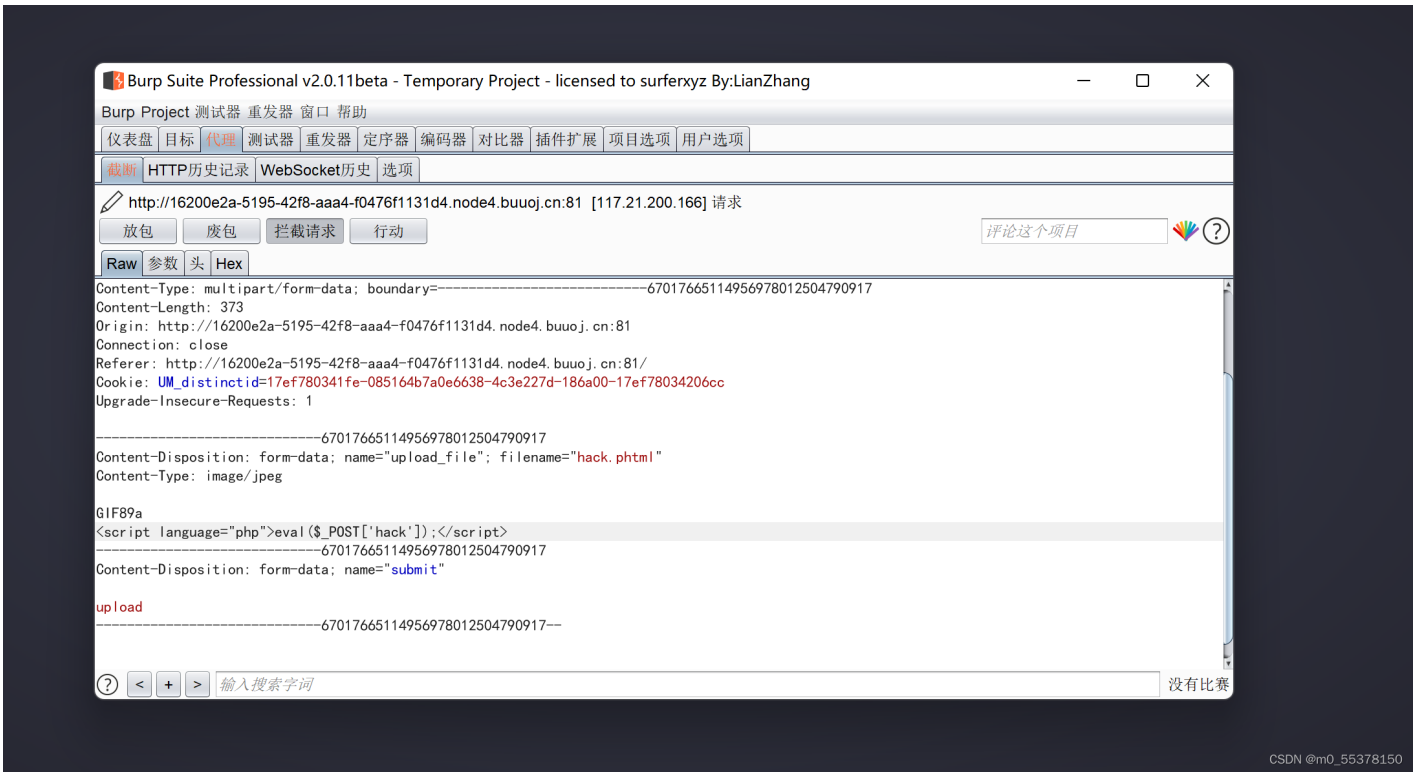
发现有白名单，所以我们试一下先将.php后缀改成.jpg，再用burp抓包给他改回来（就是看一下它是不是前端验证）



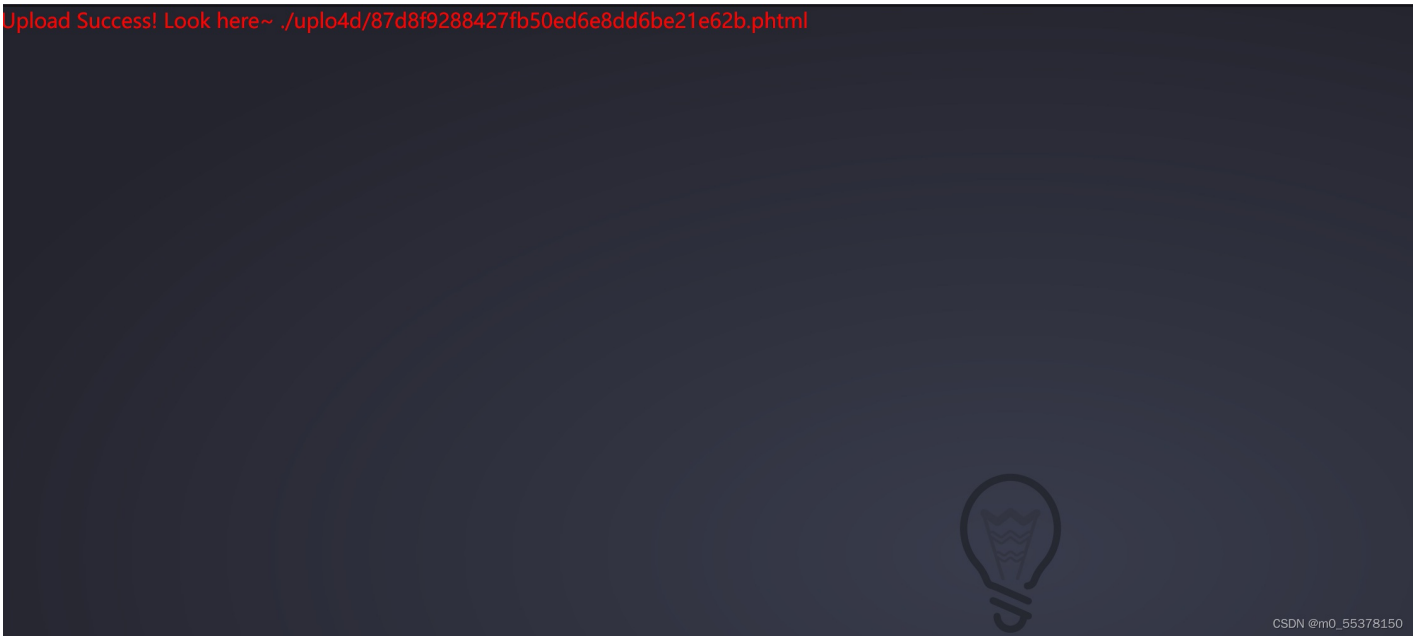
```
fe-085164b7a0e6638-4c3e227d-186a00-17ef78034206cc

460089121315268271597371 70
name="upload_file"; filename="hack.php"

460089121315268271597371 70
```


发送

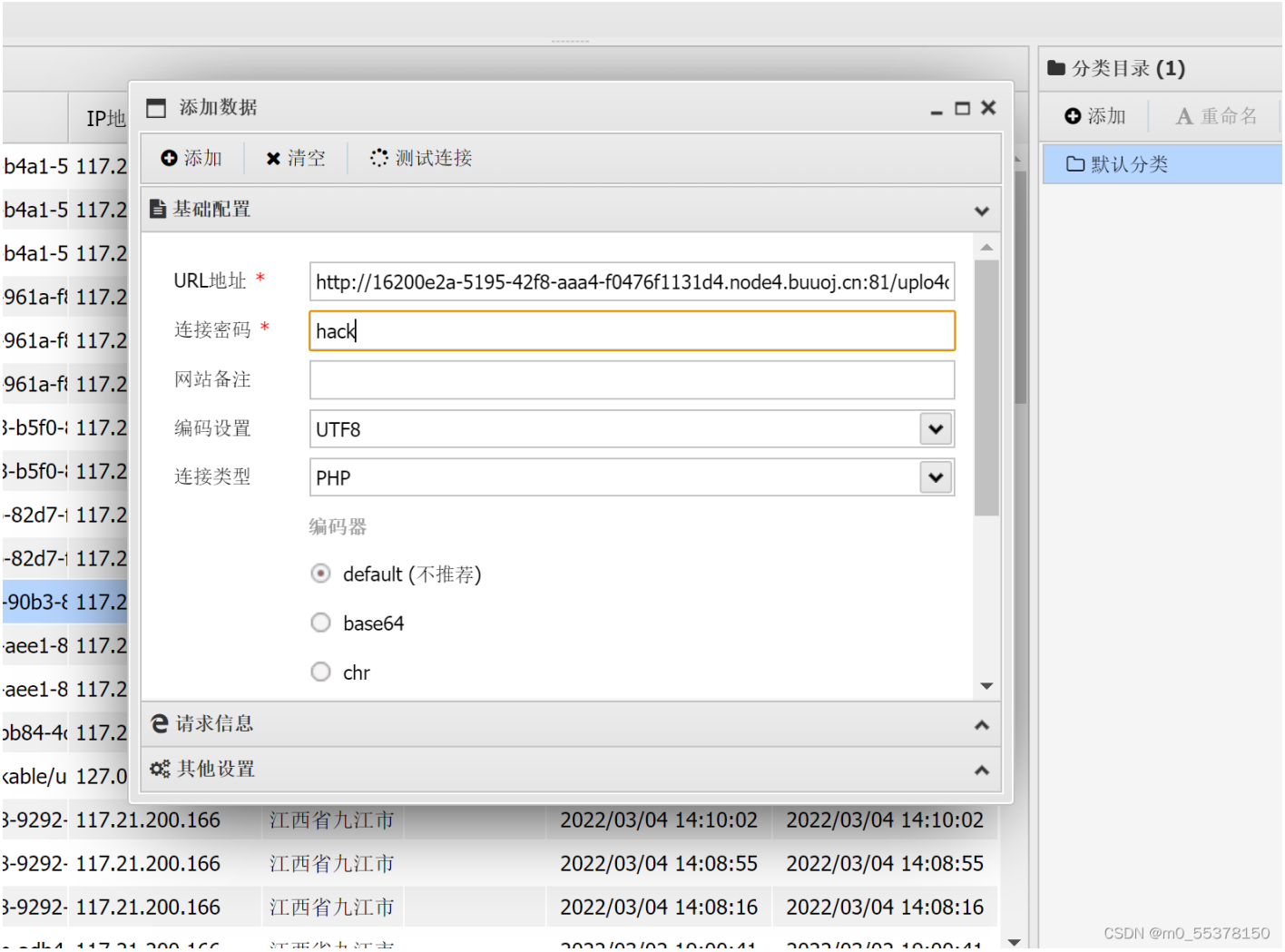
左上角有报错，看来没这么简单，试一下上一道题的phtml后缀方法

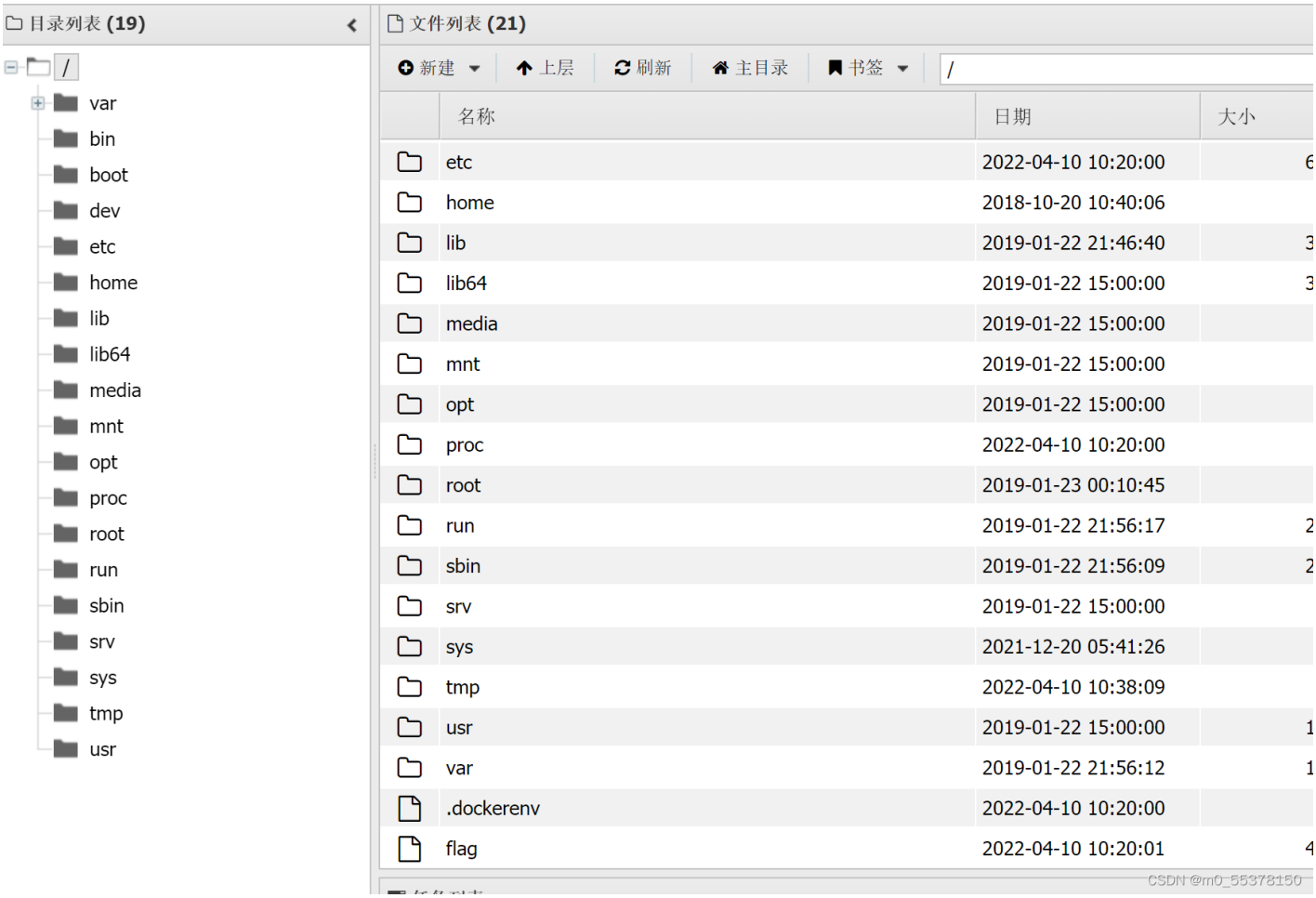


放包



成功上传，并且给出了路径，直接上蚁剑


添加数据
添加
清空
测试连接
基础配置
URL地址 *
http://16200e2a-5195-42f8-aaa4-f0476f1131d4.node4.buuoj.cn:81/uplo4
连接密码 *
hack
网站备注
编码设置
UTF8
连接类型
PHP
编码器
default (不推荐)
base64
chr
请求信息
其他设置
分类目录 (1)
添加
重命名
默认分类
117.21.200.166
江西省九江市
2022/03/04 14:10:02
2022/03/04 14:10:02
117.21.200.166
江西省九江市
2022/03/04 14:08:55
2022/03/04 14:08:55
117.21.200.166
江西省九江市
2022/03/04 14:08:16
2022/03/04 14:08:16
CSDN @m0_55378150


目录列表 (19)
/
var
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
/
名称
日期
大小
etc 2022-04-10 10:20:00
home 2018-10-20 10:40:06
lib 2019-01-22 21:46:40
lib64 2019-01-22 15:00:00
media 2019-01-22 15:00:00
mnt 2019-01-22 15:00:00
opt 2019-01-22 15:00:00
proc 2022-04-10 10:20:00
root 2019-01-23 00:10:45
run 2019-01-22 21:56:17
sbin 2019-01-22 21:56:09
srv 2019-01-22 15:00:00
sys 2021-12-20 05:41:26
tmp 2022-04-10 10:38:09
usr 2019-01-22 15:00:00
var 2019-01-22 21:56:12
.dockerenv 2022-04-10 10:20:00
flag 2022-04-10 10:20:01
CSDN @m0_55378150


117.21.200.166
编辑: /flag
/flag
1 flag{f87d1058-c01c-43df-9f94-b058145e4dd5}
2
CSDN @m0_55378150

成功！