BUU部分题的wp1

原创

Z3eyOnd 于 2021-08-07 09:55:05 发布 49 收藏

分类专栏： CTF训练日记 BUU

本文链接：https://blog.csdn.net/unexpectedthing/article/details/117392143


CTF训练日记 同时被 2 个专栏收录

63 篇文章 3 订阅

订阅专栏


BUU

6 篇文章 0 订阅

订阅专栏

ww@TOC

HCTF2018:Warm Up

运用知识点：代码审计

1.F12,看到source.php

2. 网址加入source.php,得到一段代码

3. 进行代码审计，知道需要进行目录穿越

4. 几个函数：

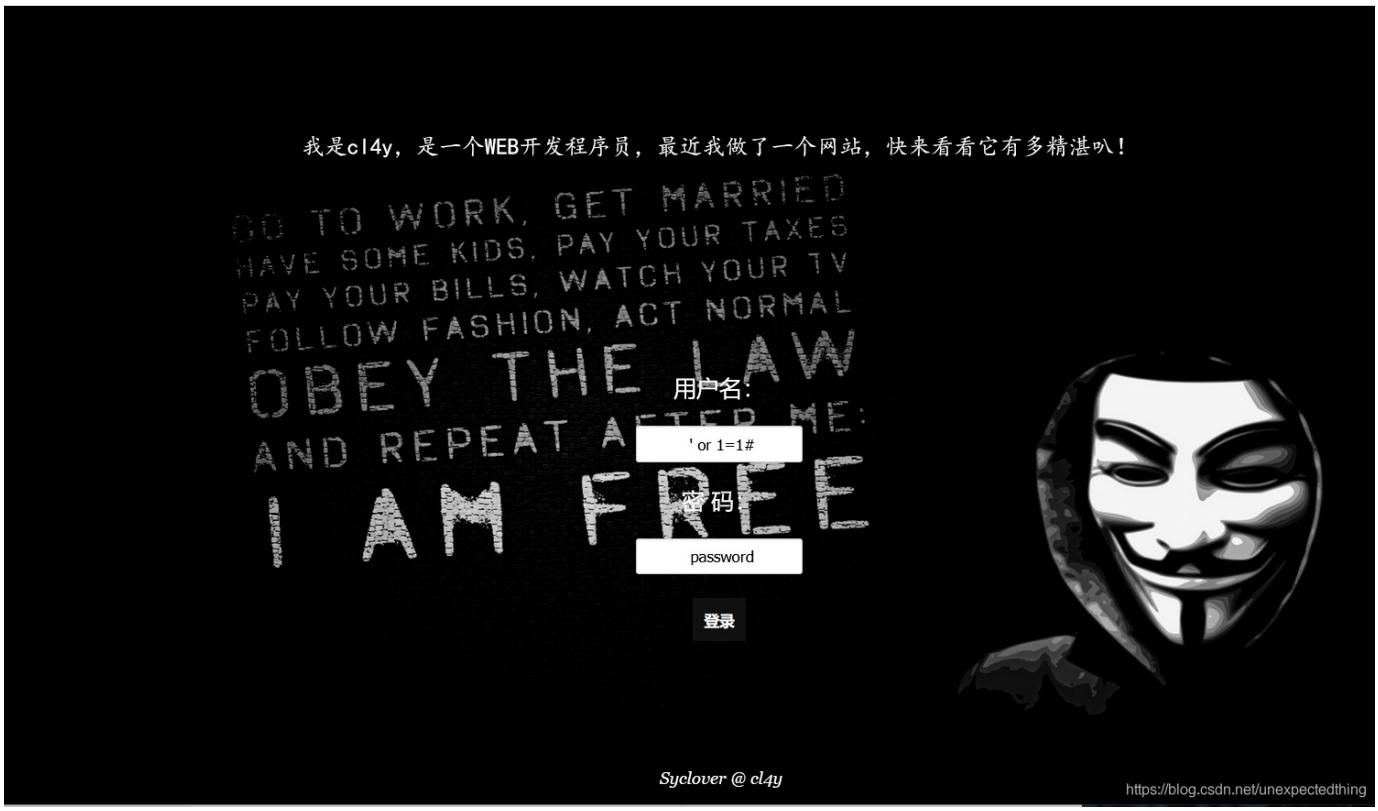
mb_substr(str1,start,[length][,[str2]]):是在str1从start开始length为长度截取字符串，str2是表示字符编码

mb_strpos(str1,str2):查找str2在str1中出现的位置

6. 所以payload为file=hint.php?/…/…/…/…/…/…/…/…/…/fffflllaaaagggg

极客大挑战EasySQL

1. 一上来，sql注入题，先使用万能密码

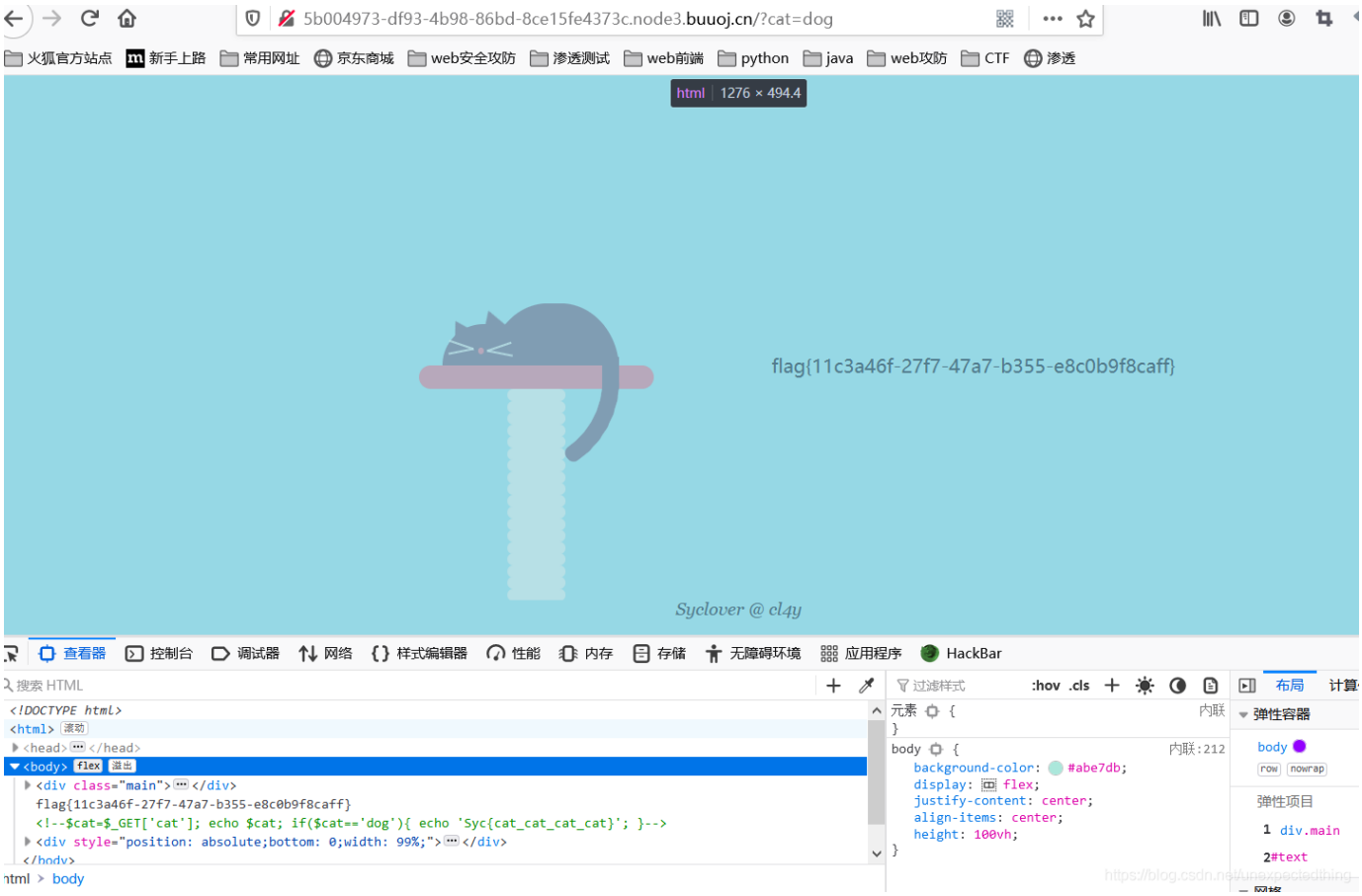


2. 得到flag

极客大挑战Havefun

1. 上来没什么反应,按F12

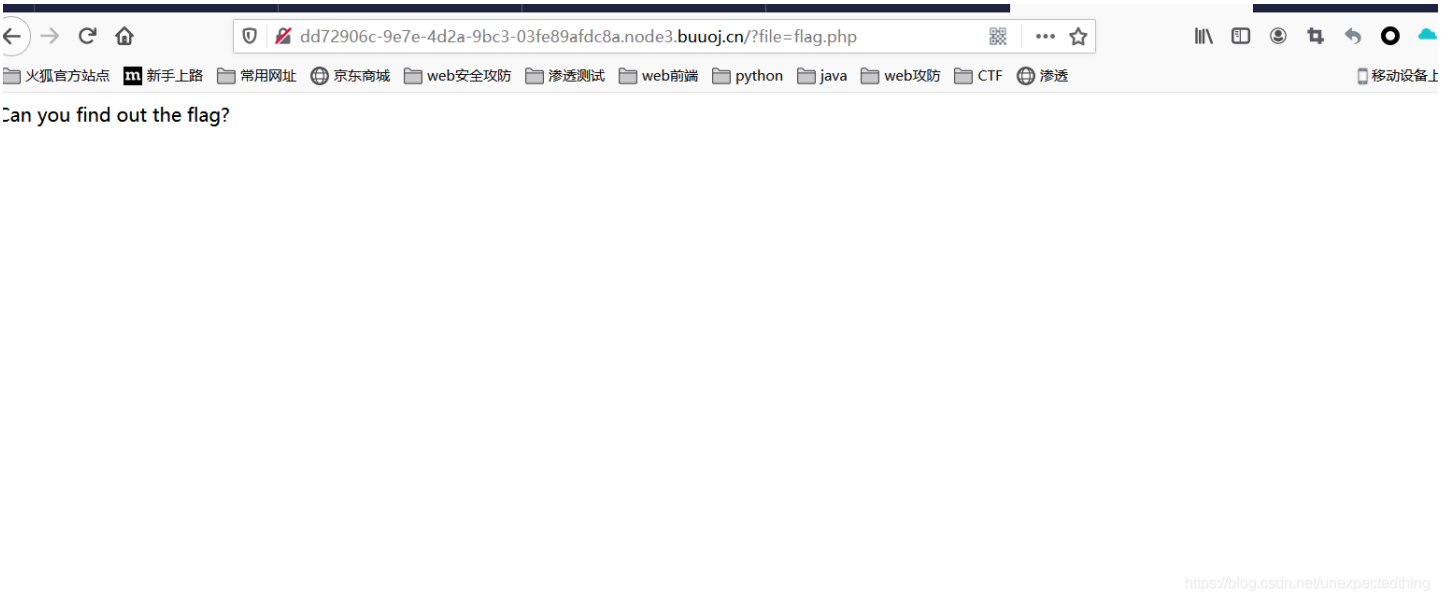
2. 查看代码，给URL赋一个变量cat=dog,得到flag



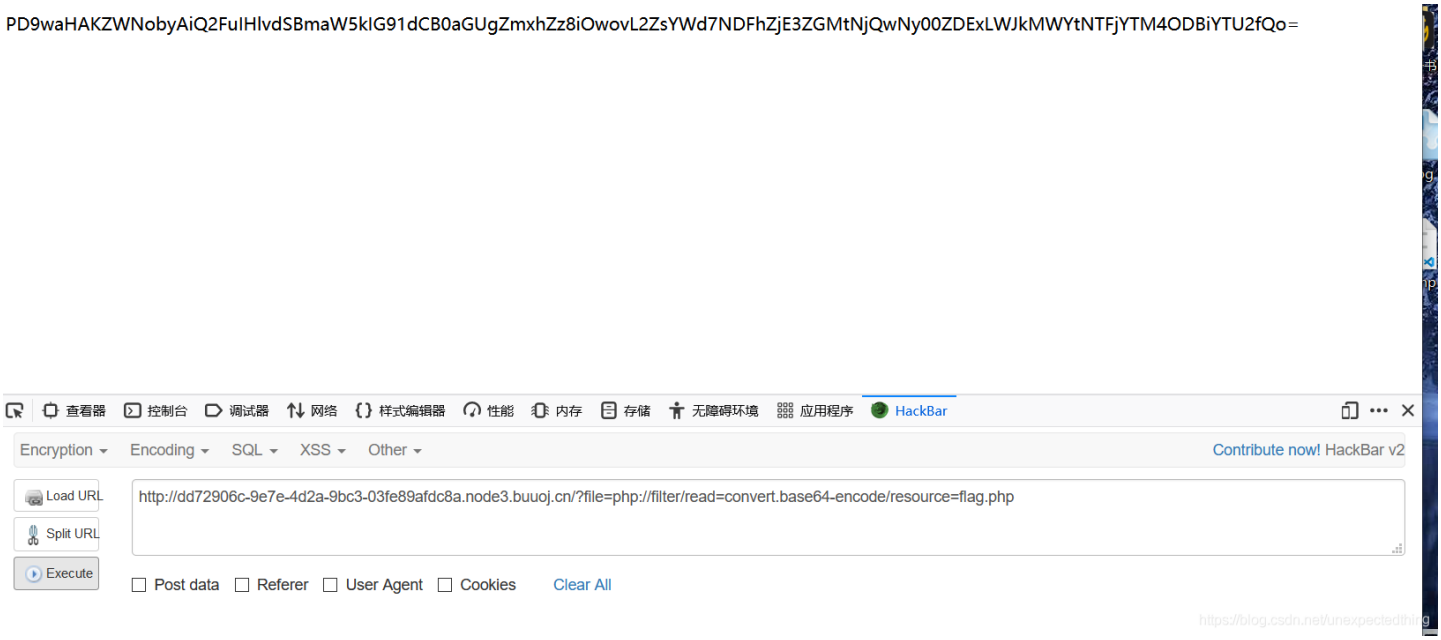
3.

ACTF新生赛， include

1.include，文件包含， 点击tips，看url



2.使用php伪协议：file=php：//filter/read=convert.base64-encode/resource=flag.php



3. 再用base64工具去解码

极客大挑战secret file

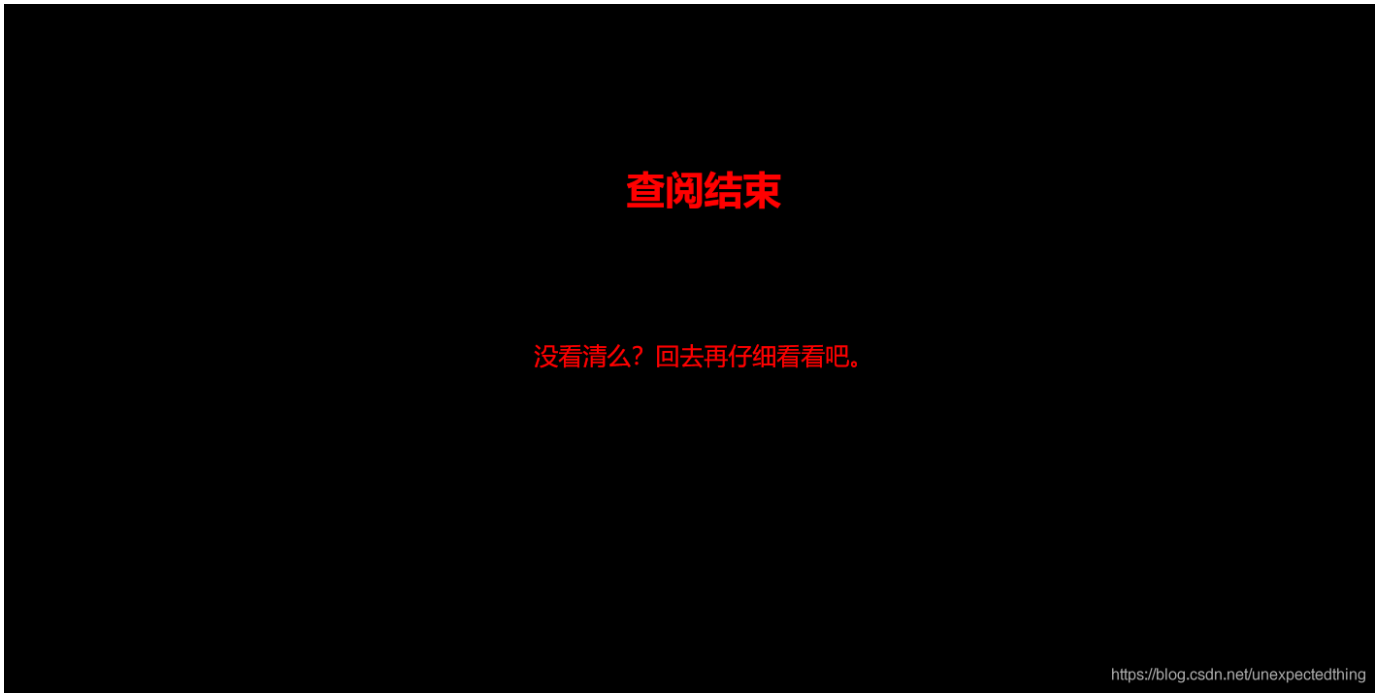
1. F12看到一个php的地址

```
    </div>
  </body>
</html>
```

html > body > p

2. 进入页面，看到select可以点击

3. 点击后，但是看到的是，查阅结束，我就想到抓包，burp得到一个拍黄片地址



```
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer:
http://c4ac0722-9df4-4c25-9128-dadc3f40a780.node3.buuoj.cn/Archive_room.php
Cookie: UM_distinctid=
179189dbc484eb-0633fca2fa3cef-4c3f2c72-144000-179189dbc493a9; session=
1348105f-5d37-4f73-bbd3-8a222df59e42.NSkXDXpuZZwv1CebHEawTHiU8S0
Upgrade-Insecure-Requests: 1
```

```
Location: end.php
X-Powered-By: PHP/7.3.11
Content-Length: 63

<!DOCTYPE html>

<html>
  <!--
  secr3t.php
  -->
</html>
```

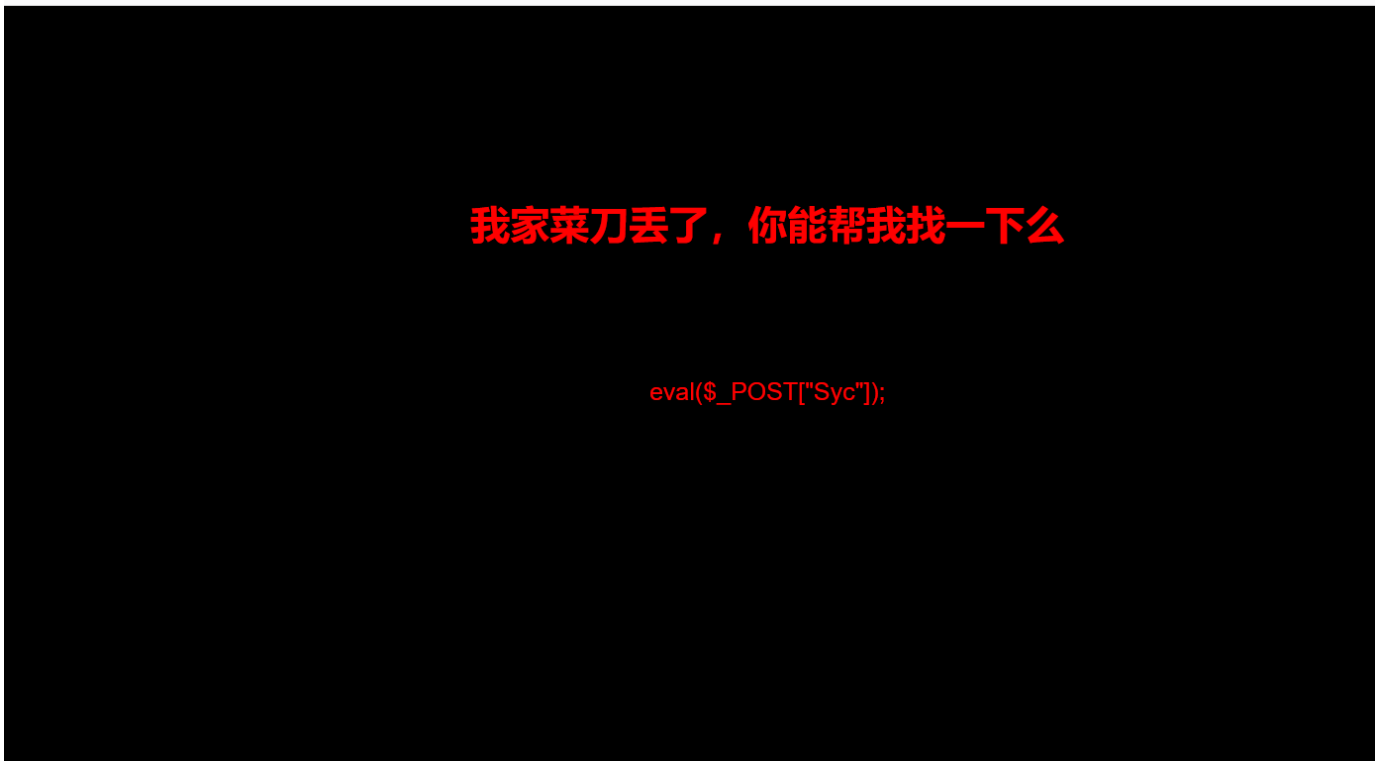

4. 打开后是代码审计

```
<html>
        <title>secret</title>
        <meta  charset="UTF-8">
<?php
        highlight_file(__FILE__);
        error_reporting(0);
        $file=$_GET['file'];
        if(strstr($file,"../")||stristr($file,  "tp")||stristr($file,"input")||stristr($file,"data")){
                echo  "Oh  no!";
                exit();
        }
        include($file);
//flag放在了flag.php里
?>
</html>
```

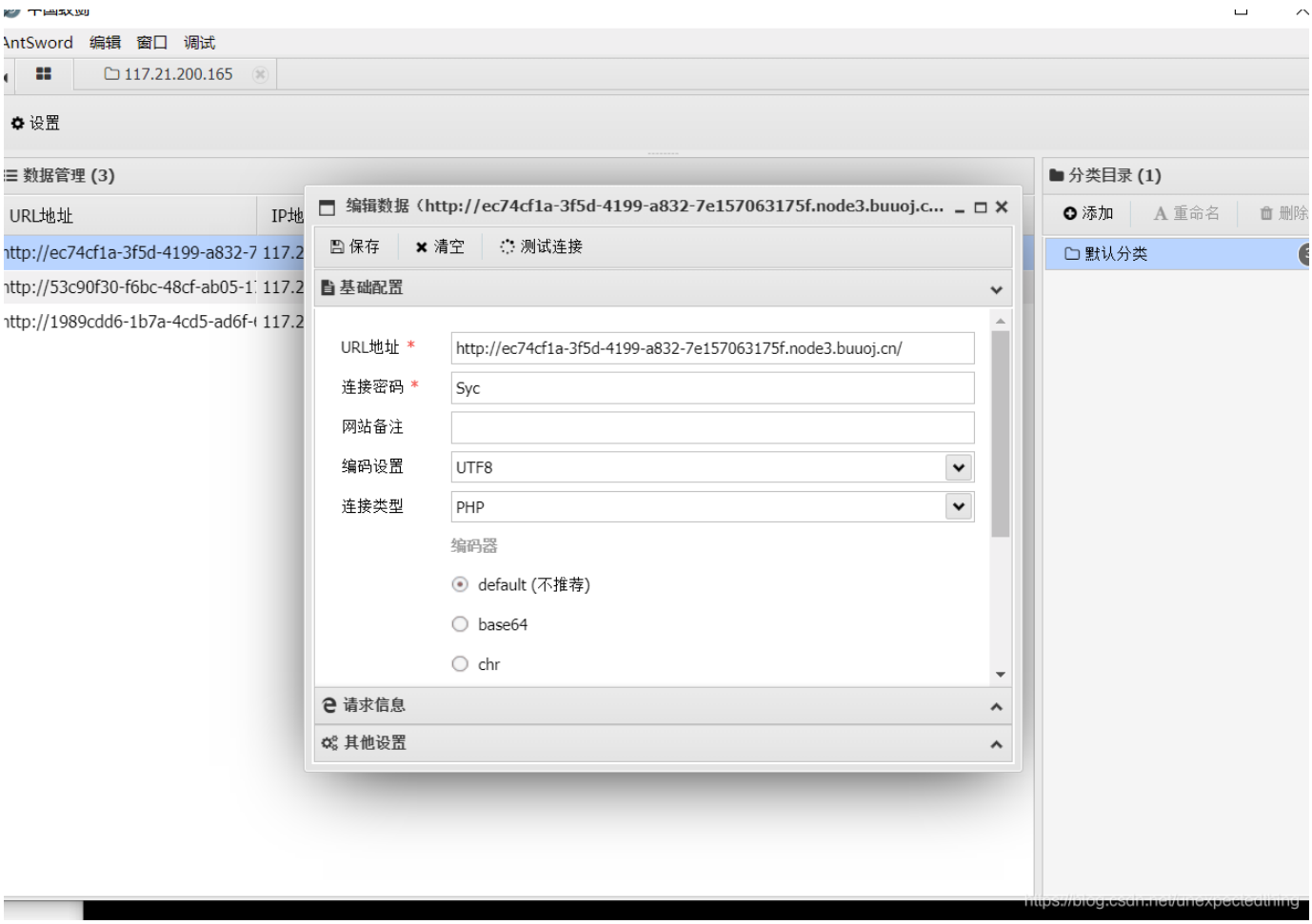

5. 看到flag在flag.php,代码中又对，目录穿越，data，input，tp过滤了，想到文件包含中的filter伪协议，file=php：//filter/read=convert.base64-encode/resource=flag.php

极客大挑战Knife

1. 由knife想到菜刀，蚁剑，还提供了免费的木马



2.用链接和密码，链接蚁剑，查看目录

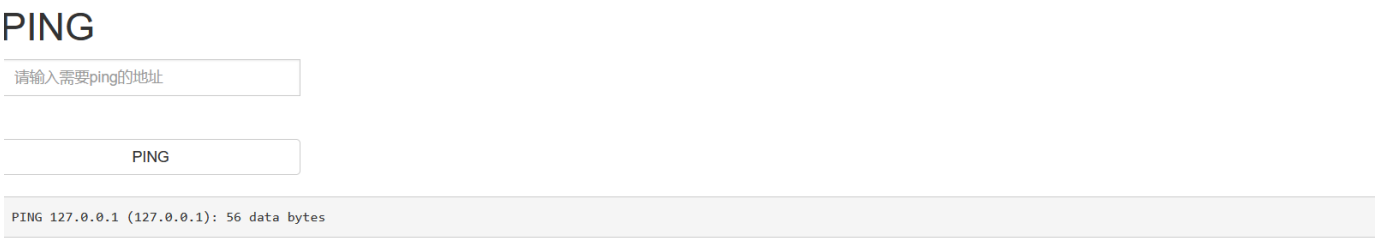


3.查看根目录，得到flag

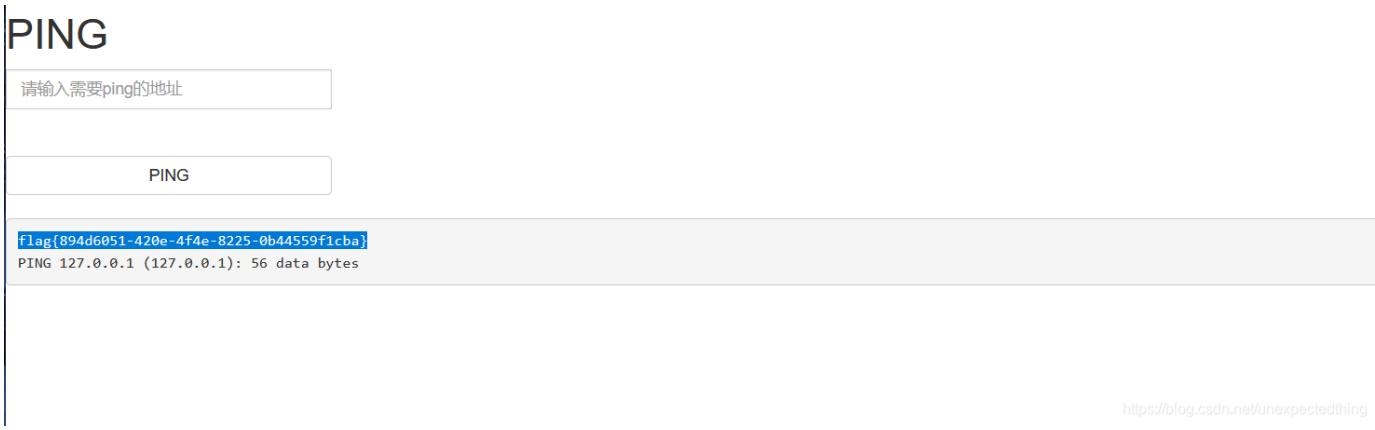
dev	2021-05-29 15:14:40	340 b	0755
etc	2021-05-29 15:14:39	66 b	0755
home	2014-04-10 22:12:14	6 b	0755
lib	2016-07-11 23:23:25	208 b	0755
lib64	2016-07-11 23:23:12	34 b	0755
media	2016-07-11 23:22:49	6 b	0755
mnt	2014-04-10 22:12:14	6 b	0755
opt	2016-07-11 23:22:49	6 b	0755
proc	2021-05-29 15:14:40	0 b	0555
root	2016-07-11 23:23:35	37 b	0700
run	2019-11-19 09:30:15	33 b	0755
sbin	2016-07-22 15:18:57	44 b	0755
srv	2016-07-11 23:22:49	6 b	0755
sys	2021-05-16 16:40:01	0 b	0555
tmp	2021-05-29 15:14:41	6 b	1777
usr	2016-07-22 15:18:57	81 b	0755
var	2019-11-19 09:28:18	28 b	0755
.dockerenv	2021-05-29 15:14:39	0 b	0755

ACTF新生赛Exec

1. 一上来，ping本地IP地址



2. 利用127.0.0.1；cat /flag来得到flag



知识点：1.cat命令是连接文件并输出到界面上。
2.&符号：无论前面命令对不对，都要执行下一个命令
3.|符号：管道符，直接执行后面的内容，但是在linux中，应该是前面的输出，作为后面的输入
4.；符号，依次执行前面的命令和后面的命令
5.||和&&这个简单，||是前面错了才执行后面的，&&是前面对才执行后面的
6.ls是展开目录的意思。

GXYCTFpingpingping

这个直接看这个：https://blog.csdn.net/qq_46184013/article/details/107061110