

# CG-CTF——WP (WEB[一])

原创

窝窝头\_233 于 2019-12-03 19:59:24 发布 501 收藏 3

分类专栏: [CTFwriteup](#) 文章标签: [ctf](#) [CG-CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/hahaha233330/article/details/103374420>

版权



[CTFwriteup](#) 专栏收录该内容

20 篇文章 1 订阅

订阅专栏

## CG-CTF——WEB

工具:

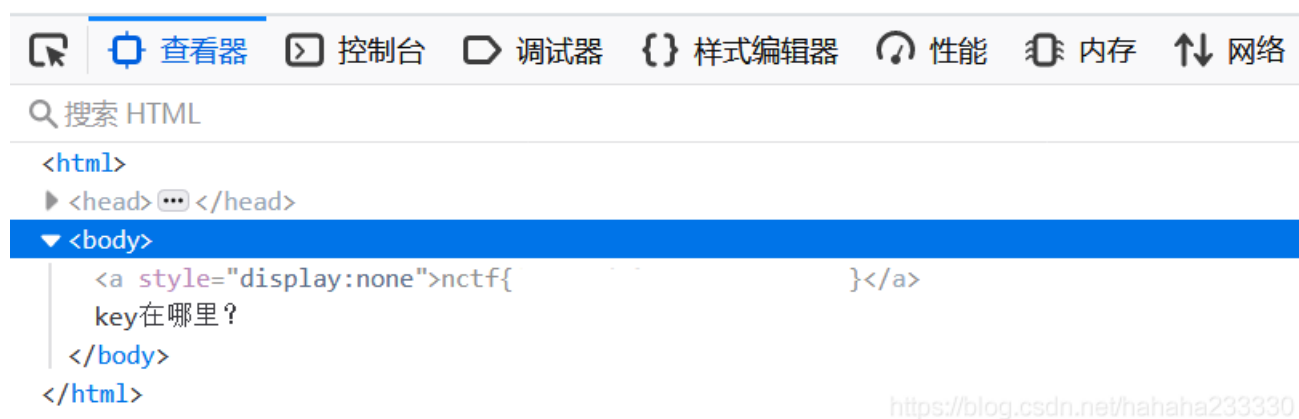
- ①Winhex: 图片隐写工具, 可通过搜索“ctf”“CTF”“key”“flag”等关键字得到flag。
- ②在线工具HtmlEncode/BASE64转换: 注意源代码里奇怪的字符串, 可以尝试解码(分清类型)。
- ③BurpSuite: 抓包工具, 这个很好用。
- ④Wireshark: 抓包工具。使用说明

## WEB

- 1、签到题  
题目地址

直接F12查看源代码就可以得到flag。

## key在哪里?



```
<html>
  <head> ... </head>
  <body>
    <a style="display:none">nctf{
      key在哪里?
    }</a>
  </body>
</html>
```

https://blog.csdn.net/hahaha233330

- 2、md5 collision

[题目地址](#)

先简单学习一下md5()加密解密。

再来看题。题目中的collision是冲突的意思，猜测可能是前后条件矛盾。

### 源码 (PHP)

```
$md51 = md5('QNKCDZO');
$a = @$_GET['a'];
$md52 = @md5($a);
if(isset($a)){
if ($a != 'QNKCDZO' && $md51 == $md52) {
    echo "nctf{*****}";
} else {
    echo "false!!!";
}}
else{echo "please input a";}
```

<https://blog.csdn.net/nahaha233330>

只有当 `$a != 'QNKCDZO' && $md51 == $md52` 的时候才会回写flag。但是这是矛盾的。

```
if ($a != 'QNKCDZO' && $md51 == $md52)
    echo "nctf{*****}";
```

这个题目利用了**php弱类型**。比如在==判等时，`0exxxx=0xsdfs=0`。而在源代码中给出的‘QNKCDZO’的md5就是以0e开头，使用a传输一个md5也是以0e开头的即可。

\*\*\*参考：[PHP Hash比较存在缺陷，影响大量Web网站登录认证、忘记密码等关键业务](#)

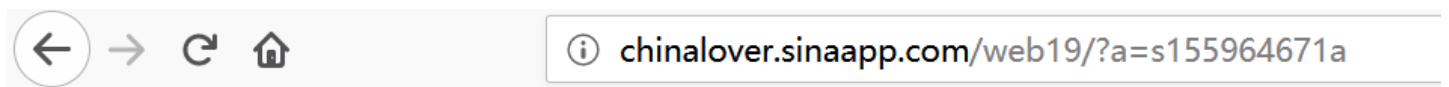
‘QNKCDZO’经过md5()解密后是‘0e830400451993494058024219903391’。

```
<?php
$str = "QNKCDZO";
echo md5($str);
?>
```

```
1 <?php
2 $str = "QNKCDZO";
3 echo md5($str);
4 ?>
```

0e830400451993494058024219903391

构造a=s155964671a（这里用所有0e开头的md5小节都可以），得到flag。



nctf [REDACTED]

### 注：0e开头的MD5小节

0e545993274517709034328855841020: s155964671a  
0e342768416822451524974117254469: s214587387a  
0e848240448830537924465865611904: s214587387a  
0e848240448830537924465865611904: s878926199a  
0e545993274517709034328855841020: s1091221200a  
0e940624217856561557816327384675: s1885207154a  
0e509367213418206700842008763514: s1502113478a  
0e861580163291561247404381396064: s1885207154a  
0e509367213418206700842008763514: s1836677006a  
0e481036490867661113260034900752: s155964671a  
0e342768416822451524974117254469: s1184209335a  
0e072485820392773389523109082030: s1665632922a  
0e731198061491163073197128363787: s1502113478a  
0e861580163291561247404381396064: s1836677006a  
0e481036490867661113260034900752: s1091221200a  
0e940624217856561557816327384675: s155964671a  
0e342768416822451524974117254469: s1502113478a  
0e861580163291561247404381396064: s155964671a  
0e342768416822451524974117254469: s1665632922a  
0e731198061491163073197128363787: s155964671a  
0e342768416822451524974117254469: s1091221200a  
0e940624217856561557816327384675: s1836677006a  
0e481036490867661113260034900752: s1885207154a  
0e509367213418206700842008763514: s532378020a  
0e220463095855511507588041205815: s878926199a  
0e545993274517709034328855841020: s1091221200a  
0e940624217856561557816327384675: s214587387a  
0e848240448830537924465865611904: s1502113478a  
0e861580163291561247404381396064: s1091221200a  
0e940624217856561557816327384675: s1665632922a  
0e731198061491163073197128363787: s1885207154a  
0e509367213418206700842008763514: s1836677006a  
0e481036490867661113260034900752: s1665632922a  
0e731198061491163073197128363787: s878926199a  
0e545993274517709034328855841020: s878926199a

- **3、签到2**

题目地址

既然提示了请输入口令zhimakaimen，输入试试，发现无法“开门”。F12查看源码，发现一行定义输入长度的代码，设定的最大值是10，数一数“zhimakaimen”一共有11位。原来如此！双击这行代码修改为11。再次输入口令，开门，即可得到flag。

## 尚未登录或口令错误

输入框:   
请输入口令: zhimakaimen 开门

!!!

查看器 控制台 调试器 样式编辑器 性能 内存

搜索 HTML

```
<head> ... </head>
<body>
  尚未登录或口令错误
  <form action="./index.php" method="post">
    <p>
      输入框:
      <input type="password" value="" name="text1" maxlength="10">
      <br>
      请输入口令: zhimakaimen
      <input type="submit" value="开门">
    </p>
  </form>
</body>
```

<https://blog.csdn.net/hahaha233330>

flag is: XXXXXXXXXX

输入框:   
请输入口令: zhimakaimen 开门

### • 4、这题不是WEB:

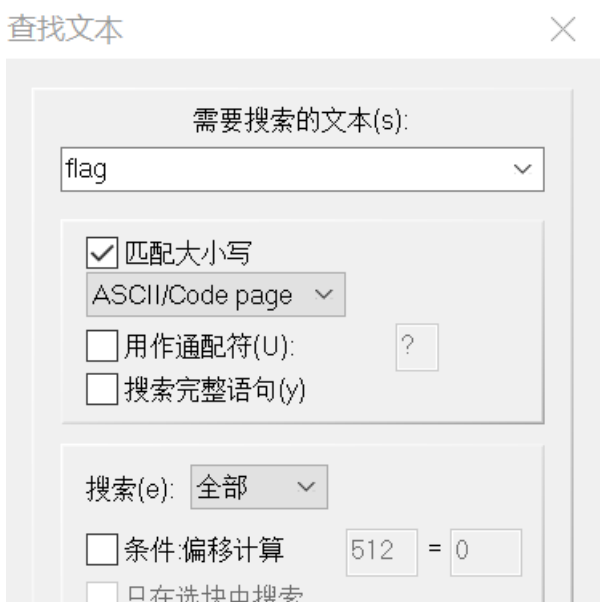
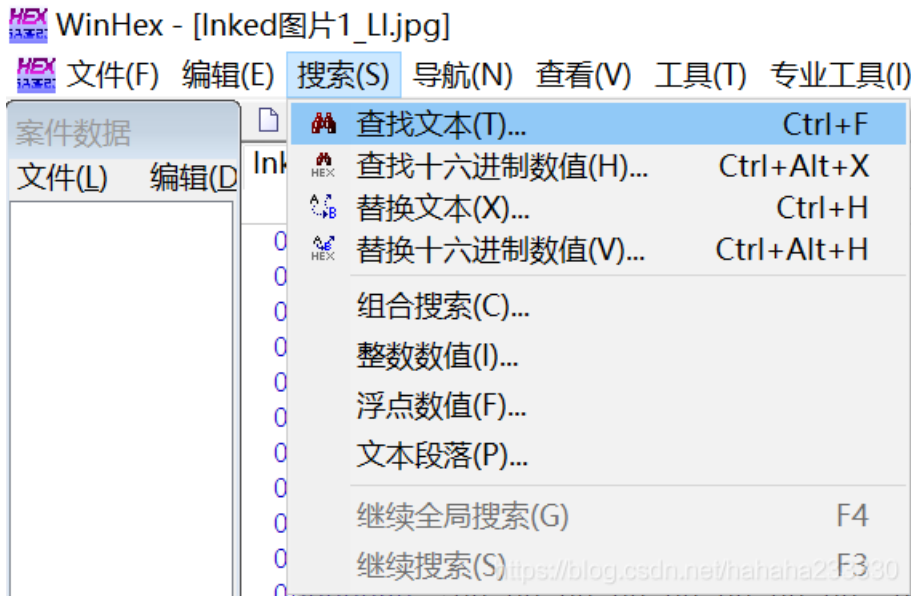
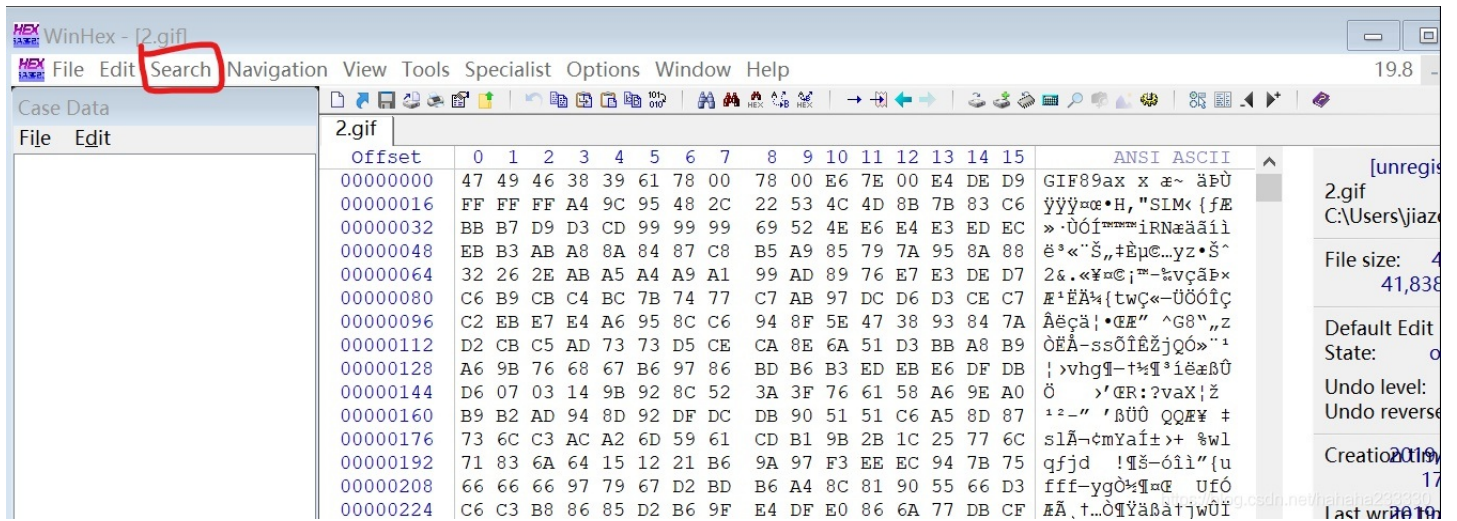
[题目地址](#)

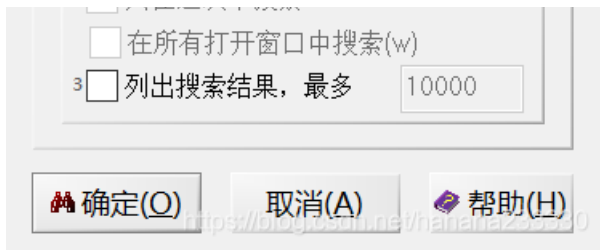
真的，你要相信我！这题不是WEB

这题的确不是web，算misc...

解压下来是个图片。用winhex打开该图片，左上角菜单栏选择Search，选择Find Text（查找文本），输入搜索“ctf”“CTF”“key”“flag”等关键字即可得到flag。

\*提示：快捷键：**ctrl+F**。





• 5、层层递进:

题目地址

打开链接发现是个网页。用F12查看器发现什么都看不出来。Ctrl+U 查看页面源代码试试。

```
view-source:http://chinalover.sinaapp.com/web3/SO.html
1 <link href="css/search.css" rel="stylesheet" type="text/css"/>
2 <div style="text-align:center;margin-top:15px;"><a href="http://www.sniffer.pro" target="_blank"></a></div>
3 <div id="soContent" style="margin:0 auto;margin-top:15px;"></div>
4 <div style="margin-top:10px; text-align:center; font-family: '微软雅黑'; font-size: 14px;">
5 <script type="text/javascript" src="js/so.js"></script>
6 <iframe runat="server" src="SO.html" width="100%" height="237" frameborder="no" border="0" marginwidth="0" marginheight="0" scrolling="no" allowtransparency="yes"></iframe>
7
```

发现里面还嵌套了一个网页，再点进去。

```
39 </style>
40 <link href="css/animate.min.css" rel="stylesheet" type="text/css"></link>
41 </head>
42 <body>
43 <body style="overflow:auto;">
44 <iframe runat="server" src="SO.htm" width="100%" height="237" frameborder="no" border="0" marginwidth="0" marginheight="0"
45 <iframe runat="server" src="http://www.lunzhiyu.com" width="100%" height="3800" frameborder="no" border="0" marginwidth="0"
46
47
48 </body>
49
50 </html>
51
```

发现仍然有嵌套，再点。经过好几层SO.html的嵌套，终于发现了一个全新的网页。

```
39 </style>
40 <link href="css/animate.min.css" rel="stylesheet" type="text/css"></link>
41 </head>
42 <body>
43 <body style="overflow:auto;">
44 <iframe runat="server" src="404.html" width="100%" height="3" frameborder="no"
45 <iframe runat="server" src="http://www.lunzhiyu.com" width="100%" height="3800"
46
47
48
```

打开网页，F12仔细观察其中代码，终于得到flag。

```
14 <!-- Placed at the end of the document so the pages load faster -->
15 <!--
16 <script src="./js/jquery-1.7.2.min.js"></script>
```

```
17 <script src="/js/jquery-7.2.min.js"></script>
18 <script src="/js/jquery-7.2.min.js"></script>
19 <script src="/js/jquery-7.2.min.js"></script>
20 <script src="/js/jquery-7.2.min.js"></script>
21 <script src="/js/jquery-7.2.min.js"></script>
22 <script src="/js/jquery-7.2.min.js"></script>
23 <script src="/js/jquery-7.2.min.js"></script>
24 <script src="/js/jquery-7.2.min.js"></script>
25 <script src="/js/jquery-7.2.min.js"></script>
26 <script src="/js/jquery-7.2.min.js"></script>
27 <script src="/js/jquery-7.2.min.js"></script>
28 <script src="/js/jquery-7.2.min.js"></script>
29 <script src="/js/jquery-7.2.min.js"></script>
30 <script src="/js/jquery-7.2.min.js"></script>
31 <script src="/js/jquery-7.2.min.js"></script>
32 <script src="/js/jquery-7.2.min.js"></script>
33 <script src="/js/jquery-7.2.min.js"></script>
34 <script src="/js/jquery-7.2.min.js"></script>
35 <script src="/js/jquery-7.2.min.js"></script>
36 -->
```

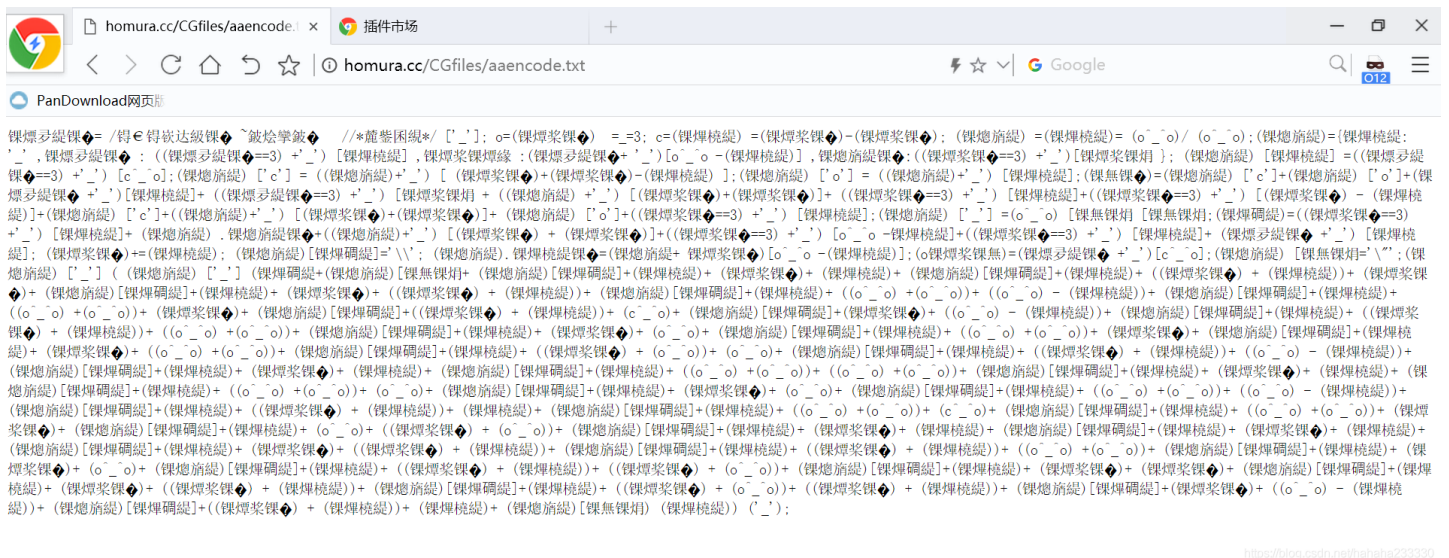
<https://blog.csdn.net/hahaha233330>

## • 6、AAencode

题目地址

javascript aaencode

在chrome中打开，发现中文乱码。这是由于还没有安装解码插件。



去扩展程序里下载Charset插件（修改网站的默认编码），将编码格式改为UTF-8。

## 扩展程序

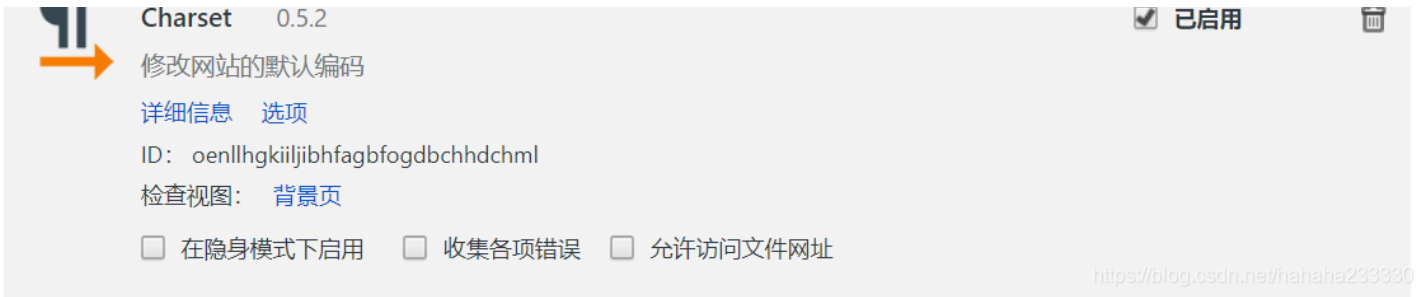
开发者模式

加载已解压的扩展程序...

打包扩展程序...

立即更新扩展程序





这串字符串就会变成这样。

° ¨ / - / \ m ' ) / ~ \_ L \_ L \_ // \* / ▽ \ \* / [ ' ' ] : ¨ ( ° = ) - - 3 : ¨ ( ° @ ) - ( ° = ) - ( ° = ) : ( ° π ) - ( ° @ ) - ( ¨ ^ ¨ ) /



ε° ]+(°θ°)+ (o^\_o)+ ((°-°) + (o^\_o))+ (°Д°)[°ε° ]+(°θ°)+ (°-°)+ (°θ°)+ (°Д°)  
[°ε° ]+(°θ°)+ (°-°)+ (°θ°)+ (°Д°)[°ε° ]+(°θ°)+ (°-°)+ ((°-°) + (°θ°))+ (°Д°)[°  
ε° ]+(°θ°)+ ((°-°) + (°θ°))+ ((o^\_o) + (o^\_o))+ (°Д°)[°ε° ]+(°θ°)+ (°-°)+  
(o^\_o)+ (°Д°)[°ε° ]+(°θ°)+ ((°-°) + (°θ°))+ ((°-°) + (o^\_o))+ (°Д°)[°ε° ]+(°  
θ°)+ (°-°)+ (°-°)+ (°Д°)[°ε° ]+(°θ°)+ (°-°)+ ((°-°) + (°θ°))+ (°Д°)[°ε° ]+(°  
θ°)+ ((°-°) + (o^\_o))+ ((°-°) + (°θ°))+ (°Д°)[°ε° ]+(°-°)+ ((o^\_o) - (°  
θ°))+ (°Д°)[°ε° ]+(°-°) + (°θ°))+ (°θ°)+ (°Д°)[°o° ] (°θ°)) (°θ°)) (°θ°);

来自 homura.cc

nctf{[REDACTED]}

确定

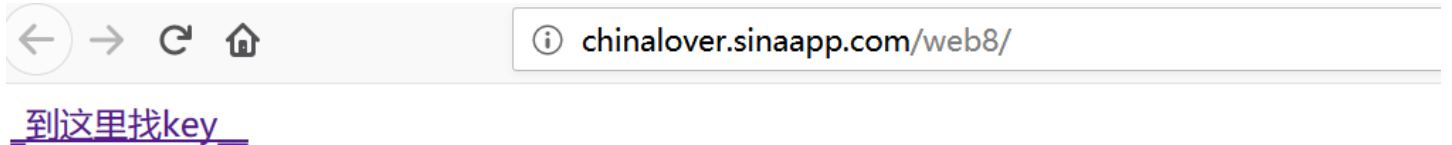
跳出一个窗口，得到flag。

### • 7、单身20年

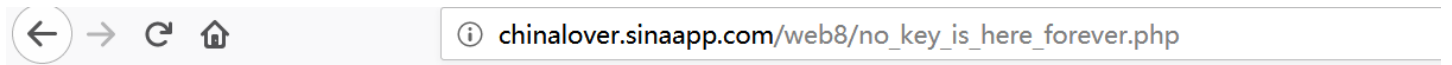
题目地址

这题可以靠技术也可以靠手速！老夫单身二十年，自然靠的是手速！

链接打开，看到提示，点击。



发现什么也没有，这就奇怪了。



这里真的没有KEY，土土哥哥说的，土土哥哥从来不坑人，PS土土是闰土，不是谭神

思考用burpsuite抓包。设置intercept is on，开始抓包。

刷新网页，发现Target变成黄字，应该是抓到了什么，去看看。

Target(目标)——显示目标目录结构的的一个功能

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project

Site map Scope

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty fold

▶ http://chinalover.sinaapp.com  
▶ http://detectportal.firefox.com

**Contents**

Host	Method	URL	Par
http://chinalover.sin...	GET	/web8/	
http://chinalover.sin...	GET	/web8/no_key_is_he...	
http://chinalover.sin...	GET	/web8/search_key.php	
http://chinalover.sin...	GET	/	

Request Response

Raw Headers Hex HTML Render

HTTP/1.1 200 OK  
Server: nginx  
Date: Tue, 03 Dec 2019 11:21:57 GMT  
Content-Type: text/html  
Connection: close  
Via: 1008  
Content-Length: 100

```
<script>window.location="/no_key_is_here_forever.php";</script>
key is : nct
```

<https://blog.csdn.net/hahaha233330>

哈哈，果然有flag。

## • 8、php decode

见到的一个类似编码的shell，请解码

了解php的都知道，eval不能回写，正确应为**echo**。

见到的一个类似编码的shell，请解码

```
<?php
function CLsI($ZzvSWE) {

    $ZzvSWE = gzinflate(base64_decode($ZzvSWE));

    for ($i = 0; $i < strlen($ZzvSWE); $i++) {

        $ZzvSWE[$i] = chr(ord($ZzvSWE[$i]) - 1);

    }

    return $ZzvSWE;
}
```

```
}  
eval (CLsI ("+7DnQGFmYVZ+eoGmlg0fd3puUoZ1fkppek1GdVZhQnJSSZq5aUImGNQBAA=="));  
?>
```

<https://blog.csdn.net/hahaha233330>

修改为echo。运行即可得到flag。

```
1 <?php  
2 function CLsI($ZzvSWE) {  
3  
4     $ZzvSWE = gzinflate(base64_decode($ZzvSWE));  
5  
6     for ($i = 0; $i < strlen($ZzvSWE); $i++) {  
7  
8         $ZzvSWE[$i] = chr(ord($ZzvSWE[$i]) - 1);  
9  
10    }  
11  
12    return $ZzvSWE;  
13  
14 }  
15 echo(CLsI ("+7DnQGFmYVZ+eoGmlg0fd3puUoZ1fkppek1GdVZhQnJSSZq5aUImGNQBAA=="));  
16 ?>
```

<https://blog.csdn.net/hahaha233330>

```
phpinfo();  
flag:nctf[REDACTED]
```

- 10、单身一百年也没用

[题目地址](#)

是的。。这一题你单身一百年也没用

看题目就知道这题与第七题很像，也是考验“手速”。还是按照第七题的方法来做，bp抓包，得到flag。