

# 程序员闯关秀

原创

浅零半泣  于 2017-09-17 10:49:23 发布  467  收藏

分类专栏: [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/sinat\\_34200786/article/details/78008885](https://blog.csdn.net/sinat_34200786/article/details/78008885)

版权



[CTF 专栏收录该内容](#)

19 篇文章 0 订阅

订阅专栏

## 第一关

[原题](#)

### 光棍节程序员闯关秀第1关(总共10关)

提示: 从所有信息中找到进入下一关的方法

[http://blog.csdn.net/sinat\\_34200786](http://blog.csdn.net/sinat_34200786)

解题思路

页面源码

WriteUp

查看页面源码即可

## 第二关

[原题](#)

## 光棍节程序员闯关秀第2关(总共10关)

密码在哪呢?

输入密码

[http://blog.csdn.net/sinat\\_34200786](http://blog.csdn.net/sinat_34200786)

解题思路

又是页面源码

WriteUp

查看页面源码即可

## 第三关

原题

## 光棍节程序员闯关秀第3关(总共10关)

这回就没那么简单了!

[http://blog.csdn.net/sinat\\_34200786](http://blog.csdn.net/sinat_34200786)

解题思路

响应头里藏数据

WriteUp

这次终于不是页面源码了，F12查看响应头即可

过滤消息头

▼ 响应头 (210 字节)

Date: Sun, 17 Sep 2017 02:37:17 GMT

[\[详细了解\]](#)

Content-Type: text/html; charset=UTF-8

[\[详细了解\]](#)

Transfer-Encoding: chunked

[\[详细了解\]](#)

The-Key-Is: a87ff679a2f3e71d9181a67b7542122c csdn.net/sinat\_34200786

## 第四关

[原题](#)

### 光棍节程序员闯关秀第4关(总共10关)

观察你密码的规律

[http://blog.csdn.net/sinat\\_34200786](http://blog.csdn.net/sinat_34200786)

解题思路

将上一关的密码解MD5即可发现规律

WriteUp

先将前面几关的密码列举如下：

04ce6e8ecb37b7142a09364df29b16dc

05b47284c25dfb30d16f5ada2c4359a1

a87ff679a2f3e71d9181a67b7542122c

逐个解MD5才发现其实只有第三关的可以解开，前两关的只是迷惑作用

a87ff679a2f3e71d9181a67b7542122c : 4

那么密码就是 5 的MD5值

e4da3b7fbbce2345d7772b0674a318d5 : 5

## 第五关

[原题](#)

## 光棍节程序员闯关秀第5关(总共10关)



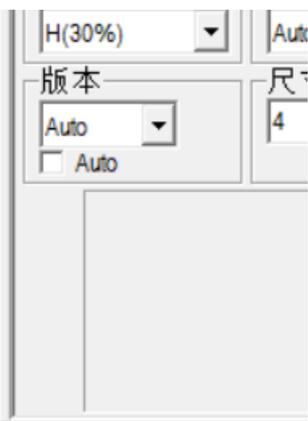
[http://blog.csdn.net/sinat\\_34200786](http://blog.csdn.net/sinat_34200786)

解题思路

简单隐写

WriteUp

直接扫一下看看



已解码数据 1:

位置:(47.6,50.6)-(228.1,50.6)-(47.6,231.1)-(228.4,231.4)

颜色正常,正像

版本:3

纠错等级:L,掩码:3

内容:

<http://sf.gg/>你被耍了什么都没有

[http://blog.csdn.net/sinat\\_34200786](http://blog.csdn.net/sinat_34200786)

好吧，被耍了。。。  
那就扔进HxD里看看好了

```
00000490 4A 72 44 49 CE 6F 25 37 23 CD 86 58 9F 90 00 00 JrDIIo7#I+XY...
000004A0 00 2E 74 45 58 74 43 6F 6D 6D 65 6E 74 00 2F 4B ..tEXtComment./K
000004B0 45 59 3A 62 64 62 66 34 36 61 33 33 37 61 63 30 EY:bdbf46a337ac0
000004C0 38 65 36 62 34 36 37 37 63 32 38 32 36 35 31 39 8e6b4677c2826519
000004D0 35 34 32 2F D0 2F 3D C3 00 00 00 00 49 45 4E 44 542/D/=Ä...IEND
000004E0 AE 42 60 82 0A 0B',.
```

[http://blog.csdn.net/sinat\\_34200786](http://blog.csdn.net/sinat_34200786)

## 第六关

原题

### 光棍节程序员闯关秀第6关(总共10关)

f4de502e58723e6252e8856d4dc8fc3b, 只能告诉你这么多

[http://blog.csdn.net/sinat\\_34200786](http://blog.csdn.net/sinat_34200786)

解题思路

没事多问Google



找到约 383 条结果 (用时 0.42 秒)

高阳Sunny on Twitter: "神马时候会被google收录 ? title ...

<https://twitter.com/sunshineg/status/266521619164434432> ▼

神马时候会被google收录 ? title: f4de502e58723e6252e8856d4dc8fc3b key:

1573402aa6086d9ce42cfd5991027022 4:44 AM - 8 Nov 2012. 1 Retweet, 2 Likes ...

f4de502e58723e6252e8856d4dc8fc3b:解密 - Md5解密

[pmd5.com/about/detail.aspx?code=f4de502e58723e6252e8856d4dc8fc3b](http://pmd5.com/about/detail.aspx?code=f4de502e58723e6252e8856d4dc8fc3b) ▼

f4de502e58723e6252e8856d4dc8fc3b的解密结果为:该记录已经过期了,请前往[首页查询](http://blog.csdn.net/sinat_34200786)

## 第七关

原题



解题思路



WriteUp



## 第八关

原题

# 光棍节程序员闯关秀第8关(总共10关)

有时候事情就是这么简单

钥匙就在手里，门却不知所踪

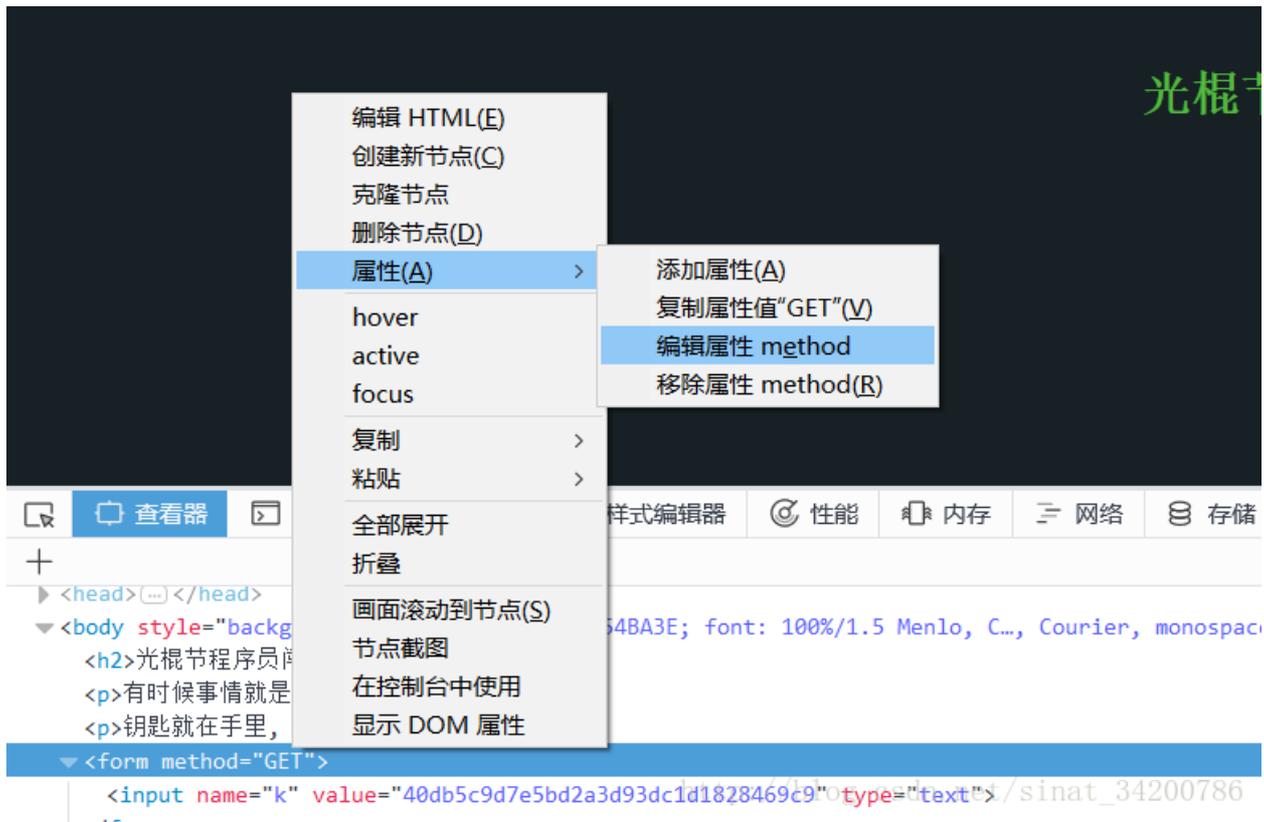
40db5c9d7e5bd2a3d93c1d1828469c9

[http://blog.csdn.net/sinat\\_34200786](http://blog.csdn.net/sinat_34200786)

解题思路

From一般都是POST的

WriteUp



涨姿势点

第一次直接改这个

第九关

# 光棍节程序员闯关秀第9关(总共10关)

## 光棍节的寂寞谁能懂

```

01001000 00110100 01110011 01001001 01000001 01000011 01001010 01001011
01101110 01101100 01000001 01000001 01000001 00101011 00110001 01011010
01000010 00110001 01010010 01010100 01010011 00110111 01100011 00101011
01001001 01010001 01000111 01101011 01101001 01000110 01010001 01010110
01000101 01001001 01101101 01000001 01100111 01001000 01010010 01000011
01000100 01010110 01001011 01101011 01000110 00110110 01101011 01000010
01010001 01110010 01010111 01000101 01000101 01000011 01000011 00110000
01010001 01000010 01001011 01110001 0110____ 0110____ 01001011 01001011
01101001 0110____ 01100111 01010101 01010001 01010101 01000010 01000001
01100111 01010101 01100111 01010000 01010011 01000111 00111000 01010111
01010101 0100____ 01101100 01100101 01110101 01100111 01101001 01001011
01011000 01000010 01010110 01110000 01001001 01101000 01100001 01110001

```

[http://blog.csdn.net/sinat\\_34200786](http://blog.csdn.net/sinat_34200786)

### 解题思路

一点脑洞，一点难度

### WriteUp

首先可以发现所有的二进制数据缺少的都是4位，那么联想到双11，猜测缺少的四位为 1111

补全后干嘛呢？按照一般思路应该把二进制转为十进制，然后再转为ASCII

```

+XqI7Azp/UY03yTejeeTkPxKnaeuLGp1Rs0jfYtDYtDumc8cnJ6KtgrZP1mJQ4tnlcQ0MjEzaQBtBZ
+Pa5r1tS6npfC/MccviUmUBsXOfFW73puTw6BZy72UN3Dr6TDX5XjcFQm6k3c6jXYnFzhGXglRmrm/ZYycqqhHjhXBQmG33vi3Q
bGJcMdlgh3nWpzu7FLyh+QnebbJuzUL15Md5OM81KnQzQ9dYcgd8LpndN2p310srHqbGonhbpd8+N7fimuMnVvHCX1/KOYhnhWrl
+ulRoQz+6+WK2sk30NhJu4QupFK/1UX6OQk5SnnIPD7ztLlyPHbd1IZXOS12i1b
+Qr5U/Oen7QsD/BHGq4BhJF63RrVFTEPhvZMialxwX5x0XFUvvJzd2fnk8Ua4wfP+eGMBc8/S3pLXpZWP4iQfs0RemaovgWZCA1V
+wX6SeJAnRryQb9BQPN2t36fi/tahUsSqrVdlhIRCeYZyKFL6CGNeoaZ8Nqw99Yqi/661zjuGiKQulxa/q4lhyR9K3t9fCGafbcI
+MdxhhEGcXGnD8QwyQ9o5DJylaXPZZ8Cjs0fot+w79kdUuykp2U0Ek0s/146ZaXSA3v8DnCxCEBt
+AYwf26ddCCUw8+KFlevZuCODxtqPFyulb470ldzbnRi8UpuFbWbTwd
+FPSpbtvDzRVNFnShZ6oKDQcqwNG3A5QLOMzaymWN3fbz8bo6Woqcjmmv/alv/P4kmoYWnjX0wl+rfcSsyovWnEphsKX70fn49tI
HXM142IUwCB7eNZitpBsZXaBntvKCKPPbQn5VbMcMRatz1DoycZ8ttJn8deIcTIu/6JfGnu3mwHYXVNIzZaq+ZHvrEANxf48+2fR
+TNM1420mNUhkVtRo0oTjnrVhuDPv5huzoiRePdWrSFkd+if/cfpL/pK/5C/5S/5/yH8BbZ04JAAoAAA=et/sinat_34200786

```

很明显这是base64加密后的数据，不过解出来的确是乱码

请输入要进行编码或解码的字符：

```
GafbcnTxSnel77IGjourN+MdxhhEGcXGnD8QwyQ9o5DJy1aXPZZ8Cjs0fot+w79kdUuykp2U0Ek0s/I46ZaX  
SA3v8DnCxCEBt+AYwf26ddCCUw8+KFlevZuCODxtqPFyulb47OldzbnRi8UpuFbWbTwd+FPSpbtvDzRVNF  
nShZ6oKDQcqWNG3A5QLQMzaymWN3fbz8bo6Woqcjmmv/a1v/P4kmoYWnjXOw1+rfCsysovWnEphsKX  
70fN49tU03iE8QJh3FbO7g6oHXMI42IUwCB7eNZitpBsZxAbntvKCKPPbQn5VbMcMRAz1DoycZ8ttJn8del  
cTlu/6JfGnu3mwHYXVNIzq+ZHvrEANxf48+2fR+TNM1420mNUhkVtRo0oTjnrvhuDPv5huzoiRePdWrSFk  
d+if/cfpL/pK/5C/5S/5/yH8BbZ04JAAoAAA=
```

编码

解码

解码结果以16进制显示

复制

清空

Base64编码或解码结果：

```
"JP 喜TSK>!TtB  
RB @A@@HHoP鞞\i"QZ□.뽕ZoYs)漚g?,dde`1□~□I絰→EYiC<Ge(**p9y  
wYHdce□<糖짱?W~;#@f,□n♀`lp3Qr/_O-(. 鯨('dup.b`l@ V_1뽕DY%`y)쥼LD.1. 濶|K[4yqvLB 罨m4#aAWlū&#9W  
"q`-"nuGi罨c1-6hućA,吻/ǰ&8□_θal$á½'濶|PI$/남/N`h7. 卍}kSC4m6%-Mh`XSv≠6P_stY^  
N+□Ot=(3öΩL=6CMH□z蚯=1& 惱y"e34筭Zm#[nÃ67] cN\yā=IlugC\stŪoyE06_ǰtc 罨8_1[;sz>X@C0  
Ω+o;:□AA
```

[http://blog.csdn.net/sinat\\_34200786](http://blog.csdn.net/sinat_34200786)

尝试过把解密后的数据直接粘贴到HxD里生成文件，不过粘贴不了

## base64 解码/编

无标题1

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

```
EGcXGnD8Qw  
w8+KFlevZuCC  
ymWN3fbz8bo  
MI42IUwCB7e  
fvrEANxf48+2f  
JAAoAAA=  
结果以16进制显
```

HxD

无法粘贴，因为剪切板包含无效十六进制字符。  
如果你想粘贴文本，请首先移动到文本列。

确定

```
/s)漚g?,dde`1□~□I絰→EYiC<Ge(**  
3Qr/_O-(. 鯨('dup.b`l@ V_1뽕DY%
```

[http://blog.csdn.net/sinat\\_34200786](http://blog.csdn.net/sinat_34200786)

后来才知道是需要用解密后的数据生成 .tag.gz 文件

```
import base64

f1 = open('01.txt','r')
f2 = open('out.tar.gz','wb')
s = ''

for i in f1.readlines():
    i = i.rstrip()
    i = list(i.replace('____','1111').split(' '))
    for n in i:
        n = int(n,2)
        s += chr(n)

f2.write(base64.b64decode(s))
f1.close()
```

解压生成的 `out.tar.gz` 文件即可



恭喜，你已经通过了所有关卡

看来你是一个很有想法的程序员，何不加入中国最具创意的开发者问答社区呢？赶紧注册 [SegmentFault.com](http://SegmentFault.com)

或者在微博上帮寂寞的我刷刷粉@joyqi...

[分享我的战绩到微博](#)

[http://blog.csdn.net/sinat\\_34200786](http://blog.csdn.net/sinat_34200786)

涨姿势点

base64解出来的乱码为什么不用 `.tar.gz` 文件试试呢？