bugkuctf练习平台reverse部分writeup

原创

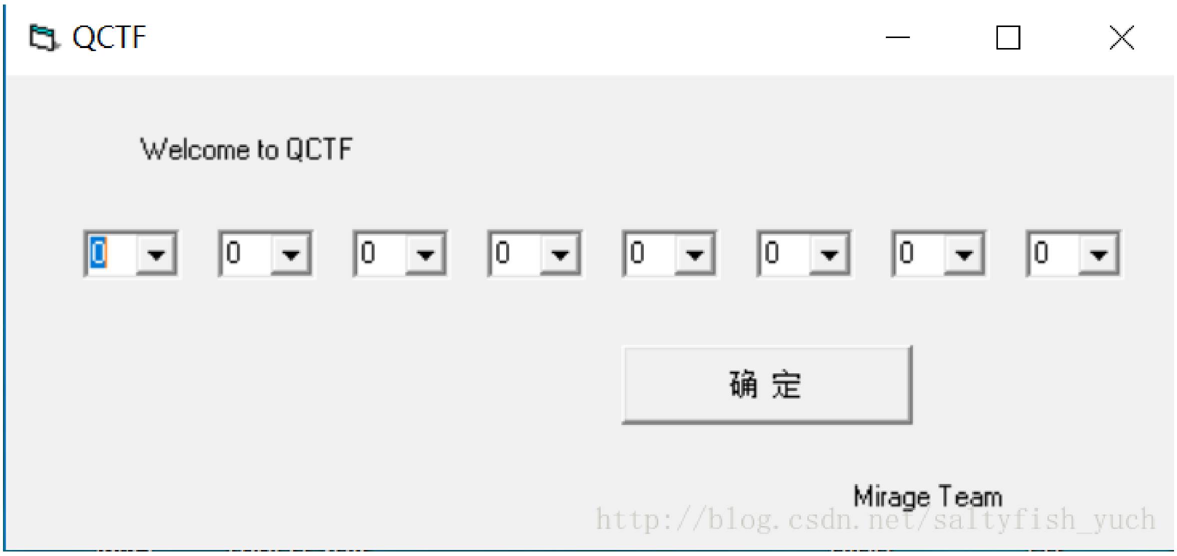
saltyfishy 于 2017-09-06 18:08:28 发布 7889 收藏 2
文章标签： ctf

题目地址：http://123.206.31.85/challenges

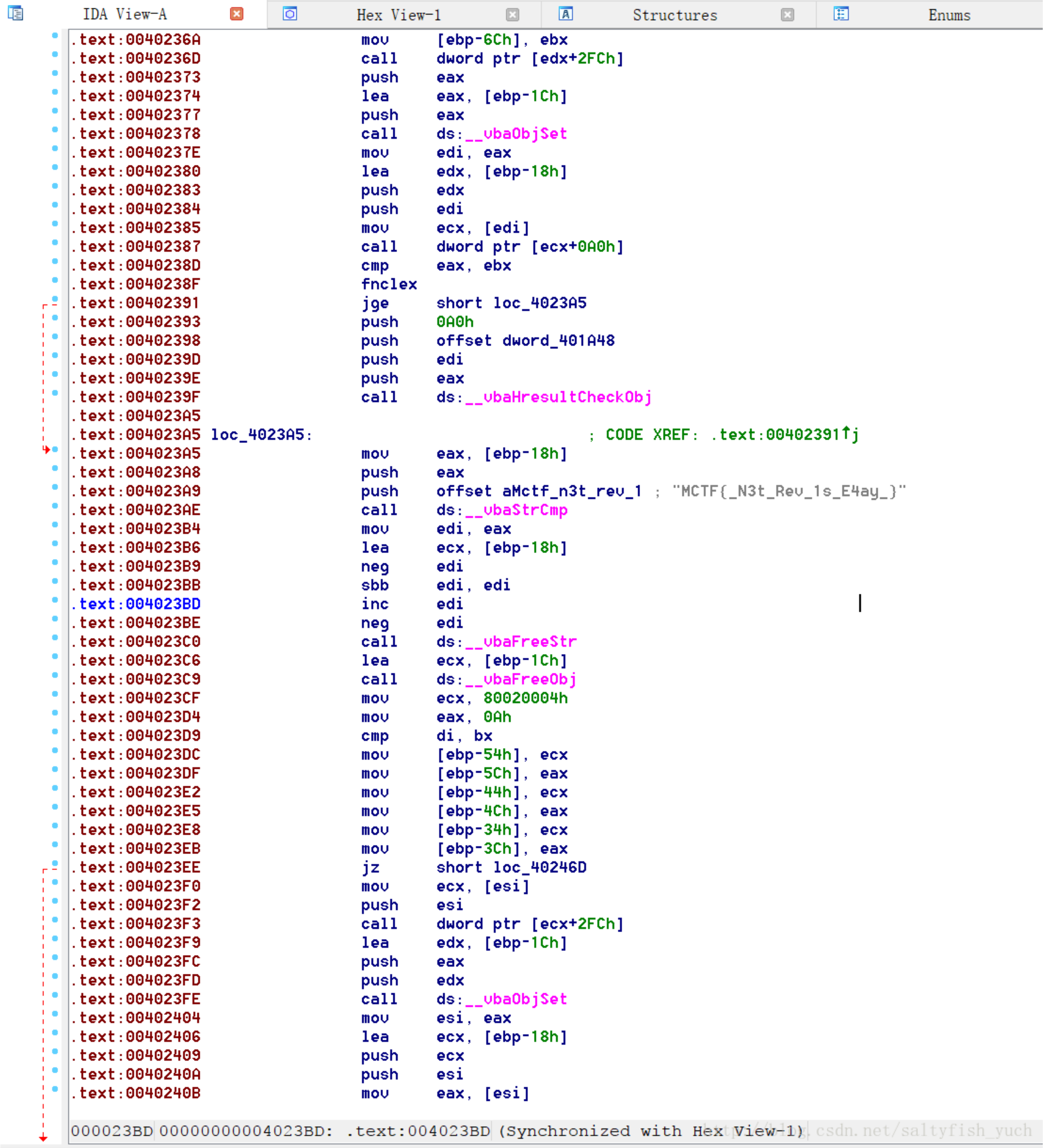
题目：Easy_vb

flag格式：flag{xxxx}
题目来自MCTF，原题目格式：MCTF{xxxx}

打开下载的文件是这样的界面



于是用IDA打开



```
.text:0040236A                 mov     [ebp-6Ch], ebx
.text:0040236D                 call    dword ptr [edx+2FCh]
.text:00402373                 push    eax
.text:00402374                 lea     eax, [ebp-1Ch]
.text:00402377                 push    eax
.text:00402378                 call    ds:__vbaObjSet
.text:0040237E                 mov     edi, eax
.text:00402380                 lea     edx, [ebp-18h]
.text:00402383                 push    edx
.text:00402384                 push    edi
.text:00402385                 mov     ecx, [edi]
.text:00402387                 call    dword ptr [ecx+0A0h]
.text:0040238D                 cmp     eax, ebx
.text:0040238F                 fnclex
.text:00402391                 jge     short loc_4023A5
.text:00402393                 push    0A0h
.text:00402398                 push    offset dword_401A48
.text:0040239D                 push    edi
.text:0040239E                 push    eax
.text:0040239F                 call    ds:__vbaHresultCheckObj
.text:004023A5
.text:004023A5 loc_4023A5:                             ; CODE XREF: .text:00402391↑j
.text:004023A5                 mov     eax, [ebp-18h]
.text:004023A8                 push    eax
.text:004023A9                 push    offset aMctf_n3t_rev_1 ; "MCTF{_N3t_Rev_1s_E4ay_}"
.text:004023AE                 call    ds:__vbaStrCmp
.text:004023B4                 mov     edi, eax
.text:004023B6                 lea     ecx, [ebp-18h]
.text:004023B9                 neg     edi
.text:004023BB                 sbb     edi, edi
.text:004023BD                 inc     edi
.text:004023BE                 neg     edi
.text:004023C0                 call    ds:__vbaFreeStr
.text:004023C6                 lea     ecx, [ebp-1Ch]
.text:004023C9                 call    ds:__vbaFreeObj
.text:004023CF                 mov     ecx, 80020004h
.text:004023D4                 mov     eax, 0Ah
.text:004023D9                 cmp     di, bx
.text:004023DC                 mov     [ebp-54h], ecx
.text:004023DF                 mov     [ebp-5Ch], eax
.text:004023E2                 mov     [ebp-44h], ecx
.text:004023E5                 mov     [ebp-4Ch], eax
.text:004023E8                 mov     [ebp-34h], ecx
.text:004023EB                 mov     [ebp-3Ch], eax
.text:004023EE                 jz      short loc_40246D
.text:004023F0                 mov     ecx, [esi]
.text:004023F2                 push    esi
.text:004023F3                 call    dword ptr [ecx+2FCh]
.text:004023F9                 lea     edx, [ebp-1Ch]
.text:004023FC                 push    eax
.text:004023FD                 push    edx
.text:004023FE                 call    ds:__vbaObjSet
.text:00402404                 mov     esi, eax
.text:00402406                 lea     ecx, [ebp-18h]
.text:00402409                 push    ecx
.text:0040240A                 push    esi
.text:0040240B                 mov     eax, [esi]
```

```
000023BD 00000000004023BD: .text:004023BD (Synchronized with Hex View-1)
```

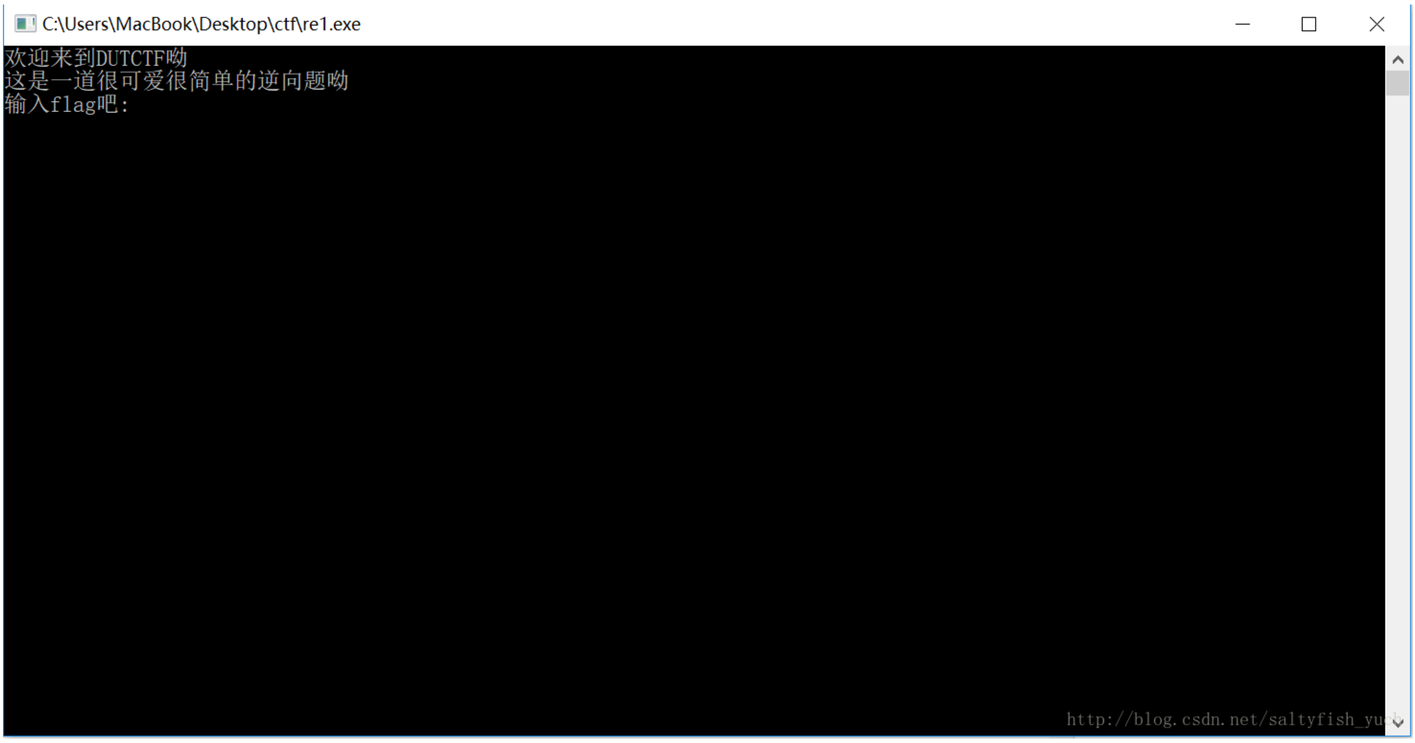
找到flag

题目：Easy_Re

flag格式：DUTCTF{xxxx}

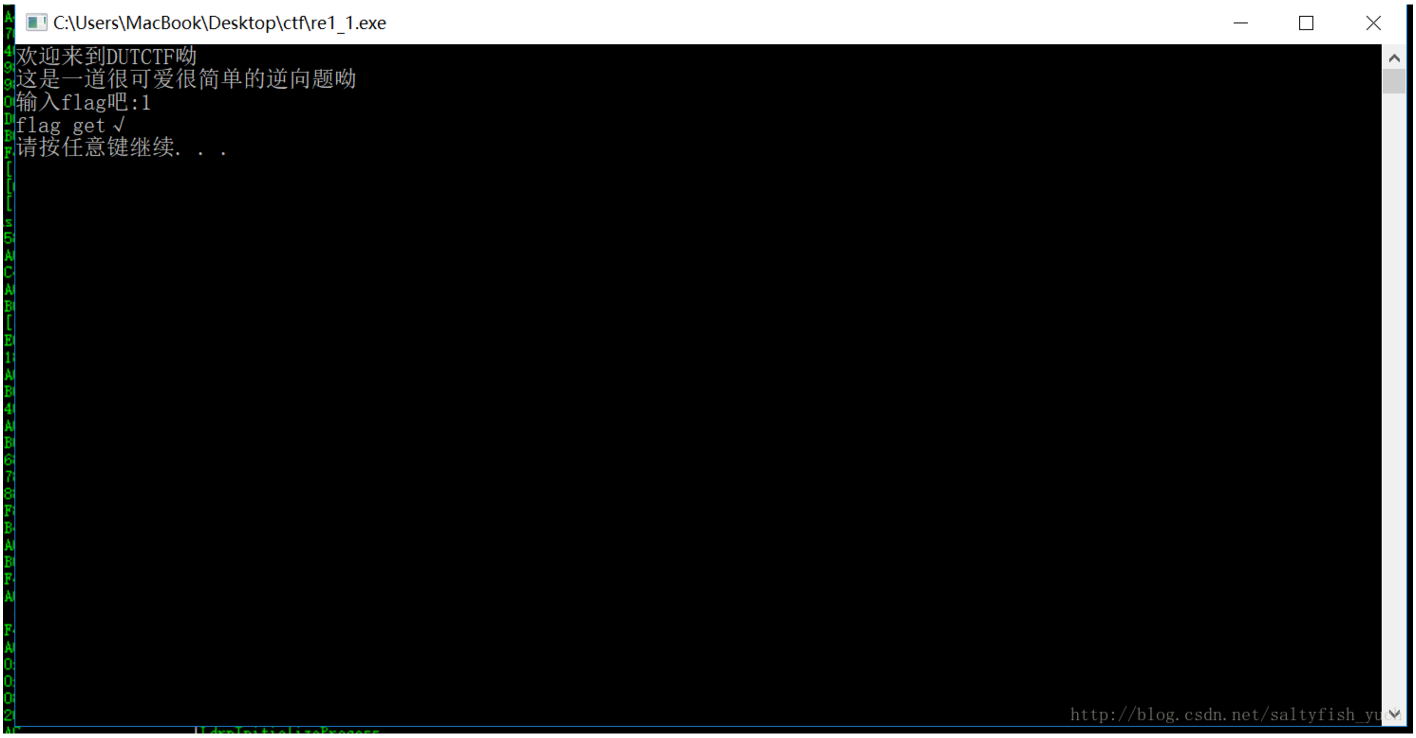
Hint: 1.逆向常用的工具有IDA 、ollydbg

打开下载的文件



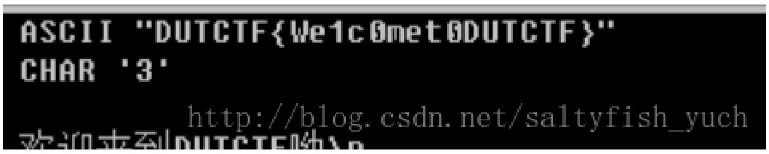
```
欢迎来到DUTCTF呦
这是一道很可爱很简单的逆向题呦
输入flag吧:
```

用oll打开，修改完后发现好像没什么卵用



```
欢迎来到DUTCTF呦
这是一道很可爱很简单的逆向题呦
输入flag吧:1
flag get √
请按任意键继续. . .
```

然后在头部发现flag. emmmmmmmm.....

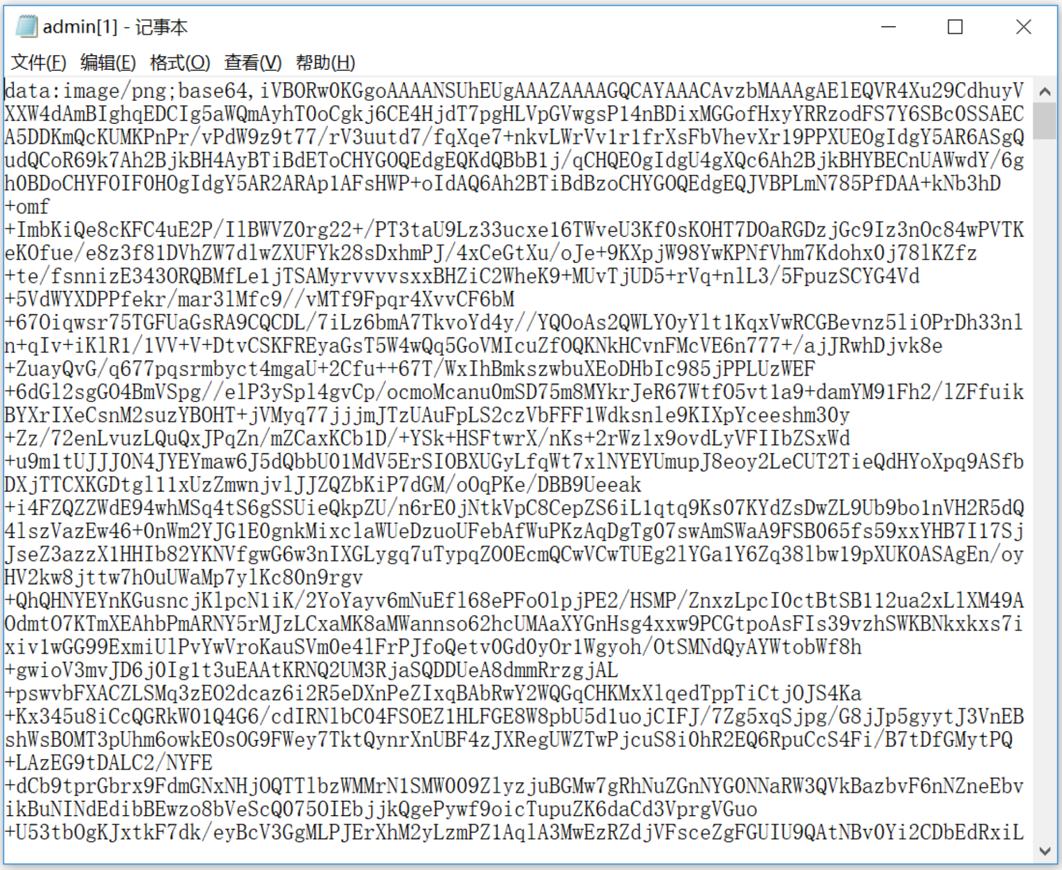


```
ASCII "DUTCTF{We1c0met0DUTCTF}"
CHAR '3'
欢迎来到DUTCTF呦\n
```

题目：逆向入门

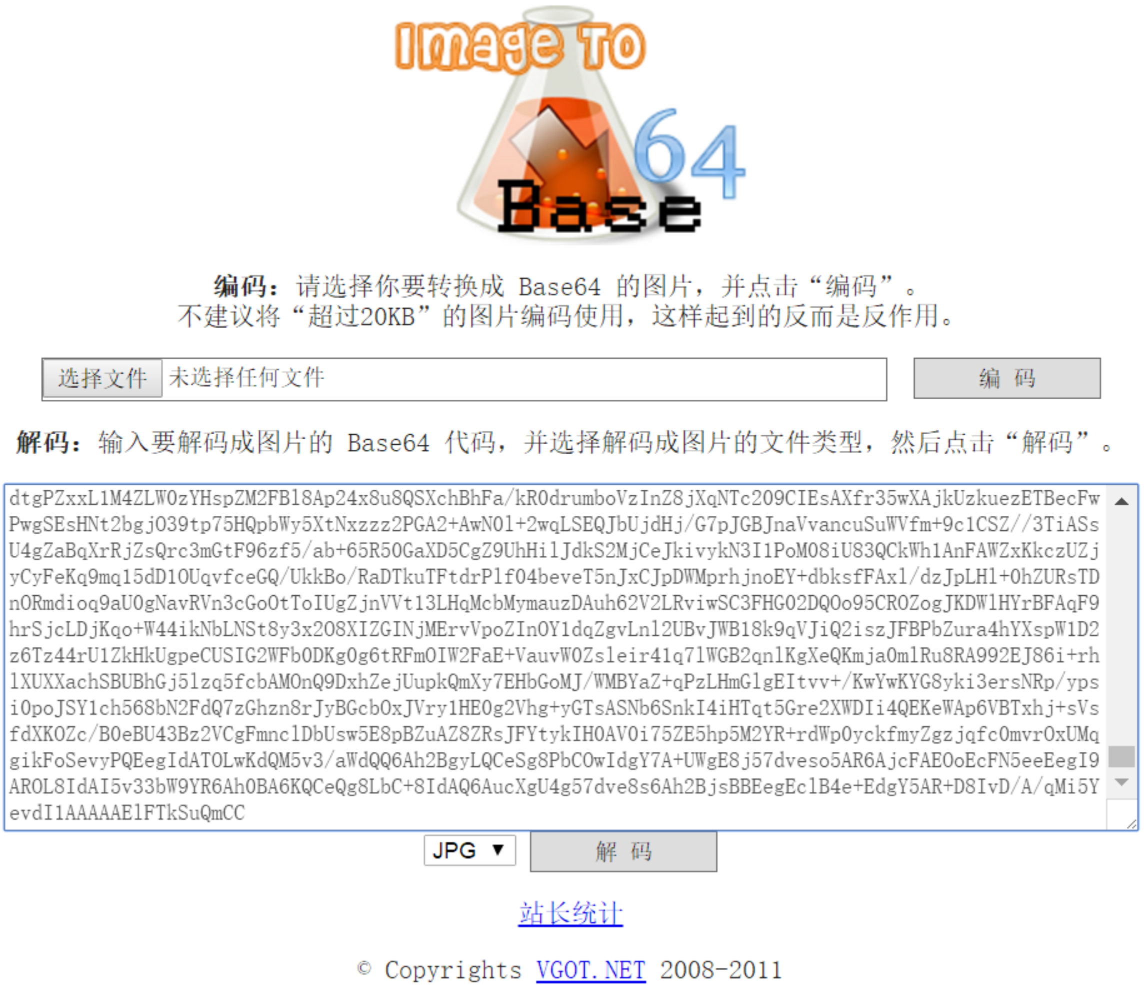
打开题目发现是base64转图片

data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAZAAAAGQCAYAAACAvzbMAAAgAElEQVR4Xu29CdhuyVXXW4dAmBIghqEDCIg5aWQmAyhT0oCgkj6CE4HjdT7pgHLVpGVwgsP14nBDixMGGofFS7Y6SBc0SSAEC5SSAEC



data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAZAAAAGQCAYAAACAvzbMAAAgAElEQVR4Xu29CdhuyV
XXW4dAmBIghqEDCIg5aWQmAyhT0oCgkj6CE4HjdT7pgHLVpGVwgsP14nBDixMGGofHxyYRRzodFS7Y6SBc0SSAEC
A5DDKmQcKUMKPnPr/vPdW9z9t77/rV3uutd7/fqXqe7+nkvLWrVv1r1frXsFVhevXr19PPXUE0gIdgY5AR6ASgQ
udQCoR69k7Ah2BjkBH4AyBTiBdEToCHYG0QEdgEQKdQBbB1j/qCHQE0gIdgU4gXQc6Ah2BjkBHYBECnUAWwdY/6g
h0BDoCHYFOIF0H0gIdgY5AR2ARAp1AFsHWP+oIdAQ6Ah2BTiBdBzoCHYG0QEdgEQJVBPLmN785PfDAA+kNb3hD
+omf
+ImbKiQe8cKFC4uE2P/I1BWVZ0rg22+/PT3taU3taU9Lz33ucxe16TWveU3U3KKf0sK0HT7DOaRGDzjGc9Iz3n0c84wPVTK
eK0fue/e8z3f81DVhZW7dlwZXUFYk28sDxhmPJ/4xCeGtXu/oJe+9KXpj78YwKPNfVhm7Kdohx0j78lKZfz
+te/fsnnizE3430RQBMfLe1jTSAMyrvvvvvsBHZiC2WheK9+MUvTjUD5+rVq+n
+5VdWYXDPPfekr/mar3lMfc9//e0e9+pq0pOSDP++/FpCfaEwFmaFaYSlTPo9Cf4xBgTHXKMhzLi8j2
+ZuayQvG/q677pqsrmbyct4mgaU+2Cfu++67T/WxIhBmkszwbuFEF1WdksSTDHKnzKwxeT2dnbCOj777+jaJRwhDvjk8e
+6dGl2sgG04BmVSpg//e1P3ySp14gvCp/ocmoMcanu0mSD75mM8MYkr6e9KrjRe
+fBe/1aYJsJY1AmHO+bjSUB7oMrxw2P04CZMiwLLDjSmgZsA6D6DVOZMLJeM6IUuf6QE9h9ftBgLqzVp7W/7ASOjmUmA5OEs
+Ae
+Zz/72enLvuzQuQxJPqZn/zg6z/+YSk+HSFtwrX/nKs+2rWz19ovdLyVFIIbZSxWd
+u9m1tUJJJ0N4JYEYmaw6J5dQbbU01MdV5ErSI0BXUGyLfqWt7xnNYYUmupJ8eoy2LeCUT2TieQdHYoXpq9ASfb
DXjTTCXKGDtgl11xUzZmwnjvlJJZQZbKiP7dGM/o0qPKe/DBB9Ueeak
+i4FZQZWdE94whMSq4tS6gSSUieQkpZU/n6rE0/n6rE0jNtkVpC8CepZS6iL1qtq9Ks07KYdZsDwZL9Ub9bo1nVH2R5dQ
41szVazEw46+0nWm2YJG1E0gnkMixclaWUeDzuoUFebAfWuPKzAqDgTg07swAmSWaA9FSB065fs59xxYHB7I17Sj
JseZ3azzX1HHIb82YKNVfgwG6w3nIXGLygq7uTypqZ0OEcmQCwVCwTUEg21YGa1Y6Zq38lbw19pXUK0ASAgEn/oy
HV2kw8jttw7h0uUWaMp7ylKc80n9rgv
+QhQHNYEYnKGusncjKlpcN1iK/2YoYayv6mNuEf168ePFo0lpjPE2/HSMP/ZnxzLpcI0ctBtSB112ua2xL1XM49A
0dmt07KTmXEAhbPmARNY5rMJzLCxaMK8aMannso62hcUMAaXYXGnHsg4xxxw9PCGtpoAsFIs39vzhSWKBNkxkxs7i
xiv1wGG99ExmiU1PvYwVroKauSVm0e41FrPJfoQetv0Gd0yOr1Wgyoh/0tSMNdQyAYWtobWf8h
+gwioV3mvJD6j0Ig1t3uEAAtKRNQ2UM3RjaSQDDUeA8dmmRrzgjAL
+pswvbFXACZLSMq3zE02dcaz6i2R5eDXnPeZIxqBAbRwY2WQGqCHKMxXlqedTppTiCtj0JS4Ka
+Kx345u8iCcQGRkW01Q4G6/cdIRN1bC04FSOEZ1HLFGE8W8pbU5d1uojCIFJ/7Zg5xqSjpg/G8jJp5gyytJ3VnEB
shWsBOMT3pUhm6owkEOsOG9FWey7TktQynrXnUBF4zJXRegUWZTwPjcuS8i0hR2EQ6RpuCcS4Fi/B7tDfGMytPQ
+LAzEG9tDALC2/NYFE
+dCb9tprGbrx9FdmGNxNHjOQTT1bzWMMrN1SMW009ZlyzjuBGMw7gRhNuZGnNYG0NNaRW3QVkBazbvF6nNZneEbv
ikBuNINdEdibBEwzo8bVeScQ0750IEbjjkQgePywf9oicTupuZK6daCd3VprgVGuo
+U53tb0gKJxtkF7dk/eyBcV3GgMLPJErXhM2yLzmPZ1AqlA3MwEzRZdjVFsceZgFGUIU9QAtNBv0Yi2CDbEdRxiL

于是百度base64转图片解码得到二维码

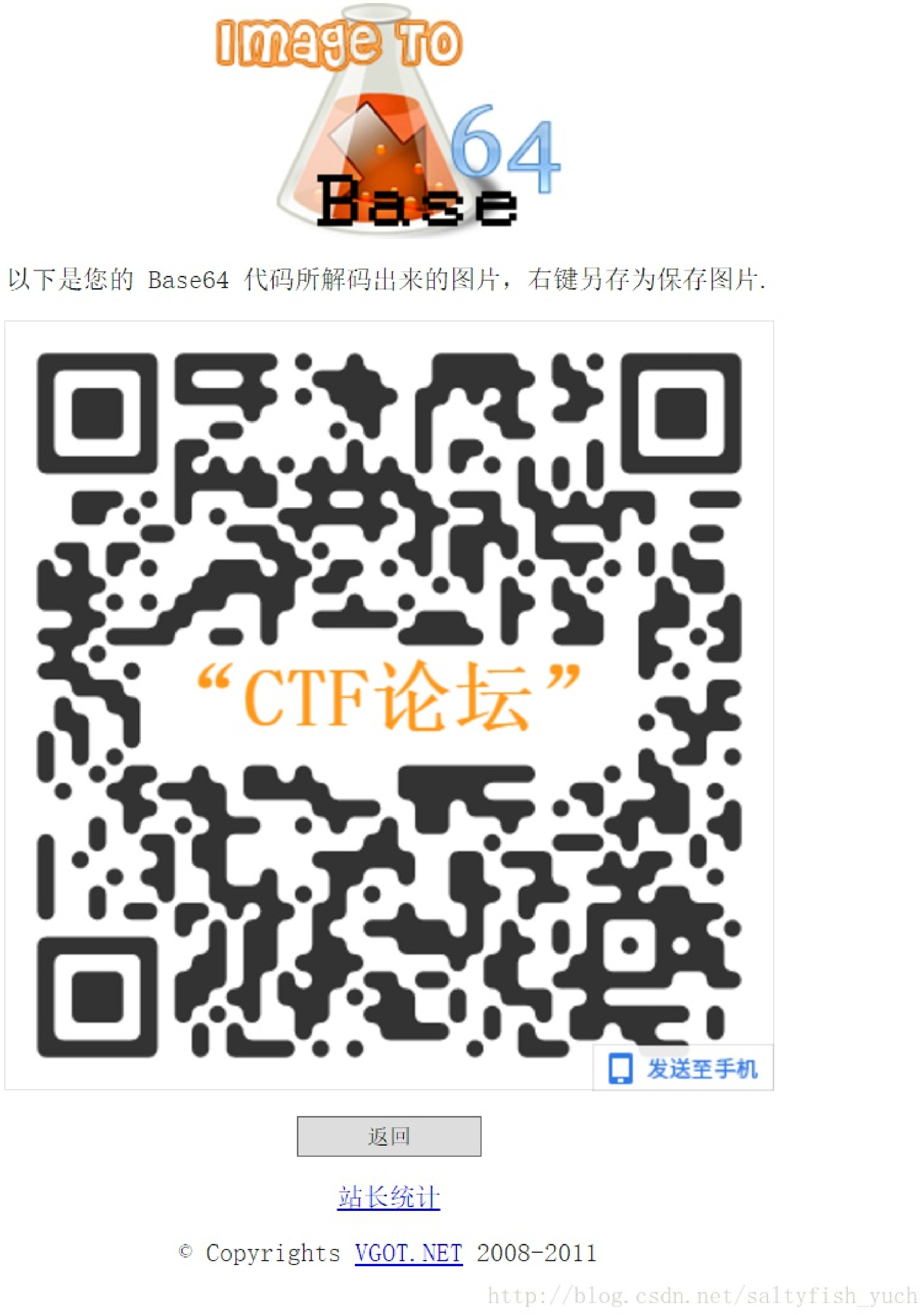


编码：请选择你要转换成 Base64 的图片，并点击“编码”。
不建议将“超过20KB”的图片编码使用，这样起到的反而是反作用。

解码：输入要解码成图片的 Base64 代码，并选择解码成图片的文件类型，然后点击“解码”。

```
dtgPZxxL1M4ZLW0zYHspZM2FBl8Ap24x8u8QSXchBhFa/kR0drumboVzInZ8jXqNTc209CIEsAXfr35wXAjkUzkuezETBecFw
PwgSEsHNt2bgj039tp75HQpbWy5XtNxzzz2PGA2+AwN0l+2wqLSEQJbUjdHj/G7pJGBJnaVvancuSuWVfm+9c1CSZ//3TiASs
U4gZaBqXrRjZsQrc3mGtF96zf5/ab+65R50GaXD5CgZ9UhHilJdkS2MjCeJkivykN3I1PoM08iU83QCkWh1AnFAWZxKkczUZj
yCyFeKq9mq15dD10UqvfceGQ/UkkBo/RaDTkuTFtdrPlf04beveT5nJxCJpDWMprhjnoEY+dbksfFAxl/dzJpLHl+0hZURsTD
nORmdioq9aU0gNavRVn3cGo0tToIUgZjnVVt13LHqMcbMymauzDAuh62V2LRviwSC3FHG02DQOo95CR0ZogJKDWlHYrBFAqF9
hrSjcLDjKqo+W44ikNbLNSt8y3x208XIZGINjMErvVpoZInOY1dqZgvLnl2UBvJWB18k9qVJiQ2iszJFBPbZura4hYXspW1D2
z6Tz44rU1ZkHkUgpeCUSIG2WFb0DKg0g6tRFmOIW2FaE+VauvW0Zsleir41q7lWGB2qnlKgXeQKmja0mlRu8RA992EJ86i+rh
lXUXXachSBUBhGj5lzq5fcbAMOnQ9DxhZejUupkQmXy7EHbGoMJ/WMBYaZ+qPzLHmGlgEItvv+/KwYwKYG8yki3ersNRp/yps
i0poJSY1ch568bN2FdQ7zGhzn8rJyBGcbOxJVry1HE0g2Vhg+yGTsASNb6SnkI4iHTqt5Gre2XWDIi4QEKeWAp6VBTxhj+sVs
fdXKOZc/B0eBU43Bz2VCgFmnclDbUsw5E8pBZuAZ8ZRsJFYtykIH0AV0i75ZE5hp5M2YR+rdWp0yckfmyZgzjqfc0mvr0xUMq
gikFoSevyPQEegIdATOLwKdQM5v3/aWdQQ6Ah2BgyLQCeSg8PbCOwIdgY7A+UWgE8j57dveso5AR6AjcFAEOoEcFN5eeEegI9
AROL8IdAI5v33bW9YR6Ah0BA6KQCeQg8LbC+8IdAQ6AucXgU4g57dve8s6Ah2BjsBBEegEclB4e+EdgY5AR+D8IvD/A/qMi5Y
evdI1AAAAAElFTkSuQmCC
```

© Copyrights VGOT.NET 2008-2011



以下是您的 Base64 代码所解码出来的图片，右键另存为保存图片.

© Copyrights VGOT.NET 2008-2011

扫二维码即得flag