Hgame2018week1

Web 部分

0x01 Are you from Europe?

F12 打开后发现

```
▼<script> == $0

        var times = 0;
        var quartz = 167;
        var money = 0;
        var woainvzhuang = true;
        var cards = [];
```

，尝试修改 quartz，

修改成功，抽出 flag

Re 部分

0x01 re0

用 ida 打开，

```
pL ; "hctf{F1r5t_St5p_Ls_Ea5y}"
```

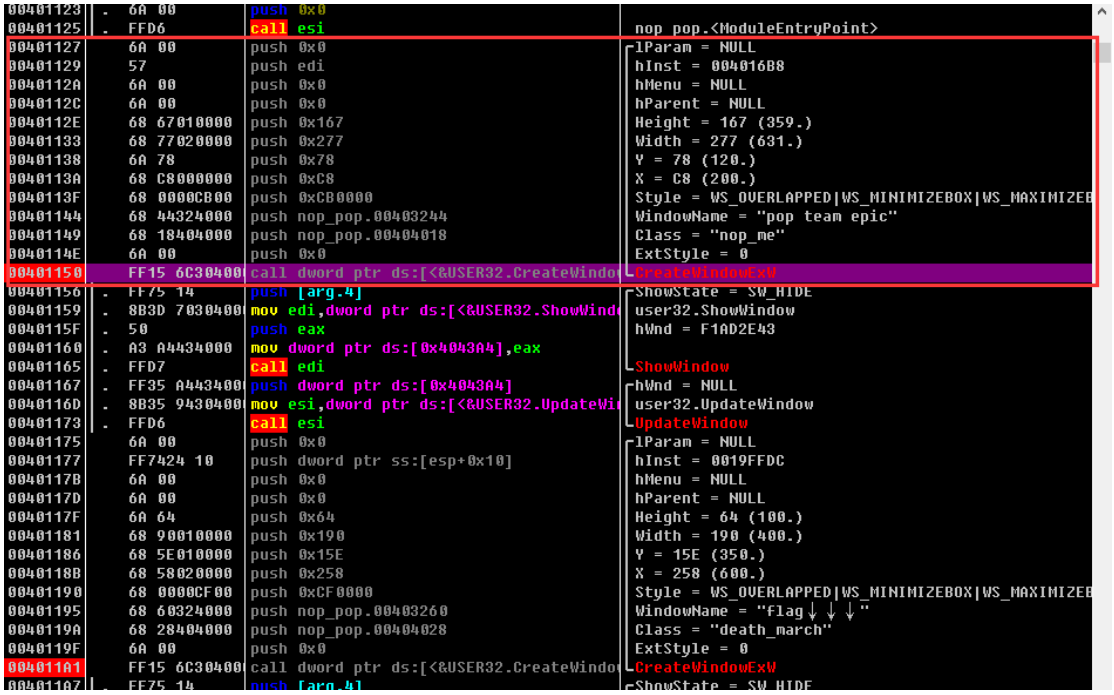
发现 flag

0x02 nop_pop

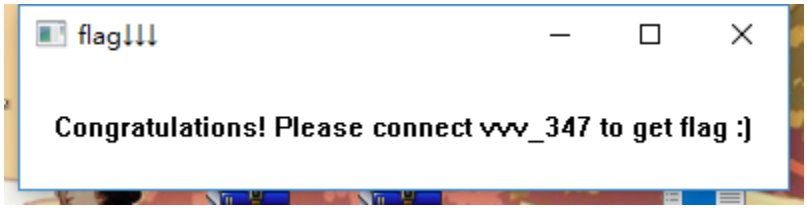
用 OD 打开，

地址	反汇编	注释
00401150	call dword ptr ds:[<&USER32.CreateWindo	user32.CreateWindowExW
004011A1	call dword ptr ds:[<&USER32.CreateWindo	user32.CreateWindowExW

查找到 2 处调用 CreateWindowExW 的地方，打断点调试



红框中为生成 pop 子窗口的代码，用 nop 指令覆盖后运行得到



联系 vvv_347 后获得 flag: hctf{Far5we1L_G0od_Cr4cker}

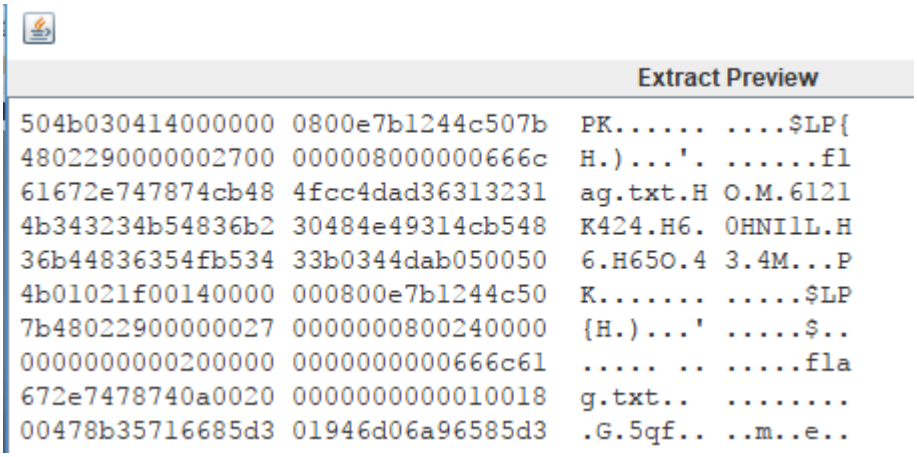
Misc 部分

0x01 白菜 1 提示：图片隐写 lsb

下载下来以后是一个 png 图片，用 binwalk 分析发现隐藏了压缩文件

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 1080 x 1920, 8-bit/color RGB, non-interlaced
41            0x29            Zlib compressed data, default compression
```

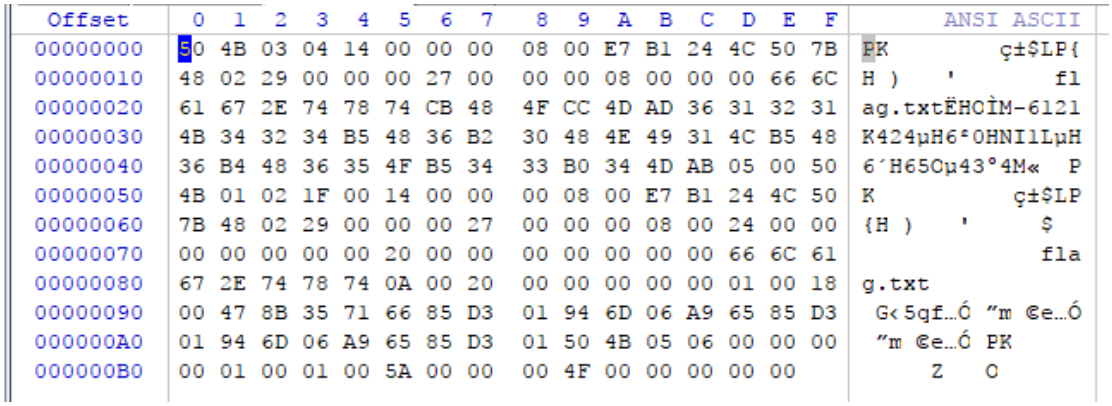
根据提示用 Stegsolve 分析在 0 位发现压缩文件



Extract Preview

```
504b030414000000 0800e7b1244c507b  PK...... ....$LP{
4802290000002700 000008000000666c  H.)...'. ......fl
61672e747874cb48 4fcc4dad36313231  ag.txt.H O.M.6121
4b343234b54836b2 30484e49314cb548  K424.H6. 0HNI1L.H
36b44836354fb534 33b0344dab050050  6.H65O.4 3.4M...P
4b01021f00140000 000800e7b1244c50  K....... .....$LP
7b48022900000027 0000000800240000  {H.)...' .....$..
0000000000200000 0000000000666c61  ..... .. .....fla
672e7478740a0020 0000000000010018  g.txt..  ........
00478b35716685d3 01946d06a96585d3  .G.5qf.. ..m..e..
```

保存后打开发现 flag.txt，打开提示压缩文件损坏，用 winhex 提取文件头到注释结束的部分

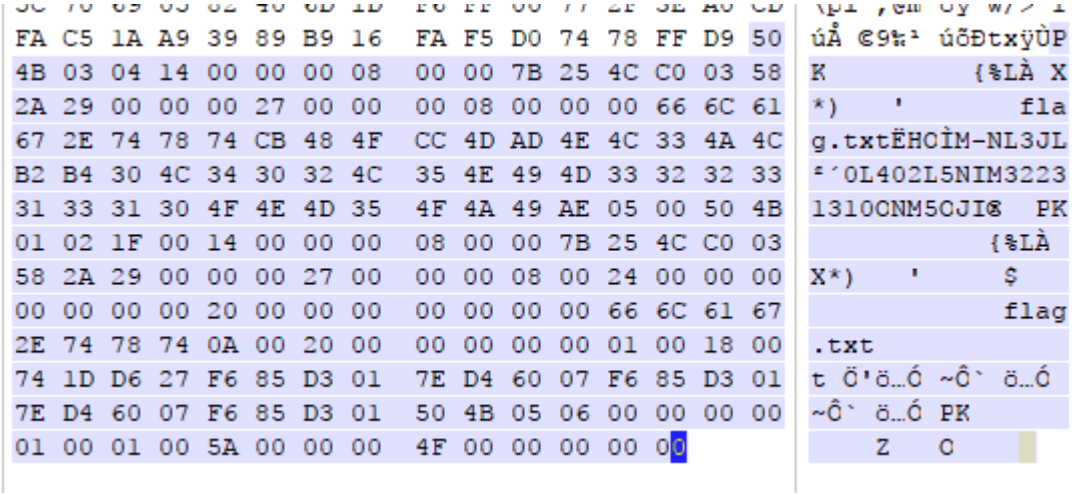


Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	50	4B	03	04	14	00	00	00	08	00	E7	B1	24	4C	50	7B	PK ç±$LP{
00000010	48	02	29	00	00	00	27	00	00	00	08	00	00	00	66	6C	H) ' fl
00000020	61	67	2E	74	78	74	CB	48	4F	CC	4D	AD	36	31	32	31	ag.txtËHOÌM-6121
00000030	4B	34	32	34	B5	48	36	B2	30	48	4E	49	31	4C	B5	48	K424µH6²0HNI1LµH
00000040	36	B4	48	36	35	4F	B5	34	33	B0	34	4D	AB	05	00	50	6´H65Oµ43°4M« P
00000050	4B	01	02	1F	00	14	00	00	00	08	00	E7	B1	24	4C	50	K ç±$LP
00000060	7B	48	02	29	00	00	00	27	00	00	00	08	00	24	00	00	{H) ' $
00000070	00	00	00	00	00	20	00	00	00	00	00	00	00	66	6C	61	fla
00000080	67	2E	74	78	74	0A	00	20	00	00	00	00	00	01	00	18	g.txt
00000090	00	47	8B	35	71	66	85	D3	01	94	6D	06	A9	65	85	D3	G‹5qf…Ó ”m ©e…Ó
000000A0	01	94	6D	06	A9	65	85	D3	01	50	4B	05	06	00	00	00	”m ©e…Ó PK
000000B0	00	01	00	01	00	5A	00	00	00	4F	00	00	00	00	00		Z O

保存后打开，得到 flag：hgame{4246a2158c280cdd1e8c18c57e96095f}

0x02 白菜 2

用 winhex 打开后发现压缩文件



```
FA C5 1A A9 39 89 B9 16  FA F5 D0 74 78 FF D9 50  úÅ ©9‰¹ úõÐtxÿÙP
4B 03 04 14 00 00 00 08  00 00 7B 25 4C C0 03 58  K         {%LÀ X
2A 29 00 00 00 27 00 00  00 08 00 00 00 66 6C 61  *)   '       fla
67 2E 74 78 74 CB 48 4F  CC 4D AD 4E 4C 33 4A 4C  g.txtËHOÌM-NL3JL
B2 B4 30 4C 34 30 32 4C  35 4E 49 4D 33 32 32 33  ²´0L402L5NIM3223
31 33 31 30 4F 4E 4D 35  4F 4A 49 AE 05 00 50 4B  1310ONM5OJI®  PK
01 02 1F 00 14 00 00 00  08 00 00 7B 25 4C C0 03  {%LÀ
58 2A 29 00 00 00 27 00  00 00 08 00 24 00 00 00  X*)   '     $
00 00 00 00 20 00 00 00  00 00 00 00 66 6C 61 67  flag
2E 74 78 74 0A 00 20 00  00 00 00 00 01 00 18 00  .txt
74 1D D6 27 F6 85 D3 01  7E D4 60 07 F6 85 D3 01  t Ö'ö…Ó ~Ô` ö…Ó
7E D4 60 07 F6 85 D3 01  50 4B 05 06 00 00 00 00  ~Ô` ö…Ó PK
01 00 01 00 5A 00 00 00  4F 00 00 00 00 00        Z   O
```

将文件后缀改为 zip 打开得到 flag：hgame{af2ab981a021e3def22646407cee7bdc}

Crypto 部分

0x01 easy Ceasar

由题得为凯撒密码，在字母偏移+14，数字偏移+3 得到
flag:hgame{The_qu1ck_br0wn_4x_jUmps_ovEr_a_La2y_dOg}

0x02 Polybius

由题得为棋盘密码，解出后得到 flag:hgame{fritz_nebel_invented_it}

0x03 Hill

由题得为希尔密码，解出后加上格式得到 flag:hgame{overthehillx}

0x04 confusion

摩斯密码解码后得到
MRLTK6KXNVZXQWBSNA2FSU2GGBSW45BSLAZFU6SVJBNDAZSRHU6Q====，用 Base32 解密后得到一串 Base64 dW5yWmsxX2h4YSF0ent2X2ZzUHZ0fQ==，解出来得到 unrZk1_hxa!tz{v_fsPvt}，感觉像是栅栏密码，尝试解出后得到 utnzr{Zvk_1f_shPxvat!}，凯撒加密解出后在偏移+13 得到 flag: hgame{Mix_1s_fuCking!}