

HGAME 2023 Week1 writeup by P34K

HGAME 2023 Week1 writeup by P34K

MISC

Sign In

e99p1ant_want_girlfriend

神秘的海报

Web

Classic Childhood Game

Become A Member

REVERSE

test your IDA

PWN

test_nc

MISC

Sign In

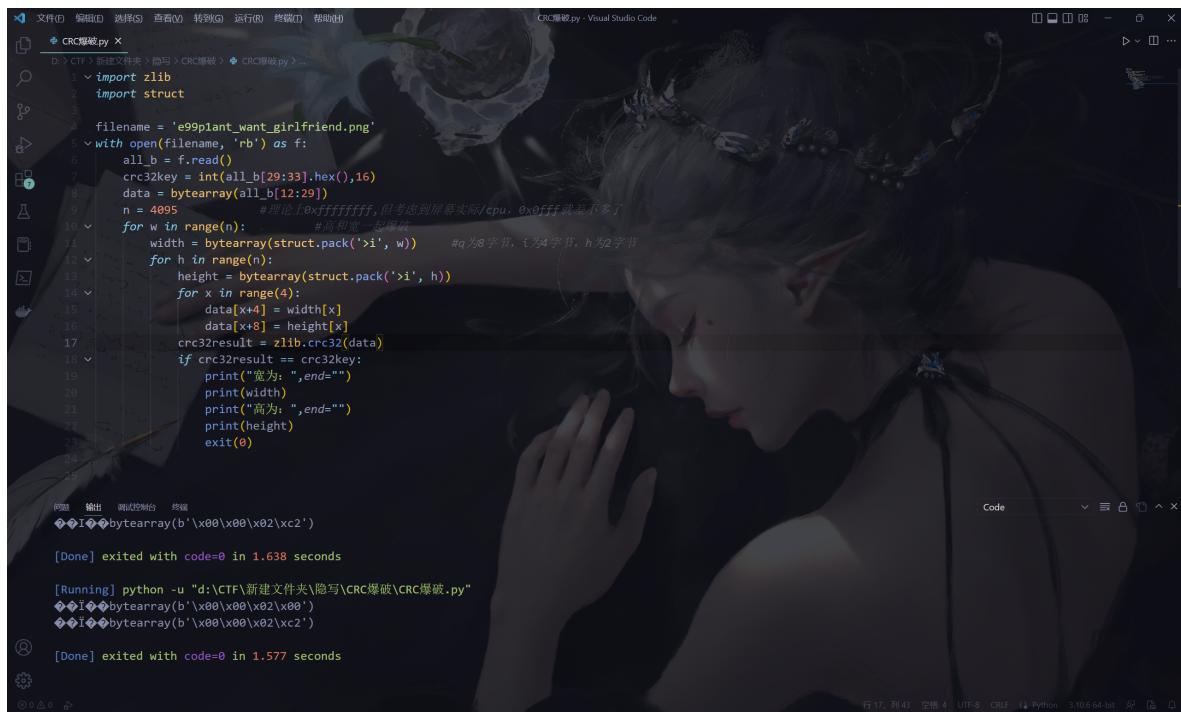
直接base64解码

flag: hgame{we1come_To_HGAME2023!}

e99p1ant_want_girlfriend

题目提示: CRC校验不对

于是脚本爆破一下



```
#!/usr/bin/python
# 导入 zlib 库
import zlib
# 导入 struct 库
import struct

# 定义文件名
filename = 'e99p1ant_want_girlfriend.png'
# 打开文件
with open(filename, 'rb') as f:
    # 读取所有字节
    all_b = f.read()
# 将所有字节转换为 hex 格式
all_b_hex = hex(all_b)
# 将 hex 格式转换为字节
all_b_hex_bytes = bytes.fromhex(all_b_hex)
# 计算 CRC32 值
crc32key = int(all_b_hex[29:33].hex(), 16)

# 定义宽度范围
width = 1
n = 4095
for w in range(n):
    # 将宽度转换为字节
    width_hex = hex(struct.pack('>I', w))
    # 将宽度转换为字节
    width_hex_bytes = bytes.fromhex(width_hex[2:6])
    # 将所有字节和宽度字节组合成一个字节流
    data = all_b_hex_bytes + width_hex_bytes
    # 计算 CRC32 值
    crc32result = zlib.crc32(data)
    # 检查 CRC32 值是否与目标值匹配
    if crc32result == crc32key:
        print("找到宽度: ", end="")
        print(width)
        print("找到高度: ", end="")
        print(hex(struct.pack('>I', width)))
        exit(0)
```

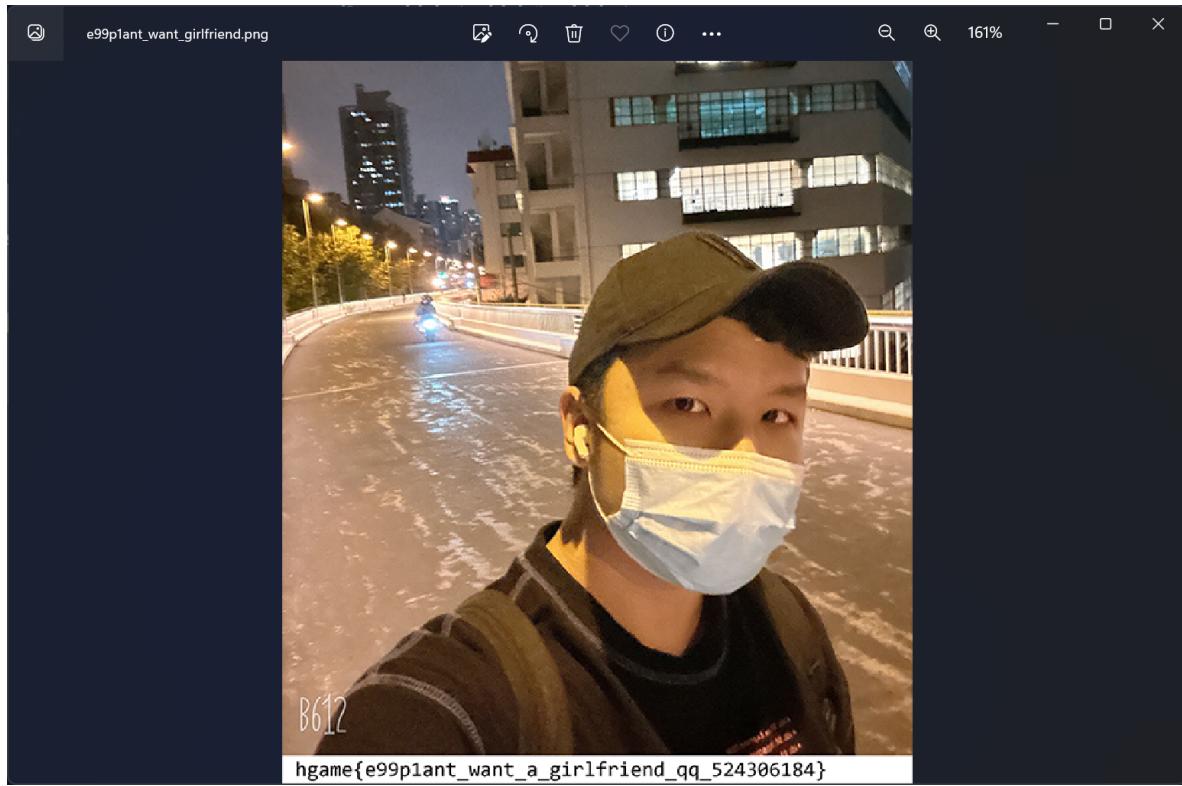
得到长&宽

再在WinHex里改相关内容

WinHex - [e99p1ant_want_girlfriend.png]

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII	UTF-8
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG	IHDR	□ □ □ □ □
00000016	00	00	04	00	00	00	02	02	08	06	00	00	00	A8	58	6B	A	"Xk	□□□□□□□
00000032	45	00	00	00	09	70	48	59	73	00	00	0B	13	00	00	0B	E	pHys	□□□□□
00000048	13	01	00	9A	9C	18	00	00	0A	4D	69	43	43	50	50	68	šæ	MiCCPPh	□□□□□
00000064	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66	otoshop	ICC prof	□ MiCCPPh
00000080	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	DF	ile	xÚ SwX"÷>ß	otoshop ICC prof
00000096	F7	65	0F	56	42	D8	F0	B1	97	6C	81	00	22	23	AC	08	÷e	VBØði-l "#¬	ile□□xø SwX□
00000112	C8	10	59	A2	10	92	00	61	84	10	12	40	C5	85	88	0A	È Y¢ ' a,,	ØÅ...^	VB □ □ □
00000128	56	14	15	11	9C	48	55	C4	82	D5	0A	48	9D	88	E2	A0	V	œHUÄ,Ö H ^å	Y□ a□ N□
00000144	28	B8	67	41	8A	88	5A	8B	55	5C	38	EE	1F	DC	A7	B5	(,gåŠ^Z<U\8i ÜŞu	(□ □ \8□	
00000160	7D	7A	EF	ED	ED	FB	D7	FB	BC	E7	9C	E7	FC	CE	79	CF	}ziiiu×û‡çœçüÙyÙ	□ □ □	
00000176	0F	80	11	12	26	91	E6	A2	6A	00	39	52	85	3C	3A	D8	€ & 'æçj	9R...<:Ø	□&□ Ø9R□
00000192	1F	8F	4F	48	C4	C9	BD	80	02	15	48	E0	04	20	10	E6	OHÆ‡€	Hà æ	□ □ □
00000208	CB	C2	67	05	C5	00	00	F0	03	79	78	7E	74	B0	3F	FC	ÈÂg Å ð	yx~t°?Ù	□□ □yx~t□
00000224	01	AF	6F	00	02	00	70	D5	2E	24	12	C7	E1	FF	83	BA	-o	põ.Ş Çáýf°	□ □ □
00000240	50	26	57	00	20	91	00	E0	22	12	E7	0B	01	90	52	00	P&W	' à" ç R	□ □ □ R□
00000256	C8	2E	54	C8	14	00	C8	18	00	B0	53	B3	64	0A	00	94	È.TÈ	È °S°d "	□ □ □ S□
00000272	00	00	6C	79	7C	42	22	00	AA	0D	00	EC	F4	49	3E	05	ly B"	^ iôI>	y B"□□
00000288	00	D8	A9	93	DC	17	00	D8	A2	1C	A9	08	00	8D	01	00	æ"Ù	øç c	□ ñ □ ï □ □

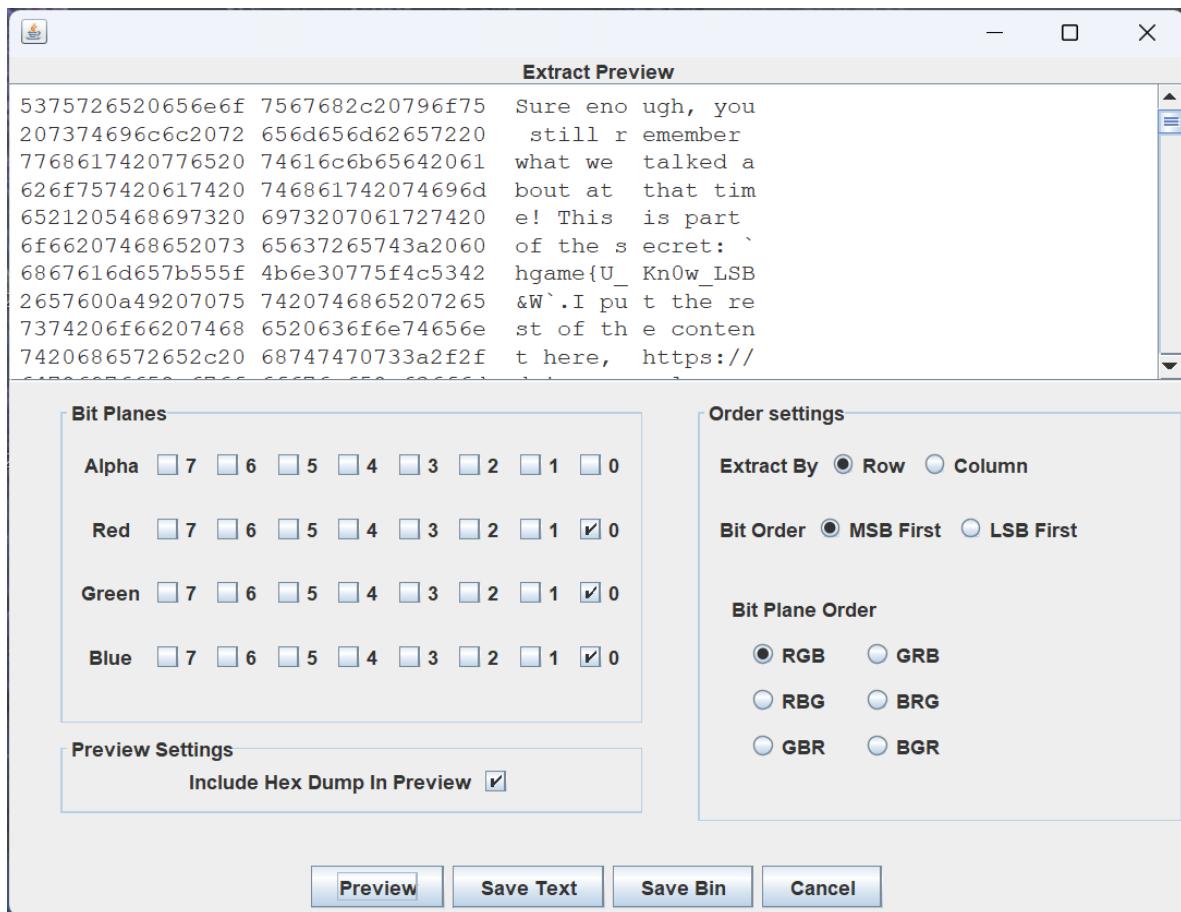
得到flag



flag: hgame{e99p1ant_want_a_girlfriend_qq_524306184}

神秘的海报

丢进Stegsolve



有一半flag，另一半要科学上网才能得到

下载是一个wav文件，有提示是**StegHide**,密码是6位数

(试了一次就对了，有点离谱，XD)



flag: hgame{U_Kn0w LSB&Wav^Mp3_Stego}

Web

Classic Childhood Game

提示：纯前端

于是查看js代码

发现 Events.js 里都是对话之类，猜测 flag 在其中

翻到最后，发现奇怪的一串

```
\x59\x55\x64\x6b\x61\x47\x4a\x58\x56\x6a\x64\x61\x62\x46\x5a\x31\x59\x6d\x35\x73
\x53\x31\x6c\x59\x57\x6d\x68\x6a\x4d\x6b\x35\x35\x59\x56\x68\x43\x4d\x45\x70\x72
\x57\x6a\x46\x69\x62\x54\x55\x31\x56\x46\x52\x43\x4d\x46\x6c\x56\x59\x7a\x42\x69
\x56\x31\x59\x35
```

明显是16进制，然后再来两次base64

The screenshot shows the Hex2Base64 tool interface. The 'Input' field contains a large hex string: \x59\x55\x64\x6b\x61\x47\x4a\x58\x56\x6a\x64\x61\x62\x46\x5a\x31\x59\x6d\x35\x73\x53\x31\x6c\x59\x57\x6d\x68\x6a\x4d\x6b\x35\x35\x59\x56\x68\x43\x4d\x45\x70\x72\x57\x6a\x46\x69\x62\x54\x55\x31\x56\x46\x6c\x56\x59\x7a\x42\x69\x56\x31\x59\x35. The 'From Hex' section is selected. The 'Output' field shows the result of the first base64 decoding: hgame{fUnnyJavascript&FunnyM0taG4me}. The 'From Base64' section is selected.

flag: hgame{fUnnyJavascript&FunnyM0taG4me}

Become A Member

打开后页面提示身份应该是Cute-Bunny



Powered By Vidar Engine | Go 1.19

BurpSuite抓包

将User-Agent内容改为 Cute-Bunny



每一个能够成为会员的顾客们都应该持有名为Vidar的邀请码 (code)

Powered By Vidar Engine | Go 1.19

提示code参数应该是 Vidar，发现响应头里的set-cookie里有code

Request

```
1 GET / HTTP/1.1
2 Host: week-1.hgame.lwsec.cn:32518
3 Pragma: no-cache
4 Cache-Control: no-cache
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Cute-Bunny
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9
10 Connection: close
11
12 |
```

Response

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Set-Cookie: code=guest; Path=/; Domain=localhost; Max-Age=3600;
HttpOnly
4 Date: Fri, 13 Jan 2023 06:25:37 GMT
5 Connection: close
6 Content-Length: 2175
7
8 <html lang="en">
9   <head>
10    <link rel="stylesheet" type="text/css" href="./static/styles.css">
11   <title>
12     Become A Member
13   </title>
14   <body>
15    <div class="wrap">
16      <div class="left">
17        <div class="header">
18          <div class="inner-header flex">
19            <svg version="1.1" class="logo" baseProfile="tiny" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox="0 0 500 500" xml:space="preserve">
20              <path fill="#FFFFFF" stroke="#000000" stroke-width="10" stroke-miterlimit="10" d="M57.283" />
21            <g>
22              <path fill="#ffff" d="M250.4,0.8C112.7,0.8,1.112.4,1.250.2c0,137.7,111.7,249.4,249.4,249.4c137.7,0.249.4-111.7,249.4-249.4C499.8,112.4,381.0,8.250.4,0.8z"/>
23              M383.8,326.3c-62.0-101.4,-117.6-46.3c-17.1-34.1-2.3-75.4,13.2-104.1
24              c-22.4,3-38.4,9.2-47.8,18.3c-11.2,10.9-13.6,26.7-16.2
25            </g>
26          </svg>
27        <div class="inner-header flex">
28          <div class="inner-header flex">
29            <div class="inner-header flex">
30              <div class="inner-header flex">
31                <div class="inner-header flex">
32                  <div class="inner-header flex">
33                    <div class="inner-header flex">
34                      <div class="inner-header flex">
35                        <div class="inner-header flex">
36                          <div class="inner-header flex">
37                            <div class="inner-header flex">
38                              <div class="inner-header flex">
39                                <div class="inner-header flex">
40                                  <div class="inner-header flex">
41                                    <div class="inner-header flex">
42                                      <div class="inner-header flex">
43                                        <div class="inner-header flex">
44                                          <div class="inner-header flex">
45                                            <div class="inner-header flex">
46                                              <div class="inner-header flex">
47                                                <div class="inner-header flex">
48                                                  <div class="inner-header flex">
49                                                    <div class="inner-header flex">
50                                                      <div class="inner-header flex">
51                                                        <div class="inner-header flex">
52                                                          <div class="inner-header flex">
53                                                            <div class="inner-header flex">
54                                                              <div class="inner-header flex">
55                                                                <div class="inner-header flex">
56                                                                  <div class="inner-header flex">
57                                                                    <div class="inner-header flex">
58                                                                      <div class="inner-header flex">
59                                                                        <div class="inner-header flex">
60                                                                          <div class="inner-header flex">
61                                                                            <div class="inner-header flex">
62                                                                              <div class="inner-header flex">
63                                                                                <div class="inner-header flex">
64                                                                                  <div class="inner-header flex">
65                                                                                    <div class="inner-header flex">
66                                                                                      <div class="inner-header flex">
67                        </div>
68                      </div>
69                    </div>
70                  </div>
71                </div>
72              </div>
73            </div>
74          </div>
75        </div>
76      </div>
77    </div>
78  </body>
79</html>
```

Inspector

Name	Value
Host	week-1.hgame.lwsec.cn:32518
Pragma	no-cache
Cache-Control	no-cache
Upgrade-Insecure-Requests	1
User-Agent	Cute-Bunny
Accept	text/html,application/...
Accept-Encoding	gzip, deflate
Accept-Language	zh-CN,zh;q=0.9
Connection	close

Response Headers

Name	Value
Set-Cookie	code=guest; Path=/; Domain=localhost; Max-Age=3600; HttpOnly
Date	Fri, 13 Jan 2023 06:25:37 GMT
Content-Length	2175

请求头里加一句 cookie: code=vidar



由于特殊原因，我们只接收来自于bunnybunnybunny.com的会员资格申请

Powered By Vidar Engine | Go 1.19

提示只能来自 **bunnybunnybunny.com**

于是请求头里加一句 `Referer: bunnybunnybunny.com`



就差最后一个本地的请求，就能拿到会员账号啦

Powered By Vidar Engine | Go 1.19

提示 **本地请求**

请求头里加一句 `X-Forwarded-For: 127.0.0.1`



username:luckytoday password:happy123 (请以json请求方式登陆)

Powered By Vidar Engine | Go 1.19

提示以 json请求 方式登录

于是请求加上 `{"username":"luckytoday", "password":"happy123"}`

```
1 GET / HTTP/1.1
2 Host: week-1.hgame.lwsec.cn:32518
3 Pragma: no-cache
4 Cache-Control: no-cache
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Cute-Bunny
7 Accept:
8   text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image/webp, image/apng, */*;q=0.8, application/signed-exchange;v=b3;q=0.9
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN, zh;q=0.9
11 Connection: close
12 cookie: code=Vidar
13 Referer: bunnybunnybunny.com
14 X-Forwarded-For: 127.0.0.1
15 Content-Length: 51
16 {
17   "username": "luckytoday",
18   "password": "happy123"
19 }
```

得到flag



hgame{H0w_ArE_Y0u_T0day?}

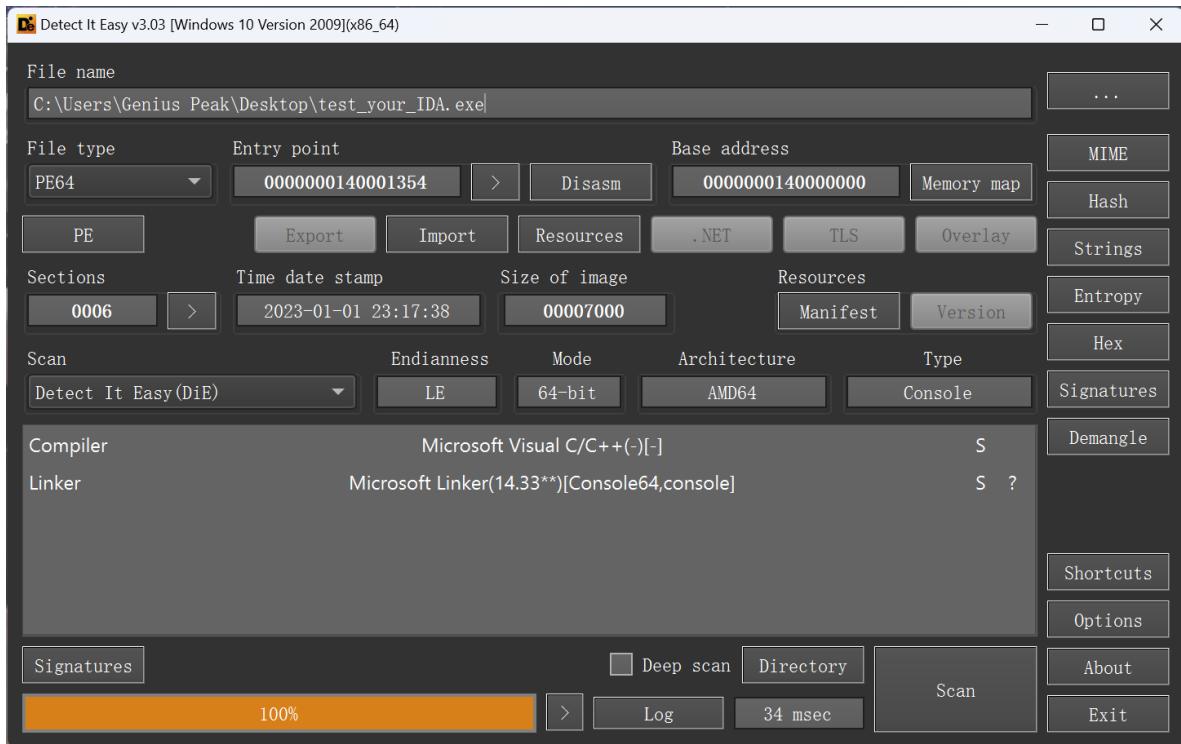
Powered By Vidar Engine | Go 1.19

flag: hgame{H0w_ArE_Y0u_T0day?}

REVERSE

test your IDA

附件拖进DIE



附件拖进64位IDA

```

.align 8
.rdata:0000000140002255 00 00 00
.rdata:0000000140002258 ; const char Str2[]
.rdata:0000000140002258 72 33 76 65 72 35 65 00 ; DATA XREF: main+15t0
.rdata:0000000140002260 ; const char Format[]
.rdata:0000000140002260 79 6F 75 72 20 66 6C 61 67 3A+Format db 'your flag:hgame{te5t_your_IDA}',0 ; DATA XREF: main+2Ato
.rdata:0000000140002260 68 67 61 6D 65 7B 74 65 35 74+ ; DATA XREF: main+2Ato
.rdata:000000014000227F 00 align 20h
.rdata:0000000140002280 65 78 70 61 6E 64 20 33 32 2D+aExpand32ByteK db 'expand 32-byte k',0
.rdata:0000000140002291 00 00 00 00 00 00 align 8
.rdata:0000000140002298 65 78 70 61 6E 64 20 31 36 2D+aExpand16ByteK db 'expand 16-byte k',0
.rdata:00000001400022A9 00 00 00 00 00 00 align 10h
.rdata:00000001400022B0 40 01 00 00 _load_config_used dd 140h ; Size
.rdata:00000001400022B4 00 00 00 00 dd 0 ; Time stamp
.rdata:00000001400022B8 00 00 00 00 dw 2 dup(0) ; Version: 0.0
.rdata:00000001400022BC 00 00 00 dd 0 ; GlobalFlagsClear
.rdata:00000001400022C0 00 00 00 dd 0 ; GlobalFlagsSet
.rdata:00000001400022C4 00 00 00 dd 0 ; CriticalSectionDefaultTimeout
.rdata:00000001400022C8 00 00 00 00 00 00 00 00 dq 0 ; DeCommitFreeBlockThreshold
.rdata:00000001400022D0 00 00 00 00 00 00 00 00 dq 0 ; DeCommitTotalFreeThreshold
.rdata:00000001400022D8 00 00 00 00 00 00 00 00 dq 0 ; LockPrefixTable
.rdata:00000001400022E0 00 00 00 00 00 00 00 00 dq 0 ; MaximumAllocationSize
.rdata:00000001400022E8 00 00 00 00 00 00 00 00 dq 0 ; VirtualMemoryThreshold
.rdata:00000001400022F0 00 00 00 00 00 00 00 00 dq 0 ; ProcessAffinityMask
.rdata:00000001400022F8 00 00 00 00 00 00 00 00 dd 0 ; ProcessHeapFlags
.rdata:00000001400022FE 00 00 dw 0 ; CSDVersion
.rdata:0000000140002300 00 00 00 00 00 00 00 00 dw 0 ; Reserved1
.rdata:0000000140002308 28 30 00 40 01 00 00 00 dq 0 ; EditList
.rdata:0000000140002308 00 00 00 00 00 00 00 00 dq 0 ; SecurityCookie
.rdata:0000000140002310 00 00 00 00 00 00 00 00 dq 0 ; SEHandlerTable

```

flag: hgame{te5t_your_IDA}

PWN

test_nc

nc week-1.hgame.lwsec.cn 30952 连接，直接ls就出了

```

[(kali㉿kali)-~/Desktop]
$ nc week-1.hgame.lwsec.cn 30068
ls
bin
dev
flag
lib
lib32
lib64
vuln
cat flag
hgame{002484b315be9f81c99e1f8ffd960f14a127b65d}

```

flag: `hgame{002484b315be9f81c99e1f8ffd960f14a127b65d}`