HGAME 2023 Week1 writeup by P34K

MISC

Sign In

直接**base64**解码

flag: `hgame{Welcome_To_HGAME2023!}`

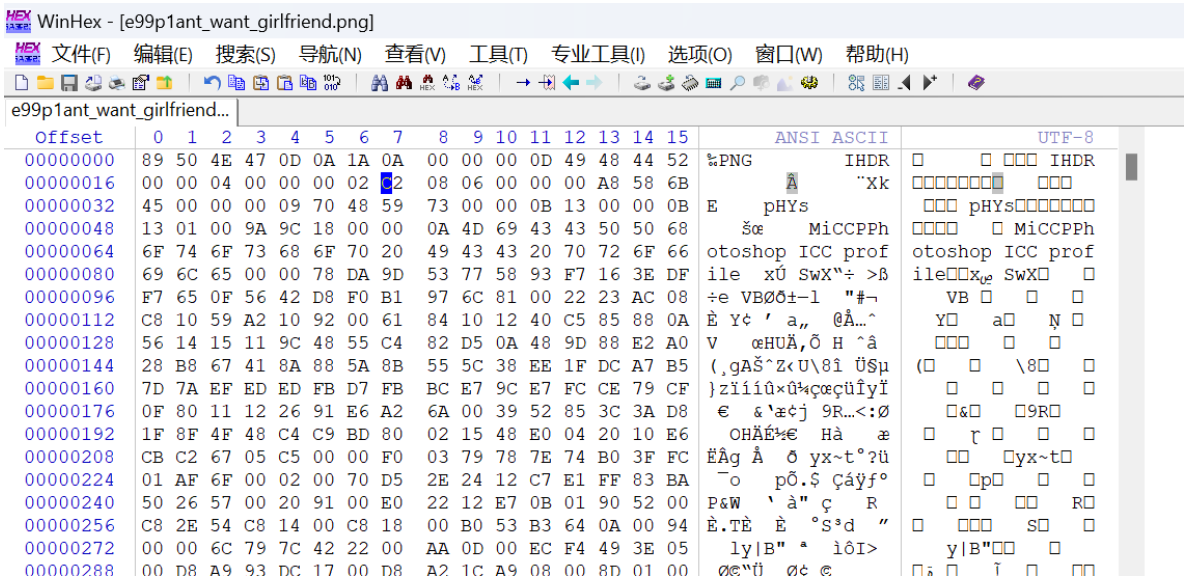
e99p1ant_want_girlfriend

题目提示：**CRC校验**不对

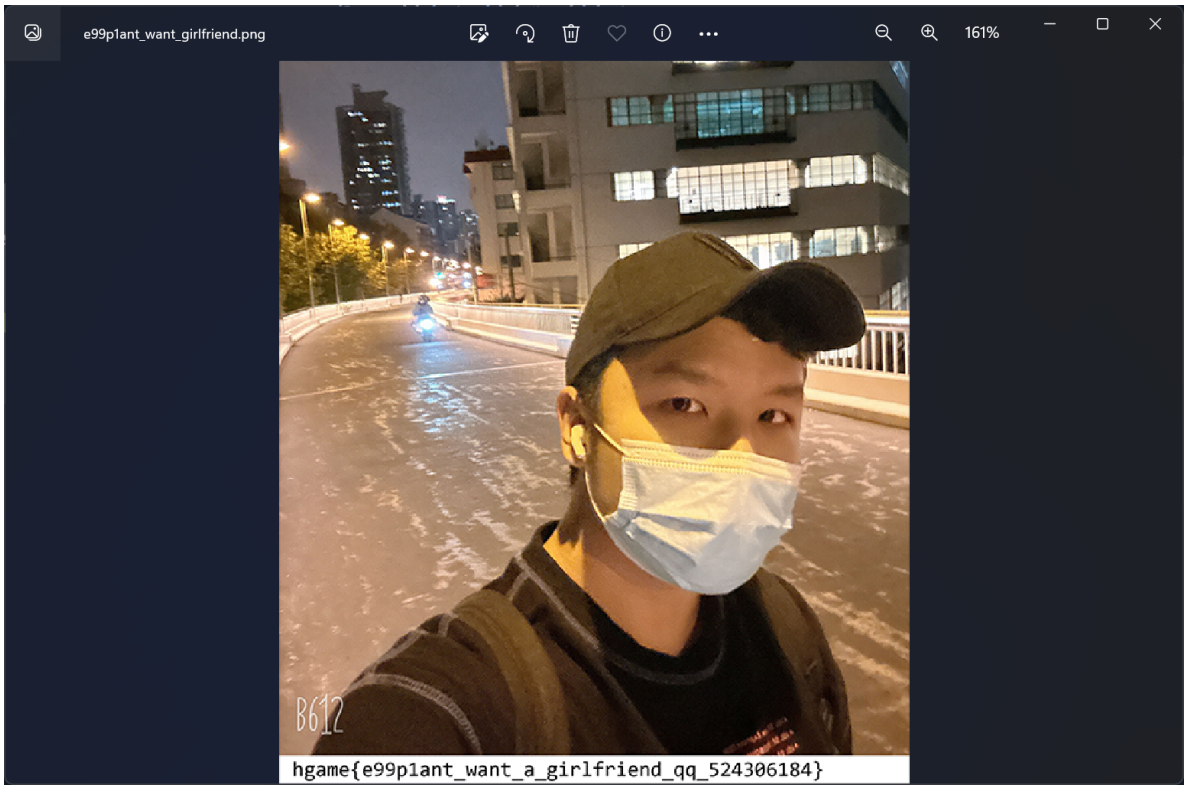
于是脚本爆破一下

得到长&宽

再在**WinHex**里改相关内容



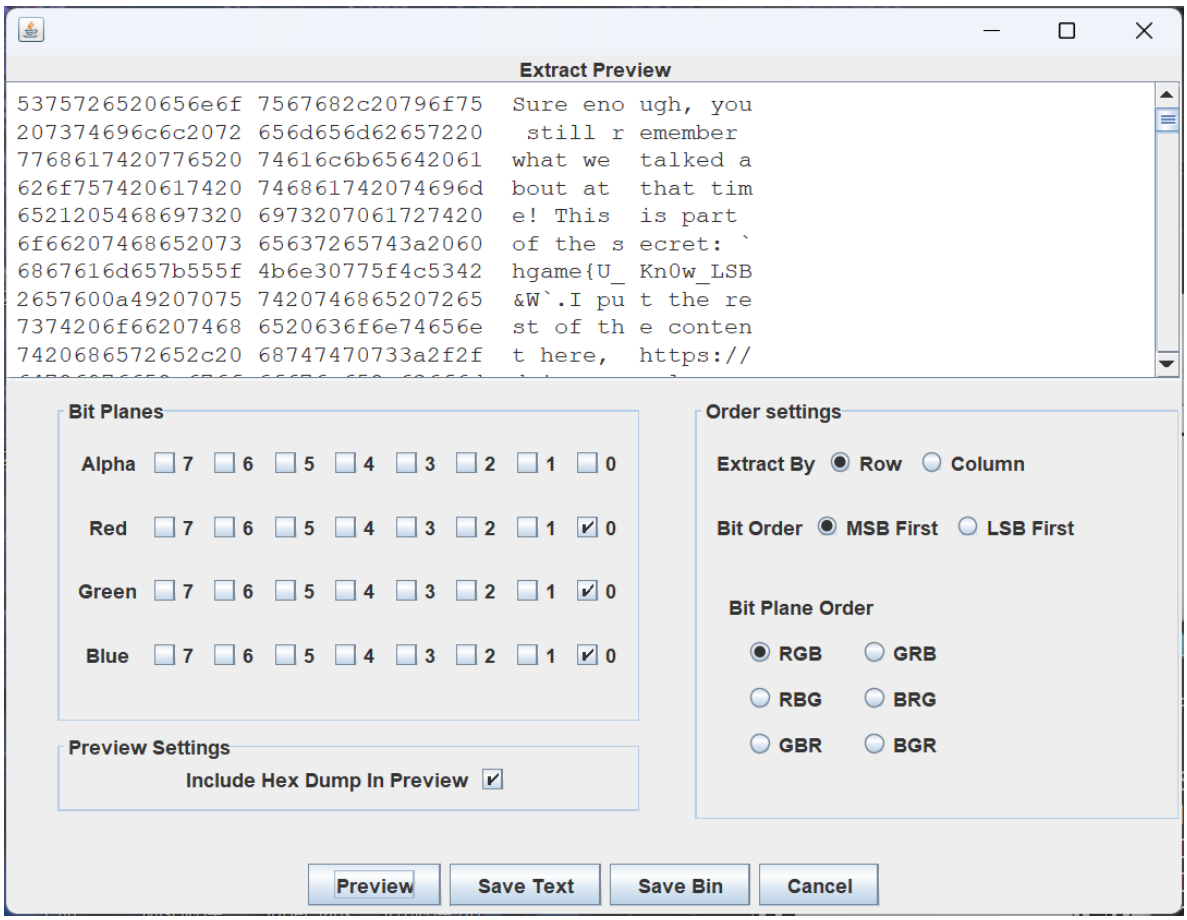
得到flag



flag: `hgame{e99p1ant_want_a_girlfriend_qq_524306184}`

神秘的海报

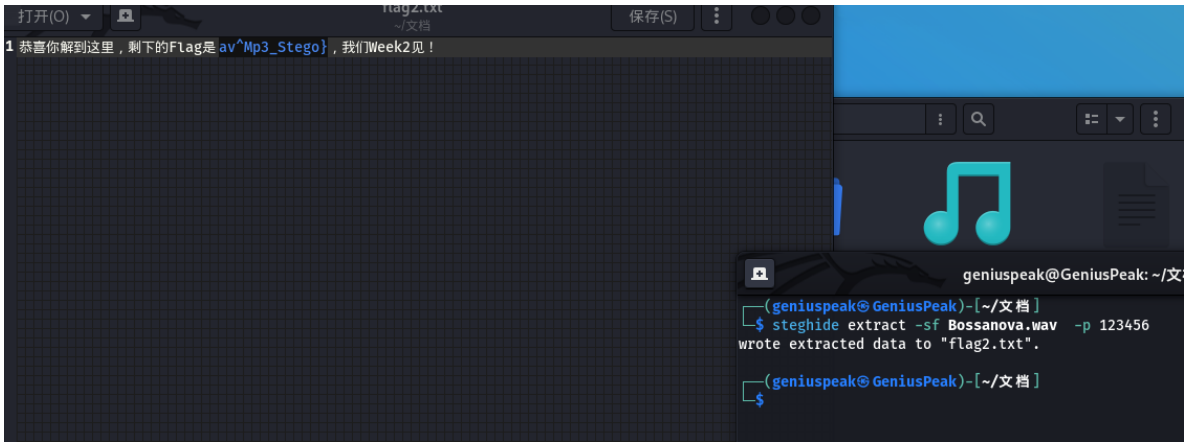
丢进**Stegsolve**



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

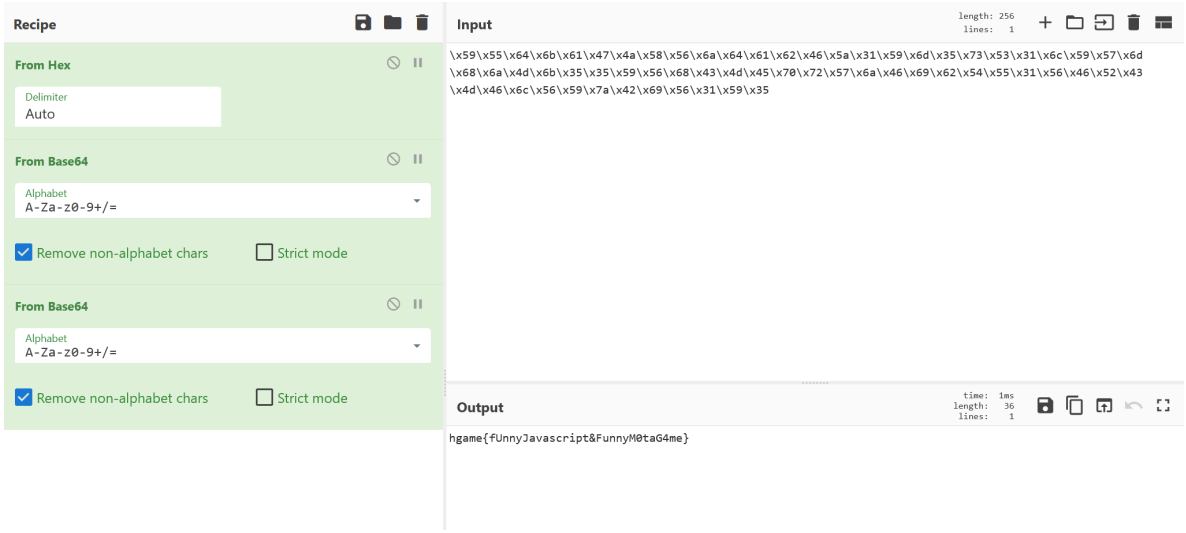
于是查看js代码

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



flag: `hgame{fUnnyJavascript&FunnyM0taG4me}`

Become A Member

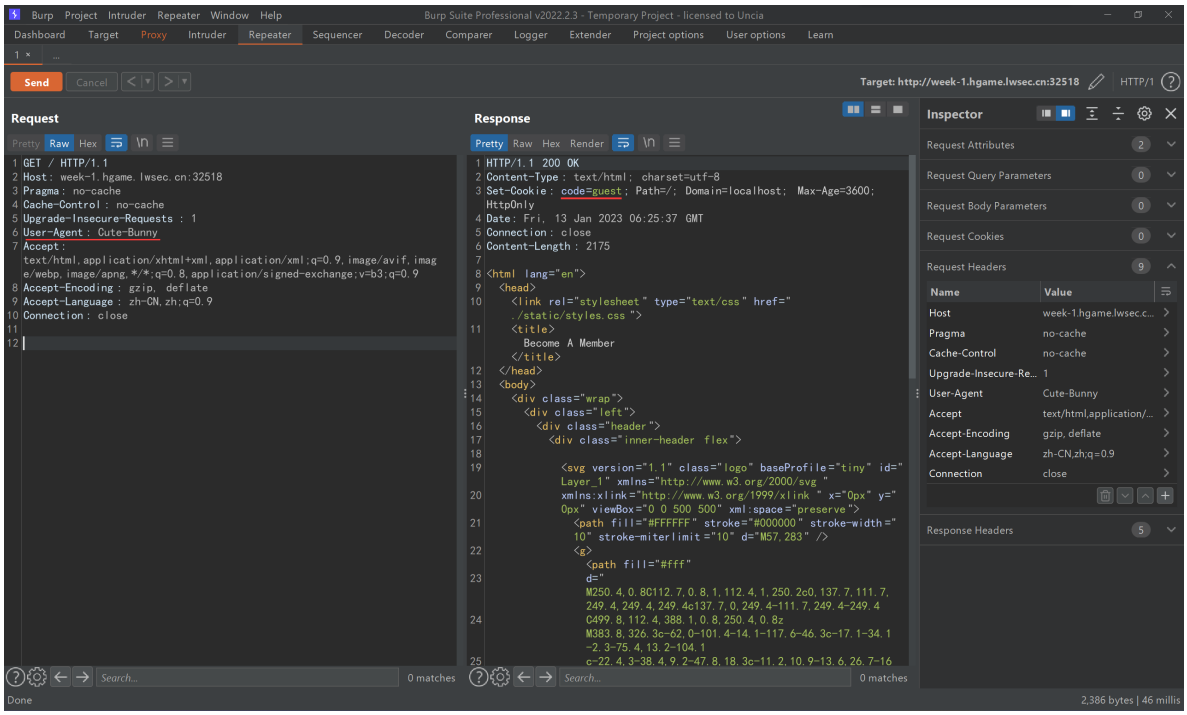
打开后页面提示身份应该是**Cute-Bunny**

BurpSuite抓包

将**User-Agent**内容改为 `Cute-Bunny`

Powered By Vidar Engine | Go 1.19

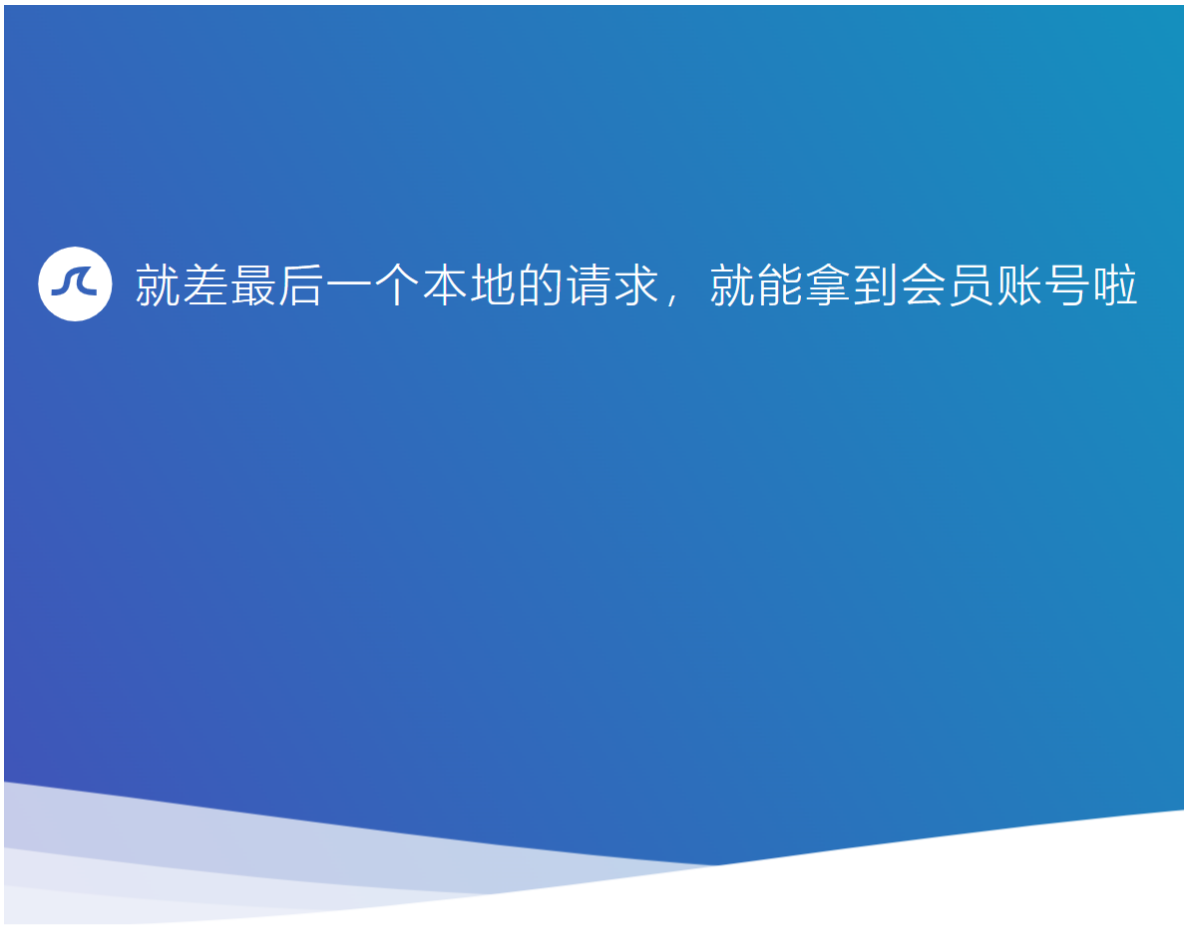
提示**code**参数应该是 **Vidar**，发现响应头里的**set-cookie**里有code



请求头里加一句 `cookie: code=Vidar`

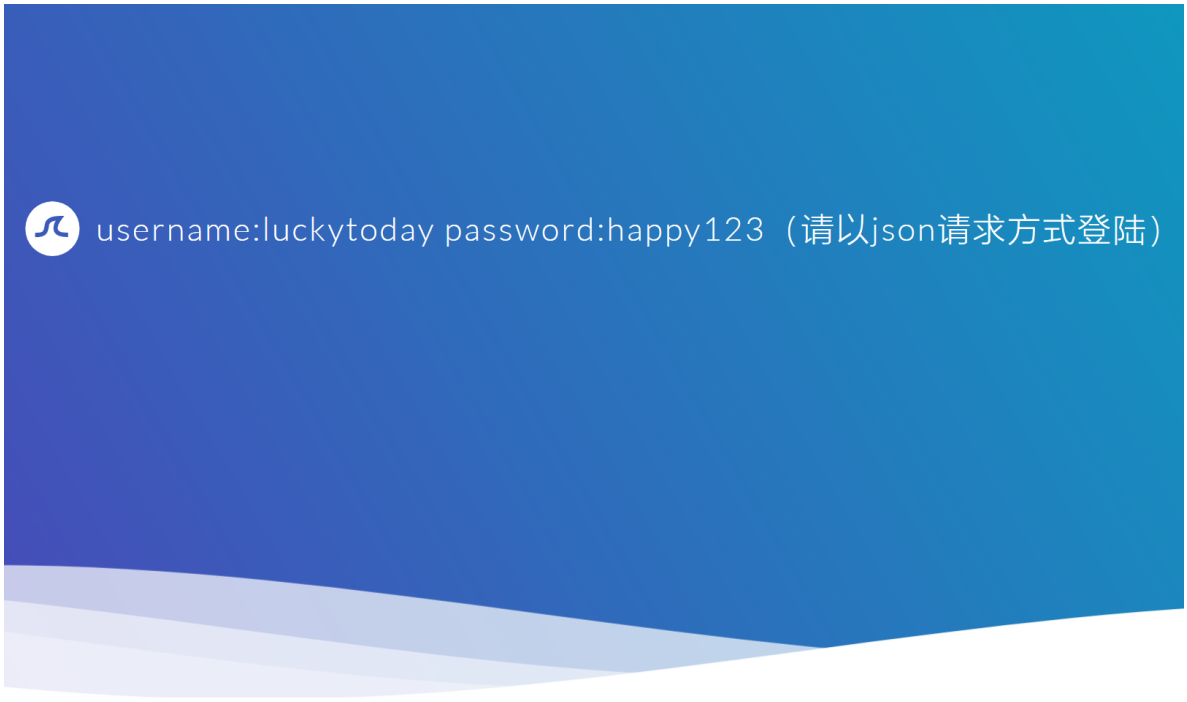
提示只能来自 **bunnybunnybunny.com**

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



提示 **本地请求**

请求头里加一句 `X-Forwarded-For: 127.0.0.1`



提示以 **json请求** 方式登录

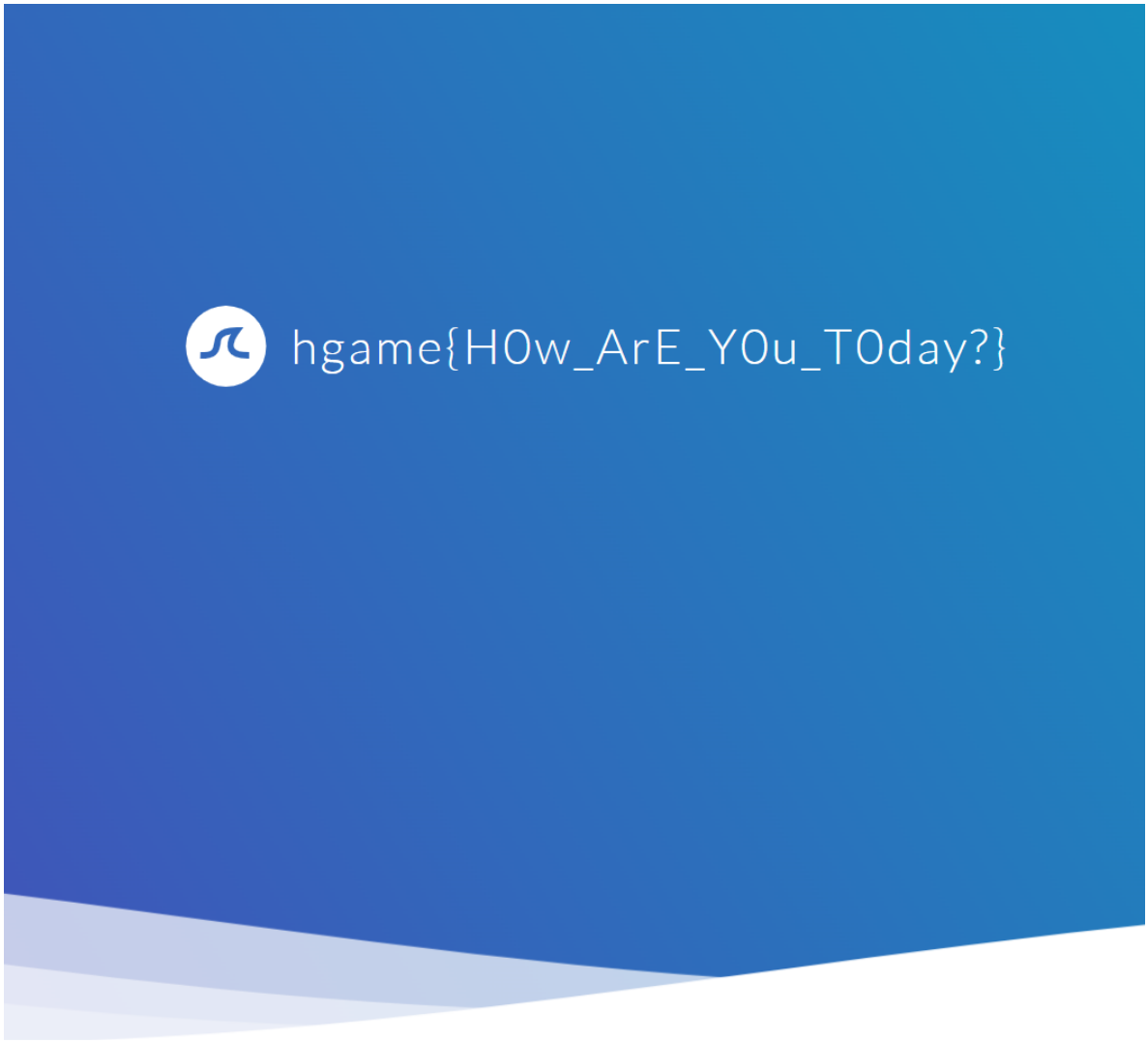
于是请求加上 `{"username":"luckytoday","password":"happy123"}`

```
GET / HTTP/1.1
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/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
cookie: code=Vidar
Referer: bunnybunnybunny.com
X-Forwarded-For: 127.0.0.1
Content-Length: 51

{
  "username":"luckytoday",
  "password":"happy123"
}

```

得到flag

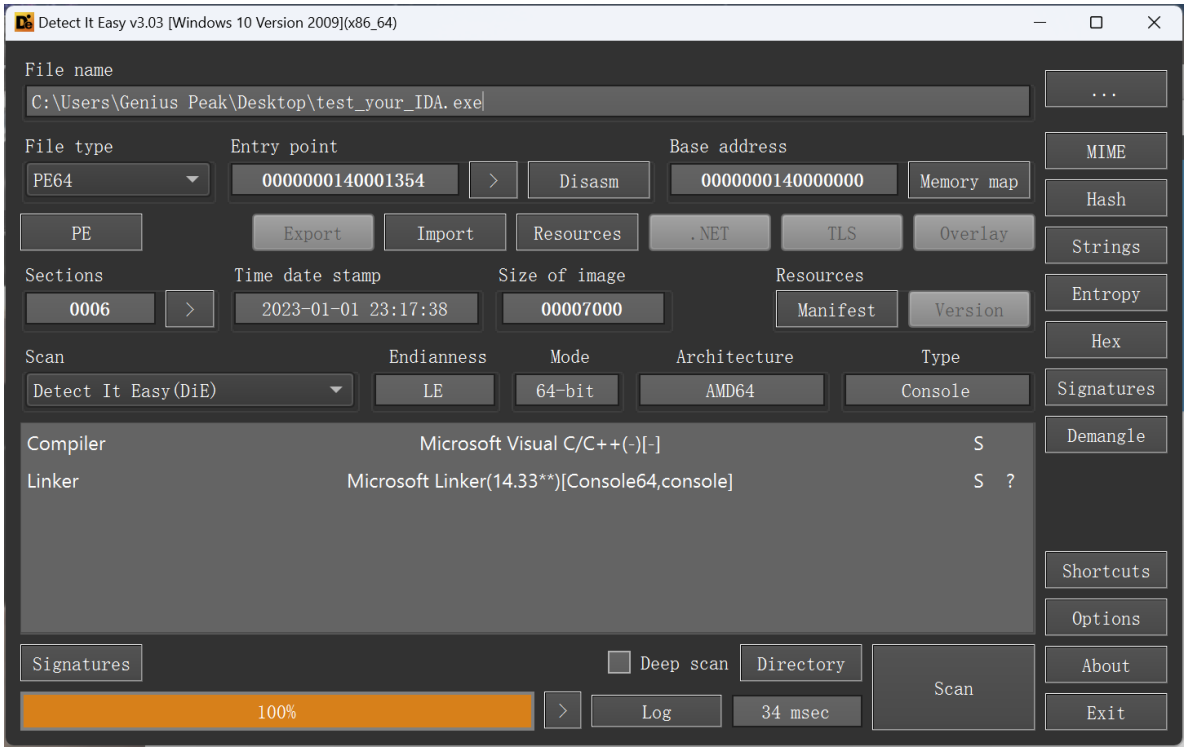


flag: `hgame{HOw_ArE_YOu_TOday?}`

REVERSE

test your IDA

附件拖进DIE



附件拖进64位IDA

```
.rdata:0000000140002255 00 00 00                    align 8
.rdata:0000000140002258                             ; const char Str2[]
.rdata:0000000140002258 72 33 76 65 72 35 65 00     Str2 db 'r3ver5e',0                 ; DATA XREF: main+15↑o
.rdata:0000000140002260                             ; const char Format[]
.rdata:0000000140002260 79 6F 75 72 20 66 6C 61 67 3A+Format db 'your flag:hgame{te5t_y0ur_IDA}',0
.rdata:0000000140002260 68 67 61 6D 65 7B 74 65 35 74+                              ; DATA XREF: main+2A↑o
.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 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 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 00                 dd 0                                ; GlobalFlagsClear
.rdata:00000001400022C0 00 00 00 00                 dd 0                                ; GlobalFlagsSet
.rdata:00000001400022C4 00 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                 dd 0                                ; ProcessHeapFlags
.rdata:00000001400022FC 00 00                       dw 0                                ; CSDVersion
.rdata:00000001400022FE 00 00                       dw 0                                ; Reserved1
.rdata:0000000140002300 00 00 00 00 00 00 00 00     dq 0                                ; EditList
.rdata:0000000140002308 28 30 00 40 01 00 00 00     dq offset __security_cookie         ; 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

flag: `hgame{OO2484b315be9f81c99e1f8ffd960f14a127b65d}`