

HGAME 2022 Week1 writeup by Serpentine Lin

[Misc.]

Sign in

将题目所给的

aGdhbWV7V2VsY29tZV9Ub19lR0FNRTlwMjMhfQ==

进行 Base64 解码得到 hgame{Welcome_To_HGAME2023!}

转换内容:

aGdhbWV7V2VsY29tZV9Ub19lR0FNRTlwMjMhfQ==

Base64编码

Base64解码

转换结果:

hgame{Welcome_To_HGAME2023!}

e99p1ant_want_girlfriend

因为 CRC 校验码错误, 可以猜想是图片宽高产生了变化,

在 010 Editor 上打开图片, (从 00 00 00 0D) 得知数据块长度为 13, (头文件 49 48 44 52) ,13 位的数据块信息 (00 00 02 00 / 00 00 02 A8 /A8 58 6B 45), 从中可知图片宽为 512, 高为 680, CRC 为 A8 58 6B 45。在 python 上使用以下代码进行宽高重新计算:

```
import os
import binascii
import struct
misc = open("egg.png","rb").read()

# 爆破宽
for i in range(1024):
    data = misc[12:16] + struct.pack('>i',i)+ misc[20:29] #IHDR 数据
    crc32 = binascii.crc32(data) & 0xA8 58 6B 45
    if crc32 == 0xA8586B45: #IHDR 块的 crc32 值
        print(i)
        print("hex:" + hex(i))

# 爆破高
for i in range(1024):
    data = misc[12:20] + struct.pack('>i',i)+ misc[24:29]
```

```
crc32 = binascii.crc32(data) & 0xA8 58 6B 45
```

```
if crc32 == 0xA8586B45:
```

```
    print(i)
```

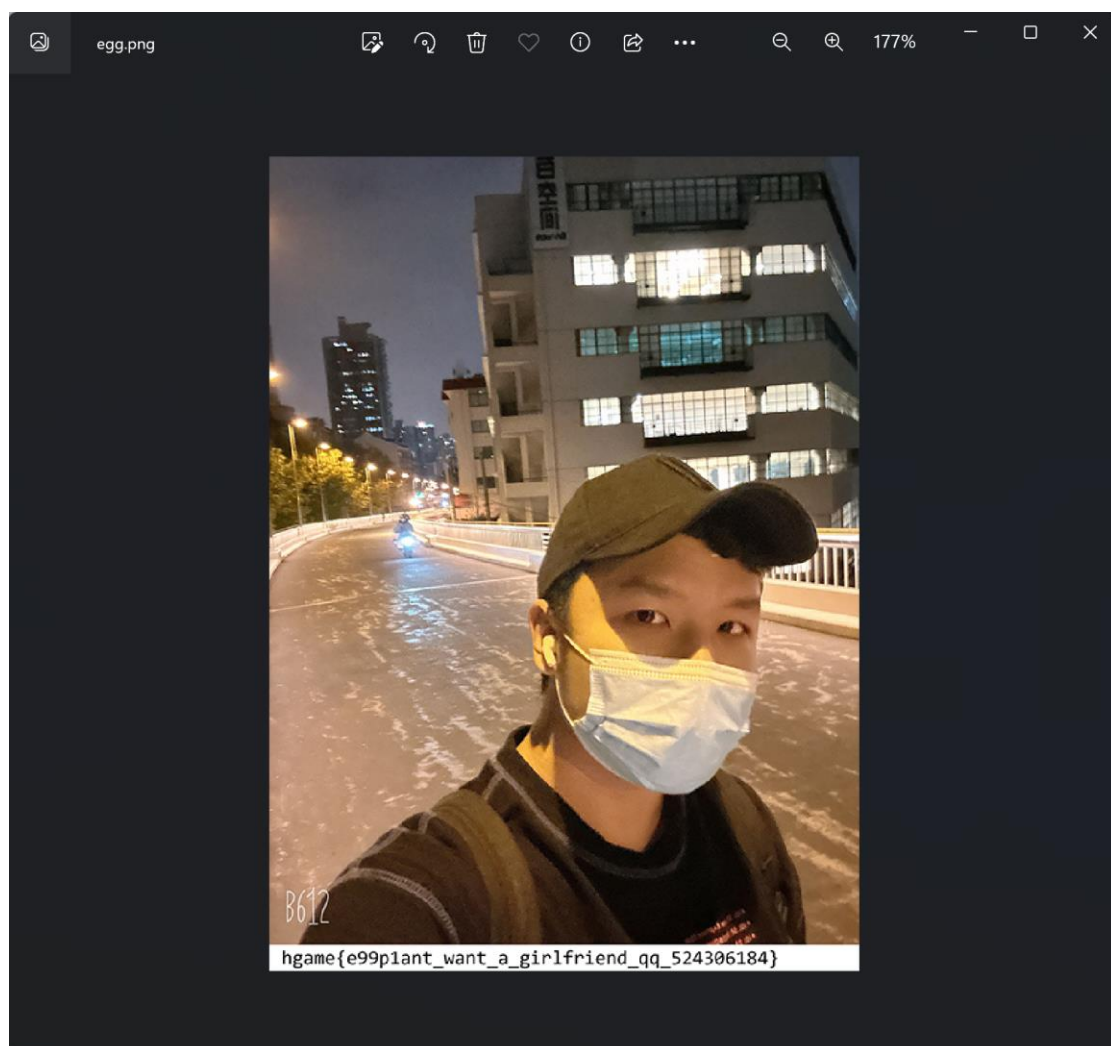
```
    print("hex:" + hex(i))
```

得到图片高的正确数据为 702，表示为 00 00 02 C2。

在 010 Editor 上将高的数据进行矫正

Startup	egg.png x																															
	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
0000h	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR															
0010h	00	00	02	00	00	00	02	C2	08	06	00	00	00	A8	58	6BÂ.....Xk															
0020h	45	00	00	00	09	70	48	59	73	00	00	0B	13	00	00	0B	E....pHYs.....															

可以得到如下图片：



得到 hgame{e99p1ant_want_a_girlfriend_qq_524306184}