

HGAME 2022 Week1 writeup by Halo

HGAME 2022 Week1 writeup by Halo

MISC

奇妙小游戏

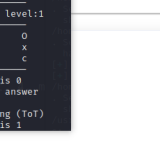
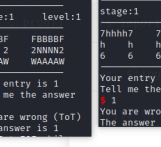
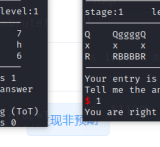
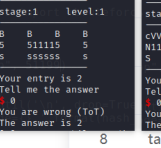
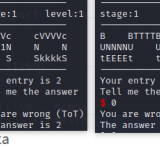
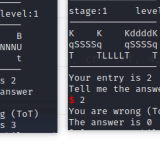
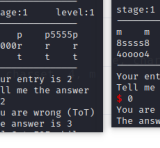
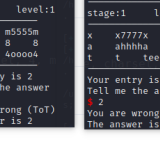
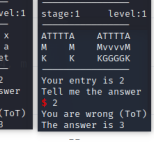
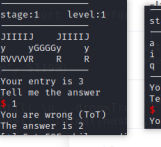
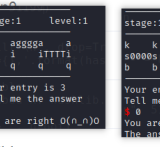
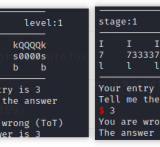
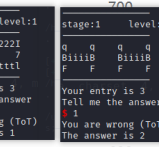
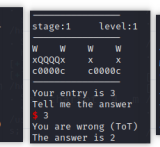
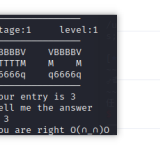
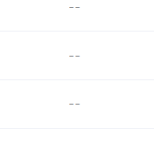
你上当了 我的很大

一张怪怪的名片

MISC

奇妙小游戏

用提供的python脚本，开始游戏。多轮游戏后，收集了一些题目和对应答案

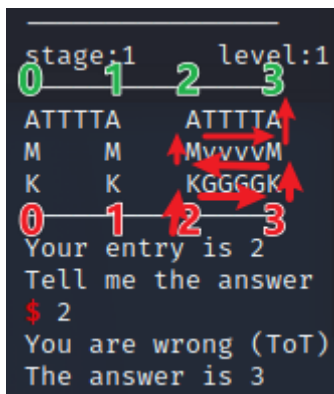
					其他			
1	t0hka		1750		--			
					--			
5	nerowander		900		--			
								--
8	taka		750		--			
								--

观察并猜测，游戏题目与出现什么字符无关，仅与是否出现字符有关。

根据 entry 为0至3，猜测以纵向的四条为入口，分别为0至3。

再观察了半天后，发现纵向的任意位置的字母，不会左右同时出现字母。经一番推理验证后，得到游戏规则如下：

路径游戏。以下方为对应入口，向上走。若遇左/右出现字母，则向对应方向走一步。如下：



得到规则后，借助辅助标记出入口列数，尝试了两三次成功通关

```

      HtttH      HtttH      HtttH      H      HtttH      H      HtttH      H
      11111      11111      1 1      11111      11111      11111      1

Your entry is 6
Tell me the answer
$ 7
You are right 0(n_n)0

stage:5      level:5

PKKKKP      P      PKKKKP      PKKKKP      P      PKKKKP      PKKKKP      P
n      nxxxxn      n      n      n      nxxxxn      n      nxxxxn      nxxxxn
KeeeeK      KeeeeK      K      K      K      KeeeeK      K      KeeeeK      K
M      MPPPPM      MPPPPM      M      M      M      MPPPPM      MPPPPM      MPPPPM
s      s      s      s      s0000s      s      s      s      s      s0000s      s
fggggf      fggggf      fggggf      fggggf      f      fggggf      fggggf      fggggf
r0000r      r      r0000r      r      r      r0000r      r      r0000r      r
j      j      j      j      jPPPPj      j      jPPPPj      j      jPPPPj      j
3xxxx3      3xxxx3

u      uDDDDu      uDDDD      stage:4      level:1
P      P0000P      P      0      1      2      3      4      5      6      7      8      9      10
N      NWWWN      NWWWN      N      N      N      N      NWWWN      N      N
7ZZZZ7      7ZZZZ7      7ZZZZ7      7      7      7ZZZZ7      7      7      7      7
svvvvs      svvvvs      svvvvs      s      s      svvvvs      svvvvs      s

Your entry is 1
Tell me the answer
$ 0
You are right 0(n_n)0
you win!here is your reward
hgame{WHAT_@_InterEstIng-GAME}
[*] Got EOF while reading in interactive
$
[*] Interrupted
[*] Closed connection to chuj.top port 51199

```

你上当了 我的很大

打开压缩包，发现为压缩包层层嵌套。利用脚本一层层全部解压。

```

import zipfile
import os
import sys

# 将zip文件解压处理，并放到指定的文件夹里面去

def unzip_file(zip_file_name,destination_path):
    archive = zipfile.ZipFile(zip_file_name,mode='r')
    for file in archive.namelist():
        archive.extract(file, destination_path)

a = "D:\Hgame_MineIsBig\level1" #zipfile 的路径
b = "D:\Hgame_MineIsBig\level1\leve12" #解压到路径unzip下

def zipfile_name(file_dir):

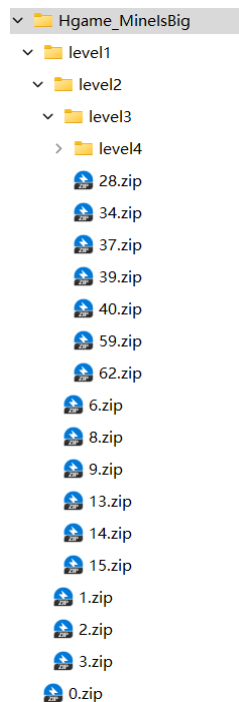
```

```
# 读取文件夹下面的文件名.zip
L=[]
for root, dirs, files in os.walk(file_dir):
    for file in files:
        if os.path.splitext(file)[1] == '.zip': # 读取带zip 文件
            L.append(os.path.join(root, file))
        #print(L)
    return L

#入口函数
def main():
    fn=zipfile_name(a)
    for file in fn:
        unzip_file(file,b)

if __name__ == "__main__":
    main()
print("done")

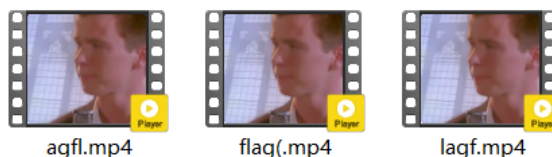
#zipfile解压中文zip文件会导致乱码，解决方案是要修改python库中的zipfile.py
#将文件中所有的'cp437'字符替换为'gbk'
```



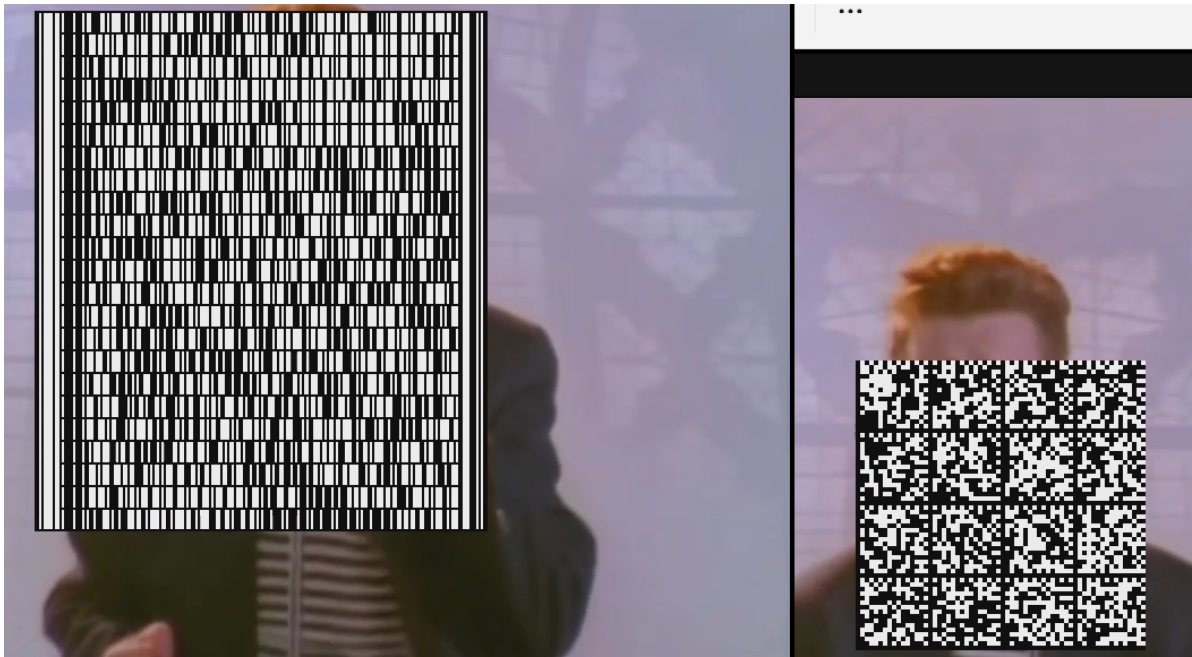
(仅展示部分)

全部解压后，在最深层发现了两个名字不同的视频

rel2 > level3 > level4 > level5 > level6 > level7 > level8



查看一遍，得到两个二维码



[在线阅读条形码 \(aspose.app\)](https://aspose.app/)

使用上述网站，解码视频中的两个二维码及题目给出的两个二维码。解码后的结果经base64解密后，得到四个 png 图片。

ivBORw0KGgoAAAAANSUhEUgAAABEAAAASCAIAAAAYm6lIDAAAACXBjWXMMAAA7EAAAOxAGVKw4bAAAAkEIEQVQokYVSQQ7AIAgD4/+3B3ISG0x9mAGUlpkAQBAROBHXNBXyUWZydcDcPzXA6hQZPt7F6HtdbVoqkvJNt/DOtc4KAuKFICHjZsRzewnt5C4Kc73lol7MrJALSx13HTYx7HuJxKbvHKCjwMj7o4WxjV eMu6HyE8dByi2Yb32JUz/nfvseVoqaZ97OeGD5rSxcDh986KAAAAAEIFtkSuQmCC

from_the-x.png

from_the-x.png

编码源格式：☒文本 ☐Hex 解码结果

自动检测

UTF-8

中文编码

编码 解码

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F

89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52
00	00	00	11	00	00	00	12	08	02	00	00	00	32	9B	A2
03	00	00	00	09	70	48	59	73	00	00	0E	C4	00	00	0E
C4	01	95	2B	0E	1B	00	00	00	90	49	44	41	54	28	91
85	52	41	0E	C0	20	08	03	E3	FF	BF	DC	1D	C8	48	6D
31	F6	60	06	52	5A	64	01	00	40	44	E0	47	5C	D0	57
C9	45	99	C9	D7	1D	0A	96	57	03	A8	50	64	FB	7B	17
A1	ED	75	B5	68	AA	4B	C9	36	DF	C3	3A	D7	38	28	0B
8A	14	80	A1	8D	9B	11	CD	EC	27	AA	DE	42	E0	A7	3B
DE	5A	08	EC	CA	C9	00	B4	B1	D7	71	D3	63	1E	C7	B8
9C	4A	6E	F1	CA	0A	3C	0C	8F	BA	38	5B	18	D5	78	CB

插件【Png】Png Image

另存为：png文件

附加信息：

Size:17x18

当前编码：[Hex]

数据长度：222 Bytes

插件数：18，耗时：1ms



将图片拼合后扫码，得到flag

一张怪怪的名片

将题图的二维码处理拼合。发现二维码中间部分有大量连续黑块。



经掩码处理后，二维码不应出现这种情况。当然也扫不出来。在
<https://merrickx.github.io/qrazybox/> 中，读取二维码信息。

QR version : **4 (33x33)**

Error correction level : **H**

Mask pattern : **0**

Number of missing bytes (erasures) : **0 bytes (0.00%)**

Data blocks :

["01000001","11110110","11100010","00110010","11100110","100001"

Final data bits :

01000001111001101000011101000111010001110000011100110011101

[0100] [00011110]

[0110100001101110100011011101000110111000001101110011001001'

Mode Indicator : **8-bit Mode (0100)**

Character Count Indicator : **30**

Decoded data : **https:~?homdginc~.homeboy~)³k**

[0100] [11101100] [000100011111110101000000010001]

Mode Indicator : **8-bit Mode (0100)**

Character Count Indicator : **236**

Decoded data : **ê**

Final Decoded string : **https:~?homdginc~.homeboy~)³k ê**

可以发现是一个类似网址的字符串。检索后，发现了homeboyc.cn域名。

在博客友链中找到了 鸿贵安的自留地 。其中有一篇文章如下

FL4G

宝，想你，呜呜。宝，下面的fl4g的密码你应该知道的，我就不说了嘎嘎。

对了，宝，你可以用这个网站解密 [CyberChef](#) 。

我先用“Derive PBKDF2 key”把密码转成了key (salt=1)，然后交给AES加密模块用ECB模式加密了（别忘了base64）。

The following text is the ciphertext of fl4g after AES-128 encryption.

```
b09nyMj9cOZ3aB8KUcnh46nli9fGTIL6XjnnW1/sj/nUR1BFYkf0JwB0qjcQhcCy7dxtsHqznOMkt6XEGKD8y5K5whenAcwuiT/Rt
```

【密码】—PBKDF2—>【key】

【Flag】—AES128/key—> —base64—>【网页密文】

加密方式如上。接下来就是猜密码了。说实话，这个密码我想鲨了出题人(bushi)

收集到的情报如下：

我获得的情报：

鸿贵安/鸿师傅； 蒙尔/宝/鸿贵安女朋友
贴贴(hint) - 应该是鸿和宝的两个信息组合在一起
生日信息 - 宝20020816， 鸿未知
ID相关 - homeginan, mener
姓名相关 - hongguian
男左女右(出题人提示)

鸿的博客提到有关盗号、弱口令等。在蒙尔的博客中有这么一行加粗的文字

1. 密码长度至少包含10位密码且至少包含大写字母、小写字母、数字、特殊字符中的至少包含一个。
2. 密码中不应包含本人、父母、子女和配偶的姓名和出生日期、纪念日期、登录名、E-mail地址等等与本人有关的信息，以及字典中的单词。
3. 不要长期使用固定密码。定期或者不定期修改密码。防止未被发现的入侵者继续使用该密码

我猜想的密码：鸿蒙（拼音、英语等）、蒙尔生日 的组合。

试了好久好久好久，一直不对。

结束后，出题人给出的答案为 hgame20020816。hgame 即两者拼音首字母。我不接受。我觉得鸿蒙太对了。可能这道题和我无缘吧。