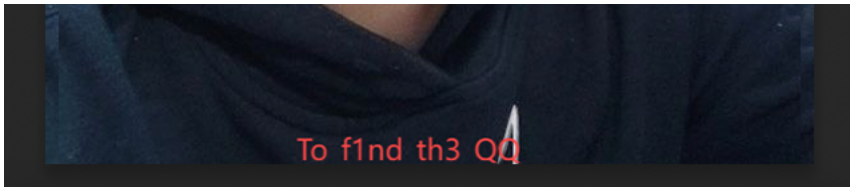
HGAME 2025 Writeup

队伍名称：Mitsuha
队伍ID：000345

Hakuya Want A Girl Friend

下载附件后，在cyberchef中发现文件有由一个压缩包和一个照片组成，照片尺寸经过裁切，复原后可得到隐藏的压缩包密码，解压后即可得到flag



Level 314 线性走廊中的双生实体

附件为pytorch模型，题目中写道“避免使用随机张量”，可知无需使用随机数生成张量，通过输出entity.code，可知枚举步长为10
用代码进行破解：

```
import torch
entity = torch.jit.load('entity.pt')
for i in range(100):
    for j in range (100):
        input_tensor = torch. linspace(i, j, steps = 10)
        print(i,j)
        output = entity(input_tensor)
```

最后运行可得i=34, j=22

Computer cleaner

打开虚拟机后，发现为ubuntu系统，安装有apache，在网站目录下发现webshell php，查看访问记录可以发现查看了文档下的flag文件，用浏览器访问其源ip，可以得到第二部分flag

Compress dot new

附件为一个Nushell的huffman编码算法，编写程序解密：

```
import json
a="""{"a":{"a":{"a":{"a":{"a":{"s":125},"b":{"a":{"s":119},"b":{"s":123}}},"b":{"a":{"s":104},"b":{"s":105}}},"b":{"a":{"s":101},"b":{"s":103}}},"b":{"a":{"a":{"a":{"s":10},"b":{"s":13}},"b":{"s":32}},"b":{"a":{"s":115},"b":{"s":116}}}},"b":{"a":{"a":{"a":{"a":{"a":{"s":46},"b":{"s":48}},"b":{"a":{"a":{"s":76},"b":{"s":78}},"b":{"a":{"s":83},"b":{"a":{"s":68},"b":{"s":69}}}}}},"b":{"a":{"a":{"s":44},"b":{"a":{"s":33},"b":{"s":38}}},"b":{"s":45}}},"b":{"a":{"a":{"s":100},"b":{"a":{"s":98},"b":{"s":99}}},"b":{"a":{"a":{"s":49},"b":{"s":51}},"b":{"s":97}}}},"b":{"a":{"a":{"a":{"s":117},"b":{"s":118}},"b":{"a":{"a":
```

{"s":112},"b":{"s":113}},"b":{"s":114}}},"b":{"a":{"a":{"s":108},"b":{"s":109}},"b":{"a":{"s":110},"b":{"s":111}}}}}}"""

```
b="""000100011101111110100100000111000101110001001110001100001000101110011100100110110
101011110111011001101000111011010011101111101110110110011101100111100111101110110101100
011110110011110001110011011110000110011000010110111011000111001010011100101110011111000011
000101001010000000100101000100010011111110110010111010101000111101000110110001110101010
101001111111100111111101101010110000110111010110111111010010011110010001011010111111111110011
000101010111011100100111110001101101011011110100000111101000001101101010110001111110001100
101001011100000110111100000010010100010001011100011100111001011101011111000101010110101
111000001100111100011100101110101111100010110101110000010100000010110001111011100011101111
111010101001001110101110010001111001001011011110111011101011110111010111100100010
111001001011100010110101000011101010001011110101001100011101010111011000110110110000110100
000000101100011101111111110001010101011100000"""
h=json.loads(a)
def d(t,e):
 o=[]
 n=t
 for c in e:
  n=n['a'] if c=='0' else n['b']
  if's'in n:o.append(chr(n['s']));n=t
 return''.join(o)
g=d(h,b)
print(g)
```

Turtle

附件为一个魔改的upx，拖进x64dbg中，在pushad执行完成后对当前栈顶的内存地址下一个硬件断点，即可获得oep，dump后发现是rc4加密解密，将被加密的部分重新加密即可获得原文

```
char *inverse_sub_401550(char *a1, int a2, char *a3) {
  char *result;        // rax
  unsigned __int8 v4; // [rsp+7h] [rbp-9h]
  int v5;              // [rsp+8h] [rbp-8h]
  int i;               // [rsp+Ch] [rbp-4h]
  int j;               // [rsp+Ch] [rbp-4h]

  v5 = 0;
  for (i = 0; i <= 255; ++i) {
    result = &a3[i];
    *result = i;
  }
  for (j = 0; j <= 255; ++j) {
    v5 = ((unsigned __int8)a3[j] + v5 + (unsigned __int8)a1[j % a2]) % 256;
    v4 = a3[j];
    a3[j] = a3[v5];
    result = (char *)v4;
```

```
    a3[v5] = v4;
  }
  return result;
}
```

Level 24 Pacman

在源码中查找gift即可得到打乱并base64的flag

Level 47 BandBomb

一个文件上传网站，其中的图片的url是在public目录下，并且猜测重命名过程中存在文件移动，将源码移动到public，即可泄漏源码，再将views中的ejs文件移出，插入代码：<%- global.process.mainModule.require('child_process').execSync('env') %>，即可获得flag

Level 69 MysteryMessageBoard

扫描后台发现还有admin页面，并且得知服务器会查看留言板，留言板直接拼接了html代码。存在xss漏洞，通过xss获得admin的cookie后访问flag页面即可得到flag

Level 25 双面人派对

反编译文件后发现minio字样，从字符串中找到key，登录minio，发现程序源码和一个update功能，修改源码加入自定义命令，获得flag

```
    g.GET("/", func(c *gin.Context) {
        out, err := exec.Command("ls", "-lah").Output()
        c.String(200, string(out))
    })
```