**签到题**

压缩包里面是一张图片，

根据压缩包的名字high.zip可以猜测可能是宽高被修改了，使用脚本进行宽高爆破

得到ISCC{D3tivtm\_zv\_Tq5I\_ Dygef}

然后进行维吉尼亚密码解密，并且很容易想到密钥是high即可得到flag

**寻找小明-1**

根据题目信息可知是LSB隐写，使用脚本获取隐藏信息

#LSB最低位隐写  
from PIL import Image  
img = Image.open("a.png")  
img\_array = img.load()  
a = [257, 1, 258, 2, 259, 3, 260, 4, 261, 5, 262, 7, 263, 8, 259, 277, 438, 300, 455, 319, 25, 300, 456, 400, 66, 366, 78, 300, 421, 259, 452, 23]  
ret = ""  
for i in range(int(len(a)/2)):  
 b = img\_array[a[i\*2],a[i\*2+1]]  
 print(b,chr(b[0]), chr(b[1]),chr(b[2]))  
 ret =ret+chr(b[0])  
print(ret)

**ISCC成绩查询-1**

使用Stegsolve打开test\_ctf.png，查看不同颜色通道，发现一个路径图。直接在Stegsolve的Green plane 1通道看。然后基本确定是一个哥尼斯堡七桥问题。观察到上图只有箭头所示的点是奇度数节点，所以是存在欧拉通路的半欧拉图。然后从两个奇度数点出发，找到符合图片顺序的欧拉通路。

连接后为：TRLNCHHAFCIEEIEEPR

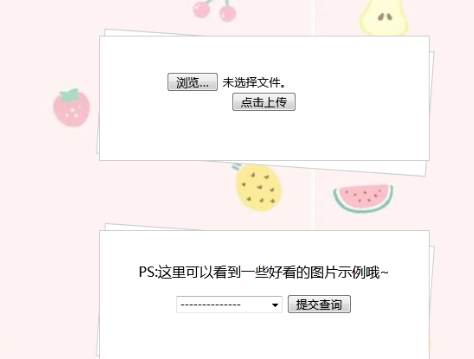
栅栏密码解密后为：THERAILFENCECIPHER

得到flag：flag{THERAILFENCECIPHER}

**What can images do**



看题目介绍，感觉应该是文件上传,进入环境后，果然是文件上传



这里来看的话应该是文件包含漏洞，php无法绕过只能上传图片  
先上传图片马，不做任何绕过操作

然后用文件包含包含这个图片马



我们直接用hackbar来读取flag

