小组 WP

一、 Checkin

a）进入网页按 F12 发现已经保存了部分登录信息

b）根据提示使用 md5 值 6a0a4c0bf572e2bc23505fb051230f36 配合掩码 2022111111111?d?d?d?d?d?d 在 hashcat 中计算 6 位密码（算出来是啥忘了）

c）使用题干提供 2021302181050 加六位密码所得的 md5 进行签到顺利得到 flag

二、 2 战挑的邪正人鬼

a）根据所给的 piz 文件用 010editor 打开，发现文件头 50 4B 03 04 以逆序形式在文件末尾出现，判断文件逆序

b）用 python 脚本进行逆序输出得到 zip 压缩包，随后解压得到 yp.ssecnirp 根据文件名判断为 py 文件逆序，于是继续逆序输出

逆序脚本在这里

```
input = open('yp.ssecnirp','rb')
input_all = input.read()
ss=input_all[::-1]
output=open('princess.py','wb')
output.write(ss)
input.close()
output.close()
```

发现可疑代码

```
text="wkhkuvcwtyfk{oSeh"
    "Tkinter Designer uses the Figma API\n"
    "lIxnimyyh0kunmbar"
    "to analyse a design file, then creates\n"
    "Rauwghesttbr1lGwig"
```

```
    "the respective code and files needed\n"
    "gebtibgt!o!d!p}"
    "for your GUI.\n\n"
```

c）截取字符 wkhkuvcwtyfk{oSehIIxnimyyhOkunmbarRauwghesttbr1lGwigg ebtibgt!o!d!p}

d）根据 whuctf 和 wkhkuvcwtyfk 判断为隔字符插值

e）处理后得到正确 flag whuctf{ShInmyOumaRugetb1Gigbig!!!}

三、 mia_is_gaming

a）通过 gaming 线索找到 WHUMia 的 steam 账号，举报后发现没有任何线索

b）通过 coding 思考是否为 github，遂发现其账号和名为 flag 的仓库

c）下载仓库内 flag.zip 到本地解压后发现 flag 已经被删除 考虑利用 git 回退

d）花了好久发现.git 文件被篡改为 git 导致回退失败（靠骗 靠偷袭 …）

e）改名后 git reset –hard HEAD^两三次后找到原 flag 文件

四、 幽霊楽団～Phantom Ensemble

a）音频文件考虑 lbs 隐写

b）使用 silenteye 分离一次得到 in here.wav 翻译其中 morse 得到线索 PASSWORDISCUTE+DARKFLYING.JPG

c）将 in here.wav 使用 silenteye 继续分离得到 actually in here.rar 解压后得到关联图片一张和 biu~的音频文件

d）音频文件再次使用 silenteye 分离得到 flag! zip 为加密压缩包

e）在图片中发现小字 rumia

f）综合以上线索得到解压密码为 cuterumia 顺利解开压缩包得到 flag 的 doc 文件

五、 X_or_Mia

a）分析代码：加密文件 msg 密钥 key

b）O[i]=msg[i]key[i mod 11]

c）根据题目描述判断 key 为 i1oveyoumia

d）写解密脚本

```
def de(o,key):
    msg=""
    for i in range(len(o)):
        t=ord(o[i])^ord(key[i % 11])
        msg+=chr(t)
    return msg

d = open('encrypted', 'r')
o = ''.join(d.readlines()).rstrip('\n')
d.close()

k = open('key', 'r')
key = ''.join(k.readlines()).rstrip('\n')
k.close()
assert key.isalnum() and (len(key) == 11)
d = open('decrypted', 'w')
d.write(de(o, key))
```