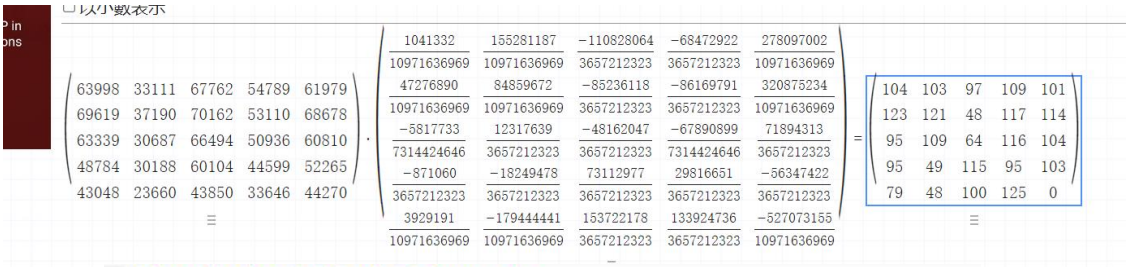
Re

Math

5*5 矩阵计算，在线找工具即可 flag

hgame{y0ur_m@th_1s_gO0d}

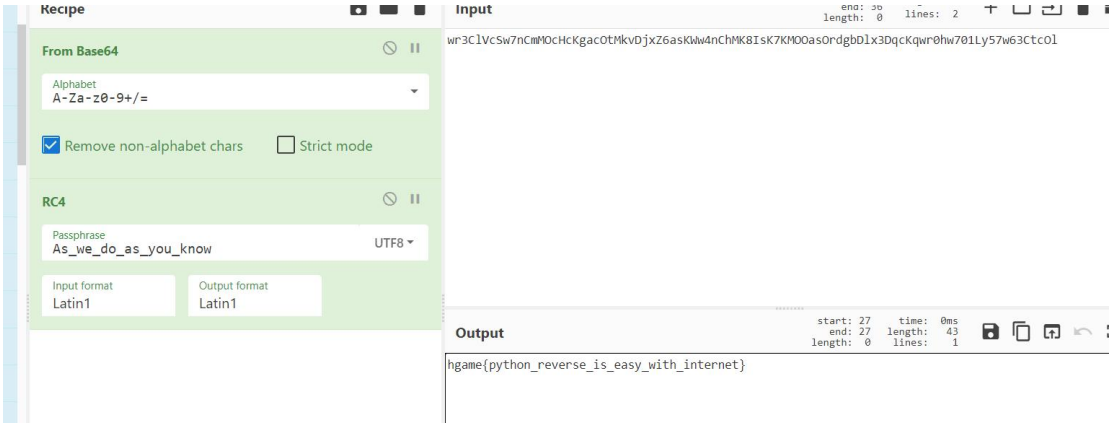


```
#include<bits/stdc++.h>
using namespace std;
char f[] = {104, 103, 97, 109, 101, 123, 121,
48, 117, 114, 95, 109, 64, 116, 104, 95, 49,
115, 95, 103, 79, 48, 100, 125};
int main()
{
    printf("%s", f);
}
```

Stream

发现是 python 打包为 exe 的文件，于是用 pyinstxtractor.py 解包，得到 pyc，再丢进在线网站，加密逻辑为 rc4+b64，用 cyberchef 解密得到 flag

hgame{python_reverse_is_easy_with_internet}



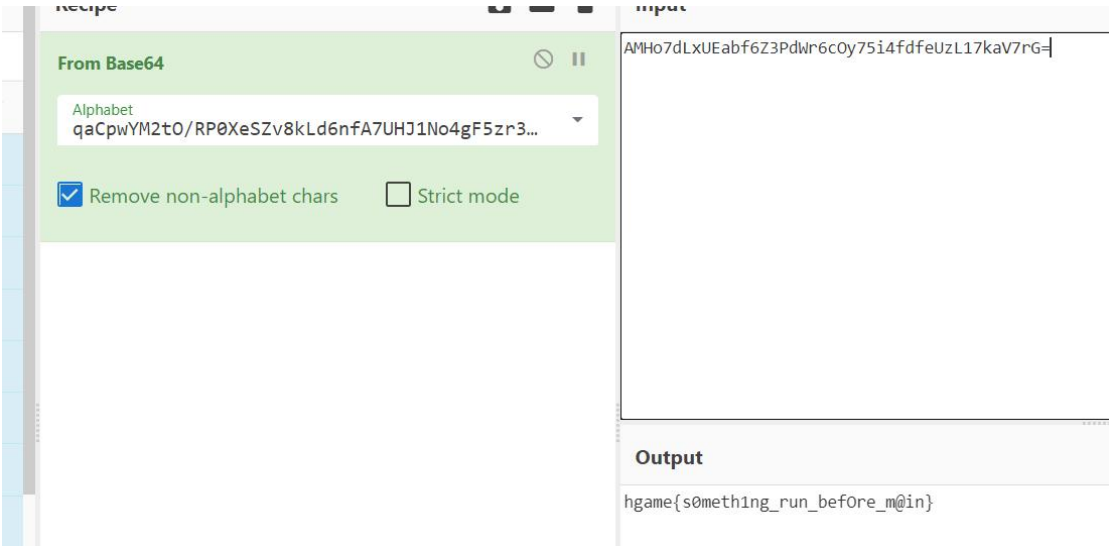
Before_main

Ida64 打开，发现是变表 base64，表存在 qword 中，在 cyberchef 解发现不对，于是按 x 跟进 qword，发现表发生更改，再一次丢进 cyberchef 得到 flag

hgame{s0meth1ng_run_befOre_m@in}

```
if ( result != -1 )
{
  strcpy((char *)&qword_4020, "qaCpwYM2tO/RP0XeSZv8kLd6nfA7UHJ1No4gF5zr3VsBQbl9juhEGymc+WTxIiDK");
  return 0x636D79474568756ALL;
}
```

```
while ( v2 < v4 - 2 )
{
  v6[v2] = *((_BYTE *)&qword_4020 + ((unsigned __int8)a1[v3] >> 2));
  v6[v2 + 1] = *((_BYTE *)&qword_4020 + ((16 * a1[v3]) & 0x30 | (unsigned int)((unsigned __int8)a1[v3 + 1] >> 4)));
  v6[v2 + 2] = *((_BYTE *)&qword_4020 + ((4 * a1[v3 + 1]) & 0x3C | (unsigned int)((unsigned __int8)a1[v3 + 2] >> 6)));
  v6[v2 + 3] = *((_BYTE *)&qword_4020 + (a1[v3 + 2] & 0x3F));
  v3 += 3;
  v2 += 4;
}
```



VidarCamara

Apk 文件，用 jadx 打开，再拖到模拟器里面下载，发现需要输入序列号，于是在 jadx 中定位，找到核心算法为 xtea（其中循环了 33 次！）写 exp 得到 flag：

hgame{d8c1d7d34573434ea8dfe5db40fbb25c0}

```
void decrypt (uint32_t* v, uint32_t* k) {
    uint32_t delta = 878077251;
    int t2 = 8;
    while (t2 >= 0)
    {
        uint32_t sum = delta * 33;
        for (int i = 0; i <= 32; i++) {
            int t = t2 + 1;
            sum -= delta;
            v[t] -= (((v[t2] << 4) ^ (v[t2] >> 5)) + v[t2]) ^ (sum + k[(sum >> 11) & 3]);
            v[t2] -= (((v[t] << 4) ^ (v[t] >> 5)) + v[t]) ^ (sum + k[sum & 3]) ^ sum;
        }
        t2--;
    }
}
```

Web

Git leakage

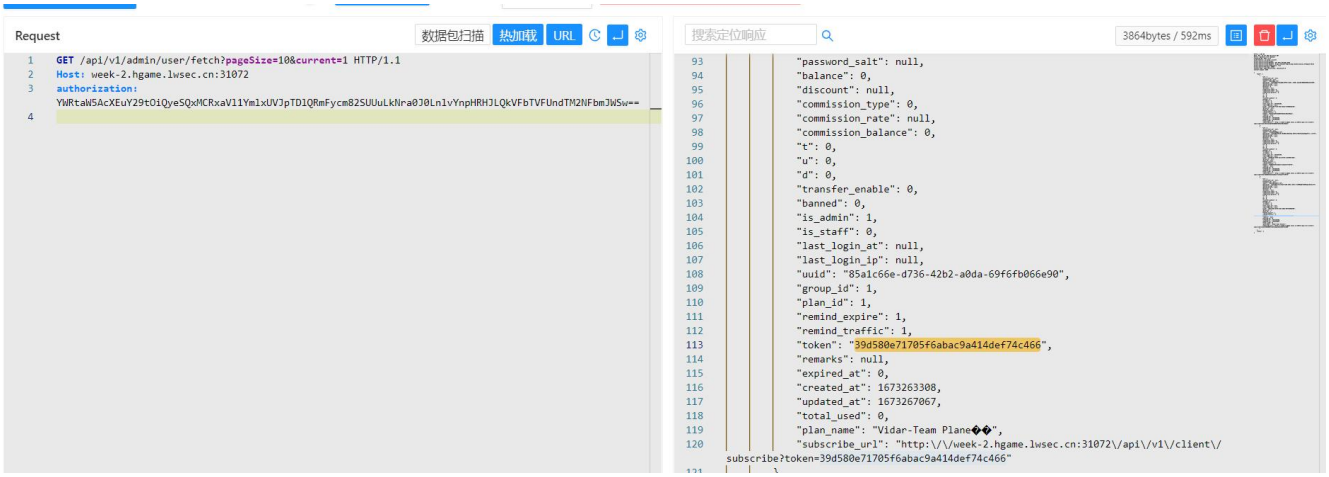
猜测 git 泄漏，用 githack 得到 flag

hgame{Don't^put*Git-in_web_directory}

V2board

V2Board Admin.php 越权访问漏洞，根据网上博客复现，成功越权拿到 token

hgame{39d580e71705f6abac9a414def74c466}



Crypto

Rabin

Rabin 加密，在网上找脚本爆破即可得到 flag

hgame{That'5_s0_3asy_to_s@lve_r@bin}

包里有什么

背包加密，a 为超递增序列，所以为私钥，b 为公钥，上网找脚本得到 flag

hgame{1t's_4n_3asy_ba9_isn7_it?}

Rsa 大冒险

打开 py 文件，四关是四种不同的 rsa 加密，网上找到对应脚本解密即可获得四个关卡的答案，分别验证即可得到 flag

hgame{W0w_you^knowT^e_CoMm0n_&t$ack_@bout|RSA}

```
m<n_But_also_m<p
make_all_modulus_independent
encrypt_exponent_should_be_bigger
never_uese_same_modulus
hgame{W0w_you^knowT^e_CoMm0n_&t$ack_@bout|RSA}
```

Misc

Tetris Master(Revenge)

Ssh 连接，发现失败之后并不会重置分数，写脚本重复点击空格与 n，到 5w 分之后拿到 flag

hgame{Bash_Game^Also*Can#Rce}

hgame{Bash_Game^Also*Can#Rce^reVenge!!!!}

Sign_in_pro_max

Txt 文件，根据提示，第一个 base 家族 f51d3a18
2，3，4 都在线 md5 解密 f91c 4952 a3ed
最后一个凯撒枚举得到提示得到 flag

hgame{f51d3a18-f91c-4952-a3ed-0bc0ea61d21c}

> Part5 is 0bc0ea61d21c, now put all the parts together, don't forget the format.

Crazy_QRcode

文件为 password 的二维码与 flag 的压缩包，尝试提取压缩包文件后发现有密码，于是猜测是扫描二维码后获得文件，使用 qrcodebox 修改 mask，尝试后得到密码 QDjkXkpM0NHNXujs，解压缩之后是 25 张图片，最后的文件打开发现是 25 个数字，猜测为旋转，1 为 90，2 为 180，3 为 270，？不知道，25 图片摆好之后发现排列顺序不变，于是根据定位符可以确定其中几个？的旋转，另外几个问号不旋转也可以扫出来，得到 flag

hgame{Cr42y_qrc0de}