

Re

Math

5*5 矩阵计算，在线找工具即可 flag

hgame{y0ur_m@th_1s_g00d}

以小数表示

63998	33111	67762	54789	61979
69619	37190	70162	53110	68678
63339	30687	66494	50936	60810
48784	30188	60104	44599	52265
43048	23660	43850	33646	44270

$$\begin{pmatrix} 1041332 & 155281187 & -110828064 & -68472922 & 278097002 \\ 10971636969 & 10971636969 & 3657212323 & 3657212323 & 10971636969 \\ 47276890 & 84859672 & -85236118 & -86169791 & 320875234 \\ 10971636969 & 10971636969 & 3657212323 & 3657212323 & 10971636969 \\ -5817733 & 12317639 & -48162047 & -67890899 & 71894313 \\ 7314424646 & 3657212323 & 3657212323 & 7314424646 & 3657212323 \\ -871060 & -18249478 & 73112977 & 29816651 & -56347422 \\ 3657212323 & 3657212323 & 3657212323 & 3657212323 & 3657212323 \\ 3929191 & -179444441 & 153722178 & 133924736 & -527073155 \\ 10971636969 & 10971636969 & 3657212323 & 3657212323 & 10971636969 \end{pmatrix} = \begin{pmatrix} 104 & 103 & 97 & 109 & 101 \\ 123 & 121 & 48 & 117 & 114 \\ 95 & 109 & 64 & 116 & 104 \\ 95 & 49 & 115 & 95 & 103 \\ 79 & 48 & 100 & 125 & 0 \end{pmatrix}$$

```
#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}

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

RC4

Passphrase
As_we_do_as_you_know UTF8

Input format
Latin1

Output format
Latin1

Input

wn3C1VcSw7nCmMOCHkgacOtMkvDjxZ6asKwW4nChMK8IsK7KMO0asOrdgbDLx3DqckQw0hw701Ly57w63ctc0l

Output

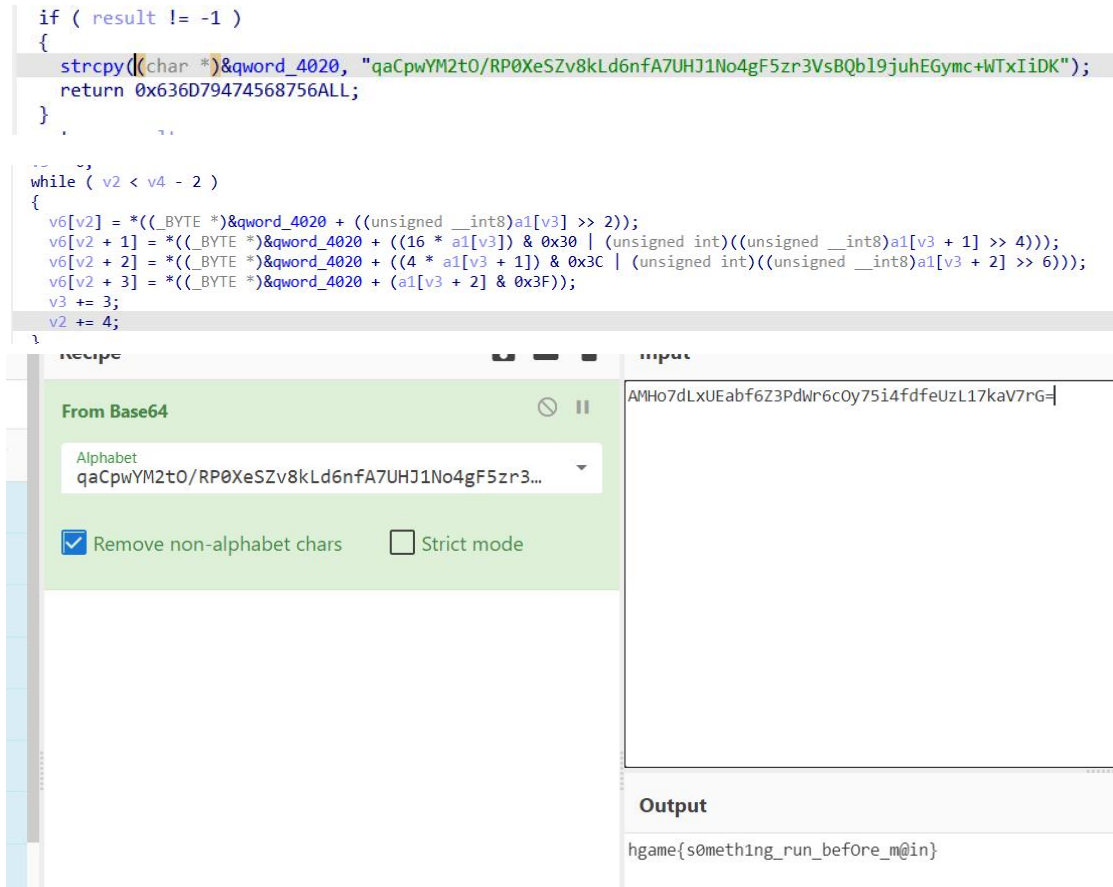
start: 27 time: 0ms
end: 27 length: 43
length: 0 lines: 1

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

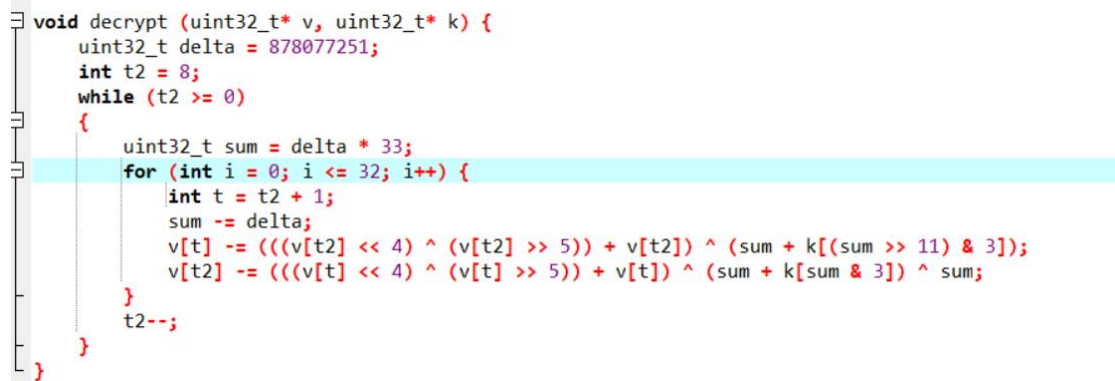
hgame{s0meth1ng_run_befOre_m@in}



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}



Web

Git leakage

猜测 git 泄漏，用 githack 得到 flag

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

```
PS C:\Users\wzf\Desktop\CTF_Tools\Web\GitHack-master> python .\GitHack.py http://week-2.hgame.lwsec.cn:31428/.git/
[+] Download and parse index file ...
[+] .gitmodules
[+] LICENSE
[+] README.md
[+] TODO.txt
[+] This_is-flag
[+] assets/Matrix-Code.ttf
```

This_is-flag - Typora

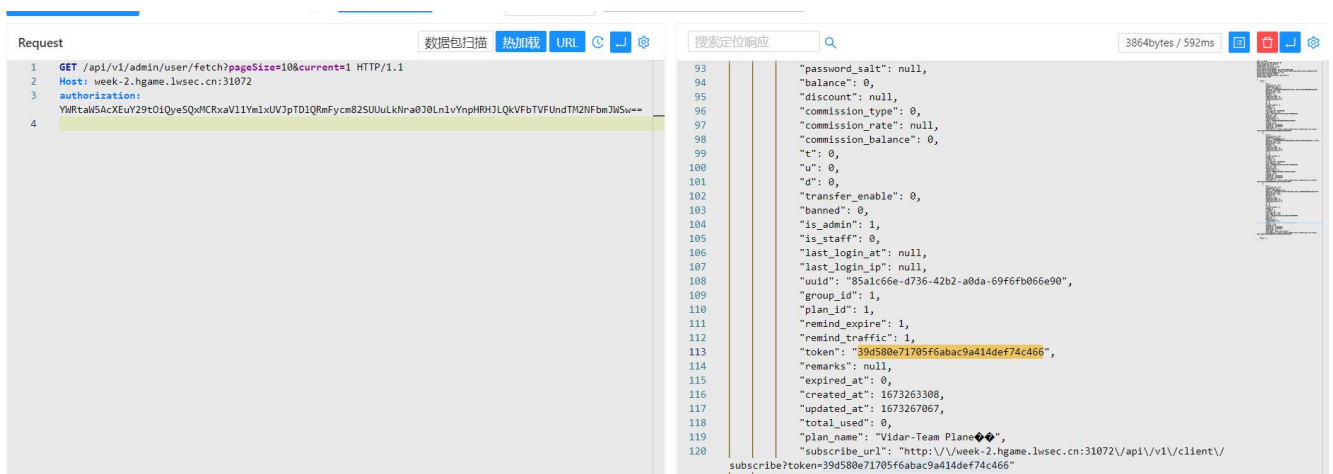
文件(F) 编辑(E) 段落(P) 格式(O) 视图(V) 主题(T) 帮助(H)

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 QDjkXkpM0NHXUjs，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}
```

