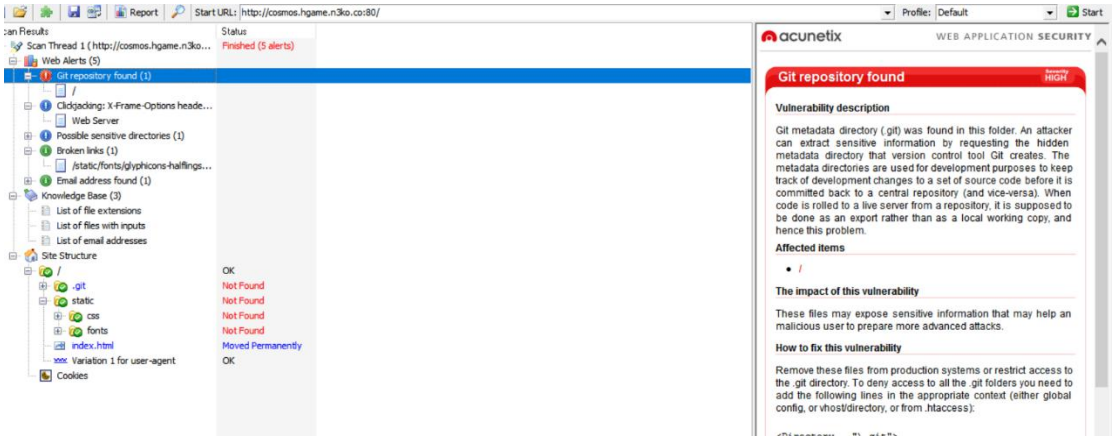
HGAME Week1 Writeup

WEB

作为一个小白，只能查查百度，看看运气。

Cosmos 的博客

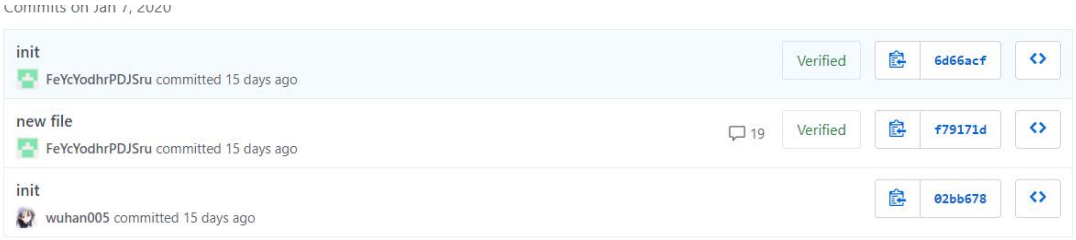
这题看到版本管理器，查询可得要用到 git，继续查询需要用 awvs 扫描，扫描到



发现一个 git 漏洞，用在网页用“/.git/config“后缀打开 git 文件：


```
[core]
        repositoryformatversion = 0
        filemode = true
        bare = false
        logallrefupdates = true
[remote "origin"]
        url = https://github.com/FeYcYodhrPDJSru/8LTUKCL83VLhXbc
        fetch = +refs/heads/*:refs/remotes/origin/*
```

打开 github 的 url，查看历史版本，由于做的时间比较靠后，只要看评论最多的就是答案。

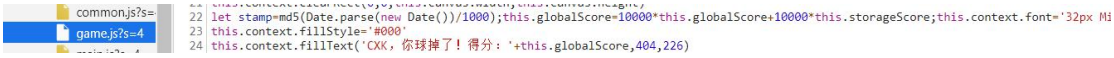


再用 base64 解码得到 flag，简直一波三折。

```
@@ -0,0 +1 @@
+ base64 解码: aGdhbWV7ZzF0X2xlQGtfMXNfZGFuZ2VyMHVzXyEhISF9
```

尼泰玫

这题是个游戏，毫无疑问就是要看 js 文件，那就 F12 大法，查看网页的源，看到有多个 js 文件（标注了 js 管辖的方面）。如果要让分数到 30000 分普通网页是不可能的（天真的我去通了一关，最多 7200），那就要对 js 做点小改动。
大致看了 js 的结构，发现其实改的方法与很多，比如将技能的消耗变成负的，或者在累加分数的时候乘以很大的系数，快速到达 30000 以上。我采用第二种方法。



增加了两个 10000，只要碰到一个砖块，分数就直接到了 1000000，得到 flag。

（很菜，就做了这点，然后去做 crypto 和 misc 了）

Crypto

InfantRSA

在搜百度时看到过这类 RSA 题目，和指数有关，根据 csdn 大法找了点脚本，得到 flag

```
import gmpy2
import binascii
c = 27569846508236107014517368841149631154217290260855985901984l
p = 681782737450022065655472455411
q = 675274897132088253519831953441
e = 13
phi_n = (p - 1) * (q - 1)
d = gmpy2.invert(e, phi_n)
m = pow(c, d, p * q)
q = int.from_bytes(b'hgame', byteorder='big')
print(q)
print("十进制:\n%s" % m)
m_hex = hex(m)[2:]
print("十六进制:\n%s" % (m_hex, ))
print("ascii:\n%s" % (binascii.a2b_hex(m_hex).decode("utf8"), ))
```

```
448411037029
十进制:
39062110472669388914389428064087335236334831991333245
十六进制:
6867616d657b74335874364f306b5f5235412121217d
ascii:
hgame{t3Xt6O0k_R5A!!!}
```

Affine

该题得先看懂加密的算法：
给定常量字符 TABLE，再 flag 中取一个字符 b，根据 b 是否存在 TABLE 中得到相应的逻辑关系和条件语句：

```
for b in flag:
    i = TABLE.find(b)
    if i == -1:
        cipher += b
    else:
        ii = (A * i + B) % MOD
        cipher += TABLE[ii]
```

既然要解密，那就要得到 A，B 的值，想到 flag 的格式是“hgame”开头的，那就用前五个字母去解二元一次方程，数字凑的可还行，A=13，B=14，根据原来的加密脚本，逆向写一个解密脚本：（想到“_”肯定不在 TABLE 中就去了下划线进行解密）

```
TABLE = 'zxcvbnmasdfghjklqwertyuiop1234567890QWERTYUIOPASDFGHJKLZXCVBNM
'
MOD = len(TABLE)
print(MOD)
result = ''

g = 'xr1AJ7havGTpH410'
for b in g:
    p = 1
    q = 0
    j = TABLE.find(b)
    while q < 15:
        m = (62 * q + j - 14) % 13
        if (m == 0):
            n = (62 * q + j - 14) // 13
            result += TABLE[n]
            p = 0
            break
        q += 1
    if (p == 1):
        result += ' '


print(result)
```

得到“flag“:
M4thu5EdiNcRYpt0
按字节添加下划线即可。

Reorder

查了 nc，简单了解了概念和用法，就在 Linux 中操作，一回车，发现类似 flag 的密码，按照 hint 可以知道，是经过了一定的顺序变换，那就先输入最常用的顺序。

```
think@ubuntu:~$ nc 47.98.192.231 25002
>
Rua!!!
5thIg+e{mm$pLUja0T3n_iRm!eA!}TuP
```

不断尝试发现长度需要和 flag 一样长，那就输入“a”-“z“+”1“-“6”，长度符合后回车得到新的顺序。根据两组数据写脚本（由于对 python 不熟悉，使用了 c）

```
think@ubuntu:~$ nc 47.98.192.231 25002
> asbd
b  s   a    d
> zbcdsefrj
cj b   zfs rd  e
> abcdefghijklmnopqrstuvwxyz123456
cinbjloagekhdpmfsy4rz25qwu1xt63v
>
Rua!!!
a$mgt5phje+UmLI{PA!_T0!3uRiTe}nm
```

```
#include <stdio.h>
#include <string.h>
int main()
{
    int c[32] = {0};
    char a[32] = "abcdefghijklmnopqrstuvwxyz123456";
    char b[32] = "cinbjloagekhdpmfsy4rz25qwu1xt63v";
    for (int i = 0; i < 32; i++)
    {
        for (int j = 0; j < 32; j++)
        {
            if (a[i] == b[j])

                c[i] = j;
        }
    }
    char d[32] = "a$mgt5phje+UmLI{PA!_T0!3uRiTe}nm";
    char e[32];
    for (int i = 0; i < 32; i++)
    {
        e[i] = d[c[i]];
    }
    printf("%s", e);
}
```

得到 flag

Misc

欢迎参加 HGame!

给我一段密文，应该是密码学的知识，那就用 base64 解一下，得到一串摩斯密码，

```
.-- ...-- .-.. -.-. ----- -- . ..--.- - --- ..--.- ..--- ----- .|--- ----- ..--.- .... --. .- -- ...--
```

那就再解密

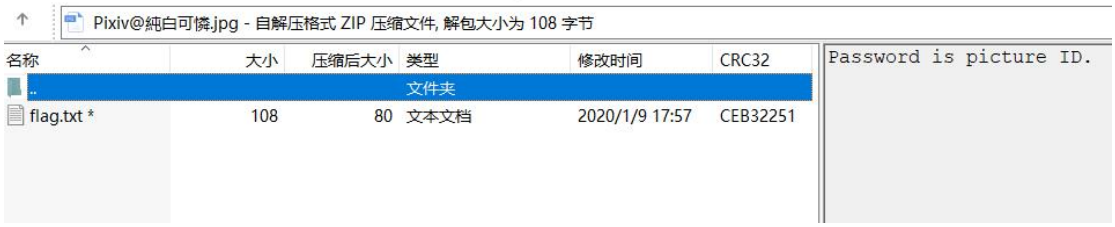
那把空格换成下划线就可，再加上 hgame{}即可。

壁纸

用 WinRAR 打开压缩包，查看文件，查到 flag.txt

得到提示，要寻找该图片的

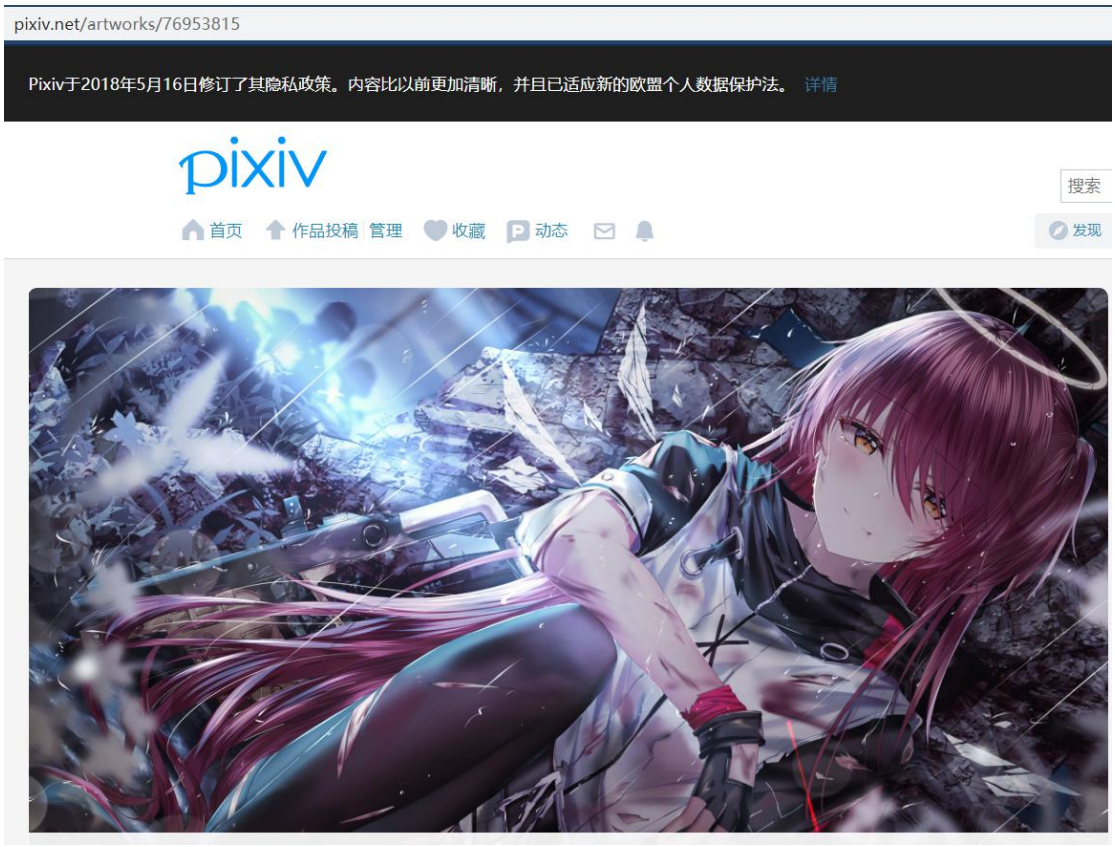
id



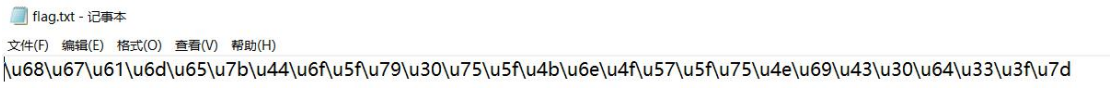
看了看图片的名字，估计是 p 站的图片。

进入 p 站，查找纯白可憐，找到这张图片，得到

id



打开 flag.txt：



用 Unicode 解码，即可得到 flag

签到题 ProPlus

根据提示：fenses—栅栏密码，Caesar—凯撒，找个在线解密
先用这个规则去解密，一般密码不会很长，所以就用了第二段。

进行一系列转换得到密码，一试就对了。

栅栏密码

JRFVJYFZVRUAGMAI

每组字数 3 加密 解密

JFARZGFVMVRAJUIY

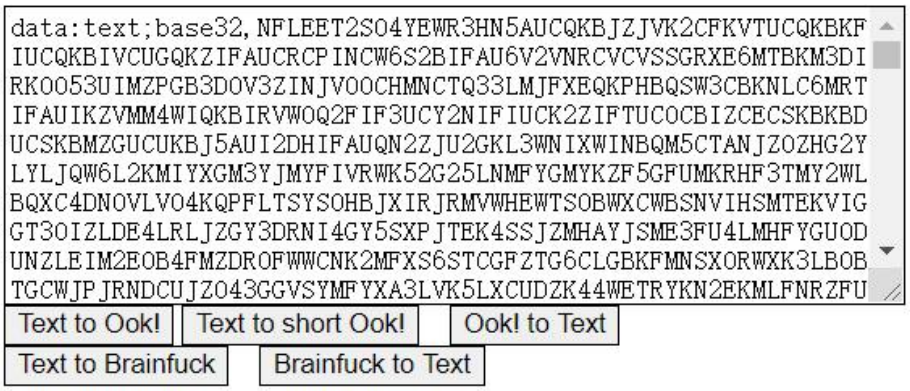
凯撒密码

JFARZGFVMVRAJUIY

位移 5 加密 解密

EAVMUBAQHQMVEPDT

打开 ok 文件，都是 ook，第一眼我看呆了，这是啥，后来查了一下可知，又是一种加密方式，那就再找一个在线转换工具。



看到开头的 base32，那就再用 base32 工具转换（得把头给去了）

Base32编码解码

NFLEET2SO4YEWR3HN5AUCQKBJZJVK2CFKVTUCQKBKFIUCQKBIVCUGQKZIFAUCRCPINCW6S2BIFAU6V2VNRCVCVSSGRXE6MTBKM3DIRKOO53UIMZPGB3DO
V3ZINJVOOCHMNCTQ33LMJFXEQKPHBQSW3CBKNLC6MRTIFAUIKZVMM4WIQKBIRVWOQ2FIF3UCY2NIFIUCK2ZIFTUCOCBIZCECSKBKBDUCSKBMZGUCUKBJ5
AUI2DHIFAUQN2ZJU2GKL3WNIXWINBQM5CTANJZOZHG2YLYLJQW6L2KMIYXGM3YJMYFIVRWK52G25LNMFYGMYKZF5GFUMKRHF3TMY2WLBQXC4DNOVLVO4K
QPFLTSYSOHBJXIRJRMVWHEWTSOBWXCWBSNVIHSMTEKVIGGT3OIZLDE4LRLJZGY3DRNI4GY5SXPJTEK4SSJZMHAYJSME3FU4LMHFYGUODUNZLEIM2EOB4F
MZDROFWWCNK2MFXS6STCGFZTG6CLGBKFMNSXORWXK3LBOBTGCWJPJRNDCUJZO43GGVSYMFYXA3LVK5LXCUDZK44WETRYKN2EKMLFNRZFU4TQNVYVQMTNK
B4TEZCWJ5FU66BRNRXHON2OJRAXGVLVOR5HGTCJMJ3XMNLNFNVUE2SDFM3XC3LHPFCVKTLOGBUE2WKUGNSFKMCIKF4WQ2ZLNNFGSQ2PF5ZG2ZZWI5KU22

编码 解码 清空

iVBORw0KGgoAAAANSUhEUgAAAQQAAAEECAYAAADOCEoKAAAOWUlEQVR4nO2aS64ENwwD3/0v7WyCSW8GcE8okbKrAO
8a+lASV/23AAD+5c9dAADkgCEAwAcMAQA+YAgA8AFDAIAPGAIAfMAQAOADhgAAH7YM4e/vj/d40gE059vNmaxZao/Jb1s3x
K0TV6WtmumapfaY/LZ1Q9w6cVXaqpmuWWqPyW9bN8StE1elrZrpmqX2mPy2dUPcOnFV2qqZrllqj8lvWzfErRNXpa2a6Zql9pj8
tnVD3DpxVdqqma5Zao/Jb1s3xK0TV6WtmumapfaY/LZ1Q9w6cVXaqpmuWWqPyW9bN8StE1elrZrpmqX2mPy2dVOKOx1lnw7
NLAsUutzsLIbwv5m+kBjC+7qmgyEUMn0hMYT3dU0HQyhk+kJiCO/rmg6GUMj0hcQQ3tc1HQyhkOkLiSG8r2s6GElh0xcSQ3hf1
3QwhEKmLySG8L6u6WAIhUxfSAzhfV3TGW8IqQt0Qp8OzVJx7Ub3DOR9didNFfaEPh2apeLaje4ZyPvsTpoq7Al9OjRLxbUb3TOQ
99mdNFXYE/p0aJaKaze6ZyDvsztpqrAn9OnQLBXXbnTPQN5nd9JUYU/o06FZKq7d6J6BvM/upKnCntCnQ7NUXLvRPQN5n91JU

转码后发现末尾还有“==”，那就再试试 base64 试试，结果发现文本头是 PNG

那就看看能不能 base64 转成图片，找了半天的工具，终于找到了，并转化成了图片。

扫码即得 flag。

虽然没做出来几道，当时我感觉还是挺有趣的，所以写了这份 wp，用来“感谢”出题者，嗯，就是这样。