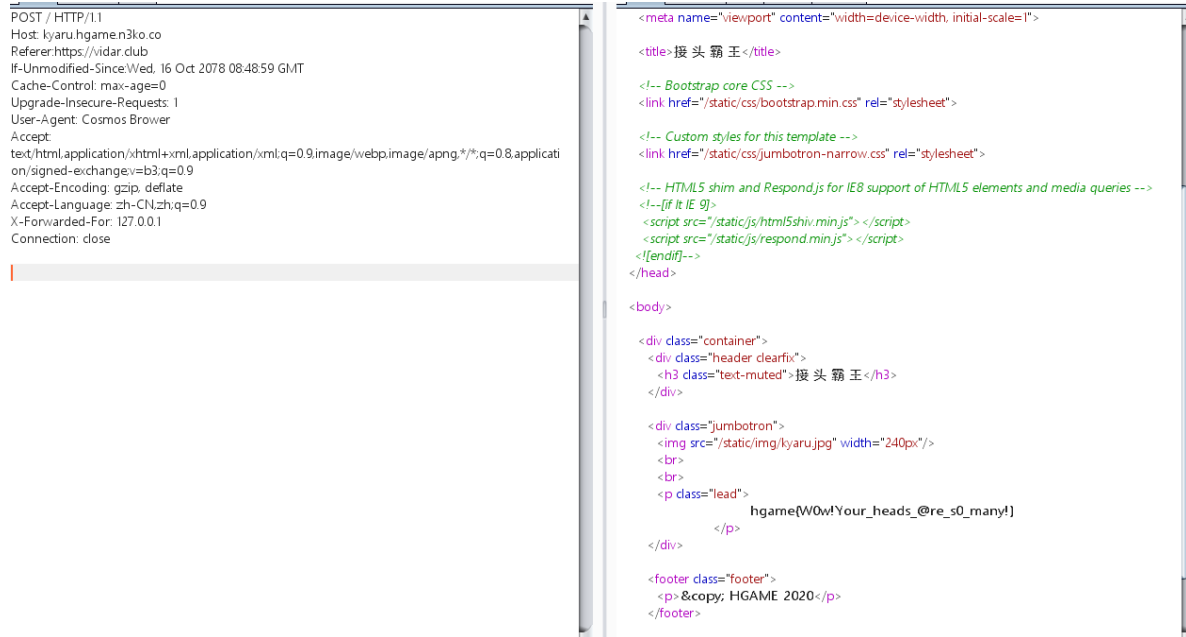


Hgame_2020_Week-1_Write-up

Web

接头霸王

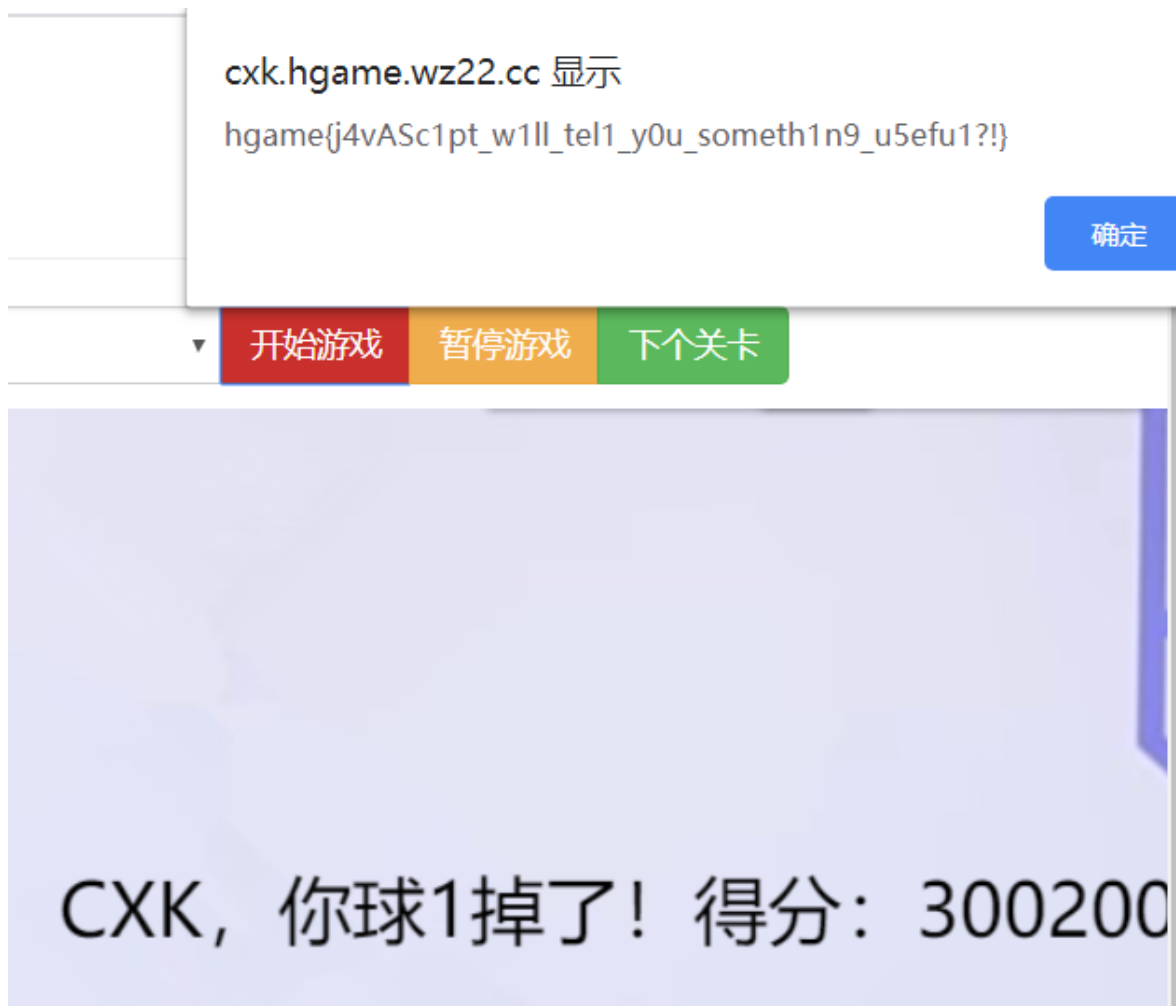
上来就看了这题，拿到一血还是挺开心的（后来好像把GET改成了POST），根据题意依次改Referer、X-Forwarded-For、User-Agent、POST请求方式、If-Unmodified-Since



尼泰玖

F12在Network里面找到game.js，猜测可以通过改js代码进行绕过

直接在开头改storageScore=30000，globalScore=30000即可



Misc

签到

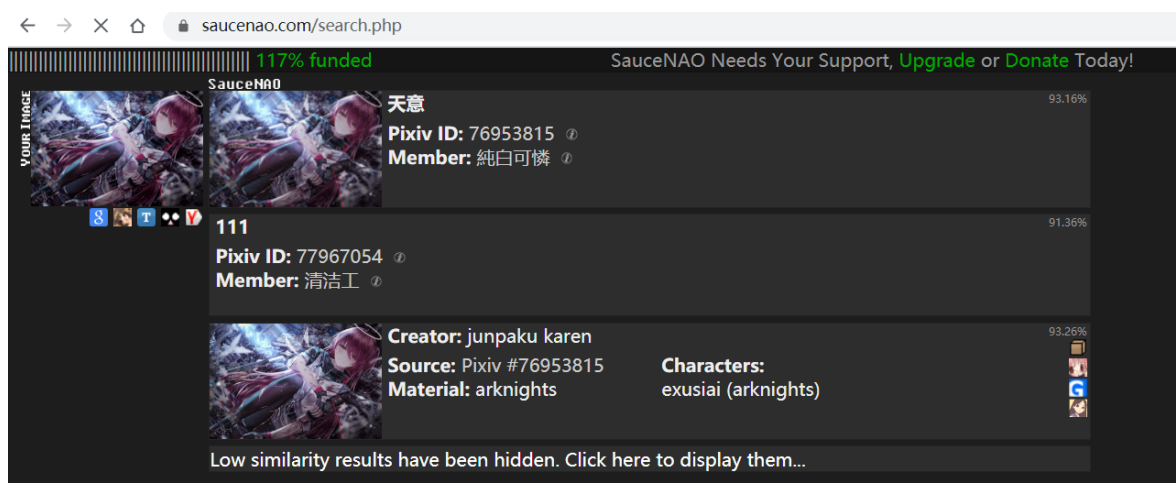
解base64再解摩斯电码得到字符串

W3LCOME_T0_2020_HGAM3

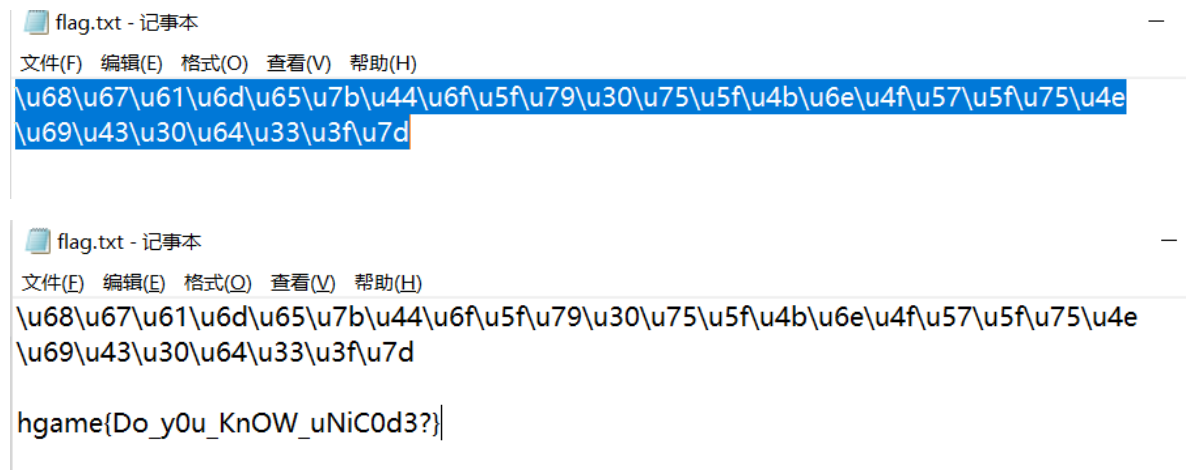
包上hgame{}即可

壁纸

题目给了一张图片，用010editor可以在图片末尾发现一个压缩包，打开需要密码，提示密码是pictureID，根据出题人的提示知道是pixiv的picture ID，直接搜索即可



拿到密码打开发现是unicode编码，进行解码即可。



克苏鲁神话

打开压缩包给了一个Bacon.txt和一个Novel.zip，Novel.zip里面还有一个Bacon.txt，猜测需要进行明文爆破，根据出题人的提示需要将Bacon.txt用7z进行压缩，再进行明文爆破可以拿到破解的压缩包



发现打开doc需要密码

回到Bacon.txt，发现上面的一段话大小写很奇怪，于是猜测先将其大小写转换为A和B

这里上一个脚本转为A和B

```
#include <iostream>

using namespace std;

int main()
{
    string A;

    A="ofSuChGrEAtpowersORbeINGStHeremayBEconCEivAblyASuRvIalofHuGelyREMoTEperiod"
    ;
    for(int i=0;i<75;i++)
    {
        if(A[i]>='a'&&A[i]<='z')
        {
            A[i]='A';
        }
        else{
            A[i]='B';
        }
    }
}
```

```
}  
cout<<A;  
}
```

AABABABABBAAAAAABBAAABBBABAAAAAABBAAABBAABAAABBABABAAAABBABABAAABBABBBAA
AABA

拿到网址<https://tool.bugku.com/peigen/>解培根密码即可

FLAGHIDDENINDOC
flaghiddenindod

解密 加密

输入密码在doc的末尾找到了flag



hgame{Y0u_h@Ve_F0Und_mY_S3cReT}

每日推荐

题目给了一个流量包，经过出题人提示流量包的大小有异常，在流量包里面找的POST包，发现了一个zip文件，（这里遇到了很多坑，首先是没有用流量包分析，直接binwalk+foremost提取的文件，发现总是存在格式错误，之后才追踪POST包的TCP流把POST的zip文件源码保存下来自己删减）将其保存即可，打开压缩包提示是6位数字，尝试爆破，拿到MP3文件，再在Audacity里面打开进行分析得到flag

Password successfully recovered !

Advanced Archive Password Recovery statistics:	
Total passwords	759,369
Total time	53s 130ms
Average speed (passwords per second)	14,292
Password for this file	759371
Password in HEX	37 35 39 33 37 31

 Save...  OK



Crypto

InfantRSA

题目直接给了p、q、e、c，上脚本解密得到m

```
def egcd(a, b):
    if a == 0:
        return (b, 0, 1)
    else:
        g, y, x = egcd(b % a, a)
        return (g, x - (b // a) * y, y)
def modinv(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
        raise Exception('modular inverse does not exist')
    else:
        return x % m

p=681782737450022065655472455411
q=675274897132088253519831953441
e=13
c=275698465082361070145173688411496311542172902608559859019841
d=modinv(e,(p-1)*(q-1))
n=p*q
m=pow(c,d,n)
print(m)
```

得到m=39062110472669388914389428064087335236334831991333245

这里将十进制数字m转为16进制再转字符串得到flag：hgame{t3Xt6O0k_R5A!!!}

Affine

查了一下，Affine是仿射密码，（也许是运气不错）根据前面的hgame{字符串推测出了A和B的值
A=13, B=14, 用脚本跑出了flag

```
import gmpy2

TABLE = 'zxcvbnmasdfghjklqwertyuiop1234567890QWERTYUIOPASDFGHJKLZXCVBNM'
m='A8I5z{xr1A_J7ha_vG_TpH410}'
A=13
B=14
MOD = len(TABLE)
#print(MOD)
cipher = ''
for b in m:
    i = TABLE.find(b)
    if i == -1:
```

```

        cipher+=b
    else:
        for x in range(MOD):
            if ((i+x*MOD)-B)%A==0:
                y=int(((i+x*MOD)-B)/A)
                cipher+=TABLE[y]
                print (cipher)
                break
            else:
                x=x+1

print(cipher)
# A8I5z{xr1A_J7ha_vG_TpH410}

#46=(A*12+B)%62
#33=(A*11+B)%62
#43=(A*7+B)%62
#计算出A=13, B=14

```

```

h
hg
hga
hgam
hgame
hgame {M
hgame {M4
hgame {M4t
hgame {M4th
hgame {M4th_u
hgame {M4th_u5
hgame {M4th_u5E
hgame {M4th_u5Ed
hgame {M4th_u5Ed_i
hgame {M4th_u5Ed_iN
hgame {M4th_u5Ed_iN_c
hgame {M4th_u5Ed_iN_cR
hgame {M4th_u5Ed_iN_cRY
hgame {M4th_u5Ed_iN_cRYp
hgame {M4th_u5Ed_iN_cRYpt
hgame {M4th_u5Ed_iN_cRYpt0
hgame {M4th_u5Ed_iN_cRYpt0}

```

Re

嗯，不会。

Pwn

嗯，不会。

这周1e1e菜🐷好像没咋做题Q@Q，不过的确有很多没有弄懂的东西，还要继续努力，比如.git泄漏做到一半就没思路了，准备康康dalao的WP学习学习，2333333

