hgame 第一周 writeup

id: XiaoYao52110

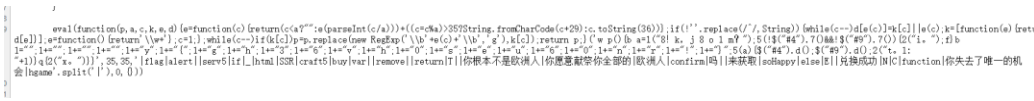
作为一个大二的老萌新，不冲奖来，不过还是学到了不少东西，也写个 writeup 来玩一玩吧。能加凑个协会名额就更好啦...

一 web

web 题可以说是很符合和谐社会要求了呀~

1. Are you from Europe?

随便抽了几次发现抽不到(果然非酋本体)，查看源代码，尝试修改晶石数据，然而并没有什么卵用，而且抽了 100 次以后翻倍还是抽不到。脑洞一开把源码复制到本地，可以运行，那就可以为所欲为了。



```
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)]]); }
        }
```

第一张图其实 flag 就在里面，不过懒得读，第二张图，显然就是概率，改一下丧心病狂一万个 0，改成 0.85，一次出。flag 忘记了，不挂了...

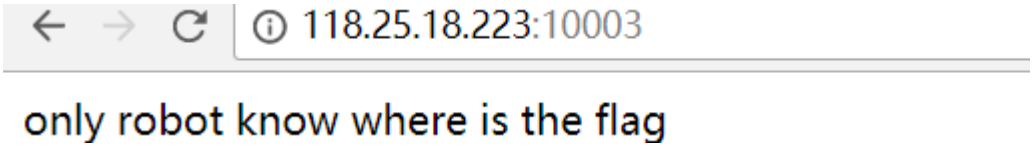
2. special number

忘了提示是什么时候出的了，开始想正则想了好久，不过试一试就知道格式了，至少 7 位，字母加数字。

```
$lock="**********";
$b = json_decode($key);
if($b==$lock)
    echo $flag;
```

这里比较用的是两个等号，php(是世界上最好的语言)不会审计类型，所以可以传奇怪的东西。开始以为是 json 类型的漏洞，传数字和字符串比，结果不行。某天突发奇想穿了个科学记数法就可以了。(果然科学记数法也是数字。)

3. can u find me?



第一步，看 robots.txt 记得加's'...（笑）

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

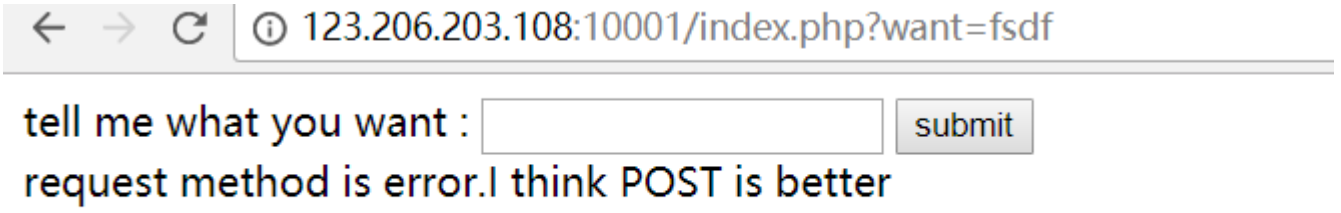
查看 flag.php

burp 截包

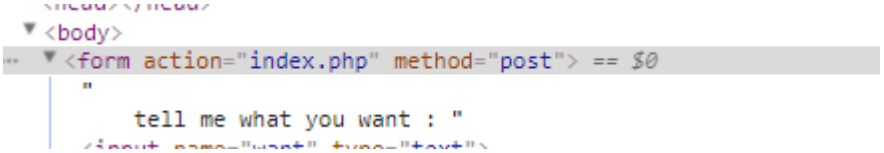
```
GET //f1aaaaaaaag.php HTTP/1.1
Host: 118.25.18.223:10003
Proxy-Connection: keep-alive
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
DNT: 1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: user=guest
```

user=admin 就行了

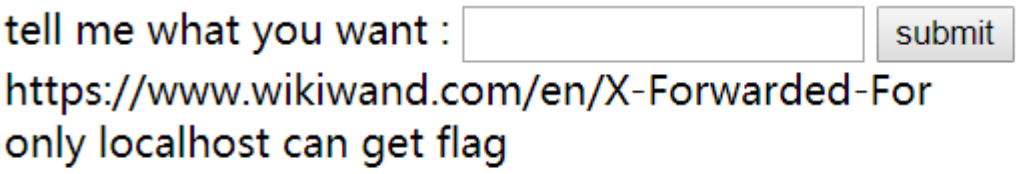
4. tell me what you want



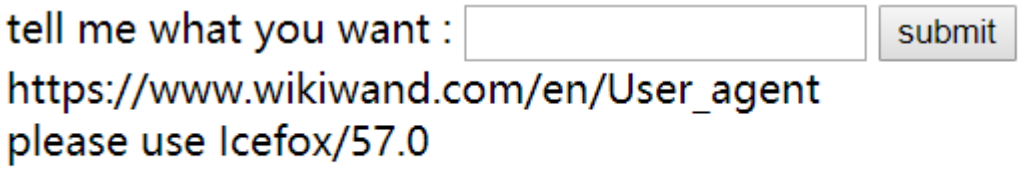
先打开随便输，改为 post，最简单的不是构造 burp 包，而是 f12...



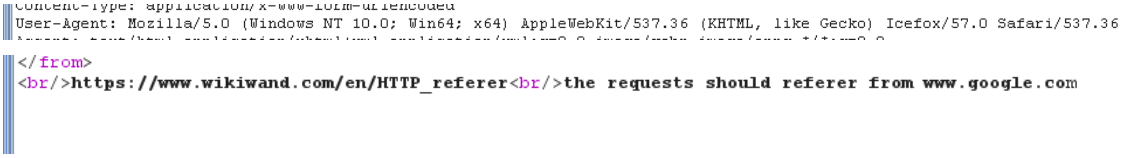
卖蛇的改为 post，然后截下来...
对了，记得 send to repeater，不然每次改起来很累的...



localhost，以为是 cookie 的问题，并卵，看维基了解是把 x-blabla 改为本地地址：127.0.0.1



用 icefox 浏览器，你要什么我就改什么...



refererfromgoogle 改 referer/p.s.referer 拼错了，不过将错就错吧。
改 referer,不要自作聪明加 http 或者 https 我就是这里卡的怀疑人生。

可以的到 flag 的数据包：

raw | params | headers | hex

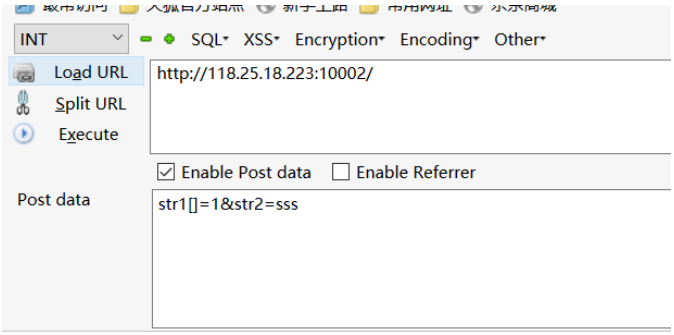
```
POST /index.php HTTP/1.1
Host: 123.206.203.108:10001
Proxy-Connection: keep-alive
Content-Length: 9
Pragma: no-cache
Cache-Control: no-cache
Referer: www.google.com
Origin: https://www.google.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Icefox/57.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
DNT: 1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
X-Forwarded-For: 127.0.0.1
Cookie: keyofcookie=valueofcookie; isadmin=1

want=flag
```

5.我们不一样

之前正好做过一个这样的题

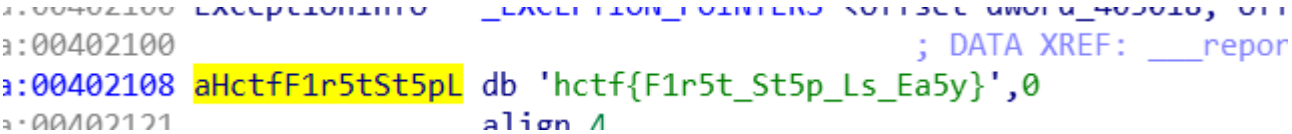

```
include_once("flag.php");
if(isset($_POST['str1'])&&isset($_POST['str2'])){

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

利用 strcmp 比较数组和字符串返回 0 的漏洞，传递一个数组和字符串就行。唯一做的速度最快的一道题，手速不够。



二.re

1.re0.exe//这个 0 看着好奇怪



丢进 ida 一进去就看到 flag，还对了...

3.其实不太了解建立窗口的前前后后，我大概学了一个假 c 语言。

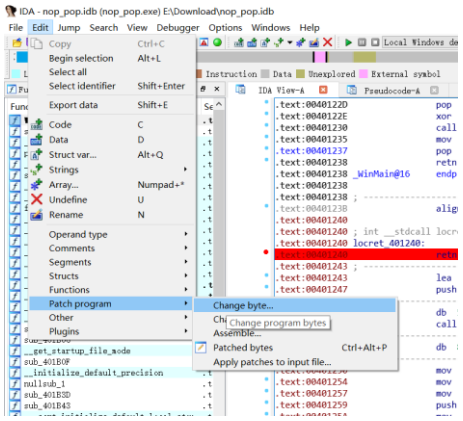
丢进 ida，f5/实在太乱，粗略看一下结构。

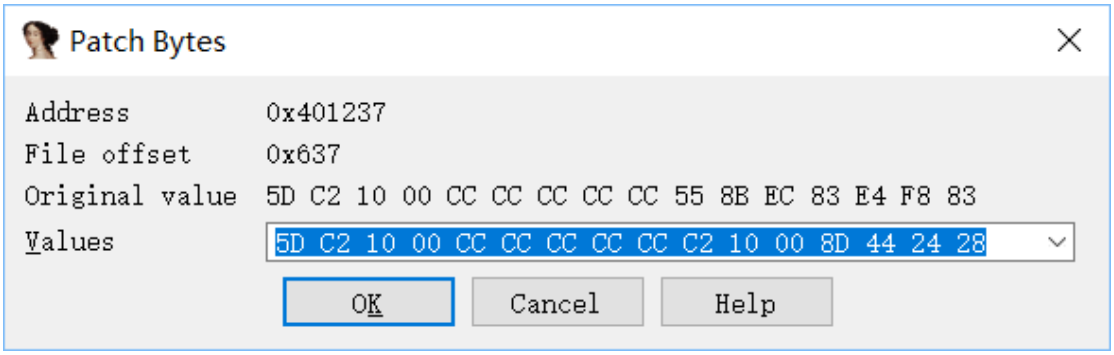
```
4  WNDCLASSW v6; // [esp+44h] [ebp-2Ch]
5
6  WndClass.style = 3;
7  WndClass.lpfnWndProc = locret_401240;
8  WndClass.cbClsExtra = 0;
9  WndClass.cbWndExtra = 0;
10 WndClass.hInstance = hInstance;
11 WndClass.hIcon = LoadIconW(0, (LPCWSTR)0x7F00);
12 WndClass.hCursor = LoadCursorW(0, (LPCWSTR)0x7F00);
13 WndClass.hbrBackground = (HBRUSH)GetStockObject(0);
14 WndClass.lpszMenuName = 0;
15 WndClass.lpszClassName = L"nop_me";
16 if ( !RegisterClassW(&WndClass) )
17   MessageBoxW(0, L"ERROR!\n", L"Wnd1", 0x10u);
18 v6.style = 3;
19 v6.lpfnWndProc = sub_401380;
20 v6.cbClsExtra = 0;
21 v6.cbWndExtra = 0;
22 v6.hInstance = hInstance;
23 v6.hIcon = LoadIconW(0, (LPCWSTR)0x7F00);
24 v6.hCursor = LoadCursorW(0, (LPCWSTR)0x7F00);
25 v6.hbrBackground = (HBRUSH)GetStockObject(0);
26 v6.lpszMenuName = 0;
27 v6.lpszClassName = L"death_march";
28 if ( !RegisterClassW(&v6) )
29   MessageBoxW(0, L"ERROR!\n", L"Wnd2", 0x10u);
30 hWnd = CreateWindowExW(0, L"nop_me", L"pop team epic", 0xCB0000u, 200, 120, 631, 359, 0, 0, hInstance, 0);
31 ShowWindow(hWnd, nShowCmd);
32 UpdateWindow(hWnd);
33 dword_4043C4 = CreateWindowExW(0, L"death_march", aFlag, 0xCF0000u, 600, 350, 400, 100, 0, 0, hInstance, 0);
34 ShowWindow(dword_4043C4, nShowCmd);
35 UpdateWindow(dword_4043C4);
36 WndClass.hCursor = (HCURSOR)dword_4043C0;
```

能看出来 wndclass 是注册 nop_me 窗口，v6 是 flag 窗口的。目的就是把 wndclass 窗口搞破坏。百度了一下相关的去 rar 广告窗的事，一句话就是保持堆栈平衡的情况下直接 return。我第一次事把 createwindows 函数搞破坏了，创建第一个窗口的时候直接 return，然后第二个的时候改回来，得到的也应该是可以换 flag 的效果，但这只是改内存，如果改程序这样应该是不行的，建立窗口函数是固定的，改了就变了。想了想不影响系统窗口的方法。注意代码的第 7 行，点进那个函数：locret_401240,里面是窗口注册相关的东西，音乐，显示文字什么的。然后我就把这个函数 return 掉，

```
.text:00401238 _WinMain@16     endp
.text:00401238
.text:00401238 ; ---------------------------------------------------------------------------
.text:0040123B                 align 10h
.text:00401240
.text:00401240 ; int __stdcall locret_401240(HWND hWnd, UINT Msg, WPARAM wParam, LPARAM lParam)
.text:00401240 locret_401240:                          ; DATA XREF: WinMain(x,x,x,x)+2C↑o
.text:00401240                 retn    10h
.text:00401243 ; ---------------------------------------------------------------------------
.text:00401243                 lea     eax, [esp+28h]
```

p. s. 操作：





这个是 return 那句话的 16 进制代码，最好在第一个 push 变量的地方就替换掉，因为没有 push，就不用费事 pop，维持堆栈平衡了(只是我的理解，理论没学太深)然后记得把替换掉的地方保存一下，以方便替换回来。/习惯而已。然后一路 f8 下去，就没有 nop 窗口了。

4.星际玩家

```
#include<iostream>
#include<cstring>
using namespace std;
#define c char
char str[]="KGQ@\\f\x19W{CJ\x13Ov|H\x15ILwJNTzV\x16RT";
char str5[]="hbve\x7fH2\x7fV|c?ReHIMte\x20rsJ\x60s\x7f|e";
c ss[]="hctf{N0t_fl4g__l0ok_cmp_p1z}";
c str1[8],str2[8],str3[8],str4[8];
c s1[8],s2[8],s3[8],s4[8];
c s[30]="11111111111111111111111111";
c s5[30];
void fun3(c str1[],c str2[],int n)
{
```

```
	for(int i=0;i<7;i++)
		str2[i]=n^(i+7*n)^str1[i+7*n];
}
void fun33(c str1[],c str2[],int n)
{
	for(int i=0;i<7;i++)
		str2[i]=str1[i+7*n]^(n^(i+7*n));
}
void fun2(c str1[],c str2[],c str3[],int n)
{
	for(int i=0;i<7;i++){
		str3[i]=str3[i+7*n]^0x34;
	}
	/*for(int i=0;i<28;i++)
		ss[i]=ss[i]^0x34;*/
	//cout<<str3<<endl;
	if(n>=0)fun3(str1,str2,n);
}
void fun1(c str1[],c str2[],c str3[],int n)
{
	for(int i=0;i<7;i++){
		str3[i]=(i+35)^str2[i+7*n];
	}
	//cout<<str3<<endl;
	if(n<35)fun2(str1,str3,str2,n);
}
void print(char a[])
{
	for(int i=0;i<7;i++)
	cout<<a[i];
}
int main()
{
	int i;
	//cout<<strlen(s)<<endl;
	fun1(s,str,str1,0);
	fun1(s,str,str2,1);
	fun1(s,str,str3,2);
	fun1(s,str,str4,3);
	//cout<<strlen(ss)<<' '<<ss<<endl;
	/*for(i=0;i<28;i++)ss[i]=ss[i]^0x34;
	for(i=0;i<28;i++)cout<<ss[i];cout<<endl;
/*	for(i=0;i<7;i++){
		s1[i]=ss[i];
```

```
            s2[i]=ss[i+7];
            s3[i]=ss[i+14];
            s4[i]=ss[i+21];
        }*/
        fun33(str5,s1,0);
        fun33(str5,s2,1);
        fun33(str5,s3,2);
        fun33(str5,s4,3);

        print(s1);print(s2);print(s3);print(s4);
        //cout<<strlen(ss)<<' '<<ss<<endl;
        //cout<<str1<<endl<<str2<<endl<<str3<<endl<<str4<<endl;
        //cout<<str5<<endl;
}
```

上面是运行出来的代码。hint 说是热键：n ida 的热键 n 是改名，然后我就把这些乱糟糟的名字改了一下，增加区分度。

```
  v13 = 0;
  printf("Input your flag: ");
  scanf_s("%s", &v4, 32);
  if ( strlen(&v4) != 28 )
  {
    printf("Never Give Up!\n");
    system("pause");
    exit(0);
  }
  fun1(&v4, &str, _str1, 0);
  fun1(&v4, &str, &str2, 1);
  fun1(&v4, &str, &str3, 2);
  fun1(&v4, &str, &str4, 3);
  if ( check(_str1, &str2, &str3, &str4, &str5, &str) != 1 )
  {
    printf("Never Give Up!\n");
    system("pause");
    exit(0);
  }
  printf("\nGood Job!\n");
  printf("Input is your flag\n");
  system("pause");
  return 0;
}
```

```
int __cdecl fun3(int a1, int a2, int a3)
{
  int result; // eax
  signed int i; // [esp+0h] [ebp-4h]

  for ( i = 0; i < 7; ++i )
  {
    *(i + a2) = a3 ^ (i + 7 * a3) ^ *(a1 + i + 7 * a3);
    result = i + 1;
  }
  return result;
}
```

fun1 里有 fun2，fun3 然而 fun1，fun2 都没什么用。传的最后一个参数总是满足函数最后的要求，都会运行 fun3. c 语言代码里有，具体看代码就行。

function1 里如果把得到的字符串全输出是个很像 flag 的东西，hctf{N0t_fl4g__l0ok_cmp_p1z}注意比较部分，本来也没想过 flag 会在这。仔细看代码，flag 经过一通异或之后编程 str5(c 代码里的)，那么就把 str5 的字符还原就行。由于分四段乱糟糟的，就仿照 fun3 写的，也分四段，感觉傻傻的。str2[i]=n^(i+7*n)^str1[i+7*n];

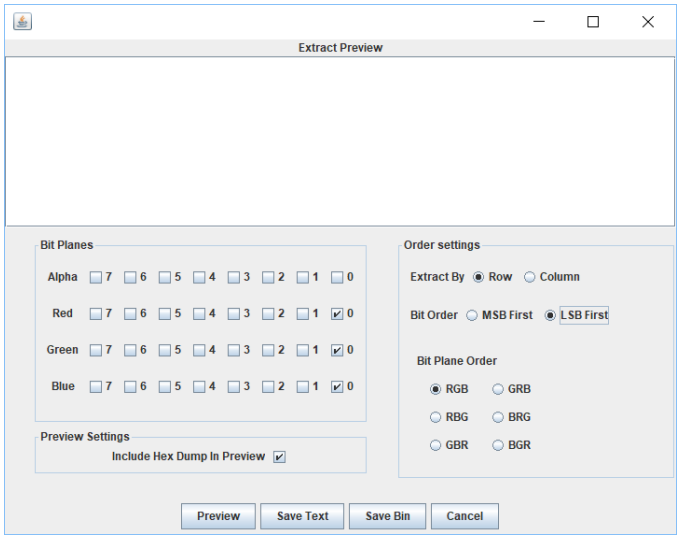
b=a^b^a,n^(i+7*n)是常数，所以把 str2[i]再异或一遍这个数就行了。直接运行出 flag。(代码丑，勿喷。)

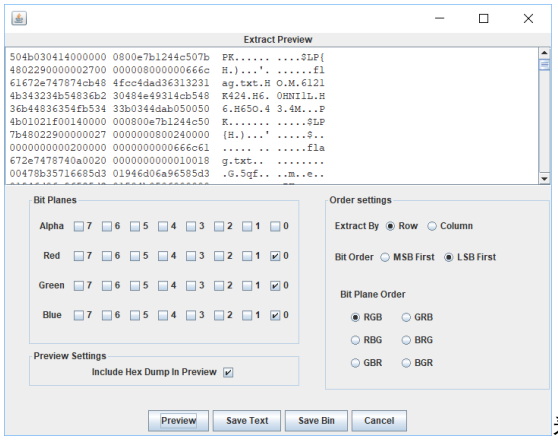
p.s. 韩宗还是真的，看不到 fun1，fun2，就能拿 flag。

三.misc

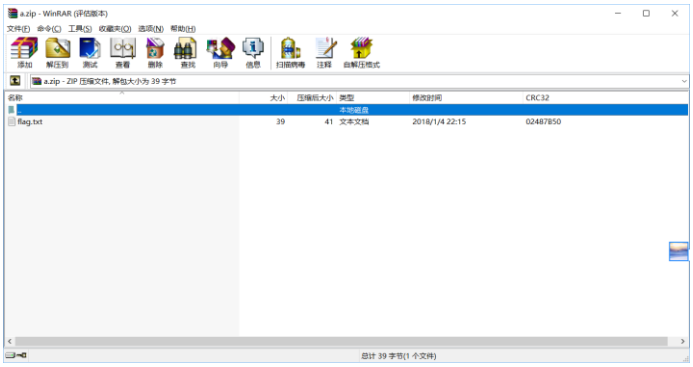
1.白菜 1

winhex 看一眼，没什么异常，png 文件，猜测是 lsb 隐写。/看过那个 ihdr 数据块没有异常。上神器。



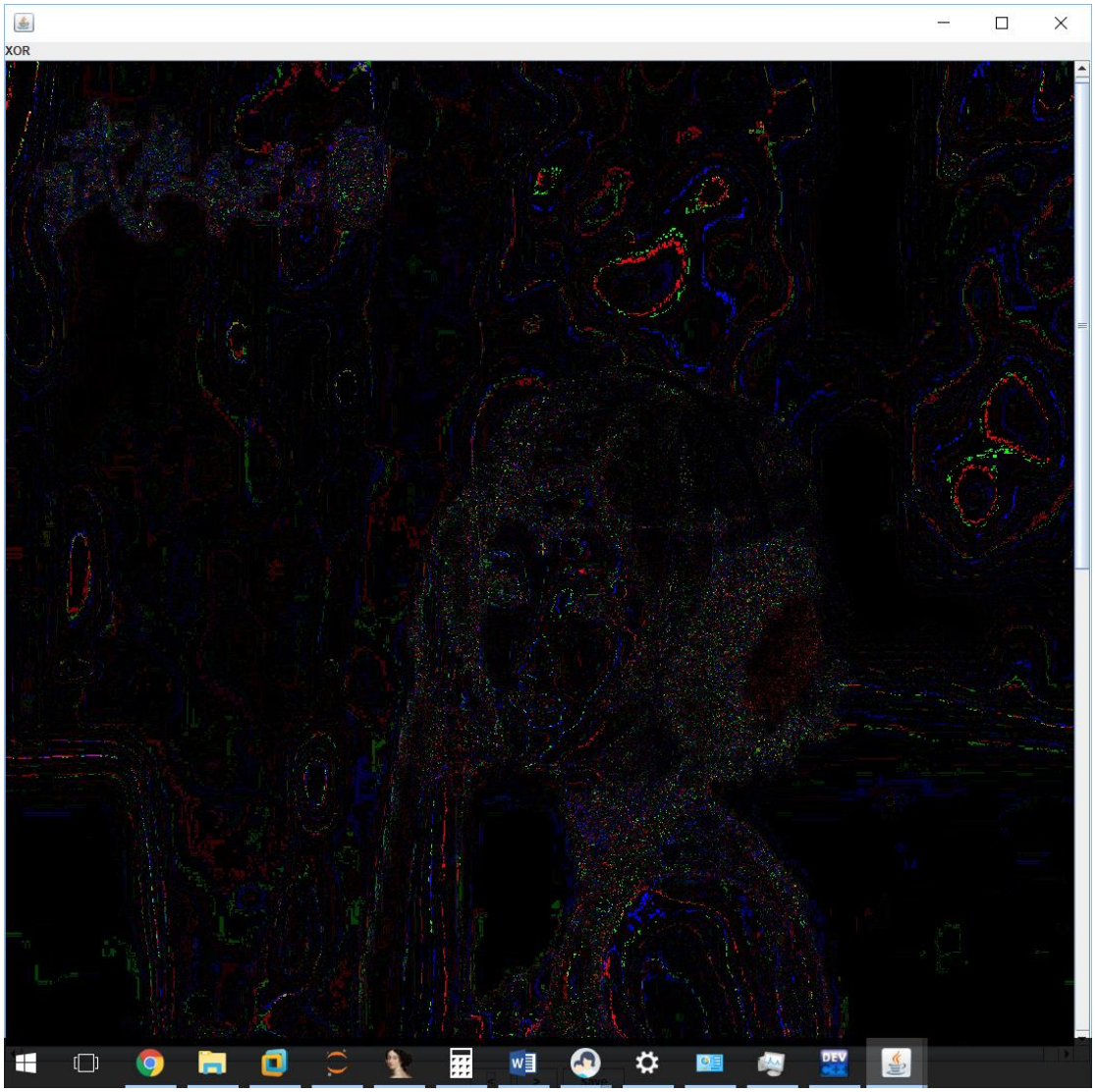


看开头，和右边 flag.txt，像是压缩文件，保存二进制为 zip 格式，



alt+r 修复一下，解压得 flag。

p.s.



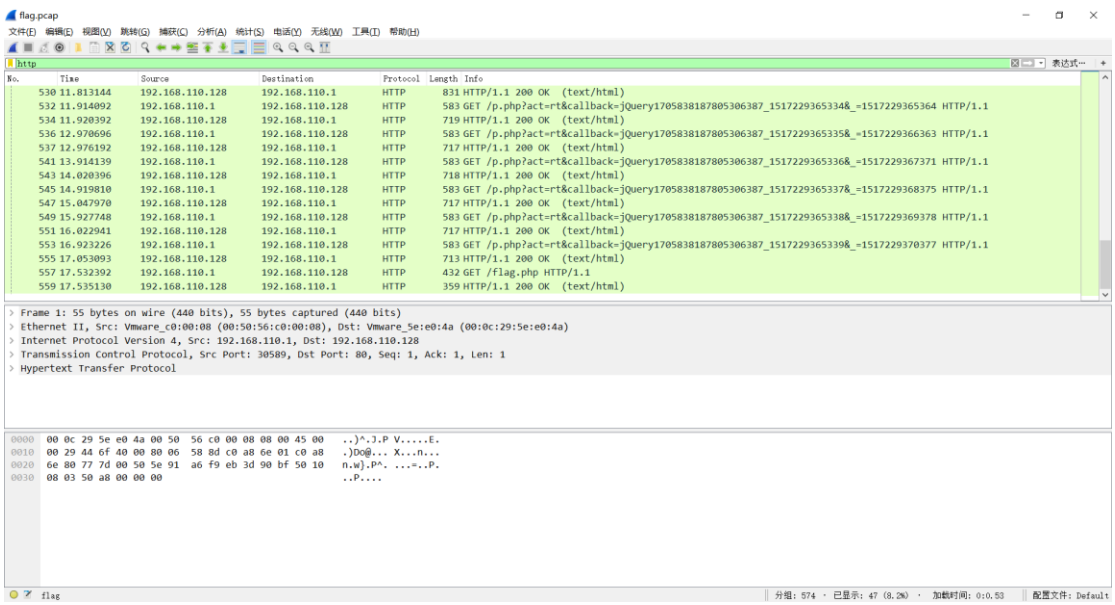
插曲，找到原图异或了一下，确实是有差别的。

2.白菜 2

图种，下载，改为 zip，解压得 flag。可以用 winhex 看一眼，判断一下。

3.数据包

wireshark 打开，筛选 http 流，发现 flag.php

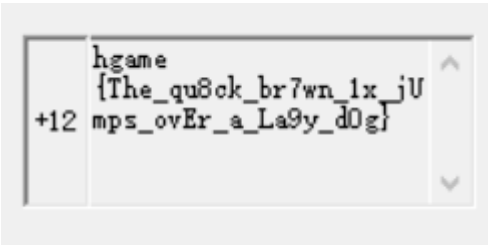


追踪 http 流，拖到底，发现 flag。

四，密码学

1.凯撒

{} 在这，前面肯定是 hgame



考察一下英文字母，quick，brown，lazy，变换一下，就得到了 flag

2.看一下介绍，就知道怎么做了。脚本如下。

In [25]:
```
list=[
    ['b','t','a','l','p'],
    ['d','h','o','z','k'],
    ['q','f','v','s','n'],
    ['g','i','c','u','x'],
    ['m','r','e','w','y'],
]
dic={'F':2,'A':0,'D':1,'G':3,'X':4}
print(list[dic['F']][dic['D']])
```

```
f
```

In [26]:
```
str='FDXDGDADDG_FXXFAAXFAG_GDFXFFXFFXADXFDA_GDAD'
str=str.split('_')
print(str)
l='hgame{'
for i in str:
    for j in range(0,len(i)-1,2):
        print(list[dic[i[j]]][dic[i[j+1]]],end='')
        l=l+list[dic[i[j]]][dic[i[j+1]]]
    print('_',end='')
    l=l+'_'
l=l+'}'
print('\n',l)
```

```
['FDXDGDADDG', 'FXXFAAXFAG', 'GDFXFFXFFXADXFDA', 'GDAD']
fritz_nebel_invented_it_
 hgame{fritz_nebel_invented_it_}
```

最后多加了一个-
密码学其他都有思路，但跑出来的是错的，可惜了…