### Hgame2018week2

### Web 部分

## 0x01 最简单的 sql 题

在用户名输入 admin'#, 得到 flag: hgame{@s0ng\_fen\_ti@}

Misc 部分

#### 0x01 White cosmos

打开压缩文件得到一个空白的 pure.txt, 先将内容复制到 word 里改变字体颜色发现没用 (好吧是我天真了

用 winhex 分析发现内容全都是水平制表符和空格,面向百度做题半天也没看见个相关的,

0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	ANSI ASCII
09	09	20	09	20	20	20	20	09	09	20	20	09	09	09	20	
09	09	20	20	20	20	09	20	09	09	20	09	09	20	09	20	
09	09	20	20	09	20	09	20	09	09	09	09	20	09	09	20	
09	20	09	20	09	09	09	20	09	09	20	20	09	20	09	20	
09	09	20	09	09	20	20	20	09	09	20	20	20	09	09	20	
20	09	09	20	20	20	20	20	09	09	20	09	09	20	09	20	
09	09	20	20	09	20	09	20	09	20	09	09	09	09	09	20	
20	09	09	20	20	09	20	20	09	20	09	09	09	09	09	20	
09	20	09	20	09	09	09	20	09	09	20	09	20	20	20	20	
09	20	20	09	20	20	09	20	09	09	09	20	09	20	20	20	
09	09	20	20	09	20	09	20	09	20	09	09	09	09	09	20	
09	09	09	20	20	09	09	20	09	09	09	20	20	20	20	20	
20	09	09	20	09	20	20	20	09	09	20	20	20	09	09	20	
09	09	20	20	09	20	09	20	09	09	09	09	09	20	09		

忽然想到可以用二进制表示, 于是得到 2 串二进制数

٠--

想到可以每 8 个一组转换为 16 进制再转换为 ascii,由于总共只有 207 位所以在前面补 1 个 0.,由第一串数得到 flag;:hgame{Welc0me\_2\_Whlte\_sp4ce}

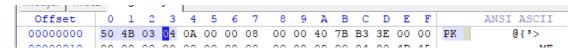
### 0x02 easy password

一个有密码的压缩包,提示密码是小写字母+数字,把压缩包丢到 Ziperello 里面跑出来密码是 hgame18,打开得到 flag:hgame{0pos\_You\_5ound\_m3\_HAHA}

## 0x03 mysterious file header

Winhex 打开发现 META-INF, 估计是个 jar 包, 后缀加上.jar 之后发现打不开, 和现成的 Stegsolve.jar 比较发现文件头不对, 把文件头改为504B0304后得到一个可以打开的jar 包。

Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F			ANSI ASCII
00000000	30	40	05	B4	14	00	08	08	08	00	DA	06	3F	4C	00	00	00	1	Ú ?L



打开后得到 4 个数字, 118 54 29 89, 感觉是一个 ip, 然而并不能访问 118.54.29.89, 看提示 4\*3\*2\*1=24 以为是一个端口号, 但是尝试 118.54.29.89:11000 也不行。之后偶然间查到 118.54.29.89 这个 ip 在韩国=-=于是想尝试换一下顺序, 最后查到 118.89.29.54 和 118.89.54.29 是 2 个广州的腾讯 ip, 试之,发现 118.89.29.54 是正确的,得到 flag:

hgame{Y0u\_Mu5t\_know\_f1le\_header\_and\_java}

所以 4\*3\*2\*1=24 是个啥提示呢=-=

# Crypto 部分

#### 0x01 Caesar&&Caesar

把文件里的密文丢到 <a href="https://www.guballa.de/vigenere-solver">https://www.guballa.de/vigenere-solver</a><a href="https://www.guballa.de/vigenere-solver]</a><a href="https://www.guballa.de/vigenere-solver]</a><a href="https://www.guballa.de/vigenere-solver]</a><a href="https://www.guballa.de/vigenere-solver]</a><a href="https://www.guballa.de/vigenere-solver]</a><a href="https://www.guballa.de/vigenere-solver]</a><a href="https://www.guballa.de/vigenere-solver]</a><a href="https://www.guballa.de/v

#### 0x02violence

根据代码可以知道 cipher 中的 5f 全都为\_, 得到 191709050607090519\_0706\_0603150519\_03\_0a0706\_170c\_1407170205101105, 从 03 入手, 因为是英文句子猜测 03 为 a,a\*(97-97+b)% 26 = ab=3, 把剩下的密文丢到 http://rumkin.com/tools/cipher/affine.php 网站中的 b 为 3, 测试得当 a 为 7 的时候能形成有意义的词语,得到 flag:{sometimes\_it\_takes\_a\_bit\_of\_violence}