# makerctf writeup

队伍 ID：膜拜楼上大佬队

队长q号：944988050

参赛队员：

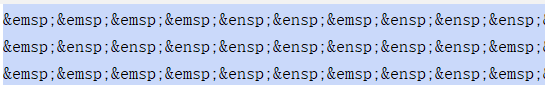
|  |  |  |
| --- | --- | --- |
| 姓名 | 学号 | qq |
| 张森泽 | 17140120009 | 1139207868 |
| 任中豪 | 16010120042 | 505254032 |
| 梁朝珲 | 15020140022 | 944988050 |

### Nazo

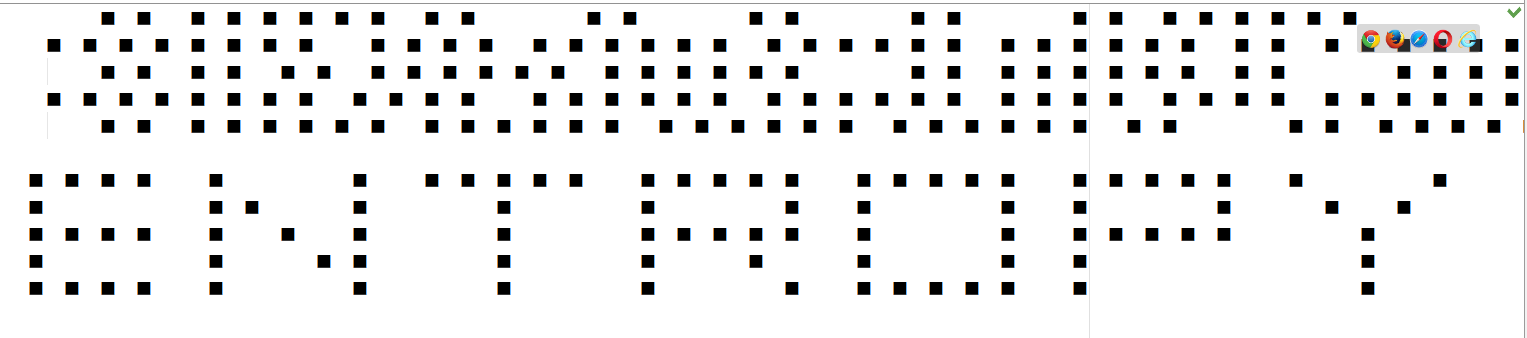
### **By张森泽**

LV1 ~ LV16 易得

LV17 ：



分别用 ■ 和 全角空格 替换可得flag



Moe

### **By张森泽**

盲水印:



### Pcap

### **By张森泽**

wireshark 看有girlfriends 的dalao们对话可知密文以及加密算法的pyc

把pyc转换成py然后分析算法，最后我们得出的解密脚本如下：

import string, sys, random

from base64 import b64encode, b64decode

password=""

enc\_ciphers = [

'rot13', 'b64e', 'caesar']

str1='1'

str2='2'

str3='3'

def rot13(s):

\_rot13 = string.maketrans( 'NOPQRSTUVWXYZnopqrstuvwxyzABCDEFGHIJKLMabcdefghijklm','ABCDEFGHIJKLMabcdefghijklmNOPQRSTUVWXYZnopqrstuvwxyz')

return string.translate(s, \_rot13)

def b64d(s):

return b64decode(s)

def caesar(plaintext, shift=23):

alphabet = string.ascii\_lowercase

shifted\_alphabet = alphabet[shift:] + alphabet[:shift]

table = string.maketrans(alphabet, shifted\_alphabet)

return plaintext.translate(table)

for num in range(1,24):

choice = password[0]

password = password[1:]

if choice == '1':

password=rot13(password)

elif choice == '2':

password=b64d(password)

else:

password=caesar(password)

print password

Rel\_password=b64d(password)

print Rel\_password

### Easy RSA

### **By张森泽**

OpenSSL分解公钥得到n，上 RSA Tool 分解 n 得到 d，然后解密密文可得flag

此题和下一题解密 RSA 是用的自己写的垃圾APP，源码太长不放了，原理是用n d还原私钥，然后解密读入的密文byte流，截图如下：



### Get\_flag

### **By张森泽**

用 dex2jar 把dex转换成jar然后再用jd-gui读源码，可以发现是RSA加密，以及密文和私钥，然后解密即可，解密工具及原理同上题



贪吃蛇

### **By任中豪**

用IDA打开，发现01010101构成的地图十分瞩目

然后再使用UltraEdit把地图内部的所有墙体删了，非常轻松的就吃完了

（如果还是手残推荐使用变速齿轮降速2.56倍）



我的世界

### **By任中豪**

挖矿挖矿挖矿挖到钻石合一把钻石剑一身铁套

砍砍砍砍砍

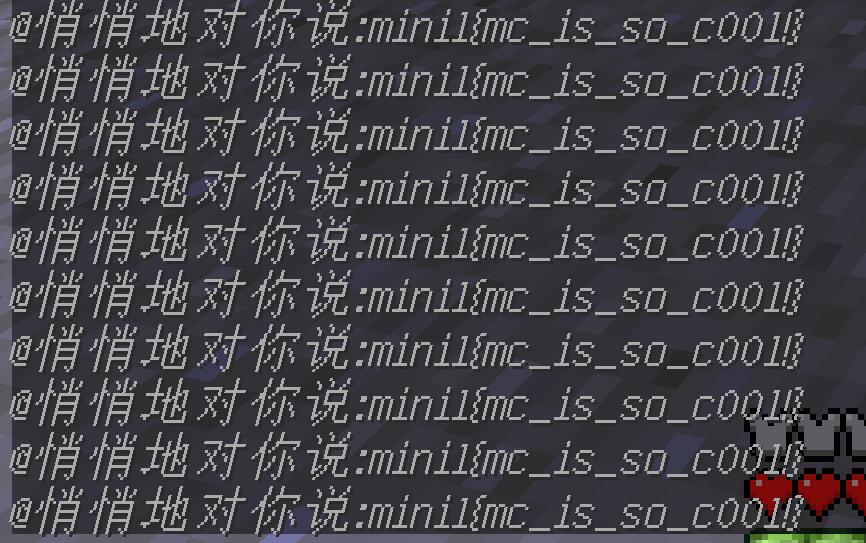
养鸡喂鸡喂鸡喂鸡喂鸡喂鸡

砍怪砍怪砍怪砍怪

喂鸡喂鸡喂鸡喂鸡喂鸡

杀鸡杀鸡杀鸡够了

（PS：我还想接着玩hhhhh盖个城堡之类的。



### easy bypass

### **By梁朝珲**

有源码 拉到本地测试并加一些echo然后传入要输入的参数

<?php

#highlight\_file(\_\_FILE\_\_);

if(empty($\_POST['hmac']) || empty($\_POST['host'])){

header('HTTP/1.0 400 Bad Request');

echo "1<br>";

exit;

}

$secret = getenv("SECRET");

echo "2<br>";

echo $secret;

echo "<br>";

if(isset($\_POST['nonce']))

{echo "3<br>";

$secret = hash\_hmac('sha256',$\_POST['nonce'],$secret);}

echo $secret;

echo "<br>";

$hmac = hash\_hmac('sha256',$\_POST['host'],$secret);

echo "4<br>";

echo $hmac;

echo "<br>";

if($hmac !== $\_POST['hmac']){

header('HTTP/1.0 403 Forbidden');

echo "5<br>";

exit;

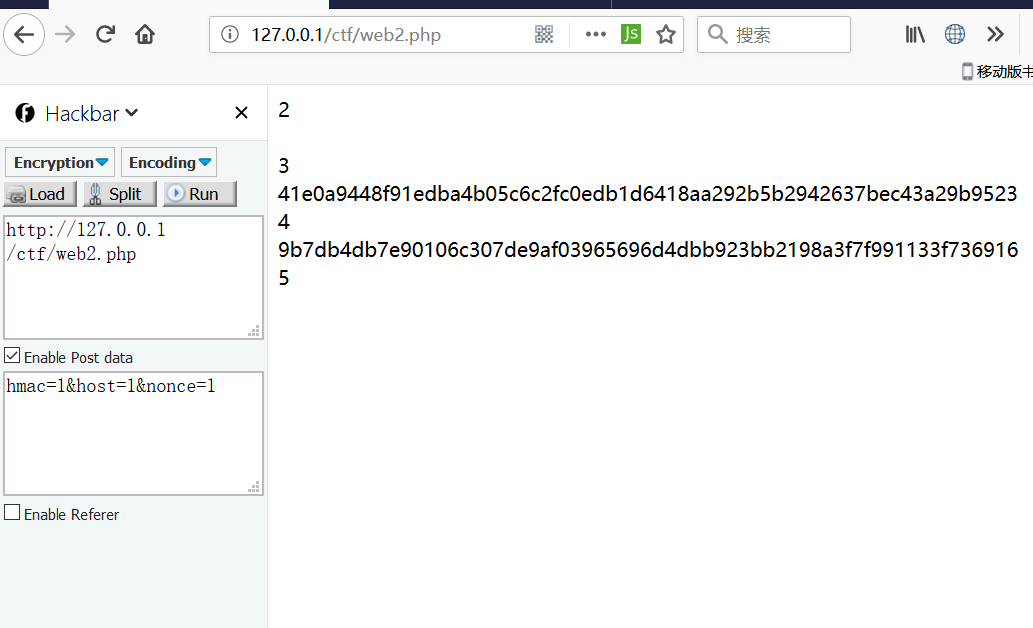
}

echo "6<br>";

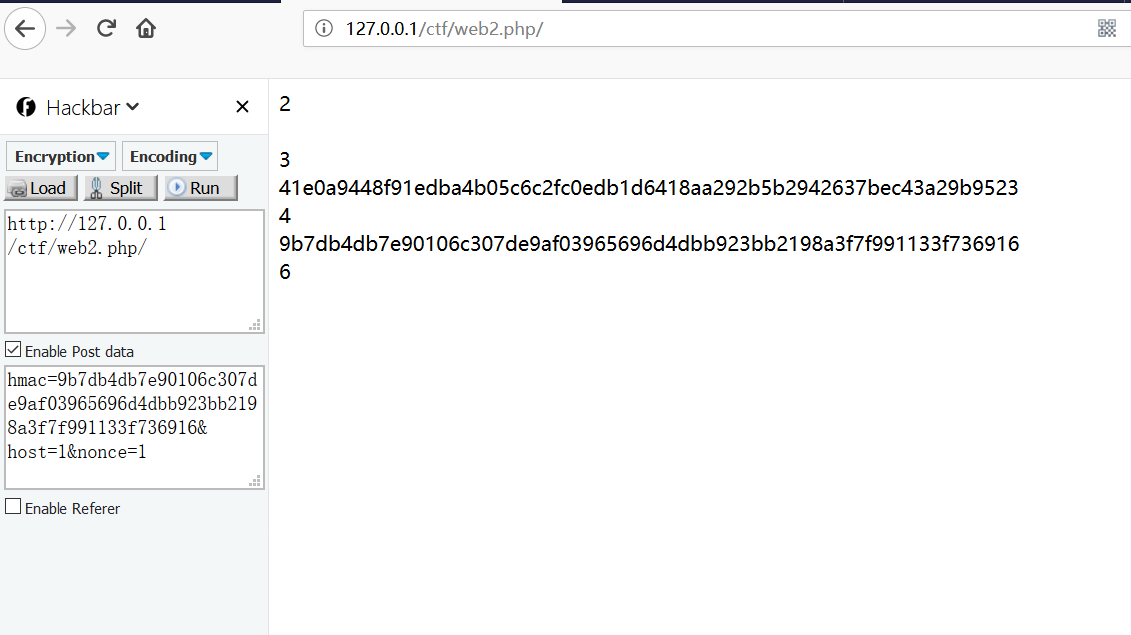
echo exec('cat ../flag.txt');

?>

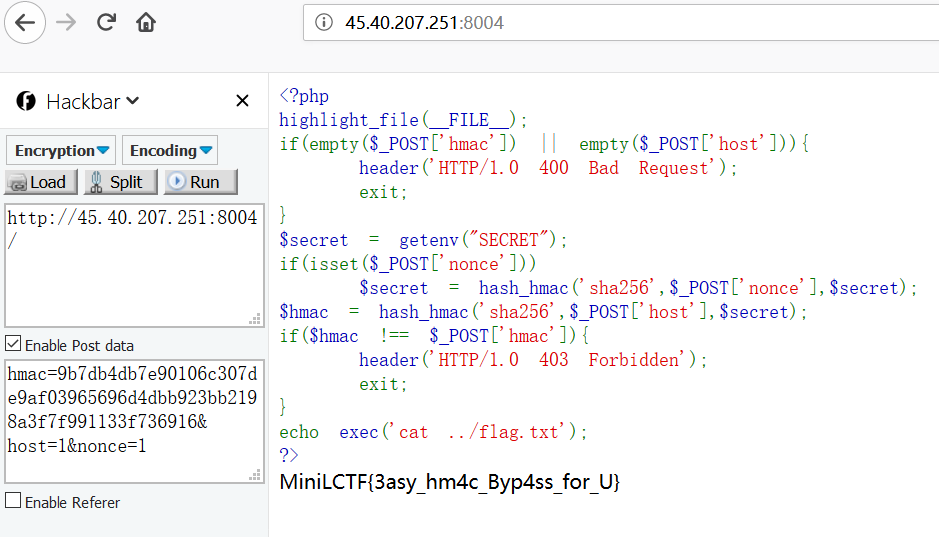
先将所有参数都用1提交，发现$hmac = hash\_hmac('sha256',$\_POST['host'],$secret);的值会变成9b7db4db7e90106c307de9af03965696d4dbb923bb2198a3f7f991133f736916，并且if($hmac !== $\_POST['hmac'])判断失败



要使flag输出，需要post进去的hmac和生成的$hmac相同，所以post中hmac填9b7db4db7e90106c307de9af03965696d4dbb923bb2198a3f7f991133f736916



然后将这些数据提交，得到flag



### see or do not see

### **By梁朝珲**

Pdf下载下来，打开后ctrl+a发现图片后面有一段文字



复制出来得到flag{security\_through\_obscurit}