1.ID: **937719a41b3ff1b9f617b2d63dcd743a 队长q**q:1628106561

2.队伍名crakeme

|  |  |  |
| --- | --- | --- |
| 名字 | 学号 | QQ |
| 张维维 | 15180120053 | 1628106561 |
| 文尧 | 17180110007 | 188006400 |
| 孙佳琳 | 17180120029 | 905907362 |

1.[Linear\_algebra](https://makerctf.com/static/uploads/73d3e86a14cc2522426ac334afbe74c7/Linear_algebra.exe) writeup.(大三)

一。题目用到的数据

a[29][29]的矩阵

a[29][29]={

0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 }；

b[29]

{

b4c

b30

b2b

b30

b4d

b56

b45

b53

b1e

b22

b34

b2d

b36

b2a

b2c

b34

b3a

b25

b2a

b3a

b27

b34

b3a

b22

b2a

b27

b2d

b35

b1c

};

//关键算法，通过内外层遍历求和

for(int i=0;i<29;i++)

{

ebp-ox30=i;

b[i]=0;

for(int j=0;j<29;j++)

{

eax=0x74\*(ebp-0x30);

ecx=ebp+eax-0xda8;//取出的是数组的首地址，第一个元素为零，后面全部为1

edx=ebp-0xe3c,为内层循环的值

eax=ebp-0xe3c,为内存循环的值

edx=ebp+edx\*4-0x7C;//取出数据，依次取出数据、

edx=[ecx+eax\*4]\*edx//乘以1不影响

eax=ebp-0xe30

edx=[ebp+eax\*4-0xe24]+edx//加上上一个数据

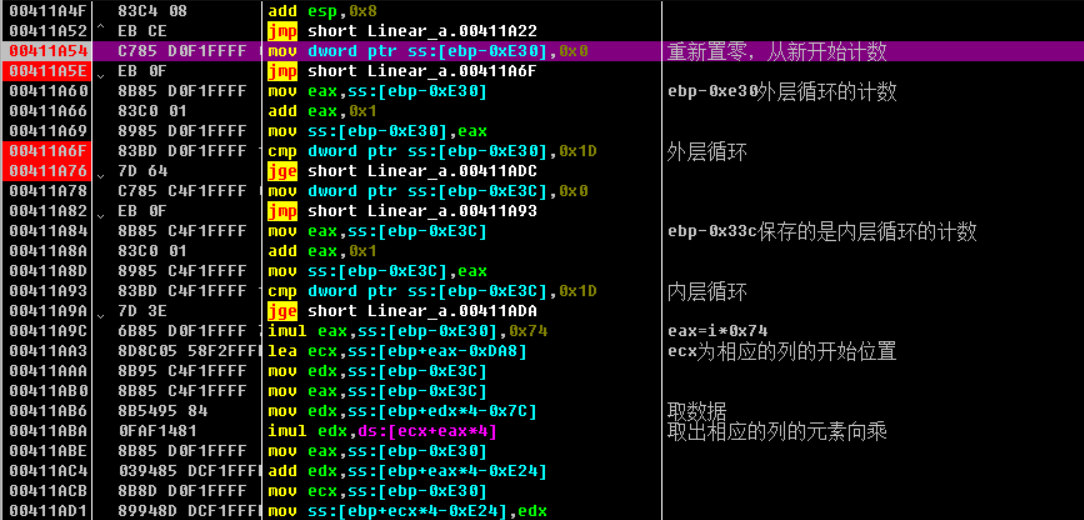
ecx=ebp-oxe30

ebp+ecx\*4-0xe24=edx

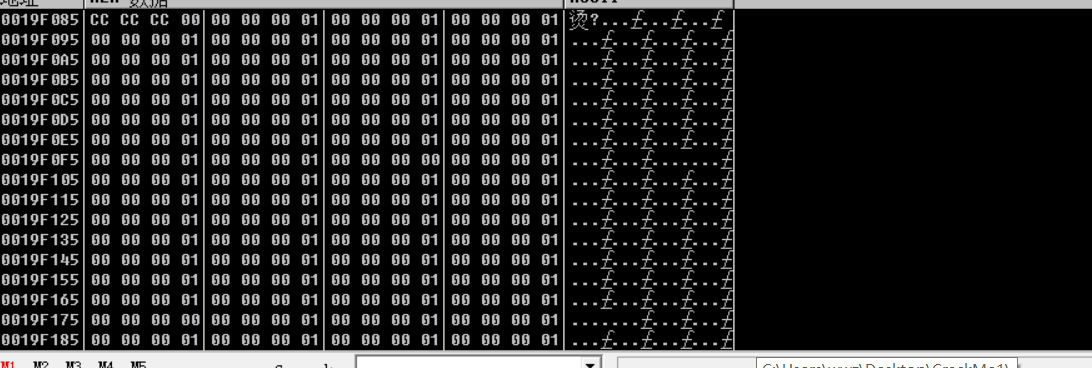
b[i]+=a[i]

}

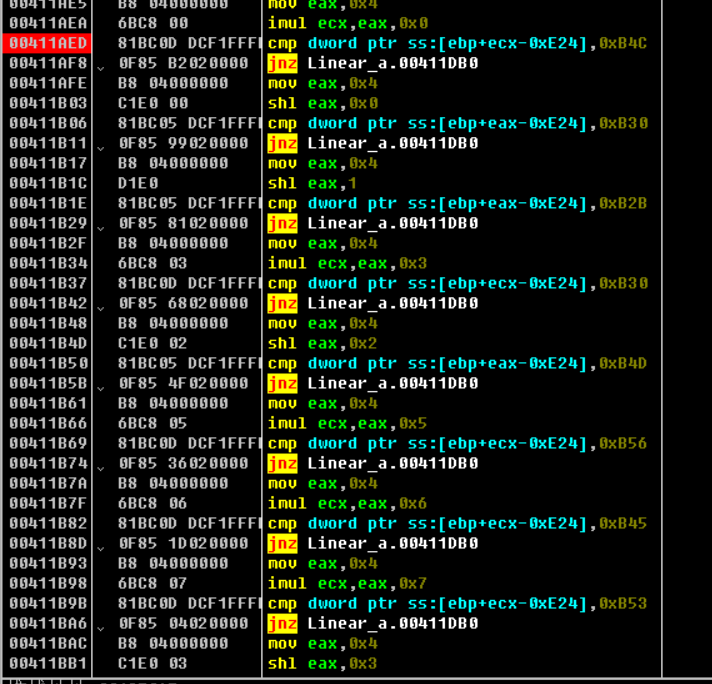
}



这里存放着矩阵A,通过跟踪可以发现矩阵的结构



这里为一系列关键的判断



主要的算法就是

A:为行列相等29的矩阵

A\*x=B

B:为29行一列的矩阵

求出x就可以了

解就是求29元一次多项式的解，网上有在线求矩阵的解的。将解密的数据安字符串输出就可以得到答案了。



简单算法

#include<iostream>

using namespace std;

int main(int argc,char \*argv[])

{

int b[29]=

{

0xb4c

,0xb30

,0xb2b

,0xb30

,0xb4d

,0xb56

,0xb45

,0xb53

,0xb1e

,0xb22

,0xb34

,0xb2d

,0xb36

,0xb2a

,0xb2c

,0xb34

,0xb3a

,0xb25

,0xb2a

,0xb3a

,0xb27

,0xb34

,0xb3a

,0xb22

,0xb2a

,0xb27

,0xb2d

,0xb35

,0xb1c

};

int c[29]={

77.0000

,105.0000

,110.0000

,105.0000

,76.0000

,67.0000

,84.0000

,70.0000

, 123.0000

, 119.0000

, 101.0000

, 108.0000

, 99.0000

, 111.0000

, 109.0000

, 101.0000

, 95.0000

, 116.0000

, 111.0000

, 95.0000

, 114.0000

, 101.0000

, 95.0000

, 119.0000

, 111.0000

, 114.0000

, 108.0000

, 100.0000

, 125.0000

};

// for(int i=0;i<29;i++)

// printf("%d ",b[i]);

for(int i=0;i<29;i++)

printf("%c",c[i]);

}

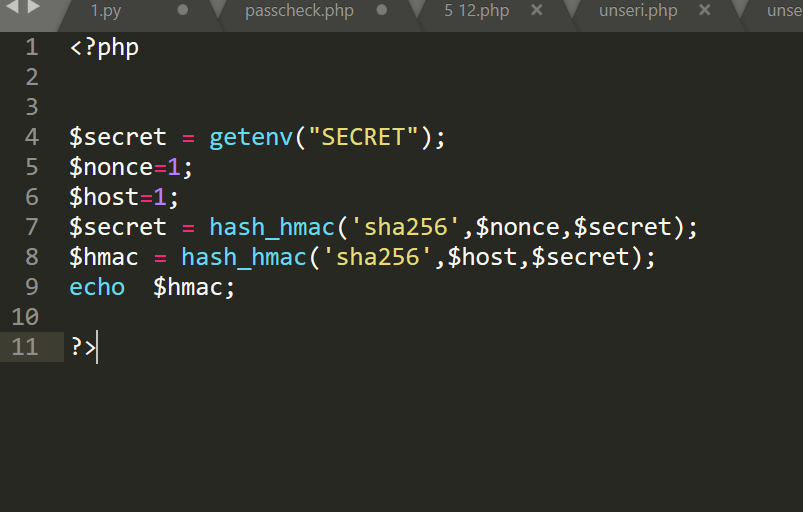
//2892 2864 2859 2864 2893 2902 2885 2899 2846 2850 2868 2861 2870 2858 2860 2868 2874 2853 2858 2874 2855 2868 2874 2850 2858 2855 2861 2869 2844

2. Web easybypass（大一）

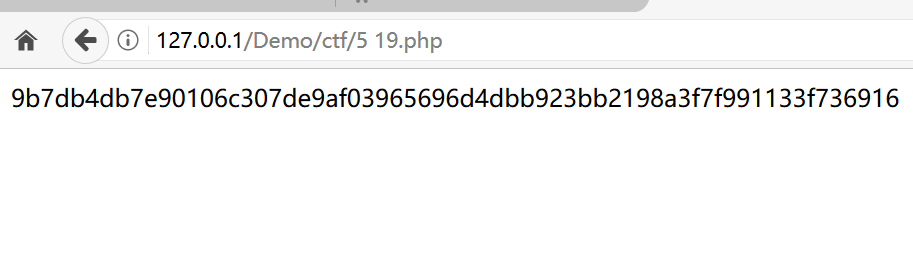
先分析代码,需要POST hmac、 host、 nonce 三个值，然后根据host 和nonce 加密出hmac,

然后判断 hmac与POST进去的hmac是否相等，相等则弹出flag;

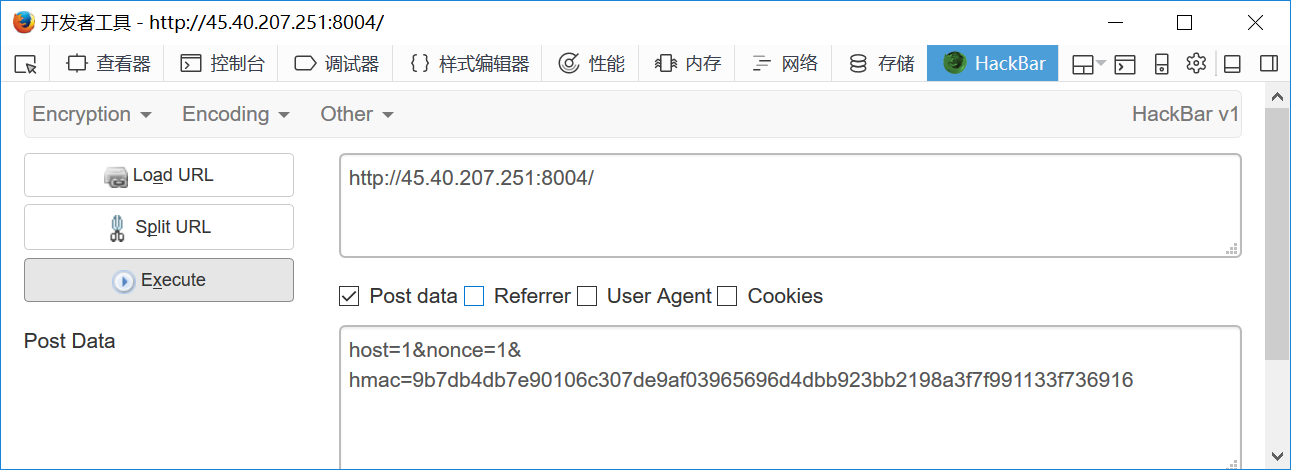
思路是，nonce host随便取了1，自己加密构造一个hmac。



输出hmac



用hackbar POST 进去,就的得到了flag





3. [see\_or\_do\_not\_see](https://makerctf.com/static/uploads/cde01c80ecda07f46ed0e14da8f974de/see_or_do_not_see.pdf)（大一）



答案在图片中间，选中以后点击右键，百度就可以了。