i春秋ctf训练营writeup-手贱的A君

原创

Gμn__ 于 2020-05-18 22:12:11 发布 1200 收藏 2

文章标签： md5 密码学

导语

i春秋也是个学东西的好地方呀。

手贱的A君

关键词：数据库，md5，拿着这一串莽头去md5在线解密

果然不会那么简单的。
定睛一看，这md5好像是33位啊¿
定睛两看，这怎么害有个l啊？众所周知md5的内容里只有0-9和abcdef呀？

删去l再解密，果然正确了。

md5

MD5算法的原理可简要的叙述为：MD5码以512位分组来处理输入的信息，且每一分组又被划分为16个32位子分组，经过了一系列的处理后，算法的输出由四个32位分组组成，将这四个32位分组级联后将生成一个128位散列值。
md5的算法可以分为五步，描述如下：
第一步，补位：
MD5算法先对输入的数据进行补位，使得数据的长度(以byte为单位)对64求余的结果是56。
即数据扩展至LEN=K*64+56个字节，K为整数。
补位方法：补一个1，然后补0至满足上述要求。相当于补一个0x80的字节，再补值
为0的字节。这一步里总共补充的字节数为0～63个。

第二步，附加数据长度：
用一个64位的整数表示数据的原始长度(以bit为单位)，将这个数字的8个字节按低位的在前，
高位在后的顺序附加在补位后的数据后面。这时，数据被填补后的总长度为：
LEN = K*64+56+8=(K+1)*64 Bytes。

※注意那个64位整数是输入数据的原始长度而不是填充字节后的长度,我就在这里栽了跟头.

第三步，初始化MD5参数：
有四个32位整数变量 (A,B,C,D) 用来计算信息摘要，每一个变量被初始化成以下
以十六进制数表示的数值，低位的字节在前面。
word A: 01 23 45 67
word B: 89 ab cd ef
word C: fe dc ba 98
word D: 76 54 32 10
※注意低位的字节在前面指的是Little Endian平台上内存中字节的排列方式，
而在程序中书写时，要写成：
A=0x67452301
B=0xefcdab89
C=0x98badcfe
D=0x10325476

第四步，定义四个MD5基本的按位操作函数：
X，Y，Z为32位整数。
F(X,Y,Z) = (X and Y) or (not(X) and Z)
G(X,Y,Z) = (X and Z) or (Y and not(Z))
H(X,Y,Z) = X xor Y xor Z
I(X,Y,Z) = Y xor (X or not(Z))

参考：
https://www.cnblogs.com/minady/articles/134379.html