

i春秋ctf训练营writeup-手贱的A君

原创

[Gyn_](#) 于 2020-05-18 22:12:11 发布 1200 收藏 2

文章标签: [md5 密码学](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/bbszhenshuai/article/details/106200702>

版权

导语

i春秋也是个学东西的好地方呀。

手贱的A君

分值: 50分 类型: Basic 题目名称: 手贱的A君

已解答

题目内容: 某天A君的网站被日, 管理员密码被改, 死活登不上, 去数据库一看, 啥, 这密码md5不是和原来一样吗? 为啥登不上咧?

d78b6f302l25cdc811adfe8d4e7c9fd34

请提交PCTF(原来的管理员密码)

Flag:

提交

解题排名: 1 L_CGL 2 迦深我混dj 3 c0deeast

提交Writeup获取泉币

<https://blog.csdn.net/bbszhenshuai>

关键词: 数

数据库, md5, 拿着这一串莽头去md5在线解密

密文: d78b6f302l25cdc811adfe8d4e7c9fd34

类型: 自动 [帮助]

查询 加密

查询结果:
密文无法识别或无法处理, 请确认密文类型是否选择正确。 [密文类型及格式帮助>>](#)

<https://blog.csdn.net/bbszhenshuai>

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, 这怎么害有个啊? 众所周知md5的内容里只有0-9和abcdef呀?

密文: d78b6f 02l25c c811adfe8d4e7c9fd34

类型: 自动 [帮助]

查询 加密

删去l再解密, 果然正确了。

密文: d78b6f30225cdc811adfe8d4e7c9fd34

类型: 自动 [帮助]

查询 加密

查询结果:
hack

<https://blog.csdn.net/bbszhenshuai>

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。

$F(X,Y,Z) = (X \text{ and } Y) \text{ or } (\text{not}(X) \text{ and } Z)$

$G(X,Y,Z) = (X \text{ and } Z) \text{ or } (Y \text{ and } \text{not}(Z))$

$H(X,Y,Z) = X \text{ xor } Y \text{ xor } Z$

$I(X,Y,Z) = Y \text{ xor } (X \text{ or } \text{not}(Z))$

参考：

<https://www.cnblogs.com/minady/articles/134379.html>