

bugku-writeup-Crypto-你以为是md5吗

原创

dark2019 于 2021-06-22 17:44:19 发布 58 收藏

分类专栏: [信息安全](#) 文章标签: [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/qq_22597955/article/details/118111901

版权



[信息安全](#) 专栏收录该内容

53 篇文章 1 订阅

订阅专栏

题目: 你以为是md5吗

你以为是md5吗

Crypto

已解决

分数: 15

金币: 2

题目作者: vFREE

一血: 犬来八荒

一血奖励: 2金币

解决: 776

提示: md5的构成

描述: flag{}

其他: [↓md5](#)

请输入flag

提交

https://blog.csdn.net/qq_22597955

01—MD5构造

MD5的全称是Message-Digest Algorithm, 是Hash算法中的一种重要算法, 具有单项加密、加密结果唯一、安全性能好等特点。MD5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位分组合级联后将生成一个128位散列值。

MD5只有0~9和a-f16个符号构成, 因此排除题目中给出的其他符号:

题目给出: bci177a7a9c7udf69c248647b4dfc6fd84o

MD5: bc177a7a9c7df69c248647b4dfc6fd84

02—解码

CMD5 本站针对md5、sha1等全球通用公开的加密算法进行反向查询, 通过穷举字符组合的方式, 创建了明文密文对应查询数据库, 创建过500TB, 查询成功率95%以上, 很多复杂密文只有本站才可查询。自2006年已稳定运行十余年, 国内外享有盛誉。

首页

请注册或登录或 qq一键登录

密文: bc177a7a9c7df69c248647b4dfc6fd84
类型: 自动 [帮助]

查询 加密

查询结果:
666666666666

https://blog.csdn.net/qq_22597955

使用MD5在线解码工具: <https://www.cmd5.com/>, 解码, 得到flag。