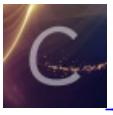
bugku-writeup-Crypto-你以为是md5吗

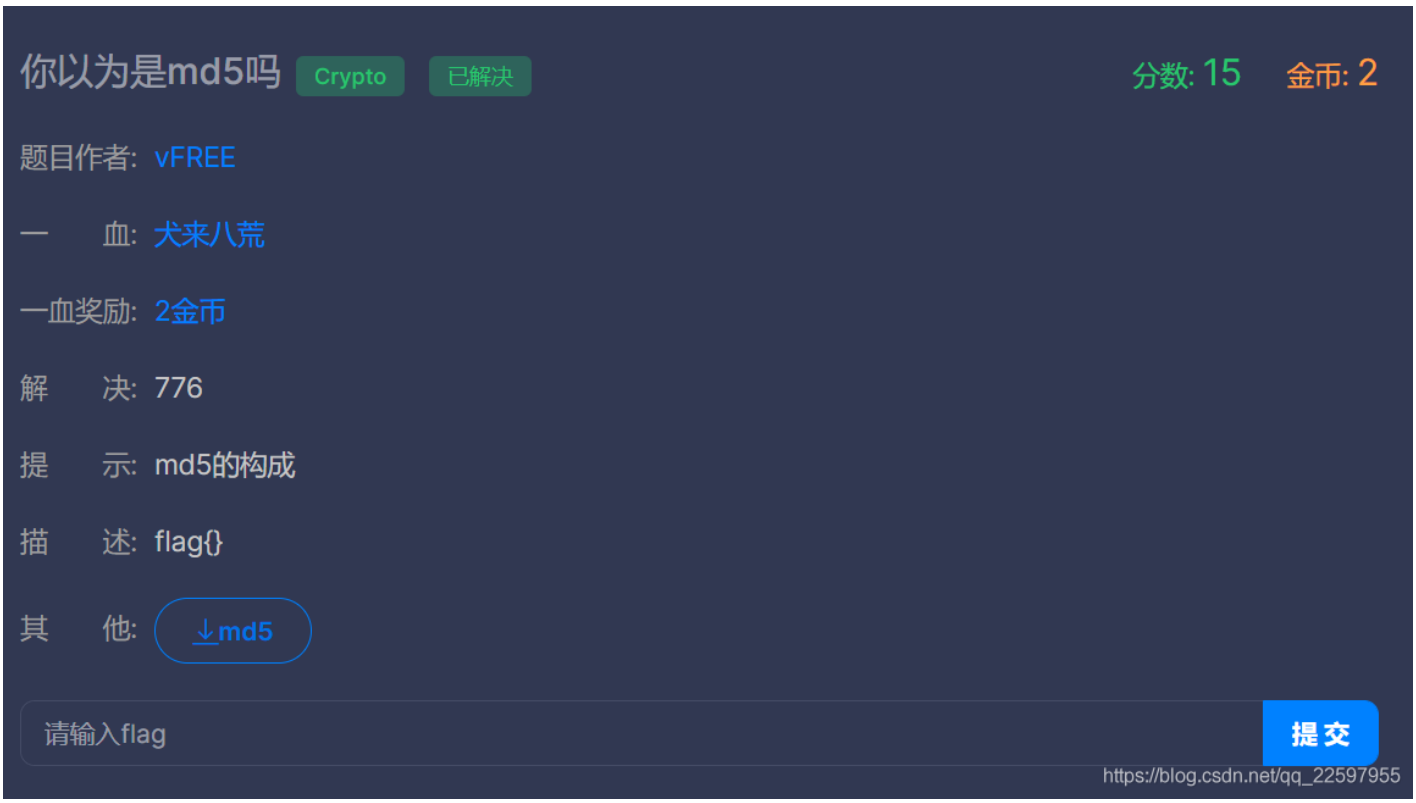
原创

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

本文链接：https://blog.csdn.net/qq_22597955/article/details/118111901



题目：你以为是md5吗



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

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