

buuctf · windows系统密码 · wp

原创

connamon 于 2022-04-01 20:46:06 发布 264 收藏

文章标签: [网络安全](#)

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/sml918451478/article/details/123907270>

版权

题目来源: buuctf·Windows系统密码 ([BUUCTF在线评测 \(buuoj.cn\)](#))

题目 解题快手榜

Windows系统密码

1

注意: 得到的 flag 请包上 flag{} 提交

272e88c8-8...

Flag

提交

CSDN @connamon

附件情况

272e88c8-8dca-4206-ba57-89882ccaba5e.zip (离购买还只剩 2 天了)

文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)

添加 解压到 测试 查看 删除 查找 向导 信息 扫描病毒 注释 自解压格

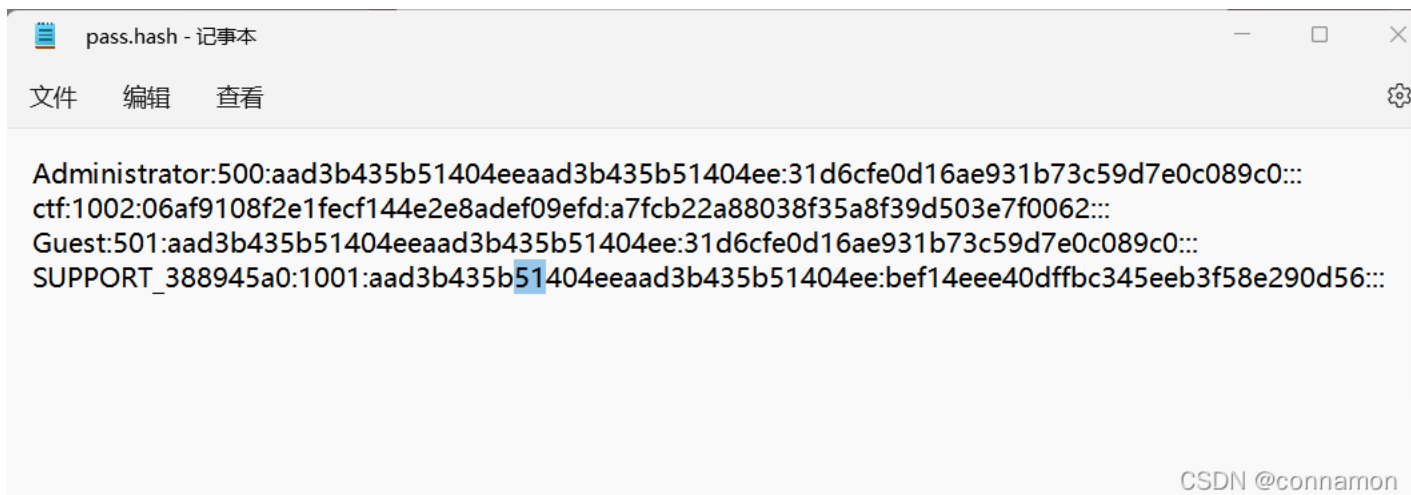
272e88c8-8dca-4206-ba57-89882ccaba5e.zip\Windows系统密码 - ZIP 压缩文件, 解包大小为 337

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
pass.hash	337	173	HASH 文件	2017/11/3 16:...	512851D9

CSDN @connamon

发现是hash拓展名的文件, 这不直接提示这要用哈希来解咯

那就先用md5看看，不行再试试sha1



```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
ctf:1002:06af9108f2e1fecf144e2e8adef09efd:a7fcb22a88038f35a8f39d503e7f0062::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::  
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:bef14eee40dffbc345eeb3f58e290d56:::
```

CSDN @connamon

正好每一段都是32位的很符合md5的加密，那就一段一段的试

前面两个是空密码，第三个解出来了要钱，再等等，第四段出现了解码，就是flag了



密文: a7fcb22a88038f35a8f39d503e7f0062
类型: NTLM [帮助]

查询 加密

查询结果:
good-luck

CSDN @connamon

哈希解密工具: [md5在线解密破解,md5解密加密 \(cmd5.com\)](http://cmd5.com)