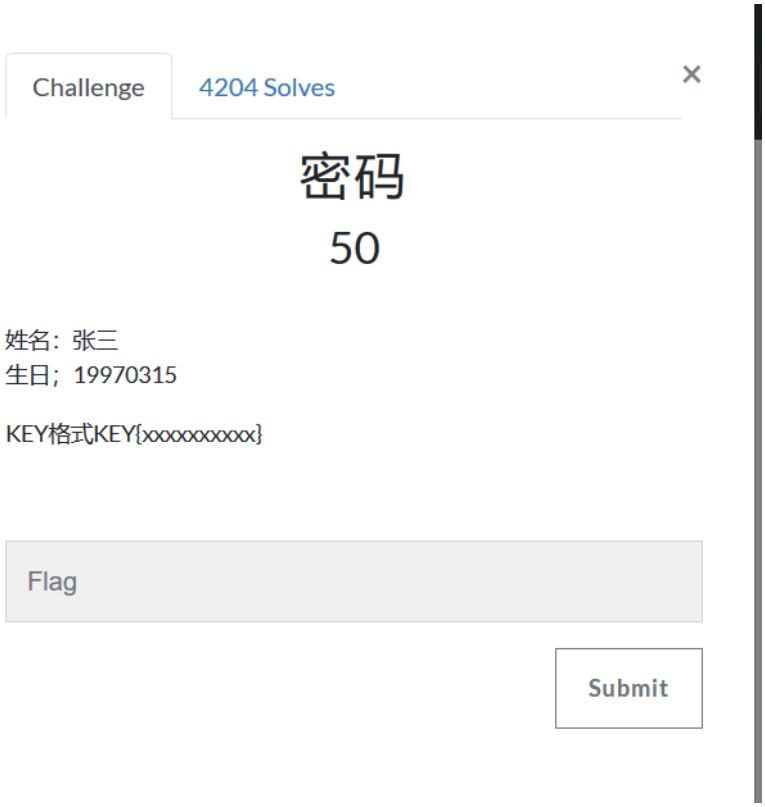
bugku社工writeup

转载

a111b11100 于 2019-08-21 18:13:00 发布 68 收藏
原文链接：http://www.cnblogs.com/lzlzzzzz/p/11390356.html

最近bugku的web和杂项刷了多半，突然心血来潮想试试社工题，bugku的社工题比较基础，而且题量不多，和大家分享一下writeup。

1.密码



根据提示，多猜几次密码就对了，然后得到flag。

2.信息查找

直接百度，发现了那个新闻，找到群号，提交flag

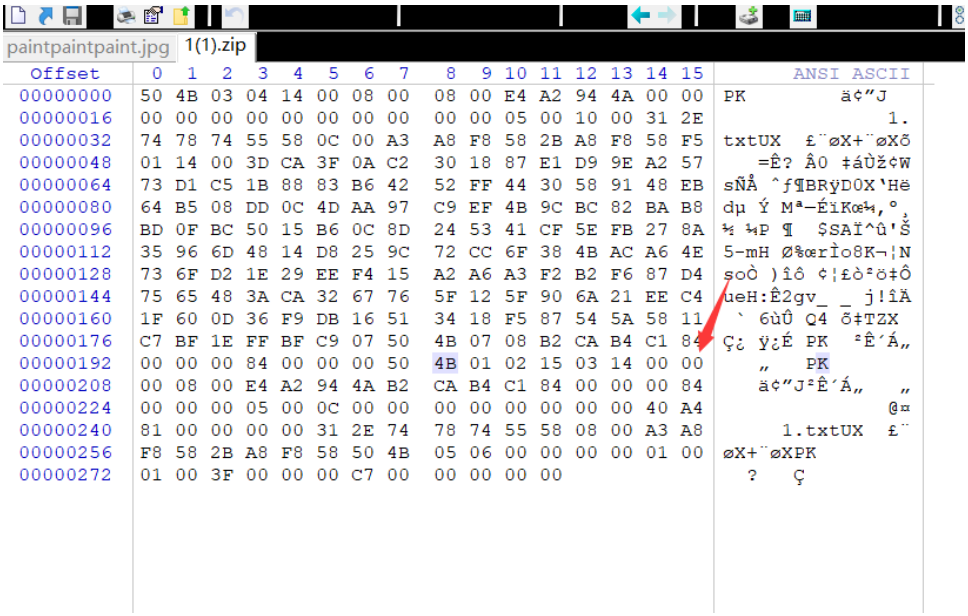
3.简单个人信息搜集

将压缩包下载下来，打开，发现有密码，而且也没有任何提示，凭空也猜不出来。

没办法，网上找了个writeup，发现居然是zip伪加密，没听说过~~

百度了一下伪加密，涨姿势了。

使用winhex打开压缩文件找到pk头，并将这一行最后一个数改为复数（最后一个数单数为加密状态，复数为未加密）



打开压缩文件，是一个TXT文本，打开一看是个地址和人名

需要使用社工库查询，但是国内的社工库基本都挂了（毕竟违法的东西）这个flag是我在网上抄的

4.社工进阶

Challenge 1127 Solves

社工进阶

100

name:孤长离

提示：弱口令

Flag

Submit

提示孤长离，直接百度这个名字，在bugku贴吧里发现了一个帖子

网易邮箱，提示弱口令，百度弱口令top100，163邮箱登陆有图片验证码，burp爆破就不可了。只能一个一个试，试了十几个，都不对，找到writeup，发现密码a123456，试一下，发现还是错的，不试了，直接抄了flag（手动滑稽）

5.王晓明的日记

提示使用bugku在线工具生成弱口令 https://tool.bugku.com/?wafcloud=2然后使用burp爆破，得到flag。

6.简单社工收集

Challenge 813 Solves

简单的社工尝试

150

这个狗就是我画的，而且当了头像
这题提示的其实很明显了
想想吧

1.png

Flag

Submit

使用百度搜图搜索这只狗，在孤长离微博中发现一个链接 http://c.bugku.com/13211.txt直接打开发现flag

学习信息安全，多多少少要用到社工，所以学好社工对于我们工作学习帮助会很大。
初学社工可以去看《社会工程》系列，可以帮助你快速入门。

转载于:https://www.cnblogs.com/lzlzzzzzz/p/11390356.html