

BJDCTF 2nd writeup

原创

abtgu 于 2020-03-23 20:21:39 发布 1139 收藏 1

分类专栏: [CTF](#)

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/weixin_43790779/article/details/105056480

版权



[CTF 专栏收录该内容](#)

22 篇文章 1 订阅

订阅专栏

文章目录

[\[BJDCTF 2nd\]签到-y1ng](#)

[\[BJDCTF 2nd\]灵能精通-y1ng](#)

[\[BJDCTF 2nd\]Real_EasyBaBa](#)

[\[BJDCTF 2nd\]圣火昭昭-y1ng](#)

[\[BJDCTF 2nd\]最简单的misc-y1ng](#)

[\[BJDCTF 2nd\]EasyBaBa](#)

[\[BJDCTF 2nd\]老文盲了](#)

[BJDCTF 2nd]签到-y1ng

题目: QkpEe1czbGMwbWVfVDBfQkpEQ1RGfQ==

解题思路: 直接base64解码即可。BJD{W3lc0me_T0_BJDCTF}

[BJDCTF 2nd]灵能精通-y1ng

题目: 身经百战的Y1ng已经达到崇高的武术境界, 以自律克己来取代狂热者的战斗狂怒与传统的战斗形式。Y1ng所受的训练也进一步将他们的灵能强化到足以瓦解周遭的物质世界。借由集中这股力量, Y1ng能释放灵能能量风暴来摧毁敌人的心智、肉体与器械。

解题思路: 为下载得到的jpg添加后缀.jpg,得到图片



观察图片, 可以知道是猪圈密码, 解密即可。

flag{IMKNIGHTSTEMPLAR}。

[BJDCTF 2nd]Real_EasyBaBa

题目：得到的 flag 建议用 flag{} 包上提交。

解题思路：



用winhex查看图片发现

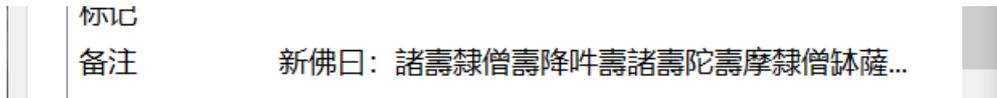


BJD{572154976}。

[BJDCTF 2nd]圣火昭昭-y1ng

题目：开局一张图，flag全靠猜，因为出题人失误搞错了，解出来的key去掉后3位的com。

解题思路：查看图片属性，发现新佛曰



解密地址：<http://hi.pcmoe.net/buddha.html>



得到gemlovecom，去掉“com”提交，发现incorrect，想到题目中的“猜”，联想到Outguess隐写，在Kali下运行

```
outguess -k 'gemlove' -r '/root/桌面/1.jpg' -t 11.txt
```

得到flag，BJD{wdnmd_misc_1s_so_Fuck1ng_e@sy}。

[BJDCTF 2nd]最简单的misc-y1ng

题目：得到的 flag 建议用 flag{} 包上提交。

解题思路：查看secret的十六进制表示，发现是缺少文件头的png，插入png文件头89 50 4e 47，添加后缀名.png,得到图片



观察图中是十六进制数据，转换成字符即可。

```
BJD{y1ngzuishuai}
```

[BJDCTF 2nd]EasyBaBa

题目：得到的 flag 建议用 flag{} 包上提交。

解题思路：用binwalk查看图片

```
binwalk ezbb.jpg
```

发现压缩文件，foremost分离文件，打开zip，里面有一张图片，查看其十六进制形式，发现是avi格式，更改后缀名，打开发现该视频中有4个二维码，扫描得到一串十六进制数字424a447b696d6167696e5f6c6f76655f59316e677d
转换成字符即得flag，BJD{imagin_love_Y1ng}。

[BJDCTF 2nd]老文盲了

题目：BJD{这里是中文}。

解题思路：

打开文本发现“畢彙締眾擴灑涸匱襖黼灑錫鵠驕黼咧眾鞞鯨”，百度一下每个字的读音，发现他们的谐音是：bjd{这就是flag直接交了吧}，故直接将“涸匱襖黼灑錫鵠驕黼咧”提交即可。BJD{涸匱襖黼灑錫鵠驕黼咧}。

更多请看：https://blog.csdn.net/weixin_43790779/article/details/105173161