BJDCTF2nd

原创

Amherstieae 于 2020-05-25 16:52:08 发布 597 收藏

分类专栏： wp 文章标签： wp

本文写于3.24，只是那个时候还莫得博客，遂现在才发出。

写在前面

大家好呀，这里是β-AS，是一枚真的小菜鸡，希望路过的师傅带带我鸭

这是第二届BJDCTF，作为真弟弟只对crypto和misc感兴趣呀，然后接着是关于这两方面这次比赛我们做出来的题的writeup,希望能对大家有所帮助，也希望路过的大佬带带我（这是关键）

哦对了，七校联盟萌新赛？？？？嗯？？？？？？

出题人出来！线下1V1来不来！！

（假的，我打不过你）

CRYPTO

。1签到-y1ng

QkpEe1czbGMwbWVfVDBfQkpEQ1RGfQ==

base64嘛BJD{W3lc0me_T0_BJDCTF}okk解决啦

也许这道题是我能做出来了最快的[沧桑]

（自信点，把也许去掉）

。2老文盲了

emmmm这道题，你们感受一下

罼蠯締眾擴灞澍匷襫黼瀨鎷豅鵲驕鰳唰眾鞹鰝？？？？？这是啥？我要重新去学语文了

看到拼音的我人给秀傻了，这就是大佬的力量吗

所以最后flag是BJD{涮匿裢黼濑鎷豅鹊驕鰳唰}

（萌新瑟瑟发抖ing）大佬能不能手下留情，说好了是基础呢！！！！

。3cat_flag

可爱不猫猫！

人家超可爱的吼

拿到这个题，哟，gif，咖啡一顿猛操作发现。。。。嗯？？？？？这是个啥？？？怎么几帧都一样？？？

仔细看看

哇，这个猫猫怎么只有两种，一只恰饭团，一只啃鸡腿，再仔细看看，哇它怎么还是八个一排，嗯。。。大胆假设，小心求证，我们先当他是个二进制吧，恰饭团的是0，啃鸡腿的是1

所以手打吧！！！（颤抖吧，不会写代码的弟弟

01000010010010100100010001111011010011010010000101100001001100000111111001111101

在线解码一看！没错，就是他

BJD{M!a0~}

。4灵能精通

下载下发现是如下图所示

emmmm再仔细一看题目描述，百度后发现是星际争霸2的一段词，题目灵能也是星际争霸2的一种能量，围绕这俩展开后。。。发现没有什么有用的。。。

后来就想啊，图形密码，不就猪圈密码最常见吗，然后就。。。。发现了这个

圣武士密码牛逼！！

（猪圈密码还有很多变种，下一次可能就不是这种了，所以——论信息收集的重要性

。5燕言燕语

小燕子，穿花衣，年年春天来这里，我问燕子你为啥来，燕子说:

这里的春天最美丽！

wai方向重点偏了啊！错了错了，重点在下面↓↓

79616E7A69205A4A517B78696C7A765F6971737375686F635F73757A6A677D20

唔。。。0-9、A-F，极大可能的十六进制，解码一看

yanzi ZJQ{xilzv_iqssuhoc_suzjg}

感觉不太对啊，提交试试，淦 果然不对

接着就虎（man）虎（wu)生(mu)风(di)的一顿操作，在尝试了栅栏，凯撒都无果后，就在想“yanzi”有没有可能是个密钥，就试试吧，维吉尼亚密码（不过我老是把他记成维尼吉亚（吐血））

so，结果。。。当然是flag啦

BJD{yanzi_jiushige_shabi}

(tajiushigeshabi)

。6Y1nglish

Y1ng根据English居然独自发明了一门语言，就叫Y1nglish

明文都是可读的英文单词，flag如果提交失败，自己读一下，把错误的单词修正，再提交(某个地方的u和i不需要调换顺序，错误点不在那里)

Nkbaslk ds sef aslckdqdqst. Sef aslckdqdqst qo lzqtbw usf ufkoplkt zth oscpslsfko. Dpkfk zfk uqjk dwcko su dscqao qt dpqo aslckdqdqst, kzap su npqap qo jkfw mzoqa. Qu wse zfk qtdkfkodkh qt tkdnsfw okaefqdw, nkbaslk ds czfdqaqczdk. Bkd lk dkbb wse z odsfw.

Q nzo pzjqtv hqttkf zd z fkodzefztd npkt Pzffw Odkkbk azlk qt, pk qo z lzcztkok ufsl lzczt med tsn pk qo tsd bqjqtv qt lzczt, lzwmk Pzffw qot’d z lzcztkok tzlk med pk qo fkzbbw z lzcztkok. Pzffw nsfwkh qt z bznwkf’o suuqak wkzfo zvs, med pk qo tsn nsfwqtv zd z mztw. Pk vkdo z vssh ozbzfw, med pk zbnzwo msffsno lstkw ufsl pqo ufqktho zth tkjkf czwo qd mzaw. Pzffw ozn lk zth azlk zthozdzd dpk ozlk dzmbk. Pk pzo tkjkf msffsnkh lstkw ufsl lk. Npqbk pk nzo kzdqtv, Q zowkh pql ds bkth lk &2. Ds lw oefcfqok, pk vzjk lk dpk lstkw qllkhqzdkbw. ‘Q pzjk tkjkf msfffsnkh ztw lstkw ufsl wse,’ Pzffw ozqh,‘os tsn wse azt czw usf lw hqttkf!’ Tsn q nqbb vqjk wse npzd wse nztd.

MlH{cwdp0t_Mfed3_u0fa3_sF_geqcgeqc_ZQ_Af4aw}

看到这题我在想。。。。他在为难我英语不好

还有就是emmmm简单的替换加密，附上网址https://quipqiup.com/

解密观察发现只有下面一段是可以的，其他都不有不显示的字符

（话说我这篇wp真的好业余啊）

Welcome to our competition. Our competition is mainly for freshmen and sophomores. There are five types of topics in this competition, each of which is very basic. If you are interested in networy security, welcome to participate. Let me tell you a story. I was having dinner at a restaurant when Harry Steele came in, he is a Japanese from Japan but now he is not living in Japan, maybe Harry isn't a Japanese name but he is really a Japanese. Harry woryed in a lawyer's office years ago, but he is now worying at a bany. He gets a good salary, but he always borrows money from his friends and never pays it bacy. Harry saw me and came andsatat the same table. He has never borrowed money from me. While he was eating, I asyed him to lend me &2. To my surprise, he gave me the money immediately. 'I have never borrrowed any money from you,' Harry said,'so now you can pay for my dinner!' Now i will give you what you want.

BJD{pyth0n_Brut3_f0rc3_oR_quipquip_AI_Cr4cy}

然后根据题目明文是可读的英语单词，单看最后的flag也没有什么，于是必不可免的通读了全文，发现上文两个标黄的地方都是单词里的k变成了y,所以第一个Python可读，只改最后一个y为k就可以啦

BJD{pyth0n_Brut3_f0rc3_oR_quipquip_AI_Cr4ck}

MISC

。1A_Beautiful_Picture

拿到这个题，emmmm画风好可爱呀哈哈哈哈哈哈，属性里没啥特别的，把它放到010里看一看，他的长x宽x3明显是小于存储大小的，所以怀疑是改了高度，于是修改高度就出来啦~

不得不说，画风是超可爱的吼

。2EasyBaBa

拿到题目，师傅是缺女朋友吗？（星星眼）不如。。。。嘿嘿嘿

回来回来，扯到正题上去

一看属性文件这么大，直觉告诉我他不是简单的图片，在010里发现jpg文件尾的后面还有很多东西，所以将他放到Kali里分离提取

出来了一个原本的图片，还有一个压缩包，压缩包包含了一个名为“里面都是出题人”的图片（为什么是这个名字？是想让我们特殊照顾嘛），此时发现该文件还是很大，放到010里看看

图中发现他并不是一个单纯的图片，是一个AVI文件，于是修改后缀名，打开看看的时候发现有什么东西一闪而过，于是怎么把他放慢呢？我们可以倍速播放视频，也可以用pr一帧帧看图，果不其然，在里面出现了四个二维码

图片已做防盗链处理
请在原文件中访问该图片

图片已做防盗链处理
请在原文件中访问该图片

但是（捂脸）这个二维码颜色如此之淡。。。。

没关系，我一开始就是用微信扫的，调一调角度就可以啦（我爱微信扫码）

二维码解码器也是可以的哟，不过区域解码时截图要截得正好扫出来的成功率大一点

扫码结果是这个↓

424A447B696D6167696E5F6C6F 76655F 59316E677D

看这样子应该是十六进制，所以转ASCII就可以啦

BJD{imagin_ *love* _Y1ng}

。3小姐姐

看到这个一个压缩包，解压后发现一个图片，属性没有什么特殊的，咱打开图片看看，哇！！！！！是小姐姐哎

仔细一看这个图片，哎？这怎么上下有点没对齐哈哈哈

抱着这个疑问用010打开瞅一瞅，开头结尾都挺正常，想到图片错位，我们在010搜一下BJD(别问，问就是直觉）

成功出现，(^ ー ^)V耶

BJD{haokanma_xjj}

。4圣火昭昭

压缩包解压没东西，打开图片，哇咔咔咔可爱耶

不，别被他蒙蔽了双眼，他藏着东西

照例看一眼属性，发现有东西，新佛曰！！

百度新佛曰，复制粘贴解码一气呵成

嗯gemlovecom，根据提示去掉com

用到了outguess
想到这个工具是因为题目描述在猜加粗了嘎
（./configure && make && make install 这个是安装命令）这不是重点

把这张图片拖进Kali里，执行这条命令

```
outguess -k "key" -r 文件名 -t 保存的文件名
```

（此时注意key是gemlove,保存的文件记得是txt的）

BJD{wdnmd_ misc_ 1s_ so_ Fuck1ng_ e@sy}

bingo

。5Real_EasyBaBa

题目如上，打开是个png文件，然后嗯？imagine师傅还没征到婚吗？不如嘿嘿嘿

咳咳咳，偏了偏了

属性一看没啥特别，咖啡也没有啥特别的，010里看一看，发现是一个jpg文件（十六进制开头FFD8,结尾FFD9）随即将后缀名改为jpg，发现jpg后面还有一个压缩包，那我还不是喜出望外，扔到Kali分离提取啊，但是。。。。竟然提取不出来。

再仔细看了一遍010,发现了不对劲的地方

这个jpg文件尾怎么还有这么一长串的FF FF？？？？？这个压缩包文件头怎么还不对？？？？

你个（）欺骗我的感情

不该有的都删掉，FFFF？删掉删掉

50 4B FF FF DE AD 不对？？？改掉改掉 50 4B 03 04 DE AD

接着继续Kali里（Kali：用我了就想起我，哼 ╭(╯^╰)╮ ）分离提取！！

可以啦，是一个hint和一个压缩包，压缩包里也有一个hint，

怎么办呢接下来

遇事不决，010搞。发现两个hint内容都是一样的

有没有很眼熟！！！他就是 二维码！！！

（不过有的可能会乱版）

激动地掏出手机，打开微信扫一扫

成功，

```
od -vtx1 ./draw.png | head -56 | tail -28
```

但是但是，扫码时靠运气的（就hin难，你晓得吧[/沧桑.jpg][/摊手.jpg]）

如果，不幸你没扫出来，那么写代码吧！

#为黑色，空格为白色，写个Python脚本就可以了

（此处空白留给脚本代码，它应该有一席之地！！！但是为什么空白呢，因为我目前还没学会如何写脚本（小声），就先空着吧）[难办.jpg]

接着把扫码得到的结果扔到Kali里跑一下

（具体就是把题目一开始的图片放进去，在图片所属文件夹下打开终端，文件名和命令里的改成一致，粘贴回车）

结果就出来啦

有没有觉得很眼熟？如果没有也不要紧，你离屏幕远一点，眯起眼睛就能看见了（斜眼笑哈哈哈哈哈哈）

其实就是ff（又是ff，怎么老是ff）连在一起就可以啦~

BJD{527154976}

完结，撒花✿✿ヽ(°▽°)ノ✿