WP 4 i春秋_细说春秋

原创

segOt 于 2017-04-16 17:28:21 发布 859 收藏

分类专栏： CTF 文章标签： writeup

---

i春秋中一些非常简单的题目——传送门。题目的引子都是春秋战国时期的典故，也算应了网站名称的景，故事还是颇为有趣的，题目比较简单。

图穷匕见

题目给出了一个图片，如下：

从题目名称就可以看出，这幅图的末尾应该附加了一些信息。打开发现果然如此

Dump of additional bytes:
Hex:
2565362562322561 3125653925393425
3939256534256264 2561302565372539
6125383425653625 3839253933256535
2562632538302565 3625393625623925
6535256263253866 2565372539612538
3425653625616425 6133256537256131
2561652565372539 6125383425656625
6263253863256539 2538302539612565
3525626525383025 6534256238253862
2565342562382538 3025653525383525
6233256537253961 2538346b65792565
3625393825616625 6566256263253961
2565382538612539 6425653925626125
6262256535256263 2538302565392539
37256138
Ascii:
%e6%b2%a 1%e9%94%
99%e4%bd %a0%e7%9
a%84%e6% 89%93%e5
%bc%80%e 6%96%b9%
e5%bc%8f %e7%9a%8
4%e6%ad% a3%e7%a1
%ae%e7%9 a%84%ef%
bc%8c%e9 %80%9a%e
5%be%80% e4%b8%8b
%e4%b8%8 0%e5%85%
b3%e7%9a %84key%e
6%98%af% ef%bc%9a
%e8%8a%9 d%e9%ba%
bb%e5%bc %80%e9%9
7%a8

附加了一系列二进制串，ascii解码之后得到明显是url编码的东西，直接解码得到结果。（其中比较坑的是BurpSuite解码得不到中文，而是乱码，纠结了一阵子。

```
没错你的打开方式的正确的，通往下一关的key是：芝麻开门
```

纸上谈兵

这道题目没有给出任何信息，自然想到查看网页源代码，发现如下端倪：

```
<div style="display:none;">通关秘钥是一个贝丝第64代的人设计的，你能解开它吗？5be05ouJ5be05ouJ5bCP6a2U5LuZ</di
```

显然是BASE64编码咯。解码如下

```
巴拉巴拉小魔仙
```

窃符救赵

这道题目比较坑，隐藏的第二张图片并没有给出任何信息，最后需要图片搜索出那个东东的名字。。。
如下，给出了一个图片

很容易就分离出第二张图片

然后谷歌图片搜索得到这个东西的名字，就是flag。涨姿势了~

杜虎符

老马识途

这道题目给出了一张图片，如下

起初摸不到头脑，看到有杠和点，以为是摩斯密码，结果不是。搜索一番，才知道是猪圈密码。
出来的结果是`horse`，不过这还不是最终密码，考虑到之前的FLAG均是中文，所以换成`马`就对啦~ (ノ ▽ ヽ)

东施效颦

上一道题目刚刚想到**莫斯密码**，结果这一题就是莫斯密码。西施的情歌如下：

```
啊哈啊啊，哈哈哈哈哈，啊啊啊哈，啊
```

啊代表·，**哈**代表-，结果就很清晰了，**l0ve**，不过要把**0**替换成o。

```
love
```

大义灭亲

这道题，很是有些奇葩。姑且可以把它算作一道社工题目。搜索一下石碏的相关信息，然后猜测密码

```
shique719
```

这可能也是很多人设置密码的方式吧，名字加数字，弱密码！

三令五申

这道题目就比较有意思了，很难想到从哪里入手，于是推测可能题目中又会泄露关键信息。题目中与史实相比多出来的那一部分是副将的哪一段，而这一段反复在讲关于盒子的权限问题。
于是联想到了LINUX系统的文件权限问题。依据文中描述，显然权限为750。尝试一下，果然正确。

最后答案

```
750
```