戏说春秋_i春秋 writeup

转载

weixin_30901729 于 2018-12-13 14:46:00 发布 112 收藏 1
文章标签： 操作系统
原文链接：http://www.cnblogs.com/xiaomulei/p/10113978.html

《戏说春秋》第一关 图穷匕见

题目：

解：用winhex打开，拉到最后可发现一段编码

放到解密网站上解码。

《戏说春秋》第二关 纸上谈兵

解：文中没有明确指出问题，也没有给出线索，所以右键查看源代码

发现有一个被隐藏的div。
“通关秘钥是一个贝丝第64代的人设计的，你能解开它吗？5be05ouJ5be05ouJ5bCP6a2U5LuZ”
贝丝第64代，即指base64加密方法。
放到解密网站中解码，可得flag

《戏说春秋》第三关 窃符救赵

题目：

解：
(1)放到kali linux上binwalk一下，发现有一个zip压缩包

(2)用dd命令拆分出来

(3)打开压缩包发现另一张图片

此图即是兵符，但是并没有flag，各种方法尝试后发现此图和图片隐写没有关系。
由前两题不正经的flag猜测，此题答案可能是还是中文，进一步猜测答案是否为图中兵符的名字。
将图片拉至百度，进行智能识别。

得知该兵符名为“杜虎符”，输入“杜虎符”，题目通过。

《戏说春秋》 第四关 老马识途

题目：

解：自然而然联想起，猪圈密码。

一一对应可知，题目所给密码为：HORSE
提交发现答案错误，译为中文：马
提交，题目通过。

《戏说春秋》第五关 东施效颦

题目：“啊哈啊啊，哈哈哈哈哈，啊啊啊哈，啊”
解：翻译成莫斯密码，可得题目所给密码为：L0VE（注意第二个字母是数字0而不是字母）

根据莫斯密码表，可得题目所给密码为：L0VE（注意第二个字母是数字0而不是字母）

然而，题目的正确答案是LOVE（必须都是大写字母）

《戏说春秋》第六关 大义灭亲

此题脑洞颇大，“以他对父亲的了解，已经大致能确定密码是多少了”，百度石碏，猜想密码为shique719

答案正确，题目通过。

《戏说春秋》第七关 三令五申

此题writeup参照高其大佬，没想到关键key在“这个盒子里面的是盛放军令状，平时将军写好军令就直接放在里面，**我和其他副将都能打开这个盒子查看，然后执行里面的命令，而其他人无法解开这个盒子查看里面的军令**”中

- 结合《信息安全系统设计》中刚接触到权限，权限分为读取、写入、执行三类，而这三类又可以分别为所有者、用户组和公共（访客）进行设置
- 对应文中内容，可理解为孙武是所有者，可以写入命令、读取命令、执行命令；副将是用户组，可以读取命令、执行命令；吴王和其他人则是公共（访客），三种权限皆不可得。而我们在Linux下使用chmod命令时，可以通过数字来代替相应的权值，所以对应的权限值为：

答案即为750，题目通过。

总结：

1. 第一题需要url编码的识别解码，url编码一般为utf-8或者gb2312，url加密一般为md5和base64。
2. 第二题谐音提示了base64编码，解码即可。
3. 第三题图片隐写需要掌握文件内容分析和分离的方法(binwalk和dd)，并且灵活使用百度图片的智能识别功能。
4. 第四题为猪圈密码。
5. 第五题为莫斯密码。

6. 第六题纯属社会工程脑洞题。
7. 第七题学习了权限的chmod权值计算。

转载于:https://www.cnblogs.com/xiaomulei/p/10113978.html