爱春秋之戏说春秋 Writeup

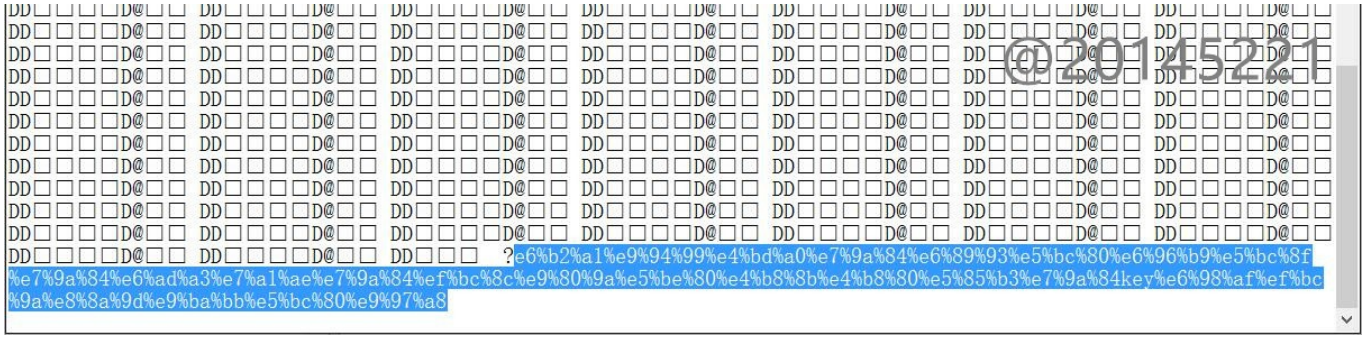
转载

weixin_30687587 于 2016-10-07 19:05:00 发布 57 收藏 1
文章标签： 操作系统
原文链接：http://www.cnblogs.com/20145221GQ/p/5936482.html

爱春秋之戏说春秋 Writeup

第一关 图穷匕见

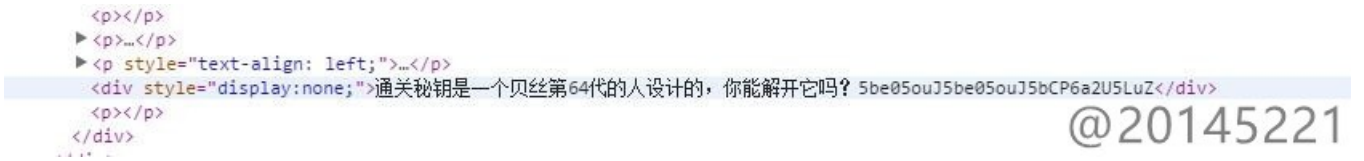
- 这一关关键是给了一个图片，将图片下载到本地后，打开以及查看属性均无任何发现，尝试把图片转换为.txt格式。在文本的最后发现这样一串有规律的代码：



- 形如这样的代码一看便想起来了URL加密方式，在搜索引擎里找到URL在线解码的工具即可（**注意：**原文最开始缺失一个%，需补齐后即可解密）

第二关 纸上谈兵

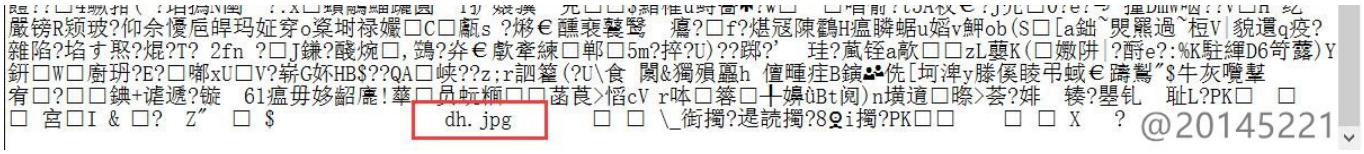
- 沿着第一关的解题思路并没有发现什么有价值的东西，接下来试试查看网页源代码，看看有什么收获（一般浏览器按F12即可查看源代码）
- 根据常识，秘密肯定是藏在正文当中，所以网页旁的一些小插件的代码可以不用看。这里有一个小技巧，当你将光标移到某行代码上，在网页的对应处会选中加深，这样可以便于我们快速过滤掉没有用的源代码。所以很快能找到下面的一行代码，如图：



- 这个已经提示的很明显了，“贝丝第64代的人”很显然说的就是base64加密方式，将后面的密文复制到网站的在线解密处解密即可。

第三关 窃符救赵

- 既然给了图片就把图片下载下来好了，老方法改为.txt格式看看有啥发现没（不过乍一看箱子应该可以想到压缩包），打开文本文件后发现文本最后有字符dh.jpg：



- 所以可以想到肯定是有一个dh.jpg文件隐藏在该文件之后，一般的隐藏方法就是压缩，所以把下载后的文件格式后缀改为.zip，打开后得到一个图片，乍一看是虎符，或许key就是虎符吧，试了试行不通，所以只有借助百度强大的识图功能，识别出来的结果即是key

第四关 老马识途

- 看到这个题其实不用多想了，这种特殊的文字表示的是猪圈密码
-
- 所以对应上原图中的符号，应该就是HORSE，可是提示错误，最后转念一想，这种中华历史题应该不会用英文作为key吧，所以输入对应的中文，顺利通过

第五关 东施效颦

- 根据这个题的文字提示，此题肯定与歌词有关：“啊哈啊啊，哈哈哈哈哈，啊啊啊哈，啊”
- 对加解密方式敏感的人应该可以立马猜到这种节奏感强的编码最可能的就是摩斯码，根据汉语发音习惯，“啊”短促，“哈”则发音较长，所以可能“啊”对应“.”，“哈”对应“-”（不行的话反过来试试，无伤大雅）
- 运气很好，一试成功

PS：这题就让我很尴尬了，简直打脸，我刚刚才说key不会是英文的

第六关 大义灭亲

- 这一题倒是要看文字靠脑洞了，所幸的是这题的提示较少，不会走什么弯路，大致的重要线索有2条：
  - 1.石厚是根据对他父亲石碏的了解猜出了密码
  - 2.石碏是个敢于面谏国君忠臣
- 百度石碏没有他的信息，所以百度卫恒公，只有他被杀的年份，所以最后试了许多遍，猜想key是`shique719`
- 这一题脑洞颇大，不是很好做

第七关 三令五申

- 这题想的时间有点久，不知从何下手作为切入点，最后在这一段中找到了一点端倪：
  - 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。**
  - 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：

写在最后

- 爱春秋之《戏说春秋》确实比较有意思，将我国历史与现代前沿的信息安全巧妙结合，古今贯通，给人以不同的感受，既能回到过去了解那段历史，也能激发自己对这类题的兴趣。
- 其实完成这些关的过程远远没有我这篇博客写的这么简单，看似很简单就破解了其中的秘密，实则是建立在反复尝试以及之前的经验这些基础上的，没有以前的练习，也不会较快的找到突破口。
- 所以完成这类题，一是要多具备一些技术一些网络攻防的工具，二是要有丰富做题的经验在实战中训练，三是需要强大的脑洞，敢于想不怕错的精神。而这三点我还做得不是很好，有待今后的继续努力，在做题中逐步成长。

特别鸣谢

- URL在线加解密
- base64在线加解密
- 百度识图
- 摩斯码在线加解密
- Unix/Linux CHMOD权限数值在线计算器

转载于:https://www.cnblogs.com/20145221GQ/p/5936482.html