hctf2014 writeup

原创

Ee1s 于 2014-11-17 23:20:41 发布 3801 收藏
分类专栏： ctf

hctf 结束有十天了吧，之前学校的课落的太多当了几天的学霸又跟得副院长商量项目，，简直忙的要炸。。终于有空来写一下htcf了。。

h

言归正传

0X01丘比龙的最爱(10pt)

这题肯定是上回去杭电的时候坐在对面的大胖子出的(ー.ー|||

Flag：甜甜圈

0X02女神(100pt)

文件下载下来解压缩然后有个txt文件，是图片的base64编码。。http://www.vgot.net/test/image2base64.php 复制粘贴就好，解出来是个女的，我对女明星也不了解，然后用图片搜索然后得出flag：爱新觉罗启星

0X03 babycrack1(100pt)

直接反编译就能看到Flag：hctf{bABy_CtsvlmE_!}

0X04gift（100pt）

f12看代码，发现提示index.php.bat下载后打开发现是个php代码，可以进行php变量覆盖（这里盗用一下萌昊的解说~：这个php的逻辑：后台有一个字符串变量flag，里面存的是一个文件名，如index.php，下一行是get方式导入不用管，再下面是个文件导入，就是把flag指向文件里面的内容提取出来删除首位空白后赋给字符串content，然后比较你输入的gift参数和content是否相同，相同时会返回hctf{...}）

所以构造网址：http://121.40.86.166:39099/index.php?flag=index.php.bak&gift=<?php$flag='xxx';extract($_GET);if(isset($gift)){$content=trim(file_get_contents($flag));if($gift==$content){echo'hctf{...}';}else{echo'Oh..';}}?>即可得到falg。。具体是啥我忘了。。万恶的居然把题封了。。

0X05babycrack2（100pt）

扔到OD，可以看到类似Flag得串。。然后发先Flag被rot了，移位就好。

1X01 entry(200pt)

介个上图吧懒得打了

提示是13，一开始不晓得怎么回事，后来想起360比赛那个坑爹现场挂0 的题觉得可能是rot13然后果然。。rot13后是md5 加密，然后查一下就好啦Flag：qoobee

2X04 normal file （300pt）

下载下了是个高清无码图~扔进hex发现里面有文件，然后用rar打开。。

发现还有张图片。。文件夹里也有张图片，把文件夹里的图片rar打开，然后出来的android。。。忍不了(＃－－)/ .。。。

然后就愉快的呵呵了~

2X05 fuckMe（350pt）

这题比较坑打开全是俄语和日语的混搭字符，一共27个字符组成如下。。

ё a
э b
г c
ш d
χ e
д f
я g
ж h
ю i
π j
ы k
θ l
ξ m
ф n
ω o低频
の p
ひ q
け r
せ s
ζ t
い u
お v
す w
え x
う y
く z
é只出现1次忽略了。。

由上可知我进行了替换，因为看着太乱了。。然后发现关键字wf qva 20qv uacqtde，，联想到of the 20th century，fwd 对应for，uwtry对应could，把第一句话弄下来使劲猜然后发现第一句话组成为in crypt analysis, frequency analysis is the study of the frequency of letters or groups of letters in a ciphertext .百度了一下居然是http://en.wikipedia.org/wiki/Frequency_analysis

言归正传字符映射为char dic[27] = "abcdefghijklmnopqrstuvwxyz";

char rot[27] = "einryfaqbxm____stlpuchogdk";jvwz

尝试寻找关键符号{} 对应上面解开即是flag~

妈蛋这题我做了3小时，眼睛都要瞎了~纯猜啊~

3X04 find（200pt）

下载是个图片，又是丘比龙。。无语。。

扔到hex没有重大发现，然后弄到Stegsolve看下通道，发现二维码，二维码有点不好弄，比较花，然后我就自己涂一涂，扫一扫的到flag~

就弄了这么几个题。。。该学学代码审计了。。。。。

明早还有马克思要点名，好讨厌~