i春秋CTF-Basic(部分Writeup)

「<u>kei</u> → 2020-11-10 20:06:57 发布 → 807 ☆ 收藏 2 分类专栏: <u>i春秋</u> 文章标签: <u>信息安全 web</u> 版权声明: 本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u> 版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/i_kei/article/details/109606150</u> 版权



i春秋 专栏收录该内容

1 篇文章 0 订阅 订阅专栏

目录

来看一下flag格式 看我回旋13踢 Base64 手贱的A君 实验室logo veryeasy 小苹果 Corrupt Transmission 熟悉的声音 取证

来看一下flag格式

分值: 10分 类型: Basic 题目名称: 来看一下flag格式

题目内容:提交flag{c7d888-36f66bfc_d2edc4f0-23def191a3} FLAG格式一般为flag{我是中间内容} 中间内容可以是中英文、大小写、特殊符号等。

直接将题目中flag提交即可

看我回旋13踢

分值: 50分 类型: Crypto Basic 题目名称: 回旋13踢

题目内容:看我回旋13踢 synt{5pq1004q-86n5-46q8-o720-oro5on0417r1}

根据题目,联想到ROT13,进入这个网址解码(https://www.qqxiuzi.cn/bianma/ROT5-13-18-47.php)

ROT13 编码: (字母) synt {5pq1004q-86n5-46q8-o720-oro5on0417r1}

 ROT47
 ROT18
 ROT13
 ROT5
 复位

 (点击第一次加密点击第二次解密)

ROT13 编码: (字母) flag{5cd1004d-86a5-46d8-b720-beb5ba0417e1} ROT47 ROT18 ROT13 ROT5 复位

(点击第一次加密 点击第二次解密)

Base64

根据题意,题目中密文可以用base64解码

分值: 50分 类型: Basic 题目名称: Base64

已解答

题目内容: GUYDIMZVGQ2DMN3CGRQTONJXGM3TINLGG42DGMZXGM3TINLGGY4DGNBXGYZTGNLGGY3DGNB WMU3WI===

进入此网站进行base64解码 (http://ctf.ssleye.com/base64.html) 但是解码过程中发现解码失败

— base编码

base16、base32、base64

GUYDIMZVGQ2DMN3CGRQTONJXGM3TINLGG42DGMZXGM3TINLGGY4DGNBXGYZTGNLGGY3DGNBWMU3WI===

| 加密或解密字符串长度不可以超过10M |
|--|
| 504354467b4a7573745f743373745f683476335f66346e7d |

16进制到文本字符串的转换,在线实时转换

16进制到文本字符串的转换,在线实时转换(支持中文转换)

复制下来进这个网站(https://www.bejson.com/convert/ox2str/) 进行16进制转字符

发现解码出一段16进制

GUYDIMZVGQ2DMN3CGRQTONJXGM3TINLGG42DGMZXGM3TINLGGY4DGNBXGYZTGNLGGY3DGNBWMU3WI===

编码 字符集 base32 utf8(unicode编码) 编码 解码 504354467b4a7573745f743373745f683476335f66346e7d

base编码

接着换base32试试

base16、base32、base64

| 编码 | base64 | ~ | 字符集 | utf8(unicode编码) | ~ | |
|------|--------|---|-----|-----------------|---|----|
| | | | | 编码 | | 解码 |
| 马失败! | | | | | | |

| 16进制转字符 | 字符转16进制 | 清空结果 | | | | | | |
|--------------------------|---------|------|--|--|--|--|--|--|
| PCTF{Just_t3st_h4v3_f4n} | | | | | | | | |

得到flag

手贱的A君

题目内容:某天A君的网站被日,管理员密码被改,死活登不上,去数据库一看,啥,这密码md5不是和原来一样吗?为啥登不上咧? d78b6f302l25cdc811adfe8d4e7c9fd34 请提交PCTF{原来的管理员密码}

题目中提到md5加密,猜测这一长串密文需要使用md5解密



然而却解密失败,之后发现原来题目中给的是33位,而完整的MD5是32,仔细查看后其中混入了一个I,删除之后继续解密

| | 密文: d78b6f302 | d78b6f30225cdc811adfe8d4e7c9fd34 | | | | | |
|---------------|---------------|----------------------------------|----|--|--|--|--|
| | 关型: 日初 | 查询 | 加密 | | | | |
| 查询结果: hack | | | | | | | |

加上格式提交

题目内容:某天A君的网站被日,管理员密码被改,死 登不上咧? d78b6f302l25cdc811adfe8d4e7c9fd34 请提交PCTF{原来的管理员密码}

Flag: PCTF{hack}

🕑 回答正确

得到flag

实验室logo

题目内容:出题人丢下个logo就走了,大家自己看着办吧



看到图片盲猜隐写 将图片下载下来丢到kali,将图片分离



打开分离出来的图片

PCTF{You_are_R3ally_Car3ful}

获得flag

veryeasy

*

分值: 50分 类型: Basic 题目名称: veryeasy

题目内容:咦,这是什么文件?难道是我打开的方式不对吗? 文件: 附件下载

先下载附件



veryeasy

加上txt后缀,用记事本打开看看有什么信息

🥘 veryeasy.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

UH夂1缷M?M魤M黓脨悙□ 4 □ ▲ □ □ □ PCTF{strings_i5_3asy_isnt_i7}

往下划拉发现flag

小苹果

分值: 80分 类型: Basic 题目名称: 小苹果

题目内容:仔细听,听到就给你Down

该文件在百度云上,下载该文件(我不是盘神~QAQ) 自行在网上下载SilentEye,打开该文件





点击decode解密

| 😫 Decode mess | age: F:/Downloads/little_apple.wav | ? | × |
|-----------------|--|---------------|-------|
| | Media's encoding format : Options Sound quality: 93.75% normal Used channels: Date distribution mode Header position: bit(s) per sample per channel: 3 ÷ | WAVE Adva | |
| Deco | ded message flag{b1a63978-cd55-4ebf-a316-5f3a96fc466b} | | |
| CharSet: UTF8 - | 🛛 🖉 🦳 Encrypted data 🗹 Compressed dat 🧕 🥹 Cancel | 🕗 De | ecode |

获得flag

Corrupt Transmission

题目内容: We intercepted this image, but it must have gotten corrupted during the transmis sion. Can you try and fix it? <u>corrupt png</u>

图片传输过程中损坏,需要我们去修,下载该文件用winhex打开

| Offset | 0 | 1 | 2 | 3 | 4 | - 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|----------|----|----|----|----|----|-----|----|----|----|----|----|----|----|----|----|----|
| 00000000 | 89 | 50 | 4E | 47 | 0D | 0A | 1A | 0A | 00 | 00 | 00 | 0D | 49 | 48 | 44 | 52 |
| 00000016 | 00 | 00 | 01 | F4 | 00 | 00 | 01 | 98 | 08 | 06 | 00 | 00 | 00 | в4 | E0 | 10 |

改成如图即可打开损坏文件(找个能打开的png文件将它正确的字节复制到损坏的文件里)



熟悉的声音

- 分值: 50分 类型: Basic 题目名称: 熟悉的声音
- 题目内容:两种不同的元素,如果是声音的话,听起来是不是很熟悉呢, 据说前不久神盾局某位特工领便当了大家都很惋惜哦 XYYY YXXX XYXX XXY XYY X XYY YX YYXX 请提交PCTF{你的答案}

只有两种声音,结合给的一串英文字母,应该是摩斯密码 使用python将'X'和'Y'转换成'.'和'-'

print ("XYYY YXXX XYXX XXY XYY X XYY YX YYXX".replace("X",".").replace("Y","-"))

print ("XYYY YXXX XYXX XXY XYY X XYY YX YYXX".replace("Y",".").replace("X","-"))

运行结果如下

======= ---- -.....-..- ..-- ...--... -.....--- -..- -...- -...-

>>>

将两串密码都解密

| 퉬 米斯特安全团队 CTFCrakTools pro v2.0 Beta |
|--------------------------------------|
| 解码方式 进制转换 插件 妹子 其他功能 |
| 填写所需检测的密码:(已输入字符数统计:36) |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| 结果: |
| JBLUWEWNZ |
| |

| 🏄 米斯特安全团队 CTFCrakTools pro v2.0 Beta |
|--------------------------------------|
| 解码方式 进制转换 插件 妹子 其他功能 |
| 填写所需检测的密码:(已输入字符数统计:36) |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| • |
| 结果: |

BJYGDTDAnull

然后用凯撒密码解密

| 解码方式 | 进制转换 插件 妹子 其他功能 |
|-----------|-----------------------------|
| 填写所需检 | 测的密码:(已输入字符数统计:9) |
| JBLUWEWNZ | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| 41 97 | |
| 35 木: | |
| | |
| MEOX7H700 | |
| NEPYALARD | |
| OGOZBJBSE | |
| PHRACKCTF | |
| QISBDLDUG | |
| RJTCEMEVH | |
| SKUDFNFWI | |
| TLVEGOGXJ | |
| UMWFHPHYK | |
| VNXGIQIZL | |
| WOYHJRJAM | |
| XPZIKSKBN | |
| YQAJLILCO | |
| | |
| 获得flag | |
| 5 criting | |
| 计一下 | |
| | |
| | |
| 昭日中応 | 西釉不同的元素 如里早青辛的话 听起来早不早泪勃来吗 |
| 巡日内谷: | 网络大力油的分散,如本这个自动中,所包不足不足的感觉。 |
| | 循项削小人种盾向来12存上视度当了人家和R的帽收 |
| | |
| | 请提交PCTF{你的答案} |
| | |
| Flag: | PCTF{PHRACKCTF} |
| 5 | |
| I | 回答正确 |
| | |
| | |

正确

取证

分值: 50分 类型: Basic 题目名称: 取证



emmm, 百度搜就可以搜出来

Volatility 简介:

Volatility是一款开源的,基于Python开发的内存取证工具集,可以分析内存中的各种数据。Volatility支持对32位或64位Wnidows、Linux、Mac、Android操作系统的RAM数据进行提取与分析。



Flag: PCTF{volatility}

🕑 回答正确

软件名称全小写即为flag

如有错误,敬请斧正

已解答