CTF-Crypto-(1)

原创

北纬33度的小白 于 2020-09-15 23:17:18 发布 867 收藏 2

分类专栏： ctf

本文链接：https://blog.csdn.net/qq_42937520/article/details/108611834

一、

题目：

59574a4b4432503243535847544859415 64d4154584559564235465356335144575758545645563d

解题：

长度是偶数位，考虑十六进制转字符串 hex-str

转换后得：

YWJKD2P2CSXGTHYAVMATXEYVB5FSV3QDWWXTVEV=

ROT 13解密：

ljwxq2c2pfktgulnizngkrlio5sfi3dqjjkgiri=

Base32 解密：

ZmxhZyU3QmFZeEhwdTlpJTdE

Base64解密：

flag%7BaYxHpu9i%7D

%7B %7D是{} 括号的Url编码，

Url解码：

flag{aYxHpu9i}

二、

题目：

NWE0ZDRhNTQ1MDRkMzMzMzU3NDEzNDUxNTY0NTQ1NGQ1NDU3NTU0OTUyMzc1NjI1MzM1MQ==

Base64解码：

5a4d4a54504d3333574134515645454d545755495 23756253351

Hex-str 十六进制转字符串

ZMJTPM33WA4QVEEMTWUIR7V%3Q

凯撒解码：

%3D是url编码的=号，找到凯撒解码结尾是%3D的。

MZWGCZ33JN4DIRRZGJHVE7I%3D

把%3D去掉或者改为=，然后进行Base32解码：

Base32解码：

flag{Kx4F92OR}

签个到吧
(一) 关卡描述
既然来了，签个到再走吧。
(二) 解题步骤
打开文件：
V1ROU2JXVXlTbWhqTWxabVRtcFNPUT09
Base64解码：
WTNSbWUySmhjMlZmTmpSOQ==
再次Base64解码：
Y3Rme2Jhc2VfNjR9
再次Base64解码：
ctf{base_64}
(三) Flag
ctf{base_64}

KeyBoard
(一) 关卡描述
看键盘看键盘看键盘！
(二) 解题步骤
密文：ytfvbhn tgbgy hjuygbn yhnmki tgvhn uygbnjm uygbn yhnijm
你能从键盘上发现什么？
将题目给出的字符串在键盘上敲一遍，注意手指的轨迹，得出flag为：
areuhack

(三) Flag
Flag{areuhack}

请破译密码
(一) 关卡描述
密码是什么呢？
(二) 解题步骤

记事本直接打开得到flag
flag{666C61677B68315F6337667D}
直接提交发现错误，{}内为十六进制，尝试十六进制转字符。
flag{h1_c7f}
(三) Flag
flag{h1_c7f}
丢失的MD5
(一) 关卡描述

题目：丢失的MD5
题目描述：python大法好！
(二) 解题步骤
python大法好！
这里有一段丢失的md5密文
e9032???da???08???911513?0???a2
要求你还原出他
已知线索 明文为： TASC?O3RJMV?WDJKX?ZM
题目为MD5碰撞
我们知道MD5理论上是不可逆的，我们只能通过明文来计算出MD5，然后再和已知的MD5进行比对。
分析可知 : 明文缺失了3个字符，写个python脚本进行爆破

```
import hashlib
for i in range(32,127):
for j in range(32,127):
for k in range(32,127):
m=hashlib.md5()
m.update('TASC'+chr(i)+'O3RJMV'+chr(j)+'WDJKX'+chr(k)+'ZM')
des=m.hexdigest()
if 'e9032' in des and 'da' in des and '911513' in des:
print des
```

e9032994dabac08080091151380478a2
(三) Flag
Flag{ e9032994dabac08080091151380478a2 }

图片中的密码
(一) 关卡描述
题目：图片中的密码
题目描述：你能发现什么？
(二) 解题步骤.
下载后是个图片：

查看图片属性，大小和实际占用存在一定差别。

Binwalk以下看看：

包含rar文件。
分离一下得到：

请将"TWpBeE5ERXdNVFE9"用Base64两次解密后得到密码。
Base64第一次解码：
MjAxNDEwMTQ=
Base64第二次解码：
20141014
(三) Flag
Flag{20141014}

AES解密
(一) 关卡描述
题目：AES解密
题目描述：高级的加密。
(二) 解题步骤
密文：U2FsdGVkX19PuxOY5/W+kfD11dhgSbz51GoOSb9pJJlGbW75qXuivEkf5fr5R03Q
在线工具解密：

Flag{Xlsro4l67Do27E}
(三) Flag
Flag{Xlsro4l67Do27E}

html解密
(一) 关卡描述
题目：html解密
题目描述：从网页中找到登陆密码。
(二) 解题步骤
访问exam.html，发现需要登录；

查看web源码，从js代码中找到ht_click()方法；
在console中，调用该方法，得到密码admin123465；

输入密码，得到flag信息。

91aee1e0d6a80a8b5fe190d7ad254d7f
(三) Flag
Flag{91aee1e0d6a80a8b5fe190d7ad254d7f}

Windows系统密码
(一) 关卡描述

题目：Windows系统密码
题目描述：我的密码忘了，你能帮我找回吗？
(二) 解题步骤
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ctf:1002:06af9108f2e1fecf144e2e8adef09efd:a7fcb22a88038f35a8f39d503e7f0062:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:bef14eee40dffbc345eeb3f58e290d56:::
看上边的格式，应该是用户名：密码。ND5解码 ctf的a7fcb22a88038f35a8f39d503e7f0062

good-luck
(三) Flag
Flag{ good-luck}

奇怪的数字
(一) 关卡描述
题目：奇怪的数字
题目描述：你用过拼音九键吗？
(二) 解题步骤
33 53 21 41 43 74 43 53 63 83 32 71 42 63 62 32
1、 根据提示，把手机调成拼音九键，33，代表第3个按键上的第三个字母，也就是F
2、 53代表的是第5个按键上的第三个字母，也就是L，以此类推…
3、 33 53 21 41组合起来，刚好是单词拼写flag
4、 把剩余的进行翻译，得到flag为flagisilovephone 直接提交。

(三) Flag
Flag{isilovephone}

Linux系统密码
(一) 关卡描述
题目：Linux系统密码
题目描述：我的密码忘了，你能帮我找回吗？
(二) 解题步骤
打开题目，发现一串密文

linux用户的密码存在/etc/shadow这个文件中，密文格式为：idsalt$encrypted$，其中id用来指定使用的算法：
使用kali下的John工具破解密码，得到ctf用户的密码。

5201314
(三) Flag
Flag{5201314}

hash还原
(一) 关卡描述
题目：31-hash还原
题目描述：小明一直将电脑密码的Hash值写在标签纸上，结果一不小心墨水撒到了上面，只能看到前十位是c2979c7124，另外小明记得他的密码是4位的数字加字母，你能帮小明恢复密码的Hash值吗？（密码的Hash值即为Flag值）
(二) 解题步骤
通过分析前十位可以猜测出这个密文的加密方式是MD5。
使用Python编写脚本进行爆破猜解：

```
import hashlib
import itertools
import hmac
key = 'c2979c7124'
dir = '1234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ'
dir_list = itertools.product(dir, repeat=4)
for i in dir_list:
res = hashlib.md5(''.join(i)).hexdigest()
if res[0:10] == key:
print i
print res
```

得到：c2979c71244dec2befc6e369941c6546

(三) Flag
Flag{c2979c71244dec2befc6e369941c6546}

大帝的密码武器
(一) 关卡描述
题目： 大帝的密码武器
题目描述： 什么？没听说过本大帝？
(二) 解题步骤
公元前一百年，在罗马出生了一位对世界影响巨大的人物，他生前是罗马三巨头之一。他率先使用了一种简单的加密函，因此这种加密方法以他的名字命名。
以下密文被解开后可以获得一个有意义的单词：FRPHEVGL
你可以用这个相同的加密向量加密附件中的密文，作为答案进行提交。
大帝的密码，猜测是凯撒加密。进行凯撒解密：

把大写的字符串转换为小写的。
security
或者采取脚本进行凯撒解密：
#! /usr/bin/env python

-- coding: utf-8 --

def translateMessage(key, message, mode):
LETTERS = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
translated = ''

```
for symbol in message:
    if symbol.upper() in LETTERS:
        num = LETTERS.find(symbol.upper())
        if mode == 'encrypt':
            num = num + key
        elif mode == 'decrypt':
            num = num - key

        if num >= len(LETTERS):
            num = num - len(LETTERS)
        elif num < 0:
            num = num + len(LETTERS)
        if symbol.isupper():
            translated = translated + LETTERS[num]
        elif symbol.islower():
            translated = translated + LETTERS[num].lower()
    else:
        translated = translated + symbol
return translated
```

if **name** == '**main**':

```
# key     = 13
mode    = 'decrypt'
#message = 'FRPHEVGL'
message = 'FRPHEVGL'

for key in range(0,26):
    print(str(key)+':'+translateMessage(key,message,mode).lower())
```

security

(三) Flag
security

又是什么加密呢
(一) 关卡描述

题目：33-又是什么加密呢
题目描述：只听说过凯撒？你OUT了！
(二) 解题步骤

打开图片：

在学习了凯撒大帝使用的神奇密码后，密码前辈们又创造出了更为奇异的加密方法。维吉尼亚是其中一种。。哎呀。。讲太多了。。顺便说一句，出题者是一个程序员，喜欢拿helloworld做秘钥~~下面是密文dlpcsegkshrij,请破解后提交。附录是一张似乎有用的表。
看到图片，是维吉尼亚解密。
根据秘钥、密文进行在线解密：http://www.metools.info/code/c71.html

得到flag：whereisthekey

(三) Flag
Flag{whereisthekey}

木册木兰
(一) 关卡描述
题目： 木册木兰
题目描述： 木册木兰是什么鬼？
(二) 解题步骤
打开题目：fsf5lrdwacloggwqi11l
木册木兰，猜测是栅栏密码解密：
在线解密：https://www.qqxiuzi.cn/bianma/zhalanmima.php

flagisrcg1fdlw15woql
(三) Flag
Flag{isrcg1fdlw15woql}

摩丝
(一) 关卡描述
题目： 摩丝
题目描述： 摩丝？我用过啊…
(二) 解题步骤
打开文件：… .-… — …- . -.-- — …-
在线摩斯解码：http://www.zhongguosou.com/zonghe/moErSiCodeConverter.aspx

lLOVEYOU
(三) Flag
Flag{lLOVEYOU}

base32
(一) 关卡描述
题目：base32
题目描述：只知道base64？你太low了! 密文:KRUGS4ZANFZSAYTBONSTGMQ=
(二) 解题步骤
base32解码：
在线解密：https://www.qqxiuzi.cn/bianma/base.php

This is base32

(三) Flag

Flag{ This is base32}

base16

(一) 关卡描述

题目： 37-base16

题目描述： 只知道base64？你太low了! 密文：54686973206973206261736531 36

(二) 解题步骤

Base16解密：

Base16在线解密：https://www.qqxiuzi.cn/bianma/base.php?type=16

This is base16

(三) Flag

Flag{This is base16}

Brainfuck

(一) 关卡描述

题目： Brainfuck

题目描述： 后面4个单词有点危险啊

(二) 解题步骤

++++++++++[>+++++++>++++++++++>+++>+<<<<-]>++.>+.+++++++..+++.>++.<<+++++++++++++++.>.+++.------.--------.>+.>.

Brainfuck在线解密：

在线工具网址：https://tool.bugku.com/brainfuck/

Hello World!

(三) Flag

Flag{Hello World!}