CTFHub学习笔记(3) - 部分题目

原创

 TRPH
 ● 2020-08-31 14:05:08 发布
 ● 409 % 收藏

 分类专栏:
 网络安全 文章标签: 信息安全 加密解密 经验分享

 版权声明:本文为博主原创文章,遵循 CC 4.0 BY-SA 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/gg 49077418/article/details/108319910</u>



网络安全专栏收录该内容

3 篇文章 0 订阅 订阅专栏

目录

回转十三位 马男波杰克 签个到 just a rar 藏藏藏 sign in

check in

hidden

一叶障目

boom

回转十三位

下载附件,先看到一串字符串像是base64加密

🥘 2we4rft67ytr5tj89edrf456gyh.txt - 记事本

文件(E) 编辑(E) 格式(Q) 查看(V) 帮助(H)

EzkuM0yGAzA2n3WbEaOJEHuOFmuOpN==

解密试试

1

2we4rft67ytr5tj89edrf456gyh.txt🔟 |

DC39.3Lx86ETX06x9Fux9BDC1xA3x89DLE{x8ESYNkx8ExA4

好像不行,又想到题目是回转十三位,那这样看来应该是先用一次rot13解密



再试试base64,得到flag

请将要加密或解密的内容复制到以下区域

FlagIS6cvkrhFpVEHAK8Ap



附件是一个图片



名字是atool,是提示要用一个工具嘛...属性里面也没有什么有用的信息

先试试stegsolve,好像不是很行

又看到hint说要百度,就去百度了一下atool,发现了网站



搜索工具关键词,例如: php

图片隐写术加密、图片隐写术解密 - aTool在线工具

【图片处理推荐:】

iOS | 安卓图片批量剪裁 | 透明图片resize / 压缩大小 | png | jpg无损压缩 | 制作透明圆角图片 | 图片格式转似 gif表情制作 | 图片隐写术 | 手绘图片制作

又去了github找到了在线工具



得到flag

签个到

下载附件。提示文件损坏

用winhex看看

	hello.zip																		
1	Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII	~
	00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR	
	00000016	00	00	01	1C	00	00	01	0E	08	06	00	00	00	5B	ΕA	A 8	[ê"	
	00000032	70	00	00	05	Α7	49	44	41	54	78	9C	$^{\rm ED}$	DD	41	6E	EC	p §IDATxœíÝAnì	
	00000048	36	10	40	C1	38	C8	$\mathbf{F}\mathbf{D}$	AF	EC	C4	AB	EF	8D	01	DA	A1	6 @Á8Èý [─] ìÄ≪ï Ú;	
	00000064	1E	9B	9E	AA	03	8C	64	8D	FC	C0	45	A3	E7	ED	\mathbf{FD}	3F	>žª Œd üÀE£çíý?	
	00000080	7F	01	04	FE	3E	7D	03	C0	EB	10	1C	20	23	38	40	46	þ>} Àë #80F	
	00000096	70	80	8C	E0	00	19	C1	01	32	82	03	64	04	07	C8	80	p€Œà Á 2, d È	

发现是png格式的,修改后缀名打开



https://blog.csdn.net/qq_49077418

得到了二维码,扫描得到flag

位置:(23.1,16.1)-(261.9,16.1)-(23.1,254.9)-(261.9,254.9) 颜色正常,正像 版本: 2 纠错等级:M, 掩码:1 内容: xaflag{i_am_a_tupian}

just a rar

附件是一个加密的rar压缩包,提示是4位数看来是个爆破

🔏 ARCH	IPR 4.54 -	20%				_	×			
文件(F)	恢复(R)	帮助(H)								
2	. R	<u></u>	()	- 🍫	2					
打开	开始!	停止	基准则证	t 升级	帮助	关于	退出			
口令已成	跋功恢复!						×			
Advanced Archive Password Recovery 统计信息:										
总计口令 2,021										
总计时	间			6s 764ms						
平均速	[度 <mark>(口令/</mark> 和	少)		298						
这个文	(件的口令			2016						
十六进制口令 32 30 31 36										
₩ 保存 ♥ 确定										
状态窗口										
\253_51 2020/8/3	d29763626 30 19:26:5	5dc8cd6dffe9 0 - 开始暴力	icfb7f362e)攻击	6fa7a8244\4	位数.rar"已	打开。	^			
2020/8/30 19:26:56 - 口令已成功恢复! 2020/8/30 19:26:56 - '2016' 是这个文件的一个有效口令										
当前口念	2	016		平均速度	: 2	98 p/s				
日令长度	。 = 4, 总计:	s : 10,000, 已;	处理 <mark>: 2,0</mark> 2		j: 2	DS				
				20%						
ARCHPR ve	ersion 4.54	(c) 1997-20	12 ElcomSo	ft Co. Ltd.	s://blog.cs	_pp\ten.nb	2190772118			

解压缩后,在图片备注里看到flag



属性	值
说明 ——	
标题	
主题	
分级	$\begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c} \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} $
标记	
备注	flag{Wadf 123}
大 で に に に に に に に に に に に に に	:://biog.csdn.nevqq_4907741

藏藏藏

是一道图片隐写题,属性里面没有藏东西,用foremost试试,分出来了一个zip



https://blog.csdn.net/qq_49077418

解压出来是一个word, 扫码得到flag

位置:(10.2,6.2)-(372.8,6.2)-(10.2,368.8)-(372.7,368.7) 颜色正常, 正像 版本: 3 纠错等级:Q, 掩码:6 内容: flag{you are the best!}

sign in

附件是一个txt

welcome to crypto world!! 密文: 424a447b57653163306d655f74345f424a444354467d

密文看起来像是16进制的,转换一下试试



得到flag

check in

打开网页,发现没有什么东西,只好先去看看header,发现了一个flag

	Elements	Console	Sources	Network	Performanc	e Men	nory	Applicatio	on Security	Lighthou	ise JavaSci	ript Profil		
• •	ଟୁ ପ୍ 🛛	Preserve	log 🗌 Disabl	e cache O	nline 🔻	<u></u>	ŧ							
Filter		□ F	lide data URLs	All XHR J	IS CSS Im	g Media	Font	Doc WS	Manifest Ot	her 🗌 Has	blocked cook	ies 🗌 B		
5 ms	10 ms	15 m	1s 20 ms	25 ms	30 r	ıs	35 ms	40 ms	s 45 ms	50 ms	55 ms	6		
Name			× Headers	Preview	Response	Initiator	r Tir	ming						
challenge	e-0b8c4c26b0)9d025a	Remote A	ddress: 47.9	8.148.7:1	080								
Referrer Policy: no-referrer-when-down														
			▼Response Headers view source											
			Access-Control-Allow-Headers: X-Requested-With Access-Control-Allow-Methods: *											
			Access-Control-Allow-Origin: *											
Connection: keep-alive														
Content-Length: 0														
Content-Type: text/html; charset=UTF-8														
			Date: Sun	, 30 Aug 20	20 11:57:	LØ GMT								
			FLAG: Y3RmaHVie2EyZj11MGUxND1iNWNiYjI0NmYwYWI5YjdmOTdkODBkZmU3NTViZWF9											
Server: openresty/1.15.8.2														

base64解密得到flag

hidden

图片属性没什么东西,用foremost分离出一个zip,发现文件被加密了,又没有什么提示,先试了试伪加密,发现不对,直接试 试爆破

ARCHPR 4.54 - 12%		_	×						
文件(F) 恢复(R) 帮助(H)									
a a a	े 🍫 🌘	2							
打开 开始! 停止 基准	题版式 升级 帮	1助 关于	退出						
]令已成功恢复!			×						
Advanced Archive F	Password Recovery 统计	·信息:							
总计口令	1,231		_						
总计时间 10ms									
平均速度(口令/秒)	123,100								
这个文件的口令 1235									
十六进制口令 31 32 33 35									
┏ 保存…	V	确定							
状态窗口									
\00000148.zip"已打开。			^						
2020/8/30 20:12:59 - 开始暴力攻击。 2020/8/30 20:12:59 - 口令已成功恢	夏!								
2020/8/30 20:12:59 - 开始暴力攻击。 2020/8/30 20:12:59 - 口令已成功恢 2020/8/30 20:12:59 - '1235' 是这个文	夏! 【件的一个有效口令		~						
2020/8/30 20:12:59 - 开始暴力攻击; 2020/8/30 20:12:59 - 口令已成功恢; 2020/8/30 20:12:59 - '1235' 是这个交 当前口令: 1235 已用时间: 口令长度 = 4, 总计: 10,000, 已处理:	夏! (件的一个有效口令 平均速度: 剩余时间: 1,231	175,857 p/s	~						



得到了一半的二维码

winhex改变图片高度并解码

QR Research	_		×
文件(F) 工具(T) 帮助(H)			
in the second se	ti 🕡 ,		
	纠错等级 H(30%) ▼ 版本 Auto Auto	掩码 Auto 尺寸 4	•
			^
			~
已解码数据 1:			~
位置:(-0.0,-0.0)-(132.0,-0.0)-(0.0,132.0)-(132.0,132 颜色正常,正像 版本:4 纠错等级:Q,掩码:5 内容: flag{04255185-de22-4ac6-a1ae-da4f187ddb8c}	-		~
解码完成	https://blog.osdm.r	iet/cld_490	1774118

得到flag

一叶障目

foremost查看图片,没有隐藏文件,用stegsolve也没有发现什么隐藏

最后用kali打开图片的时候发现



用crc修复工具修复图片

得到flag



boom

```
附件是一个exe, 用ida打开
                                     три Атем и 📖
                     🚤 i bouuvovuo ii 🧫
     48 v21 = 189;
     49
        v22 = 1;
     50
        puts("first:this string md5:46e5efe6165a5afb361217446a2dbd01");
        scanf("%s", &v5);
     51
        MD5Init(&v23);
     52
     53
        v3 = strlen(&v5);
        MD5Update((int)&v23, &v5, v3);
     54
     55
         MD5Final(&v23, v6);
     56
         v28 = 1;
     57
         for (i = 0; i \le 15; ++i)
     58
         {
           if ( v6[i] != *(&v7 + i) )
     59
     60
           {
             v28 = 0;
     61
     62
             break;
     63
           }
     64
         }
     65
         if ( v28 != 1 )
     66
         {
     67
           printf("Game over");
     68
           system("pause");
     69
           exit(0);
     70
         }
     71
         puts("Great next level");
     72
         system("pause");
     73
         system("cls");
     74
        puts("This time:Here are have some formulas");
     75
        puts("3x-y+z=185");
        puts("2x+3y-z=321");
     76
     77
         puts("x+y+z=173");
     78
         printf("input: x = ");
     79
         scanf("%d", &v27);
         printf("input: y = ");
     80
     81
         scanf("%d", &v26);
         printf("input : z = ");
     82
     83 scanf("%d", &v25);
```

先是一个md5,直接在线解密

!)您查询的字符串是"46e5efe6165a5afb361217446a2dbd01",解密的结果为"<mark>en5oy</mark>"!

```
10
  74
      puts("This time:Here are have some formulas");
75
     puts("3x-y+z=185");
  76 puts("2x+3y-z=321");
.
  77
      puts("x+y+z=173");
  78 printf("input: x = ");
scanf("%d", &v27);
  79
printf("input: y = ");
80
      scanf("%d", &v26);
81
      printf("input : z = ");
  82
      scanf("%d", &v25);
  83
      if ( 3 * v27 - v26 + v25 != 185 || 2 * v27 + 3 * v26 - v25 != 321
  84
۰
  85
      {
  86
        printf("Game over");
  87
        exit(0);
   88
      }
      printf("Great last level coming...");
  89
  90 printf("pause");
91
     system("cls");
92
      puts("Last time: Kill it");
      puts("x*x+x-7943722218936282=0");
93
      printf("input x: ");
94
95
      scanf("%11d", &v24);
  96
      if ( v24 * (v24 + 1) != 7943722218936282LL )
  97
      {
        printf("Game over");
  98
 99
        exit(0);
  100
      }
      puts("Great This is your FLAG"); https://blog.csdn.net/qq_49077418
0101
```

后面按部就班的算就行了,得到flag

x*x+x-7943722218936282=0 input x: 89127561 Great This is your FLAG flag{en5oy_746831_89127561}