

CTFHub学习笔记(3) - 部分题目

原创

7RPH 于 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: https://blog.csdn.net/qq_49077418/article/details/108319910

版权



[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(O) 查看(V) 帮助(H)
EzkuM0yGAzA2n3WbEaOJEHuOFmuOpN==

解密试试

```
2we4rft67ytr5tj89edrf456gyh.txt x |  
1 DC39.3Lx86ETX06x9Fu x9BDC1xA3x89DLE { x8E SYNk x8E xA4
```

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

字符串

```
EzkuM0yGAzA2n3WbEaOJEHuOFmuOpN==
```

计算

解码结果

```
RmxhZ0ITNmN2a3JoRnBWRUhBSzhBcA==
```

复制

https://blog.csdn.net/qq_49077418

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
```

马男波杰克

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 | 图片格式转换
gif表情制作 | 图片隐写术 | 手绘图片制作


https://blog.csdn.net/qq_49077418

又去了github找到了在线工具

A stego tool in pure HTML5 by Zach Oakes.
Works well in Chrome, Firefox, Opera, and IE10+.
[How it works.](#)

CHOOSE AN IMAGE

选择文件 atool.png



HIDDEN MESSAGE

flag{jioiuojoi666}

https://blog.csdn.net/qq_49077418

得到flag

签个到

下载附件。提示文件损坏

用winhex看看

hello.zip																ANSI ASCII		
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	%PNG	IHDR
00000016	00	00	01	1C	00	00	01	0E	08	06	00	00	00	5B	EA	A8	[è	
00000032	70	00	00	05	A7	49	44	41	54	78	9C	ED	DD	41	6E	EC	p SIDATxœíYAni	
00000048	36	10	40	C1	38	C8	FD	AF	EC	C4	AB	EF	8D	01	DA	A1	6 @Á8Èý~iÄ«i Ú;	
00000064	1E	9B	9E	AA	03	8C	64	8D	FC	C0	45	A3	E7	ED	FD	3F	>žª Qd ùÀÈ£çíý?	
00000080	7F	01	04	FE	3E	7D	03	C0	EB	10	1C	20	23	38	40	46	p>} Àè #8@F	
00000096	70	80	8C	E0	00	19	C1	01	32	82	03	64	04	07	C8	08	pegà Á 2, d È	

发现是png格式的，修改后缀名打开



https://blog.csdn.net/qq_49077418

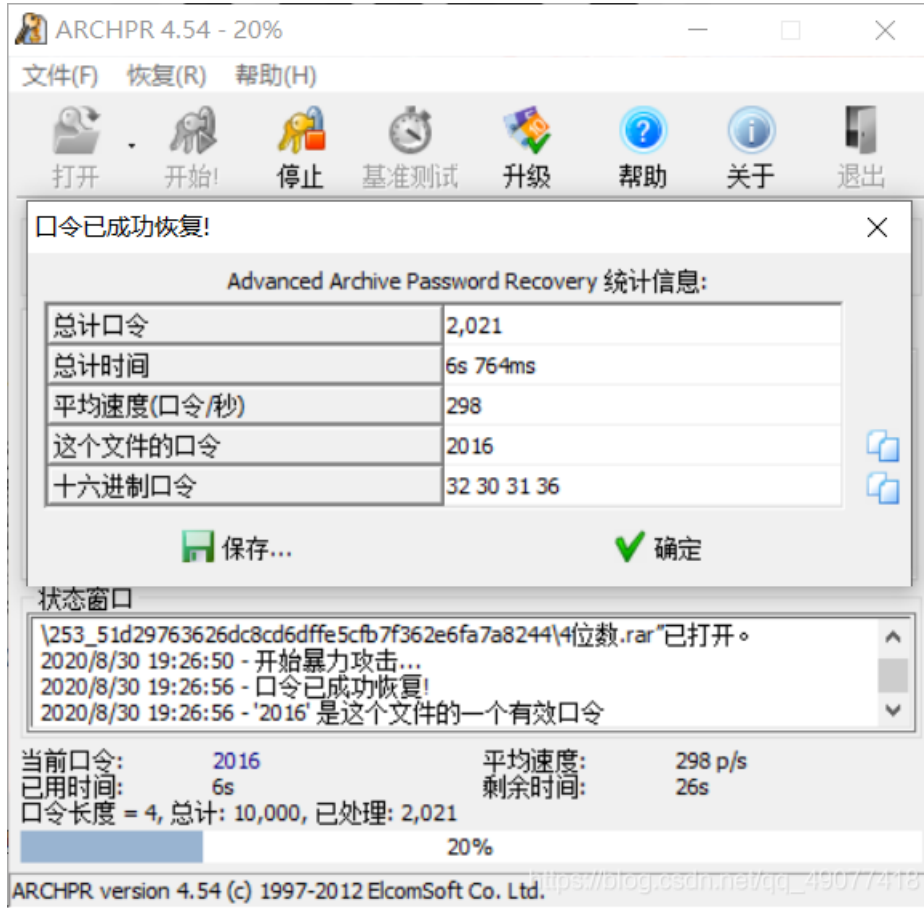
得到了二维码，扫描得到flag

```
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

先试试纯数字，直接爆出了密码



解压缩后，在图片备注里看到flag



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!}
```

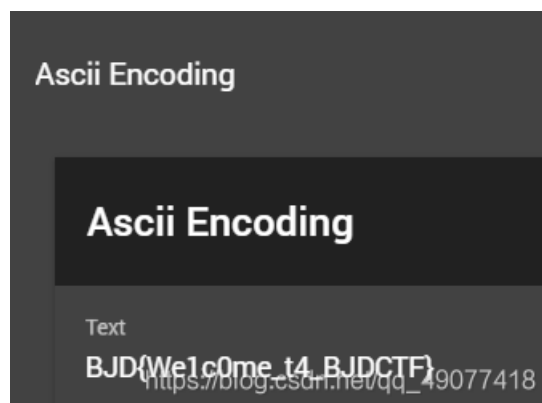
sign in

附件是一个txt

welcome to crypto world! !

密文: 424a447b57653163306d655f74345f424a444354467d|

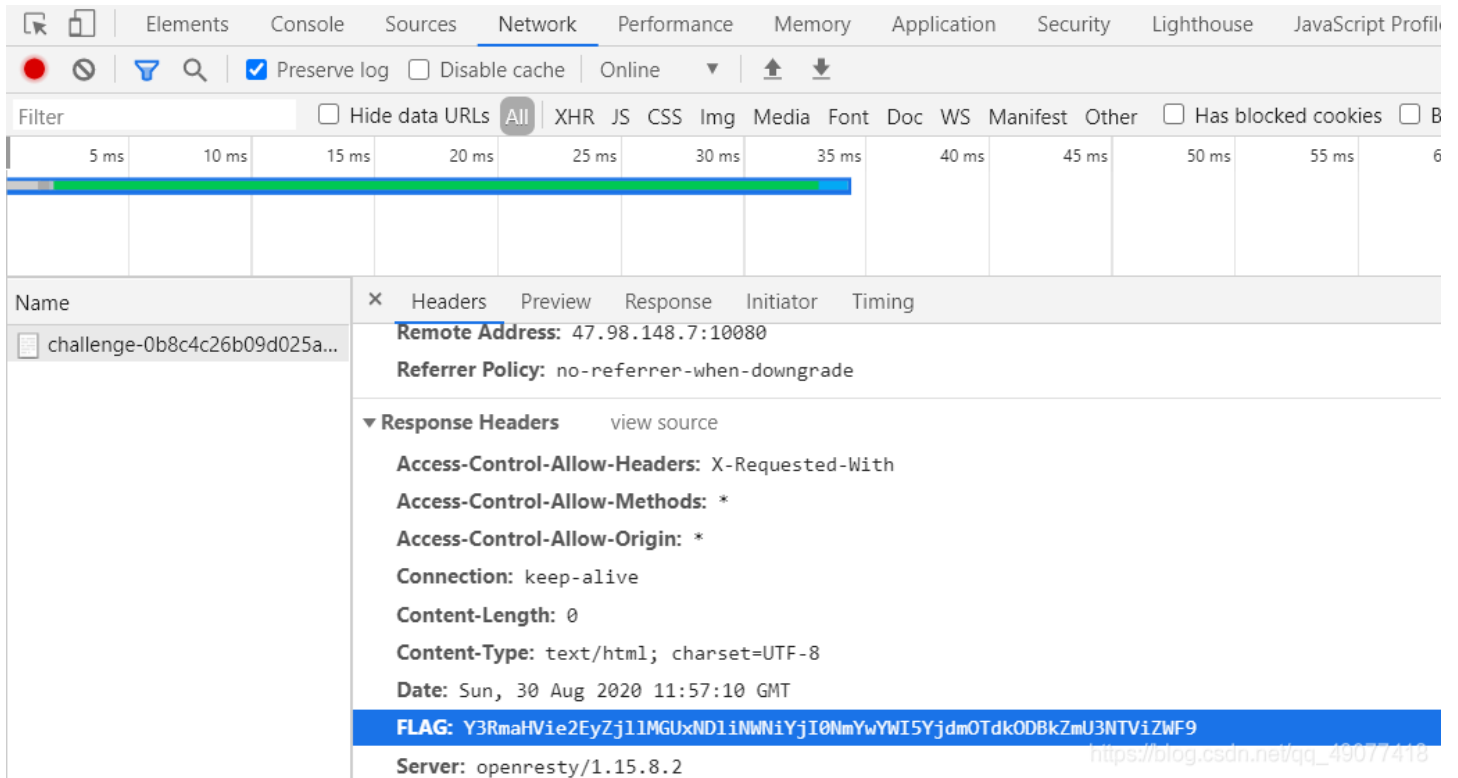
密文看起来像是16进制的，转换一下试试



得到flag

check in

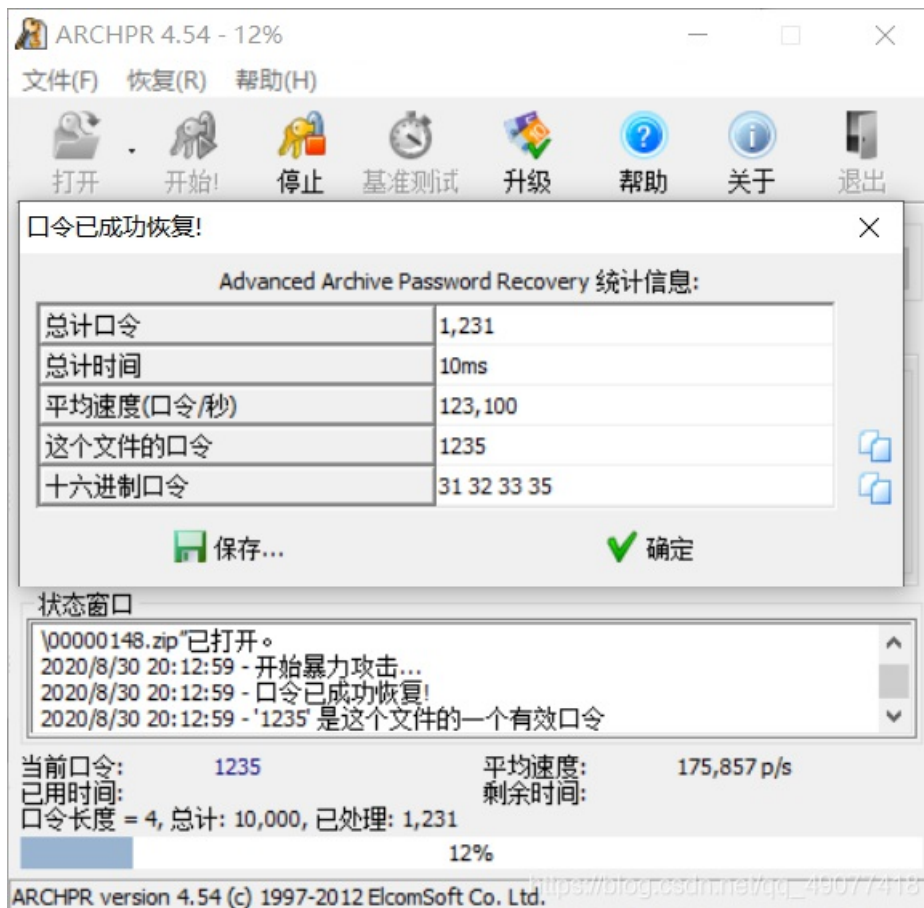
打开网页，发现没有什么东西，只好先去看看header，发现了一个flag



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



解压看看

附件 > output > zip > 00000148



得到了一半的二维码

winhex改变图片高度并解码

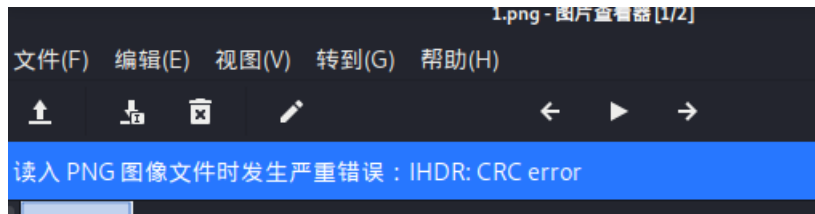


得到flag

一叶障目

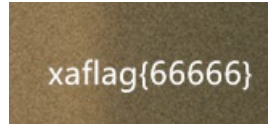
foremost查看图片，没有隐藏文件，用stegsolve也没有发现什么隐藏

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

```
48  v21 = 189;
49  v22 = 1;
50  puts("first:this string md5:46e5efe6165a5afb361217446a2dbd01");
51  scanf("%s", &v5);
52  MD5Init(&v23);
53  v3 = strlen(&v5);
54  MD5Update((int)&v23, &v5, v3);
55  MD5Final(&v23, v6);
56  v28 = 1;
57  for ( i = 0; i <= 15; ++i )
58  {
59      if ( v6[i] != *(&v7 + i) )
60      {
61          v28 = 0;
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");
76  puts("2x+3y-z=321");
77  puts("x+y+z=173");
78  printf("input: x = ");
79  scanf("%d", &v27);
80  printf("input: y = ");
81  scanf("%d", &v26);
82  printf("input : z = ");
83  scanf("%d", &v25);
```

https://blog.csdn.net/qq_49077418

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"en5oy"!

```

73  system("cls");
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 = ");
79  scanf("%d", &v27);
80  printf("input: y = ");
81  scanf("%d", &v26);
82  printf("input : z = ");
83  scanf("%d", &v25);
84  if ( 3 * v27 - v26 + v25 != 185 || 2 * v27 + 3 * v26 - v25 != 321
85  {
86      printf("Game over");
87      exit(0);
88  }
89  printf("Great last level coming...");
90  printf("pause");
91  system("cls");
92  puts("Last time: Kill it");
93  puts("x*x+x-7943722218936282=0");
94  printf("input x: ");
95  scanf("%lld", &v24);
96  if ( v24 * (v24 + 1) != 7943722218936282LL )
97  {
98      printf("Game over");
99      exit(0);
100 }
101 puts("Great This is your FLAG");

```

https://blog.csdn.net/qq_49077418

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}

```