

BugKu ——WP (MISC[一])

原创

窝窝头_233 于 2019-11-26 10:58:43 发布 157 收藏

分类专栏: [CTFwriteup](#) 文章标签: [ctf](#) [BugKuCTF](#)

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/hahaha233330/article/details/103252311>

版权



[CTFwriteup](#) 专栏收录该内容

20 篇文章 1 订阅

订阅专栏

BugKu —— MISC部分

- [0]工具

①Winhex: 图片隐写工具, 可通过搜索“ctf”“CTF”“key”“flag”等关键字得到flag。

②在线工具HtmlEncode/BASE64转换: 注意源代码里奇怪的字符串, 可以尝试解码(分清类型)。

③Binwalk: 可查看多重文件。使用说明

④VMware (kali_Linux): 虚拟机, 方便解压。

MISC

- 1、签到题

关注微信公众号: Bugku

即可获得flag

下面也有二维码

这题没什么好说的, 扫码关注公众号即可得到flag。

- 2、这是一张单纯的图片

FLAG在哪里??

把图片放到winhex，拉到最后一行可以看到如下奇怪的编码：

1D 64 06 8A 28 03 D0 A8 A2 8A 00 28 A2 8A 00 28	d Š(Đ"ćŠ (ćŠ (
A2 8A 00 FF 26 23 31 30 37 3B 26 23 31 30 31 3B	ćŠ Ÿke
26 23 31 32 31 3B 26 23 31 32 33 3B 26 23 31 32	y{
31 3B 26 23 31 31 31 3B 26 23 31 31 37 3B 26 23	1;ou&#
33 32 3B 26 23 39 37 3B 26 23 31 31 34 3B 26 23	32;ar&#
31 30 31 3B 26 23 33 32 3B 26 23 31 31 34 3B 26	101; r&
23 31 30 35 3B 26 23 31 30 33 3B 26 23 31 30 34	#105;gh
3B 26 23 31 31 36 3B 26 23 31 32 35 3B D9 D9	;t}ÙÙ

<https://blog.csdn.net/hahaha233330>

看类型是html编码，

通过在线解码器转换一下即可得到flag。

• 3、隐写

可以正常打开图片，鼠标右键查看一下图片的属性。

猜测可能是照片的宽和高信息被改了，放到 winhex 中尝试改宽高信息后发现是高被改了，将高修改为和宽一致即可得到flag。



• 5、眼见非实 (ISCCCTF)

下载得到的是一个文件的格式，放到winhex中，发现有50 4B 03 04，这是压缩文件的头，而且发现还有 .docx 格式的文件，应该压缩包有一个文档，改文件后缀为 .zip，解压得到文档-眼见非实.docx。

zip	Offset																ANSI ASCII	
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
00000000	50	4B	03	04	14	00	00	00	08	00	1A	80	87	49	5C	DC	PK	€+I\Û
00000010	E4	DA	04	28	00	00	AC	36	00	00	0D	00	00	00	D1	DB	ăú (-6	ÑÛ
00000020	BC	FB	B7	C7	CA	B5	2E	64	6F	63	78	9D	7A	05	40	15	¼û ·ÇÊµ .docx	z @
00000030	DB	F7	F5	25	25	25	25	A5	BB	A4	BB	A5	BB	BB	BB	E1	Û÷ð%§§§§»»»»»»»»á	
00000040	22	1D	92	D2	8A	74	09	48	77	4A	77	77	87	74	8A	80	" 'òŠt HwJww+tšE	



但是该文档打开后是乱码，再次放在winhex中查看，发现还是 .zip 的格式。

眼见非实.docx	Offset																ANSI ASCII	
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
00000000	50	4B	03	04	0A	00	00	00	00	00	E2	20	0F	49	00	00	PK	ã I
00000010	00	00	00	00	00	00	00	00	00	00	09	00	16	00	D1	DB		ÑÛ
00000020	BC	FB	B7	C7	CA	B5	2F	75	70	12	00	01	19	91	A4	C1	¼û ·ÇÊµ/up	'oÁ
00000030	E7	9C	BC	E8	A7	81	E9	9D	9E	E5	AE	9E	2F	50	4B	03	çœ¼èš é žâšž/PK	
00000040	04	0A	00	00	00	00	00	C1	20	0F	49	00	00	00	00	00	Á I	
00000050	00	00	00	00	00	00	00	13	00	20	00	D1	DB	BC	FB	B7		ÑÛ¼û ·
00000060	C7	CA	B5	2F	63	75	73	74	6F	6D	58	6D	6C	2F	75	70	ÇÊµ/customXml/up	
00000070	1C	00	01	7D	DA	81	AF	E7	9C	BC	E8	A7	81	E9	9D	9F	Û - çœ¼èš é ž	

那就再次



改后缀为 .zip，再次解压，得到一个文件夹。

桌面 > 眼见非实				搜索"眼见非实"
名称	修改日期	类型	大小	
📁 _rels	2019/11/23 18:25	文件夹		
📁 customXml	2019/11/23 18:25	文件夹		
📁 docProps	2019/11/23 18:25	文件夹		
📁 word	2019/11/23 18:25	文件夹		
📄 [Content_Types].xml		XML 文档		https://blog.csdn.net/hahaha233330

word->document.xml中找到了flag。

```

- <w:body>
  - <w:p w:rsidRDefault="002B3D8D" w:rsidR="002B3D8D">
    - <w:r>
      <w:t>Flag</w:t>
    </w:r>
    - <w:r>
      <w:t>在这里呦! </w:t>
    </w:r>
  </w:p>
  - <w:p w:rsidRDefault="002B3D8D" w:rsidR="002B3D8D" w:rsidRPr="002B3D8D">
    - <w:pPr>
      - <w:rPr>
        <w:rFonts w:hint="eastAsia"/>
        <w:vanish/>
      </w:rPr>
    </w:pPr>
    - <w:r w:rsidRPr="002B3D8D">
      - <w:rPr>
        <w:vanish/>
      </w:rPr>
      <w:t>flag{ . }</w:t>
    </w:r>
  </w:p>

```

<https://blog.csdn.net/hahaha233330>

- 8、猜

题目地址

flag格式key{某人名字全拼}

这题竟然真的盲猜，可以百度识图，我猜是***~

*注意flag格式：key{某人名字全拼}