

CG-CTF——WP (MISC[三])

原创

窝窝头_233 于 2020-09-24 13:03:41 发布 73 收藏

分类专栏: [CTFwriteup](#)

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/103420649>

版权



[CTFwriteup](#) 专栏收录该内容

20 篇文章 1 订阅

订阅专栏

CG-CTF——MISC部分

工具:

①Winhex: 图片隐写工具, 这个很好用。

MISC

- 1、Coding Gay

见About图片

在主页中找到About标签, 找到该图片保存到本地。



CG CTF

Challenges



Scoreboard

History

Notice

About

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



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

未完。。。

- 2、丘比龙De女神

没错 里面隐藏了一张女神的照片 flag是照片文件的md5值(小写) 记住加上flag{}

下载得到一个无后缀名的文件。



用winhex打开，发现文件头是GIF，于是把后缀名改成 `.gif`。

gif																	ANSI	ASCII
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
00000000	47	49	46	38	37	61	64	00	64	00	E7	D7	00	00	00	00	GIF	37ad d ç×
00000010	33	00	00	66	00	00	99	00	00	CC	00	00	FF	00	00	00	3	f º ì ÿ



再打开就是下面这个gif图片。

接下来没有头绪了，再次用winhex打开图片。发现这个文件其实是以 `.gif` 开头，以 `.zip` 结尾的包。

文件头尾无法对应，怀疑是修改了文件头。

0001C160	00	00	6E	76	73	68	65	6E	2E	6A	70	67	0A	00	20	00	<u>nvshen.jpg</u>	
0001C170	00	00	00	00	01	00	18	00	F0	51	B7	92	B8	1B	D1	01		øQ·', N
0001C180	B8	89	5F	22	BA	1B	D1	01	B8	89	5F	22	BA	1B	D1	01		¸ "° Ñ ,¸_ "° Ñ
0001C190	50	4B	05	06	00	00	00	00	01	00	01	00	5C	00	00	00	PK	\
0001C1A0	70	E8	00	00	00	00											pe	

改后缀名为 `.zip`。