

# 【BugKu-CTF论坛writeup(杂项)】爆照

原创

Kingyo12 于 2018-03-05 21:58:48 发布 2211 收藏

分类专栏: [BugKu-CTF论坛writeup\(杂项\)](#)

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/preserphy/article/details/79451103>

版权



[BugKu-CTF论坛writeup\(杂项\)](#) 专栏收录该内容

28 篇文章 1 订阅

订阅专栏

下载下来的图片是一个萌萌哒的二次元妹子。

先扔binwalk看一下

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
40499	0x9E33	Zip archive data, encrypted at least v2.0 to extract, compressed size: 8362, uncompressed size: 92278, name: 8
48892	0xBEFC	Zip archive data, at least v2.0 to extract, compressed size: 14906, uncompressed size: 15739, name: 88
63830	0xF956	Zip archive data, at least v2.0 to extract, compressed size: 11129, uncompressed size: 18479, name: 888
74992	0x124F0	Zip archive data, at least v2.0 to extract, compressed size: 10371, uncompressed size: 11782, name: 8888
85397	0x14D95	Zip archive data, at least v2.0 to extract, compressed size: 6945, uncompressed size: 92278, name: 88888
92377	0x168D9	Zip archive data, at least v2.0 to extract, compressed size: 6824, uncompressed size: 92278, name: 888888
99237	0x183A5	Zip archive data, at least v2.0 to extract, compressed size: 7076, uncompressed size: 92278, name: 8888888
106350	0x19F6E	Zip archive data, at least v2.0 to extract, compressed size: 8219, uncompressed size: 92278, name: 88888888
168452	0x29204	End of Zip archive

要被吓死了.....

foremost提取得到了以下这一堆东西(出题人也是很无聊啊)

- 8
- 88
- 888
- 8888
- 88888
- 888888
- 8888888
- 88888888
- 888888888

 愉快的排序吧哈哈.gif

把这8个没有后缀的文件逐个binwalk

```

root@kali:~/桌面# binwalk 8
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         PC bitmap, Windows 3.x format,, 303 x 300 x 8

root@kali:~/桌面# binwalk 88
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01
30          0x1E         TIFF image data, big-endian, offset of first image
directory: 8

root@kali:~/桌面# binwalk 888
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01
30          0x1E         TIFF image data, big-endian, offset of first image
directory: 8
4396        0x112C      Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"/
></x:xmpmeta>

root@kali:~/桌面# binwalk 8888
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01
30          0x1E         TIFF image data, big-endian, offset of first image
directory: 8
10976       0x2AE0      Zip archive data, at least v2.0 to extract, compre
ssed size: 644, uncompressed size: 1202, name: 1509126368.png
11760       0x2DF0      End of Zip archive

```

```

root@kali:~/桌面# binwalk 88888
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         PC bitmap, Windows 3.x format,, 303 x 300 x 8

root@kali:~/桌面# binwalk 888888
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         PC bitmap, Windows 3.x format,, 303 x 300 x 8

root@kali:~/桌面# binwalk 8888888
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         PC bitmap, Windows 3.x format,, 303 x 300 x 8

root@kali:~/桌面# binwalk 88888888
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         PC bitmap, Windows 3.x format,, 303 x 300 x 8

```

发现88、888、8888是被修改过的图片。

用HxD看了一下，在8的最后发现了【flag】字符串——

```

32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 2222222222222222
32 66 6C 61 67 00

```

又可以清楚的看到88图片自带二维码，扫描得到 bilibili

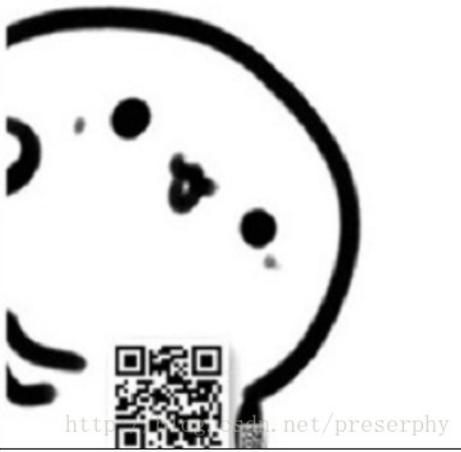


图888也被修改过，HxD没有看到异常，修改后缀然后打开属性看到了一串BASE64



解码得 silisili

图8888里面有个压缩包，改后缀解压得到一张二维码



在线扫描可以得到 panama

最后根据题目提示的 `flag格式 flag{xxx_xxx_xxx}` 进行组合，得到 `flag{bilibili_silisili_panama}`