

CTF-Misc-[BJDCTF2020]鸡你太美

原创

归子莫 于 2020-05-14 12:29:03 发布 1589 收藏 1

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_45163122/article/details/106117456

版权

CTF-Misc-[BJDCTF2020]鸡你太美

博客说明

文章所涉及的资料来自互联网整理和个人总结，意在于个人学习和经验汇总，如有什么地方侵权，请联系本人删除，谢谢！本文仅用于学习与交流，不得用于非法用途！

CTP平台

网址

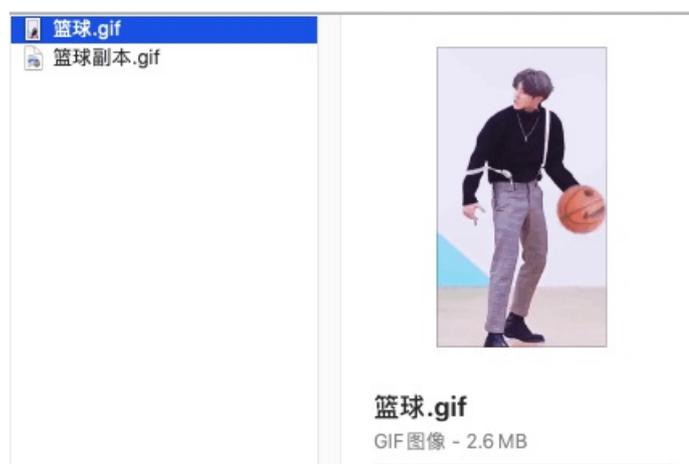
<https://buuoj.cn/challenges>

题目

Misc类，[BJDCTF2020]鸡你太美

思路

这类题目首先把文件下载下来，是一个gif



第一张能够打开，第二张打不开

使用 bless

我是在linux下，当然你可以在windows下使用winhex

```

篮球.gif x  篮球副本.gif x
00000000 47 49 46 38 39 61 B4 00 40 01 F6 31 00 1C 18 25 1D 1A GIF89a...@...1...%..
00000012 2B 1E 1F 36 21 1C 2C 24 1E 34 28 23 39 36 28 39 27 26 +..6!.,$.4(#96(9'&
00000024 43 3C 2D 43 45 37 4D 51 43 56 56 4F 67 6A 58 6D 78 64 C<-CE7MQCVVOgjXmxd
00000036 78 77 6D 89 8A 74 89 88 7A 97 8E 77 8B 96 84 9B 8D 83 xwm..t..z..w.....
00000048 A4 96 8A A8 9C 95 B4 9C 91 AA A5 9B B6 A9 95 AA B2 A9 .....
0000005a BA D5 AF B7 B7 AF C6 CB BE CE CE C9 CA D3 CB CE D7 CD .....
0000006c D4 D7 D0 D2 DB D2 D4 DD D5 DA C8 C8 DC E1 D6 DA E3 D8 .....
0000007e DE E4 C9 D1 D9 D4 E6 DA DD F0 E5 DC E0 E5 DC E9 E6 E6 .....
00000090 F4 E8 E7 F5 E8 E8 F5 EB EB F9 F0 E9 F9 F4 ED F8 17 12 .....
000000a2 1E 1A 16 21 BB C2 D5 A4 D9 F3 A9 D7 F1 B7 D7 F0 D7 E4 ....!.....
000000b4 FC 3F 3C 64 93 A8 C5 AA DD F4 9E D9 F0 25 18 25 51 31 .?<d.....%.%Q1
000000c6 3E 53 37 4E 62 49 58 7C 65 67 85 6C 6C 84 6A 77 B0 7E >S7NbIX|eg.ll.jw.~
000000d8 86 AD 8B 98 E3 BC CA CD 9F AC 8A 5A 56 8B 71 78 B2 74 .....ZV.qx.t
000000ea 70 CA 92 8E D8 A3 9D 7E 49 3F A8 5C 4E C8 79 69 B7 69 .....~T?.\N.vi.i

```

```

篮球.gif x  篮球副本.gif x
00000000 39 61 68 01 80 02 F7 00 31 00 FF 00 04 04 0A 0B 09 14 9ah.....1.....
00000012 0F 0C 1A 15 21 2C 15 2C 3A 16 10 1B 16 11 21 17 16 21 .....!.,,:.....!..!
00000024 19 17 28 1B 17 23 1B 17 28 1B 1C 2D 1C 19 2A 1C 1A 2A ..(..#..(..-..*...*
00000036 1F 19 2B 20 16 24 20 1D 29 20 1D 2D 21 1D 31 23 20 35 ..+.$.).-!.1# 5
00000048 24 22 37 24 28 3C 28 20 31 28 23 3B 29 18 22 29 1D 2C $"7$(<( 1(#;).").,
0000005a 2A 27 3E 2B 29 34 2D 2C 3F 34 1F 2B 34 26 39 34 31 3A *'+)4-,?4.+4&941:
0000006c 35 2D 43 35 36 50 37 36 44 3C 5B 6A 3E 2B 38 3F 32 46 5-C56P76D<[j>+8?2F
0000007e 40 3A 51 40 3D 47 42 4A 53 45 3E 53 46 2C 37 49 33 46 @:Q@=GBJSE>SF,7I3F
00000090 4C 56 69 4D 4B 57 4E 3C 47 4F 3E 50 50 42 59 52 4F 63 LViMKWN<GO>PPBYROc
000000a2 53 2F 36 54 4D 59 58 52 64 5F 48 59 61 79 86 62 50 61 S/6TMYXRd_HYay.bPa
000000b4 64 57 6D 64 59 62 64 5A 68 67 61 6E 68 41 42 69 61 74 dWmdYbdZhganhABiat
000000c6 6B 65 7A 73 58 5E 73 74 7F 74 80 96 75 5D 6B 75 62 68 kezszX^st.t.u]kubh
000000d8 76 67 79 76 6B 80 77 62 70 77 6C 86 77 75 83 7A 68 6E vgyvk.wbpwl.wu.zhn
000000ea 7B 76 87 7B 8F A0 7E 9E B2 80 76 85 80 77 8E 81 62 66 {v.{...~...v..w..bf
000000cf 82 6D 80 82 6E 86 82 7A 95 83 6B 72 83 6C 79 84 69 6B .m..n..z..kr.ly.ik
0000010e 84 7A 8E 84 7A 95 85 73 7F 85 74 87 86 58 58 86 7C 96 .z..z..s..t..XX.|.

```

对比两张gif，找到了问题所在，第二张没有gif文件头，所以打不开

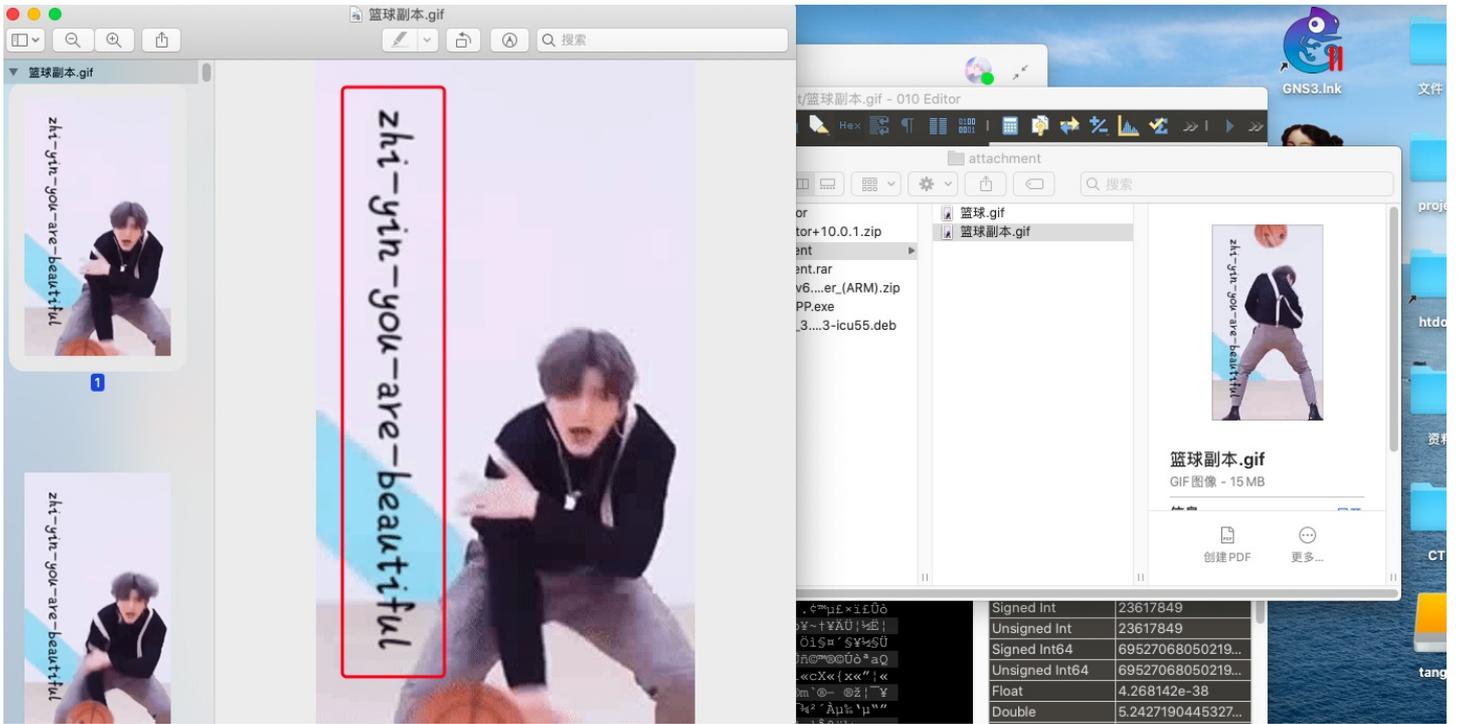
GIF文件头 47 49 46 38，直接给它加上，点击开始的数字直接编辑就好，然后保存

```

篮球.gif x  篮球副本.gif* x
00000000 47 49 46 38 39 61 B4 00 40 01 F6 31 00 1C 18 25 1D 1A GIF89ah.....1.....
00000012 0A 0B 09 14 0F 0C 1A 15 21 2C 15 2C 3A 16 10 1B 16 11 .....!.,,:.....!..!
00000024 21 17 16 21 19 17 28 1B 17 23 1B 17 28 1B 1C 2D 1C 19 !...!(..#..(..-..
00000036 2A 1C 1A 2A 1F 19 2B 20 16 24 20 1D 29 20 1D 2D 21 1D *..*..+.$.).-!.
00000048 31 23 20 35 24 22 37 24 28 3C 28 20 31 28 23 3B 29 18 1# 5$"7$(<( 1(#;).").,
0000005a 22 29 1D 2C 2A 27 3E 2B 29 34 2D 2C 3F 34 1F 2B 34 26 ")..,*'+)4-,?4.+4&
0000006c 39 34 31 3A 35 2D 43 35 36 50 37 36 44 3C 5B 6A 3E 2B 941:5-C56P76D<[j>+
0000007e 38 3F 32 46 40 3A 51 40 3D 47 42 4A 53 45 3E 53 46 2C 8?2F@:Q@=GBJSE>SF,
00000090 37 49 33 46 4C 56 69 4D 4B 57 4E 3C 47 4F 3E 50 50 42 7I3FLViMKWN<GO>PPB
000000a2 59 52 4F 63 53 2F 36 54 4D 59 58 52 64 5F 48 59 61 79 YROcS/6TMYXRd_HYay
000000b4 86 62 50 61 64 57 6D 64 59 62 64 5A 68 67 61 6E 68 41 .bPadWmdYbdZhganhA
000000c6 42 69 61 74 6B 65 7A 73 58 5E 73 74 7F 74 80 96 75 5D BiatkezsX^st.t.u]
000000d8 6B 75 62 68 76 67 79 76 6B 80 77 62 70 77 6C 86 77 75 kubhvgyvk.wbpwl.wu
000000ea 83 7A 68 6E 7B 76 87 7B 8F A0 7E 9E B2 80 76 85 80 77 .zhn{v.{...~...v..w
000000cf 8E 81 62 66 82 6D 80 82 6E 86 82 7A 95 83 6B 72 83 6C ..bf.m..n..z..kr.l
0000010e 79 84 69 6B 84 7A 8E 84 7A 95 85 73 7F 85 74 87 86 58 y.ik.z..z..s..t..XX

```

然后就可以打开了，发现flag（使用bless发现不能保存，然后使用010）



感谢

BUUCTF
以及勤劳的自己