

# CTFjpg图片隐写之zlib压缩数据包的提取

原创

胖虎很忙 于 2019-11-16 23:17:11 发布 11169 收藏 17

分类专栏: [ctf ctf图片隐写](#) 文章标签: [CTFjpg图片隐写之zlib压缩数据包的提取](#)

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/weixin\\_43877387/article/details/103102842](https://blog.csdn.net/weixin_43877387/article/details/103102842)

版权



[ctf](#) 同时被 2 个专栏收录

10 篇文章 0 订阅

订阅专栏



[ctf图片隐写](#)

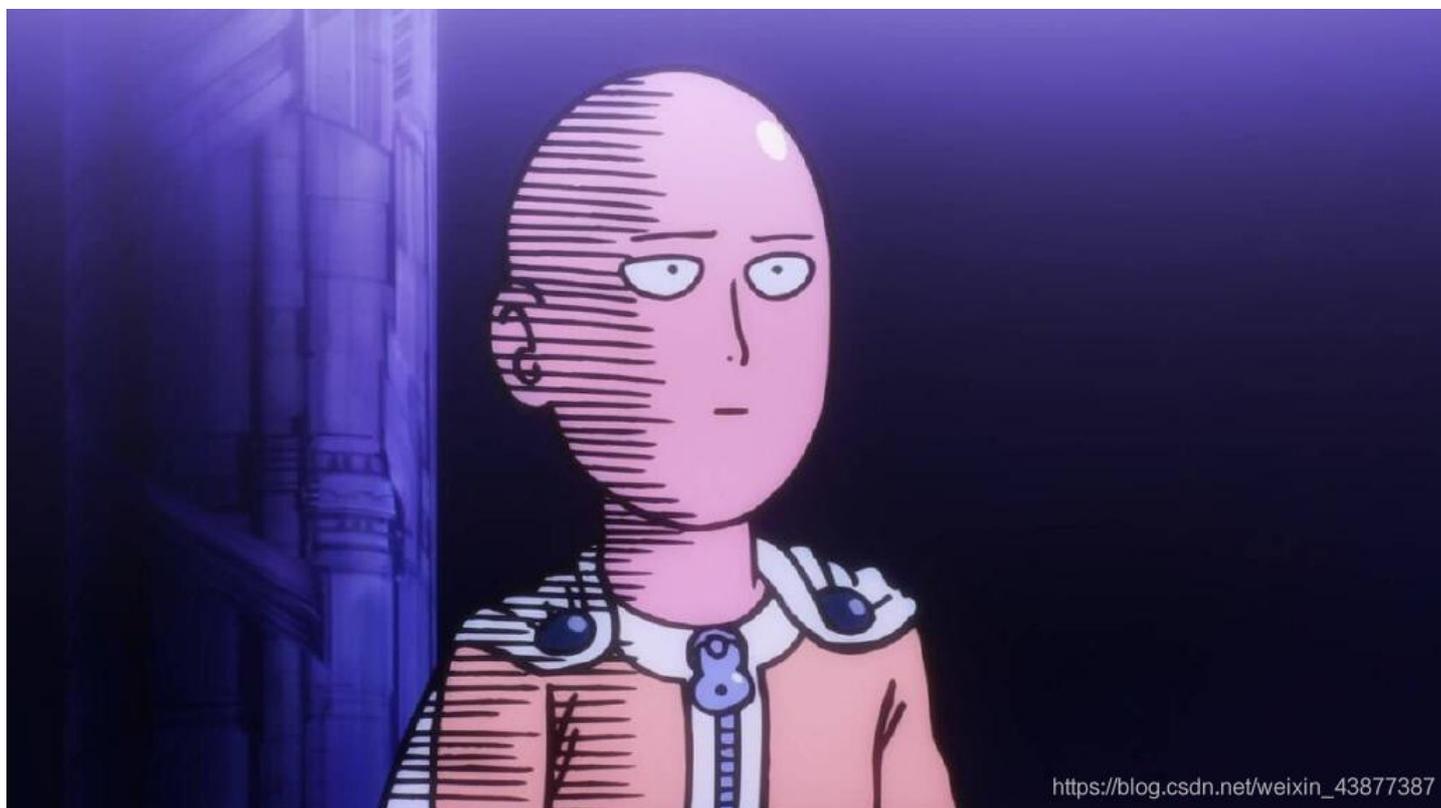
4 篇文章 0 订阅

订阅专栏

## CTFjpg图片隐写之zlib压缩数据包的提取

今天萌新很开心有幸给萌萌萌萌新们讲解, 大周六的按说该睡懒觉, 想到了CTF毅然选择了早起, 就像毒品一样, 哈哈。进入正题。

看到群里有人发了一张隐写图片, 就简单做了一下, 没错就是这张, 光头。。。头强吧, 哈哈。



拿到隐写图片后对他进行进本操作:

- (1) 右击选择属性, 发现没有重要信息;
- (2) 放到stegsolve里面, 试了试各种通道, 没有收获;



```

00000100 9A F6 00 50 D3 1E 00 6A DA 03 40 4D 7B 00 A8 69 89 80.P0..jU.@M{."i..5
00000110 0F 00 35 ED 01 A0 A6 3D 00 D4 B4 07 80 9A F6 00 ..5i. |=.ô´.eššö.
00000120 50 D3 1E 00 6A DA 03 40 4D 7B 00 A8 69 0F 00 35 P0..jU.@M{."i..5
00000130 ED 01 A0 A6 3D 00 D4 B4 07 80 9A F6 00 50 D3 1E i. |=.ô´.eššö.P0.
00000140 00 6A DA 03 40 4D 7B 00 A8 69 0F 00 35 ED 01 A0 .jU.@M{."i..5i.
00000150 A6 3D 00 D4 B4 07 80 9A F6 00 50 D3 1E 00 6A DA |=.ô´.eššö.P0..jU

```

偏移: 0 块: 0-1 长度: 2 [https://blog.csdn.net/weixin\\_43877387](https://blog.csdn.net/weixin_43877387) 覆盖

查下资料png图片开头: 89 50 4E 47 添加89 50 后保存成.png 格式

HxD - [C:\Users\DZY\Desktop\\*.png]

文件(F) 编辑(E) 搜索(S) 查看(V) 分析(A) 附加(X) 窗口(W) 关于(A)

16 ANSI 十六进制

3.jpg 2.zlib .png

```

Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 PNG.....IHDR
00000010 00 00 02 29 00 00 01 86 08 02 00 00 00 31 53 86 ...)...t.....lSt
00000020 EF 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 i....sRGB.@f.é...
00000030 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 ..gAMA..t..üa...
00000040 00 09 70 48 59 73 00 00 0E C3 00 00 0E C3 01 C7 ..pHYs...Ä...Ä.ç
00000050 6F A8 64 00 00 09 15 49 44 41 54 78 5E ED D9 5B o`d...IDATx^iU[
00000060 6A 1B 67 18 80 E1 2E 24 97 59 89 EF B2 93 DC 64 j.g.éá.é-Y%i^"Üd
00000070 2B BE E8 56 02 DE 4B BB 87 42 C0 50 08 04 52 CD +%èV.ßK»+BÀP..RÍ
00000080 41 D2 8C 4E B6 8A E7 AD 43 9F 87 21 58 D2 F8 9F AÖENŦšç.CY#!XÖøY
00000090 C3 C5 F7 7A 94 DF 7E 02 40 4B 7B 00 A8 69 0F 00 ÄÄ=z"B~.@K{."i..
000000A0 35 ED 01 A0 A6 3D 00 D4 B4 07 80 9A F6 00 50 D3 5i. |=.ô´.eššö.P0
000000B0 1E 00 6A DA 03 40 4D 7B 00 A8 69 0F 00 35 ED 01 ..jU.@M{."i..5i.
000000C0 A0 A6 3D 00 D4 B4 07 80 9A F6 00 50 D3 1E 00 6A |=.ô´.eššö.P0..j
000000D0 DA 03 40 4D 7B 00 A8 69 0F 00 35 ED 01 A0 A6 3D Ű.@M{."i..5i. |=
000000E0 00 D4 B4 07 80 9A F6 00 50 D3 1E 00 6A DA 03 40 .ô´.eššö.P0..jU.@
000000F0 4D 7B 00 A8 69 0F 00 35 ED 01 A0 A6 3D 00 D4 B4 M{."i..5i. |=.ô´
00000100 07 80 9A F6 00 50 D3 1E 00 6A DA 03 40 4D 7B 00 .eššö.P0..jU.@M{
00000110 A8 69 0F 00 35 ED 01 A0 A6 3D 00 D4 B4 07 80 9A "i..5i. |=.ô´.eš
00000120 F6 00 50 D3 1E 00 6A DA 03 40 4D 7B 00 A8 69 0F ö.P0..jU.@M{."i.
00000130 00 35 ED 01 A0 A6 3D 00 D4 B4 07 80 9A F6 00 50 .5i. |=.ô´.eššö.P
00000140 D3 1E 00 6A DA 03 40 4D 7B 00 A8 69 0F 00 35 ED Ö..jU.@M{."i..5i
00000150 01 A0 A6 3D 00 D4 B4 07 80 9A F6 00 50 D3 1E 00 . |=.ô´.eššö.P0..

```

偏移: 0 块: 0-1 长度: 2 [https://blog.csdn.net/weixin\\_43877387](https://blog.csdn.net/weixin_43877387) 覆盖

打开后得到 flag

flag{You\_@re\_great}

[https://blog.csdn.net/weixin\\_43877387](https://blog.csdn.net/weixin_43877387)

我遇到的问题: 第一次遇到Zlib压缩数据包, 不知道如何提取, 然后就百度了许久, 最后也没发现啥, 只好放到Hxd里面分析, 这个办法比较笨 但很实用, 很适合我们这些小白们, 希望大佬们勿喷哟。打了一天ctf。是时候喝茶去了, 溜了溜了。。。。

