

bugkuCTF平台逆向题第四道逆向入门题解

原创

iqiqiya 于 2017-12-28 14:40:15 发布 5071 收藏 1

分类专栏: [-----bugkuCTF 我的CTF进阶之路](#) 文章标签: [CTF bugku 逆向入门 reverse writeup](#)

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/xiangshangbashaonian/article/details/78921926>

版权



[-----bugkuCTF 同时被 2 个专栏收录](#)

9 篇文章 0 订阅

订阅专栏

[我的CTF进阶之路](#)

108 篇文章 18 订阅

订阅专栏

题目链接:

<http://123.206.31.85/files/b2be7f63b064e490ca13a1aa2f594610/admin.exe>

tips:

逆向入门
110

admin.exe

Key

SUBMIT

双击无法运行 提示版本不对 (win10)

查壳显示不是有效的PE文件

入口点: EP 段: >

文件偏移: 首字节: >

连接器版本: 子系统: >

PEsniffer: >

PEiDDSCAN: 不是有效的PE文件 >

总在最前(S)

用WinHex打开显示

```

on View Tools Specialist Options Window Help
admin.exe
Offset 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
00000000 64 61 74 61 3A 69 6D 61 67 65 2F 70 6E 67 3B 62 data:image/png;base64,iVBORw0KGg
00000016 61 73 65 36 34 2C 69 56 42 4F 52 77 30 4B 47 67 ase64,ivBORw0KGg
00000032 6F 41 41 41 41 4E 53 55 68 45 55 67 41 41 41 5A oAAAANSUHEUgAAAZ
00000048 41 41 41 41 47 51 43 41 59 41 41 41 43 41 76 7A AAAAGQCAyAAACAvz
00000064 62 4D 41 41 41 67 41 45 6C 45 51 56 52 34 58 75 bMAAAgAE1EQVR4Xu
00000080 32 39 43 64 68 75 79 56 58 58 57 34 64 41 6D 42 29CdhuyVXXW4dAmB
00000096 49 67 68 71 45 44 43 49 67 35 61 57 51 6D 41 79 IghqEDCIg5aWcmAy
00000112 68 54 30 6F 43 67 6B 6A 36 43 45 34 48 6A 64 54 hT0ocGkj6CE4HjdT
00000128 37 70 67 48 4C 56 70 47 56 77 67 73 50 31 34 6E 7pgHLVpGVwgsPl4n
00000144 42 44 69 78 4D 47 47 6F 66 48 78 79 59 52 52 7A BDixMGGoFHxyYRRz
00000160 6F 64 46 53 37 59 36 53 42 63 30 53 53 41 45 43 odFS7Y6Sbc0SSAEC
00000176 41 35 44 44 4B 6D 51 63 4B 55 4D 4B 50 6E 50 72 A5DDKmCqKUMKpPr
00000192 2F 76 50 64 57 39 7A 39 74 37 37 2F 72 56 33 75 /vPdW9z9t77/rV3u
00000208 75 74 64 37 2F 66 71 58 71 65 37 2B 6E 6B 76 4C utd7/fqXqe7+nkvL
00000224 57 72 56 76 31 72 31 66 72 58 73 46 62 56 68 65 WrVv1r1frXsFbVhe
00000240 76 58 72 31 39 50 50 58 55 45 4F 67 49 64 67 59 vXr19PPXUEGIdgY
00000256 35 41 52 36 41 53 67 51 75 64 51 43 6F 52 36 39 5AR6ASgQudQCOR69
00000272 6B 37 41 68 32 42 6A 6B 42 48 34 41 79 42 54 69 k7Ah2BjkBH4AyBTi
00000288 42 64 45 54 6F 43 48 59 47 4F 51 45 64 67 45 51 BdEToCHYGOQEdgEQ
00000304 4B 64 51 42 62 42 31 6A 2F 71 43 48 51 45 4F 67 KdQBb1j/qCHQEOg
00000320 49 64 67 55 34 67 58 51 63 36 41 68 32 42 6A 6B IdgU4gXQc6Ah2Bjk
00000336 42 48 59 42 45 43 6E 55 41 57 77 64 59 2F 36 67 BHYBECnUAWwdY/6g
00000352 68 30 42 44 6F 43 48 59 46 4F 49 46 30 48 4F 67 h0BDoCHYFOIF0HOG
00000368 49 64 67 59 35 41 52 32 41 52 41 70 31 41 46 73 IdgY5AR2ARAp1AFs
00000384 48 57 50 2B 6F 49 64 41 51 36 41 68 32 42 54 69 HWP+oIdAQ6Ah2BTi
00000400 42 64 42 7A 6F 43 48 59 47 4F 51 45 64 67 45 51 BdBzoCHYGOQEdgEQ
00000416 4A 56 42 50 4C 6D 4E 37 38 35 50 66 44 41 41 2B JVBPImN785PfdAA+
00000432 6B 4E 62 33 68 44 2B 6F 6D 66 2B 49 6D 62 4B 69 kNb3hD+cmf+ImbKi
00000448 51 65 38 63 4B 46 43 34 75 45 32 50 2F 49 6C 42 Qe8cKFC4uE2P/1lB
00000464 57 56 5A 30 72 67 32 32 2B 2F 50 54 33 74 61 55 WV20rg22+/PT3taU
00000480 39 4C 7A 33 33 75 63 78 65 31 36 54 57 76 65 55 9Lz33ucxe16TWveU
00000496 33 4B 66 30 73 4B 4F 48 54 37 44 4F 61 52 47 44 3Kf0sKOHT7DcaRGD

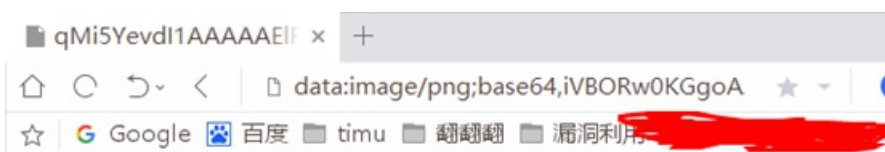
```

一看发现是图片的base64编码

可以这样

将文档保存为.html文件 用浏览器打开即可

(也可以直接复制到浏览器地址栏 我是这样做的)



也可以这样

在线base64转图片

<http://www.vgot.net/test/image2base64.php>

扫码得到flag

