

endianness-v2

By: Kyou

Jujur aku masih awam banget di Forensics, jadi kalau ada kesalahan bisa dikoreksi ya bang @Achideon. Anyway here's the chall:

endianness-v2

Medium

Forensics

picoCTF 2024

browser_webshell_solvable

AUTHOR: JUNIAS BONOU

Description

Here's a file that was recovered from a 32-bits system that organized the bytes a weird way. We're not even sure what type of file it is.
Download it [here](#) and see what you can get out of it

4,334 users solved

95% Liked

picoCTF{FLAG}

Submit Flag

Dari challenge tersebut, kita diberi sebuah binary file

Pertama-tama yang harus kita lakukan adalah mengidentifikasi file tersebut dengan menggunakan 'exiftool'

```
ordinarycat@ordinarycat-VirtualBox:~/CTF/Forensics/endianness-v2$ exiftool challengefile
ExifTool Version Number      : 12.76
File Name                    : challengefile
Directory                    : .
File Size                    : 3.4 kB
File Modification Date/Time   : 2025:07:17 20:20:53+07:00
File Access Date/Time        : 2025:07:17 20:20:53+07:00
File Inode Change Date/Time   : 2025:07:17 20:21:19+07:00
File Permissions              : -rw-rw-r--
Warning                      : Processing JPEG-like data after unknown 1-byte header
```

Nah bisa dilihat pada gambar, cluenya itu ada di message warning pada gambar yang menyatakan bahwa byte header pertama dari gambar itu mirip dengan format JPG. Selanjutnya kita dapat mengidentifikasi hexdump dari file tersebut dengan menggunakan tool 'ghex'

```
ordinarycat@ordinarycat-VirtualBox:~/CTF/Forensics/endianness-v2$ ghex challengefile
```

```

challengefile
/home/ordinarycat/CTF/Forensics/endianness-v2

00000000 E0 FF D8 FF 46 4A 10 00 01 00 46 49 01 00 00 01 ...FJ....FI....
00000010 00 00 01 00 43 00 DB FF 06 06 08 00 08 05 06 07 ....C.....
00000020 09 07 07 07 0C 0A 08 09 0B 0C 0D 14 12 19 0C 0B .....
00000030 1D 14 0F 13 1D 1E 1F 1A 20 1C 1C 1A 20 27 2E 24 ..... '$
00000040 1C 23 2C 22 29 37 28 1C 34 31 30 2C 27 1F 34 34 .#,")7(.410,'.44
00000050 32 38 3D 39 34 33 2E 3C 00 DB FF 32 09 09 01 43 28=943.<...2...C
00000060 0C 0B 0C 09 18 0D 0D 18 21 1C 21 32 32 32 32 32 .....!..!22222
00000070 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 2222222222222222
00000080 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 2222222222222222
00000090 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 222222222222..22
000000A0 00 08 11 00 03 2C 01 96 02 00 22 01 11 03 01 11 .....,".....
000000B0 00 C4 FF 01 01 00 00 1F 01 01 01 05 00 01 01 01 .....
000000C0 00 00 00 00 01 00 00 00 05 04 03 02 09 08 07 06 .....
000000D0 C4 FF 0B 0A 00 10 B5 00 03 03 01 02 05 03 04 02 .....
000000E0 00 04 04 05 01 7D 01 00 04 00 03 02 21 12 05 11 .....}.....!...
000000F0 13 06 41 31 22 07 61 51 81 32 14 71 23 08 A1 91 ..A1".aQ.2.q#...
00000100 15 C1 B1 42 24 F0 D1 52 82 72 62 33 17 16 0A 09 ...B$..R.rb3....
00000110 25 1A 19 18 29 28 27 26 36 35 34 2A 3A 39 38 37 %...)(('&654*:987
00000120 46 45 44 43 4A 49 48 47 56 55 54 53 5A 59 58 57 FEDCJIHGVUTSZYXW
00000130 66 65 64 63 6A 69 68 67 76 75 74 73 7A 79 78 77 fedcjihgvutszyxw
00000140 86 85 84 83 8A 89 88 87 95 94 93 92 99 98 97 96 .....
00000150 A4 A3 A2 9A A8 A7 A6 A5 B3 B2 AA A9 B7 B6 B5 B4 .....
00000160 C2 BA B9 B8 C6 C5 C4 C3 CA C9 C8 C7 D5 D4 D3 D2 .....
00000170 D9 D8 D7 D6 E3 E2 E1 DA E7 E6 E5 E4 F1 EA E9 E8 .....
00000180 F5 F4 F3 F2 F9 F8 F7 F6 00 C4 FF FA 03 00 01 1F .....
00000190 01 01 01 01 01 01 01 01 00 00 00 01 01 00 00 00 .....
000001A0 05 04 03 02 00 00 07 06 C4 FF 0B 0A 00 11 B5 00 .....

```

Offset: 0x3; 0x4 bytes from 0x0 to 0x3 selected

Nah 4 byte pertama dari filenya itu sendiri sebenarnya cuma 4 byte header dari format file JPG yang di-reverse.

JPG Header : FF D8 FF E0

Tugas kita sekarang adalah ngereverse 4 byte tersebut kembali ke bentuk semulanya.

```

ordinarycat@ordinarycat-VirtualBox:~/CTF/Forensics/endianness-v2$ hexdump -v -e
'1/4 "%08x" -e '"\n"' challengefile | xxd -r -p > reversed

```

Singkatnya, cara kerja dari command itu adalah untuk membaca file biner terus membalik urutan byte tiap 4 byte (endianness reversal), lalu nyimpen hasilnya ke output file.

```
reversed
/home/ordinarycat/CTF/Forensics/endianness-v2

00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01 ...JFIF.....
00000010 00 01 00 00 FF DB 00 43 00 08 06 06 07 06 05 08 .....C.....
00000020 07 07 07 09 09 08 0A 0C 14 0D 0C 0B 0B 0C 19 12 .....
00000030 13 0F 14 1D 1A 1F 1E 1D 1A 1C 1C 20 24 2E 27 20 ..... $. '
00000040 22 2C 23 1C 1C 28 37 29 2C 30 31 34 34 34 1F 27 ",#..(7),01444.'
00000050 39 3D 38 32 3C 2E 33 34 32 FF DB 00 43 01 09 09 9=82<.342...C...
00000060 09 0C 0B 0C 18 0D 0D 18 32 21 1C 21 32 32 32 32 .....2!..!2222
00000070 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 2222222222222222
00000080 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 2222222222222222
00000090 32 32 32 32 32 32 32 32 32 32 32 32 32 32 FF C0 222222222222222..
000000A0 00 11 08 00 96 01 2C 03 01 22 00 02 11 01 03 11 .....,".....
000000B0 01 FF C4 00 1F 00 00 01 05 01 01 01 01 01 01 00 .....
000000C0 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 .....
000000D0 0A 0B FF C4 00 B5 10 00 02 01 03 03 02 04 03 05 .....
000000E0 05 04 04 00 00 01 7D 01 02 03 00 04 11 05 12 21 .....}.....!
000000F0 31 41 06 13 51 61 07 22 71 14 32 81 91 A1 08 23 1A..Qa."q.2....#
00000100 42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 17 B...R..$3br.....
00000110 18 19 1A 25 26 27 28 29 2A 34 35 36 37 38 39 3A ...%&'()*456789:
00000120 43 44 45 46 47 48 49 4A 53 54 55 56 57 58 59 5A CDEFGHIJSTUVWXYZ
00000130 63 64 65 66 67 68 69 6A 73 74 75 76 77 78 79 7A cdefghijstuvwxyz
00000140 83 84 85 86 87 88 89 8A 92 93 94 95 96 97 98 99 .....
00000150 9A A2 A3 A4 A5 A6 A7 A8 A9 AA B2 B3 B4 B5 B6 B7 .....
00000160 B8 B9 BA C2 C3 C4 C5 C6 C7 C8 C9 CA D2 D3 D4 D5 .....
00000170 D6 D7 D8 D9 DA E1 E2 E3 E4 E5 E6 E7 E8 E9 EA F1 .....
00000180 F2 F3 F4 F5 F6 F7 F8 F9 FA FF C4 00 1F 01 00 03 .....
00000190 01 01 01 01 01 01 01 01 01 00 00 00 00 00 01 .....
000001A0 02 03 04 05 06 07 08 09 0A 0B FF C4 00 B5 11 00 .....

Offset: 0x3; 0x4 bytes from 0x0 to 0x3 selected A[ ^
```

picoCTF{cert!f1Ed_iNd!4n_s0rrY_3nDian_004850bf}

Yey dapet flagnya

flag: picoCTF{cert!f1Ed_iNd!4n_s0rrY_3nDian_004850bf}



"yayayayayayayayayayayaya ctf india jir"
~Kyou