CsecIITB CTF 2020

Category: Forensics

Challenge: Magic

Points: 500

Description:

> I wanted to show you guys my magic. But it keeps saying your file format is not supported. At this point i wonder what formats really are magic.png

Idea:

If you try to open the image in Ubuntu it will not open because the image is corrupted. So we will resolve the issue and try to recover the image. After that the flag will be in the image or will be encoded in it.

I use two tools here `pngcheck` and `PCRT`.

First lets see what pngcheck says about the image. It will tell us where the image is corrupted. For that just run pngcheck on the image

```
$ pngcheck -pv magic.png
  File: magic.png (67168 bytes)
  File is CORRUPTED.  It seems to have suffered EOL conversion.
  It was probably transmitted in text mode.
  ERRORS DETECTED in magic.png
```

Without doing any more efforts run `PCRT` on the image. It is a python2 based tool.

```
$ python2 PCRT.py -i magic.png -o output.png
     ____    ____ ____ _____
    |  _ \ / ___|  _ \_   _|
    | |_) | |   | |_) || |
    |  __/| |___|  _ < | |
    |_|    \____|_| \_\|_|

    PNG Check & Repair Tool

  Project address: https://github.com/sherlly/PCRT
  Author: sherlly
  Version: 1.1

  [Detected] Wrong PNG header!
  File header: 2E504E470000000D
  Correct header: 89504E470D0A1A0A
  [Notice] Auto fixing? (y or n) [default:y] y
```

```
    [Finished] Now header:89504E470D0A1A0A
    [Finished] Correct IHDR CRC (offset: 0x19): 2C09475A
    [Finished] IHDR chunk check complete (offset: 0x4)
    [Finished] Correct IDAT chunk data length (offset: 0x4F length: FFA5)
    [Finished] Correct IDAT CRC (offset: 0xFFFC): D384964C
    [Detected] Error IDAT chunk data length! (offset: 0x10000)
    chunk length:648
    actual length:654
    [Notice] Try fixing it? (y or n) [default:y] y
    [Warning] Only fix because of DOS->Unix conversion
    [Failed] Fixing failed, auto discard this operation...
    [Finished] Correct IDAT chunk data length (offset: 0x10660 length: 648)
    [Finished] Correct IDAT CRC (offset: 0x10CB0): 3FB84667
    [Finished] IDAT chunk check complete (offset: 0x4F)
    [Finished] Correct IEND chunk
    [Finished] IEND chunk check complete
    [Finished] PNG check complete
    [Notice] Show the repaired image? (y or n) [default:n] y
```

You will then see the image with the flag.

Flag :

> CsecIITB{Do_You_b3li3v3_in_m4gic?}