

Mark Seliternikov

picoCTF - c0rrupt [250 points]



לאתגר הזה מקבלים קובץ. לפי התיאור של האתגר הקובץ הוא שבור.

לאחר פתיחה של הקובץ ב-Hex Editor, ניתן לראות קובץ לא ברור. לפחות לא לפי ה-Header.

כשעברתי על הקובץ, חשבתי לעצמי שאולי לפי ה-Footer אוכל לזהות את הקובץ.

לאחר מכן ראיתי ב-Footer שהוא מסתיים ב-IEND.B.

לאחר חיפוש באינטרנט, גיליתי שקובץ PNG מסתיים בסיומת כזו.

לאחר שגיליתי זאת התחלתי לתקן את הקובץ בעזרת האתר <http://www.libpng.org/pub/png/spec/1.2/PNG-Contents.html>

בין היתר נעזרתי גם בתמונות ובויקיפדיה.

היו 3 דברים שהייתי צריך לתקן ב-Header כדי שהקובץ יהיה PNG רשמי.

ה-8 הבייטים הראשונים אשר מייצגים קובץ PNG.

89 50 4E 47 0D 0A 1A 0A
הבייטים אשר מייצגים IHDR (שהיו קודם C"DR)

49 48 44 52
והבייטים אשר מייצגים IDAT (שהיו קודם DET).

49 44 41 54

למרות שבשלב זה כבר פתרתי את האתגר וכל מה שהיה עליי לעשות זה לפתוח את הקובץ ולראות איזו הפתעה מחכה לי. לצערי זה עדיין לא קרה. התחלתי לשנות ולהחזיר דברים שונים בקובץ ללא הצלחה.

לאחר זמן מה, החלטתי לנסות לתקן בווינדוס. התיקון היה אותו הדבר כמו שתיארתי עד עכשיו.

```
00000089 65 4E 34 0D 0A B0 AA 00 00 0D 43 22 44 52 eN4.....C"DR
00000100 00 06 6A 00 00 04 47 08 02 00 00 7C 8B AB...j...G....|..
00000208 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00x....sRGB.....
00000300 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00..gAMA.....a...
00000400 09 70 48 59 73 AA 00 16 25 00 00 16 25 01 49..pHYs...%...I
00000502 24 F0 AA AA FF A5 AB 44 45 54 78 5E EC BD 3FR$......DETx^..?
```

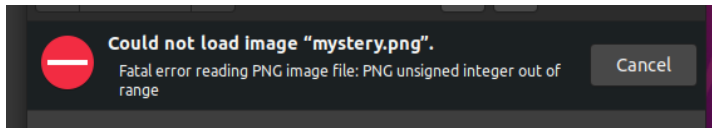
```
0A F6 19 00 00 00..S.....
1 3C 6F F1 75 B8.L.....l<o.u.
50 82.....IEND.B`.
```

לפני

```
89 65 4E 34 0D 0A B0 AA 00 00 0D 43 22 44 52 eN4.....C"DR
00 00 06 6A 00 00 04 47 08 02 00 00 7C 8B AB...j...G....|..
78 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00x....sRGB.....
00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00..gAMA.....a...
00 09 70 48 59 73 AA 00 16 25 00 00 16 25 01 49..pHYs...%...I
52 24 F0 AA AA FF A5 AB 44 45 54 78 5E EC BD 3FR$......DETx^..?
```

אחרי

```
89 50 4E 47 0D 0A 1A 0A 00 00 0D 49 48 44 52 PNG.....IHDR
00 00 06 6A 00 00 04 47 08 02 00 00 7C 8B AB...j...G....|..
078 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00x....sRGB.....
000 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00..gAMA.....a...
000 09 70 48 59 73 AA 00 16 25 00 00 16 25 01 49..pHYs...%...I
052 24 F0 AA AA FF A5 49 44 41 54 78 5E EC BD 3FR$......IDATx^..?
```



```
89 50 4e 47 0d 0a 1a 0a 00 00 0d 49 48 44 52 %PNG.....IHDR
00 00 06 6a 00 00 04 47 08 02 00 00 7c 8b ab ...j...G....|<«
78 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 x....sRGB.®İ.é...
00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 ..gAMA..±.üa...
00 09 70 48 59 73 aa 00 16 25 00 00 16 25 01 49 ..pHYs^...%...I
52 24 f0 aa aa ff a5 49 44 41 54 78 5e ec bd 3f R$ø^aYIDATx^1¼?
```



לשמחתי הקובץ סוף סוף נפתח!
ובתמונה היה הדגל של האתגר

אחרי שסיימתי את האתגר, שוחחתי עם חבר שיש לו המון ניסיון
באתגרי CTF לגבי הבעיה שהייתה לי באתגר.

הבעיה היא שגם לאחר ש"תיקנתי" את הקובץ, הוא עדיין שבור...
פשוט הוא מתוקן מספיק כדי שהאפליקציה שמציגה תמונות
בווינדוס תוכל להציג אותו.