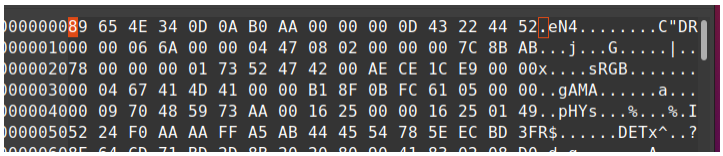
**Mark Seliternikov**
**picoCTF - c0rrupt [250 points]**

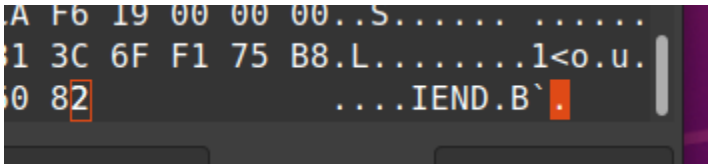
---

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.

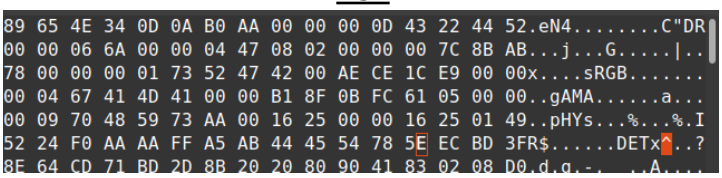



לאחר מכן ראיתי ב-Footer שהוא מסתיים ב-`IEND.B.

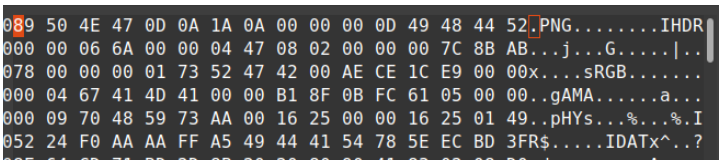
לאחר חיפוש באינטרנט, גיליתי שקובץ PNG מסתיים בסיומת כזו.
לאחר שגיליתי זאת התחלתי לתקן את הקובץ בעזרת האתר [http://www.libpng.org/pub/png/spec/1.2/PNG-Contents.html](http://www.libpng.org/pub/png/spec/1.2/PNG-Contents.html)

בין היתר נעזרתי גם בתמונות ובויקיפדיה.

**לפני**

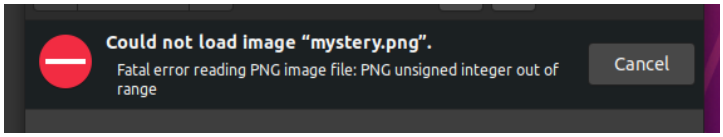



**אחרי**

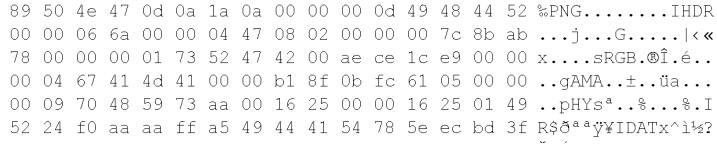



היו 3 דברים שהייתי צריך לתקן ב-Header כדי שהקובץ יהיה PNG רשמתי.

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.

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.