רז אברג'ל

פתרון תרגיל secret

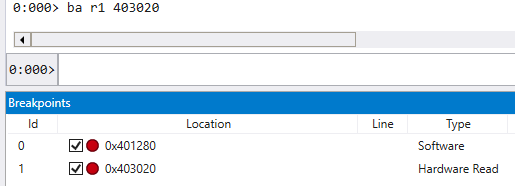
תחילה נמצא את מיין:

בהרצת התוכנית בCMD אנחנו מקבלים את המחרוזת " Magic word"

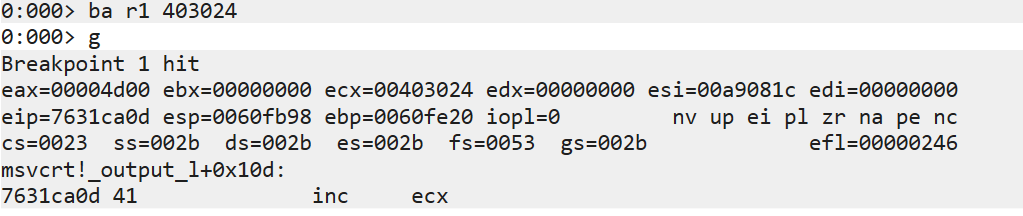
ועל כן נחפש את הכתובת שבה שמורה המחרוזת במודול secret (כמובן לאחר ביצוע bp $exentry ו g וlm .)



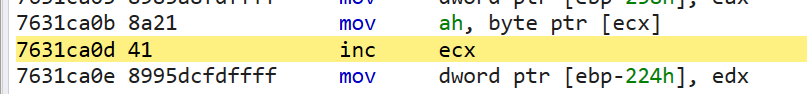
נראה שהמחרוזת נמצאת בכתובת 403024 אנחנו יודעים שאיפשהו המחרוזת הזאת תודפס על ידי פונקציית הדפסה ולכן נרצה ליצור break point access על מנת לקבל את התראה כמישהו מנסה לגשת לכתובת הזאת



נקיש את הפקודה g ונראה איפה יש לי פגיעה

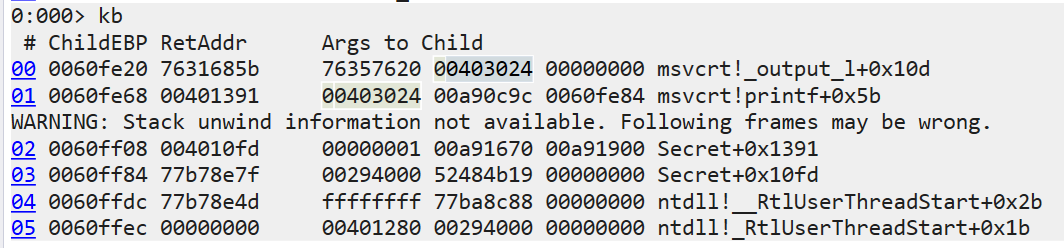


הברייק פוינט נעצר בפקודה הבאה



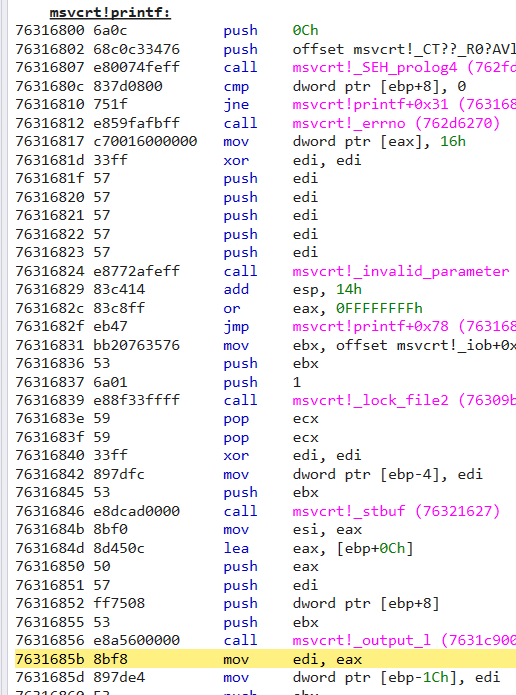
בשלב זה נתבונן במחסנית על מנת לנסות להבין איפה המיין נמצא ביחס לנקודה שעצרנו בה

נבצע את פקודת kb ונראה שאנחנו מזהים את המחרוזת שלנו מועברת פעמיים



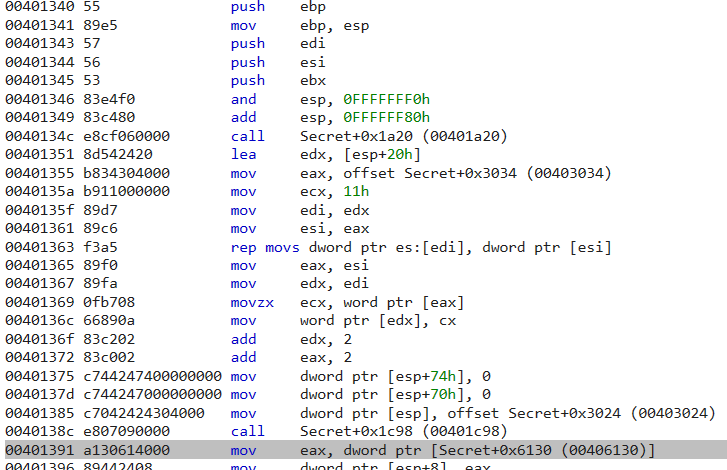
מכיון שסדר ההתרחשות של הפונקציות הוא מלמעלה למטה lifo אז הקריאה שמעניינת אותנו היא במיקום 1 במחסנית שלנו ,לכן הכתובת שתכוון אותנו לכיוון הMAIN היא כתובת החזרה 401391

כיוון שהכתובת במיקום 0 גם חשודה שהיא מיין נבדוק אותה



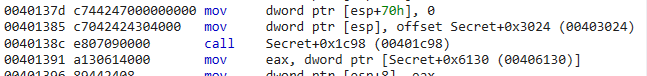
רואים בבירור שמדובר בפונקציה PRINTF ולכן הפונקציה היא לא מיין

ואילו בכתובת החזרה 401391 נראית כך



מכאן הגענו למסקנה שפונקציה זאת היא אכן המיין.(גם מכיוון שאין עוד אופציות אפשריות במחסנית שמקבלות את המחרוזת שלנו)

1. באיזה פונקציה יש הפניה למחרוזת הראשונה שמודפסת?



ההפניה הראשונה למחרוזת המודפסת נמצאת במיין בדחיפה למחסנית (המחרוזת נמצאת בכתובת 403024 בזיכרון) לפני הקריאה לפונקציה PRINTF

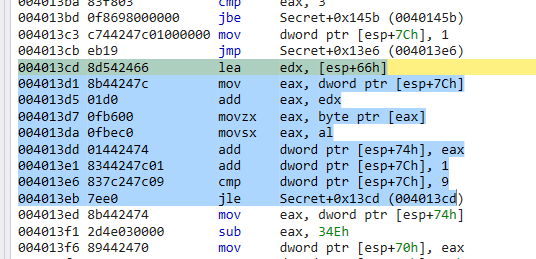
1. מהי ההודעה הסודית?

אחרי הדפסה יש בדיקה של אורך המחרוזת אם היא קטנה או שווה לשלוש התוכנית תגמר ולכן אנו צריכים להכניס קלט שגדול משלוש



לאחר מכן

זהינו שיש פה לולאה בתחום המסומן הכחול



דיבגתי וראיתי שהלולאה רצה 9 פעמים .הלולאה סוכמת בכל איטרציה את כל הערכים האקסדצימלים של כל תו שהוכנס במחרוזת כקלט לתוך המיקום  **(למעט האיבר הראשון במחרוזת כיוון שהלולאה מתחילה ב1 ולא ב0)**

ביציאה מהלולאה נעביר את תוצאת הסכימה לתוך רגיסטר EAX ונפחית את הערך ב 



לאחר מכן נשווה את התוצאה לערך 14H



אם הערך שנקלט מהמשתמש (באורך 8 תווים) ולאחר מכן הלולאה סכמה אותו ותוסיף גם את הערך 10H בגלל הלחיצה על אנטר שמורידה אותנו שורה וגם היא מחושבת בBUFFER ,ואז נפחית ממנו וגם את האנטר (10H) שבו אנחנו לא מעוניינים, וההשוואה לערך 14h תתקבל והם אכן שווים אז נגיע להודעה הסודית .

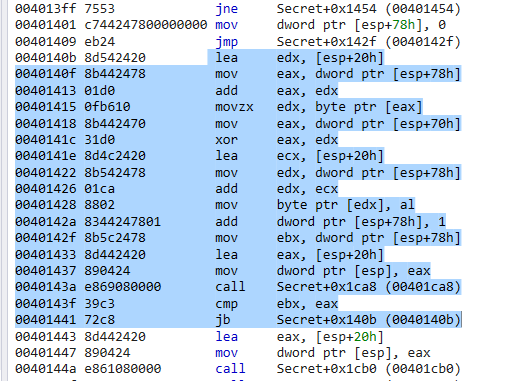
למעשה כל קלט באורך 8 תווים בו הסכום ההקסהדצימלי של כל האיברים החל מאינדקס 1 יהיה שווה ל (מומר לעשרוני)

סכום כל הערכים של התוים במחרוזת) - 846 + 10) == 20

אז נכנס לאזור שבו מפוענח הקוד המוצפן ונקבל את ההודעה הסודית

איך ההודעה הסודית מופיעה ?

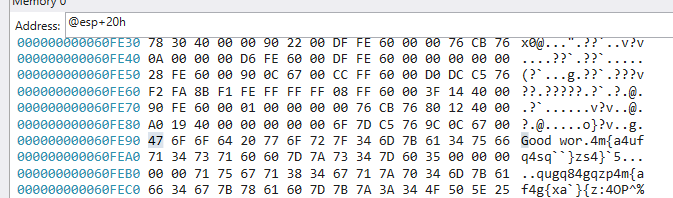
משם נקפוץ ללולאה שתפענח את הקטע המוצפן שנמצא בזכרון בכתובת 



הפענוח קורה על ידי ביצוע XOR על כל אחד מהתווים המוצפנים וככה מקבלים את ההודעה הברורה

(מדובר פה בהצפנת XOR)

בתמונה אפשר לראות את תהליך הפיענוח של המחרוזת המוצפנת



כמו שאמרנו האיבר הראשון במחרוזת לא משנה לנו כיוון שהלולאה הראשונה לא סוכמת אותו



ופיצחנו את ההודעה הסודית

1. **כתיבה של תוכנית בפייתון שמממשת את התפקוד העיקרי של main**

\*\*מוגש בקוובץ נפרד\*\*