בס"ד

MoedA2022 WriteUp – ישי לוטווק

דבר ראשון נריץ את הקובץ בcmd:

נחפש את המחרוזת שקיבלנו בxdbg (בחלונית של המחרוזות):

ננסה להריץ בxdbg:

ננסה למצוא את מנגנון האנטידיבאג:

נבצע אנליזה סטטית בida:

נבדוק באמצעות windbg האם הקוד ניגש לpeb+2 כדי לבדוק אם אנו במצב דיבאג, (נעשה זאת באמצעות הפקודה ba r1 $peb+2):

אם כן יוצא שהסיסמא היא:

מ.ש.ל