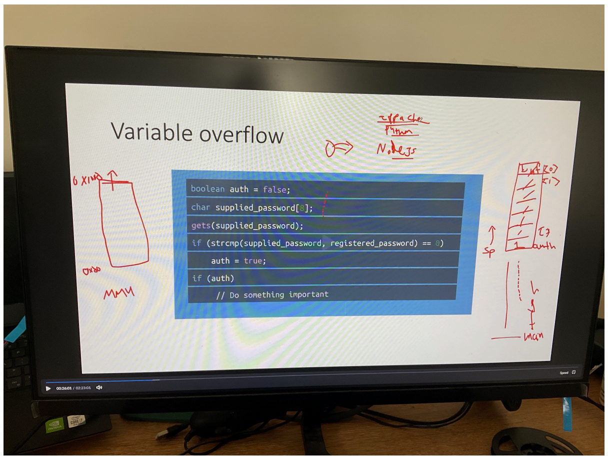
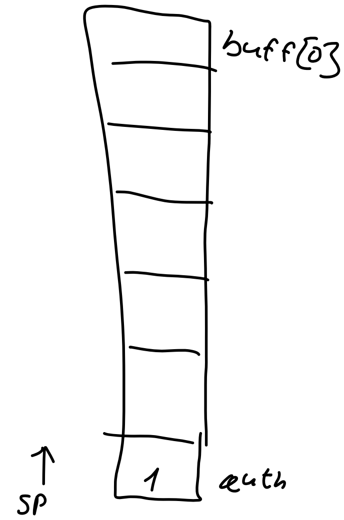
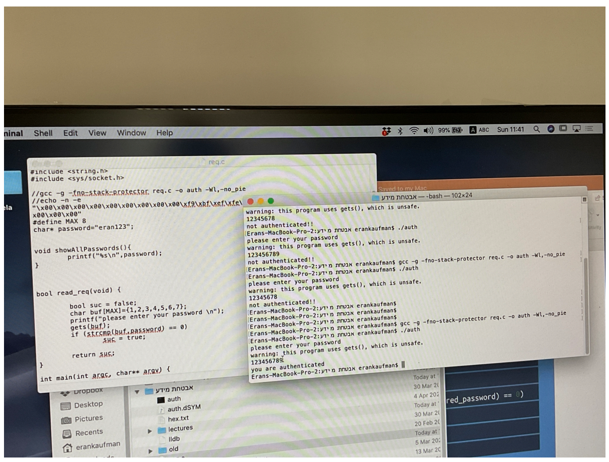






להסתכל על ב define הגודל שלו לעומת המערך

להפעיל debugger gdb

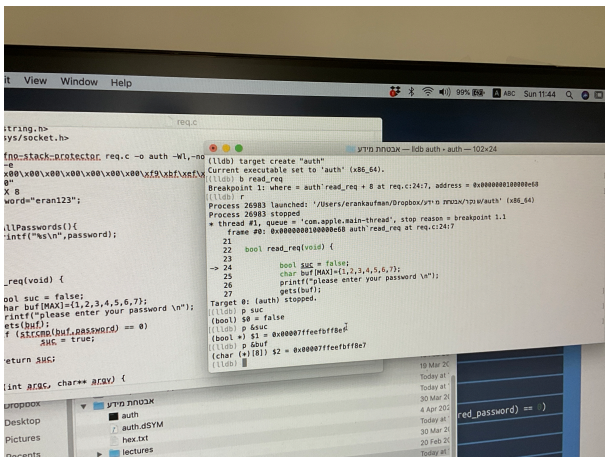
b func_name

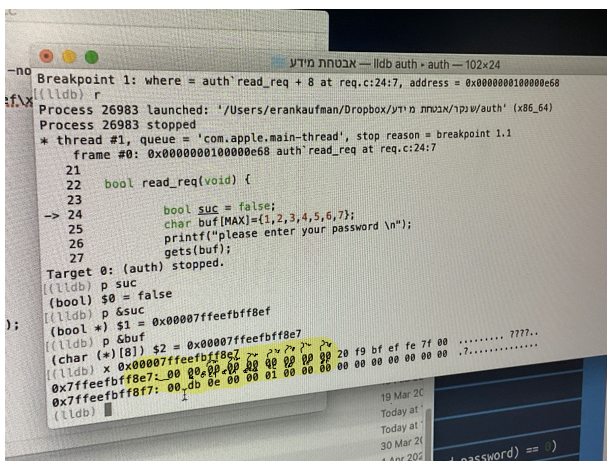
run

בשביל להפעיל דיבאגר מכניסים את ה -g

p var_name עושה פרינט של המשתנה ברגע

r



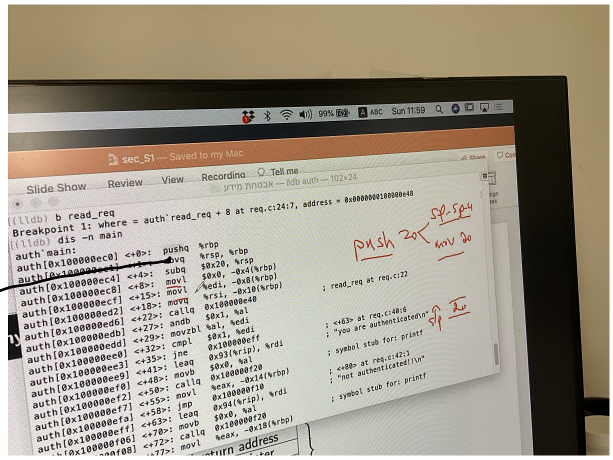


x = examine

h = next

Segfault אם יש

dis -n func_name (ex main)



sp = sp-4

מינוס
inc=4 bytes

ומוצים מקום את הערך

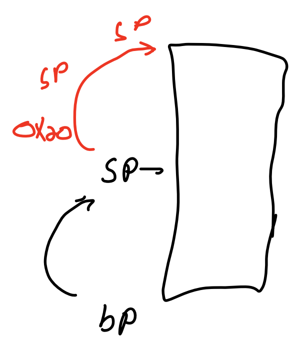
20 כלומר push עושה 2 דברים.

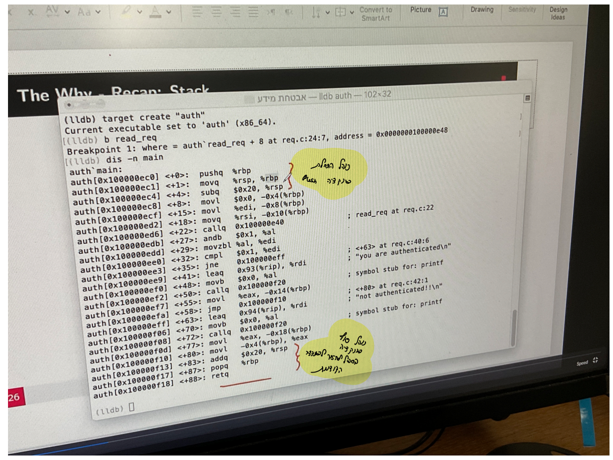
בפונקציה חדשה נקראת ה basePtr יהיה שווה StackPtr בשביל להתחיל

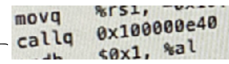
mov &rsp, %rsp ה base יהפוך להיות StackPtr

subq 0x20,%rsp תפנה לי 0x20 במחסנית שיהיה מקום

כך בפונקציה יש header







קורא ל כתובת איפה שהפונקציה

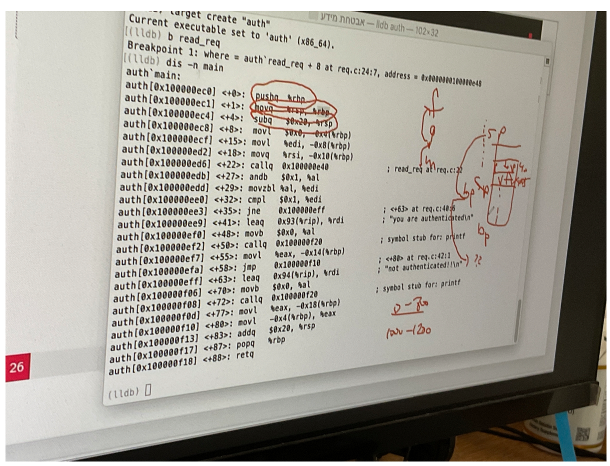
read req

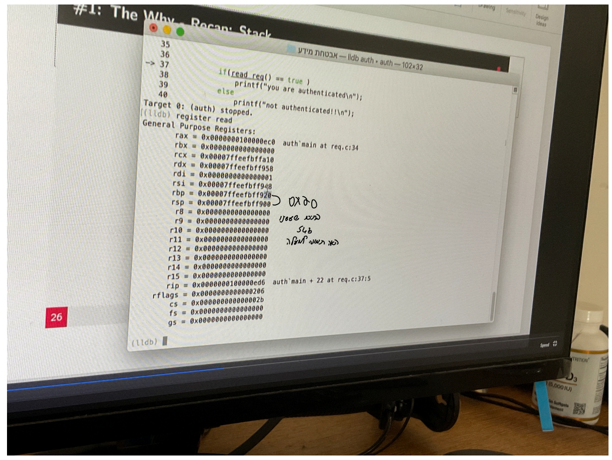
call – push
call – jump

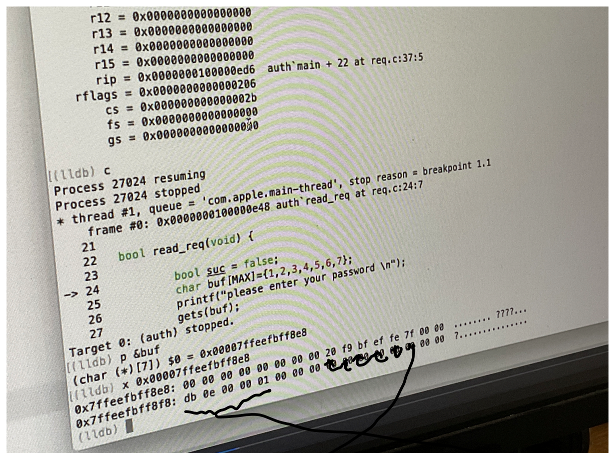
ה instructions נמצא במצביע זיכרון אחר של התוכנה מה sp

ret – pop
ret – jump
stop

ה ret צריך לשמור על הכתובת הבאה







פה קראנו ? את ה stack ורואים שבאמת למעלה של ה stack

נשמר ה prev base pointer

7ffe fe bf f9 20

return address

01:16:29 כאן הוא מתחיל להסביר על החלפת ה return address

לפונקציה show_passwords