**. Rivals of Catan – ' חלק ג**

1. בעזרת F12 נכנסנו לDeveloper Console. מעבר על הקוד המקור של האתר גילה שיש כפתור חבוי שמיועד שלחזור סיסמאות:

<div class="button disabled" onclick="challenge\_me()">Passwords Recovery</div>   
שינוי הclass ל " button" גילה את הכפתור.

1. לחיצה על הכפתור Passwords Recovery העביר אותנו לעמוד ה- Challenge.  
   לפי ההוראות כתבנו תוכנית המקבלת קלט המכיל בכל שורה אלמנט מטרה בודד ומחשבת את סך העלות במשאבים הנדרשים לבניה של כל האלמנטים. כתבנו את התוכנית ב-C ותרגמנו אותה לאסמבלי בעזרת האתר [godbolt.org](https://godbolt.org/). מכיוון שהדרישה שנפח התוכנית תהיה קטנה מ2KB-, ערכנו את קוד האסמבלי והחלפנו קריאות מפורשות לפונקציות ספריה (strcomp, printf, scanf ) בקריאה עקיפה ע"י טעינה ידנית של msvcrt.dll וחיפוש כתובת הפונק' בזמן ריצה. השתמשנו בשיטה שהוצגה בתרגול: LoadLibrary, FindFunction , GetProcAddress. מצורף קוד של התוכנית challenge.S.  
   לאחר מכן קמפלנו את התוכנית, חילצנו את הקוד הבינארי מתוך קובץ ה-obj שנוצר ושירשנו אותו עם קובץ PE.bin ו- find\_function.bin בצורה הבאה:

gcc -c challenge.S -o challenge.o

objcopy -O binary challenge.o challenge.bin

type PE.bin challenge.bin find\_function.bin > challenge.exe

לבסוף בעזרת CFF Explorer פתחנו לעריכה challenge.exe שיצרנו וערכנו את ה- Section Header.  
עדכנו את הגדלים Virtual Size ו- Raw Size לגודל 39A שזה הגודל בבתים של הקוד הבינארי ( הגודל של challenge.bin + find\_function.bin )