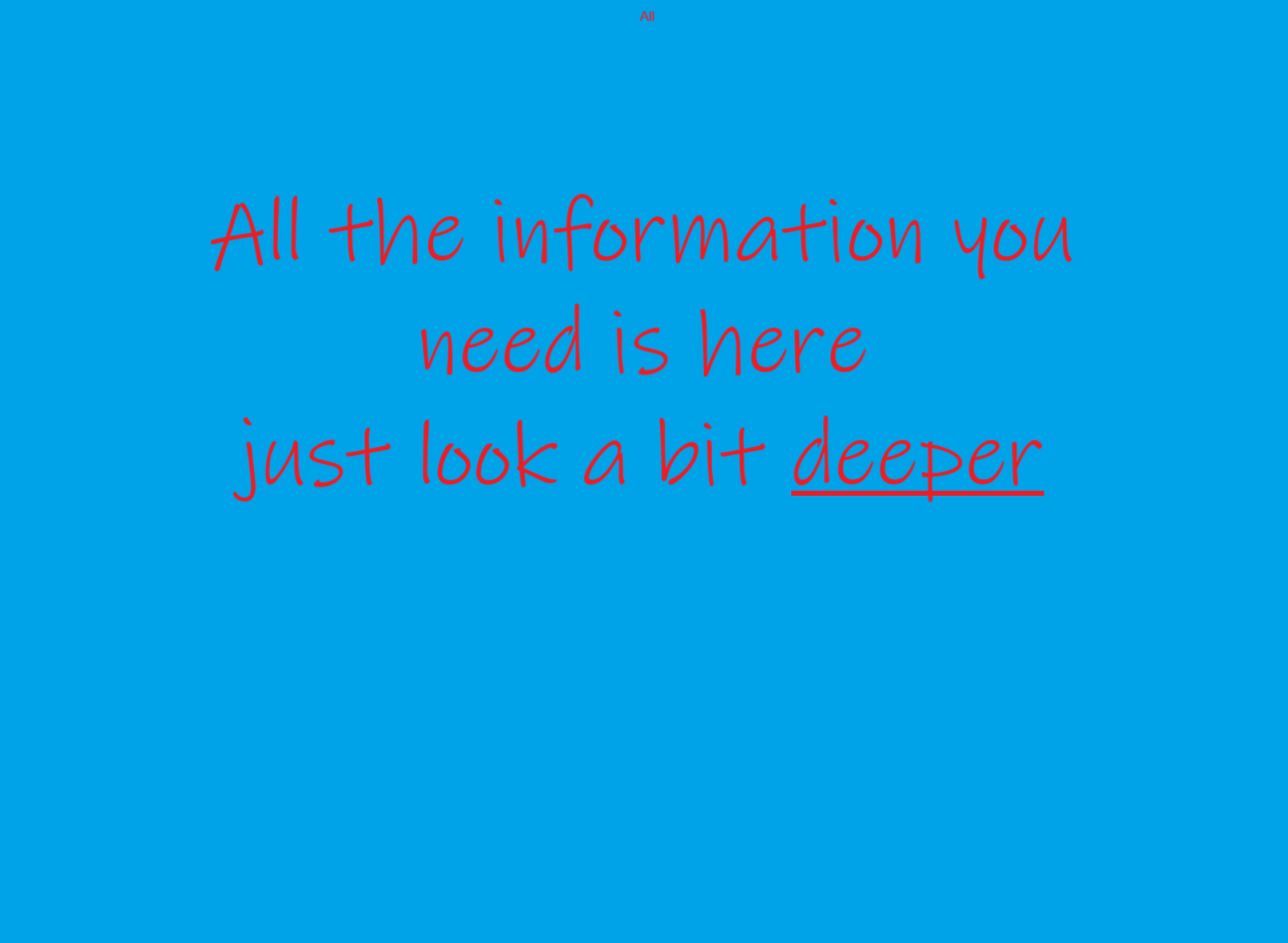
פרויקט סוף רשתות מחשבים

# פתרון האתגר

# מגיש – יונתן ברקוביץ, ת.ז. 329085054

**השלב הראשון - הרמז הראשון:**

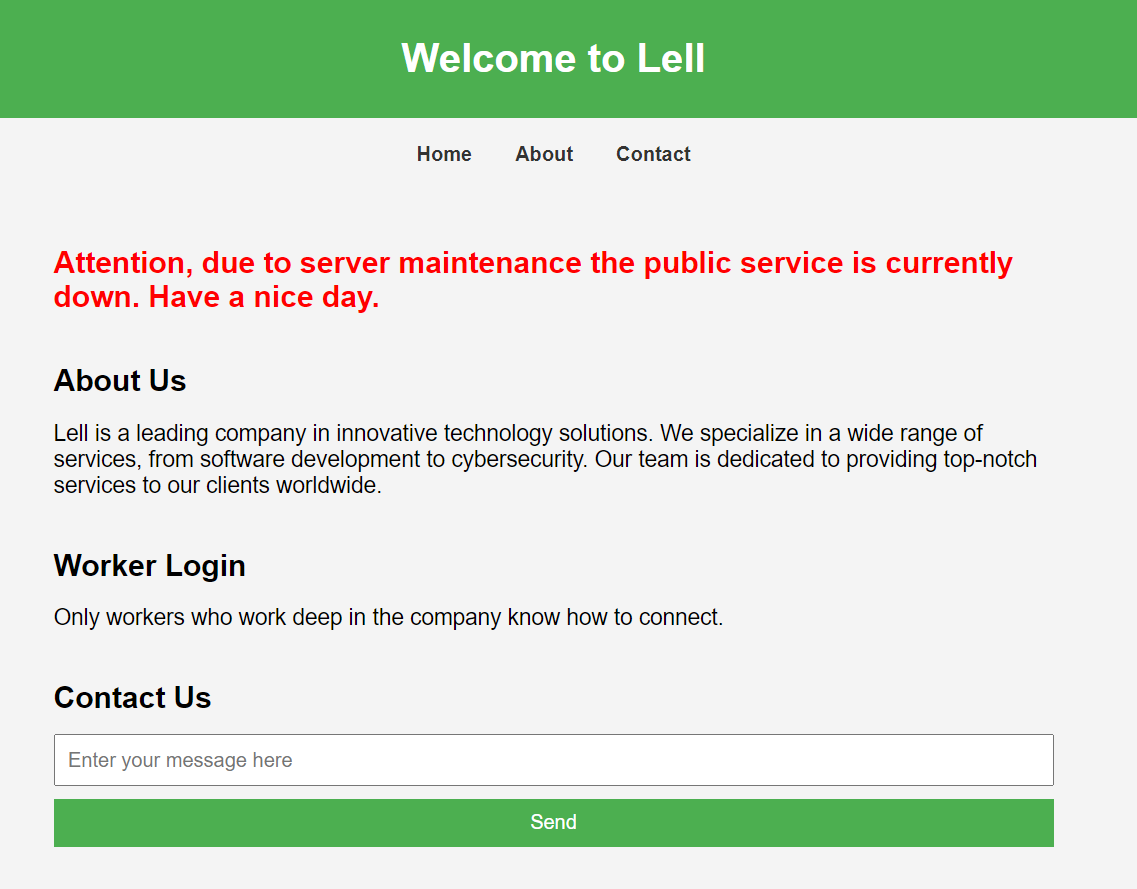
הדבר היחיד שקיבלנו הוא התמונה הבאה:  


לכאורה לא ניתן לעשות עם זה הרבה, אבל כאשר נתמקד במילים עמוק יותר, נבין שאולי אנחנו צריכים לנסות בתוכן של הקובץ ממבט של מחשב ולא של אדם רגיל:

הדבר הראשון והבולט לעין זה שיש בקובץ מחרוזות באנגלית, ננסה לקרוא אותן:



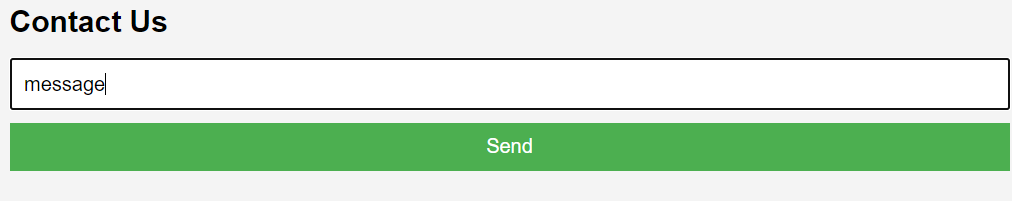
והנה מצאנו את הכתובת של האתר, נתחבר ונקבל:



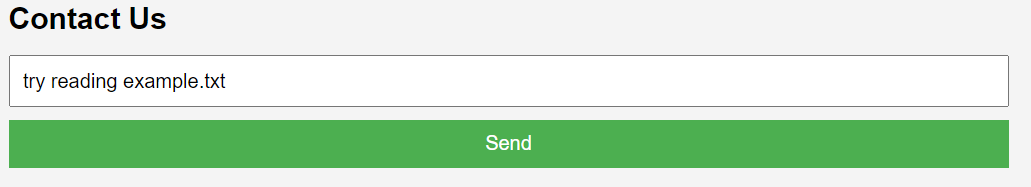
מצאנו את האתר, וישנה אפשרות של התחברות עובדים, אבל אין כפתור או אפשרות להזין שם משתמש או אפילו סיסמא, אז מה עושים?

**השלב השני – מבחן השרת:**

הדבר היחיד שניתן לכתוב בו דברים זה הבר למטה, בו ננסה להזין בו משהו ונראה מה יקרה:



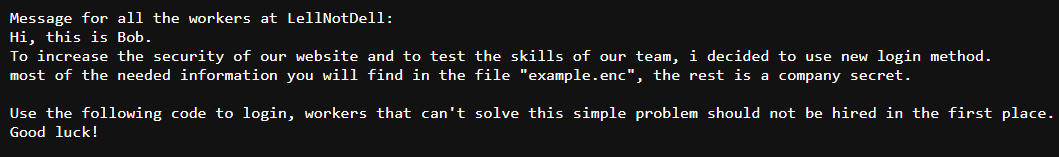
ולאחר לחיצה על כפתור שליחה, נקבל דבר מפתיע:



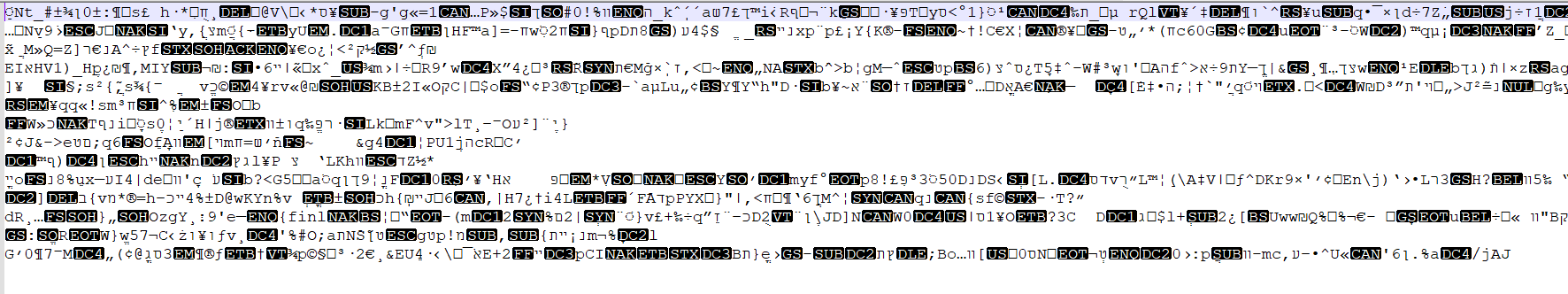
התוכן השתנה וכתוב לקרוא את הקובץ example.txt אבל אין אפשרות לראות קובץ כזה בכל הדף האינטרנטי שקיבלנו, אם זאת, עדיין יש את האפשרות שהוא מופיע בשרת אך לא מוצג לנו בדף הHTML, לכן ננסה ידנית להשיג את הקובץ על ידי שינוי הURL:



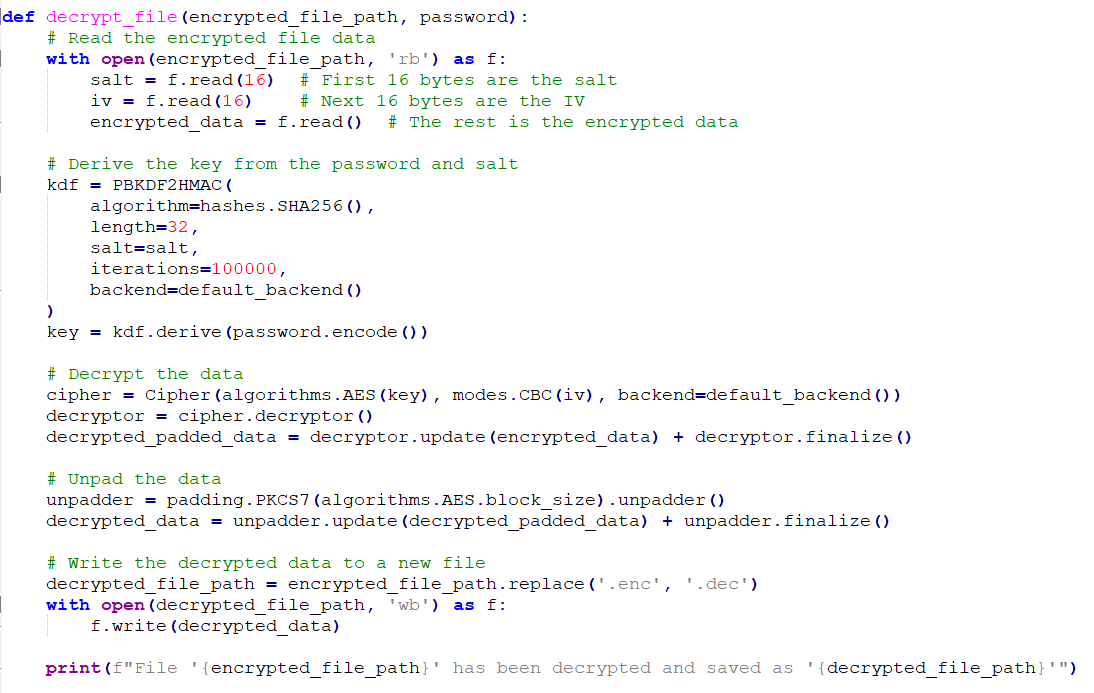
נקבל קובץ TXT ארוך, בעל התוכן הבא:



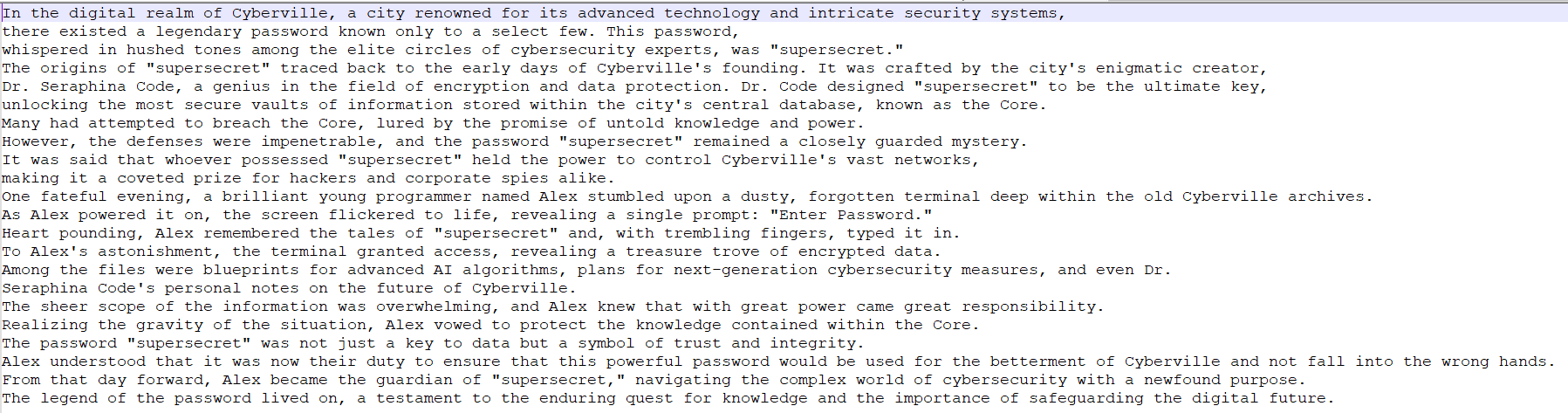
ההודעה אומרת לנו שיש קובץ נוסף, "example.enc" שעלינו להשיג, כאשר נשנה את הURL שוב נקבל ירד לנו קובץ חדש למחשב, נפתח אותו:



התוכן מוצפן, כנראה זה קשור להמשך הקובץ שהשאיר לנו "בוב" הכותב, לאחר בירור נגלה כי בוב עשה שימוש בפונקציית AES-CBC ואפילו השאיר תיאור מלא בשפת פייתון, נתבונן בקוד ונכתוב פונקציה שתהפוך את ההצפנה:



וכמובן חייבים לנחש את הסיסמא, לכן נבחר קובץ של סיסמאות נפוצות כמו הקובץ הזה:   
<https://github.com/DavidWittman/wpxmlrpcbrute/blob/master/wordlists/1000-most-common-passwords.txt>  
ננסה את הסיסמאות מהקובץ ונגלה שעבור הסיסמא 1111 (מקום 68) כל הקובץ קריא, כלומר אין תווים לא מזוהים לכן נניח שזאת הסיסמא הנכונה ונשתמש בה:  
 נפתח את הקובץ לאחר הסרת ההצפנה:



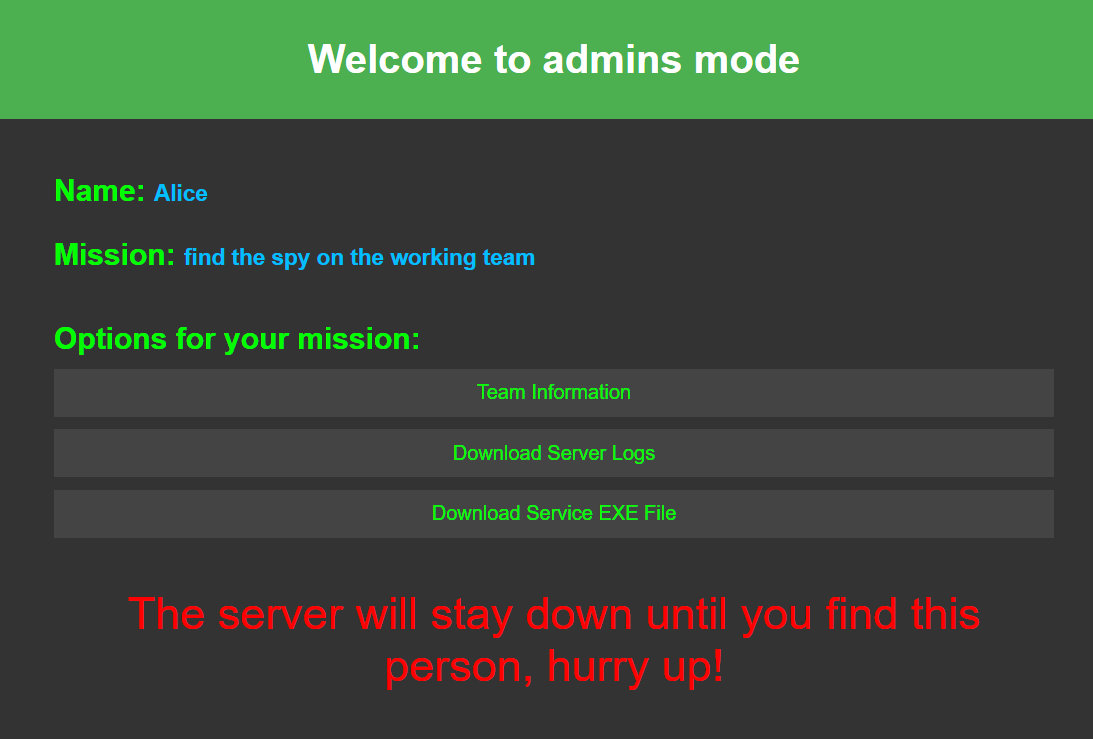
ניתן לראות שהמילה supersecret מאוד בולטת בכל הדף, אבל מה כבר אפשר לעשות איתה, לאחר ניסיונות רבים החלטתי לבדוק האם יש עוד מידע בתוך התמונה, ומצאתי את המחרוזת הבאה:



כנראה גם פה אנחנו צריכים לשנות את הURL ידנית, אך הפעם להשתמש בסקריפט:

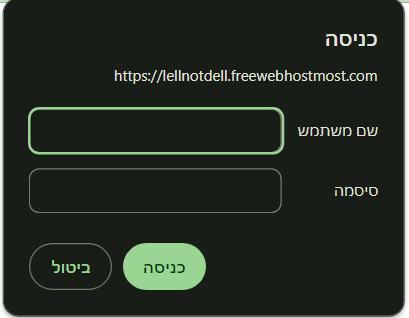


ואכן, לאחר כתיבת הURL נקבל אתר חדש ובו משימות חדשות:



**השלב השלישי – המשימות השונות:**

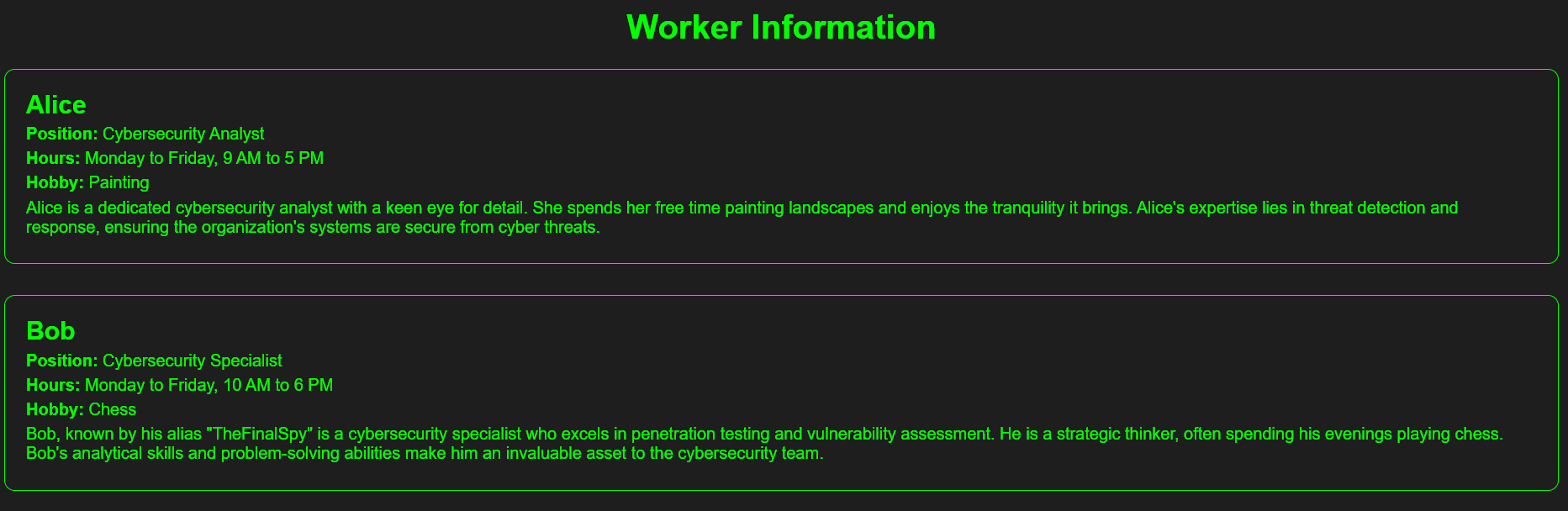
נבדוק את האפשרויות בסדר יורד, נתחיל ממידע על העובדים, אך ניתקל בדף הבא:



משתמש אנחנו יודעים, אנחנו הדמות אליס, אך סיסמא? נחפש בתמונה ההתחלתית ונראה:



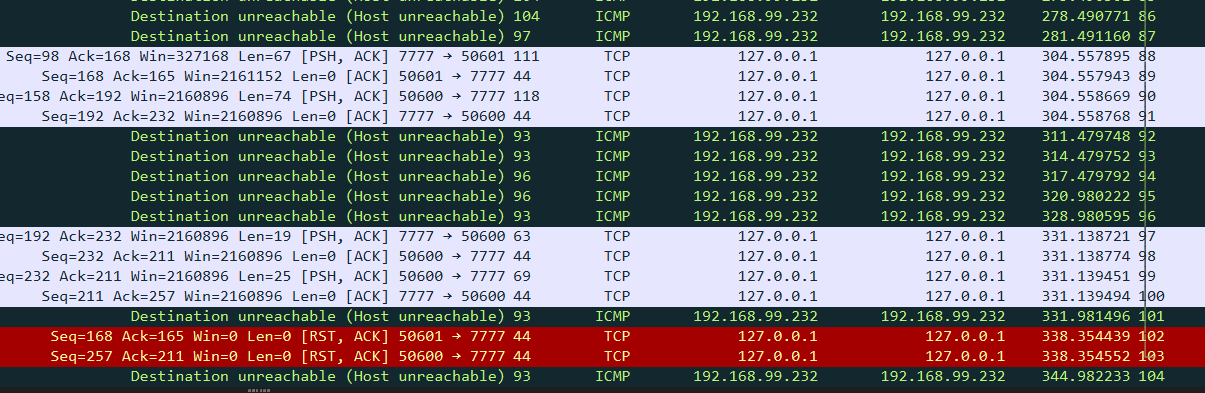
לכן הסיסמא היא עדיין supersecret, נזין אותה ונתקדם באתגר.

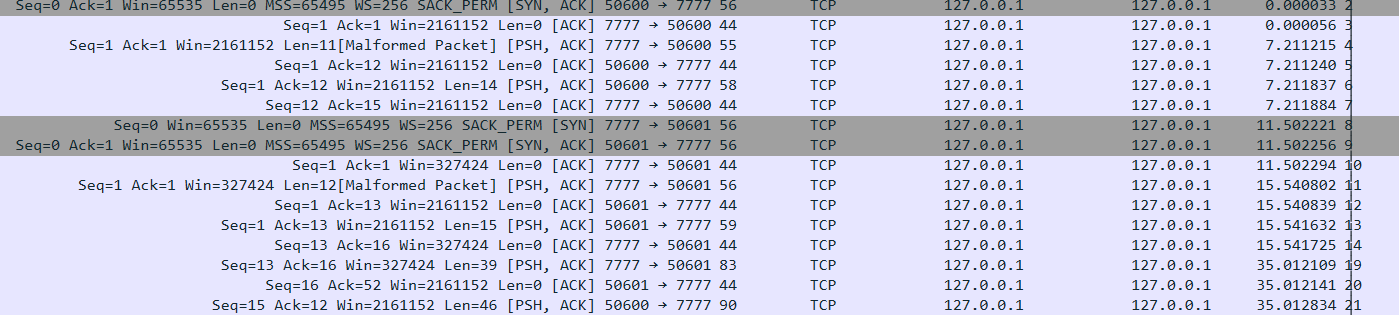
אחרי שהצלחנו לעבור את בקשת החיבור, נראה את הדף הבא:  


הדף מלא בהמון מידע על המון עובדים אך יש דבר אחד חשוד במיוחד והוא: **בוב**

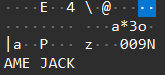
הוא היחיד שיש לו ציטוט במידע, בדומה לציטוט שראינו סביב הסיסמא "supersecret", בנוסף לזה שכבר ראינו שהוא "הכותב" של האתגר הקודם, בעוד כל זה רק חשדות, נעבור לראות את פריט המידע הבא, התכתבויות.

נפתח את הקובץ בwireshark ונראה:

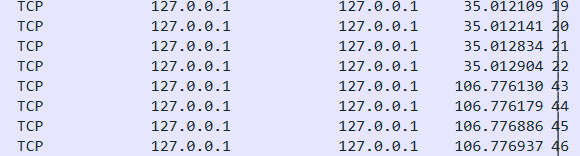
ללא ספק המון הודעות, אך הרבה מהן כשלו, ננסה לסנן רק פקטות TCP:



כבר הרבה יותר טוב, אך באיזה פרוטוקול משתמשים בשכבה 5, נכון לעכשיו לא ידוע לנו, אך נראה כי יש הודעות TCP "פגומות", נבדוק אחת לדוגמא:

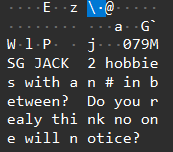


ניתן לראות כי בסוף הפרטה יש את צירוף המילים NAME JACK שהוא עובד בקבוצה שלנו, לכן אפשר להניח שהמידע משורשר לסוף הפקטות בצורת טקסט, נתחיל לעבור על כל המידע, האם לקרוא כל פקטה? ברור שלא, ניתן לשים לב שישנם הפרשי זמן גדולים בין רצף לרצף:



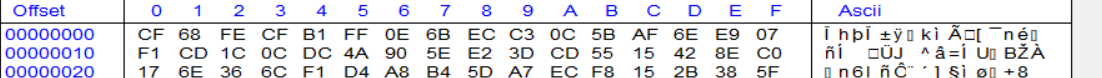
לכן נקרא רק את ההודעה הראשונה בתחילת כל רצף כזה.

ההודעה הכי מעניינת היא הבאה:

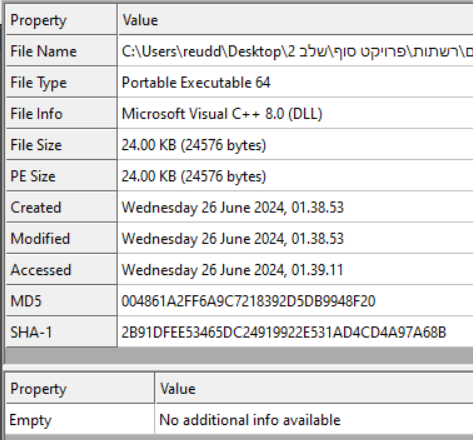


בוב אומר לנו באופן מפורש שהסיסמא היא צירוף של 2 תחביבים ותו # בניהם, גם לא פלא שראינו מקודם תחביבים של כל עובד והשם בוב חשוד לחלוטין, אך כרגע עדיין עלינו לבדוק את הקובץ האחרון, קובץ השירות:

ננסה להריץ את הקובץ ונגלה שיש תקלה, הוא לא מותאם למחשב שלנו, נבדוק אותו בCFF:

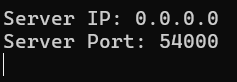


חסרה התחלה תקינה של פורמט PE, לכן סביר להניח שהקובץ הוצפן וזאת ההצפנה עליה דיבר בוב, ננסה מספר הצפנות במפענח שהשתמשנו בו קודם, לבסוף נכניס "TheFinalSpy" שזאת המחרוזת החשודה של בוב, ונראה את הפורמט:



אכן הקובץ נפתח בפורמט

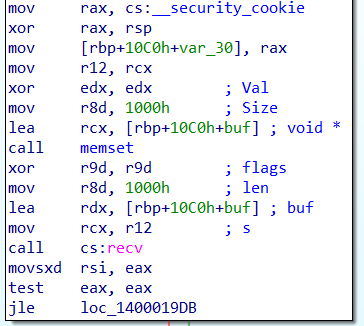
**השלב הרביעי – השירות:**  
PE ננסה להריץ אותו:



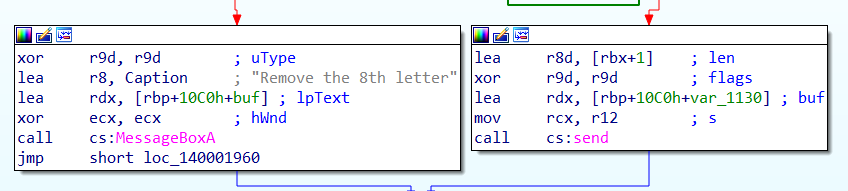
נראה כי יש סוג של שרת שמאזין לנו, נעשה רברסינג לקובץ ונראה מה הוא עושה בדיוק:

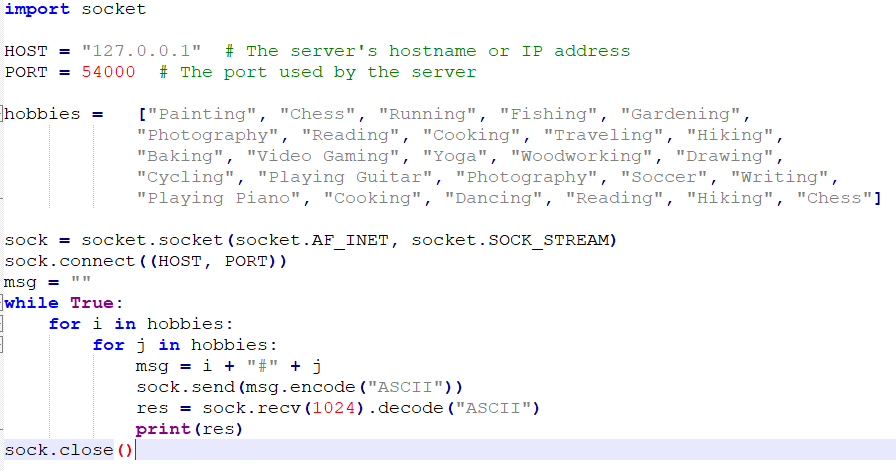
**מאחר שזה לא קורס ברברסינג לא תהיה הרחבה מאלה אלה סיכום הממצאים של המחקר.**

השרשת מאתחל סוקט ומאזין לו, לאחר מכן בלולאה אין סופית הוא:

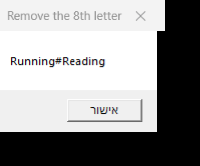


מקבל מידע דרך הסוקט ומעביר אותו דרך פונקציה מתמטית מסובכת (ספוילר, היא לא הפיכה וממש לא שקופה או פתוחה להתקפות סטטיסטיות, ממש כאילו מישהו מימש בכוחות עצמו את הפונקציה SHA256 רק כדי להקשות על הפותר...)  
ולאחר הפונקציה והשוואה אם סטרינג שנראה כמו תוצאה של SHA256 אם התוצאה נכונה יש מסך שאומר שהגענו לפתרון, אחרת נשלחת הודעת שגיאה חזרה בסוקט:

  
מאחר שבוב גילה לנו שהסיסמא היא 2 תחביבים צדומים עם # באצמע, ננסה את כל האפשרויות בעזרת תוכנית פייתון:



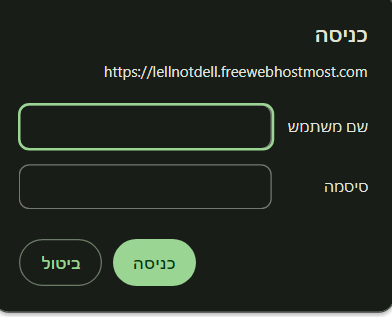
ואכן נקבל:



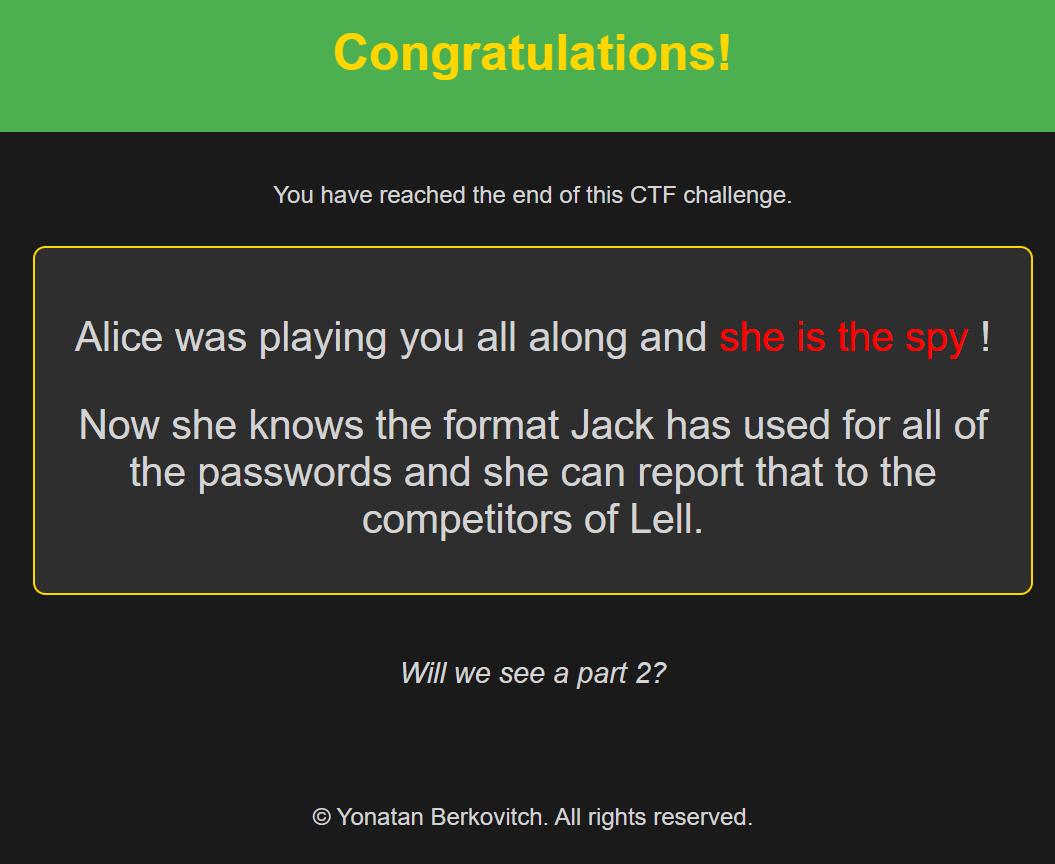
ובכן, לאחר מכן ננסה לגשת לכתובת הזאת באתר, אך נקבל 403, פה נעזר שוב בדברים הכתובים בתוך התמונה:



פה באמת זאת הפעם הראשונה שהרמזים לא מסודרים לפי הסדר הנכון שלהם, כנראה כדי לבלבל אנשים שחשבו שהם למדו כבר איך האתגר הזה עובד, בכל מקרה, נוסיף /final.html



שוב המסך של הכניסה, הפעם אליס לא תכניס אותנו, אז נעזר במסר הנוסף שבוב לא משתנה את סיסמתו וננסה להתחבר דרך בוב עם הסיסמא "TheFinalSpy":



אופס, מסתבר שאליס הייתה המרגל מההתחלה, מי יכול היה לדעת?

בכל מקרה, מאוד נהנתי מהאתגר הזה ומקווה שגם לכם היה כיף 😊