**פתרון - Mossad CTF**

**פתרון ל CTF – אבישי גונן**

**שלב א:**

מה המשתמש מקבל:

המשתמש מקבל קובץ pdf שמכיל בתוכו סיפור, וכן קובץ הסנפה.

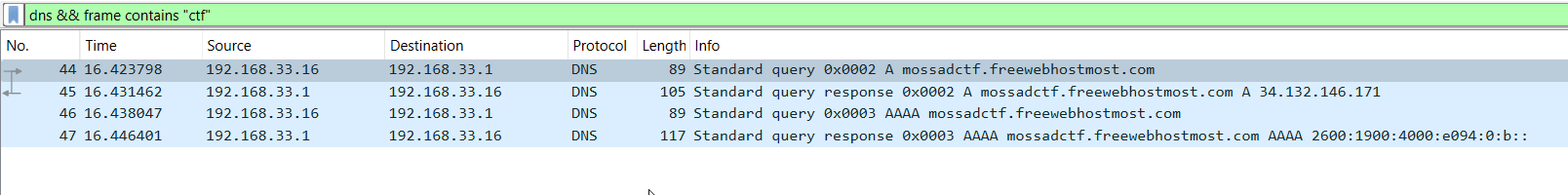
מה הרמזים שהוא רואה:

בסיפור הוא מקבל שני רמזים:

1. יש שאילתת DNS לאתר, ששמה ניתן למצוא את ה domain name
2. "סוכן המוסד" שכח את הסיסמא שלו
3. בסיפור הוא גם מקבל את שם המשתמש של סוכן המוסד

מה צריך לעשות:

צריך לחפש בקובץ ההסנפה שאילתות DNS שקשורות באיזשהו אופן לאתגר.

לדוגמא: 

לאחר מכן, יש לגלוש לדפדפן ולראות מה יש שם.

מה התוצאה לשלב הבא:

A screenshot of a computer

Description automatically generated

יש פה הוראות לשלב הבא.

**שלב ב:**

מה המשתמש מקבל:

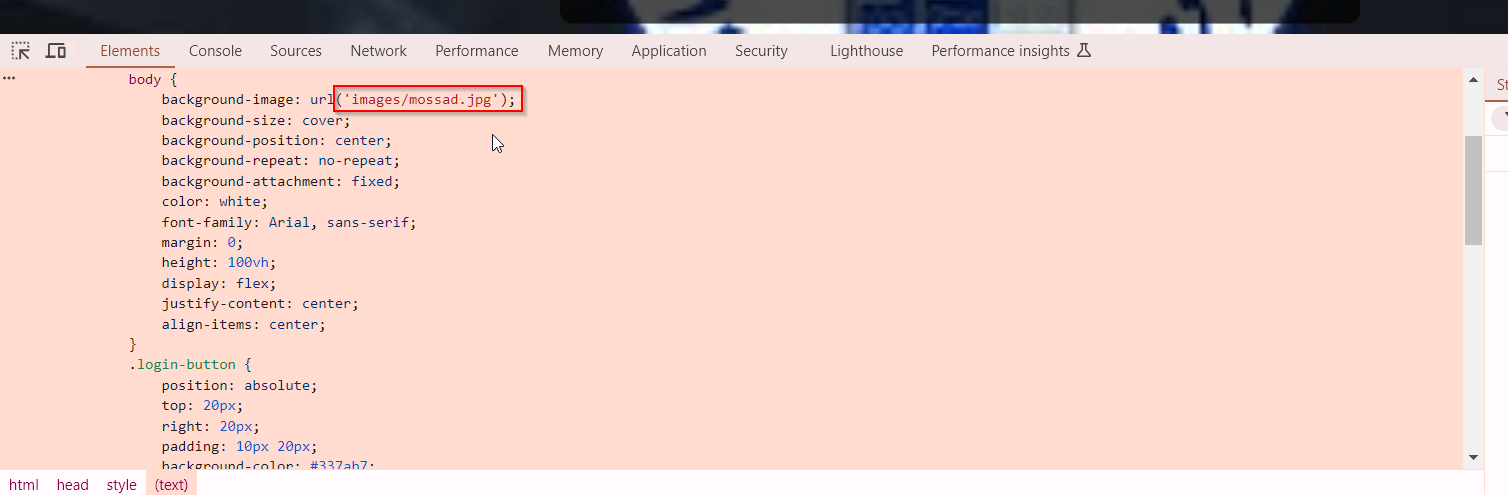
המשתמש מקבל KEY, IV.

מה הרמזים שהוא רואה:

ישנה תמונה שעליו להצפין, הוא בסה"כ מקבל שתי תמונות

מה צריך לעשות:

על המשתמש למצוא את תמונת הרקע באופן הבא:

לעשות f12 ולמצוא את ה url אל התמונה

לגשת resource הזה ולהוריד אותו:  
A computer screen shot of a logo

Description automatically generated

להצפין את תמונת הרקע באמצעות אלגוריתם AES-CBC, והמפתח וה IV שהוא קיבל. (לדוג', באמצעות שימוש ב openssl).

מה התוצאה לשלב הבא:

קובץ בינארי כלשהוא.

**שלב ג:**

מה המשתמש מקבל:

קובץ בינארי כלשהוא

מה הרמזים שהוא רואה:

אין

מה צריך לעשות:

לנסות לפענח מה הקובץ מייצג, על ידי הסתכלות ב hex-editor או לחילופין, שימוש באתר כלשהוא כגון <https://www.checkfiletype.com>.

לאחר מכן, יש להמיר את הקובץ הבינארי הזה לסיומת של jpg, כי זה הפורמט שלו, ולראות מה התמונה אומרת.

מה התוצאה לשלב הבא:

תמונה של ראיסי, עם מסר מוחבא בפנים



**שלב ד:**

מה המשתמש מקבל:

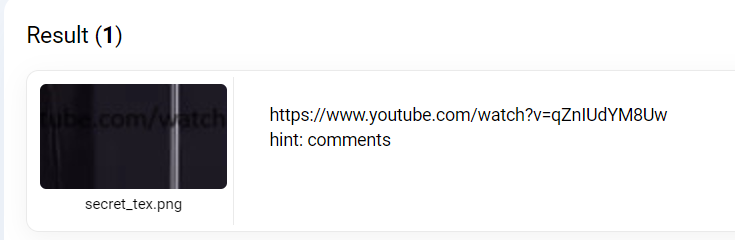
תמונה של ראיסי עם מסר מוחבא בפנים

מה הרמזים שהוא רואה:

אין

מה צריך לעשות:

עליו למצוא את המסר שמוחבא בתוך התמונה. יש להגדיל את התמונה, ולנסות להבין מה רשום בטקסט למטה. ניתן למשל להשתמש באתר שיודע לפענח טקסט מתוך תמונות, כגון <https://www.imagetotext.info>.



מה התוצאה לשלב הבא:

קישור לסרטון יוטיוב ובנוסף, איזשהו רמז: תגובות.

**שלב ה:**

מה המשתמש מקבל:

קישור לסרטון יוטיוב.

A person standing on a deck with his hands pointing at the camera

Description automatically generated

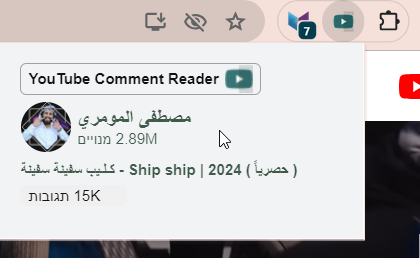
מה הרמזים שהוא רואה:

"תגובות". הוא קיבל רמז להסתכל בתגובות

מה צריך לעשות:

על המשתמש לנסות לנתח את התגובות של הסרטון, ולחפש אם יש שם משהו מעניין.

לשם כך, יש להשתמש באיזשהו כלי אוטומטי שעושה את זה, כגון התוסף הבא: <https://chromewebstore.google.com/detail/youtube-comment-reader/jbjbjeceipecokoeocnkcfjpanlipamf>



לאחר מכן, יש לחפש מילות מפתח שאולי קשורות לאתגר שלנו, כגון mossad, ctf, Eli Copter, password וכו'.

המטרה היא למצוא את התגובה שהחביא שם סוכן המוסד.

A screenshot of a computer

Description automatically generated

מה התוצאה לשלב הבא:

סיסמא שאותה החביא הסוכן, MossadRules

**שלב ו:**

מה המשתמש מקבל:

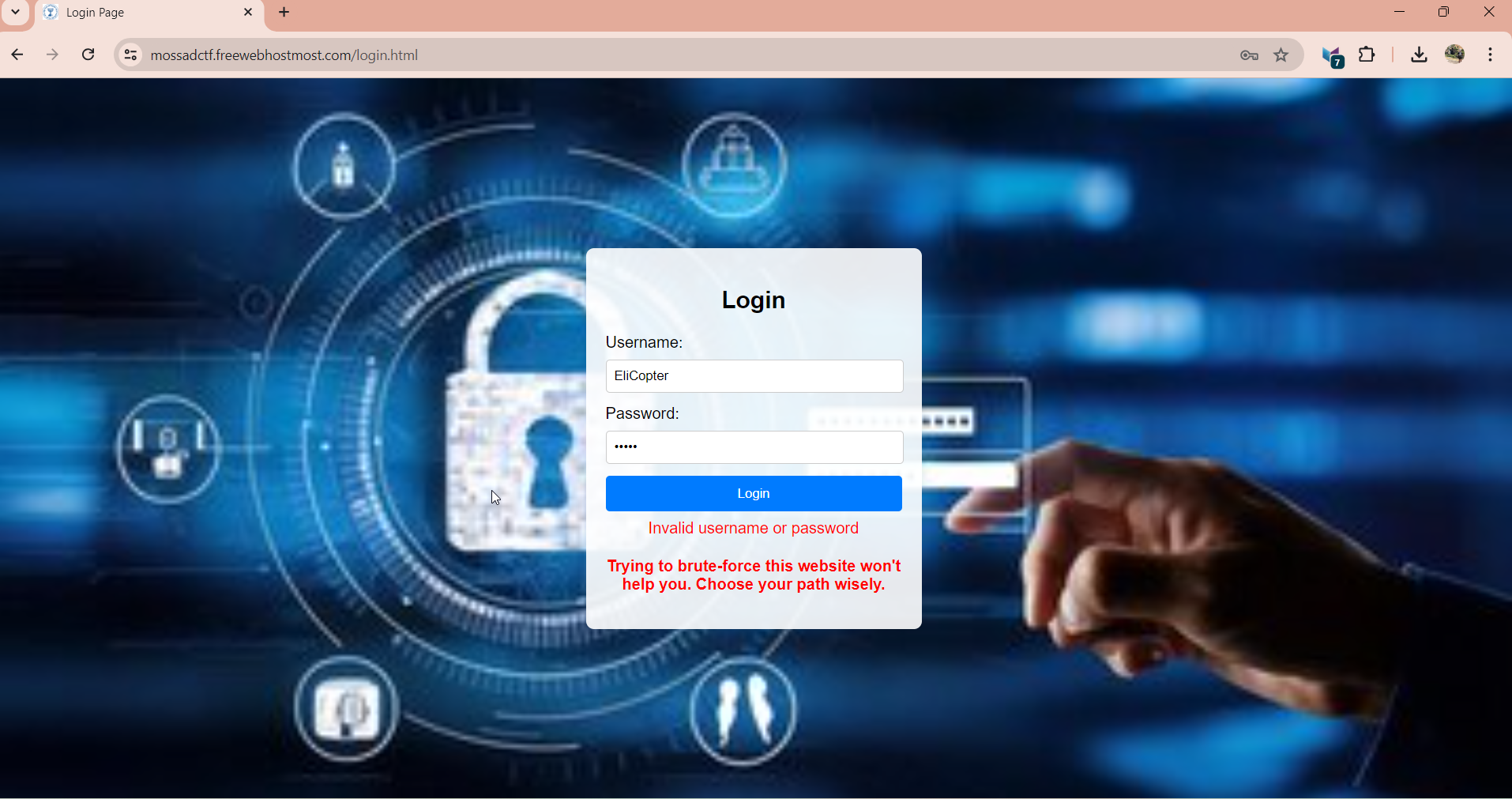
סיסמא שאותה החביא הסוכן

מה הרמזים שהוא רואה:

בשלב הראשון הוא קיבל את שם המשתמש של הסוכן, וכן איזשהוא נתון שאומר שהסוכן שכח את הסיסמא שלו.

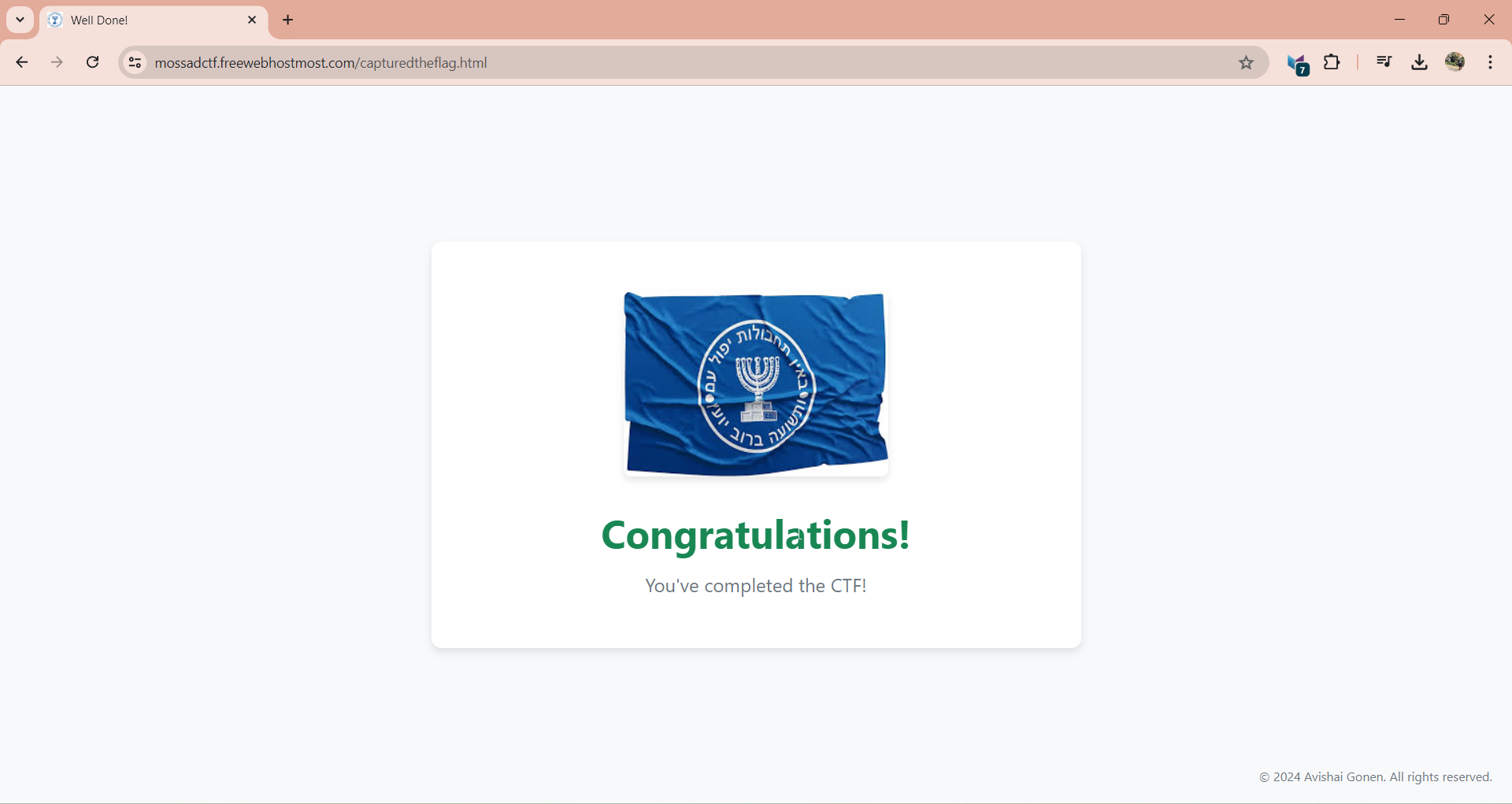
מה צריך לעשות:

יש לחזור לאתר וללחוץ על הכפתור login, שמה יש להכניס את שם המשתמש והסיסמא הנכונים.



Username: EliCopter, Password: MossadRules

מה התוצאה לשלב הבא:



**סיום ה CTF.**