בס"ד

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:

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

מה צריך לעשות:

צריך לחפש בקובץ ההסנפה שאילתות DNS שקשורות באיזשהו אופן לאתגר.

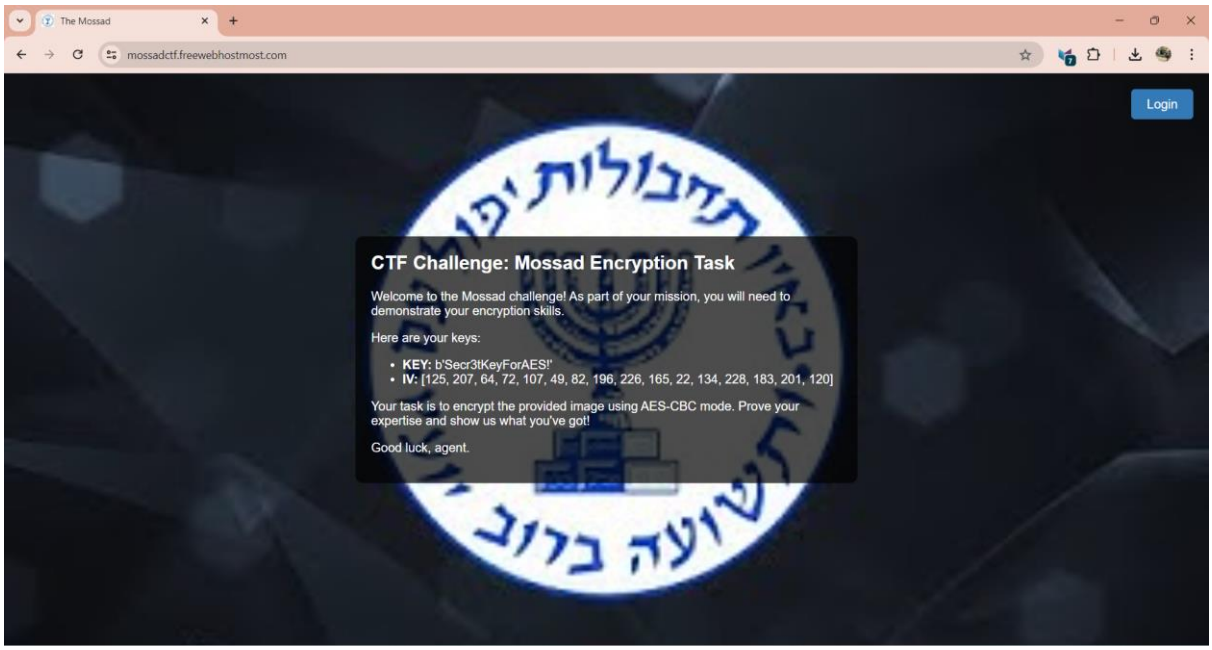
לדוגמא:

dns && frame contains "ctf"

No.	Time	Source	Destination	Protocol	Length	Info
44	16.423798	192.168.33.16	192.168.33.1	DNS	89	Standard query 0x0002 A mossadctf.freewebhostmost.com
45	16.431462	192.168.33.1	192.168.33.16	DNS	105	Standard query response 0x0002 A mossadctf.freewebhostmost.com A 34.132.146.171
46	16.438047	192.168.33.16	192.168.33.1	DNS	89	Standard query 0x0003 AAAA mossadctf.freewebhostmost.com
47	16.446401	192.168.33.1	192.168.33.16	DNS	117	Standard query response 0x0003 AAAA mossadctf.freewebhostmost.com AAAA 2600:1900:4000:e094:0:b::

לאחר מכן, יש לגלוש לדפדפן ולראות מה יש שם.

מה התוצאה לשלב הבא:



יש פה הוראות לשלב הבא.

בס"ד

שלב ב:

מה המשתמש מקבל:

המשתמש מקבל KEY, IV.

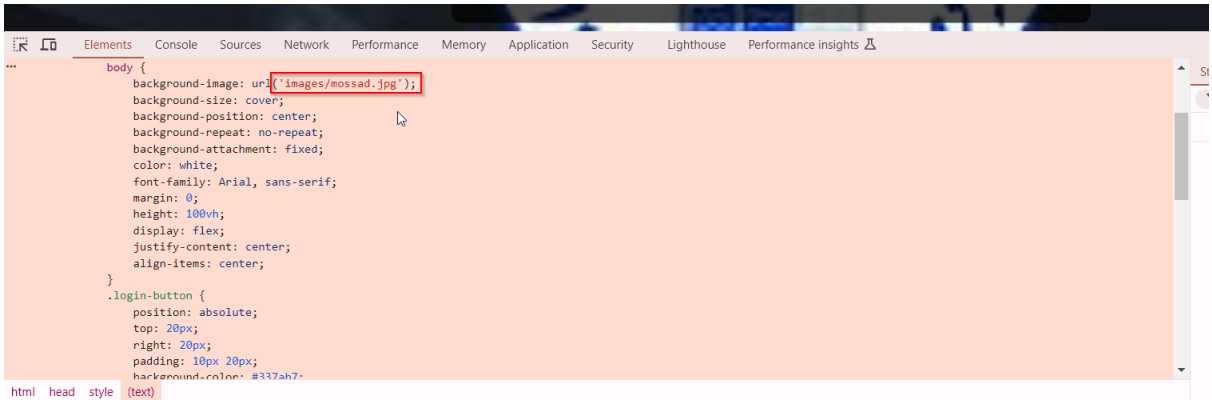
מה הרמזים שהוא רואה:

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

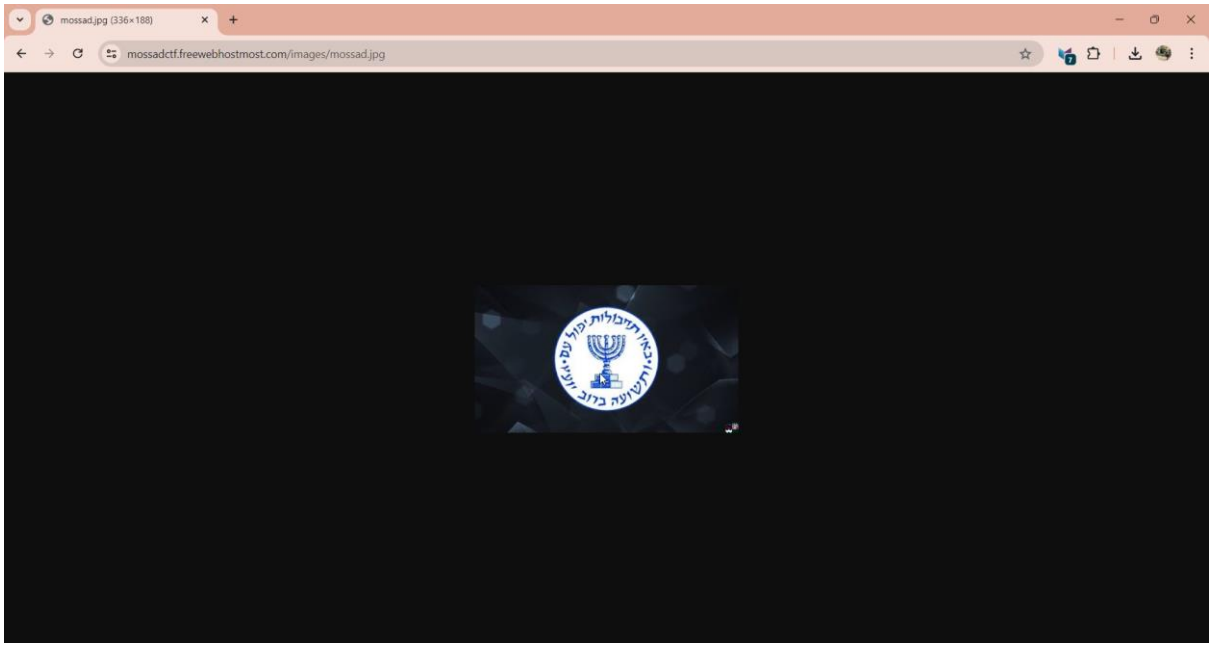
מה צריך לעשות:

על המשתמש למצוא את תמונת הרקע באופן הבא:

לעשות f12 ולמצוא את ה url אל התמונה



לגשת resource הזה ולהוריד אותו:



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.

בס"ד

<u>שלב ג:</u>

<u>מה המשתמש מקבל:</u>

קובץ בינארי כלשהוא

<u>מה הרמזים שהוא רואה:</u>

אין

<u>מה צריך לעשות:</u>

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.

<u>מה התוצאה לשלב הבא:</u>

תמונה של ראיסי, עם מסר מוחבא בפנים

בס"ד

שלב ד:

מה המשתמש מקבל:

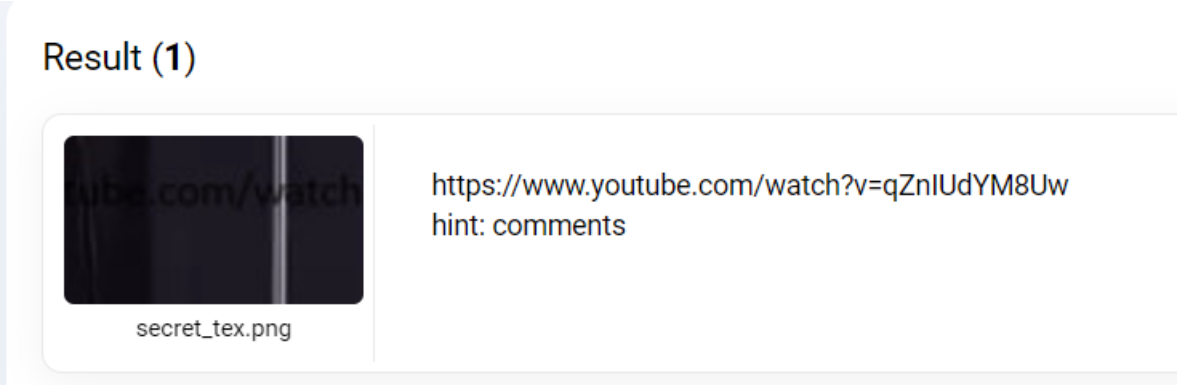
תמונה של ראיסי עם מסר מוחבא בפנים

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:

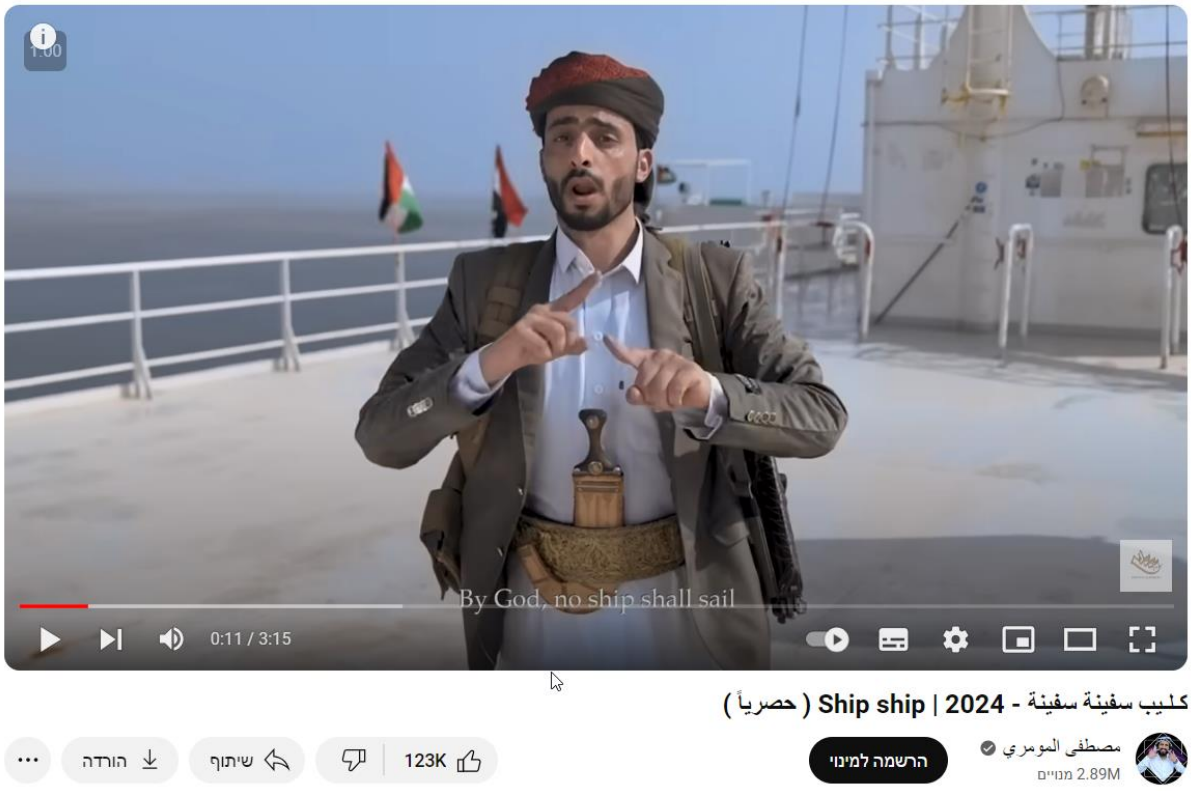
קישור לסרטון יוטיוב ובנוסף, איזשהו רמז: תגובות.

בס"ד

<u>שלב ה:</u>

<u>מה המשתמש מקבל:</u>

קישור לסרטון יוטיוב.



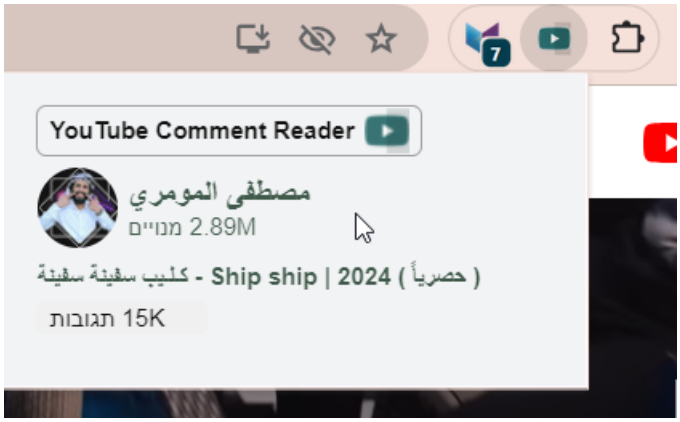
<u>מה הרמזים שהוא רואה:</u>

"תגובות". הוא קיבל רמז להסתכל בתגובות

<u>מה צריך לעשות:</u>

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

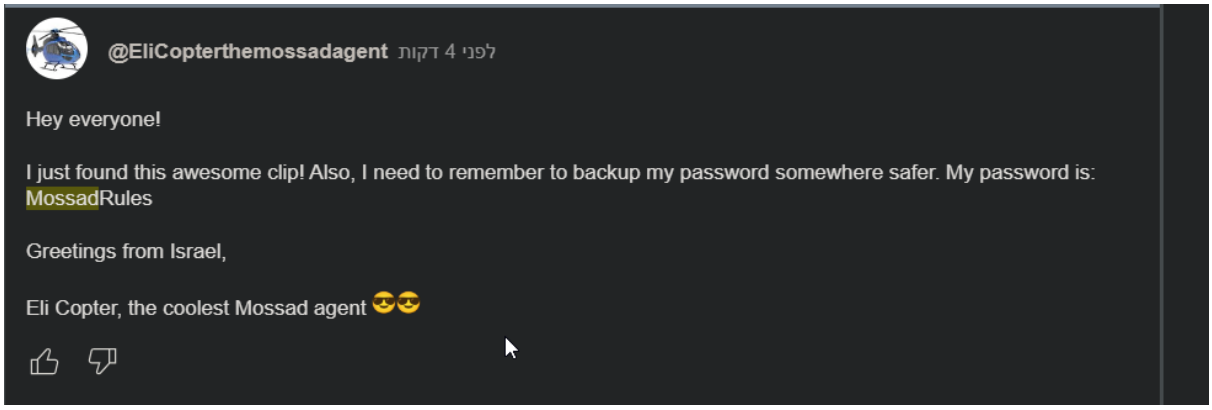
לשם כך, יש להשתמש באיזשהו כלי אוטומטי שעושה את זה, כגון התוסף הבא:
https://chromewebstore.google.com/detail/youtube-comment-reader/jbjbjeceipecokoeocnkcfjpanlipamf



בס"ד

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.



<u>מה התוצאה לשלב הבא:</u>

סיסמא שאותה החביא הסוכן, MossadRules

בס"ד

שלב ו:

מה המשתמש מקבל:

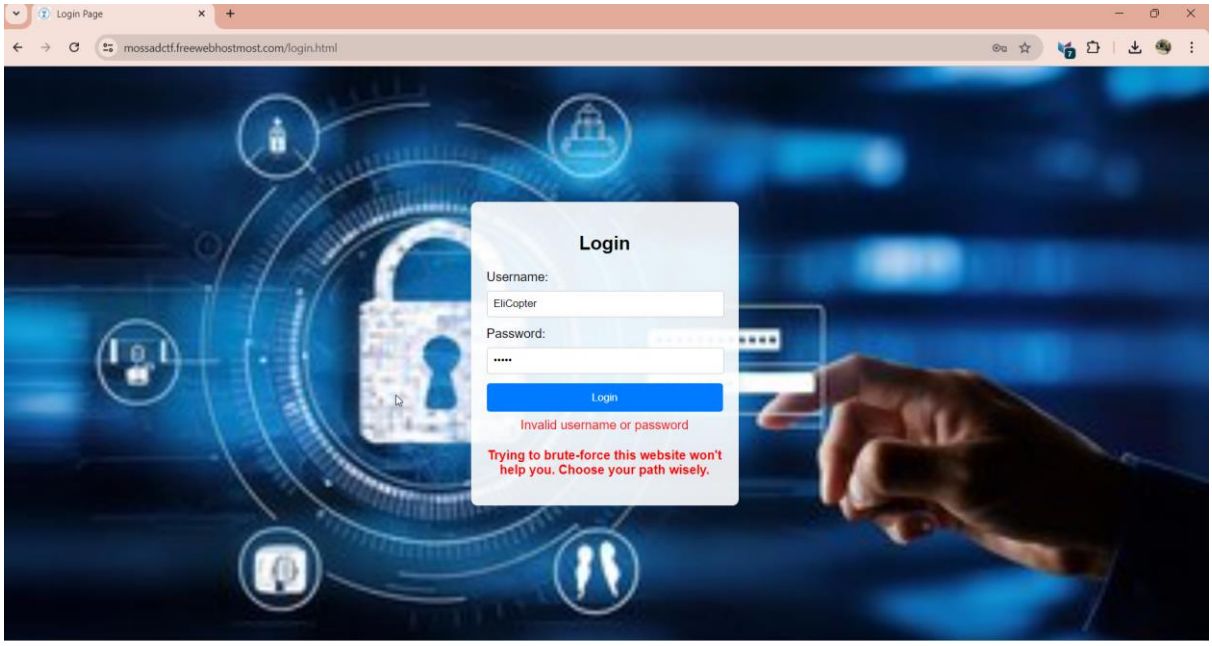
סיסמא שאותה החביא הסוכן

מה הרמזים שהוא רואה:

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

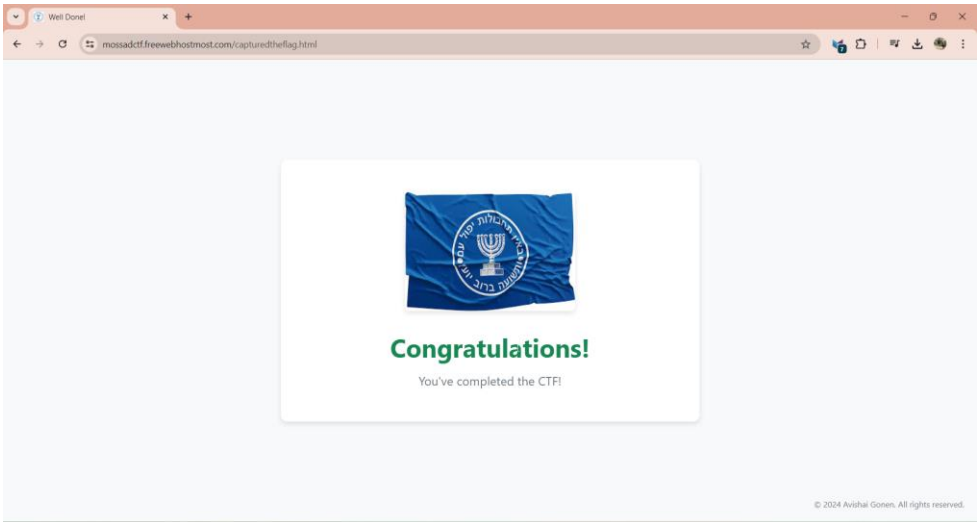
מה צריך לעשות:

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.