

## הצעת פתרון – Mossad CTF

בתור התחלה אנחנו מקבלים איזשהו סיפור, מה שניתן ללמוד מהסיפור זה שיש לנו איזשהו סוכן מוסד, אלי קופטר, ששכח את הסיסמא לאתר שלו.

כמו כן, הוא לא הצליח לגשת לאתר כי נמחקו הרשומות, לשם כך הוא ביצע שאילתת DNS למצוא את ה IP של האתר שלו.

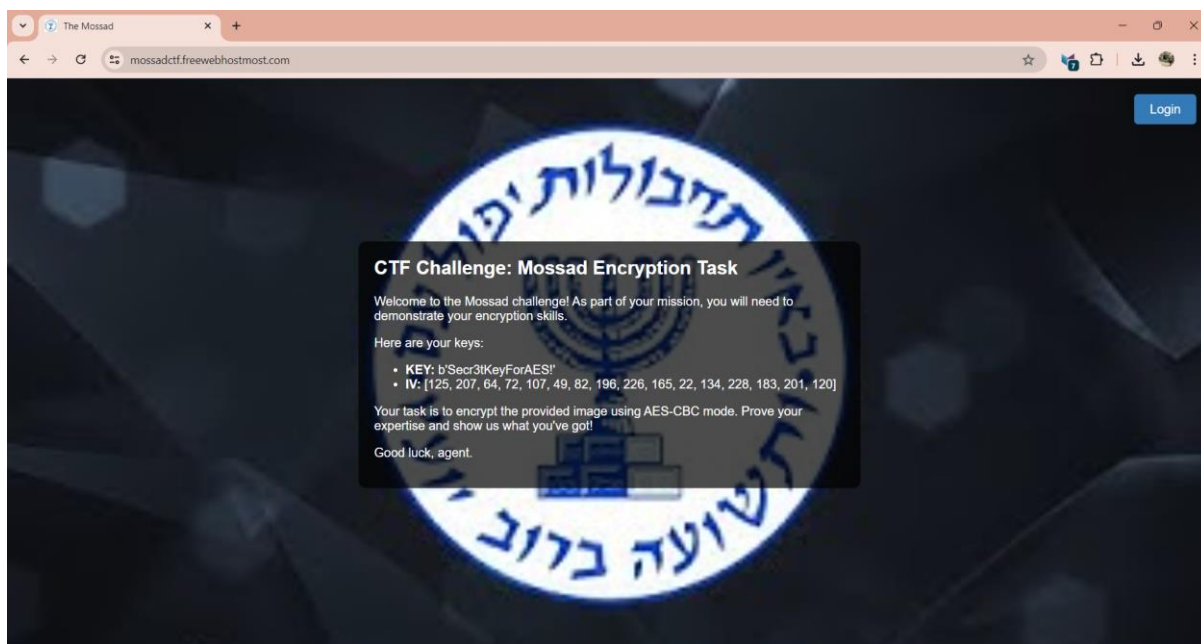
מצורף קובץ הסנפה, נחפש את שאילתת ה DNS בשביל למצוא את האתר.

אנחנו יודעים שזה איזשהו ctf שקשור למוסד, אז אולי נחפש מילות מפתח, כגון ctf או mossad

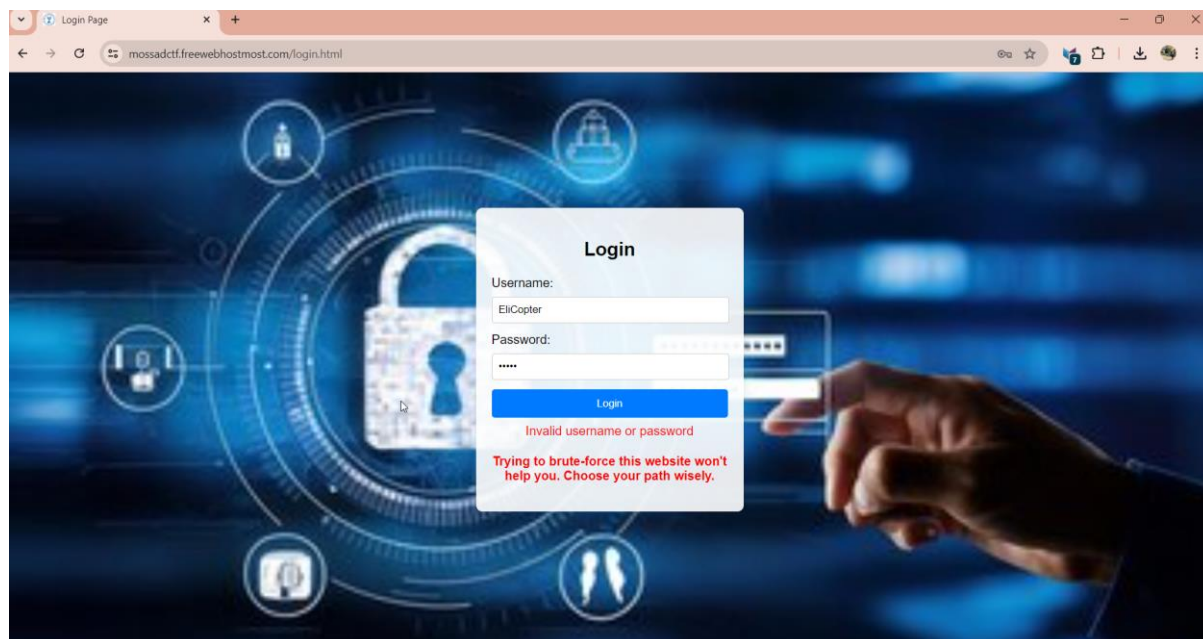
No.	Time	Source	Destination	Protocol	Length	Info
44	16.423798	192.168.33.16	192.168.33.1	DNS	89	Standard query 0x0002 A mossadctf.freewebhostmost.com
45	16.431462	192.168.33.1	192.168.33.16	DNS	105	Standard query response 0x0002 A mossadctf.freewebhostmost.com A 34.132.146.171
46	16.438047	192.168.33.16	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::

יפה! מצאנו את השאילתא ואת ה domain, אם ככה, ה domain הוא:  
mossadctf.freewebhostmost.com

ננסה לגלוש אליו בדפדפן



יפה, פה אנחנו רואים איזשהו כפתור login, בלחיצה אליו אנחנו מגיעים לאתר אחר ששם ניתן לראות שאפשר לראות שיש מקום להכניס פרטי הזדהות, וכמו כן ממליצים לנו לא לנסות brute force. אוקי.



טוב, אז ננסה לנתח את שאר הדף.

אומרים לנו פה שיש מפתח IV, וכן שמצורפת תמונה שיש להצפינה עם המפתחות האלה באלגוריתם AES-CBC.

מוזר?

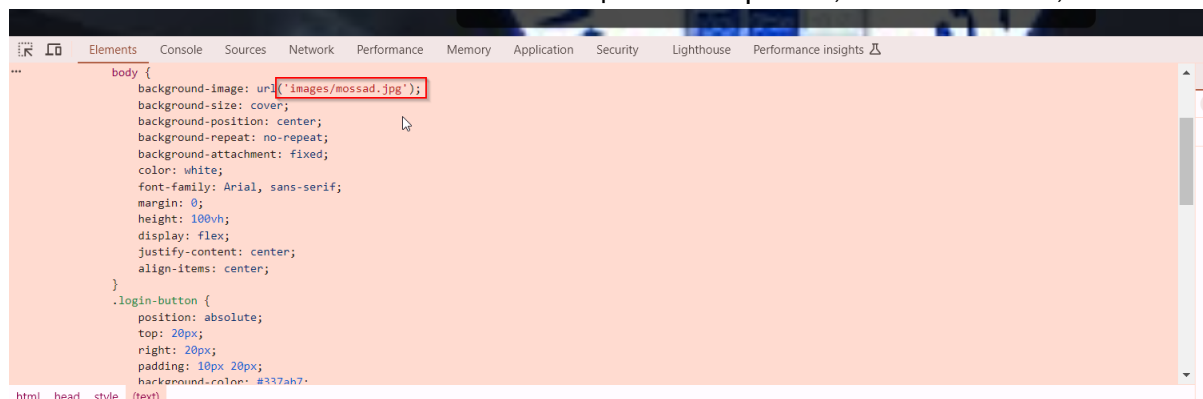
- א. על איזו תמונה מדובר?
- ב. איך הצפנה של תמונה תעזור לי?

טוב, בוא ננסה ונראה...

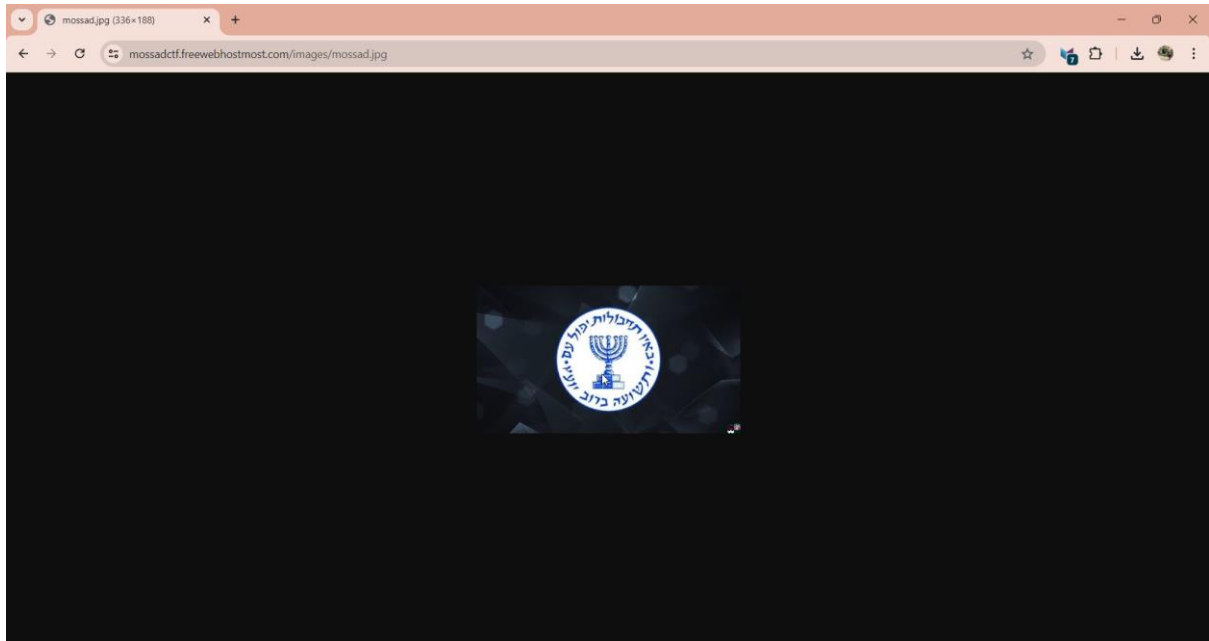
ניתנות לנו פה שתי תמונות בסה"כ, ה icon של האתר ותמונת הרקע של הדף הנוכחי.

בוא ננסה באמת להצפין את התמונה:

בתור התחלה, עלינו להוריד אותה, לשם כך נעשה inspect



וניגש ל resource הזה:



נשמור את התמונה על המחשב שלנו, ונצפין אותה באמצעות openssl.  
בתור התחלה, נכתוב script קצר שתפקידו יהיה להמיר את המפתח ו IV ל hex.

```

bytes_to_hex.py X
C: > Users > avish > solve_CTF > bytes_to_hex.py > ...
1  import binascii
2
3  # Your byte sequence
4  key = b'Secr3tKeyForAES!'
5  iv = bytes([125, 207, 64, 72, 107, 49, 82, 196, 226, 165, 22, 134, 228, 183, 201, 120])
6
7  # Convert to hex
8  key_hex = binascii.hexlify(key).decode('utf-8')
9  iv_hex = binascii.hexlify(iv).decode('utf-8')
10
11 print("Key (hex):", key_hex)
12 print("IV (hex):", iv_hex)
13
PROBLEMS 12 SERIAL MONITOR COMMENTS DEBUG CONSOLE OUTPUT TERMINAL PORTS
PS C:\Users\avish\solve_CTF> python -u "c:\Users\avish\solve_CTF\bytes_to_hex.py"
Key (hex): 5365637233744b657946667241455321
IV (hex): 7dcf40486b3152c4e2a51686e4b7c978

```

ואז, נריץ את השורה הבאה:

```

PS C:\Users\avish\solve_CTF> openssl enc -aes-128-cbc -K 5365637233544b657946667241455321 -iv 7dcf40486b3152c4e2a51686e4b7c978 -in mossad.jpg -out encryptedfile
PS C:\Users\avish\solve_CTF> ls
Directory: C:\Users\avish\solve_CTF
Mode                LastWriteTime         Length Name
----                -
-a----             7/5/2024   1:51 PM           333 bytes_to_hex.py
-a----             7/5/2024   1:52 PM        124032 encryptedfile
-a----             7/5/2024   1:47 PM        124016 mossad.jpg

```

יפה מאוד. עכשיו, כשפותחים את זה ב hex editor, יוצא ג'יבריש

```

HxD - [C:\Users\avish\solve_CTF\encryptedfile]
File Edit Search View Analysis Tools Window Help
16 Windows (ANSI) hex
encryptedfile

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 FF D8 FF FE 30 2F 00 00 00 00 00 00 00 00 00 00 00yb0/.....
00000010 06 BE 90 6A 0B 68 8A 9E 81 68 6D 82 0C 38 71 23 .%.j.hšž.hm,.8q#
00000020 78 3C A9 7B B8 83 44 A6 EA C7 FE 70 6A 52 C8 B5 x<@{,fD|êÇppjRÊµ
00000030 9A 0D D2 6B 33 F6 3A AC E5 8C 63 55 61 6F DA 98 š.Ôk3ô:~āĖcUaoŮ~
00000040 CC 5A 4F C7 24 DD 56 83 71 F7 20 49 09 A9 BD CB îZOÇ$ŸVfq÷ I.©~Ė
00000050 6B D1 76 DD 6A DE A3 78 14 B4 85 9E 06 06 FD 45 kŇvŸjBfx.'...ž..ýE
00000060 7F 19 C8 9C 3F 43 B4 EA D9 C3 7B 9D 6D B8 D5 7E ..Ėæ?C'êŮĀ{.m,Ů~
00000070 6C 0D A3 32 11 BF CB F7 06 8C D6 51 CB C9 EE E6 1.Ł2.¿Ė÷.ĖŖŖĖĖiæ
00000080 AF 69 70 6B 6C B8 3A 64 8E D4 E2 A3 B8 F7 C3 19 ĩpkł,:džŖāŁ,÷.Ā.
00000090 8E 99 FC 31 52 20 7D 6D 01 85 09 BA 4D 31 FF 05 ž~ulR }m.....°MlŸ.
000000A0 45 03 C1 87 EE A6 FE 18 5F 91 39 EC CF 49 A0 2E E.Ā+î|p._'9iĪI .
000000B0 71 BF 23 AA 1E A2 CB 86 6B 1D CE 06 80 0A 8E 8E q¿#°.ēĖ+k.Ī.ē.žž
000000C0 0C C1 14 D5 E3 9A 7B C0 09 B7 CA E8 9B 89 FC 7E .Ā.Ŗās{Ā.·Ėè»ũ~
000000D0 7A AD 39 CE A8 59 D3 B3 A8 D5 96 41 7C 85 7C 80 z.9Ī''YŖ''Ŗ-Ā|...|ē
000000E0 91 BB F9 15 1D 30 1D DA E6 36 F4 BF 65 DF CA F5 '»ù..Ŗ.ŮæŖŖēēēēēē
000000F0 BC 0E ED 03 4B C7 E7 18 F3 71 84 88 48 41 71 FB Ÿ.i.KÇÇ.Ŗq„^ĤAqŮ
00000100 78 8A 8C 79 DD 2C 5C CB 62 7F 6E 61 9A 36 9F F9 xšŖyŸ,\Ėb.naşŖŸù
00000110 E4 C7 69 87 32 97 AC CF 6D 2C F7 2A 92 5B C7 16 āÇi÷2—Īm,÷*' [Ç.
00000120 80 2B D4 D7 50 E1 90 F9 69 E0 A7 D3 C1 3D 9D 3A ē+Ŗ×Pā.ùiašŖĀ=. :
00000130 B1 B2 C5 2C 0B C9 67 25 DA 62 D1 16 52 C1 23 D6 ±'Ā,.Ėg%ŮbŇ.RĀ#Ŗ
00000140 53 E0 9E A4 EF 9A 2D 9E F4 7E A5 C7 B1 C2 4F 2A Sāžxīš-žŖ~ŸÇ±ĀŖ*
00000150 27 C5 34 84 C2 20 54 0E 3F 1E A1 91 79 3D 54 D6 'Ā4„Ā T.?.; 'y=TŖŖ
00000160 31 57 8D E8 18 6F F6 13 34 88 34 62 EF 03 F6 6D lW.ē.ŖŖ.4^4bi.Ŗm
00000170 27 DC F6 1A 8E E4 05 5C 61 CC 83 30 92 8C E8 33 'ŮŖ.žā.\aĪfŖ'Ŗē3
00000180 C5 1C 9A AC 50 AB CD B1 5C 20 17 98 77 A9 80 DC Ā.š~P«Ī±\ .~wŖŖŮ
00000190 2C 7A 57 03 C9 4D 2F CF E3 48 53 D2 49 27 D9 0C ,zW.ĖM/ĪāHSŖŖI'Ů.
000001A0 61 8F 49 78 83 2F CD 5A 23 E8 2E 04 7B 54 FE 76 a.Ixf/Īž#è...{TpŸ
000001B0 6F 50 17 98 70 75 36 35 09 F6 5F 70 08 10 01 25 ŖP."pu65.Ŗ_p...%
000001C0 BE CB CE 09 13 15 11 7B D8 5B 27 0C 66 28 40 52 %ĖĪ....{Ŗ['.f(ŖR
000001D0 D2 E8 94 D7 58 5E 5A E9 CC D5 3F 44 2B 4E 48 47 Ŗè~"X^žēĪŖŖ?D+NHG

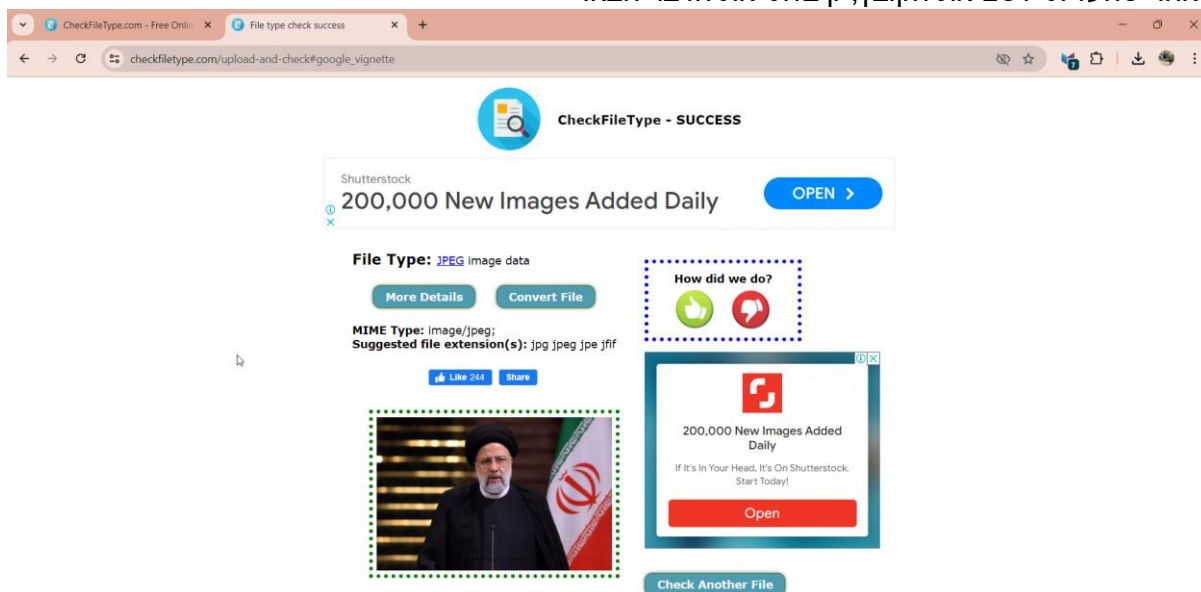
```

אולם, בוא ננסה את מזלנו ונעלה את זה למזהה פורמטים אינטרנטי חינוכי, אולי יהיה לנו מזל ונזכה לגלות משהו.

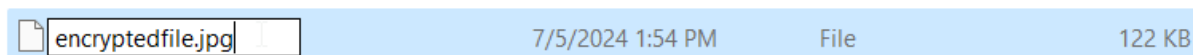
אני השתמשתי באתר הבא: <https://www.checkfiletype.com>



לאחר שהעליתי לשם את הקובץ, קיבלתי את הדבר הבא:



וואו! יצאה לנו תמונה! בוא ננסה להמיר את הקובץ במחשב שלנו ל .jpg, ולראות מה יצא:



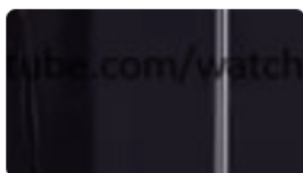
במבט ראשוני התמונה נראית סתם תמונה משעממת, אלא שאם מסתכלים טוב, אפשר לראות שיש משהו שמסתתר למטה.



יש פה איזשהו טקסט, ננסה לפענח מה בדיוק רשום שם, נשמור רק את החלק הזה בתור תמונה חדשה, ונעלה לאתר שידוע לפענח text מתוך תמונות, <https://www.imagetotext.info>.

זה מה שהתקבל:

## Result (1)



secret\_tex.png

<https://www.youtube.com/watch?v=qZnIUdYM8Uw>  
hint: comments

קישור לסרטון יוטיוב ובנוסף, איזשהו רמז: תגובות.

ניגש לסרטון היוטיוב הזה



كليب سفينة سفينة - 2024 | Ship ship ( حصرياً )

... הורדה ⬇️ שיתוף ↻ 123K

הרשמה למיני

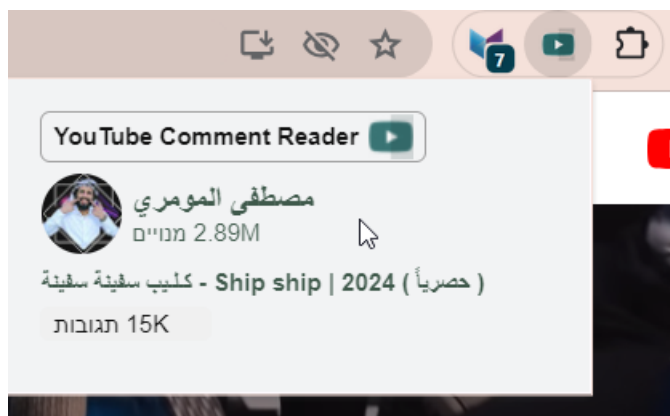
مصطفى المومري  
2.89M מנויים

או אה, סרטון מעניין:

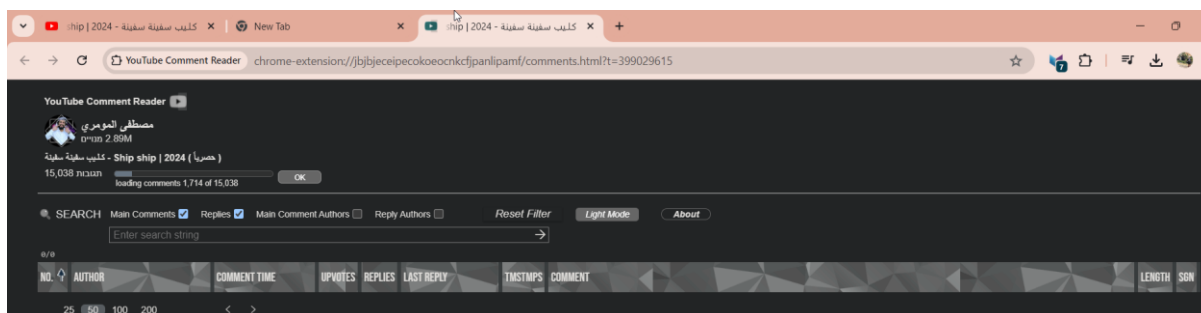
בכל מקרה, אנחנו באנו ל CTF! הרמז שקיבלנו הוא תגובות. יכול להיות שמישהו החביא משהו בתגובות?

כיוון שיש פה מעל ל 15 אלף תגובות, אנחנו נצטרך להשתמש בכלי שיעזור לנו לנתח את התגובות. נשתמש בתוסף שמישהו הכין ל chrome:

<https://chromewebstore.google.com/detail/youtube-comment-reader/jbjbjeceipocokoeocnkcjfpanlipamf>

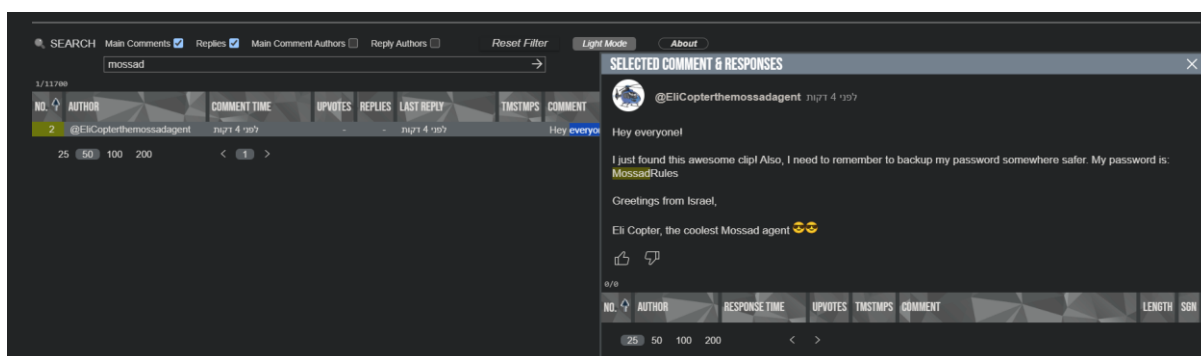


בלחיצה על התוסף אפשר לעבור לדף אחר שבו ננתח את התגובות:

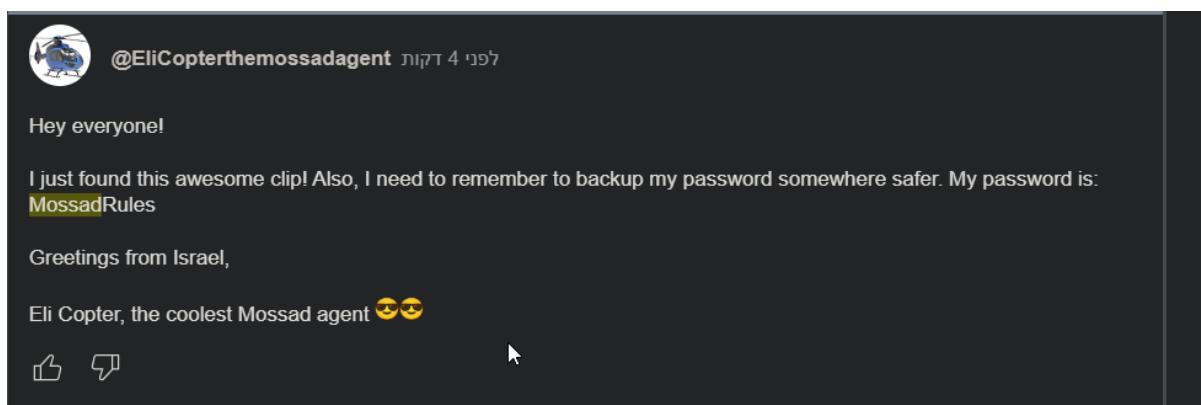


ייקח קצת זמן לכל התגובות להיטען, נחכה שהם יסיימו להיטען ואז ננסה למצוא את התגובה שהחביאו עבורנו. אחרי הכל, הרמז זה תגובות.

בוא ניזכר, מה שאנחנו מחפשים זה משהו שקשור ל EliCopter, סוכן המוסד שלנו, שמהסיפור למדנו שהוא שמר את הסיסמא איפשהו ושכח איפה בדיוק. אם כך, אולי נוכל לחפש באמצעות מילות מפתח, לדוגמא, :mossad



וואו! מה מצאנו!



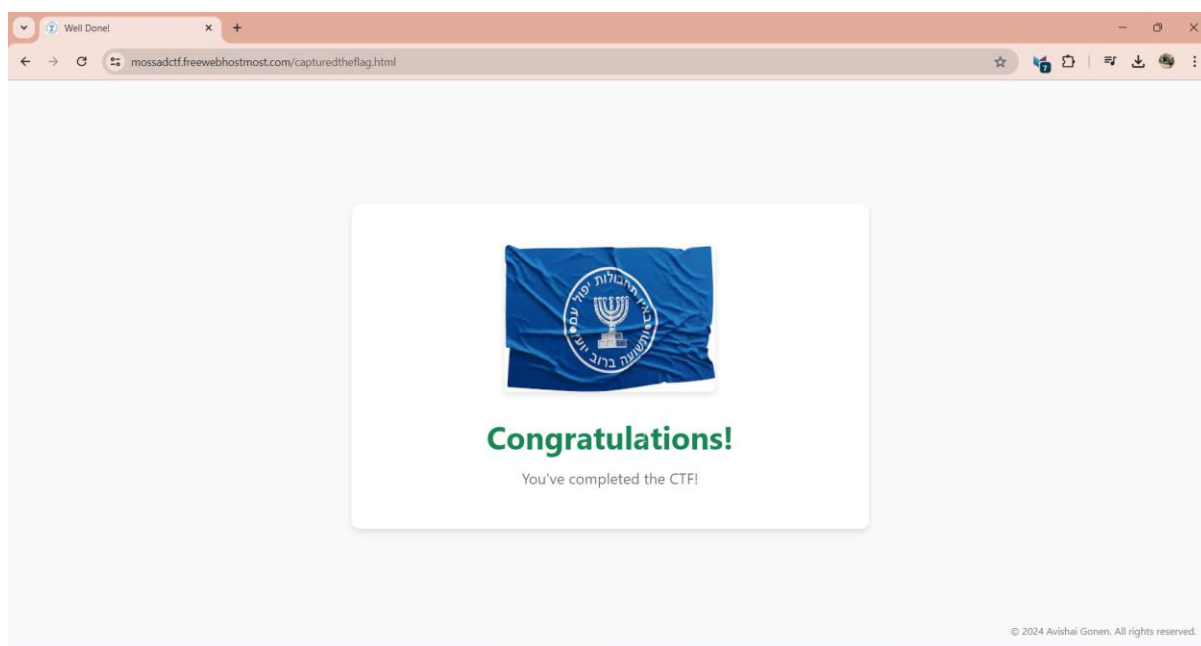
גילינו מה הסיסמא!

MossadRules

בוא נחזור לאתר מההתחלה, ונכניס את הפרטים הבאים:

Username: EliCopter

Password: MossadRules



וזוהו! סיימנו את ה CTF!!