**התקפה שלב 1- פתרון:**

נכנסים לאתר:

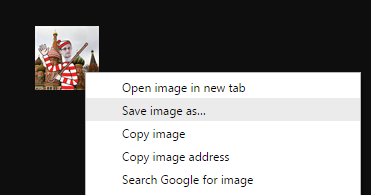
<http://cybersnowdenchallenge.azurewebsites.net/>

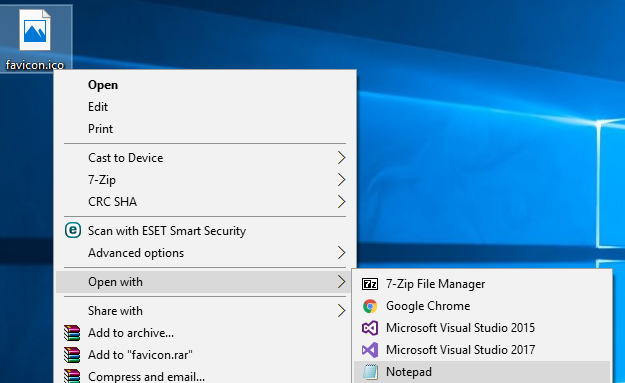
זהו מסך הראשי של האתר, כל כמה שניות התמונה מהבהבת, והיא בעצם ה favicon בגדול יותר וזה נותן רמז שצריך לפנות לfavicon.

נכנסים לfavicon דרך :

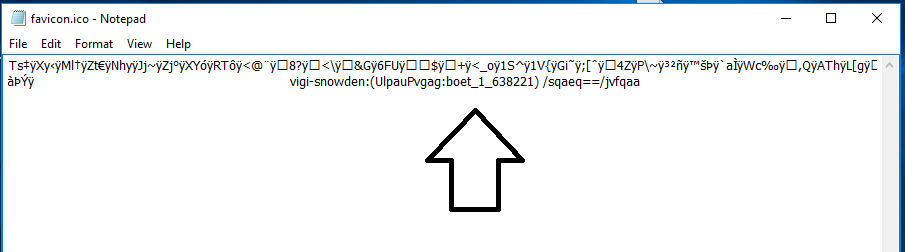
<http://cybersnowdenchallenge.azurewebsites.net/favicon.ico>

ורואים את האייקון. מורידים אותו, ופותחים את האייקון ב TEXT EDITOR.





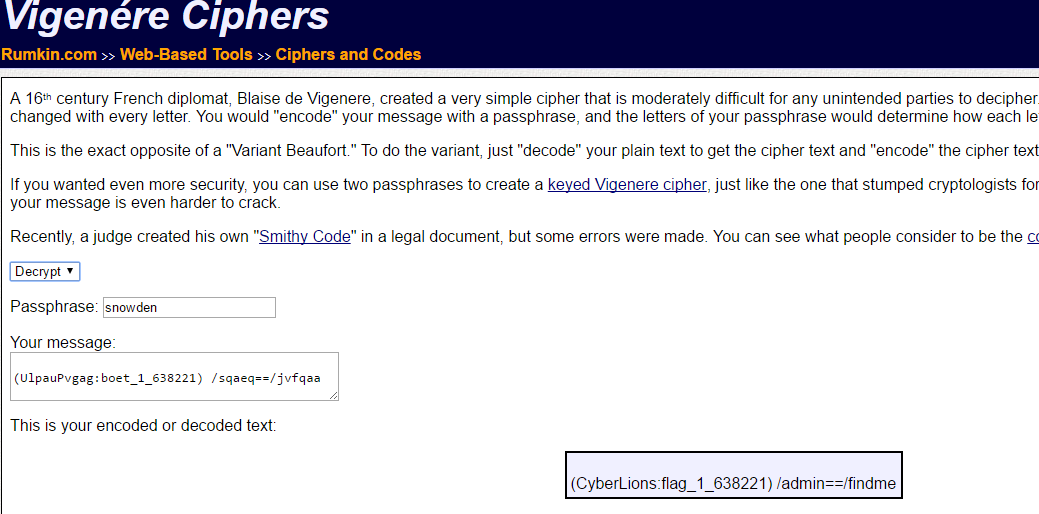
ומקבלים את הקובץ ובסוף יש קטע נמצא הצופן:



נכנסים לאתר:

http://rumkin.com/tools/cipher/vigenere.php

ומפענחים:

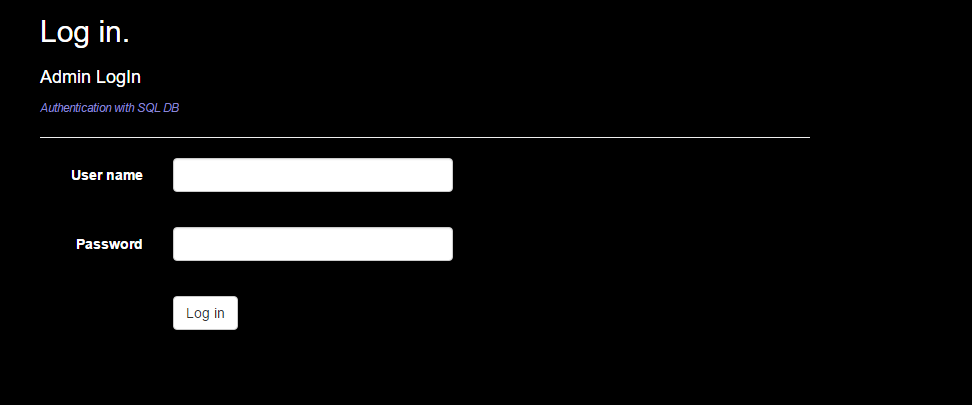


קיבלנו שני דברים.

1. את הפלאג הראשון באתגר.
2. רמז לגבי ההמשך, להיכן צריך לגשת בכתובת:

<http://cybersnowdenchallenge.azurewebsites.net/findme>

כאשר נכנסים לדף ההתחברות לאדמין ניתן לראות :

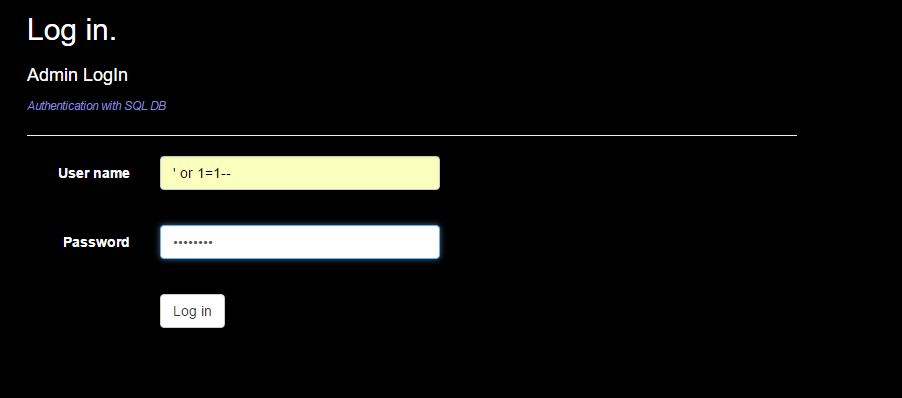


קיים רמז שההתחברות מתבצעת בעזרת SQL DB, אשר מעיד שנשתמש ב SQL INJECTION

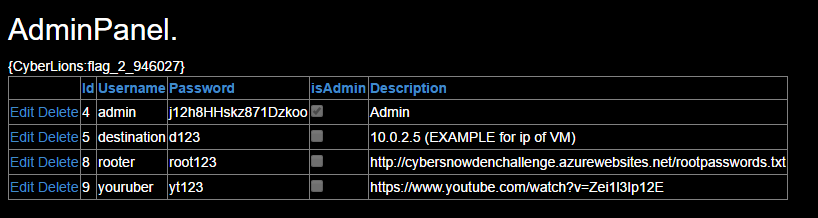
נרשום את הפקודה בשם משתמש:

‘ or 1=1--

אשר תגרום לשאילתה תמיד להיות חיובית, ולא להתייחס בכלל לשם משתמש או הססמא האמיתיים שצריכים להיות לאדמין ובכך נעקוף את ההתחברות לפאנל אדמין.



לאחר שנתחבר, נגיע לפאנל האדמין נוכל להסתכל על הטבלה שמכילה את ה"משתמשים" של המערכת:



כל משתמש מחזיק רמז להמשך האתגר ובעזרתם מתקדמים.

ובנוסף, קיבלנו את הפלאג השני שלנו.

**הערה חשובה:**

הIP מדמה את הIP של המכונה הוירטואלית שלנו.

ז"א יש להשתמש בIP של המכונה הוירטואלית המגנה שהקמת ,

ניתן לדעת מה הIP ע"י שימוש בפקודה ifconfig בתוך המכונה המגינה.