תרגיל פיתוח מגשימים **2024**

שלב 1 – פיתוח **WEB**

אתה מפתח Full stack העובד במוסד.

בידיעת מודיעין שהגיעה זה עתה התברר כי מספר קבוצות תקיפה מתכננות לבצע מתקפת סייבר רחבה על ישראל תוך ניצול חולשה באפליקציית Office.

על מנת להגן מפני המתקפה עליכם לעזור למוסד למצוא מידע אודות המתקפה וכיצד ניתן להגן עליה.

מטרתך הינה לכתוב אפליקציית WEB אשר תעזור לאנשי המודיעין בזיהוי המתקפות הפוטנציאליות שבהן ישתמש התוקף והצגת דרך ההתגוננות.

הדרישות עבור אפליקציית הWEB הינן:

1. נדרש לבנות את שרת Frontend באמצעות React ואת שרת ה-Backend באמצעות NodeJS\Python (מומלץ להשתמש גם ב-expressJS)
2. ניתן להוריד את הקבצים עם המידע מהנתיב הבא:
https://github.com/mitre/cti/tree/master/enterprise-attack/attack-pattern
3. כתיבת התוכן של הקבצים במסד נתונים לבחירתך.
   a. המסד צריך להכיל את הנתונים הבאים:
      i. Name – שם המתקפה
      ii. Description – תיאור המתקפה
      iii. Id – מזהה ייחודי למתקפה
      iv. x_mitre_platforms – מערכות פגיעות
      v. x_mitre_detection – דרכי זיהוי
      vi. phase_name – שלב המתקפה
   b. במידה וחסרים נתונים ניתן להציג ערך NA

ג. עם פתיחת האפליקציה יוצגו המתקפות בצורת רשימה או Grid

ד. האפליקציה צריכה לאפשר חיפוש לפי מילות מפתח ב-Description לדוגמא להחזיר את כל המתקפות שמדברות על DLL

ה. ניתן להשתמש בספריות צד שלישי במידת הצורך

ו. בונוס 1 – אתר מעוצב, חדשני, חשיבה מחוץ לקופסא ופיצ'רים נוספים

ז. בונוס 2 – הצגת קשרים בין טכניקות שונות

שלב 2 – סייבר-בוט

לאחר בניית האפליקציה איש מודיעין הסייבר הבין כי הוא לא עומד בעומס התקיפות והחליט לבקש עזרה.

במשימה זו מטרתך ליצור סייבר-בוט אשר יעזור לאיש המודיעין בביצוע המשימות שלו, על הבוט לעבוד בתצורת צ'ט ולקבל פקודות מהמשתמש.

על הבוט לתמוך לכל הפחות בפקודות הבאות:

- ביצוע חיפוש בDB של האתר והחזרת תוצאות
- ביצוע שאילתות מול מאגר חיצוני (דוגמת VIRUSTOTAL) והחזרת תוצאות – לדוגמא: Check the md5 xxxxxx – הבוט יחזיר האם החתימה מוכרת כזדונית ב-Virustotal

בונוס: ניתוח שפה טבעית ותמיכה פקודות נוספות

שלב 3 – חקירות

באמצעות הבוט לאיש המודיעין התפנה זמן רב ביומן ולכן החליט לבצע חקירות של קבצים באופן עצמאי.

לצורך החקירות ביצע התקנה של מערכת sandbox אבל נתקל בבעיה.

מטרתך במשימה זו היא לעזור לאיש המודיעין להתקין מערכת sandbox (מערכת לחקירת קבצים מומלץ לחפש פתרונות קוד פתוח ב-GITHUB או להשתמש בפתרון עננ). לצורך ההתקנה ניתן להשתמש במכונה וירטואלית.

לאחר ההתקנה עלייך להוסיף לבוט תמיכה בפקודות API מול מערכת ה- sandbox שיצרת. לדוגמא העלת קובץ מהאתר, שאילתא עבור קובץ מסוים וכו.

בונוס: הצגת תוצאות החקירה באופן ויזואלי באפליקציה

דגשים לביצוע התרגיל

כתוב מסמך תיעוד מפורט של הקוד.
במסמך תן דגש על ההנחיות הרשומות מטה וצילומי מסך.

- הסבר מדוע בחרת לפעול בצורה שבחרת ולא בצורה אחרת.
המסמך במידה רבה חשוב יותר מהתרגיל – תשקיע בו.
- הקוד צריך להיות מחולק באופן הגיוני, תאר את החלוקה שביצעת
- במסמך חשוב להציג את ארכיטקטורת המערכת ולפרט את הנושאים הבאים:
  - כיצד כתבת את הנתונים למסד הנתונים
  - כיצד הנתונים נשלפים
  - כיצד המידע מוצג למשתמש
- תאר את הטכנולוגיות/תוכנות צד שלישי שבהן השתמשת ומדוע בחרת להשתמש בהן
- הוסף צילומי מסך של האפליקציה וכיצד עוזרת לאיש המודיעין לאתר את המתקפה אשר קיבל בדו"ח

<u>שאלות נוספות</u>

1. ספר לנו על אתגר שהיה לך בתרגיל ואיך התמודדת איתו
2. האם נהנית מבניית האפליקציה? מאיזה חלק יותר/פחות?
3. האם היית משנה משהו? שימוש בשפות אחרות? מבנה הצגה שונה?

בסיום האתגר, נדרש לשלוח מייל חזרה למייל הזה (**rafaelsninjas@gmail.com**) עם הנושא "**finished**" ועם קובץ **ZIP** <u>אחד</u> אשר מכיל:

- קוד הפרויקט
- מסמך תיעוד של הקוד (שכולל מענה לשאלות הרשומות בתרגיל הרטוב)
- מענה על השאלות הרשומות מעלה.
- סרטון וידאו של עד כ-2 דק המציג כל אחד מהשלבים שפתרת
- נא לתת הרשאות לקישור לכתובת המייל **rafaelsninjas@gmail.com** - ללא הרשאות התרגיל לא ייבדק
- את הפתרון יש לשלוח עד לתאריך 5.10.24 בשעה 23:59 לא יתקבלו פתרונות לאחר מועד זה
- צילום תעודת זהות כולל ספח (למי שיש תעודה ביומטרית נדרש לצלם אותה משני הצדדים)

* המסמך כתוב בלשון זכר אך פונה שכל המינים

בהצלחה!