מיני פרויקט בהגנת רשתות – תיעוד העבודה:

בן דהן 305633786

אבלינה ברסטוביצקי 316720028

**מבוא :**

במיני פרויקט שלנו רצינו לבנות כלי הגנה אשר מטרתו תהיה לסרוק קובץ אשר אותו המשתמש מתכוון להוריד ולהתריע האם הוא בעל נוֹזְקָה.

כלי ההגנה שלנו מורכב ממנהל הורדות שכתבנו כתוסף של Google Chrome בשפת JavaScript, שרת Python מסוג Flask שנמצא בענן של heroku ועושה שימוש ב-API של VirusTotal.

**שימוש:**

* לפני שהמשתמש שמוריד קובץ מהרשת הוא יכול להבחור ללחוץ קליק ימני על הקובץ המבוקש ולבחור באופציה של Safe Download באמצעות מנהל ההורדות.
* במידה והקובץ המבוקש מכיל שני נתיבי הורדה (לדוגמא: תמונה שמכילה לינק להורדת התמונה או לדף בה היא מוצגת) התוסף יציג שאלה למשתמש איזה נתיב הוא מעוניין להוריד.
* במידה והמשתמש בוחר באפשרות של הורדה בטוחה מנהל ההורדות יבצע בקשת XMLhttprequest על מנת לקבל את הקידוד של הקובץ ולשלוח אותו לשרת כאובייקט מסוג blob, שם נבנה הקובץ ונשלח לסריקה על ידי VirusTotal.
* VirusTotal מחזיר תוצאות סריקה לשרת שלפיהן מחזיר סטטוס למנהל ההורדות שמצג למשתמש את תוצאות התהליך.
* לאחר קבלת תשובה המשתמש יקבל התראה האם הקובץ עבר את הסריקה בהצלחה, במידה וכן והקובץ ירד אל תיקיית ההורדות, ובנוסף תהיה למשתמש אפשרות לצפות בסריקה ע"י לחיצה על כפתור Go to scan ולהחליט אם להשתמש באפשרות Download anyway לאחר הצפיה.

**דרך העבודה שלנו :**

בתחילת הדרך התלבטנו האם לבנות כלי הגנה עבור שרת מייל ואחרי זה החלטנו שיהיה מעניין לבנות תוסף לכרום – מנהל ההורדות. התחלנו לחשוב איך היינו רוצים לסרוק את הקבצים וחשבנו תחילה על הרצה בסביבה וירטואלית. התחלנו לקרוא וגילינו כלי בשם cuckoo sandbox אשר משמש סביבה לביצוע אמולציה של קבצים בכדי לזהות האם קיימת בהם נוזקה.

התחלנו לכתוב את מנהל ההורדות, שם נעזרנו ב-API של גוגל ובתוספות של jQuery, לפעמים התקשינו להשתמש באפשרויות שכרום מספק לצרכים שלנו ואז עמדנו בפנינו שתי אפשרויות, לפתור את הקשיים בצורה קצת יצירתית תוך כדי שימוש במחלקות הכתובות של chrome או להשתמש בתוספות של jQuery.

במקביל לבניית התוסף הרמנו את השרת לקבלה ושמירה של קבצים, קושי מסויים שנתקלנו בו היה לזהות את הסיומת של הקובץ מתוך הקידוד על מנת לדעת מה סוג הקובץ בשרת, בסופו של דבר כתבנו קובץ json ששימש כטבלת האש המפענחת mimetype של קובץ לסיומת הנדרשת. הממשק של Flask היה נוח לשימוש ואפשר לנו באופן מיידי לבדוק את העבודה שלנו על התוסף.

כאשר סיימנו לבנות את התוסף, העלנו את השרת ל-Herokuapp.com וחשבנו איך לחבר אליו את ה-sandbox, ככל שקראנו יותר הבנו שלא נוכל לעשות זאת מבלי לשלם כסף מכיוון שההרשאות ומקום האחסון שקיבלנו באופן חינמי לא אפשרו זאת, בדקנו אפשרות לעשות זאת בענן אחר אבל נתקלנו באותן המגבלות. התחלנו לחפש דרך חלופית לסריקת הקבצים והחלטנו להעלות אותם מהשרת לסריקה ב-VirusTotal.

ניתן להרשם לאתר בחינם ולקבל apikey שמאפשר גישה ל-API של האתר דרך הקוד שלנו. בעיה שנגרמה ע"י שימוש בדרך זו היא הגבלה של מספר הגישות לאתר בדקה, מכיוון שנרשמו בהרשמה חינמית אנחנו ניתנת לנו האפשרות לבצע רק 4 גישות לאתר בדקה דרך ה- API, לכן לאחר העלאה של הקובץ לסריקה יש אפשרות לבצע באותה דקה רק 3 גישות על מנת לבדוק אם הסריקה הסתיימה, מה שאומר שבין כל שתי גישות עלינו להמתין כ-15 שניות, דבר שגרם להמתנה ממושכת להורדה, יש לציין כי פנינו למרצה האחראי על הפרויקט בעניין זה ונאמר לנו שאין זו בעיה הפוגעת באיכות העבודה. ברור כי עבור גישת בתשלום יכולנו לבצע מספר גישות בלתי מוגבל לאתר ולכן לקבל את הסריקה ברגע שהיא מוכנה.

בסופו של דבר נאלצנו להיאבק בעוד מספר קשיים עבור מקרי חריגים כמו ניתוק של התקשורת עם השרת או בעיה בהעברת הקבצים, לעיתים הקובץ שרצינו להעביר לשרת נחסם ע"י גישת הגנה קודמת ברמת האינטרנט ורצינו לדעת לנתר זאת, לעיתים קישור שכביכול קיים לו Url היה מסתמן כניתן להורדה בטוחה אך בעצם הוא רק הפעיל אנימציה מסויימת באתר. טיפלנו בבעיות אלו ע"י חלוקה למקרים ובדיקה של התקשורת עם השרת.

לבסוף יש לציין שהתוכנית נבדקה על קבצים ספציפיים הידועים כנוזקה ונמצא כי היא מזהה אותם, וכמובן גם על קבצים שלא מכילים נוזקה כלל שעברו את הסריקה בהצלחה.

**תיקיית העבודה מכילה את הקבצים הבאים:**

1. תיקיית Safe Download Manager המכילה:

* Readme.md
* Background.backl.html
* Background.html
* Jquery.js
* Jquery\_ui.js
* Main.js – **המימוש של התוסף עצמו**
* Manifest.json

1. תיקיית Server המכילה:

* Procfile
* Main.py
* mimeToExt.json
* mimeToExt.py
* mimeToExt.pyc
* requirements.txt

1. תיעוד העבודה שנכתב במלואו תוך כדי ולאחר סיום העבודה.
2. אפיון העבודה שהוגש בהתחלה.
3. רשימה של הקבצים שעליהם נבדק התוסף.

* לצורכי נוחות מצורפות שתי גרסאות של הקוד, גרסה אחת עבור הרצה של התוסף עם השרת ב-Herokuapp.com וגרסה נוספת עבור הרצה לוקלית של השרת.