תוכנית העבודה :

1. מסמך אפיון :

**מטרת התוסף:** למנוע ממשתמש להוריד קובץ בעל **נוֹזְקָה** .

**כתיבת תרחישים ( Test Cases ):**

נבדוק את התוכנה ע"י הורדת קבצים הידועים כ –malware מהמקור:

https://github.com/rshipp/awesome-malware-analysis#malware-collection

**מי משתמש בתוכנה -קהל יעד:** מיועד עבור כל משתמש שרוצה להוריד קובץ ( כגון: סרט ,שיר , תמונה , מסמך doc וכו') דרך דפדפן של כרום .

מתאים עבור כל משתמש בעל בסיסי בשימוש של דפדפן כרום.

**תרשים**

אתר אינטרנט המכיל קובץ הורדה

תוסף בכרום

מחשב של משתמש

שרת פייטון ב-heroku

SandBox

1. משתמש שהתוסף קיים אצלו בגוגל chrome רוצה להוריד קובץ.
2. לחיצה על עכבר ימני תיתן למשתמש לו את האפשרות לסמן safe download.
3. לאחר הלחיצה התוסף יקבל את קידוד הקובץ המבוקש שם יבוצעו בדיקות בנוגע לסוג הקובץ המבוקש.
4. הקובץ ישלח מהתוסף אל שרת מסוג flask בפייטון שרץ בכתובת של heroku.
5. השרת יבנה את הקובץ מהקידוד ויבצע אמולציה של הקובץ על sandbox בכדי לקבוע האם הקובץ "נקי".
6. התוסף יקבל הודעת אישור או דחיה מהתוסף , במידה והתקבל אישור התוסף יבצע הורדה של הקובץ למחשב של המשתמש. אחרת, המשתמש יקבל אפשרות להוריד את הקובץ בניגוד להוראת התוסף.
7. מטרה/יעדים :

* לתת למשתמש אפשרות הורדה בטוחה של קבצים למחשב.
* מנהל ההורדות שלנו יתן אפשרות להוריד קבצים לאחר שנבדקו .
* מנהל הורדות שלנו יהיה מסוגל לזהות את רוב סוגי **נוֹזְקָה**  שכבר מוכרים כיום.

1. אבני דרך ולוח זמנים:

* בין שבוע לשבועיים לבנות שלד שמכיל תוסף לכרום ומתקשר עם שרת שבו מתבצעת בדיקה של הקובץ.

תוסף צריך להיות מסוגל לשלוח קידוד של הקובץ שמנסים להוריד מהאתר והשרת צריך להיות מסוגל לפענח את הקובץ ולשמור אותו לפי סיומת של סוג קובץ שנשלח.

ולשלוח תשובה חזרה לתוסף.

* בין שבוע לשבועיים להוסיף לשרת שלנו שלב הבא שזהו חיבור לsandbox-.
* שבוע: לבחון שאכן השרת מחזיר תשובה לגבי התקינות של הקובץ ועל פי זה התוסף שלנו מוריד או לא מוריד את הקובץ.
* שבוע :לעבור לשרת פעיל באינטרנט (יכול להיות שנעשה את זה לפני חיבור של לsandbox)
* בין שבוע לשבועיים לארגן גרפיקה יפה לתוסף !

1. אתגרים וקשיים:

* היינו צרכים להבין איך הקובץ מקודד ונשלח ממנהל הורדות לשרת .

איך לחלץ את הסיומת של הקובץ עפ"י ה- mime types שלו בשרת בשביל שנוכל לשמור ולהריץ אותו בsandbox על פי האפיון הנכון.

* להתגבר על בעיית זמן ההורדה, כלומר בקבצים גדולים בניית הקובץ מהקידוד, בדיקתו והורדתו עלולות לקחת יותר מפי 2 מהזמן שהיה נדרש להוריד אותו בלבד.

1. חוזקות:

* מכיוון שאנחנו בונים תוסף ל chrome ה-API של גוגל נותן לנו מענה להרבה שיטות הנוגעות להורדת הקובץ , קבלת אינפורמציה מהמשתמש וביצוע debug לקוד התוסף בתוף התבנית של  chrome.