 

**עבודת גמר בתכנון ותכנות מערכות – התמחות סייבר**

**5 יח"ל – שאלון 883589**



**תוסף – Masterwall**

**מגיש:** איתי שגיא שרון

**ת"ז:** 215279704

**מורה מנחה:** שרית שוורץ

**שנת הגשה:** 2023, תשפ"ג

**תוכן עניינים**

[מבוא 3](#_Toc134695038)

[ייזום: 3](#_Toc134695039)

# מבוא

## ייזום:

תוסף masterwall הוא תוסף לכרום, שמטרתו היא סקירת אבטחה של אתרים והתראה למשתמש לגבי אתרים לא בטוחים.

בתום הפרויקט התוסף אמור לבצע לפחות: בדיקת אבטחה עצמית של אתרים, בדיקת אבטחה במאגרי מידע על אתרים, הצגה למשתמש דירוג בטיחות לכל אתר, ואפשרות למשתמש לדווח בעצמו על אתר למאגר מידע שהתוסף ינהל.

בחרתי בפרויקט כי נושא בטיחות באינטרנט זה נושא מאוד חשוב שרוב משתמשי האינטרנט לא יודעים עליו כמעט כלום. אנשים כיום מסתפקים באנטיוירוס, אם בכלל, בשביל לנהל להם את כל האבטחה של המכשיר. אבל אנטיוירוס לא מכסה הכול, ורוב המוחלט של האנשים לא יעמיקו לחפש עוד דרכים לכסות פרצות אבטחה. עם התוסף שלי הכול יהיה יותר פשוט ונגיש לאנשים. בכללי אבטחה ופרטיות הם נושאים שמעניינים אותי במחשבים, והפרויקט הזה הוא הדרך המושלמת לעסוק בהם.

האתגרים שלי בפרויקט יהיו בעיקר חוסר ידע. צריך לדעת על הרבה פרצות אבטחה, ולדעת גם איך לזהות אותן. צריך לדעת איך בכלל לכתוב את כל זה בקוד, ושאתה ניגש לפרויקט כזה אין לך ידע בכלום כמעט.

אתגר שני יהיה זמן, אני תלמיד י"ב עם בגרויות ומטלות וחיים פרטיים ולפעמים קשה למצוא את הזמן לקדם את הפרויקט בזמן הפנוי שלי, באופן שיהיה מספיק מהיר בשביל לכסות את כל הפרויקט עד תאריך ההגשה.

הלקוחות שלי יהיו משתמשי אינטרנט ממוצעים- כל אחד שרוצה אבטחה בסיסית וקלה לשימוש. אני מניח שגיקים של מחשבים ידעו דבר או שניים גם בלי התוסף שלי, אבל עצם הנוחות והנגישות למידע שהתוסף מביא יכולה לעזור אפילו להם. הפרויקט אמור לעזור בעיקר לאנשים שלא מבינים הרבה במחשבים.

מטרות הפרויקט: יכולת לנתח רמת אבטחה ואמינות של אתרים, והצגת תוצאות הניתוח למשתמש.

הבעיה העיקרית שהפרויקט מנסה לפתור היא תמימות של אנשים שנופלים בתרמיות כאלה ואחרות באינטרנט. הפרויקט אמנם לא יכול לשנות אופי של בן אדם, אבל הוא כן יכול לעשות את העבודה המסובכת במקום האדם התמים, ככה שגם ילד בן 5 יכול להבין איזה אתר בטוח ואיזה אתר לא.

פתרונות קיימים:

1. תוסף אחר – כדוגמת Malwarebytes browser guard. היתרון שלי על זה הוא שהתוסף שלי לא רק חוסם אתרים לא בטוחים, הוא גם מציג דירוג אבטחה לכל אתר. יכולה להיות פרצה שלא מספיק חשובה בשביל להיחסם בתוסף שלהם, אבל אצלי זה ייכנס לאלגוריתם החישוב ויוצג בסוף בתוצאה.
2. לסמוך על גוגל והדפדפנים לעשות את שלהם- זה נכון שגוגל והדפדפנים משאירים אותך בטוח ומתריעים מאתרים מסוכנים, אבל עובדה שיש אנשים שעדיין נופלים לתרמיות. אף פעם לא רע שתהיה עוד שכבת אבטחה.

סקירת טכנולוגיה: טכנולוגיה קיימת, אבל גם לא פשוטה ליישום. ייתכן שחלק יהיה בלתי אפשרי ליישום בגלל שהוא כל כך חדש ומסובך שאני לא אוכל להשיג מידע על איך ליישם אותו בפרויקט שלי.

תיחום: הפרויקט עוסק בתקשורת עם שרתים ומאגרי מידע, עוסק באבטחה ופרטיות ברשת, הצפנה. לא עוסק במערכות הפעלה, לא דורש התאמה לאנדרואיד או ווינדואוס.

**פירוט תיאור המערכת (אפיון):**

המערכת אמורה לזהות מתי המשתמש מגיע לאתר חדש, ועל כל אתר לבצע אלגוריתם שיחשב רמת בטיחות. התוסף יציג את התוצאות כמספר עם טקסט בחלון קופץ. המערכת אמורה לאפשר למשתמש לדווח על אתר לבסיס מידע של המערכת, ולהכניס אתרים ל"רשימה שחורה" פרטית שהמערכת לא תבדוק יותר. המערכת תבצע סינון של דיווחי ספאם. המערכת תשתמש בבסיס המידע שלה בתוך האלגוריתם כך שהוא תמיד מתעדכן.

יש רק סוג משתמש אחד שהוא הלקוח. הלקוח יקבל התראה של אתרים לא בטוחים, ייחסם מאתרים לא בטוחים (אלא אם יחליט להמשיך לאתר), הלקוח יכול לפתוח את חלון התוסף בכל עת כדי לבדוק את רמת הבטיחות של האתר הנוכחי, ולדווח עליו.

בדיקות קופסא שחורה:

1. התוסף רץ על הדפדפן ללא שגיאות- הולכים לניהול תוספים של כרום ובודקים אם יש שגיאות.
2. התוסף בודק רמת בטיחות של אתרים – עוברים מאתר לאתר ובודקים אם התוסף משנה את תוצאת הבטיחות. אותו דבר לגבי הקפצת חלון קופץ לאתרים לא בטוחים.
3. התוסף מאפשר דיווח תקין של המשתמש לאתרים – לוחצים על כפתור "דווח" הרבה פעמים ברצף. אם במאגר מידע התווסף רק דיווח אחד סימן שהכול תקין.

תכנון זמנים:

חקירה ראשונית ויצירת תוסף – סוף אוקטובר

יצירת חלון קופץ, שרת, מאגר מידע בסיסיים – סוף דצמבר

חלון קופץ עובד לגמרי (עם פניה לשרת) – סוף ינואר

סינון דיווחי שווא – סוף פברואר

אלגוריתם סביר לבדיקת בטיחות – סוף מרץ

חיזוק האלגוריתם וזמן מרווח לתיקונים – עד ההגשה הסופית

סיכונים:

1. הפרויקט גדול מידיי לטווח הזמן – אני אסיים כמה שיותר, לפחות שיהיה לי את הרעיון עובד, גם אם לא ברמה של משהו שאני אפרסם עכשיו.
2. בלתי אפשרי ליישם את בדיקות האבטחה הנדרשות בגלל חוסר ידע – אני אלמד כמה שיותר פרצות ואיך מכסים אותן. שוב, אולי אני לא יכול לעשות הכול אבל אני יכול לעשות כמות שתספיק.

**תיאור תחום הידע**

**יכולות צד שרת**

שם היכולת: לגשת למאגרי מידע קיימים באינטרנט

מהות: גישה למאגרי מידע קיימים על אתרים לא אמינים ובדיקה אם האתר הפתוח אצל הלקוח נמצא בהם

פעולות נדרשות: קליטת נתונים מהמאגר, קליטת כתובת האתר הנוכחי, השוואה בין המאגר לאתר הנוכחי, החזרת תשובה לאלגוריתם

אובייקטים נחוצים: בסיס נתונים, תקשורת

שם היכולת: עדכון בסיס נתונים

מהות: לעדכן את בסיס הנתונים של המערכת בדיווחים החדשים

פעולות נדרשות: קליטת דיווחים מהמשתמש, בדיקת ספאם (יפורט בהמשך), בדיקת נתונים קיימים בבסיס הנתונים, עדכון בסיס הנתונים במידע החדש

אובייקטים נחוצים: תקשורת, בסיס נתונים, ממשק משתמש

שם היכולת: עדכון נתונים בזמן אמת ללקוח

מהות: הצגת רמת אבטחה של אתר ללקוח, עם המידע הכי מעודכן

פעולות נדרשות: קליטת כתובת אתר נוכחי, הרצת אלגוריתם בטיחות לאתרים (יפורט בהמשך), עדכון החלון הקופץ שיהיה מתואם עם התוצאה, הקפצת החלון למשתמש

אובייקטים נחוצים: ממשק משתמש

שם היכולת: בדיקת בטיחות לאתרים

מהות: אלגוריתם שבודק את רמת הבטיחות של האתר הנוכחי

פעולות נדרשות: קליטת כתובת אתר נוכחי, בדיקה אם הוא ברשימה השחורה, השוואה עם בסיס נתונים של המערכת, השוואה עם מאגרי מידע אחרים, בדיקת פרוטוקולים, החזרת תוצאה של רמת בטיחות כמספר.

אובייקטים נחוצים: בסיס נתונים, תקשורת, אבטחה

שם היכולת: סינון דיווחי ספאם

מהות: סינון לדיווחי המשתמש על אתרים כדי שבסיס הנתונים לא ינוצל לרעה

פעולות נדרשות: קליטת דיווח וip של משתמש, בדיקה בבסיס נתונים מתי לאחרונה דיווח, עדכון בסיס הנתונים, הפלת/אישור הדיווח.

אובייקטים נחוצים: בסיס נתונים, תקשורת

שם היכולת: חסימת אתר ללקוח

מהות: חסימת אתר מזיק לפני שהלקוח מגיע אליו

פעולות נדרשות: קליטת כתובת אתר, הרצת אלגוריתם בטיחות, החזרה של מסך אזהרה למשתמש

אובייקטים נחוצים: ממשק משתמש

שם היכולת: הקפצת חלון קופץ

מהות: הצגת רמת הבטיחות של האתר למשתמש

פעולות נדרשות: לקלוט את רמת הבטיחות, לשנות את החלון הקופץ בהתאם לקלט, להציג חלון על המסך

אובייקטים נחוצים: ממשק משתמש

שם היכולת: זיהוי מעבר של הלקוח לאתר חדש

מהות: זיהוי מתי הלקוח עובר בין אתרים כדי להריץ עליהם את האלגוריתם

פעולות נדרשות: נתינת גישה של התוסף לכתובת האתרים שהלקוח מבקר בהם, פתיחת "מאזין" שבודק מתי הכתובת משתנה

אובייקטים נחוצים: התוסף עצמו

שם היכולת: בדיקת הרשימה השחורה

מהות: בדיקה אם האתר הנוכחי נמצא כבר ברשימה השחורה של הלקוח

פעולות נדרשות: קלט כתובת אתר, השוואה עם בסיס נתונים, החזרת תשובה

אובייקטים נחוצים: תקשורת, בסיס נתונים

**יכולות צד לקוח**

שם היכולת: לפתוח את חלון התוסף

מהות: הלקוח יוכל ללחוץ על אייקון התוסף כדי לפתוח את החלון עם המידע

פעולות נדרשות: ממשק משתמש

אובייקטים נחוצים: תוסף תקין, ממשק משתמש

שם היכולת: דיווח על אתר

מהות: דיווח לבסיס הנתונים של המערכת על אתר לא בטוח

פעולות נדרשות: ממשק משתמש, קליטת האתר הנוכחי, שליחה לשרת, בדיקת ספאם, עדכון בסיס הנתונים, שליחת תשובה למשתמש, הצגת התשובה למשתמש

אובייקטים נחוצים: תקשורת, בסיס נתונים, ממשק משתמש

שם היכולת: הכנסה/הוצאה של אתר לרשימה השחורה

מהות: הלקוח יוכל לסמן אתרים לרשימה השחורה הפרטית שלו כדי שהמערכת לא תבדוק אותם

פעולות נדרשות: ממשק משתמש, קלט כתובת אתר, עדכון מאגר מידע, החזרת תשובה למשתמש

אובייקטים נחוצים: מאגר מידע מקומי, ממשק משתמש