דו"ח סופי לפרויקט גמר במערכות להרצת קוד בסביבה בטוחה

כספת סיסמאות

מגישות:

רבקי שחר- סטודנטית שנה ג סמסטר א מדעי המחשב במרכז האקדמי לב קמפוס תבונה.

ת"ז 212078828 , דוא"ל [rivkyvider@gmail.com](mailto:rivkyvider@gmail.com)

עטרה גינזבורג- סטודנטית שנה ד סמסטר א מדעי המחשב במרכז האקדמי לב קמפוס תבונה.

ת"ז 315263442 דוא"ל [ataraeg613@gmail.com](mailto:ataraeg613@gmail.com)

מנחה: ד"ר ברק עינב

תוכן עניינים

**הגדרת הבעיה3**

**פתרון הבעיה3**

**תיאור הפרויקט4**

**יתרון של פתרון זה על פני פתרונות אחרים בשוק7**

**ניתוח אבטחה9**

**שיפורים לעתיד10**

**חלוקת עבודה11**

**הדרכה להתקנת התוסף12**

**הדרכה להרצת השרת13**

**אופן השימוש בתוסף14**

הגדרת הבעיה

כיום, הרבה מאד אתרי אינטרנט דורשים לבצע כניסה והרשמה לאתר שלהם. וניתן להיכנס לאתר ע"י הזנה של שם משתמש וסיסמא.

בהרבה מאתרי האינטרנט יש פרטים אישיים כמו פרטים רפואיים, מיילים או התכתבויות אישיות, זכויות יוצרים שיכולים לגנוב, וכן בהרבה מהמקרים יש גם פרטי אשראי באתרי קניות, בנקים וכו' וכו'

הבעיה הקיימת שסיסמאות קשה לזכור, אם עושים את אותה סיסמא לכל האתרים אז ברגע שמישהו הצליח לפרוץ לאתר אחד הוא עכשיו יכול להיכנס לכל האתרים שהמשתמש רשום אליהם ללא בעיה.

וכאשר הסיסמא לבנק ולאתר מתכונים מטופש שמתכנת פשוט בנה היא אותה סיסמא. ניתן לפרוץ לאתר זה או לבסיס הנתונים שלו בקלות יחסית. ואז לפורץ יש ביד סיסמאות גם לאתרים החשובים יותר.

אופציה אחרת היא שהמשתמש משתמש בסיסמא נפרדת לכל אתר. במקרה זה המשתמש לא יוכל לזכור אותם בעל פה ולכן ישמור אותם איפשהו באתר כלשהו או על המחשב. אולם, ברגע שפורץ הצליח לפרוץ למחשב הזה הוא יוכל לגלות את כל הסיסמאות של המשתמש ולעשות בהם שימוש לרעה.

כיום, כמעט לכל מחשב ולכל מערכת הפעלה ניתן לפרוץ, מערכות ההפעלה הם גדולות ומכילות הרבה מאד קוד וקשה עד בלתי אפשרי לכתוב אותם באופן שלא ניתן יהיה לפרוץ אליהם.

וכן, בגלל שיש צורך שהסיסמא תהיה זכירה וקלה להקלדה משתמשים בוחרים סיסמאות חלשות שקל לנחש ולא סיסמאות חזקות מספיק וברגע שהסיסמא חלשה ניתן לפענח אותה.

ואם הסיסמא מספיק חשובה וקריטית בעייתי מאד שתהיה שמורה בזיכרון של מחשב שניתן לפרוץ אליו

הפתרון

קיימת סביבה בטוחה מבוססת חומרה ממערכת ההפעלה הראשית (אנדרואיד, לינוקס, OS/X, Windows). היא פועלת במקביל למערכת ההפעלה הראשית.

הסביבה הבטוחה(TEE) פועלת על השבבים הראשיים של המחשב ויש לה הרשאת גישה למשאבים במחשב.

הפתרון הוא שימוש בסביבה בטוחה להנפקה של סיסמאות רנדומליות וחזקות עבור כל אתר ושמירת שלהן בסביבה בטוחה זו. סביבה זו קטנה מאד ומאובטחת, עם יכולות עיבוד קטנה וזיכרון קטן ממש. מה שמאפשר שכל קלט שנכנס ופלט שיוצא ממנה עובר בידוק קפדני ממש כדי לנסות לכסות כל פרצה אפשרית. בנוסף, למערכת ההפעלה של המחשב אפילו אין גישה אליה והמשמעות של זה היא שאפילו אם האקר הצליח לפרוץ למחשב ואפילו למערכת ההפעלה לא תהיה לו אפשרות להגיע לסיסמאות השמורות בסביבה הזו. בנוסף המערכת מתקשרת עם ההוסט שבמחשב ולא ישירות עם משתמש מהרשת כך שעובדה זו מקשה עוד יותר לפרוץ אליה.

נסביר בקצרה ממש את העיקרון של הפרויקט ובהמשך נרחיב עליו.

בנינו תוכנה שכוללת תוסף של כרום שבפעם הראשונה שמתחברים אליו מכניסים סיסמא ראשית שנשמרת בסביבה הבטוחה שרק אותה המשתמש צריך לזכור. כאשר המשתמש נמצא בעמוד הרשמה הוא לוחץ על התוסף שמופיע באייקון בדפדפן הכרום. מכניס את הסיסמא הראשית שלו ואז מוגרלת סיסמא חזקה אשר נשמרת ביחד עם שם המשתמש שהמשתמש בחר בזיכרון הסביבה הבטוחה, ואז כשנמצאים בעמוד כניסה נדרש להכניס רק את הסיסמא הראשית וללחוץ על הזנה אוטומטית ואז שם המשתמש והסיסמא יוזנו בשדות המתאימים.

מצרפת סרטון הדמיה של התהליך.

תיאור הפרויקט

אנחנו רוצות לפתח כספת לסיסמאות שזה אומר שאנחנו בונות תוסף של כרום שהוא מזהה באיזה אתר המשתמש גולש, ינפיק סיסמאות חדשות, וייבא סיסמאות קיימות

תחילה בפעם הראשונה כשהמשתמש מתחיל להשתמש בתוכנה הוא יצטרך לבחור לעצמו סיסמא אחת שהיא תשמש אותו בכל הפעמיים שהוא רוצה להיכנס לאתר שהוא רשום אליו כבר או להירשם לאתר חדש(על אחריות המשמש לבחור סיסמא חזקה)

ואז יש 2 אופציות שונות

כאשר המשתמש נרשם פעם ראשונה לאתר:

הוא מזין את הפרטים שלו אך כדי שהתוכנה תנפיק לו שם משתמש וסיסמא חזקים ותשמור אותם בצורה מאובטחת בסביבה הבטוחה, על המשתמש ללחוץ על התוסף ולהזין את הסיסמא האישית שלו ואז התוכנה תנפיק שם משתמש וסיסמא, תזין אותם במקום הנכון ותשמור את שם המשתמש והסיסמא שהנפיקה יחד עם כתובת האתר בסביבה הבטוחה.

כאשר המשתמש רוצה להיכנס לאתר שהוא כבר רשום אליו:

עליו ללחוץ על התוסף ולהזין את הסיסמא האישית שלו ואז התוכנה תייבא את שם המשתמש והסיסמא של אותו אתר מהסביבה הבטוחה ותזין אוטומטית את הנתונים במקום המתאים

הזיכרון שלי בנוי באופן הבא:

|  |
| --- |
| סיסמא אישית: 11112222 |

|  |  |  |
| --- | --- | --- |
| כתובת של האתר | סיסמא | שם משתמש |
| https://www.kosher.com | KQnC=g8v | rivky@gmail.com |
| https://lib.biu.ac.il | 5E$ivppr | RivkaShachar |
| https://shop.super-pharm.co.il | P\_J4ouFe | Atara |
| https://account.next.co.il | FdM5vje& | rivky@gmail.com |
|  |  |  |

הנפקת סיסמא אישית חדשה- יוודא שאין סיסמא שמורה כבר במערכת, אם באמת אין כזאת ישמור את הסיסמא החדשה

אימות סיסמא- המשתמש מכניס את הסיסמא שלו והמערכת בודקת אם זוהי אכן הסיסמא השמורה במערכת.

הרשמה- אימות המשתמש ע"י הזנת הסיסמא הראשית ולאחר מכן ינפיק סיסמא חדשה או המשתמש יזין סיסמא חדשה ושם משתמש. אם האתר לא קיים במערכת הסיסמא תשמר בסביבה הבטוחה ואם הוא כן, ישאל את המשתמש אם ירצה לעדכן את הסיסמא ואם המשתמש בחר שכן יעדכן אותה במערכת. לאחר מכן המשתמש ילחץ על הכפתור של הזנה אוטומטית ושם המשתמש והסיסמא יוזנו אוטומטית. על המשתמש למלא ידנית את שאר הפרטים הדרושים.

כניסה-אימות המשתמש ע"י הזנת הסיסמא הראשית, לאחר מכן המשתמש ילחץ על הכפתור של הזנה אוטומטית. אם קיימת סיסמא לאתר היא תוזן אוטומטית אחרת יודיע שלא קיימת סיסמא לאתר.

אם המשתמש לוחץ על התוסף בעמוד שהוא לא כניסה או הרשמה תצא הודעה שזהו לא עמוד כניסה או הרשמה

הTEE שומר את הסיסמאות, מנפיק סיסמאות חדשות ומאמת את הסיסמא האישית כאשר רוצים לעשות פעולות.

ההוסט בוויז'ואל מתקשר עם הTEE וגם עם התוסף

מצורף סרטון הדגמה של כניסה בפעם הראשונה ושמירה של הסיסמא הראשית ואז הרשמה לאתר. וכן סרטון של כניסה לאתר ששמור כבר במערכת.

תרשים זה מתאר בכל שלב את האופציות האפשריות שיכולות לקרות במסלול של שימוש בתוכנה.

טבלה זו היא תיאום הקישור בין התוסף לשרת כאשר התוסף שולח פקודת מסוימות מה הוא מצפה לקבל בחזרה.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ערך מוחזר: | קוד חוזר: | משמעות: | קוד נשלח: | פונקציה: |
| 0 אם לא התקבל הpassword הנכון  “0,0”  1 אם כן התקבל הpassword הנכון  “0,1”  "0,2" אם יש שגיאה כשלהי | 0 | מקבל סיסמא של 8 תווים בדיוק ובודק אם היא הסיסמא הראשיות | 0 | CheckMainPassword(string password) |
| מחזיר מחרוזת עם 2 אלמנטים המחולקים בפסיק:  שם משתמש, password  “1,password,name”  אם אין password קיים לאתר אז מחזיר“1,0”  "1,1" אם יש שגיאה כלשהי | 1 | מקבל URL | 1 | retrieve\_password\_user(string url) |
| “2,1” אם הכל נשמר בצורה טובה  "2,0" אם יש בעיה כלשהי | 2 | מקבל Url,pwd,usr | 2 | save\_password\_use(Url,pwd,usr); |
| מחזיר password רנדומלי באורך 8 כולל תו אחד מיוחד אות גדולה אות קטנה ומספר.  “3,password”  "3,0" אם יש בעיה כלשהי | 3 |  | 3 | autoGenPassword(); |
| אם הוא נשמר בהצלחה מחזיר "4,1"  אם הוא לא נשמר בהצלחה מחזיר "4,0"  אם כבר קיים משתמש מחזיר "4,2" | 4 | מקבל סיסמא של 8 תווים ושומר אותה לapplet | 4 | new\_user(pwd) |

ייתרון של פתרון זה על פני פתרונות אחרים הקיימים בשוק

בשוק קיימים כיום המון כספות סיסמאות כאלו ואחרות. חלקם משתמשים בהצפנה של החלפת מפתחות וכל מיני שיטות הצפנה מגוונות. אבל, המשותף בין כולם הוא שגם אם הסיסמאות מוגנות באמצעות מפתח הצפנה והמפתח נמצא במחשב שלי שאליו כפי שציינו קודם ניתן לפרוץ, וברגע שפורצים למחשב ומוצאים את מפתח ההצפנה ניתן יהיה לפתוח את כל הסיסמאות, וכן בכל שיטה אחרת הנתונים נשמרים במחשב כלשהו בצורה כזאת או אחרת שניתן לפרוץ אליו אם מתאמצים.

בניגוד לפתרונות אלו המערכת שלנו שומרת את הסיסמאות בסביבה בטוחה וכפי שציינו קודם היא מאובטחת הרבה יותר וזהו הייתרון של הפתרון שלנו על פני כל שאר הפתרונות הקיימים בשוק

ההתמקדות של הפרויקט שלנו הוא שהסיסמאות יהיו שמורות במקום בטוח. וכן, שיהיה סיסמא נפרדת לכל אתר ושהסיסמאות יהיו חזקות.

התוכנה שלנו לא מאפשרת לייצא סיסמא לפני שהמשתמש הזין את הסיסמא האישית שלו, ורק אז הוא מוציא אותה ומזין אותה באתר.

התוכנה תנפיק סיסמאות מורכבות יחסית רנדומליות וארוכות שיהיה מאד קשה עד בלתי אפשרי לפרוץ אותם, וגם תזין אותם אוטומטית וכן לכל אתר תהיה סיסמא שונה

זה משהו שהמשתמש לא היה יכול לעשות, לזכור מלא סיסמאות קשות וארוכות אשר אין שום קשר ביניהם וגם כל פעם להקליד אותם וכל זה בצורה מאובטחת שגם אם מישהו פורץ למחשב הוא לא יכול לגשת אליהם ואפילו במקרה של גנבה של המחשב עצמו לא יהיה לגנב גישה לסיסמאות.

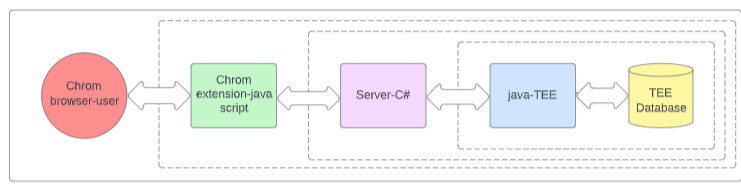
יתרון נוסף ומשמעותי שיש לתוכנה זו היא שאין צורך לייבא את הסיסמא משרת חיצוני כי השרת עצמו רץ על המחשב. התוסף והסביבה הבטוחה גם הם נמצאים במחשב ולכן מרגע הבקשה של הסיסמא עד שהסיסמא מוזנת באתר הסיסמא לא נמצאת ברשת חיצונית מלבד הרשת הביתית, וגם הסביבה הבטוחה נמצאת במחשב האישי ולא ביחד עם סיסמאות של כל המשתמשים האחרים בתוכנה, כך שגם זה פחות אטרקטיבי לפריצה כי יש סיסמאות רק של אדם בודד והאקר פחות ישקיע מאמצים לפרוץ סיסמאות של אדם בודד לאומת סיסמאות של משתמשים רבים. וגם חברה חיצונית צריך לסמוך עליה שאם הסיסמאות שמורות אצלה שלא תשתמש בהם בעצמה לרעה כמו מקרים שקרו בעבר. אצלנו אנחנו מספקים את התוכנה ומנתקים קשר עם הלקוחות, אין לנו יכולת לראות סיסמאות של לקוחות המשתמשים בתכנה.

אולם, חיסרון שקיים הוא שהתוכנה יכולה לעבוד רק על המחשב של הסביבה הבטוחה, והמשמעות של זה היא שאם המשתמש רוצה להיכנס לאתר מהפלאפון שלו או ממחשב אחר הוא לא יוכל לדעת מה הסיסמא.

ניתוח אבטחה של הפרויקט

מטרת האבטחה העיקרית היא שהתקשורת עם הסביבה הבטוחה תהיה דרך חוצץ כלשהו ולא דרך הרשת, ושסיסמא לא תצא מהסביבה הבטוחה אם לא הוזנה סיסמא ראשית נכונה.

התרשים הבא מתאר את זרימת המידע מהרגע שהלקוח לוחץ בדפדפן עד האייקון של התוסף ושולח בקשה עד שהתשובה חוזרת אליו בחזרה.



הלקוח יש לו כמות מוגבלת של כפתורים כאשר כל לחיצה על כפתור מגיעה לjavascript ושם עושה בדיקות קלט בסיסיות כמו אורך סיסמא, אורך של שם משתמש ושהשדה של שם משתמש לא ריק.

הוא שולח הודעה בפורמט מסויים לשרת C# כאשר השרת רץ על המחשב של הלקוח ולכן הבקשה מועברת ברשת הפרטית שלו .הוא קורא את ההודעה ומפענח אותה.

בשלב זה אם מישהו פרץ לרשת הפרטית של הלקוח הוא יכול לראות את התעבורה מהתוסף לשרת שמועברת ברשת הביתית וכרגע במימוש של הפרויקט הנוכחי ההודעות לא מוצפנות ולכן יכול לזהות את הסיסמאות שמועברות כולל את הסיסמא הראשית, ואם הסיסמא הראשית בידיו הוא יכול עבור כל אתר אינטרנט לבדוק אם קיים סיסמא או לא ואם כן לגלות את הסיסמא.

חשוב להדגיש, הסיסמאות לא יוצאות מהנתב של הרשת הפרטית ולכן כל עוד הרשת הפרטית לא נפרצה לא ניתן יהיה לראות את הסיסמאות שמועברות.

השרת לא סומך על הקלט מהתוסף ולכן עושה בדיקות שהקוד תקין אם לא מחזיר מחרוזת ריקה אם תקין מוודא שכל שאר הקלט באורך הנכון ורק אם הוא באורך הנכון הוא שולח פנייה לאפלט JAVA עם הקוד ושאר הקלט.

האפלט הוא לא סומך על כלום ומבצע בדיקות על הכל. כאשר המשתמש נכנס ומזין את הסיסמא שלו רק אם היא נכונה הוא יוגדר במערכת באותה פעם בתור logged\_in כך שאם נכנס מעמוד אחר יפתח סשן חדש והמשתמש לא יוגדר כרשום עד שיזין את הסיסמא הנכונה. בדיקה זו בעצם גורמת לכך שגם אם מישהו פרץ למחשב והוא מתקשר איתו ישירות עד שלא יזין סיסמא נכונה לא יוכל לבצע אף פעולה, ואין לו גישה גם אם פרץ את מערכת ההפעלה לזיכרון של הסביבה הבטוחה.

מעבר לבדיקה שהמשתמש רשום בתחילת כל פונקציה. לפני כל שימוש בקלט עושים בדיקה שגודל הקלט תקין וכך בזיכרון יישמר בדיוק גודל הקלט שציפינו לו.

וגם לפני כתיבה לזיכרון תמיד מוודאים שגודל הזיכרון הוא כמו שמצופה שיהיה. ואחרי כתיבה לזיכרון מוודאים שאכן גודל החדש ששמור בזיכרון הוא מה שאמור להיות.

בעיה משמעותית שקיימת היא שברגע שהצליחו לגנוב את הסיסמא הראשית, ניתן יהיה לגשת לכל הסיסמאות. ולכן על אחריות המשתמש לפחות לדאוג שססימא זו תהיה חזקה ושלא תישמר בזיכרון של המחשב וכדו'

בכל שלב ביצענו בדיקות בלי להסתמך על השלב הקודם כדי למנוע ככל האפשר בעיות של קלט שגוי. ואיפשרנו לקבל רק פקודות מסוימות ומה שלא מתאים לא עובר הלאה בשרשרת של הקוד אלא מוחזר שגיאה.

המערכת לא מאבטחת את הרשת המחברת בין התוסף לשרת כך שיכולות להיות שם מתקפות של man in the middle

שיפורים לעתיד

בעתיד נרצה שהמעבר בין גאווה סקריפט לשרת יהיה מאובטח כדי שגם אם הרשת הפרטית נפרצת לא ניתן יהיה לראות את התעבורה.

כרגע הגדרנו סיסמא באורך 8, בדיעבד היינו צריכים ליצור סיסמא באורך 10 ומעלה כדי לשפר משמעותית את חוזק הסיסמא.

יש אפשרות גם להרחיב שהתוכנה תזהה הרבה יותר דפי הרשמה וכניסה ותשפר את המילוי האוטומטי שיהיה יותר מדוייק.

כרגע אם המילוי האוטומטי לא עובד לא ניתן לדעת מה הסיסמא לאתר ולכן צריך להוסיף אופציה להצגת הסיסמא בתוסף ולא רק למילוי אוטומטי.

צריך גם לשנות את התוסף שבדפי כניסה לא יציג את האפשרות ליצירת סיסמא חדשה אלא רק מילוי אוטומטי כי אין צורך בשאר.

כרגע אין דרך לשנות את הסיסמא הראשית, מסיבות בטיחותיות וטכניות זה ככה, אבל ניתן ליצור אפשרות להחליף את הסיסמא הראשית.

כדאי להוסיף אפשרות של מחיקת סיסמא.

בתוסף יש כמה מקומות שכדאי לאפשר לחזור אחורה שצריך לסדר.

הייתי מוסיפה שברירת המחדל של שם משתמש יהיה נגיד כתובת המייל של הלקוח.

אם רוצים להרחיב ממש, הזיכרון של הסביבה הבטוחה הוא קטן מאד ניתן ליצור מפתח הצפנה ולהצפין את הסיסמאות ולשמור אותם בזיכרון הרגיל של המחשב מוצפנות ואז לפתוח את ההצפנה עם מפתח ההצפנה ששמור בסביבה הבטוחה כשצריך.

**אופן חלוקת העבודה**: באיזה בעיות נתקלנו

בגדול חלוקת העבודה הייתה עטרה בונה את התוסף ורבקי את כל השאר.

**רבקי ועטרה ביחד:**

* בנינו יחד את השרת והלקוח. השרת בC# ואת הלקוח בjavascript
* תיאמנו ביניינו מה השרת מצפה לקבל ואיזו תגובה הלקוח מצפה לקבל בחזרה עבור כל מקרה אפשרי.

**עטרה:**

* תכנון רצף הפעולות של התוסף והגדרת הפונקציונליות של הaplett
* בניית תוסף כרום שירוץ בעת לחיצה על התוסף
* עיצוב התוסף
* הפעלת התוסף רק אם המשתמש נמצא בעמוד של loggin, וכתיבת הודעת שגיאה למסך בכל עמוד אחר.
* כניסה למאגר האישי ע"י סיסמא כדי להכנס/להרשם לאתר
* מילוי אוטומטי של השדות של שם משתמש וסיסמא
* במידת הצורך להנפיק סיסמא רנדומלית
* לשמור או לעדכן שם משתמש וסיסמא למאגר הנתונים
* הדפסת הודעות למסך כדי שהמשתמש יבין מה קורה בכל שלב.
* כתיבת קוד לשרת ולקוח ראשוני כולל תכנון מהלך התקשורת בינהם.

הקושי שנתקלתי בו היה:

* התעסקות בעיקר עם java script,HTML ,CSS ,JAVA שפות שלא הכרתי כלל לפני כתיבת הפרוייקט.
* בניית התוסף דרש המון זמן להתעמקות וקריאה על הנושא כדי להבין כיצד בונים אותו נכון. היום הגרסה העדכנית לכתיבת תוסף כרום היא עדיין יחסית חדשה ולכן אין עליה הרבה מידע באינטרנט, היה הרבה יותר מידע וסרטונים לגרסה 2 שלא עובדת בד בבד עם גרסה 3. מהבחינה הזו הקושי היה בעיקר כאשר היה צריך לשלוף מידע מעמוד web ולהכניס אותו לתוסף. ובמיוחד בזמן כתיבת הקוד, נתקלתי בהרבה אתגרים מכיוון שלא ניתן לדבג את התוסף בסביבת עבודה רגילה, אלא רק מהעמוד chrome.
* בניית השרת היה מאוד מאתגר, מכיוון שזה היה ההכרות הראשוני שלי עם כל הנושא של socket ושרתים.
* כל שינוי קטן לתוסף ולשרת דרש המון בדיקות מעמיקות שהיו מאוד מסובכות להריץ (שרת שהיה בתהליך בניה+קוד בשפה חדשה). היו המון מקרי קצה שהייתי צריכה לחשוב עליהם, ובעצם כדי לפענח איפה הבעיות ולפתור אותם הייתי צריכה להכניס את כל התסריטים האלו באופן ידני לתוסף או לשרת.

**רבקי:**

* שדרוג השרת שלא יקרוס בשום אופן.
* כאשר הלקוח נכנס מדפי WEB שונים הוא צריך ליצור session חדש.
* זיהוי מתי הלקוח מתנתק ומתחבר מחדש.
* השרת מקבל בקשות בפורמט מיוחד וחייב לשלוח תשובות גם בפורמט זה.

לשם כך נדרש כאשר השרת מקבל בקשה לפענח אותה ולהמיר אותה לסטרינג, להבין מתוך הסטרינג את הפקודה המבוקשת, לשלוף את הנתונים שנדרשים כדי לשלוח לTEE להמיר אותם לbyte array אבל בפורמט שהTEE מצפה לקבל כי אחרת התוסף יזרוק שגיאה.

* התוסף מקבל קוד בקשה, מערך של ביטים מעבד את הבקשה ומחזיר תשובה וקוד

לפי קוד התגובה נזהה אם הבקשה התבצעה כמו שצריך או התרחש שגיאה, אם התרחש שגיאה נבין איזו שגיאה התרחשה

* כל אופציה של קלט מהמשתמש עוברת בדיקת קלט לפני שהבקשה נשלחת לTEE
* כל סוג בקשה שנשלח לTEE נשלח עם קוד אחר וצריך לארגן את המידע

הקושי שנתקלתי בו היה:

* התעסקות עם 3 שפות שונות java script, c#, JAVA שהתעסקתי בהם בעבר אבל ממש לא זכרתי כלום כי זה היה מזמן. וסביבת עבודה eclipse שהיא קצת מסורבלת.
* על הDAL לא היה כמעט אף מידע באינטרנט, וגם היה אסור להשתמש בכל הפעולות הקלאסיות שאני רגילה על מערכים וכו'
* היה קושי להבין איך התוסף והC# אמורים לתקשר ביניהם, ואז לממש לקוח בשפה שאני לא מכירה כלל(ביחד עם עטרה שבחיים לא ראתה מימוש של socket או בנתה שרת). ושרת בשפה שאף פעם לא עשיתי בה socket וגם אני למדתי בפייתון לעשות socket רגיל ולא ידעתי שאני אמורה לממש webSocket שזה אחר כי הוא לא מקבל את ההודעות http רגיל וגם מפענח אותם בצורה מפורטת ממש ומחזיר תגובות שלא ידעתי שצריך להחזיר. ובפורמט ממש מוזר של משחק עם ביטים ומבנה מיוחד של הודעה שהייתי צריכה ללמוד עליה כדי להבין את הקוד שרשמתי כי העתקתי אותו מהאינטרנט אחרי הרבה מאד קודים שניסיתי ולא עבדו.

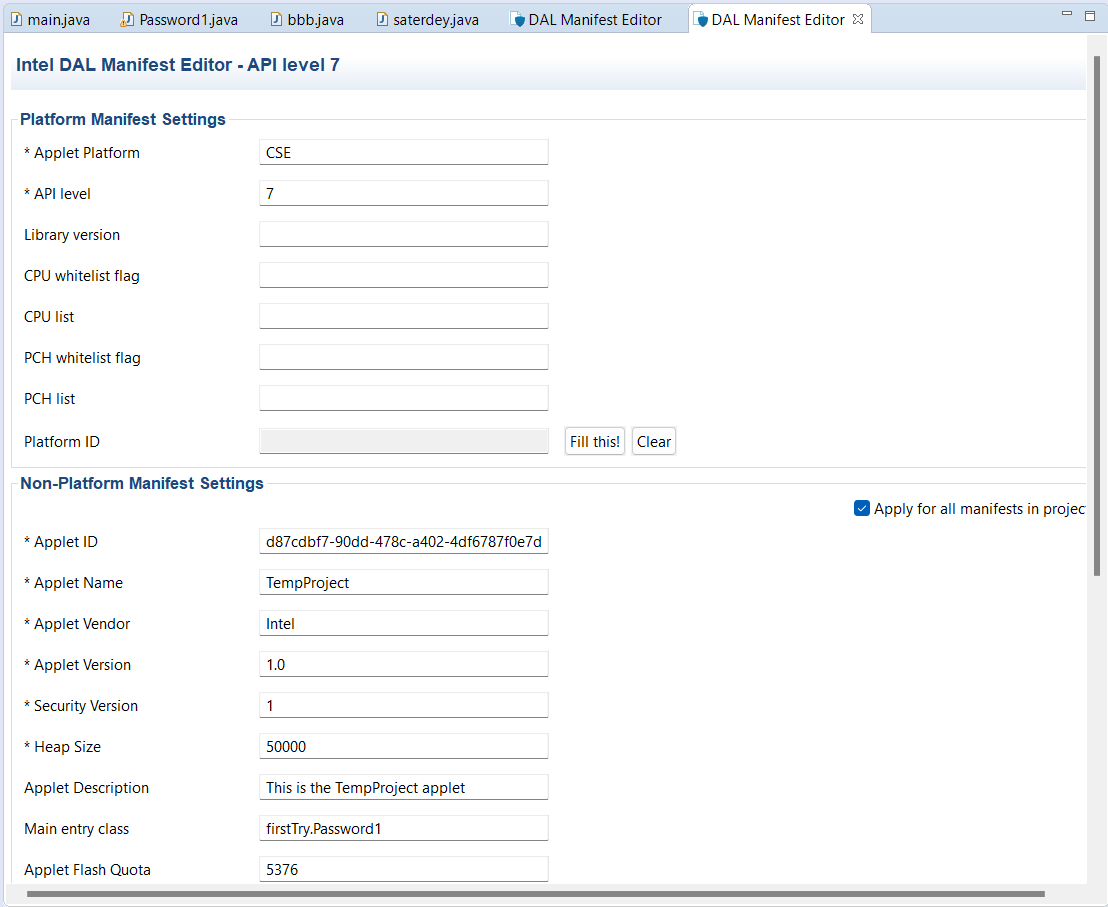
ואז היה בעיה שכל פעם שאני פותחת את התוסף כל הנתונים נמחקו ולכן לא היה אפשרות לבצע אפילו כניסה והרשמה פעם אחת. הייתי צריכה להבין את העניין של התקנת האפלט ופתיחת סשן מה עושה כל אחד וגם אם לקוח התנתק לזהות את זה שזה גם דרש הבנה ולהבין מה לעשות במקרה הזה.

הדרכה להרצת השרת:

יש להוריד את תיקיית JAVA ששם יש את הDAL של הTEE יש לוודא שבתיקיית ה manifests יש קובץ manifests editor והוא צריך להופיע כמו בתמונה המצורפת. כאשר הזיכרון מקסימלי.

בנוסף, יש להוריד את תקיית C# שזה ההוסט שהוא שרת אשר מתקשר בין הTEE לבין התוסף.

בשביל להשתמש בתוסף צריך להפעיל את האימולטור ולהריץ את C# ואז ניתן יהיה להשתמש בתוסף כרגיל.



הדרכה להתקנת התוסף:

שלב א: יש להוריד את קובץ התוסף למחשב שלכם.

שלב ב: קובץ התוסף נתון בתור קובץ zip יש לחלץ אותו ולשמור אותו במקום הרצוי במחשב שלכם.

שלב ג: פתחו את דפדפן הכרום, לחצו על 3 הנקודות שמופיע למעלה בצד ימין, יפתח לכם תפריט שבו תבחרו את האופציה של more tools וממנו יפתח תפריט נוסף שיש לבחור בו Extensions

שלב ד: וודאו שכפתור הDeveloper mode דלוק ולחצו על load unpacked

שלב ה: תגשו למקום ששמרתם את קובץ התוסף במחשב שלכם, לחצו עליו ובחרו select folder

שלב ו: זהו התוסף מותקן על המחשב שלכם ועכשיו תוכלו להתחיל לעבוד.

מצורף סרטון הדרכה להתקנת התוסף.

אופן השימוש בתוסף:

שלב א: היכנסו לאתר שאם רוצים לבצע הרשמה אליו ולחצו על האיקון של הפאזל למעלה בצד ימין בדפדפן.

שלב ב: בשלב זה יופיע לכם האיקון של התוסף של כספת הסיסמאות יש ללחוץ עליו

שלב ג: אם אכן אתם בעמוד כניסה או הרשמה יפתח לכם האפשרות של signin or loggin אם זו הפעם הראשונה בה אתם משתמשים בתוסף עליכם ללחוץ על signin להכניס את הסיסמא שאתם רוצים שתהיה הסיסמא הראשית שלכם ולשמור אותה, שימו לב שסיסמא זו תשמש אתכם בכל פעם שתרצו להשתמש בתוסף ולכן חשוב מאד לזכור אותה כי אם סיסמא זו נאבדת לא יהיה לכם אפשרות להשתמש בתוסף או לשנות אותה.

שלב ד: לחצו על login והזינו את הסיסמא הראשית שלכם

שלב ה: לחצו על Password generation יווצר לכם סיסמא חזקה, עליכם להקליד שם משתמש לבחירתכם ולעשות save ואז שם המשתמש והסיסמא של אתר זה ישמרו, לחילופין אם אתם בכל זאת רוצים סיסמא משלכם שתישמר במערכת לחצו על Save user and password הזינו שם משתמש וסיסמא זו תישמר במערכת.

שלב ו: לחצו על Autofill user and password ושם המשתמש והסיסמא החדשה יוזנו אוטומטית, מלאו את שאר הפרטים הדרושים להרשמה.

שלב ז: כאשר תרצו להיכנס לאתר שאתם כבר רשומים אליו עליכם ללחוץ על התוסף, להכניס את הסיסמא הראשית וללחוץ על Autofill user and password ושם המשתמש והסיסמא יוזנו אוטומטית.

בכל שלב אם ברצונכם לעדכן את הסיסמא ניתן לעשות שוב את שלב ד עד ו שם יופיע לכם שיש לכם כבר סיסמא האם לעדכן אותה ותלחצו על OK ואז הסיסמא תעודכן לסיסמא החדשה.

כרגע בגלל שהתוכנה רצה על אימולטור ולא על הסביבה הבטוחה בעצמה תוגרל כל פעם אותה סיסמא, אבל במציאות הקוד שרשום מייצר סיסמא חזקה ורנדומלית אחרת כל פעם.