< KeyPass>

מסמך אפיון

<עדי בלייר>

<גרסה 0.2>

<13.12.18>

**היסטוריית גרסאות המסמך**

|  |  |  |
| --- | --- | --- |
| **תאריך** | גרסה | **תקציר השינויים** |
| 4.12.18 | 0.1 | התחלת כתיבה על פרוטוקולי תקשורת |
| 13.12.18 | 0.2 | הוספת פונקציונאליות של אדמיין ומדיניות מפתחות. |
| 23.5.19 | 1.3 | עדכון לפי מה שקיים בפועל |
|  |  |  |



1. **הקדמה**
   1. מטרה

מסמך תכנון ראשוני, מוגדר בשפה פשוטה ככל הניתן לתת סיקרה על הפרויקט לאנשים שאינם בעלי ידע מקצועי בנושא.

* 1. המוצר

*המוצר שומר את הסיסמאות של המשתמש בשירותים השונים ומאפשר התחברות קלה.*

*המוצר שואף לעשות בצורה אוטומטית ככל הניתן את ההרשמה וההתחברות שאפליקציות שונות.*

*המוצר ייתן מעלה לכל תוכנת וינדוס, ולא רק לאתרי אינטרנט.*

* 1. הגדרות

*מזהה התוכנה- מחרוזת כלשהי שמזהה את סוג השירות (שם התוכנה או הURI של האתר).*

1. תיאור כללי

*המערכת בנויה משני חלקים, צד שרת וצד לקוח.*

* 1. צד לקוח:
     1. התחברות למערכת
     2. הזרקת שם משתמש וסיסמא לאחר לחיצה על מקש insert
     3. בכל מסך הרשמה ניתן לבקש מהתוכנה להוסיף רשומה חדשה (על ידי קיצור מקלדת), יפתח מסך עם סיסמא רנדומלית מומלצת לשימוש ומקום להקליד את שם המשתמש של תוכנה זו.
  2. צד שרת:
     1. זיהוי משתמשים:
        1. שומר בסיס נתונים של שמות משתמש וסיסמאות בhash
        2. מנפיק טוקן למתחברים ומעדכן את ממסד הנתונים בהתאם.
     2. שמירת המידע
        1. שומר את כל סיסמאות המשתמשים לשירותים השונים.
        2. מאפשר קבלה, עדכון, הוספה ומחיקה של סיסמאות.
  3. קהל היעד

*כל אדם עם ידע בסיס בתפעול מחשב. לקוחות שרוצים לנהל ולשמור את הסיסמאות שלהם. ממשק משתמש מיועד לאדם ממוצע ללא הבנה במחשבים או הבטחת מידע.*

* 1. אילוצים עיקריים
     1. המערכת דורשת חיבור לאינטרנט.
     2. המערכת תומכת בריבוי משתמשים.
  2. הנחות ותלויות
     1. *הלקוח ירוץ רק בסביבת וינדוס.*
     2. הזרקת הסיסמאות תעבוד רק בchrome. לשימוש בדפדפנים אחרים ניתן לצפות בסיסמאות במסך ממשק המשתמש ולהעתיקם ידנית.

1. דרישות מפורטות
   1. צד שרת
      1. *כניסת משתמש*

*עדיפות:חיוני*

*קלט: שם משתמש וסיסמא*

*תהליך: בדיקה האם השם משתמש והסיסמא קיימים.*

*פלט: מפתח הזדהות או הודעת שגיאה.*

*סוג שגיאות: שם משתמש וסיסמא לא נכונים.*

* + 1. *הגשת שאלת הבטחה*

*עדיפות: חיוני*

*קלט: שם משתמש נוכחי, התשובה לשאלת ההבטחה ושם משתמש וסיסמא חדשים.*

*תהליך: הכנסת המשתמש וכל הטוקנים שנוצרו לפני לblacklist (לפי userid ,iat). עדכון בממסד נתונים של שם המשתמש והסיסמא החדשים.*

*פלט: אין*

*סוג שגיאות: ??*

* + 1. *קבלת שאלת ההבטחה*

*עדיפות: חיוני*

*קלט: שם משתמש*

*תהליך: בדיקה האם שם המשתמש קים, עם כן מחזיר את שאת האבטחה עם לא שגיאה*

*פלט: החזרת שאלת ההבטחה.*

*סוג שגיאות: שם משתמש לא קיים*

*בכל התהליכים הבאים מפתח הזדהות יהיה קלט של התכונה. לפני ביצוע הפעולה הנדרשת ייבדק המפתח, ורק עם הוא תקף הפעולה תתבצע. עם לא תוחזר שגיאה שהמפתח לא תקף.*

* + 1. *הוספת סיסמא*

*עדיפות: חיוני*

*קלט: מזהה התוכנה, שם משתמש וסיסמא לתוכנה.*

*תהליך: הוספת הרשומה לממסד הנתונים.*

*פלט: כלום או הודעת שגיאה.*

*סוג שגיאות: מזהה תוכנה כבר קיים.*

* + 1. *מחיקת סיסמא*

*עדיפות: חיוני*

*קלט: מזהה התוכנה.*

*תהליך: מחיקת הרשומה מממסד הנתונים.*

*סוג שגיאות: הרשומה לא קיימת.*

* + 1. *שינוי סיסמא*

*עדיפות: חשוב*

*קלט: מזהה התוכנה, שם משתמש וסיסמא חדשה.*

*תהליך: עדכון הרשומה מממסד הנתונים.*

*סוג שגיאות: מזהה התוכנה לא בממסד נתונים.*

* + 1. *קבלת סיסמא*

*עדיפות: חיוני*

*קלט: אין*

*תהליך: הוצאת הרשומה ממסד הנתונים*

*פלט: החזרת הרשומה*

*סוג שגיאות: הרשומה לא קיימת.*

* + 1. *קבלת כל האתרים*

*עדיפות: חשוב*

*תהליך: הוצאת כל מזהה התוכנות של המשתמש.*

*פלט: כל שמות המשתמש והאתרים שלהם. אין דרך לקבל את כל הסיסמאות בבקשה אחת משיקולי אבטחה.*

* 1. צד לקוח
     1. *יצירת סיסמא*

*עדיפות: חיוני*

*קלט אופציונאלי: מפתח הצפנה*

* + 1. *הרשמה אוטומטית*

*פלט: סיסמא רנדומלית.*

*עדיפות: חשוב*

*קלט: מזהה התוכנה*

*תהליך: נרשם לתוכנה על ידי מילוי כל השדות הידועים לו, לאחר אישור המשתמש מוסיף את הסיסמא למערכת. לא לוחץ על אישור ונותן למשתמש לשנות/להוסיף פרטים.*

*פלט: אין*

*סוגי בשגיאות: אין.*

* + 1. *הכנסת סיסמאות אוטומטית*

*עדיפות: חיוני*

*תהליך: התוכנה תרוץ ברקע וכל פעם שתהיה לחיצה על insert שם המשתמש והסיסמא יוכנסו אוטומתית.*

* + 1. *Remind me*

*לא מצריך הזדהות מחדש עם מפתח ההזדהות עדיין תקף.*

* 1. דרישות הבטחה

*כל התקשורת המפורטת להעיל תהייה בhttps*

*שרת זיהוי משתמשים:*

*מאמת את המשתמש באמצעות שם וסיסמא ומספק מפתחות התחברות.*

*שרת משאבים:*

*מקבל בקשות מהלקוח ומעדכן את ממסד הנתונים.*

*לכל בקשה שנשלחת לAPI יצורף האישור. האישור ייבדק ואם הוא הונפק על ידי גורם מאושר יינתנו ההרשאות למשתמש על פי רישומו בממסד הנתונים.*

* 1. מדיניות שחזור חשבון

לאחר מענה נכון על שאלת הבטחה ניתן יהיה להחליף שם משתמש וסיסמא. לאחר איפוס סיסמא כל המכשירים המחוברים יתנתקו וידרשו התחברות מחודשת עם הסיסמא החדשה.

* 1. מדיניות מפתחות JWT – להזיז למסמך שני

אימות מפתח:

1. בדיקת החתימה
2. בדיקה ברשימת המבוטלים
3. בדיקת הexp

|  |  |
| --- | --- |
| HEADER  {  "alg": "HS256",  "typ": "JWT"  } | Alg- the algorithm to decrepit the signature, only HS256 supported  Type- the type of the token, only JWT supported |
| PAYLOAD  {  "sub": "1234567890",  "exp" : 1516239082  } | Sub- user ID  Exp- time of token expansion |
| HMACSHA256(  base64UrlEncode(header) + "." +  base64UrlEncode(payload), secret  ) | Secret- the secret key that used by the initiator of the token |