design document

* התוסף מאפשר למשתמש מרגע התחברותו לנהל לעצמו סיסמאות בצורה מוצפנת.
* התוסף מאזין לדפדן מזהה פרטי התחברות ושומר אותם בדאה בייס MONGO DB בצורה מוצפנת .
* התוסף מציג למשתמש את סיסמאותיו בצורה גלויה.
* התוסף מאזין לאתר מסוים וברגע אירוע התחברות, שולח לשרת את המידע של ההתחברות.
* השרת שומר את המידע בצורה מוצפנת ומאומתת
* ברגע בקשת המידע מהמשתמש השרת שולף את המידע מפענח את המידע ומציג אותו למשתמש.

הצפנת הפרוייקט

* הרשמה לאתר, פרטי המשתמש נשמרים בדאטה בייס בצורה מוצפנת בעזרת פונקציית האש שמופעת על הסיסמא ושם המשתמש משורשר שמשמש בSALT משום שהוא יחודי.
* בהתחברות נבצע את התליך עם המידע שקיבלנו מהמשתמש ונשווה האם הוא שווה למידע ששמור לנו בדאטה בייס מפונקציית האש. במידה וכן נוכל להוסיף סיסמאות מוצפנות או להאזין לאתר מסוים.
* סיסמאות הלקוח הרשום נשמרות בצורה מוצפנת ומאומתת כל אחת מהן.
* ישנו שימוש במפתח סודי עבור ההצפנה ועבור הMAC
* כל שדה של הלקוח מוצפן ומאומת בהכנסתו לדאטה בייס, ואחר כך מאומת ואז מפוענח ברגע הצגתו ללקוח.
* בנוסף מבוצעת הצפנה ואימות על כל המידע ברגע שליחתו מהלקוח לדאטה בייס, ובדיקה שגם היא לא שונתה בצורה זדונית, אם היא שונתה או כל אחד מהשדות של הלקוח שונו בצורה זדונית, יופיע ללקוח ATTACK בשדה ששונה, או אם נגעו בכל המידע הוא יקבל הודעה שנגעו בבלוק המידע שהוא שלח .
* בשביל לבדוק את הפרוייקט ,ניתן להוסיף סיסמאות ואחר כך לשנות אותן בצורה ידנית מהדאטה ביייס ולשמור, בעת הצגת תוכנו של הללקוח כעת תוצג הודעת תקיפה.

נהוראי מרציאנו ,דור שרון.