**CommunicationLTD**

**מגישים:**

**ליאת אדלשטיין - 313584682**

**ספיר בקאל - 307923789**

**נתנאל אלמליח - 205597735**

**יבגני איסייב - 319289534**

**רקע:**כיום לכל חברה ישנו אתר אינטרנט, בו נשמרים הפרטים של הלקוחות והמשתמשים.   
המידע שנשר הוא מאוד רגיש להתקפות מסוגים שונים ולכן הקמנו אתר מאובטח לחברת CommunicationLTD, אשר מאבטח את בסיסי הנתונים שלה.

**מטרה:**

ליצור אתר מאובטח אשר ממזער את הסיכון להפרץ על ידי תוקפים עם סוגי התקפות שונות, בין היתר SQLinjection ו XSS.

**תיאור המערכת:**

המערכת תייצר בסיס נתונים בעל 2 טבלאות, האחת ללקוחות והשניה למשתמשים.  
סיסמאות המשתמשים יהיו מוצפנות בעזרת אלגוריתם SHA-1 ובנוסף יוצמד אליהם ערך רנדומאלי SALT.   
טבלת הלקוחות תהיה זמינה רק עבור משתמשים שרשומים במערכת.   
במערכת ניתן להרשם, להכנס בתור משתמש רשום ולהזין לקוחות.

**אבטחה:**

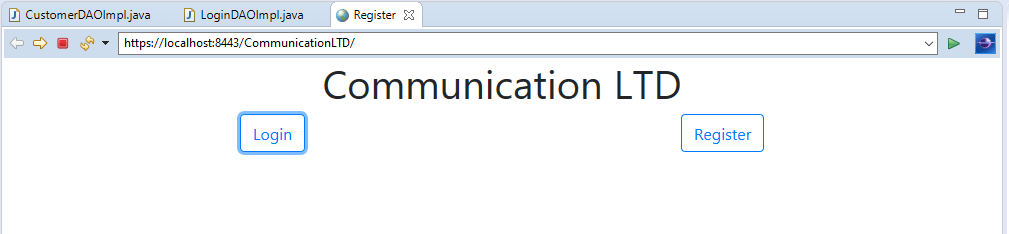
המערכת משתמשת ב SSL ב - self-signed certificate על מנת לייצר חיבור מאובטח ( https ).  
בנוסף, כל הסיסמאות מוצפנות בעזרת SALT ו- HMAC-SHA1. אימות סיסמא דרך המייל מתבצע גם הוא בעזרת אלגוריתם SHA1.

***תכנות בסיס הנתונים:***למערכת תהיה בסיס נתונים אחד המכיל 2 טבלאות.   
**טבלת לקוחות, המכילה:**  
מספר לקוח - ערך מפתח ,  
שם הלקוח,  
כתובת מייל,   
חבילת אינטרנט,  
סקטור,  
ת''ז של הלקוח.

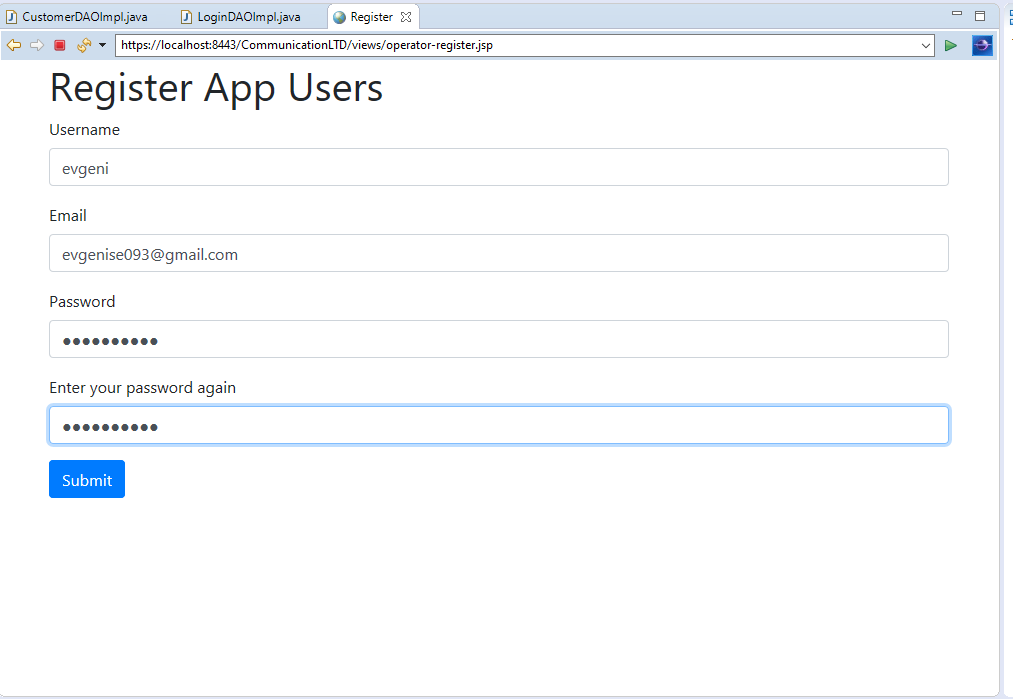
**טבלת משתמשים, המכילה:**מספר משתמש - ערך מפתח,  
שם משתמש - ערך ייחודי,  
סיסמא ( מוצפנת ),   
 Salt,   
כתובת אימייל.

***המערכת:***

בדף הכניסה למערכת יהיו 2 כפתורים.   
האחד להרשמת יוזר ( משתמש ) , והשני לכניסת משתמש קיים.

****

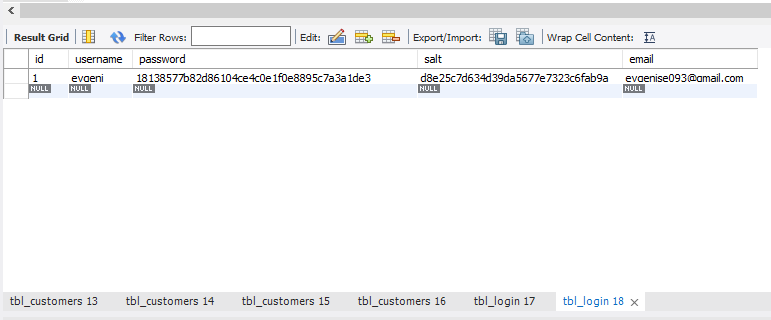
**בעת לחיצת הרשמה, נעבור לדף ההרשמה:**

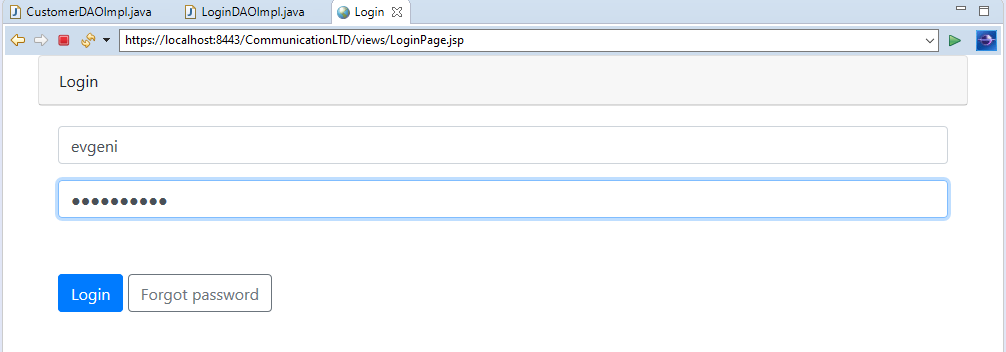
****

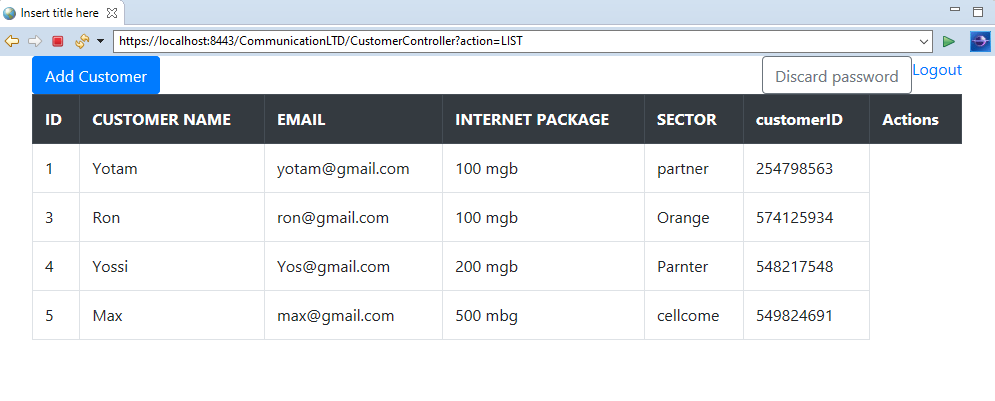
לפני שמירת המשתמש, המערכת תוודא שהסיסמא עומדת בתנאי קובץ הקונפיגורציה ורק לאחר מכן תכניס את המשתמש החדש אל בסיס הנתונים.

סיסמאת המשתמש תתווסף לערך רנדומאלי SALT ולאחר מכן תעבור באלגוריתם HMAC -SHA1 על מנת להצפין את הסיסמא.

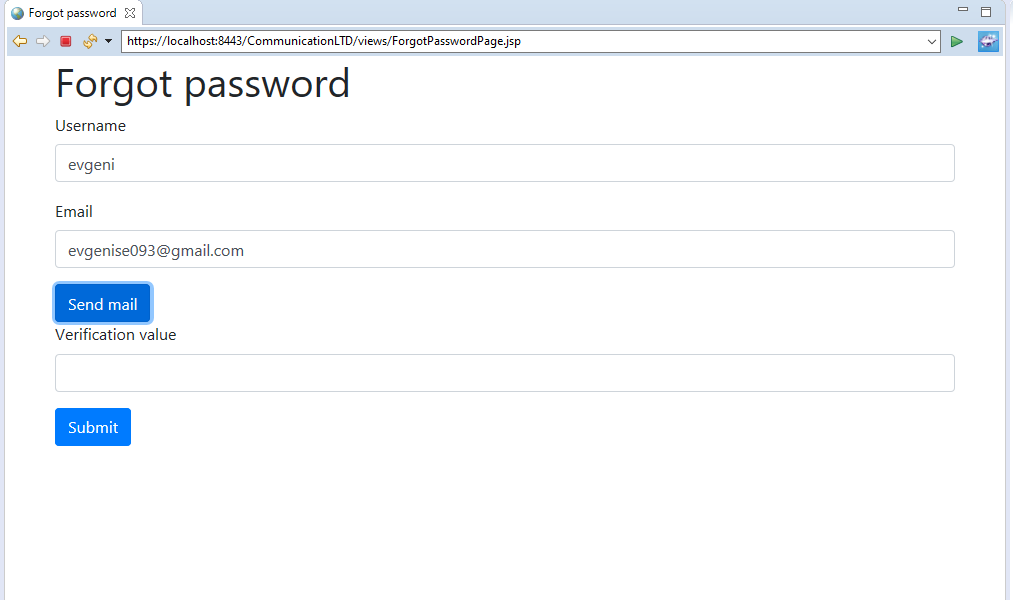
לאחר הכנסת המשתמש,במידה והכל תקין, בסיס הנתונים יראה כך:

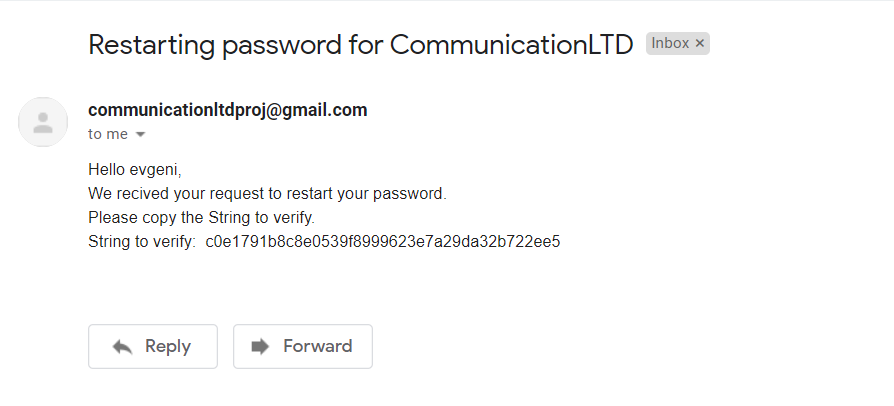
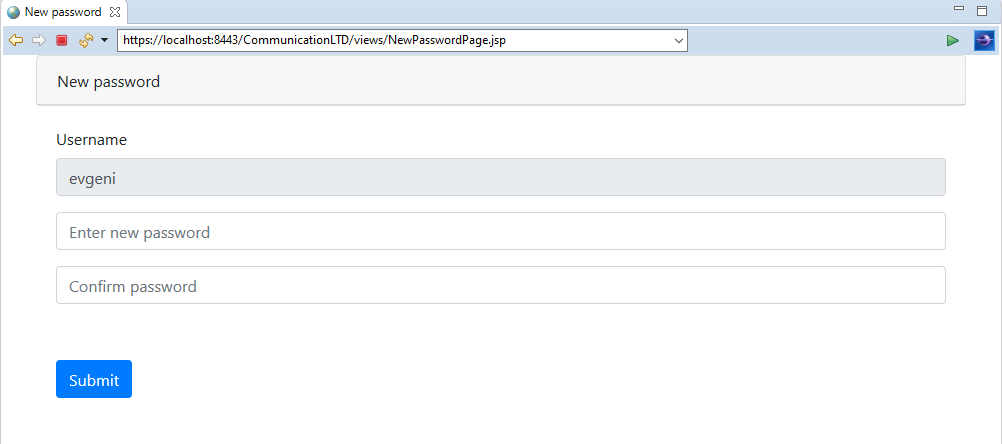


כעת אנו יכולים לגשת ולהכנס לדף המערכת.  
נחזור לדף הראשי ומשם נעבור ל Login:   
  
המערכת ראשית תוודא שאכן קיים משתמש בשם הנתון.  
לאחר שהמערכת אכן אישרה שקיים משתמש מסוג זה, היא תמשוך את ערך ה SALT שלו מבסיס הנתונים, תשרשר לסיסמא אשר המשתמש הכניס, תצפין בעזרת HMAC-SHA1 ותשווה לסיסמא אשר נשמרה בבסיס הנתונים.   
במידה והשם משתמש או הסיסמא שגויים נקבל 3 נסיונות להזנת שם משתמש וסיסמא נכונים ולאחר מכן המערכת תנעל לזמן המוגדר מראש.

במידה והתהליך עבר בהצלחה, נעבור לדף המערכת.

בדף המערכת ניתן להוסיף משתמש חדש, לאפס סיסמא ולהתנתק.  
חשוב לציין שבמידה וסגרנו את המערכת ללא ביצוע Logout, המשתמש שלנו עדיין יהיה רשום וכאשר נדליק שוב את המערכת, היא תזהה אותנו כהמשתמש האחרון ותעביר אותנו מיידית למסך המערכת.

במידה ושכחנו את הסיסמא, מתוך דף ה Login נלחץ על כפתור ה Forgot password ונגיע לדף הבא:   


בדף זה נזין את השם משתמש שלנו ואת כתובת המייל.   
המערכת תדוודא שאכן כתובת המייל תואמת את המשתמש שלה, תייצר ערך רנדומאלי בעזרת אלגוריתם SHA1 ותשלח למייל של המשתמש. במידה ואכן מדובר בשחזור סיסמא, המשתמש יכניס את הערך שקיבל למייל.   
במידה והמערכת מזהה התאמה בין הערך שנשלח למייל לבין הערך שהמשתמש החזיר, אנו נעבור לחידוש סיסמא.   
  


הסיסמא החדשה תהיה מחויבת לעמוד בדרישות קובץ הקונפיגורציה ולאחר מכן תעבור הצפנה כמו ב register user ותשמר במקום הסיסמא הישנה.