**מימוש מנגנון TwoStep authentication -combining text & graphical password**

ברצוננו לממש מנגנון אימות לLOGIN מורכב הכולל אימות שם משתמש, סיסמא ואימות לפי סידרת תמונות. המנגנון הוא מימוש פראקטי של המחקר - <https://www.ccsl.carleton.ca/paper-archive/van-Oorschot-MCETECH-09.pdf>

השיטה המקובלת כיום לביצוע Login באינטרנט היא שימוש ב-שם משתמש וסיסמא. שיטה זו חלשה מול איומים רבים כגון phishing attacks או keylogging attacks.

מטרת המנגנון החדש היא לנטרל את האיום הללו ע"י עימום תהליך ההזדהות.

על מנת לחזקת את תהליך הAuthentication של המשתמש אל מול אתר האינטרנט, ידרש המשתמש לבחור בנוסף לפרטים הרגילים (שם משתמש וסיסמא) סידרת תמונות הידועה לו מראש ולבצע התחברות.

הרעיון שלנו הוא לבנות פלטפורמה שתהיה תוסף לאתר אינטרנט אשר מעוניין לחזק את מנגנון האימות אצלו. הפלטפורמה תהיה גמישה כך שלא תהיה בעיה להוסיף אותה לכל אתר קיים.

הפלטפורמה תכלול את המרכיבים הבאים:

* ממשק WEBי לניהול משתמשים\סיסמאות , המימשק יאפשר להגדיר משתמשים חדשים למערכת ולהגדיר להם פרמטרי התחברות: שם משתמש, סיסמא וסידרת תמונות. את סידרת התמונות המשתמש יוכל לטעון מתוך סדרות קיימות או להוסיף תמונות משלו.

המידע הנ"ל ישמר בצורה מוצפנת בשרת backend בו תהיה הלוגיקה העיסקית.

* ממשק login גינרי (גם WEBי) אשר יכלול את כל הדרוש לצורך התחברות (שם משתמש,סיסמא, בחירת תמונות) למערכת.

כלי פיתוח וסביבה:

HTML, Java (JDE) – Servlet (EE)

GlassFish – Web service

Db - MySql

ארכיטקורה 3 layers: front-end --> backend --> db

**לצורך הרצת הפרויקט להלן לינק להורדת המכונה ה-וירטואלית (VirtualBox vm)**

[https://dl.dropboxusercontent.com/u/61763835/Linux-ubunto.ova](https://dl.dropboxusercontent.com/u/61763835/Linux-ubunto.ova%20) **הסבר על הסביבה:**

מכונה וירטואלית Linux Ubunto 14 (guest) שמתארחת בסביבת Oracle Virtual Box (לינק להורדה).

**הערה:** במכונה הוירטואלית מוגדרים שני כרטיסי רשת: אחת NAT והשני HOST-ONLY ADAPTER

זה מאפשר לגשת למכונה גם מבחוץ וגם מפנים – הIP מוכר גם ב- host וגם בguest.

על המכונה מותקן:

* NetBeans IDE 7.1.2 (הפרויקט נקראה TwoStep)
* GlassFish Server 3.x
* MySQL Server
* MyPhpAdmin

**שם משתמש להתחברות במכונה:** **developer**, סיסמא: **1**

כדי לגשת ל-phpMyAdmin יש לגלוש ל 192.168.56.101

[*http://192.168.56.101/phpmyadmin/index.php*](http://192.168.56.101/phpmyadmin/index.php)

**שם משתמש להתחברות ל DB:** **root**, סיסמא: **1**

**הקוד שמור בrepository GIT, ניתן לגשת עליו מהדפדפן**

URL:[**https://github.com/kfir4ik/TwoStep**](https://github.com/kfir4ik/TwoStep)

במידה ורוצים להתחבר לrepository להלן פרטי ההתחברות:

UserName: **kfir4ik** (kfir.sahartov@gmail.com(

Password: **Mamman13**

***Install GitHub for windows* - https://windows.github.com/**

**הסבר על מבנה הפרויקט:**

הפרויקט הוא **Java** **Servlet** – **Web** **Project**. הIDE הוא **Netbeans**.

**JDK 1.7 - CLR**

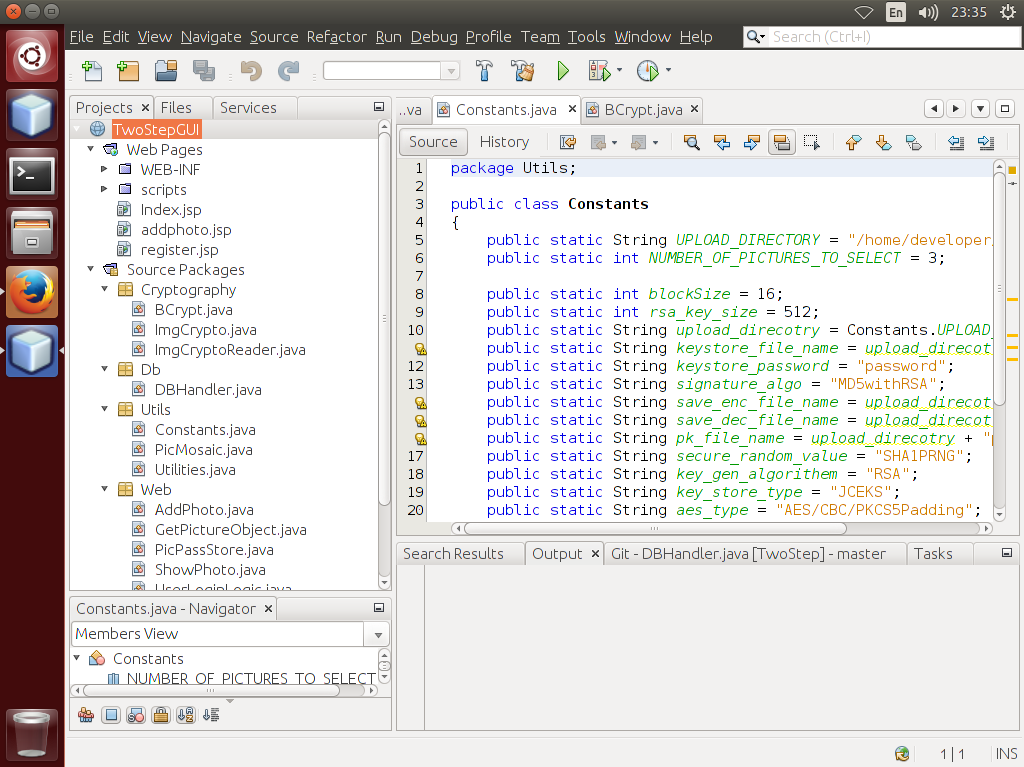
|  |  |
| --- | --- |
| **החלוקה לחבילות packages:**  **Cryptography** – מתודות להצפנה ופענוח של נתונים (מדובר בהצפנה של תמונות ושל טקסט).  **Db** – כל הקשור להתחברות לבסיס הנתונים והגישה עליו. שאילתות ועדכונים.  **Utilites** – מתודות עזר לטיפולים שונים שאינם נכללים בחבילות העובדה האחרות והחבילות האחרות משתמשות בהן.  **Web** – הקוד שמורץ בצד השרת בזמן הגלישה באתר. מכיל טיפולים שונים לשלושת הדפים של האתר.  **הדפים באתר:**  Index.jsp  Addphoto.jsp  Register.jsp  **חבילות חיצוניות בשימוש:**   * MySql JDBC driver * Commons-fileupload (מאפשר להעלות קבצים לאינטרנט) * Bcrypt - מאפשר לבצע hashing   <http://www.mindrot.org/projects/jBCrypt/> |  |

|  |  |
| --- | --- |
| דף ה**Index.jsp**  דף זה המייצג התחברות לאתר sample שלי.  בדף הזה מזינים שם משתמש וסיסמא (שלב ראשון בהזדהות). |  |
| דף ה**register.jsp-**  נועד לרישום משתמש חדש לאתר. שם המשתמש הוא חייב להיות ייחודי. |  |
| דף (נועד למנהל האתר) -**addphoto**.**jsp**  הדף נועד להוספת תמונה למאגר התמונות.  כמו כן, ניתן לצפות בתמונות שבמאגר ע"י הקשת שם התמונה. |  |
| השלב השני בתהליך ההתחברות .  למשתמשים מוצגים תמונות מהם הוא צריך לבחור את התמונות אותם הוא שמר ולפי הסדר שהוא שמר אותם. |  |

**הערות:**

כל הנתונים ניתנים לשינוי, החל מסוג ההצפנה של התמנות\סיסמאות ועד למספר התמונות שיוצגו למשתמש באת הרישום\התחברות לאתר.

**ניתן לנהל ולשנות הגדרות דרך קובץ הconstants.java-.**



**הסבר על הDB:**

|  |  |
| --- | --- |
| התחברות דרך הכתובת:  <http://192.168.56.101/phpmyadmin/index.php>  שם משתמש:root  סיסמא: 1 | C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\pic1.png |
| שם בסיס הנתונים:  TwoStep  מכיל שתי טבלאות:  Pictures  Users | C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\pic3.png |
| **טבלת Pictures:**  השדה **DATA** מכיל את התמונה מוצפנת.  השדה **TITLE**: כינוי לתמונה (ללא הצפנה).  השדה **CryptoKey** – מפתח ההצפנה  (מקודד לא מוצפן).  השדה **pubkey**- מפתח ציבורי  השדה **privkey** – מפתח פרטי  שני השדות מיוצגים כ-binary מסוג BLOB.  השדה pic\_id – הוא מספר רץ לתמונה  (זה גם המפתח לטבלה). | C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\pic4.png |
| **טבלת Users:**  השדה **uid** – מספר רץ המייצג מספר משתמש.  השדה **username** – שם משתמש (ללא הצפנה).  השדה **password** – hashed עם salt מכולל באורך 55 ביטים.  השדה **salt** ערך מכולל מיוצג כ binary  השדה **picpassword** – מייצג רשימת מספרי תמונה שנבחרו על ידי המשתמש באת הרישום לאתר. הערך hashed עם הsalt הנ"ל. | pic5 |
| דוגמא לערכים בטבלת  **Pictures** | pic6 |
| דוגמא לערכים בטבלת  **Users** | C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\pic7.png |