Escalona, J.M.

Group 10

**Case Study 1 - Authentication**

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Issue** | **Java File** | **Vulnerabilities** | **Solution** |
| No input validation on login input fields | Login.java SQLite.java | Logging in does not verify login input fields and will let the user proceed to the main screen of the application regardless of the content.  Unvalidated inputs also make the application susceptible to SQL injections. | Login.java: (**IMPLEMENTED**)  Verify that both the username AND password fields are not empty and comply with character validity will be based on the rules on minimum credential requirements upon registering which are:   1. Lowercase letters: a-z 2. Numbers: 0-9 3. Symbols (Username): \_-. 4. Symbols (Password): ~`!@#$%^&\*()\_-+={[}]|\:;"'<,>.?/ |
| No user verification | Login.java  SQLite.java | Users are not necessarily verified to exist on the database before proceeding to checking authenticity.  \*This is not strictly for security purposes but rather includes performance ones. | Login.java: (**IMPLEMENTED**)  Add user verification which will dictate whether the user authenticity will proceed or not. Assumes login input verification returns true.  SQLite.java: (**IMPLEMENTED**)  Implement function that would only return a Boolean value to indicate whether user exists or not instead of the already implemented SQLite.getUsers() which returns all users including plaintext passwords of users. |
| Password visible | Login.java  Register.java | Password visible on screen. | Login.java & Register.java:  Change password fields and confirm password fields from JTextField to JPasswordField. |
| Passwords not hashed | SQLite.java User.java (via the DB) | Passwords are stored and accessed in the DB in plaintext.  Prone to brute force or dictionary attacks should a known user be found. | SQLite.java: (**IMPLEMENTED**) Implement hashing at a controller level for both password verification (read) and password saving (write).  User.java: (**IMPLEMENTED**)  Change values of ‘password’ to hash equivalent in database.  \*DB was rewritten such that all passwords in plaintext are hashed. |
| No user authenticity verification (i.e., username & password match) | Login.java | User can enter application’s main screen without proper credentials.  Login logging is also recommended to be implemented should login attempts be successful or not. | Login.java: (**IMPLEMENTED**) Implement controls that would verify the username and password before proceeding to the main screen should it be successful. Logging (both successful and not) will also be added for audit purposes. |
| No invalid login pop-ups/notifiers | Login.java | Should an login-related error occur, the user should be notified so in a manner that is ambiguous or generic. | Login.java: (**IMPLEMENTED**) Implement necessary login error pop-ups that is generic should an invalid log-in condition occur. |
| No lock-out mechanism | Login.java  SQLite.java | Repetitive unsuccessful login attempts should not be allowed and does not stop user from logging in after certain retries at a certain time.  Prone to brute force attacks.  Note the ff.:   1. By this point, a known username must have been known by the malicious actor already. 2. User’s locked (int) variable will only be used with 0/1 values as supposed to time as user may inadvertently or knowingly have different times that may bypass if the locked variable indicates time when the user was locked. Unlocking the account is recommended to be done with user (administrator) intervention. | Login.java: (**IMPLEMENTED**)  Implement login lockout measure should successive missed logins are attempted.  SQLite.java: (**IMPLEMENTED**)   1. Add a function that will set a given (valid) user as locked (1). 2. Add a function that will set a given (valid user as unlocked (0). |
| Exposed and incorrectly placed function | Register.java  Frame.java | Users (programmers) may accidentally call the function which could unwantedly alter contents of the database as its functionality is not intended to be used as a parent class function (i.e., one that can be called by other View components). | Register.java & Frame.java: (**IMPLEMENTED**)   1. Remove Frame.registerAction() 2. Transfer it to Register.java |
| No input validation on register input fields | Register.java | Inputs for user account credentials do not require minimum credential requirements such as minimum length (especially for passwords) and character composition.  Action of register was also found to be lost and accessible (public) on another class file Frame.java | Register.java: (**IMPLEMENTED**)   1. Add input validations for each user field such that it meets the following:    1. Uppercase letters (Username only): A-Z    2. Lowercase letters: a-z    3. Numbers: 0-9    4. Symbols (Username): \_-.    5. Symbols (Password): ~`!@#$%^&\*()\_-+={[}]|\:;"'<,>.?/ 2. Add username availability checking. |
|  |  |  |  |