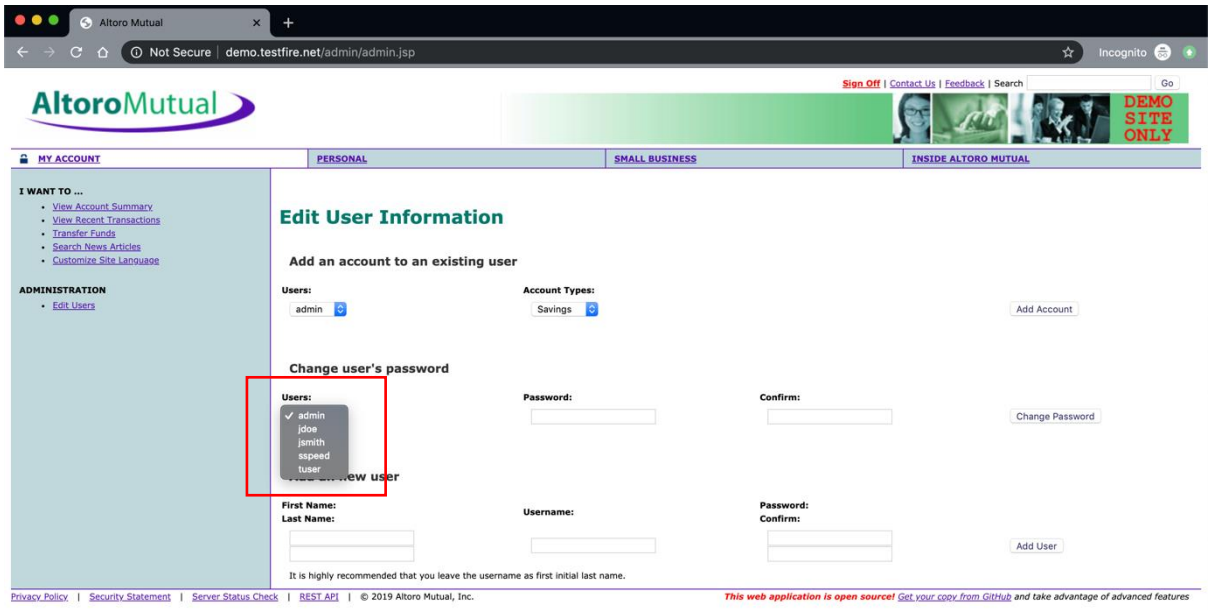
2. The ‘WHERE’ clause for the SQL statement for login:

By observing the behavior of login, we can be sure that the implementation of the underlying SQL query must be concatenated like:

```
query = "SELECT * FROM users
            WHERE username='" + username
            + "' AND password=' + password + "';";
```

Adding -- to username would skip the execution of password check

While being in the admin user, if we go to edit user, we can find various other usernames that are in the system:



By using one of the usernames and the above-mentioned method to circumvent to password check, we can login to a non-admin account.