MySQL Data

MySQL would require a few more changes. After the password is encyrpted using password_hash, the database can be opened, the record inserted, and then the database can be closed.

```
$password = password_hash($password, PASSWORD_DEFAULT);
$mysqli =mysqli_connect($server, $db_username, $db_password, $database);

if (mysqli_connect_errno())
  {
          throw new Exception("MySQL connection error: " . mysqli_connect_error());
  }

$sql="INSERT INTO Users (userid, password) VALUES('" . $userid . "','" . $password . "');";
$result=mysqli_query($con,$sql);
If($result===null)
{
          throw new Exception("Userid/Password not added to Database");
}
mysqli_close($con);
$login_string = date('mdYhis') . " | New Userid | " . $userid . "\n";
error_log($login_string,3,$user_log_file);
header("Location: e7login.php");
```

Logging In

In addition to providing the users with the ability to create their own user IDs and passwords, an application should also provide them the ability to change their passwords. The ability to provide a date limit to expire passwords is very beneficial to increase security. Everytime the user logs on, a comparision can be made on this value. If the current date is more than xx days older than the date saved, the user would be required to change the password.

Since password sniffer programs will try to guess passwords, it is also a good idea to limit to the number of attempts to sign in with the right user ID and password combination. This would reduce the chances that a password sniffing program could generate the correct combination. It is important not allow a valid signin for a period of time after the maximum amount of attempts have been made. Even though this is frustrating to the user, it reduces the chances that a password sniffing program would discover the right combination. If the program does not know that the attempts have timed out, it will receive invalid user ID/password messages, even if it guessed the right combination during the *timeout* period. These adjustments will require additional fields to the user ID/password file (or database).

```
<users>
<user>
<userid>Fredfred</userid>
<password>$2y$10$VosI32FejL.bOMaCjGbBp.Jre6Ipa.tLYQrVqj9kiVpef5zZ25qQK</password>
<datestamp>2015-09-03</datestamp>
<attempts>0</attempts>
<lastattempt>08052015044229</lastattempt>
<validattempt>08052015045431</validattempt>
</user>
```