TLEN 5839: Homework 6

Web Application Authentication

Due Tuesday 3/8 at noon.

Description

We have found a weakness in our app that anyone can add users to the database. To fix this we will enable authentication.

The application should now use sessions, and a password with unique salts for each user.

The application should only allow the admin user to add users to the database.

The application should redirect requests for /hw6 to https://… hw6

Deliverables

You must make a new directory called /hw6 .
Remove the add characters functionality from index.php and put in a new file called add.php.
Create a login page called login.php. This page accepts usernames and passwords.

Create the ability to add users to the application. This MUST use a unique salt in the password. The salt MUST be stored in the salt column of the database. The button to add users should only appear if you are admin.

If a user who is not authenticated tries to connect to add.php, redirect them to login.php

If a user who is not admin tries to manually enter new users to the database (i.e. puts s=90 in the url) print an error message.

Create a logout button.

Create a page to display all of the users in the application. Make sure only the admin user has access to this page.

Extra Credit:

Allow the admin user to update the password for users.
Tips:

You have a user table file stored in /tmp with a sample user admin with a password ralphie.

Authenticate function:

```
function authenticate($db, $postUser, $postPass){
    $query="select userid, email, password, salt from users where username=?";
    if ($stmt = mysqli_prepare($db, $query)) {
        mysqli_stmt_bind_param($stmt, "s", $postUser);
        mysqli_stmt_execute($stmt);
        mysqli_stmt_bind_result($stmt, $userid, $email, $password, $salt);
        while(mysqli_stmt_fetch($stmt)) {
                $userid=$userid;
                $password=$password;
                $salt=$salt;
                $email=$email;
        }
        mysqli_stmt_close($stmt);
        $epass=hash('sha256', $postPass.$salt);
        if ($epass == $password) {
            $_SESSION['userid']=$userid;
            $_SESSION['email']=$email;
            $_SESSION['authenticated']="yes";
            $_SESSION['ip']=$_SERVER['REMOTE_ADDR'];
        } else {
            echo "Failed to Login";
            header("Location: /hw6/login.php");
            exit;
        }
    }
}
```

Authentication check in add.php

```
if (!isset($_SESSION['authenticated'])) {
    authenticate($db, $postUser, $postPass);
}
```