Secure Web-Based Systems
CS 5339

Swapnil Samant
80073690

Assignment 3a - Report

Summary

The object of this assignment is to design and implement an authentication module which can be used to incorporated into another software in the future. Three types of users are supported on this authentication module:

- Visitors, who can access certain parts of the website without logging in, regular users
- Regular users, who can login to the website and access certain parts of the website
- Administrators, who can access the whole website and register new users on the website.

The information of registered users is stored on a MySQL database. The passwords are hashed using SHA256. A random salt and the username is used to salt the password before hashing.

The website has the following pages:

- mainpage.php, this page can be accessed by all users
- signin.php, this page can be accessed by all users. This page lets the users login to the website.
- signout.php, this page can be accessed by all users. Visiting this page will end the active session, if one exists.
- user.php, this page is accessible only to logged in users who are regular users or administrators. This page displays the user details.
- admin.php, this page is accessible only to logged in administrators. This page lets the administrators add new registered users and has a link to view the list of all registered users.
- list_users.php, this page lists all the registered users on the website along with their user details.
- includes/common.php, this page has common functions which can be used by other pages.
- includes/config.php, this page can store configuration settings for the website. Currently the random salt is the only configuration setting in this page.

- includes/conn.php, this page establishes a connection to the MySQL database, which can be used by other pages.
- includes/topnav.php, this page creates the top navigation for all pages based on the session state.
- scripts/admin.js, this a javascript file which contains the validation functions for adding new users form in admin.php.

The database has one table names user, the structure of this table is as follows:

Column Name	Data Type	Attributes	Comments
user_id	int(11)	Not Null, Auto Increment	Primary key for the table
user_name	varchar(64)	Not Null	User name
user_password	varchar(256)	Not Null	Salted and hashed password
first_name	varchar(256)	Not Null	User's first name
last_name	varchar(256)	Not Null	User's last name
creation_time	timestamp	Not Null	Account creation time
last_login_time	datetime		Time of last login for the user
access_level	varchar(10)	Not Null	User's access level. Can be user or admin

Website access

The website can be accessed at `http://cssrvlab01.utep.edu/Classes/cs5339/sssamant/assignment3a/mainpage.php`. The website has one administrator account with user name **admin** and password **nimda18**. The website also has one user account with user name **user1** and password **user123**. The validations for various user attributes are as follows:

- First name, cannot be null or longer than 255 characters
- Last name, cannot be null or longer than 255 characters
- User name, cannot be null or longer than 64 characters or shorter than 5 characters. Valid characters are A-Z, a-z, 0-9, -, _
- Password, cannot be null or longer than 64 characters or shorter than 6 characters. Must have at least one lower case(a-z) character and at least one numeric(0-9) character.

Concluding remarks

It took us about eight hours to finish this assignment. The one issue we ran into was that local testing setup uses PHP 5, which is the default for AMPPS, whereas the CS

server runs PHP 7. This difference in versions meant that the code which was working on local machine had to be modified to work on the server. This assignment was useful to understand the details of user authentication and learning about different vulnerabilities such as session fixation, cross site request forgery, cross site scripting and the importance of input validation.