**WAPH-Web Application Programming and Hacking**

**Instructor: Dr. Phu Phung**

**Mini Facebook**

**Team – 01**

**Team members**

1. Tulasiram Nakkanaboina, [nakkantm@mail.uc.edu](mailto:nakkantm@mail.uc.edu)

2. Vihasith Rasala, [rasalavh@mail.uc.edu](mailto:rasalavh@mail.uc.edu)

3. Grahika Rampudi, [Rampudga@mail.uc.edu](mailto:Rampudga@mail.uc.edu)

4. Sai Sandeep Pasham, [pashamsp@mail.uc.edu](mailto:pashamsp@mail.uc.edu)

*Team members headshot*

A person with a mustache and a black shirt

Description automatically generatedA person wearing glasses and a suit jacket

Description automatically generated A person with long hair wearing glasses

Description automatically generated A person in a blue shirt

Description automatically generated

**Project Management Information**

Source code repository (private access):[**Click\_here**](https://github.com/waph-team01/waph-teamproject)

Project homepage (public): [**Click\_here**](https://github.com/waph-team01/waph-team01.github.io)

**Revision History**

|  |  |  |
| --- | --- | --- |
| Date | Version | Description |
| 26/03/2024 | 0.0 | Initial draft |
| 26/03/2024 | 0.1 | Drafting template overview |
| 26/03/2024 | 1.0 | Sprint 1 update |

**Date Version Description**

**26/03/2024 0.0 Init draft**

**31/03/2024 0.1 Drafting template**Overview

This Project aims to develop a Mini Facebook web application using full stack web

development technologies, secure programming/hacking principles, and the practices of

agile development. This is a team project where all the team members collaborated and

worked together to create a database, creating simple login page and created an index.html

containing information about course overview, each member headshot and each members

personal portfolio link. We divided the tasks among us and pushed the code files into the

main branch.

System Analysis

Functional Requirements

• Creating Database

• User registration and authentication

• Posting texts, images etc.

• Messaging

• Notifications

• Connection request

• Search functionality

Non - Functional Requirements

• Implementing security features

• Session information

• Cookies

• Error handling

System Design

Front-End:

• In the front end we have implemented the new features that the user can be able to

change the password if they have any issues with the current.

• And also, we have implemented the edit profile option where the user will be able to

edit their full name, email and phone number respectively.

• We have implemented the posts visibility option. Once the user was login the user

will be able to see the posts that are posted over the site.

Back-End:

• We have created a database with two main tables which are required for our

application.

• The first table is users where it will store all the information of a user. Like full name,

username, password, Email, and phone number.

• The second table is posts where it will store all the posts which are posted by the

different users. The fields are Post ID, Title, content, postdate and owner.

• The database was connected with the front end where all the data as per the inputs

will be saved in the database.

Use-Case Realization

Database

User Interface

Implementation

Form.php:

In this file we have include the two buttons called login and signup.

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="utf-8">

<title>Facebook-Login page</title>

<script type="text/javascript">

function displayTime() {

document.getElementById('digit-clock').innerHTML = "Current time:" + new Date();

}

setInterval(displayTime,500);

</script>

</head>

<body>

<h1>A Simple login form, WAPH Facebook</h1>

<h2>Team Project: Team 13</h2>

<div id="digit-clock"></div>

<?php

//some code here

echo "Visited time: " . date("Y-m-d h:i:sa")

?>

<form action="index.php" method="POST" class="form login">

Username:<input type="text" class="text\_field" name="username" /> <br>

Password: <input type="password" class="text\_field" name="password" /> <br>

<button class="button" type="submit">Login</button>

</form>

<button onclick="window.location.href='registrationform.php'">Signup</button>

</body>

</html>

Index.php:

In this file we have implemented the posts visibility, password change and profile edit

buttons are included.

<?php

session\_set\_cookie\_params(15\*60, "/","waph-team13.minifacebook.com",TRUE,TRUE);

session\_start();

if (isset($\_POST["username"]) and isset($\_POST["password"])) {

if (checklogin\_mysql($\_POST["username"], $\_POST["password"])) {

$\_SESSION['authenticated'] = TRUE;

$\_SESSION['username'] = $\_POST["username"];

$\_SESSION["browser"] = $\_SERVER["HTTP\_USER\_AGENT"];

}else{

session\_destroy();

echo "<script>alert('Invalid username/password');window.location='form.php';</script>";

die();

}

}

if (!$\_SESSION['authenticated'] or $\_SESSION['authenticated']!=TRUE) {

session\_destroy();

echo "<script>alert('You have not login. Please login first!');</script>";

header("Refresh: 0; url=form.php");

die();

}

if ($\_SESSION["browser"]!= $\_SERVER["HTTP\_USER\_AGENT"]){

session\_destroy();

echo "<script>alert('Session hijacking attack is detected!');</script>";

header("Refresh:0; url=form.php");

die();

}

function checklogin\_mysql($username, $password) {

$mysqli = new mysqli('localhost', 'waphteam13', 'waph13', 'waph\_team13');

if ($mysqli->connect\_errno) {

printf("Database connection failed: %s\n", $mysqli->connect\_error);

exit();

}

$sql = "SELECT \* FROM users WHERE username=? AND password= md5(?);";

$stmt = $mysqli->prepare($sql);

$stmt->bind\_param("ss", $username, $password);

$stmt->execute();

$result = $stmt->get\_result();

if ($result->num\_rows == 1)

return true;

return false;

}

// Fetch and display posts

$mysqli = new mysqli('localhost', 'waphteam13', 'waph13', 'waph\_team13');

if ($mysqli->connect\_errno) {

printf("Database connection failed: %s\n", $mysqli->connect\_error);

exit();

}

$prepared\_posts = "SELECT title, content, posttime FROM posts"; // Assuming 'posts'

table structure

$result\_posts = $mysqli->query($prepared\_posts);

if ($result\_posts->num\_rows > 0) {

echo "<h3>Recent Posts:</h3>";

while ($row = $result\_posts->fetch\_assoc()) {

echo "<div>";

echo "<h4>" . htmlentities($row['title']) . "</h4>";

echo "<p>" . htmlentities($row['content']) . "</p>";

echo "<p>" . htmlentities($row['posttime']) . "</p>";

echo "</div>";

}

} else {

echo "<p>No posts found.</p>";

}

// Close the database connection

$mysqli->close();

?>

<h2> Welcome <?php echo htmlentities($\_POST['username']); ?> !</h2>

<a href="changepasswordform.php">Change Password</a> <br>

<a href="changeprofileform.php">Edit Profile</a><br>

<a href="logout.php">Logout</a>

Changepasswordform.php:

We have implemented the change password option where user will be able to change

password and the respective changes will be reflected in the database through

changepassword.php file.

<?php

require "session\_auth.php";

?>

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="utf-8">

<title>Change Password</title>

<script type="text/javascript">

function displayTime() {

document.getElementById('digit-clock').innerHTML = "Current time:" + new Date();

}

setInterval(displayTime,500);

</script>

</head>

<body>

<h1>Change Password, facebook</h1>

<h2>Facebook Application</h2>

<div id="digit-clock"></div>

<?php

//some code here

echo "Visited time: " . date("Y-m-d h:i:sa")

?>

<form action="changepassword.php" method="POST" class="form login">

Username:<!--input type="text" class="text\_field" name="username" /--> <?php echo

htmlentities($\_SESSION['username']); ?>

<br>

New Password: <input type="password" class="text\_field" name="newpassword" /> <br>

<button class="button" type="submit">Change password</button>

</form>

</body>

</html>

Changeprofile.php:

<?php

require "session\_auth.php";

$Username = $\_SESSION['username'];

$Fullname = $\_REQUEST['new\_fullname'];

$Email = $\_REQUEST['new\_email'];

$Phone = $\_REQUEST['new\_phone'];

if (isset($Username) && isset($Fullname) && isset($Email) && isset($Phone)){

echo "Debug> changeprofile.php got username=$Username; fullname=$Fullname;

email=$Email; phone=$Phone";

if (changeprofile($Username, $Fullname, $Email, $Phone)) {

echo "Profile has been updated";

} else {

echo "Update failed";

}

} else {

echo "Required fields are missing!";

}

function changeprofile($Username, $Fullname, $Email, $Phone) {

$mysqli = new mysqli('localhost', 'waphteam13', 'waph13', 'waph\_team13');

if ($mysqli->connect\_errno){

printf("Database connection failed: %s\n", $mysqli->connect\_error);

return FALSE;

}

$prepared\_sql = "UPDATE users SET Fullname = ?, Email = ?, Phone = ? WHERE

Username = ?";

$stmt = $mysqli->prepare($prepared\_sql);

$stmt->bind\_param("ssss", $Fullname, $Email, $Phone, $Username);

if($stmt->execute()) {

return TRUE;

} else {

return FALSE;

}

}

?>

<br>

<a href="logout.php">Logout</a>

In this file we have implemented the option to Edit their profile, including name, additional

email, phone. The users can access this option through the changeprofileform.php.

registrationform.php:

In this form we have implemented the options to do the intial registration for a user

through the addnewuser.php form.

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="utf-8">

<title>Facebook-Login page</title>

<script type="text/javascript">

function displayTime() {

document.getElementById('digit-clock').innerHTML = "Current time:" + new Date();

}

setInterval(displayTime,500);

</script>

</head>

<body>

<h1>New User Registration, WAPH</h1>

<h2>Facebook User Registration</h2>

<div id="digit-clock"></div>

<?php

//some code here

echo "Visited time: " . date("Y-m-d h:i:sa")

?>

<form action="addnewuser.php" method="POST" class="form login">

Username:<input type="text" class="text\_field" name="username" /> <br>

Password: <input type="password" class="text\_field" name="password" /> <br>

Fullname: <input type="text" class="text\_field" name="fullname" /> <br>

Email: <input type="email" class="email" name="email" /> <br>

Phone: <input type="tel" id="phone" name="phone" class="phone" placeholder="Enter

your phone number" /> <br>

<button class="button" type="submit">Submit</button>

</form>

</body>

</html>

Security Analysis

1) How did you apply the security programming principles in your project?

Input validation : Once the username and password are provides the code will check the

details against the database to make sure if the credentials are valid or not. And also we

have implemented the parametrised statements which will help us to reduce the risk of

injection attacks.

Hashing Passwords: All the passwords in the database are stored in hashed way. So, that

we make sure that the passwords secure. For this we have used the md5 algorithm for

hashing the passwords.

2) What database security principles have you used in your project?

The parametrised statements are used in the queries which are used for validation against

the database records. This will help us to reduce the risk of injection attacks and also

“waphteamSpring” user has been provided with the least privileges than root user.

3) Is your code robust and defensive? How?

Session Management: we uses session\_start() and $\_SESSION to manage user sessions,

which is crucial for maintaining user authentication and preventing unauthorized access.

Error Handling: We includes error handling for database connection ($mysqli-

>connect\_errno) and login failures, which helps maintain our system integrity and prevents

information leakage.

Protection Against Session Hijacking: By comparing the user agent

($\_SERVER["HTTP\_USER\_AGENT"]) of the current request with the one stored in the session,

the code attempts to detect and prevent session hijacking attacks. Password Hashing: We

use md5() to hash passwords before comparing them in the SQL query, which is a basic but

essential step in protecting against password-related attacks.

Prepared Statements: To protect against SQL injection attacks, we use prepared

statements ($stmt->bind\_param()) in the database query. This helps to separate the SQL

code from user input, making the system more secure.

4) How did you defend your code against known attacks such as XSS, SQL Injection, CSRF,

Session Hijacking.

XSS (Cross-Site Scripting): WE use a technique called HTML entities to make sure that any

special characters entered by users are treated as plain text and not as code. This helps to

prevent attacks where hackers try to inject harmful code into a website.

SQL Injection: Our code uses a method called prepared statements with parameterized

queries to separate the user's input from the actual SQL code. This helps to prevent attacks

where hackers try to manipulate the database by inserting malicious SQL commands.

Session Hijacking: Our code checks if the user's browser matches the one stored in the

session. If they do not match, it assumes that someone is trying to hijack the session and

terminates it. This is an effective way to defend against session hijacking.

5) How do you separate the roles of super users and regular users?

Role-Based Access Control: To distinguish users with different roles, we added a column

in the database that specifies the role for each user. By doing this, we can utilize this role

information to decide which actions each user is permitted to perform.

Software Process Management

In general, every project in an organization requires a bigger team to work on the project.

There will be n number of tasks and subtasks that every team should work on. Then all the

subtasks will be integrated as a single task. For this to be complete without any

communication gap, there is a tool called GitHub to manage work collaborations. We

followed the pipeline process where we divided the tasks among ourselves and then

developed code is pushed to the main branch. Like this all of us are aware of the new files

created/deleted.

Scrum process

Sprint 1

Duration: 03/25/2024-03/31/2024

Completed Tasks:

1. Task 1: Created the database as per the requirements mentioned in the rubrics.

2. Task 2: Implemented the login form and the registration form.

3. Task 3: Implemented the basic functions for the logged-in users. That is to change

passwords, edit their profile, including name, additional email, phone, and View posts

from the database.

Contributions:

1. Pushpa Kafley, 2 commits, 5 hours, contributed in changing database, form.php and

modifying readme contents

2. Lakshmi Narayana, 3 commits, 5 hours, contributed in modifying index.php,

changeprofile.php and modifying readme contents

3. Ganesh Atmakuri, 4 commits, 5 hours, contributed in implementing

registrationform.php, addnewuser.php, readme and modifying readme contents

4. Sai Keerthi Vadnala, 2 commits, 5 hours, contributed in modifying recent posts,

updating database and modifying readme contents