

[23:36, 4/25/2024] DILIP KUMAR: # WAPH-Web Application Programming and Hacking

**Instructor: Dr. Phu Phung**

## Mini-Facebook

### Team members

1. Sai Kumar Gadde, gaddesr@mail.uc.edu
2. Dilip Kumar Sanipina, sanipidr@mail.uc.edu
3. Uma Satwik Meka, mekauk@mail.uc.edu
4. Siva Sai Manoj Korlepara, korlepsj@mail.uc.edu

### Project Management Information

Source code repository (private access): <https://github.com/waph-team10/waphteamproject/>

Project homepage (public): <https://github.com/waph-team24/waph-team24.git>

### Revision History

Date	Version	Description
21/03/2024	0.0	Sprint 0
04/04/2024	0.1	Sprint 1
20/04/2024	0.2	Sprint 2.

## Overview

S...

[23:44, 4/25/2024] DILIP KUMAR: # WAPH-Web Application Programming and Hacking

**Instructor: Dr. Phu Phung**

## Mini-Facebook

### Team members

1. Sai Kumar Gadde, gaddesr@mail.uc.edu

2. Dilip Kumar Sanipina, sanipidr@mail.uc.edu
3. Uma Satwik Meka, mekauk@mail.uc.edu
4. Siva Sai Manoj Korlepara, korlepsj@mail.uc.edu

## Project Management Information

Source code repository (private access): <https://github.com/waph-team10/waphteamproject/>

Project homepage (public): <https://github.com/waph-team24/waph-team24.git>

## Revision History

Date	Version	Description
21/03/2024	0.0	Sprint 0
04/04/2024	0.1	Sprint 1
20/04/2024	0.2	Sprint 2.

## Overview

## System Analysis

(Start from Sprint 0, keep updating)

## Demo (screenshots)

## Software Process Management

(Start from Sprint 0, keep updating)

## Scrum process

All of our teammates uses Google Meet and Discord to communicate efficiently. We have a stand-up meeting on Google Meet every day to go over tasks and make sure everyone is informed of their responsibilities. With the help of this conference, we can identify any dependencies or hurdles so that we may tackle challenges head-on. Throughout the day, we exchange questions, quick updates, and quick cooperation via Discord. We speak often. At the conclusion of the day, we meet together to talk about what happened, evaluate our progress, and establish plans for the next day. This comprehensive approach to communication promotes accountability, transparency, and fruitful teamwork among our members.

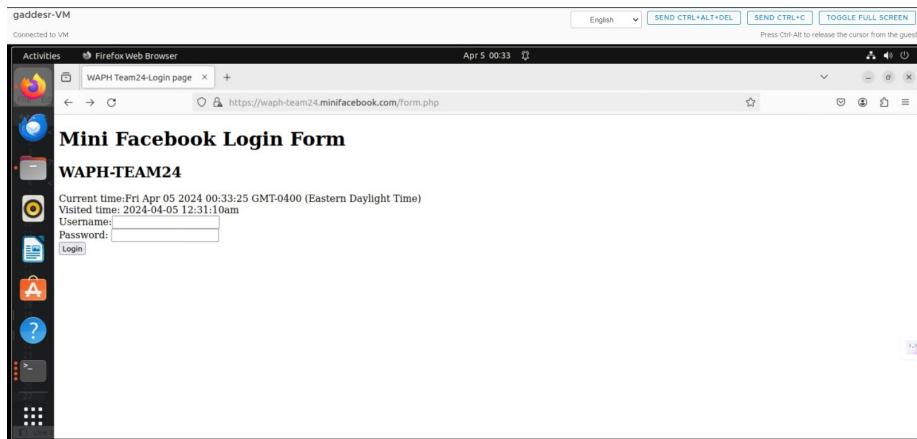


Figure 1: Login\_Form

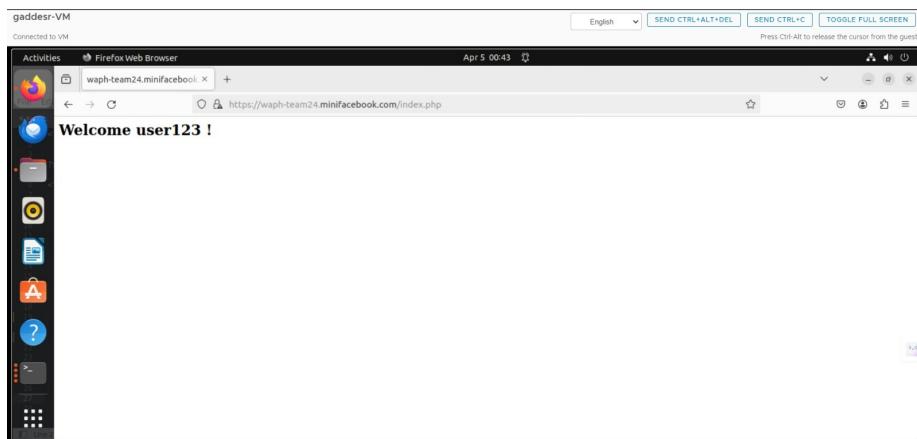


Figure 2: sucessful\_Login

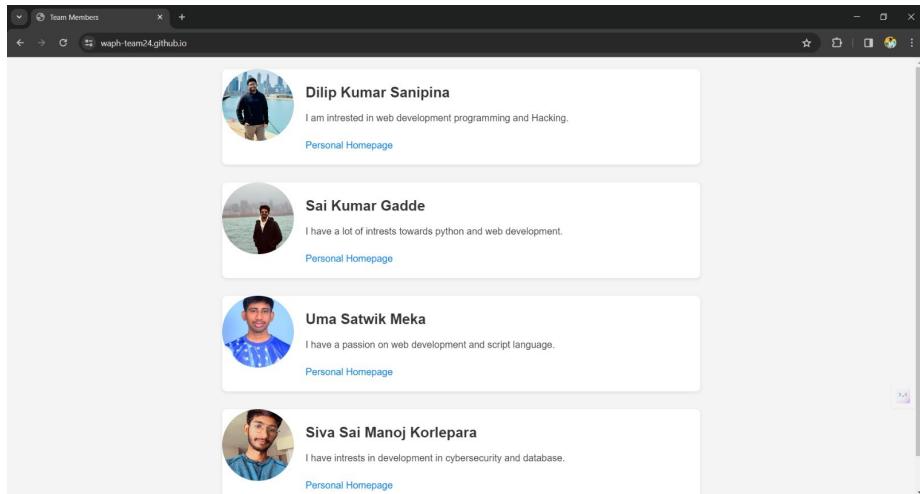


Figure 3: Team\_members\_personalPage

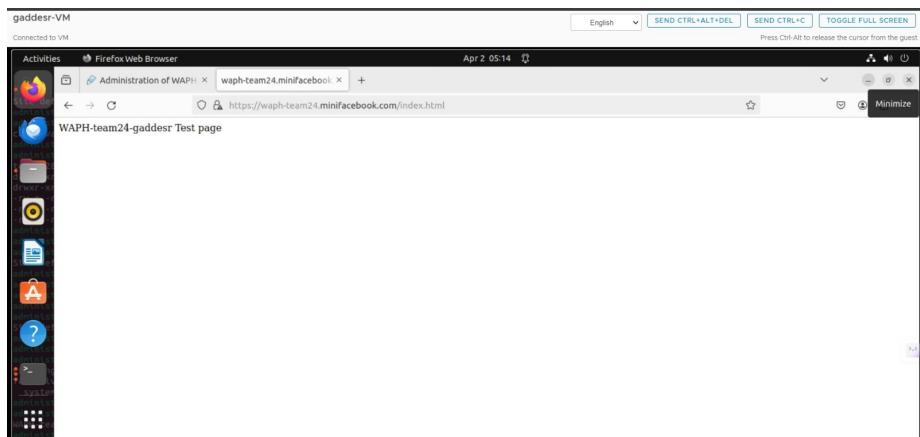


Figure 4: Test\_page\_gaddesr

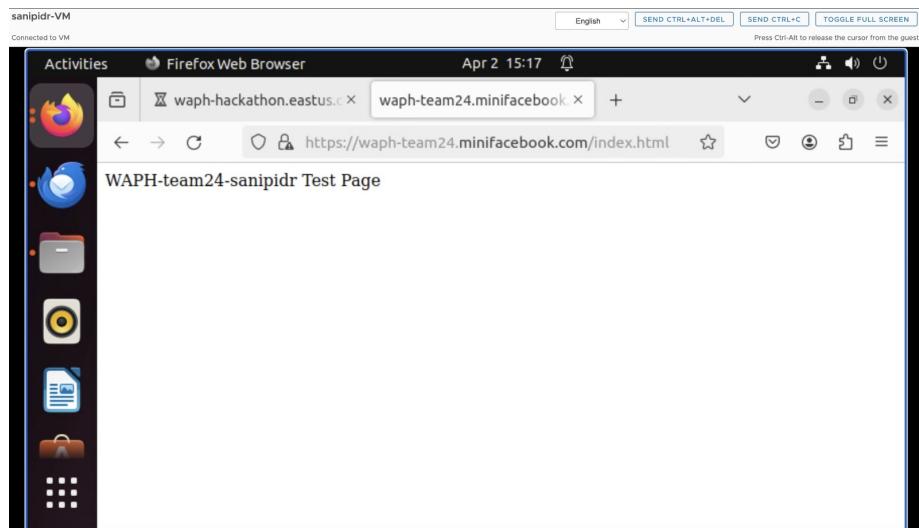


Figure 5: Test\_page\_sanipidr

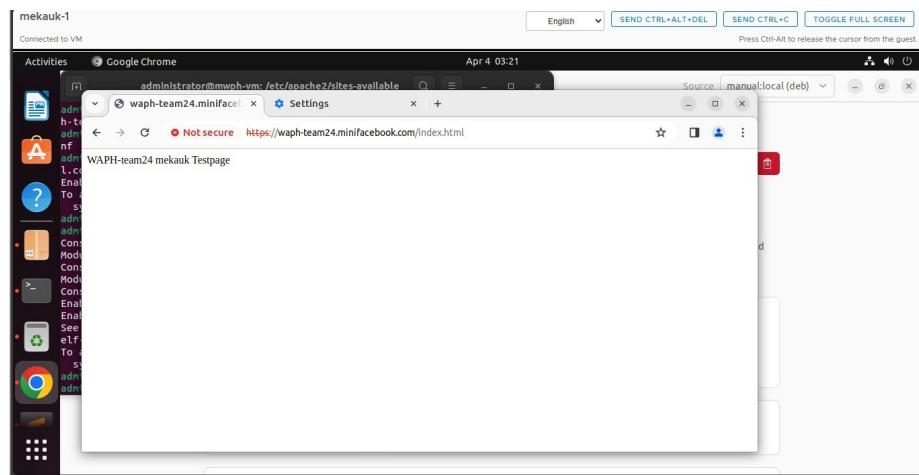


Figure 6: Test\_page\_mekauk

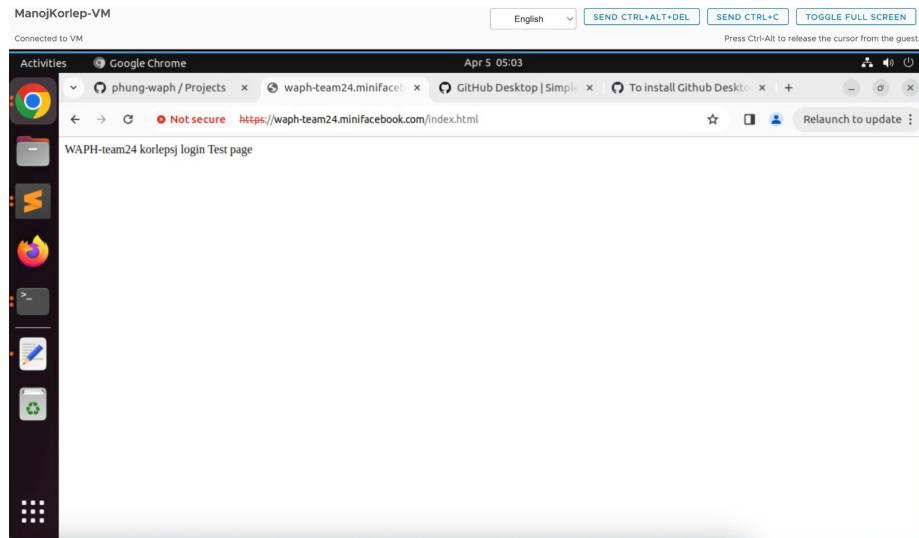


Figure 7: Test\_page\_korlepsj

## Sprint 0

Duration: 21/03/2024-27/03/2024

### Completed Tasks:

1. In sprint 0 we have created public and private repositories and name them as "Waph-teamproject" and " Waph-team24.github.io".
2. We have generated ssl keys and certificates for the team project and configure the https for the local domain.
3. We have develop the database for team project.
4. We also developed a individual home page for all of them and we have satisfied the requirements based on lab3 & lab4 for the team project.
5. We have tested the functionality using using index.html.

### Contributions:

1. Saikumar Gadde has done 7 commits over 5 hours and contributed in creating ssl keys and certificates for the team project amd creation of team personal home page.
2. Dilip Kumar Sanipina has done 4 commits over 4 hours and contributed in creating team repo's and public repo and database creation and contirbuted in developing form and index .php files.
3. Uma Satwik Meka has done 2 commits over 3 hours contributed in creation of setup database structure and index.html.
4. Manoj Kumar Korelpara has done 2 commits over 3 hours contributed in

readme file and database setup.

## Sprint 1

Duration: 28/03/2024-07/03/2024

### Completed Tasks:

1. In sprint 1 we have completed designing the database and created the user-table,host tables and also created database-data.sql file.
2. we also created the user registration and login and change passwords

### Contributions:

1. Saikumar Gadde has done 5 commits over 6 hours and contributed in creating database design and developing database-data.sql
2. Dilip Kumar Sanipina has done 3 commits over 5 hours and contributed in creating registration form and other php files.
3. Uma Satwik Meka has done 2 commits over 4 hours contributed in modification of userregistrationform and index files.
4. Manoj Kumar Korelpara has done 2 commits over 3 hours contributed in dealing with change password and creating readme file.

**Database-account.sql** sql create database waph\_team; CREATE USER ‘waph-team24’@‘localhost’ IDENTIFIED BY “team@24”; GRANT ALL ON waph\_team.\* TO ‘waph-team24’@‘localhost’;

**Database-data.sql** sql use waph\_team; DROP TABLE IF EXISTS comments; DROP TABLE IF EXISTS posts; DROP TABLE IF EXISTS users; create table users( username varchar(255) PRIMARY KEY, password varchar(100) NOT NULL, fullname varchar(100), otheremail varchar(100), phone varchar(10), status ENUM(‘active’, ‘disabled’) DEFAULT ‘active’; ); INSERT INTO users(username,password) VALUES (‘test1’,md5(‘test1’)); INSERT INTO users(username,password) VALUES (‘test2’,md5(‘test2’)); create table posts ( postID INT AUTO\_INCREMENT PRIMARY KEY, title VARCHAR(100) NOT NULL, content VARCHAR(100), posttime TIMESTAMP DEFAULT CURRENT\_TIMESTAMP, owner VARCHAR(50), FOREIGN KEY (owner) REFERENCES users(username) ON DELETE CASCADE ); create table comments ( commentID INT AUTO\_INCREMENT PRIMARY KEY, postID INT, comment VARCHAR(255) NOT NULL, commenter VARCHAR(50), commentTime TIMESTAMP DEFAULT CURRENT\_TIMESTAMP, FOREIGN KEY (postID) REFERENCES posts(postID) ON DELETE CASCADE, FOREIGN KEY (commenter) REFERENCES users(username) ON DELETE CASCADE );

```
create table superuser ( username varchar(255) PRIMARY KEY, password varchar(100) NOT NULL, );
```

```
INSERT into superuser values ('admin',md5('admin'));
```

The screenshot shows a terminal window with the following content:

```
administrator@mwh-vm: ~/waph-teamproject/database$ sudo mysql waph_team < database-data.sql
[Output of database-data.sql follows]
Administrator@MWH-VM:~/waph-teamproject$
```

Below the terminal, a Sublime Text editor window is open with the file `database-data.sql`. The code in the editor is as follows:

```
--waph-teamproject/database/database-data.sql - Sublime Text (UNREGISTERED)
File

1 describe posts
2
3
4
5 ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
6 corresponds to your MySQL server version for the right syntax to use near 'descrit
7 pos' at line 1
8 mysql> describe posts;
9
10
11 describe posts
12
13
14 +-----+-----+-----+-----+-----+
15 | Field | Type | Null | Key | Default | Extra |
16 +-----+-----+-----+-----+-----+
17 | postID | int | NO | PRI | NULL |
18 | title | varchar(100) | NO | NULL |
19 | content | varchar(1000) | YES | NULL |
20 | postTime | varchar(100) | YES | NULL |
21 | owner | varchar(100) | YES | MUL | NULL |
22 +-----+-----+-----+-----+-----+
23 5 rows in set (0.01 sec)
24
mysql>
```

Figure 8: database-data

- The ER (Entity-Relationship) diagram shows the structure and relationships between the “users” and “posts” tables. In the graphic, the “users” table is the primary entity, comprising characteristics such as “username,” “password,” “fullname,” “otheremail,” and “phone,” with “username” serving as the primary key. This table contains information about specific system users, each of whom is recognized by a username.
  - In contrast, the “posts” table stores information about user-created postings. It contains attributes such as “postID,” “title,” “content,” “posttime,” and “owner.” Here, “postID” is the primary key. The “owner” field has a link with the “username” attribute in the “users” table, indicating who created each post. This relationship is represented as a one-to-many association, which means that one user can create several postings.
  - Furthermore, the ER diagram exhibits referential integrity between the two tables using a foreign key constraint. The “owner” element in the “posts” table refers to the “username” field in the “users” table. This constraint requires a post’s owner to be a genuine user in the system, eliminating orphaned records and maintaining data consistency. Furthermore, the ON DELETE CASCADE constraint given on the foreign key ensures that when a user is deleted from the system, all posts connected with that user are automatically removed, preventing referential integrity issues.

Form.php

## change password.php

```

waph-teamproject / form.php
Code Blame Executable file - 98 lines (93 loc) - 2.42 KB Code 55% faster with GitHub Copilot
53     }
54     .button {
55       width: 100px;
56       padding: 10px;
57       background-color: #e0e0ff;
58       color: #fff;
59       border: none;
60       border-radius: 3px;
61       cursor: pointer;
62     }
63     .button:hover {
64       background-color: #0056b3;
65     }
66   </style>
67   <script type="text/javascript">
68   function displayTime() {
69     document.getElementById('digit-clock').innerHTML = "Current time:" + new Date();
70   }
71   setInterval(displayTime, 1000);
72   </script>
73 </head>
74 <body>
75   <div class="container">
76     <h1>Mini Facebook Login Form</h1>
77     <h2>WAF-TEAM4</h2>
78     <div id="digit-clock"></div>
79   </div>
80   <php>
81     //some code here
82     echo "Visited time: " . date("Y-m-d H:i:s");
83   </php>
84
85   <form action="index.php" method="POST" class="form login">
86     <input type="text" class="text_field" name="username" /> <br>
87     <input type="password" class="text_field" name="password" /> <br>
88     <button class="button" type="submit">Login</button>
89   </form>
90
91   <form action="registrationForm.php" method="POST" class="form register">
92     <button class="button" type="submit">Signup</button>
93   </form>
94
95 </body>
96 </html>

```

Figure 9: form.php code

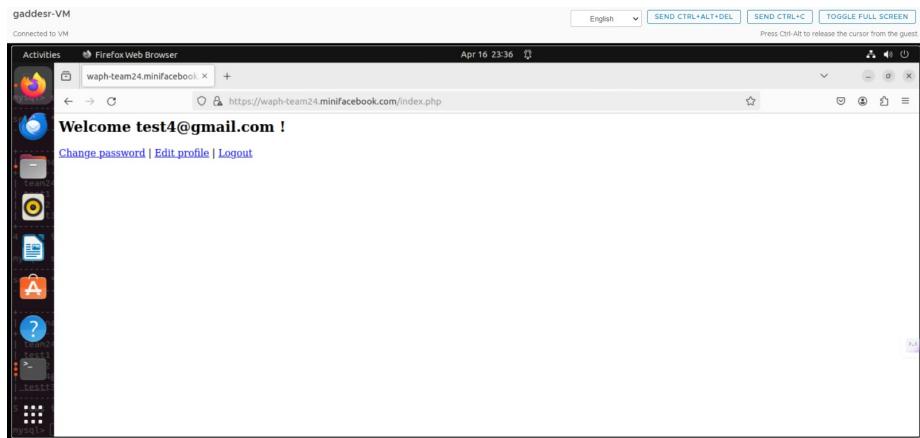


Figure 10: successful\_login\_page

The screenshot shows a GitHub code editor interface for the file `changepassword.php`. The code is written in PHP and includes session handling, token verification, and password change logic. It also contains a debug message and a link to a login page.

```

1 <?php
2 require "session_auth.php";
3 require "minifacebook.php";
4 $token = $_REQUEST['token'];
5 if (!isset($token) or $token!=$_SESSION['noscrfToken']) {
6 echo "CSRF Attack is detected!";
7 die();
8 }
9 $username = $_SESSION['username'];
10 $oldpassword = $_REQUEST['oldpassword'];
11 $newpassword = $_REQUEST['newpassword'];
12
13 if (isset($username) and isset($oldpassword) and isset($newpassword)) {
14 // Debug> changepassword.php got username=$username&newpassword=$newpassword
15 echo "password has been changed<a href='https://waph-team24.minifacebook.com/logout.php'>Logout</a>";
16 if($changepassword!=$username,$oldpassword,$newpassword){
17 echo "password has been changed<a href='https://waph-team24.minifacebook.com/logout.php'>Logout</a>";
18 }else{
19 echo "Change password failed<a href='https://waph-team24.minifacebook.com/logout.php'>Logout</a>";
20 }
21 }else{
22 echo "No username/password provided!";
23 }
24
25 ?>

```

Figure 11: chnagepassword.php code

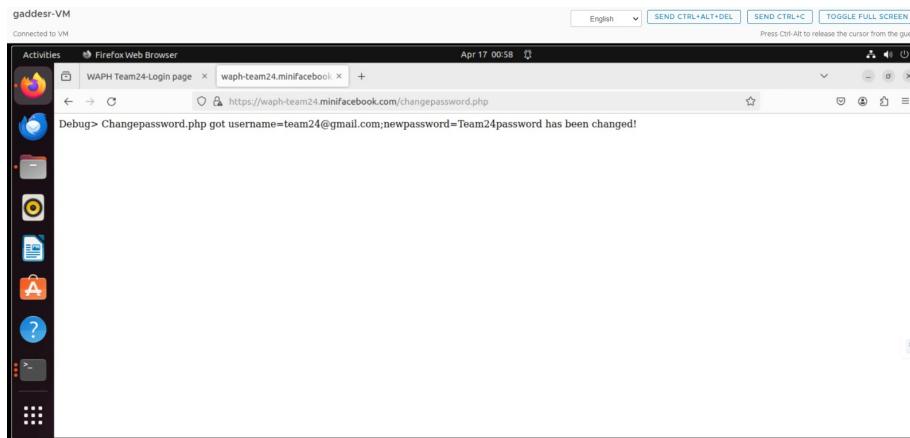


Figure 12: Changed\_password\_page

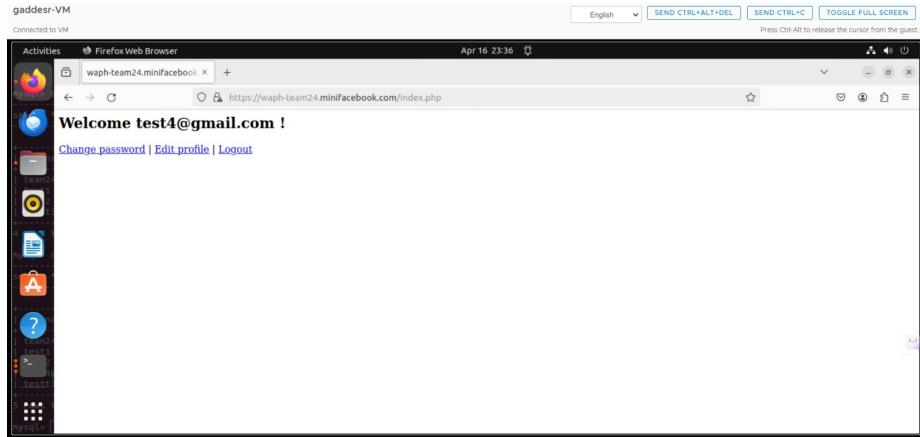


Figure 13: session auth.php code

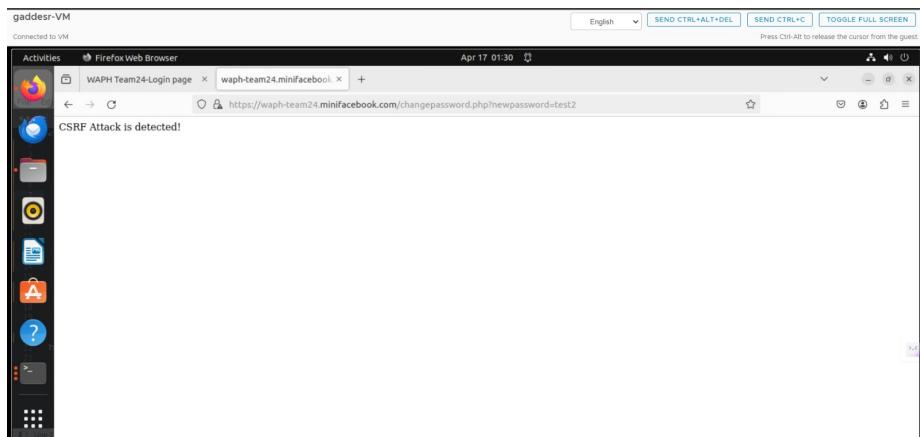


Figure 14: Attack\_detected

**session\_auth.php**

**Registration\_form.php**

**SPRINT : 2**

**Completed Tasks:**

**Task-1: Database Restructuring**

- Created new tables: posts, messages, comments for better data organization.

##### Task-2: User Post Viewing

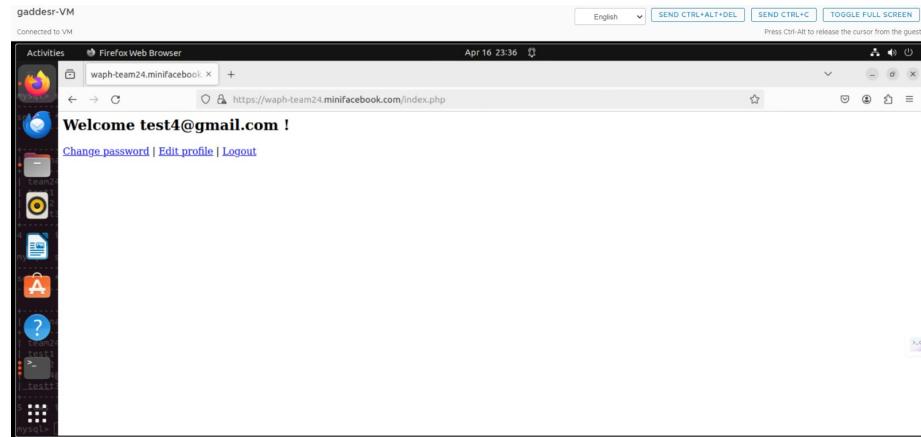


Figure 15: Registrationfprm.php code

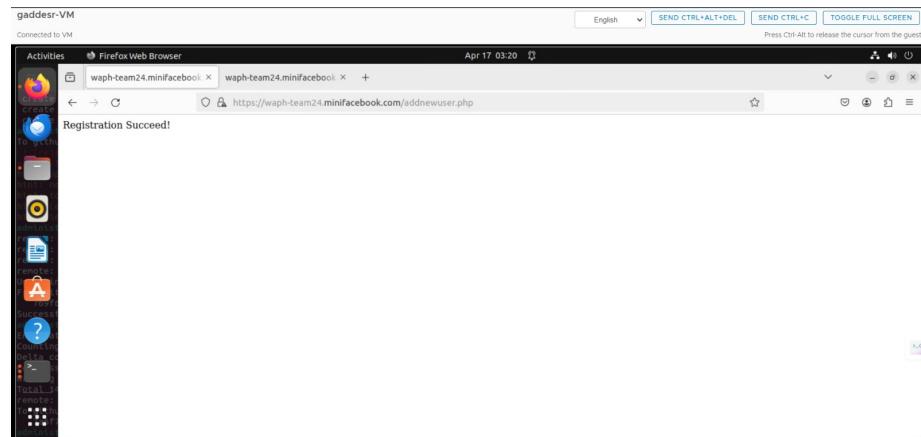


Figure 16: Registration\_form

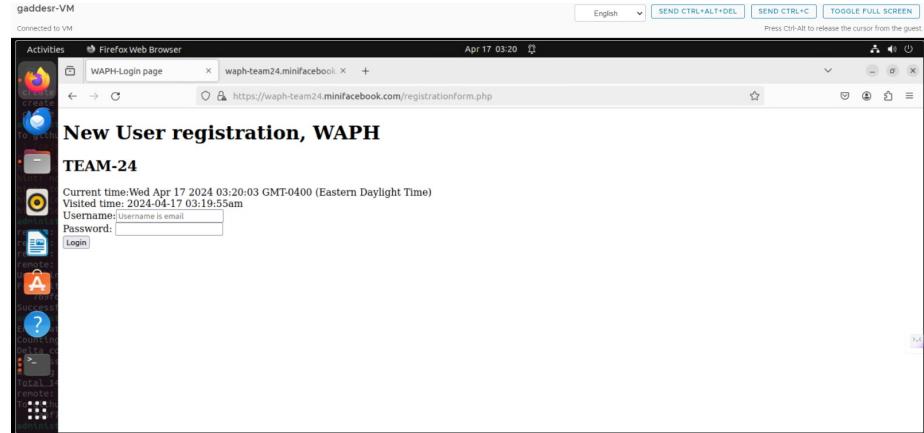


Figure 17: Successful\_registration

- Implemented functionality allowing users to view posts of other users post-login. ##### Task-3: User Post Creation
- Enabled users to add new posts post-login. ##### Task-4: Post Editing and Deletion
- Restricted post editing and deletion to the original user for security and control purposes. ##### Task-5: Post Comments
- Implemented the ability for users to comment on posts made by others. ##### Task-6: Documentation Update
- Updated the README file to reflect changes made in this sprint. c

#### **Team Members Contribution:**

1. Dilip Kumar Sanipina contribution in completing Task-3, Task-6, and updated Index.php file, 5 hours and 3 commits.
2. Sai Kumar Gadde contribution 2 commits, 3 hours, contributed in Task-4 frontend and backend, and also made changes to database.php file.
3. Siva Sai Manoj Korlepara Contributed in Task-5, and Task-4 delete post with 2 commits and 3 hours.
4. Uma Sathvik Meka contribution 2 commits, 3 hours, contributed in Task-3 and contributed in solve the bugs and documentation

#### **SPRINT :3**

#### **Completed Tasks:**

- Here we have created database for superuser and created super userform.

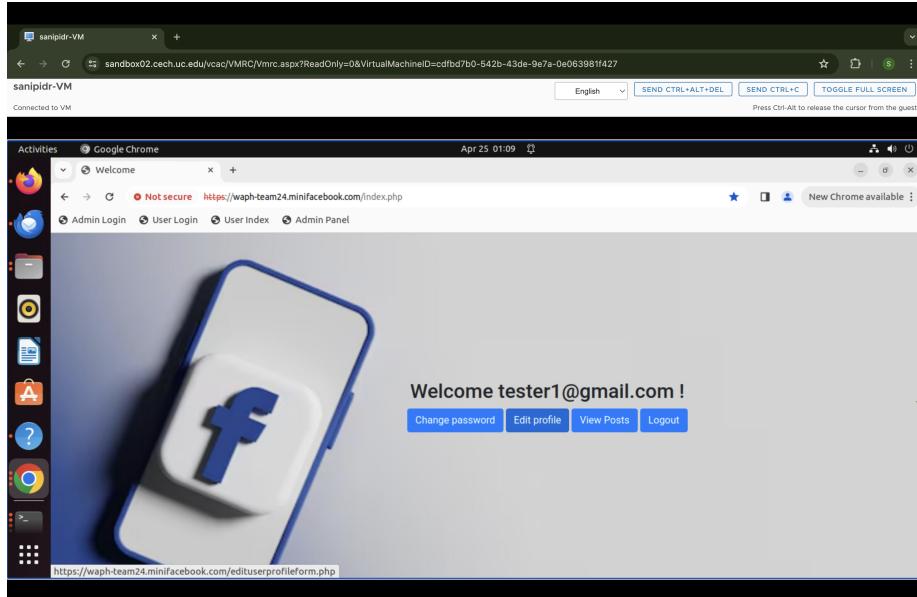


Figure 18: After\_Login\_Successfully

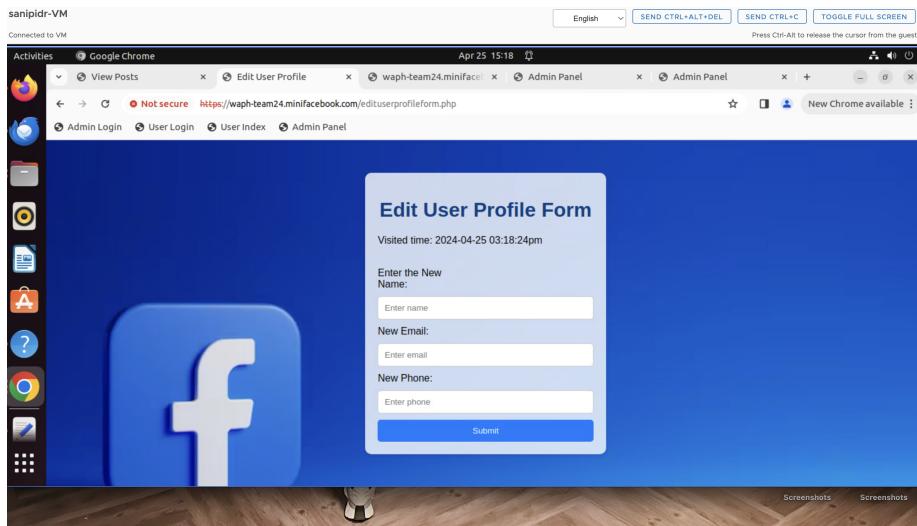


Figure 19: EditUser\_ProfileForm

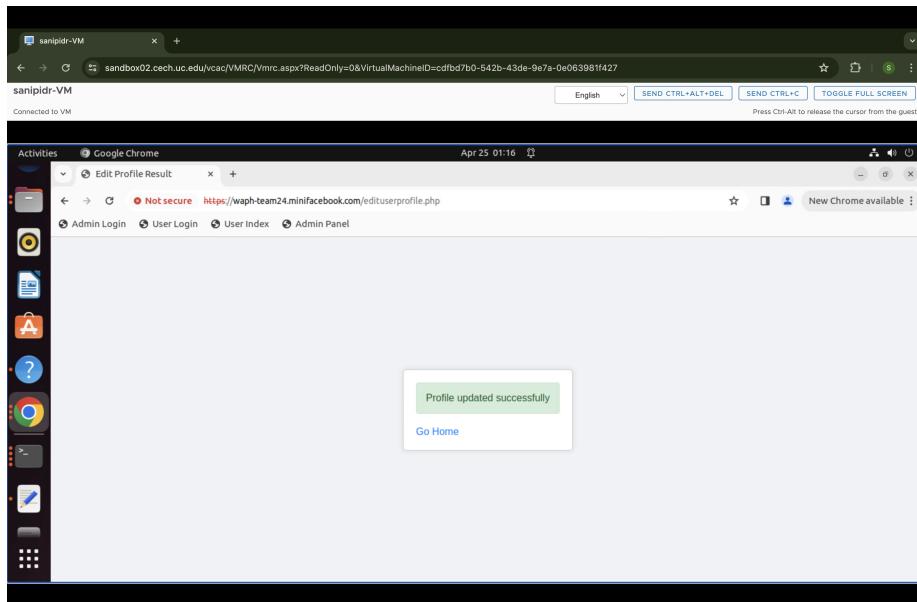


Figure 20: Profile Updated\_Successfully

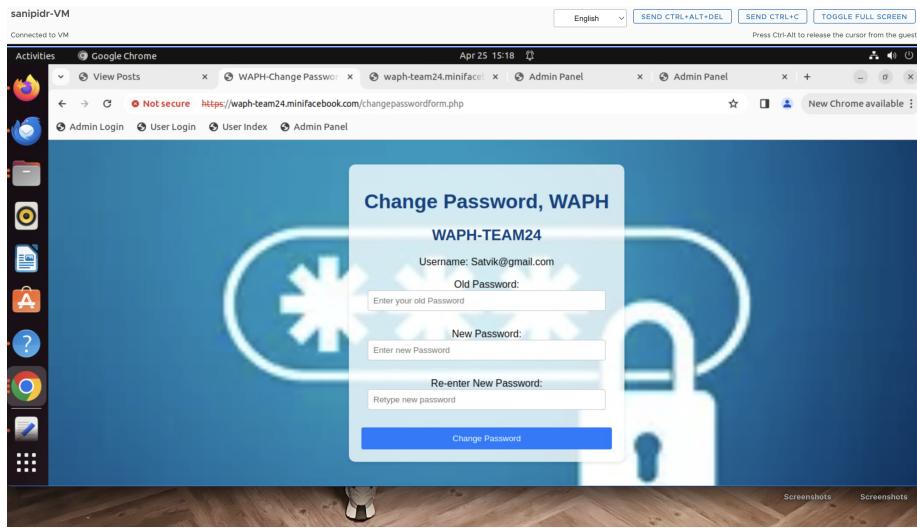


Figure 21: ChangePassword\_form

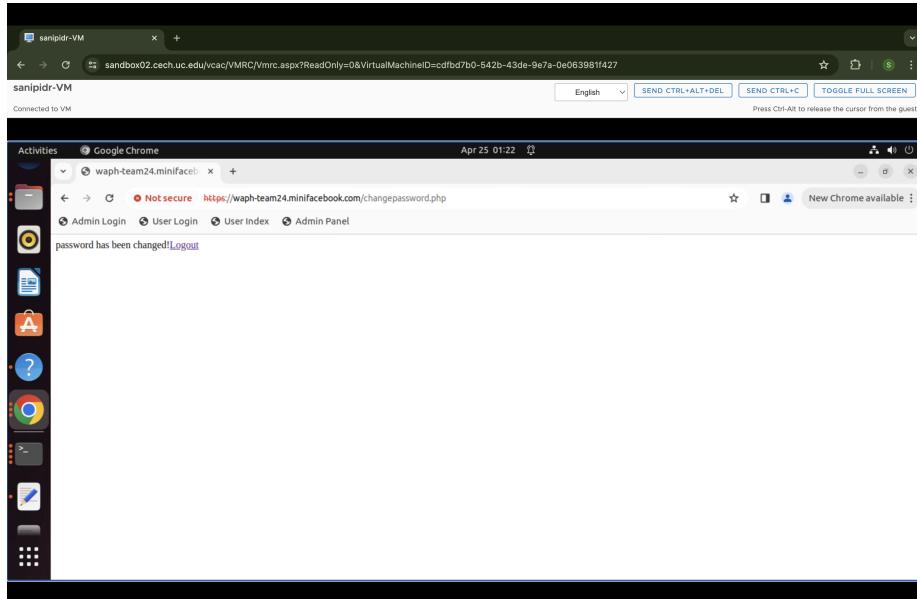


Figure 22: Password\_changed

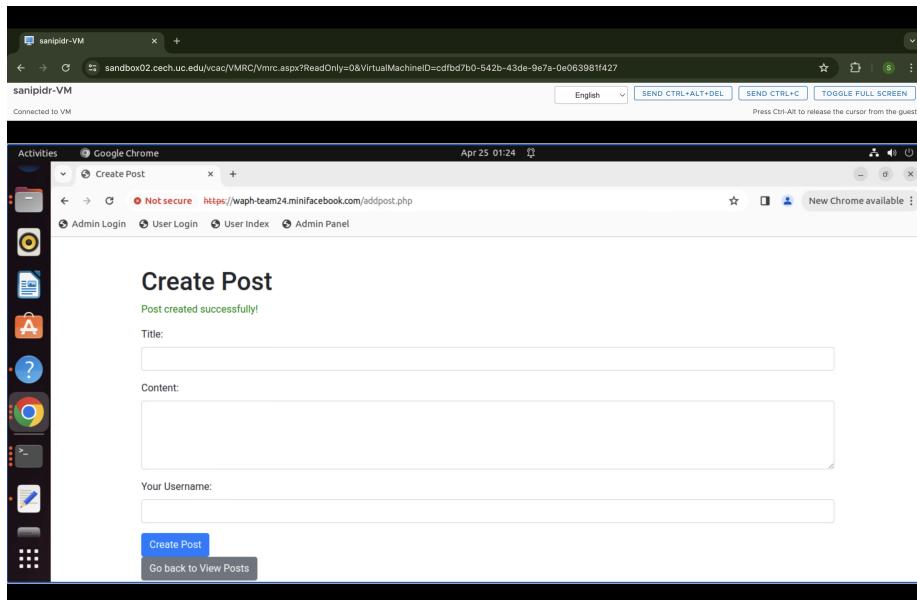


Figure 23: Creating Post

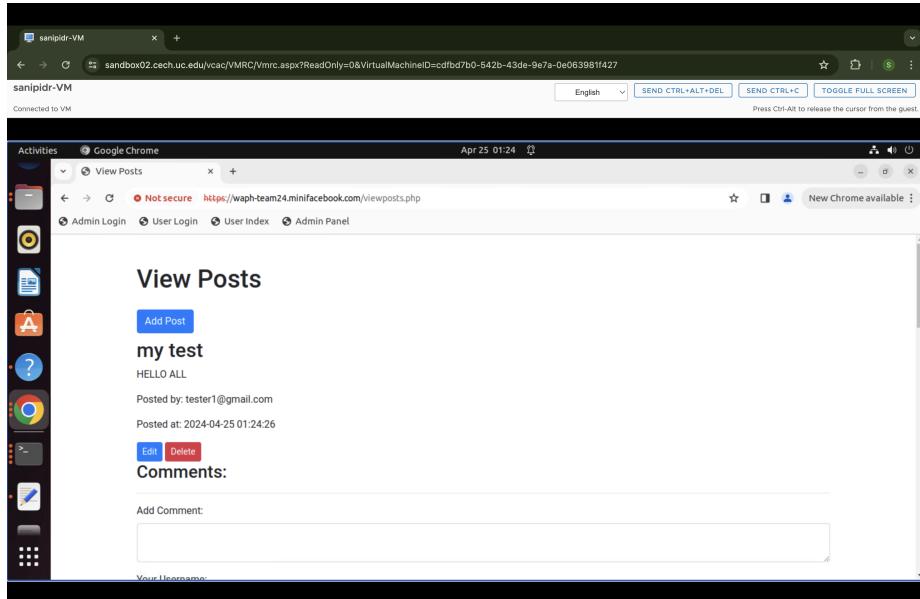


Figure 24: View Post

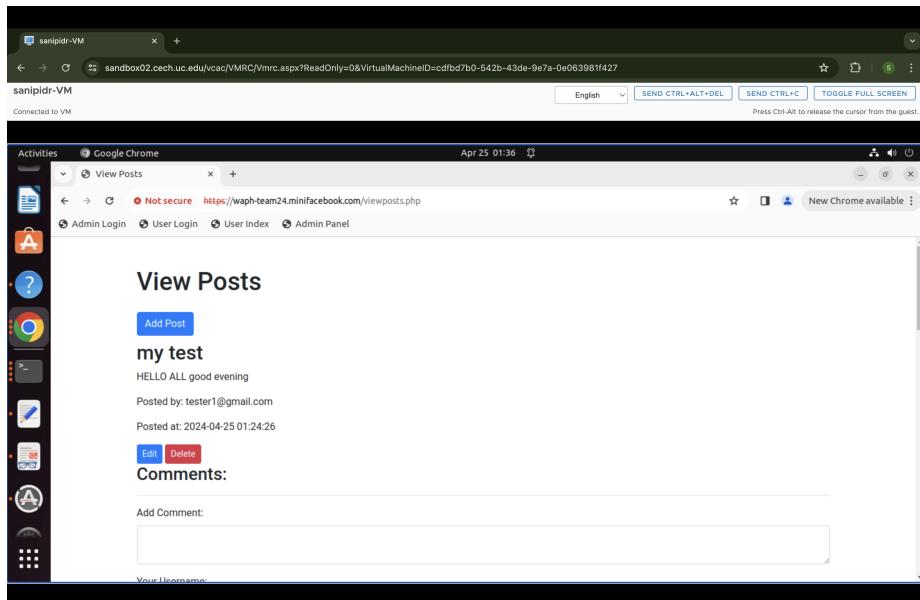


Figure 25: Comment\_Post

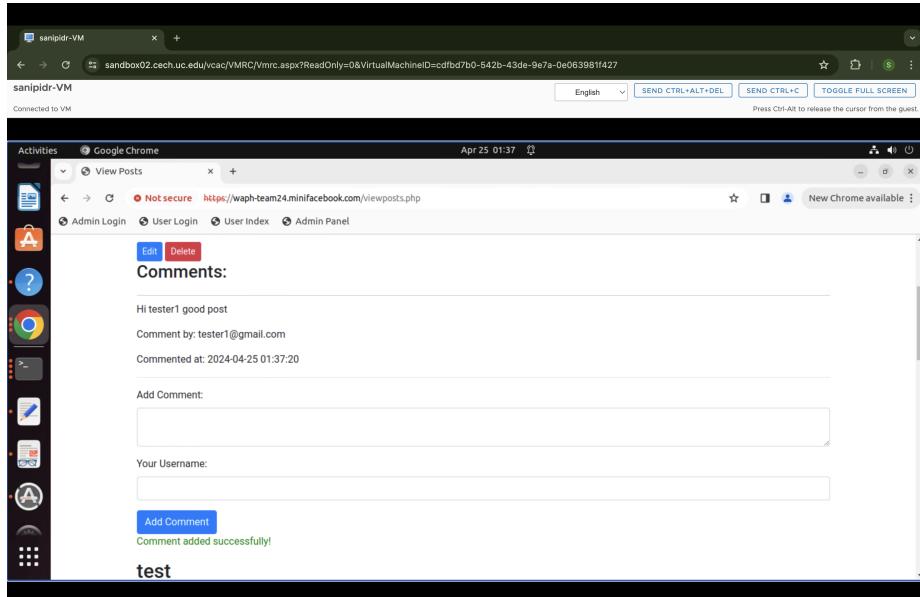


Figure 26: Comment Post

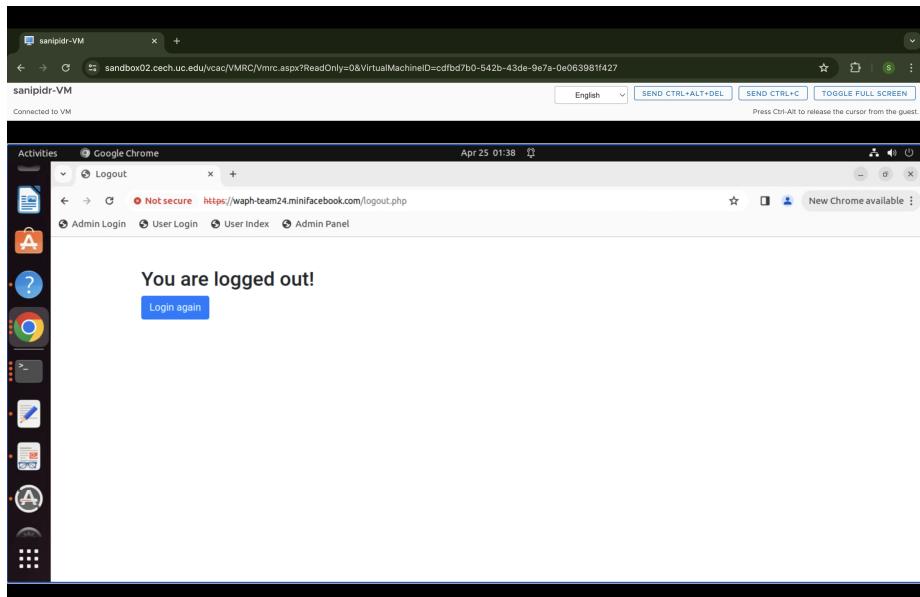


Figure 27: Log out

**Mini Facebook Admin Login Form**

WAPH-TEAM24

Current time: Thu Apr 25 2024 01:55:04  
GMT-0400 (Eastern Daylight Time)

Visited time: 2024-04-25 01:54:48am

Username: admin

Password: \*\*\*\*

Login

**Admin Panel**

Welcome, admin!

[Logout](#)

**User Management**

Username	Status	Action
dilipkumar@gmail.com	disabled	<a href="#">Enable User</a>
Manoj@gmail.com	active	<a href="#">Disable User</a>
Saikumar@gmail.com	active	<a href="#">Disable User</a>
Satvik@gmail.com	active	<a href="#">Disable User</a>
test1	active	<a href="#">Disable User</a>

## SECURITY AND NON-FUNCTATIONAL REQUIREMENTS

sanipidr-VM

Connected to VM

Activities Google Chrome Apr 25 22:45

View Posts Admin-Login page waph-team24.minifacebook.com Admin-Login page

Admin Login User Login User Index Admin

Certificate Viewer: waph-team24

General Details

Issued To

- Common Name (CN) waph-team24
- Organization (O) University of Cincinnati
- Organizational Unit (OU) Web Application Programming and Hacking

Issued By

- Common Name (CN) waph-team24
- Organization (O) University of Cincinnati
- Organizational Unit (OU) Web Application Programming and Hacking

Validity Period

- Issued On Tuesday, April 2, 2024 at 3:34:44 AM
- Expires On Wednesday, April 2, 2025 at 3:34:44 AM

SHA-256 Fingerprints

- Certificate 1b566d7969a1b6341990e2f16942d1f8b2b7697f0174607e95eb64
- Public Key 63d3fcdf 2275520150e131d161334d669ae095a037b6517edba cb968af66 8bf984a07

sanipidr-VM

Connected to VM

Activities Terminal Apr 25 22:47

administrator@mwh-vm: ~/waph-teamproject

```

+----+-----+-----+-----+-----+-----+-----+
| test2 | ad0234829205b9933196ba810f7a872b | NULL | NULL | NULL | 1234567789 | disabled |
+----+-----+-----+-----+-----+-----+-----+
6 row In set (0.00 sec)

mysql> select * from users;
+-----+-----+-----+-----+-----+-----+-----+
| username | password | fullname | otheremail | phone | status |
+-----+-----+-----+-----+-----+-----+-----+
| dillpkumar@gmail.com | 3cc31cd246149aec68079241e71e98f6 | Dilli Kumar | santipidr@gmail.com | 5132002741 | disabled | |
| Manoj@gmail.com | 3cc31cd246149aec68079241e71e98f6 | Manoj | korpelsj@gmail.com | 5132002741 | active |
| Sakumara@gmail.com | 3cc31cd246149aec68079241e71e98f6 | Silva Sal Manojo | Salumar284@gmail.com | 7005514321 | active |
| Satvik@gmail.com | 3cc31cd246149aec68079241e71e98f6 | Satvik Meka | Mekag@gmail.com | 5132002749 | active |
| test1 | Sa105eb89404e1329780dd62e226508a | NULL | NULL | NULL | active |
| test2 | ad0234829205b9933196ba810f7a872b | NULL | NULL | NULL | disabled |
| test3@gmail.com | 3cc31cd246149aec68079241e71e98f6 | test3 | NULL | NULL | 1234567789 | disabled |
+-----+-----+-----+-----+-----+-----+
7 row In set (0.00 sec)

mysql> select * from users;
+-----+-----+-----+-----+-----+-----+-----+
| username | password | fullname | otheremail | phone | status |
+-----+-----+-----+-----+-----+-----+
| dillpkumar@gmail.com | 3cc31cd246149aec68079241e71e98f6 | Dilli Kumar | santipidr@gmail.com | 5132002741 | disabled | |
| Manoj@gmail.com | 3cc31cd246149aec68079241e71e98f6 | Manoj | korpelsj@gmail.com | 5132002741 | active |
| Sakumara@gmail.com | 3cc31cd246149aec68079241e71e98f6 | Silva Sal Manojo | Salumar284@gmail.com | 7005514321 | active |
| Satvik@gmail.com | 3cc31cd246149aec68079241e71e98f6 | Satvik Meka | Mekag@gmail.com | 5132002749 | active |
| test1 | Sa105eb89404e1329780dd62e226508a | NULL | NULL | NULL | active |
| test2 | ad0234829205b9933196ba810f7a872b | NULL | NULL | NULL | disabled |
| test3@gmail.com | 3cc31cd246149aec68079241e71e98f6 | test3 | NULL | NULL | 1234567789 | disabled |
+-----+-----+-----+-----+-----+
7 rows In set (0.00 sec)

mysql>
```

```

function addnewuser($username, $password, $otheremail,$fullname,$phone) {
    global $mysqli;
    $prepared_sql ="INSERT INTO users (username,password,otheremail,fullname,phone) VALUES (?,md5(?),?, ?,?)";
    $stmt = $mysqli->prepare($prepared_sql);
    $stmt-> bind_param("sssss",$username,$password,$otheremail,$fullname,$phone);
    if($stmt->execute()) return TRUE;
    return FALSE;
}

```

Chrome File Edit View History Bookmarks Profiles Tab Window Help

Thu Apr 25 11:10PM

sandbox02.cech.uc.edu/vcac/VmRC/vmrc.aspx?ReadOnly=0&VirtualMachineID=cdfbd7b0-542b-43de-9e7a-0e06398f1427

sanipidr-VM Connected to VM

Activities

Google Chrome Apr 25 23:10

View Posts Admin-Login page WAPH-Login page

Admin Login User Login User Index Admin Panel

**WAPH-TEAM24**

Current time: 4/25/2024, 11:10:24 PM

Username:

A part following '@' should not contain the symbol '<'.

Retype Password:

Re-enter the Password

Fullname:

Please provide fullname

Other Email:

Please provide email

Phone:

Please provide phonenumber

Register

addnewuser.php

```

18     if(isset($_username) and isset($_password))
19     {
20         $username=sanitize_input($_POST['username']);
21         $password=sanitize_input($_POST['password']);
22         $email=sanitize_input($_POST['email']);
23         $name=sanitize_input($_POST['name']);
24         $contact = sanitize_input($_POST['contact']);
25
26         #input length check
27         if(strlen($username) < 3)
28         {
29             ?>
30             <div class="title">
31                 Invalid Length for username : <?php echo htmlentities($username);?>!
32             </div>
33             <?php
34         }
35         else if(strlen($password) < 8)
36         {
37             ?>
38             <div class="title">
39                 Invalid Length in password for Username: <?php echo htmlentities($username);?>!
40             </div>
41             <?php
42         }
43         else if(strlen($email)< 3 || strlen($name)<1)
44         {
45             ?>
46             <div class="title">
47                 Invalid Length in email for Username : <?php echo htmlentities($username);?>!
48             </div>
49             <?php
50         }
51         else if(strlen($name)<1)
52         {
53             ?>
54             <div class="title">
55                 Invalid Length in name for Username : <?php echo htmlentities($username);?>!
56             </div>
57             <?php
58         }
59         else if(strlen($contact)<10)
60         {
61             ?>
62             <div class="title">
63                 Invalid Length in contact for Username : <?php echo htmlentities($username);?>!
64             </div>
65             <?php
66         }
67
68         //Reg exp check
69         else if (!preg_match('/^([a-zA-Z]+[a-zA-Z-0-9_]+)$/', $username))
70         {
71             ?>
72             <div class="title">
73                 Invalid pattern matching for Username input <?php echo htmlentities($username);?>!
74             </div>
75             <?php
76         }

```

Line 46, Column 15

main PHP Tab Size: 4

github.com/waph-team24/waph-teamproject/blob/main/session\_auth.php

```

session_start();
if(!isset($_SESSION['authenticated']) || $_SESSION['authenticated']!= TRUE){
$_SESSION['authenticated']=TRUE;
$_SESSION['nocsrftoken']=md5(uniqid(rand(),true));
setcookie("nocsrftoken",$_SESSION['nocsrftoken'],time()+(60*60*24),"/");
}
if($_SESSION['nocsrftoken'] != $_SERVER['HTTP_USER_AGENT']){
$_SESSION['authenticated']=FALSE;
$_SESSION['nocsrftoken']=md5(uniqid(rand(),true));
setcookie("nocsrftoken",$_SESSION['nocsrftoken'],time()+(60*60*24),"/");
}
header("Refresh: 0; url=form.php");
die();
}
if($_SESSION['authenticated']) {
$_SESSION['authenticated']=TRUE;
$_SESSION['nocsrftoken']=md5(uniqid(rand(),true));
setcookie("nocsrftoken",$_SESSION['nocsrftoken'],time()+(60*60*24),"/");
}
echo "Session hijacking attack is detected!";
header("Refresh: 0; url=form.php");
die();
}

```

Connected to VM

Activities    Google Chrome    April 25 23:19

View Posts    Admin-Login page    View Posts    waph-team24.minifacebook.com

Admin Login    User Login    User Index    Admin Panel

CSRF Attack detected

sanipidr-VM

Connected to VM

Username	Status	Action
dilipkumar@gmail.com	disabled	<b>Enable User</b>
Manoj@gmail.com	active	Disable User
Saikumar@gmail.com	active	Disable User
Satvik@gmail.com	active	Disable User

sanipidr-VM

Connected to VM

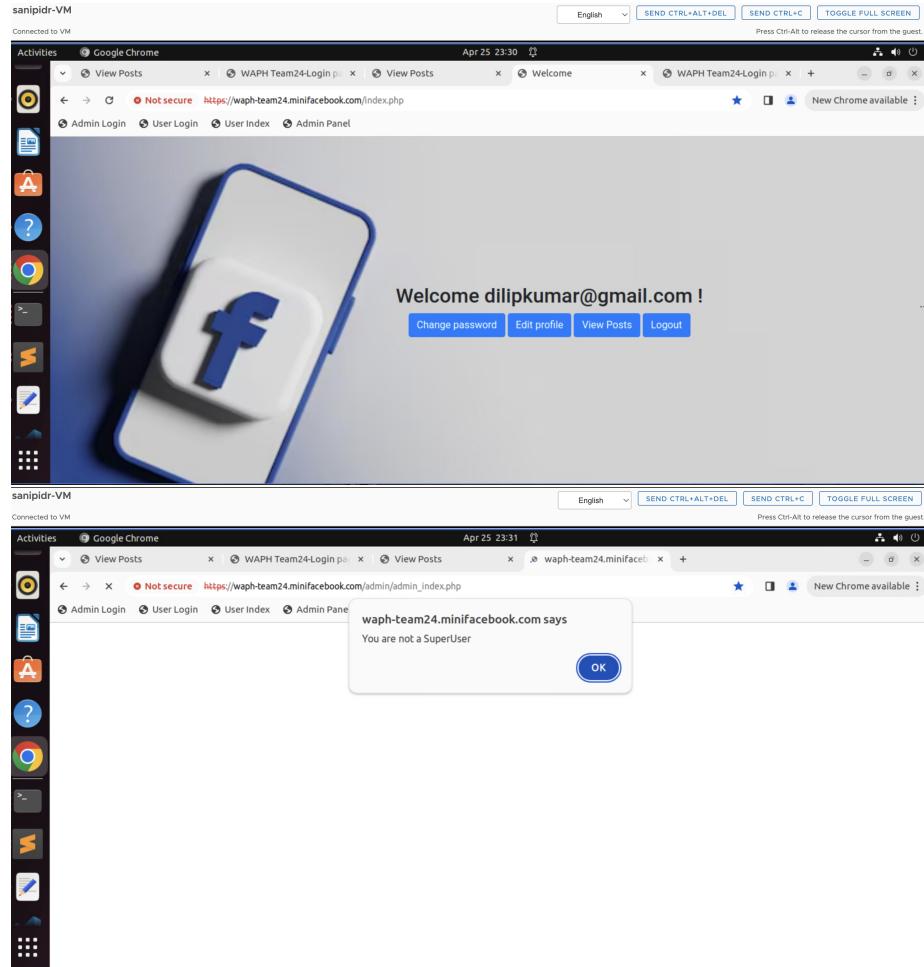
waph-team24.minifacebook.com says  
Your Account is disabled

OK

sanipidr-VM

Connected to VM

Username	Status	Action
<b>dilipkumar@gmail.com</b>	active	Disable User
Manoj@gmail.com	active	Disable User
Saikumar@gmail.com	active	Disable User
Satvik@gmail.com	active	Disable User



A screenshot of a GitHub code editor interface. The tab bar at the top shows 'Code' (selected), 'Blame', 'Executable File · 112 lines (106 loc) · 3.66 KB', and 'Code 55% faster with GitHub Copilot'. On the right side of the header are buttons for 'Raw', 'Copy', 'Download', 'Edit', and 'File'. The main area contains the following CSS code:

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4 <meta charset="utf-8">
5 <title>WAPH-Login page</title>
6 <style>
7   body {
8     font-family: Arial, sans-serif;
9     background-color: #768d9;
10    margin: 0;
11    padding: 0;
12    display: flex;
13    justify-content: center;
14    align-items: center;
15    height: 100vh;
16  }
17  h1, h2 {
18    text-align: center;
19    color: #333;
20  }
21  #digit-clock {
22    text-align: center;
23    font-size: 18px;
24    margin-bottom: 20px;
25  }
26  .container {
27    width: 350px;
28    background-color: #fff;
29    padding: 20px;
30    border-radius: 10px;
31    box-shadow: 0 2px 5px rgba(0, 0, 0, 0.1);
32  }
33  .form.login {
```

## Appendix