[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.github.io

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.github.io

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.

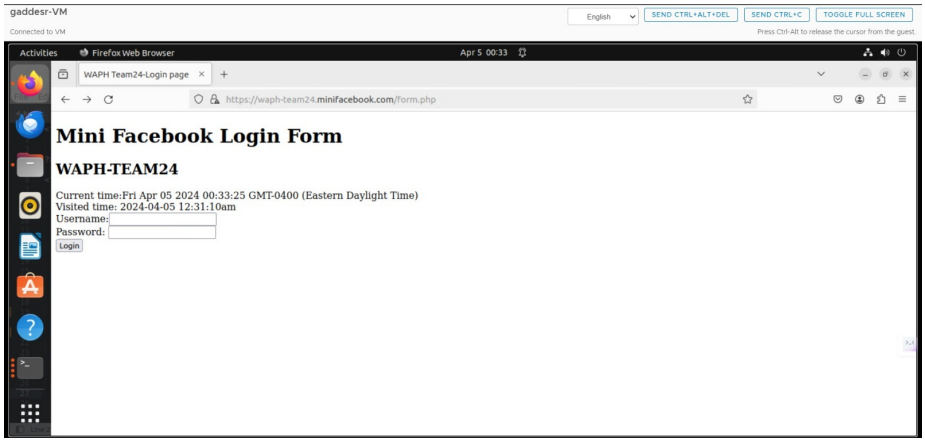


Figure 1: Login_Form

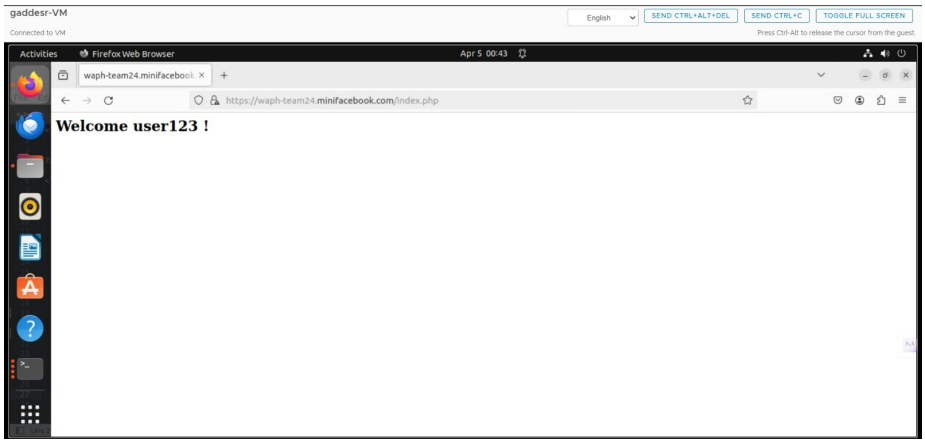


Figure 2: sucessful_Login

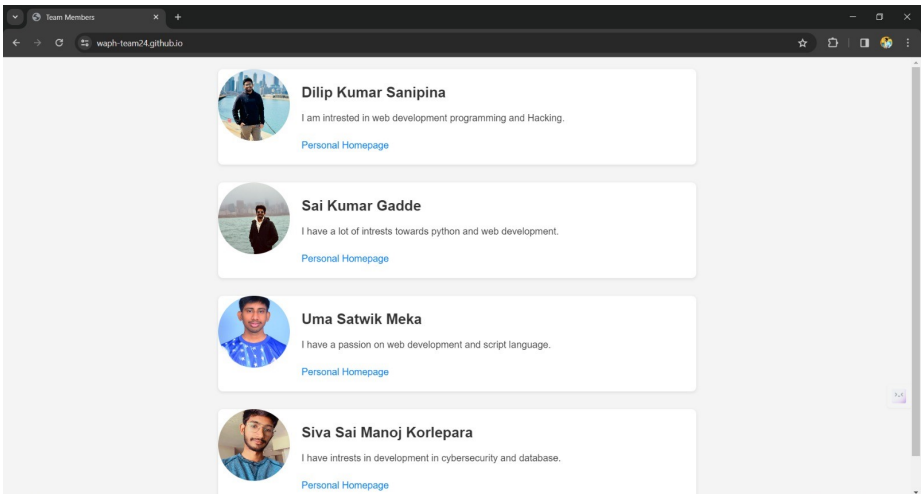


Figure 3: Team_members_personalPage

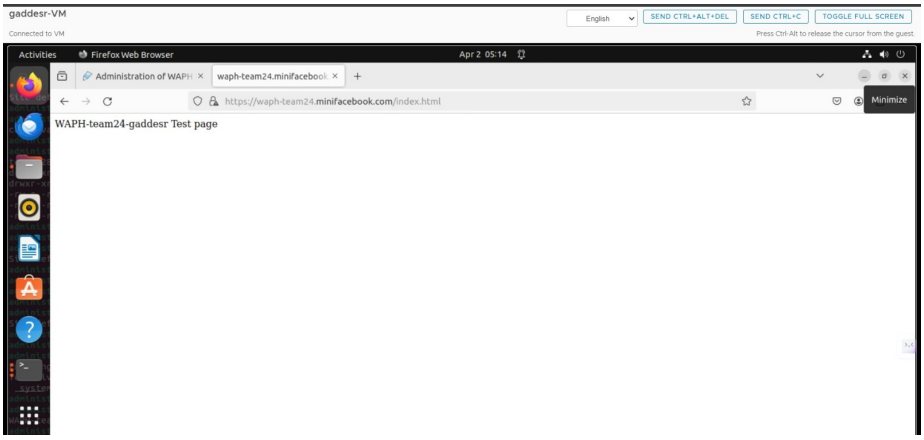


Figure 4: Test_page_gaddesr

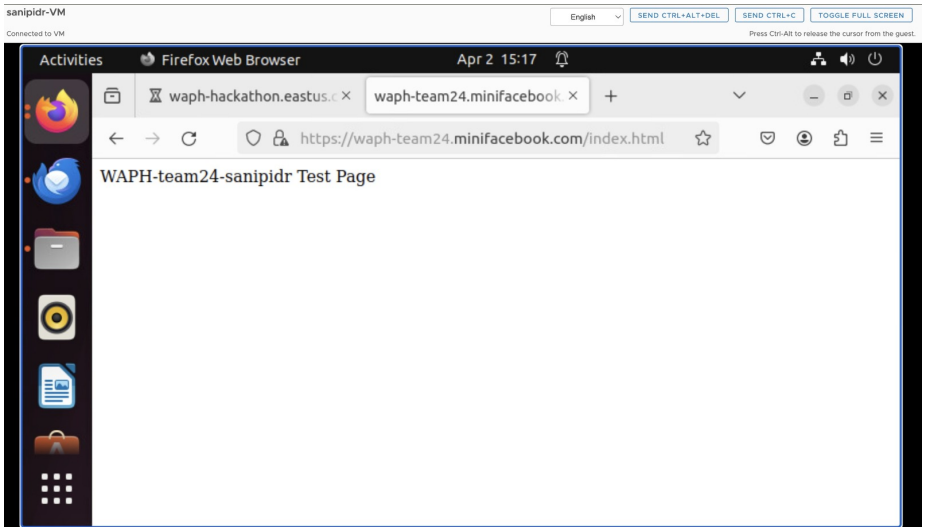


Figure 5: Test_page_sanipidr

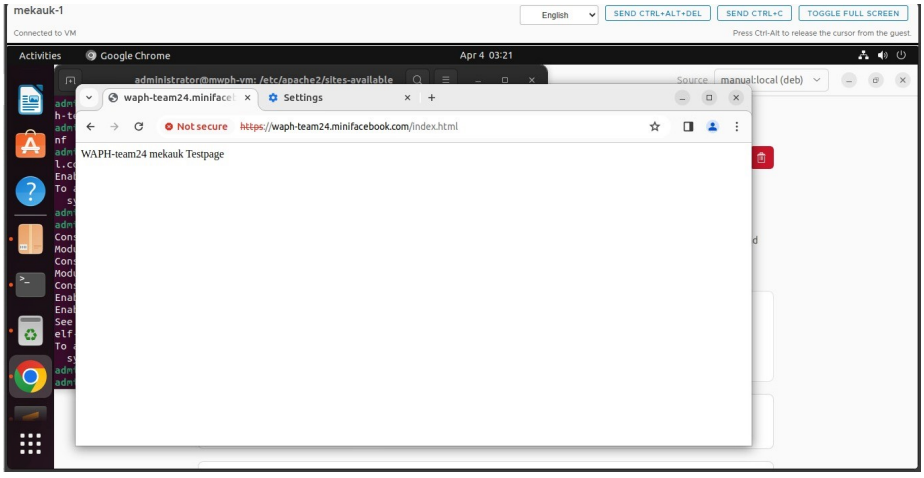


Figure 6: Test_page_mekauk

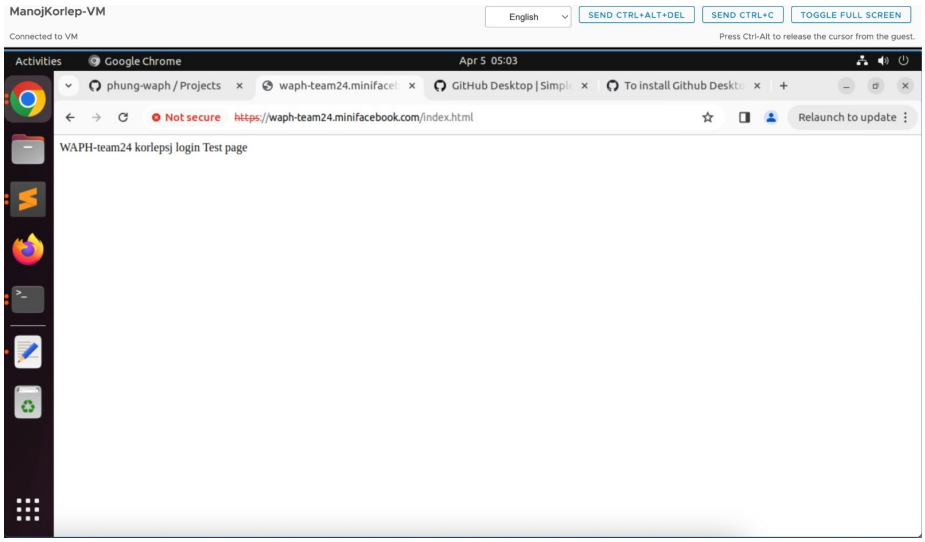


Figure 7: Test_page_korlepsj

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 modificarion 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'));

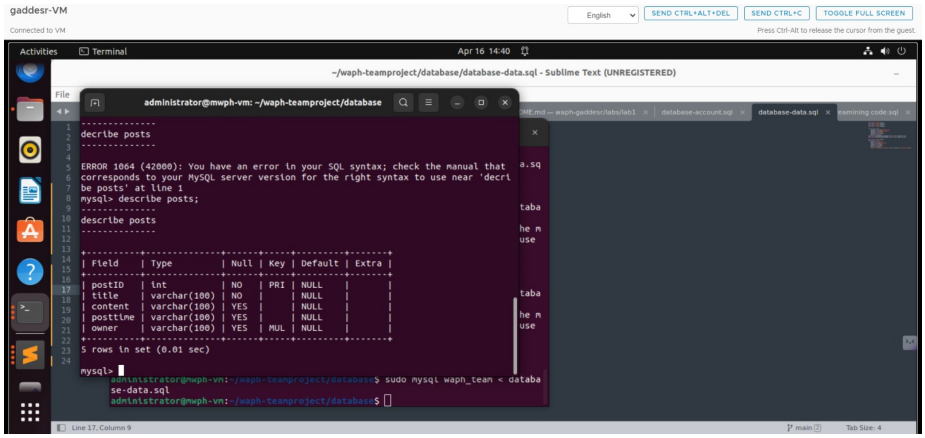


Figure 8: database-data

- 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

changepassword.php

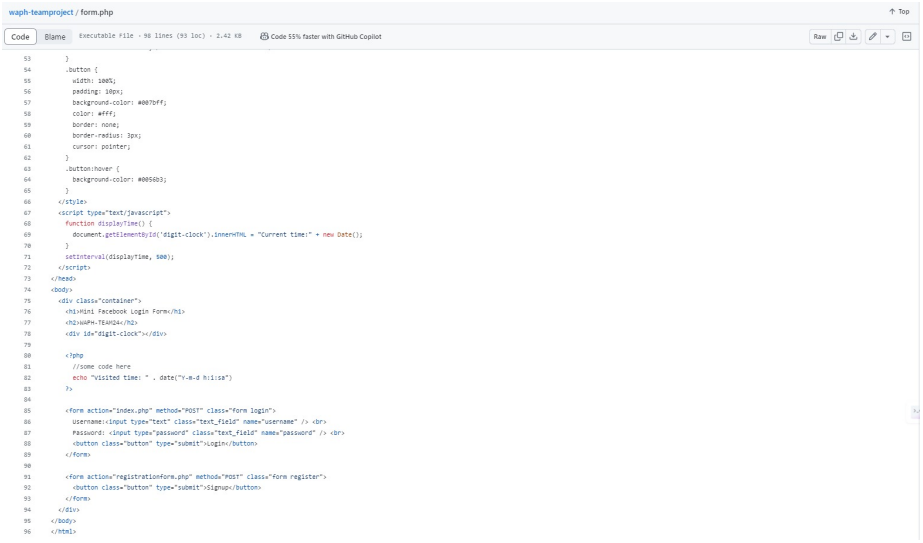


Figure 9: form.php code

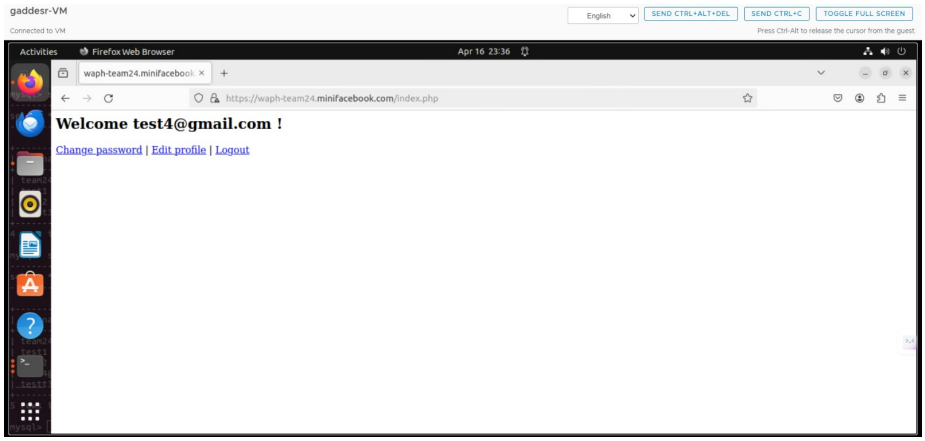


Figure 10: successful_login_page

waph-teamproject / changepassword.php

sanipidr ..

dd8c578 · 19 hours ago History

Code Blame Executable File · 26 lines (23 loc) · 1001 Bytes Code 55% faster with GitHub Copilot Raw

```php
<?php
  require "session_auth.php";
  require "database.php";
  $token = $_POST['nocsrftoken'];
  if ((isset($token) or $token!=$_SESSION['nocsrftoken']) {
    echo "CSRF Attack is detected!";
    die();
  }
  $username = $_SESSION['username'];
  $oldpassword = $_REQUEST['oldpassword'];
  $newpassword = $_REQUEST['newpassword'];

  if (isset($username) and isset($oldpassword) and isset($newpassword) ){
   //  echo "Debug> Changepassword.php got username=$username;newpassword=$newpassword";
    echo "password has been changed!<a href='https://waph-team24.minifacebook.com/logout.php'>Logout</a>";
      if(changepassword($username,$oldpassword,$newpassword)){
           echo "password has been changed!<a href='https://waph-team24.minifacebook.com/logout.php'>Logout</a>";
      }else{
           echo " Change password Failed!<a href='https://waph-team24.minifacebook.com/logout.php'>Logout</a>";
      }
  }else{
    echo " No username/password provided!";
  }

?>
```

Figure 11: chnagepassword.php code

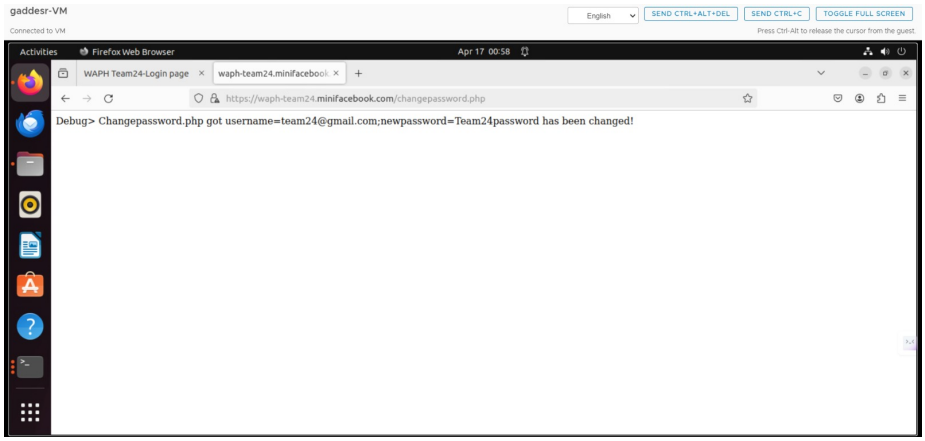


Figure 12: Changed_password_page

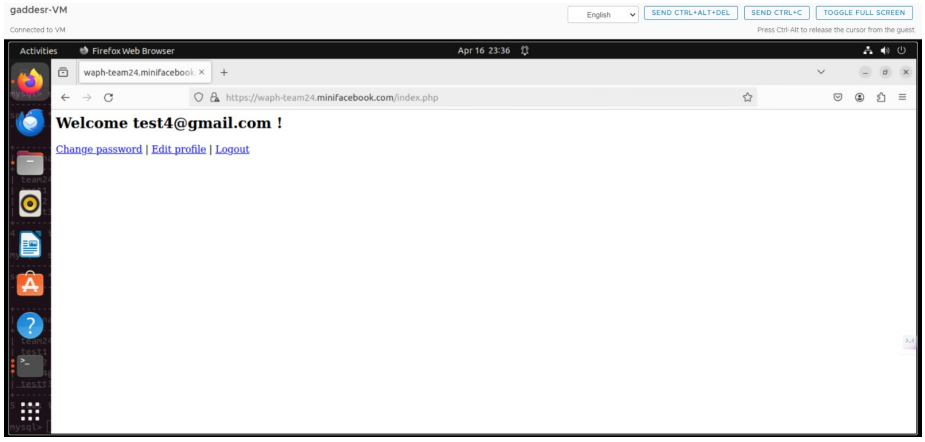


Figure 13: session auth.php code

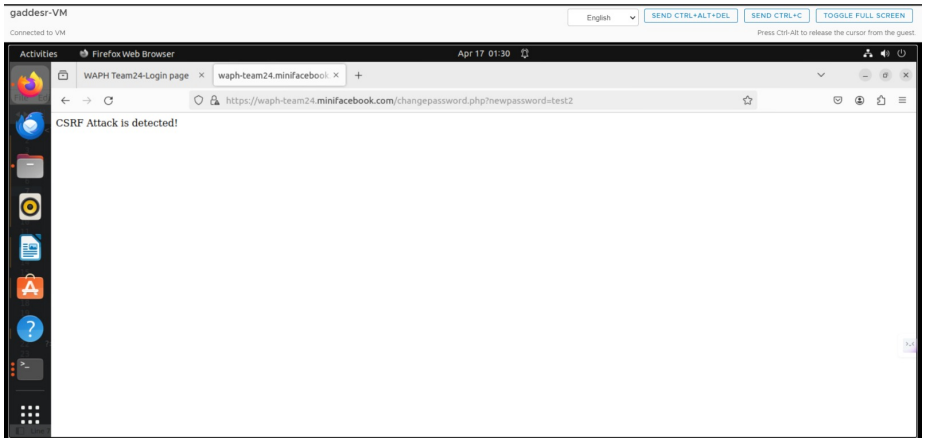


Figure 14: Attack_detected

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

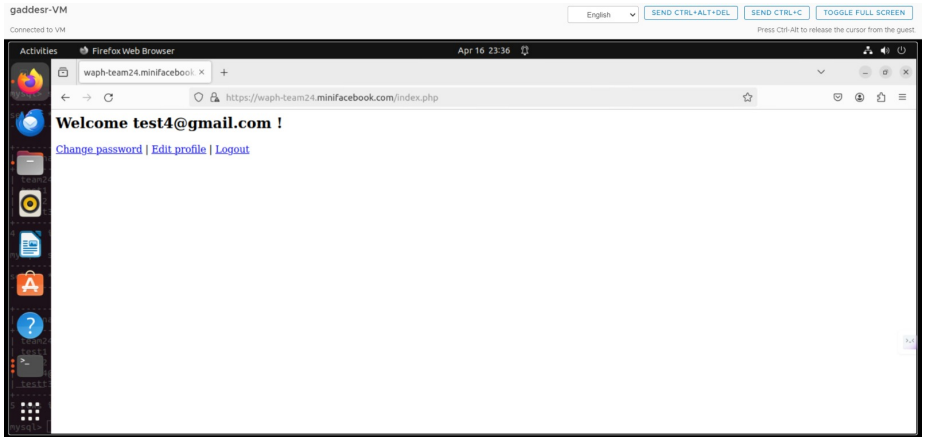


Figure 15: Registrationfprm.php code

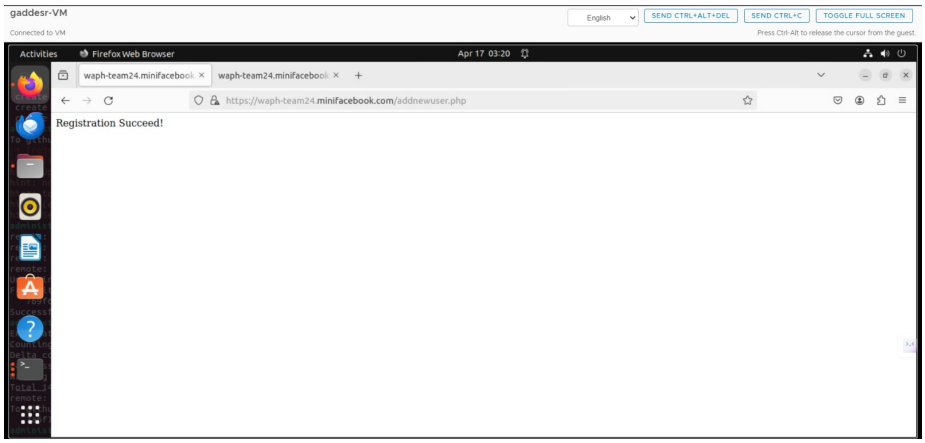


Figure 16: Registration_form

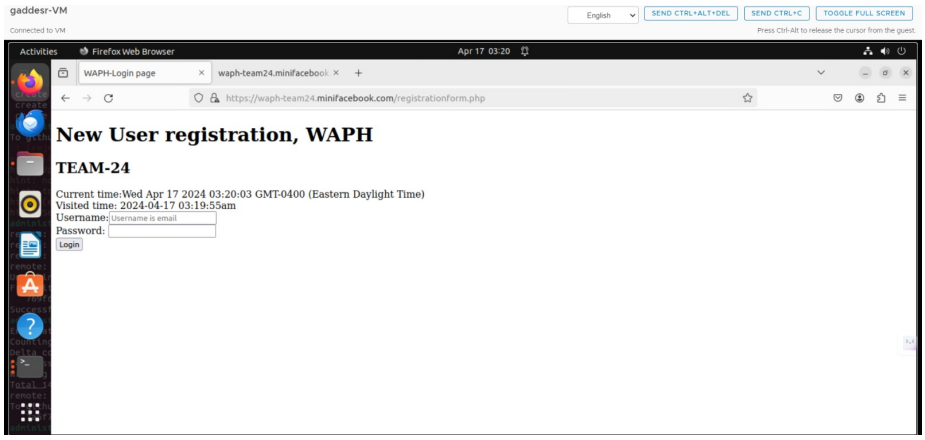


Figure 17: Successful_registration

- 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.

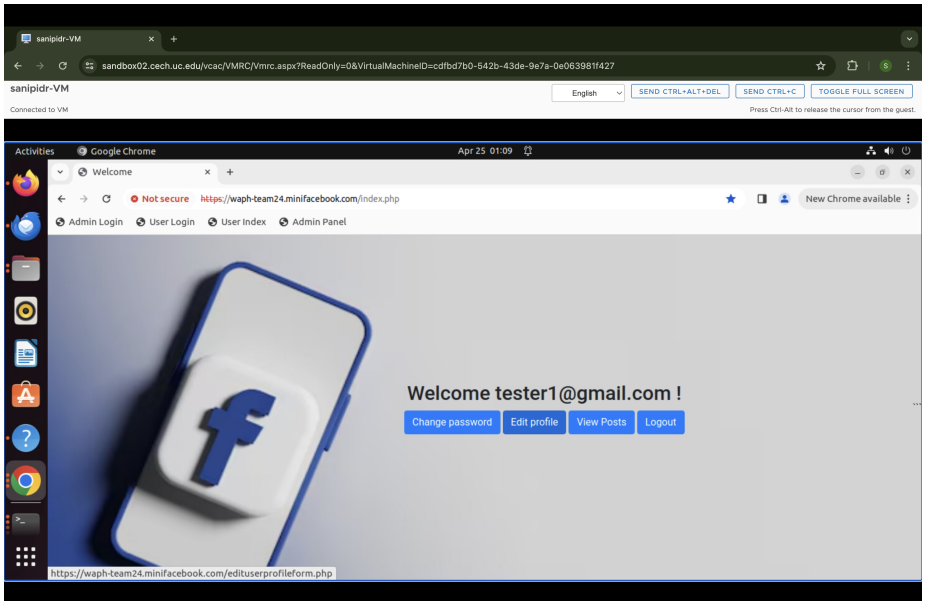


Figure 18: After_Login_Successfully

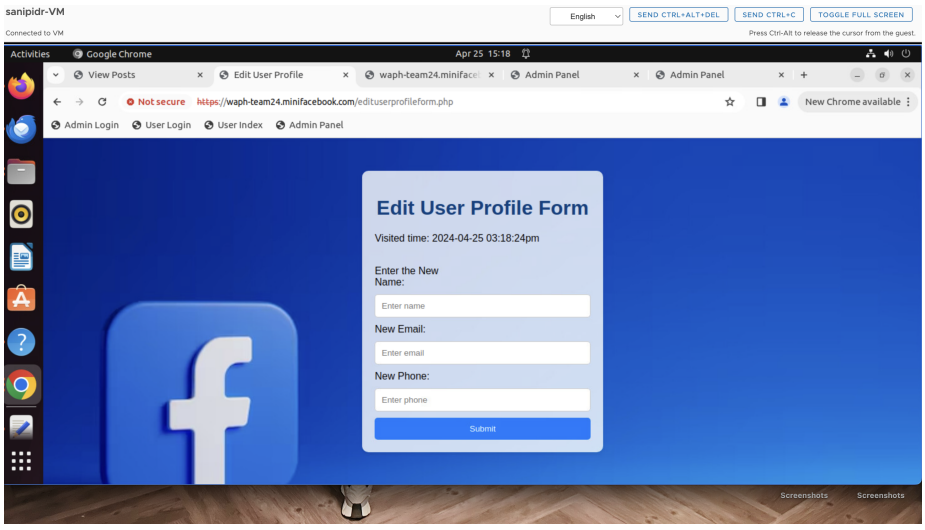


Figure 19: EditUser_ProfileForm

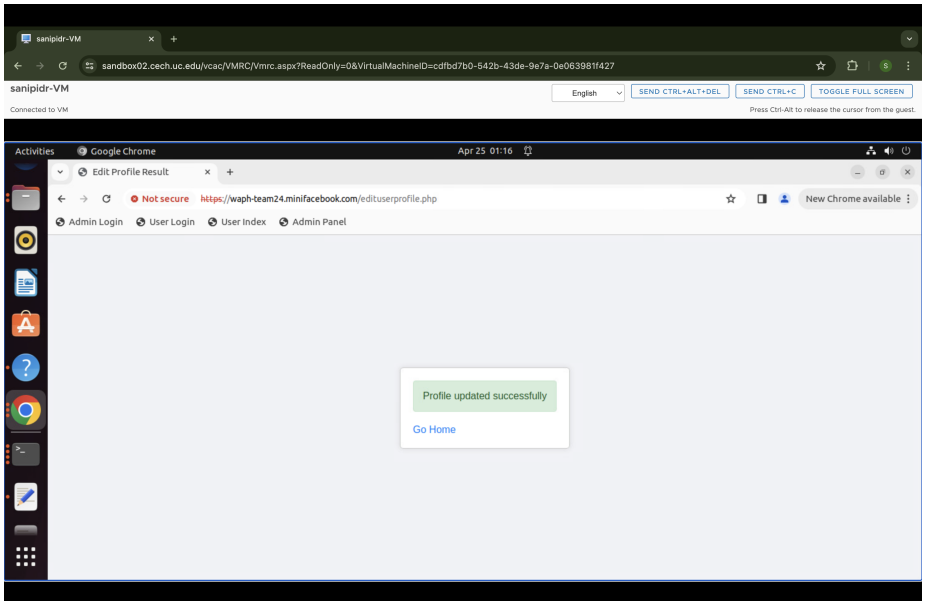


Figure 20: Profile Updated_Successfully

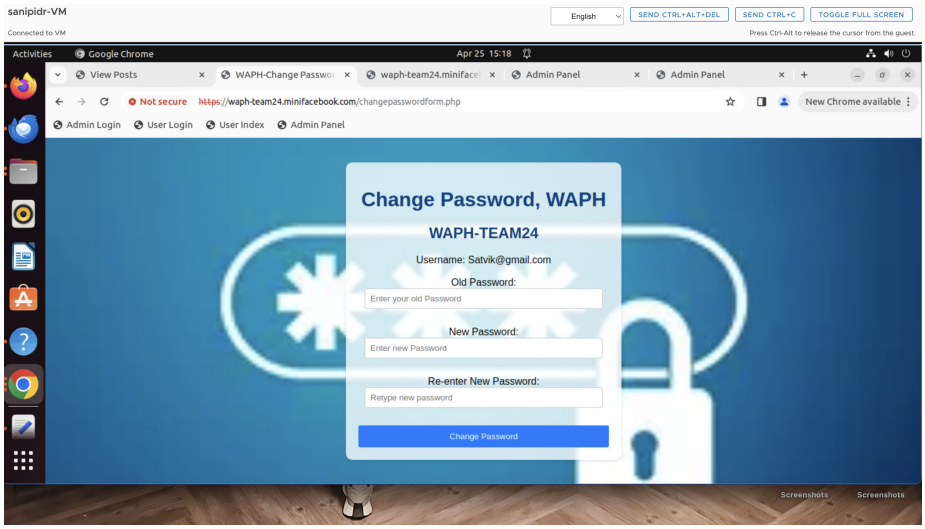


Figure 21: ChangePassword_form

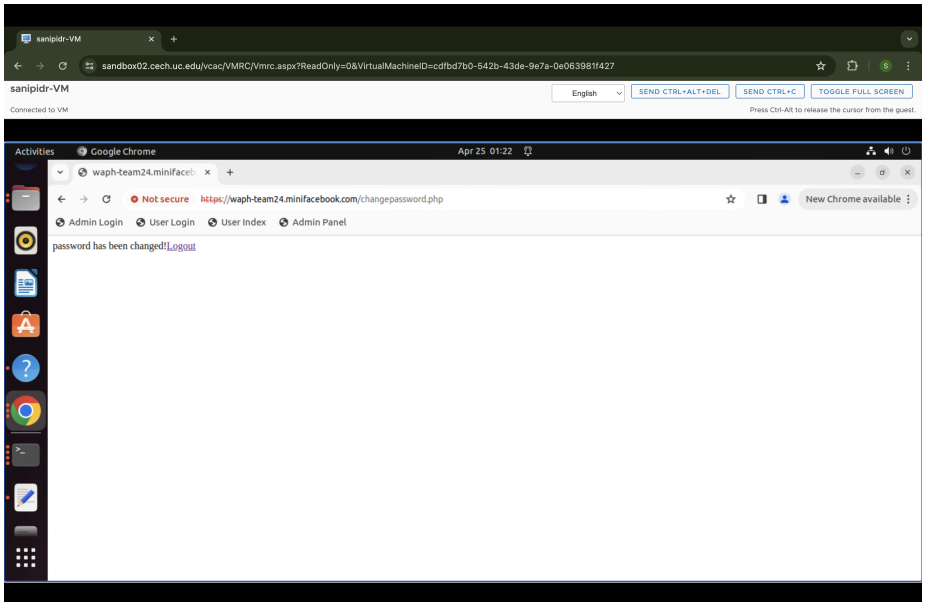


Figure 22: Password_changed

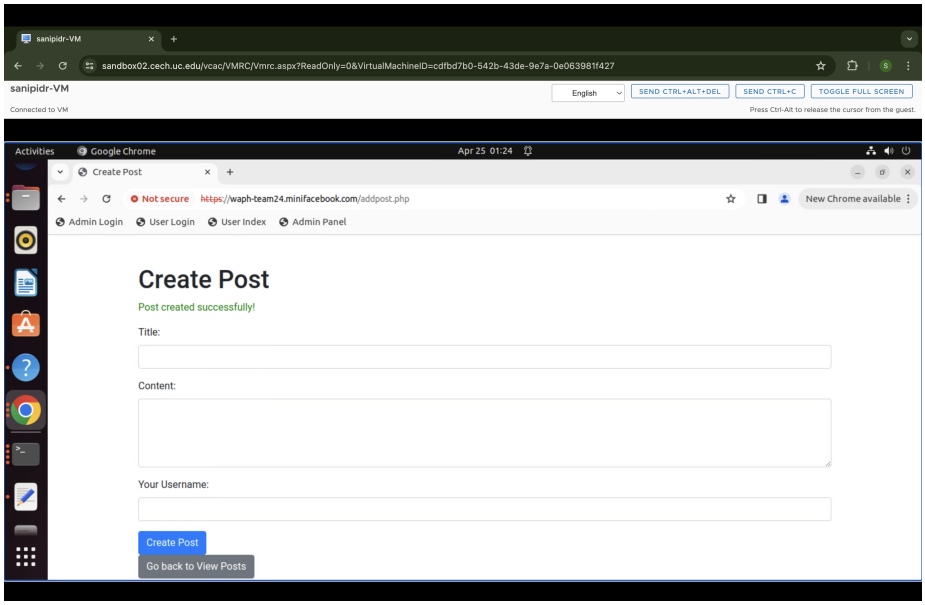


Figure 23: Creating Post

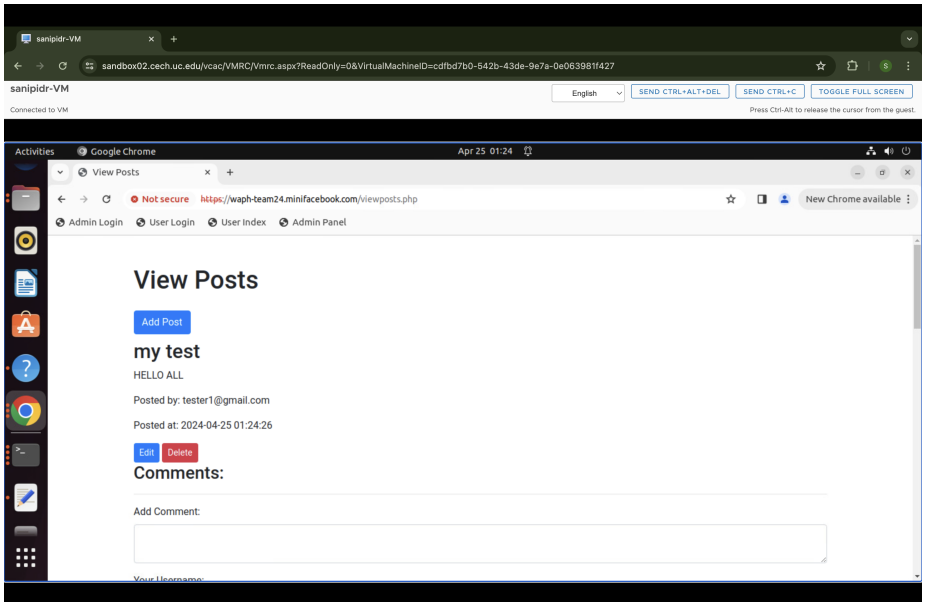


Figure 24: View Post

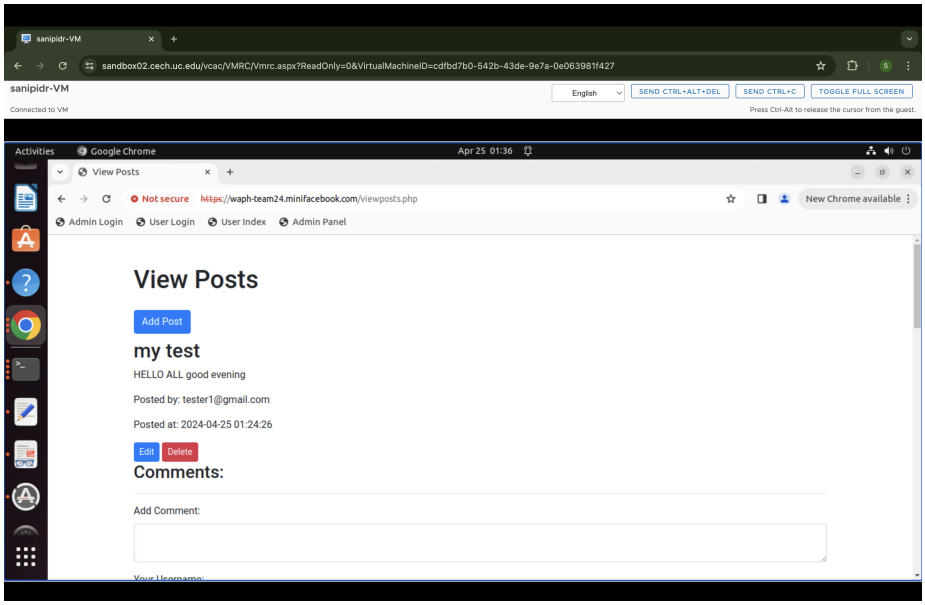


Figure 25: Comment_Post

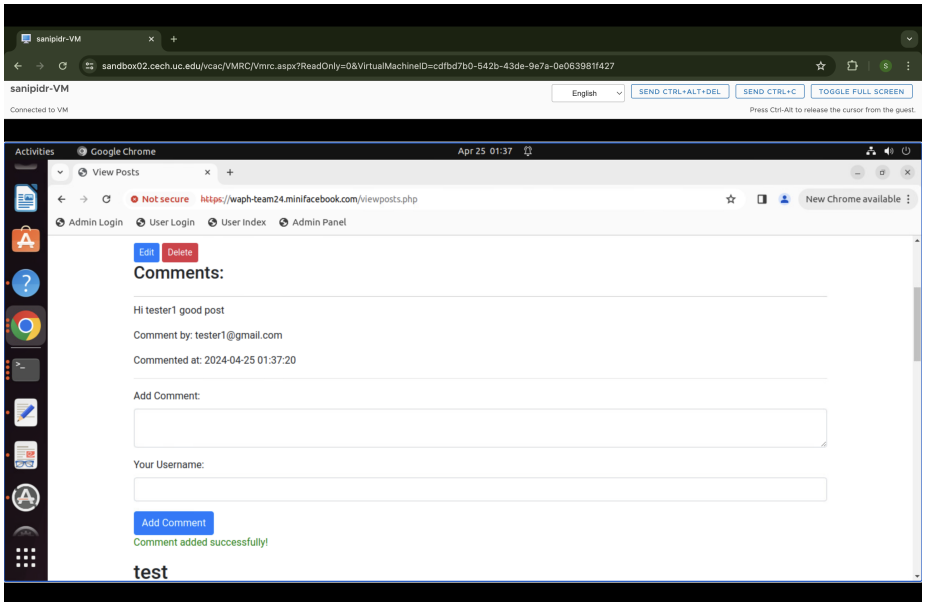


Figure 26: Comment Post

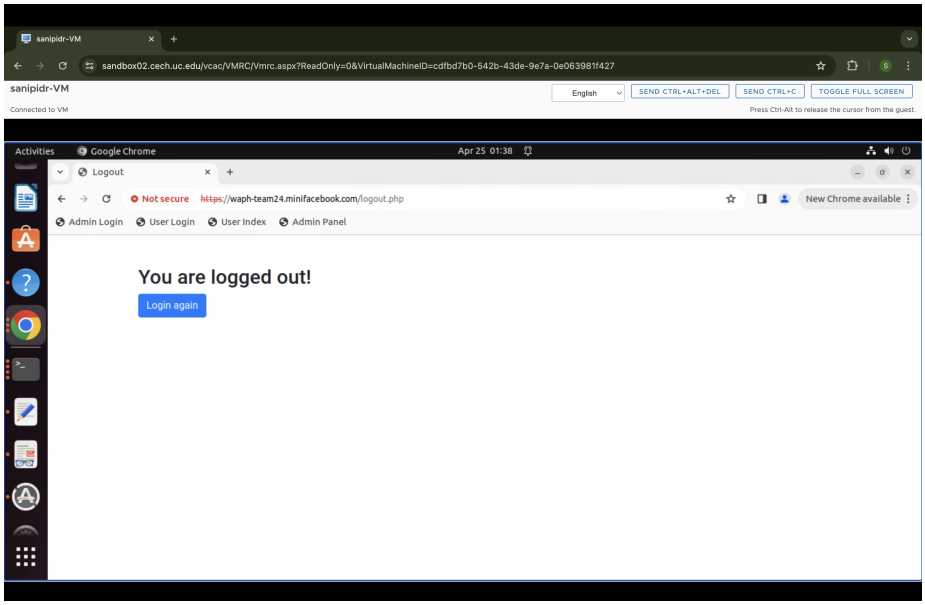
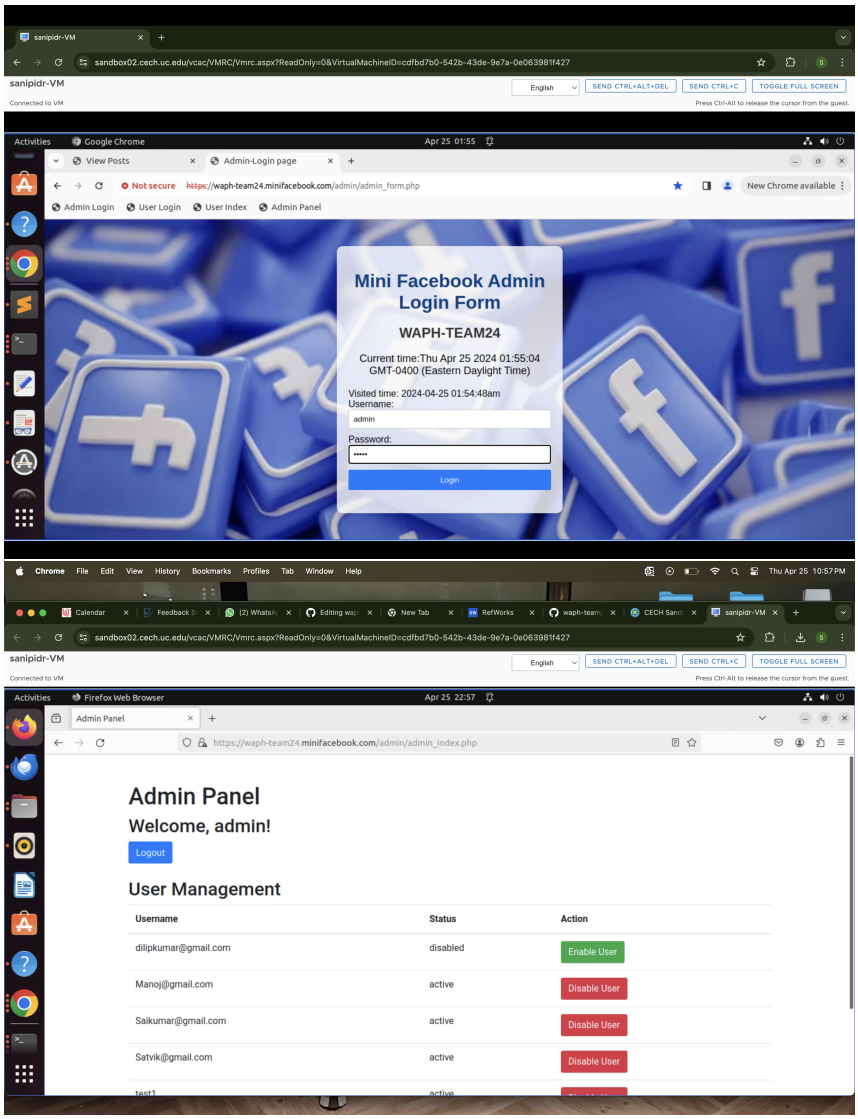
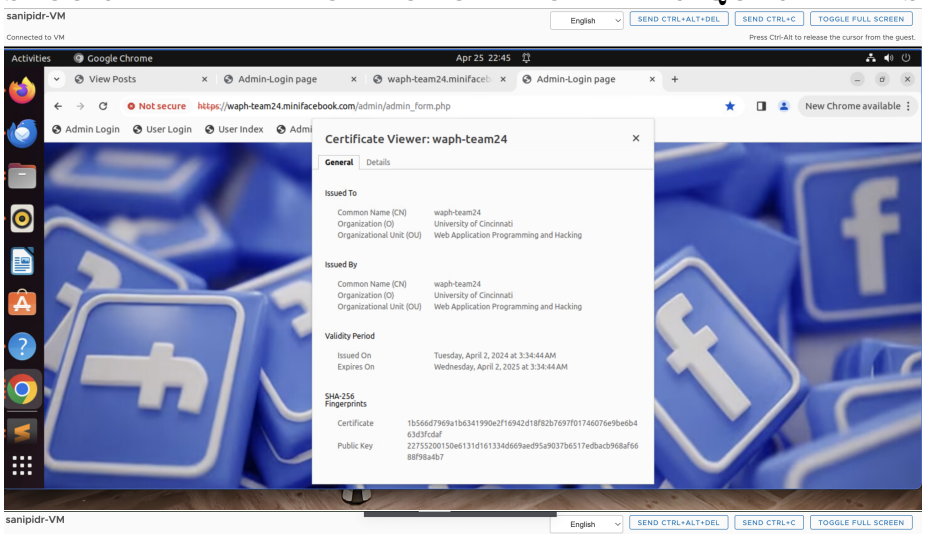
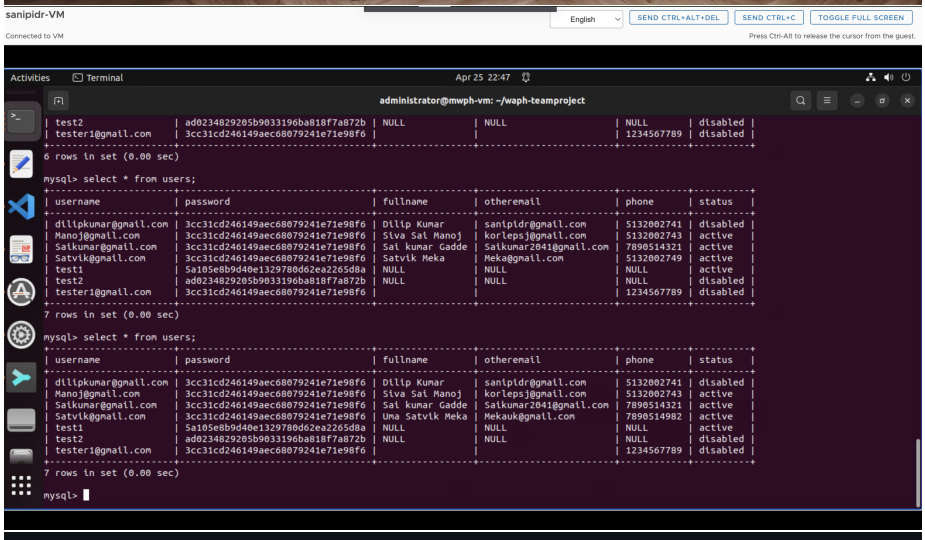


Figure 27: Log out

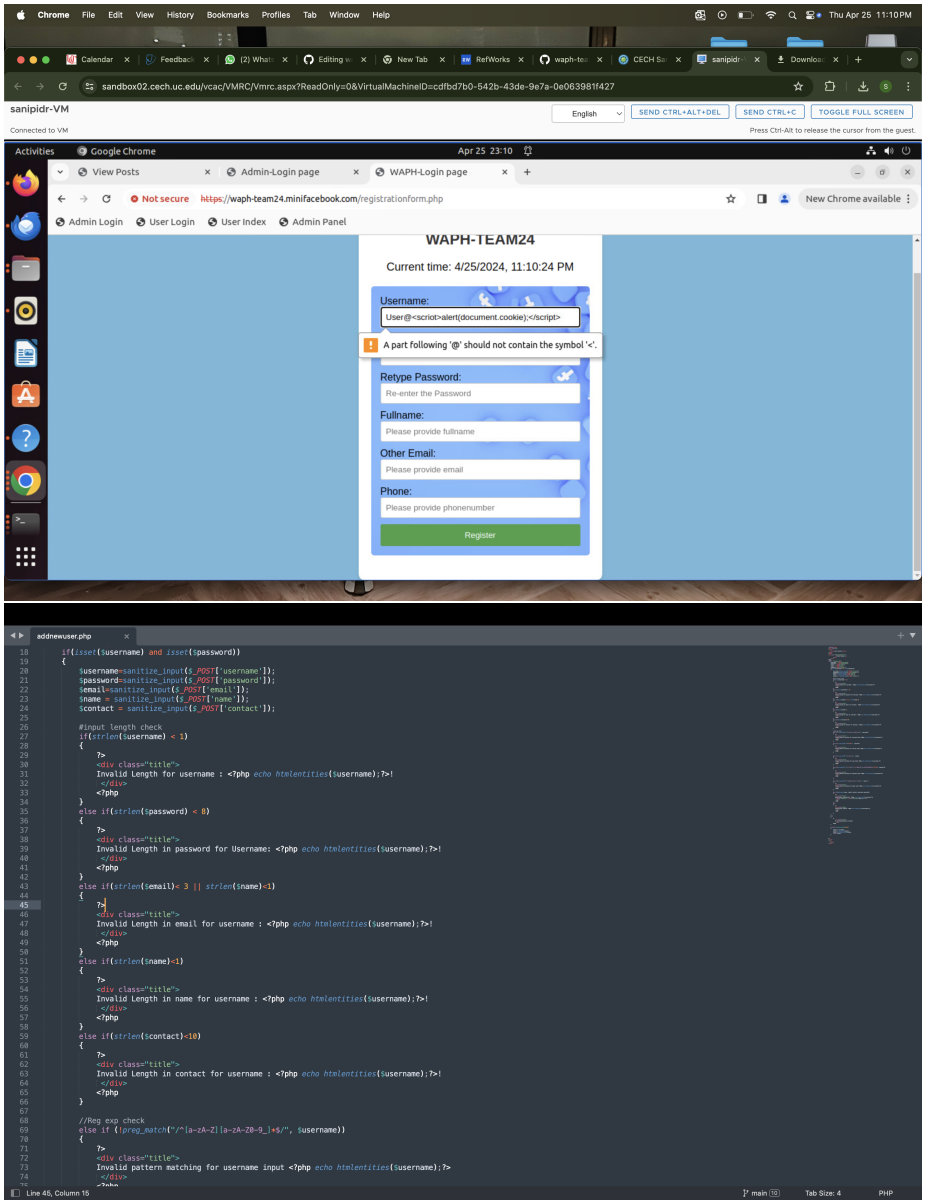

sanipidr-VM
sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=cdfbd7b0-542b-43de-9e7a-0e063981f427
Activities
Google Chrome
Apr 25 01:55
View Posts
Admin-Login page
Not secure
https://waph-team24.minifacebook.com/admin/admin_form.php
Admin Login
User Login
User Index
Admin Panel
Mini 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
Chrome
File
Edit
View
History
Bookmarks
Profiles
Tab
Window
Help
Thu Apr 25 10:57 PM
Firefox Web Browser
Apr 25 22:57
Admin Panel
https://waph-team24.minifacebook.com/admin/admin_index.php
Admin Panel
Welcome, admin!
Logout
User Management
Username
Status
Action
dilipkumar@gmail.com
disabled
Enable User
Manoj@gmail.com
active
Disable User
Saikumar@gmail.com
active
Disable User
Satvik@gmail.com
active
Disable User

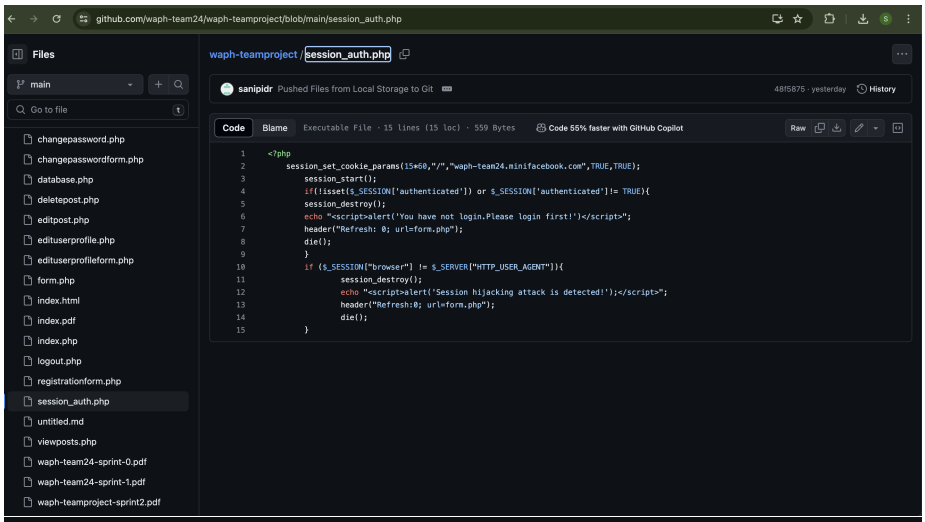
SECURITY AND NON-FUNCTATIONAL REQUIREMENTS



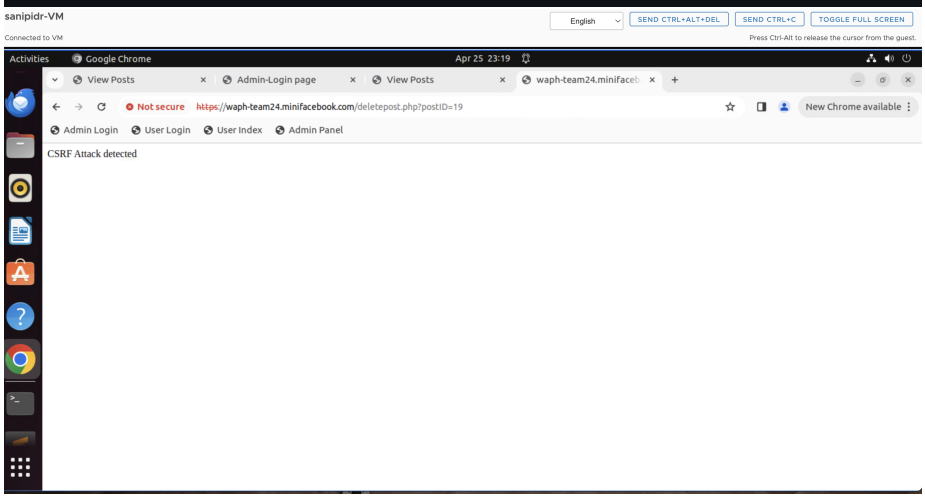


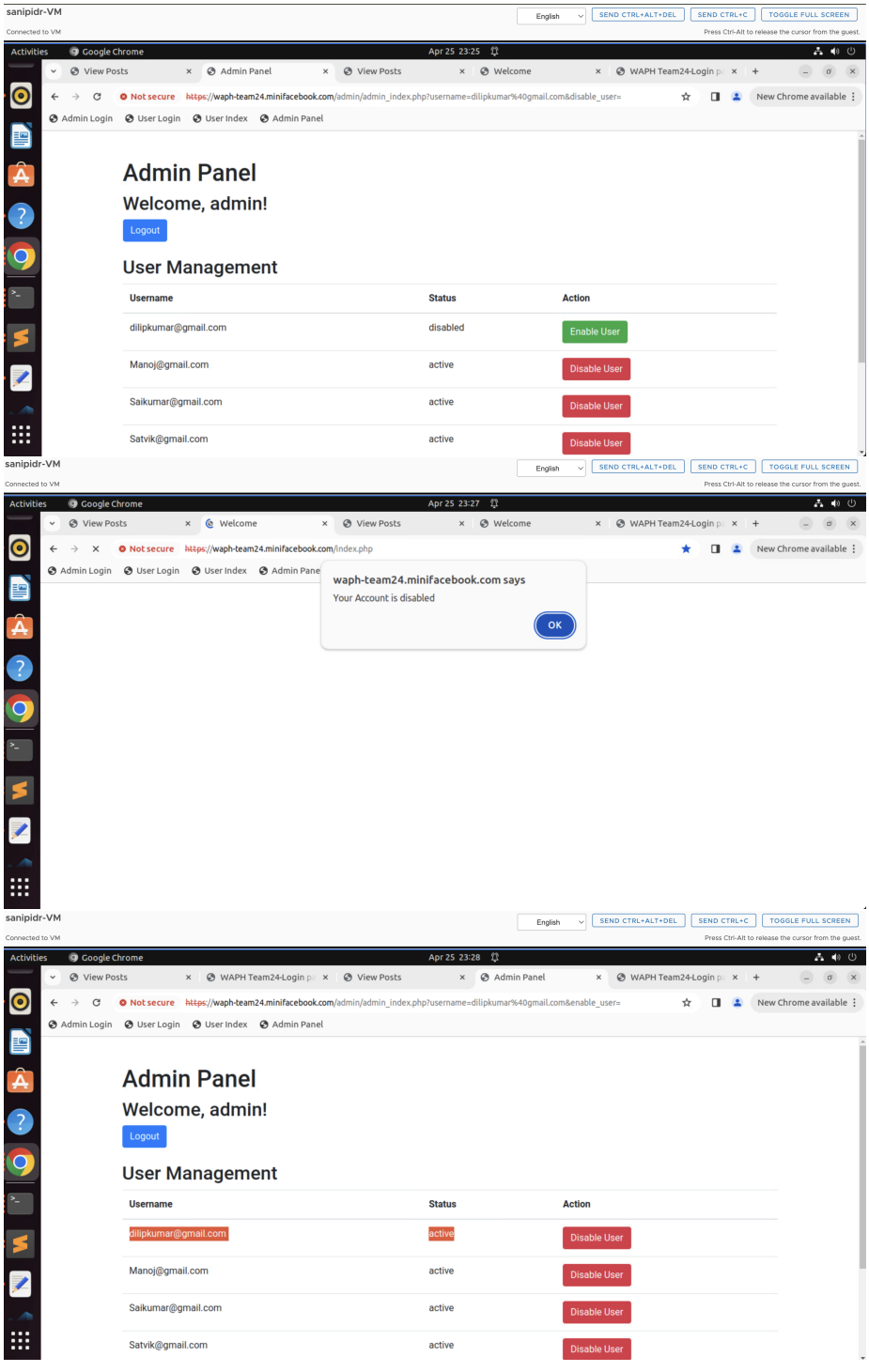

```php
function addnewuser($username, $password,$otheremail,$fullname,$phone) {
  global $mysqli;
 $prepared_sql ="INSERT INTO users (username,password,otheremail,fullname,phone) VALUES (?,md5(?),?,?,?);";
 $stmt = $mysqli->prepare($prepared_sql);
 $stmt-> bind_param("sssss",$username,$password,$otheremail,$fullname,$phone);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

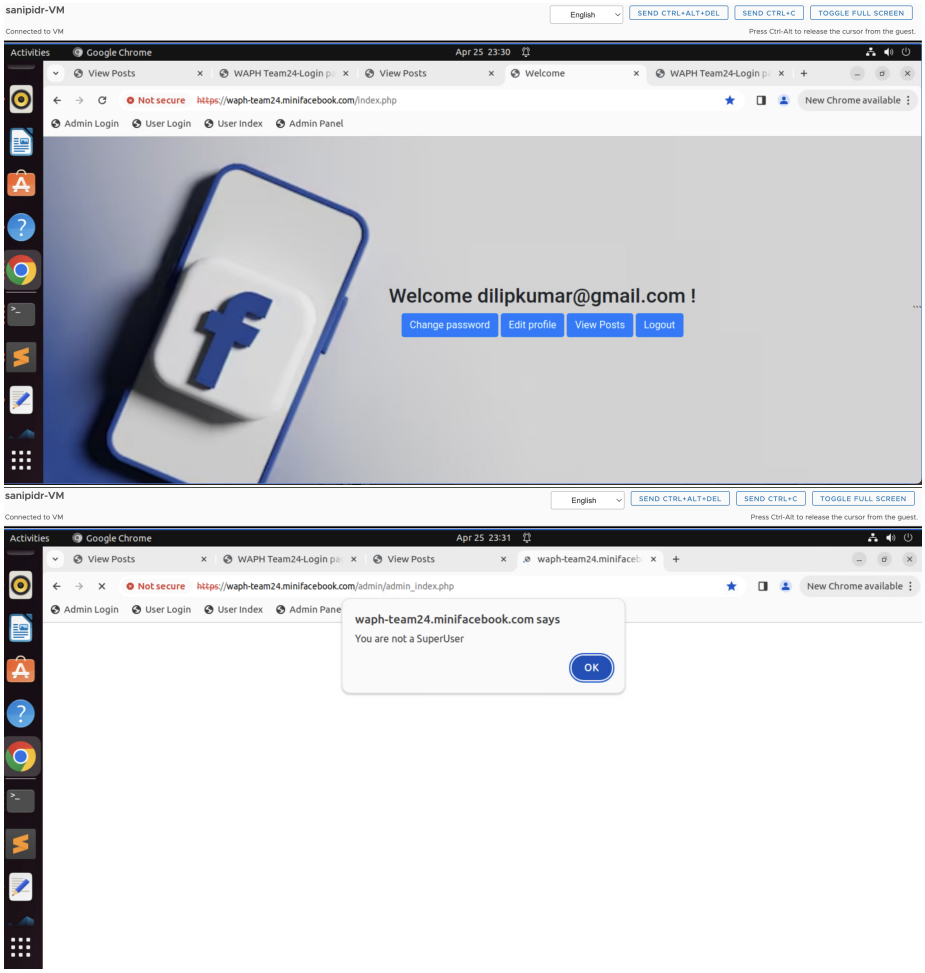

sanipidr-VM
Activities
Google Chrome
Apr 25 23:10
View Posts
Admin-Login page
WAPH-Login page
Not secure
https://waph-team24.minifacebook.com/registrationform.php
Admin Login
User Login
User Index
Admin Panel
WAPH-TEAM24
Current time: 4/25/2024, 11:10:24 PM
Username:
User@<scriot>alert(document.cookie);</script>
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

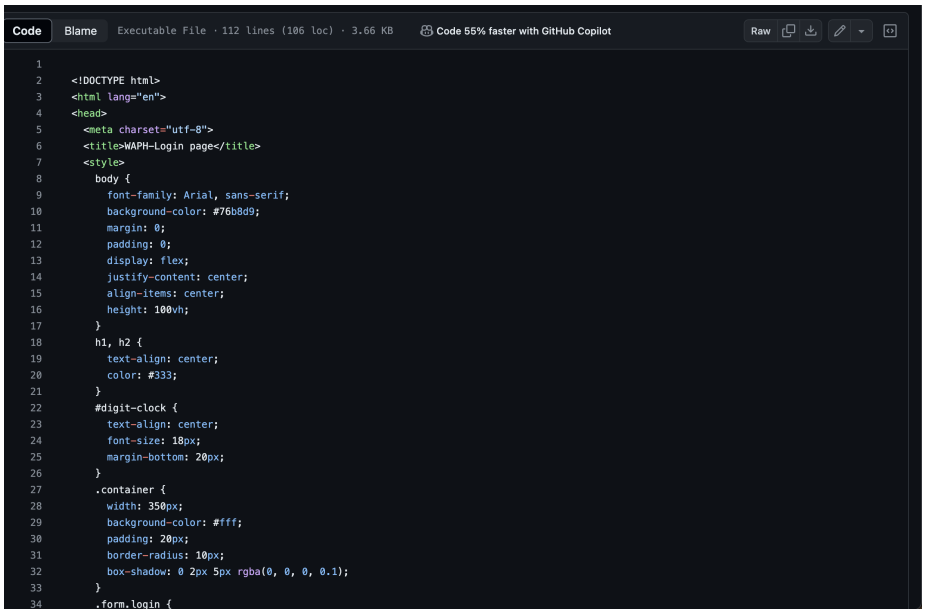



```php
<?php
  require "session_auth.php";
  require "database.php";
  $token = $_POST['nocsrftoken'];
  if (!isset($token) or $token!=$_SESSION['nocsrftoken']) {
     echo "CSRF Attack is detected!";
     die();
  }
```




sanipidr-VM
Connected to VM
English
SEND CTRL+ALT+DEL
SEND CTRL+C
TOGGLE FULL SCREEN
Press Ctrl-Alt to release the cursor from the guest.
Activities
Google Chrome
Apr 25 23:25
View Posts
Admin Panel
View Posts
Welcome
WAPH Team24-Login p
Not secure
https://waph-team24.minifacebook.com/admin/admin_index.php?username=dilipkumar%40gmail.com&disable_user=
New Chrome available
Admin Login
User Login
User Index
Admin Panel
Admin Panel
Welcome, admin!
Logout
User Management
Username
Status
Action
dilipkumar@gmail.com
disabled
Enable User
Manoj@gmail.com
active
Disable User
Saikumar@gmail.com
active
Disable User
Satvik@gmail.com
active
Disable User
sanipidr-VM
Connected to VM
English
SEND CTRL+ALT+DEL
SEND CTRL+C
TOGGLE FULL SCREEN
Press Ctrl-Alt to release the cursor from the guest.
Activities
Google Chrome
Apr 25 23:27
View Posts
Welcome
View Posts
Welcome
WAPH Team24-Login p
Not secure
https://waph-team24.minifacebook.com/index.php
New Chrome available
Admin Login
User Login
User Index
Admin Pane
waph-team24.minifacebook.com says
Your Account is disabled
OK
sanipidr-VM
Connected to VM
English
SEND CTRL+ALT+DEL
SEND CTRL+C
TOGGLE FULL SCREEN
Press Ctrl-Alt to release the cursor from the guest.
Activities
Google Chrome
Apr 25 23:28
View Posts
WAPH Team24-Login p
View Posts
Admin Panel
WAPH Team24-Login p
Not secure
https://waph-team24.minifacebook.com/admin/admin_index.php?username=dilipkumar%40gmail.com&enable_user=
New Chrome available
Admin Login
User Login
User Index
Admin Panel
Admin Panel
Welcome, admin!
Logout
User Management
Username
Status
Action
dilipkumar@gmail.com
active
Disable User
Manoj@gmail.com
active
Disable User
Saikumar@gmail.com
active
Disable User
Satvik@gmail.com
active
Disable User


sanipidr-VM
Connected to VM
English
SEND CTRL+ALT+DEL
SEND CTRL+C
TOGGLE FULL SCREEN
Press Ctrl-Alt to release the cursor from the guest.
Activities
Google Chrome
Apr 25 23:30
View Posts
WAPH Team24-Login p
View Posts
Welcome
WAPH Team24-Login p
Not secure
https://waph-team24.minifacebook.com/index.php
New Chrome available
Admin Login
User Login
User Index
Admin Panel
Welcome dilipkumar@gmail.com !
Change password
Edit profile
View Posts
Logout
sanipidr-VM
Connected to VM
English
SEND CTRL+ALT+DEL
SEND CTRL+C
TOGGLE FULL SCREEN
Press Ctrl-Alt to release the cursor from the guest.
Activities
Google Chrome
Apr 25 23:31
View Posts
WAPH Team24-Login pa
View Posts
waph-team24.minifaceb
Not secure
https://waph-team24.minifacebook.com/admin/admin_index.php
New Chrome available
Admin Login
User Login
User Index
Admin Pane
waph-team24.minifacebook.com says
You are not a SuperUser
OK




```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>WAPH-Login page</title>
  <style>
    body {
      font-family: Arial, sans-serif;
      background-color: #76b8d9;
      margin: 0;
      padding: 0;
      display: flex;
      justify-content: center;
      align-items: center;
      height: 100vh;
    }
    h1, h2 {
      text-align: center;
      color: #333;
    }
    #digit-clock {
      text-align: center;
      font-size: 18px;
      margin-bottom: 20px;
    }
    .container {
      width: 350px;
      background-color: #fff;
      padding: 20px;
      border-radius: 10px;
      box-shadow: 0 2px 5px rgba(0, 0, 0, 0.1);
    }
    .form.login {
```

Appendix