TASK 14

Steps to Deploy a Web Application on a Cloud VM

REPORT SUBMITTED BY

MALAVIKA.MS

Steps to Deploy a Web Application on a Cloud VM

Step 1: Connect to the Cloud VM

- Access the Kali Linux terminal and establish a connection to the cloud VM using SSH.
- Command:

sudo ssh -i Documents/cloudkey.pem ec2-user@34.230.49.137

- Screenshot: [SSH_LOGIN Screenshot]

Step 2: Clone the GitHub Repository

- Download the application files by cloning the repository from GitHub.
- Command:

Step 3: Transfer Files to Apache Directory

- Move the cloned web application files to the Apache web server's root directory for deployment.
- Command:

sudo cp -r /home/ec2-user/webapp/cloudweb /var/www/html

Step 4: Launch Apache Web Server

- Start the Apache web server to serve the web application.
- Command:

sudo systemctl start httpd

Step 5: View the Web Application

- Use a browser to access the deployed application by navigating to the public IP of the cloud VM.
- Screenshot

Step 6: Install PHP and MySQL

- Check for existing installations of PHP and MySQL, and install them if required.
- Command:

sudo yum install php

Step 7: Start MySQL Service

- Start the MySQL server and log in to the MySQL database system.
- Command:

sudo systemctl start mysqld

mysql -u root -p

Step 8: Set Up the Database and Table

- Create a database and a table to store user registration data.
- SQL Command:

sql

```
CREATE TABLE IF NOT EXISTS users (
   id INT(6) UNSIGNED AUTO_INCREMENT PRIMARY KEY,
   firstName VARCHAR(50) NOT NULL,
   lastName VARCHAR(50) NOT NULL,
   email VARCHAR(100) NOT NULL UNIQUE,
   phoneNumber VARCHAR(15),
   password VARCHAR(255) NOT NULL
)
;
```

Step 9: Develop User Registration Files

- Create the PHP files required for the user registration feature, ensuring data is stored in the MySQL database.

Step 10: Log In as Registered User

- Log in as the newly registered user and display the saved data from the database.

Step 11: Test Web Page Accessibility

- Verify the accessibility of the deployed web page by using the public IP of the cloud VM.

Step 12: Share Public IP for Verification

- Document the public IP address and share it with team members for verification

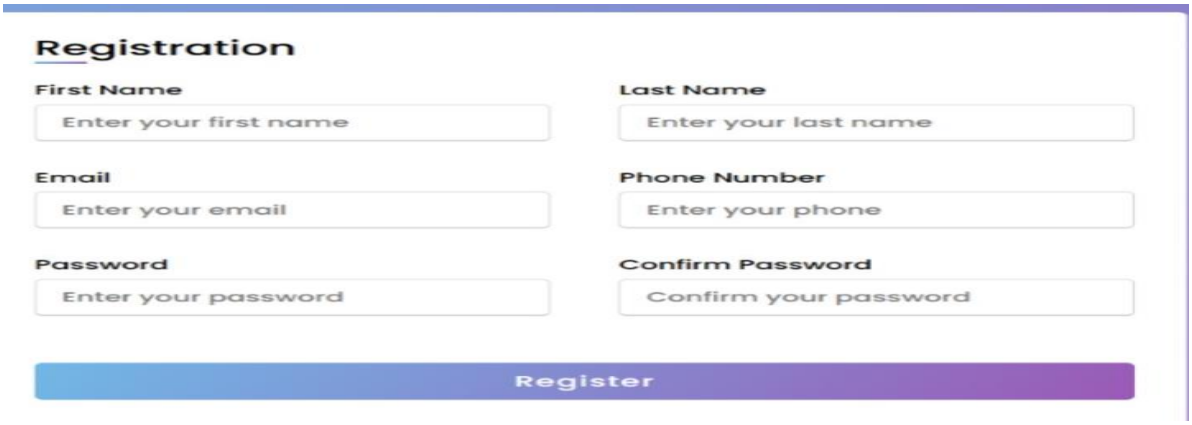
```
+------------------+
| Tables_in_trash  |
+------------------+
| users            |
+------------------+
1 row in set (0.00 sec)

mysql> CREATE TABLE IF NOT EXISTS users (
    ->     id INT(6) UNSIGNED AUTO_INCREMENT PRIMARY KEY,
    ->     firstName VARCHAR(50) NOT NULL,
    ->     lastName VARCHAR(50) NOT NULL,
    ->     email VARCHAR(100) NOT NULL UNIQUE,
    ->     phoneNumber VARCHAR(15),
    ->     password VARCHAR(255) NOT NULL
    -> );
Query OK, 0 rows affected, 2 warnings (0.00 sec)

mysql> describe users;
+-------------+----------------+------+-----+---------+----------------+
| Field       | Type           | Null | Key | Default | Extra          |
+-------------+----------------+------+-----+---------+----------------+
| id          | int unsigned   | NO   | PRI | NULL    | auto_increment |
| firstName   | varchar(50)    | NO   |     | NULL    |                |
| lastName    | varchar(50)    | NO   |     | NULL    |                |
| email       | varchar(100)   | NO   | UNI | NULL    |                |
| phoneNumber | varchar(15)    | YES  |     | NULL    |                |
| password    | varchar(255)   | NO   |     | NULL    |                |
+-------------+----------------+------+-----+---------+----------------+
6 rows in set (0.00 sec)

mysql>
```

```
+----+-----------+----------+-----------------+-------------+--------------------------------------------------------------+
| id | firstName | lastName | email           | phoneNumber | password                                                     |
+----+-----------+----------+-----------------+-------------+--------------------------------------------------------------+
|  1 |           |          |                 |             | $2y$10$Z3wUB4yQRsbWtkIbuBIg5.f2ZM2w19pNK7aHOTyJw3GMcriNlb7sC |
|  2 | ewfw      | wefw     | qw@gmail.com    | 1234567890  | $2y$10$.ZlQG.a/8T0agDEMjr7JxeHIvzVTqdlRgHuhv3Op6VnCr238KrW1C |
|  3 | anomy     | hack     | anomy@hack.onion| 9876543210  | $2y$10$r2/WfTL5Yzr2qQfhjzctgONsWPlleYjX.YK0ghdBmdF4tf.D3Ltiu |
+----+-----------+----------+-----------------+-------------+--------------------------------------------------------------+
3 rows in set (0.001 sec)
```




```
└─$ sudo ssh -i Documents/cloudkey.pem ec2-user@34.230.49.137
[sudo] password
The authenticity of host '34.230.49.137 (34.230.49.137)' can't be established.
ED25519 key fingerprint is SHA256:9JnfV2zCMsSaAmaRE2KmpgYA5vbHJVOXNraXvDw5vcg.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '34.230.49.137' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 05:30:37 2024 from 18.206.107.28
[ec2-user@ip-172-31-41-204 ~]$ ls
[ec2-user@ip-172-31-41-204 ~]$ git
```