# Course-end Project 2

**Description**

To demonstrate the deployment of a multi-tier application using Docker compose, including configuring public IP addresses and setting up necessary security group rules for accessing the frontend, API, and database services.

**Real-time scenario:** A user is tasked to deploy a multi-tier application on a cloud-based virtual machine using Docker Compose. After installing Docker, Docker Compose, and Git, they clone the application repository and update configuration files with the machine's public IP to ensure proper communication between the frontend, API, and backend components.

Post these updates, the user runs docker compose to bring up the application, adjust the security group settings to allow traffic on specific ports (8080, 5000), and verify the deployment by accessing the application via the public IP. This confirms that all components are accessible and functional.

**Steps:**

1. Setup a docker server OR use the docker lab
2. Clone the repo: <https://github.com/GithubWorkstation/docker-compose-lab-01.git>
3. cd into the code dir:
   1. cd docker-compose-lab-01
4. edit backend api to add your server ip address in below line:
   1. vim api/index.php

header('Access-Control-Allow-Origin: http://172.31.84.12:3000');

1. edit frontend to add serverIP
   1. vim frontend/index.html

fetch("http://172.31.84.12:5000/")

1. bring all the services up
   1. docker compose up -d
2. check out all the services in the browser
   1. <http://3.82.187.145:5000/>
   2. <http://3.82.187.145:3000/>
   3. *http://3.82.187.145:8080/*