COS20019 – Cloud Computing Architecture

Assignment 2: Developing a Highly Available Photo Album Website

Student ID: 104082552

Student Name: Nhat Minh Tran

Lab section: Tuesday 06:30PM

I. Introduction

In this assignment two, we used the foundation that we created in the previous assignment-assignment 1b, we have known how to create a basic web server and security groups, different subnets and run phpMyAdmin. This assignment, we are enhancing and extending the infrastructure. We make the web becomes highly available with auto scaling groups, Application Load Balancer, Lambda function. With all this being done, we will have more vision and knowledge of a scalability, reliability, security website that managers and company use.

II. Infrastructure deployment

1. VPC

VPC "MTranVPC" is created, and it is a fundamental networking service provided by AWS. I created the VPC with configuration match the architecture diagram. Here is a clearer look of VPC provided by resource map. Two public subnet and two private subnets are created within two AZs.

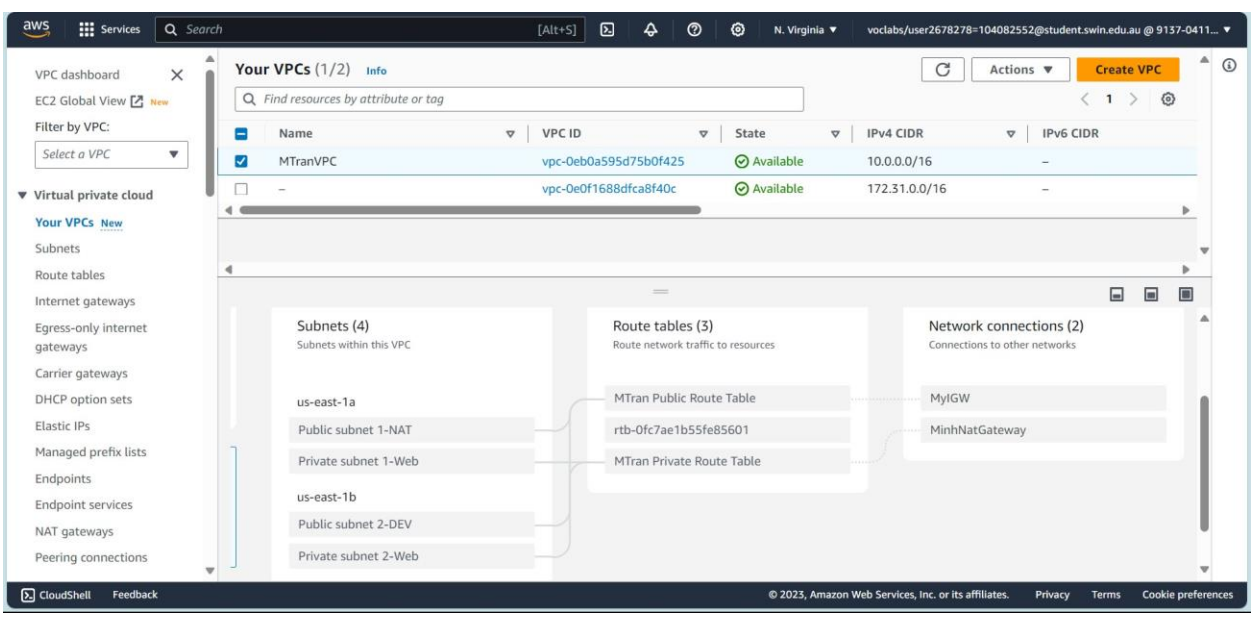

Figure 1: Resource Map

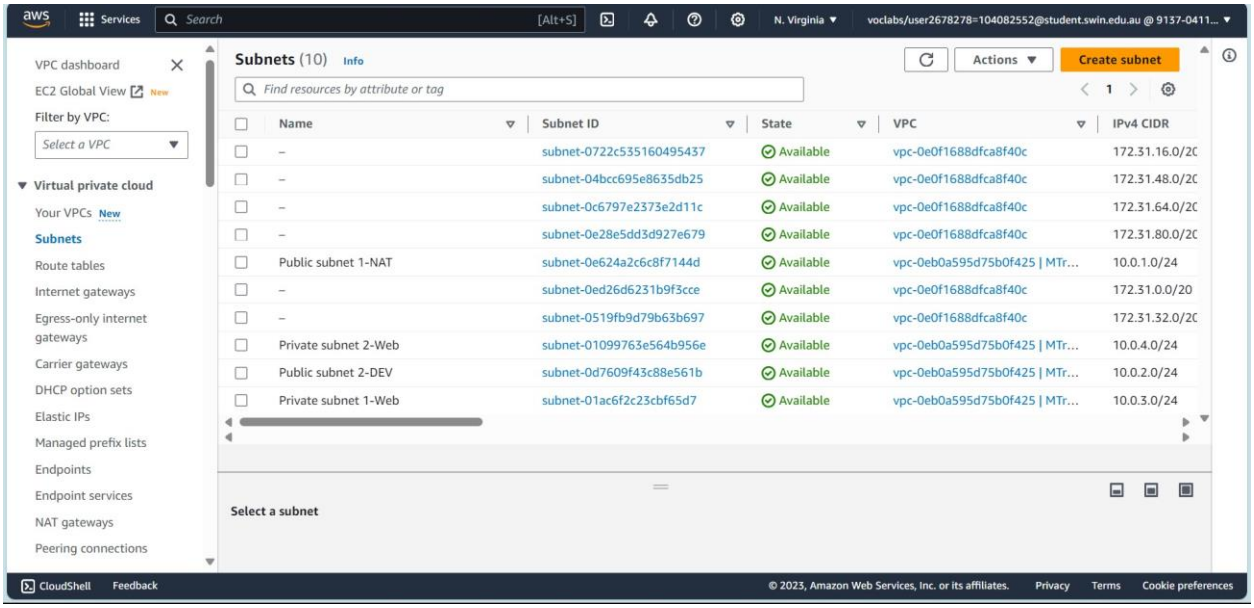

Figure 2: 4 subnets with 2AZ

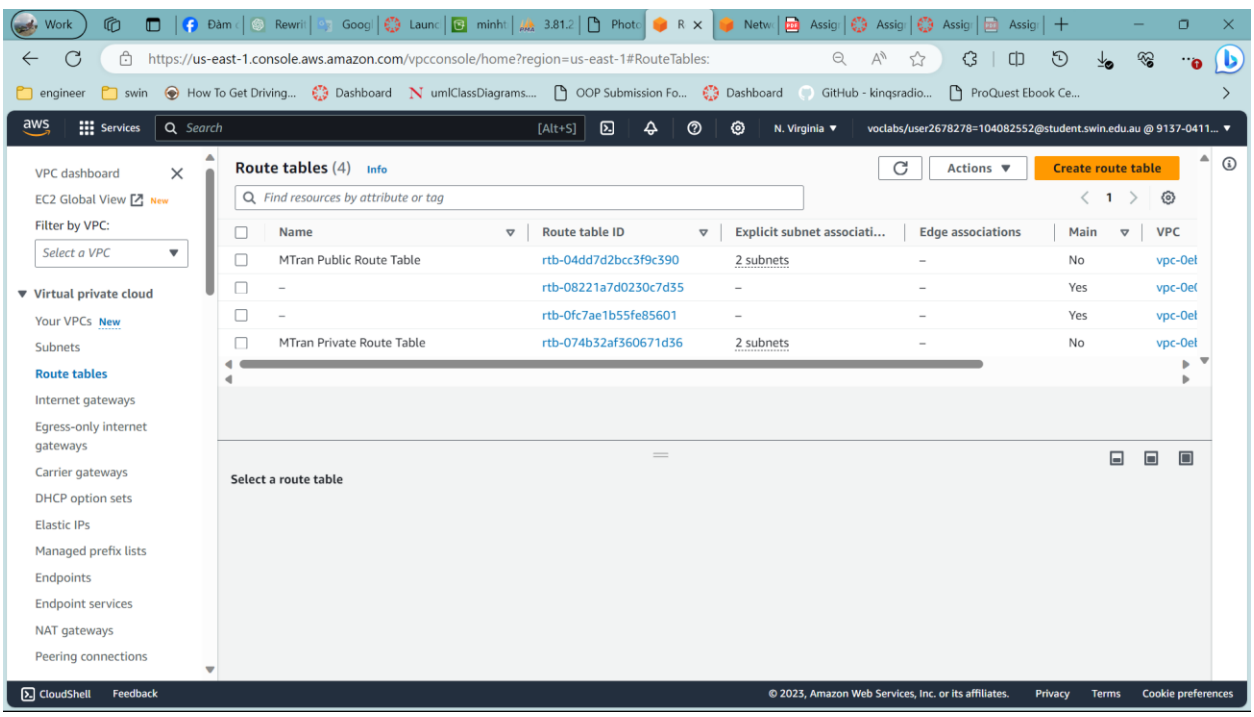

Figure 3: 2 Route Table associated with different subnets.

Moreover, the Public Subnet 2-DEV is routed to Internet Gateway to go to users. In the Public Subnet 1-Web, I created a NAT gateway for scalability and reliability instead of NAT instance. The NAT gateway allows resources within private subnets to access the internet for updating software or uploading things, but keep it hidden from inbound traffic from the internet. The two private subnets are configured to route the traffic through this NAT gateway.

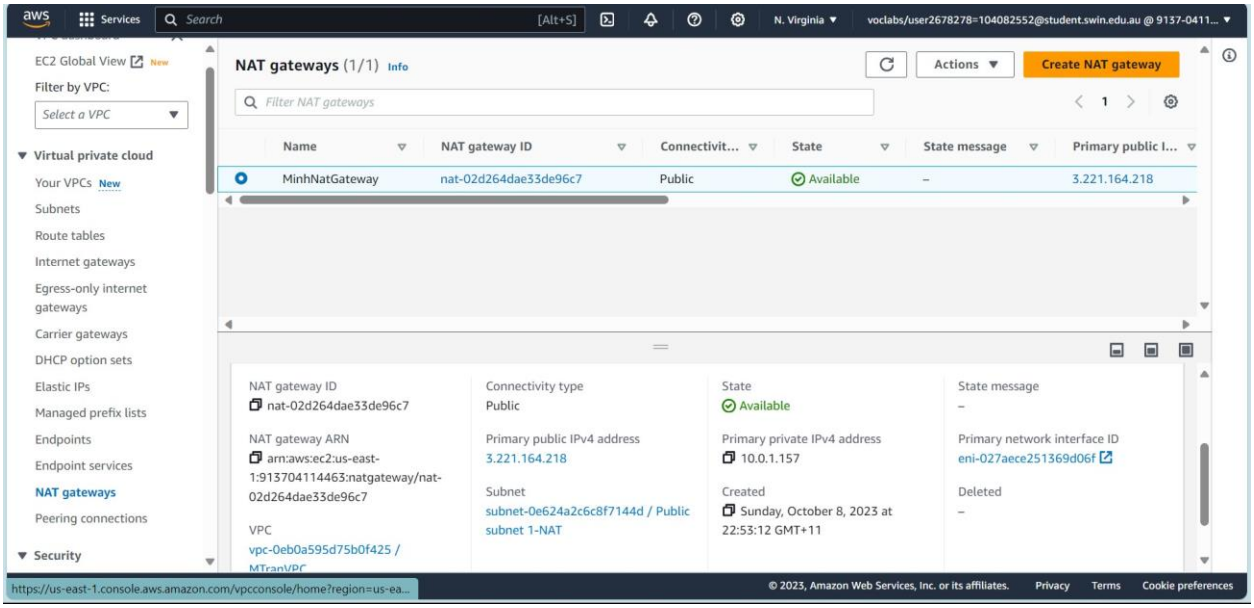

Figure 4: NAT gateway

2. S3 photo storage

S3 bucket is created to store images, which has been created in assignment 1b. However, the policy and permission of this will be different due to the Application Load Balancer (ALB) and the S3 is also staying outside of VPC.

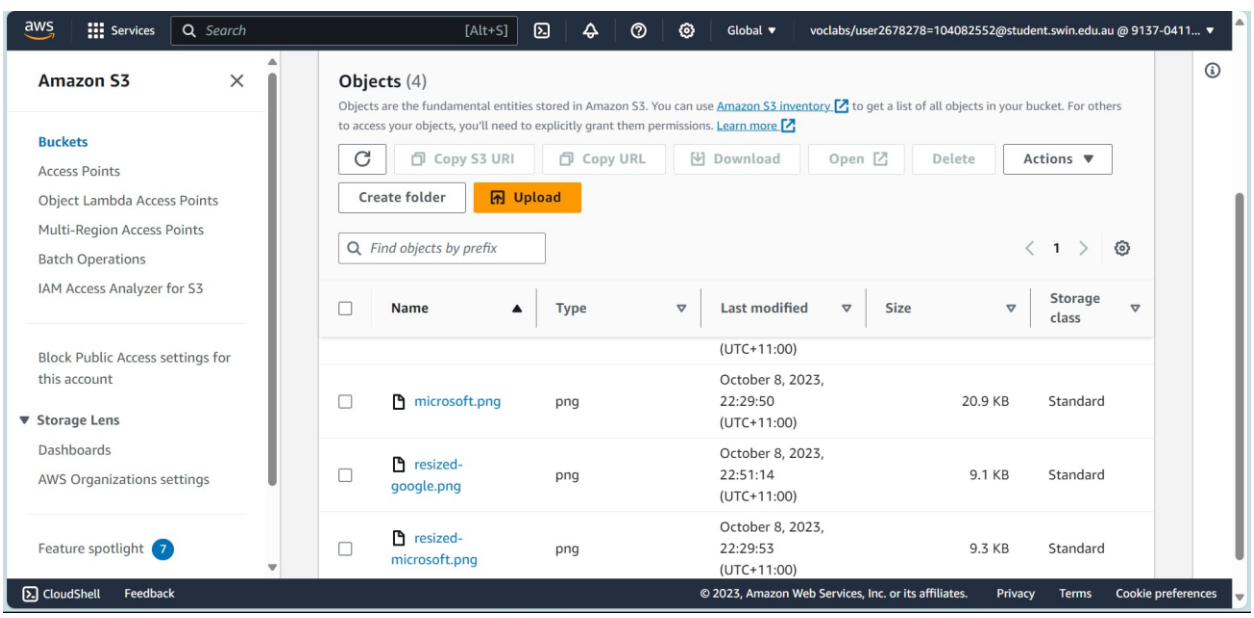

Figure 5: Minhtranbucket

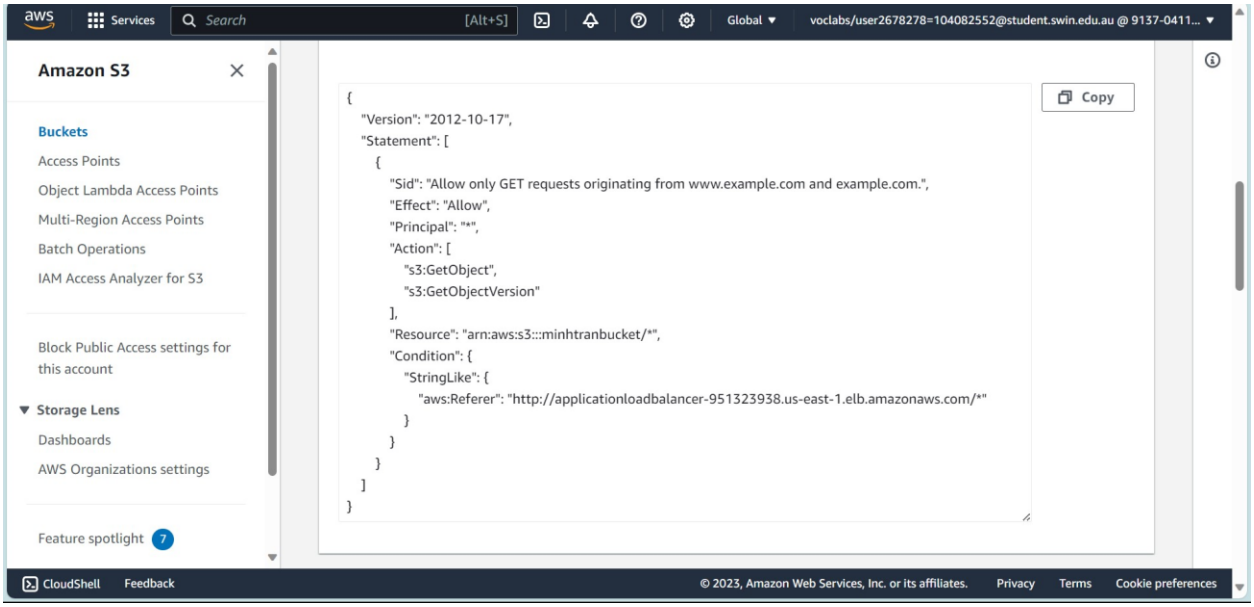

Figure 6: S3 Bucket policy

This IAM policy statement allow the GET requests to object in my bucket but only if the Referer header in the HTTP matches the value. This policy is a way to restrict people getting to the website, ensuring that only requests from a particular domain are permitted to access the S3 objects. The permission also goes through ALB, enhancing the overall security of the website.

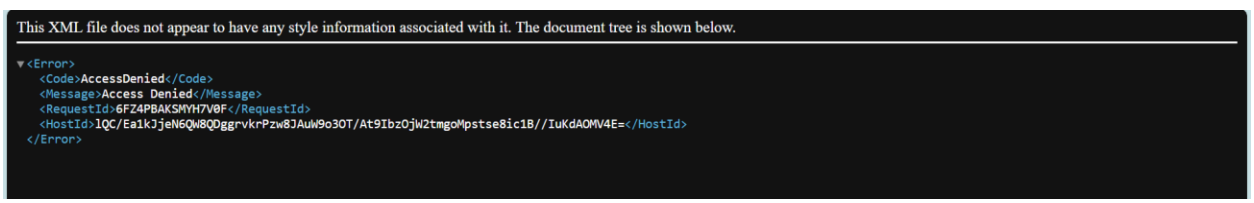

Figure 7: Access denied to S3 objects

3. Security Groups and Network ACL

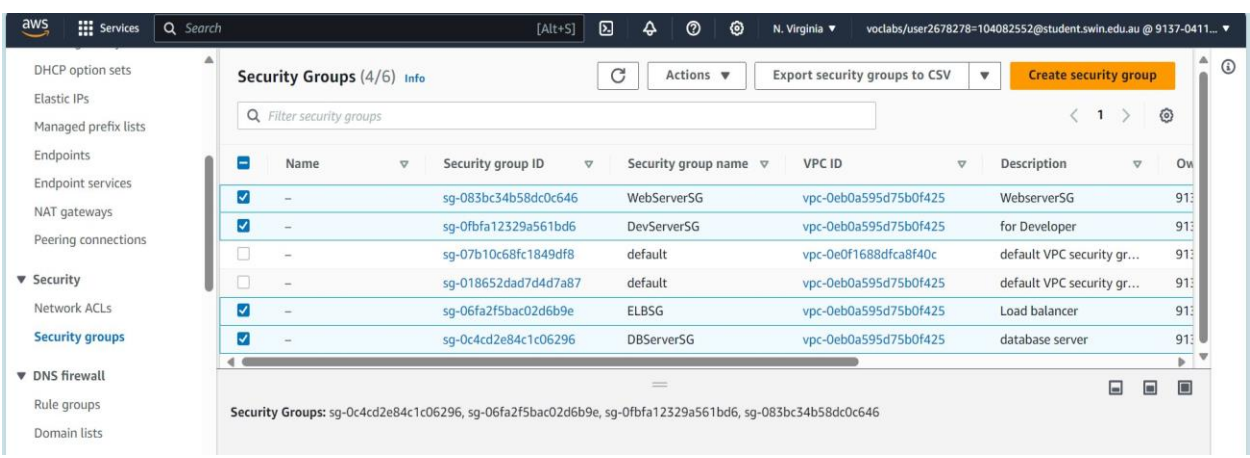

Figure 8: Security groups

To ensure the website secured and working great, I have security groups with different configurations on inbound and outbound rules.

Inbound rules (2)

Manage tags | Edit inbound rules

Filter security group rules

Name	Security group rule...	IP version	Type	Protocol	Port
–	sgr-0ce615607892934...	–	HTTPS	TCP	443
–	sgr-08ba9e1d19b417...	–	HTTP	TCP	80

Figure 9: Inbound WebServerSG

Inbound rules (3)

Manage tags | Edit inbound rules

Filter security group rules

Name	Security group rule...	IP version	Type	Protocol	Port
–	sgr-05030d9e04f6c10db	IPv4	SSH	TCP	22
–	sgr-012fff6b5d2717262	IPv4	HTTP	TCP	80
–	sgr-049e13fb26856320f	IPv4	HTTPS	TCP	443

Figure 10: Inbound DevServerSG

Inbound rules (2)

Manage tags | Edit inbound rules

Filter security group rules

Name	Security group rule...	IP version	Type	Protocol	Port
–	sgr-06f44bdcc6d96e99a	IPv4	HTTPS	TCP	443
–	sgr-006d441c06aca408b	IPv4	HTTP	TCP	80

Figure 11: Inbound ELBSG

Inbound rules (2)

Manage tags | Edit inbound rules

Filter security group rules

Name	Security group rule...	IP version	Type	Protocol	Port
–	sgr-0c671c52be6a989fb	–	MYSQL/Aurora	TCP	3306
–	sgr-0fb94be957f4647a8	–	MYSQL/Aurora	TCP	3306

Figure 12: Inbound DBServerSG

The outbound of these security groups remained unchanged. These rules maintain a controlled and secure environment, only allow specific interactions and restricted other unnecessary sources.

To make the website better and more security, advance configuration such as Network ACL are asked to be done and deployed. This NACL limits ICMP traffic to the corresponding subnets, blocking all the ICMP traffic to/from Dev server.

Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
33	All traffic	All	All	0.0.0.0/0	Allow
34	All ICMP - IPv4	ICMP (1)	All	10.0.2.0/24	Deny
*	All traffic	All	All	0.0.0.0/0	Deny

Figure 13: Inbound rules

Filter outbound rules

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
44	All traffic	All	All	0.0.0.0/0	Allow
45	All ICMP - IPv4	ICMP (1)	All	10.0.2.0/24	Deny
*	All traffic	All	All	0.0.0.0/0	Deny

Figure 14: Outbound rules

4. EC2 Instances

The EC2 instances provides a virtual server in cloud. With EC2 instance I can create web application, database, and more. For this assignment, I created one instance, the WebServer instance.

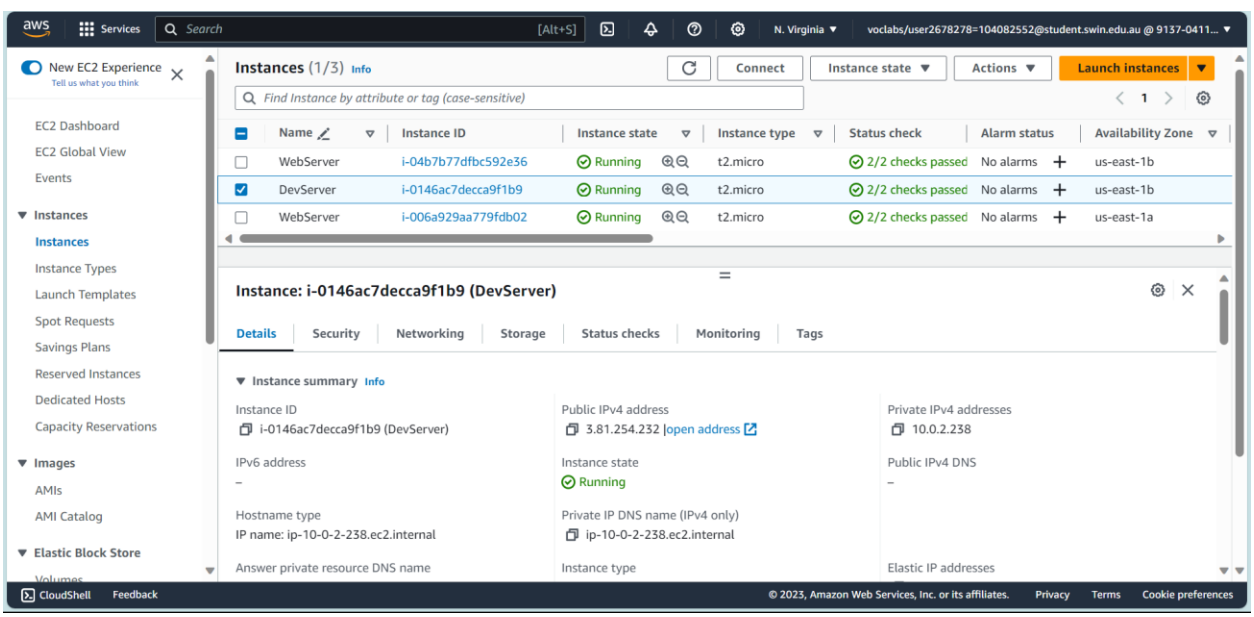

Figure 15: DevServer Instance

5. CreateThumbnail Lambda function

Following the task, I uploaded the code to Lambda to resize images, download and upload images to S3. Also, a test is run to check correction.

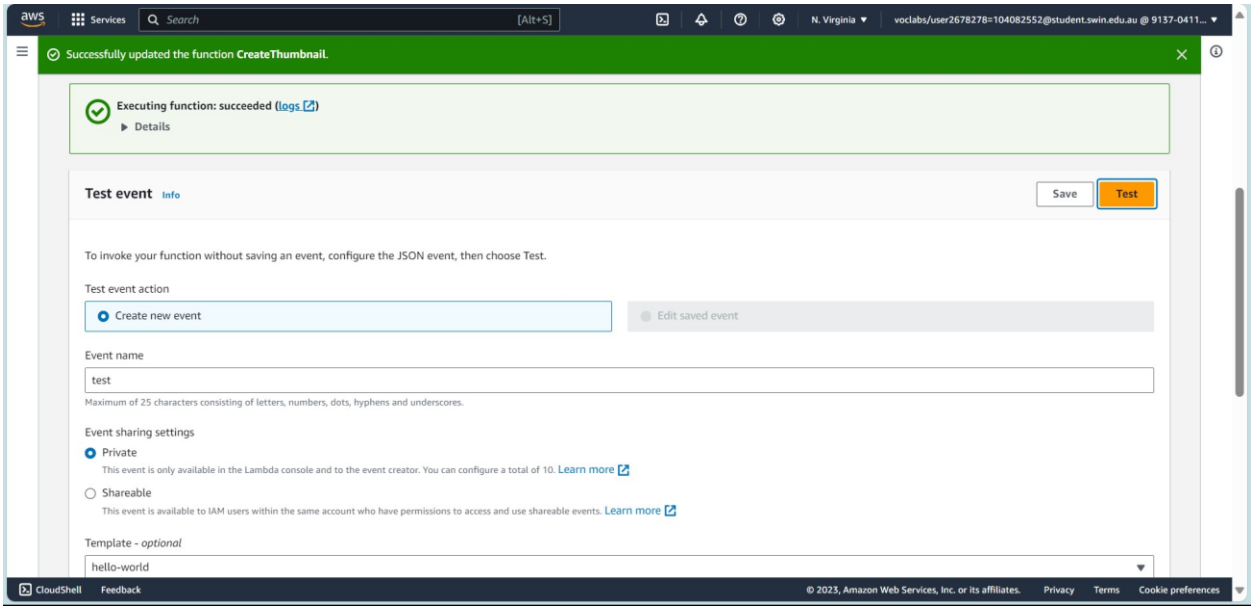

Figure 16: Function testing

6. RDS

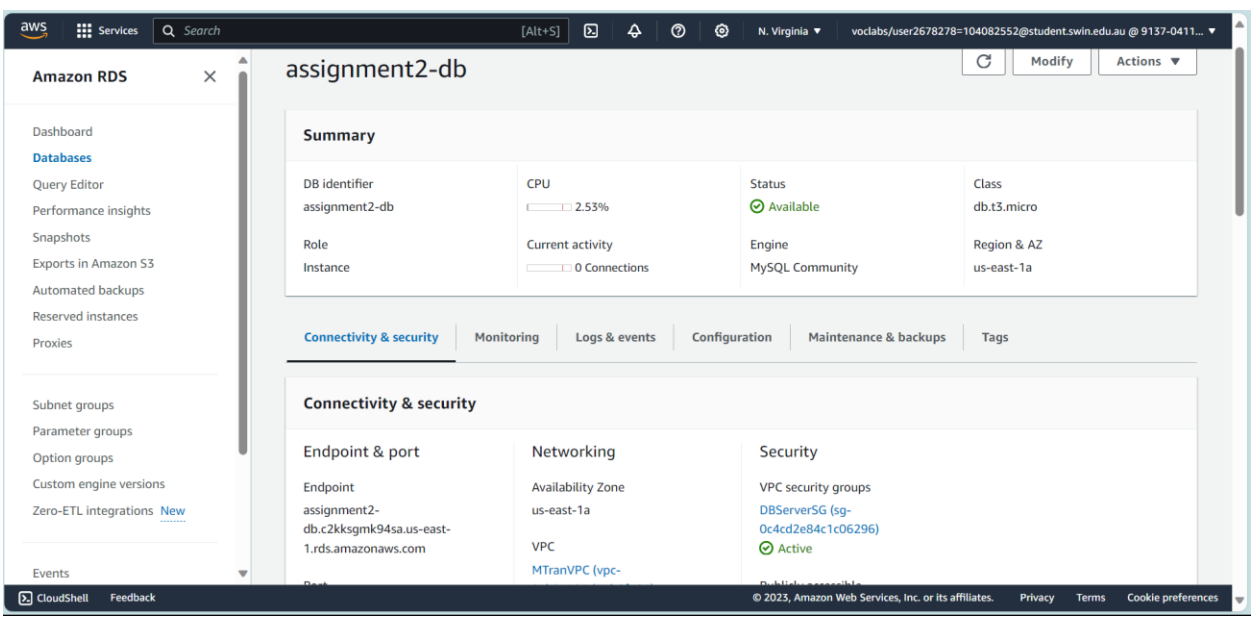

Figure 17: Assignment2-db

The Relational Database Service allows us to instantly launch a database. This RDS is created with MySQL server. It automatically replicates the database to a standby instance in different availability zone for failover protection.

7. Load balancing

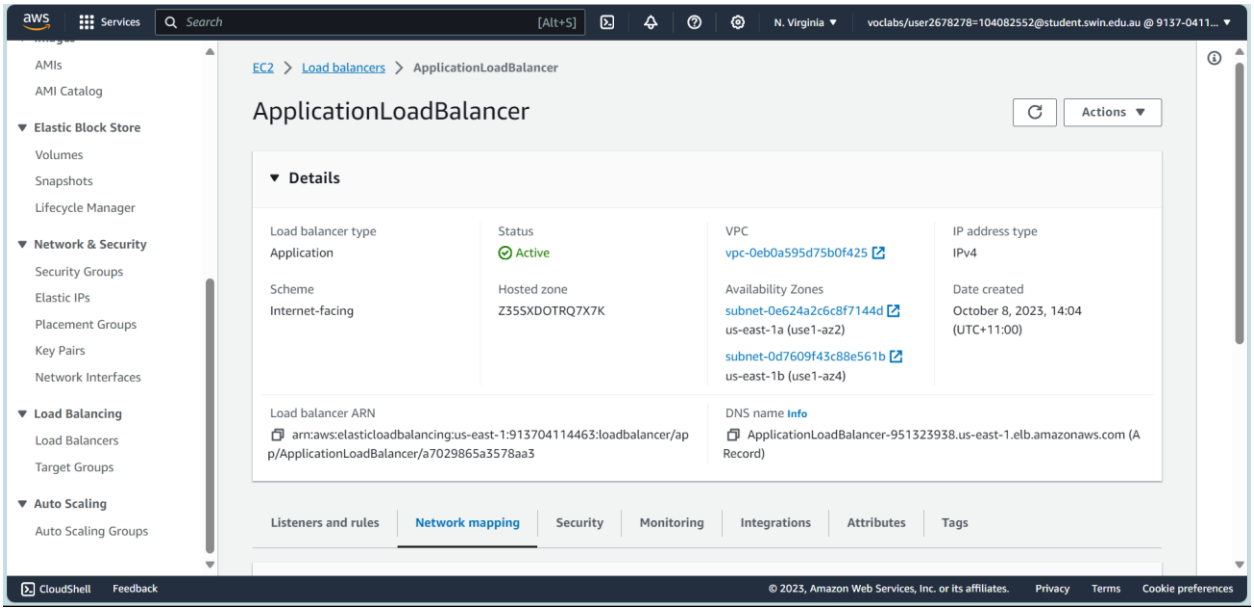

Figure 18: ApplicationLoadBalancer

The mission of Load Balancer is to ensure there is no single server of resource overwhelmed with traffic. It improves the fault tolerance, availability of a system. Also, Target Groups are created to run health checks on all instances.

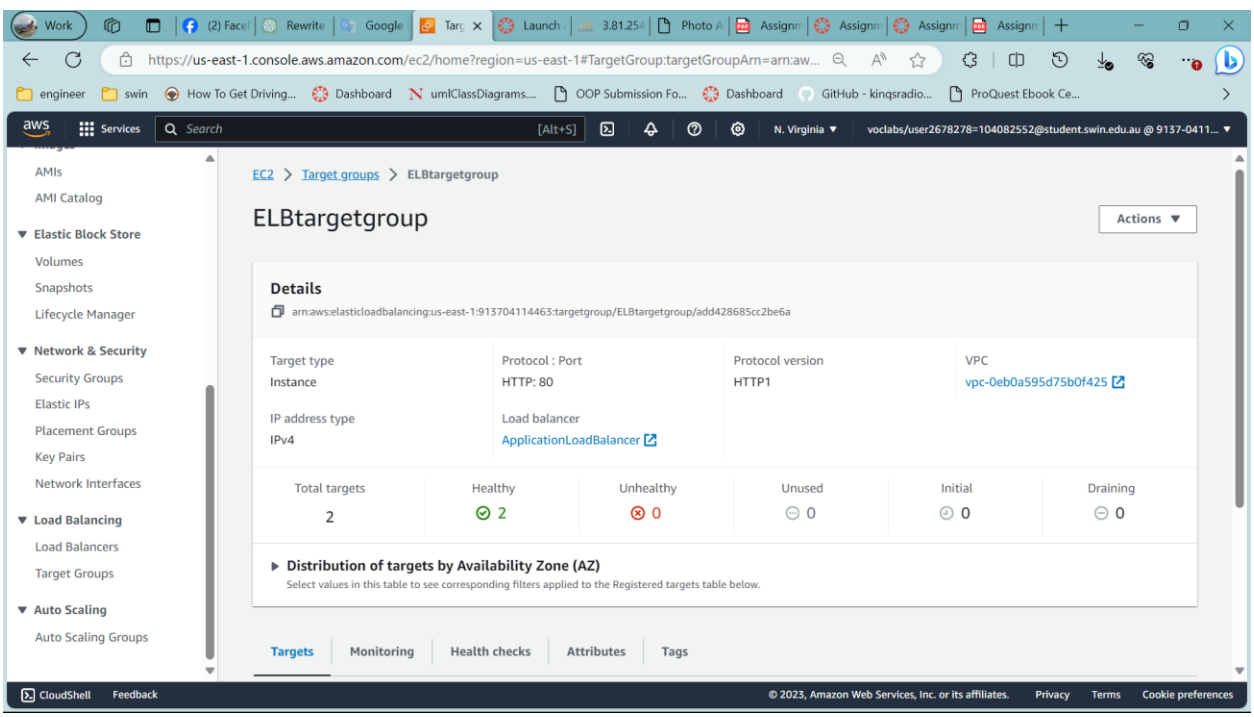

Figure 19: Target group

8. Auto Scaling Group

This feature will scale up the web server, making it highly available, and it has the ability to recover from failures. The ASG, Load Balancer and health checks all go together to create the environment.

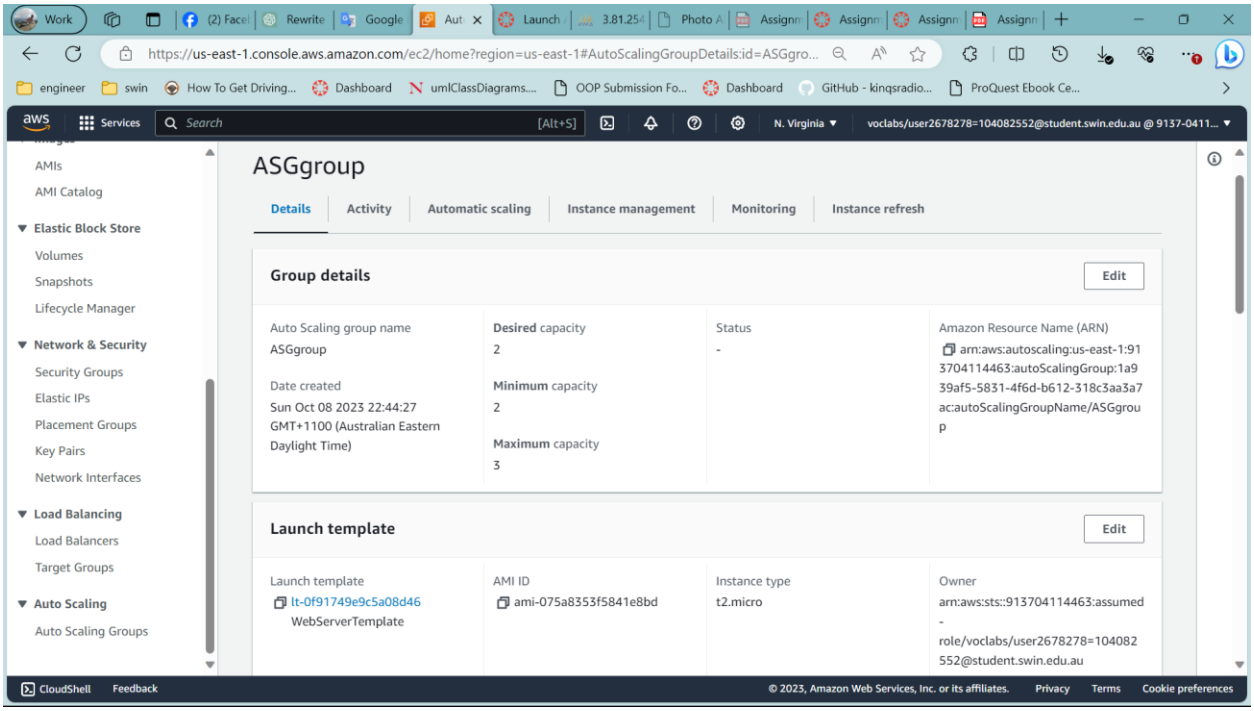

Figure 19: ASG group

9. Photo Album

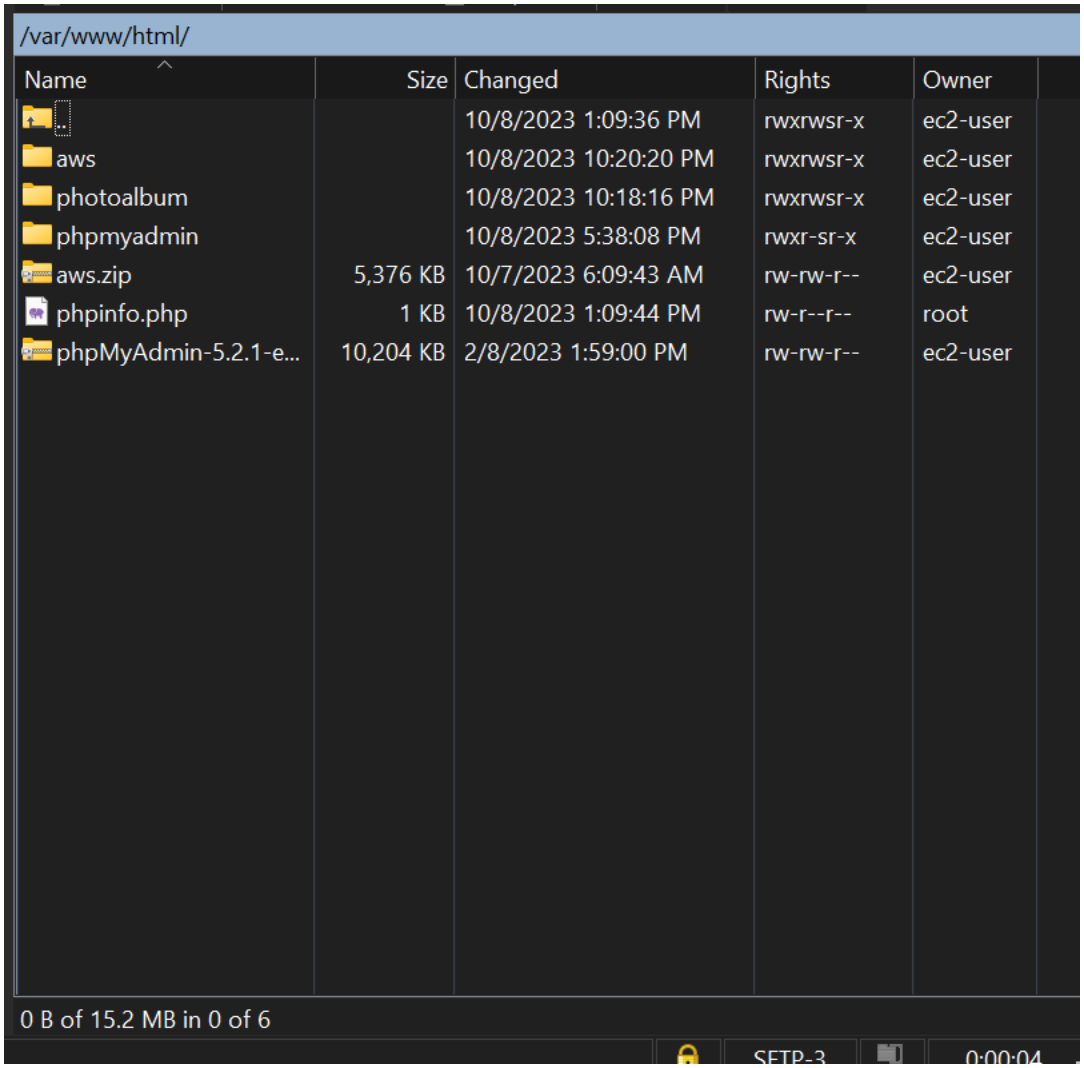

Figure 20: WinSCP

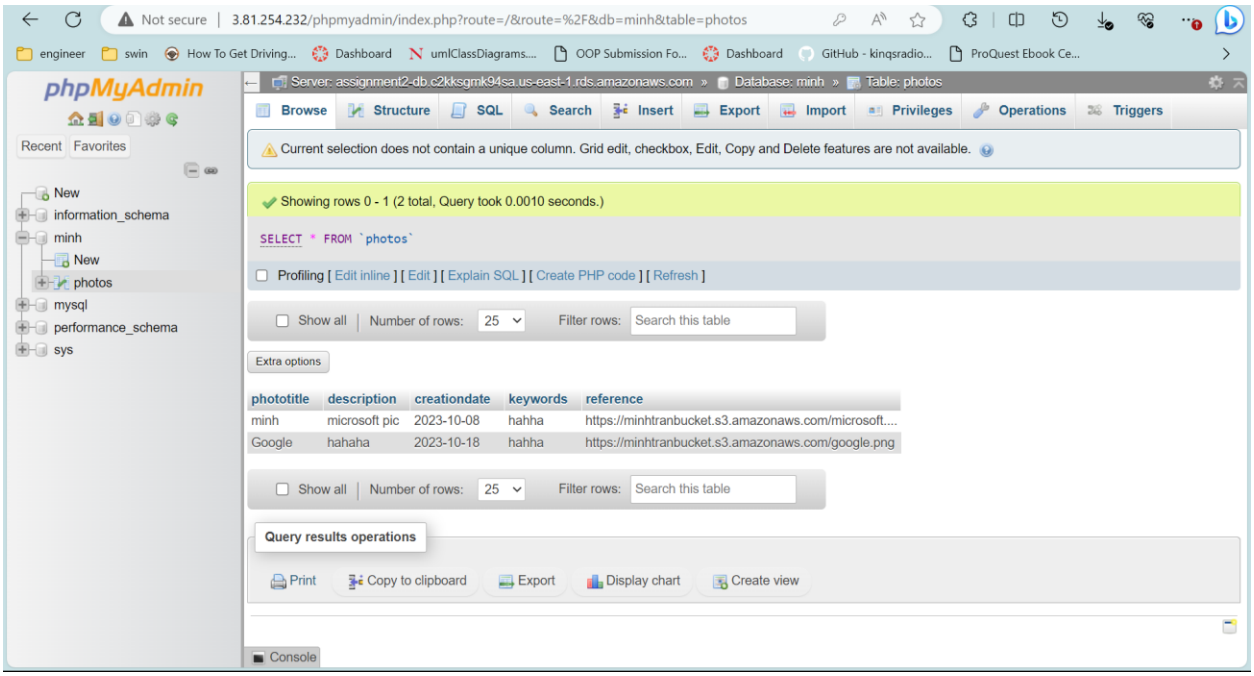

Figure 21: phpMyAdmin

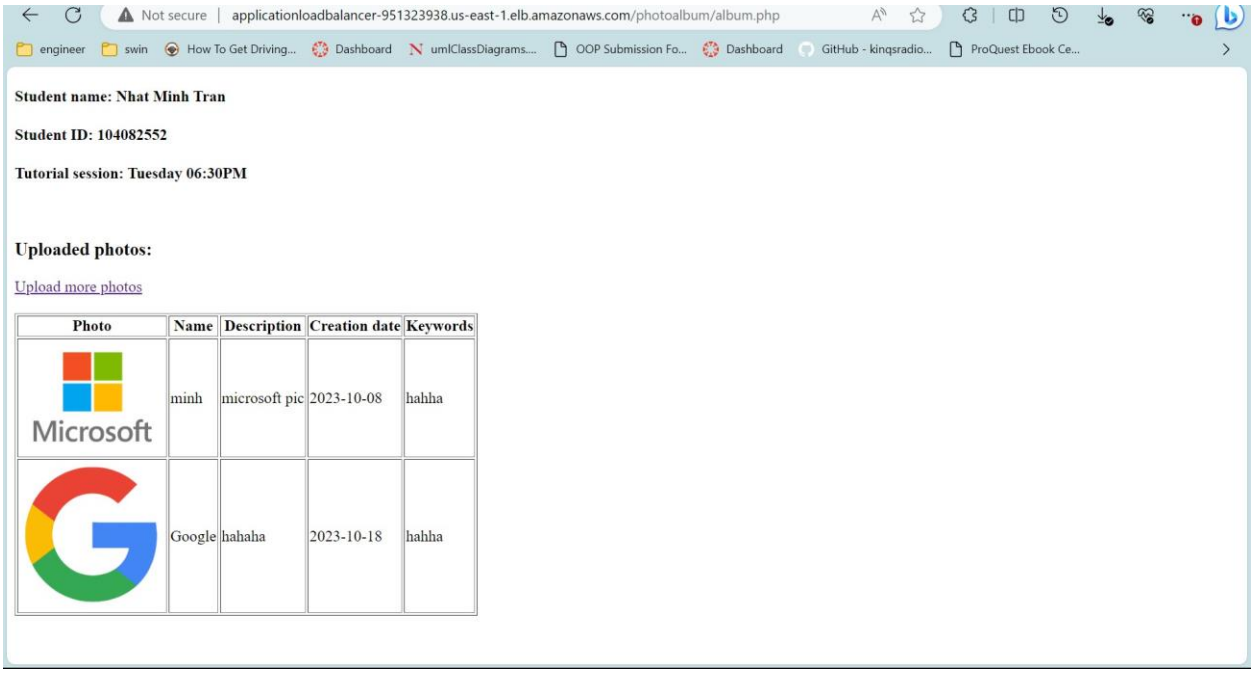

Figure 22: Album.php

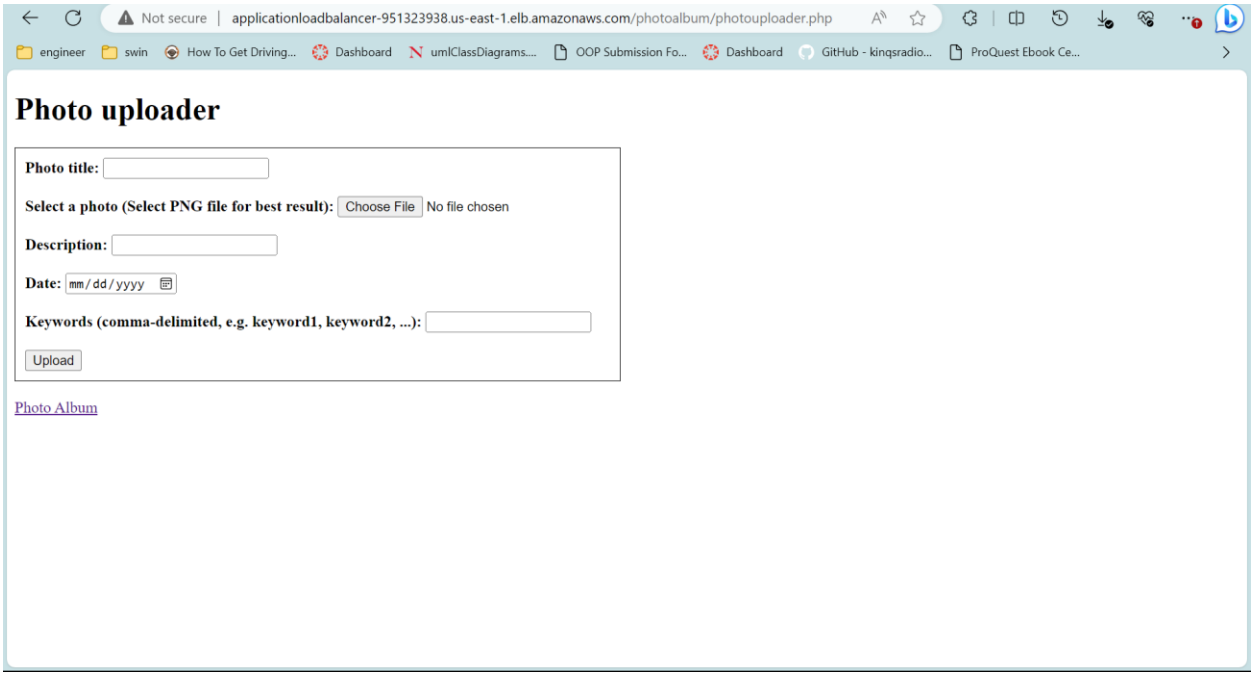

Figure 23: Photo uploader

The link is no more elastic Ip like assignment 1b, because we have created the load balancer, now we are accessing the photoalbum through load balancer link. It indicates that we have successfully create the highly available environment.

Link to ELB album.php: [Photo Album (applicationloadbalancer-951323938.us-east-1.elb.amazonaws.com)]

Link to ELB photouploader.php: [Photo Album (applicationloadbalancer-951323938.us-east-1.elb.amazonaws.com)]