Lab notebook Week 5

Submitted by: Vishrut Sharma (OdinID: vishrut)

Table of Contents

05.1g: Storage, IAM

2. GCP Cloud Storage #1 (USGS)

- **What roles are attached to the Compute Engine default service account?**

Answer: Editor

- **Would they be sufficient for the VM to perform its functions (i.e. creating buckets and reading/writing objects in them)?**

Answer: Yes, it would be sufficient.

- **What permissions are given by the default access scope to Cloud Storage?**

Answer: Read-only access to Storage and Service Management, write access to Stackdriver Logging and Monitoring, read/write access to Service Control.

- **Would they be sufficient for the VM to perform its functions (i.e. creating buckets and reading/writing objects in them)?**

Answer: No, it would be sufficient.

- **What settings are possible for setting the VM's access to the Storage API?**

Answer: None, Read Only, Write Only, Read Write, Full

4. USGS data and setup

- **What time did the latest earthquake happen?**

Answer: 2023-05-02T00:33:20.710Z

- **What was the magnitude (mag)?**

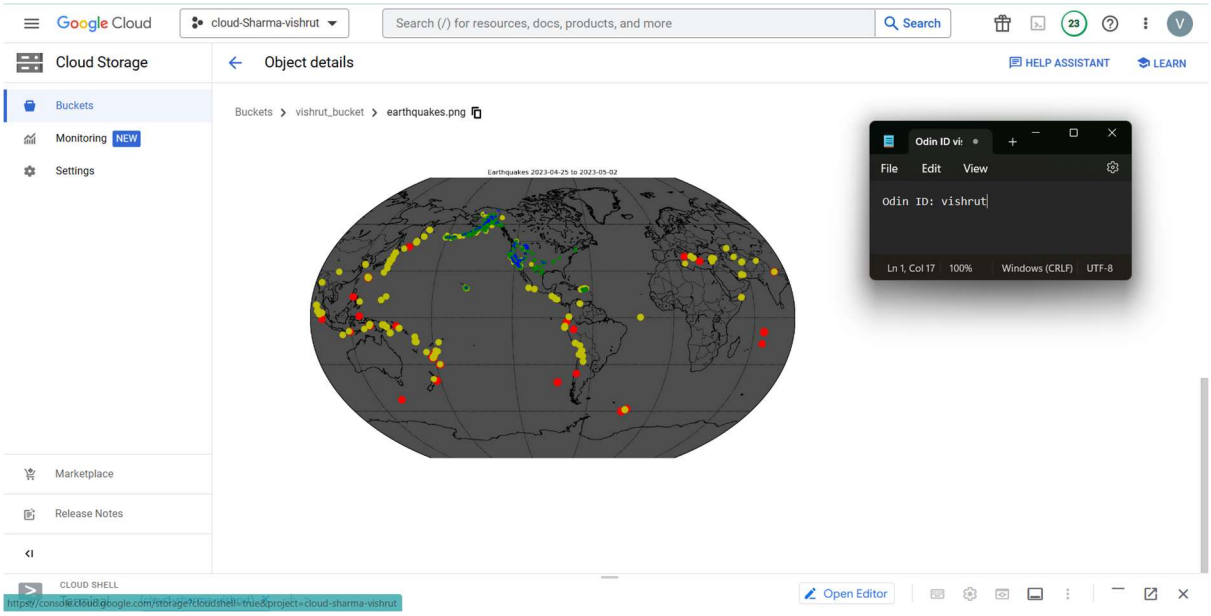
Answer: 0.92

- **Where was the place it happened?**

Answer: 3km WSW of Cobb, CA

5. Python plotting code

- **Take a screenshot of the image that has been created for your lab notebook.**



9. Service account roles (Compute)

- **What is the exact error message that is returned?**

```
vishrut@gcs-lab-vm:~$ gcloud compute instances list
ERROR: (gcloud.compute.instances.list) Some requests did not succeed:
 - Required 'compute.instances.list' permission for 'projects/cloud-sharma-vishrut'
```

- **What role needs to be added to the service account's permissions for the VM to have access to list the project's Compute Engine instances?**

Answer: Compute Viewer role needs to be added.

- **Take a screenshot of the output for your notebook.**

```
vishrut@gcs-lab-vm:~$ gcloud compute instances list
NAME         ZONE        MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP     STATUS
gcs-lab-vm   us-west1-b  e2-medium                  10.138.0.11  35.247.54.133   RUNNING
usgs         us-west1-b  e2-medium                  10.138.0.10  35.233.208.34   RUNNING
```

10. Service account roles (Storage)

- **What is the exact error message that is returned?**

Answer: AccessDeniedException: 403 gcs-lab@cloud-sharma-vishrut.iam.gserviceaccount.com does not have storage.objects.create access to the Google Cloud Storage object. Permission 'storage.objects.create' denied on resource (or it may not exist).

- **What role needs to be added to the service account's permissions for the VM to have access to add an object to a storage bucket?**

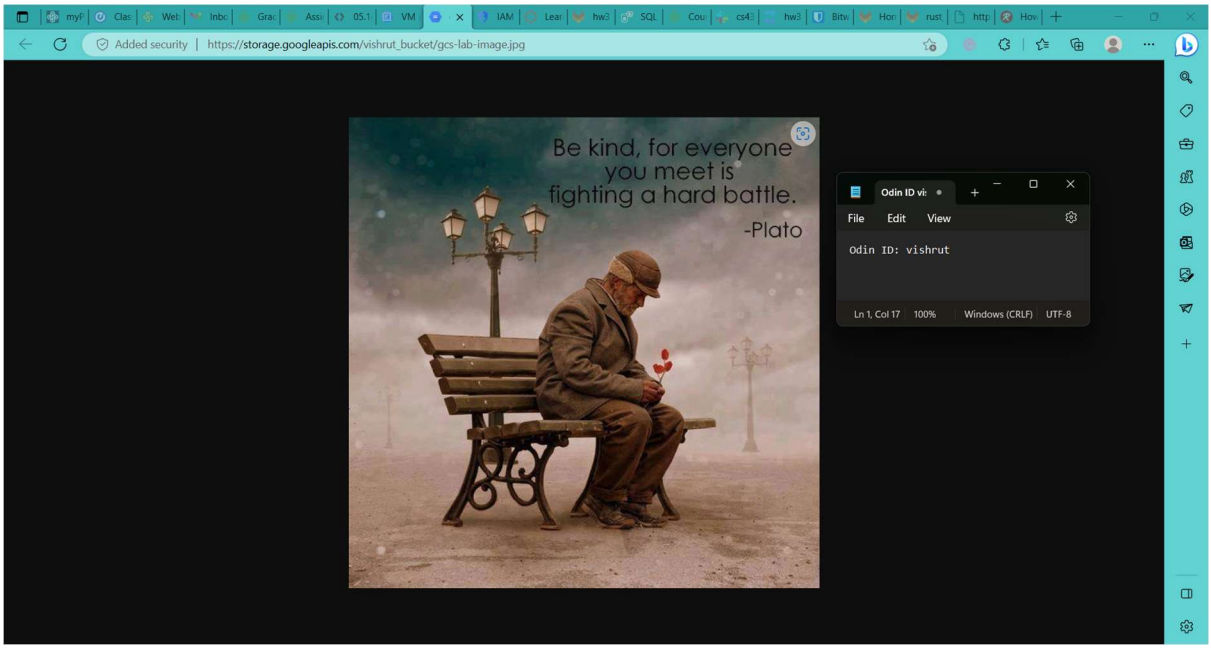
Answer: The storage Object Creator role needs to be added.

- **Take a screenshot of the output for your notebook.**

```
vishrut@gcs-lab-vm:~$ gsutil cp moonquakes.png gs://vishrut_bucket/
Copying file://moonquakes.png [Content-Type=image/png]...
/ [1 files][316.0 KiB/316.0 KiB]
Operation completed over 1 objects/316.0 KiB.
```

13. View object

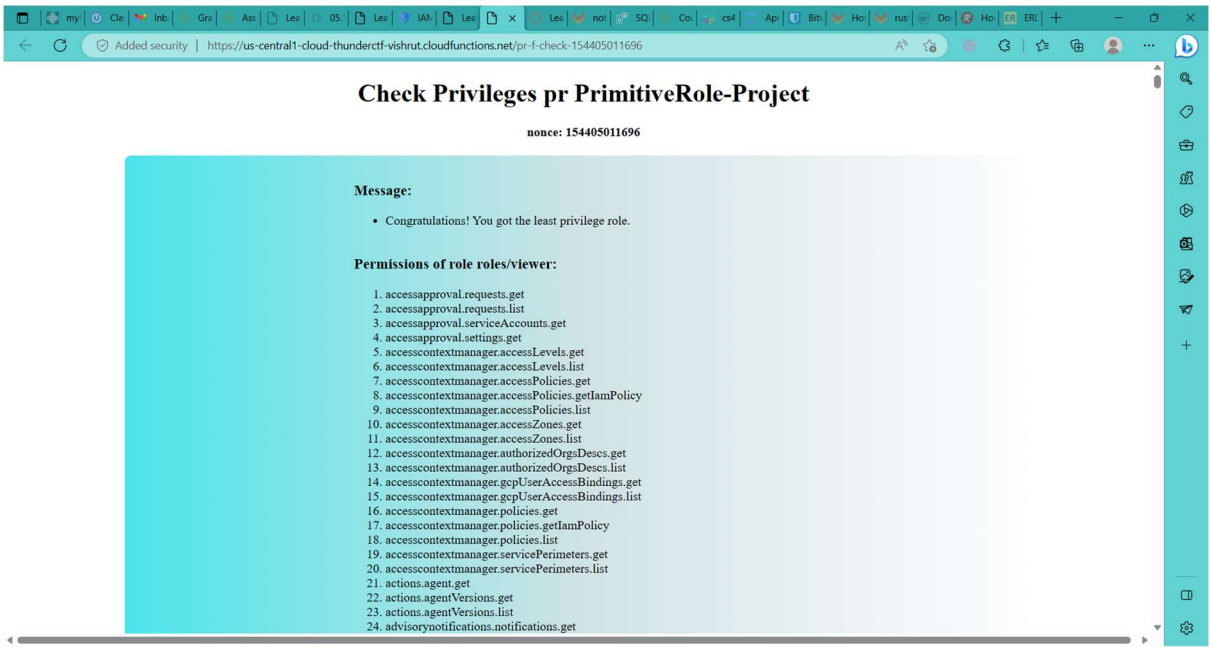
- **Take a screenshot the shows the entire URL and the image that has been retrieved:**

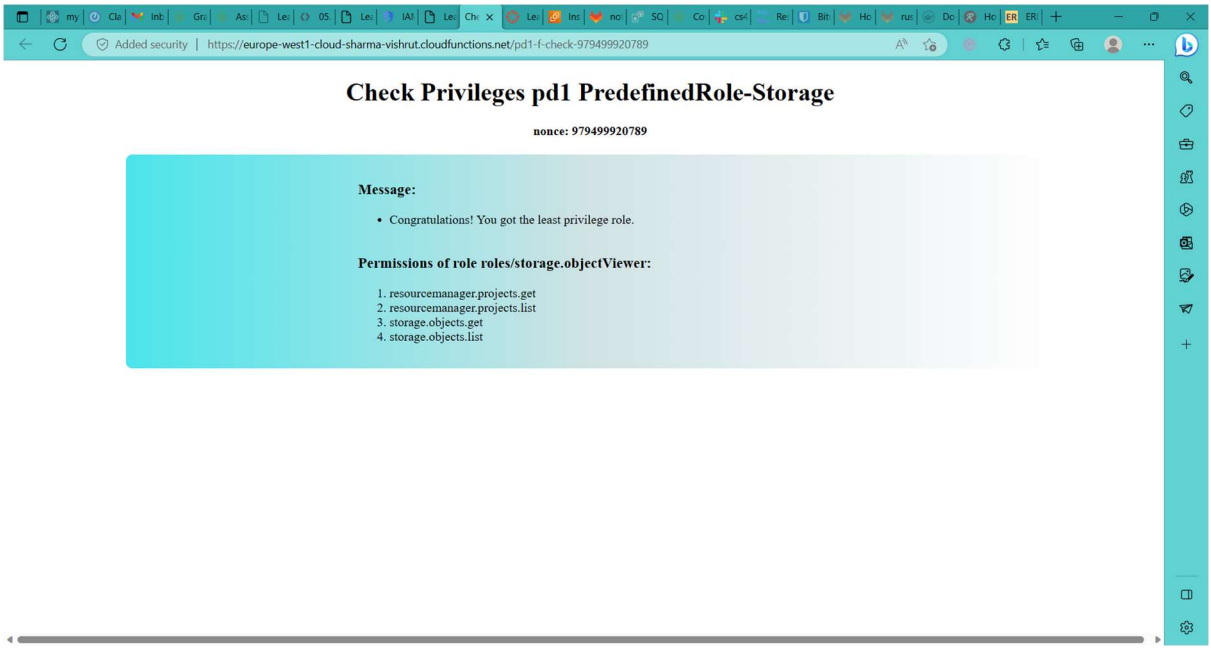


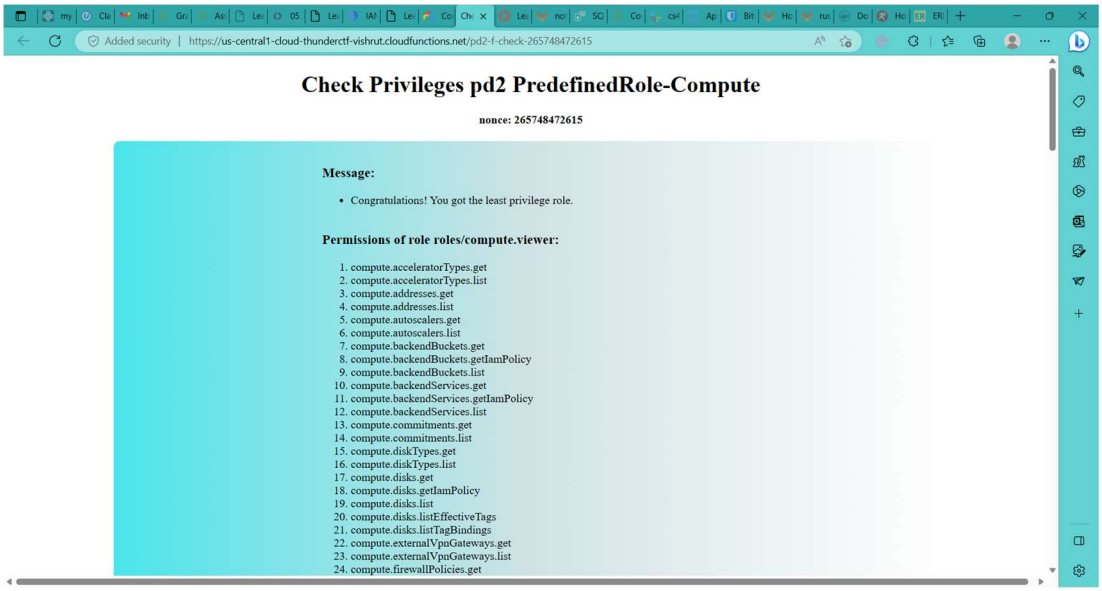
15. IAM and least privileges #4

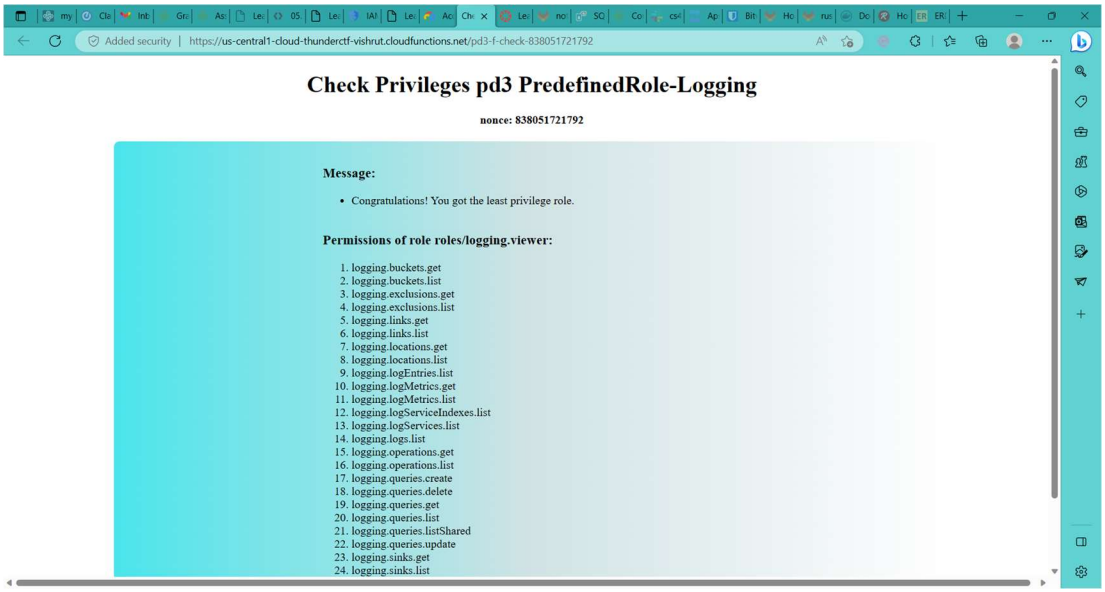
- **Take a screenshot that includes your project name in it.**

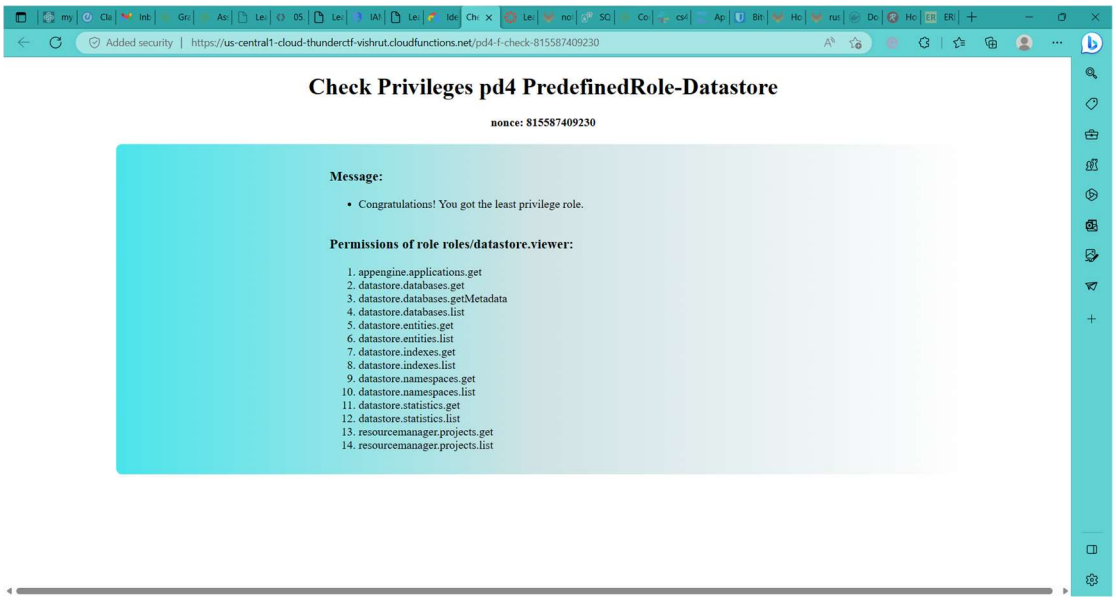
Odin ID and the project name are visible in the URL






Added security | https://us-central1-cloud-thunderctf-vishrut.cloudfunctions.net/pd2-f-check-265748472615
Check Privileges pd2 PredefinedRole-Compute
nonce: 265748472615
Message:
Congratulations! You got the least privilege role.
Permissions of role roles/compute.viewer:
1. compute.acceleratorTypes.get
2. compute.acceleratorTypes.list
3. compute.addresses.get
4. compute.addresses.list
5. compute.autoscalers.get
6. compute.autoscalers.list
7. compute.backendBuckets.get
8. compute.backendBuckets.getIamPolicy
9. compute.backendBuckets.list
10. compute.backendServices.get
11. compute.backendServices.getIamPolicy
12. compute.backendServices.list
13. compute.commitments.get
14. compute.commitments.list
15. compute.diskTypes.get
16. compute.diskTypes.list
17. compute.disks.get
18. compute.disks.getIamPolicy
19. compute.disks.list
20. compute.disks.listEffectiveTags
21. compute.disks.listTagBindings
22. compute.externalVpnGateways.get
23. compute.externalVpnGateways.list
24. compute.firewallPolicies.get


Added security | https://us-central1-cloud-thunderctf-vishrut.cloudfunctions.net/pd3-f-check-838051721792
Check Privileges pd3 PredefinedRole-Logging
nonce: 838051721792
Message:
Congratulations! You got the least privilege role.
Permissions of role roles/logging.viewer:
1. logging.buckets.get
2. logging.buckets.list
3. logging.exclusions.get
4. logging.exclusions.list
5. logging.links.get
6. logging.links.list
7. logging.locations.get
8. logging.locations.list
9. logging.logEntries.list
10. logging.logMetrics.get
11. logging.logMetrics.list
12. logging.logServiceIndexes.list
13. logging.logServices.list
14. logging.logs.list
15. logging.operations.get
16. logging.operations.list
17. logging.queries.create
18. logging.queries.delete
19. logging.queries.get
20. logging.queries.list
21. logging.queries.listShared
22. logging.queries.update
23. logging.sinks.get
24. logging.sinks.list


Added security | https://us-central1-cloud-thunderctf-vishrut.cloudfunctions.net/pd4-f-check-815587409230
Check Privileges pd4 PredefinedRole-Datastore
nonce: 815587409230
Message:
Congratulations! You got the least privilege role.
Permissions of role roles/datastore.viewer:
1. appengine.applications.get
2. datastore.databases.get
3. datastore.databases.getMetadata
4. datastore.databases.list
5. datastore.entities.get
6. datastore.entities.list
7. datastore.indexes.get
8. datastore.indexes.list
9. datastore.namespaces.get
10. datastore.namespaces.list
11. datastore.statistics.get
12. datastore.statistics.list
13. resourcemanager.projects.get
14. resourcemanager.projects.list

Added security | https://us-central1-cloud-thunderctf-vishrut.cloudfunctions.net/pd5-f-check-233547341718

Check Privileges pd5 PredefinedRole-Vision

nonce: 233547341718

Message:

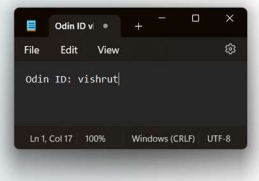
- Congratulations! You got the least privilege role.

Permissions of role roles/datastore.user:

1. appengine.applications.get
2. datastore.databases.get
3. datastore.databases.getMetadata
4. datastore.databases.list
5. datastore.entities.allocateIds
6. datastore.entities.create
7. datastore.entities.delete
8. datastore.entities.get
9. datastore.entities.list
10. datastore.entities.update
11. datastore.indexes.list
12. datastore.namespaces.get
13. datastore.namespaces.list
14. datastore.statistics.get
15. datastore.statistics.list
16. resourcemanager.projects.get
17. resourcemanager.projects.list

Permissions of role roles/storage.admin:

1. firebase.projects.get
2. orgpolicy.policy.get
3. recommender.iamPolicyInsights.get



Added security | https://us-central1-cloud-thunderctf-vishrut.cloudfunctions.net/ct1-f-check-354548260940

Check Privileges ct1 CustomRole-Project

nonce: 354548260940

Message:

- Congratulations! You get the least privileges.

Permissions of custom role projects/cloud-thunderctf-vishrut/roles/ct1_access_role_354548260940:

1. compute.instances.list
2. storage.buckets.list

Added security | https://us-central1-cloud-thunderctf-vishrut.cloudfunctions.net/ct2-f-check-424103715722

Check Privileges ct2 CustomRole-Storage

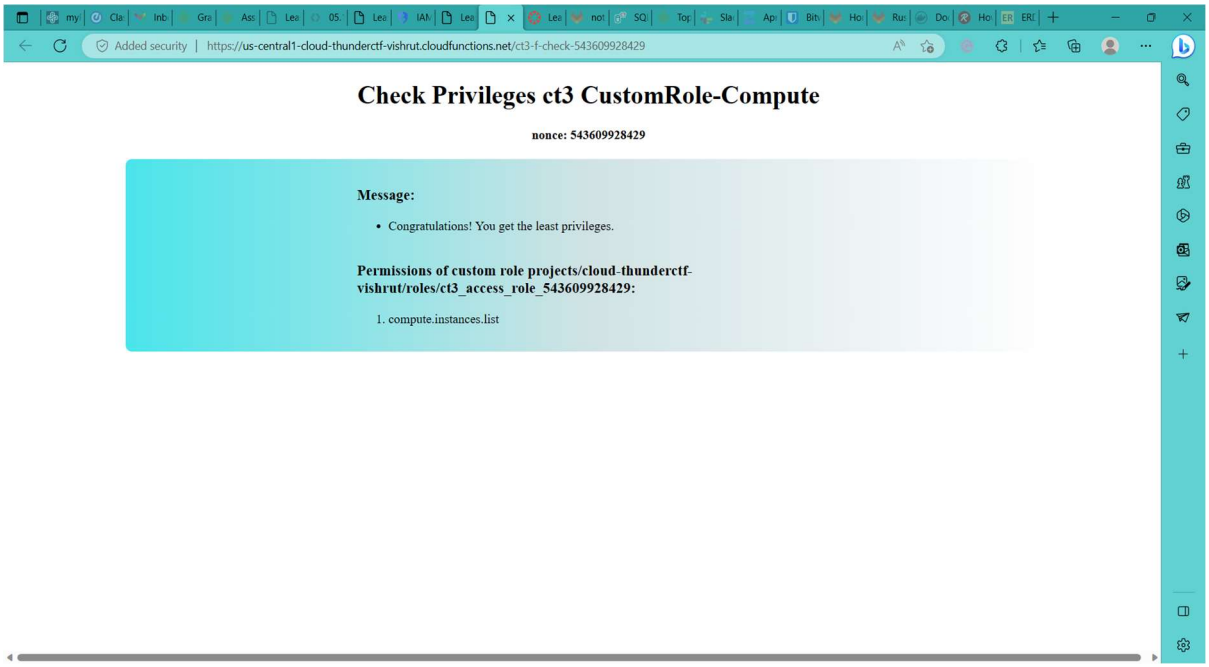
nonce: 424103715722

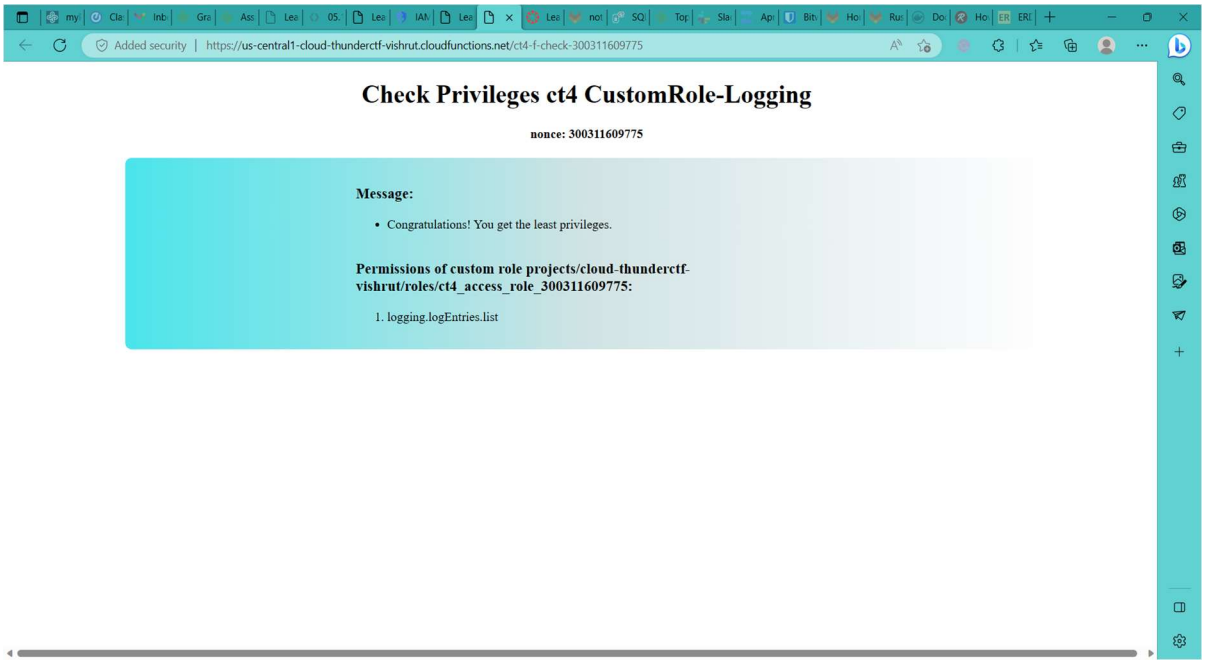
Message:

- Congratulations! You get the least privileges.

Permissions of custom role projects/cloud-thunderctf-vishrut/roles/ct2_access_role_424103715722:

1. storage.objects.list

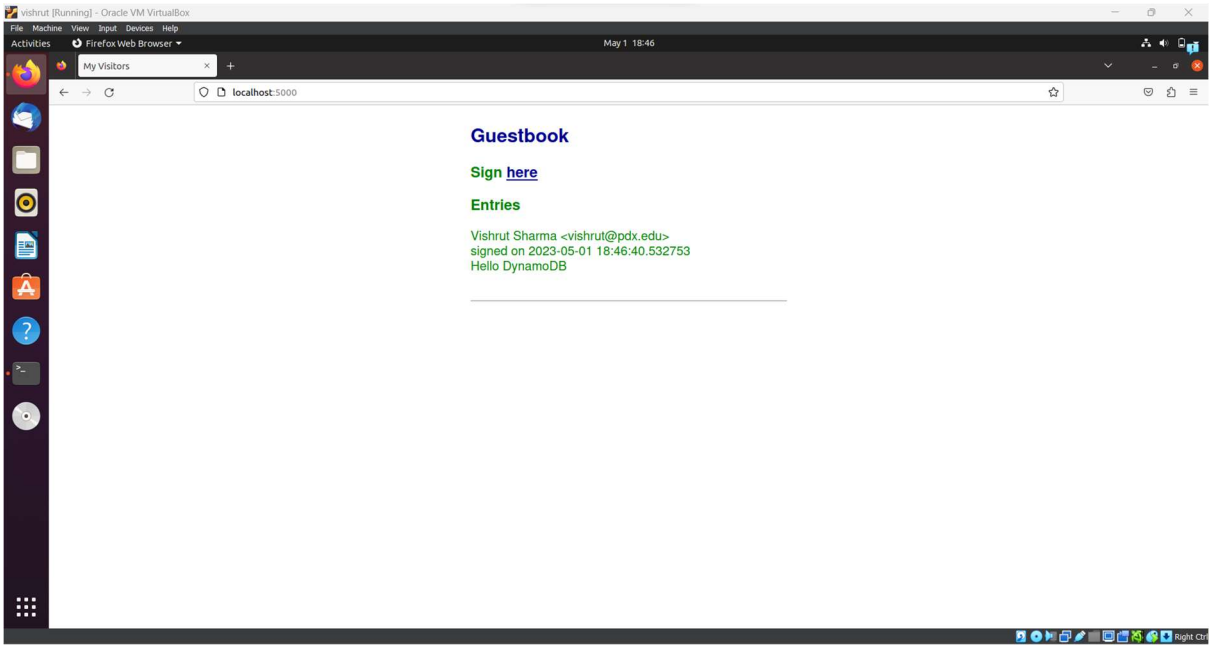

Added security | https://us-central1-cloud-thunderctf-vishrut.cloudfunctions.net/ct3-f-check-543609928429
Check Privileges ct3 CustomRole-Compute
nonce: 543609928429
Message:
Congratulations! You get the least privileges.
Permissions of custom role projects/cloud-thunderctf-vishrut/roles/ct3_access_role_543609928429:
1. compute.instances.list


Added security | https://us-central1-cloud-thunderctf-vishrut.cloudfunctions.net/ct4-f-check-300311609775
Check Privileges ct4 CustomRole-Logging
nonce: 300311609775
Message:
Congratulations! You get the least privileges.
Permissions of custom role projects/cloud-thunderctf-vishrut/roles/ct4_access_role_300311609775:
1. logging.logEntries.list

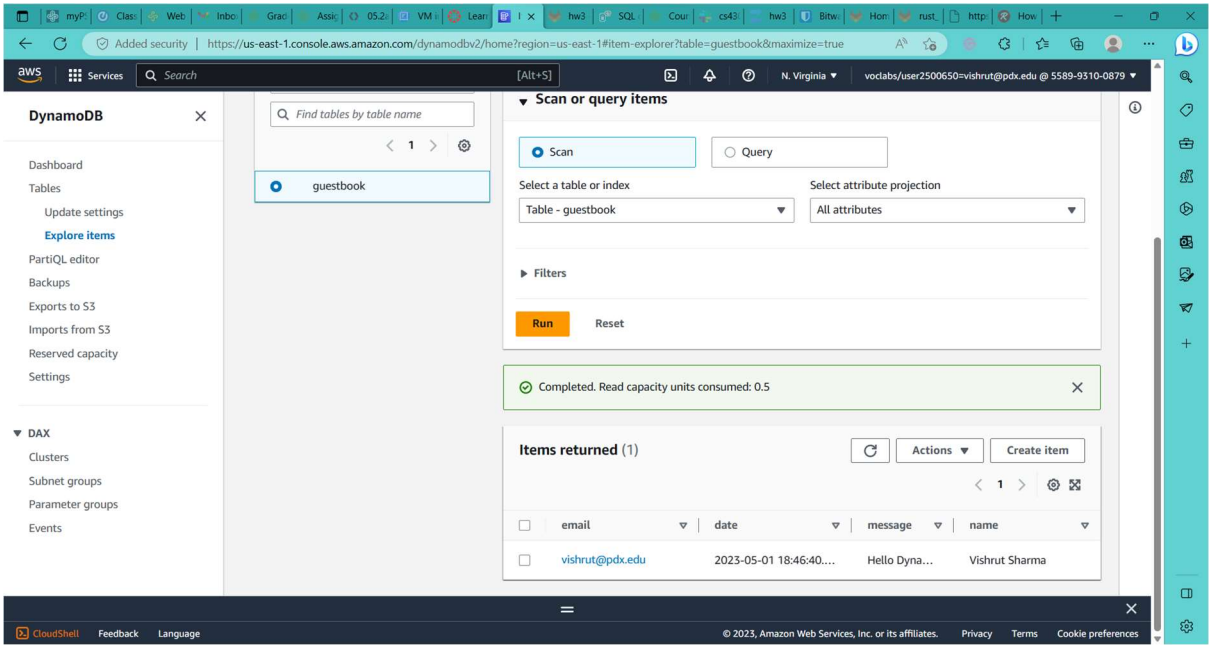
05.2a: DynamoDB Guestbook

5. Run the application

- **Take a screenshot of the output for your lab notebook.**

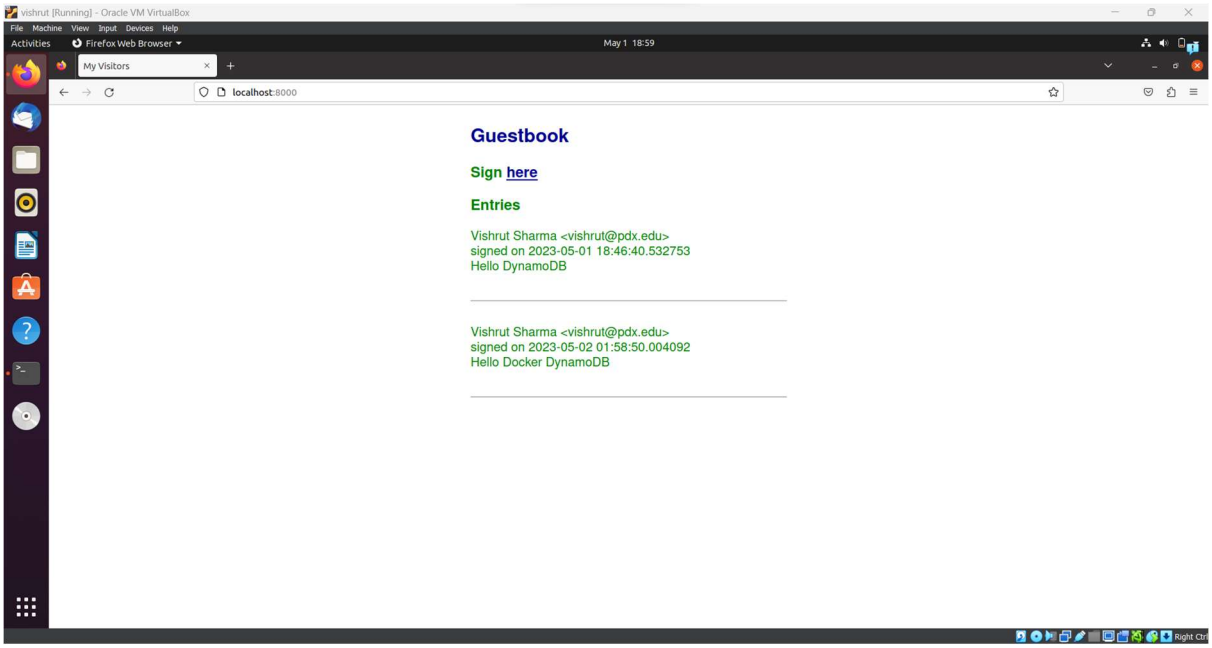


Click on the "Items" tab and view the entry you have just added to your DynamoDB table.

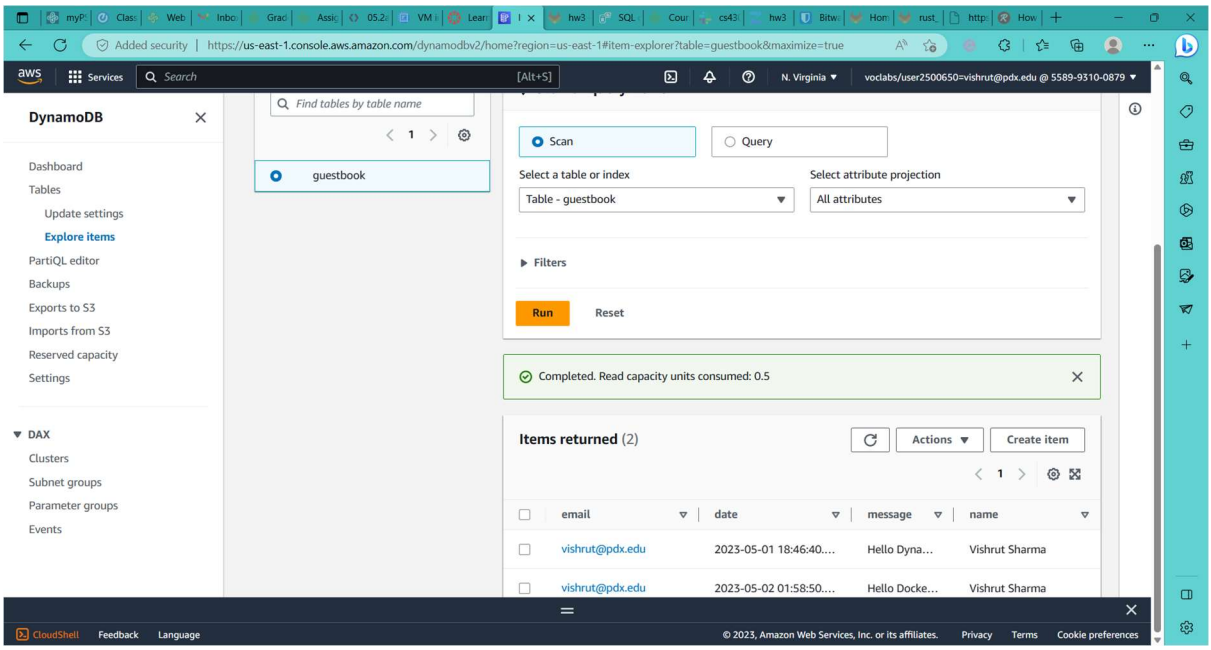


7. Run the application

- **Take a screenshot of the output for your lab notebook.**

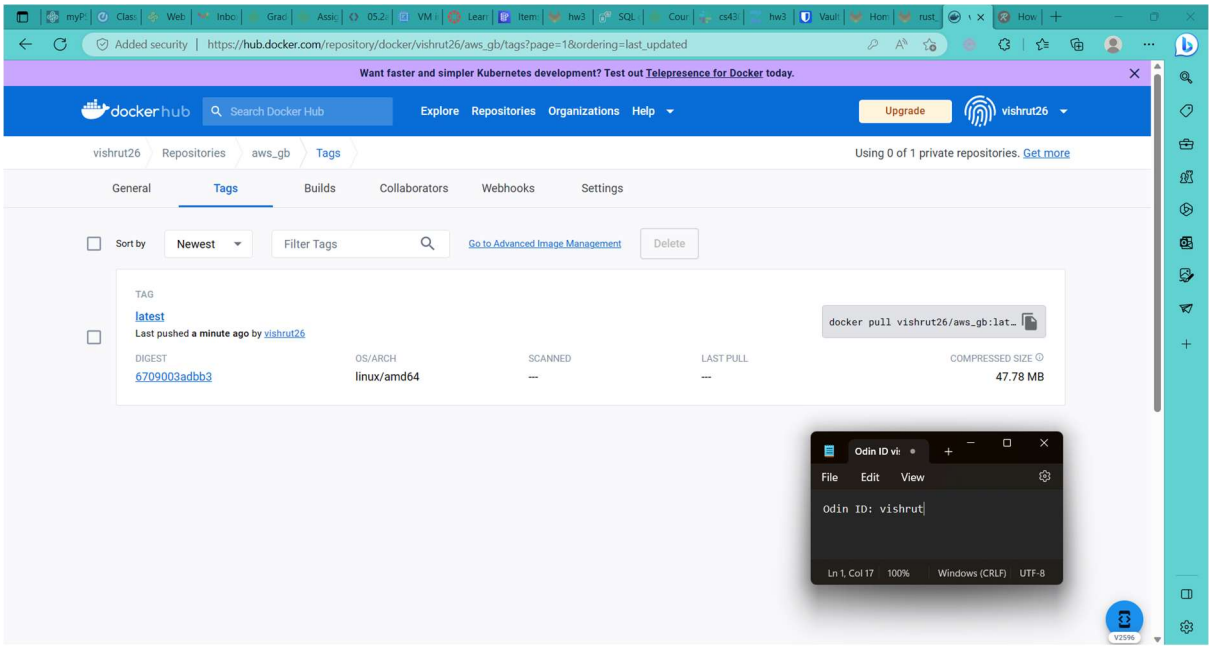


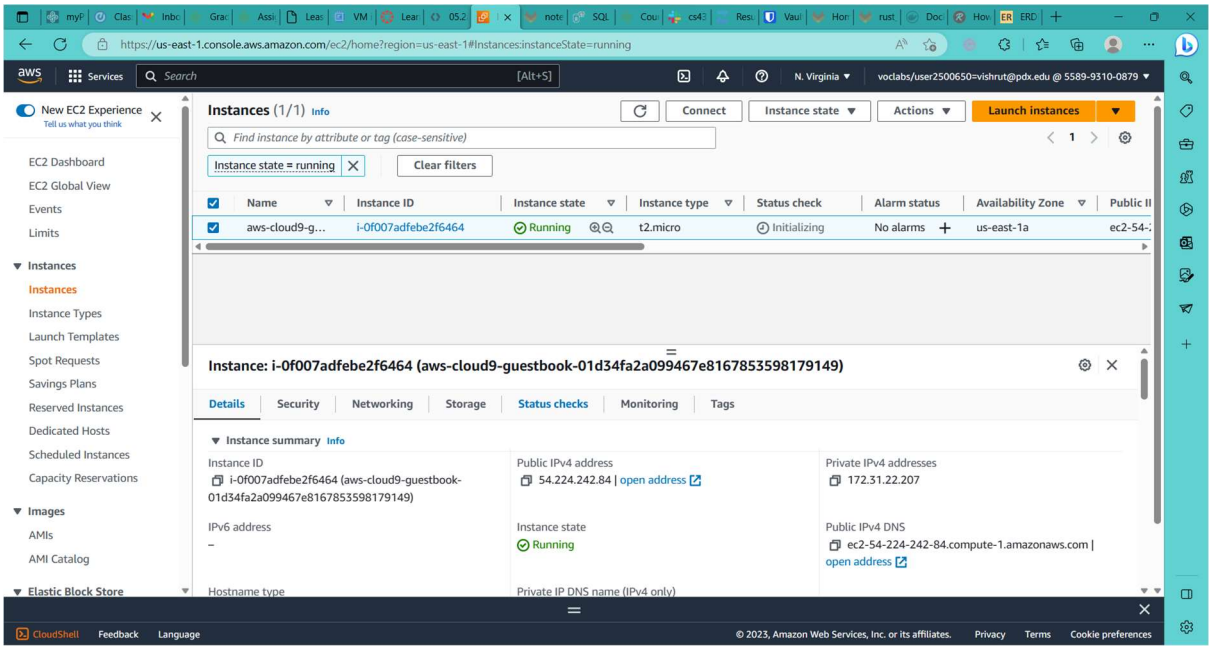
Go back to the AWS DynamoDB console and see that a second item has been added to the table.



8. Push the container image

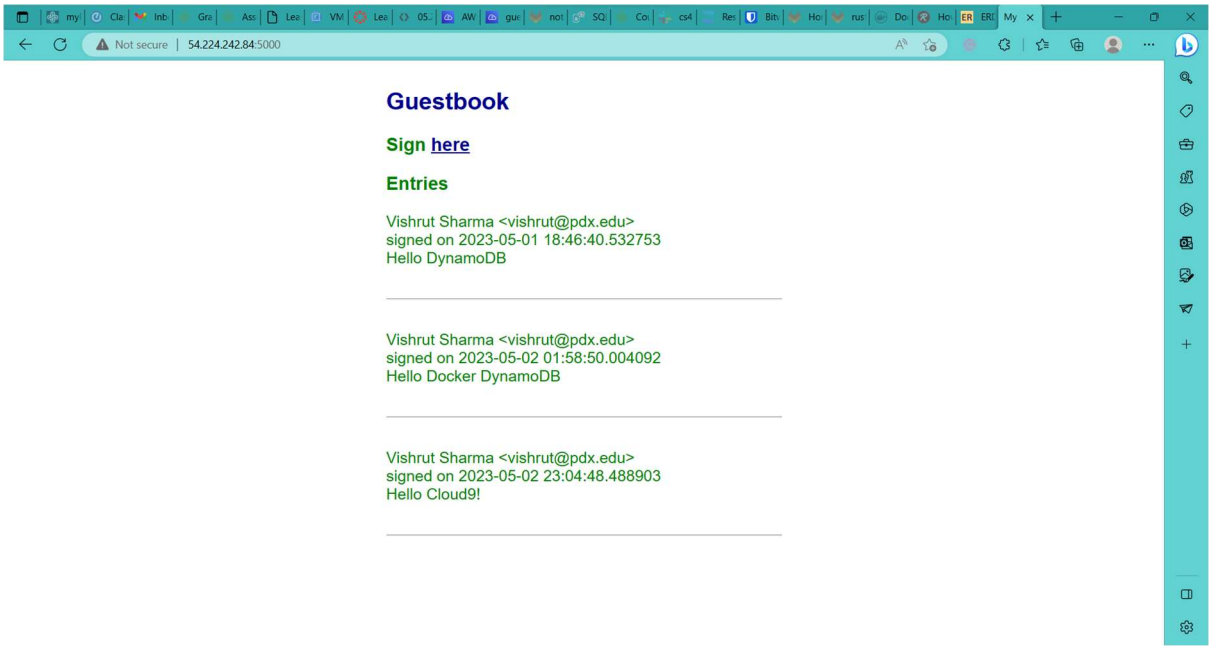
- **Take a screenshot of the container image on DockerHub.**





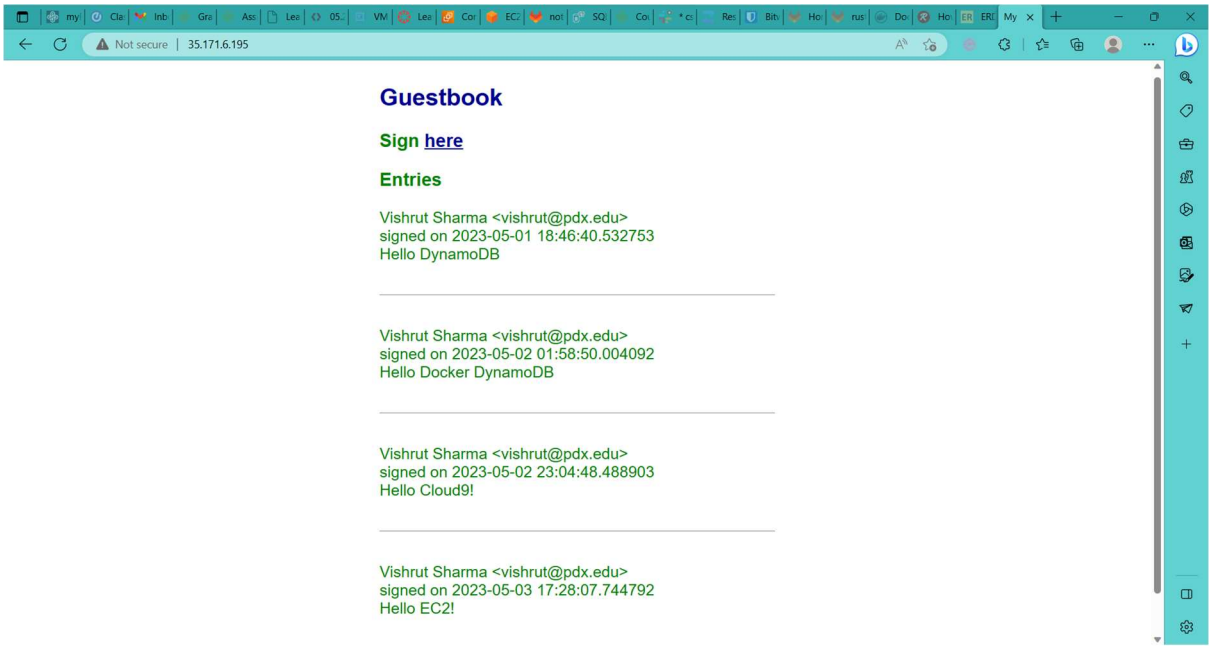
11. Run the application

- **Take a screenshot as before that shows your entry and the IP address in the URL bar.**



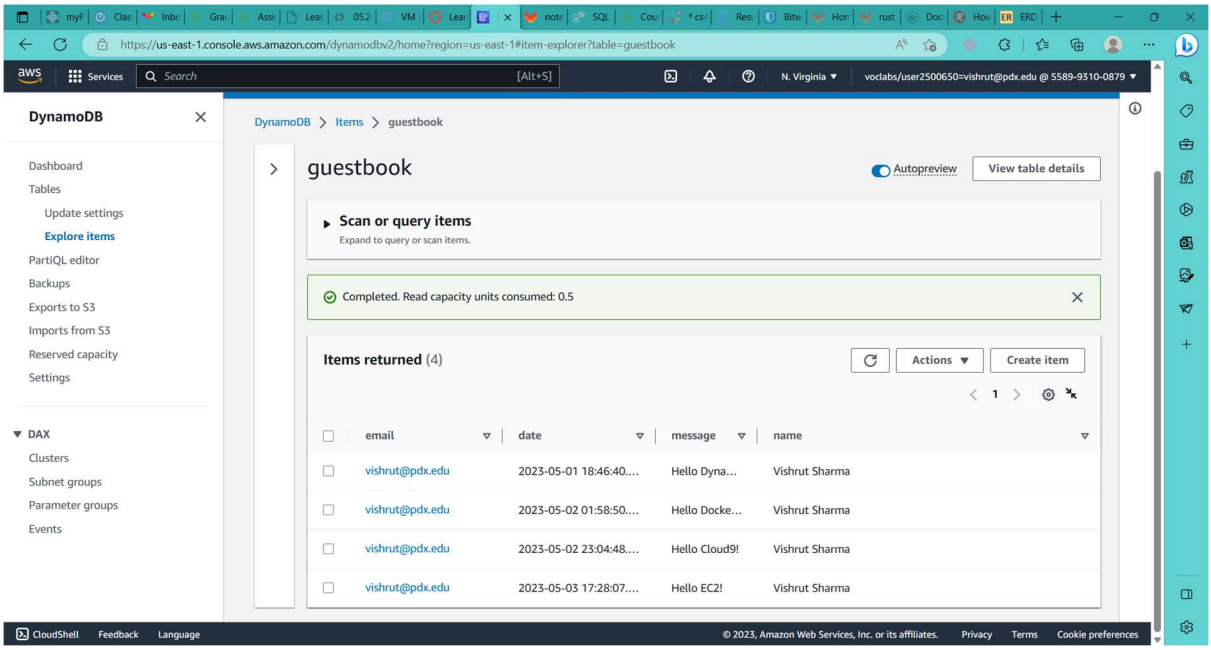
15. Visit the application

- **Take a screenshot as before that shows your entry and the IP address in the URL bar.**



16. View the database

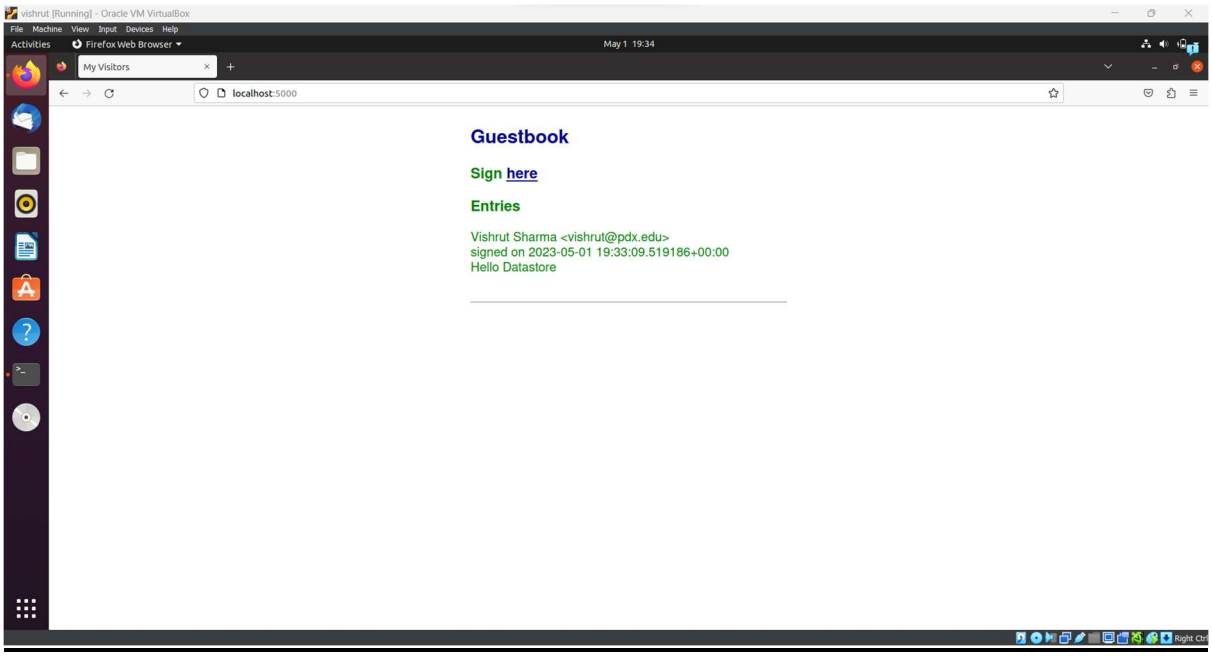
- **Take a screenshot that shows all of the guestbook entries that you added to the DynamoDB table including their timestamps.**



05.2g: Cloud Datastore Guestbook

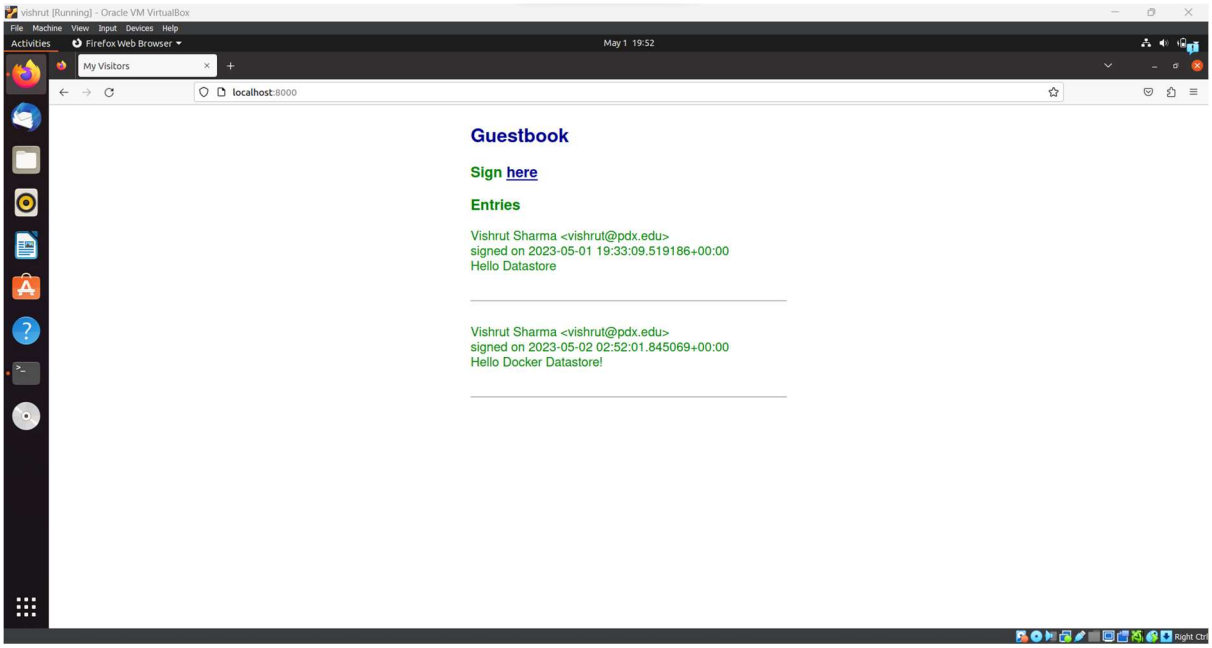
7. Run the application

- **Take a screenshot of the output for your lab notebook.**



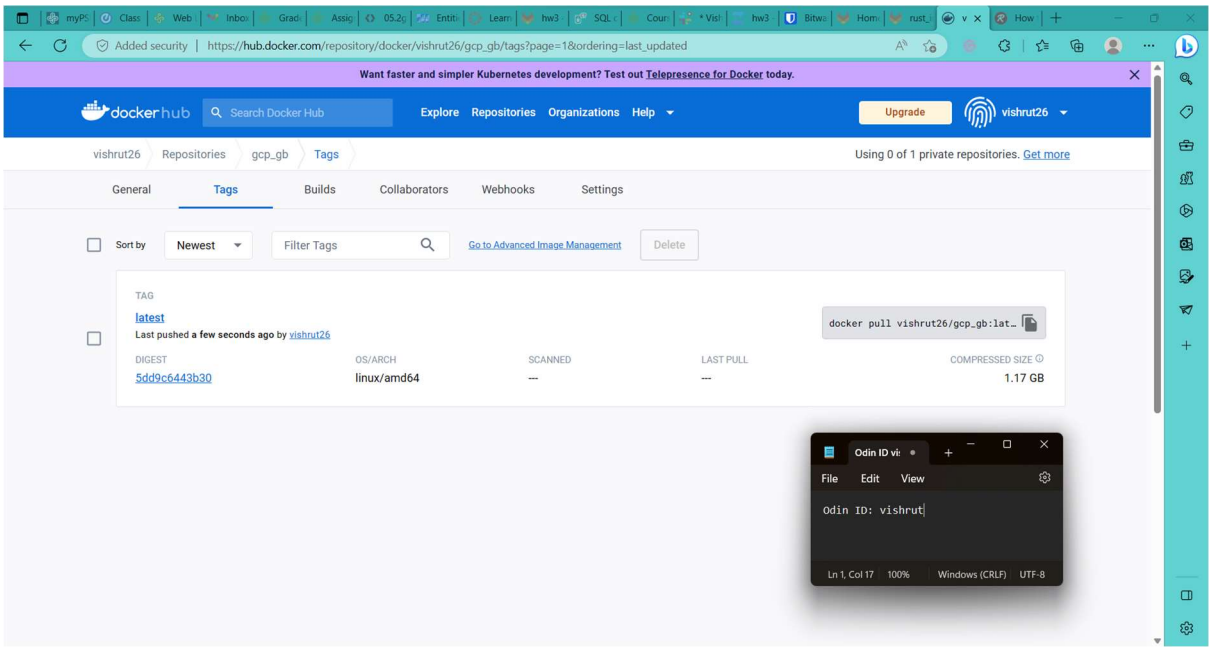
9. Run the application

- **Take a screenshot of the output for your lab notebook.**



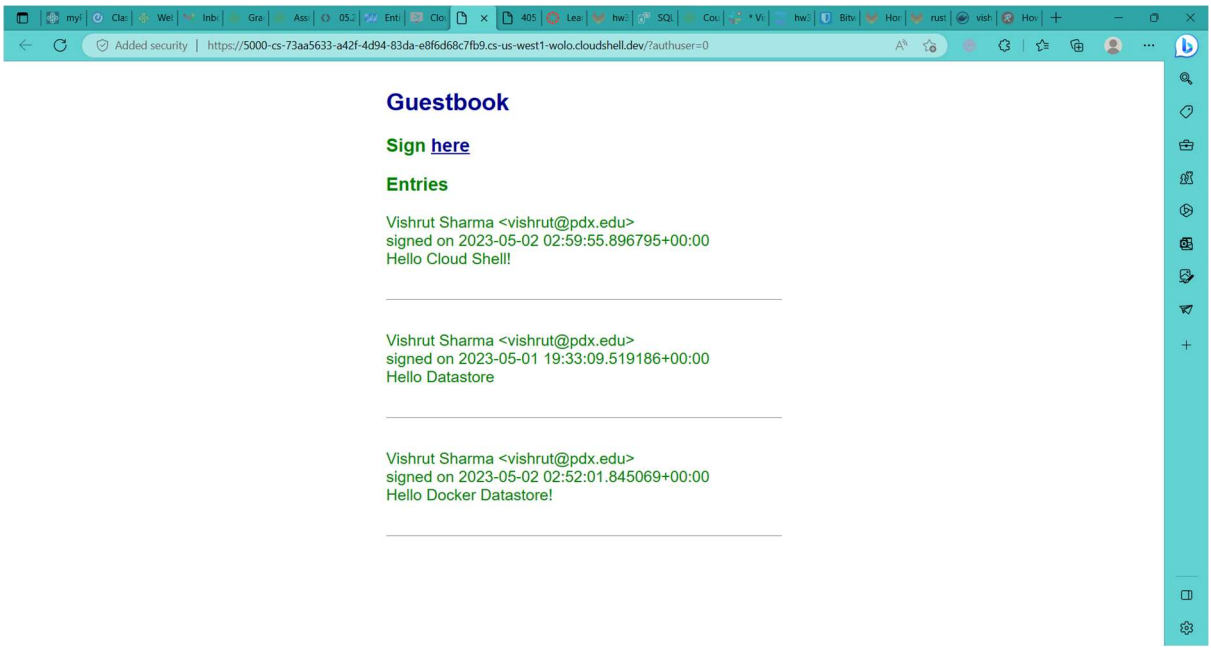
10. Push the container image

View the container image on DockerHub.



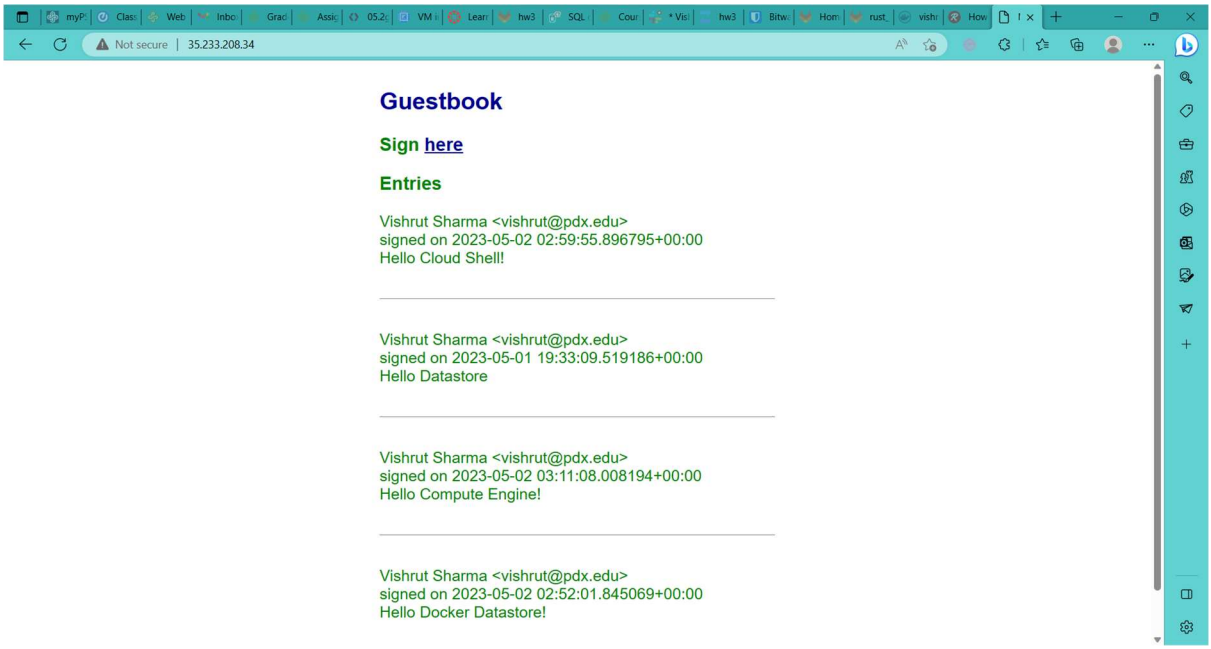
12. Run the application

- **Take a screenshot as before that shows your entry and the URL bar.**



15. Visit the application

- **Take a screenshot as before that shows your entry and the IP address in the URL bar.**



16. View the database

- **Take a screenshot of all of the entries that have been added including their timestamps for your lab notebook.**