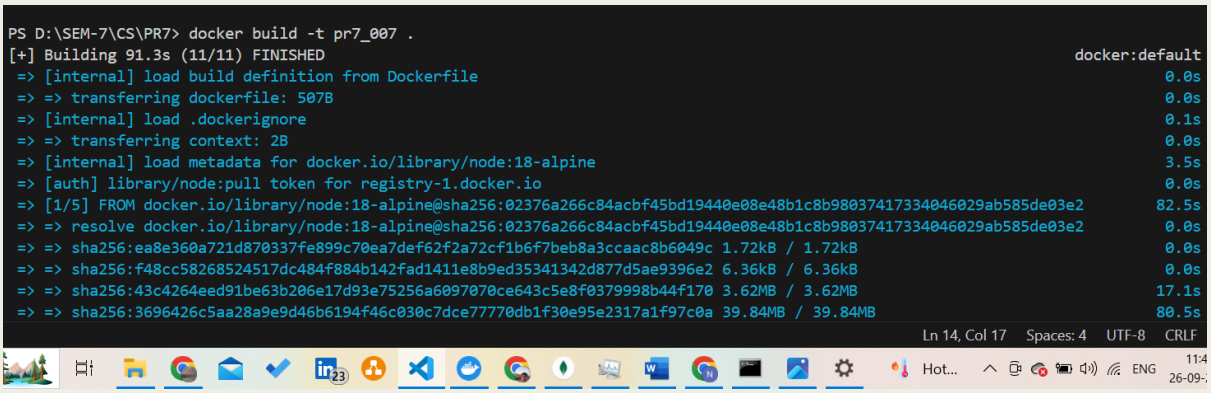
NAME: KSHITIJ GUPTA
Enrolment Number: 21162101007
Sub: CS

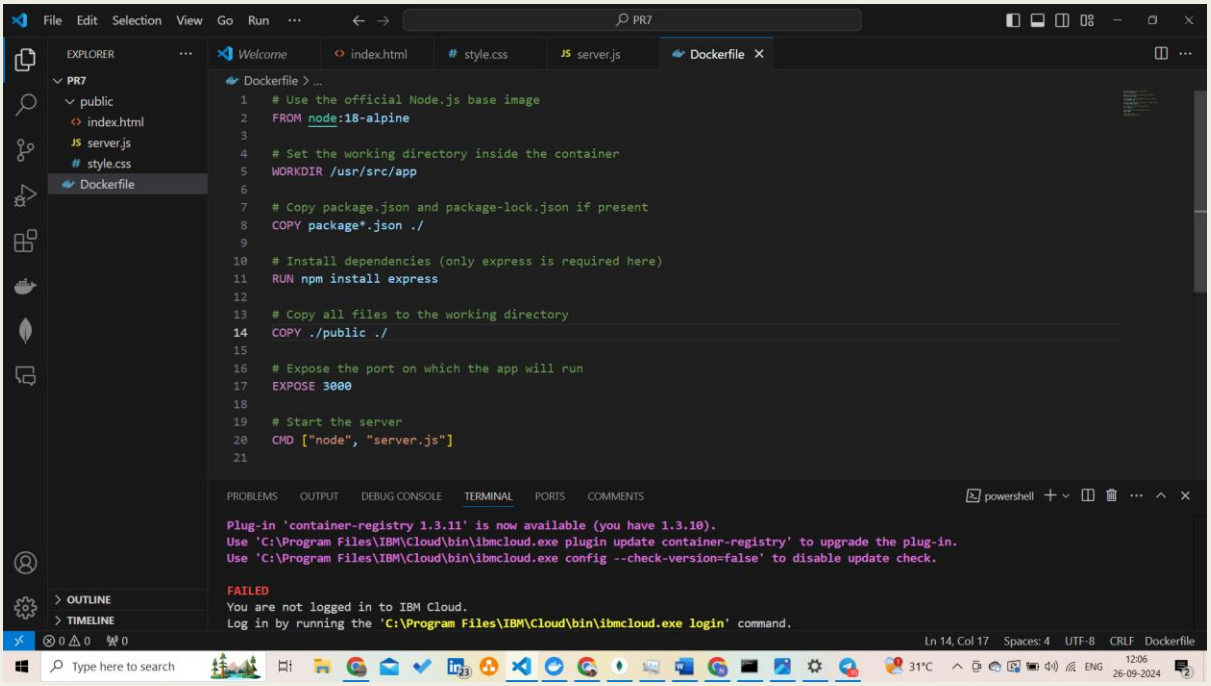
Practical – 7[Batch-71]

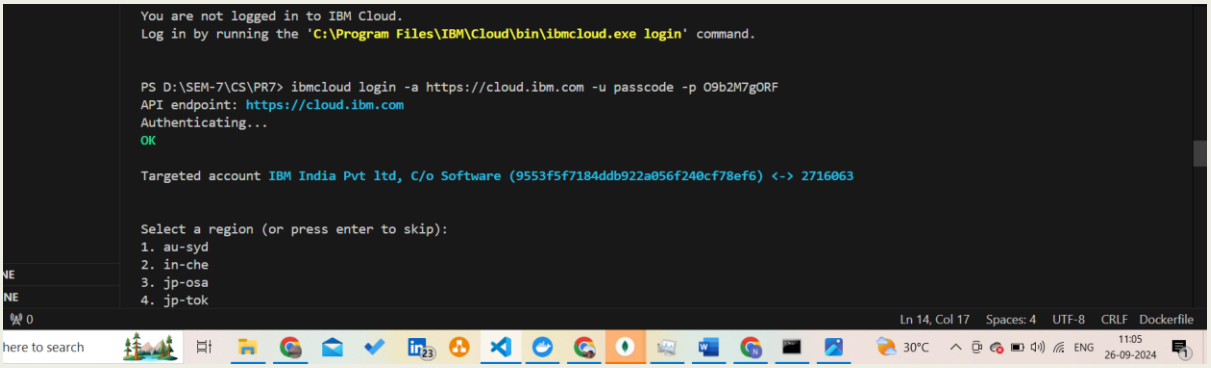
Securing a Docker Image Before Deployment to
Production John, a developer, is working on a web application called *SecureApp* that his team plans to deploy to a Kubernetes cluster in IBM Cloud. Before deployment, John wants to ensure the Docker image for *SecureApp* is secure and free from vulnerabilities. He decides to use IBM Cloud Container Registry and Vulnerability Advisor to scan the image for security issues and make the necessary corrections.

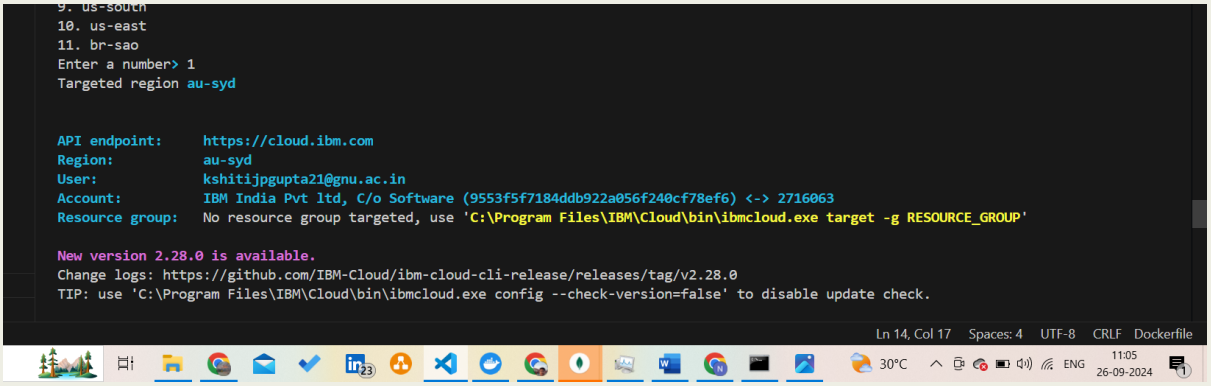
Step-1: create a docker image and run it



Step-2: login into IBM Cloud account

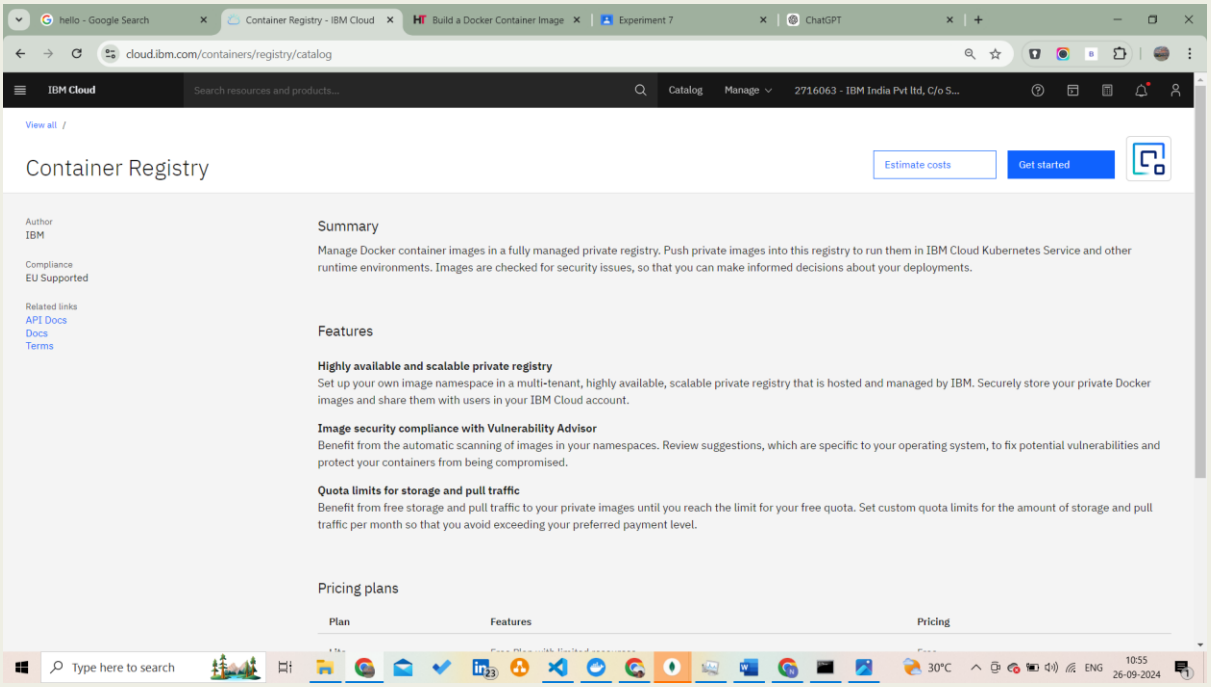


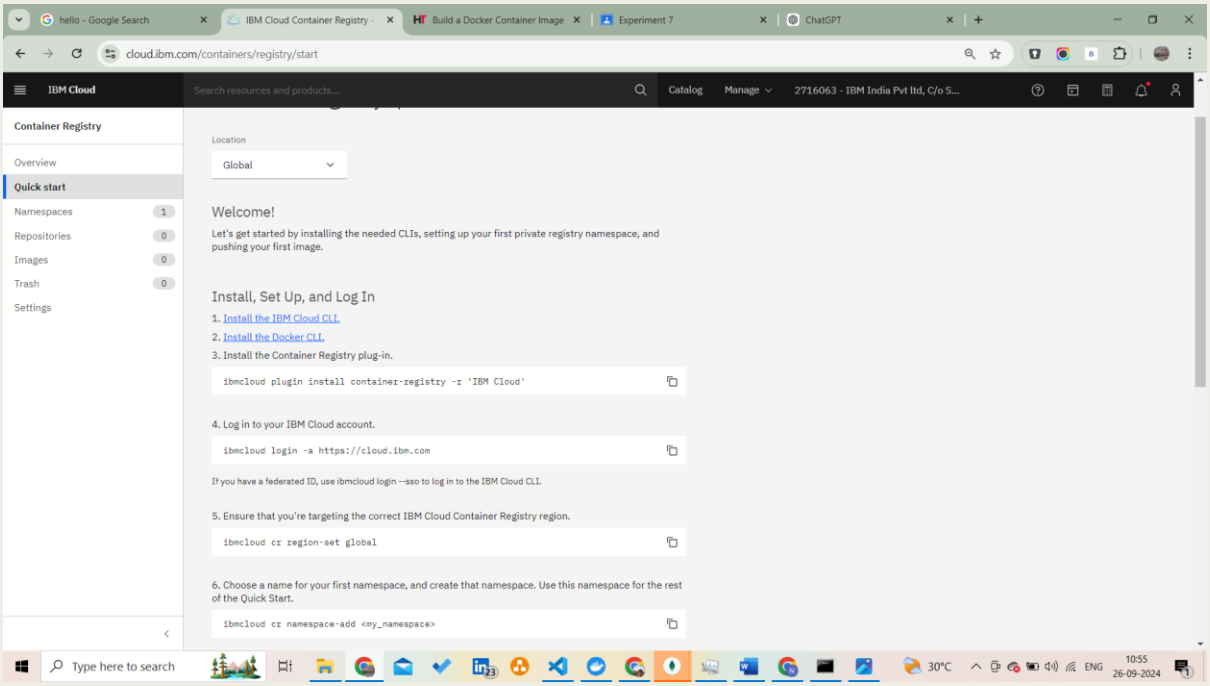


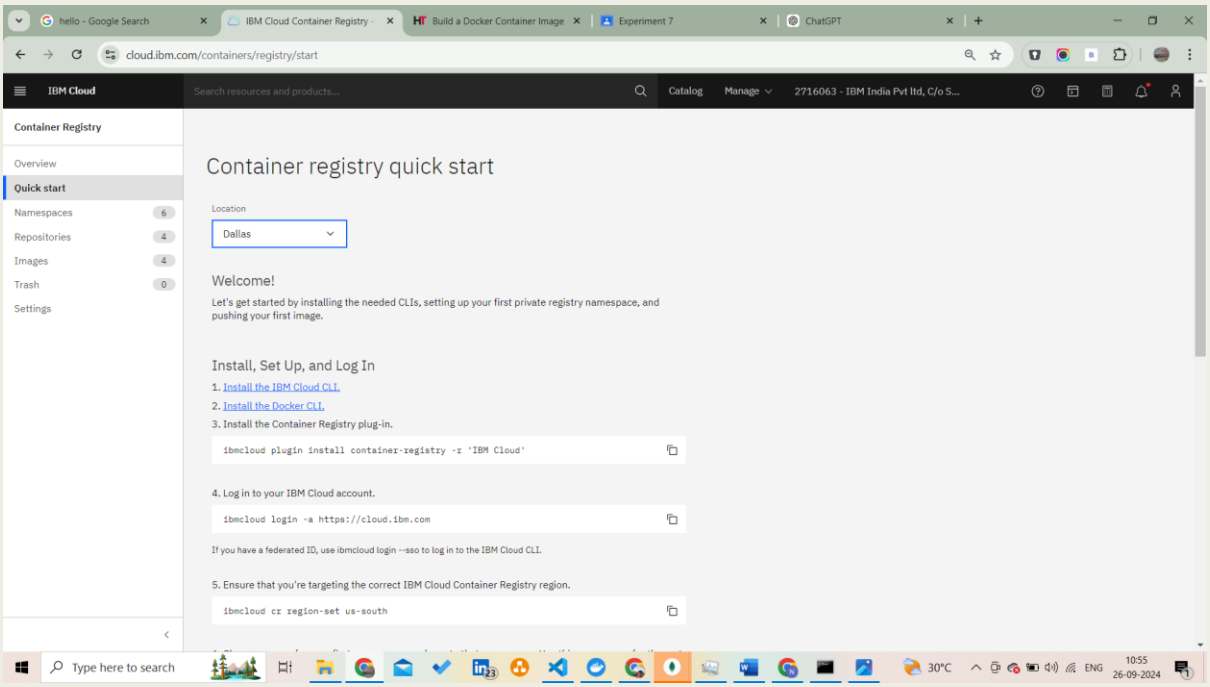


Step-3: create a container Registry

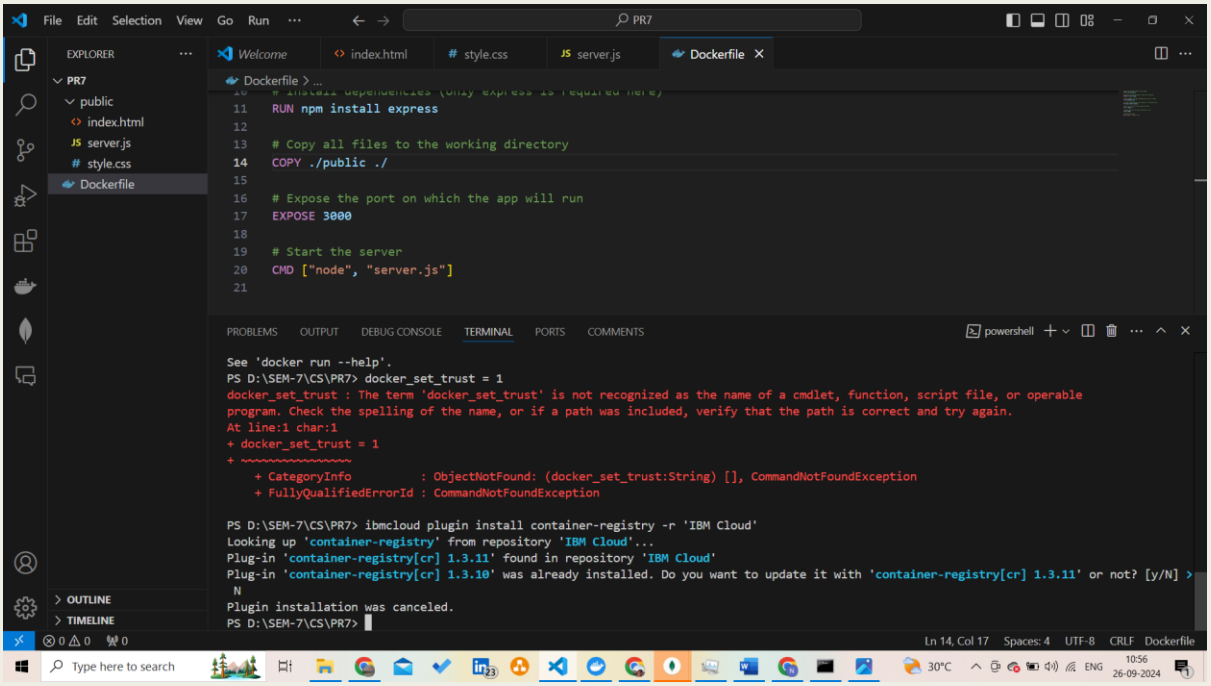
Now onwards we just performing the given step provided by Container registry




hello - Google Search
IBM Cloud Container Registry
Build a Docker Container Image
Experiment 7
ChatGPT
cloud.ibm.com/containers/registry/start
IBM Cloud
Search resources and products...
Catalog
Manage
2716063 - IBM India Pvt ltd, C/o S...
Container Registry
Overview
Quick start
Namespaces 1
Repositories 0
Images 0
Trash 0
Settings
Location
Global
Welcome!
Let's get started by installing the needed CLIs, setting up your first private registry namespace, and pushing your first image.
Install, Set Up, and Log In
1. Install the IBM Cloud CLI.
2. Install the Docker CLI.
3. Install the Container Registry plug-in.
ibmcloud plugin install container-registry -r 'IBM Cloud'
4. Log in to your IBM Cloud account.
ibmcloud login -a https://cloud.ibm.com
If you have a federated ID, use ibmcloud login --sso to log in to the IBM Cloud CLI.
5. Ensure that you're targeting the correct IBM Cloud Container Registry region.
ibmcloud cr region-set global
6. Choose a name for your first namespace, and create that namespace. Use this namespace for the rest of the Quick Start.
ibmcloud cr namespace-add <my_namespace>
Type here to search
30°C
ENG
10:55
26-09-2024


hello - Google Search
IBM Cloud Container Registry
Build a Docker Container Image
Experiment 7
ChatGPT
cloud.ibm.com/containers/registry/start
IBM Cloud
Search resources and products...
Catalog
Manage
2716063 - IBM India Pvt ltd, C/o S...
Container Registry
Overview
Quick start
Namespaces 6
Repositories 4
Images 4
Trash 0
Settings
Container registry quick start
Location
Dallas
Welcome!
Let's get started by installing the needed CLIs, setting up your first private registry namespace, and pushing your first image.
Install, Set Up, and Log In
1. Install the IBM Cloud CLI.
2. Install the Docker CLI.
3. Install the Container Registry plug-in.
ibmcloud plugin install container-registry -r 'IBM Cloud'
4. Log in to your IBM Cloud account.
ibmcloud login -a https://cloud.ibm.com
If you have a federated ID, use ibmcloud login --sso to log in to the IBM Cloud CLI.
5. Ensure that you're targeting the correct IBM Cloud Container Registry region.
ibmcloud cr region-set us-south
Type here to search
30°C
ENG
10:55
26-09-2024

- Install the Container Registry plug-in. [ibmcloud plugin install container-registry -r 'IBM Cloud']



Ensure that you're targeting the correct IBM Cloud Container Registry region also add the name space into cr

ibmcloud cr region-set global and ibmcloud cr namespace-add pr7_007(name of your)

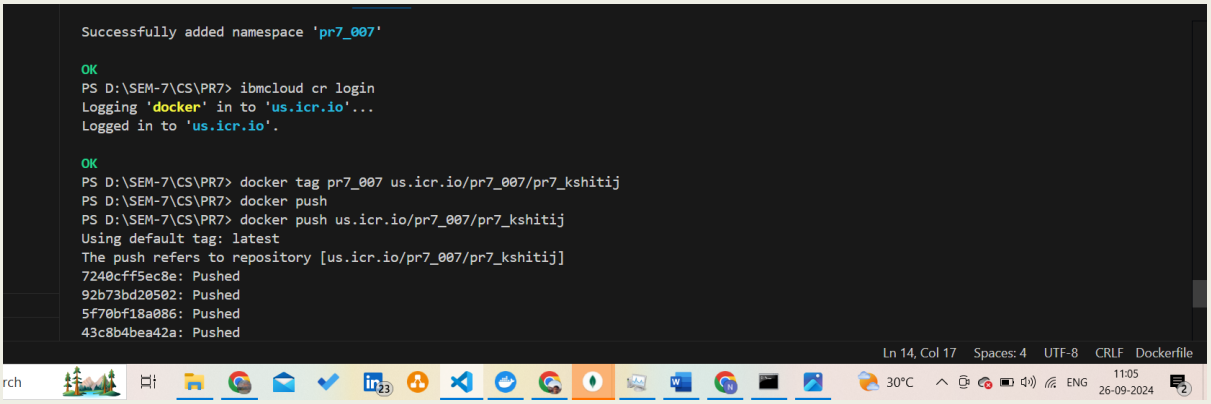
Log your local Docker daemon into the IBM Cloud Container Registry and tag your Choose a repository.

tag by which you can identify the image. Use the same repository and tag for the rest of this Quick Start.

Push the image. [**docker push icr.io/<my_namespace>/<my_repository>:<my_tag>**]

ibmcloud cr login

docker tag hello-world icr.io/<my_namespace>/<my_repository>:<my_tag>



Check Your Repository and you NameSpace

View by: Digest | Search | Create +

Repository@digest	Tags	Manifest type	Created	Size	Security status
pr7_007/pr7_kshitij@sha256:9def47d17e3b...	latest	Docker	1 hour ago	47 MB	--
dhruvinamespaceus/flask-docker@sha256:559513173c5e...	2.0	Docker	1 hour ago	385 MB	--
yagna_ns/ibmimageyagna@sha256:2d1953327c9f...	latest	Docker	1 hour ago	47 MB	--
bhavesh-namespace-us/bhavesh-18alpline1@sha256:2ae15b7f0678...	1	Docker	2 hours ago	47 MB	--
yashlani-nmspc/yslnewimage@sha256:25b731cde788...	2.0	Docker	2 hours ago	47 MB	--
thevivek/vivek@sha256:28b850b44a3a...	latest	Docker	21 days ago	32 MB	--

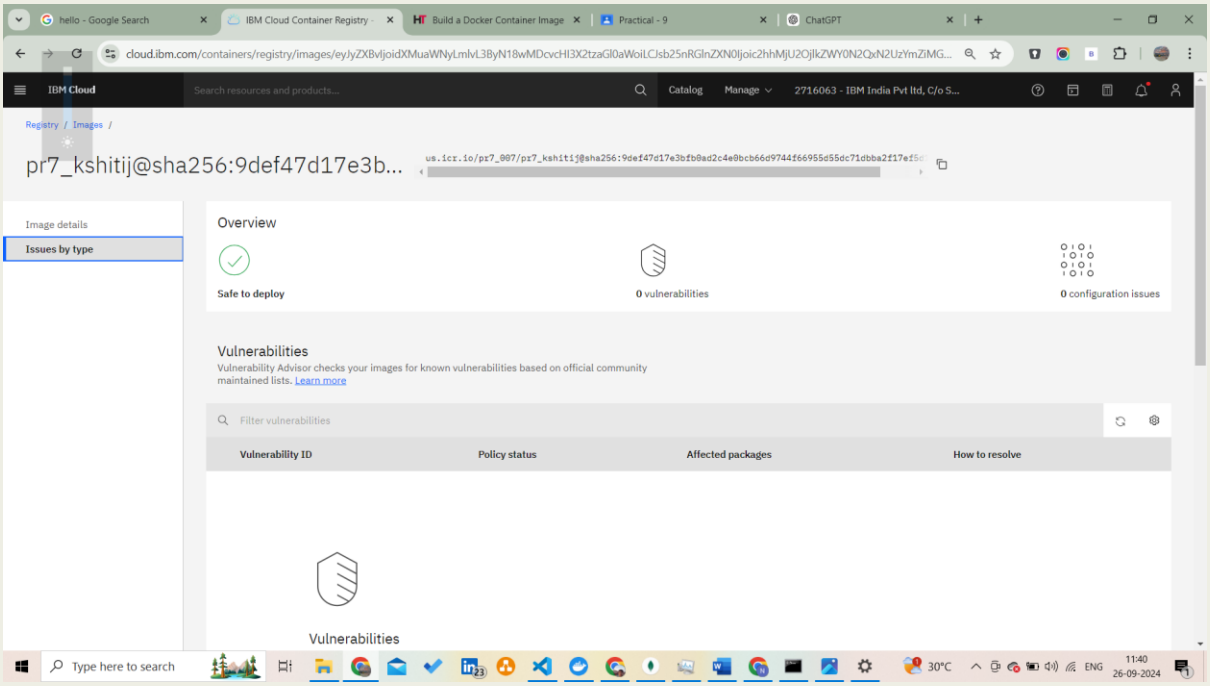
Search | Create +

Name	Image count	Namespace	Last updated
pr7_kshitij us.icr.io/pr7_007/pr7_kshitij	1	pr7_007	1 hour ago
flask-docker us.icr.io/dhruvinamespaceus/flask-docker	1	dhruvinamespaceus	1 hour ago
ibmimageyagna us.icr.io/yagna_ns/ibmimageyagna	1	yagna_ns	1 hour ago
bhavesh-18alpline1 us.icr.io/bhavesh-namespace-us/bhavesh-18alpline1	1	bhavesh-namespace-us	2 hours ago
yslnewimage us.icr.io/yashlani-nmspc/yslnewimage	1	yashlani-nmspc	2 hours ago
vivek us.icr.io/thevivek/vivek	1	thevivek	21 days ago

Resource group: Filter... | Search | Create +

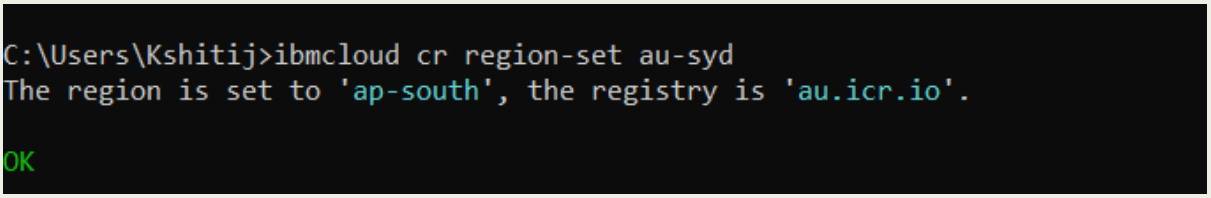
Name	Resource group	Repository count	Image count	Retention policy
pr7_007	default	1	1	Retain all images
thevivek	default	1	1	Retain all images
dhruvinamespaceus	default	1	1	Retain all images
yagna_ns	default	1	1	Retain all images
yashlani-nmspc	default	1	1	Retain all images
bhavesh-namespace-us	default	1	1	Retain all images
testobject	Ganpat-2021-Sem6-rg	0	0	Retain all images

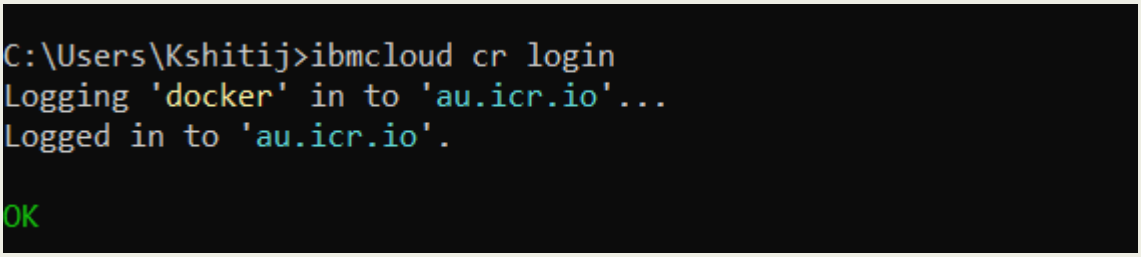
There are zero Vulnerability in my image.



To check vulnerabilities using CLI [**ibmcloud cr va us.icr.io/<nmspc-name>/<image-name>**]

Set The region using CLI [**ibmcloud cr region-set au-syd**] and login [**ibmcloud cr login**]





To perform the task I use the DK image and perform the task like issue finding

To check vulnerabilities using CLI [**ibmcloud cr va us.icr.io/<nmspc-name>/<image-name>**]

```
C:\Users\Kshitij>ibmcloud cr va au.icr.io/dhyey-deployment/dhyey-k-img@sha256:3980b3fc3b745cf8f082c70dbc596e03db4ec0f07fb9a8c232ac46595501a1c5
Checking security issues for 'au.icr.io/dhyey-deployment/dhyey-k-img@sha256:3980b3fc3b745cf8f082c70dbc596e03db4ec0f07fb9a8c232ac46595501a1c5'...

Image 'au.icr.io/dhyey-deployment/dhyey-k-img@sha256:3980b3fc3b745cf8f082c70dbc596e03db4ec0f07fb9a8c232ac46595501a1c5' was last scanned on Thu Sep 26 03:44:23 UTC 2024
The scan results show that 19 ISSUES were found for the image.

Vulnerable Packages Found
=========================

Vulnerability ID   Policy Status   Affected Packages                    How to Resolve
CVE-2023-3817      Active          libcrypto3 and libssl3               Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-6237      Active          libcrypto3 and libssl3               Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-42366     Active          ssl_client, busybox-binsh and busybox   Upgrade 3 packages. Re-run command with --extended to view.
CVE-2024-5535      Active          libcrypto3 and libssl3               Upgrade 2 packages. Re-run command with --extended to view.
CVE-2024-4603      Active          libcrypto3 and libssl3               Upgrade 2 packages. Re-run command with --extended to view.
CVE-2024-6119      Active          libcrypto3 and libssl3               Upgrade 2 packages. Re-run command with --extended to view.
CVE-2024-4741      Active          libcrypto3 and libssl3               Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-3446      Active          libcrypto3 and libssl3               Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-42364     Active          ssl_client, busybox-binsh and busybox   Upgrade 3 packages. Re-run command with --extended to view.
CVE-2024-0727      Active          libcrypto3 and libssl3               Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-1255      Active          libssl3 and libcrypto3               Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-42365     Active          ssl_client, busybox-binsh and busybox   Upgrade 3 packages. Re-run command with --extended to view.
CVE-2024-2511      Active          libcrypto3 and libssl3               Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-6129      Active          libcrypto3 and libssl3               Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-5363      Active          libssl3 and libcrypto3               Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-2650      Active          libcrypto3 and libssl3               Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-2975      Active          libcrypto3 and libssl3               Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-5678      Active          libcrypto3 and libssl3               Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-42363     Active          ssl_client, busybox-binsh and busybox   Upgrade 3 packages. Re-run command with --extended to view.

To see the details about the fixes for these packages, run the command again with the '--extended' flag.

OK
```

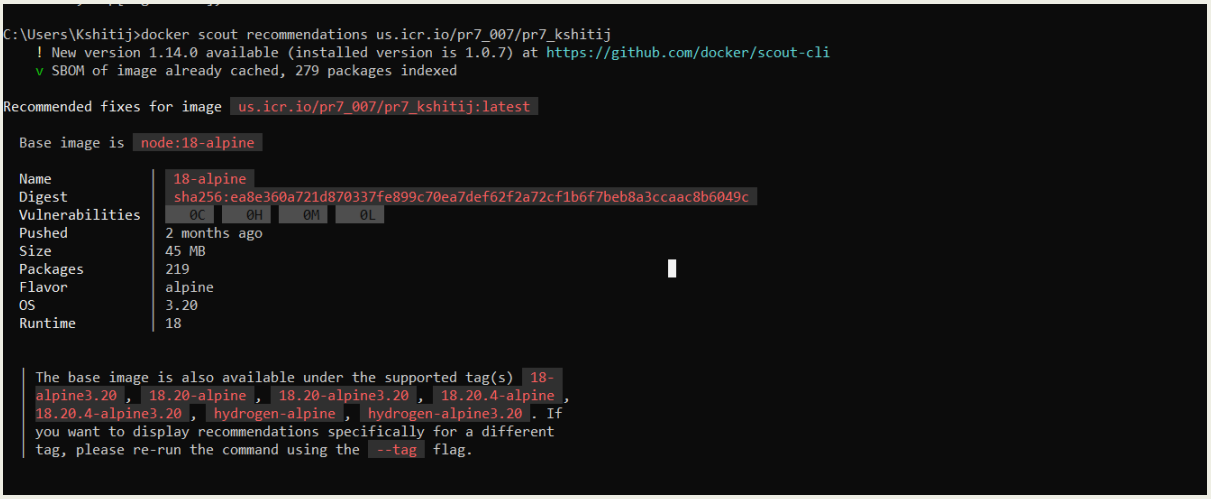
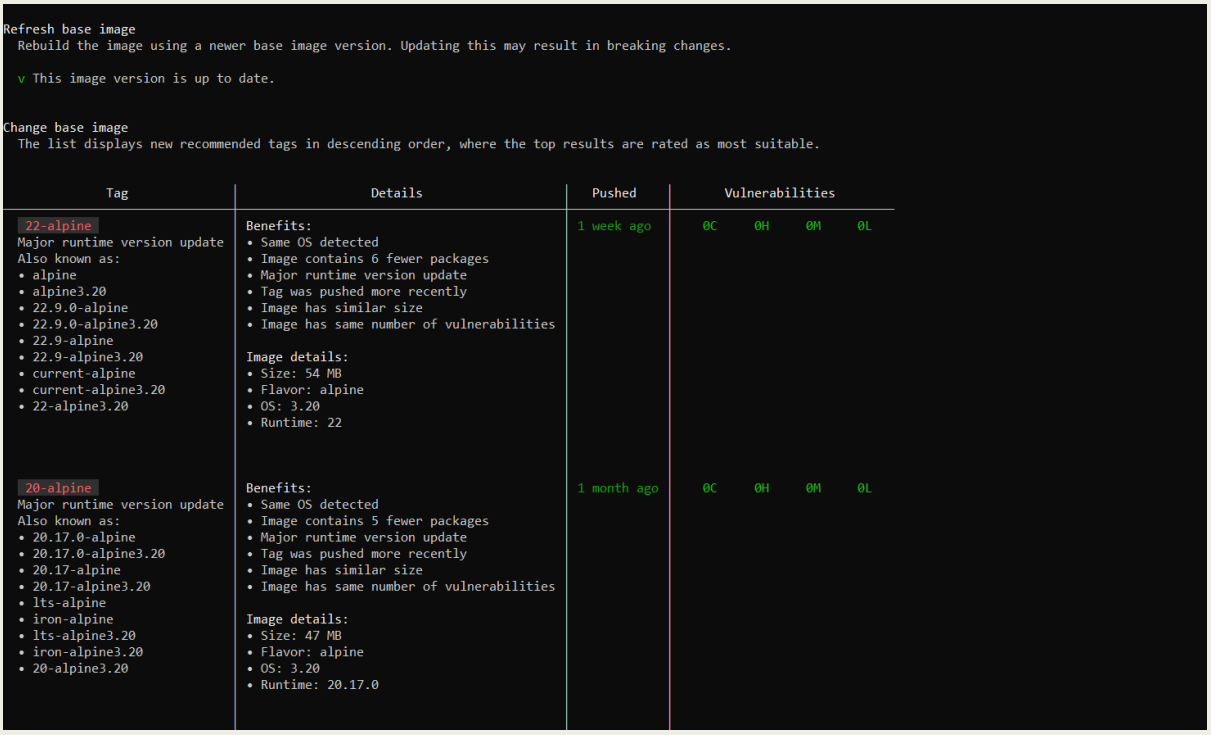
To see the vulnerability in detail use - -**extended**

```
C:\Users\Kshitij>ibmcloud cr va au.icr.io/dhyey-deployment/dhyey-k-img@sha256:3980b3fc3b745cf8f082c70dbc596e03db4ec0f07fb9a8c232ac46595501a1c5 --extended
Checking security issues for 'au.icr.io/dhyey-deployment/dhyey-k-img@sha256:3980b3fc3b745cf8f082c70dbc596e03db4ec0f07fb9a8c232ac46595501a1c5'...

Image 'au.icr.io/dhyey-deployment/dhyey-k-img@sha256:3980b3fc3b745cf8f082c70dbc596e03db4ec0f07fb9a8c232ac46595501a1c5' was last scanned on Thu Sep 26 03:44:23 UTC 2024
The scan results show that 19 ISSUES were found for the image.

Vulnerable Packages Found
=========================

CVE-2023-3817

   Policy Status
   Active

   Summary


   Vendor Security Notice IDs   Official Notice
   ALPINE-CVE-2023-3817         https://www.cve.org/CVERecord?id=CVE-2023-3817

   Affected Packages   Policy Status   How to Resolve                  Security Notice
   libcrypto3          Active          Upgrade libcrypto3 to >= 3.0.10-r0   ALPINE-CVE-2023-3817
   libssl3             Active          Upgrade libssl3 to >= 3.0.10-r0      ALPINE-CVE-2023-3817


CVE-2023-6237

   Policy Status
   Active

   Summary


   Vendor Security Notice IDs   Official Notice
   ALPINE-CVE-2023-6237         https://www.cve.org/CVERecord?id=CVE-2023-6237

   Affected Packages   Policy Status   How to Resolve                  Security Notice
   libcrypto3          Active          Upgrade libcrypto3 to >= 3.0.12-r3   ALPINE-CVE-2023-6237
   libssl3             Active          Upgrade libssl3 to >= 3.0.12-r3      ALPINE-CVE-2023-6237


CVE-2023-42366

   Policy Status
   Active

   Summary
```

```
C:\Users\Kshitij>docker images
REPOSITORY                                                TAG                                                                 IMAGE ID       CREATED             SIZE
pr7_007                                                   latest                                                              07c3ad3d1e05   33 minutes ago      135MB
us.icr.io/pr7_007/pr7_kshitij                             latest                                                              07c3ad3d1e05   33 minutes ago      135MB
car_rental                                                latest                                                              1e90e03384e7   About an hour ago   1.13GB
au.icr.io/kshitijname/new_img_007                         1.0                                                                 83d79decd86f   3 weeks ago         95.9MB
img1_007                                                  1.0                                                                 83d79decd86f   3 weeks ago         95.9MB
postgres                                                  latest                                                              d60dc4bd84c0   7 months ago        431MB
car                                                       latest                                                              3451ec0204d6   10 months ago       1.13GB
<none>                                                    <none>                                                              08ff98d671f2   10 months ago       1.13GB
kshitijgupta505/pr_14_test                                latest                                                              8c243906c869   11 months ago       122MB
kshitijgupta505/kshitijgupta505                           <none>                                                              8d2702bdff0a   11 months ago       64.5MB
hubproxy.docker.internal:5555/docker/desktop-kubernetes   kubernetes-v1.27.2-cni-v1.2.0-critools-v1.27.0-cri-dockerd-v0.3.2-1-debian   c763812a4530   15 months ago       418MB
registry.k8s.io/kube-apiserver                            v1.27.2                                                             c5b13e4f7806   16 months ago       121MB
registry.k8s.io/kube-controller-manager                   v1.27.2                                                             ac2b7465ebba   16 months ago       112MB
registry.k8s.io/kube-scheduler                            v1.27.2                                                             89e70da428d2   16 months ago       58.4MB
registry.k8s.io/kube-proxy                                v1.27.2                                                             b8aa50768fd6   16 months ago       71.1MB
docker/desktop-vpnkit-controller                          dc331cb22850be0cdd97c84a9cfecaf44a1afb6e                            556098075b3d   16 months ago       36.2MB
registry.k8s.io/coredns/coredns                           v1.10.1                                                             ead0a4a53df8   19 months ago       53.6MB
registry.k8s.io/etcd                                      3.5.7-0                                                             86b6af7dd652   20 months ago       296MB
registry.k8s.io/pause                                     3.9                                                                 e6f181688397   23 months ago       744kB
docker/desktop-storage-provisioner                        v2.0                                                                99f89471f470   3 years ago         41.9MB
```

To check vulnerability using docker scout

Command [**docker scount recommendations us.icr.io/<nmspc-name>/<image-name>**]

You can also run other command like

docker scount recommendations local://<localimagename> [local view]