Name: Tushar Panchal

En.No: 21162101014

Sub: CS(Cloud Security)

Branch: CBA

Batch:71

---------------------------PRACTICAL 07---------------------------

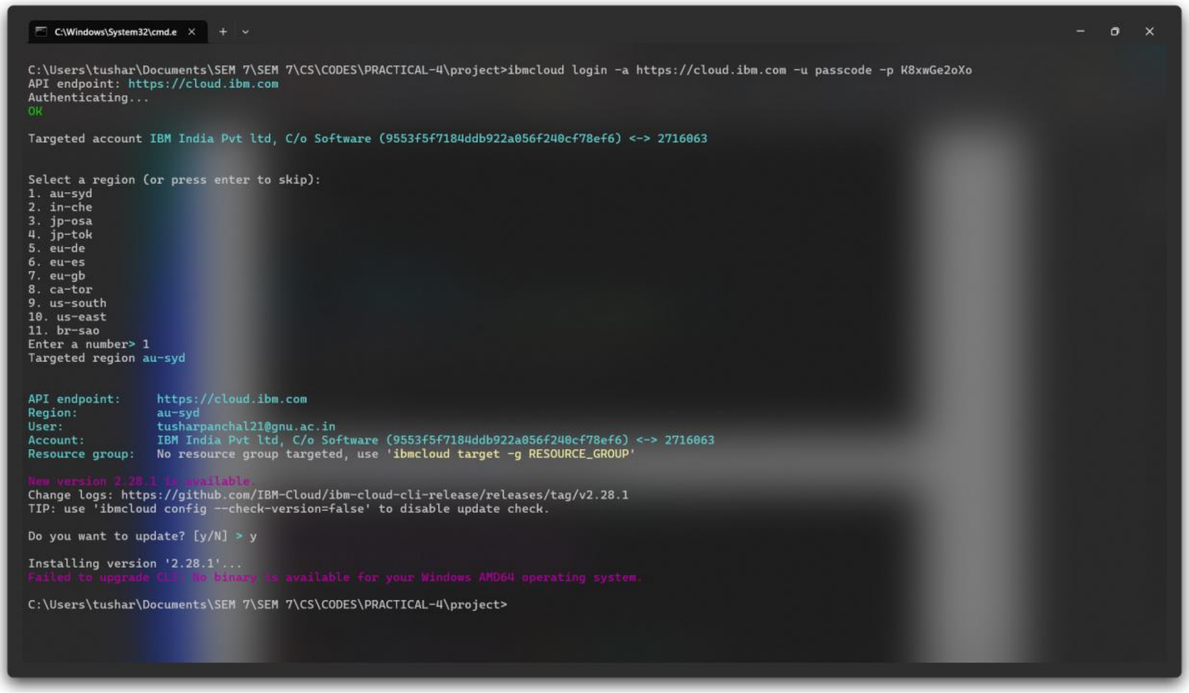
Securing a Docker Image Before Deployment to Production

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.

Steps:

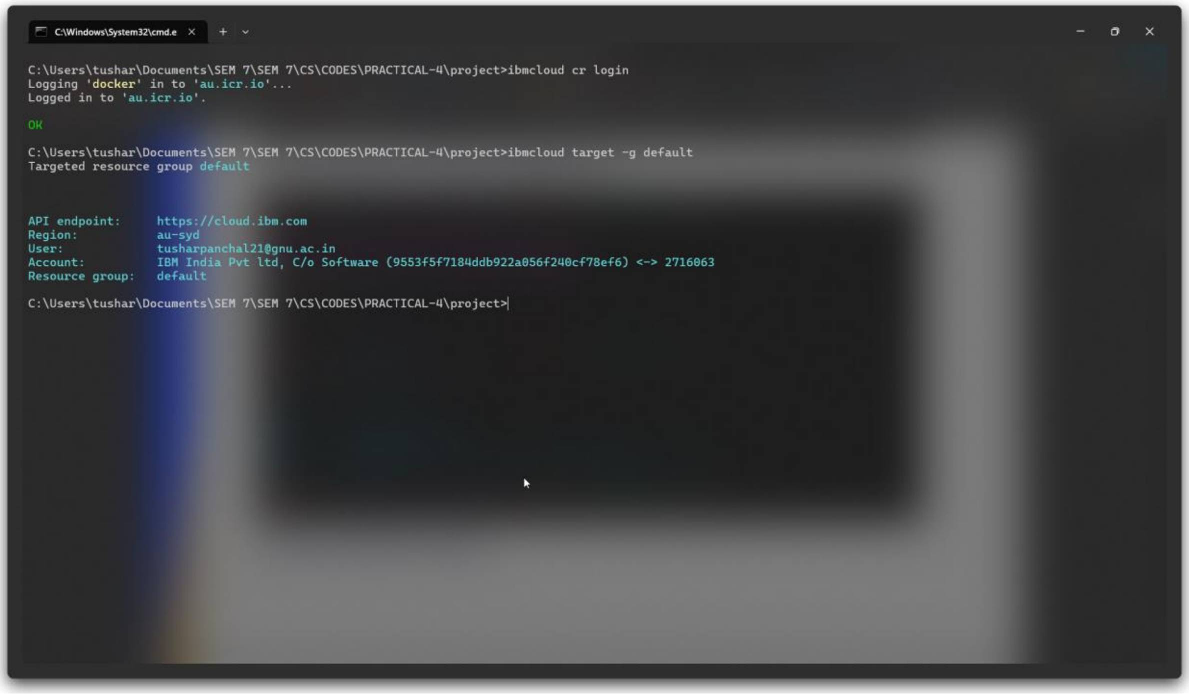
- **Building the Docker Image**
- **Tag the image for container registry**
- **Login to IBM Cloud Container Registry**
- **Push Image to Container Registry**
- **Check Vulnerability Scan Results**
- **Address Vulnerabilities**
- **Rebuild and Re-scan the Image**
- **Deploy the Secure Image**

First we login to IBM cloud



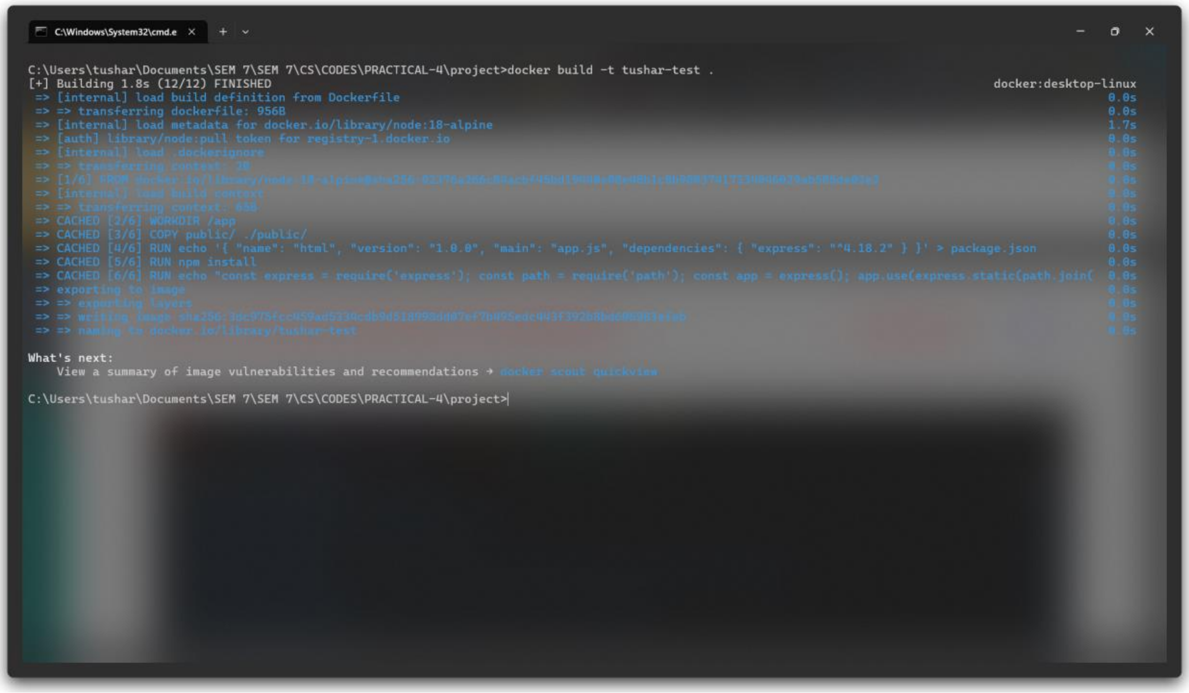
```
C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>ibmcloud login -a https://cloud.ibm.com -u passcode -p K8xwGe2oXo
API endpoint: https://cloud.ibm.com
Authenticating...
OK

Targeted account IBM India Pvt ltd, C/o Software (9553f5f7184ddb922a056f240cf78ef6) <-> 2716063


Select a region (or press enter to skip):
1. au-syd
2. in-che
3. jp-osa
4. jp-tok
5. eu-de
6. eu-es
7. eu-gb
8. ca-tor
9. us-south
10. us-east
11. br-sao
Enter a number> 1
Targeted region au-syd


API endpoint:     https://cloud.ibm.com
Region:           au-syd
User:             tusharpanchal21@gnu.ac.in
Account:          IBM India Pvt ltd, C/o Software (9553f5f7184ddb922a056f240cf78ef6) <-> 2716063
Resource group:   No resource group targeted, use 'ibmcloud target -g RESOURCE_GROUP'

New version 2.28.1 is available.
Change logs: https://github.com/IBM-Cloud/ibm-cloud-cli-release/releases/tag/v2.28.1
TIP: use 'ibmcloud config --check-version=false' to disable update check.

Do you want to update? [y/N] > y

Installing version '2.28.1'...
Failed to upgrade CLI: No binary is available for your Windows AMD64 operating system.

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>
```

And we'll login to container registry too



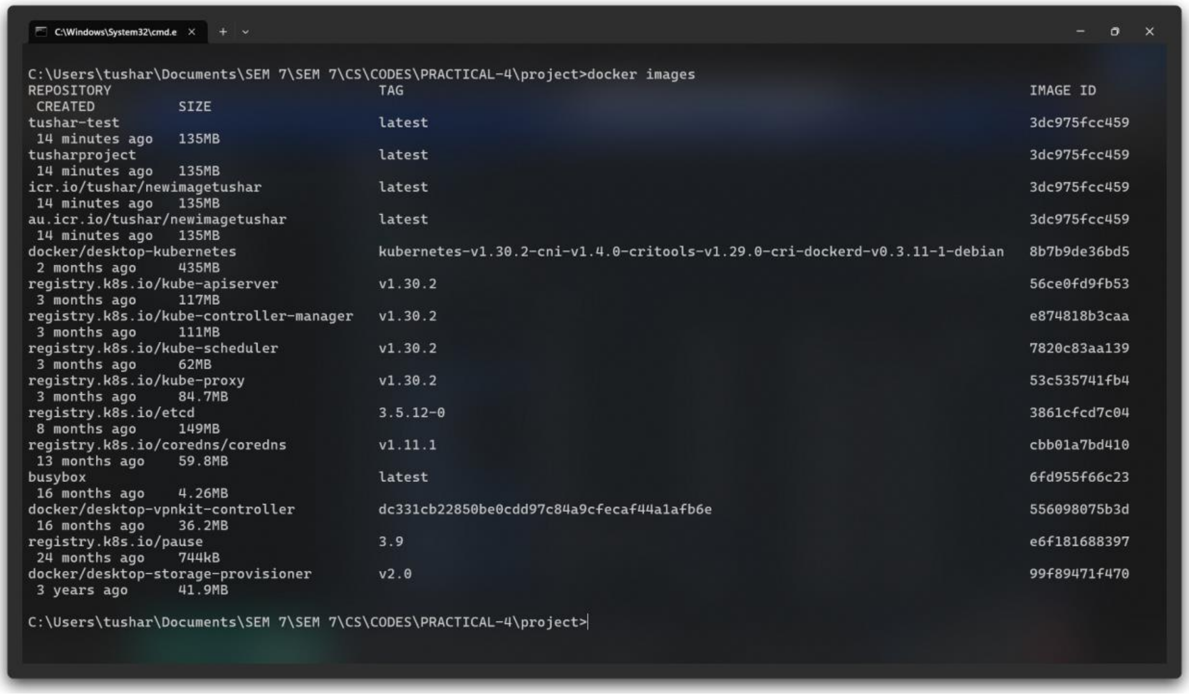
```
C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>ibmcloud cr login
Logging 'docker' in to 'au.icr.io'...
Logged in to 'au.icr.io'.

OK

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>ibmcloud target -g default
Targeted resource group default



API endpoint:     https://cloud.ibm.com
Region:           au-syd
User:             tusharpanchal21@gnu.ac.in
Account:          IBM India Pvt ltd, C/o Software (9553f5f7184ddb922a056f240cf78ef6) <-> 2716063
Resource group:   default

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>
```

And than build the image



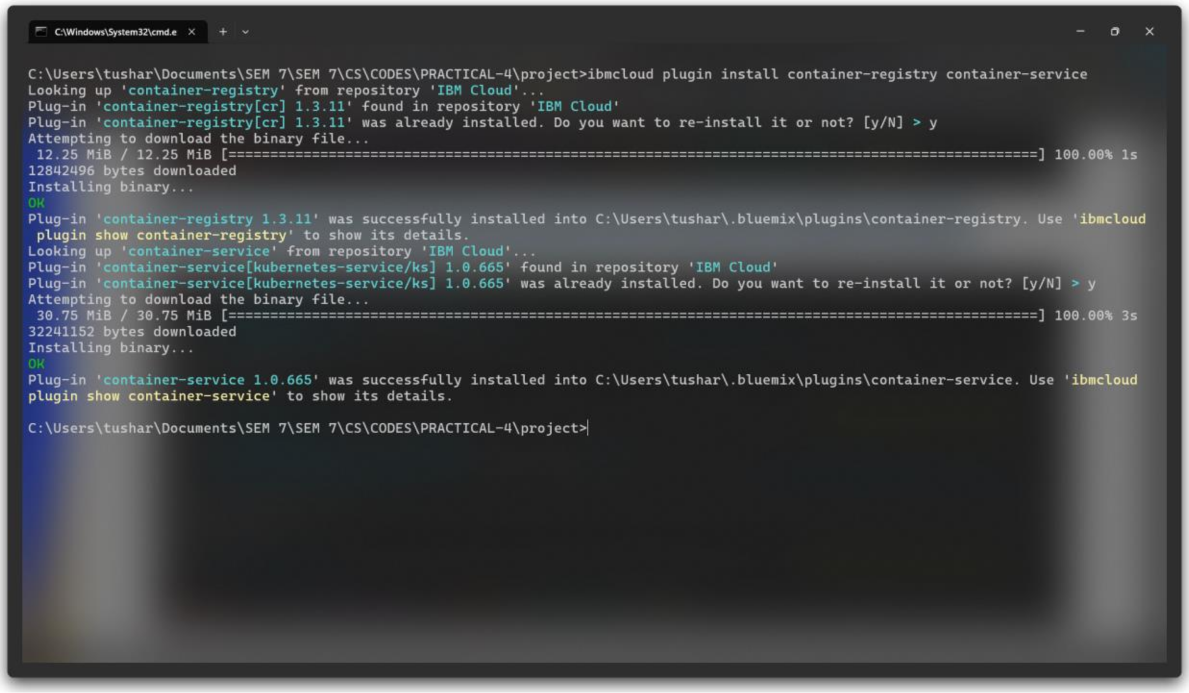
```
C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>docker build -t tushar-test .
[+] Building 1.8s (12/12) FINISHED                                                              docker:desktop-linux
 => [internal] load build definition from Dockerfile                                                           0.0s
 => => transferring dockerfile: 956B                                                                           0.0s
 => [internal] load metadata for docker.io/library/node:18-alpine                                              1.7s
 => [auth] library/node:pull token for registry-1.docker.io                                                    0.0s
 => [internal] load .dockerignore                                                                              0.0s
 => => transferring context: 2B                                                                                0.0s
 => [1/6] FROM docker.io/library/node:18-alpine@sha256:[illegible]                                             0.0s
 => [internal] load build context                                                                              0.0s
 => => transferring context: 60B                                                                               0.0s
 => CACHED [2/6] WORKDIR /app                                                                                  0.0s
 => CACHED [3/6] COPY public/ ./public/                                                                        0.0s
 => CACHED [4/6] RUN echo '{ "name": "html", "version": "1.0.0", "main": "app.js", "dependencies": { "express": "^4.18.2" } }' > package.json   0.0s
 => CACHED [5/6] RUN npm install                                                                               0.0s
 => CACHED [6/6] RUN echo "const express = require('express'); const path = require('path'); const app = express(); app.use(express.static(path.join(  0.0s
 => exporting to image                                                                                         0.0s
 => => exporting layers                                                                                        0.0s
 => => writing image sha256:3dc975fcc459[illegible]                                                            0.0s
 => => naming to docker.io/library/tushar-test                                                                 0.0s

What's next:
    View a summary of image vulnerabilities and recommendations → docker scout quickview

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>
```

Here we can see our new image is created



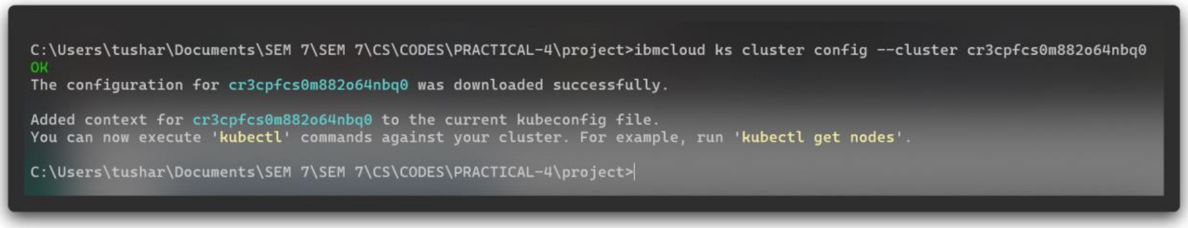
```
C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>docker images
REPOSITORY                                TAG                                                                        IMAGE ID
 CREATED          SIZE
tushar-test                               latest                                                                     3dc975fcc459
 14 minutes ago   135MB
tusharproject                             latest                                                                     3dc975fcc459
 14 minutes ago   135MB
icr.io/tushar/newimagetushar              latest                                                                     3dc975fcc459
 14 minutes ago   135MB
au.icr.io/tushar/newimagetushar           latest                                                                     3dc975fcc459
 14 minutes ago   135MB
docker/desktop-kubernetes                 kubernetes-v1.30.2-cni-v1.4.0-critools-v1.29.0-cri-dockerd-v0.3.11-1-debian   8b7b9de36bd5
 2 months ago     435MB
registry.k8s.io/kube-apiserver            v1.30.2                                                                    56ce0fd9fb53
 3 months ago     117MB
registry.k8s.io/kube-controller-manager   v1.30.2                                                                    e874818b3caa
 3 months ago     111MB
registry.k8s.io/kube-scheduler            v1.30.2                                                                    7820c83aa139
 3 months ago     62MB
registry.k8s.io/kube-proxy                v1.30.2                                                                    53c535741fb4
 3 months ago     84.7MB
registry.k8s.io/etcd                      3.5.12-0                                                                   3861cfcd7c04
 8 months ago     149MB
registry.k8s.io/coredns/coredns           v1.11.1                                                                    cbb01a7bd410
 13 months ago    59.8MB
busybox                                   latest                                                                     6fd955f66c23
 16 months ago    4.26MB
docker/desktop-vpnkit-controller          dc331cb22850be0cdd97c84a9cfecaf44a1afb6e                                   556098075b3d
 16 months ago    36.2MB
registry.k8s.io/pause                     3.9                                                                        e6f181688397
 24 months ago    744kB
docker/desktop-storage-provisioner        v2.0                                                                       99f89471f470
 3 years ago      41.9MB

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>
```

We need to install container-service and container-registry plugins



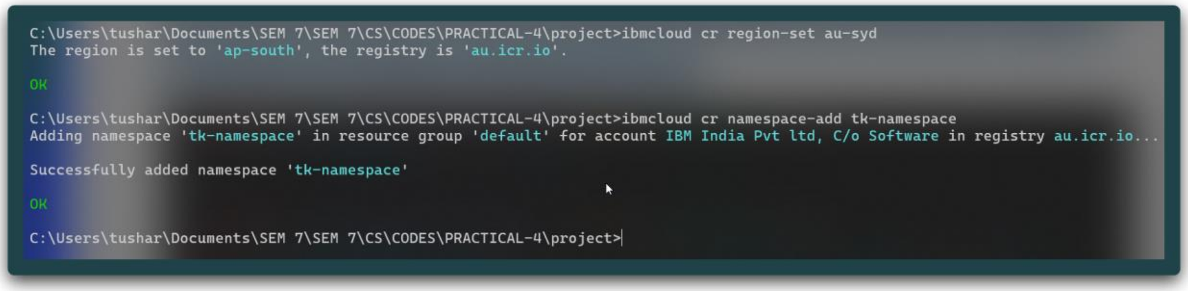
```
C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>ibmcloud plugin install container-registry container-service
Looking up 'container-registry' from repository 'IBM Cloud'...
Plug-in 'container-registry[cr] 1.3.11' found in repository 'IBM Cloud'
Plug-in 'container-registry[cr] 1.3.11' was already installed. Do you want to re-install it or not? [y/N] > y
Attempting to download the binary file...
 12.25 MiB / 12.25 MiB [=========================================================================================] 100.00% 1s
12842496 bytes downloaded
Installing binary...
OK
Plug-in 'container-registry 1.3.11' was successfully installed into C:\Users\tushar\.bluemix\plugins\container-registry. Use 'ibmcloud
 plugin show container-registry' to show its details.
Looking up 'container-service' from repository 'IBM Cloud'...
Plug-in 'container-service[kubernetes-service/ks] 1.0.665' found in repository 'IBM Cloud'
Plug-in 'container-service[kubernetes-service/ks] 1.0.665' was already installed. Do you want to re-install it or not? [y/N] > y
Attempting to download the binary file...
 30.75 MiB / 30.75 MiB [=========================================================================================] 100.00% 3s
32241152 bytes downloaded
Installing binary...
OK
Plug-in 'container-service 1.0.665' was successfully installed into C:\Users\tushar\.bluemix\plugins\container-service. Use 'ibmcloud
plugin show container-service' to show its details.

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>
```

Now login to your cluster



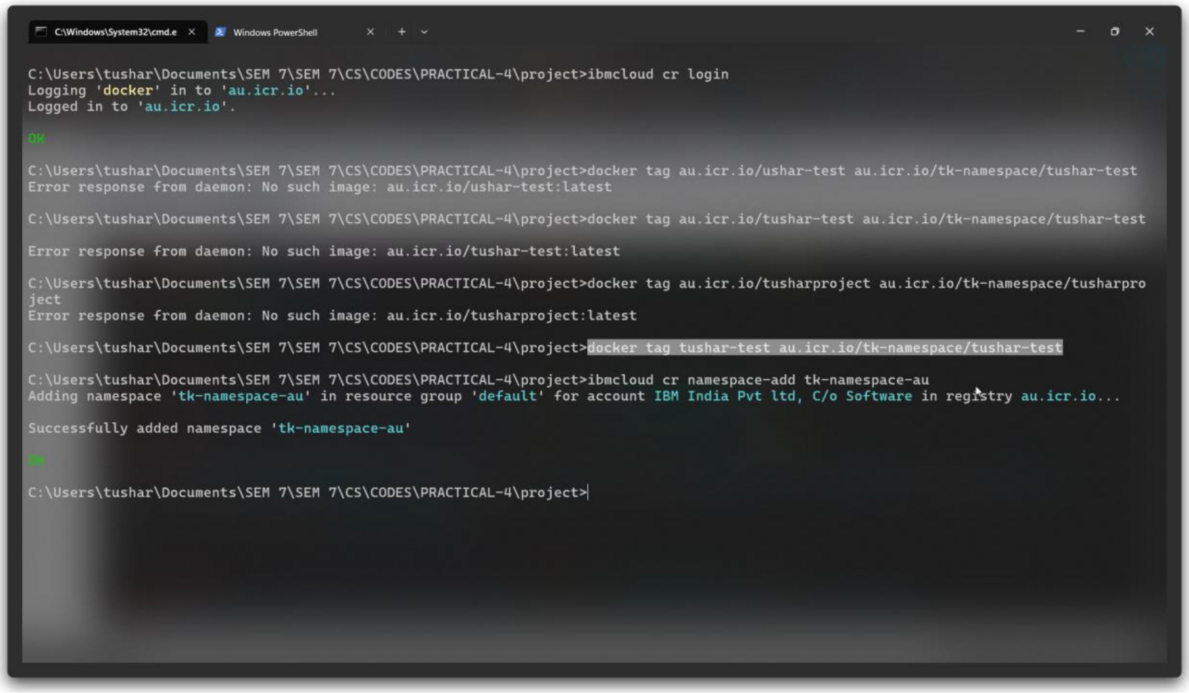
```
C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>ibmcloud ks cluster config --cluster cr3cpfcs0m882o64nbq0
OK
The configuration for cr3cpfcs0m882o64nbq0 was downloaded successfully.

Added context for cr3cpfcs0m882o64nbq0 to the current kubeconfig file.
You can now execute 'kubectl' commands against your cluster. For example, run 'kubectl get nodes'.

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>
```

Now add namespace into your registry and make sure that your region is au-sydney and registry should be au.icr.io



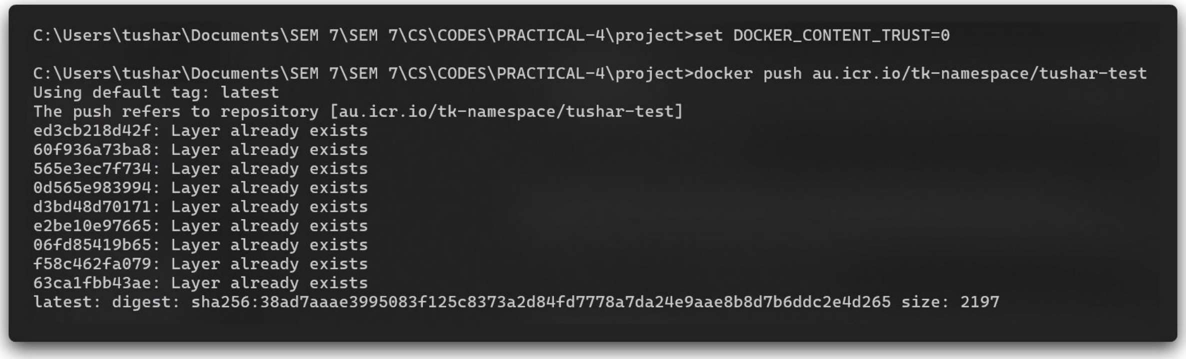
```
C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>ibmcloud cr region-set au-syd
The region is set to 'ap-south', the registry is 'au.icr.io'.

OK

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>ibmcloud cr namespace-add tk-namespace
Adding namespace 'tk-namespace' in resource group 'default' for account IBM India Pvt ltd, C/o Software in registry au.icr.io...

Successfully added namespace 'tk-namespace'

OK

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>
```

So i just exceed the quota for uploading image so i'm creating namespace in new region



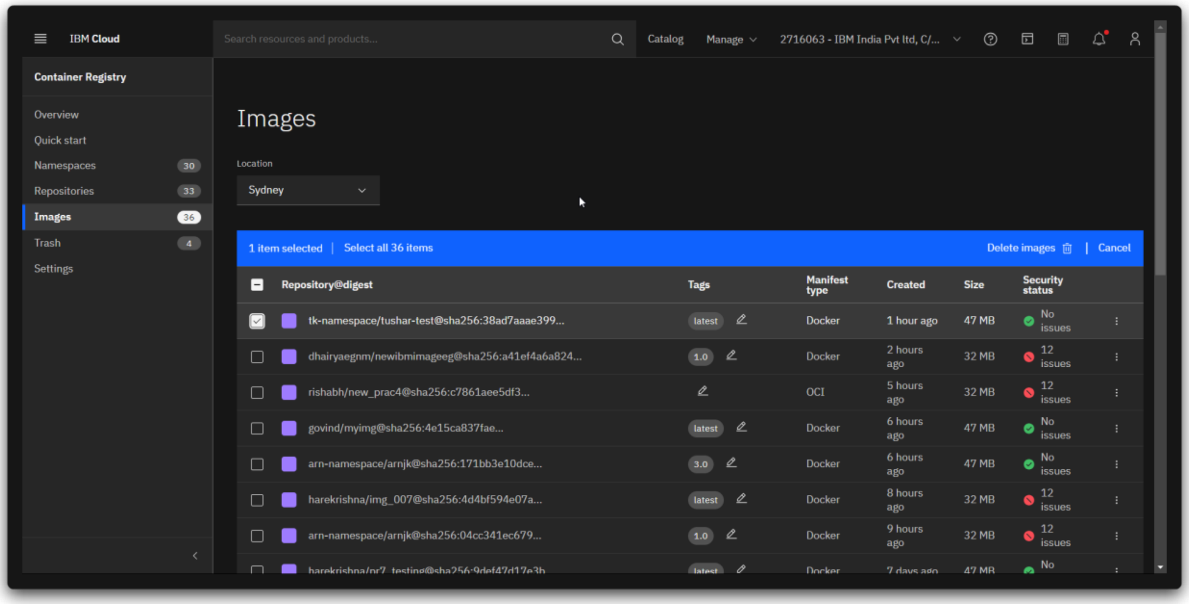
```
C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>ibmcloud cr login
Logging 'docker' in to 'au.icr.io'...
Logged in to 'au.icr.io'.

OK

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>docker tag au.icr.io/ushar-test au.icr.io/tk-namespace/tushar-test
Error response from daemon: No such image: au.icr.io/ushar-test:latest

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>docker tag au.icr.io/tushar-test au.icr.io/tk-namespace/tushar-test

Error response from daemon: No such image: au.icr.io/tushar-test:latest

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>docker tag au.icr.io/tusharproject au.icr.io/tk-namespace/tusharpro
ject
Error response from daemon: No such image: au.icr.io/tusharproject:latest

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>docker tag tushar-test au.icr.io/tk-namespace/tushar-test

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>ibmcloud cr namespace-add tk-namespace-au
Adding namespace 'tk-namespace-au' in resource group 'default' for account IBM India Pvt ltd, C/o Software in registry au.icr.io...

Successfully added namespace 'tk-namespace-au'

OK

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>
```

And than push image:



```
C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>set DOCKER_CONTENT_TRUST=0

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>docker push au.icr.io/tk-namespace/tushar-test
Using default tag: latest
The push refers to repository [au.icr.io/tk-namespace/tushar-test]
ed3cb218d42f: Layer already exists
60f936a73ba8: Layer already exists
565e3ec7f734: Layer already exists
0d565e983994: Layer already exists
d3bd48d70171: Layer already exists
e2be10e97665: Layer already exists
06fd85419b65: Layer already exists
f58c462fa079: Layer already exists
63ca1fbb43ae: Layer already exists
latest: digest: sha256:38ad7aaae3995083f125c8373a2d84fd7778a7da24e9aae8b8d7b6ddc2e4d265 size: 2197
```

Now we can see on container registry that our image is there



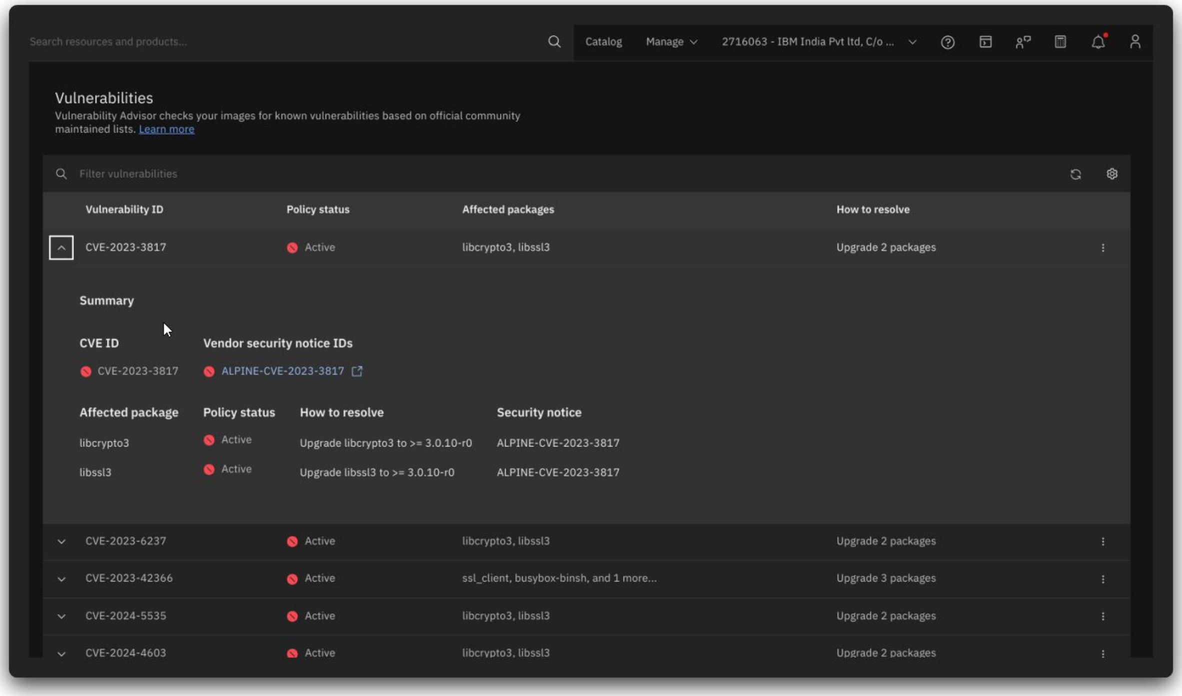
Images

Location: Sydney

1 item selected | Select all 36 items | Delete images | Cancel

▣	Repository@digest	Tags	Manifest type	Created	Size	Security status
☑	tk-namespace/tushar-test@sha256:38ad7aaae399...	latest	Docker	1 hour ago	47 MB	No issues
□	dhairyaegnm/newibmimageeg@sha256:a41ef4a6a824...	1.0	Docker	2 hours ago	32 MB	12 issues
□	rishabh/new_prac4@sha256:c7861aee5df3...		OCI	5 hours ago	32 MB	12 issues
□	govind/myimg@sha256:4e15ca837fae...	latest	Docker	6 hours ago	47 MB	No issues
□	arn-namespace/arnjk@sha256:171bb3e10dce...	3.0	Docker	6 hours ago	47 MB	No issues
□	harekrishna/img_007@sha256:4d4bf594e07a...	latest	Docker	8 hours ago	32 MB	12 issues
□	arn-namespace/arnjk@sha256:04cc341ec679...	1.0	Docker	9 hours ago	32 MB	12 issues
□	harekrishna/pr7_testing@sha256:9def47d17e3b	latest	Docker	7 days ago	47 MB	No

And also it has many issues So what we do to remove that issue is we check for the issue in detailed


Search resources and products...
Catalog
Manage
2716063 - IBM India Pvt ltd, C/o ...
Filter vulnerabilities

Vulnerabilities

Vulnerability Advisor checks your images for known vulnerabilities based on official community maintained lists. Learn more

Vulnerability ID	Policy status	Affected packages	How to resolve
CVE-2023-3817	Active	libcrypto3, libssl3	Upgrade 2 packages

Summary

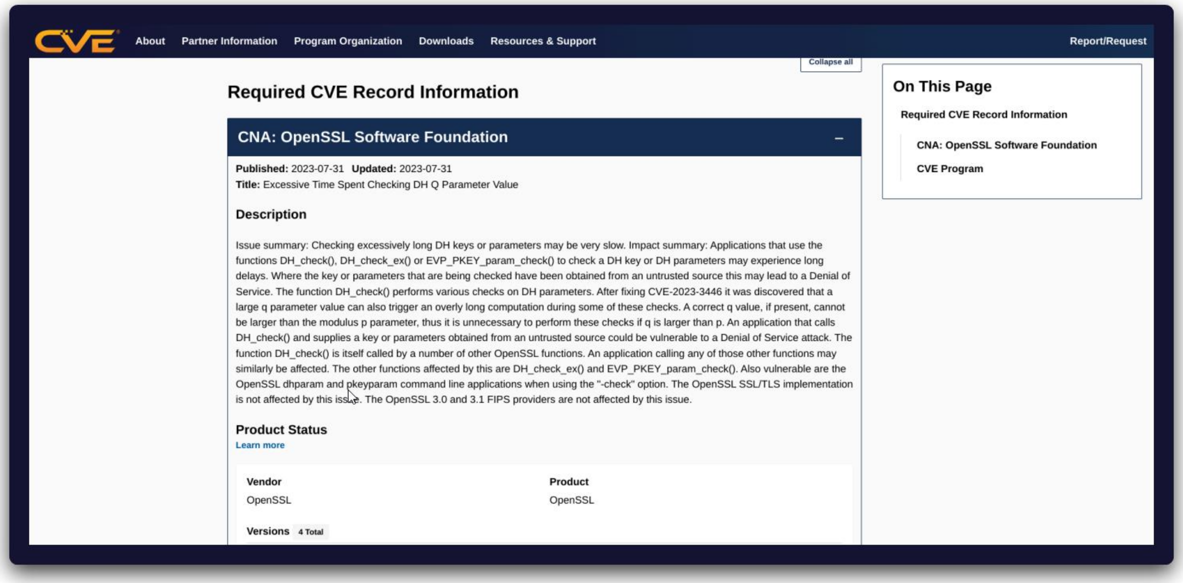
CVE ID: CVE-2023-3817

Vendor security notice IDs: ALPINE-CVE-2023-3817

Affected package	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

Vulnerability ID	Policy status	Affected packages	How to resolve
CVE-2023-6237	Active	libcrypto3, libssl3	Upgrade 2 packages
CVE-2023-42366	Active	ssl_client, busybox-binsh, and 1 more...	Upgrade 3 packages
CVE-2024-5535	Active	libcrypto3, libssl3	Upgrade 2 packages
CVE-2024-4603	Active	libcrypto3, libssl3	Upgrade 2 packages

Than check for it that what is error we'll search for it see what kind of issues we're getting



Required CVE Record Information

CNA: OpenSSL Software Foundation

Published: 2023-07-31 **Updated:** 2023-07-31
Title: Excessive Time Spent Checking DH Q Parameter Value

Description

Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. After fixing CVE-2023-3446 it was discovered that a large q parameter value can also trigger an overly long computation during some of these checks. A correct q value, if present, cannot be larger than the modulus p parameter, thus it is unnecessary to perform these checks if q is larger than p. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the "-check" option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

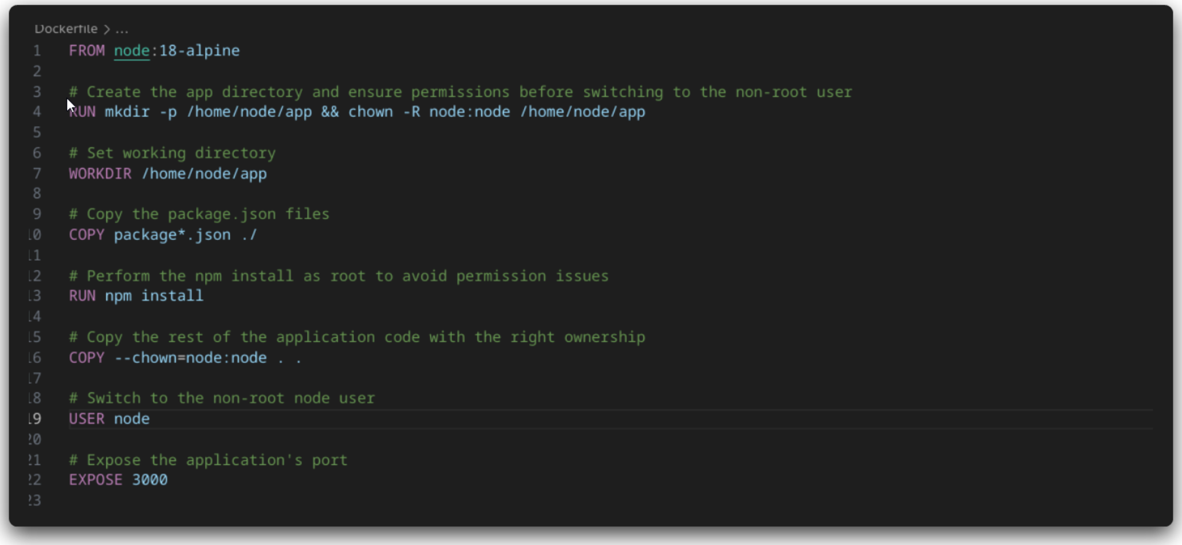
Product Status
Learn more

Vendor	Product
OpenSSL	OpenSSL

Versions 4 Total

On This Page
- Required CVE Record Information
  - CNA: OpenSSL Software Foundation
  - CVE Program

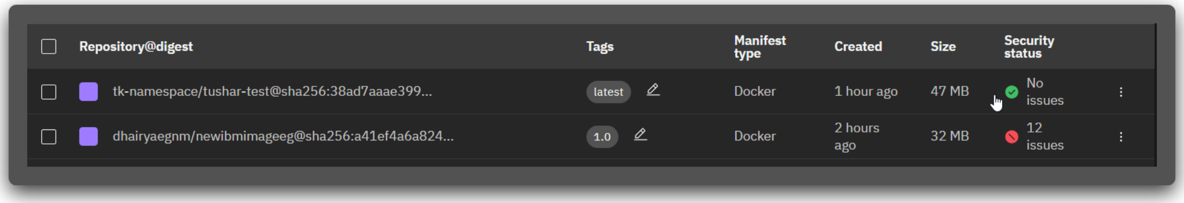
So we learn that our alpine version 12 is giving the issue so we'll update it to alpine18 . Now again we have to build the docker file



```
Dockerfile > ...
FROM node:18-alpine

# Create the app directory and ensure permissions before switching to the non-root user
RUN mkdir -p /home/node/app && chown -R node:node /home/node/app

# Set working directory
WORKDIR /home/node/app

# Copy the package.json files
COPY package*.json ./

# Perform the npm install as root to avoid permission issues
RUN npm install

# Copy the rest of the application code with the right ownership
COPY --chown=node:node . .

# Switch to the non-root node user
USER node

# Expose the application's port
EXPOSE 3000
```

Now we again build image and tag image and pus that image

And now if we see on registry we can see there is no issues now

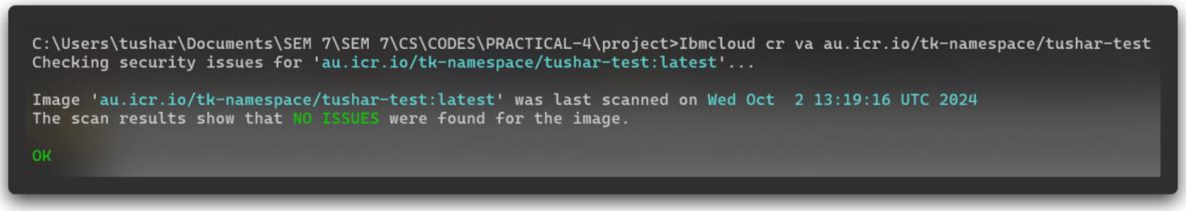


□	Repository@digest	Tags	Manifest type	Created	Size	Security status
□	tk-namespace/tushar-test@sha256:38ad7aaae399...	latest	Docker	1 hour ago	47 MB	✓ No issues
□	dhairyaegnm/newibmimageeg@sha256:a41ef4a6a824...	1.0	Docker	2 hours ago	32 MB	● 12 issues

We can find issues through vulnerability adviser

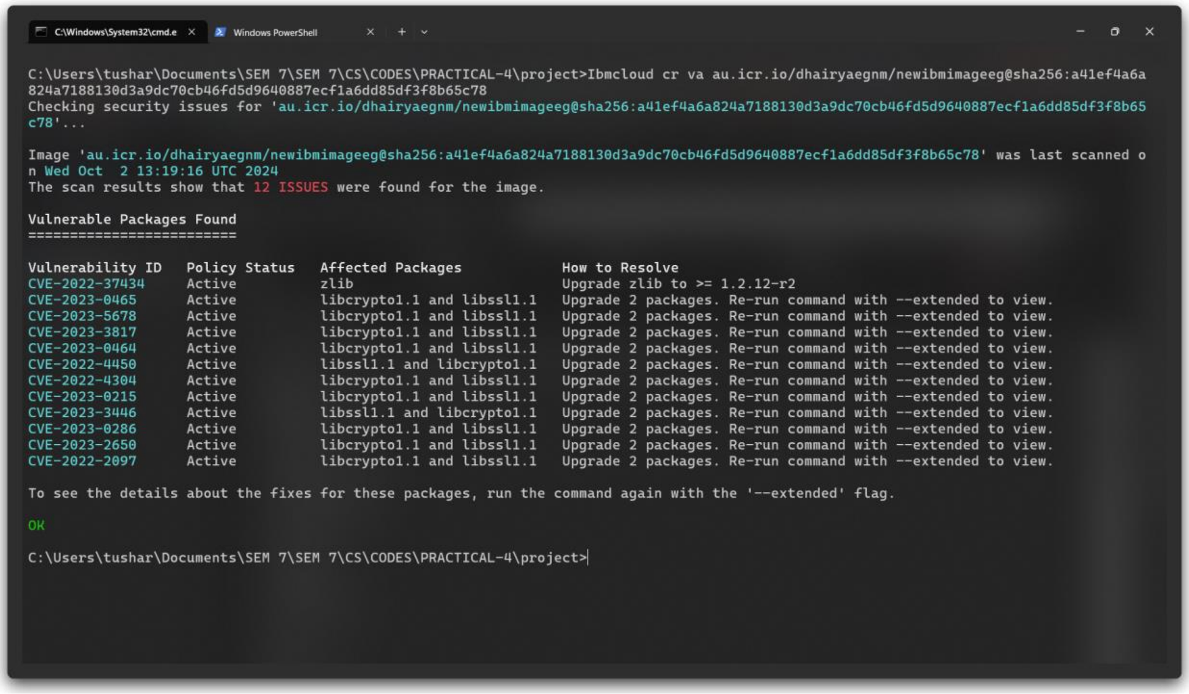
We can scan image with

Ibmcloud cr va au.icr.io/tk-namespace/tushar-test



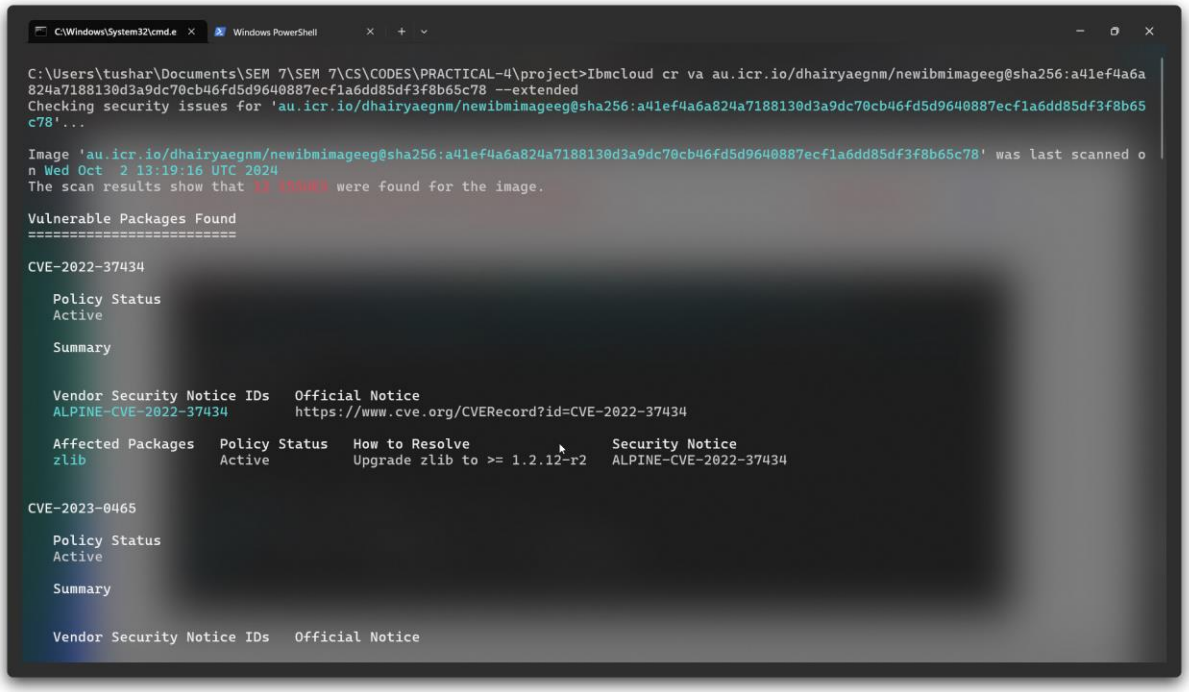
```
C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>Ibmcloud cr va au.icr.io/tk-namespace/tushar-test
Checking security issues for 'au.icr.io/tk-namespace/tushar-test:latest'...

Image 'au.icr.io/tk-namespace/tushar-test:latest' was last scanned on Wed Oct  2 13:19:16 UTC 2024
The scan results show that NO ISSUES were found for the image.

OK
```

We know that there is not any issue for this image so we'll check for another image which is on sydney region



```
C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>Ibmcloud cr va au.icr.io/dhairyaegnm/newibmimageeg@sha256:a41ef4a6a
824a7188130d3a9dc70cb46fd5d9640887ecf1a6dd85df3f8b65c78
Checking security issues for 'au.icr.io/dhairyaegnm/newibmimageeg@sha256:a41ef4a6a824a7188130d3a9dc70cb46fd5d9640887ecf1a6dd85df3f8b65
c78'...

Image 'au.icr.io/dhairyaegnm/newibmimageeg@sha256:a41ef4a6a824a7188130d3a9dc70cb46fd5d9640887ecf1a6dd85df3f8b65c78' was last scanned o
n Wed Oct  2 13:19:16 UTC 2024
The scan results show that 12 ISSUES were found for the image.

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

Vulnerability ID   Policy Status   Affected Packages             How to Resolve
CVE-2022-37434     Active          zlib                          Upgrade zlib to >= 1.2.12-r2
CVE-2023-0465      Active          libcrypto1.1 and libssl1.1    Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-5678      Active          libcrypto1.1 and libssl1.1    Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-3817      Active          libcrypto1.1 and libssl1.1    Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-0464      Active          libcrypto1.1 and libssl1.1    Upgrade 2 packages. Re-run command with --extended to view.
CVE-2022-4450      Active          libssl1.1 and libcrypto1.1    Upgrade 2 packages. Re-run command with --extended to view.
CVE-2022-4304      Active          libcrypto1.1 and libssl1.1    Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-0215      Active          libcrypto1.1 and libssl1.1    Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-3446      Active          libssl1.1 and libcrypto1.1    Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-0286      Active          libcrypto1.1 and libssl1.1    Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-2650      Active          libcrypto1.1 and libssl1.1    Upgrade 2 packages. Re-run command with --extended to view.
CVE-2022-2097      Active          libcrypto1.1 and libssl1.1    Upgrade 2 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

C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>
```

We can see extended version with adding –extended in command

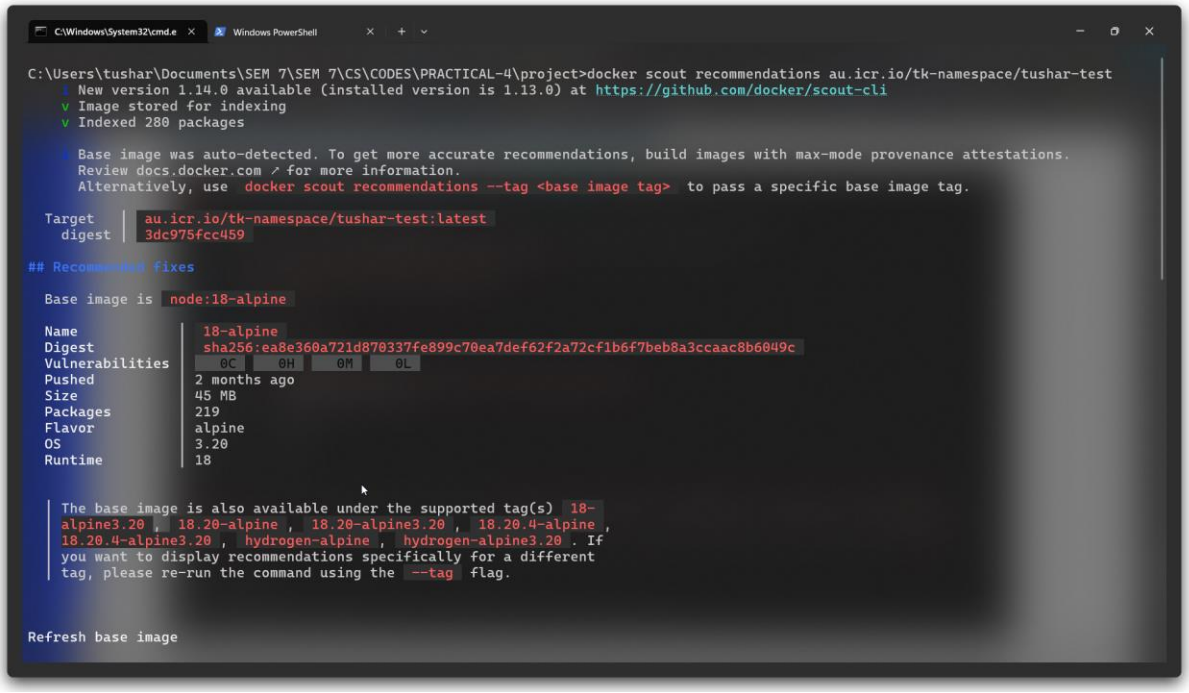


```
C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>Ibmcloud cr va au.icr.io/dhairyaegnm/newibmimageeg@sha256:a41ef4a6a
824a7188130d3a9dc70cb46fd5d9640887ecf1a6dd85df3f8b65c78 --extended
Checking security issues for 'au.icr.io/dhairyaegnm/newibmimageeg@sha256:a41ef4a6a824a7188130d3a9dc70cb46fd5d9640887ecf1a6dd85df3f8b65
c78'...

Image 'au.icr.io/dhairyaegnm/newibmimageeg@sha256:a41ef4a6a824a7188130d3a9dc70cb46fd5d9640887ecf1a6dd85df3f8b65c78' was last scanned o
n Wed Oct  2 13:19:16 UTC 2024
The scan results show that 13 ISSUES were found for the image.

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

CVE-2022-37434

   Policy Status
   Active

   Summary


   Vendor Security Notice IDs   Official Notice
   ALPINE-CVE-2022-37434        https://www.cve.org/CVERecord?id=CVE-2022-37434

   Affected Packages   Policy Status   How to Resolve              Security Notice
   zlib                Active          Upgrade zlib to >= 1.2.12-r2   ALPINE-CVE-2022-37434


CVE-2023-0465

   Policy Status
   Active

   Summary


   Vendor Security Notice IDs   Official Notice
```

Now we can scan our image locally through Scout

Through this command

Docker scout recommendation ImageName



```
C:\Users\tushar\Documents\SEM 7\SEM 7\CS\CODES\PRACTICAL-4\project>docker scout recommendations au.icr.io/tk-namespace/tushar-test
    i New version 1.14.0 available (installed version is 1.13.0) at https://github.com/docker/scout-cli
    v Image stored for indexing
    v Indexed 280 packages

    i Base image was auto-detected. To get more accurate recommendations, build images with max-mode provenance attestations.
      Review docs.docker.com ↗ for more information.
      Alternatively, use  docker scout recommendations --tag <base image tag>  to pass a specific base image tag.

  Target   │  au.icr.io/tk-namespace/tushar-test:latest
    digest │  3dc975fcc459

## Recommended fixes

  Base image is  node:18-alpine

  Name            │  18-alpine
  Digest          │  sha256:ea8e360a721d870337fe899c70ea7def62f2a72cf1b6f7beb8a3ccaac8b6049c
  Vulnerabilities │    0C     0H     0M     0L
  Pushed          │ 2 months ago
  Size            │ 45 MB
  Packages        │ 219
  Flavor          │ alpine
  OS              │ 3.20
  Runtime         │ 18


    │ The base image is also available under the supported tag(s)  18-
    │ alpine3.20 ,  18.20-alpine ,  18.20-alpine3.20 ,  18.20.4-alpine ,
    │ 18.20.4-alpine3.20 ,  hydrogen-alpine ,  hydrogen-alpine3.20 . If
    │ you want to display recommendations specifically for a different
    │ tag, please re-run the command using the  --tag  flag.


Refresh base image
```