

# **Lab notebook Week 6**

**Submitted by: Vishrut Sharma (OdinID: vishrut)**

## **Table of Contents**

<b>06.1a: EB Guestbook.....</b>	<b>2</b>
3. Running the application.....	2
4. Handling failures seamlessly.....	3
7. Deploying the Guestbook.....	3
<b>06.1g: App Engine Guestbook.....</b>	<b>4</b>
4. Deploying the Guestbook.....	4
5. Handling failures seamlessly.....	5
<b>06.2g: Cloud Run, Secret Manager (Web proxy).....</b>	<b>5</b>
8. Setup secret proxy.....	5
9. Cloud Build and Container Registry.....	6
10. Deploy to Cloud Run.....	7
12. Deploy to Cloud Run with Secret Manager.....	8
<b>06.3a: ECS Guestbook.....</b>	<b>9</b>
5. Examine the service.....	9
6. Visit the site.....	9
<b>06.3g: Cloud Run Guestbook.....</b>	<b>10</b>
2. Prepare a container image.....	10
4. View the Guestbook.....	11
<b>06.4g: Cloud Functions, PubSub.....</b>	<b>11</b>
4. -.....	11
7. Test function.....	12
10. PubSub via CLI.....	13
11. -.....	13
14. Test programs and clean up.....	13

## 06.1a: EB Guestbook

### 3. Running the application

- Take a screenshot showing it has been brought up successfully

The screenshot shows the AWS Elastic Beanstalk console for the application 'eb-hello'. The main panel displays a green success message: 'Environment successfully launched.' It shows the Environment ID 'e-ac2mg2rzki', Application name 'eb-hello', and Platform 'Python 2023/4'. A modal window titled 'Odin ID vishrut' is open, showing the text 'Odin ID: vishrut'. Below the main panel, the 'Events' tab is selected, showing a list of 20 events, all of which are INFO level messages related to the successful launch of the environment.

The screenshot shows the AWS Elastic Beanstalk environment page for 'eb-hello-env'. The main area features a large green 'Congratulations' banner with the text: 'Your first AWS Elastic Beanstalk Python Application is now running on your own dedicated environment in the AWS Cloud'. Below the banner, it says 'This environment is launched with Elastic Beanstalk Python Platform'. To the right, there's a 'What's Next?' sidebar with links to various AWS Elastic Beanstalk documentation and deployment guides. A modal window titled 'Odin ID vishrut' is open, showing the text 'Odin ID: vishrut'.

## 4. Handling failures seamlessly

- Take a screenshot of the replacement VM being started.

The screenshot shows the AWS EC2 Instances page. There are three instances listed:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
Eb-hello-env	i-08fb93dec21931fb	Running	t3.micro	2/2 checks passed	No alarms	us-east-1a	ec2-18-2
Eb-hello-env	i-094478424b286ce86	Terminated	t3.micro	-	No alarms	us-east-1c	-
Eb-hello-env	i-0c4cb8714a3e567ec	Running	t3.micro	Initializing	No alarms	us-east-1c	ec2-18-2

A modal window titled "Select an instance" is open, displaying the text "Odin ID: vishrut".

## 7. Deploying the Guestbook

- Take a screenshot of the Guestbook including the URL with the entry in it.

The screenshot shows a web browser displaying a guestbook entry. The URL in the address bar is `guestbook-env.eba-vcpz3ry.us-east-1.elasticbeanstalk.com`. The entry is as follows:

Vishruth Sharma <vishrut@pdx.edu>  
signed on 2023-05-01 18:46:40.532753  
Hello DynamoDB

Vishruth Sharma <vishrut@pdx.edu>  
signed on 2023-05-02 01:58:50.004092  
Hello Docker DynamoDB

Vishruth Sharma <vishrut@pdx.edu>  
signed on 2023-05-02 23:04:48.488903  
Hello Cloud9!

Vishruth Sharma <vishrut@pdx.edu>  
signed on 2023-05-03 17:28:07.744792  
Hello EC2!

Vishruth Sharma <vishrut@pdx.edu>  
signed on 2023-05-07 02:33:38.164476  
Hello Elastic Beanstalk!

- Take a screenshot of them.

The screenshot shows the AWS CloudShell interface. At the top, there's a browser-like header with tabs and a URL bar pointing to <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#instances;instanceState=running>. Below the header is the AWS Management Console sidebar with various services like EC2 Dashboard, EC2 Global View, Events, Limits, Instances, Images, and AMIs. The main content area displays a table titled "Instances (3) Info" showing three running t3.micro instances named "guestbook-env". A modal window titled "Select an instance" is open, showing a terminal session with the command "Odin ID: vishrut". The bottom of the screen shows the AWS CloudShell interface with tabs for CloudShell, Feedback, Language, and a footer with copyright information and links.

## 06.1g: App Engine Guestbook

### 4. Deploying the Guestbook

- Take a screenshot of the output that includes the URL in the address bar for your lab notebook.

The screenshot shows a web browser window displaying the "Guestbook" application. The URL in the address bar is <https://cloud-sharma-vishrut.wl.appspot.com>. The page content includes a "Sign here" button, a "Entries" section, and three entries from the guestbook:

- Vishrut Sharma <vishrut@pdx.edu>  
signed on 2023-05-02 02:59:55.896795+00:00  
Hello Cloud Shell!
- Vishrut Sharma <vishrut@pdx.edu>  
signed on 2023-05-01 19:33:09.519186+00:00  
Hello Datastore
- Vishrut Sharma <vishrut@pdx.edu>  
signed on 2023-05-07 18:09:00.731423+00:00  
Hello App Engine!
- Vishrut Sharma <vishrut@pdx.edu>  
signed on 2023-05-02 03:11:08.008194+00:00  
Hello Compute Engine!

## 5. Handling failures seamlessly

- Take a screenshot of them.

The screenshot shows the Google Cloud Platform interface for the App Engine service. The left sidebar has 'Instances' selected. The main area displays a summary message: 'No data is available for the selected time frame.' Below this, there's a table titled 'Instances' with two rows of data. The columns are ID, OPS, Latency, Requests, Errors, and Mem. The first row has ID '00c61b117c50ba07cb283c08b4b18...' with OPS 0, Latency 0 ms, Requests 5, Errors 0, and Mem 92.7 kB. The second row has ID '00c61b117cce5357217743e09377c...' with similar values. A 'Cloud Shell' terminal tab is open at the bottom left.

## 06.2g: Cloud Run, Secret Manager (Web proxy)

### 8. Setup secret proxy

- Take a screenshot of the proxy and its results including the URL containing your OdinID

The screenshot shows a browser window with a proxy setup. The address bar shows 'Added security | https://8000-cs-73aa5633-a42f-4d94-83da-e8f6d68c7fb9.cs-us-west1-wolo.cloudshell.dev/vishrut'. Below the address bar, there's a 'Proxy' section with a text input field 'Enter URL to access by proxy:' containing 'https://oregonctf.org/'. At the bottom of the browser window, a terminal window titled 'Odin ID v' is open, displaying the text 'Odin ID: vishrut'. The terminal window has a status bar at the bottom showing 'Ln 1, Col 17 100% Windows (CRLF) UTF-8'.

Capture-the-Flag security games and codelabs

Ones we've developed:

- Computer Systems Programming (CS 205) [CTF](#)
- Malware Reverse Engineering (CS 492) [CTF](#)
- angr Symbolic Execution (CS 492) [CTF](#)
- Cloud Security (CS 430/495) [Thunder CTF](#)
- Fuzzing (CS 492) [codelab](#)
- Smart contract symbolic execution (CS 410) [codelabs](#)
- Divergent Cryptography and Security (CyberPDX camp) [CTF](#)

Ones we like to teach from:

- bandit (Linux tools) [CTF](#)
- natas (Web Security) [CTF](#)
- PortSwigger (Web Security) [CTF](#)
- OWASP Damn Vulnerable NodeJS Application (Web Security) [CTF](#)
- flaws.cloud (Cloud Security) [v1](#) | [v2](#)
- CloudGoat (Cloud Security) [exercises](#)
- Microcorruption (Reverse Engineering) [CTF](#)
- Security Innovation (Ethereum) [CTF](#)
- Etherernaut (Ethereum) [CTF](#)
- CryptoPals (Cryptanalysis) [CTF](#)

Portland State's CTF Slack channel [here](#)

**Resources**

Some recommended resources include:

- Download a Windows XP VM with IDA Pro Free installed [here](#)
- Or download IDA Pro Free [here](#)
- Download a Linux OS Box [here](#)
- PSU's CS 205 Computer Systems Programming [course](#)
- PSU's CS 430 Internet, Web, and Cloud Systems [course](#)

- **What is the security advantage of passing in the secret proxy route as an environment variable?**

Answer: Using the secret proxy route as an environment variable enhances security by separating sensitive information, enabling access control, simplifying configuration management, providing auditing capabilities, and integrating with cloud service providers.

## 9. Cloud Build and Container Registry

- Take a screenshot of the image in the registry that shows the size of the container for your lab notebook.

Container Registry

Images

Name	Tags	Virtual Size	Created	Uploaded
42ad4fe43aec	latest	50.3 MB	1 minute ago	Just now

Marketplace

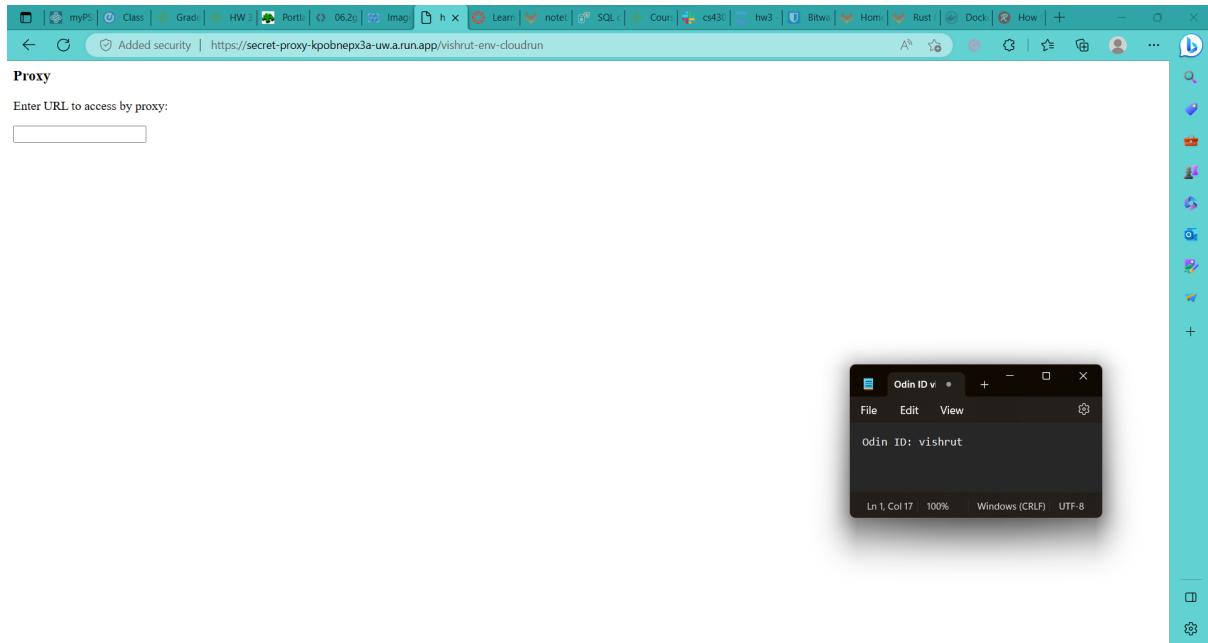
Release Notes

CLOUD SHELL

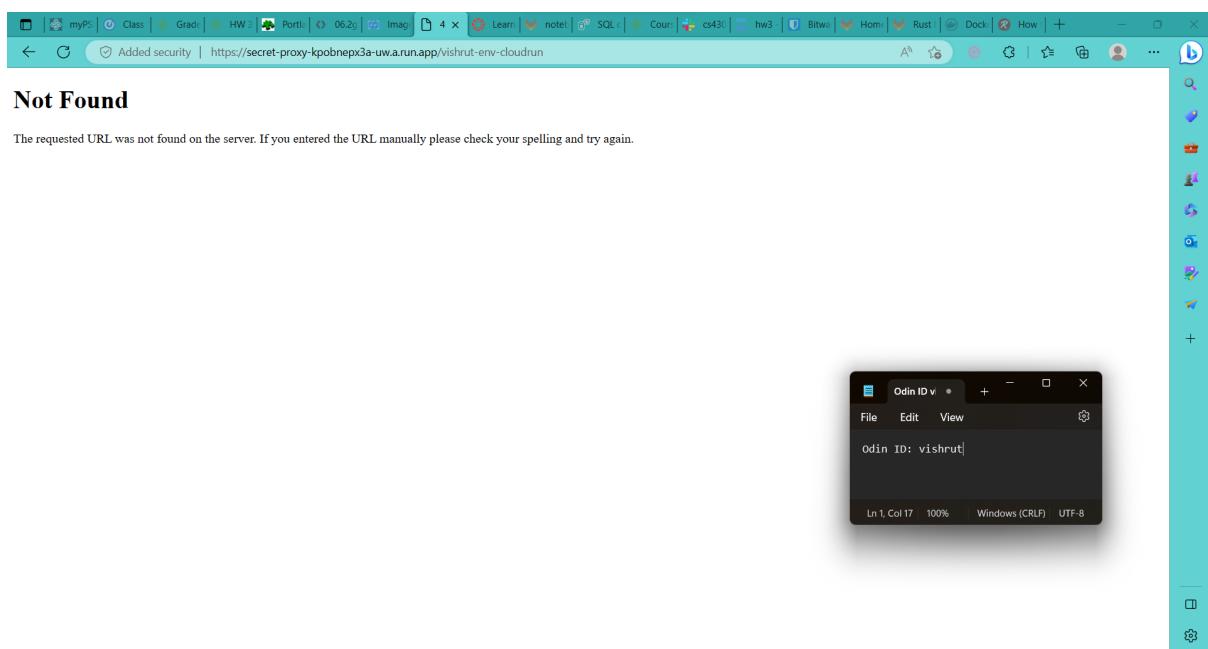
```
IMAGEs: gcr.io/cloud-sharma-vishrut/secret-proxy (+1 more)
STATUS: SUCCESS
vishrut@cloudshell:/secret-proxy (cloud-sharma-vishrut)$ gcloud container images list
NAME: gcr.io/cloud-sharma-vishrut/secret-proxy
Only listing images in gcr.io/cloud-sharma-vishrut. Use --repository to list images in other repositories.
vishrut@cloudshell:/secret-proxy (cloud-sharma-vishrut)$ 
```

## 10. Deploy to Cloud Run

- Take a screenshot of it that includes the proxy URL for your lab notebook.

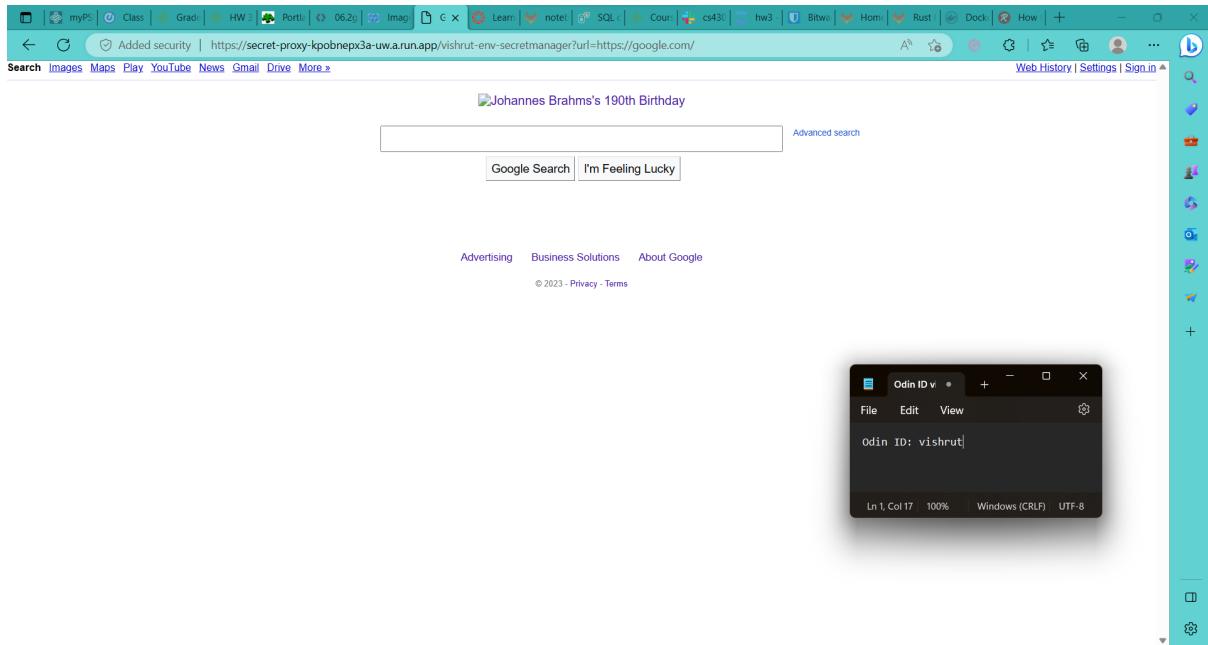


- Take a screenshot of the error page that includes the proxy URL for your lab notebook.



## 12. Deploy to Cloud Run with Secret Manager

- Take a screenshot of it that includes the proxy URL for your lab notebook.



- Identify the vulnerability in your lab notebook that Google has prevented.

It seems that Google has taken measures to prevent a vulnerability that could potentially allow unauthorized access to sensitive information via the Metadata service linked to the virtual machine (VM) that runs a container. This service can be accessed through the two URLs provided, <http://169.254.169.254/computeMetadata> and <http://169.254.169.254/computeMetadata/v1>, and provides crucial information about the VM's identity and configuration, such as authentication tokens. If a container running on a VM gains access to this service, an attacker could exploit this vulnerability to obtain unauthorized access to the sensitive information stored on the VM or conduct other malicious actions.

## 06.3a: ECS Guestbook

### 5. Examine the service

- Take a screenshot of the DNS name of the guestbook-lb load balancer for your lab notebook

The screenshot shows the AWS EC2 Load Balancers console. In the search bar, 'guestbook-lb' is entered. The results table shows one entry:

Name	DNS name	State	VPC ID	Availability Zones	Type
guestbook-lb	guestbook-lb-140560230...	Active	vpc-0b9c4137070e0204a	6 Availability Zones	application

A modal window titled 'Odin ID v' is open, displaying the text 'Odin ID: vishrut'. The URL in the browser's address bar is <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LoadBalancers:search=guestbook-lb;sort=descdnsName>.

### 6. Visit the site

- Take a screenshot of the Guestbook app running in a browser that includes the DNS name of the site.

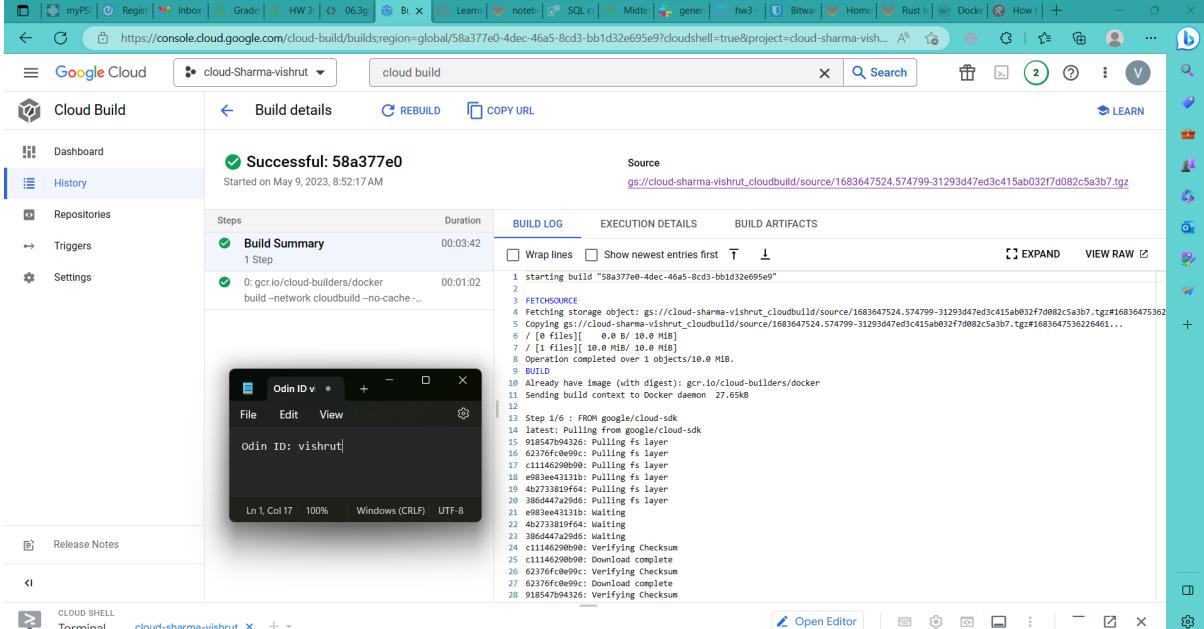
The screenshot shows a web browser displaying the Guestbook application. The URL in the address bar is <https://guestbook-lb-1405602305.us-east-1.elb.amazonaws.com>. The page content shows several signed messages from 'Vishrut Sharma <vishrut@pdx.edu>':

- signed on 2023-05-02 01:58:50.004092  
Hello Docker DynamoDB
- Vishrut Sharma <vishrut@pdx.edu>  
signed on 2023-05-02 23:04:48.488903  
Hello Cloud9!
- Vishrut Sharma <vishrut@pdx.edu>  
signed on 2023-05-03 17:28:07.744792  
Hello EC2!
- Vishrut Sharma <vishrut@pdx.edu>  
signed on 2023-05-07 02:33:38.164476  
Hello Elastic Beanstalk!
- Vishrut Sharma <vishrut@pdx.edu>  
signed on 2023-05-08 00:23:49.041902  
Hello ECS!

## 06.3g: Cloud Run Guestbook

### 2. Prepare a container image

- Take a screenshot that includes the output of the command and the time it took to execute.

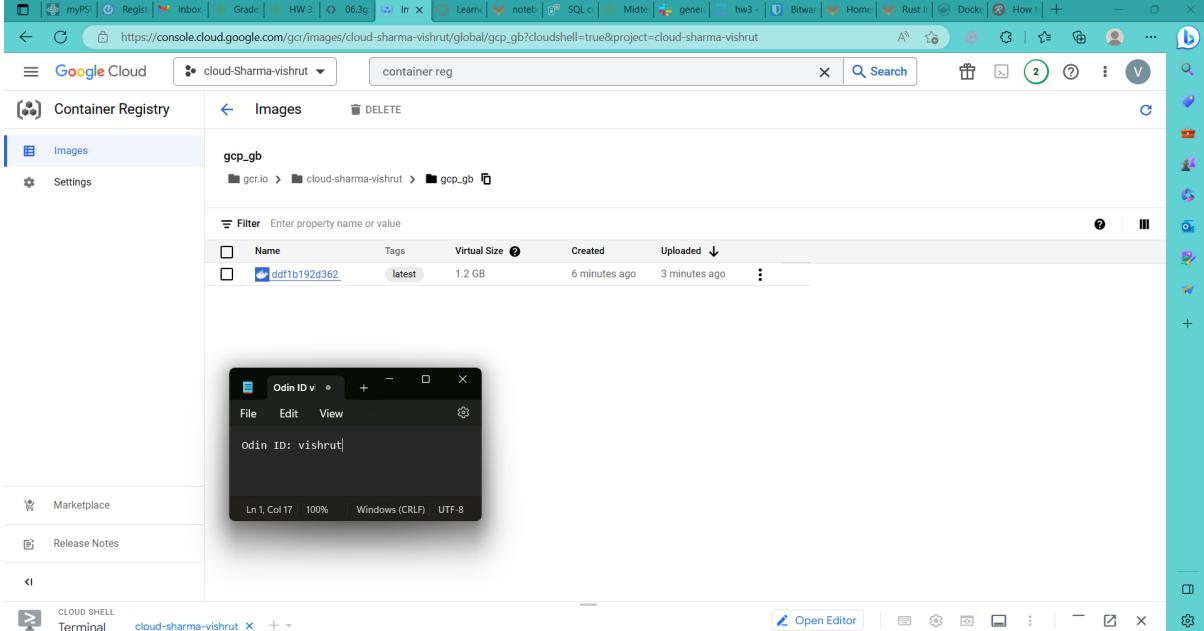


The screenshot shows the Google Cloud Build interface. On the left, there's a sidebar with 'Cloud Build' selected, followed by 'Dashboard', 'History', 'Repositories', 'Triggers', and 'Settings'. The main area displays a successful build summary for build ID 58a377e0. It shows the build started on May 9, 2023, at 8:52:17 AM. The 'Build Log' tab is active, showing the command output:

```
1 starting build "58a377e0-4dec-46a5-8cd3-bb1d32e695e9"
2
3 FETCHSOURCE
4 Fetching storage object: gs://cloud-sharma-vishrut_cloudbuild/source/1683647524.574799-31293d47ed3c415ab032f7d082c5a3b7.tgz#16836475362
5 Copying gs://cloud-sharma-vishrut_cloudbuild/source/1683647524.574799-31293d47ed3c415ab032f7d082c5a3b7.tgz#1683647536226461...
6 / [1 files] 10.0 MB/ 10.0 MB]
7 Operation completed over 1 objects/10.0 MB.
8 BUILD
9
10 Already have image (with digest): gcr.io/cloud-builders/docker
11 Sending build context to Docker daemon 27.65kB
12
13 Step 1/6 : FROM google/cloud-sdk
14 latest: Pulling from google/cloud-sdk
15 918547b94326: Pulling fs layer
16 62376fc099c: Pulling fs layer
17 c1146209009c: Pulling fs layer
18 ddf1b192d362: Pulling fs layer
19 4b273819464: Pulling fs layer
20 3866d44729d6: Pulling fs layer
21 e993ee43131b: Waiting
22 4b273819464: Waiting
23 3866d44729d6: Waiting
24 c1146209009c: Verifying Checksum
25 c1146209009c: Download complete
26 62376fc099c: Verifying Checksum
27 62376fc099c: Download complete
28 918547b94326: Verifying Checksum
```

Below the log, there's a terminal window showing the command 'odin ID: vishrut'. At the bottom, there's a 'CLOUD SHELL Terminal' tab.

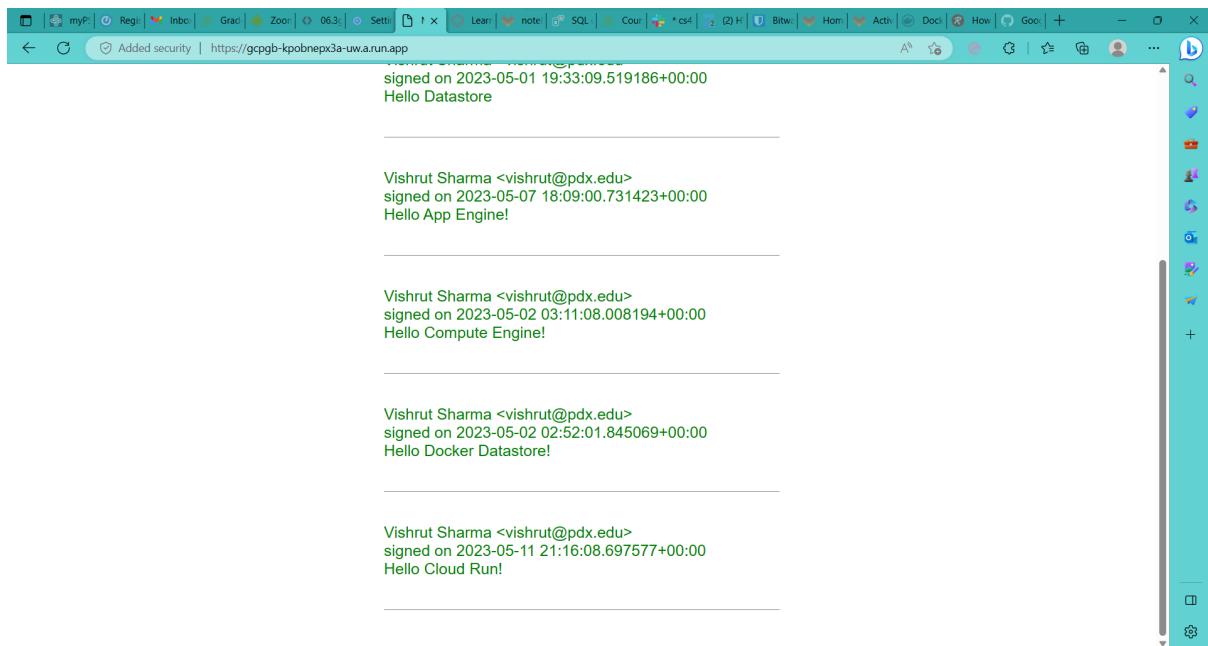
- Take a screenshot showing the container image and its virtual size



The screenshot shows the Google Container Registry interface. On the left, there's a sidebar with 'Container Registry' selected, followed by 'Images' and 'Settings'. The main area displays a list of images under the 'gcp\_gb' repository. There is one entry: 'ddf1b192d362' with the tag 'latest', created 6 minutes ago and uploaded 3 minutes ago. A 'Filter' input field is present. Below the list, there's a terminal window showing the command 'odin ID: vishrut'. At the bottom, there's a 'CLOUD SHELL Terminal' tab.

## 4. View the Guestbook

- Take a screenshot that includes the URL Cloud Run has created for your site.



- What port do container instances listen on?

Answer: 8080

- What are the maximum number of instances Cloud Run will autoscale up to for your service?

Answer: 100 instances

## 06.4g: Cloud Functions, PubSub

4.-

- After downloading the file from the bucket, where is it stored?

Answer: After downloading the file from the bucket the file is stored in temp\_local\_filename.

- What class in the ImageMagick package is used to do the blurring of the file?

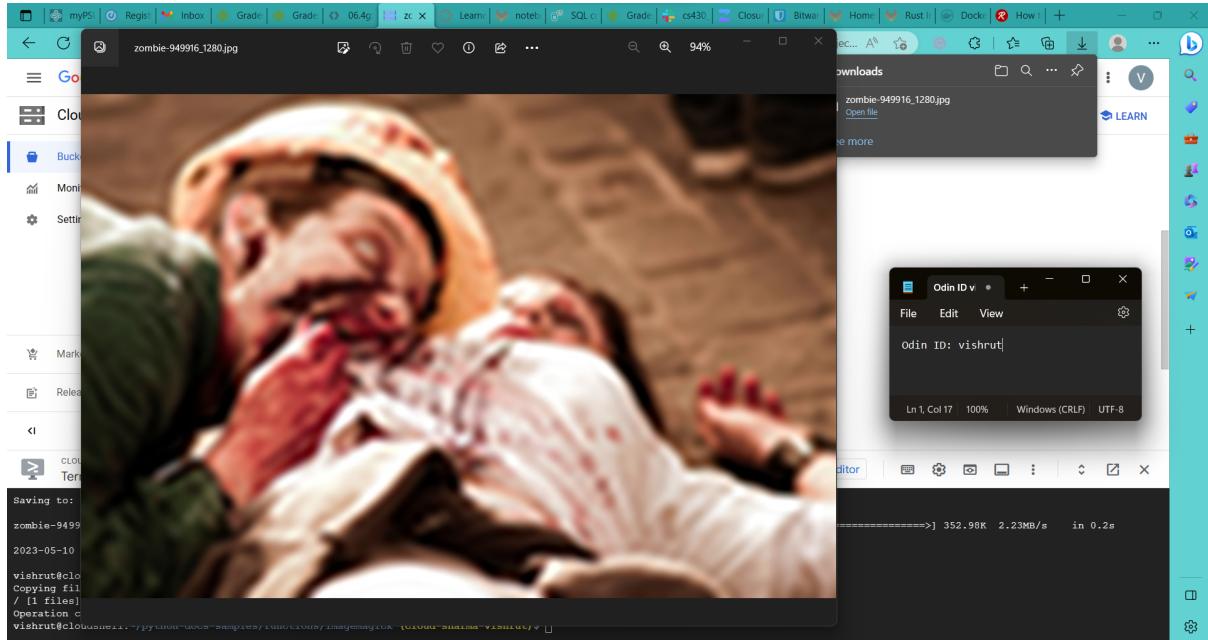
Answer: \_\_blur\_image class is used to do the blurring of the file.

- What lines of code perform the blurring of the image and its storage back into the filesystem?

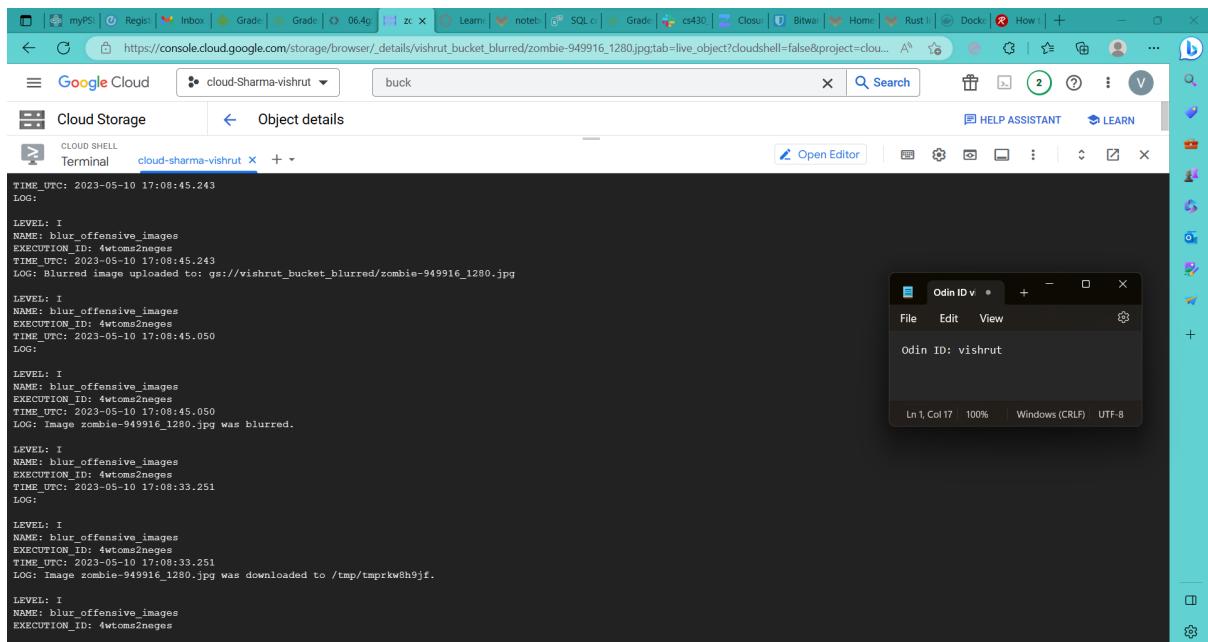
Answer: Lines 72 to 74 of the code are used to perform the blurring of the image and store it back in the filesystem.

## 7. Test function

- Take a screenshot of the blurred image in the output bucket for your lab notebook



- Include a screenshot of the output logs that show that the above image was blurred.



## 10. PubSub via CLI

- Why are there no items returned?

Answer: This is because we created the subscription after publishing message #1. When message #1 was published there were no subscribers to send the message to. When message #2 was published the subscription was already active which is why we were able to view it in the VM.

## 11. -

- What is the messageId of the published message?

```
vishrutm@cloudshell:~ (cloud-sharma-vishrutm) $ gcloud pubsub topics publish projects/cloud-sharma-vishrutm/topics/topic-vishrutm --message="Message #1"
messageIds:
- '7647814835072160'
vishrutm@cloudshell:~ (cloud-sharma-vishrutm) $ gcloud pubsub topics publish projects/cloud-sharma-vishrutm/topics/topic-vishrutm --message="Message #2"
messageIds:
- '7647814756710774'
vishrutm@cloudshell:~ (cloud-sharma-vishrutm) $
```

- Take a screenshot of the output of the successful pull that includes the message and its messageId.

```
https://ssh.cloud.google.com/v2/ssh/projects/cloud-sharma-vishrutm/zones/us-west1-b/instances/pubsub?authuser=0&hl=en_US&projectNumber=800044206461&useAdminProxy=true - Work - Microsoft Edge
https://ssh.cloud.google.com/v2/ssh/projects/cloud-sharma-vishrutm/zones/us-west1-b/instances/pubsub?authuser=0&hl=en_US&projectNumber=800044206461&useAdminProxy=true
SSH-in-browser
System information as of Wed May 10 17:15:24 UTC 2023
System load: 0.1176578125 Processes: 108
Usage of /: 19.8% of 9.51GB Users logged in: 0
Memory usage: 6% IPv4 address for ens4: 10.138.0.13
Swap usage: 0%
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

vishrutm@pubsub:~$ gcloud pubsub subscriptions create sub-$USER \
--topic=projects/cloud-sharma-vishrutm/topics/topic-vishrutm.
Created subscription [projects/cloud-sharma-vishrutm/subscriptions/sub-vishrutm].
vishrutm@pubsub:~$ gcloud pubsub subscriptions pull sub-$USER
Listed 0 items.
vishrutm@pubsub:~$ gcloud pubsub subscriptions pull sub-$USER
DATA | MESSAGE_ID | ORDERING_KEY | ATTRIBUTES | DELIVERY_ATTEMPT | ACK_ID
|-----+-----+-----+-----+-----+-----|
| Message #2 | 7647814756710774 | 00RQB8yexXUZIUTc2CGhR0k9e1z811ChFEGAHTwIoXXXxtSJBNnFoUQ02cn1gWJaFVBXEFArC1EbB2hOBXUk5jG4EtDWl1cFwYRFd5W1oDGH
DW3Ev387Bw10j1daKdnA0izsaXvSwg0-Zim9XhJLL5-NsXFQV5AEkw-GURJUYtDCypYEU4EISE-MDSF |
vishrutm@pubsub:~$
```

## 14. Test programs and clean up

- Take a screenshot showing the messageIds and messages sent

```
(env) vishrutm@cloudshell:~ (cloud-sharma-vishrutm) $ python3 publisher.py
Enter a message to send: message 1
Published 7647939257604256 to topic projects/cloud-Sharma-vishrutm/topics/my_topic
Enter a message to send: message 2
Published 7647912924268368 to topic projects/cloud-Sharma-vishrutm/topics/my_topic
Enter a message to send: message 3
Published 7647964843866737 to topic projects/cloud-Sharma-vishrutm/topics/my_topic
Enter a message to send: 
```

- Take a screenshot showing the same messageIds and messages received

```
(env) vishrut@pubsub:~$ python3 subscriber.py
Received message: 2023-05-10 17:34:02 (projects/cloud-Sharma-vishrut/topics/my_topic) : message 1
Received message: 2023-05-10 17:35:00 (projects/cloud-Sharma-vishrut/topics/my_topic) : message 2
Received message: 2023-05-10 17:35:05 (projects/cloud-Sharma-vishrut/topics/my_topic) : message 3
|
```