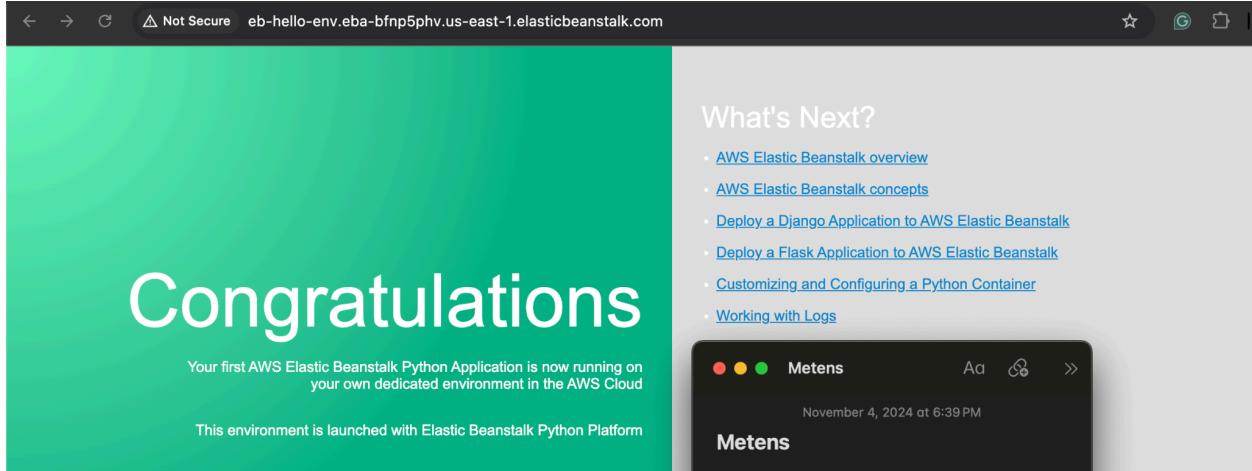


Week #6 Labs

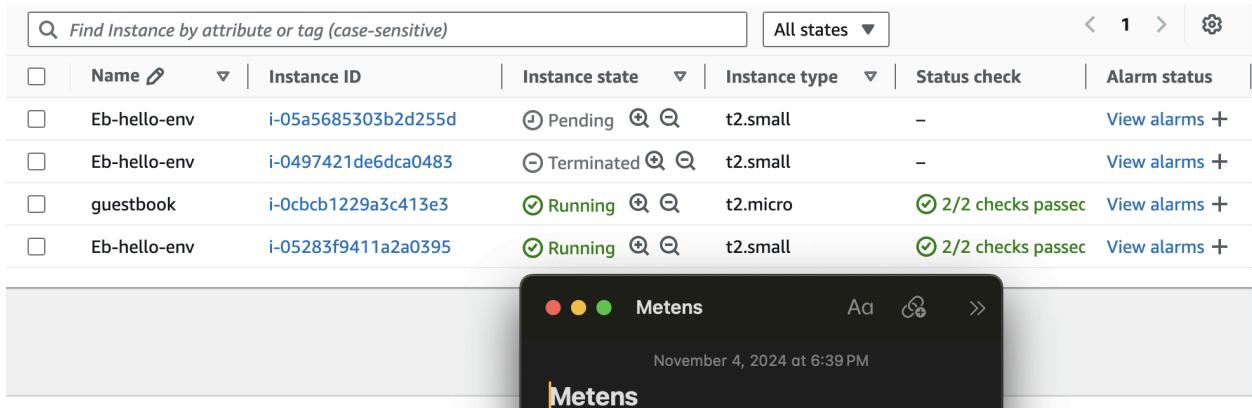
06.1a: EB Guestbook	2
3. Running the application	2
4. Handling failures seamlessly	2
7. Deploying the Guestbook	3
06.1g: App Engine Guestbook	4
3. Deploying the Guestbook	4
4. Handling failures seamlessly	5
06.2g: Cloud Run, Secret Manager (Web proxy)	5
8. Setup secret proxy	5
10. Cloud Build	6
11. Deploy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

06.1a: EB Guestbook

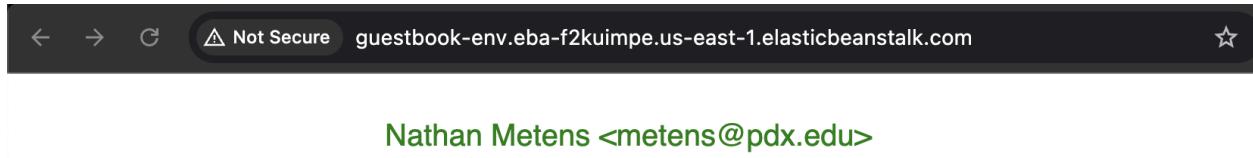
3. Running the application



4. Handling failures seamlessly

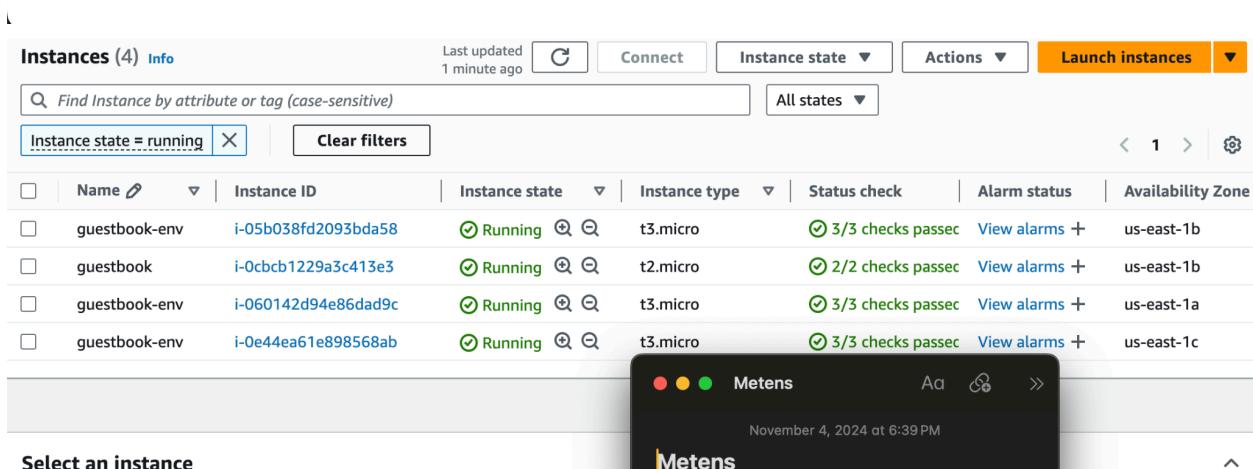


7. Deploying the Guestbook



Nathan Metens <metens@pdx.edu>
signed on 2024-11-05 04:39:52.560737
Hello EC2!

Nathan Metens <metens@pdx.edu>
signed on 2024-11-06 05:41:14.756183
Hello Elastic Beanstalk!



Instances (4) Info Last updated 1 minute ago Connect Instance state Actions Launch instances

Find Instance by attribute or tag (case-sensitive) All states

Instance state = running Clear filters

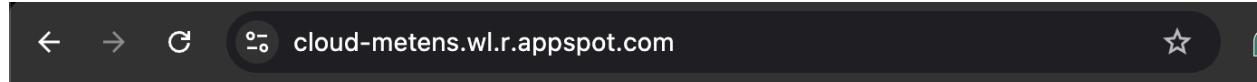
<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	guestbook-env	i-05b038fd2093bda58	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1b
<input type="checkbox"/>	guestbook	i-0cbc1229a3c413e3	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1b
<input type="checkbox"/>	guestbook-env	i-060142d94e86dad9c	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1a
<input type="checkbox"/>	guestbook-env	i-0e44ea61e898568ab	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1c

Select an instance

Metens November 4, 2024 at 6:39 PM Metens

06.1g: App Engine Guestbook

3. Deploying the Guestbook



Guestbook

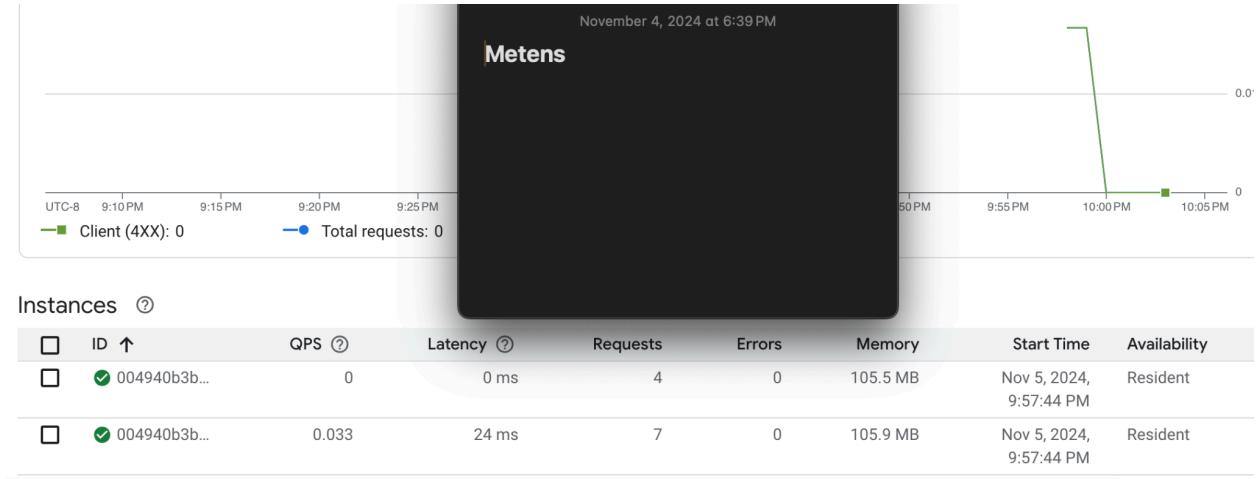
[**Sign here**](#)

Entries

Nathan Metens <metens@pdx.edu>
signed on 2024-11-05 06:07:00.327416+00:00
Hello Datastore

Nathan Metens <metens@pdx.edu>
signed on 2024-11-06 06:03:37.677092+00:00
Hello App Engine!

4. Handling failures seamlessly



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

8. Setup secret proxy

The screenshot shows a web browser window with the URL `8000-cs-292029700782-default.cs-us-west1-ijlt.cloudshell.dev/metens?url=%20https://oregonctf.org`. The page content includes:

- A 'Toggle navigation' button.
- A logo for Portland State University Computer Science.
- A logo for Oregon CTF.
- A section titled "Capture-the-Flag security games and codelabs".
- A list of "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](#)
 - Divergent Cryptography and Security (CyberPDX camp) [CTF](#)
- A list of "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](#)
 - CryptoPals (Cryptanalysis) [CTF](#)

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

Resources

The advantage of passing in a secret proxy route as an environment variable is that the secret proxy route won't be embedded in the application code which would make it visible to anyone who has access to the application.

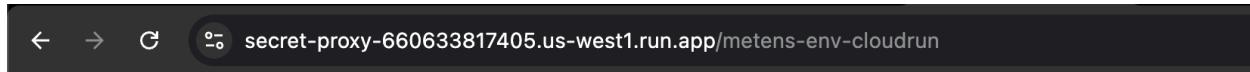
10. Cloud Build

The screenshot shows the Google Cloud Artifact Registry interface. At the top, there are navigation links for 'Google Cloud' and 'cloud-metens' (selected), and a search bar with 'artifact'. Below this, the main area is titled 'Artifact Registry' with a 'Repositories' tab selected. A breadcrumb path shows the location: 'us-west1-docker.pkg.dev > cloud-metens > secret-proxy-repo > secret-proxy'. The central part of the screen displays the 'OVERVIEW' tab for a specific Docker image. The image details are as follows:

Format	Docker
Media type	application/vnd.docker.distribution.manifest.v2+json
Project	cloud-metens
Location	us-west1 (Oregon)
Repository	secret-proxy-repo
Image	secret-proxy
Digest	sha256:8f82c3b9f57bbe4e443c74927b65ee786723c97ad804f8adb
Virtual size	52.5 MB
Built	Nov 5, 2024, 11:37:20 PM
Created	Nov 5, 2024, 11:37:34 PM
Updated	Nov 5, 2024, 11:37:34 PM
Tags	latest
Subject digest	—
Artifact type	—

11. Deploy to cloud run

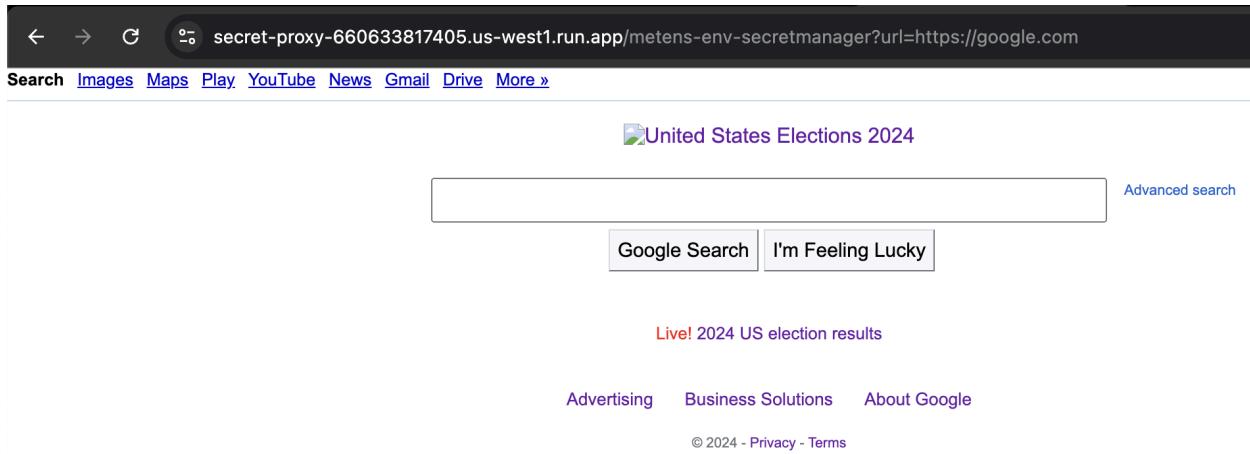
The screenshot shows a browser window with the URL 'secret-proxy-660633817405.us-west1.run.app/metens-env-cloudrun'. The page content is titled 'Proxy' and contains the instruction 'Enter URL to access by proxy:' followed by an empty input field.



Not Found

The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

13. Deploy to Cloud Run with Secret Manager



Upon attempting to access the metadata service associated with the VM by entering the two urls into the proxy, Google is preventing us from accessing this metadata from the url as we are not directly inside the VM itself. The metadata is highly sensitive and shouldn't be accessible outside of itself. "An SSRF allows an external attacker to access the endpoint because the request originates from the machine (server side) but sends the output to the attacker's browser/client."

06.3a: ECS Guestbook

1. Prepare a container image

The screenshot shows the Docker Hub interface. At the top, there's a blue header bar with the Docker Hub logo, navigation links for 'Explore', 'Repositories', 'Organizations', and 'Usage', and a search bar labeled 'Search Docker Hub'. Below the header, a search bar shows the query 'nmetens'. To its right is another search bar with the placeholder 'Search by repository name'. Further right are dropdown menus for 'All Content' and 'Create repository'. A large button labeled 'Create repository' is visible on the far right. The main content area displays three repository cards for 'nmetens / aws_gb', 'nmetens / hw3small', and 'nmetens / hw3large'. Each card includes the repository name, a brief description ('Contains: Image'), the last push time ('less than a minute ago' or '8 days ago'), a star icon with '0' stars, a down arrow icon with '11' or '10' items, a public icon, and a 'Scout inactive' status.

5. Examine the service

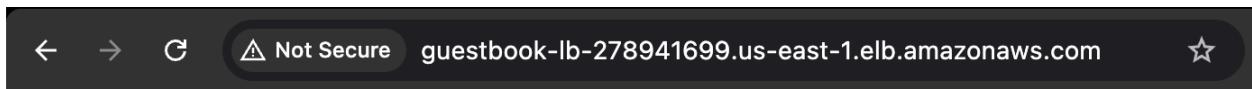
The screenshot shows the AWS EC2 Load Balancers console. The URL in the address bar is 'EC2 > Load balancers > guestbook-lb'. The main title is 'guestbook-lb'. On the right, there are two buttons: a refresh icon and an 'Actions' dropdown menu. The left side features a sidebar with a 'Details' section. The main content area contains several tabs: 'Overview', 'Listeners', 'Rules', 'Inbound IP rules', 'Metrics', and 'Logs'. The 'Overview' tab is selected. It displays the following information:

Load balancer type	Status	VPC	Load balancer IP address type
Application	Active	vpc-0a69d8c4861c0e6ec	IPv4
Scheme	Hosted zone	Availability Zones	Date created
Internet-facing	Z35SXDOTRQ7X7K	subnet-009a2eb118e611d7a us-east-1c (use1-az6)	November 6, 2024, 11:13 (UTC-08:00)
		subnet-008867a4c105054af us-east-1b (use1-az4)	
		subnet-0e4842f465dcbf57c us-east-1e (use1-az3)	
		subnet-0d4262a3df0d55cad us-east-1d (use1-az1)	
		subnet-0ef7abb344bd1e37a us-east-1a (use1-az2)	
		subnet-00c92cd43943dc9f3 us-east-1f (use1-az5)	

Below the table, there's a note about the 'Load balancer ARN' and its value: 'arn:aws:elasticloadbalancing:us-east-1:428528723226:loadbalancer/app/guestbook-lb/c3c56d9d6913ebea'. In the bottom right corner of the main content area, there's a small preview window showing a terminal session with the text 'Metens' and the date 'November 4, 2024 at 6:39 PM'.

The DNS name of the guestbook-lb load balancer is in the bottom right corner of the image.

6. Visit the site



Nathan Metens <metens@pdx.edu>
signed on 2024-11-06 05:41:14.756183
Hello Elastic Beanstalk!

Nathan Metens <metens@pdx.edu>
signed on 2024-11-06 19:25:05.569209
Hello ECS!

06.3g: Cloud Run Guestbook

2. Prepare a container image

The screenshot shows the Google Cloud Build History page. The left sidebar has options: Dashboard, History (which is selected), Repositories, Triggers, and Settings. The main area shows a successful build summary:

- Status: Successful: cd598f45-e0d7-47ec-9e93-3f0eb735a463
- Started on Nov 6, 2024, 5:48:22 PM
- Source: gs://cloud-metens_cloudbuild/source/1730944100.722678-f613d32744374e7f8a4b7bef2ff702ef.tgz
- Build Summary:
 - 1 Step
 - Duration: 00:04:05
- Step Details:
 - 0: gcr.io/cloud-builders/docker build --network cloudbuild --no-cac... Duration: 00:01:26

On the right, there's a "Build Summary" section with tabs for Build log, Execution details, and Build artifacts. The Build log tab is active, showing a list of log entries:

```
216 The push refers to repository [us-west1-docker.pkg.dev/clo  
217 2291abb5d464: Preparing  
218 e7a47f585198: Preparing  
219 bfe78bbdc673: Preparing  
220 291f90f559d0: Preparing  
221 d048c852986a: Preparing  
222 744a36b3b6e5: Preparing  
223 1f2242bb8a0f: Preparing  
224 5fd0946a90ac: Preparing  
225 ef5f5dde80a6: Preparing  
226 744a36b3b6e5: Waiting  
227 1f2242bb8a0f: Waiting  
228 5fd0946a90ac: Waiting  
229 ef5f5dde80a6: Waiting  
230 e7a47f585198: Pushed  
231 bfe78bbdc673: Pushed  
232 744a36b3b6e5: Pushed  
233 1f2242bb8a0f: Pushed  
234 5fd0946a90ac: Pushed
```



23be91769e65e

DELETE

SETUP INSTRUCTI

us-west1-docker.pkg.dev > cloud-metens > guestbook-repo

[OVERVIEW](#)[PULL](#)[MANIFEST](#)[FILES](#)[ATT/](#)

Format	Docker
Media type	application/vnd.docker.distribution.manifest.v2+json
Project	cloud-metens
Location	us-west1 (Oregon)
Repository	guestbook-repo
Image	gcp_gb
Digest	sha256:23be91769e65ed88165213cf4c650e34a4e605
Virtual size	1.2 GB
Built	Nov 6, 2024, 5:49:54 PM
Created	Nov 6, 2024, 5:52:27 PM
Updated	Nov 6, 2024, 5:52:27 PM
Tags	latest
Subject digest	—
Artifact type	—

4. View the guestbook

Apparently this step has to do with previous labs working. I was unable to get lab 5 to work, so this step inevitably isn't working, no matter what I tried.

06.4g: Cloud Functions, PubSub

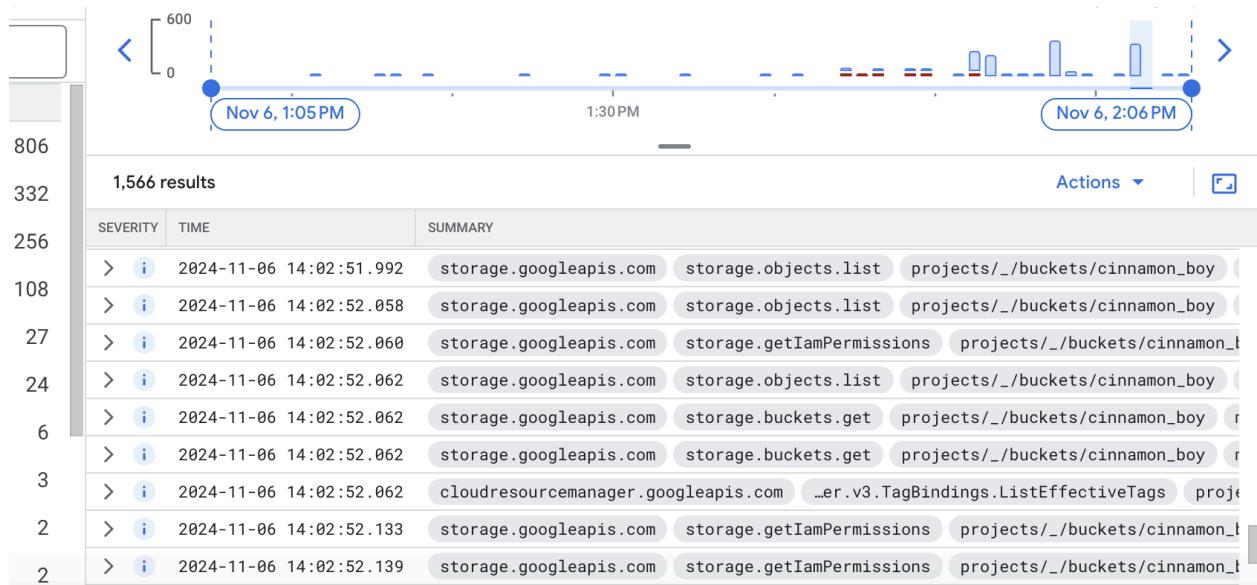
4. -

After downloading the file from the bucket, the file is stored in **temp_local_filename**.

The **Image** class from the **ImageMagic** package is used to blur the file.

Lines 71-74 in main.py blur the image and store it back into the file system.

7. Test function



```

metens@cloudshell:~/python-docs-samples/functions/imagemagick (cloud-metens)$ gcloud functions logs read blur_offensive_images --region=us-west1
LEVEL:
NAME: blur-offensive-images
EXECUTION_ID: rLi8COHgHbH1
TIME UTC: 2024-11-06 21:59:37.763
LOG: Blurred image uploaded to: gs://cinnamon_boy/zombie-949916_1280.jpg

LEVEL:
NAME: blur-offensive-images
EXECUTION_ID: rLi8COHgHbH1
TIME UTC: 2024-11-06 21:59:37.576
LOG: Image zombie-949916_1280.jpg was blurred.

LEVEL:
NAME: blur-offensive-images
EXECUTION_ID: rLi8COHgHbH1
TIME UTC: 2024-11-06 21:59:29.571
LOG: Image zombie-949916_1280.jpg was downloaded to /tmp/tmpp6mga60w.

LEVEL:
NAME: blur-offensive-images
EXECUTION_ID: rLi8COHgHbH1
TIME UTC: 2024-11-06 21:59:29.469
LOG: The image zombie-949916_1280.jpg was detected as inappropriate.

LEVEL:
NAME: blur-offensive-images
EXECUTION_ID: rLi8COHgHbH1
TIME UTC: 2024-11-06 21:59:29.204
LOG: Analyzing zombie-949916_1280.jpg.

LEVEL: I
NAME: blur-offensive-images
EXECUTION_ID:
TIME UTC: 2024-11-06 21:59:28.983
LOG:

LEVEL: I
NAME: blur-offensive-images
EXECUTION_ID:
TIME UTC: 2024-11-06 21:58:17.921
LOG: Default STARTUP TCP probe succeeded after 1 attempt for container "worker" on port 8080.

LEVEL: I
NAME: blur-offensive-images
EXECUTION_ID:
TIME UTC: 2024-11-06 21:53:41.611
LOG: Default STARTUP TCP probe succeeded after 1 attempt for container "worker" on port 8080.
metens@cloudshell:~/python-docs-samples/functions/imagemagick (cloud-metens)$

```

11. PubSub via CLI

There were no messages returned because we created the pubsub subscription account AFTER we published a message in the cloud shell. When a message is published, it's delivered to all **active subscriptions** at the time of publishing, so our subscription account wasn't active at that moment.

12. -

The message id: **12536115043899277**.

```

metens@pubsub:~$ gcloud pubsub subscriptions pull sub-$USER
+-----+
| DATA | MESSAGE_ID | ORDERING_KEY | ATTRIBUTES | DELIVERY_ATTEMPT |
+-----+
| Message #2 | 12536115043899277 |           |           |           |
|           | W1sfDmBVVXcAViWo9MSPubelNRs-fay9wN1tLdW5t-Q1Zi19XhJLLD5-NTUJFQV5AEkw-BORJUYtDCypYEU4EISE-MD5FU0RQ | BhYsXUZIUTc2CGhRdk9eIz81IChFFwMCTwIoXXkwTSBBXXMDPg0Zcn1hdGNZEwJQFwV8C1
+-----+
metens@pubsub:~$ 

```

```

metens@pubsub:~$ gcloud pubsub subscriptions pull sub-${USER} --auto-ack
+-----+
| DATA | MESSAGE_ID | ORDERING_KEY | ATTRIBUTES | DELIVERY_ATTEMPT | ACK_STATUS |
+-----+
| Message #2 | 12536115043899277 |           |           |           | SUCCESS |
+-----+
metens@pubsub:~$ 

```

15. Test programs and clean up

```
(env) metens@cloudshell:~/pub (cloud-metens)$ vim publisher.py  
[1]+  Stopped                  vim publisher.py  
(env) metens@cloudshell:~/pub (cloud-metens)$ python3 publisher.py  
Enter a message to send: Hello World!  
Published 12537239037791892 to topic projects/cloud-metens/topics/my_topic  
Enter a message to send: Message #2  
Published 12537246088049295 to topic projects/cloud-metens/topics/my_topic  
Enter a message to send: Meessage #3  
Published 12886888364888768 to topic projects/cloud-metens/topics/my_topic  
Enter a message to send: █
```

```
(env) metens@pubsub:~$ python3 subscriber.py  
Received message 12537239037791892: 2024-11-06 23:35:00 (projects/cloud-metens/topics/my_topic) : Hello World!  
Received message 12537246088049295: 2024-11-06 23:35:22 (projects/cloud-metens/topics/my_topic) : Message #2  
Received message 12886888364888768: 2024-11-06 23:35:36 (projects/cloud-metens/topics/my_topic) : Meessage #3  
█
```