Addison Wurtz
CS 530
notebooks/Week6

Lab Notebook – Week 6

Table of Contents:

06.1a: EB Guestbook
- Running the application
- Handling failures seamlessly
- Deploying the Guestbook

06.1g: App Engine Guestbook
- Deploying the Guestbook
- Handling failures seamlessly

06.2g: Cloud Run, Secret Manager (Web proxy)
- Setup secret proxy
- What is the security advantage of passing in the secret proxy route as an environment variable?
- Cloud Build and Container Registry
- Deploy to Cloud Run
- Deploy to Cloud Run with Secret Manager
- Identify the vulnerability in your lab notebook that Google has prevented.

06.3a: ECS Guestbook

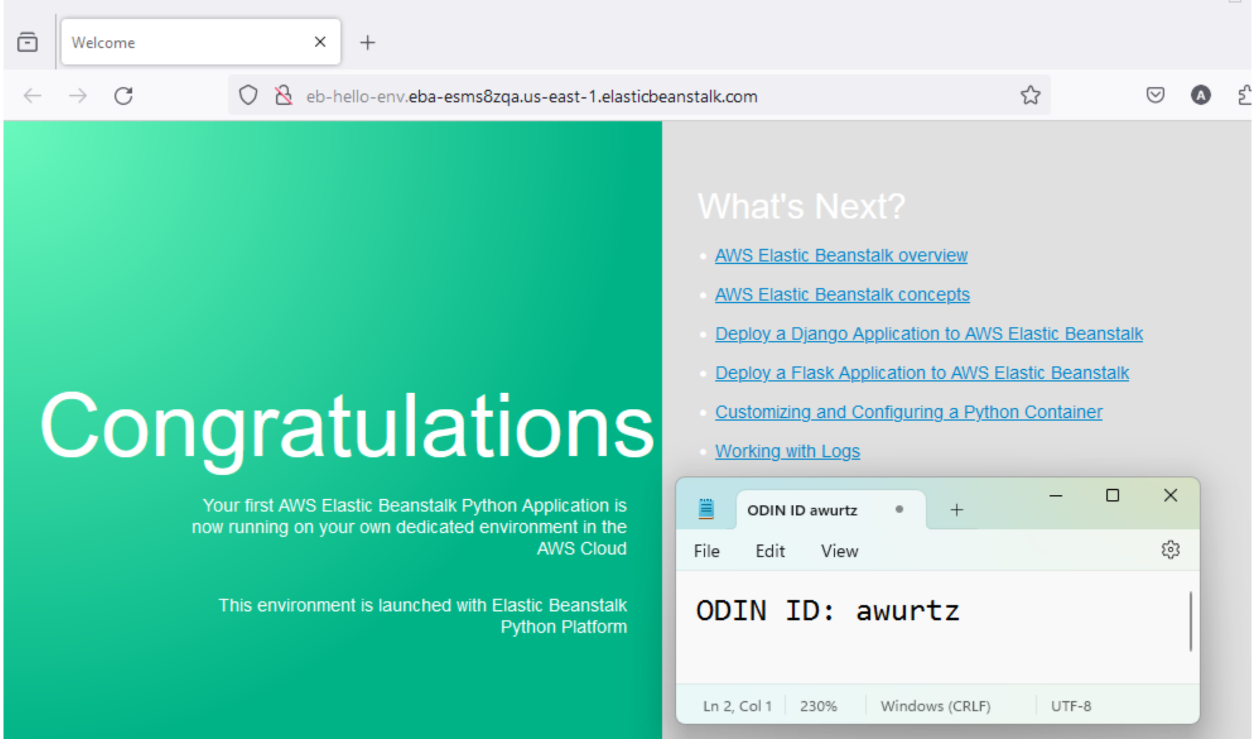
06.3g: Cloud Run Guestbook

06.4g: Cloud Functions, PubSub

Addison Wurtz
CS 530
notebooks/Week6

06.1a: EB Guestbook

Running the application



eb-hello-env.eba-esms8zqa.us-east-1.elasticbeanstalk.com

Congratulations

Your first AWS Elastic Beanstalk Python Application is now running on your own dedicated environment in the AWS Cloud

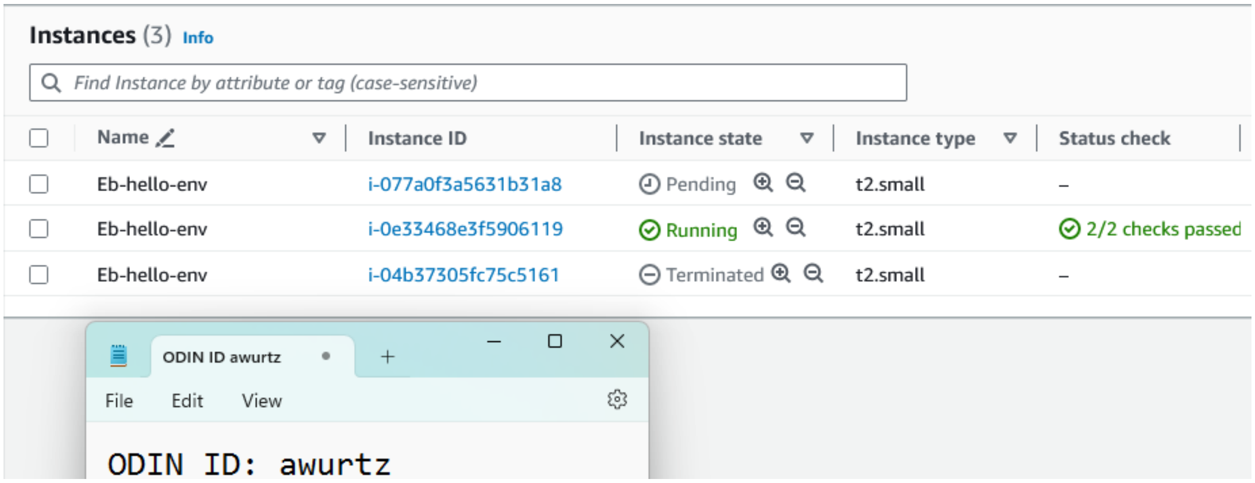
This environment is launched with Elastic Beanstalk Python Platform

What's Next?

- AWS Elastic Beanstalk overview
- AWS Elastic Beanstalk concepts
- Deploy a Django Application to AWS Elastic Beanstalk
- Deploy a Flask Application to AWS Elastic Beanstalk
- Customizing and Configuring a Python Container
- Working with Logs

```
ODIN ID: awurtz
```

Handling failures seamlessly



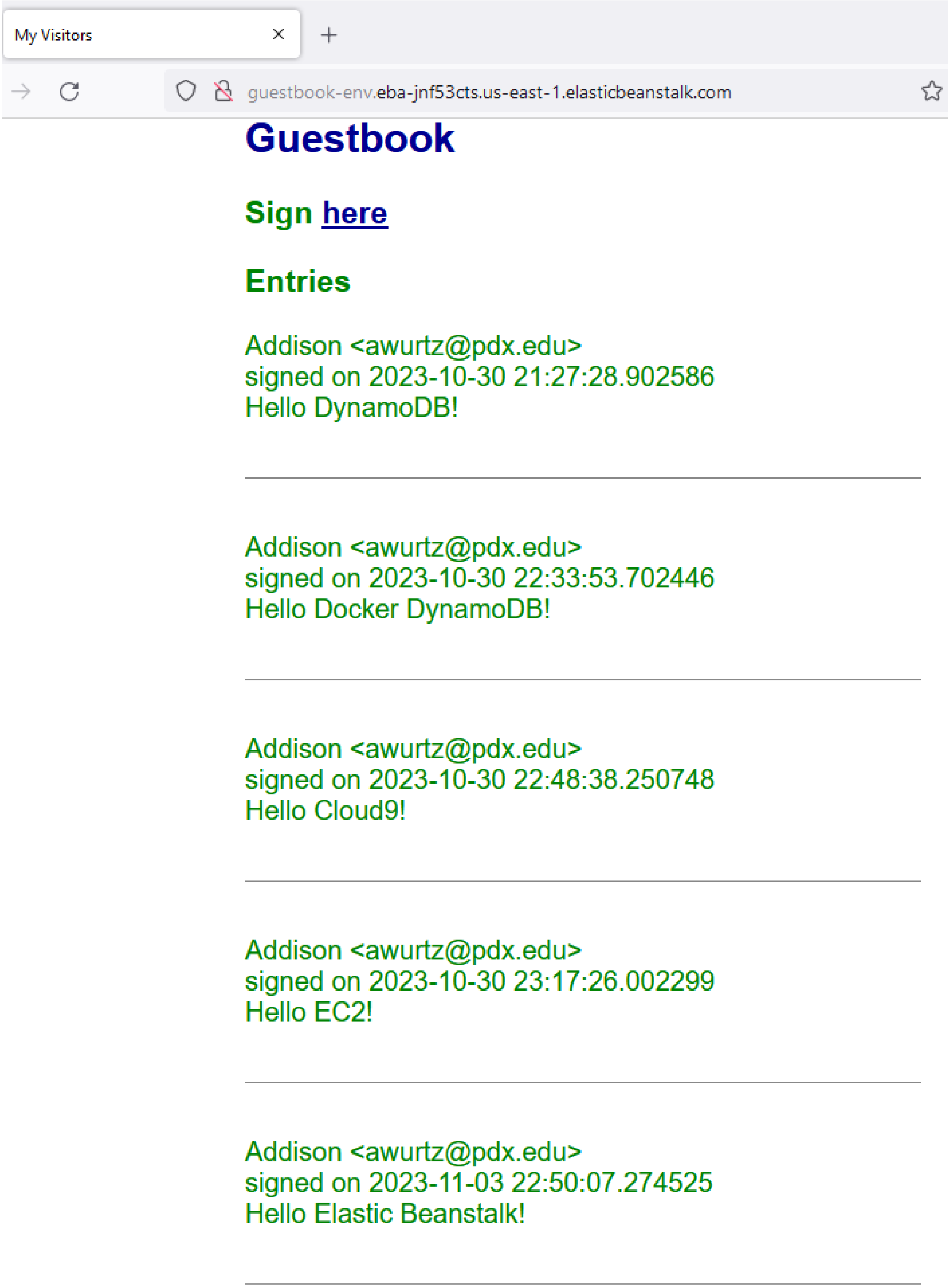
Instances (3) Info

□	Name	Instance ID	Instance state	Instance type	Status check
□	Eb-hello-env	i-077a0f3a5631b31a8	Pending	t2.small	–
□	Eb-hello-env	i-0e33468e3f5906119	Running	t2.small	2/2 checks passed
□	Eb-hello-env	i-04b37305fc75c5161	Terminated	t2.small	–

```
ODIN ID: awurtz
```

Addison Wurtz
CS 530
notebooks/Week6

Deploying the Guestbook



Guestbook

Sign here

Entries

Addison <awurtz@pdx.edu>
signed on 2023-10-30 21:27:28.902586
Hello DynamoDB!

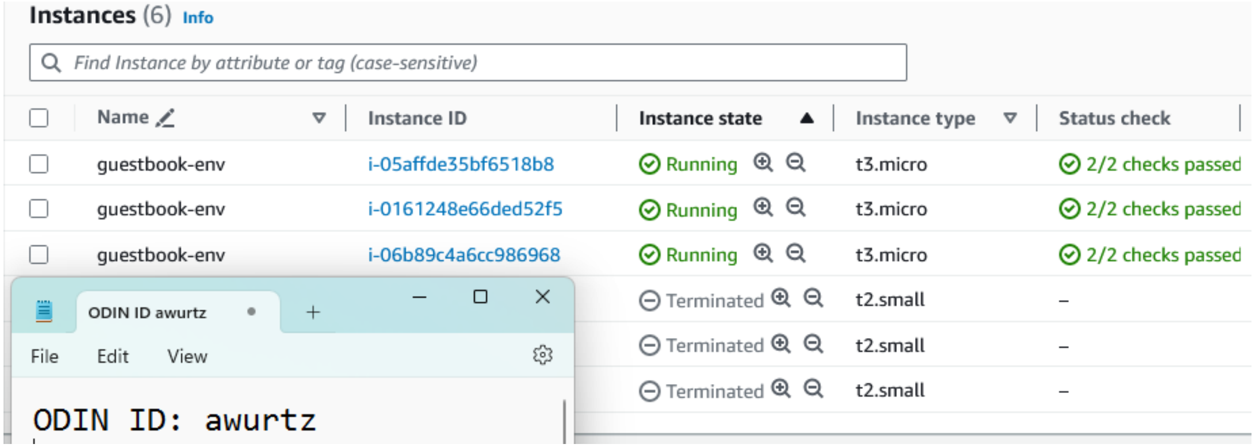
Addison <awurtz@pdx.edu>
signed on 2023-10-30 22:33:53.702446
Hello Docker DynamoDB!

Addison <awurtz@pdx.edu>
signed on 2023-10-30 22:48:38.250748
Hello Cloud9!

Addison <awurtz@pdx.edu>
signed on 2023-10-30 23:17:26.002299
Hello EC2!

Addison <awurtz@pdx.edu>
signed on 2023-11-03 22:50:07.274525
Hello Elastic Beanstalk!

Addison Wurtz
CS 530
notebooks/Week6



Instances (6) Info

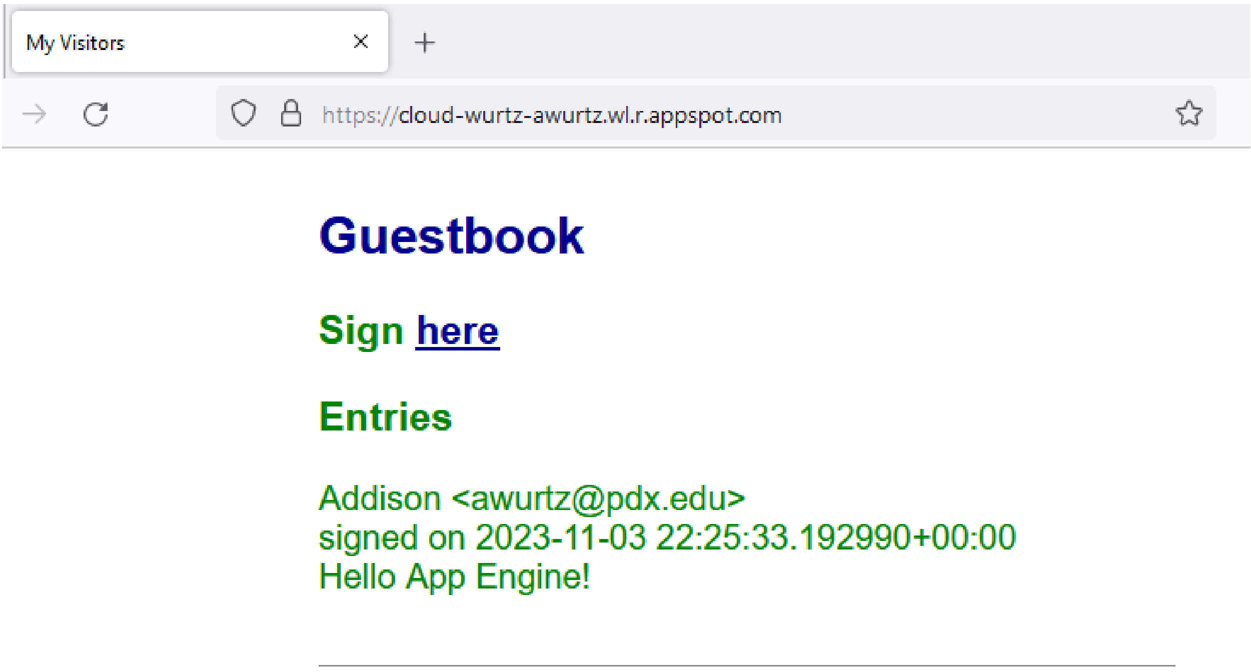
Find Instance by attribute or tag (case-sensitive)

□	Name	Instance ID	Instance state	Instance type	Status check
□	guestbook-env	i-05affde35bf6518b8	✓ Running	t3.micro	✓ 2/2 checks passed
□	guestbook-env	i-0161248e66ded52f5	✓ Running	t3.micro	✓ 2/2 checks passed
□	guestbook-env	i-06b89c4a6cc986968	✓ Running	t3.micro	✓ 2/2 checks passed
			⊖ Terminated	t2.small	–
			⊖ Terminated	t2.small	–
			⊖ Terminated	t2.small	–

```
ODIN ID: awurtz
```

06.1g: App Engine Guestbook

Deploying the Guestbook



Guestbook

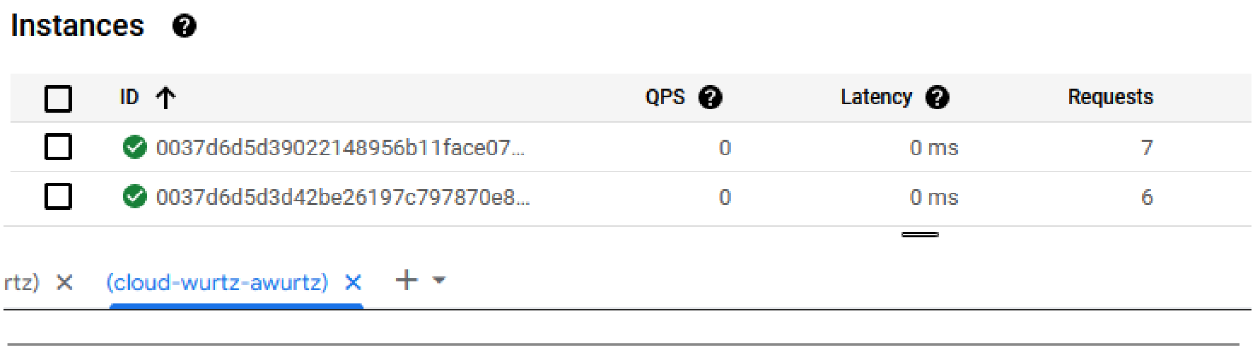
Sign here

Entries

Addison <awurtz@pdx.edu>
signed on 2023-11-03 22:25:33.192990+00:00
Hello App Engine!

Addison Wurtz
CS 530
notebooks/Week6

Handling failures seamlessly

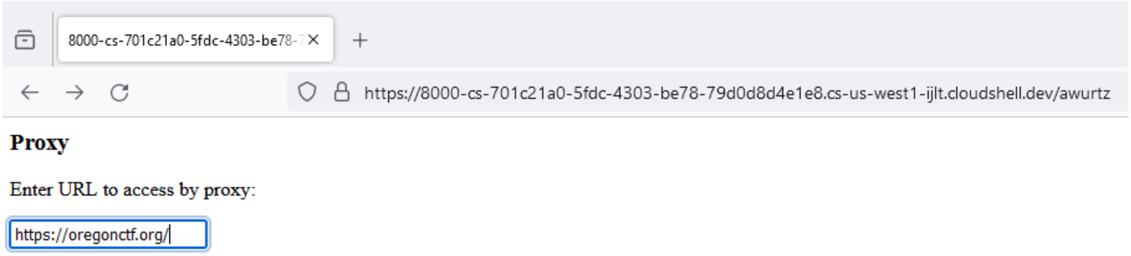


Instances ?

□	ID ↑	QPS ?	Latency ?	Requests
□	✓ 0037d6d5d39022148956b11face07...	0	0 ms	7
□	✓ 0037d6d5d3d42be26197c797870e8...	0	0 ms	6

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

Setup secret proxy

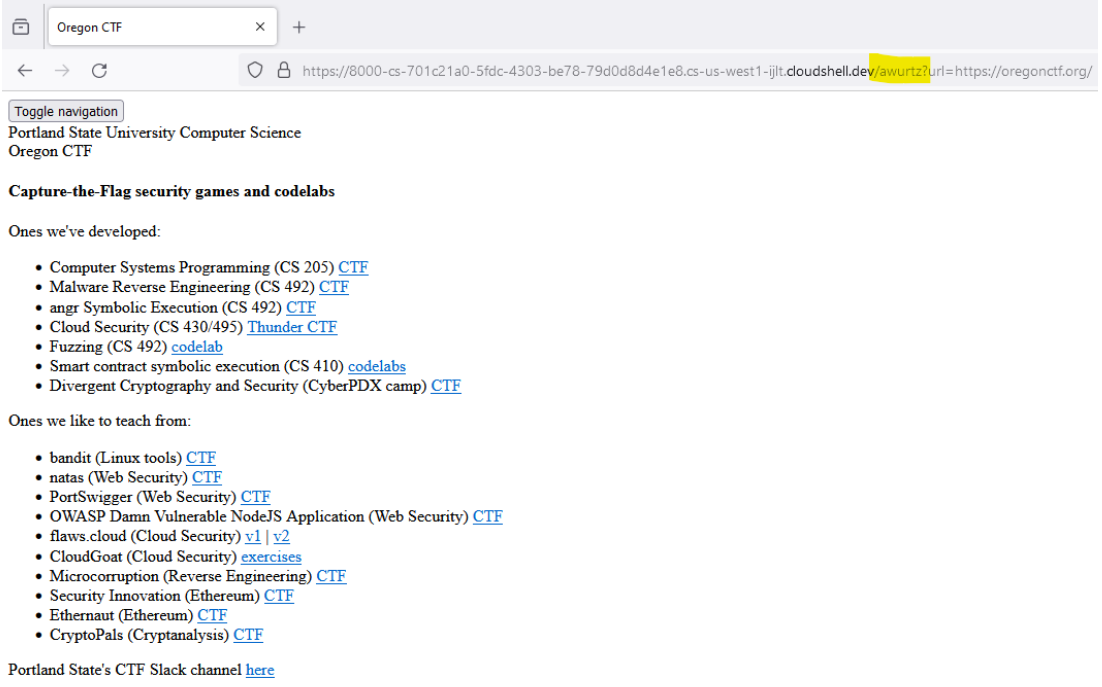


8000-cs-701c21a0-5fdc-4303-be78-
https://8000-cs-701c21a0-5fdc-4303-be78-79d0d8d4e1e8.cs-us-west1-ijlt.cloudshell.dev/awurtz

Proxy

Enter URL to access by proxy:

https://oregonctf.org/



Oregon CTF
https://8000-cs-701c21a0-5fdc-4303-be78-79d0d8d4e1e8.cs-us-west1-ijlt.cloudshell.dev/awurtz?url=https://oregonctf.org/
Toggle navigation

Portland State University Computer Science
Oregon CTF

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
- Ethernaut (Ethereum) CTF
- CryptoPals (Cryptanalysis) CTF

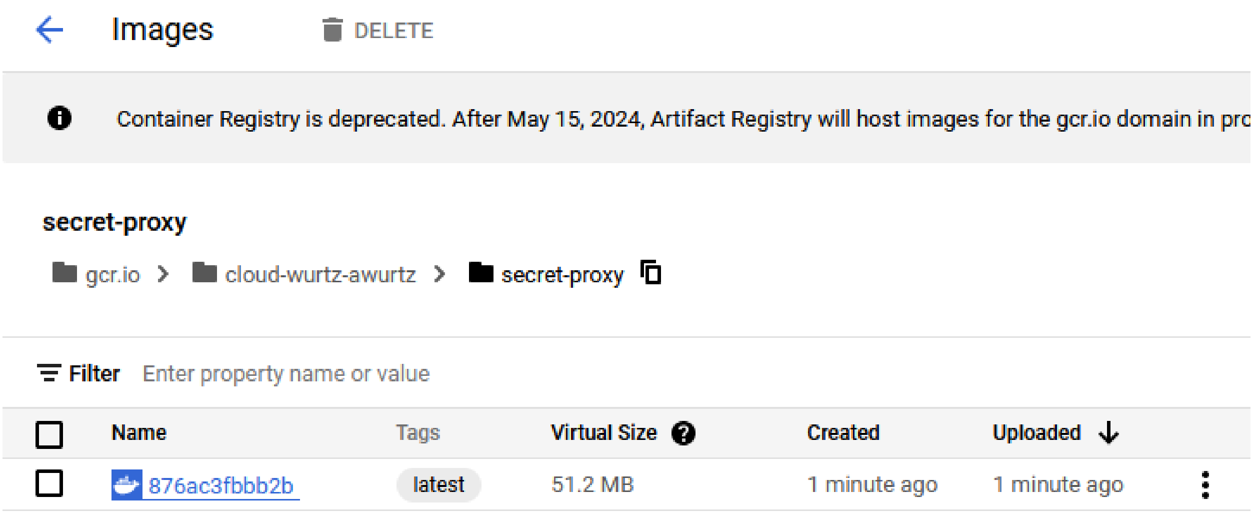
Portland State's CTF Slack channel here

Addison Wurtz
CS 530
notebooks/Week6

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

Passing the secret proxy route as an environment variable means that you don't have to include the secret in the docker image. This means you can share the docker image publicly without revealing your secrets.

Cloud Build and Container Registry



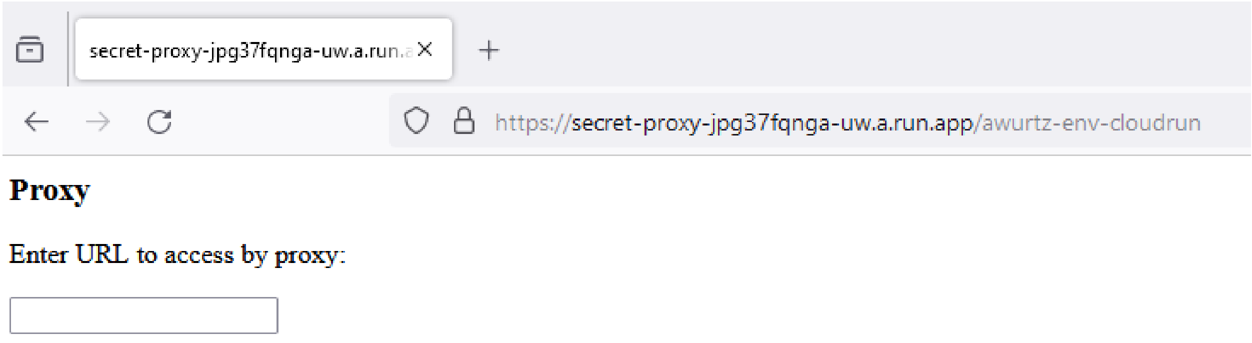
Container Registry is deprecated. After May 15, 2024, Artifact Registry will host images for the gcr.io domain in pro

secret-proxy

gcr.io > cloud-wurtz-awurtz > secret-proxy

□	Name	Tags	Virtual Size	Created	Uploaded
□	876ac3fbbb2b	latest	51.2 MB	1 minute ago	1 minute ago

Deploy to Cloud Run

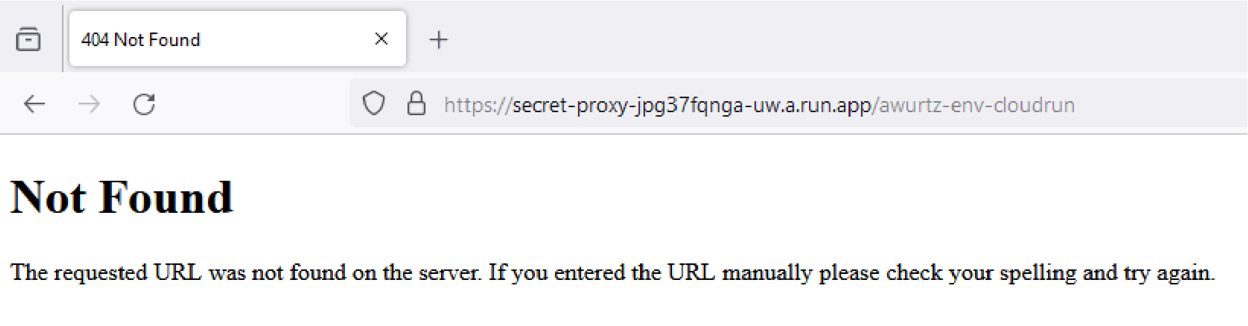


https://secret-proxy-jpg37fqnga-uw.a.run.app/awurtz-env-cloudrun

Proxy

Enter URL to access by proxy:

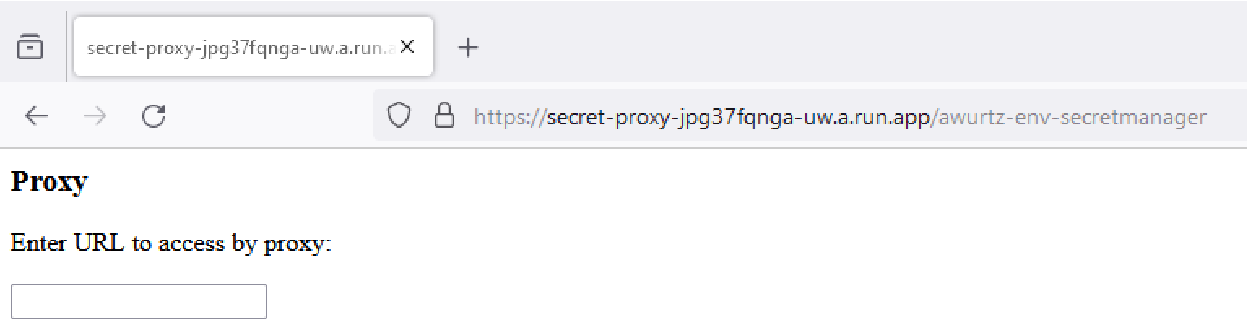
Addison Wurtz
CS 530
notebooks/Week6


404 Not Found
https://secret-proxy-jpg37fqnga-uw.a.run.app/awurtz-env-cloudrun

Not Found

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

Deploy to Cloud Run with Secret Manager


secret-proxy-jpg37fqnga-uw.a.run.a
https://secret-proxy-jpg37fqnga-uw.a.run.app/awurtz-env-secretmanager

Proxy

Enter URL to access by proxy:

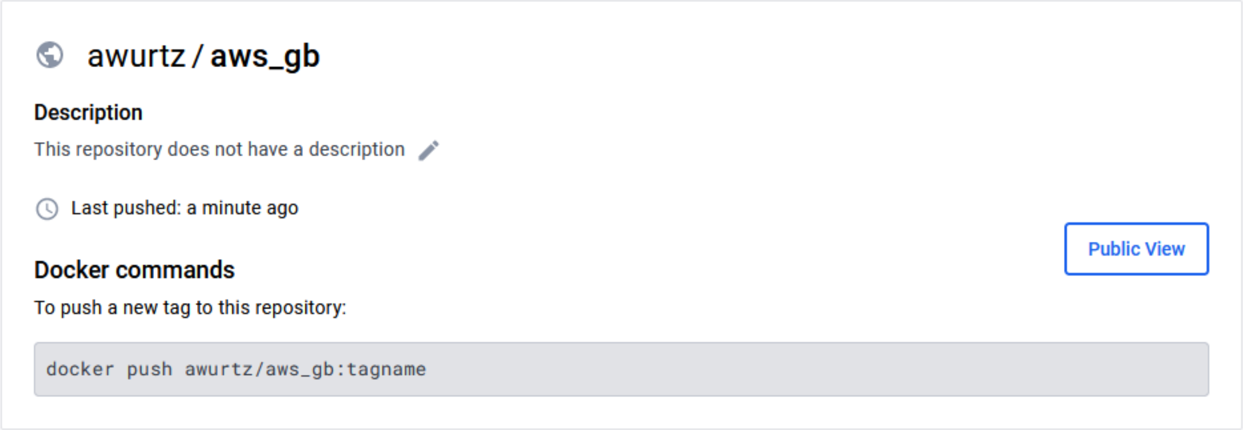
Identify the vulnerability in your lab notebook that Google has prevented.

Google prevented an SSRF (Server Side Request Forgery)

Addison Wurtz
CS 530
notebooks/Week6

06.3a: ECS Guestbook

Preparing the container image



awurtz / aws_gb

Description

This repository does not have a description

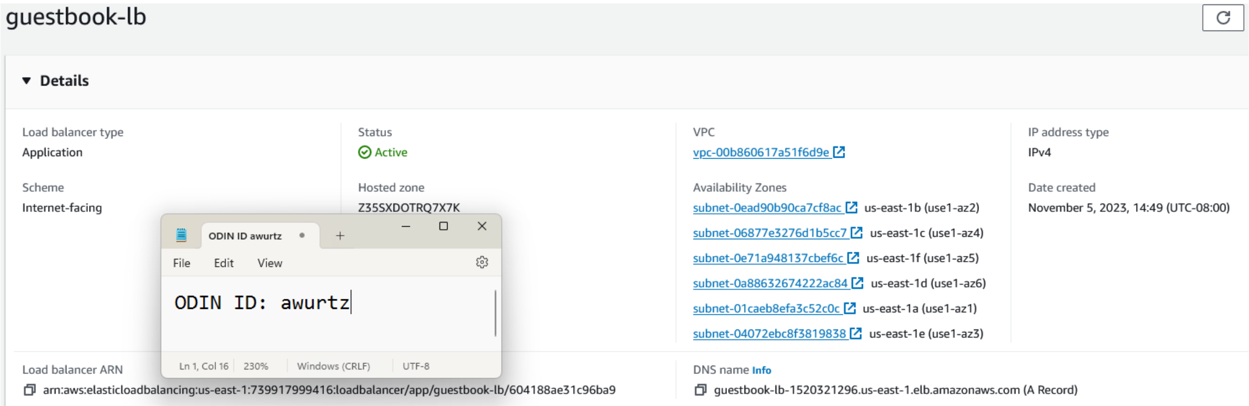
Last pushed: a minute ago

Docker commands

To push a new tag to this repository:

```
docker push awurtz/aws_gb:tagname
```

Examine the service



guestbook-lb

▼ **Details**

Load balancer type
Application

Scheme
Internet-facing

Status
Active

Hosted zone
Z35SXDOTRQ7X7K

VPC
vpc-00b860617a51f6d9e

Availability Zones
subnet-0ead90b90ca7cf8ac us-east-1b (use1-az2)
subnet-06877e3276d1b5cc7 us-east-1c (use1-az4)
subnet-0e71a948137cbef6c us-east-1f (use1-az5)
subnet-0a88632674222ac84 us-east-1d (use1-az6)
subnet-01caeb8efa3c52c0c us-east-1a (use1-az1)
subnet-04072ebc8f3819838 us-east-1e (use1-az3)

IP address type
IPv4

Date created
November 5, 2023, 14:49 (UTC-08:00)

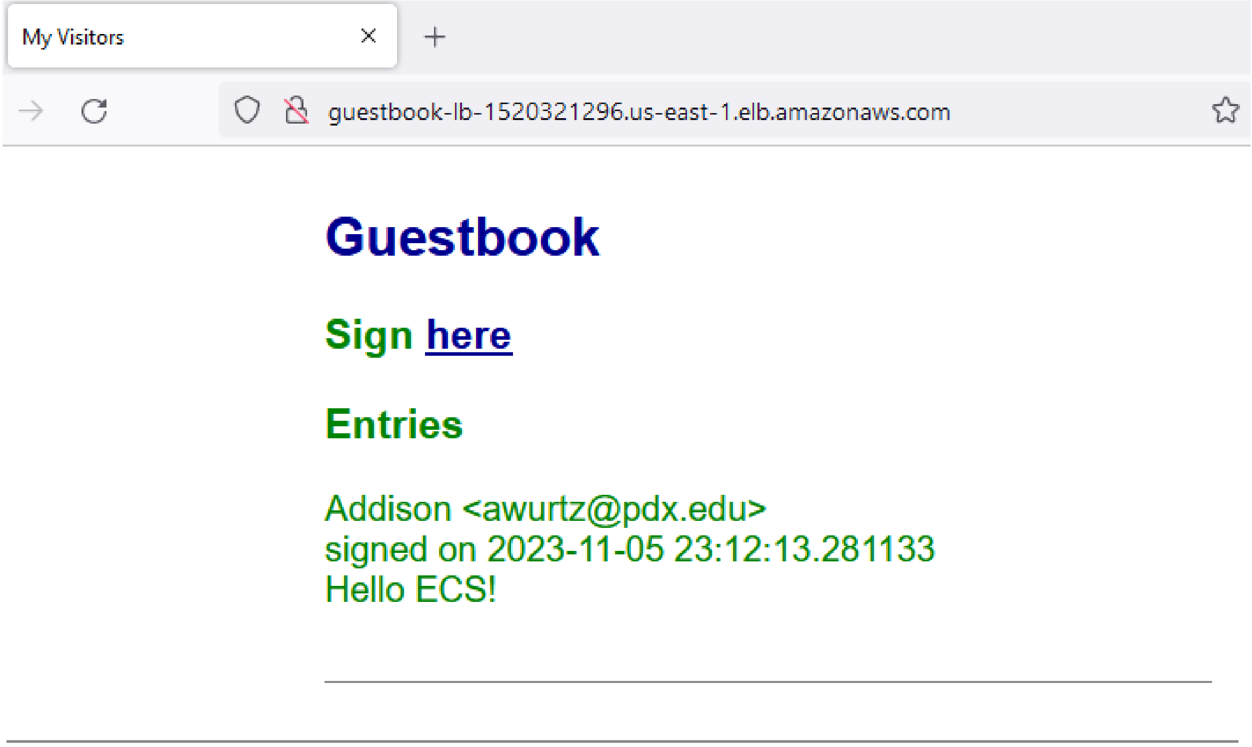
Load balancer ARN
arn:aws:elasticloadbalancing:us-east-1:739917999416:loadbalancer/app/guestbook-lb/604188ae31c96ba9

DNS name Info
guestbook-lb-1520321296.us-east-1.elb.amazonaws.com (A Record)

ODIN ID: awurtz

Addison Wurtz
CS 530
notebooks/Week6

Visit the site



Guestbook

Sign here

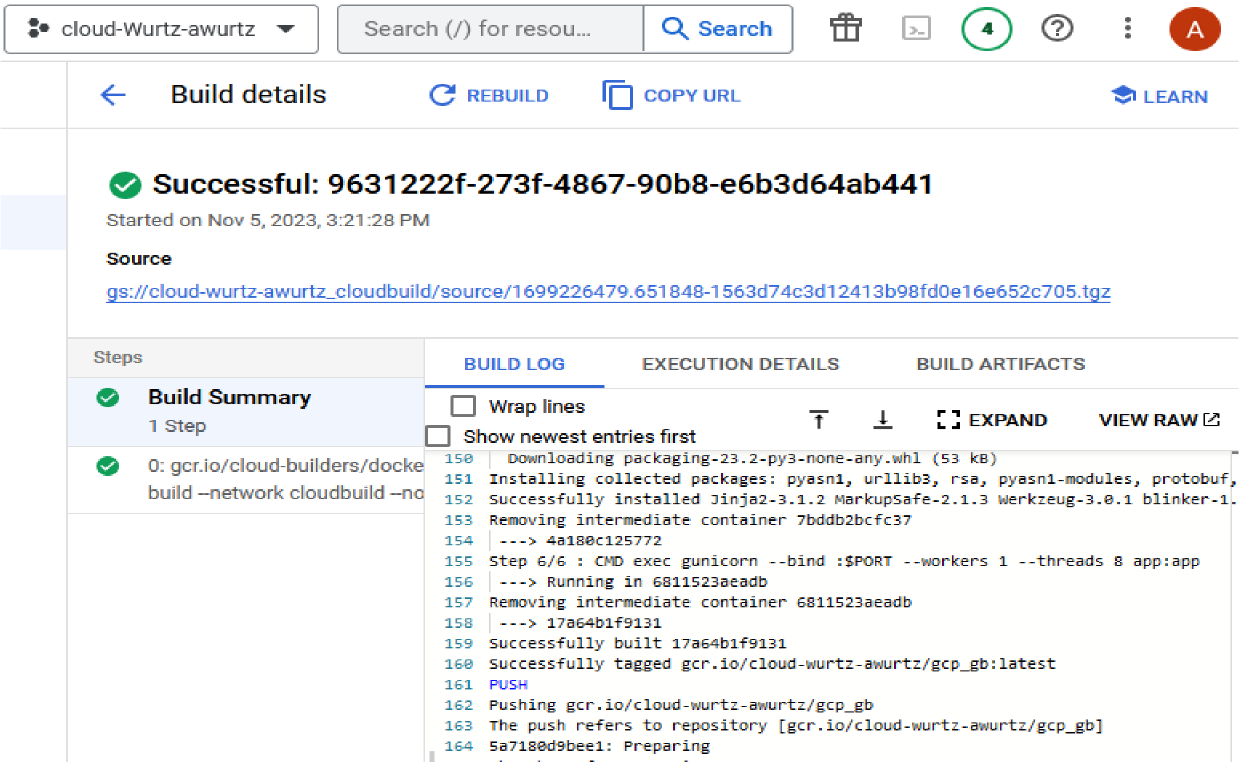
Entries

Addison <awurtz@pdx.edu>
signed on 2023-11-05 23:12:13.281133
Hello ECS!

Addison Wurtz
CS 530
notebooks/Week6

06.3g: Cloud Run Guestbook

Prepare a container image



Successful: 9631222f-273f-4867-90b8-e6b3d64ab441

Started on Nov 5, 2023, 3:21:28 PM

Source

gs://cloud-wurtz-awurtz_cloudbuild/source/1699226479.651848-1563d74c3d12413b98fd0e16e652c705.tgz

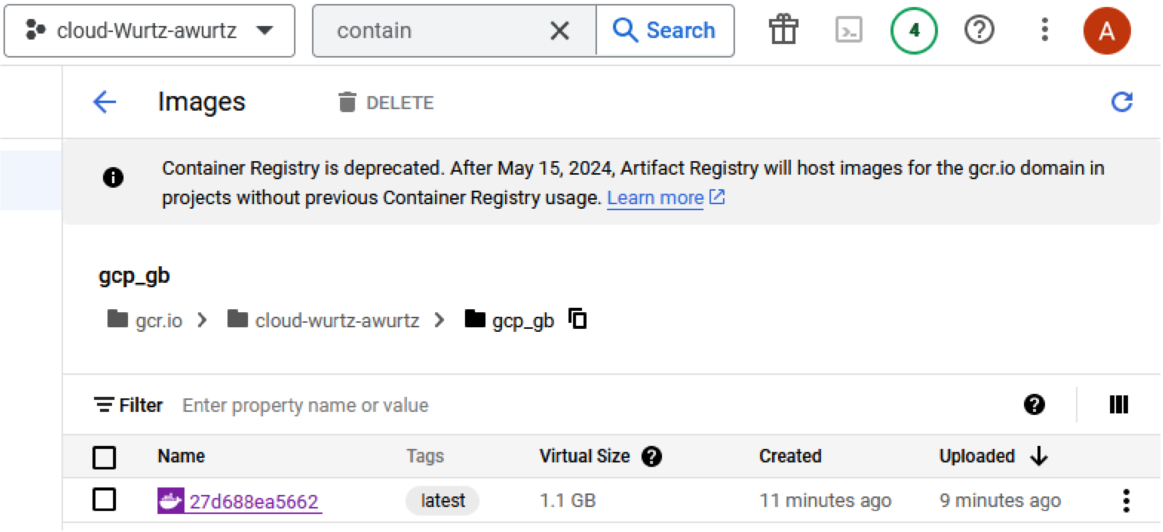
Build Summary
1 Step

0: gcr.io/cloud-builders/docke
build --network cloudbuild --no

☐ Wrap lines
☐ Show newest entries first

```
  Downloading packaging-23.2-py3-none-any.whl (53 kB)
Installing collected packages: pyasn1, urllib3, rsa, pyasn1-modules, protobuf,
Successfully installed Jinja2-3.1.2 MarkupSafe-2.1.3 Werkzeug-3.0.1 blinker-1.
Removing intermediate container 7bddb2bcfc37
 ---> 4a180c125772
Step 6/6 : CMD exec gunicorn --bind :$PORT --workers 1 --threads 8 app:app
 ---> Running in 6811523aeadb
Removing intermediate container 6811523aeadb
 ---> 17a64b1f9131
Successfully built 17a64b1f9131
Successfully tagged gcr.io/cloud-wurtz-awurtz/gcp_gb:latest
PUSH
Pushing gcr.io/cloud-wurtz-awurtz/gcp_gb
The push refers to repository [gcr.io/cloud-wurtz-awurtz/gcp_gb]
5a7180d9bee1: Preparing
```

View container image



Container Registry is deprecated. After May 15, 2024, Artifact Registry will host images for the gcr.io domain in projects without previous Container Registry usage. Learn more

gcp_gb

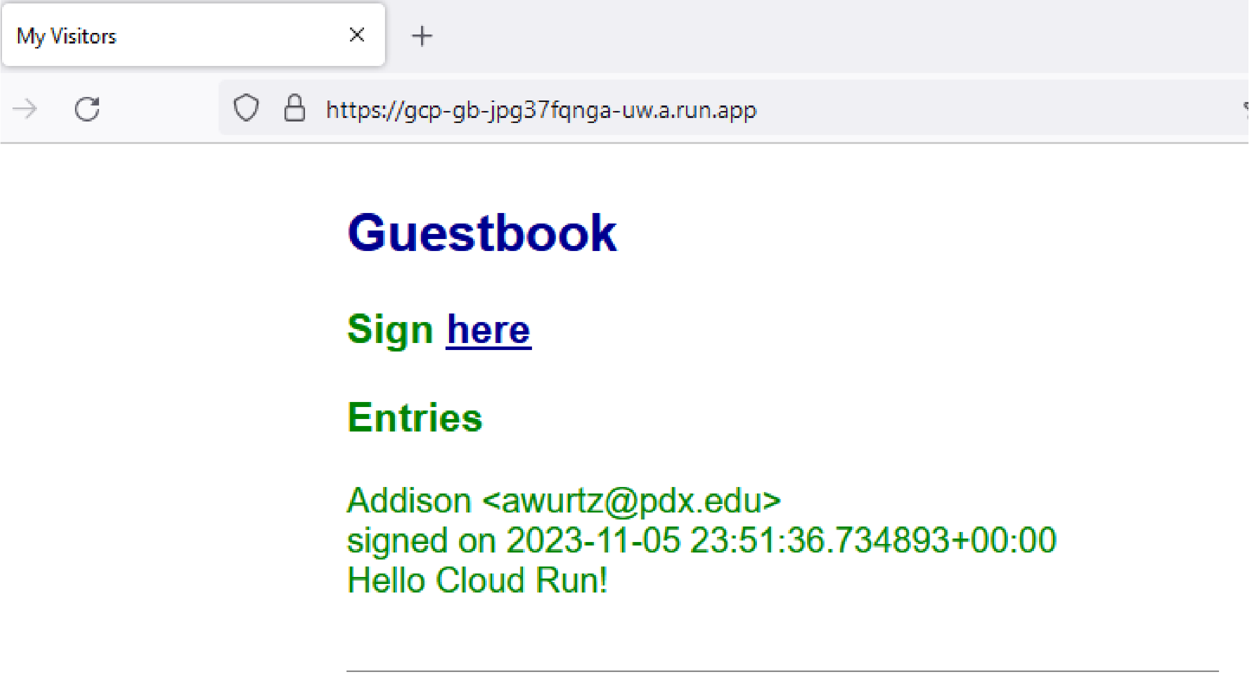
gcr.io > cloud-wurtz-awurtz > gcp_gb

Filter Enter property name or value

☐	Name	Tags	Virtual Size	Created	Uploaded
☐	27d688ea5662	latest	1.1 GB	11 minutes ago	9 minutes ago

Addison Wurtz
CS 530
notebooks/Week6

View the Guestbook



https://gcp-gb-jpg37fqnga-uw.a.run.app

Guestbook

Sign here

Entries

Addison <awurtz@pdx.edu>
signed on 2023-11-05 23:51:36.734893+00:00
Hello Cloud Run!

What port do container instances listen on?

8080

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

100

06.4g: Cloud Functions, PubSub

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

In a temporary local file.

Addison Wurtz
CS 530
notebooks/Week6

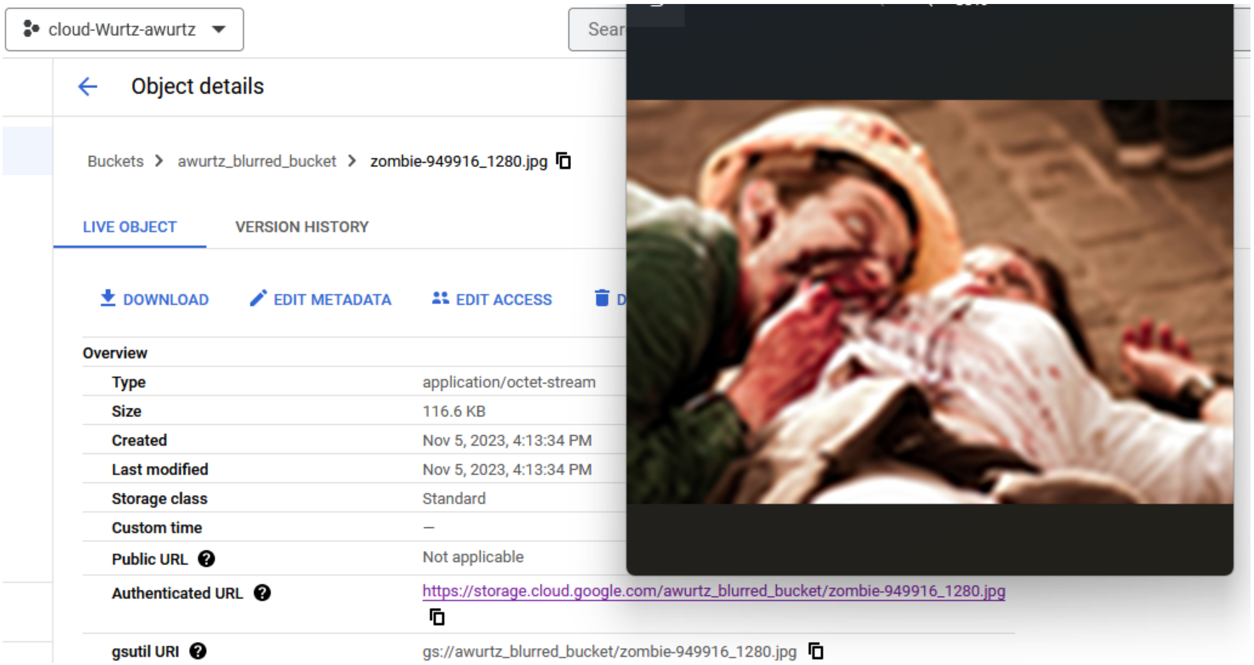
What class in the ImageMagick package is used to do the blurring of the file?

The Image class is used to blur the file.

What lines of code perform the blurring of the image and its storage back into the file system?

Lines 72-74 blur the image and save it to a temporary local file. Lines 81-84 upload the image to a storage bucket for blurred images.

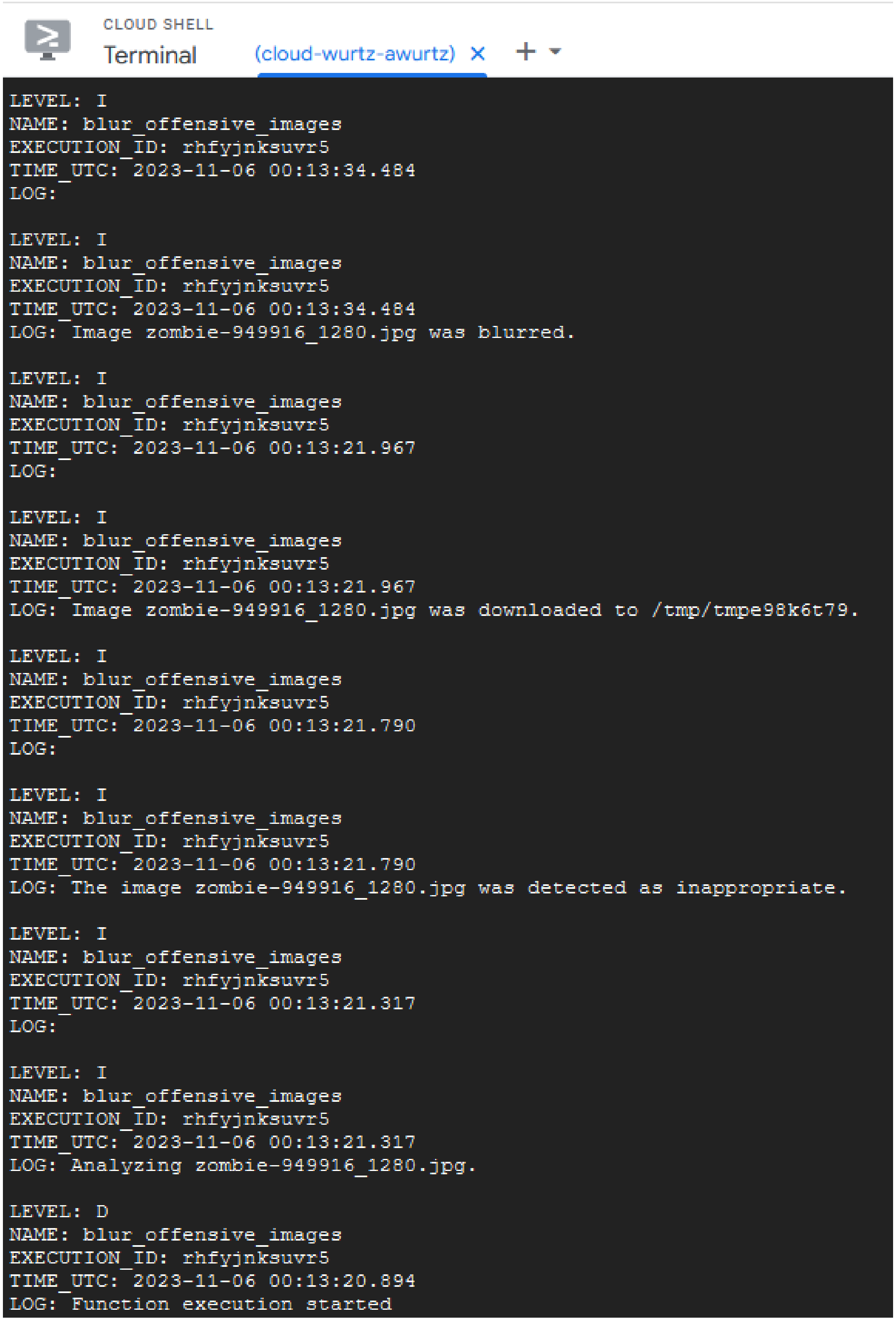
Test function



Overview

Type	application/octet-stream
Size	116.6 KB
Created	Nov 5, 2023, 4:13:34 PM
Last modified	Nov 5, 2023, 4:13:34 PM
Storage class	Standard
Custom time	—
Public URL	Not applicable
Authenticated URL	https://storage.cloud.google.com/awurtz_blurred_bucket/zombie-949916_1280.jpg
gsutil URI	gs://awurtz_blurred_bucket/zombie-949916_1280.jpg

Addison Wurtz
CS 530
notebooks/Week6



```
LEVEL: I
NAME: blur_offensive_images
EXECUTION_ID: rhfyjnksuvr5
TIME_UTC: 2023-11-06 00:13:34.484
LOG:

LEVEL: I
NAME: blur_offensive_images
EXECUTION_ID: rhfyjnksuvr5
TIME_UTC: 2023-11-06 00:13:34.484
LOG: Image zombie-949916_1280.jpg was blurred.

LEVEL: I
NAME: blur_offensive_images
EXECUTION_ID: rhfyjnksuvr5
TIME_UTC: 2023-11-06 00:13:21.967
LOG:

LEVEL: I
NAME: blur_offensive_images
EXECUTION_ID: rhfyjnksuvr5
TIME_UTC: 2023-11-06 00:13:21.967
LOG: Image zombie-949916_1280.jpg was downloaded to /tmp/tmpe98k6t79.

LEVEL: I
NAME: blur_offensive_images
EXECUTION_ID: rhfyjnksuvr5
TIME_UTC: 2023-11-06 00:13:21.790
LOG:

LEVEL: I
NAME: blur_offensive_images
EXECUTION_ID: rhfyjnksuvr5
TIME_UTC: 2023-11-06 00:13:21.790
LOG: The image zombie-949916_1280.jpg was detected as inappropriate.

LEVEL: I
NAME: blur_offensive_images
EXECUTION_ID: rhfyjnksuvr5
TIME_UTC: 2023-11-06 00:13:21.317
LOG:

LEVEL: I
NAME: blur_offensive_images
EXECUTION_ID: rhfyjnksuvr5
TIME_UTC: 2023-11-06 00:13:21.317
LOG: Analyzing zombie-949916_1280.jpg.

LEVEL: D
NAME: blur_offensive_images
EXECUTION_ID: rhfyjnksuvr5
TIME_UTC: 2023-11-06 00:13:20.894
LOG: Function execution started
```

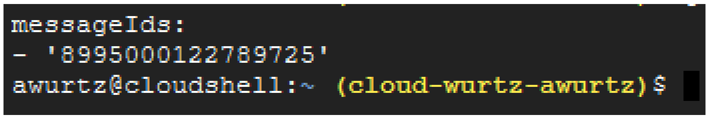
Addison Wurtz
CS 530
notebooks/Week6

PubSub via CLI

Why are no items returned?

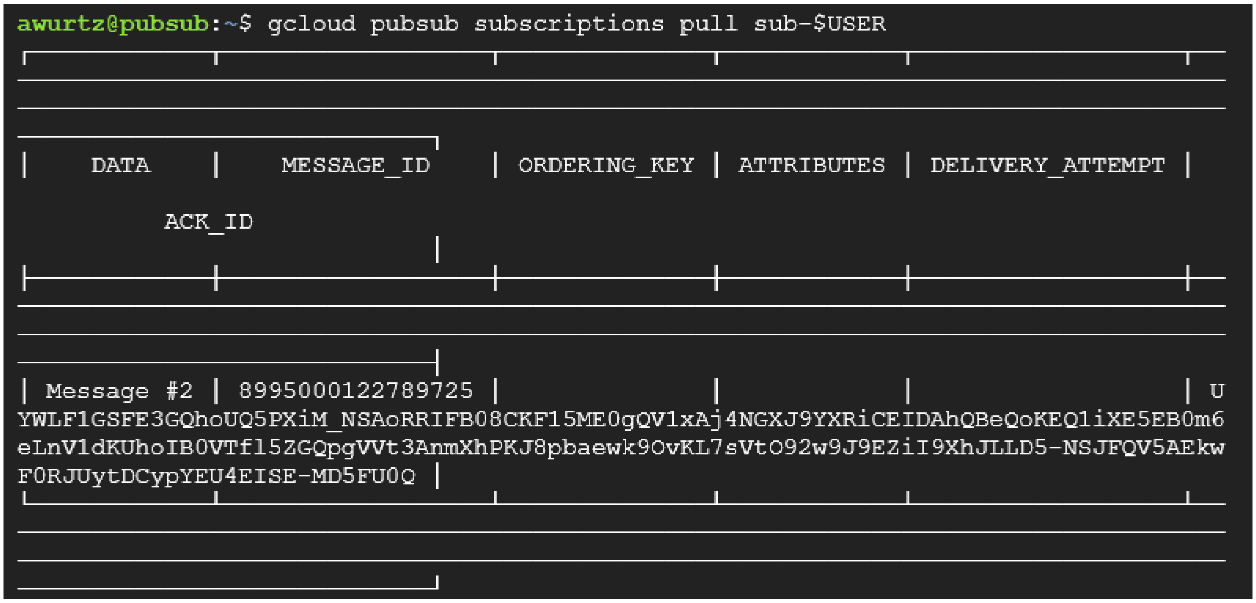
Because when the first message was created there were no subscribers, so the message was deleted.

What is the `messageId` of the published message?



```
messageIds:
- '8995000122789725'
awurtz@cloudshell:~ (cloud-wurtz-awurtz)$
```

Screenshot of the output of successful pull that includes the message and its `messageId`



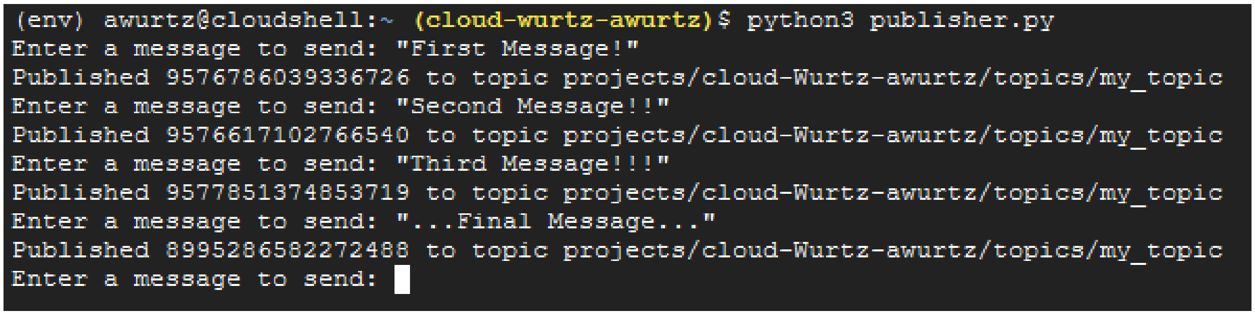
```
awurtz@pubsub:~$ gcloud pubsub subscriptions pull sub-$USER
┌─────────────┬──────────────────┬──────────────┬─────────────┬──────────────────┬──
────────────────────────────────────────────────────────────────────────────────────
────────────────────────────────────────────────────────────────────────────────────
──────────────────────────────┐
│    DATA     │    MESSAGE_ID    │ ORDERING_KEY │ ATTRIBUTES  │ DELIVERY_ATTEMPT │

          ACK_ID
                              │
├─────────────┼──────────────────┼──────────────┼─────────────┼──────────────────┼──
────────────────────────────────────────────────────────────────────────────────────
────────────────────────────────────────────────────────────────────────────────────
──────────────────────────────┤
│ Message #2 │ 8995000122789725 │              │             │                  │ U
YWLF1GSFE3GQhoUQ5PXiM_NSAoRRIFB08CKF15ME0gQV1xAj4NGXJ9YXRiCEIDAhQBeQoKEQ1iXE5EB0m6
eLnV1dKUhoIB0VTfl5ZGQpgVVt3AnmXhPKJ8pbaewk9OvKL7sVtO92w9J9EZiI9XhJLLD5-NSJFQV5AEkw
F0RJUytDCypYEU4EISE-MD5FU0Q │
└─────────────┴──────────────────┴──────────────┴─────────────┴──────────────────┴──
────────────────────────────────────────────────────────────────────────────────────
────────────────────────────────────────────────────────────────────────────────────
──────────────────────────────┘
```

Addison Wurtz
CS 530
notebooks/Week6

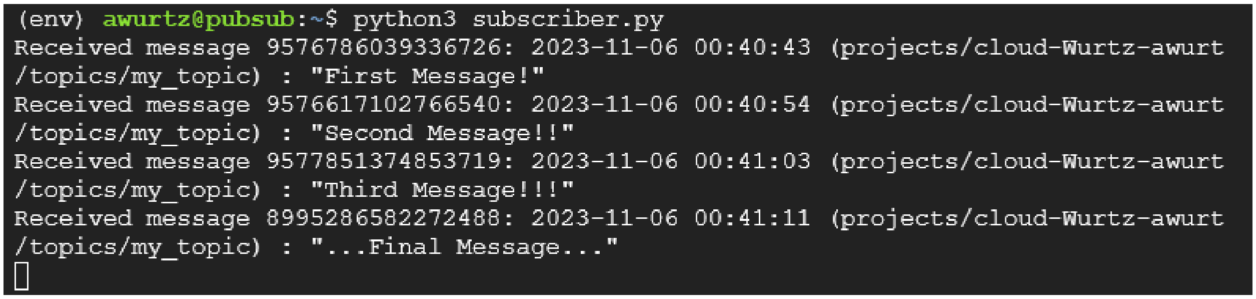
Test Programs

Messages Sent



```
(env) awurtz@cloudshell:~ (cloud-wurtz-awurtz)$ python3 publisher.py
Enter a message to send: "First Message!"
Published 9576786039336726 to topic projects/cloud-Wurtz-awurtz/topics/my_topic
Enter a message to send: "Second Message!!"
Published 9576617102766540 to topic projects/cloud-Wurtz-awurtz/topics/my_topic
Enter a message to send: "Third Message!!!"
Published 9577851374853719 to topic projects/cloud-Wurtz-awurtz/topics/my_topic
Enter a message to send: "...Final Message..."
Published 8995286582272488 to topic projects/cloud-Wurtz-awurtz/topics/my_topic
Enter a message to send:
```

Messages Received



```
(env) awurtz@pubsub:~$ python3 subscriber.py
Received message 9576786039336726: 2023-11-06 00:40:43 (projects/cloud-Wurtz-awurt
/topics/my_topic) : "First Message!"
Received message 9576617102766540: 2023-11-06 00:40:54 (projects/cloud-Wurtz-awurt
/topics/my_topic) : "Second Message!!"
Received message 9577851374853719: 2023-11-06 00:41:03 (projects/cloud-Wurtz-awurt
/topics/my_topic) : "Third Message!!!"
Received message 8995286582272488: 2023-11-06 00:41:11 (projects/cloud-Wurtz-awurt
/topics/my_topic) : "...Final Message..."
```