SRM INSTITUTE OF SCIENCE & TECHNOLOGY
FACULTY OF ENGINEERING & TECHNOLOGY
SCHOOL OF COMPUTING

DEPARTMENT OF SOFTWARE ENGINEERING
SUBJECT CODE: 15SE376L-MINOR PROJECT

Topic Name: Detecting app's vulnerabilities on cloud platform

NAME : Prithish Ghosh (RA1711020010165) **Harsh J Shah(RA1711020010131)**

SEMESTER : 7th **Faculty : Siva R**

Abstract :

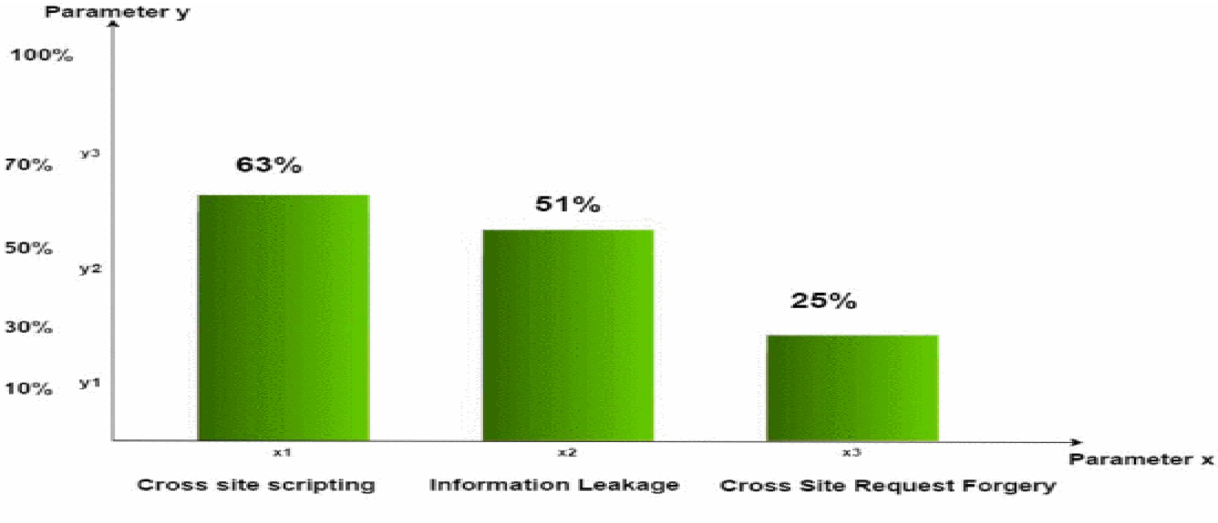
The approach of cloud computing signifies a outlook changes in traditional computing system frameworks. It is one of the present most energizing innovation because of its capacity to lessen costs related with registering while at the same time expanding adaptability also versatility for pc measures. Associations have communicated worry about basics issues (for example: security, internal structure issue) that exists with the far-reaching execution of cloud computing. These sorts of concern begin from the way is information stored remotely from the user's location. In this project two methodologies are adopted & utilized. These are deployed app to cloud, web scanning and detection of vulnerabilities with various user's working in the cloud platform. Furthermore two of such security threats, data loss prevention, leak of data & insecure application programming interfaces that are duly reviewed and detection proposed in this project.

Introduction:

Web security is an important aspect for web applications. Today web security is a real concern related to the Internet. It is considered as the principle framework for the worldwide data society. Web applications provide a better interface for a client through a web page. The web page script gets executed on client web browser.

Web applications are a main base of attacks such as cross-site scripting, cookie-session theft, browser attack, self-propagating worms in web email and web sites. These types of attacks are called '**injection attacks'** which attacks by the use of malicious code. Injection attacks have commanded the highest point of web application vulnerability lists for a significant part of the previous decade.

There are two most common security vulnerabilities today: SQL injection and cross-site scripting. A security evaluation of application prevent center, which had more than 250 e-commerce applications, online banking and the corporate sites came up with a statement that more than 85% of web applications are vulnerable to attacks.



Percentage of websites containing the Vulnerabilities

Domain Study:

We observed the security measures and it’s difficulty for internal mechanism while accessing app’s functionality so we would like to go with “security domain”.

Cloud computing is the delivery of on-demand computing services -- from applications to storage and processing power -- typically over the internet and on a pay-as-you-go basis.

Cloud computing services cover a vast range of options now, from the basics of storage, networking, and processing power through to natural language processing and artificial intelligence as well as standard office applications.

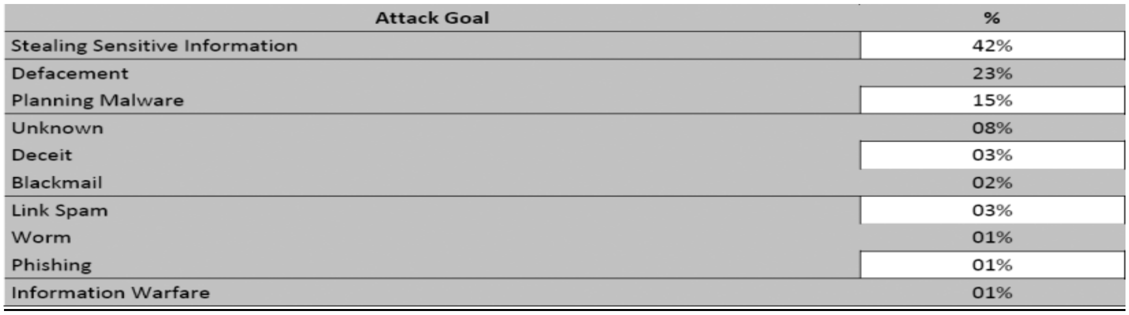
One benefit of using cloud computing services is that firms can avoid the upfront cost and complexity of owning and maintaining their own IT infrastructure, and instead simply pay for what they use, when they use it.

Literature Survey :

The main issue in web security research is in enabling a user a safe and trusted platform for communication with the web application. But some people continue to do business with insecure site. Some organizations or companies don't want to reveal the information about their own security holes. So, it's very hard task to get the reliable information about the state of web security today.

There are two common important security vulnerabilities today: SQL injection and cross-site scripting. These types of vulnerabilities directly affect web servers, application servers, and web application environment.

OWASP in this paper explores a number of Table : Reasons for Attacks methods for detecting threats and assess why they have not proven more successful. A better mechanism for minimizing such type of web vulnerabilities is proposed in this paper. Currently, there are many privacy risks in web applications. Today too many websites are hacked by anonymous people. They target website because of different types of reasons. They are mentioned in table.

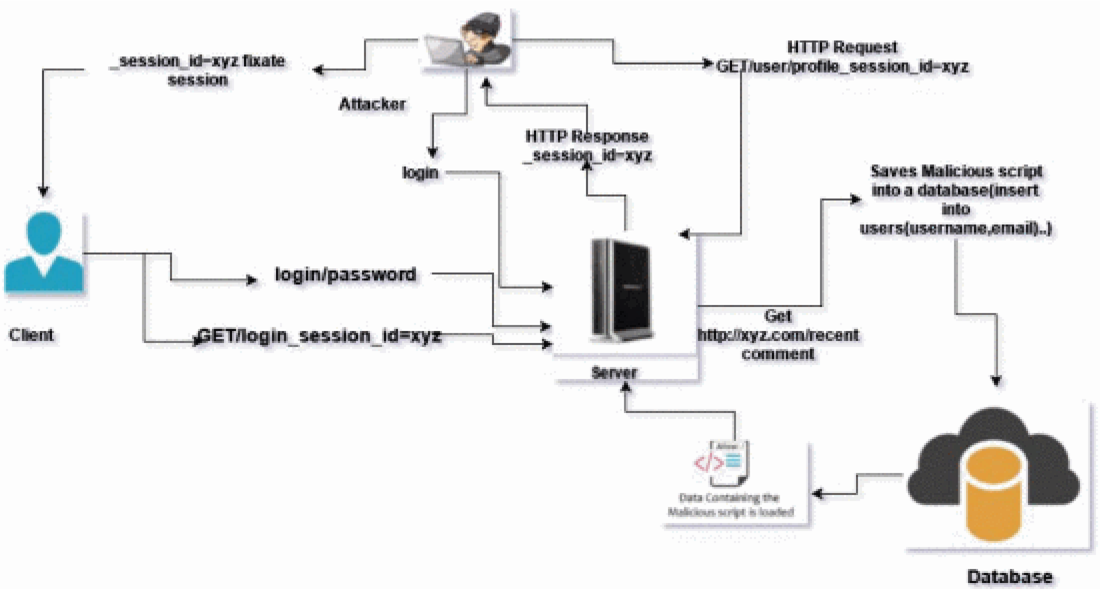


Attack Goal	%
Stealing Sensitive Information	42%
Defacement	23%
Planning Malware	15%
Unknown	08%
Deceit	03%
Blackmail	02%
Link Spam	03%
Worm	01%
Phishing	01%
Information Warfare	01%

Problem Statement

To identify the vulnerabilities of the website/app for the purpose of improving the security features and creating a blockchain based functionality. Website/app is made for the registration of the certain system information which contains the personal details of the individual & working mechanism (i.e. storage, cloud , internal database , files etc)security scan is performed on the sample app which is created of our own using Google Cloud shell and python documentation which can sent through web server and deploy through cloud environment's security scanner which will show us the vulnerability description.

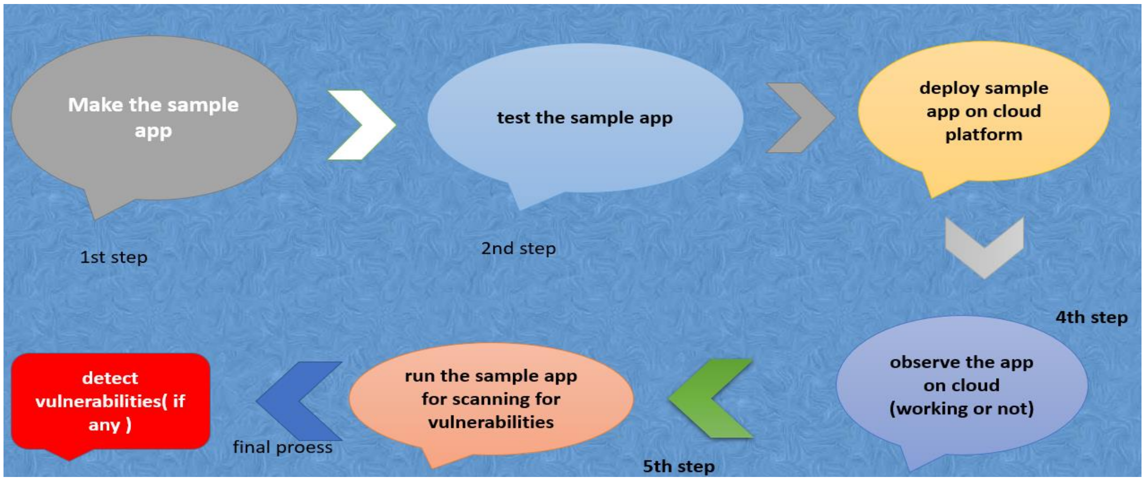
Proposed Architecture and Frame for Detecting Security Vulnerabilities:

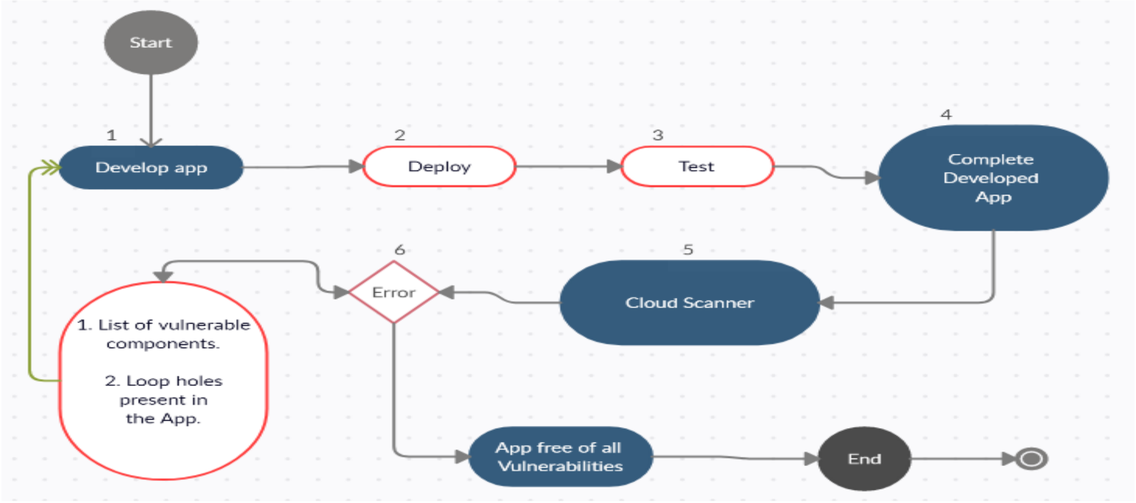

_session_id=xyz fixate session
Attacker
HTTP Request GET/user/profile_session_id=xyz
HTTP Response _session_id=xyz
login
Saves Malicious script into a database(insert into users(username,email)..)
Client
login/password
GET/login_session_id=xyz
Server
Get http://xyz.com/recent comment
Data Containing the Malicious script is loaded
Database

Objective of our Work:

1. The project is directives of security purpose.
2.Through cloud platform we will evaluate vulnerabilities for sample app.
3.Through this whole system we will try to identify security vulnerabilities in our any App Engine or web applications.
4.This process will secure our any app-design and development that will be used on cloud platform.

Process:

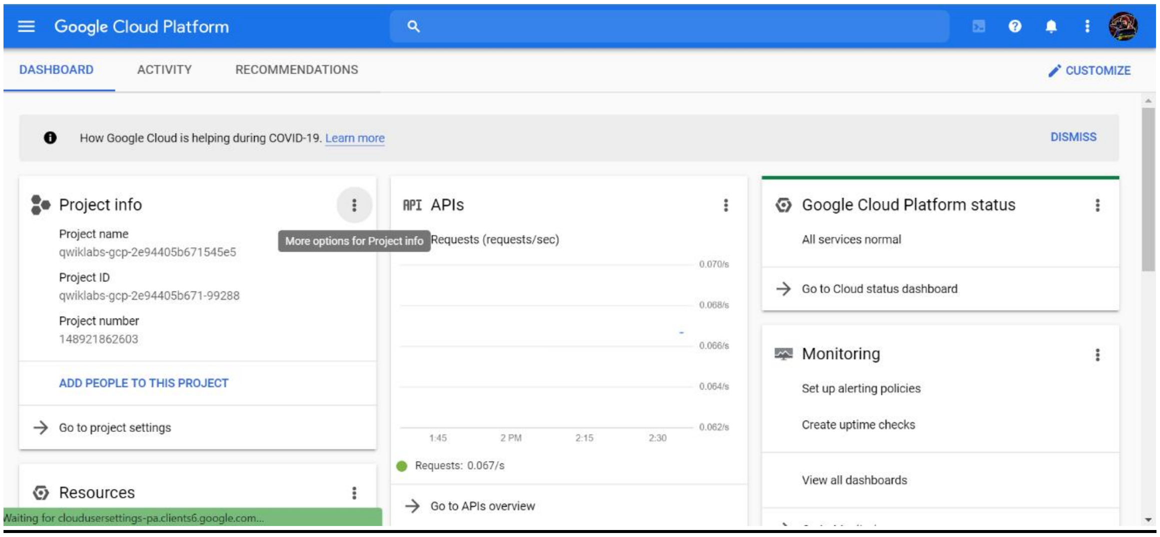

Make the sample app
1st step
test the sample app
2nd step
deploy sample app on cloud platform
4th step
observe the app on cloud (working or not)
5th step
run the sample app for scanning for vulnerabilities
final proess
detect vulnerabilities(if any)


Start
1
Develop app
2
Deploy
3
Test
4
Complete Developed App
5
Cloud Scanner
6
Error
1. List of vulnerable components.
2. Loop holes present in the App.
App free of all Vulnerabilities
End

Implementation :

Step 1: SET-UP

Firstly we need to open https://console.cloud.google.com/?pli=1 for Google Cloud platform where we will start our process.



How Google Cloud is helping during COVID-19. Learn more

Project name
qwiklabs-gcp-2e94405b671545e5

Project ID
qwiklabs-gcp-2e94405b671-99288

Project number
148921862603

Requests: 0.067/s

All services normal

Waiting for cloudusersettings-pa.clients6.google.com...

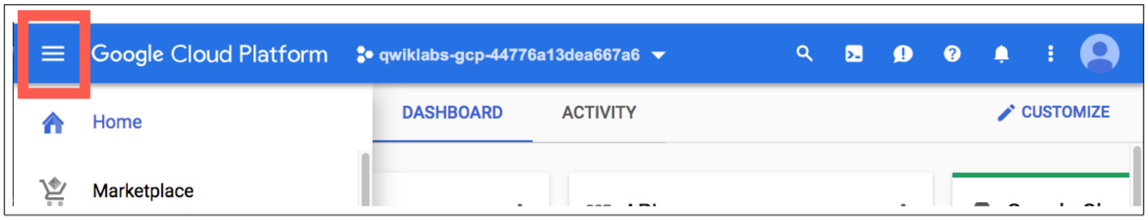
We will have to sign-in with our personal gmail account .

In the **Sign in** page, we need to paste the username that you copied from the Connection Details panel. Then copy and paste the password .

Click through the subsequent pages:

- Accept the terms and conditions.
- Do not add recovery options or two-factor authentication (because this is a temporary account).
- Do not sign up for free trials.

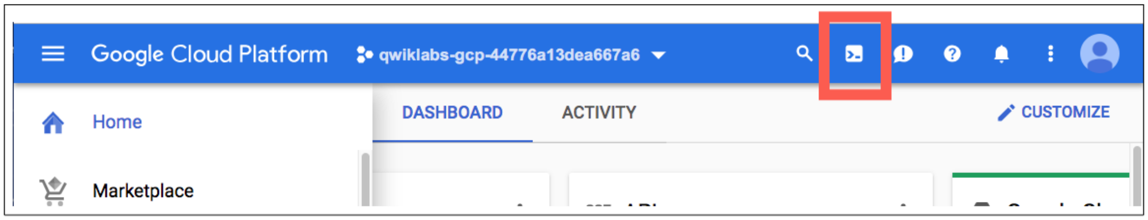
After a few moments, the Cloud Console opens in this tab.



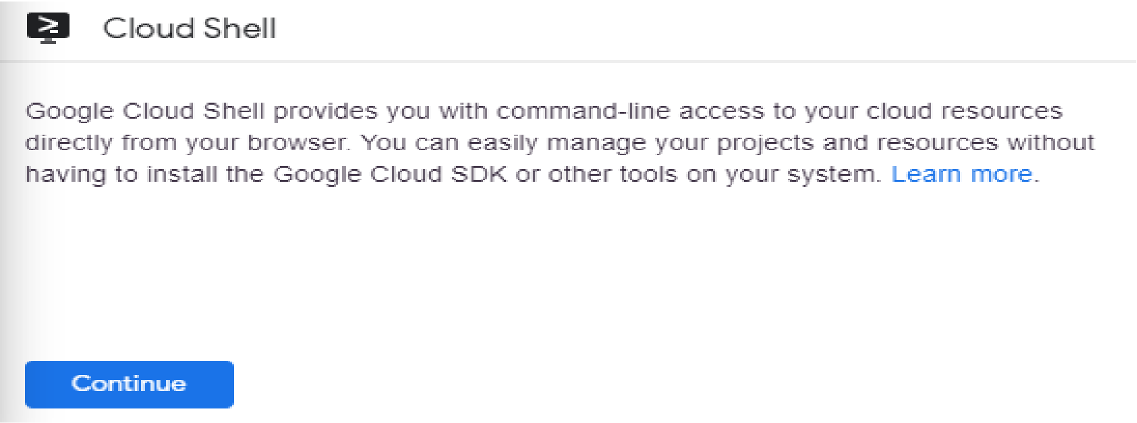
STEP 2: Activate Cloud Shell

Cloud Shell is a virtual machine that is loaded with development tools. It offers a persistent 5GB home directory and runs on the Google Cloud. Cloud Shell provides command-line access to your Google Cloud resources.

In the Cloud Console, in the top right toolbar, click the **Activate Cloud Shell** button.

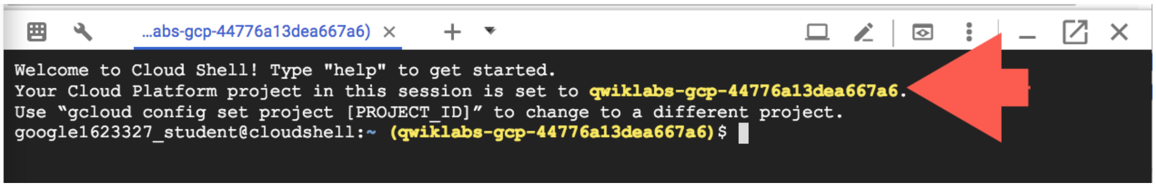


Click **Continue**


Cloud Shell

Google Cloud Shell provides you with command-line access to your cloud resources directly from your browser. You can easily manage your projects and resources without having to install the Google Cloud SDK or other tools on your system. Learn more.

It takes a few moments to provision and connect to the environment. When you are connected, you are already authenticated, and the project is set to your *PROJECT_ID*. For example:



```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to qwiklabs-gcp-44776a13dea667a6.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
google1623327_student@cloudshell:~ (qwiklabs-gcp-44776a13dea667a6)$
```

STEP 3: **<u>Cloud Shell operation through command:</u>**

we will have to configure single project id with our project :

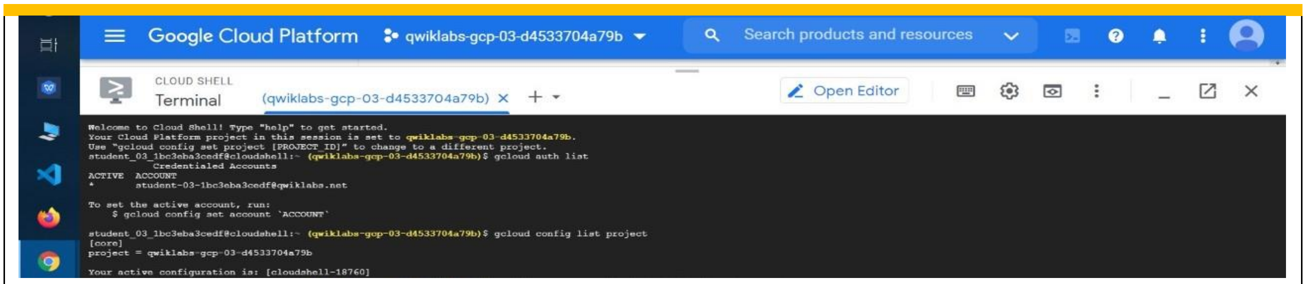
for this we can list the active account name for configuration with this command:

gcloud auth list

Now we will have to confirm the list of active project-id , through this command :

gcloud config list project

OUTPUT :


Google Cloud Platform
qwiklabs-gcp-03-d4533704a79b
Search products and resources
CLOUD SHELL
Terminal
(qwiklabs-gcp-03-d4533704a79b)
Open Editor

```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to qwiklabs-gcp-03-d4533704a79b.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
student_03_1bc3eba3cedf@cloudshell:~ (qwiklabs-gcp-03-d4533704a79b)$ gcloud auth list
           Credentialed Accounts
ACTIVE  ACCOUNT
*       student-03-1bc3eba3cedf@qwiklabs.net

To set the active account, run:
    $ gcloud config set account `ACCOUNT`

student_03_1bc3eba3cedf@cloudshell:~ (qwiklabs-gcp-03-d4533704a79b)$ gcloud config list project
[core]
project = qwiklabs-gcp-03-d4533704a79b

Your active configuration is: [cloudshell-18760]
```

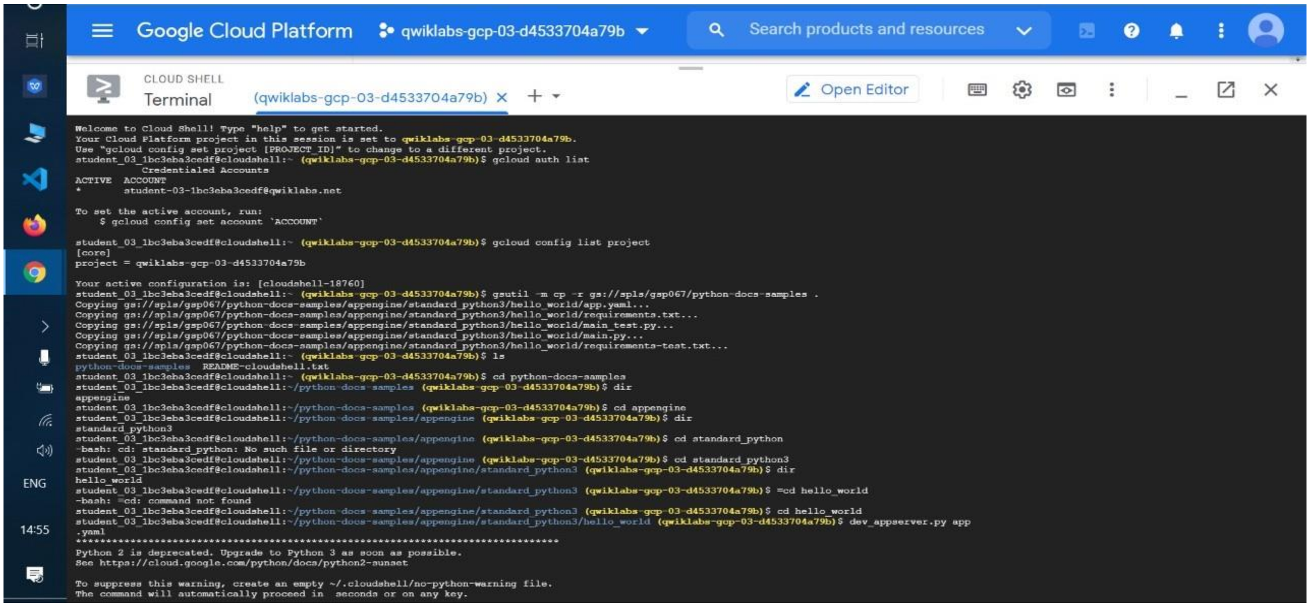
STEP 4: DEPLOY APP TO CLOUD PLATFORM

In this section, we will deploy a sample Hello World application to run Security Scanner on. Run the following command in Cloud Shell to clone the repo : https://github.com/GoogleCloudPlatform/python-docs-samples/tree/master/appengine/standard/hello_world

```
gsutil -m cp -r gs://spls/gsp067/python-docs-samples .
```

Then go to the directory that contains the sample code :

```
cd python-docs-samples/appengine/standard_python3/hello_world
```

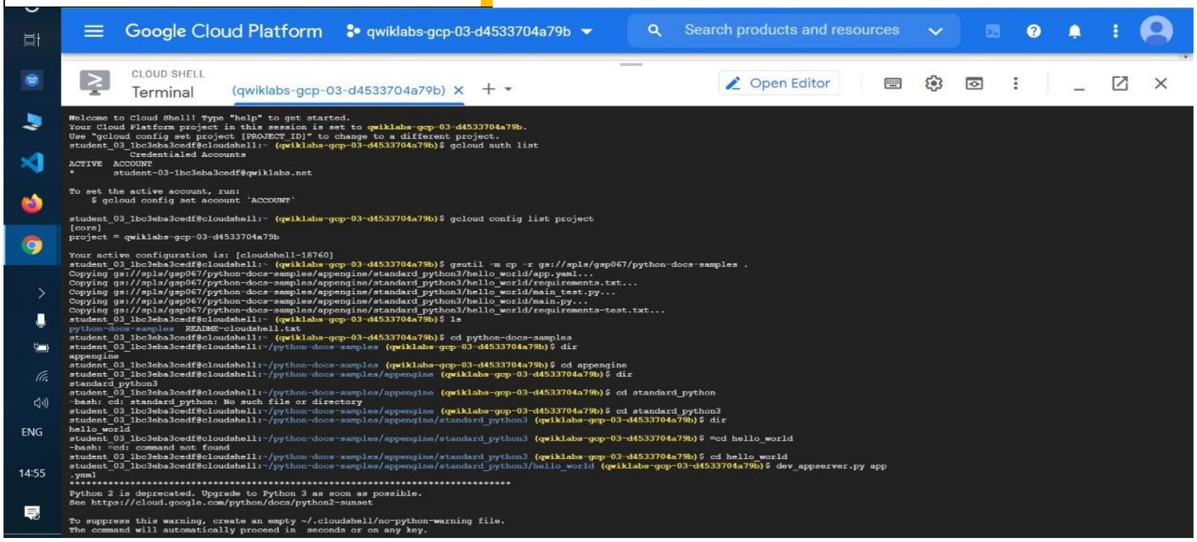

Google Cloud Platform
qwiklabs-gcp-03-d4533704a79b
Search products and resources
CLOUD SHELL
Terminal
(qwiklabs-gcp-03-d4533704a79b)
Open Editor
ENG
14:55

```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to qwiklabs-gcp-03-d4533704a79b.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
student_03_1bc3eba3cedf@cloudshell:~ (qwiklabs-gcp-03-d4533704a79b)$ gcloud auth list
          Credentialed Accounts
ACTIVE  ACCOUNT
*       student-03-1bc3eba3cedf@qwiklabs.net

To set the active account, run:
    $ gcloud config set account `ACCOUNT`

student_03_1bc3eba3cedf@cloudshell:~ (qwiklabs-gcp-03-d4533704a79b)$ gcloud config list project
[core]
project = qwiklabs-gcp-03-d4533704a79b

Your active configuration is: [cloudshell-18760]
student_03_1bc3eba3cedf@cloudshell:~ (qwiklabs-gcp-03-d4533704a79b)$ gsutil -m cp -r gs://spls/gsp067/python-docs-samples .
Copying gs://spls/gsp067/python-docs-samples/appengine/standard_python3/hello_world/app.yaml...
Copying gs://spls/gsp067/python-docs-samples/appengine/standard_python3/hello_world/requirements.txt...
Copying gs://spls/gsp067/python-docs-samples/appengine/standard_python3/hello_world/main_test.py...
Copying gs://spls/gsp067/python-docs-samples/appengine/standard_python3/hello_world/main.py...
Copying gs://spls/gsp067/python-docs-samples/appengine/standard_python3/hello_world/requirements-test.txt...
student_03_1bc3eba3cedf@cloudshell:~ (qwiklabs-gcp-03-d4533704a79b)$ ls
python-docs-samples  README-cloudshell.txt
student_03_1bc3eba3cedf@cloudshell:~ (qwiklabs-gcp-03-d4533704a79b)$ cd python-docs-samples
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples (qwiklabs-gcp-03-d4533704a79b)$ dir
appengine
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples (qwiklabs-gcp-03-d4533704a79b)$ cd appengine
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine (qwiklabs-gcp-03-d4533704a79b)$ dir
standard_python3
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine (qwiklabs-gcp-03-d4533704a79b)$ cd standard_python
-bash: cd: standard_python: No such file or directory
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine (qwiklabs-gcp-03-d4533704a79b)$ cd standard_python3
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine/standard_python3 (qwiklabs-gcp-03-d4533704a79b)$ dir
hello_world
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine/standard_python3 (qwiklabs-gcp-03-d4533704a79b)$ =cd hello_world
-bash: =cd: command not found
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine/standard_python3 (qwiklabs-gcp-03-d4533704a79b)$ cd hello_world
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine/standard_python3/hello_world (qwiklabs-gcp-03-d4533704a79b)$ dev_appserver.py app
.yaml
********************************************************************************
Python 2 is deprecated. Upgrade to Python 3 as soon as possible.
See https://cloud.google.com/python/docs/python2-sunset

To suppress this warning, create an empty ~/.cloudshell/no-python-warning file.
The command will automatically proceed in  seconds or on any key.
```

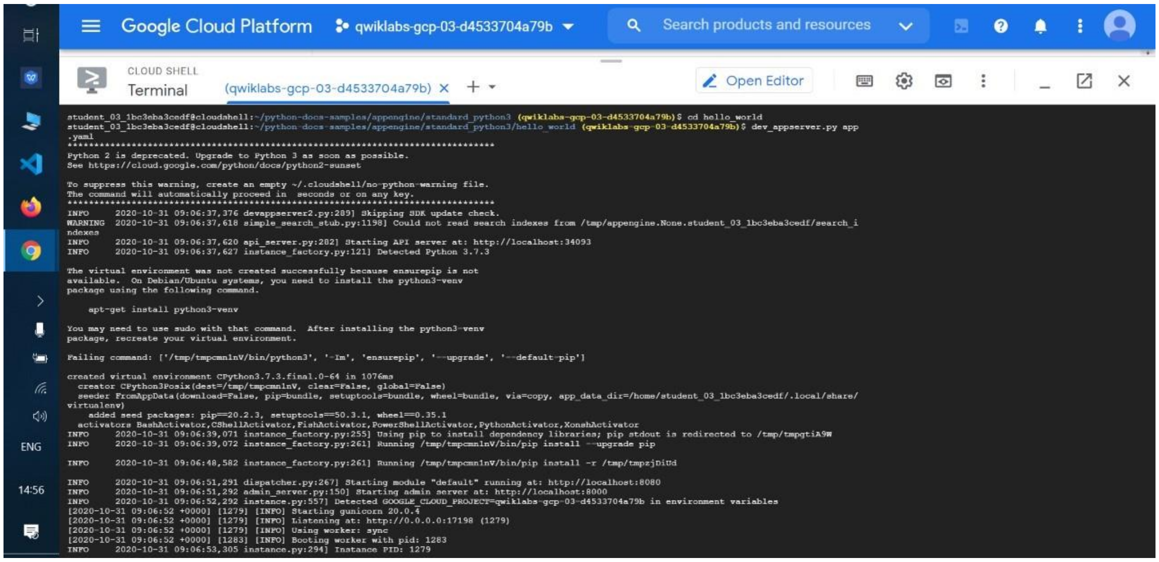
STEP 5 : TESTING APP ON CLOUD PLATFORM

From within the **hello_world** directory where the app's app.yaml configuration file is located, start the local development server with the following command:

```
dev_appserver.py app.yaml
```

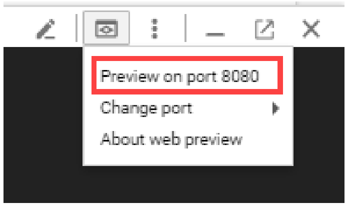

Google Cloud Platform
qwiklabs-gcp-03-d4533704a79b
Search products and resources
CLOUD SHELL
Terminal
(qwiklabs-gcp-03-d4533704a79b)
Open Editor
ENG
14:55

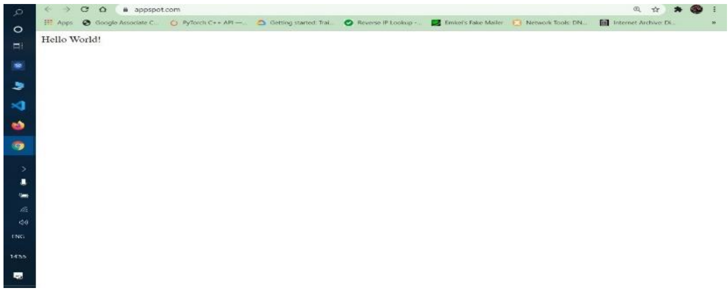
```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to qwiklabs-gcp-03-d4533704a79b.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
student_03_1bc3eba3cedf@cloudshell:~ (qwiklabs-gcp-03-d4533704a79b)$ gcloud auth list
           Credentialed Accounts
ACTIVE  ACCOUNT
*       student-03-1bc3eba3cedf@qwiklabs.net

To set the active account, run:
    $ gcloud config set account `ACCOUNT`

student_03_1bc3eba3cedf@cloudshell:~ (qwiklabs-gcp-03-d4533704a79b)$ gcloud config list project
[core]
project = qwiklabs-gcp-03-d4533704a79b

Your active configuration is: [cloudshell-18760]
student_03_1bc3eba3cedf@cloudshell:~ (qwiklabs-gcp-03-d4533704a79b)$ gsutil -m cp -r gs://spls/gsp067/python-docs-samples .
Copying gs://spls/gsp067/python-docs-samples/appengine/standard_python3/hello_world/app.yaml...
Copying gs://spls/gsp067/python-docs-samples/appengine/standard_python3/hello_world/requirements.txt...
Copying gs://spls/gsp067/python-docs-samples/appengine/standard_python3/hello_world/main_test.py...
Copying gs://spls/gsp067/python-docs-samples/appengine/standard_python3/hello_world/main.py...
Copying gs://spls/gsp067/python-docs-samples/appengine/standard_python3/hello_world/requirements-test.txt...
student_03_1bc3eba3cedf@cloudshell:~ (qwiklabs-gcp-03-d4533704a79b)$ ls
python-docs-samples  README-cloudshell.txt
student_03_1bc3eba3cedf@cloudshell:~ (qwiklabs-gcp-03-d4533704a79b)$ cd python-docs-samples
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples (qwiklabs-gcp-03-d4533704a79b)$ dir
appengine
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples (qwiklabs-gcp-03-d4533704a79b)$ cd appengine
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine (qwiklabs-gcp-03-d4533704a79b)$ dir
standard_python3
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine (qwiklabs-gcp-03-d4533704a79b)$ cd standard_python
-bash: cd: standard_python: No such file or directory
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine (qwiklabs-gcp-03-d4533704a79b)$ cd standard_python3
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine/standard_python3 (qwiklabs-gcp-03-d4533704a79b)$ dir
hello_world
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine/standard_python3 (qwiklabs-gcp-03-d4533704a79b)$ =cd hello_world
-bash: =cd: command not found
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine/standard_python3 (qwiklabs-gcp-03-d4533704a79b)$ cd hello_world
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine/standard_python3/hello_world (qwiklabs-gcp-03-d4533704a79b)$ dev_appserver.py app
.yaml
********************************************************************************
Python 2 is deprecated. Upgrade to Python 3 as soon as possible.
See https://cloud.google.com/python/docs/python2-sunset

To suppress this warning, create an empty ~/.cloudshell/no-python-warning file.
The command will automatically proceed in  seconds or on any key.
```


Google Cloud Platform
qwiklabs-gcp-03-d4533704a79b
Search products and resources
CLOUD SHELL
Terminal
(qwiklabs-gcp-03-d4533704a79b)
Open Editor
ENG
14:56

```
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine/standard_python3 (qwiklabs-gcp-03-d4533704a79b)$ cd hello_world
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine/standard_python3/hello_world (qwiklabs-gcp-03-d4533704a79b)$ dev_appserver.py app
.yaml
********************************************************************************
Python 2 is deprecated. Upgrade to Python 3 as soon as possible.
See https://cloud.google.com/python/docs/python2-sunset

To suppress this warning, create an empty ~/.cloudshell/no-python-warning file.
The command will automatically proceed in  seconds or on any key.
********************************************************************************
INFO     2020-10-31 09:06:37,376 devappserver2.py:289] Skipping SDK update check.
WARNING  2020-10-31 09:06:37,618 simple_search_stub.py:1198] Could not read search indexes from /tmp/appengine.None.student_03_1bc3eba3cedf/search_i
ndexes
INFO     2020-10-31 09:06:37,620 api_server.py:282] Starting API server at: http://localhost:34093
INFO     2020-10-31 09:06:37,627 instance_factory.py:121] Detected Python 3.7.3

The virtual environment was not created successfully because ensurepip is not
available.  On Debian/Ubuntu systems, you need to install the python3-venv
package using the following command.

    apt-get install python3-venv

You may need to use sudo with that command.  After installing the python3-venv
package, recreate your virtual environment.

Failing command: ['/tmp/tmpcmnlnV/bin/python3', '-Im', 'ensurepip', '--upgrade', '--default-pip']

created virtual environment CPython3.7.3.final.0-64 in 1076ms
  creator CPython3Posix(dest=/tmp/tmpcmnlnV, clear=False, global=False)
  seeder FromAppData(download=False, pip=bundle, setuptools=bundle, wheel=bundle, via=copy, app_data_dir=/home/student_03_1bc3eba3cedf/.local/share/
virtualenv)
    added seed packages: pip==20.2.3, setuptools==50.3.1, wheel==0.35.1
  activators BashActivator,CShellActivator,FishActivator,PowerShellActivator,PythonActivator,XonshActivator
INFO     2020-10-31 09:06:39,071 instance_factory.py:255] Using pip to install dependency libraries; pip stdout is redirected to /tmp/tmpgtiA9W
INFO     2020-10-31 09:06:39,072 instance_factory.py:261] Running /tmp/tmpcmnlnV/bin/pip install --upgrade pip

INFO     2020-10-31 09:06:48,582 instance_factory.py:261] Running /tmp/tmpcmnlnV/bin/pip install -r /tmp/tmpzjDiUd

INFO     2020-10-31 09:06:51,291 dispatcher.py:267] Starting module "default" running at: http://localhost:8080
INFO     2020-10-31 09:06:51,292 admin_server.py:150] Starting admin server at: http://localhost:8000
INFO     2020-10-31 09:06:52,292 instance.py:557] Detected GOOGLE_CLOUD_PROJECT=qwiklabs-gcp-03-d4533704a79b in environment variables
[2020-10-31 09:06:52 +0000] [1279] [INFO] Starting gunicorn 20.0.4
[2020-10-31 09:06:52 +0000] [1279] [INFO] Listening at: http://0.0.0.0:17198 (1279)
[2020-10-31 09:06:52 +0000] [1279] [INFO] Using worker: sync
[2020-10-31 09:06:52 +0000] [1283] [INFO] Booting worker with pid: 1283
INFO     2020-10-31 09:06:53,305 instance.py:294] Instance PID: 1279
```

The local development server is now running and listening for requests on port 8080. Click on the **web preview** button in Cloud Shell, and select **Preview on port 8080** to see it:





Hello World!

STEP 6 :

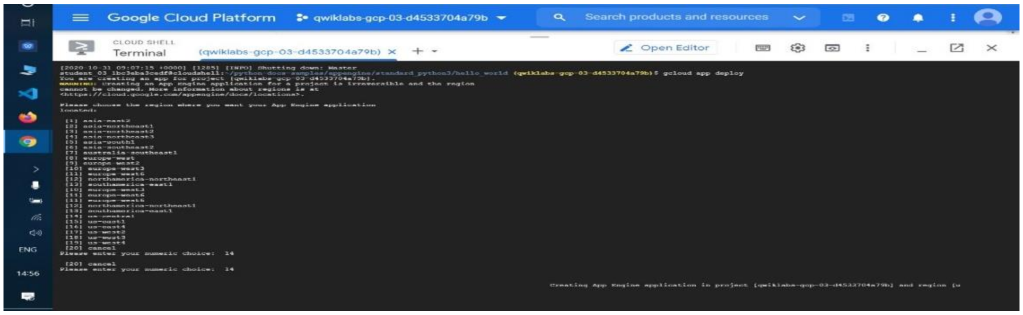
DEPLOY OUR SAMPLE APP ON CLOUD

Deploy our app to App Engine by running the following command from within the root directory of your application (hello_world):

```
gcloud app deploy
```

Need to select a region. Choose the number for one that is near where you are. After the app is created in your lab, you'll be asked if you want to continue. Click **Y** to continue.

Deployment of your app will then begin.


Google Cloud Platform
qwiklabs-gcp-03-d4533704a79b
Search products and resources
CLOUD SHELL
Terminal
(qwiklabs-gcp-03-d4533704a79b)
Open Editor
ENG
14:56

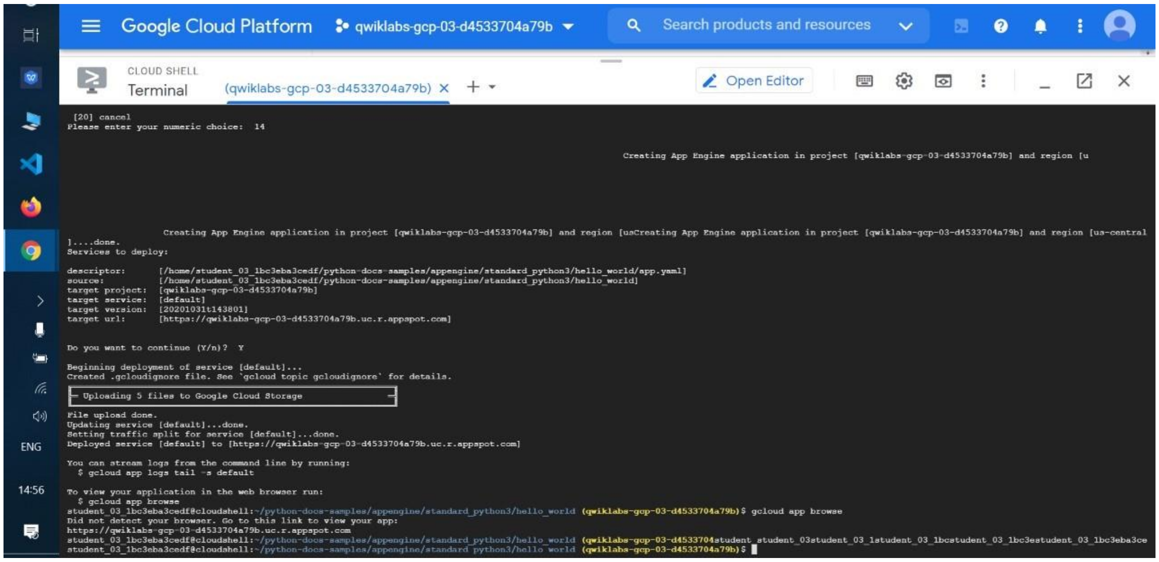
```
[2020-10-31 09:07:15 +0000] [1285] [INFO] Shutting down: Master
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine/standard_python3/hello_world (qwiklabs-gcp-03-d4533704a79b)$ gcloud app deploy
You are creating an app for project [qwiklabs-gcp-03-d4533704a79b].
WARNING: Creating an App Engine application for a project is irreversible and the region
cannot be changed. More information about regions is at
<https://cloud.google.com/appengine/docs/locations>.

Please choose the region where you want your App Engine application
located:

 [1] asia-east2
 [2] asia-northeast1
 [3] asia-northeast2
 [4] asia-northeast3
 [5] asia-south1
 [6] asia-southeast2
 [7] australia-southeast1
 [8] europe-west
 [9] europe-west2
 [10] europe-west3
 [11] europe-west6
 [12] northamerica-northeast1
 [13] southamerica-east1
 [10] europe-west3
 [11] europe-west6
 [12] northamerica-northeast1
 [13] southamerica-east1
 [14] us-central
 [15] us-east1
 [16] us-east4
 [17] us-west2
 [18] us-west3
 [19] us-west4
 [20] cancel
Please enter your numeric choice:  14

 [20] cancel
Please enter your numeric choice:  14

                                        Creating App Engine application in project [qwiklabs-gcp-03-d4533704a79b] and region [u
```

STEP 7: VIEW OUR SAMPLE APP

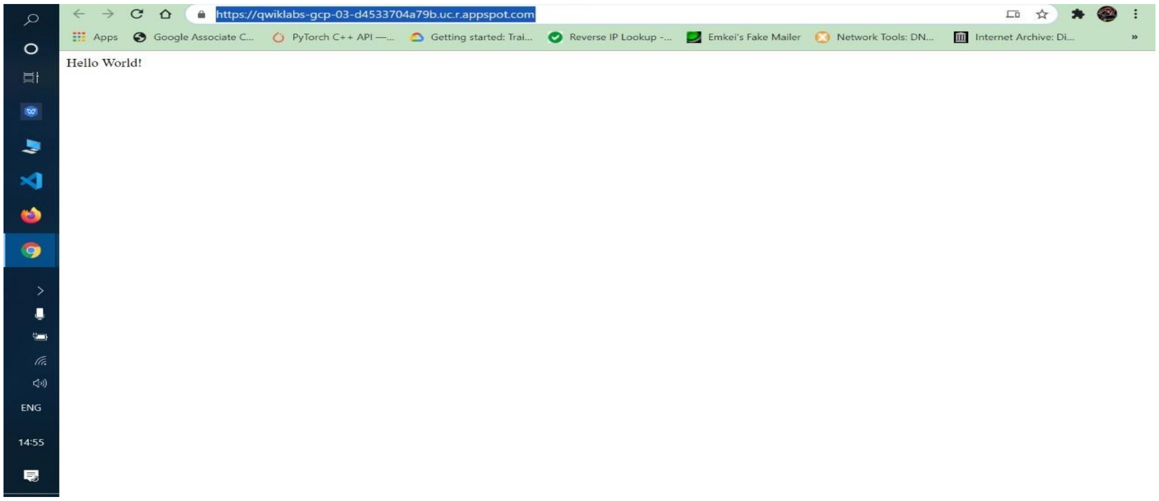
Deploy your app to App Engine by running the following command from within the root directory of your application (**hello_world**):

```
gcloud app browse
```

There will be a link in Cloud Shell that you can use, or view the app at **http://[YOUR_PROJECT_ID].appspot.com.** This is the URL you'll scan for vulnerabilities and it will be added to our scan parameters in the next step:


Google Cloud Platform
qwiklabs-gcp-03-d4533704a79b
Search products and resources
CLOUD SHELL
Terminal
(qwiklabs-gcp-03-d4533704a79b)
Open Editor
ENG
14:56

```
 [20] cancel
Please enter your numeric choice:  14

                                                                                        Creating App Engine application in project [qwiklabs-gcp-03-d4533704a79b] and region [u




              Creating App Engine application in project [qwiklabs-gcp-03-d4533704a79b] and region [usCreating App Engine application in project [qwiklabs-gcp-03-d4533704a79b] and region [us-central
]....done.
Services to deploy:

descriptor:      [/home/student_03_1bc3eba3cedf/python-docs-samples/appengine/standard_python3/hello_world/app.yaml]
source:          [/home/student_03_1bc3eba3cedf/python-docs-samples/appengine/standard_python3/hello_world]
target project:  [qwiklabs-gcp-03-d4533704a79b]
target service:  [default]
target version:  [20201031t143801]
target url:      [https://qwiklabs-gcp-03-d4533704a79b.uc.r.appspot.com]


Do you want to continue (Y/n)?  Y

Beginning deployment of service [default]...
Created .gcloudignore file. See `gcloud topic gcloudignore` for details.
╔═ Uploading 5 files to Google Cloud Storage                ═╣
File upload done.
Updating service [default]...done.
Setting traffic split for service [default]...done.
Deployed service [default] to [https://qwiklabs-gcp-03-d4533704a79b.uc.r.appspot.com]

You can stream logs from the command line by running:
  $ gcloud app logs tail -s default

To view your application in the web browser run:
  $ gcloud app browse
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine/standard_python3/hello_world (qwiklabs-gcp-03-d4533704a79b)$ gcloud app browse
Did not detect your browser. Go to this link to view your app:
https://qwiklabs-gcp-03-d4533704a79b.uc.r.appspot.com
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine/standard_python3/hello_world (qwiklabs-gcp-03-d4533704student_student_03student_03_1student_03_1bcstudent_03_1bc3estudent_03_1bc3eba3ce
student_03_1bc3eba3cedf@cloudshell:~/python-docs-samples/appengine/standard_python3/hello_world (qwiklabs-gcp-03-d4533704a79b)$ 
```

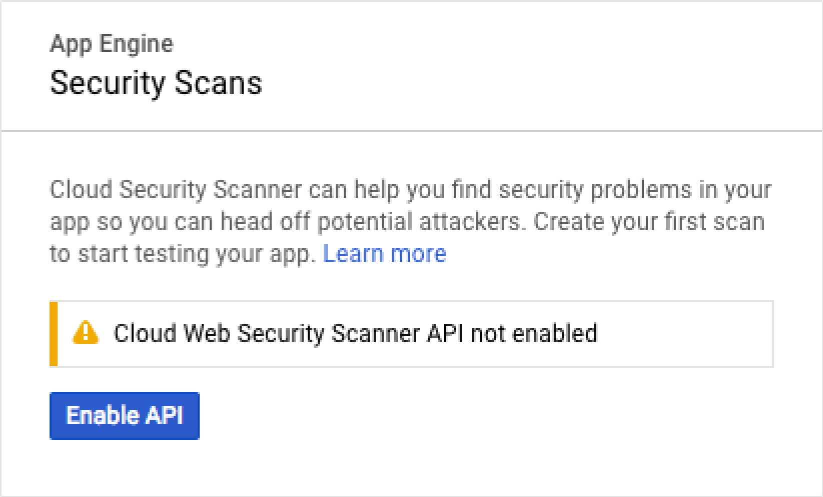


Hello World!

FINAL STEP : **RUN OUR APP FOR SCANNING**

The scan does not run immediately, but is queued for later execution; it can take hours before the scan executes, depending on current load.

Navigation menu > **App Engine** > **Security scans**:



App Engine

Security Scans

Cloud Security Scanner can help you find security problems in your app so you can head off potential attackers. Create your first scan to start testing your app. Learn more

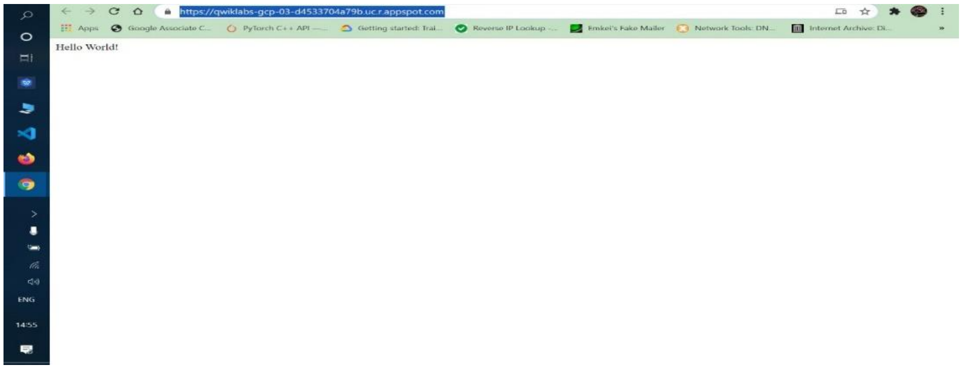
⚠ Cloud Web Security Scanner API not enabled

Click **Enable API** > **Create scan**.

Under Starting URLs, enter the URL of the application you want to scan.

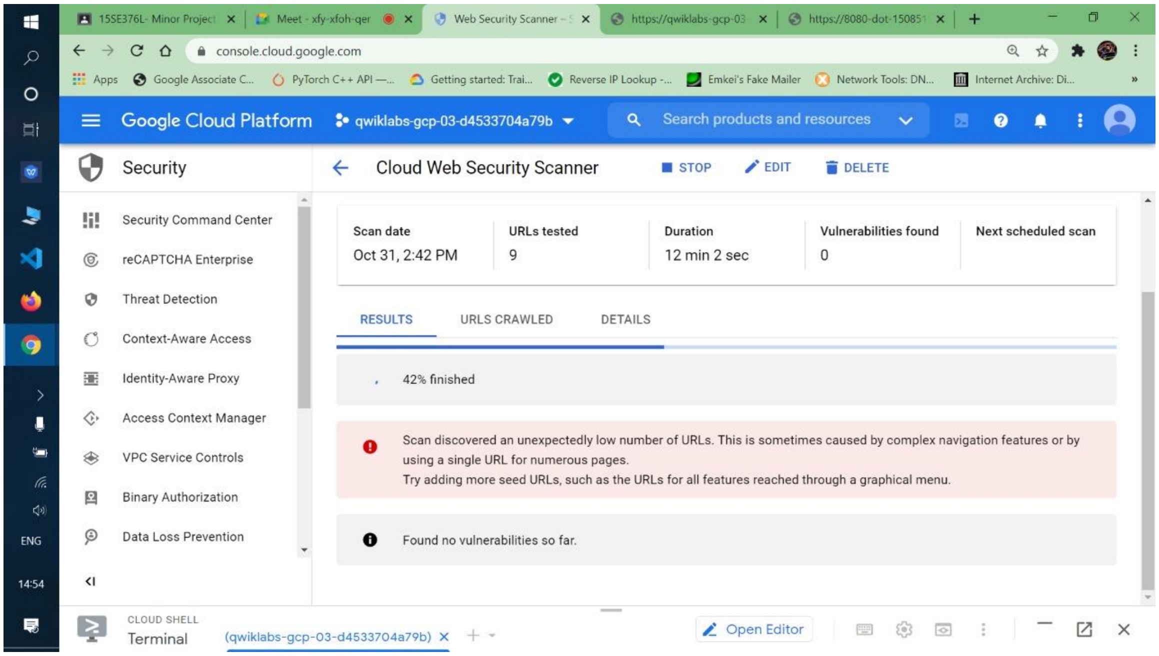
We will use the sample app's URL and start for scanning:

The app link is below :



https://qwiklabs-gcp-03-d4533704a79b.uc.r.appspot.com

Hello World!



Scan date	URLs tested	Duration	Vulnerabilities found	Next scheduled scan
Oct 31, 2:42 PM	9	12 min 2 sec	0	

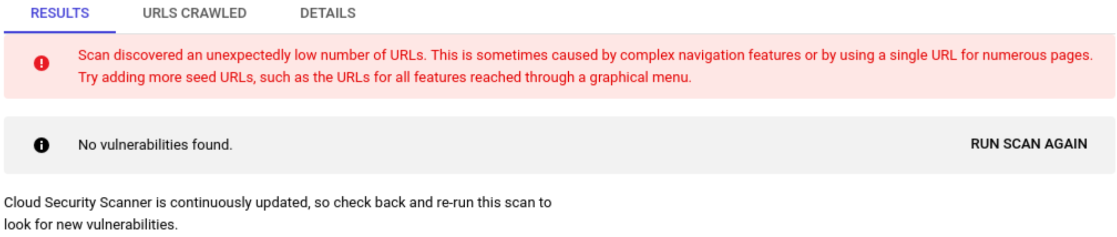
42% finished

Scan discovered an unexpectedly low number of URLs. This is sometimes caused by complex navigation features or by using a single URL for numerous pages.
Try adding more seed URLs, such as the URLs for all features reached through a graphical menu.

Found no vulnerabilities so far.

It will take some time …………….

RESULT :



Scan discovered an unexpectedly low number of URLs. This is sometimes caused by complex navigation features or by using a single URL for numerous pages.
Try adding more seed URLs, such as the URLs for all features reached through a graphical menu.

No vulnerabilities found.

Cloud Security Scanner is continuously updated, so check back and re-run this scan to look for new vulnerabilities.

After all scanning the results will confirm if app has any vulnerability otherwise it will confirm as shown in the above pic. No vulnerability found . The scan overview page displays a results section when the scan completes. The following image shows example scan results when no vulnerabilities are detected.