

Cloud Security Scanner: Qwik Start

GSP112



Google Cloud Self-Paced Labs

Overview

The Cloud Security Scanner identifies security vulnerabilities in your Google App Engine web applications. It crawls your application, following all links within the scope of your starting URLs, and attempts to exercise as many user inputs and event handlers as possible.

The scanner is designed to complement your existing secure design and development processes. To avoid distracting developers with false positives, the scanner errs on the side of under reporting and will not display low confidence alerts. It does not replace a manual security review, and it does not guarantee that your application is free from security flaws. For more information on web security, see the [OWASP Top Ten Project](#).

Setup

Before you click the Start Lab button

Read these instructions. Labs are timed and you cannot pause them. The timer, which starts when you click **Start Lab**, shows how long Google Cloud resources will be made available to you.

This Qwiklabs hands-on lab lets you do the lab activities yourself in a real cloud environment, not in a simulation or demo environment. It does so by giving you new, temporary credentials that you use to sign in and access Google Cloud for the duration of the lab.

What you need

To complete this lab, you need:

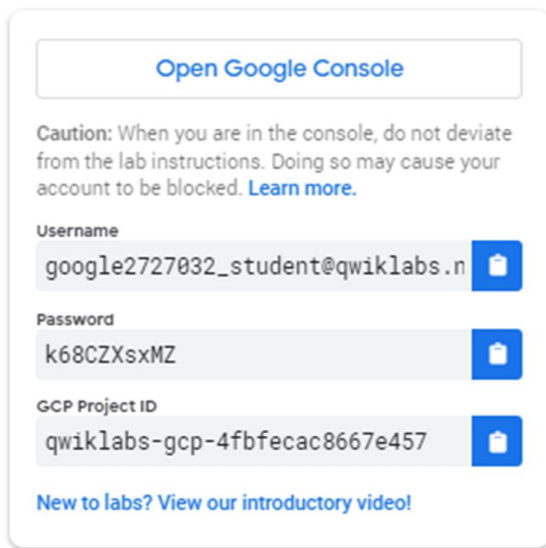
- Access to a standard internet browser (Chrome browser recommended).
- Time to complete the lab.

Note: If you already have your own personal Google Cloud account or project, do not use it for this lab.

Note: If you are using a Pixelbook, open an Incognito window to run this lab.


How to start your lab and sign in to the Google Cloud Console


1. Click the **Start Lab** button. If you need to pay for the lab, a pop-up opens for you to select your payment method. On the left is a panel populated with the temporary credentials that you must use for this lab.




[Open Google Console](#)

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. [Learn more.](#)

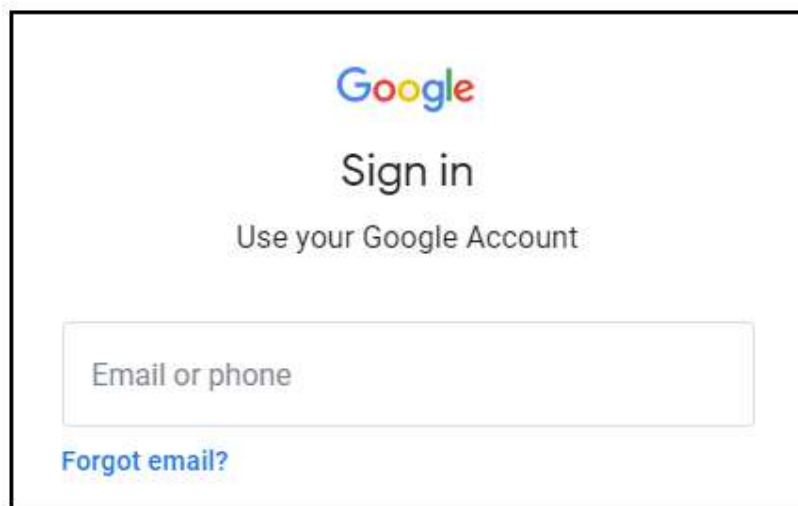
Username
google2727032_student@qwiklabs.n 

Password
k68CZXsxMZ 

GCP Project ID
qwiklabs-gcp-4fbfecac8667e457 

[New to labs? View our introductory video!](#)

2. Copy the username, and then click **Open Google Console**. The lab spins up resources, and then opens another tab that shows the **Sign in** page.



Google

Sign in

Use your Google Account

Email or phone

[Forgot email?](#)

Tip: Open the tabs in separate windows, side-by-side.

If you see the **Choose an account** page, click **Use Another**



Account.

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

Important: You must use the credentials from the Connection Details panel. Do not use your Qwiklabs credentials. If you have your own Google Cloud account, do not use it for this lab (avoids incurring charges).

4. 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.

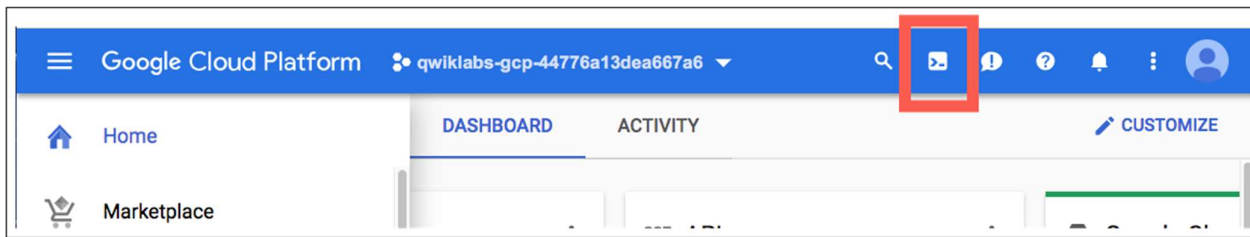
Note: You can view the menu with a list of Google Cloud Products and Services by clicking the **Navigation menu** at the top-left.



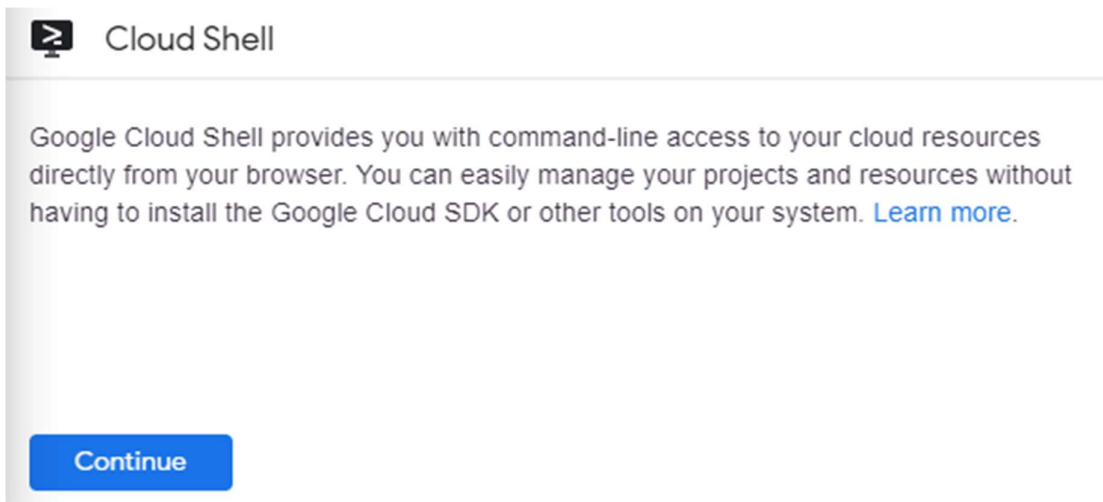
Activate Cloud Shell

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.

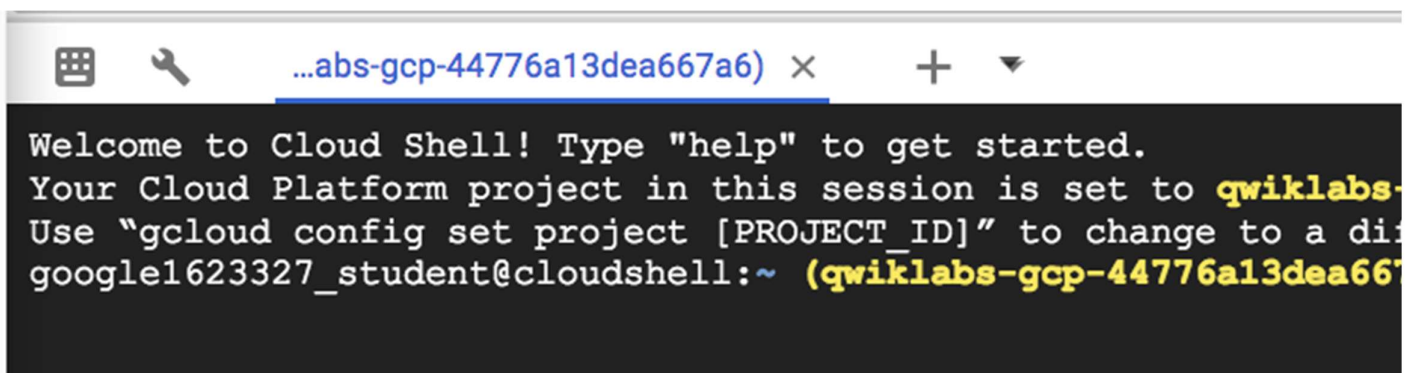
In the Cloud Console, in the top right toolbar, click the **Activate Cloud Shell** button.



Click **Continue**.



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:



`gcloud` is the command-line tool for Google Cloud. It comes pre-installed on Cloud Shell and supports tab-completion.

You can list the active account name with this command:

```
gcloud auth list
```

(Output)

```
Credentialed accounts:  
- <myaccount>@<mydomain>.com (active)
```

(Example output)

```
Credentialed accounts:  
- google1623327_student@gwiklabs.net
```

You can list the project ID with this command:

```
gcloud config list project
```

(Output)

```
[core]  
project = <project_ID>
```

(Example output)

```
[core]  
project = qwiklabs-gcp-44776a13dea667a6
```

For full documentation of `gcloud` see the [gcloud command-line tool overview](#).

Before you begin, you need an app to scan

In this lab, you will deploy a sample Hello World application to run Security Scanner on.

Run the following command in Cloud Shell to clone the [Hello World sample app repository](#):

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

Then go to the directory that contains the sample code:

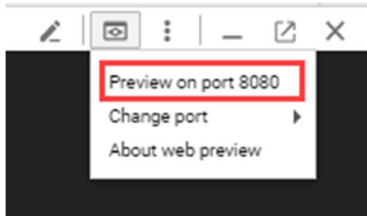
```
cd python-docs-samples/appengine/standard_python3/hello_world
```

Test App

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
```

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:



(If you cannot see the web preview icon, close the Navigation menu, top left corner.)

Press **Ctrl+c** to stop the local app and return to the command line.

Deploy App

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

```
gcloud app deploy
```

You'll be asked 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.

View App

To launch the app in your browser, run the following command:

```
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 your scan parameters in the next step.

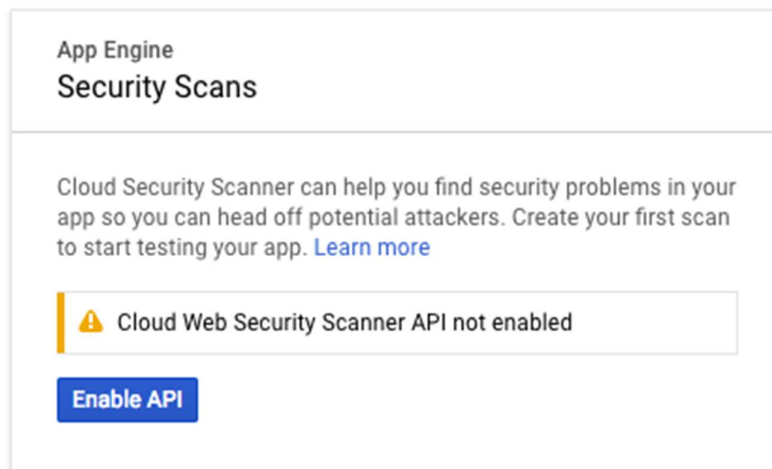
Test Completed Task

Click **Check my progress** to verify your performed task. If you have completed the task successfully you will be granted with an assessment score.

Run the scan


The scan does not run immediately, but is queued for later execution; it can take hours before the scan executes, depending on current load. For more information about these form settings, see [Using Cloud Security Scanner](#).

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




Click **Enable API > Create scan**.

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

 **Create a new scan**


Name

A unique name for your scan config


Starting URLs 

List one or more apps you wish to scan hosted on App Engine Standard or Flexible, Compute Engine or GKE environments. You can also provide IP addresses mapped to starting URLs, but these must be explicitly reserved as Static for the current project. HTTP URLs with an IP Address (e.g. `http://172.217.3.206`) can be used in lieu of an FQDN name. [Learn more](#)


[+ ADD A URL](#)

Excluded URLs 

[+ ADD A URL](#)


Authentication 


None



Schedule

Never



Export options 

☒ **Export to Cloud Security Command Center**
Automatically export scan configurations and scan results to Cloud Security Command Center after scans are finished.

[SHOW MORE](#)

SAVE

CANCEL

Click **Save** to create the scan.

Click **Run** to start scanning:

Scan_ searchtest-1216.appspot.com_952

Results URLs tested Details

i You have not run this scan yet

The scan will be queued, and you can watch the status bar progress as it scans. The scan overview page displays a results section when the scan completes. The following image shows example scan results when no vulnerabilities are detected:

RESULTS URLs CRAWLED DETAILS

i 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.

i No vulnerabilities found.

[RUN SCAN AGAIN](#)

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

Note: Try refreshing the page if you aren't seeing any updates.

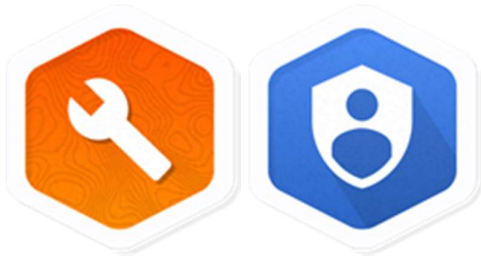
Nice job! You just completed a scan using Cloud Security Scanner. You will see a warning to let you know that only scanning 1 URL isn't ideal. This lab is just to demonstrate a simple example. Your production environment will have plenty of URLs to scan.

Test your Understanding

Below are multiple-choice questions to reinforce your understanding of this lab's concepts. Answer them to the best of your abilities.

Cloud Security Scanner is a web security scanner for common vulnerabilities in Google App Engine applications.
True

Congratulations!



Finish Your Quest

This self-paced lab is part of the [Baseline: Deploy & Develop](#) and [Security & Identity Fundamentals](#) Quests. A Quest is a series of related labs that form a learning path. Completing this Quest earns you the badge above, to recognize your achievement. You can make your badge (or badges) public and link to them in your online resume or social media account. Enroll in a Quest and get immediate completion credit if you've taken this lab. [See other available Qwiklabs Quests](#).

Next Steps / Learn More

This lab is also part of a series of labs called Qwik Starts. These labs are designed to give you a little taste of the many features available with Google Cloud. Search for "Qwik Starts" in the [lab catalog](#) to find the next lab you'd like to take!

Google Cloud Training & Certification

...helps you make the most of Google Cloud technologies. [Our classes](#) include technical skills and best practices to help you get up to speed quickly and continue your learning journey. We offer fundamental to advanced level training, with on-demand, live, and virtual options to suit your busy schedule. [Certifications](#) help you validate and prove your skill and expertise in Google Cloud technologies.

Manual Last Updated September 08, 2020

Lab Last Tested September 08, 2020

Copyright 2021 Google LLC All rights reserved. Google and the Google logo are trademarks of Google LLC. All other company and product names may be trademarks of the respective companies with which they are associated.