Table of Contents

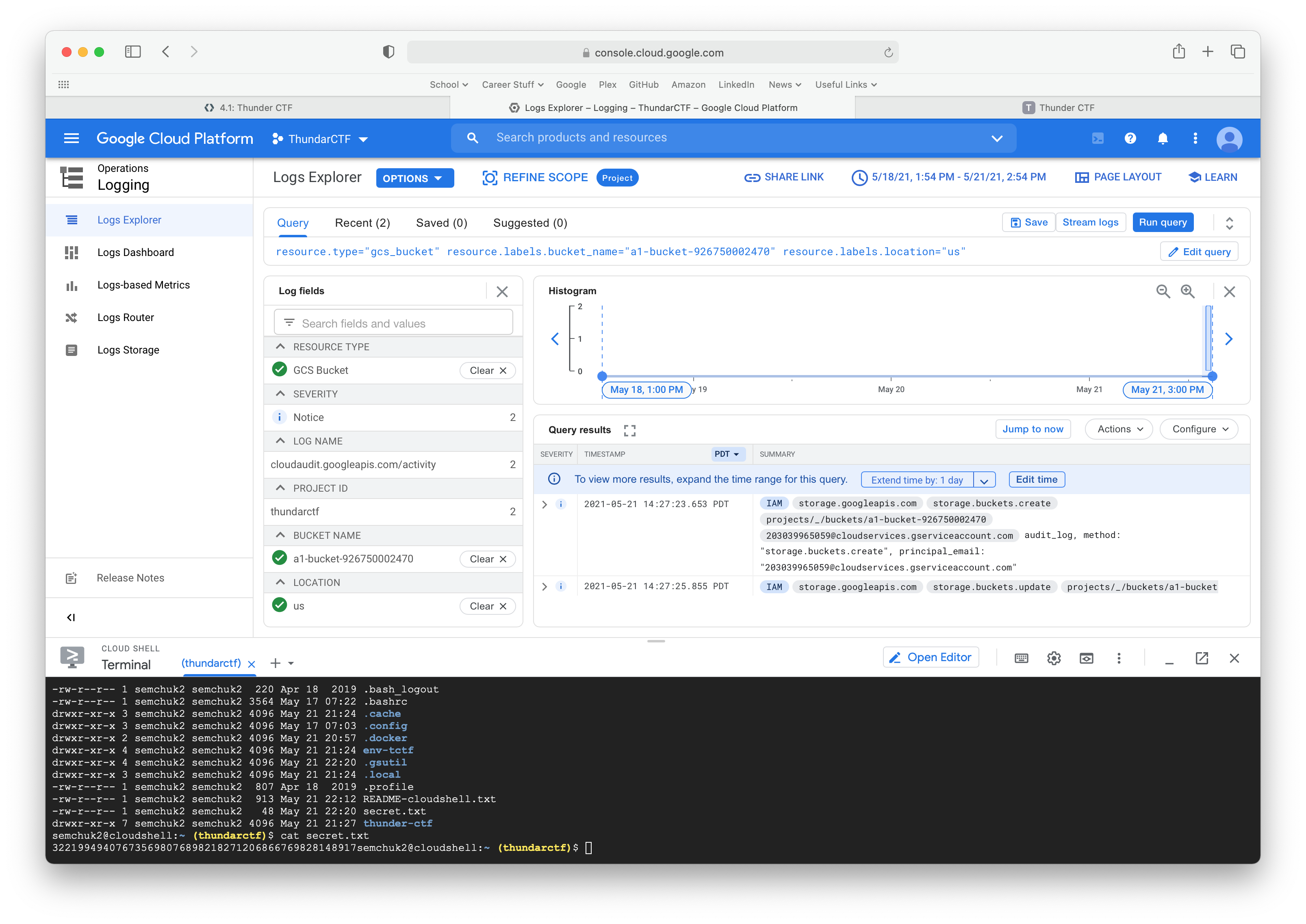
[4.1.3 Take a screenshot of the secret obtained 2](#__RefHeading___Toc119_257206326)

[4.1.4 Examine logs via project activity 3](#__RefHeading___Toc121_257206326)

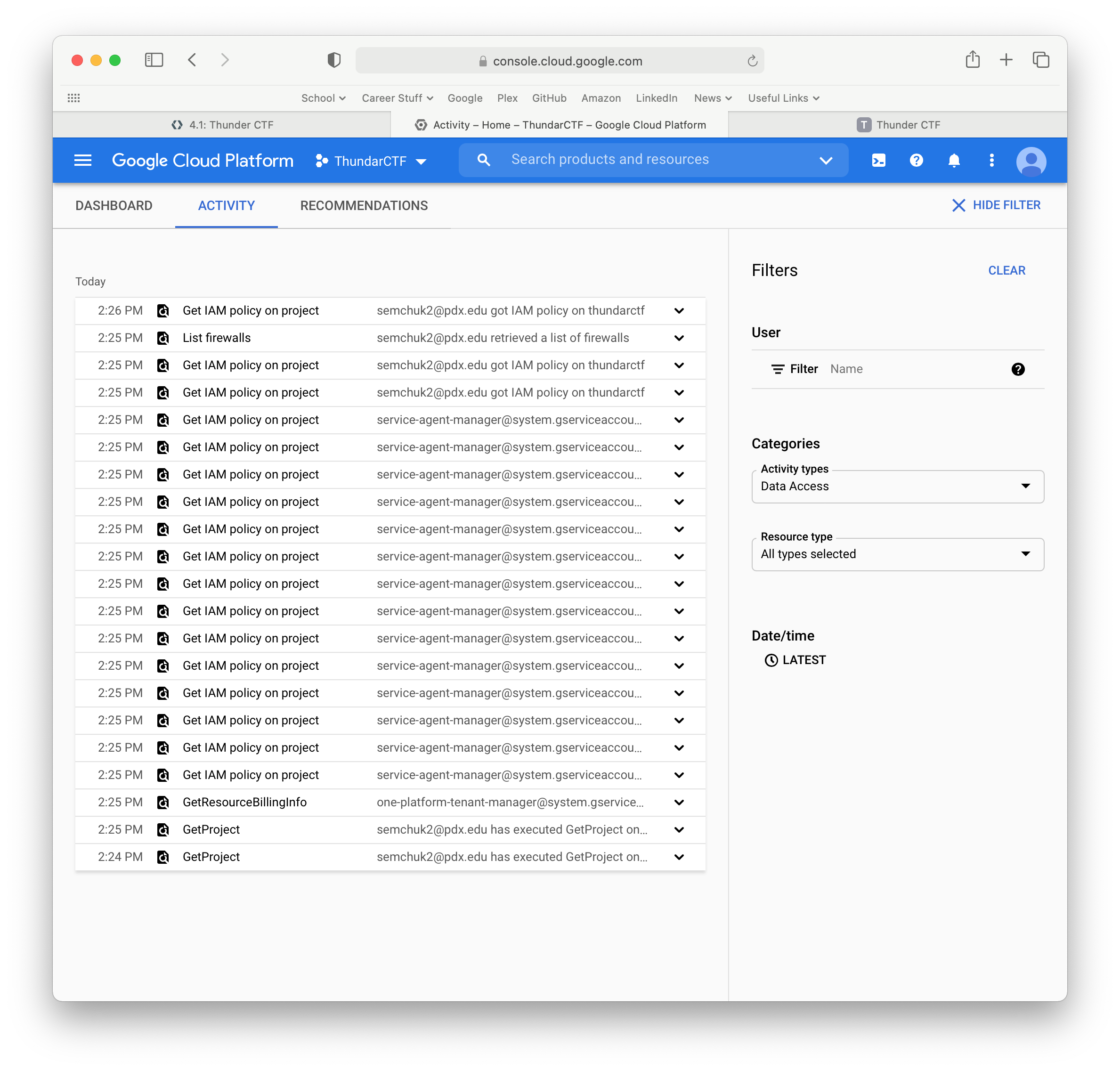
[4.1.6 Clean-up level 4](#__RefHeading___Toc123_257206326)

Labs 4.1 Thunder CTF:

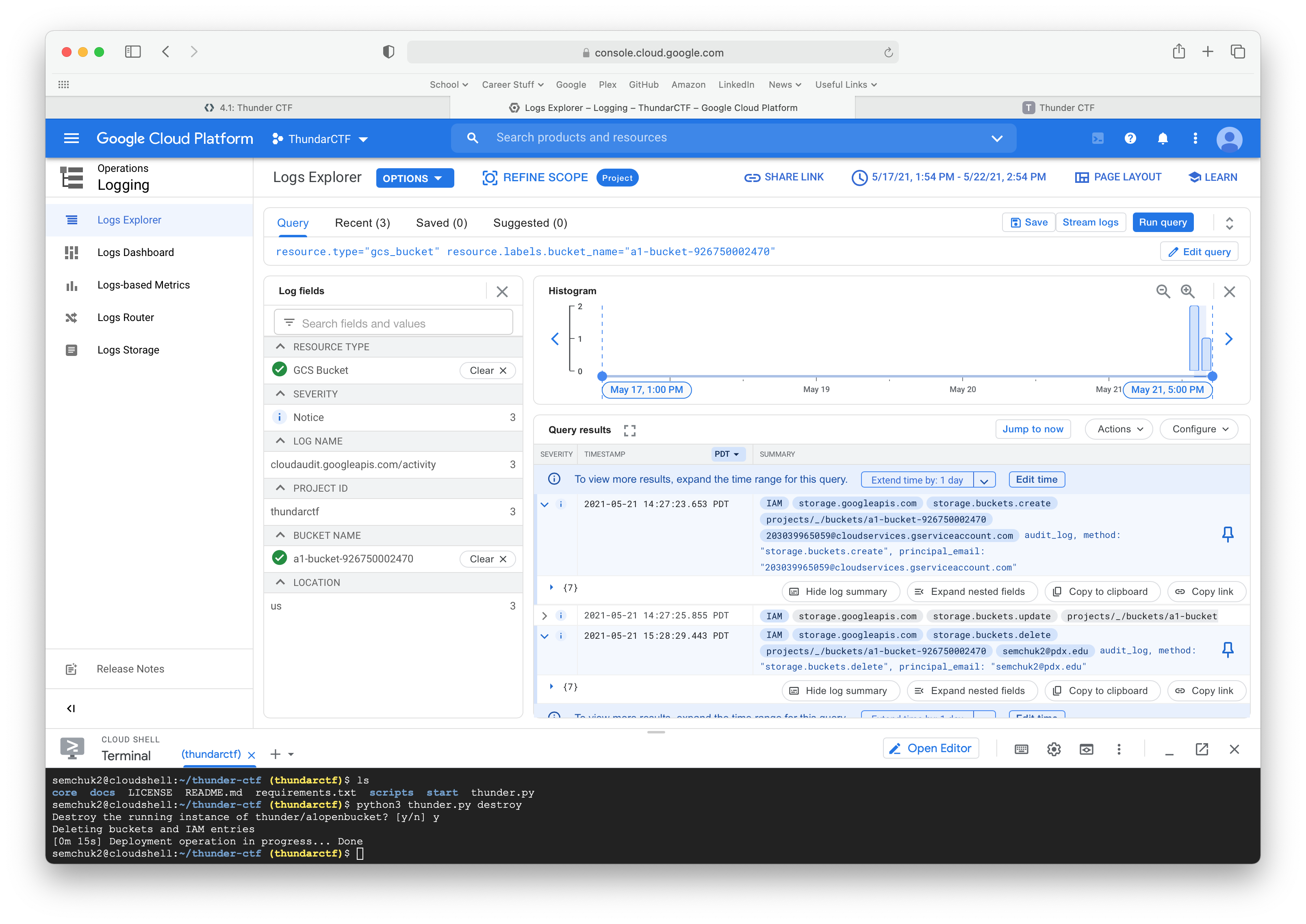
4.1.3 Take a screenshot of the secret obtained:



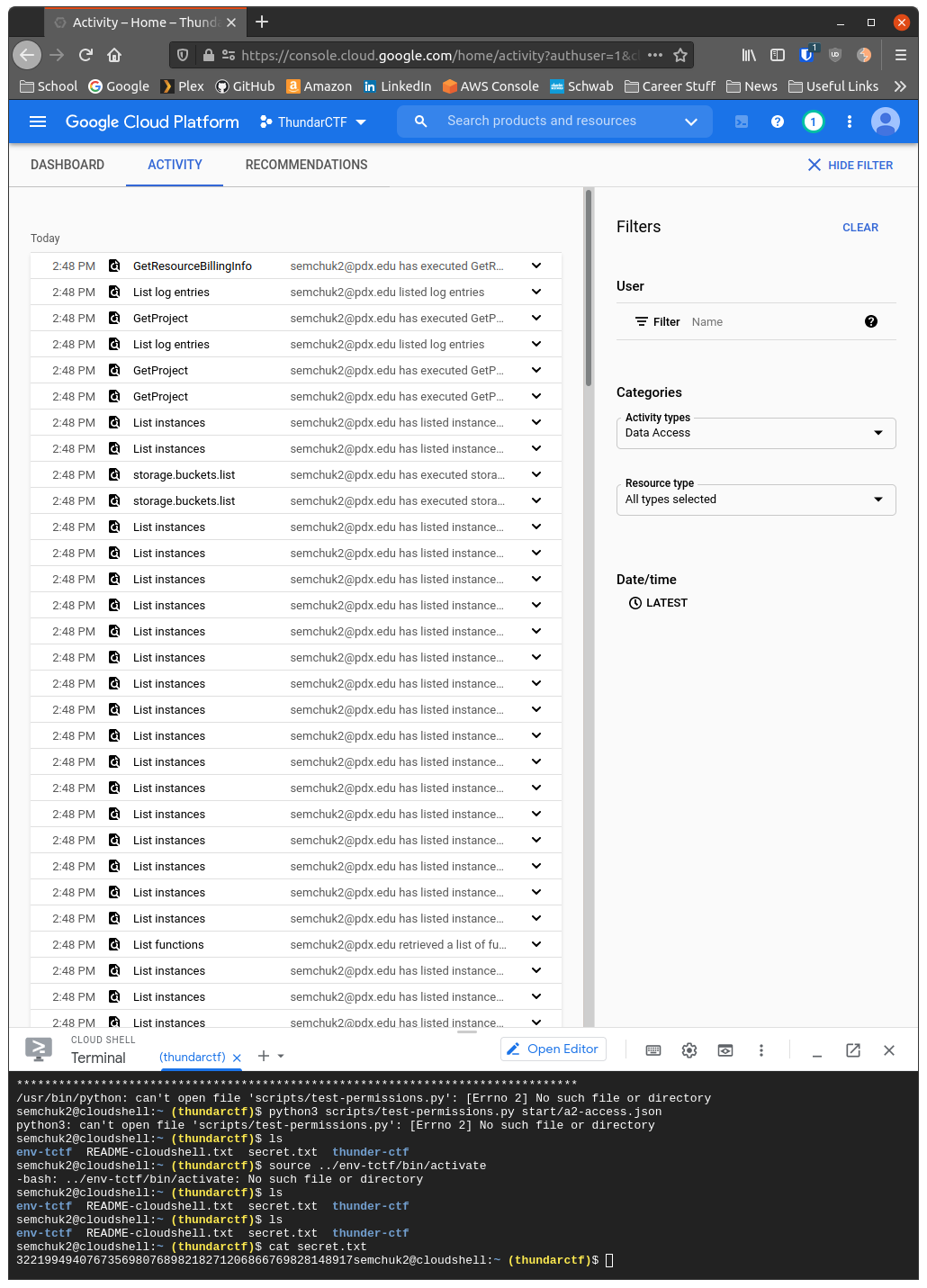
4.1.4 Examine Logs via Project Activity:



4.1.6 Clean-up Level:



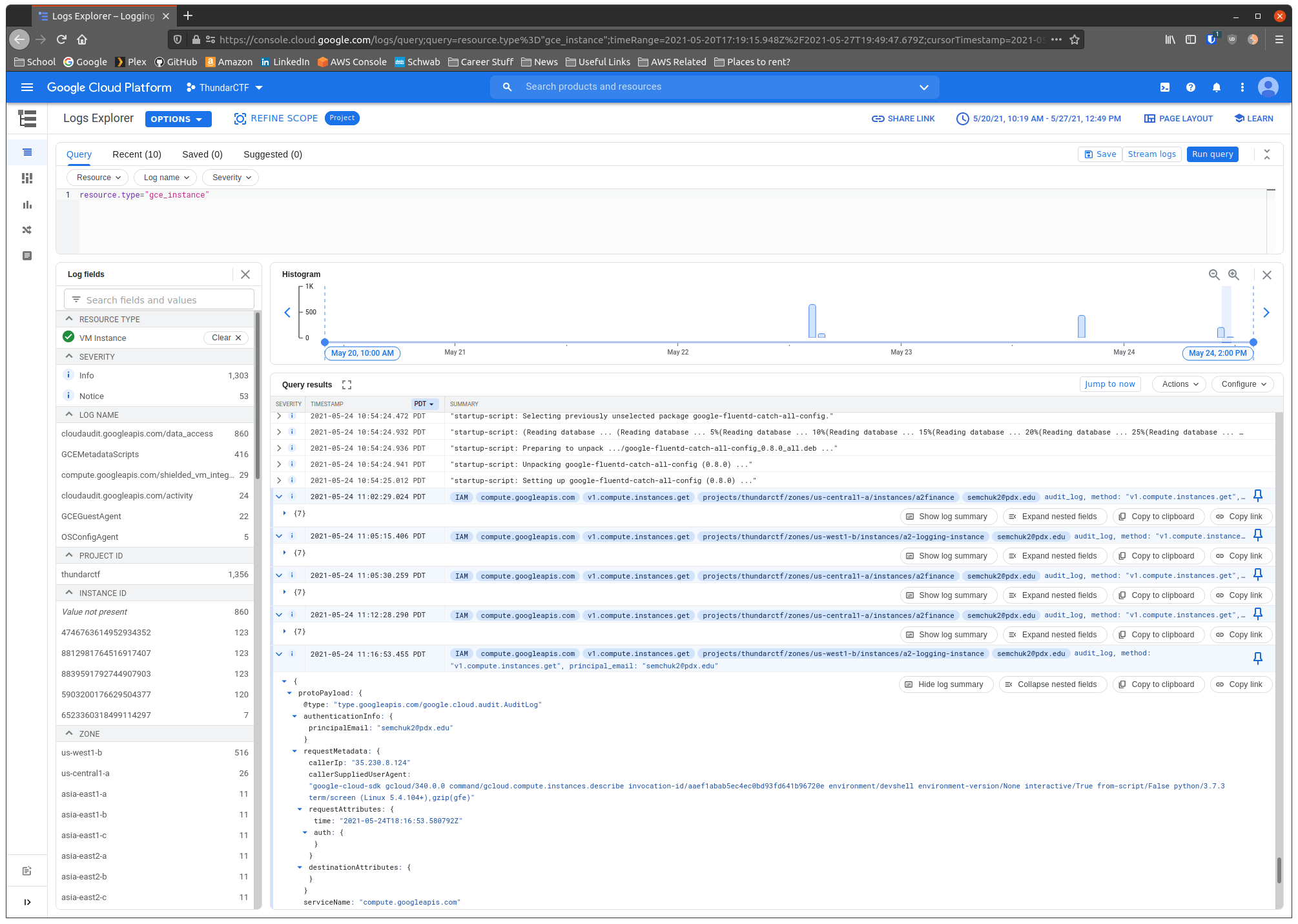
4.1.7 a2finance:



4.1.7 a2finance

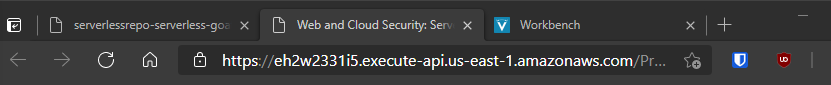


4.1.8 Examine Compute Engine logs:



Lab 4.2 Serverless Goat

4.2.8 The endpoint exposes the region it is being run in. What region does it reside in?:



It resides in the east-1 region of the USA

4.2.8 Take a screenshot of the endpoint that handles the submission

Graphical user interface, text

Description automatically generated

4.2.8 Take a screenshot of code and its associated header

Text

Description automatically generated

4.2.8 What AWS-specific headers are included?

Text

Description automatically generated

4.2.9 Test adversarial input:

What is the path to the file that is being executed?

A screenshot of a computer

Description automatically generated

It is NULL

What line of code in this file does the error happen?

at log (/var/task/index.js:9:49)

What line of code called the function that the error happens in (e.g. the call stack)?

at exports.handler (/var/task/index.js:25:11)

4.2.10 Command injection:

A computer screen capture

Description automatically generated with low confidenceUse command injection to obtain the working directory the application is run in. Show a screenshot of the result at the end of the page returned.

4.2.10 Then use command injection to obtain a listing of the directory and show the files that are there:

Graphical user interface

Description automatically generated

4.2.10 Use command injection to dump out the source file that implements this Lambda function.

A screenshot of a computer

Description automatically generated

4.2.10 Lambda functions have a timeout value of 5 minutes. Use command injection to trigger this timeout and take a screenshot of the error that results from invocations that take too much time to run.

A computer screen capture

Description automatically generated with medium confidence

4.2.11 Reverse-engineer the source

Show the line of code that the command is injected into.



Show the packages that this file requires. How is each package used in this code?



Find the part of the code that writes the converted document into the S3 bucket. How is the name of the bucket obtained by the application code?



What database is being used to store information about requests? What information is stored? How does the application obtain the name of the table that this information is stored in?

Text

Description automatically generated

Use command injection to dump the contents of the package manifest file for the application. What version of packages does the source file depend upon? Look up this package and version to determine how old the package is? Find any known vulnerabilities in this package.

Graphical user interface, text

Description automatically generated

Vulnerability found:

Graphical user interface, text, application

Description automatically generated

How does the application use this package in its operation? What would be the impact of a vulnerability in this package (if any)?

It is used as a key, and then put into a s3 bucket:

Text

Description automatically generated

4.2.12 Information Exposure:

Show the variable that stores the bucket name in a screenshot

Text

Description automatically generated

Show the table name that is used to store activity information from the application

PATH=/var/lang/bin:/usr/local/bin:/usr/bin/:/bin:/opt/bin TABLE\_NAME=serverlessrepo-serverless-goat-Table-12UE822VMCZYY AWS\_DEFAULT\_REGION=us-east-1



4.2.12 Find a document that has been converted by another user previously and use its object key to get access to the converted data

Text

Description automatically generated

4.2.13 Expose and leverage credentials

Graphical user interface, text

Description automatically generated

4.2.14 Excess permissions

Does the application ever need to read from the table specified?

No, it shouldn’t need to read, since dynamodb is a log file, and only needs to write to it. Another instance should be used to read from this with proper permissions.

What permissions might not be necessary in this policy?

Permissions management. This account should not be able to manage its own permissions, rather just use what it is specified to use as a non admin account.

4.2.15 Data exfiltration:

My IP Address:

A screenshot of a computer

Description automatically generated with medium confidence

Ip Address 67.171.227.105

A screenshot of a computer

Description automatically generated with medium confidence

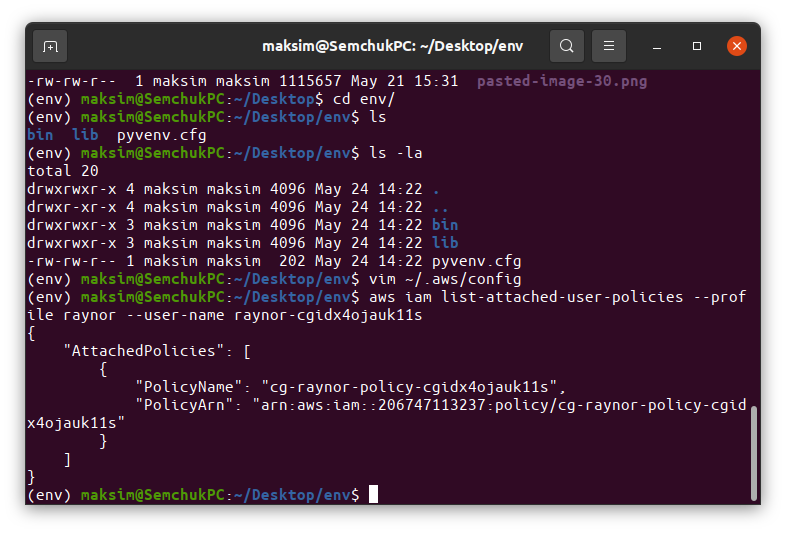
Using the profile, show a screenshot of the objects in the S3 bucket that the function is using to store its results.

A picture containing text, electronics

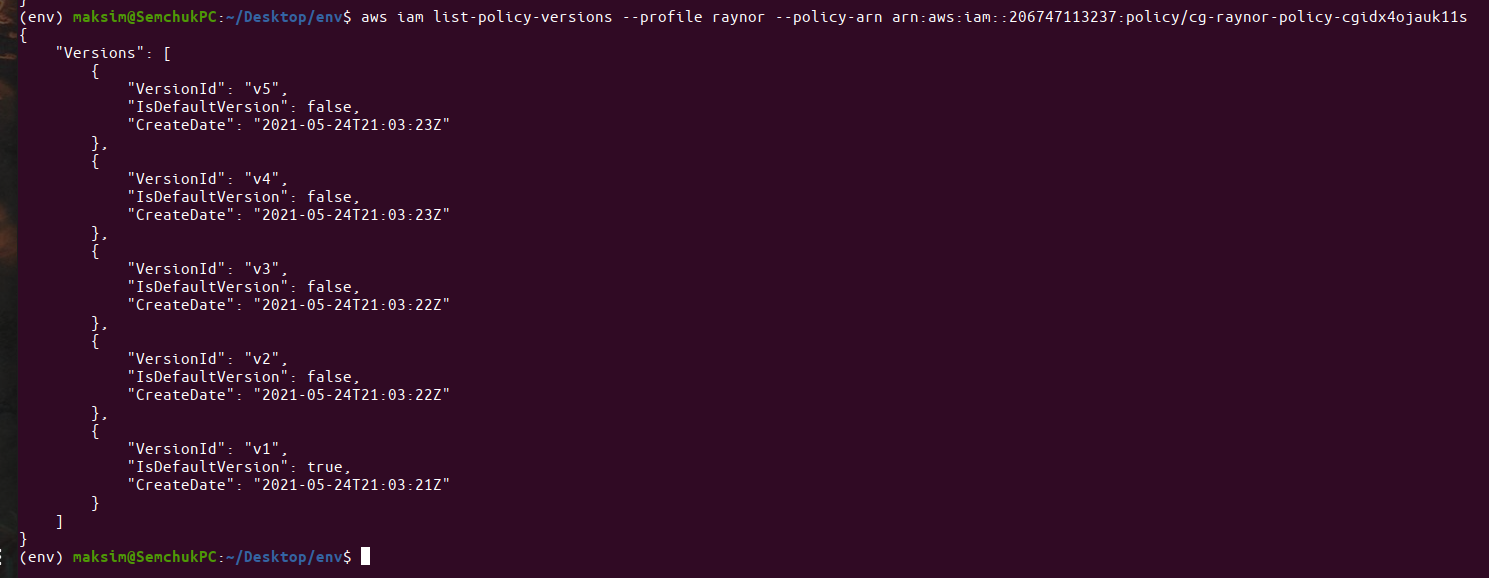
Description automatically generated

Labs 4.5 CloudGoat

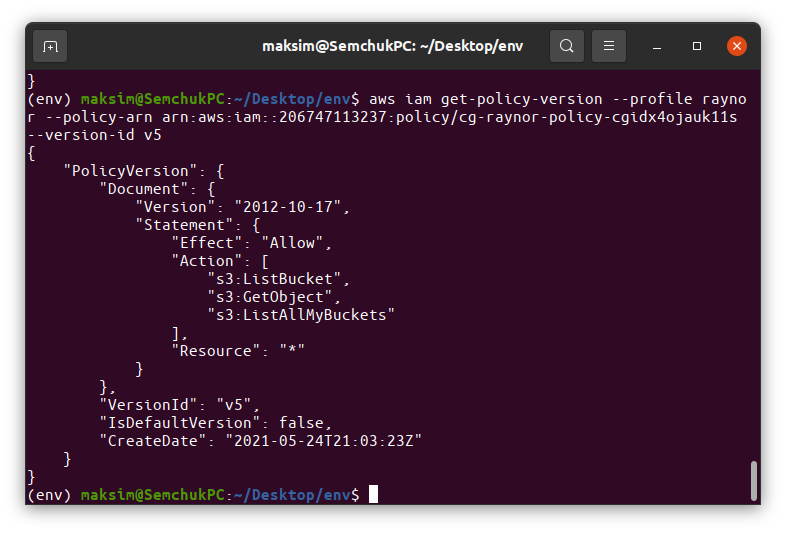
4.5.3 Show the policies attached to the credentials given:



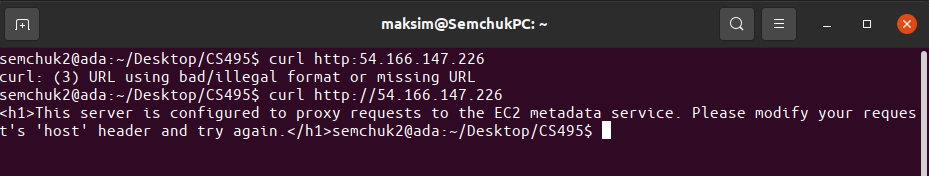
4.5.3 Which version of the policy is set as the default?



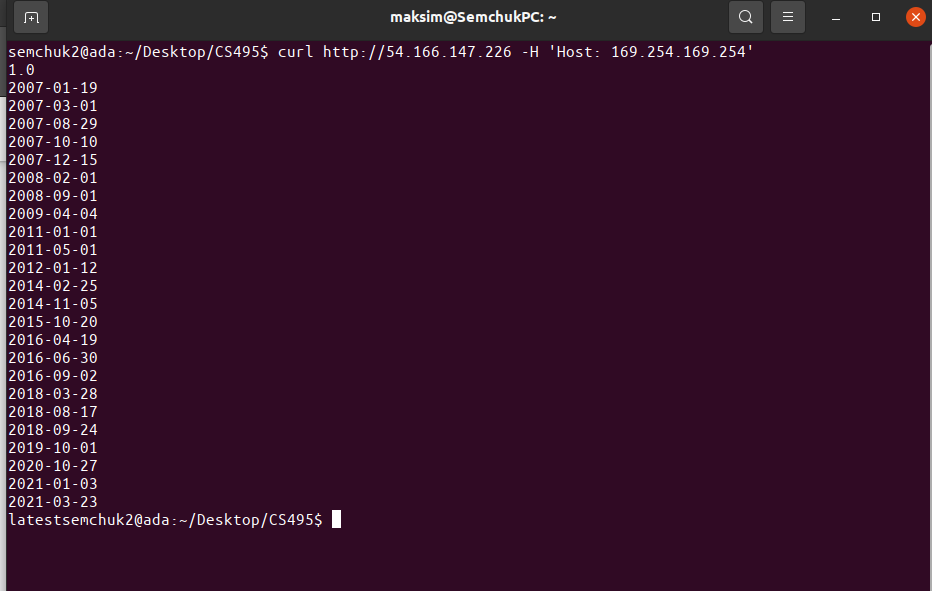
4.5.3 Show the output of the version in which all actions have been allowed (e.g full admin privileges)



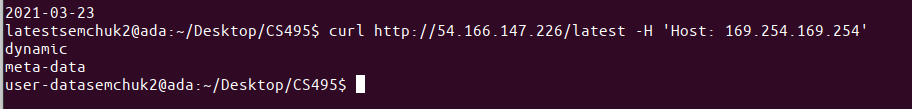
4.5.5.1 Show the error page returned.



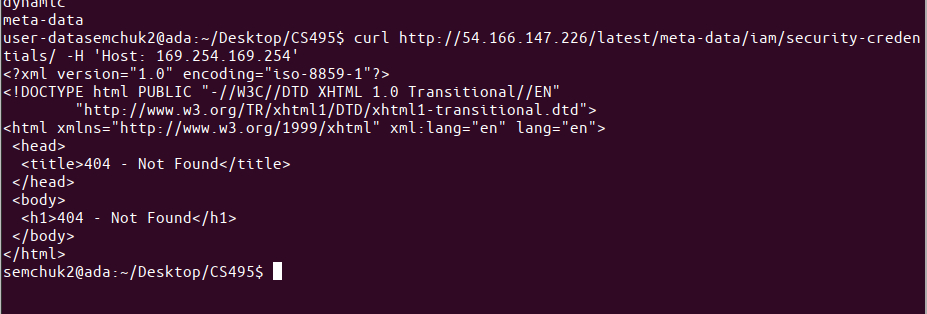
4.5.5.2 Show the results.



4.5.5.2 Show its contents via the following command:



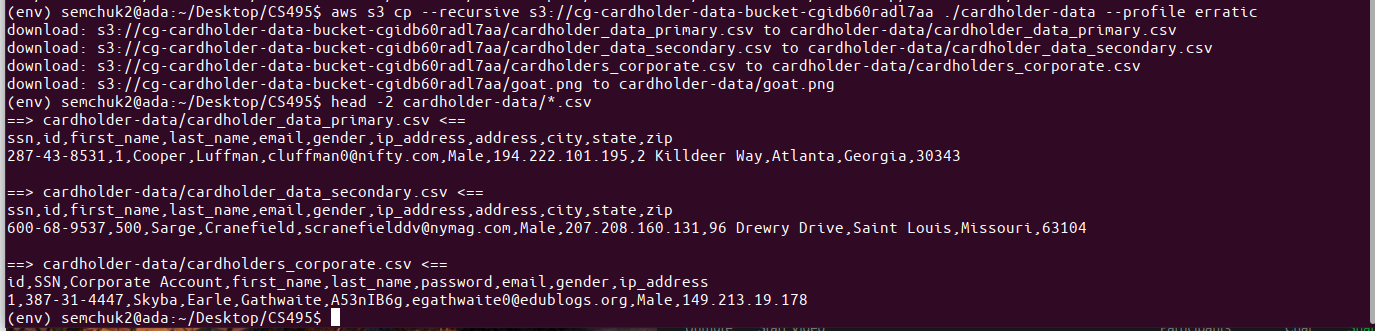
4.5.5.3 To do so, show the name of the AWS role the following command exposes:



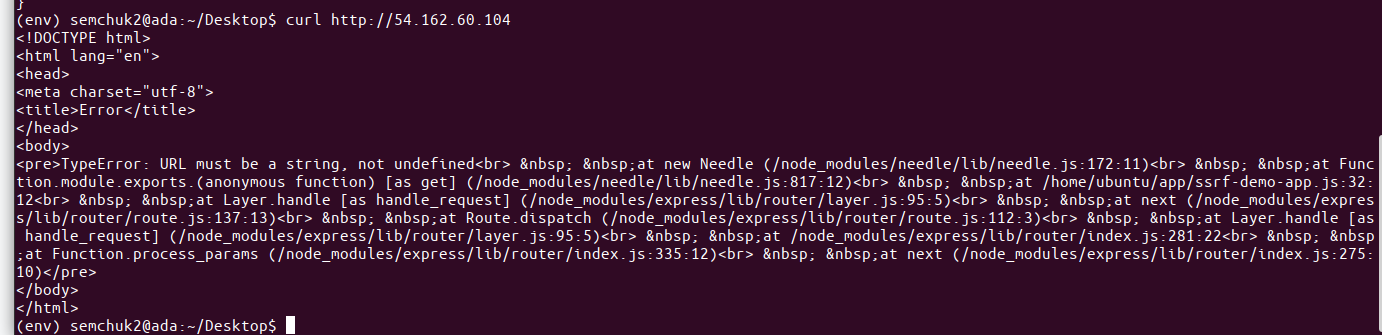
4.5.5.3 Then, show the credentials associated with the role.



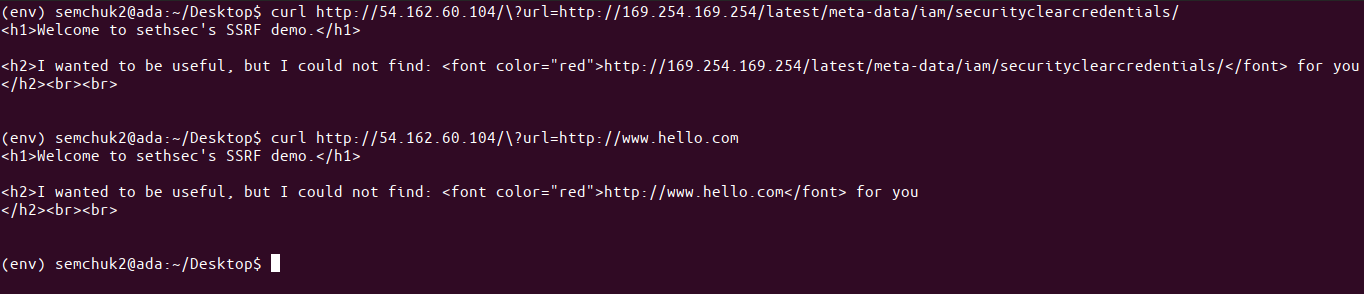
4.5.6.6 Show the first two lines of each of the CSV files you have copied over from the bucket via the command below.



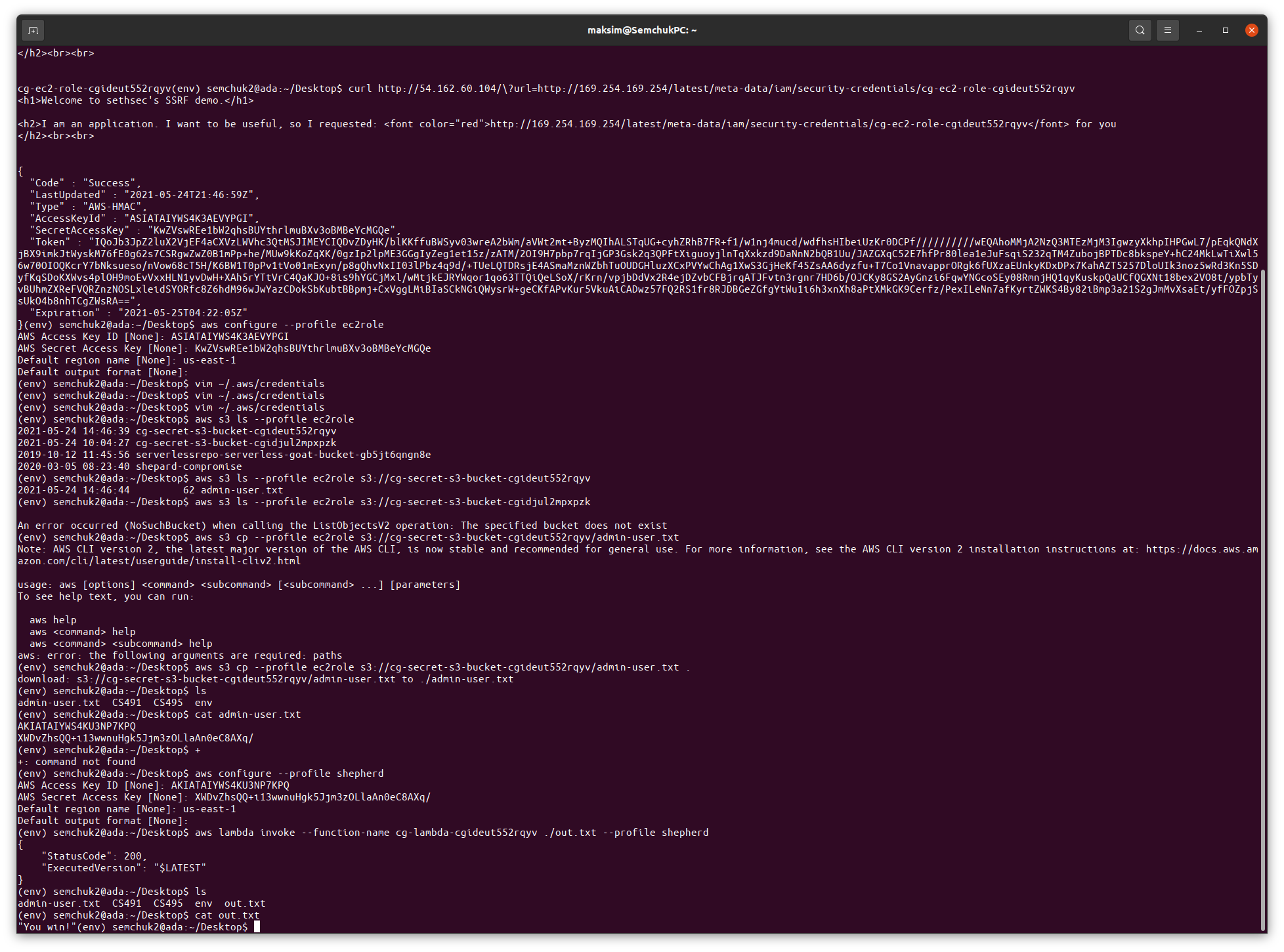
4.5.8.8.1 Take a screenshot of the page that is returned.



4.5.8.2 Take a screenshot showing the information associated with the role.



4.5.9.5 Take a screenshot of the output in out.txt



4.5.13.8 Show a directory listing of the account you've logged into.

A picture containing text, screenshot

Description automatically generated

4.5.13.11 Show the contents of the file.

Text

Description automatically generated

4.5.14.14 Show the table that is stored and its contents.

Text

Description automatically generated