**Vulnarability name: Exposure of S3 bucket**

**How to configure aws cli(*command line interface*):**
- First you got to have linux desktop or we can use cloud to use that.
- Then to install aws cli we can just google it and get the command to install or go to amazon we can find the command there since i have ubuntu i basically used command(apt-get install awscli) to install it.

**Steps to complete the first challenge of flaws.cloud:**
- Go to flaws.cloud and go to challenge the first level.
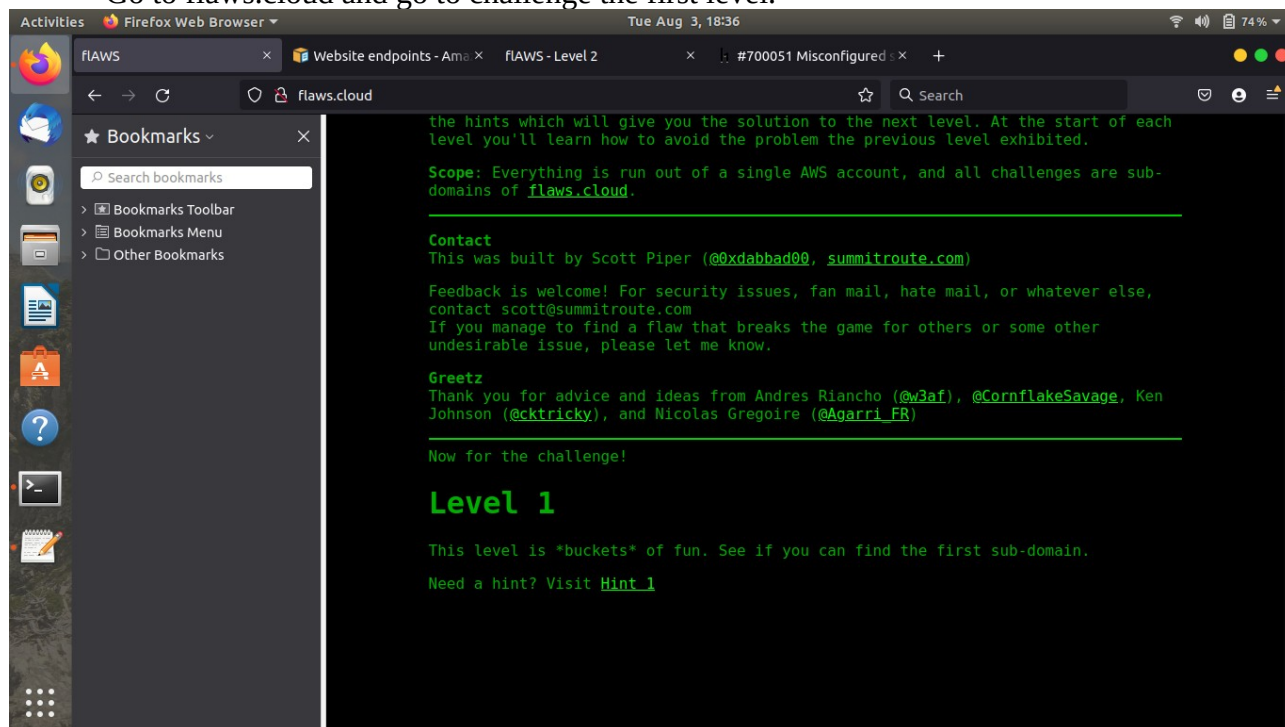
- Check flaws.cloud ip address at the terminal
- Then put ip address and we'll get some thing like s3-website-us-west-2.amazonaws.com.
- Then put s3 –region us-west-2 ls flaws.cloud –mo-sign-request to get the list items present in the s3 bucket of flaws.cloud.
- When the above step is complete we'll see s3 bucket listed is the terminal why? Cause this s3 is publicly available to everyone and after that we'll select last in the list secret-dd02c7c.html.
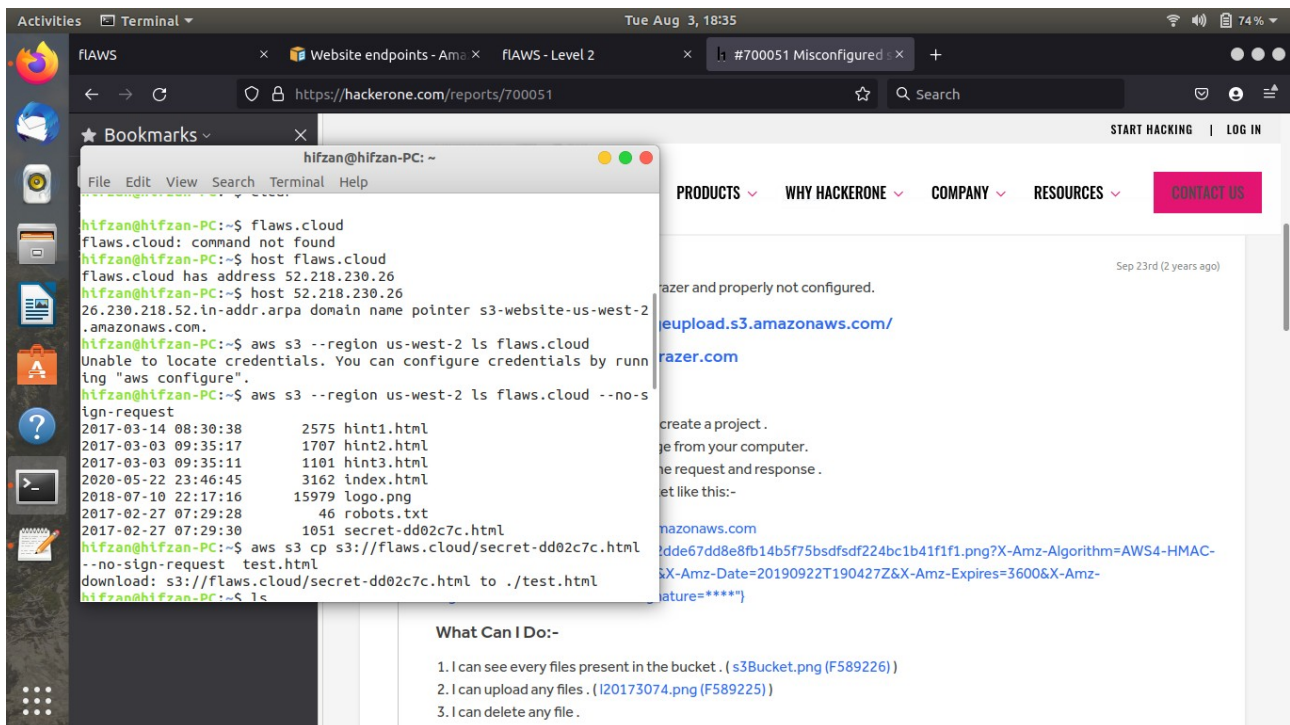
- After that we'll copy it to see what is actually present over there to copy it we basically to put command aws s3 cp s3://flaws.cloud/secret-dd02c7c.html –no-sign-request test.html.
- After that it'll download the file in test.html and we can directly check it's location in the computer or use command check as well.
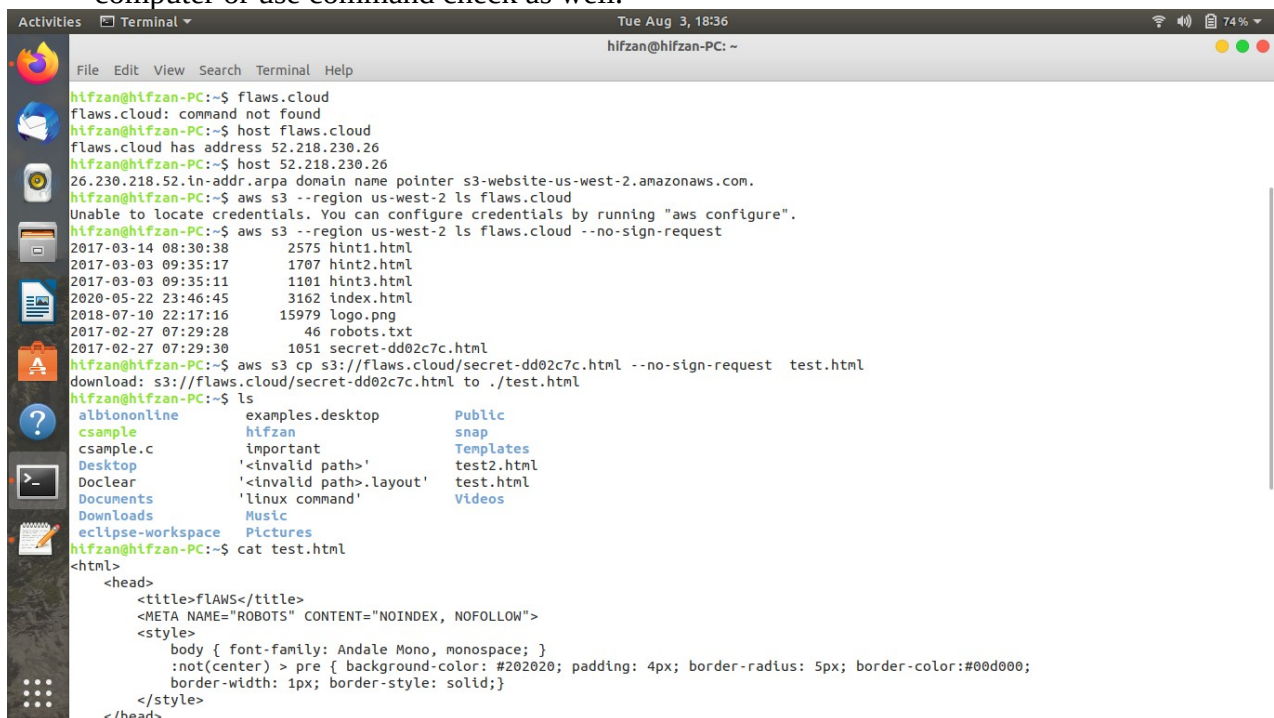
- Then we'll check what is inside and to do that we'll type command cat test.html and it'll congrats us to find the secret file and give us the link level2.
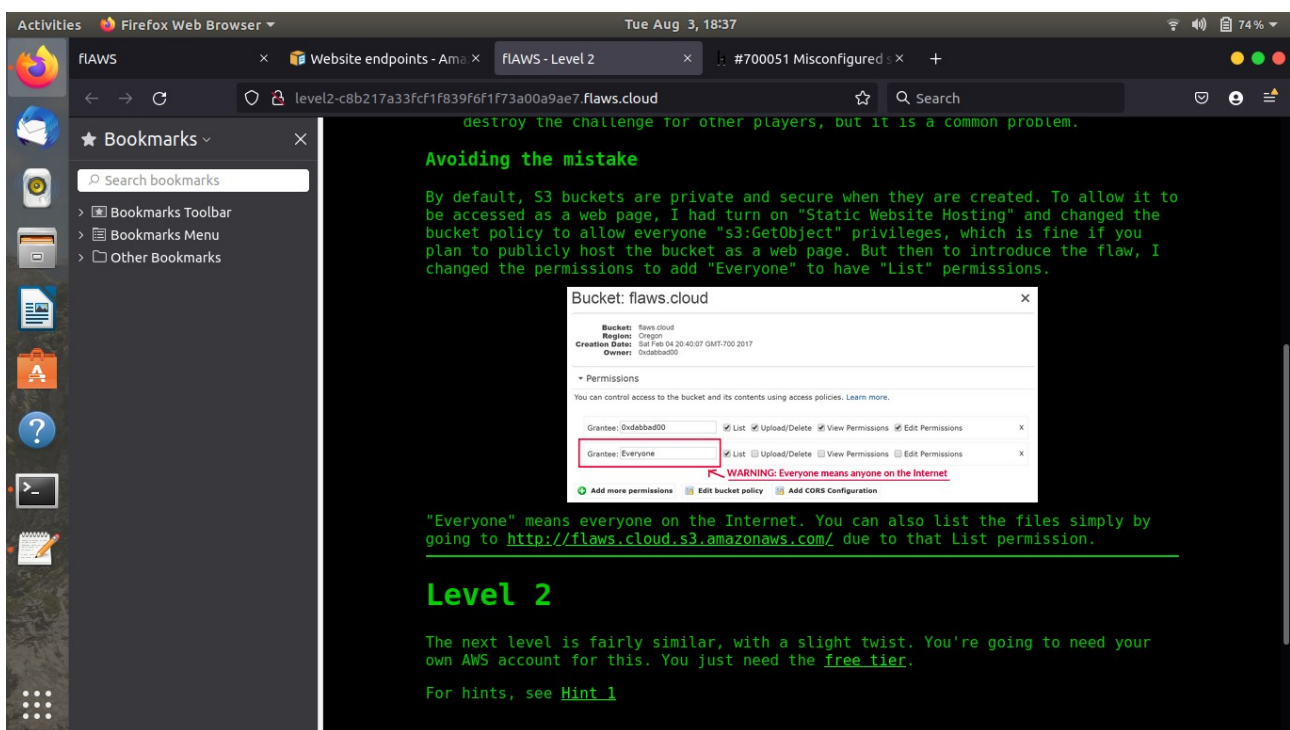
Basically the mistake was the bucket where all the file was available to everyone which voilated the privacy.