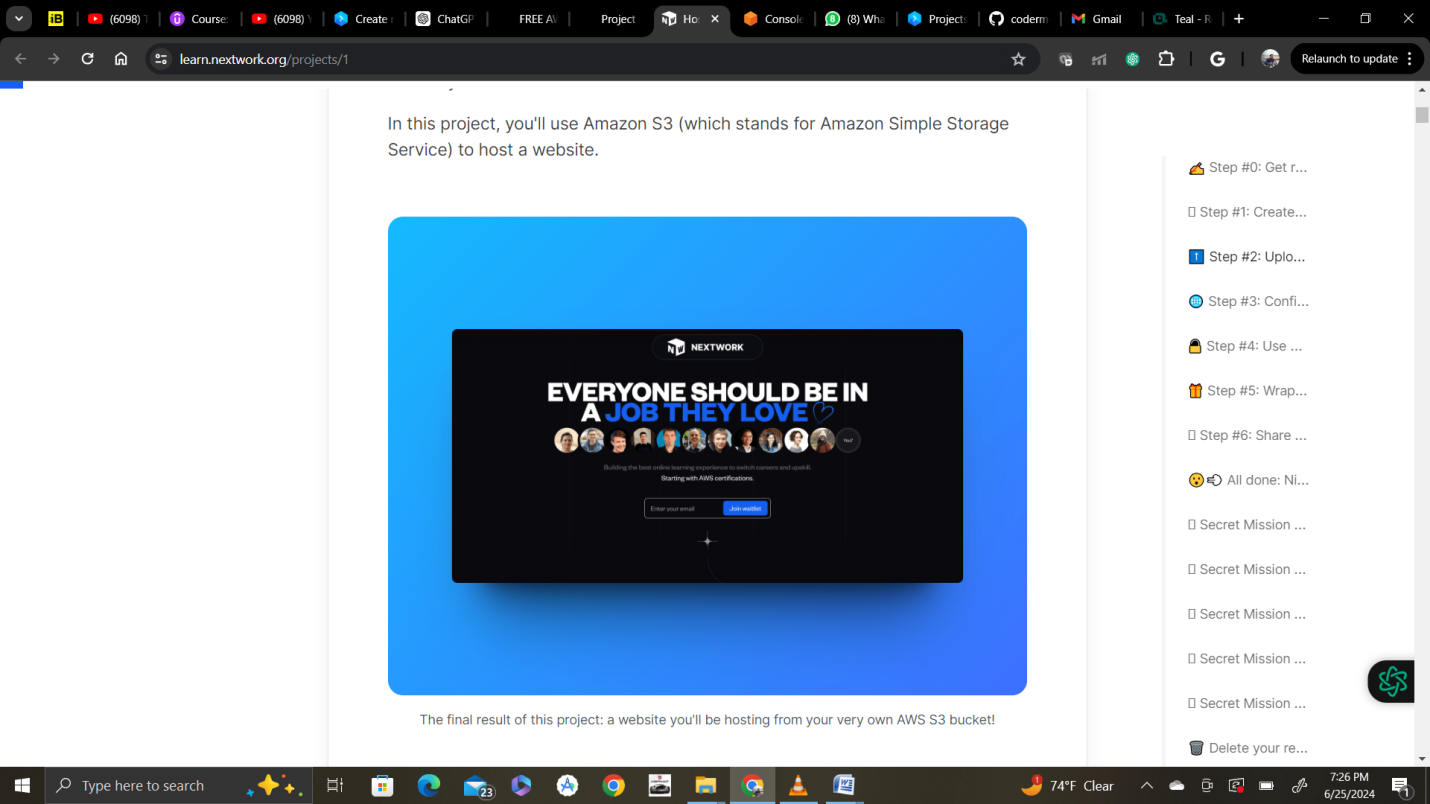
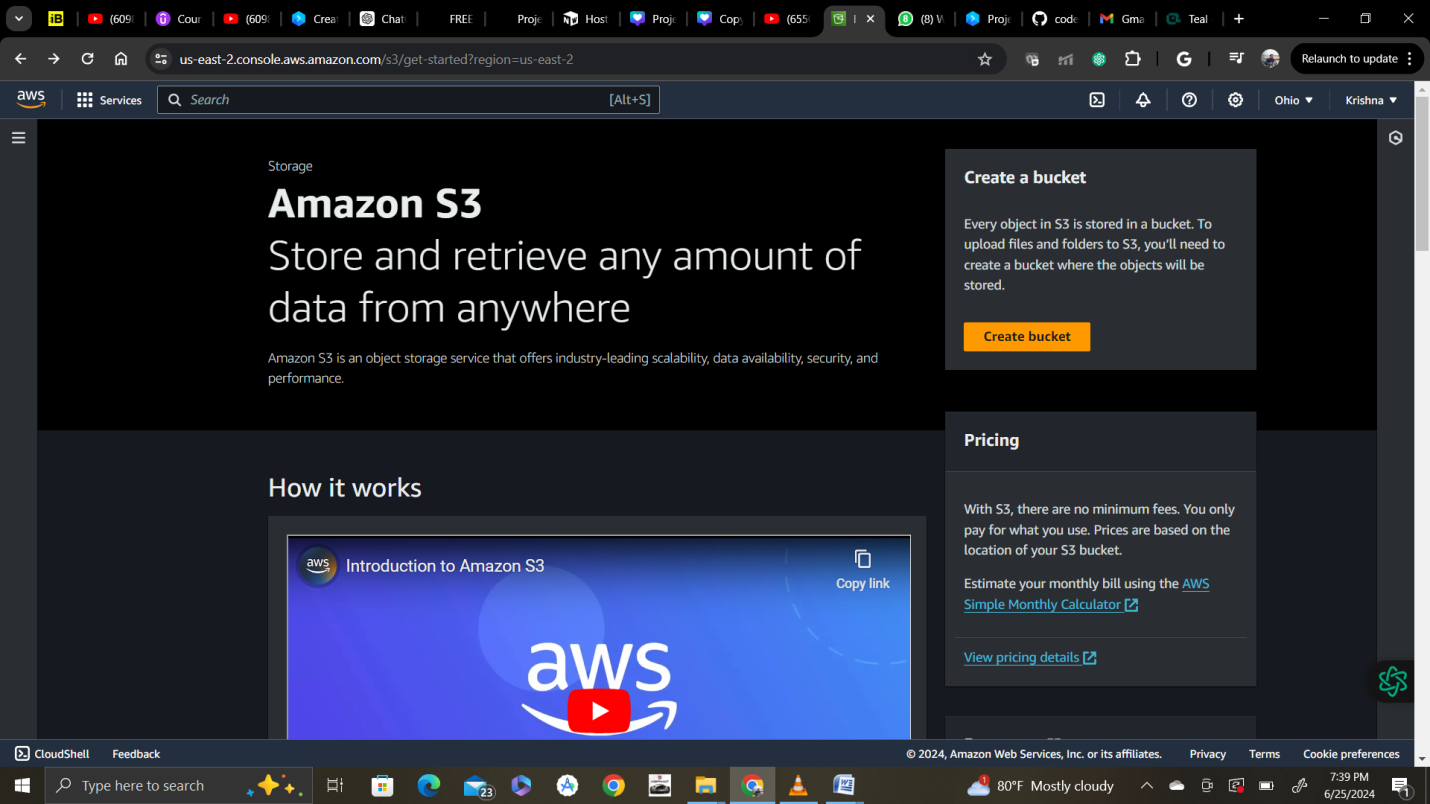
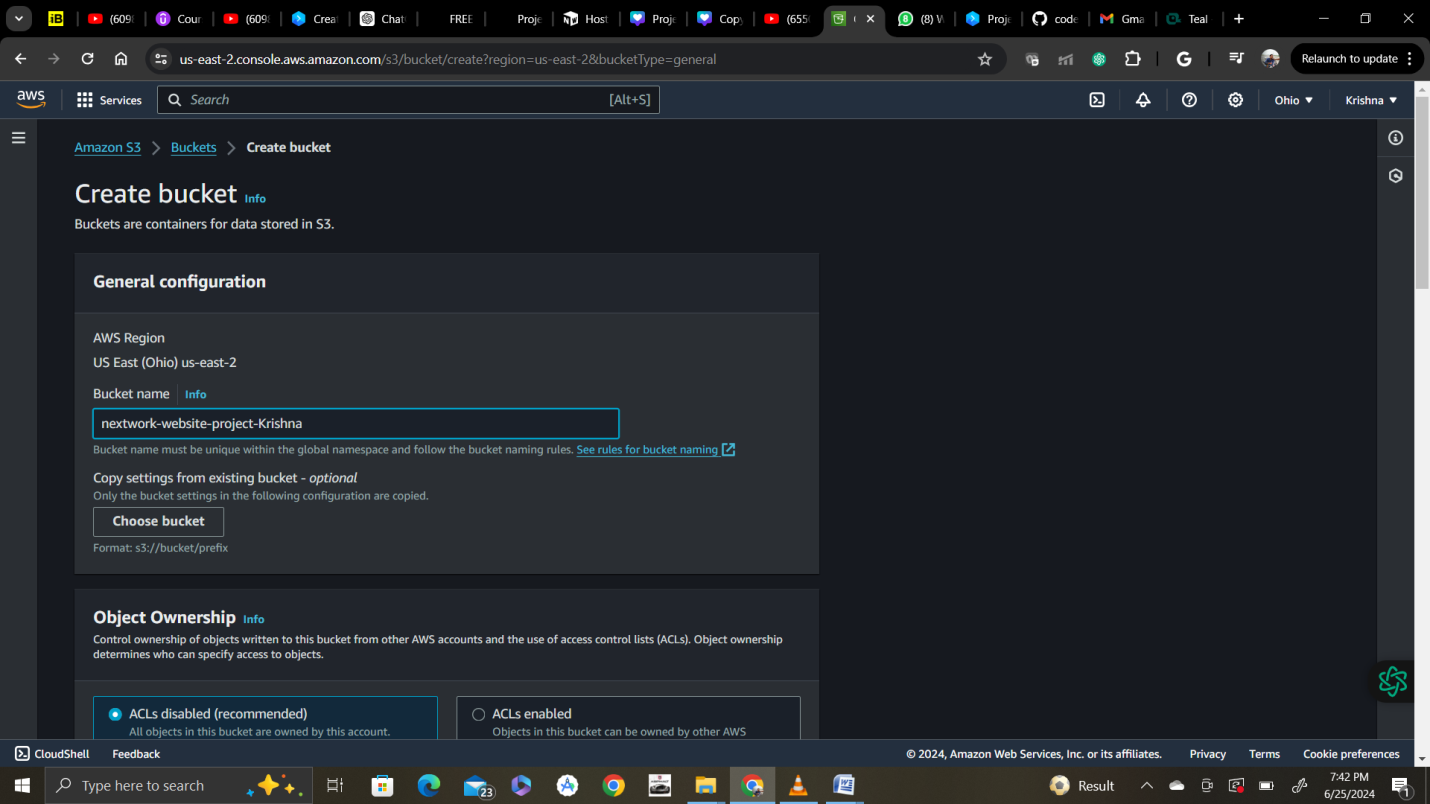
Final output result expected:



First Search for S3 in the AWS console and click on create bucket

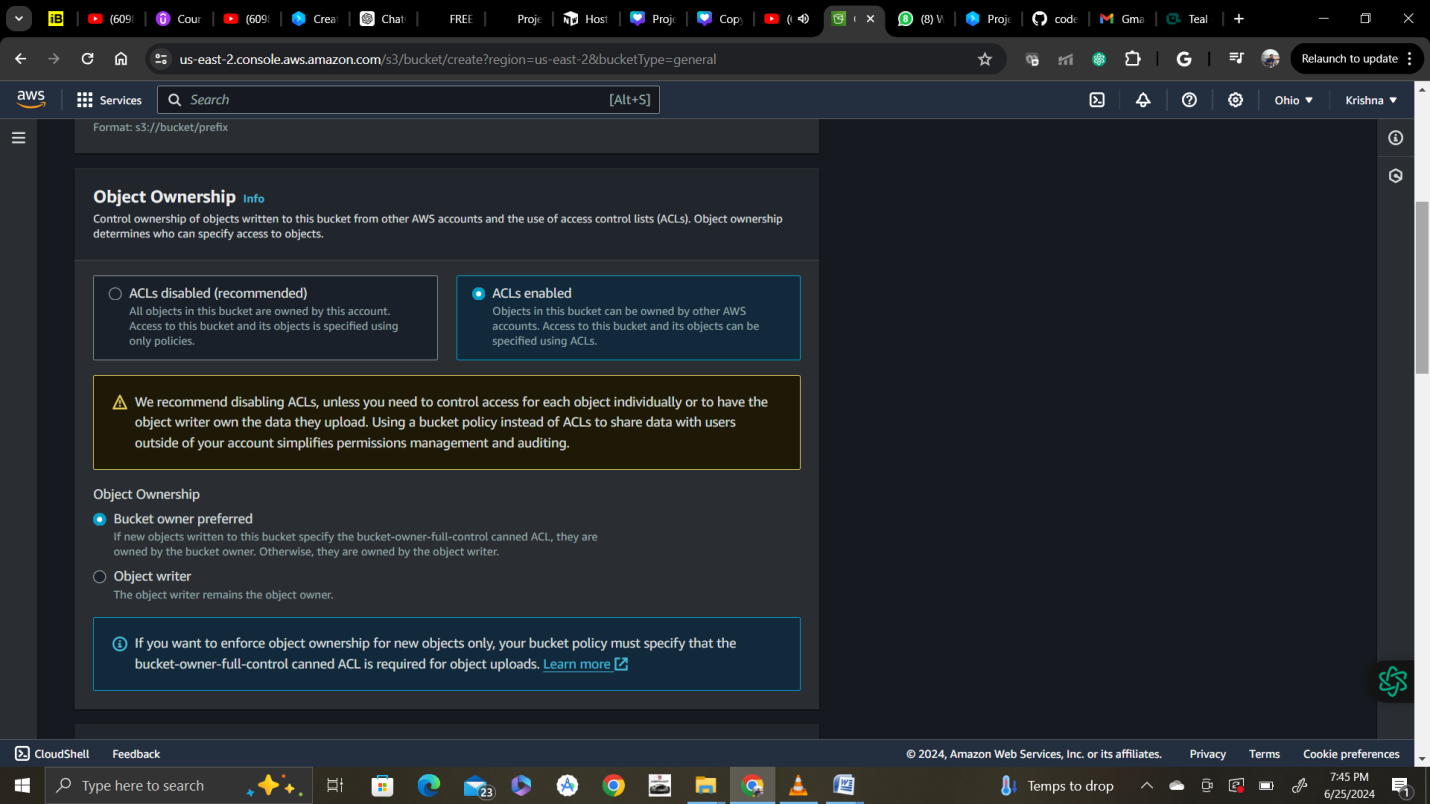


Select region and then bucket name as below



 An S3 bucket name is globally unique, and all AWS accounts share the namespace. After you create a bucket, **no other AWS account in the entire world** can use your bucket's name unless you delete the bucket.

Select ACLs(access control lists) enabled and Bucket Owner Prefferred



**Ooo what are ACLs (Access Control Lists)?**  
An **ACL** = a set of rules that decides who can get access to a resource.

Enabling ACLs in this S3 setup lets you control who can access and do things with the objects (i.e. website files) you upload into your bucket.

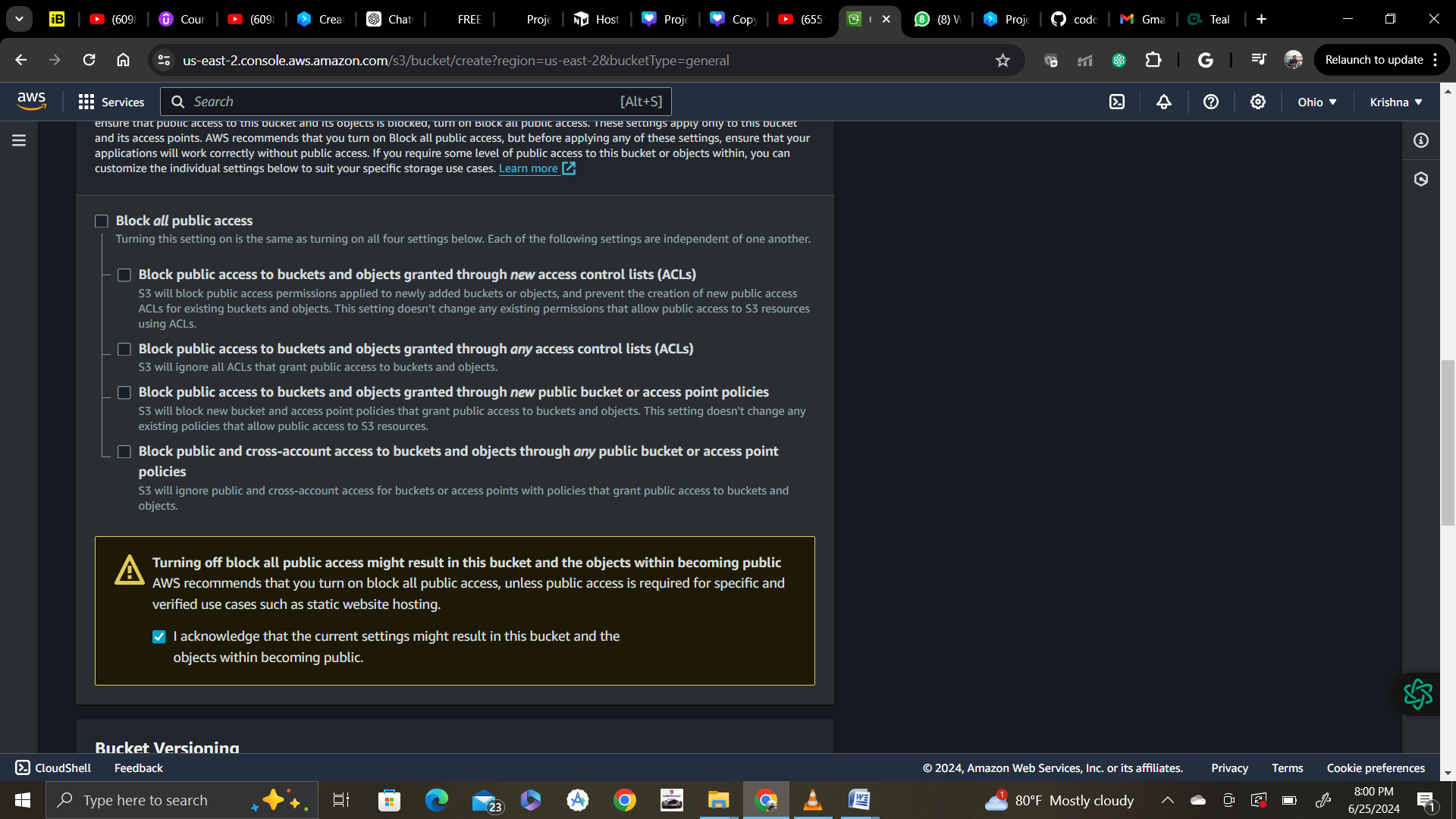
With ACLs, different AWS accounts can own and control different files in your bucket.

The warning that pops up suggests that it's **simpler** to use something called "bucket policies". While they let you control access for the entire bucket (e.g. making the entire bucket and its objects public), bucket policies don't give you fine grained control over individual objects in your bucket.

Bottom line, if you know that the entire bucket contains no sensitive information, you can use a bucket policy. But if there's even one object in the bucket that you want to keep private, use ACLs.

In this exercise, we're enabling ACLs to show you how they work.

Then clear check box of Block all public access and select “ I acknowledge that the current settings might result in this bucket and the objects within becoming public.”

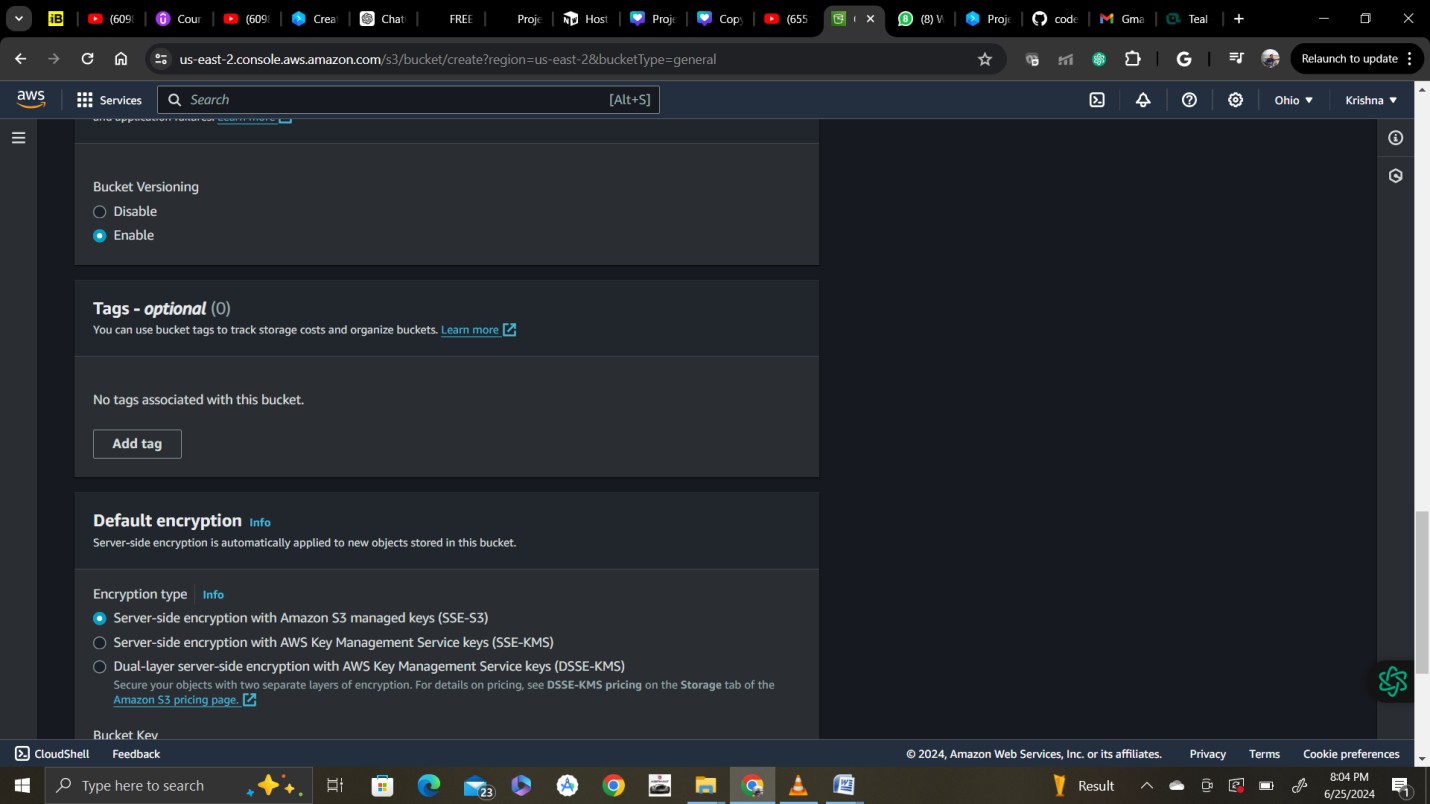


**A yellow banner has popped up!** This banner is telling us that the bucket and its objects might become public if we untick the checkbox. This is what we want to host a public website!

Step 1:

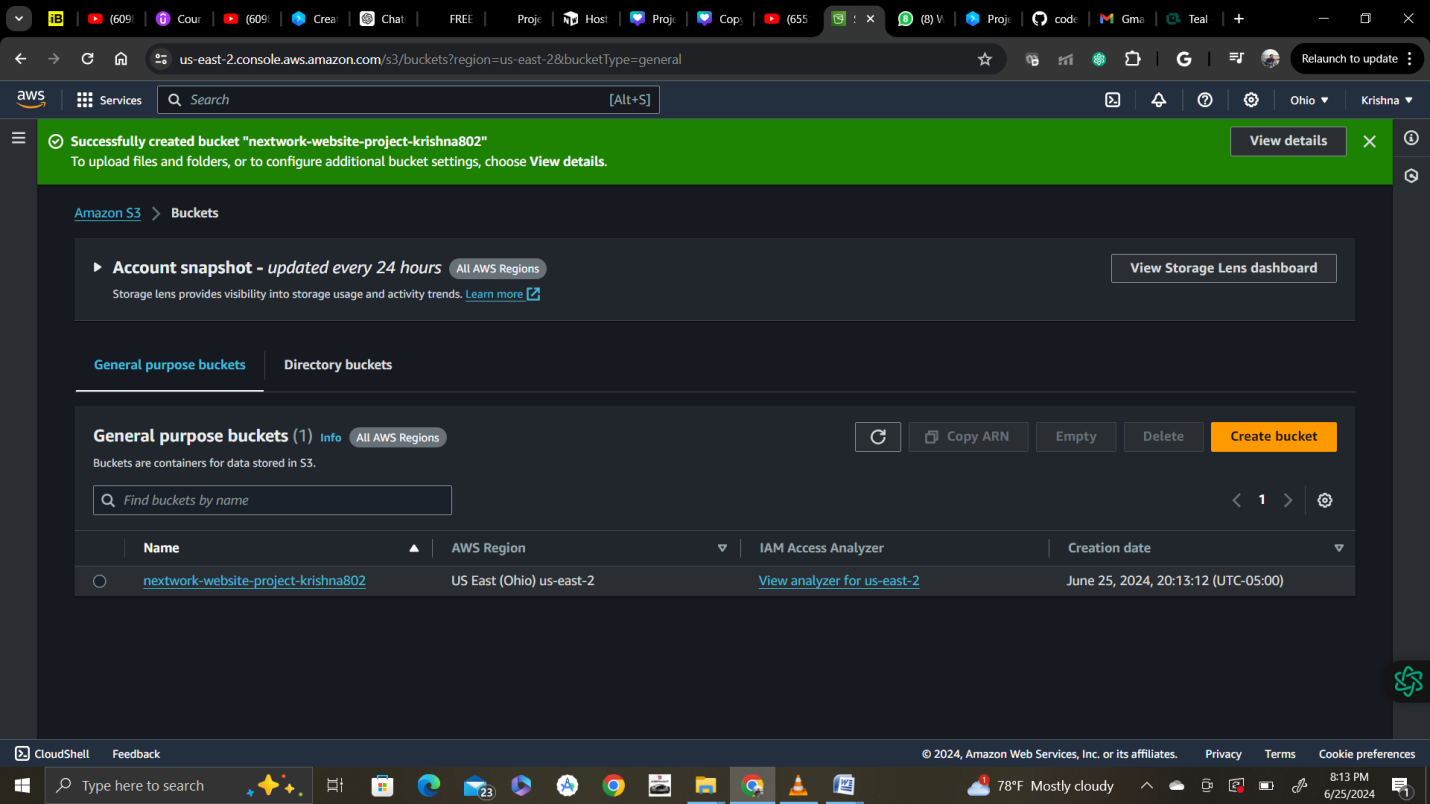
 Public access to buckets is blocked by default. Because the files in your static website will need to be accessible through the internet, you must permit public access.

For bucket Versioning turn on ( enable)

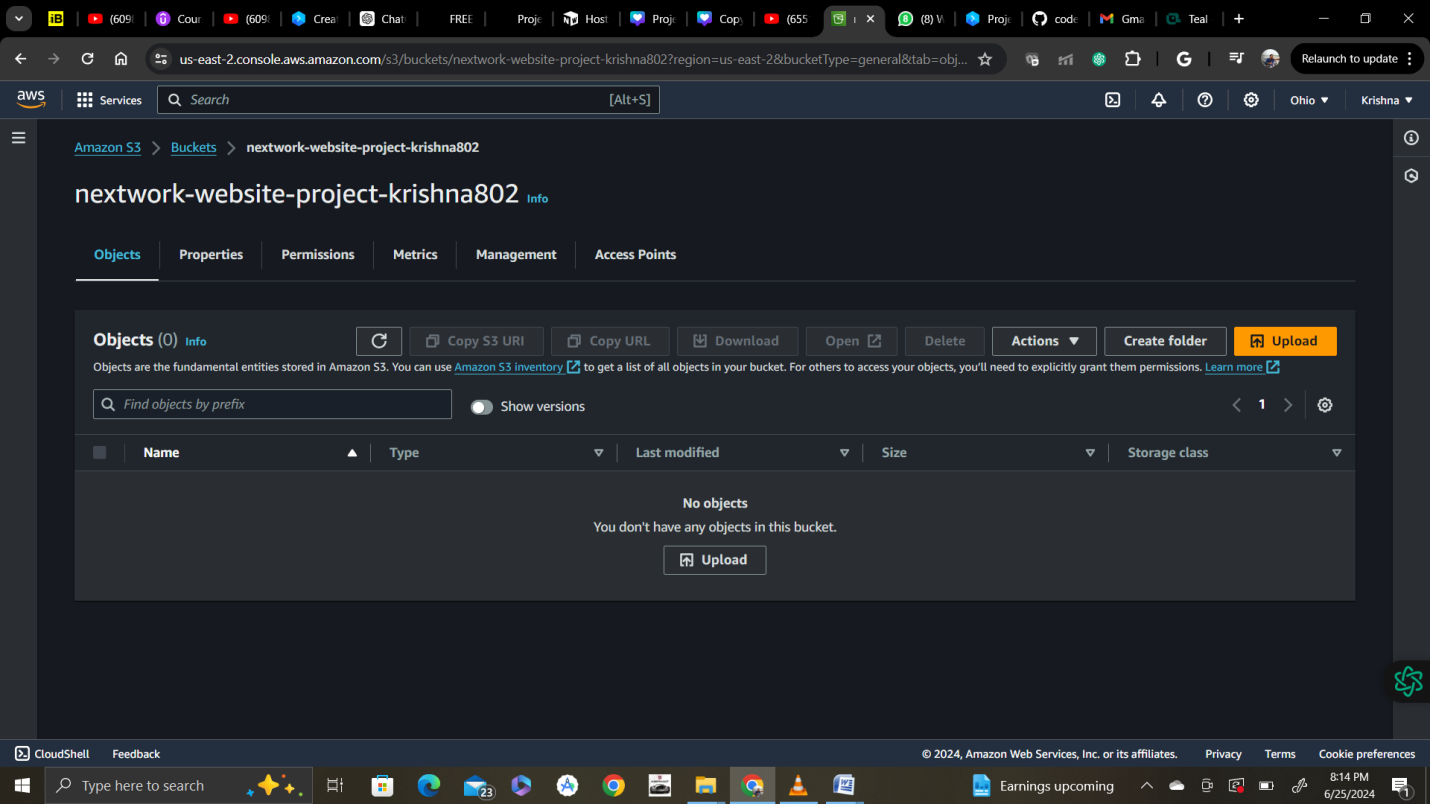


Once you turn on (enable) bucket versioning, you can't turn it off. We'll show you why we've enabled this as a last step in this exercise.

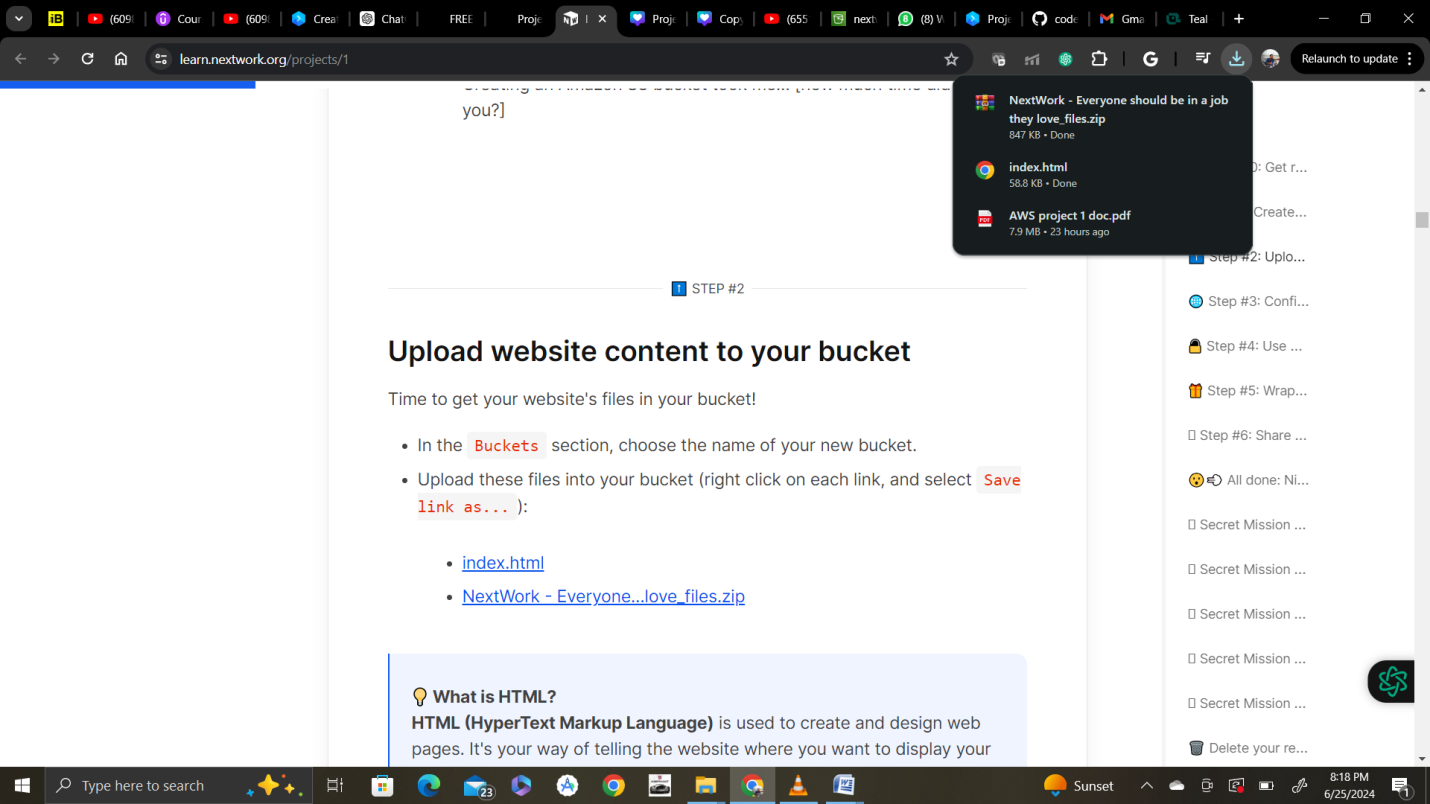
Keep default encryption and then create Bucket.



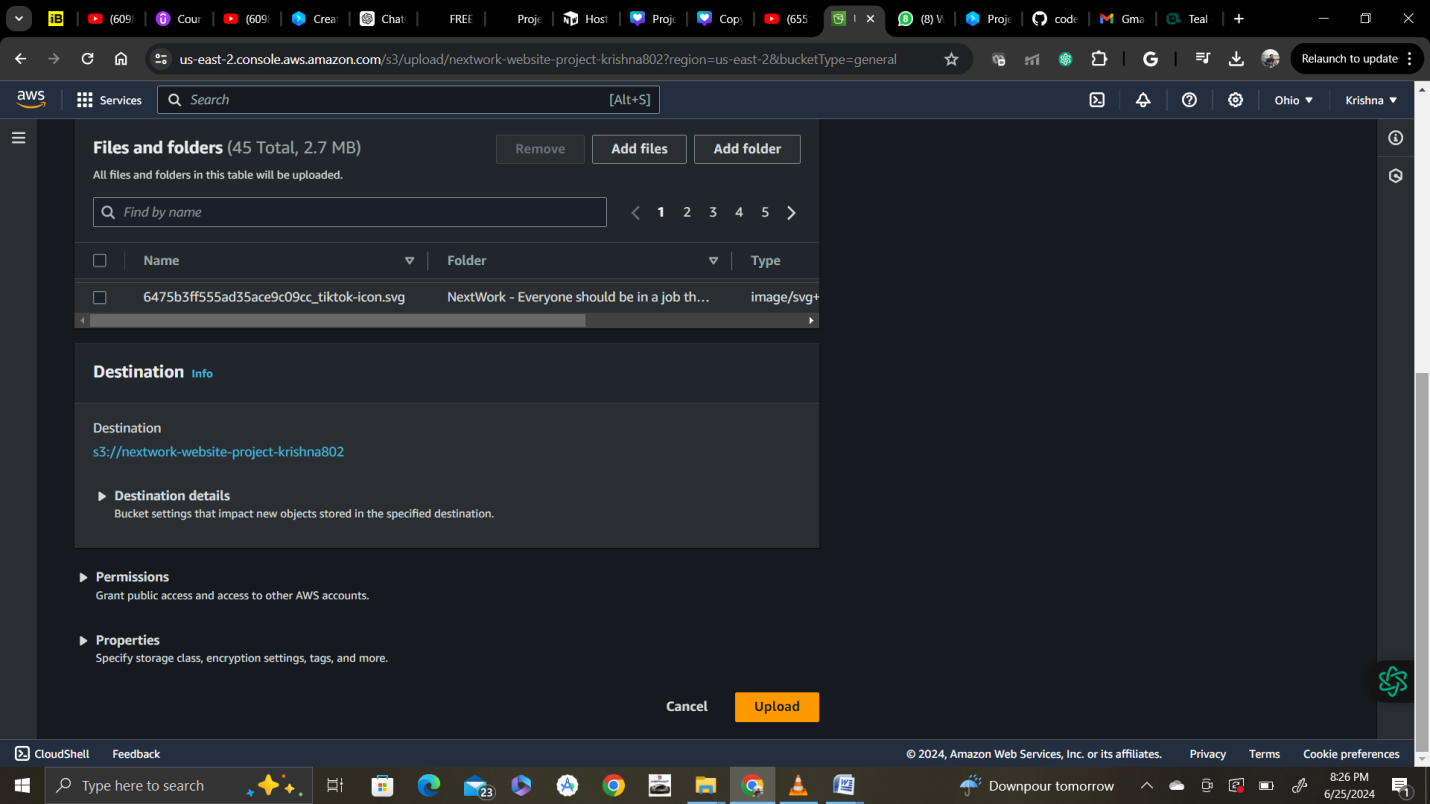
Next upload website content to the bucket by clicking on bucket

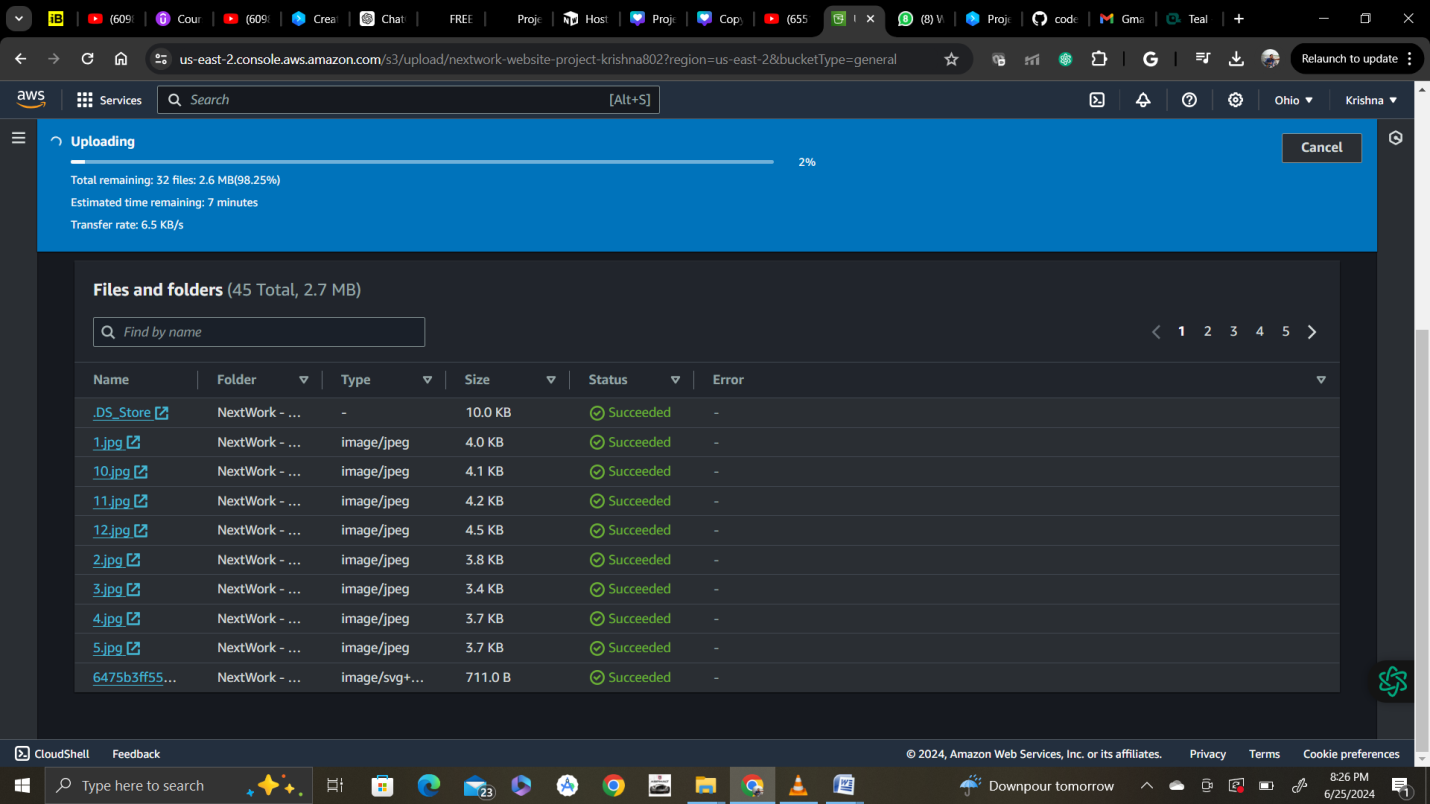


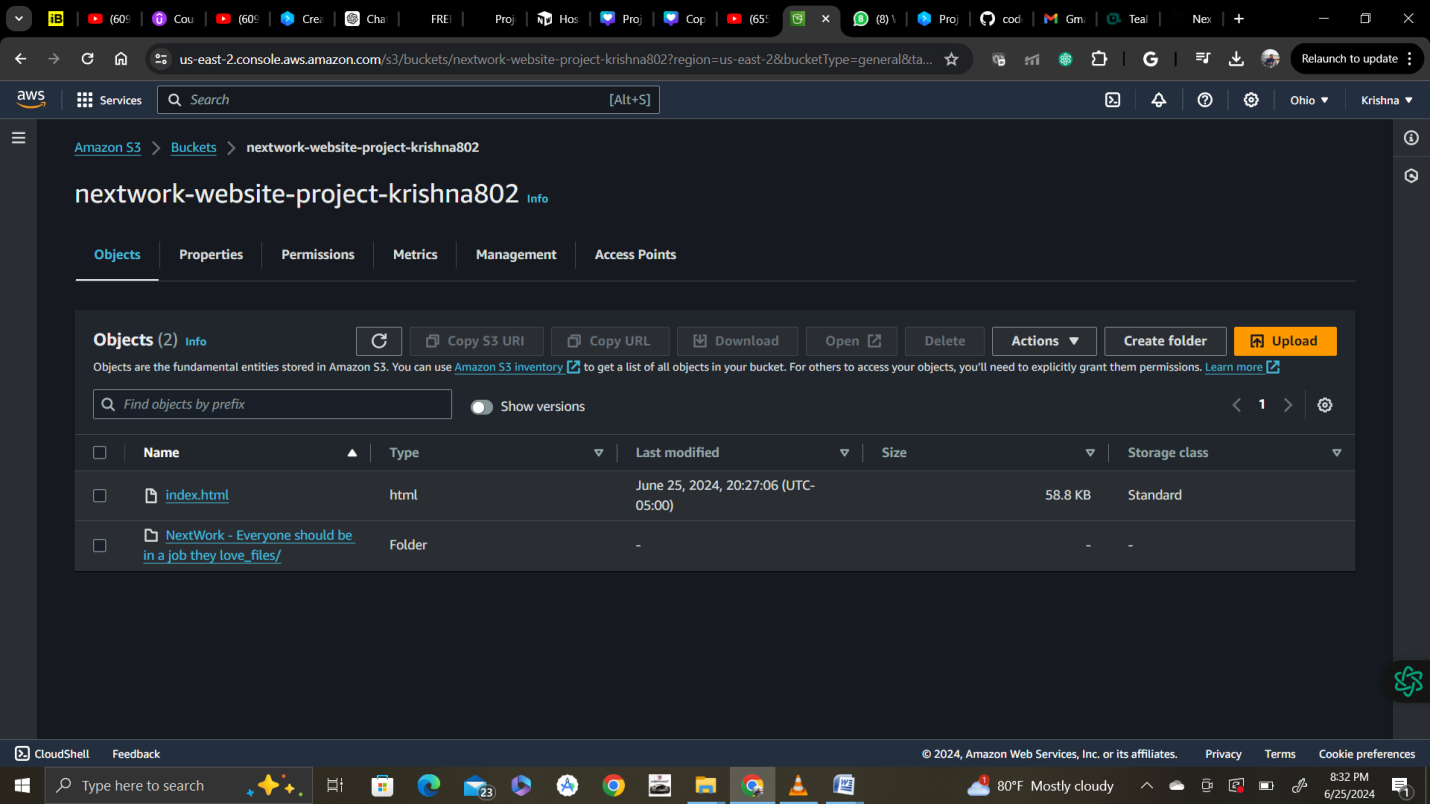
Save the html and zip file in your computer. And make sure you unzip the file.



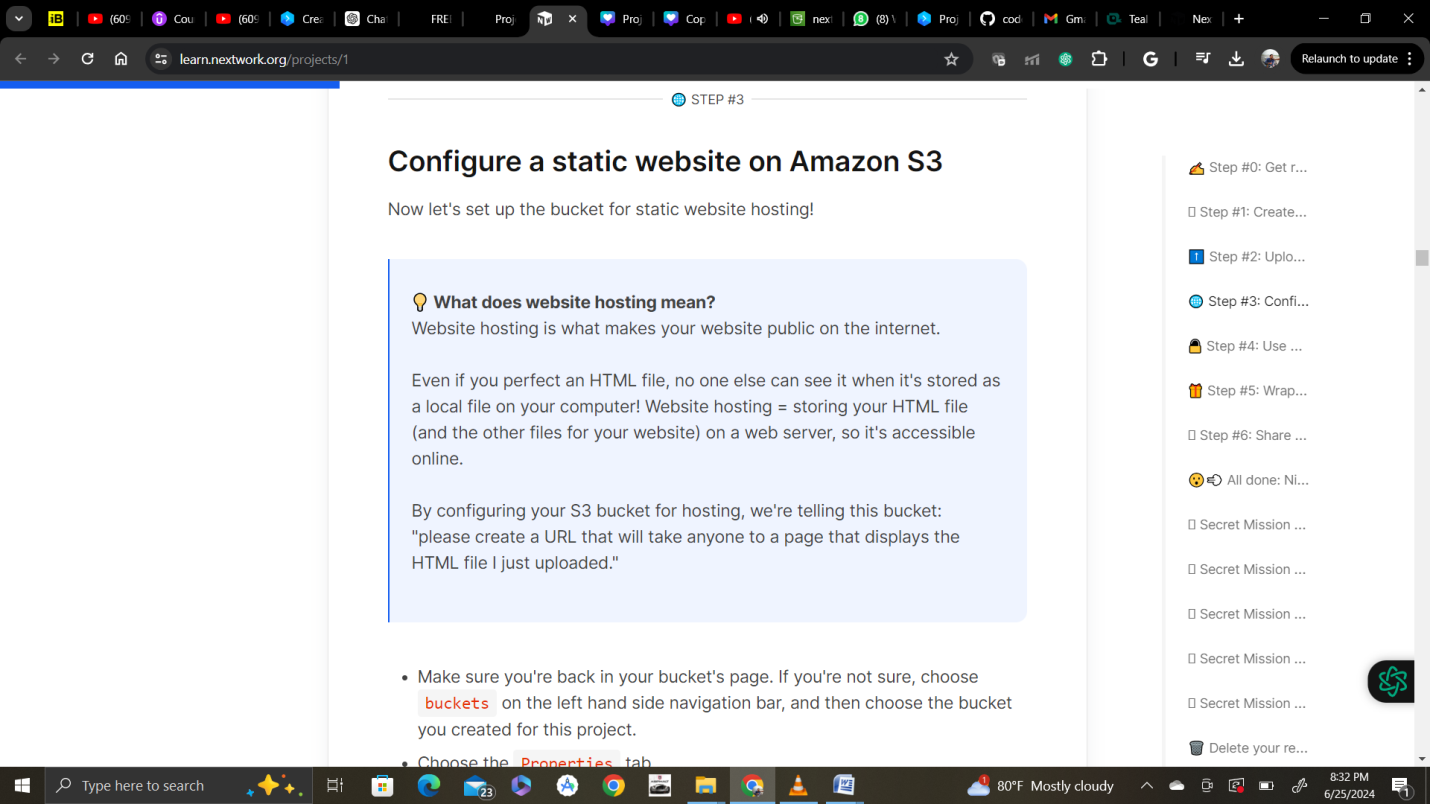
Add all files and folder and then click on upload.





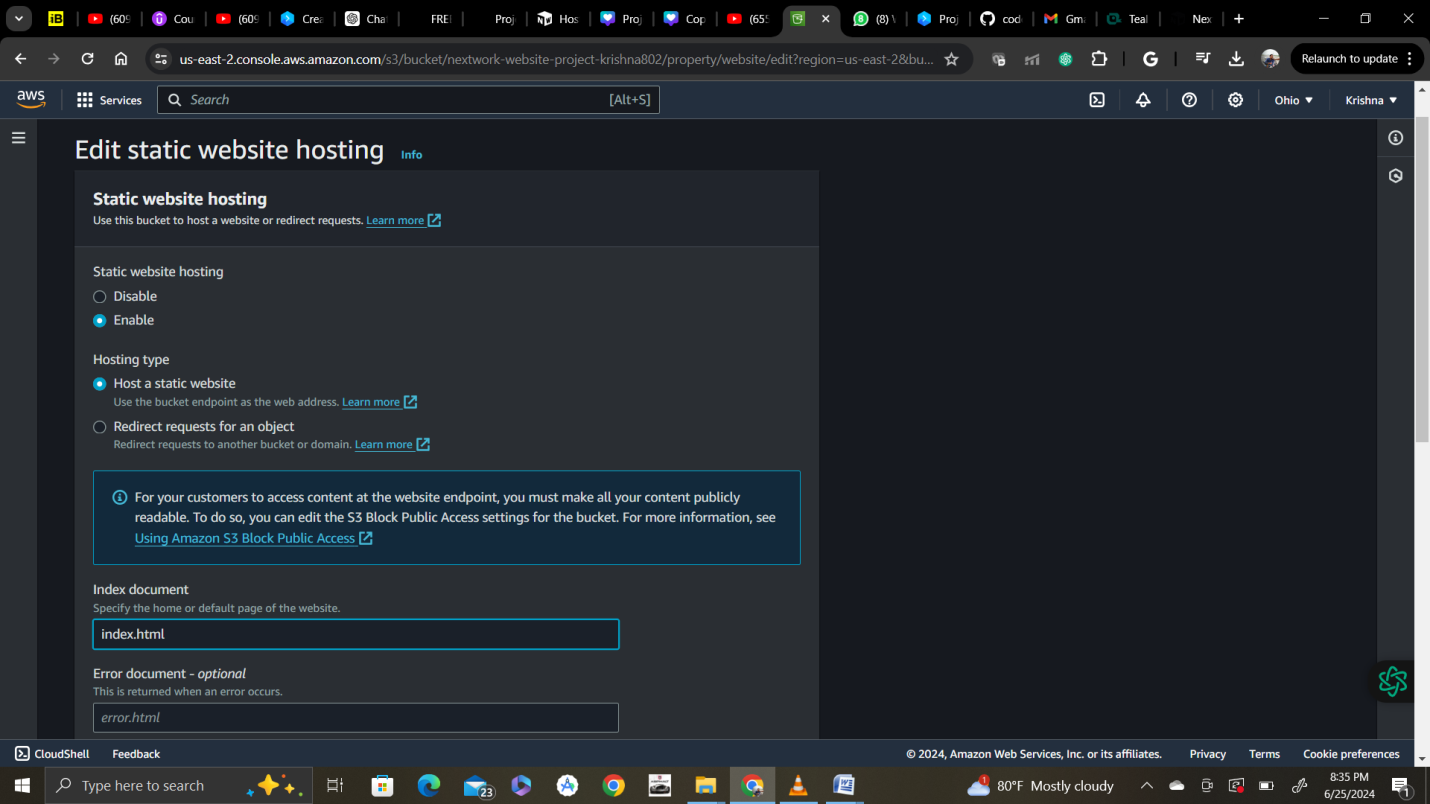


Step 3:

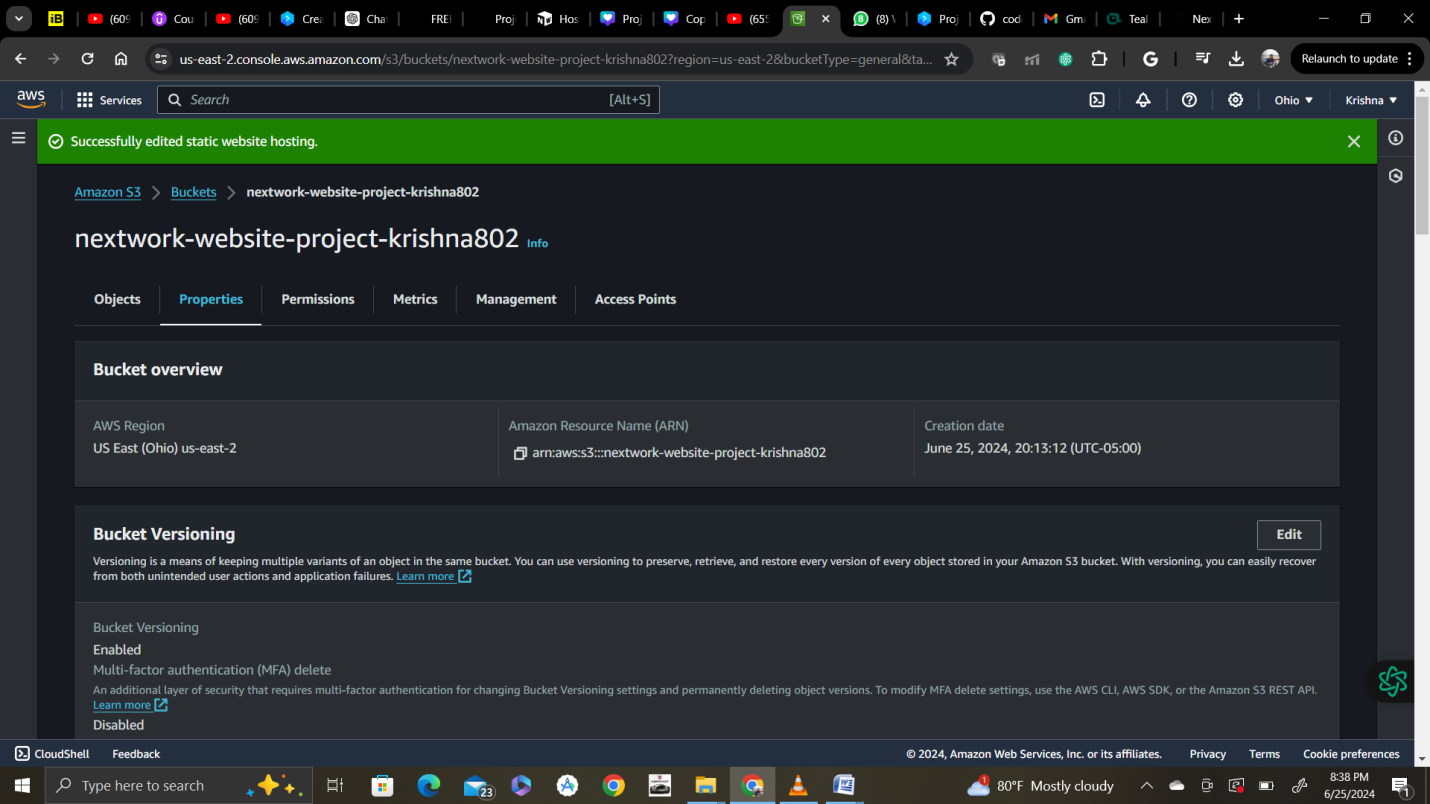


Choose properties tab inside your bucket and scroll all the way bottom to static website hosting

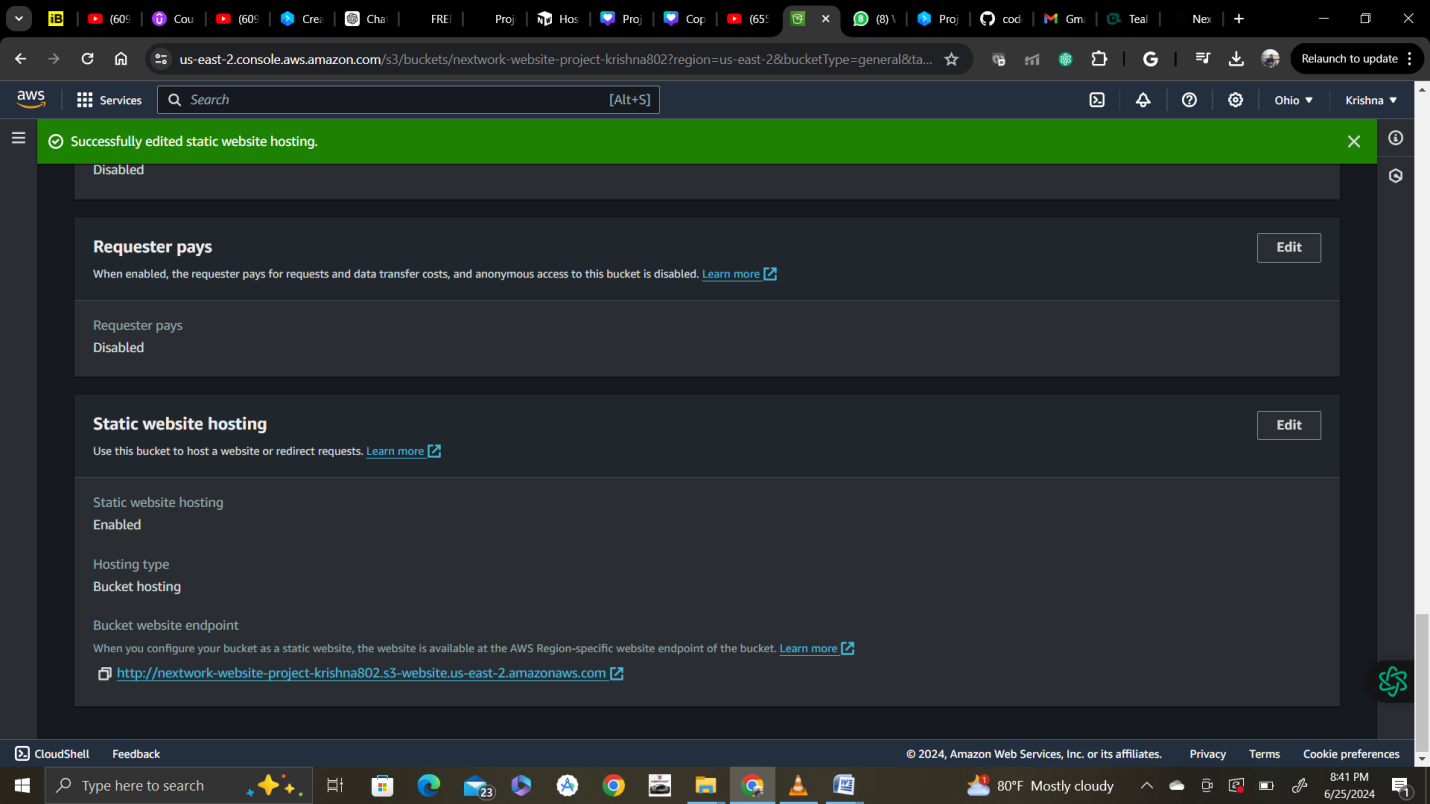
Now click edit static website hosting and enable static website hosting and host a static website option and then selector give the file name which you want to host( a web page) or the file (index.html)

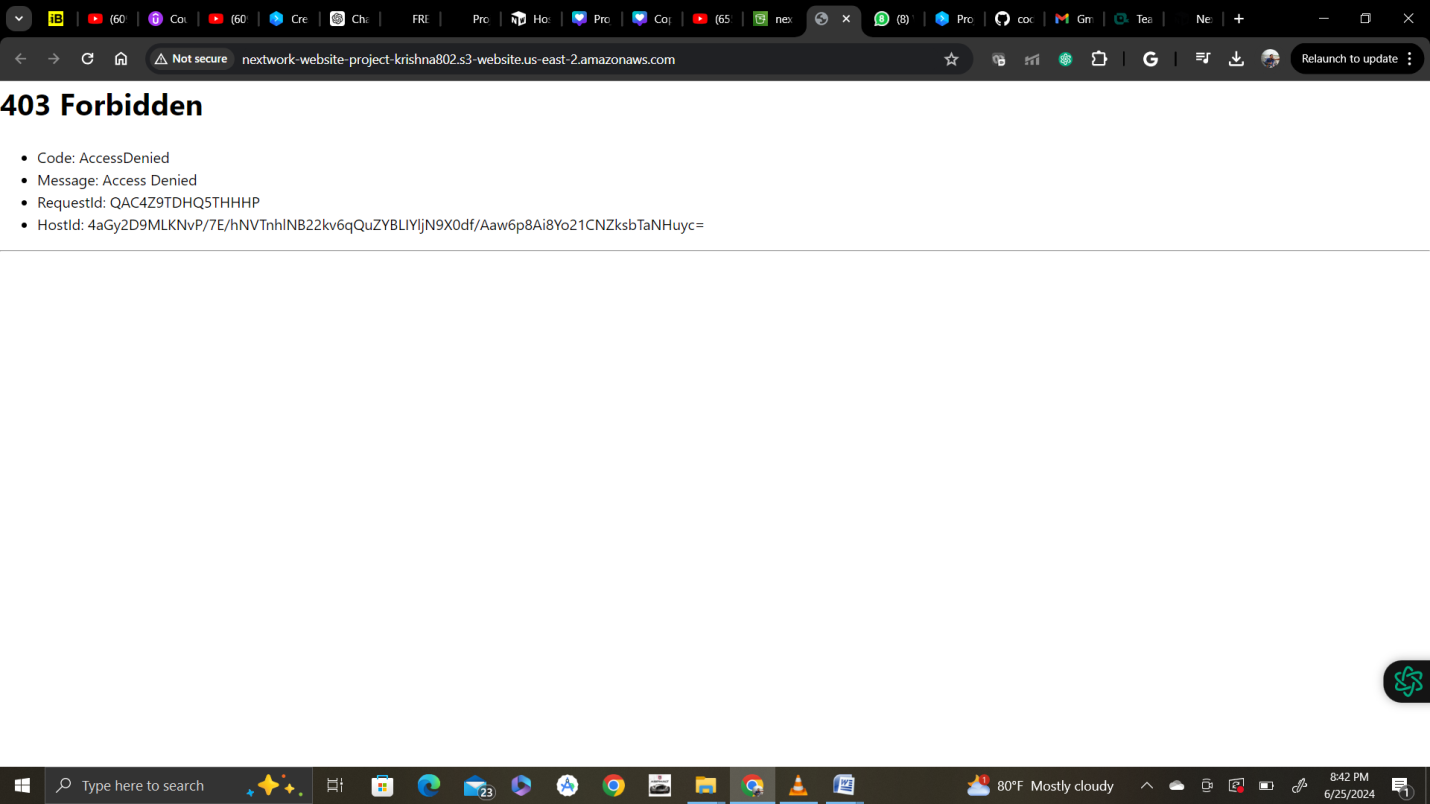


Click save changes.



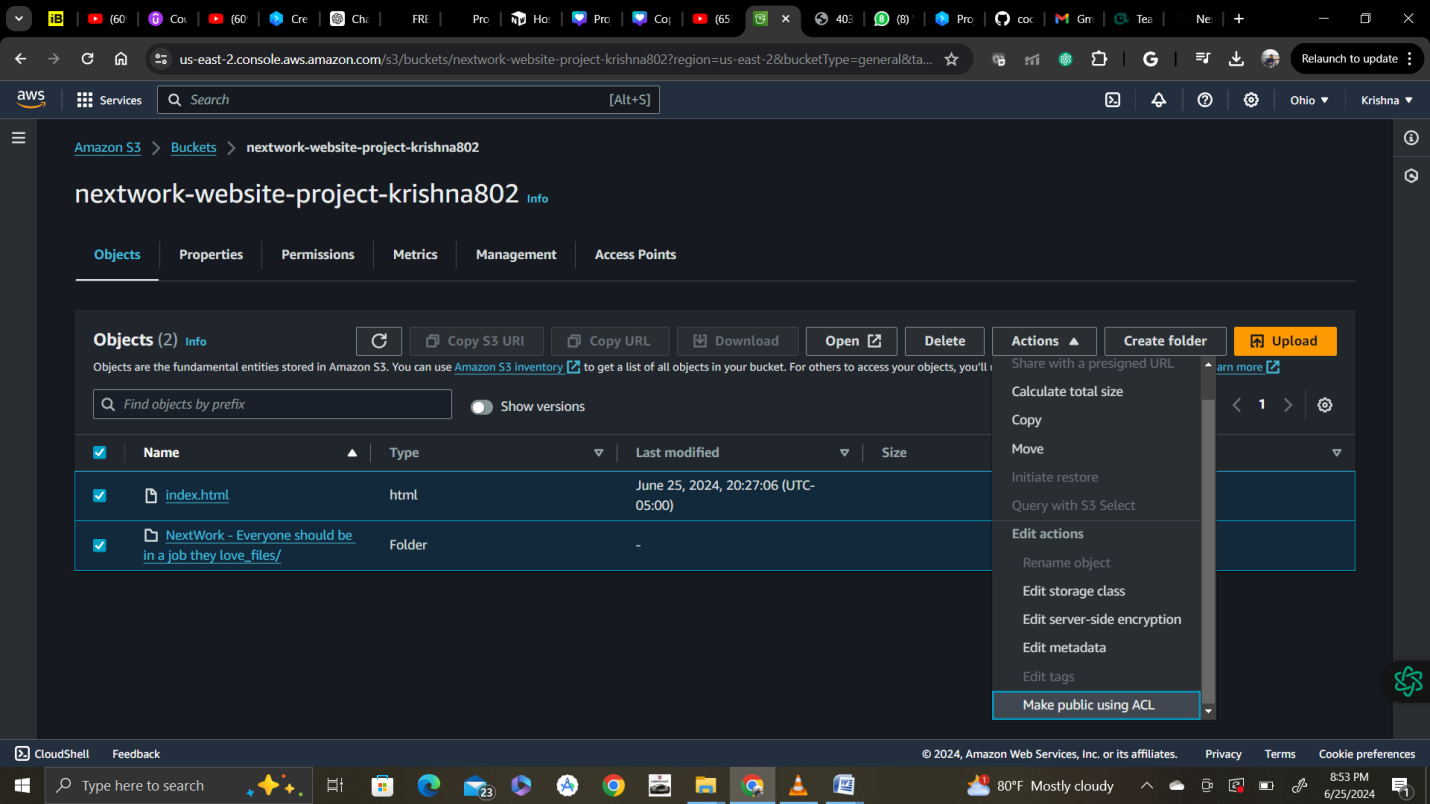
Now click on the link of your static website generated.

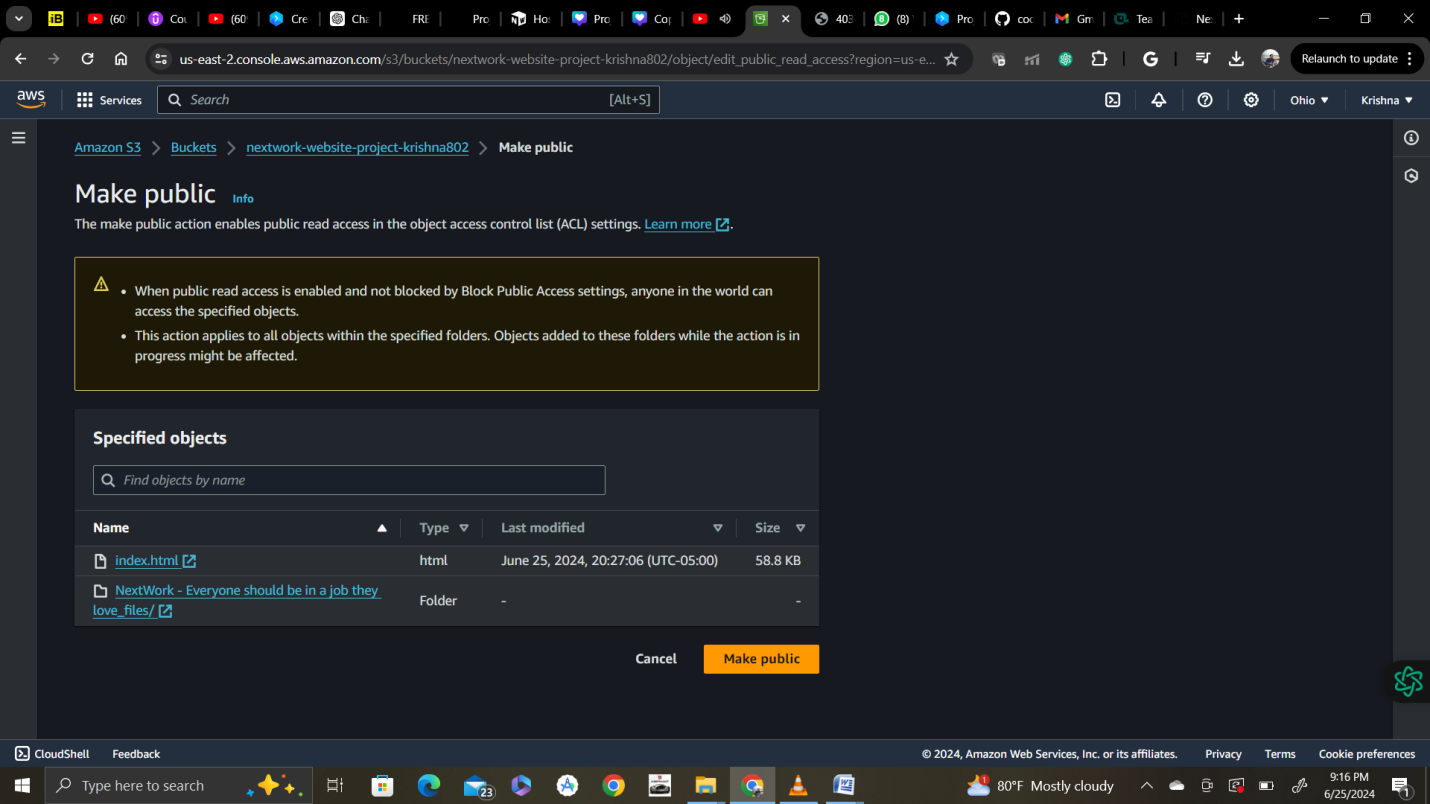




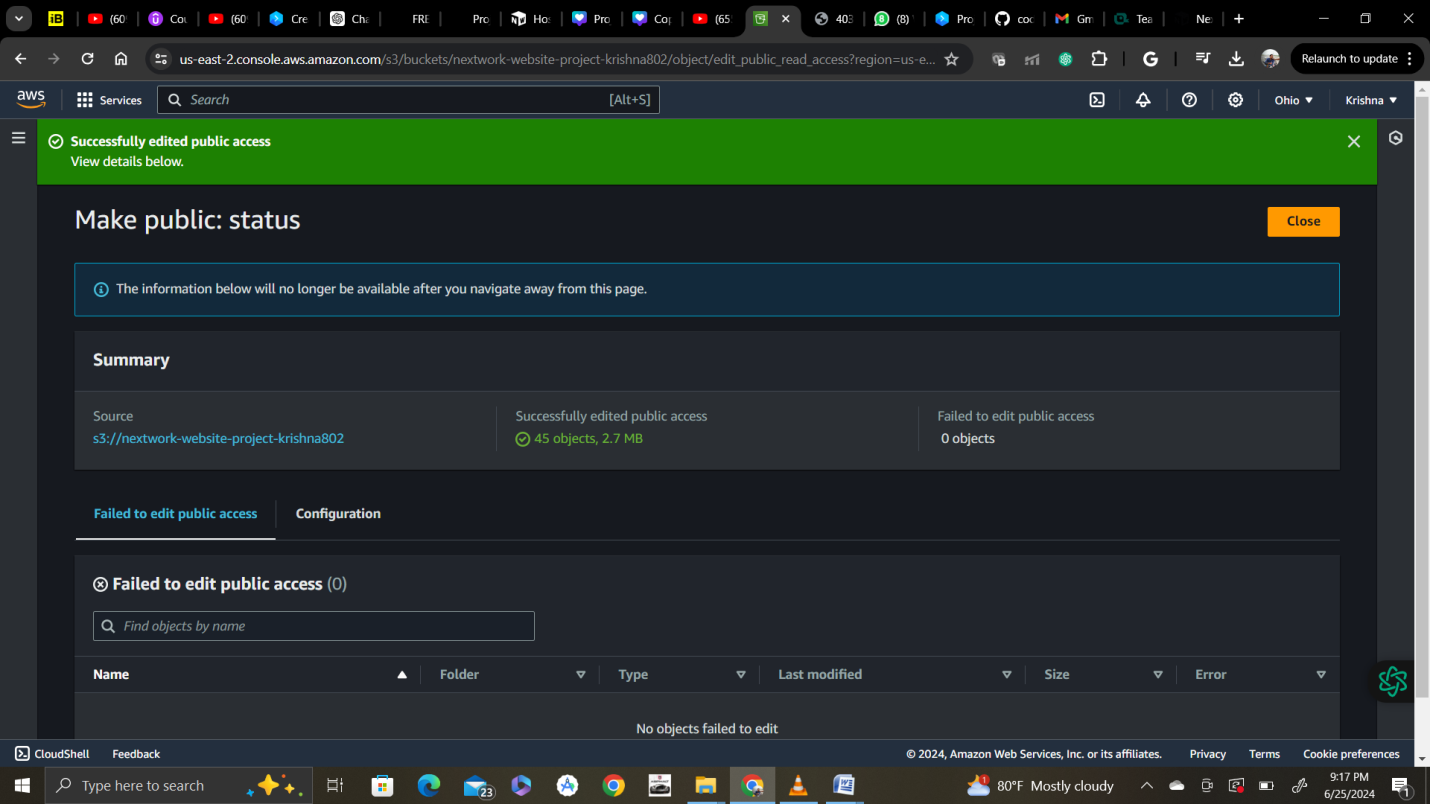
💡 **Why did I get this error?**  
Objects (in this case, the HTML and images files you uploaded) are private by default. This default setting helps keep your account's data secure.  
  
The error message you're seeing is telling you that your static website is being hosted by S3, but the actual HTML/image files you've uploaded are still private. It's kind of like having a bucket on display, so everyone can see the bucket - but the contents are covered up, preventing anyone from seeing what's inside.  
  
To solve this error, we need to set the permission of the objects to public - this is why we enabled ACLs in Task 1!

Click objects tab in the bucket and select files uploaded





Click make public so it makes files publicly available.



Link generated :

http://nextwork-website-project-krishna802.s3-website.us-east-2.amazonaws.com

now you can access website

