

## **ELEVATE-LABS-TASK-6**

Name - Mohammad Mansur

Gmail Id - [mohdmansur1913@gmail.com](mailto:mohdmansur1913@gmail.com)

Designation - Cloud Intern

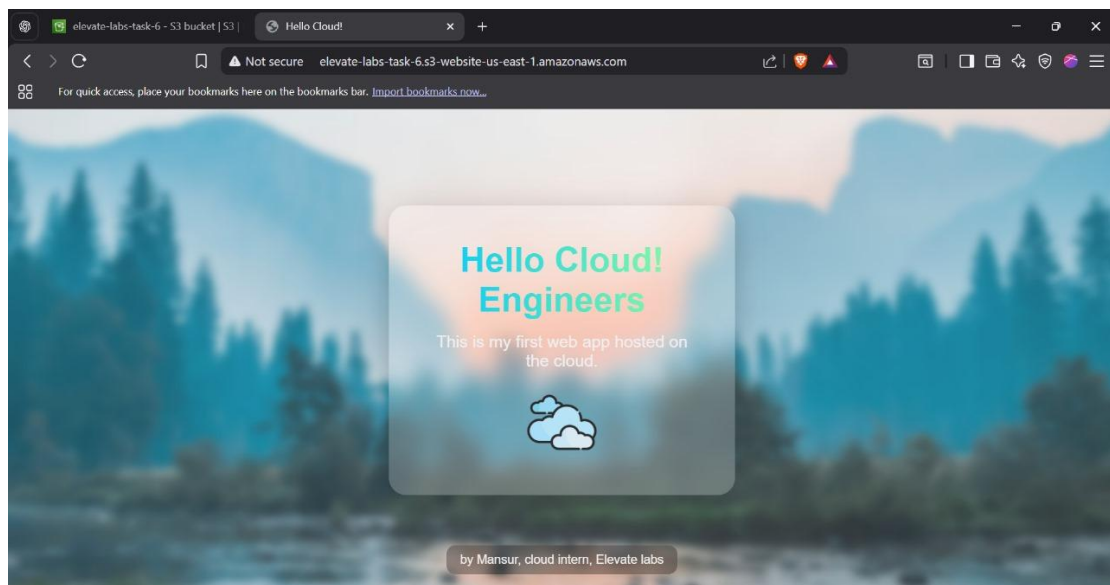
Git-hub: <https://github.com/mansur1913/elevate-labs-task-6>

### **Task 6:** Host and Deploy a Web Application on the Cloud\*

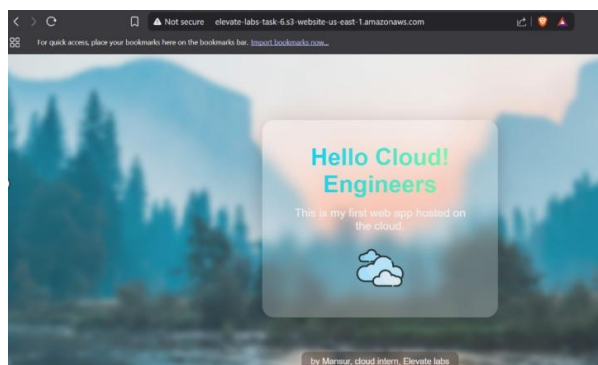
**Objective:** To deploy a static or dynamic web application (like a simple portfolio or basic HTML app) on a cloud platform using a virtual machine, App Engine, or web hosting service.

## **Deliverables:**

### **Deployed web app URL (running live):**



### **Cloud Console with your app running:**



## Source code folder (ZIP or GitHub repo):

<https://github.com/mansur1913/elevate-labs-task-6/blob/main/index.html>

## Short note explaining deployment steps:

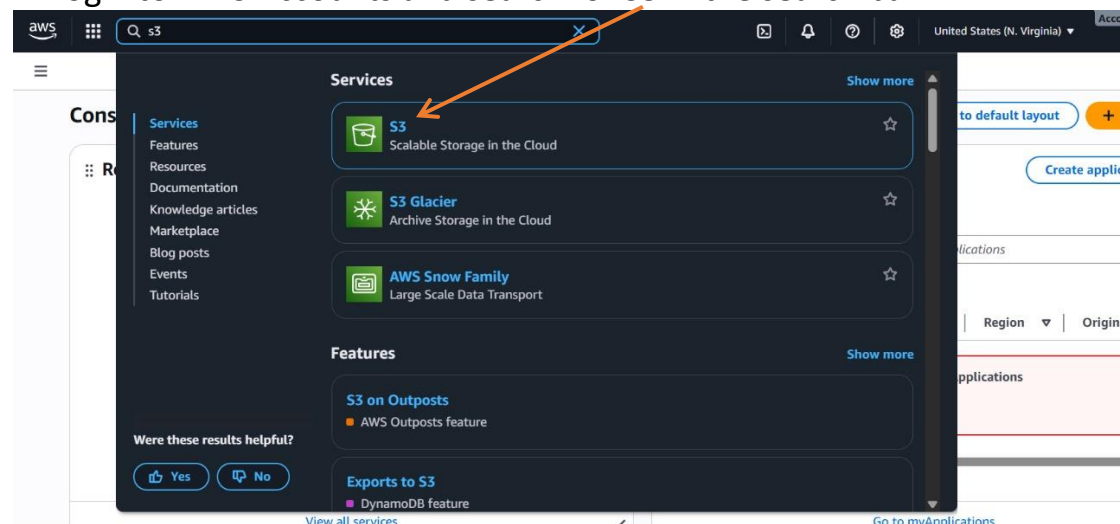
*Develop the web application and test it locally, then choose a cloud platform like AWS or Azure. Upload project files or use Git for deployment.*

*Then I Configure the server, database, and domain settings.*

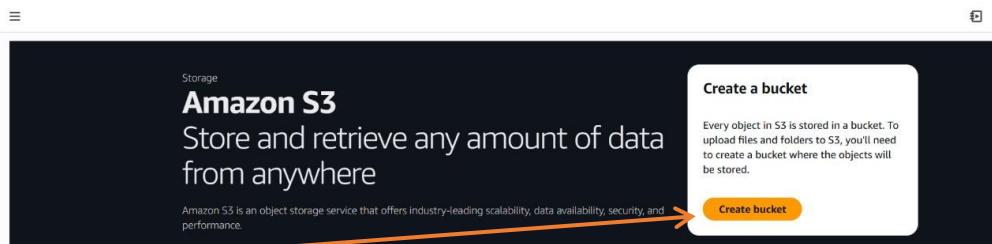
*Enable HTTPS for security and test the application online to ensure smooth performance.*

## Step-by-step Explanation of the (Host and Deploy a Web Application on the Cloud)

1. Login to AWS Accounts and search for S3 in the search bar.

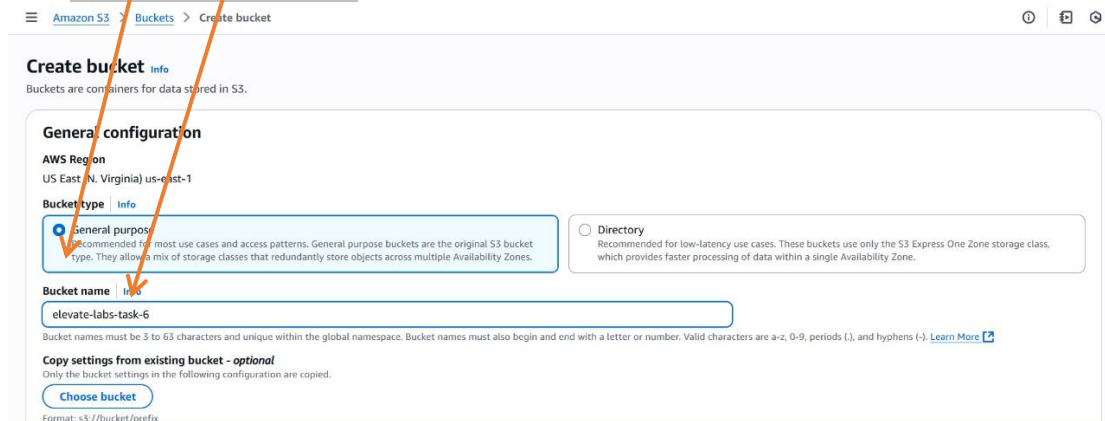


Click on S3 you see like this:

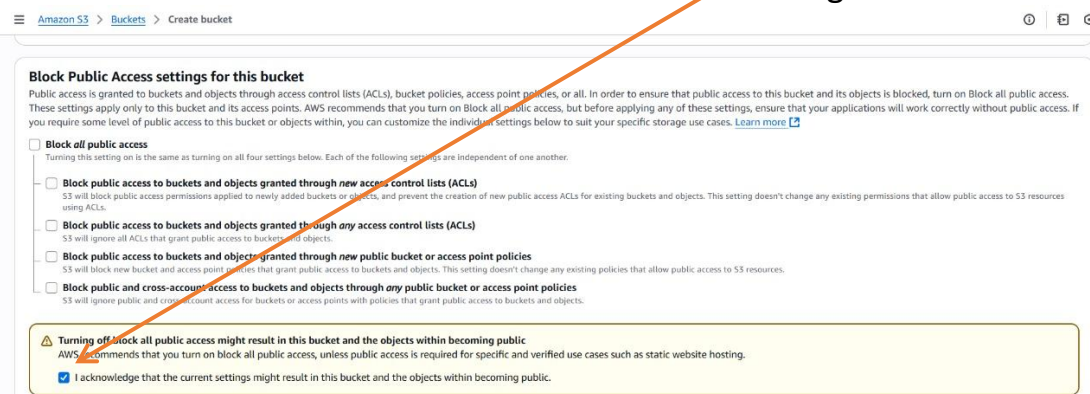


Click on “Create bucket”

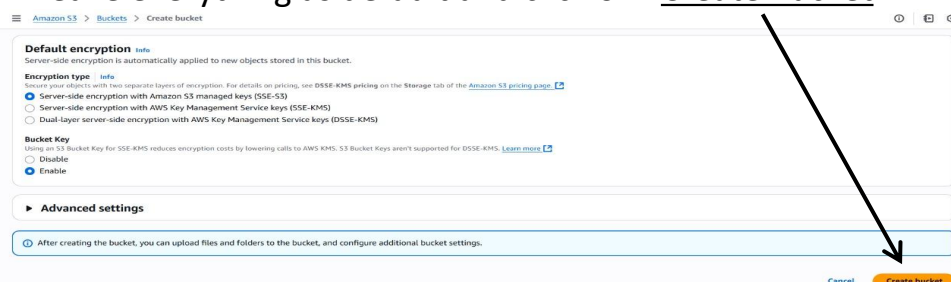
2. After that, Select your bucket type in this example I am selecting as “General purpose” Name your bucket as I am naming eg: “elevate-labs-task-6” You can give name as per your choice.



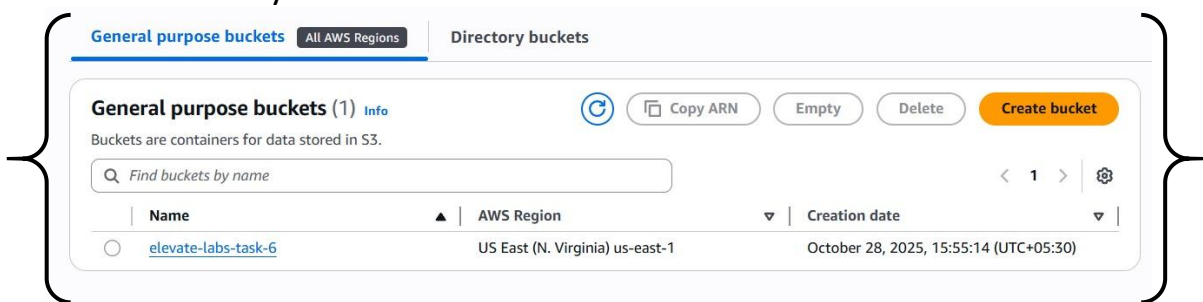
3. Untick Block Public Access and click on “I Acknowledge”



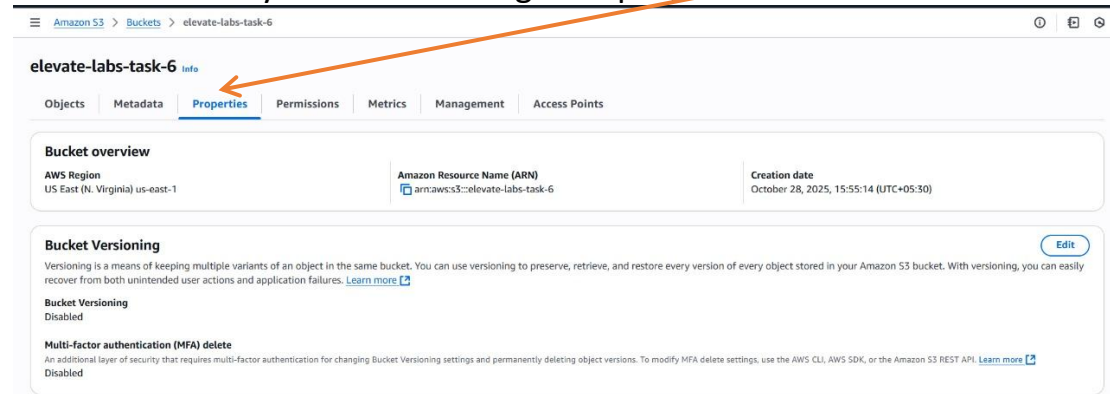
4. Leave everything as default and click on “Create Bucket”



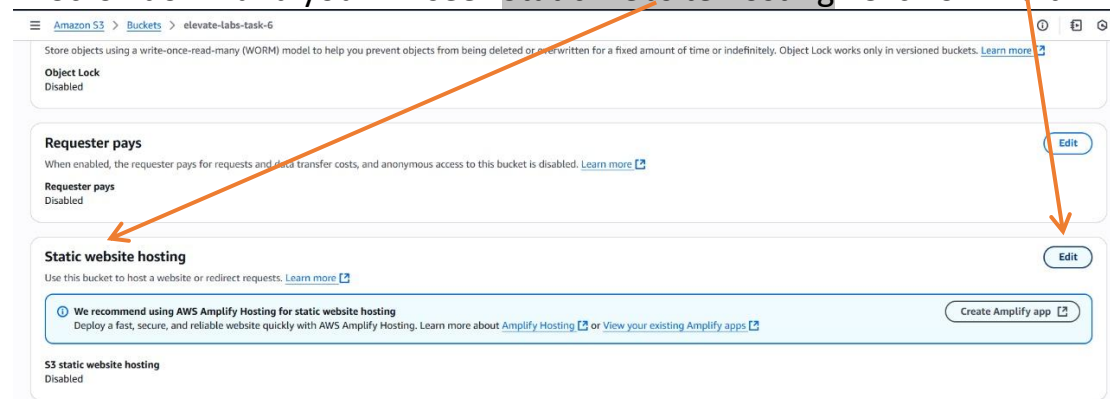
5. You can see you “Bucket” As I show below:



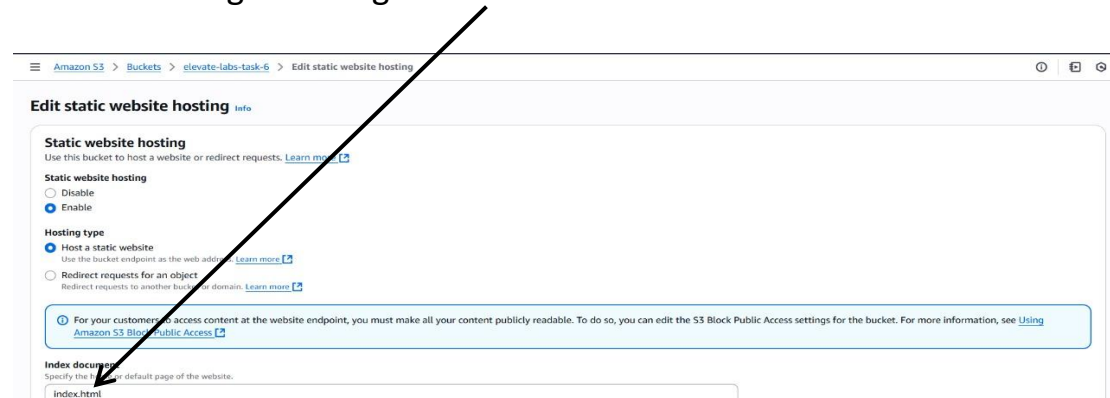
6. Then Click on your bucket and go to “properties”



7. Scroll down and you will see “Static website hosting” Click on “Edit”



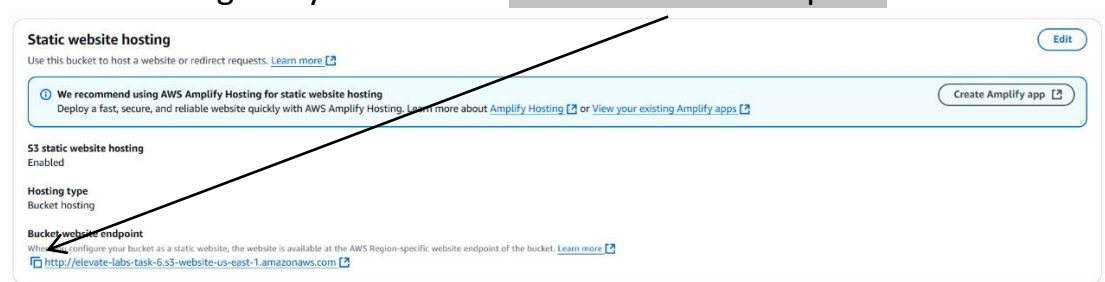
8. After that leave everything as default as Name your Index Document As I am naming in this eg: “Index.html”



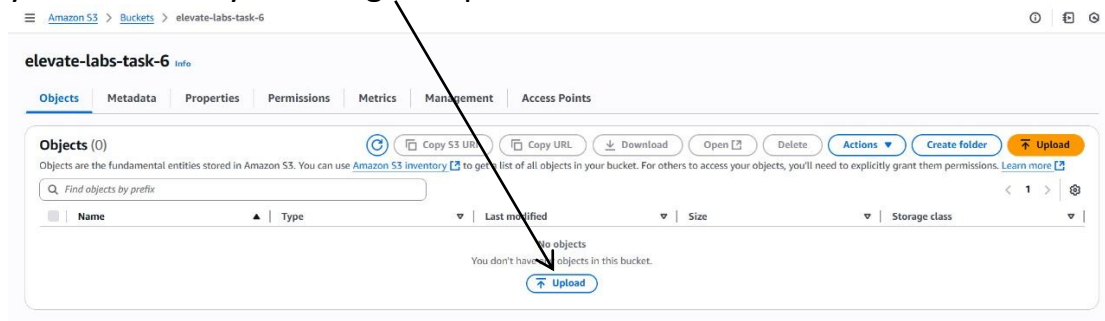
9. Then click on “Save changes”



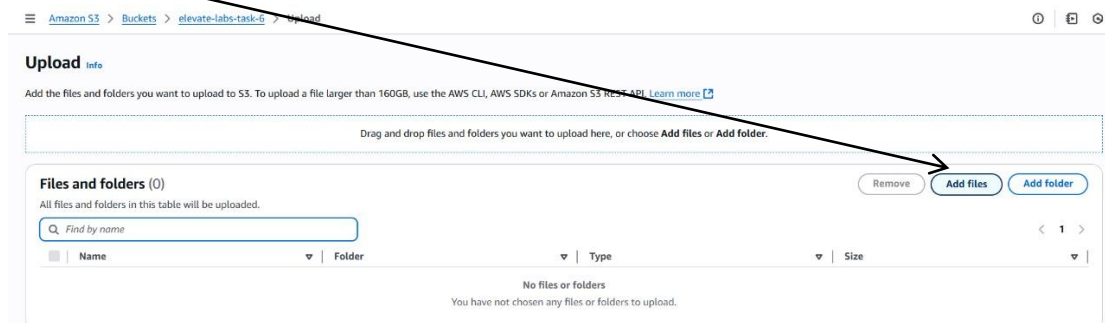
10. After doing this you can see “Bucket website endpoint” or URL link



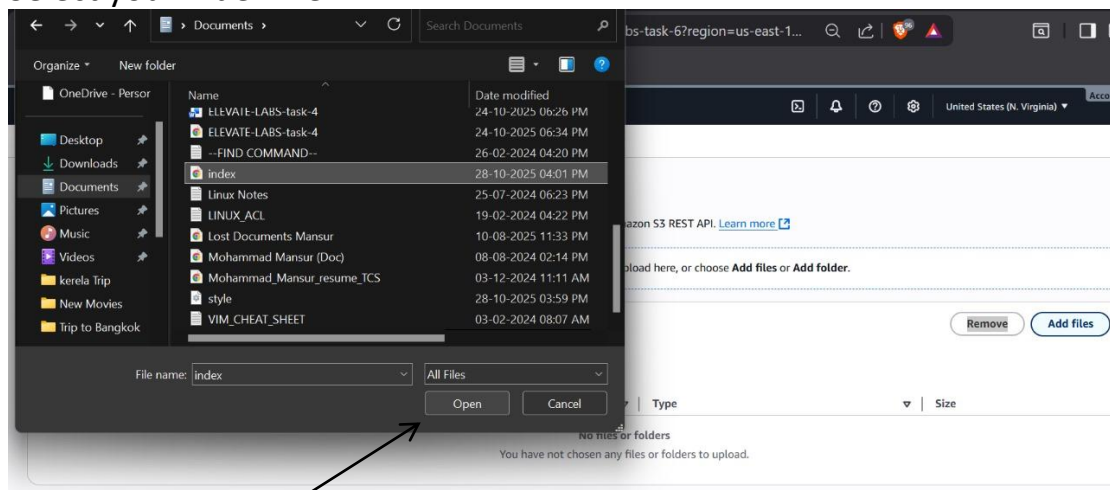
11. Then go to Objectives and upload your both “Index and Style” File in your bucket. By “Clicking on Upload”.



click in “Add file”

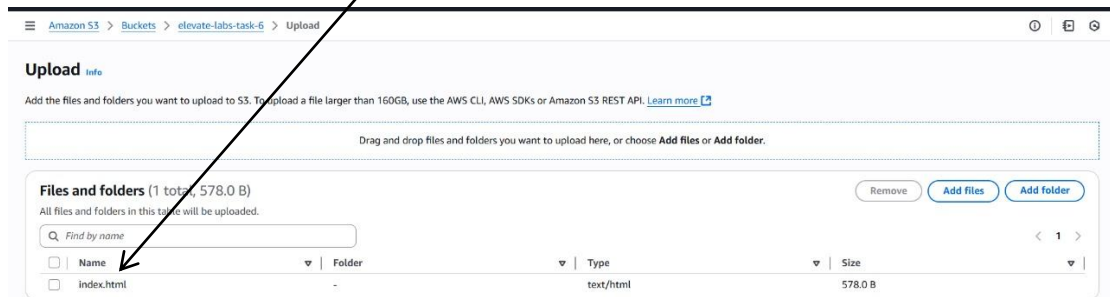


## Select your index file

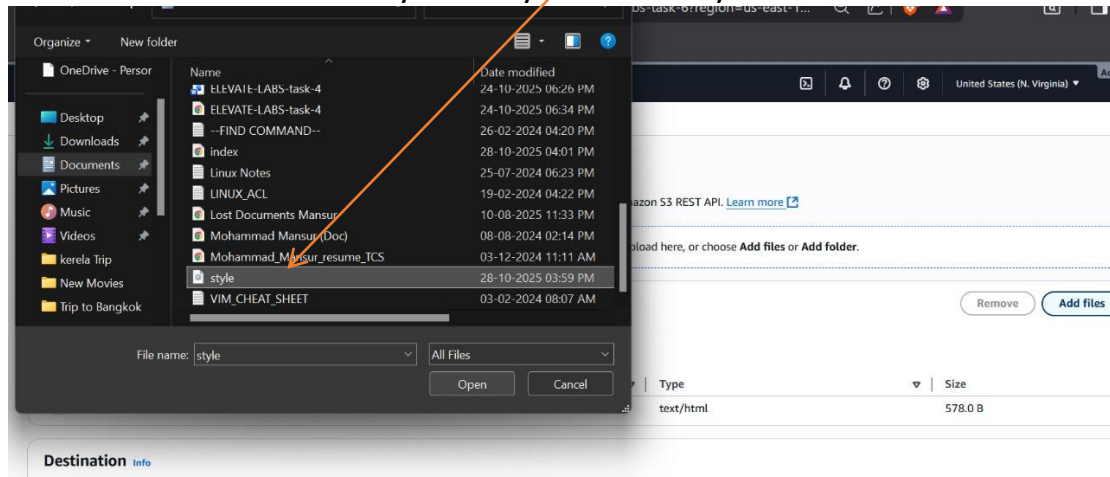


Click on “open”

As you can see your “index file” in your bucket do the same process for another file.



Click on Add file and add your “Style file” into your bucket





Then you can see your both files in your bucket

**Upload** Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose [Add files](#) or [Add folder](#).

**Files and folders** (2 total, 2.0 KB)

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	style.css	-	text/css	1.4 KB
<input type="checkbox"/>	index.html	-	text/html	578.0 B

**Destination** Info

**Destination**

[s3://elevate-labs-task-6](#)

**► Destination details**

Bucket settings that impact new objects stored in the specified destination.

**► Permissions**

Grant public access and access to other AWS accounts.

**► Properties**

Specify storage class, encryption settings, tags, and more.

[Cancel](#) [Upload](#)

After doing this click on “Upload”

12. Now after doing this all steps click on “Permission”

Amazon S3 > Buckets > elevate-labs-task-6

**elevate-labs-task-6** Info

Objects Metadata Properties **Permissions** Metrics Management Access Points

**Permissions overview**

**Access finding**

Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#)

[View analyzer for us-east-1](#)

**Block public access (bucket settings)** [Edit](#)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

**Block all public access**

Off

**► Individual Block Public Access settings for this bucket**

Go to “Bucket policy” and click on “Edit”

**Bucket policy**

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

[Edit](#) [Delete](#)

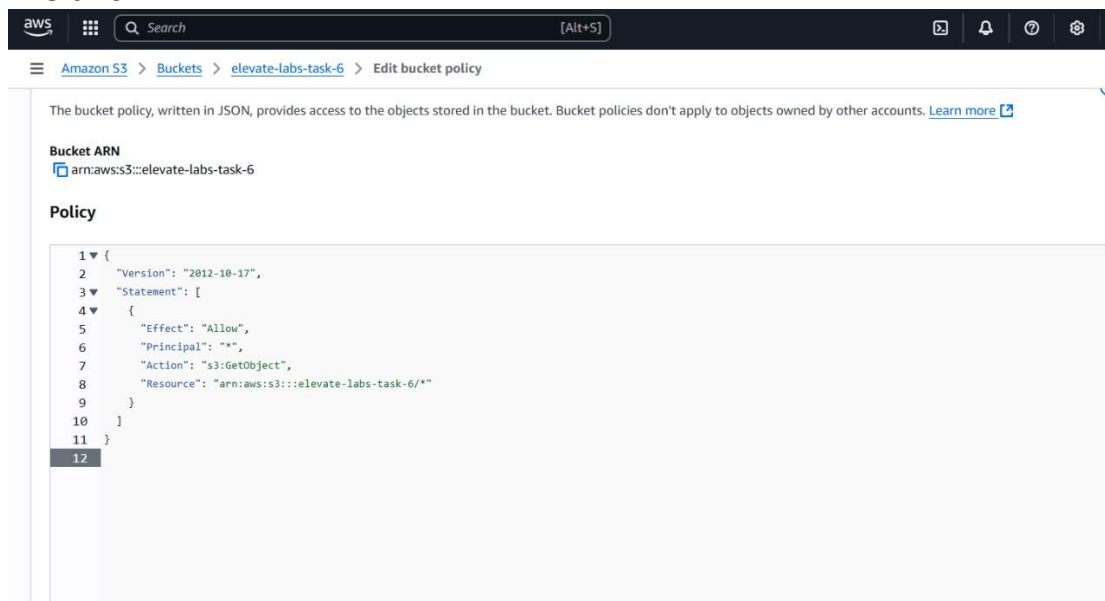
No policy to display.

[Copy](#)

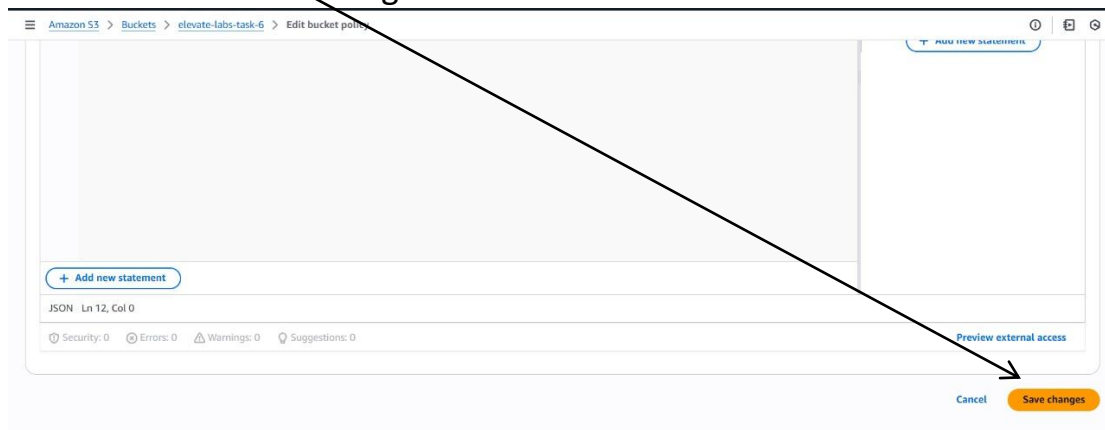
Write the below code In the edit box

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::elevate-labs-task-6/*"
    }
  ]
}
```

like this

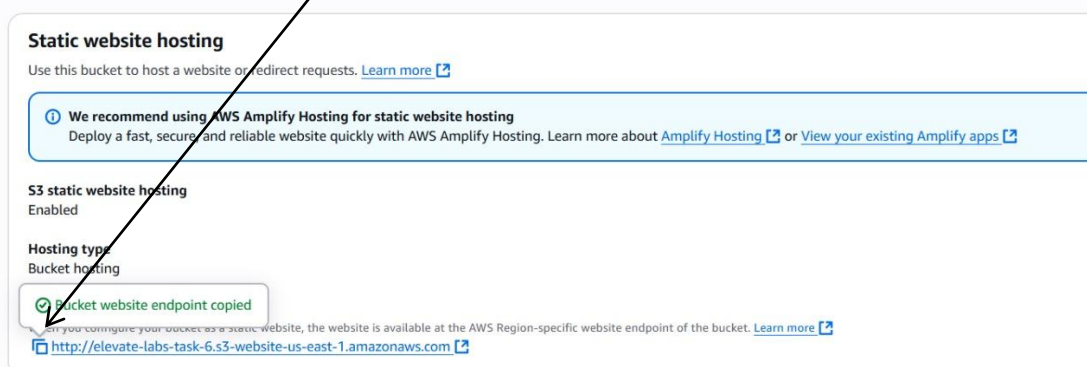


Then click on "Save changes"

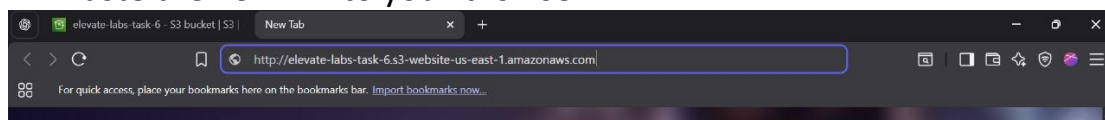


We have successfully given the permission

13. Now copy the "URL"



14. Paste the "URL" into your browser





15. And then click on enter... You will see the final output like this:

