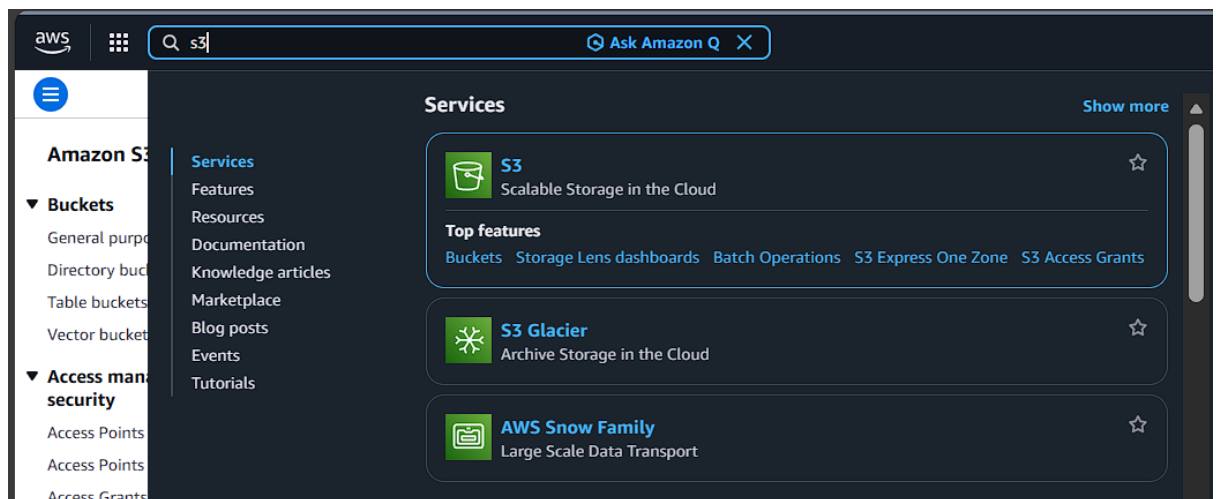
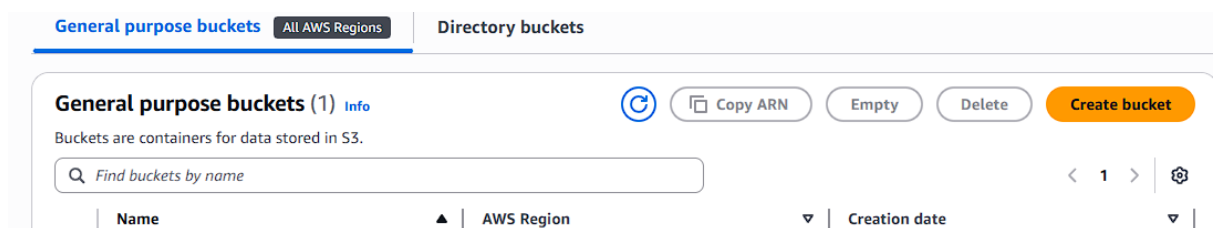


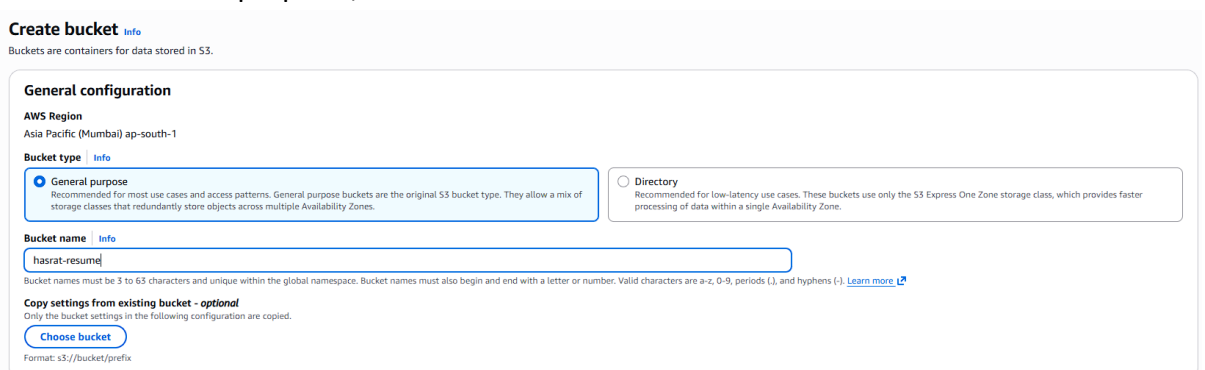
1. Search S3 and click buckets:



2. Click on Create bucket :



3. Select General purpose , Give a bucket Name:



#### 4. Untick Block all public access and Click create bucket:

**Block Public Access settings for this bucket**

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 this bucket and its 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 this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☐ **Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.

☐ **Block public access to buckets and objects granted through new public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

**Turning off block all public access might result in this bucket and the objects within becoming public**  
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

#### 5. Click on the Bucket Name (hasrat-resume) :

**General purpose buckets** All AWS Regions Directory buckets

**General purpose buckets (1)** Info

Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	Creation date
<a href="#">hasrat-resume</a>	Asia Pacific (Mumbai) ap-south-1	December 17, 2025, 19:58:31 (UTC+05:30)

#### 6. Click upload and upload the static website files (index.html , style.css) :

Amazon S3 Buckets hasrat-resume

**hasrat-resume** Info

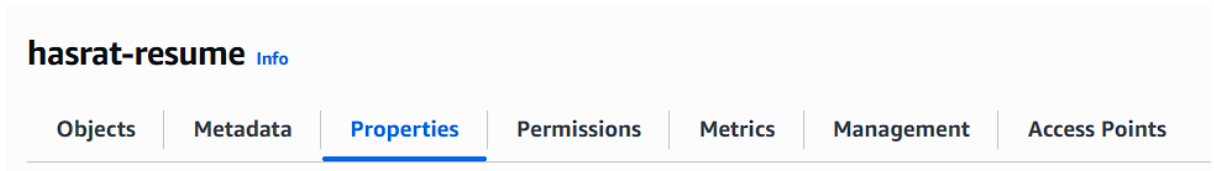
Objects

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

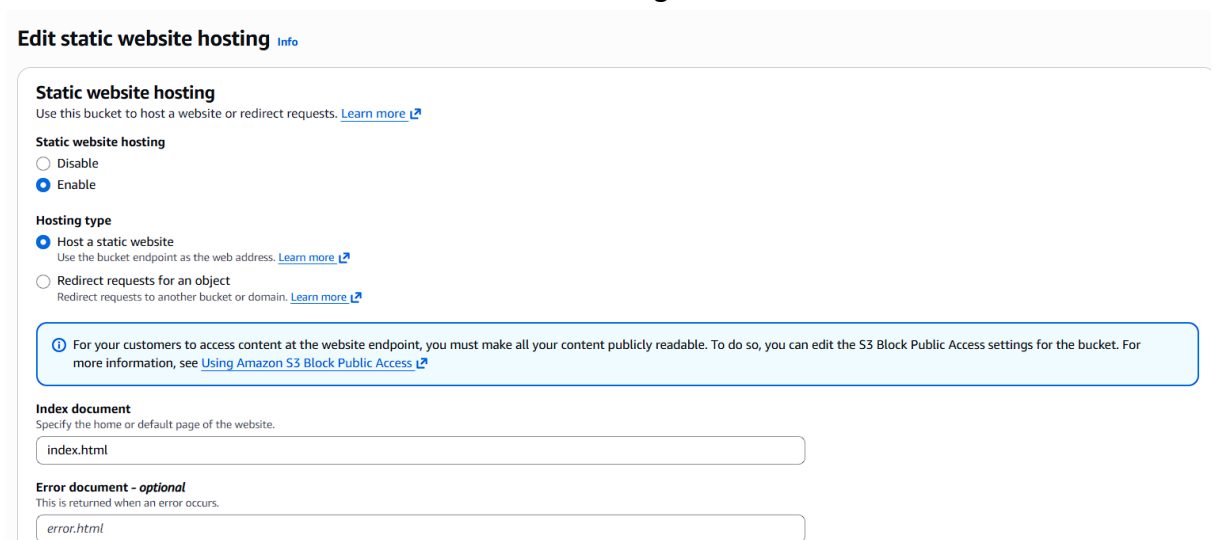
Find objects by prefix

Name	Type	Last modified	Size	Storage class
<a href="#">index.html</a>	html	December 17, 2025, 19:59:03 (UTC+05:30)	2.3 KB	Standard
<a href="#">style.css</a>	css	December 17, 2025, 19:59:03 (UTC+05:30)	1.0 KB	Standard

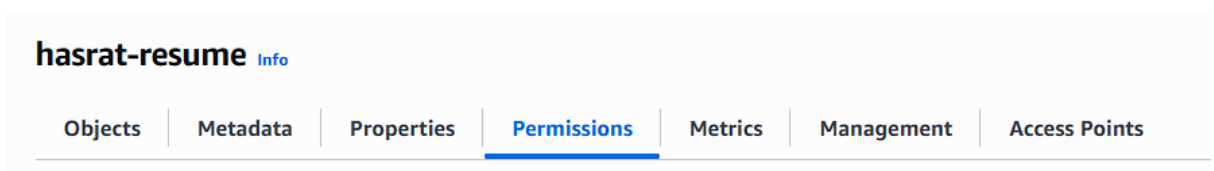
7. Inside the Bucket click on Properties Tab:



8. Scroll down and Click on edit Static web hosting and Select Enable and Save :



9. Now click on Permissions Tab:



## 10. Select Bucket policy and Update the Policy.

(Public access is enabled, and Static website hosting is ON  
Without a bucket policy, users will get “403 Access Denied”  
So this policy allows public read access.) :

**Edit bucket policy** [Info](#)

**Bucket policy** [Policy examples](#)

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](#)

**Bucket ARN**  
[arn:aws:s3::hasrat-resume](#)

**Policy**

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "PublicRead",  
6       "Effect": "Allow",  
7       "Principal": "*",  
8       "Action": "s3:GetObject",  
9       "Resource": "arn:aws:s3::hasrat-resume/*"  
10    }  
11  ]  
12 }
```

**Edit statement**

**Select a statement**

Select an existing statement in the policy or add a new statement.

[+ Add new statement](#)

## 11. Now copy the Bucket website Endpoint From the Properties Tab :

**Static website hosting** [Edit](#)

Use this bucket to host a website or redirect requests. [Learn more](#)

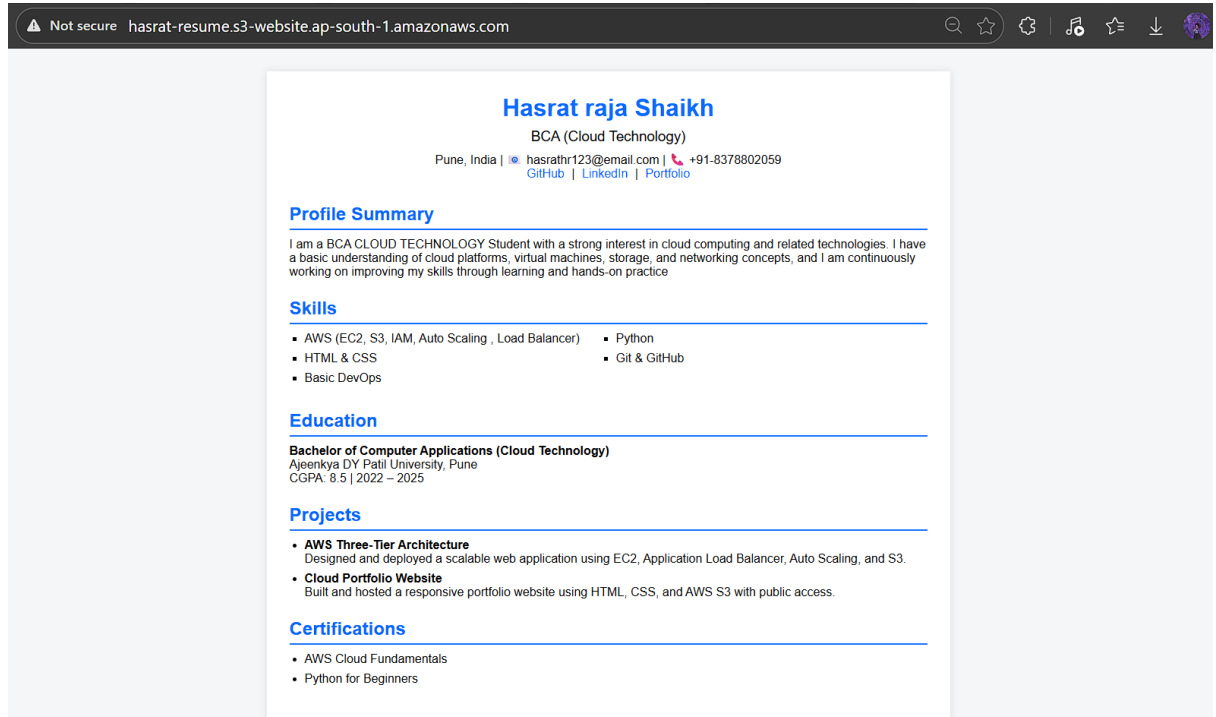
[We recommend using AWS Amplify Hosting for static website hosting](#)  
Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [View your existing Amplify apps](#) [Create Amplify app](#)

**S3 static website hosting**  
Enabled

**Hosting type**  
Bucket hosting

**Bucket website endpoint**  
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)  
<http://hasrat-resume.s3-website-ap-south-1.amazonaws.com>

## 12. Paste the Endpoint in the Browser URL tab:



We can see the Static website on S3 is running.