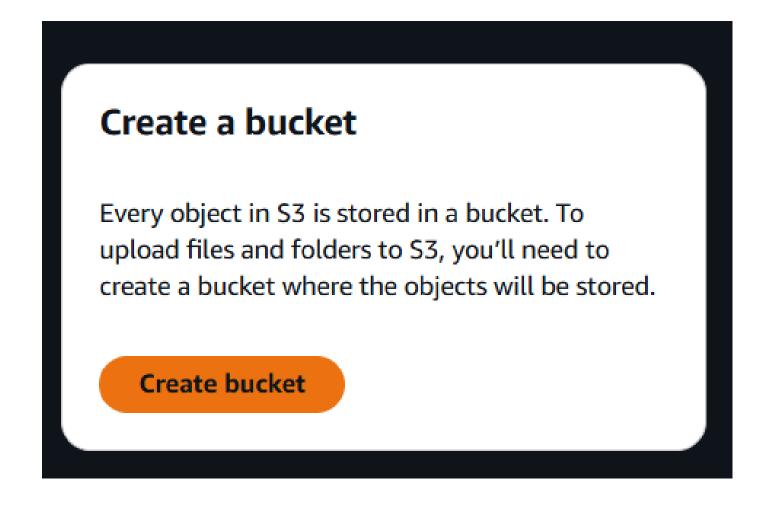


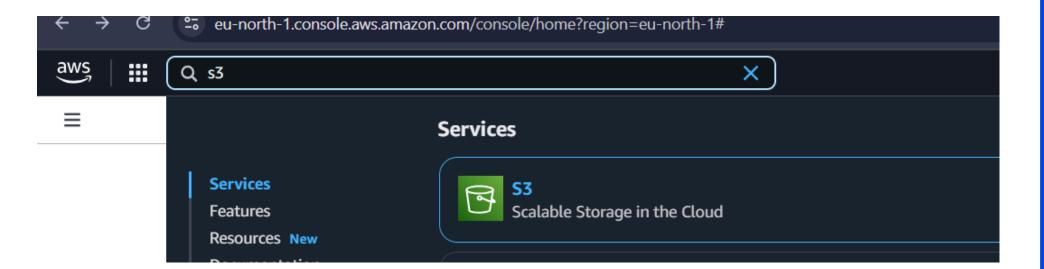
Hosted a website using a S3 services of AWS



- Vibhanshukumarshubham46@gmail.com
- ttp://project1hostingawebusings3.s3-website.eu-north-1.amazonaws.com/

Login your Aws acc on console Search S3 and click on it





You see Create Bucket Button click on it

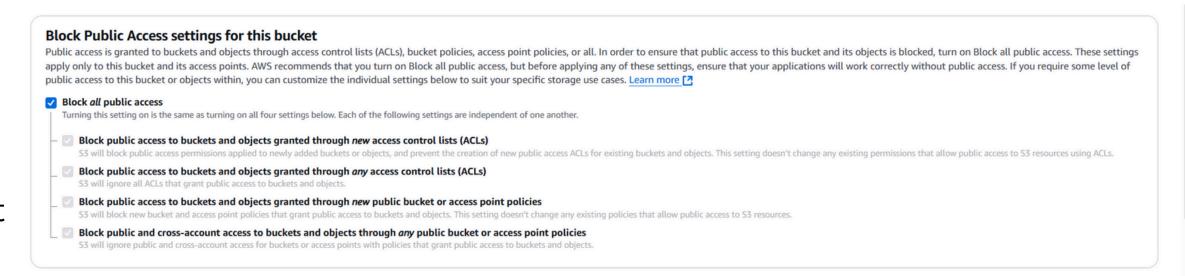
Now u r on create bucket page here u can fill Bucket name In object ownership select acls

Bucket owner enforced

Create bucket Info Buckets are containers for data stored in S3. **General configuration AWS Region** Europe (Stockholm) eu-north-1 Bucket type Info Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster storage classes that redundantly store objects across multiple Availability Zones. processing of data within a single Availability Zone. Bucket name Info project1hostingawebusings3 Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). Learn More [7] Copy settings from existing bucket - optional Only the bucket settings in the following configuration are copied. Choose bucket Format: s3://bucket/prefix Object Ownership Info Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects. ACLs disabled (recommended) ACLs enabled All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies. Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs. **Object Ownership**

after that you see
Block Public Access settings for this
bucket
this is ticked from all bcz no one access it

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



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

public access to this bucket of objects within, you can custofffize the mainfulant settings below to suit your specific storage use cases.
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 <i>any</i> 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 <i>new</i> 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 <i>any</i> 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.

untick this bcz you Hosted a web so this is accessed by publicly

in Bucket version select disable
if you want to add tag then add tag from tags
select all things like select in figure

Bucket Versioning Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more 2 Bucket Versioning Disable Tags - optional (0) You can use bucket tags to track storage costs and organize buckets. Learn more 2 No tags associated with this bucket.

Default encryption info Server-side encryption is automatically applied to new objects stored in this bucket. Encryption type Info Server-side encryption with Amazon 53 managed keys (SSE-S3) Server-side encryption with AWS Key Management Service keys (SSE-KMS) Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS) Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page. Bucket Key Using an 53 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS, S3 Bucket Keys aren't supported for DSSE-KMS. Learn more Disable Enable

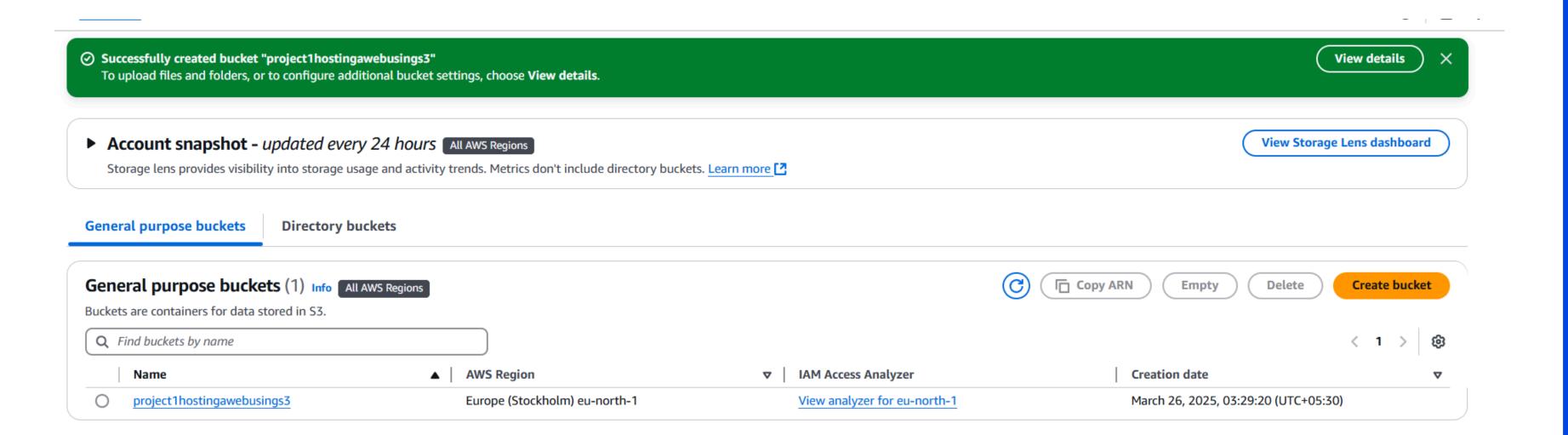
click on create bucket

Bucket Key Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more Disable Inable	
► Advanced settings	
After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.)

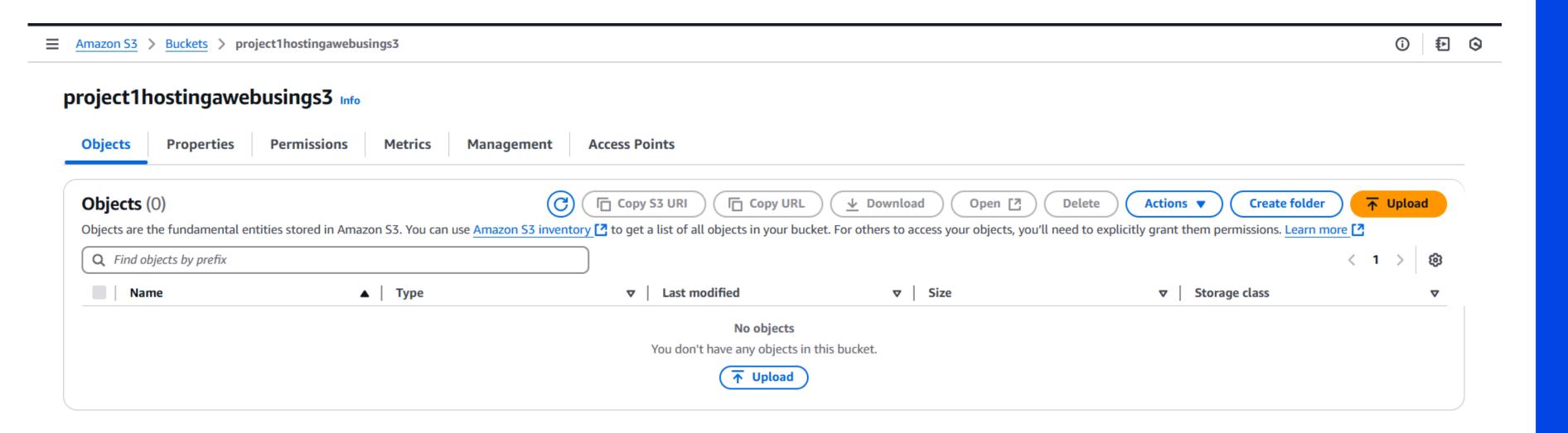
Create bucket

Cancel

after that u get notificatio your bucket is successfully created and you see general purpose bucket then click on your bucket name

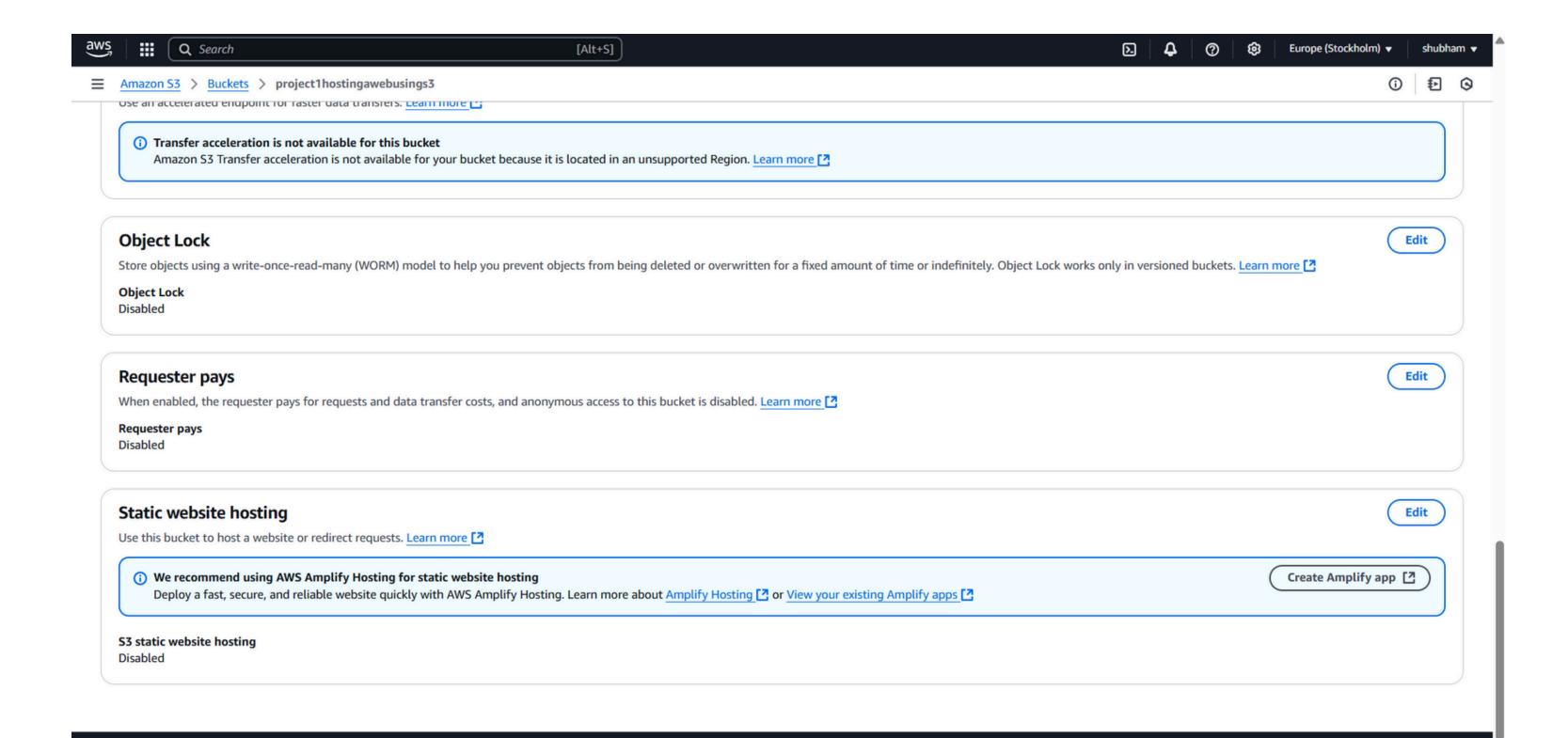


CONTENT



Then click on properties and slide down

Then you see static website hosting click on edit

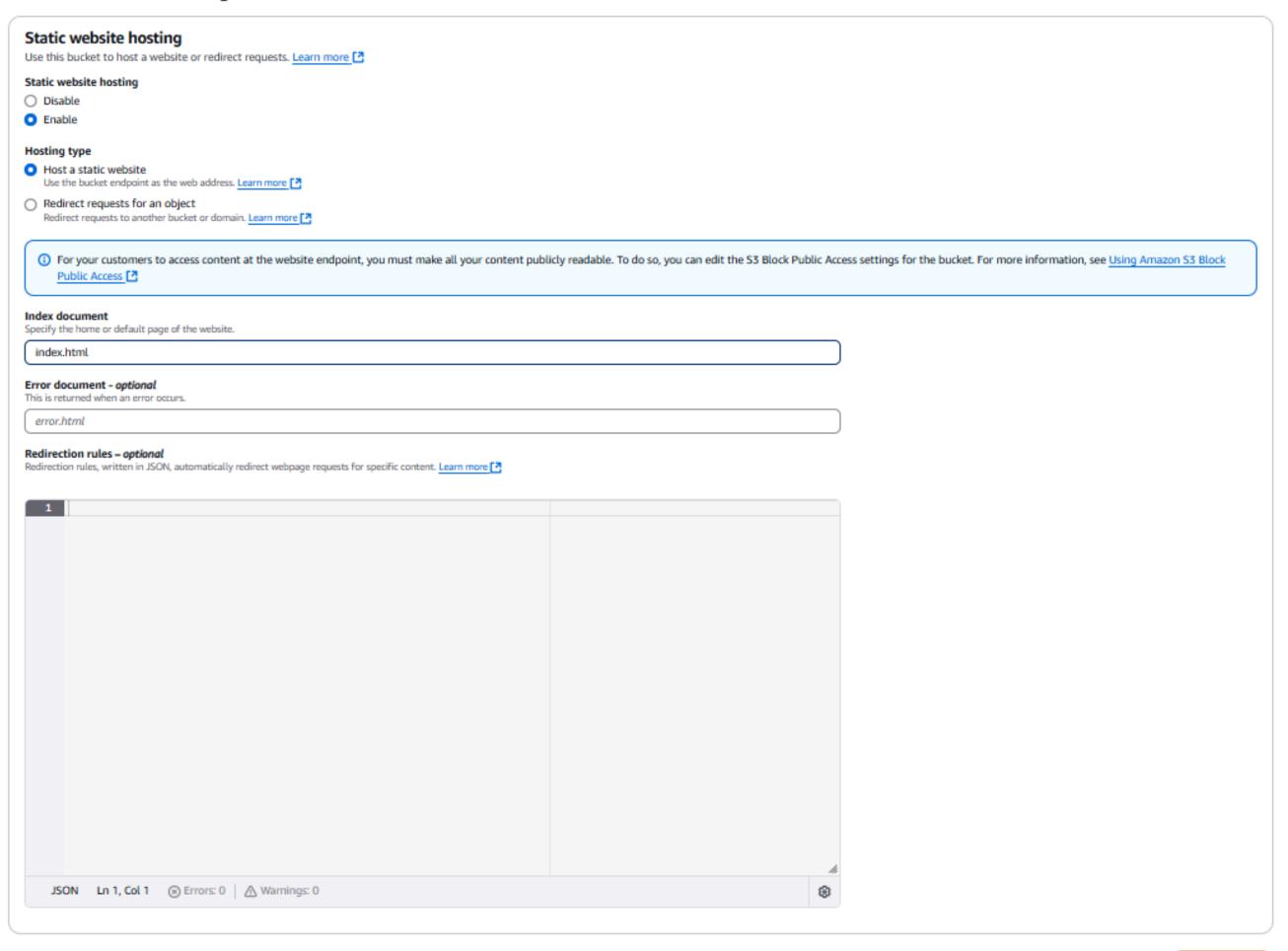


click on enable on static website hosting

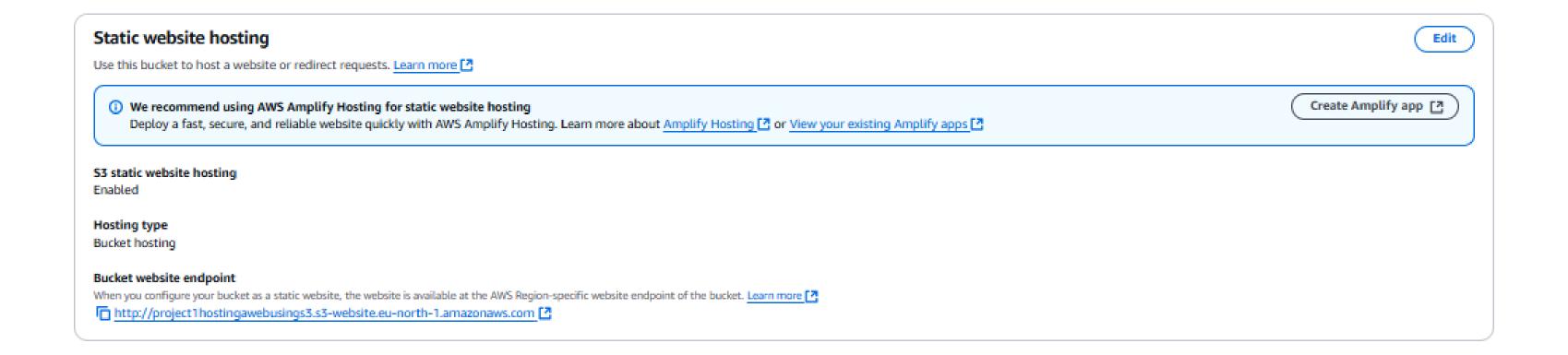
in index document write index.html

click on save changes

Edit static website hosting Info



After that you see on static website hosting, your endpoint so copy it and search on browser



After seaching you get 403 forbidden, Acces denied

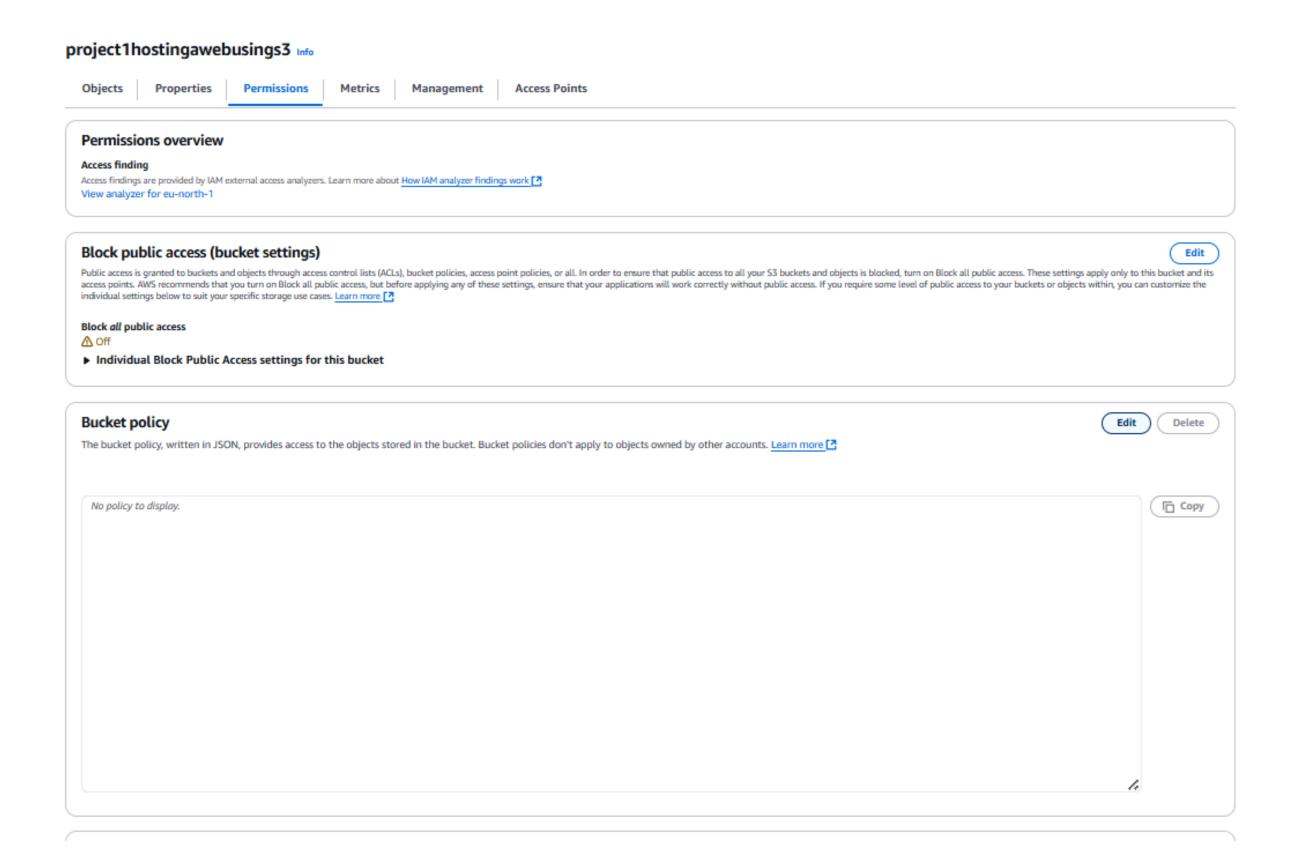
because you dont write or give permission policy



403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: CS21XQ2FADN9GW39
- HostId: BKIjB9YWOQPMpkHtnxjUGHILpBJA7YLe6mPYvb7hgdQqGpQSserXRtnpLr+x0BHigCF8XgcH7FU=

Then go on permission tab and go to the bucket policy and click on edit



Write the code in permission in the resource you write your arn or endpoit like this

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 Bucket ARN arn:aws:s3:::project1hostingawebusings3 Policy "Version": "2812-18-17",

Policy examples [2] Policy generator [2]

Select a statement

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

+ Add new statement

Preview external access

Edit statement

Edit bucket policy Info

"Statement": [

12 13

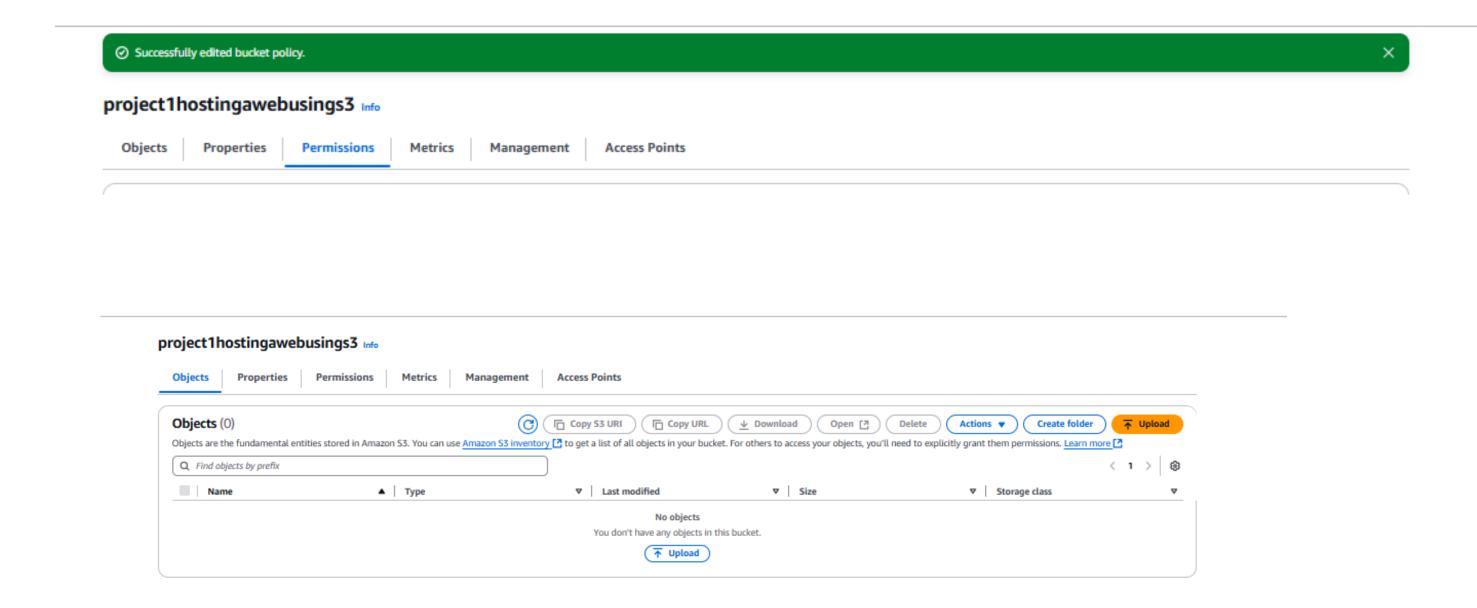
14 15

+ Add new statement

JSON Ln 1, Col 0

"Sid": "PublicReadGetObject",
"Effect": "Allow",
"Principal": "*",
"Action": [

After giving the permmision then you upload your website code so here iam uploading my portfolio website code



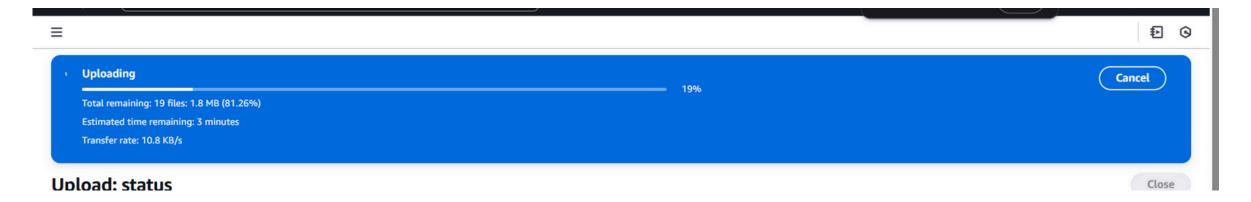
here i select my all code file and click on upload

Properties

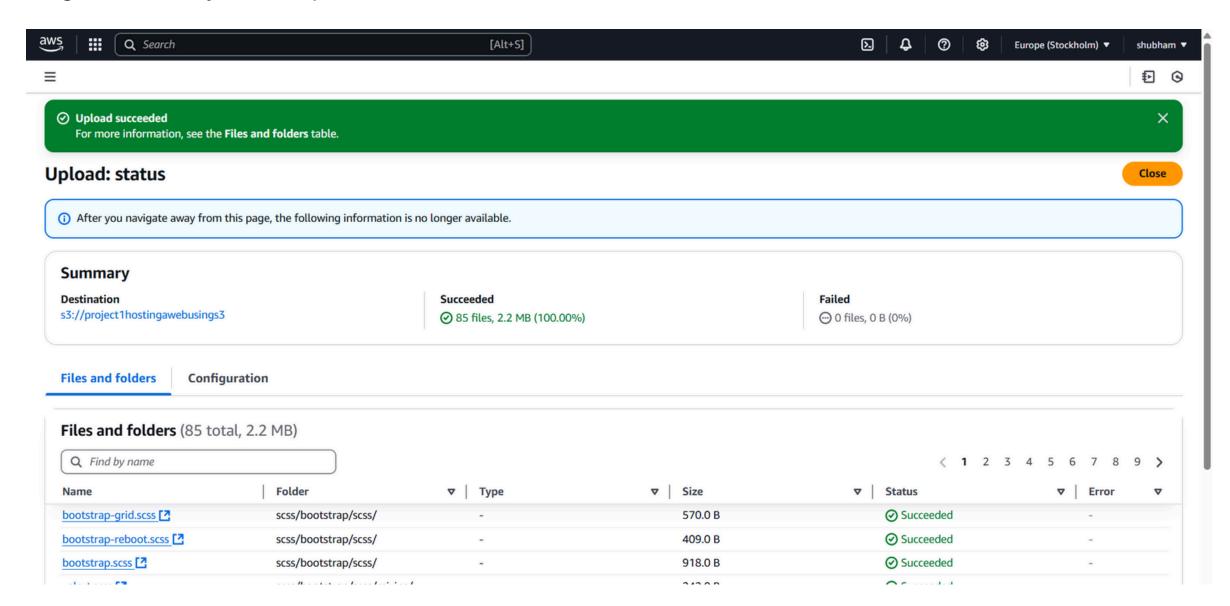
Specify storage class, encryption settings, tags, and more.

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 (85 total, 2.2 MB) Add folder All files and folders in this table will be uploaded. Q Find by name < 1 2 3 4 5 6 7 8 9 > ■ Name ▼ Folder ▼ Type ▼ Size bootstrap-grid.scss scss/bootstrap/scss/ 570.0 B bootstrap-reboot.scss 409.0 B scss/bootstrap/scss/ 918.0 B bootstrap.scss scss/bootstrap/scss/ __ _alert.scss 242.0 B scss/bootstrap/scss/mixins/ _background-variant.scss scss/bootstrap/scss/mixins/ 695.0 B _badge.scss scss/bootstrap/scss/mixins/ 320.0 B _border-radius.scss scss/bootstrap/scss/mixins/ 1.8 KB _box-shadow.scss scss/bootstrap/scss/mixins/ 532.0 B 4.4 KB _breakpoints.scss scss/bootstrap/scss/mixins/ scss/bootstrap/scss/mixins/ 3.4 KB Destination Info Destination s3://project1hostingawebusings3 <a>[2 Destination details Bucket settings that impact new objects stored in the specified destination. ▶ Permissions Grant public access and access to other AWS accounts.

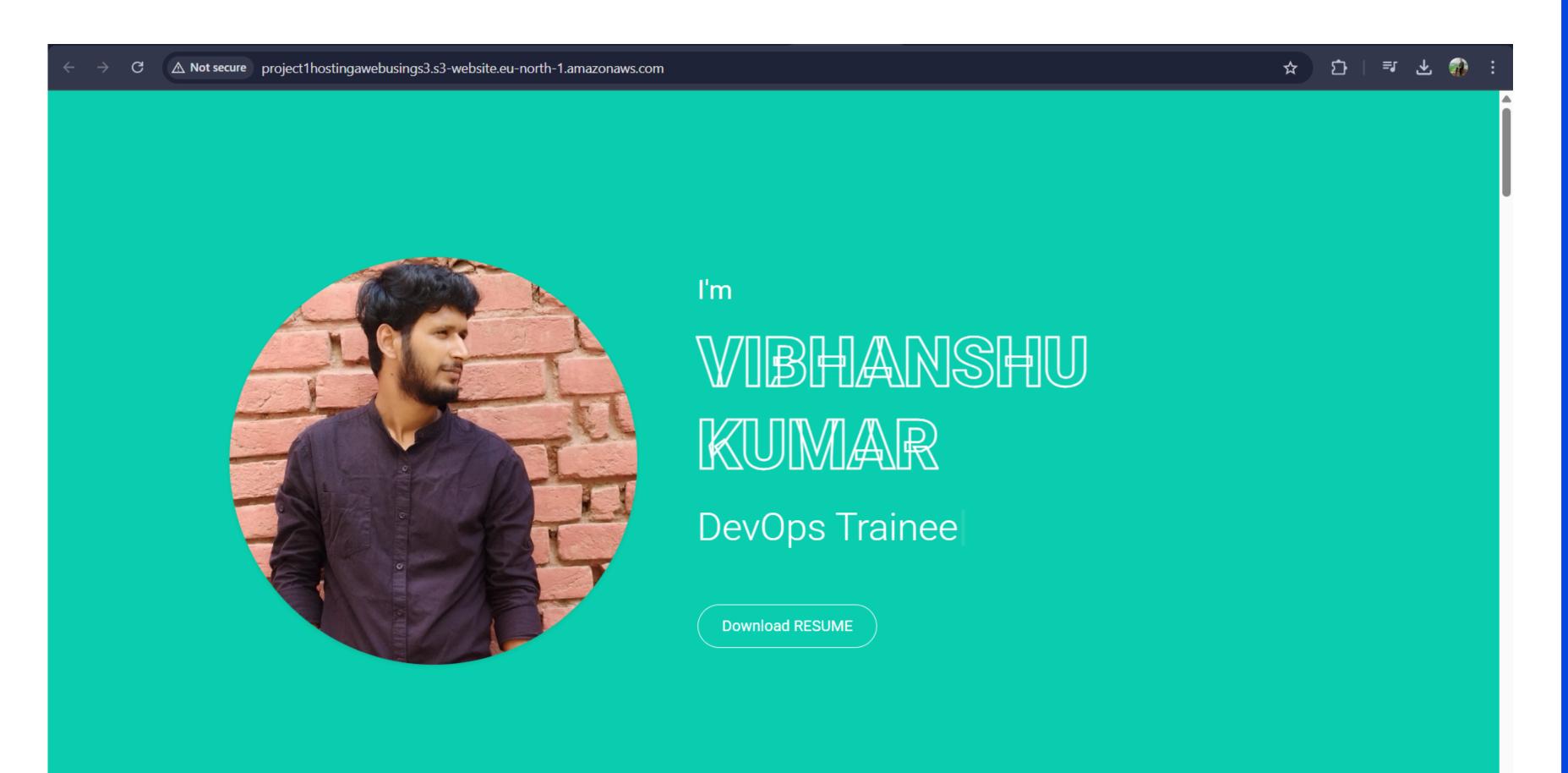
Then you seen your file is uploading



After successfully uploaded your file again search your endpoint on browser



Now you seen your website is succesfully hosted



THANK YOU

