

4. Deploy static Web application using AWS S3 service

- Name: Om Deore
- PRN: 22110318
- Div: TY(A)
- RollNo: 321022
- github: [All Assignments](#)

What is S3 service of AWS

AWS S3 stands for Amazon Simple Storage Service. It is a cloud-based storage service that can scale to an enormous size and provide high performance, availability, reliability, and security. It is a very cost-effective and secure replacement for your on-premises data center. The data is stored on cloud servers can be accessed through other web applications and websites globally.

Apart from data storage functionality, the AWS S3 bucket provides a remarkable feature of static website hosting over it.

Hosting a static website on Amazon S3

A website that doesn't involve server side communication is called a static website. Using S3 bucket we can host our static website in simple and easy steps.

Step 1: Create an S3 bucket

To create a S3 bucket first login to your AWS management console, search of S3 in services and click on that option. Next click on create bucket. You will be greeted with following form. In this tab give your bucket unique name. Keep other options as default.

← → ↻ <https://eu-north-1.console.aws.amazon.com/s3/bucket/create?region=eu-north-1&bucketType=general>

aws Services Search [Alt+S]

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region
Europe (Stockholm) eu-north-1

Bucket type [Info](#)

☒ **General purpose**
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory - New**
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#) [↗](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

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.

CloudShell Feedback

Since we wanted the website to be accessible to the audience, we had to grant the public access to the objects of this S3 bucket. For that, uncheck the Block all public access checkbox

in the “Block Public Access setting for this bucket” section:

← → ↻

🔒 https://eu-north-1.console.aws.amazon.com/s3/bucket/create?region=eu-north-1&bucketType=general

aws

Services

🔍 Search [Alt+S]

Object Ownership

Bucket owner enforced

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.

CloudShell

Feedback

Keep other options default and click on "Create bucket"

The screenshot shows the AWS console interface for creating a new S3 bucket. The browser address bar indicates the URL: `https://eu-north-1.console.aws.amazon.com/s3/bucket/create?region=eu-north-1&bucketType=general`. The AWS logo and navigation menu are visible at the top. The main content area is titled "No tags associated with this bucket." and includes an "Add tag" button. Below this, the "Default encryption" section is expanded, showing "Server-side encryption is automatically applied to new objects stored in this bucket." The "Encryption type" section has three radio button options: "Server-side encryption with Amazon S3 managed keys (SSE-S3)" (selected), "Server-side encryption with AWS Key Management Service keys (SSE-KMS)", and "Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)". The "Bucket Key" section has two radio button options: "Disable" and "Enable" (selected). At the bottom right, there are "Cancel" and "Create bucket" buttons. The "Create bucket" button is orange and highlighted.

← → ↻ `https://eu-north-1.console.aws.amazon.com/s3/bucket/create?region=eu-north-1&bucketType=general`

aws Services Search [Alt+S]

No tags associated with this bucket.

Add tag

Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info

☒ Server-side encryption with Amazon S3 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 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

☒ Enable

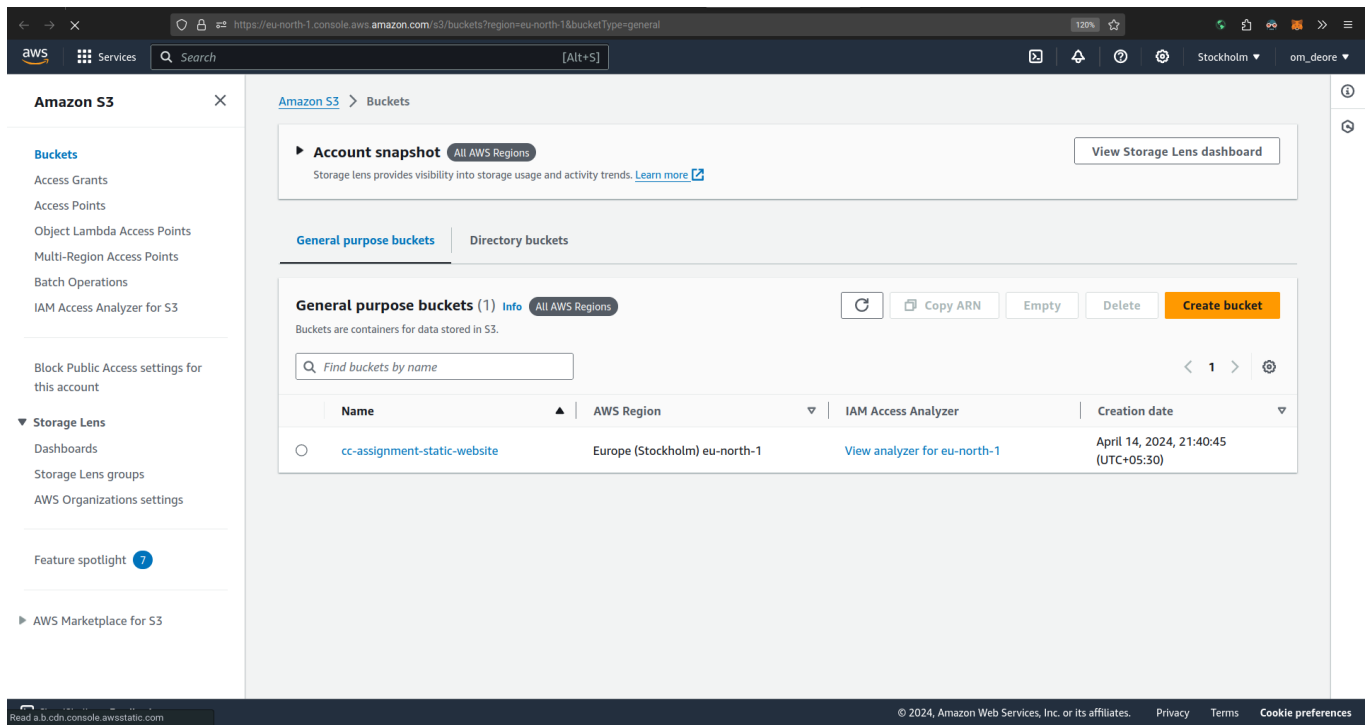
► **Advanced settings**

ⓘ After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel Create bucket

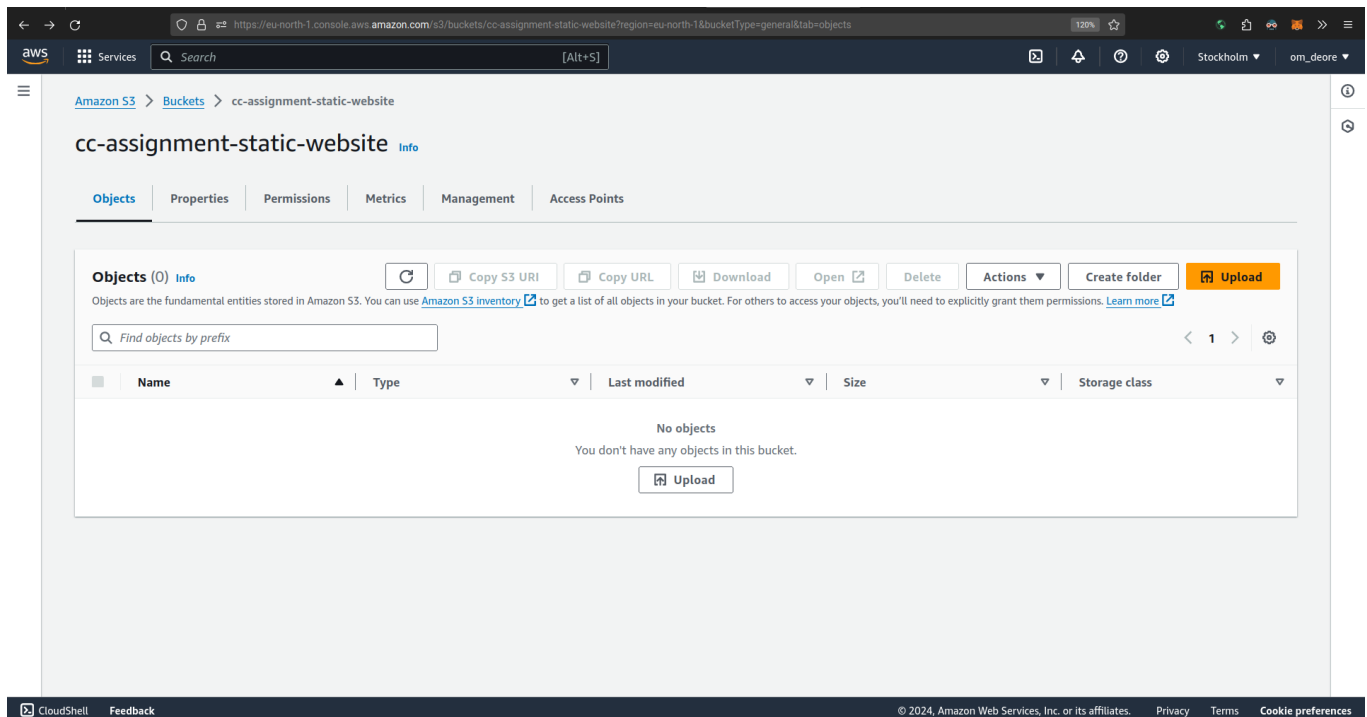
CloudShell Feedback

Now you can go to your buckets and see our recently created bucket being seen in list.

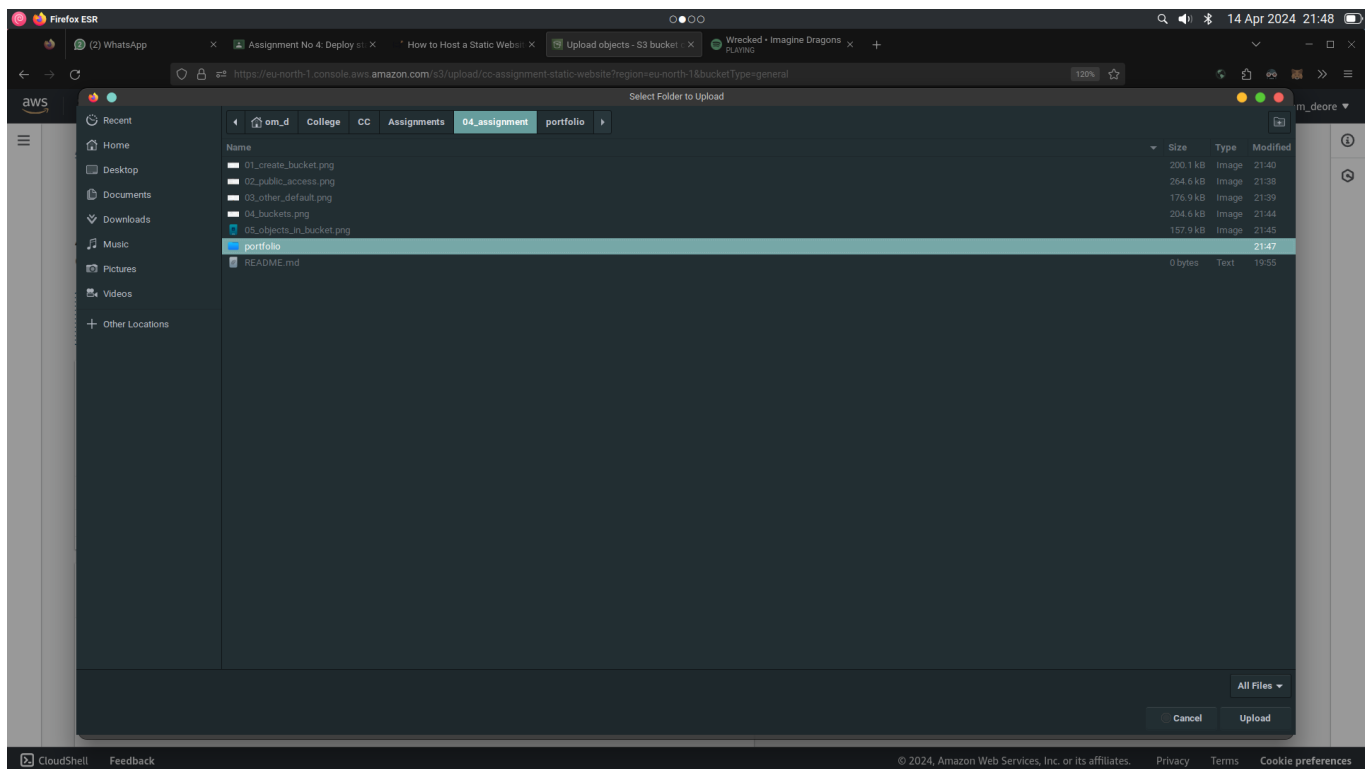


Step 2: Uploading contents of your website to S3 bucket

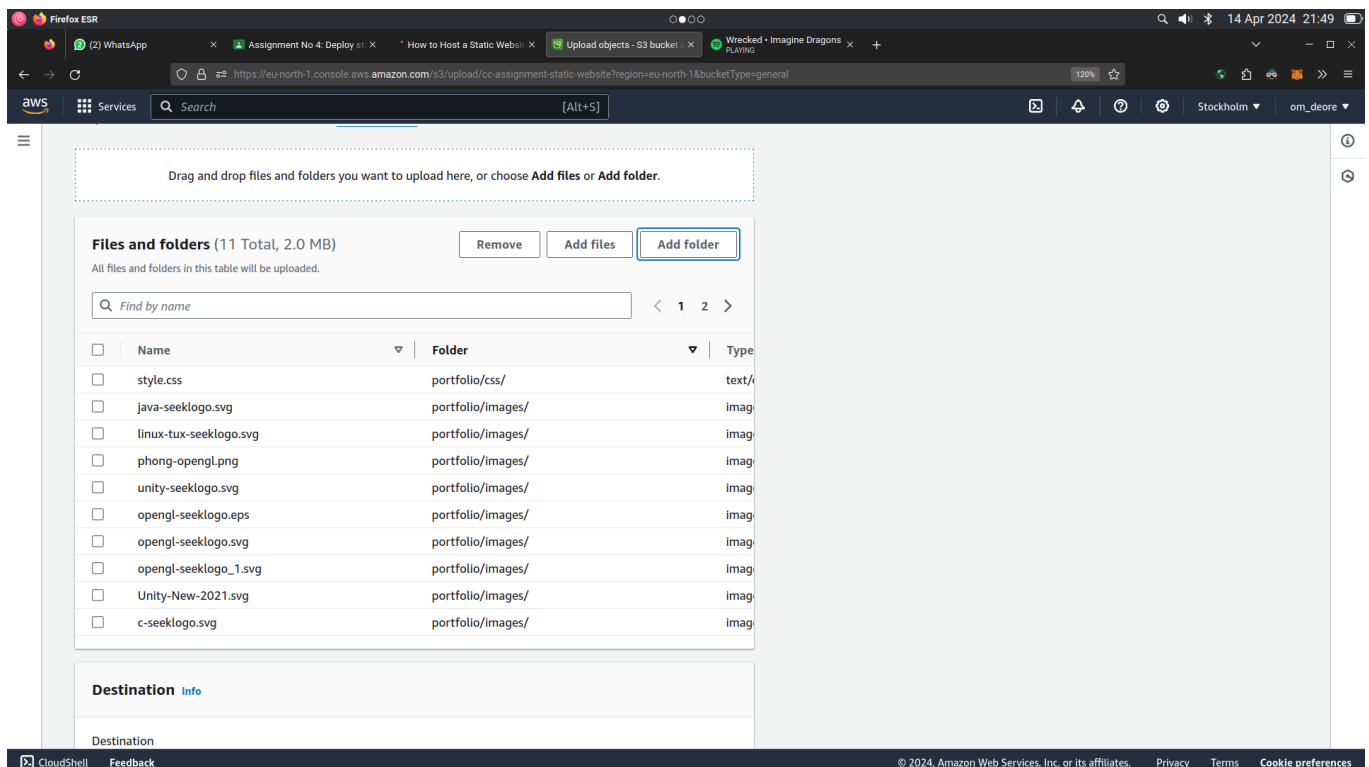
After creating bucket, it's time to upload our website on this storage we just created. Select the bucket. Go to objects tab. And click on upload. With this we can add our files to S3 bucket.



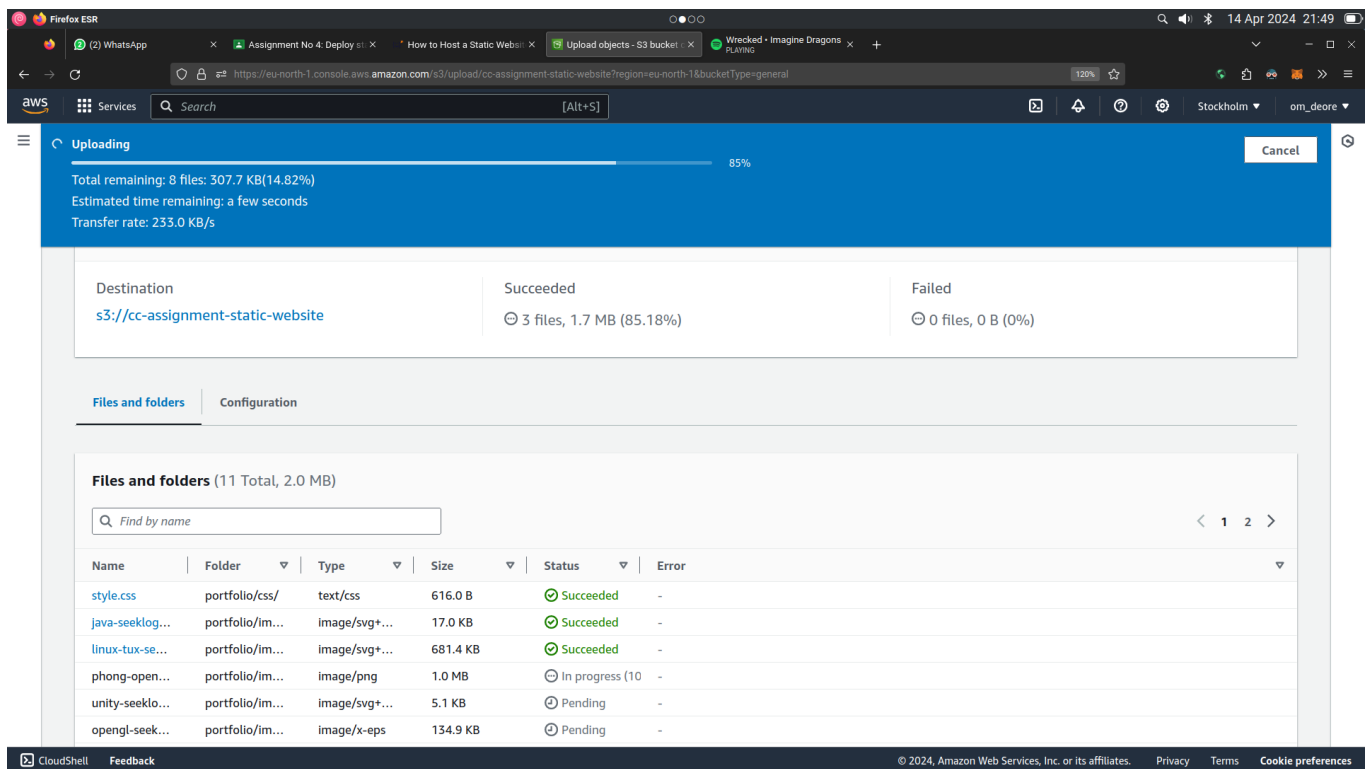
After clicking on upload, click on "Add Folder" button. It will prompt you to select the folder of our website



Now we can see files of our webpage.

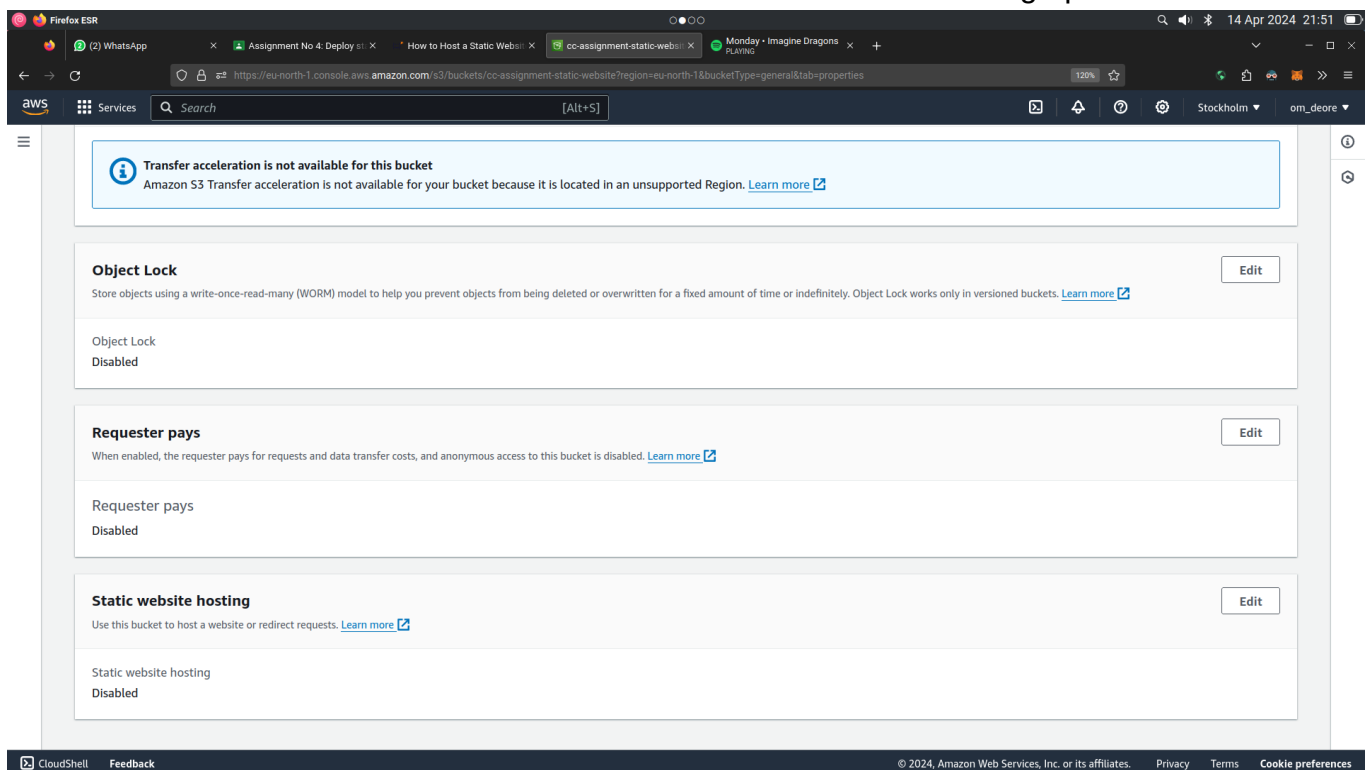


After clicking on "Upload", you see uploading being initiated. Once it is done your files are saved on this S3 bucket.

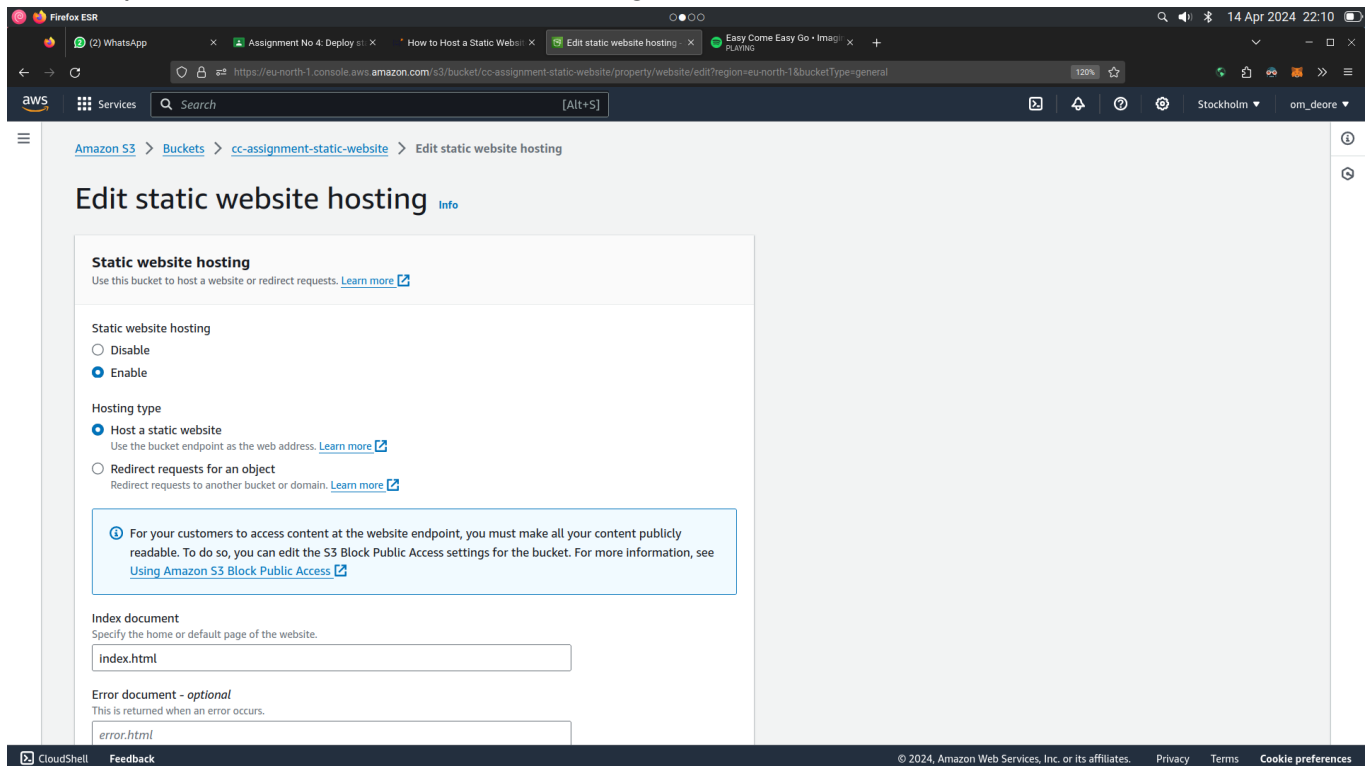


Step 3: Setting up static web hosting in S3

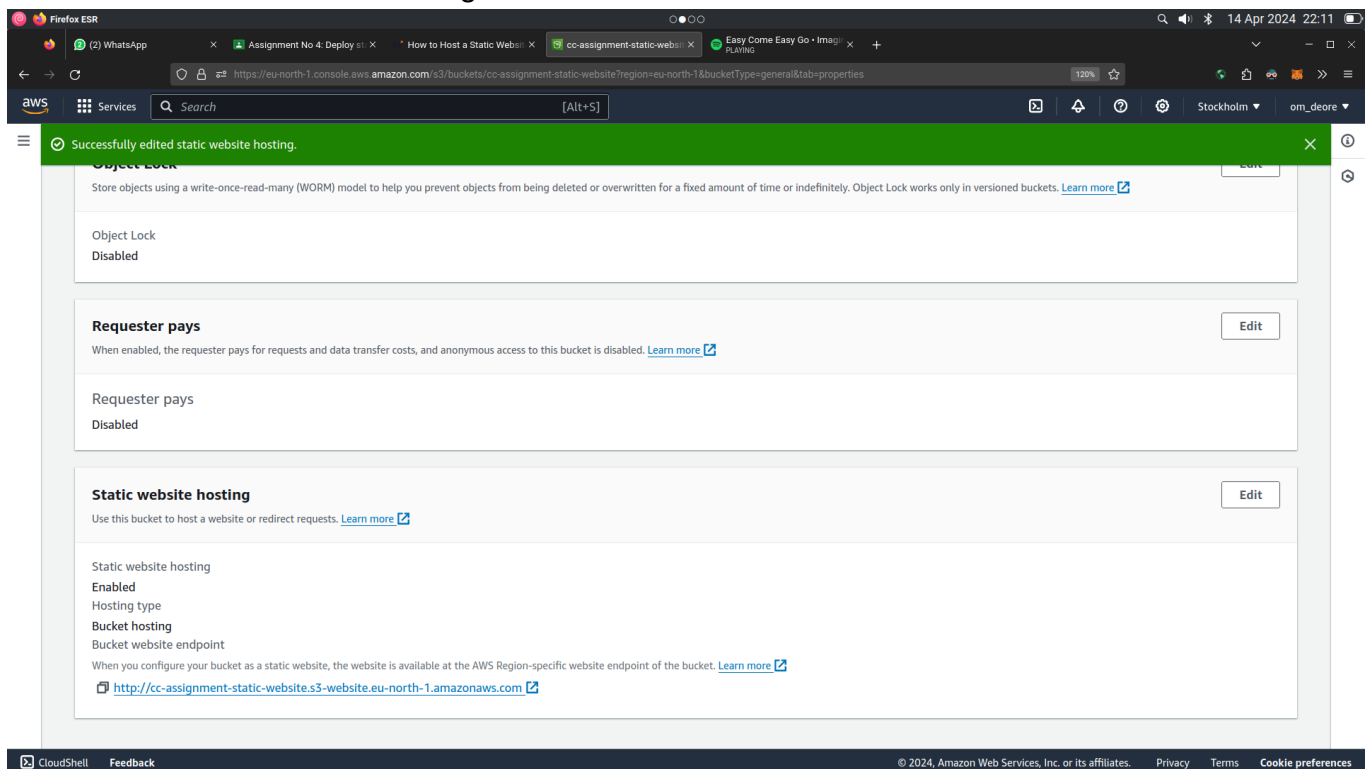
After uploading static site content, enable hosting on your S3 bucket. For this go to properties tab in current bucket. Scroll down and click edit on Static website hosting option.



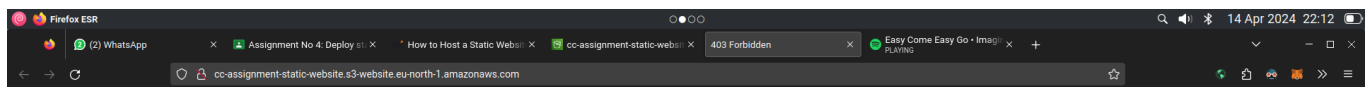
Select option to enable static website hosting



Now, our S3 bucket is hosting the website content uploaded to it and is publicly accessible. In order to access the website, we need a public URL that AWS itself provides. This URL can be seen in the static website hosting section of the S3 bucket:



Go to the URL provided by S3, and the website will not be accessible because we have made the S3 bucket public, but the objects inside the S3 bucket are not public yet. This problem can be solved by using the S3 bucket policies.

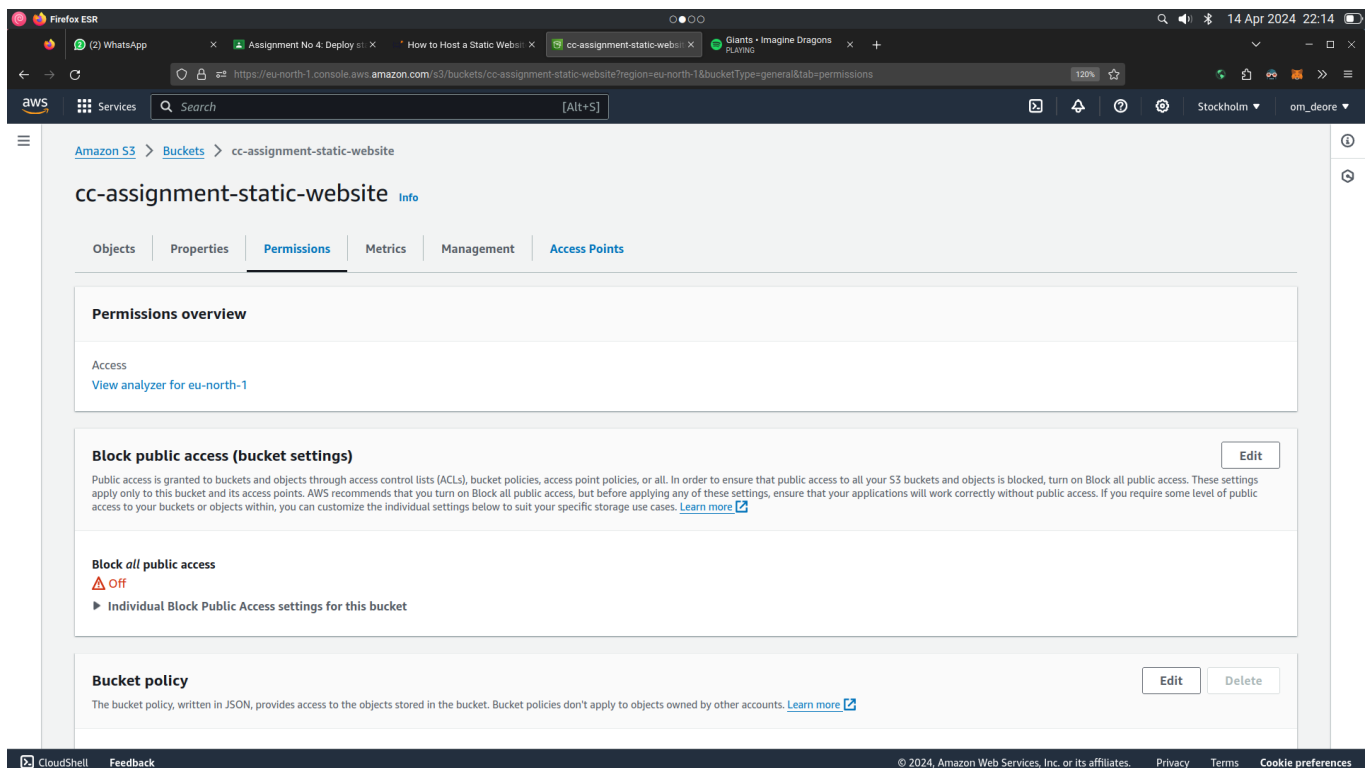


403 Forbidden

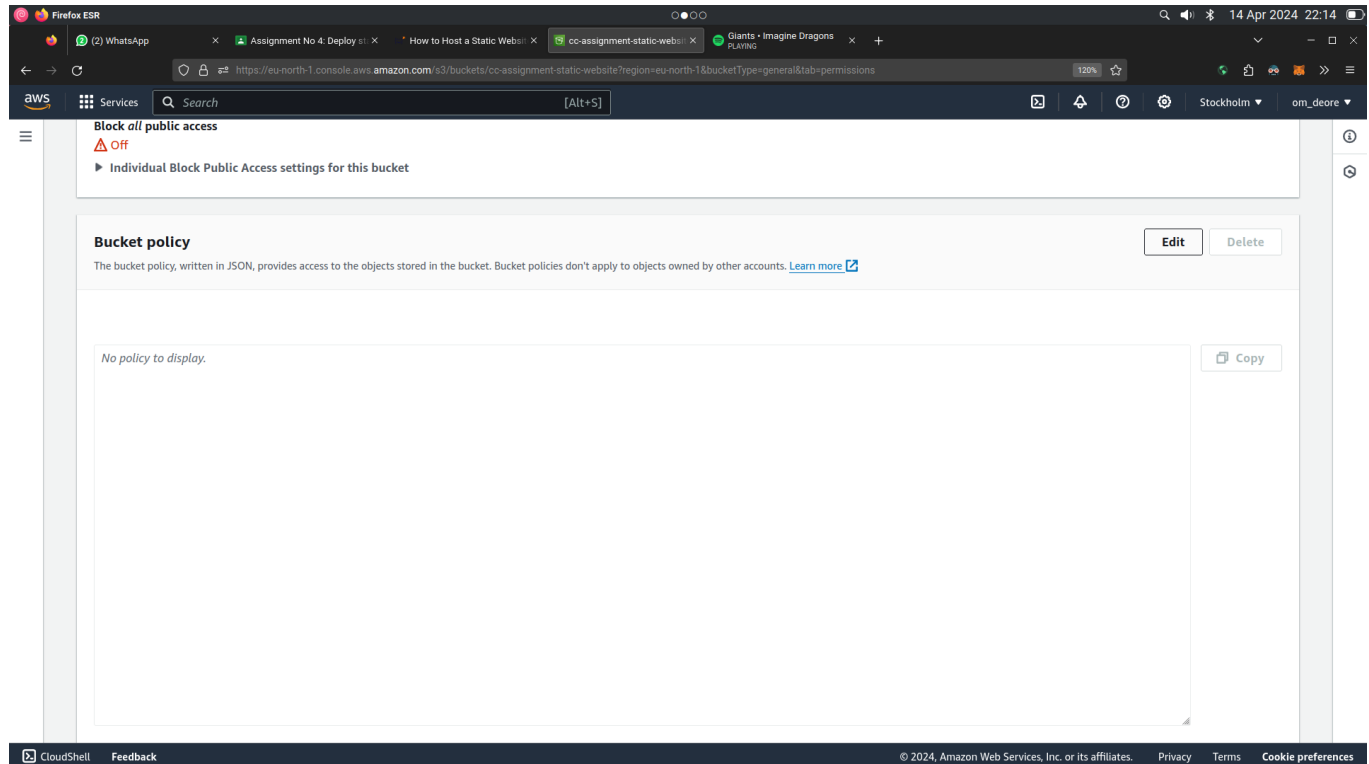
- Code: AccessDenied
- Message: Access Denied
- RequestId: S4P072YQ7N4ANNRZ
- HostId: IK4/5XIWwmjUyLvIdkLp1PazCftcn6UC65UTMoZk5vDAXkSGZnMeFLsPC63k+oQ/B7FPqKk4+oE=

Step 4: setting up permissions in S3 bucket

To make our content accessible publicly, we need to add a bucket policy for which we have to go to the permissions tab of our S3 bucket to make some changes to the permissions of our S3 bucket:



Now, move to the bucket policy section and click on the **Edit** button.



Paste the following JSON in the editor to allow the public to read files from the bucket

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicRead",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::cc-assignment-static-website/*"
    }
  ]
}
```

Click on save changes to continue.

The screenshot shows the AWS IAM console's bucket policy editor. The bucket ARN is `arn:aws:s3::cc-assignment-static-website`. The policy is a JSON document with a single statement named `PublicRead` that allows `s3:GetObject` and `s3:GetObjectVersion` actions for the principal `/*` (everyone) on the specified resource. The right-hand sidebar shows the 'Add actions' section with a search bar and a list of services including S3, AMP, API Gateway, and others.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "PublicRead",
6       "Effect": "Allow",
7       "Principal": "*",
8       "Action": [
9         "s3:GetObject",
10        "s3:GetObjectVersion"
11      ],
12      "Resource": "arn:aws:s3::cc-assignment-static-website/*"
13    }
14  ]
15 }
```

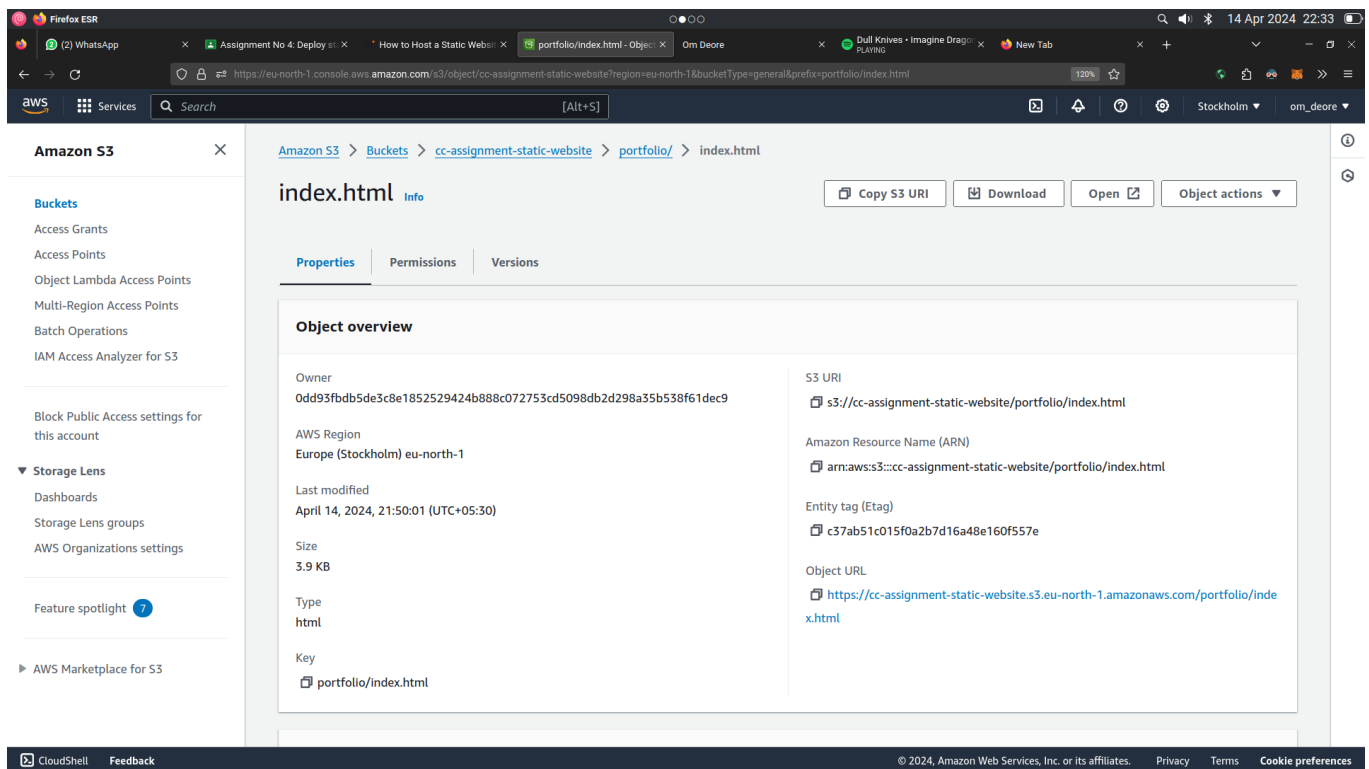
Step 5: Accessing the Website Through URL

Now we are ready to get our URL to `index.html` file and see our hosted website. Go to "Objects" tab and navigate to `index.html` file. Click on it

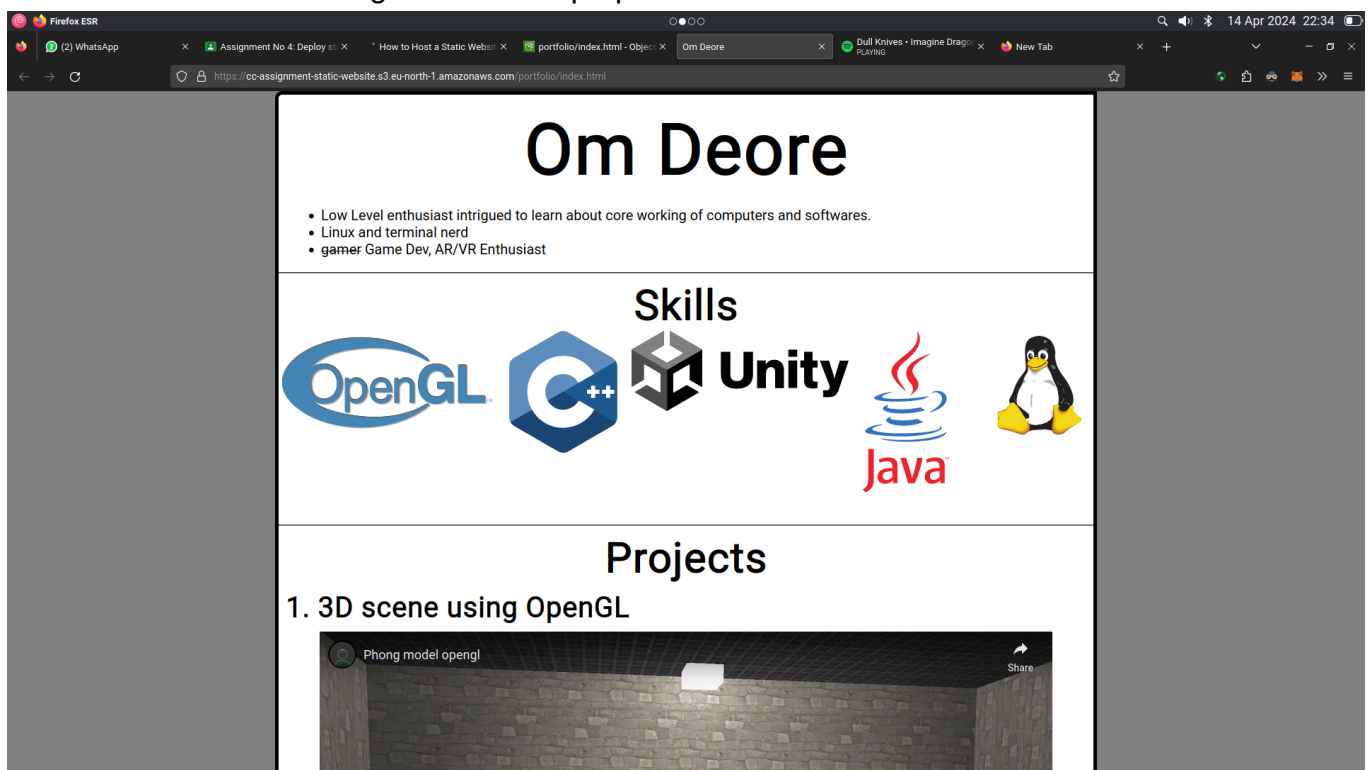
The screenshot shows the Amazon S3 console for the bucket `cc-assignment-static-website`. The 'Objects' tab is active, displaying a list of objects. The `index.html` object is selected. The console provides a search bar and a table of objects with columns for Name, Type, Last modified, Size, and Storage class.

	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	css/	Folder	-	-	-
<input type="checkbox"/>	images/	Folder	-	-	-
<input type="checkbox"/>	index.html	html	April 14, 2024, 21:50:01 (UTC+05:30)	3.9 KB	Standard

Here you can see object url. Click on it to visit your webpage you just hosted.



You can see website being hosted on laptop and mobile browser





Om Deore

- Low Level enthusiast intrigued to learn about core working of computers and softwares.
- Linux and terminal nerd
- ~~gamer~~ Game Dev, AR/VR Enthusiast

Skills