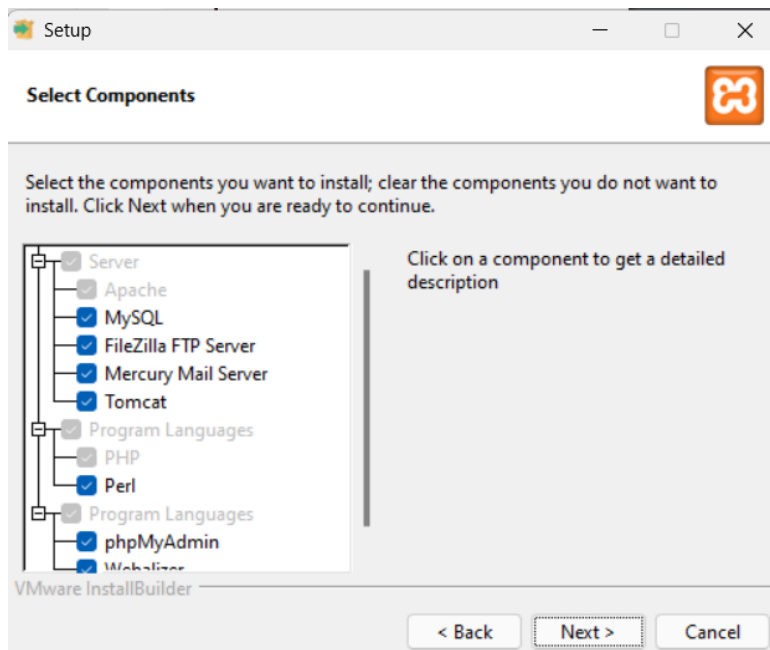## Static Hosting on Local Server (Xampp)

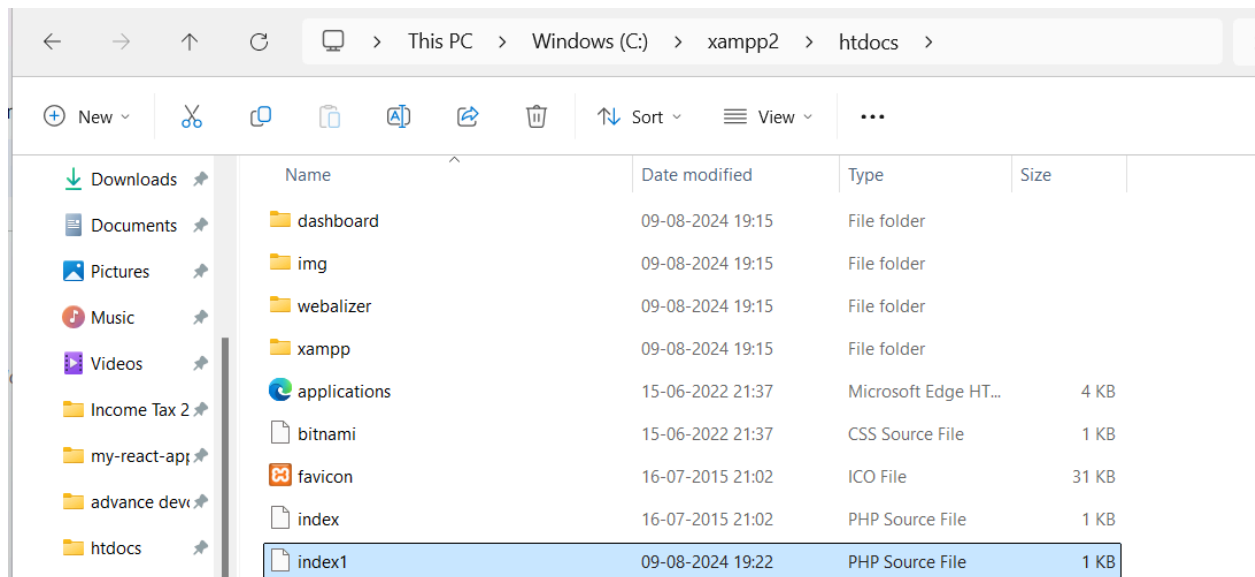Install Xampp from https://www.apachefriends.org/ and follow the default steps for installing xampp
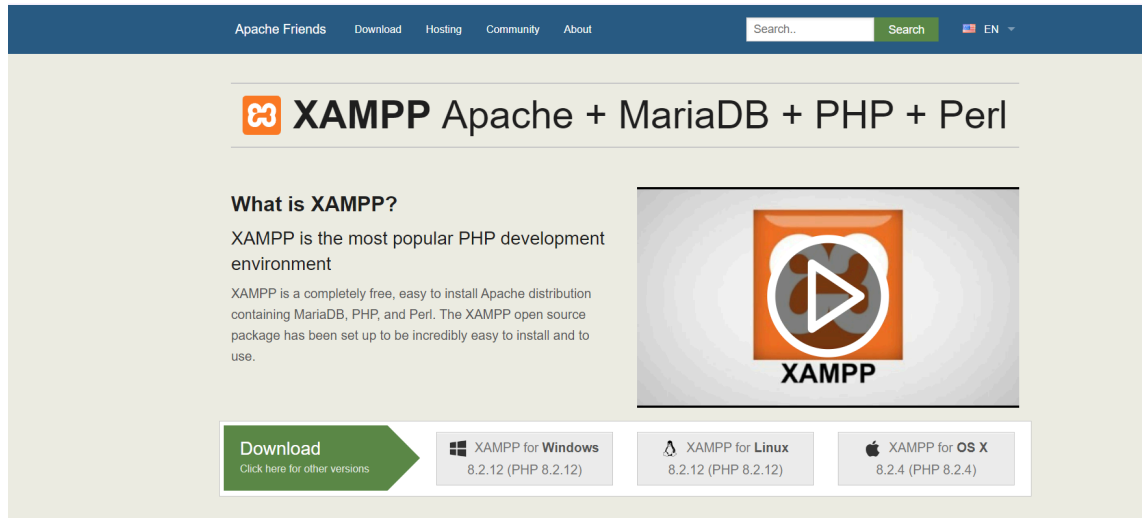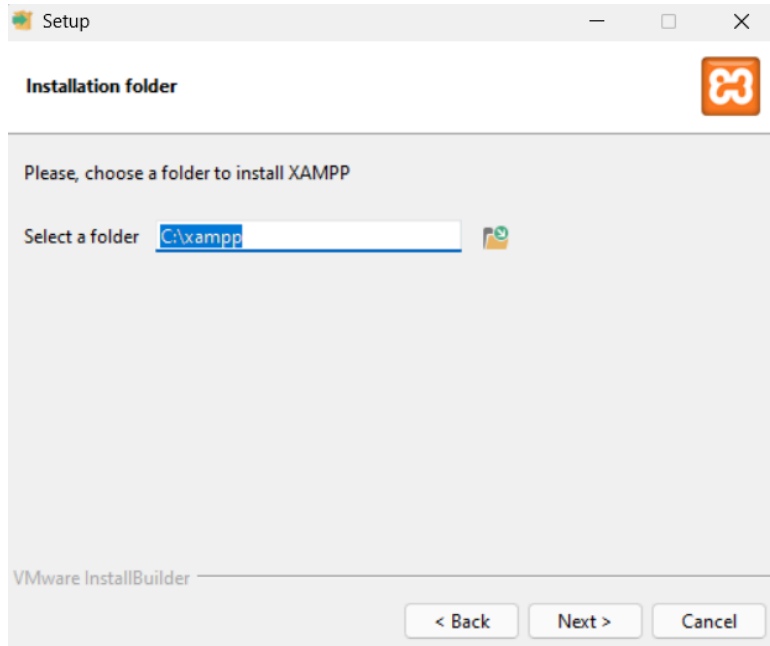
Setup a file that is to be hosted on the server. Make sure the file has extension .php
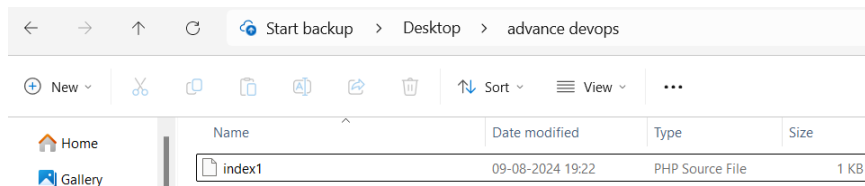
Go to the directory where XAMPP was installed. Go to htdocs folder. Place your folder in this directory.

Open XAMPP Control Panel, start the Apache service (Required) and mySQL service (if needed)
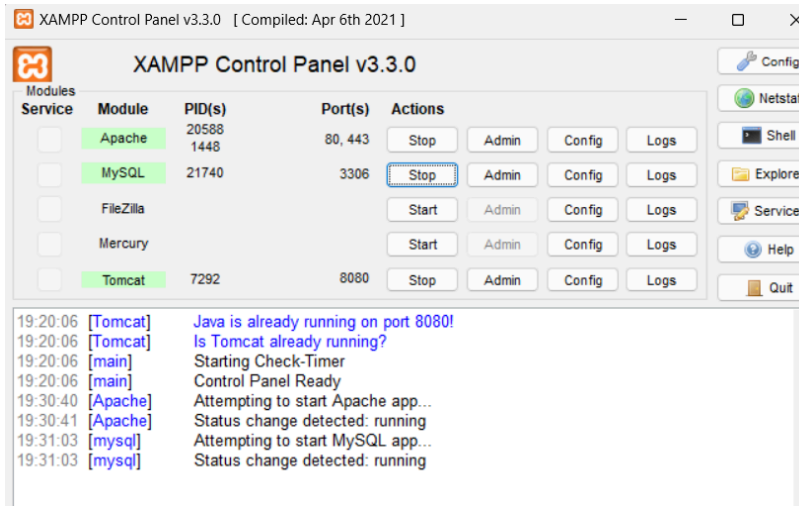
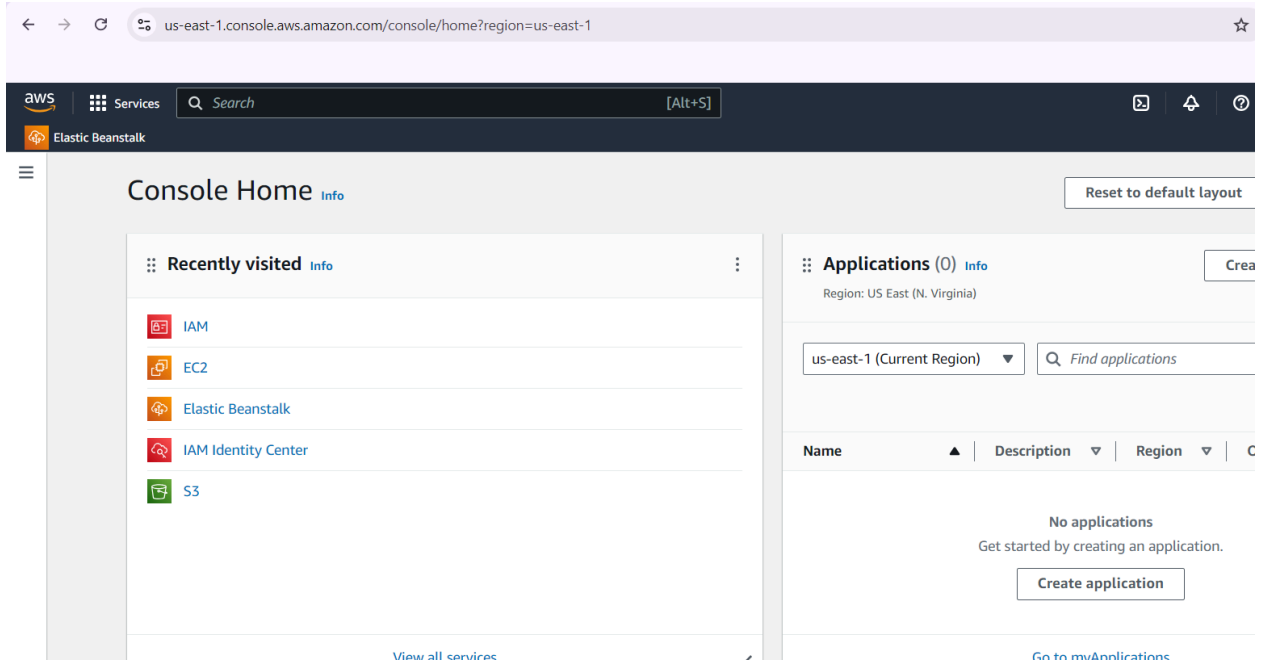
Open your web browser. Type localhost/YOUR_FILENAME.php. This will open your website on your browser.
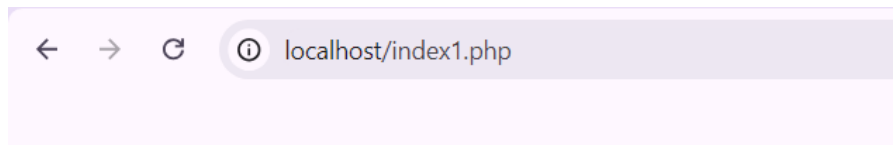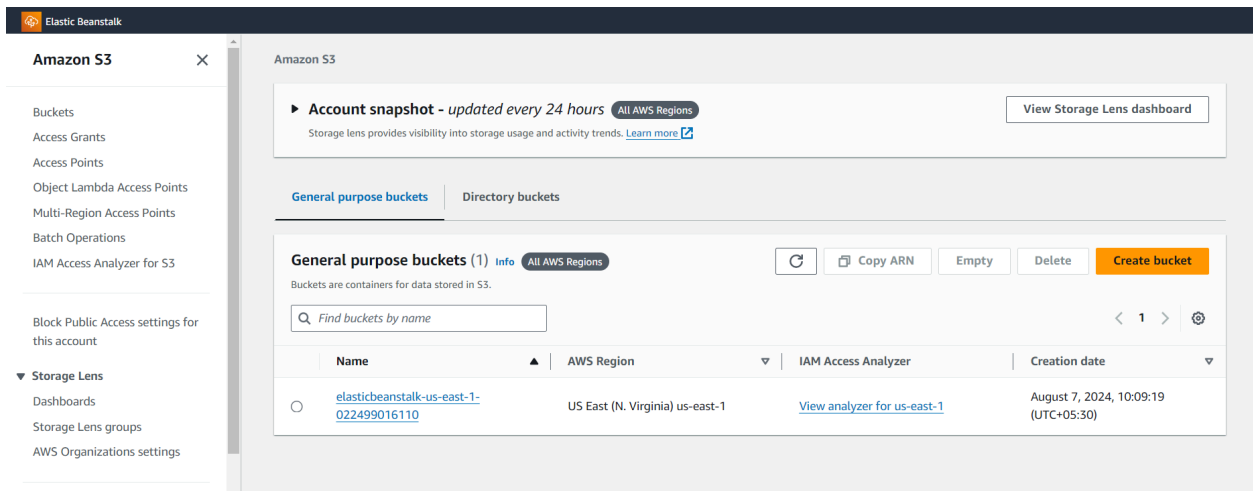

Hello World!This website was created by Shiven Bansal

Hosting a static website on amazon s3

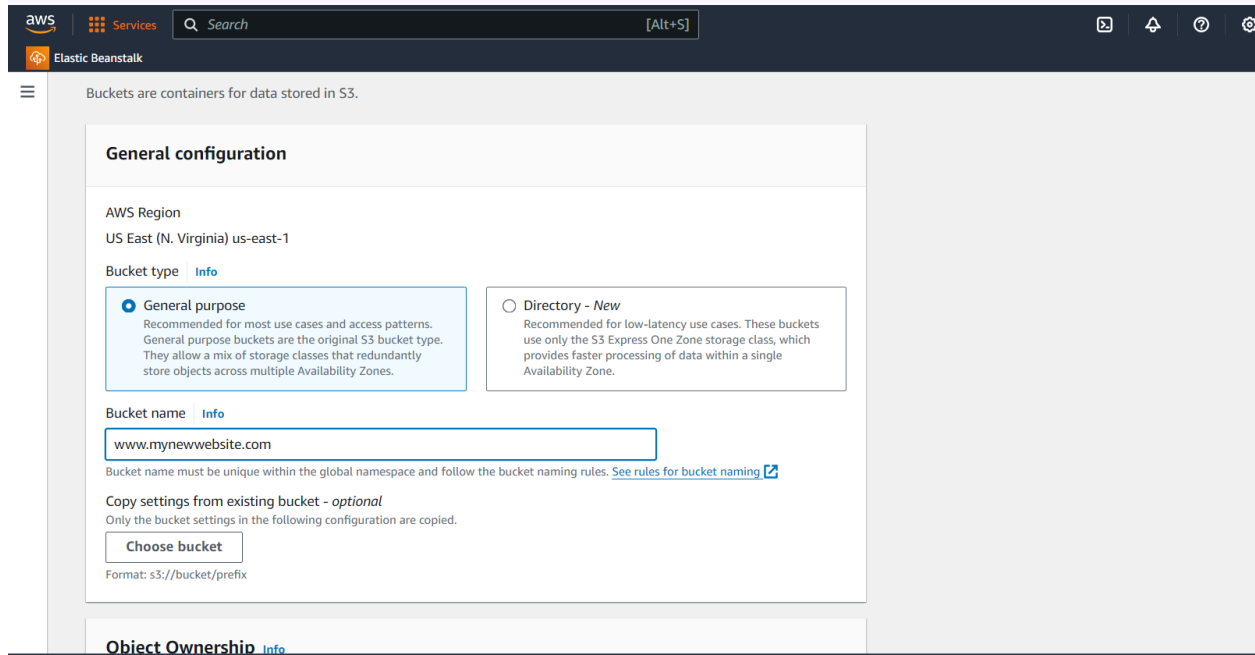Go to console.aws.amazon.com and click on S3

Click on Create Bucket

Write the bucket name for your website and click create bucket

Enable static website hosting after creating the bucket and fill in the details as follows. Then click on Save changes

Hosting type

● Host a static website
Use the bucket endpoint as the web address. Learn more 🗗

○ Redirect requests for an object
Redirect requests to another bucket or domain. Learn more 🗗

> ⓘ For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access 🗗

Index document
Specify the home or default page of the website.

| index.html |

Error document - *optional*
This is returned when an error occurs.

| 404.html |

Redirection rules – *optional*
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. Learn more 🗗

Now you can access your website from the endpoint http://www.mynewwebsite.com.s3-website-us-east-1.amazonaws.com . Now go to the bucket and click on upload files to upload your files in your website.

Amazon S3 > Buckets > www.mynewwebsite.com > Upload

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 SDK 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 (1 Total, 292.0 B)   Remove | Add files | Add folder
All files and folders in this table will be uploaded.

🔍 Find by name   < 1 >

☑	Name	▽	Folder	▽	Type
☑	index.html		-		text/html

Destination Info

By clicking on the url the website gives 403 forbidden error because contents of the bucket are not available for the public users.

403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: Q3K0QMPPMMBQ8TCR
- HostId: 2GN7HpN25IH4RV1BD7b1+l8CCLIxbi7fU046fJj/GwR/dbv1BPlHEeAftyqGhVGVLGH6GrIxanU=

An Error Occurred While Attempting to Retrieve a Custom Error Document

- Code: AccessDenied
- Message: Access Denied

To change this, go to Permissions tab, go to Block public access and click on edit . Uncheck the block all public access checkbox and click save.

Edit Block public access (bucket settings) Info

Block public access (bucket settings)

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**

  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.

Update your bucket policy as follows and click save changes

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 oth

Bucket ARN

📋 arn:aws:s3:::www.mynewwebsite.com

Policy

```
 1 ▼ {
 2     "Version": "2012-10-17",
 3 ▼   "Statement": [
 4 ▼   {
 5       "Sid": "PublicReadGetObject",
 6       "Effect": "Allow",
 7 ▼     "Principal": {
 8         "AWS": "*"
 9       },
10       "Action": "s3:GetObject",
11       "Resource": "arn:aws:s3:::www.mynewwebsite.com/*"
12     }
13     ]
14 }
15
```

Now after reloading your website, you will be able to see it.

⬅ ➡ C ⚠ Not secure mynewwebsite.com.s3-website-us-east-1.amazonaws.com

Hello World!

This website was created by Shiven Bansal