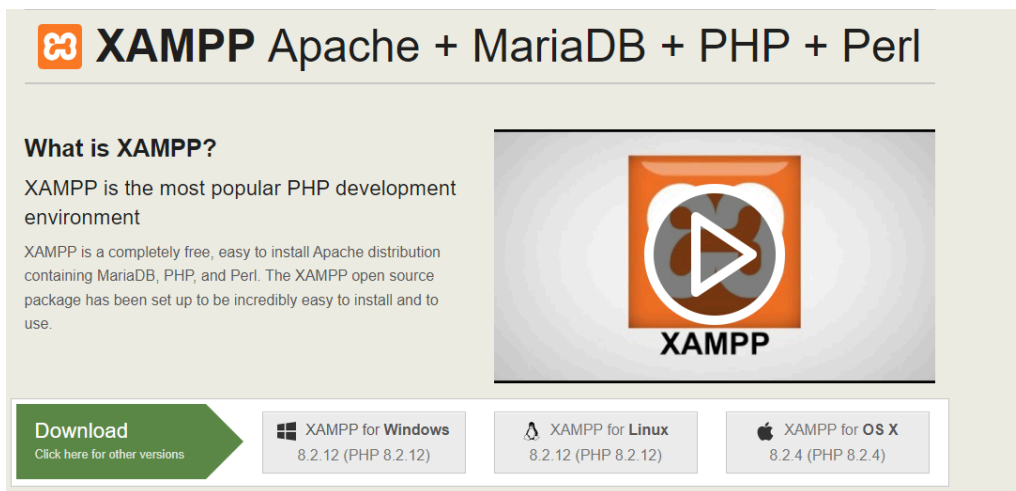**NAME: HIMANSHU NAIK**
DIV:D15C
ROLL NO :63
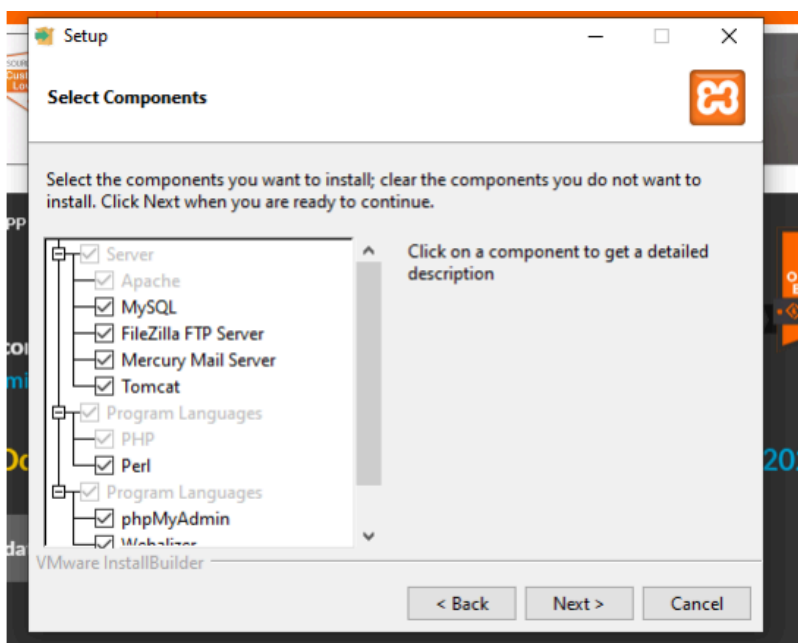
Exp 1A :Static Hosting:
1) On local server (XAMPP) Step 1: Install XAMPP

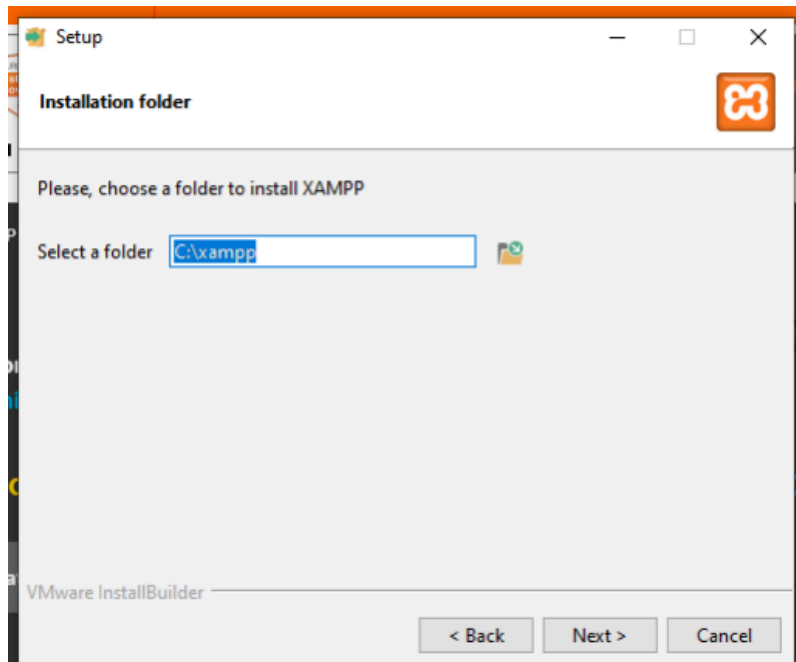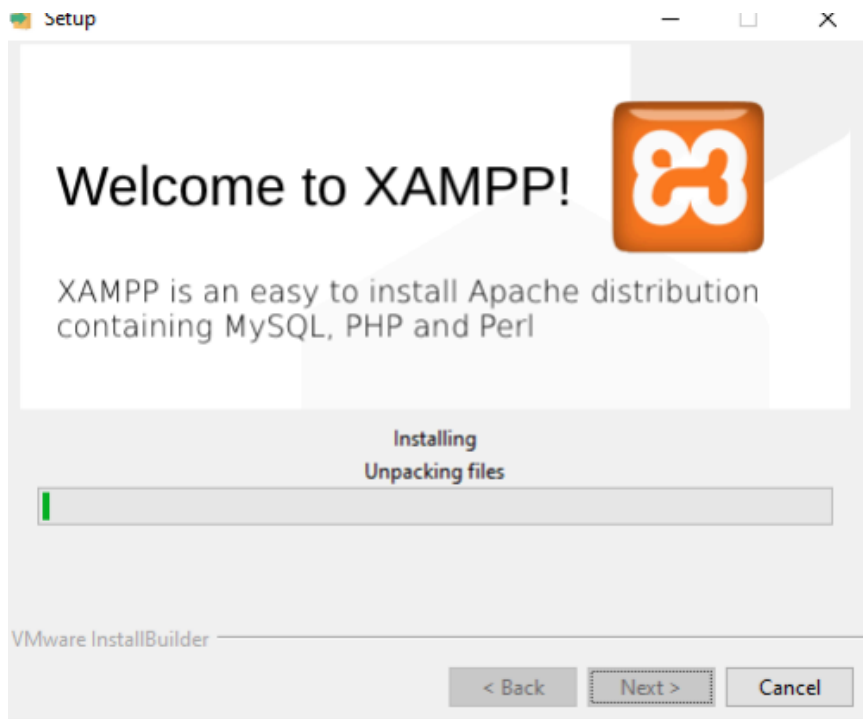**1)** Select your OS. It will automatically start downloading.

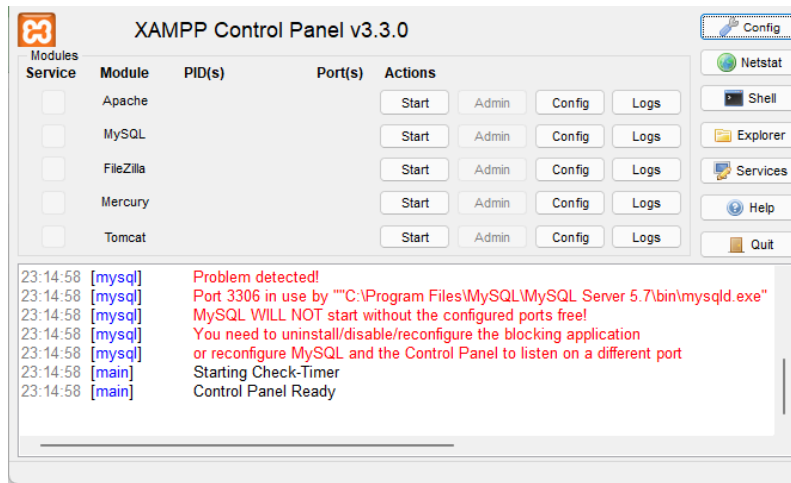**2) Open the setup file. Select all the required components and click next**

3) Choose the folder to install XAMPP in. Make sure the folder is empty. Click next

4) Select the language, click next. XAMPP starts to install

Open XAMPP Control Panel, start the Apache service (Required) and mySQL service

Go in the browser and type localhost and hit enter you will get to see the file you created like in this case index1.php

Index of /php-practice

Name	Last modified	Size	Description
Parent Directory		-	
index1.php	2024-09-20 00:14	0	

Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at localhost Port 80

Open your web browser. Type localhost/YOUR_FILENAME.php. This will open your website on your browser

II , Himanshu naik from d15c

Hosting a static website on Amazon S3

After creating the bucket on AWS add the file in it that is to be hosted and configure the visibility as public and add /* at the end of the resource key.

2) AWS S3 Step 1: Login to your AWS account. Go to services and open S3
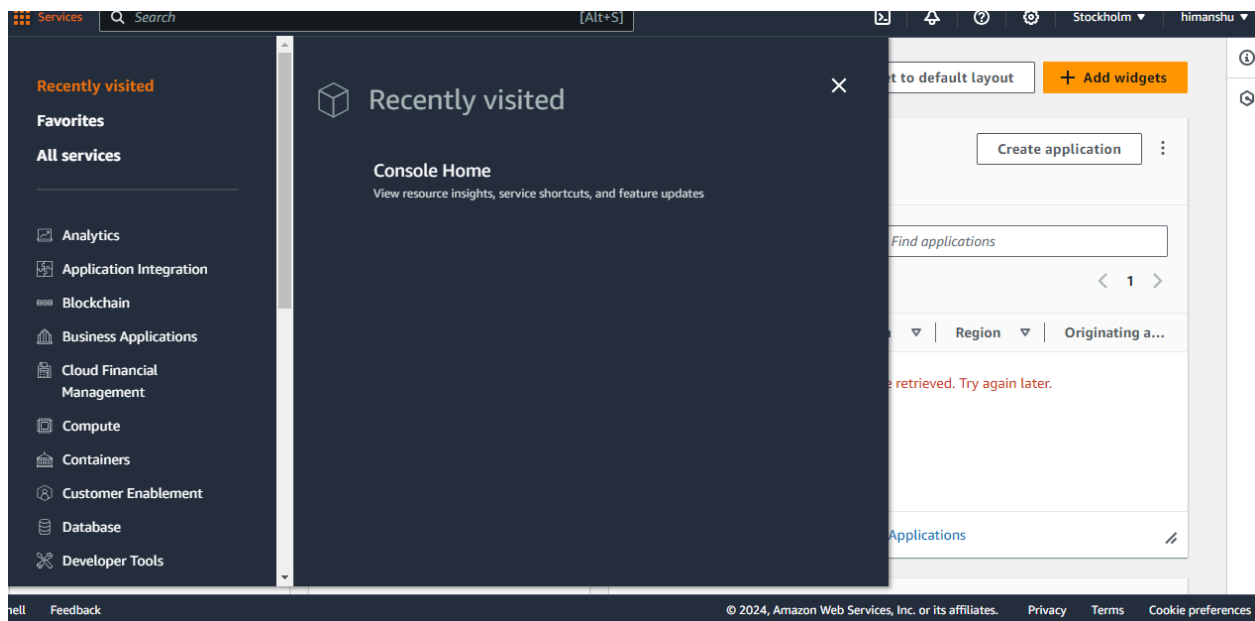
Step 2: Click on Create Bucket
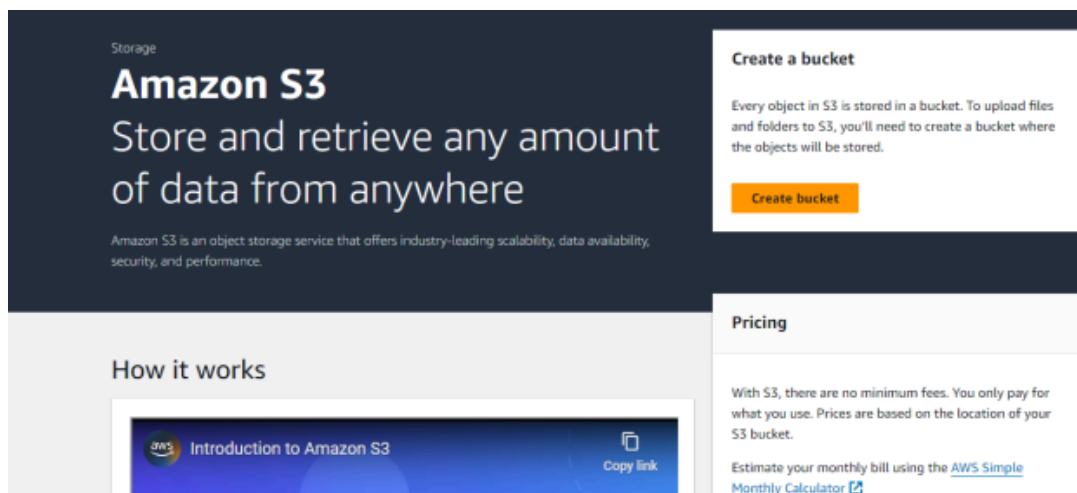
Step 3: Give a name to your bucket, keeping other options default, scroll down and click on Create Bucket

Step4: Scroll down till you find Static website hosting, click on edit

Step 5: Enable static website hosting, in Index document, write the name of your document and in error document, give name as 404.html. Save your changes

Step 6: Go to Objects tab and click on upload file

Step 7: This will take you to the Objects screen. Switch to Properties, scroll down to Static web hosting. There you would find the link (Bucket website endpoint) to your website.

Static website hosting
Use this bucket to host a website or redirect requests. Learn more ⃞

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 ⃞

Step 8: Open the link. It will show a 403 forbidden error screen as the contents of the bucket are not available for the public users. To change this, go to Permissions tab, go to Block public access and click on edit

403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: DM25X6E297MM1SXZ
- HostId: 4fGfAMLunY2ZQ8i9NcuIEDV8CDSLvqSbUj5+gtTqRIGOB5x2rj3/2w4/0mp3CvqJ+IXAPOvq+/4=

Step 9: Uncheck the Block all public access checkbox and click on 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.

```
{
"Version": "2012-10-17",
 "Statement": [
{
"Sid": "PublicReadGetObject",
"Effect": "Allow",
"Principal": { "AWS": "*"
 },
"Action": "s3:GetObject",
"Resource": "arn:aws:s3:::YOUR-BUCKET-NAME-HERE/*" }
]
}
```

 Paste this code snippet in the policy textarea.
Replace YOUR-BUCKET-NAME-HERE with the name you have given to your bucket.

Save the changes.

```
▼ {
    "Version": "2012-10-17",
▼ "Statement": [
▼ {
    "Sid": "PublicReadGetObject",
    "Effect": "Allow",
▼ "Principal": {
    "AWS": "*"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::YOUR-BUCKET-NAME-HERE/*"
    }
    ]
    }
```