

**Name: Vidhi Gulhane**

**Division:D15B**

**RollNo:17**

## **EXPERIMENT 01**

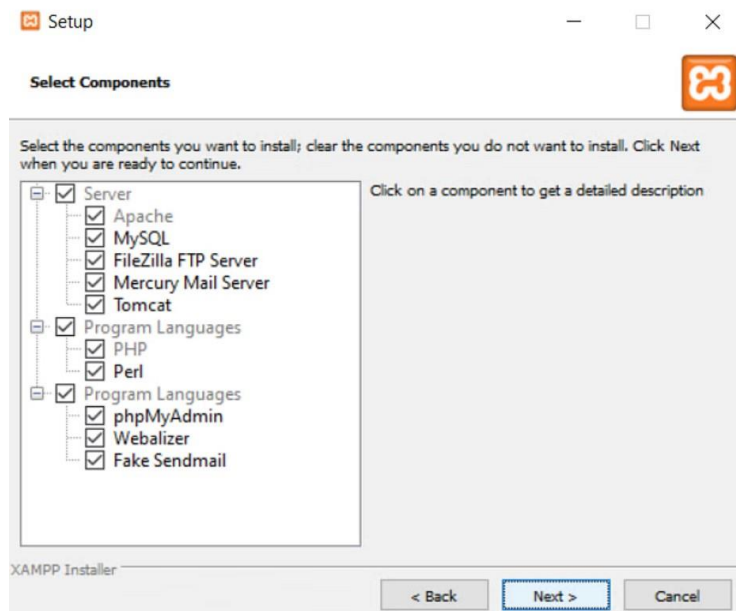
**Aim:** To develop a website and host it on i) local machine or virtual machine  
ii) Amazon S3 Bucket

### **Static Hosting:**

1) On local server (XAMPP)

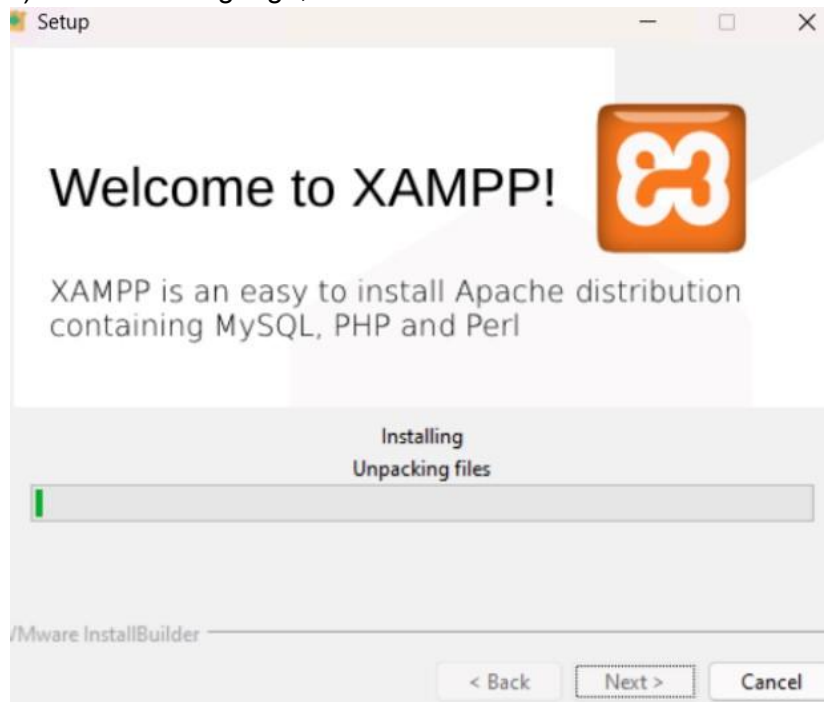
**Step 1:** Install XAMPP from <https://www.apachefriends.org/> .

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

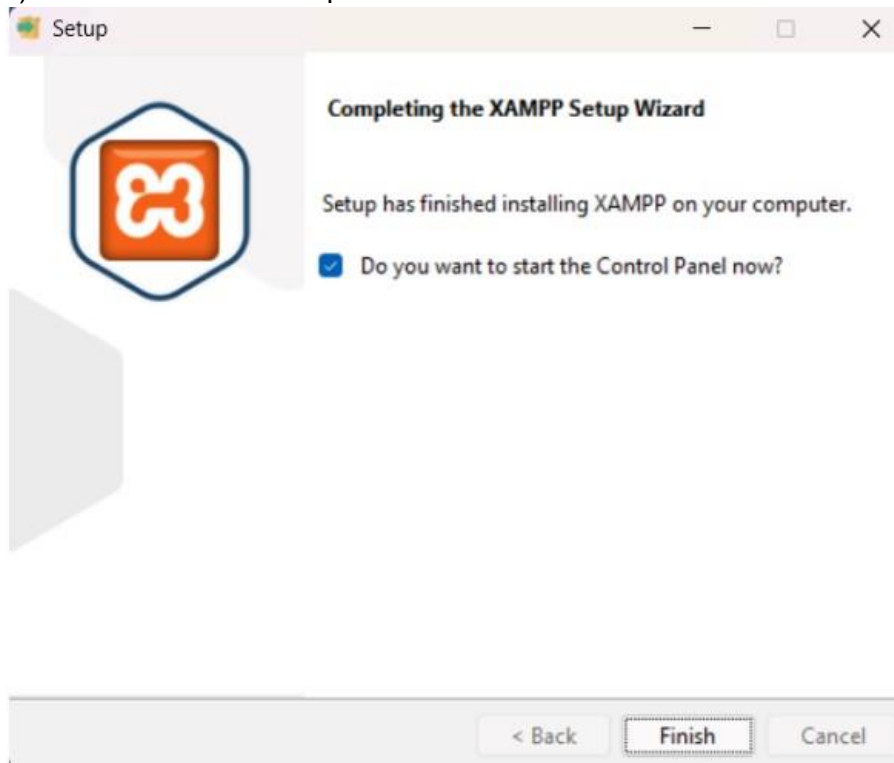




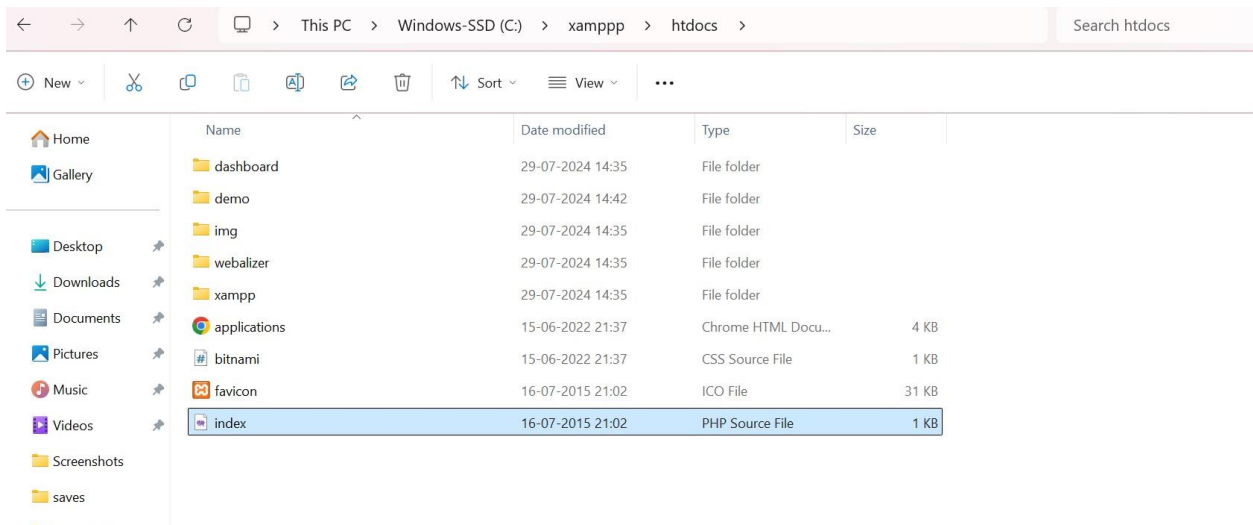
- 2) Open the setup file. Select all the required components and click next.
- 3) Select the language, click next. XAMPP starts to install.



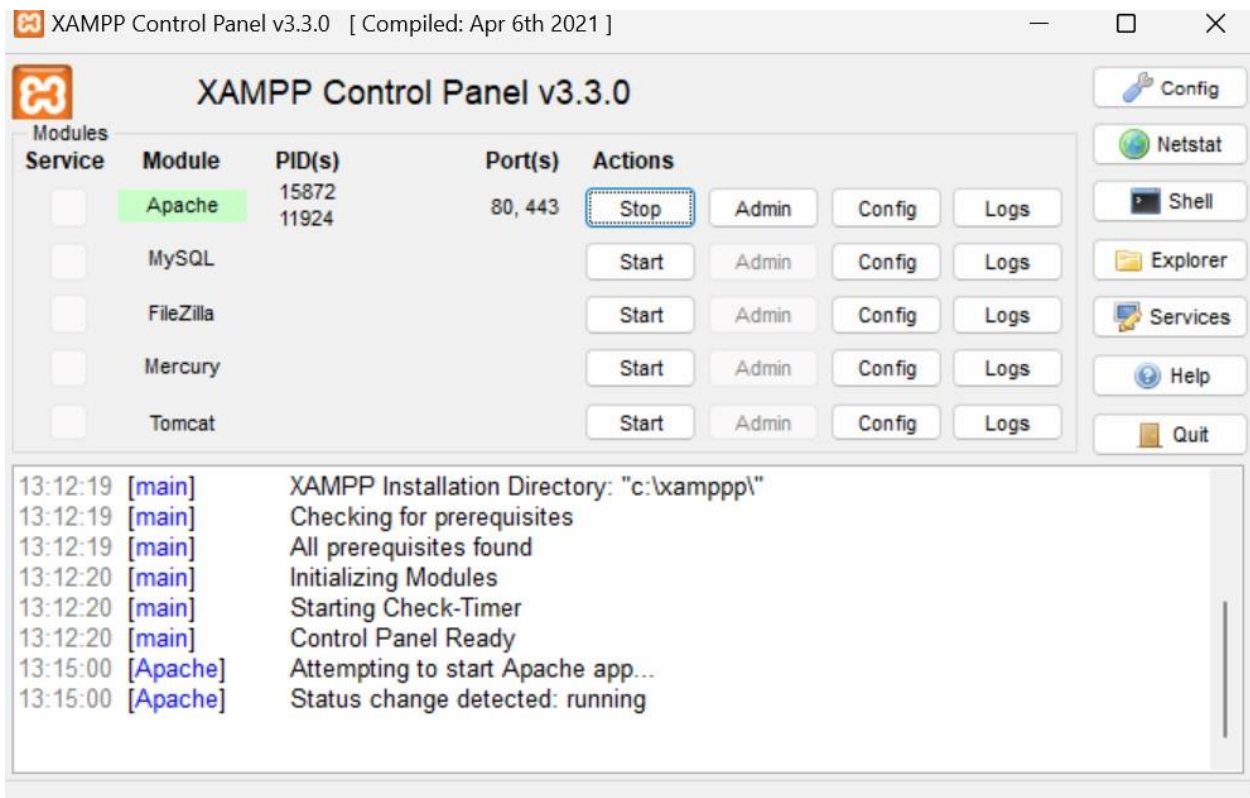
4) The installation is complete. Click Finish.



**Step 2:** Go to the directory where XAMPP was installed. Go to htdocs folder. Place your folder in this directory.



**Step 3:** Open XAMPP Control Panel, start the Apache service (Required) and mySQL service (if needed)

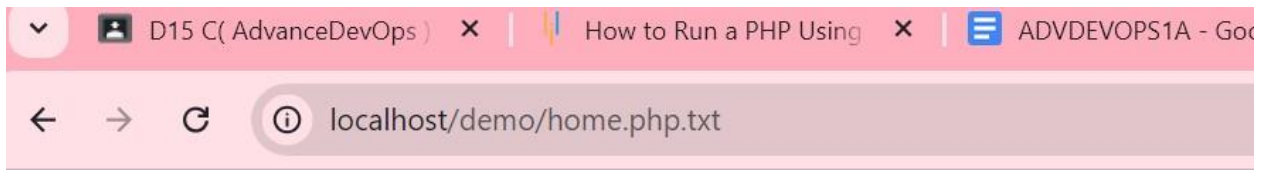


**Step 4:** Write a php file for your website.

```
File Edit View

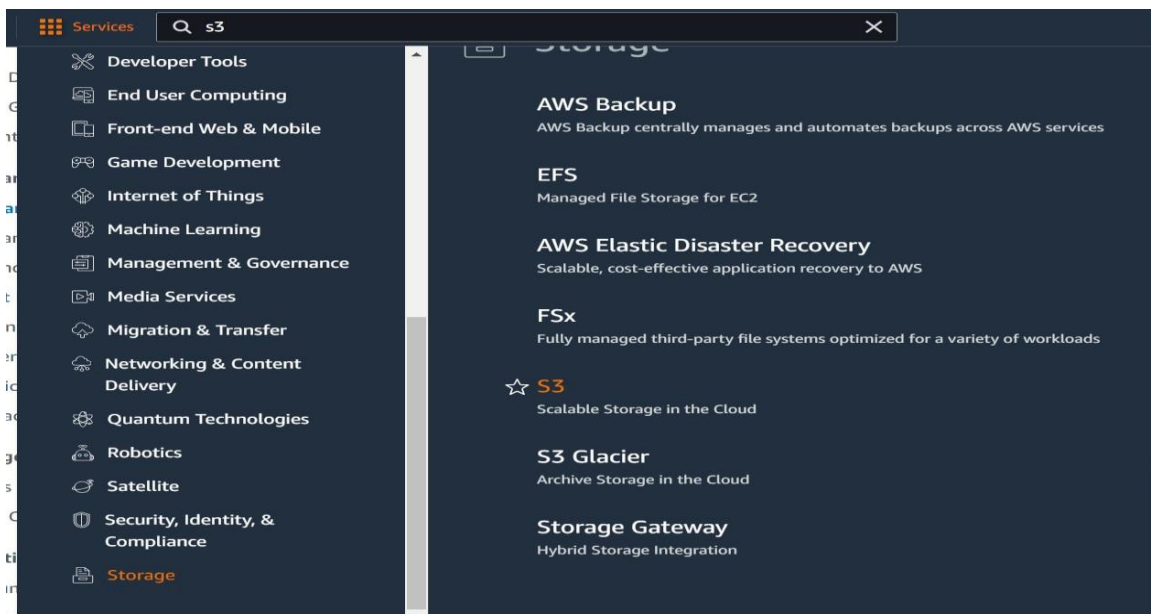
<?php
    echo "Welcome to Advance DevOps"
?>
```

**Step 5:** Open your web browser. Type localhost/YOUR\_FILENAME.php. This will open your website on your browser



## 2) AWS S3

**Step 1:** Login to your AWS account. Go to services and open S3.



**Step 2:** Click on Create Bucket. Give a name to your bucket, keeping other options default, scroll down and click on Create Bucket.

[Amazon S3](#) > [Buckets](#) > Create bucket

## Create bucket [Info](#)

Buckets are containers for data stored in S3.

### General configuration

AWS Region  
Asia Pacific (Sydney) ap-southeast-2

Bucket name [Info](#)

boomweb

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.

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.

### 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

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

Cancel

Create bucket

### Step 3: Go to the Objects tab and click on upload file.

The screenshot shows the Amazon S3 console interface. At the top, there's a navigation bar with 'Services', a search bar, and user information. Below the navigation bar, the breadcrumb trail reads 'Amazon S3 > Buckets > boomweb'. The main heading is 'boomweb' with an 'Info' link. A horizontal menu contains 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' tab is selected, showing 'Objects (0)' with an 'Info' link. A toolbar includes icons for refresh, copy S3 URI, copy URL, download, open, delete, an actions dropdown, 'Create folder', and a prominent orange 'Upload' button. A text block explains that objects are fundamental entities in Amazon S3 and provides a link to 'Amazon S3 inventory'. Below this is a search bar 'Find objects by prefix' and a pagination control showing '< 1 >'. A table header lists columns: Name, Type, Last modified, Size, and Storage class. The table content area displays 'No objects' and a message 'You don't have any objects in this bucket.' with an 'Upload' button.

The screenshot shows the 'Upload' page in the Amazon S3 console. The breadcrumb trail is 'Amazon S3 > Buckets > boomweb > Upload'. The main heading is 'Upload' with an 'Info' link. A text block instructs users to add files and folders for upload, mentioning the AWS CLI, AWS SDK, and Amazon S3 REST API, with a 'Learn more' link. Below this is a dashed border box containing the text 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' Underneath, a section titled 'Files and folders (0)' includes 'Remove', 'Add files', and 'Add folder' buttons. A note states 'All files and folders in this table will be uploaded.' There is a search bar 'Find by name' and a pagination control '< 1 >'. A table header lists columns: Name, Folder, and Type. The table content area displays 'No files or folders' and a message 'You have not chosen any files or folders to upload.' at the bottom.

## Step

4: Click on Add files. Add all the files you want to upload. Then scroll down and click on Upload.

The screenshot shows the AWS S3 console interface. The top section, titled 'Files and folders (2 Total, 266.0 B)', contains a search bar with the placeholder 'Find by name', a pagination control showing '1', and three buttons: 'Remove', 'Add files', and 'Add folder'. Below this is a table with the following data:

<input type="checkbox"/>	Name	Folder	Type
<input type="checkbox"/>	static.html.txt	staticweb/	text/plain
<input type="checkbox"/>	static.html.txt	-	text/plain

Below the table is a horizontal scrollbar. The bottom section of the console shows the 'Destination' details for the upload. It includes a 'Destination' field with the value 's3://boomweb', a 'Destination details' section with the text 'Bucket settings that impact new objects stored in the specified destination.', a 'Permissions' section with the text 'Grant public access and access to other AWS accounts.', and a 'Properties' section with the text 'Specify storage class, encryption settings, tags, and more.'. At the bottom right are 'Cancel' and 'Upload' buttons.

Step 5: This will take you to the Objects screen. Switch to Properties and scroll down to Static Website Hosting. There you would find the link (Bucket website endpoint) to your website.



## Step

Amazon S3 > Buckets > boomweb

### boomweb Info

Objects | **Properties** | Permissions | Metrics | Management | Access Points

#### Bucket overview

AWS Region Asia Pacific (Sydney) ap-southeast-2	Amazon Resource Name (ARN) arn:aws:s3::boomweb	Creation date August 11, 2024, 22:53:06 (UTC+05:30)
--	---	--

#### Bucket Versioning Edit

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](#)

Bucket Versioning  
Disabled  
Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the

**6:** Scroll down till you find Static website hosting, click on edit.

#### Static website hosting Edit

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

Static website hosting  
Disabled

**Step 7:** Enable static website hosting, in Index document, write the name of your document. Save your changes.

### 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.

## Step

### Edit static website hosting [Info](#)

#### Static website hosting

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

#### Static website hosting

- ☐ Disable
- ☒ Enable

#### 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](#)

**i** 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.

static.html

**Step 8:** Uncheck the Block all public access checkbox and click on save changes.

**9:** Scroll down to bucket policy and click edit.

The screenshot shows the 'Edit bucket policy' page in the Amazon S3 console. The breadcrumb navigation at the top reads: Amazon S3 > Buckets > statichosting27 > Edit bucket policy. The page title is 'Edit bucket policy' with an 'Info' link. Below the title, there are links for 'Policy examples' and 'Policy generator'. A descriptive text states: '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](#)'. The 'Bucket ARN' is displayed as 'arn:aws:s3:::statichosting27'. The 'Policy' section shows a JSON policy document with line numbers 1 through 14. The policy grants 'PublicReadGetObject' permission to 'arn:aws:s3:::statichosting27/\*'. On the right side, there is a panel with 'Edit statement' (PublicReadGetObject), 'Add actions' (Choose a service, Filter services), and a list of 'Included' services (S3) and 'Available' services (AMP, API Gateway, API Gateway V2). The footer includes 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc. or its affiliates, along with links for Privacy, Terms, and Cookie preference.