

## EXPERIMENT 1A

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

### Static Hosting:

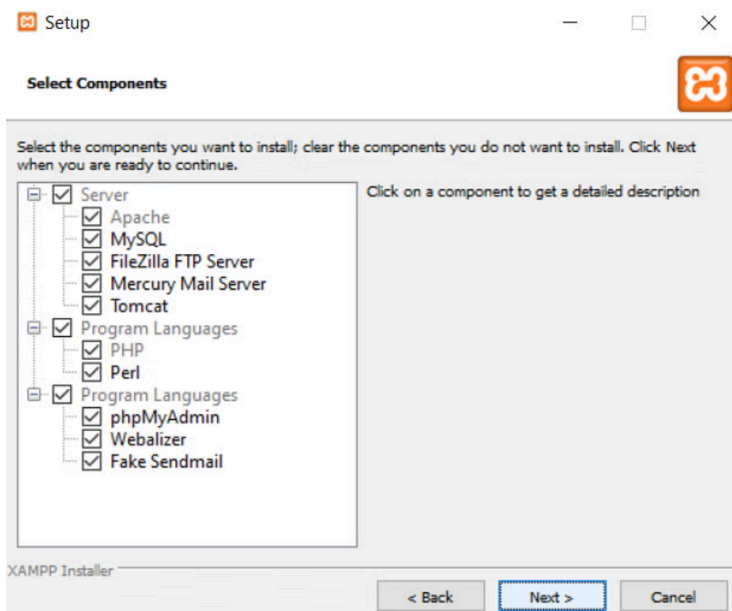
1) On local server (XAMPP)

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

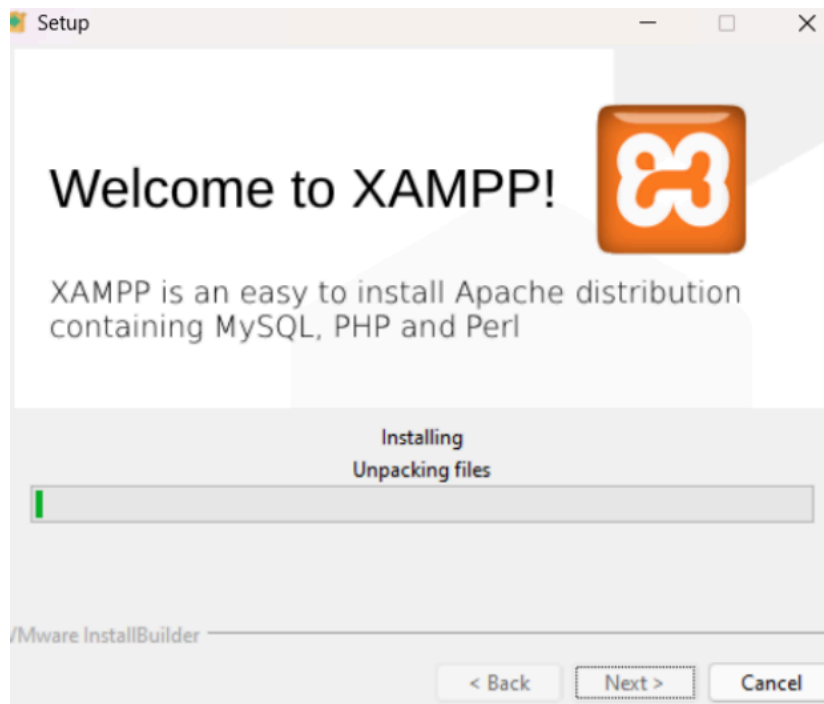
1) Select your OS. It will automatically start downloading.



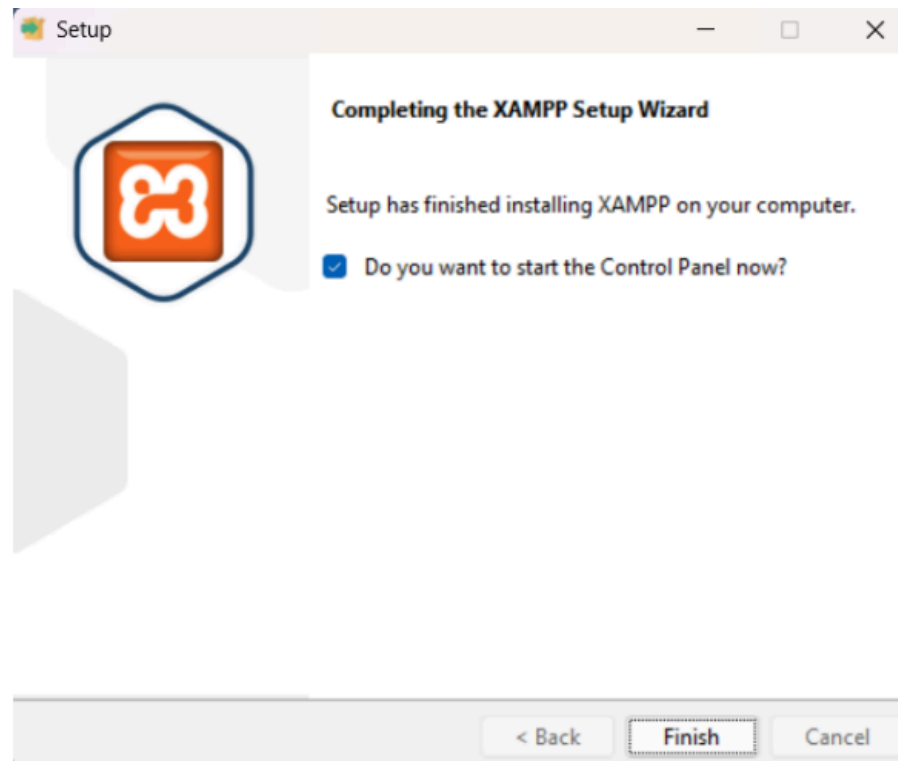
2) Open the setup file. Select all the required components and click next.



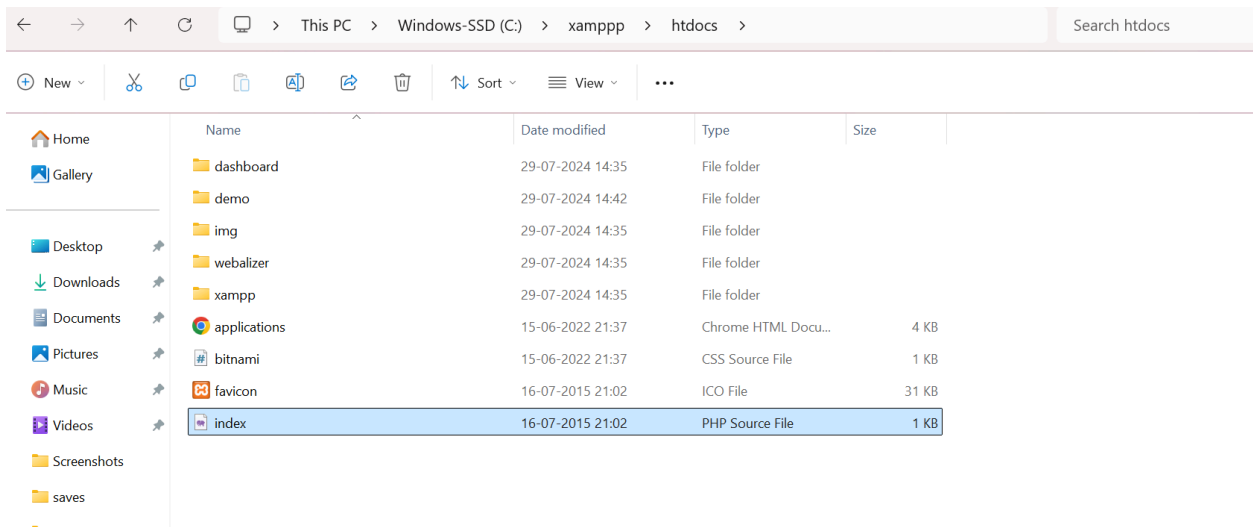
3) Select the language, click next. XAMPP starts to install.



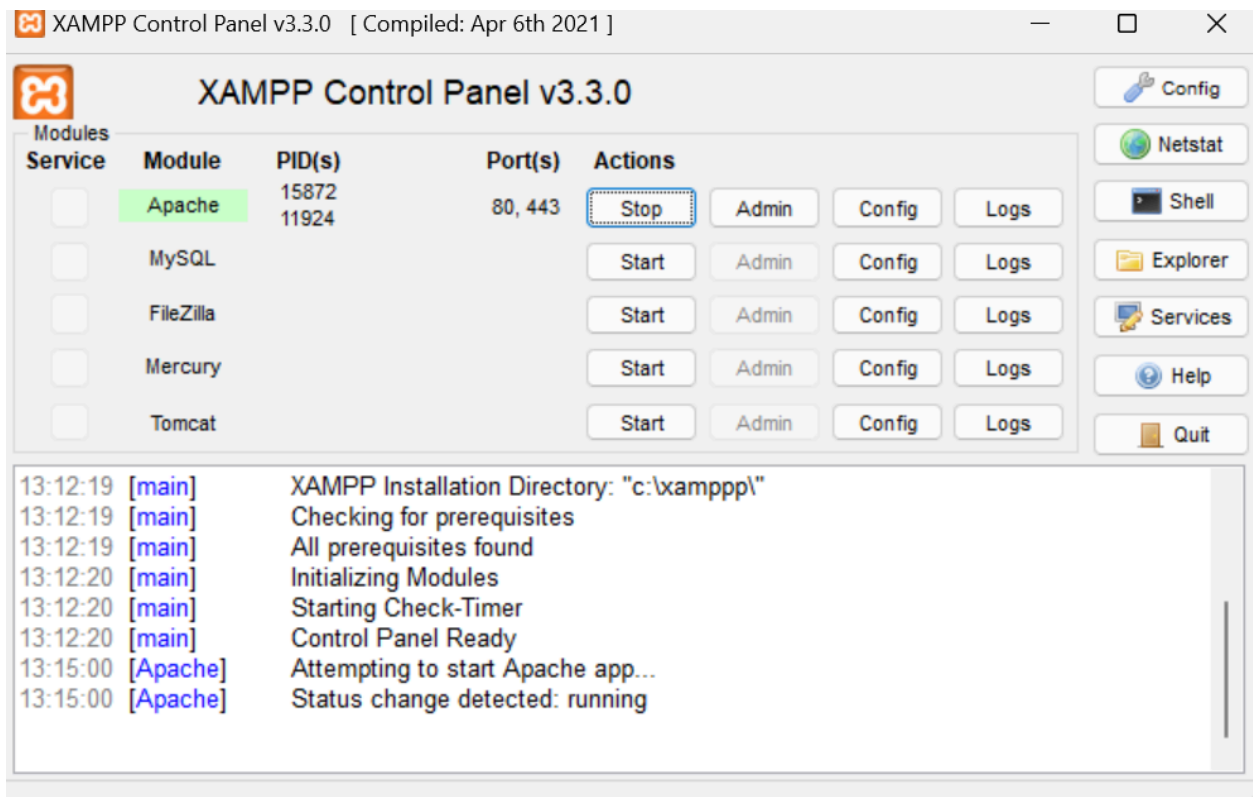
4) The installation is complete. Click Finish.



**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)

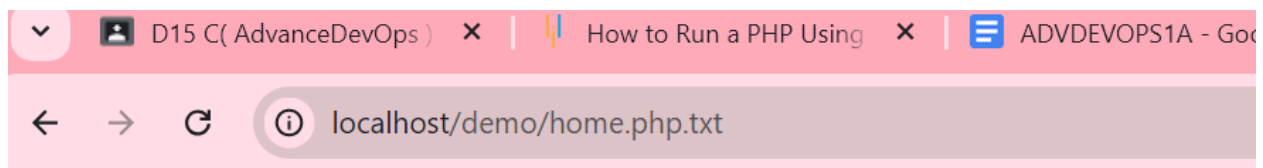


**Step 4:** Write a php file for your website.

```
File Edit View

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

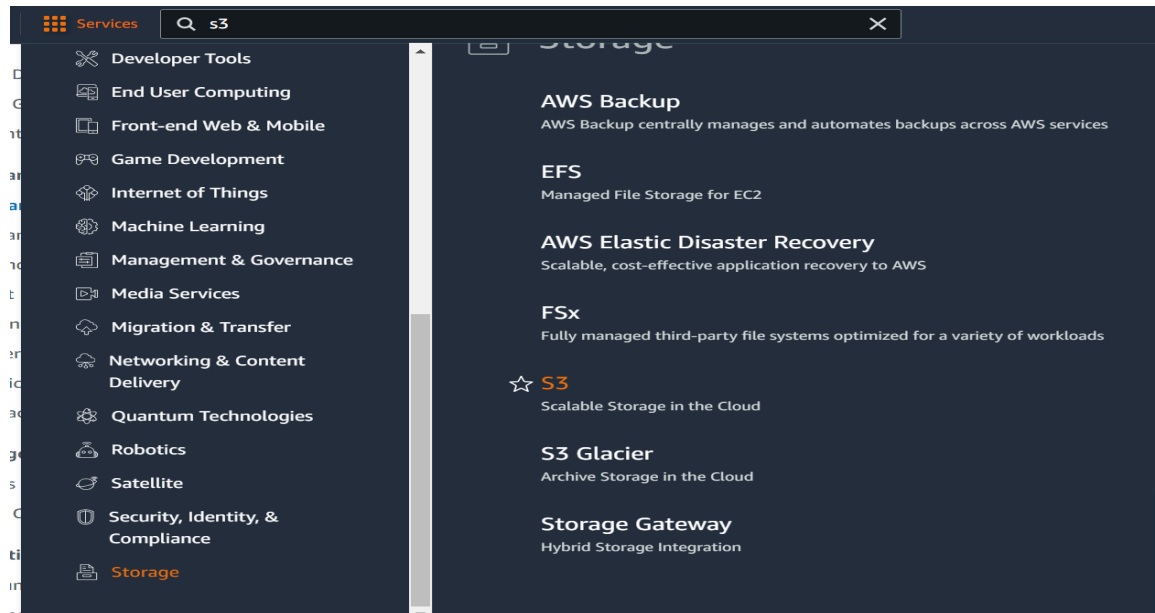
**Step 5:** Open your web browser. Type localhost/YOUR\_FILENAME.php. This will open your website on your browser



Welcome to Advance DevOps

## 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](#)

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.

**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

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

Services  [Alt+S]

Amazon S3 > Buckets > boomweb

**boomweb** [Info](#)

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (0) [Info](#)

🔄

📄 Copy S3 URI

📄 Copy URL

📄 Download

🔗 Open [↗](#)

Delete

Actions ▼

Create folder

📁 Upload

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) [↗](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#) [↗](#)

< 1 > ⚙️

Name

Type

Last modified

Size

Storage class

No objects  
You don't have any objects in this bucket.

📁 Upload

Amazon S3 > Buckets > boomweb > 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 (0)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

< 1 >

Name

Folder

Type

No files or folders  
You have not chosen any files or folders to upload.

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

Files and folders (2 Total, 266.0 B)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

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

Destination [Info](#)

Destination

s3://boomweb

► Destination details

Bucket settings that impact new objects stored in the specified destination.

► Permissions

Grant public access and access to other AWS accounts.

► Properties

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

Cancel

Upload

**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.

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

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

<b>Static website hosting</b>	<a href="#">Edit</a>
Use this bucket to host a website or redirect requests. <a href="#">Learn more</a>	
Static website hosting Disabled	

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

## Edit static website hosting

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

☐ Redirect requests for an object

Use the bucket endpoint as the web address. [Learn more](#)

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.

static.html

**Step 8:** Uncheck the Block all public access checkbox and click on save 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](#)

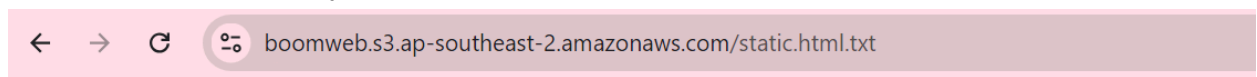
- ☒ **Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
- ☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access 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 9:** Scroll down to bucket policy and click edit.

The screenshot shows the AWS IAM console interface for editing a bucket policy. The breadcrumb navigation at the top reads: [Amazon S3](#) > [Buckets](#) > [statichosting27](#) > [Edit bucket policy](#). The main heading is 'Edit bucket policy' with an 'Info' link. Below this, there's a section for 'Bucket policy' with a description and a 'Learn more' link. 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 allows 'PublicReadGetObject' for the principal '\*' on the resource 'arn:aws:s3:::statichosting27/\*'. To the right of the JSON editor, there are controls for 'Edit statement' (PublicReadGetObject) and 'Remove'. Below these are 'Add actions' and 'Choose a service' (with a search bar and 'Filter services' text). A list of 'Included' services shows 'S3'. A list of 'Available' services includes 'AMP', 'API Gateway', and 'API Gateway V2'. The footer of the console shows 'CloudShell', 'Feedback', and copyright information for 2024.

**Step 10:** You can access your website now.



My First Lab

My name is Bhumisha.

Class: D15C

Roll No: 38