

ASSIGNMENT 5

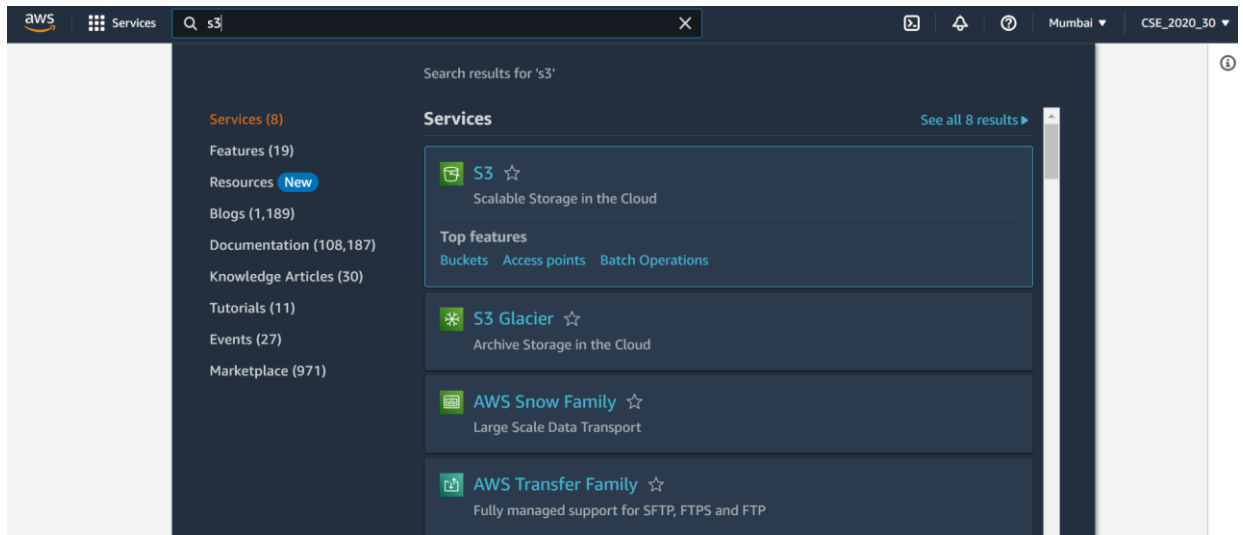
Problem Statement: Create a public bucket in AWS. Upload a file and give the necessary permission to check the file URL is working or not.

Procedure:

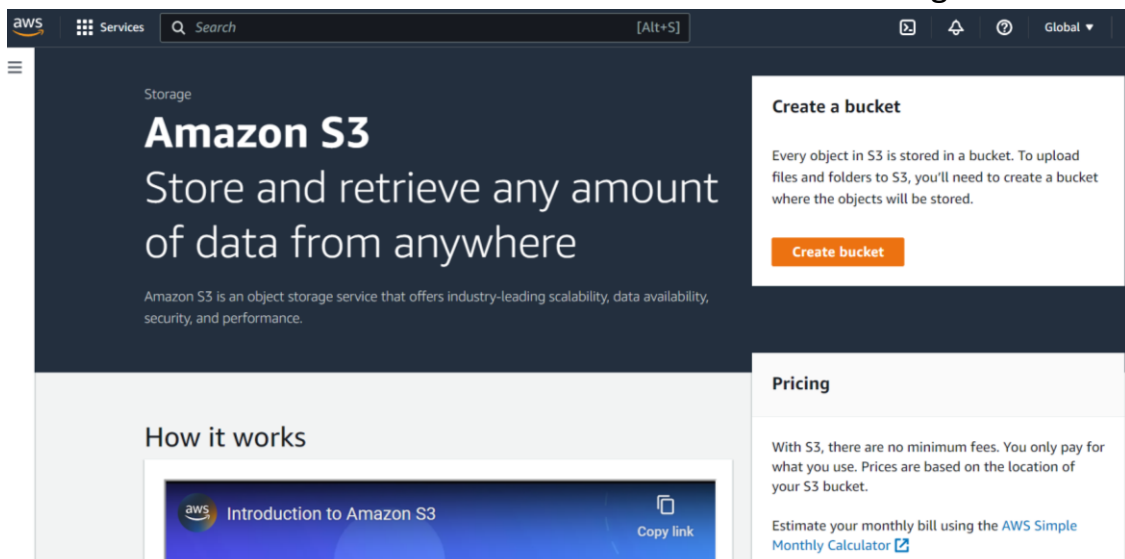
1. Sign in to your **AWS account** as root user.



2. Now in the **homepage** search for **S3** in the **search box** and then select the first option displayed.



3. After clicking on it, you will be redirected to the **Amazon S3** homepage. There we have to click on the **create bucket** button on the right-hand side.



4. Next you will go to the **Create bucket screen** where you have to configure your bucket before creating it.
 - a. Choose a globally unique name for your bucket. It should NOT contain any spaces or any uppercase letters.
 - b. Select the **AWS Region as Asia Pacific (Mumbai) ap-south-1**. **Remember** you can avail other options but each server region has **different pricing** associated with it. Since, we are **living in India**, we are choosing the one **closest to us** to remain fairly priced.
 - c. Next, we go to Object Ownership section where we keep ACLs enabled option checked. We also keep “Bucket owner preferred” option checked in the object ownership choice
 - d. Next, we UNCHECK the Block all public access option.
 - e. Remember to check the “I acknowledge that the current settings might result in this bucket and the objects within becoming public” option just below.
 - f. Everything else remains unchanged.
 - g. Now click on the Create bucket button.

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

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

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.

☐ ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☒ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

☒ Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

☐ Object writer
The object writer remains the object owner.

[Info](#) If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)

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**

 **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.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Default encryption [Info](#)
Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption key type [Info](#)

☒ Amazon S3-managed keys (SSE-S3)


☐ AWS Key Management Service key (SSE-KMS)

Bucket Key
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS 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](#)





- After that we are redirected to the buckets page where we can see all our buckets in a table format.

✔ **Successfully created bucket "s3debruppublic1"** [View details](#)

To upload files and folders, or to configure additional bucket settings choose [View details](#).

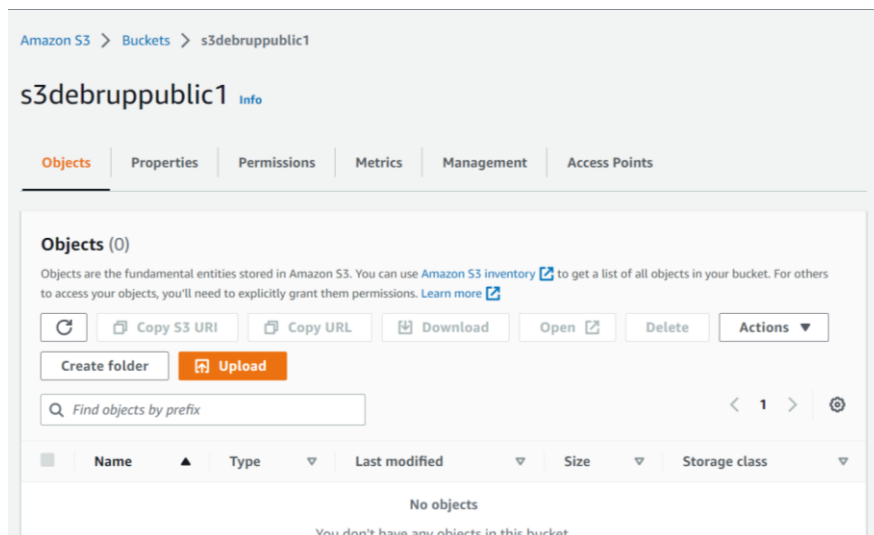
► **Account snapshot** [View Storage Lens dashboard](#)
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

Buckets (2) [Info](#)
Buckets are containers for data stored in S3. [Learn more](#)

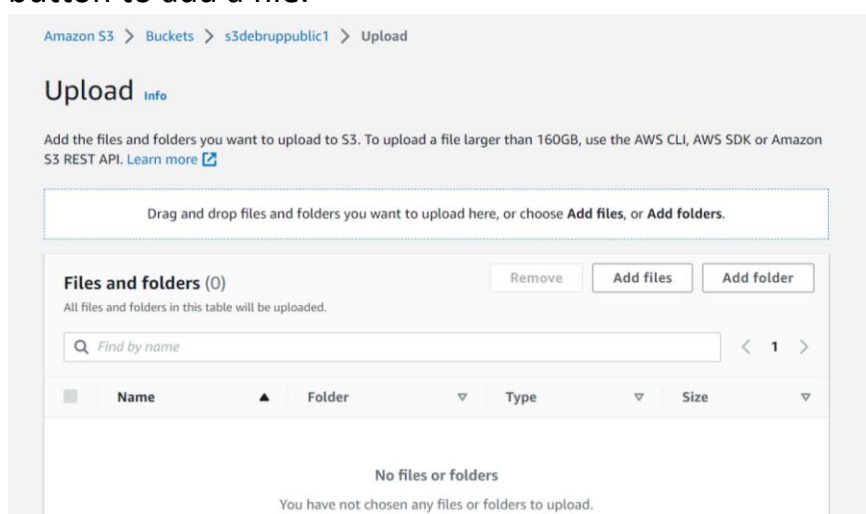
  Copy ARN  Empty  Delete [Create bucket](#)

	Name	AWS Region	Access	Creation date
<input type="radio"/>	s3debrupprivate1	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 24, 2023, 20:36:52 (UTC+05:30)
<input type="radio"/>	s3debruppublic1	Asia Pacific (Mumbai) ap-south-1	Objects can be public	February 25, 2023, 00:04:32 (UTC+05:30)

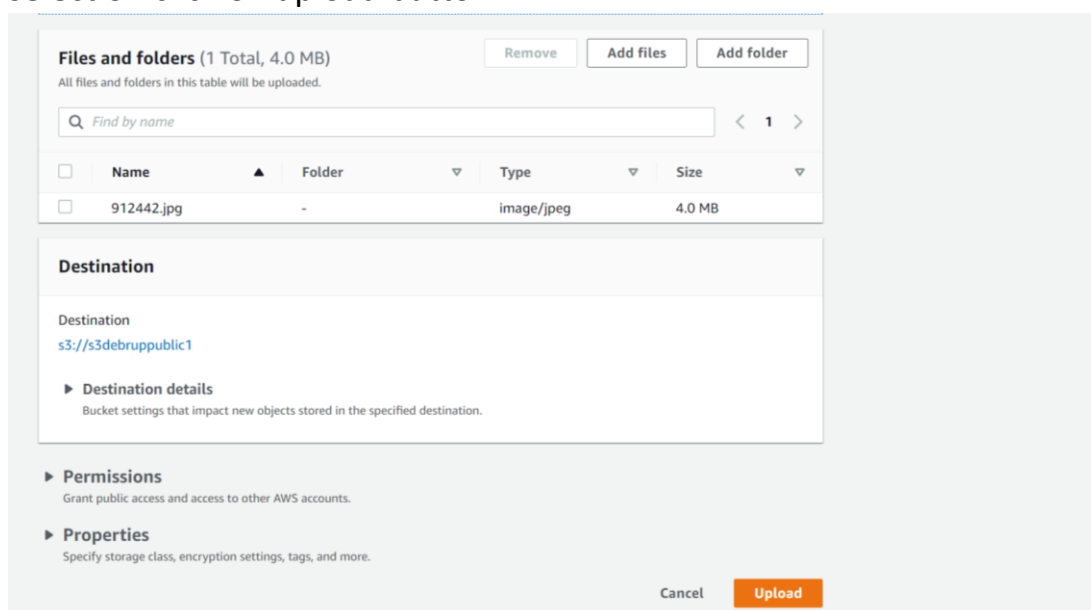
- Now we click on our newly selected bucket (on the name).
- Now we have successfully entered into our newly created bucket.
- Click the Upload button to upload a file in our bucket.



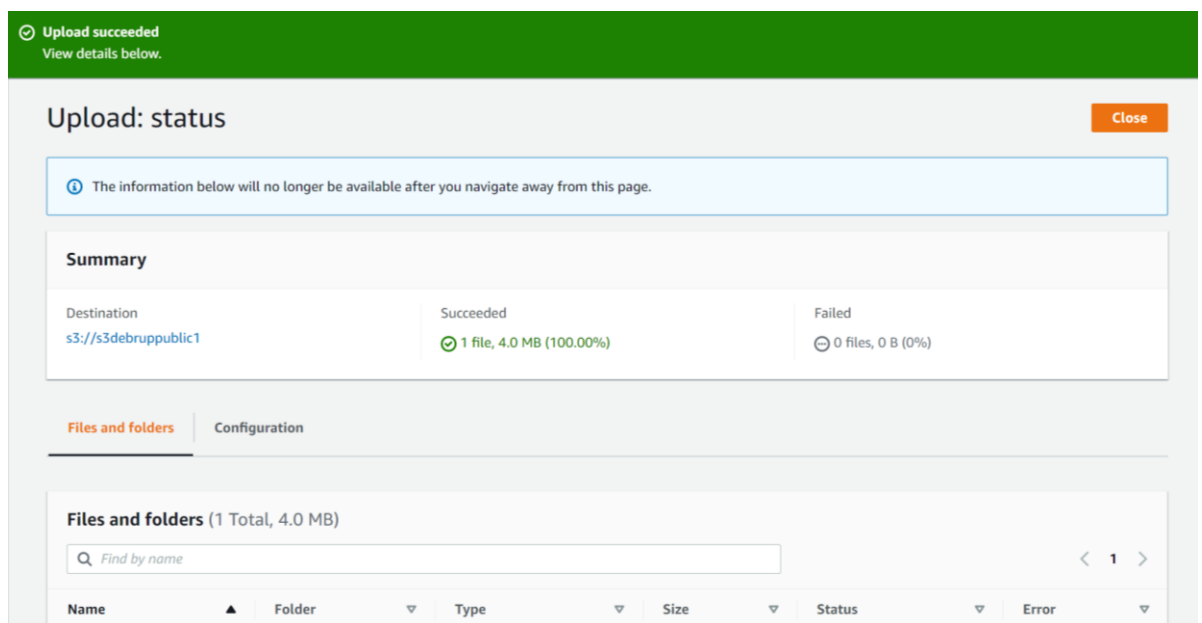
- After clicking you will be redirected to the Upload page. Click on Add files button to add a file.



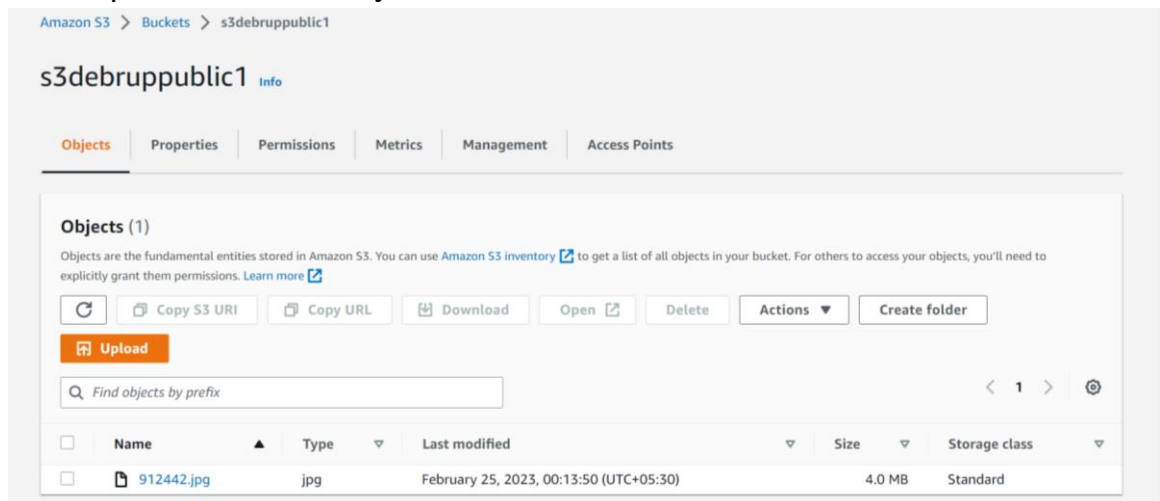
- You will be shown a box to browse from your pc to upload a file. After selection click on upload button.



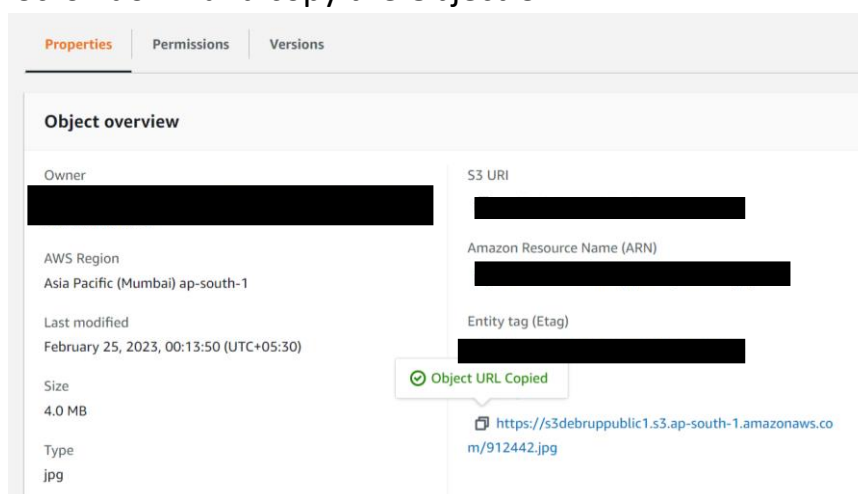
- You will then be redirected to the upload status page where a status bar will be present showing the progress of your upload. After completion it will look like the following.



12. Close your status page. Now in the bucket page you will see the file you have uploaded in the objects section.



13. Now click on the file.
14. Scroll down and copy the Object URL.



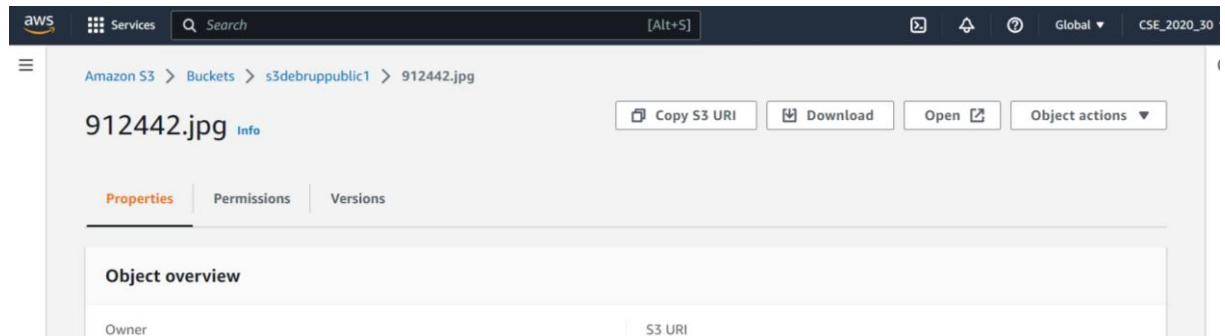
15. Paste it in another browser.
16. IT WILL SHOW ERROR.

This is because your uploaded file, though present in a public bucket, has to be given specific permission so that others can access it. Hence, it cannot

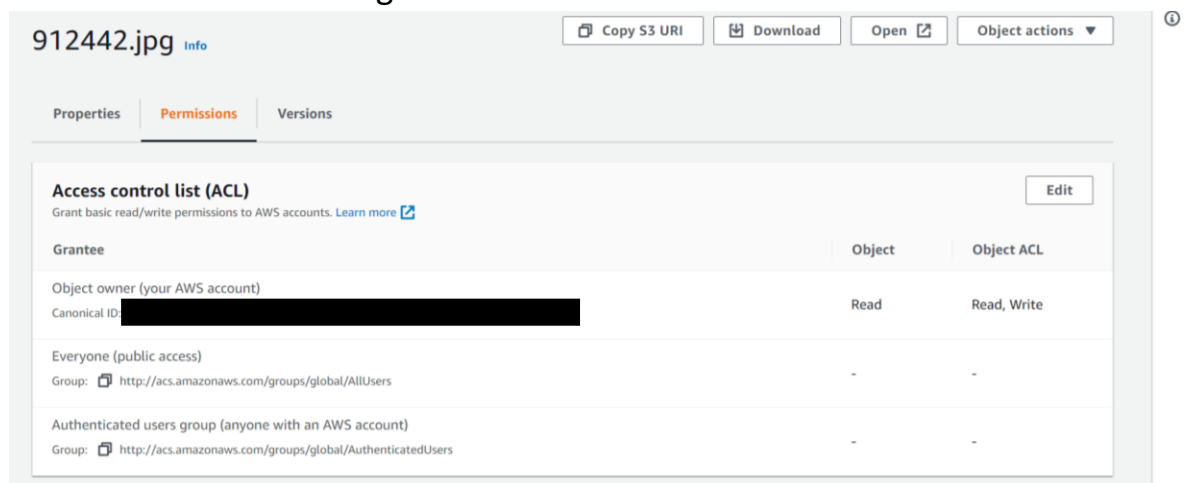
be accessed by anyone other than you. Now, to let others access, you can change the permissions associated with your file using the ACL.

17. NOW WE WILL GIVE PERMISSIONS.....

18. Scroll to the top and Click on the permissions bar on the top below the filename and beside the properties bar (in orange font).

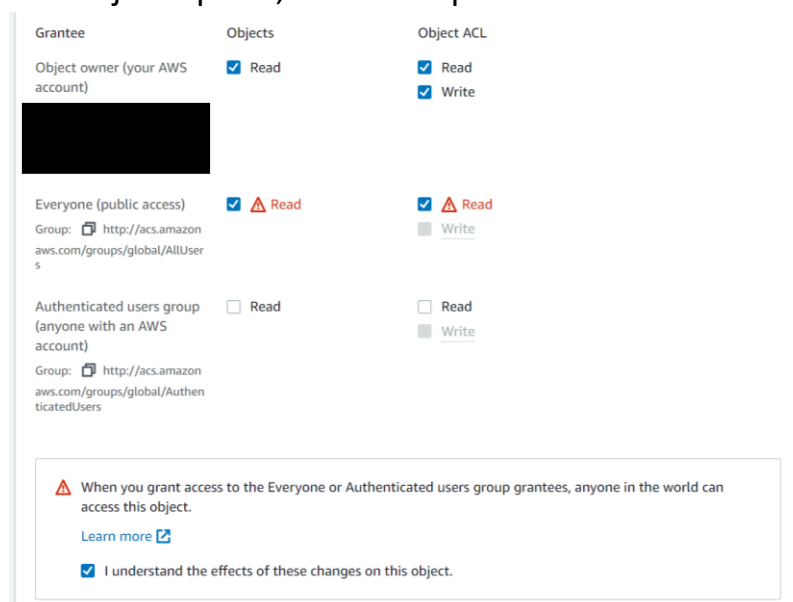


19. You will arrive in the permissions section of your file. You will clearly see the first section as the ACL or Access Control List of your file. Now click on the Edit button on the right hand side of the ACL section.



20. Now select CHECK both “Read”(Object & Object ACL) option for **Everyone(public access)**

Also, remember to check the I understand the effects of these changes on this object option, to further proceed.



21. Now, scroll down and click the save changes button.

⚠ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.

[Learn more](#)


☒ I understand the effects of these changes on this object.

Access for other AWS accounts

No other AWS accounts associated with the resource.

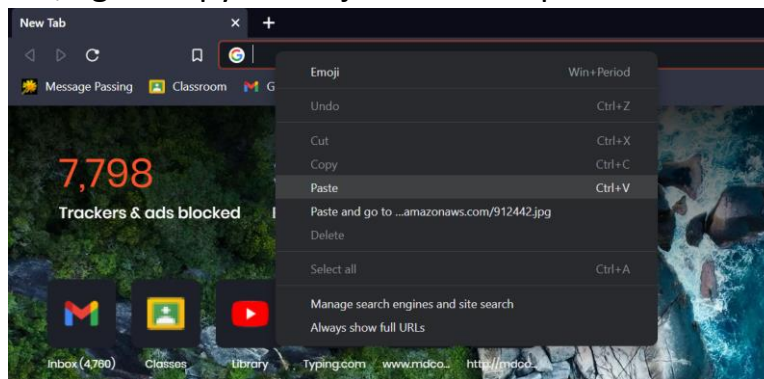
[Add grantee](#)

Specified objects

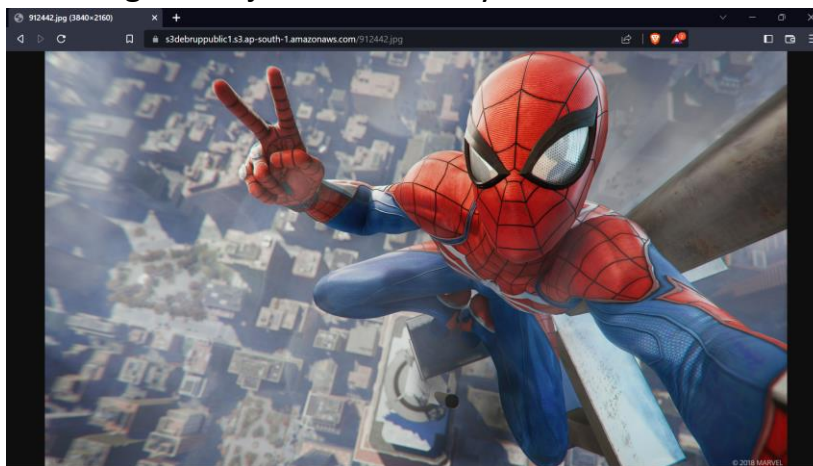
Name	Type	Last modified	Size
 912442.jpg	jpg	February 25, 2023, 00:13:50 (UTC+05:30)	4.0 MB

[Cancel](#) [Save changes](#)

22. Now, again copy the object URL and paste it in a different browser.



23. After pasting the link in the bar, press Enter key. Now we can access our file using the object URL directly.



So, our file is public and can be accessed by those with the object URL(link) anytime anywhere. The URL is working perfectly as intended.