

ASSIGNMENT 4

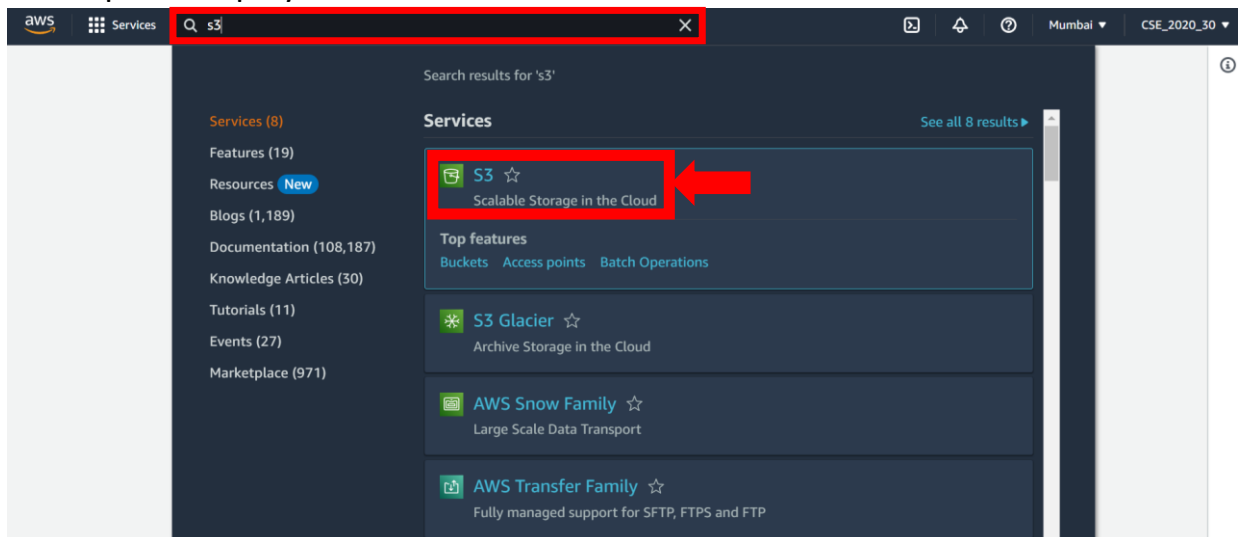
Problem Statement: Create a private bucket in AWS. Upload a file and check that through pre-signed URL whether you can access the file or not.

Procedure:

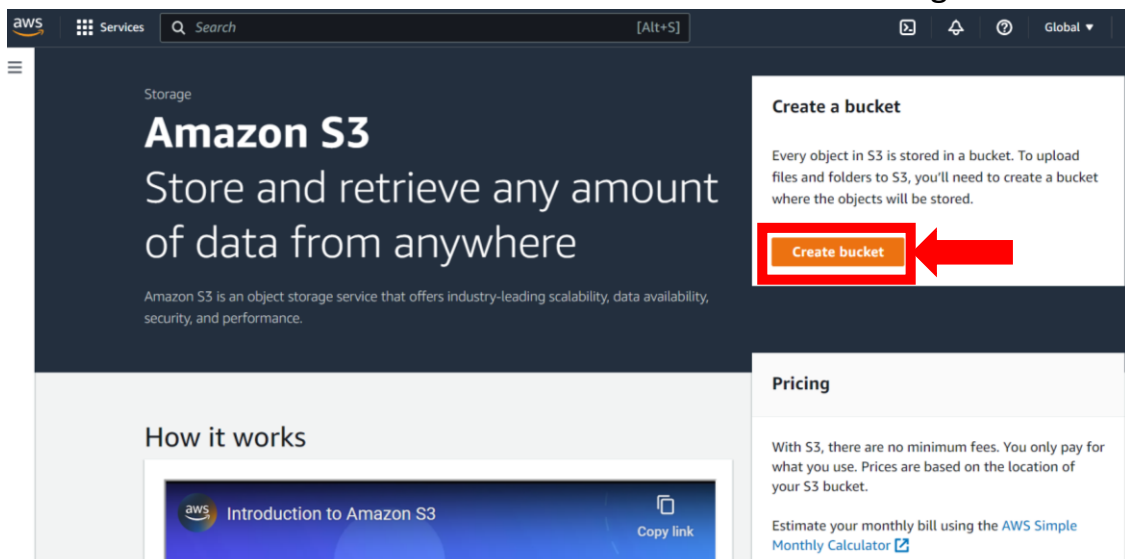
1. Sign in to your **AWS account** as **root user**.



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 disabled option CHECKED (as it is)**.
 - d. Next, we keep **all public access BLOCKED (as it is)**.
 - e. Everything else remains **unchanged**.
 - f. 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
 [See rules for bucket naming](#)

AWS Region
Asia Pacific (Mumbai) ap-south-1

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
[Choose bucket](#)

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 enforced

Upcoming permission changes to disable ACLs
Starting in April 2023, to disable ACLs when creating buckets by using the S3 console, you will no longer need the `s3:PutBucketOwnershipControls` permission. [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**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

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**

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

Amazon S3 > Buckets

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

Buckets (1) [Info](#)
Buckets are containers for data stored in S3. [Learn more](#)

[Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) **Create bucket**

Name	AWS Region	Access	Creation date
s3debrupprivate1	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 24, 2023, 20:36:52 (UTC+05:30)

6. Now we click on our **newly created bucket (on the name)**.
7. Now we have successfully **entered** into our newly created bucket.

Amazon S3 > Buckets > s3debrupprivate1

s3debrupprivate1 [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Objects (0)
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](#)

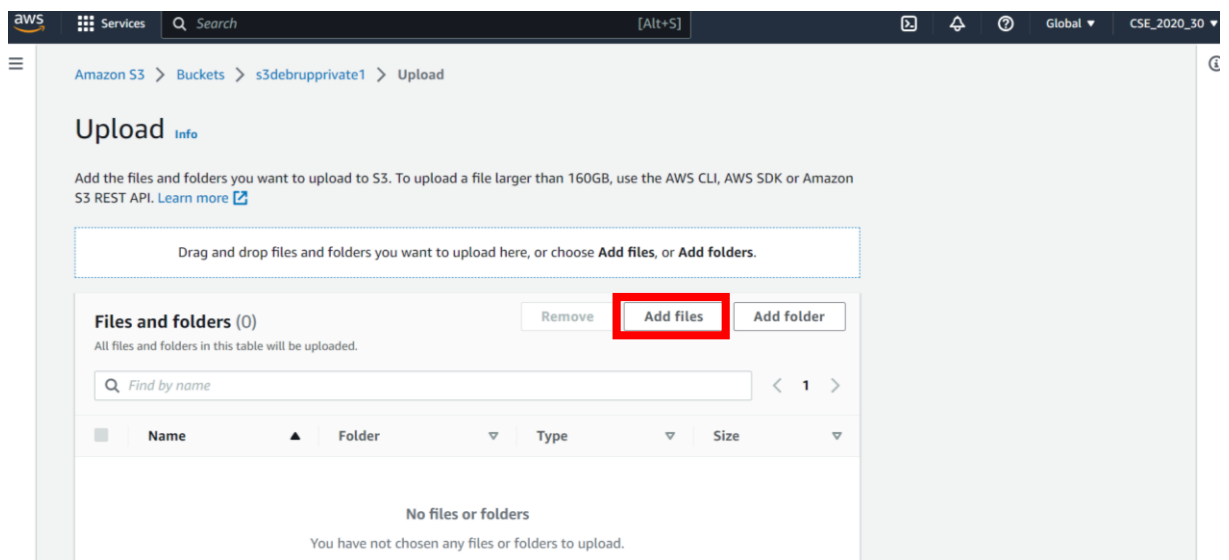
[Refresh](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#)

Upload

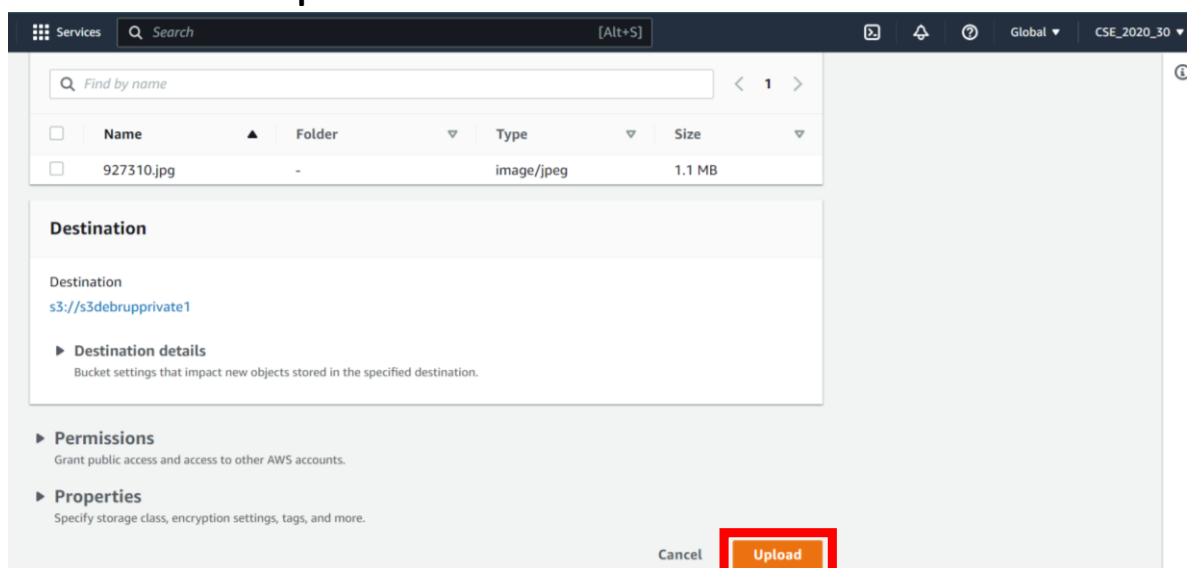
Name	Type	Last modified	Size	Storage class
No objects You don't have any objects in this bucket.				

[Upload](#)

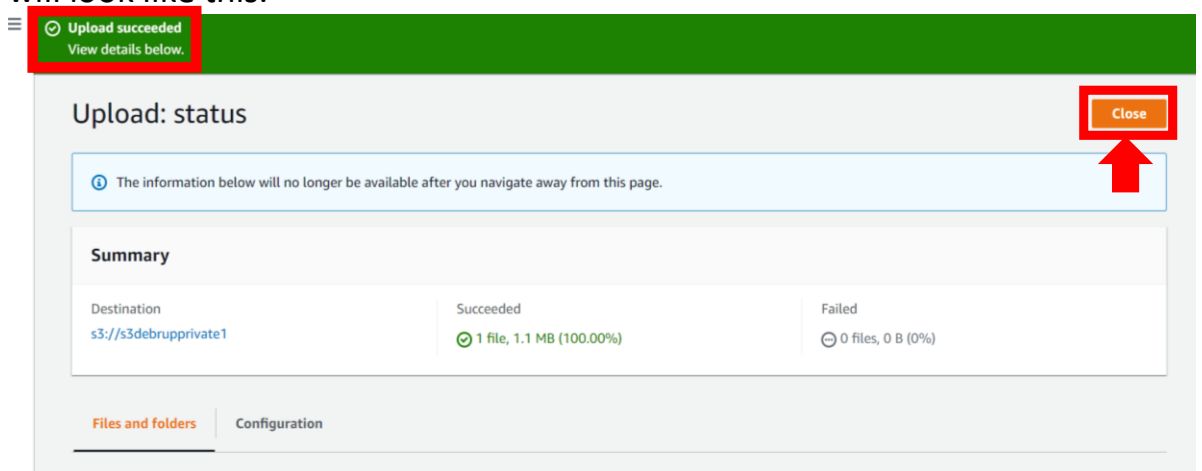
8. **Click the Upload button** to upload a file in our bucket.
9. After clicking you will be redirected to the Upload page. Click on **Add files** button to add a file.



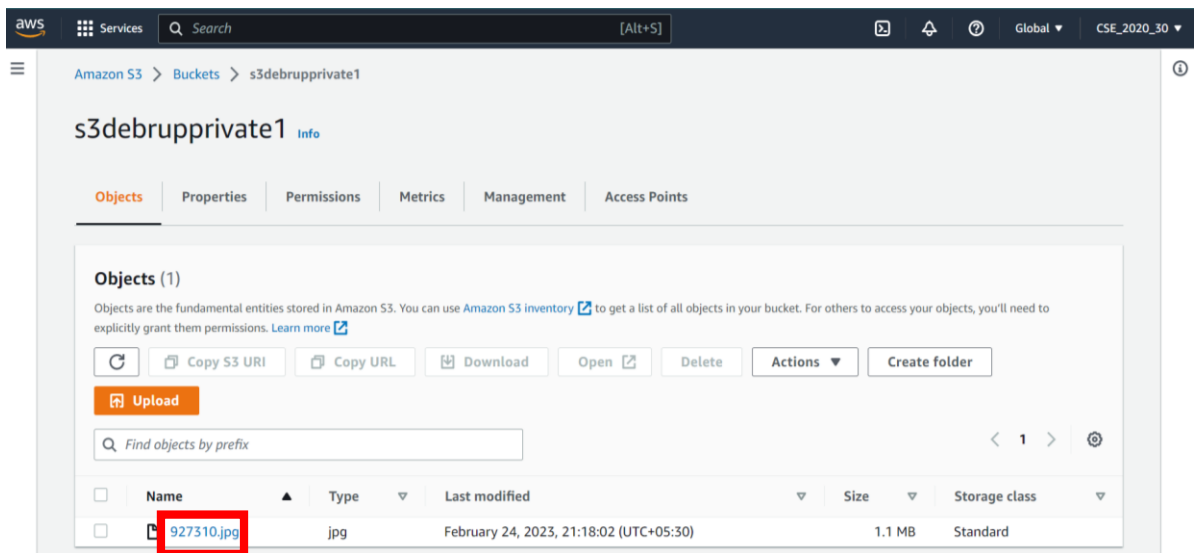
10. You will open a pop up to browse from your pc to upload a file. After selection **click on upload** button.



11. 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 this.

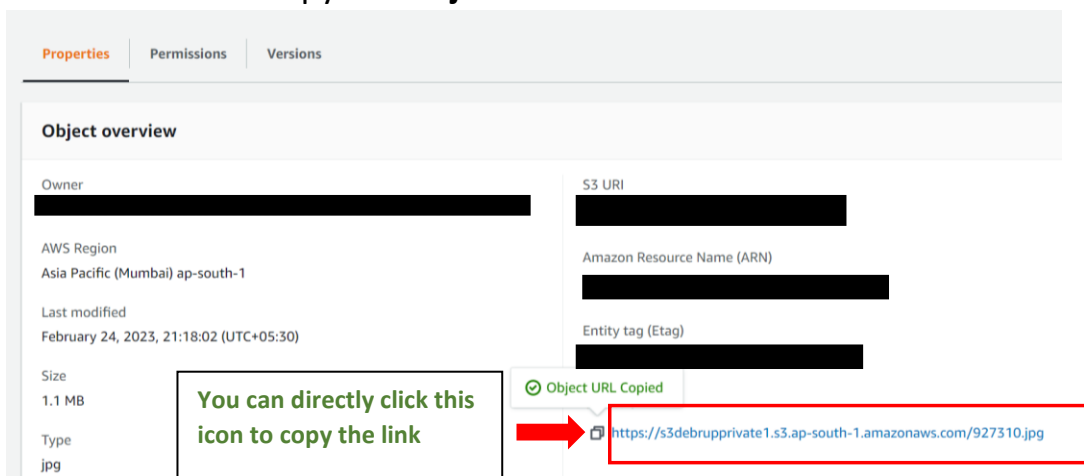


12. **Close** your status page. Now in the bucket page you will see the file you have uploaded in the objects section.



13. Now **Click** on the file.

14. Scroll down and copy the **Object URL**.



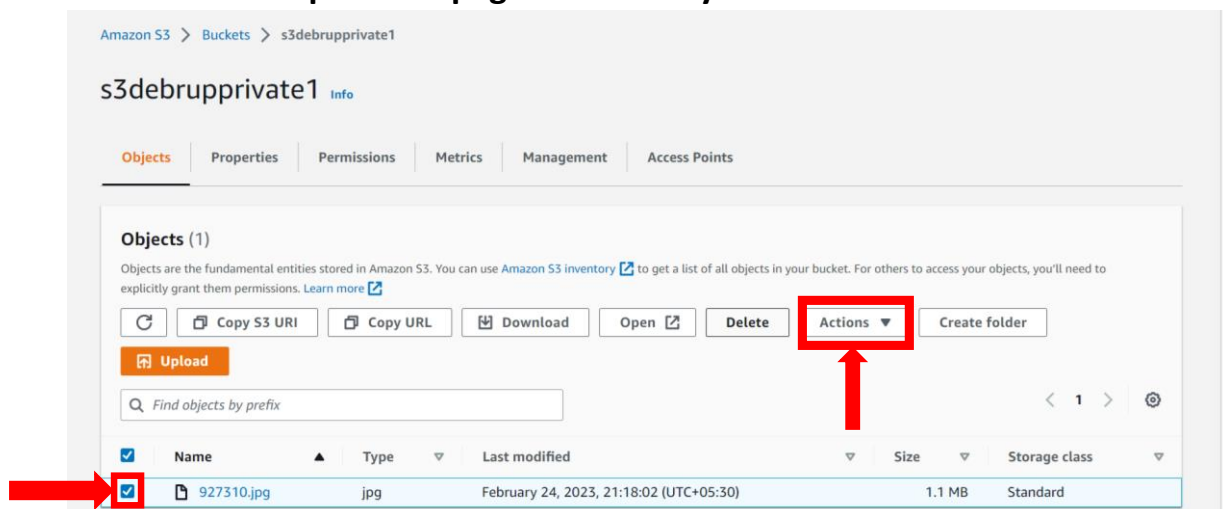
15. **Paste it in another browser.**

16. **IT WILL SHOW ERROR!!!!**

This is because your **uploaded file** is in a **private bucket**. Hence, it **cannot be accessed** by anyone other than you. Now, to let others access, you can only send them a **pre-signed URL** which remains active for a specific duration.

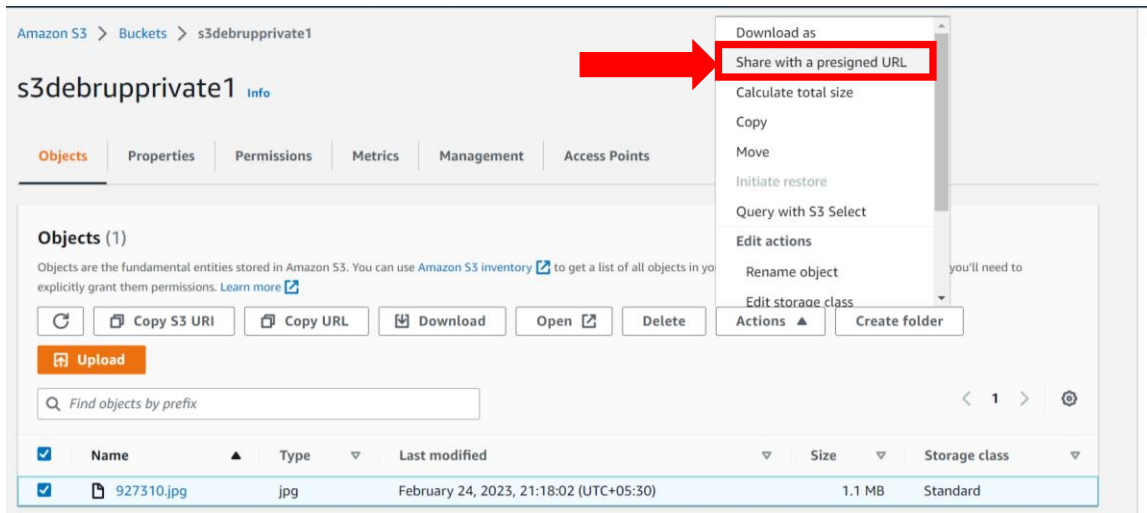
17. **NOW WE WILL GENERATE A PRESIGNED URL**

18. Go back to the **previous page** and **select your file**.



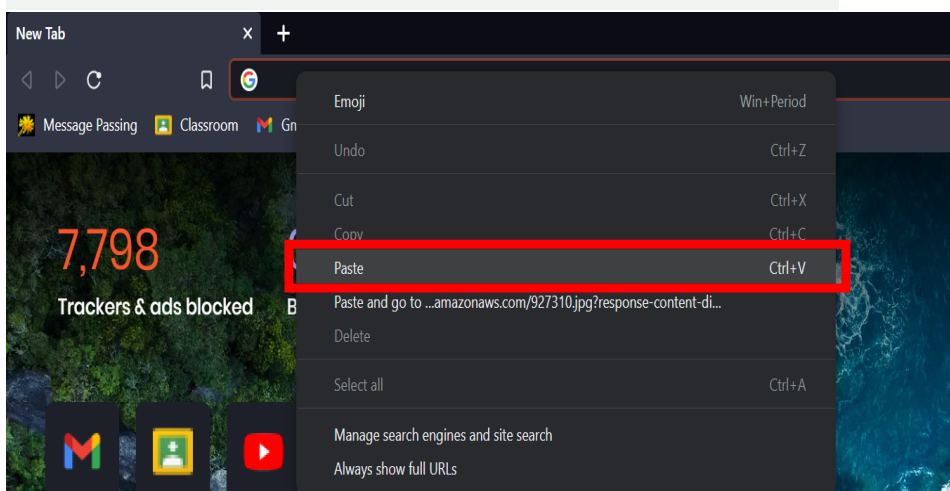
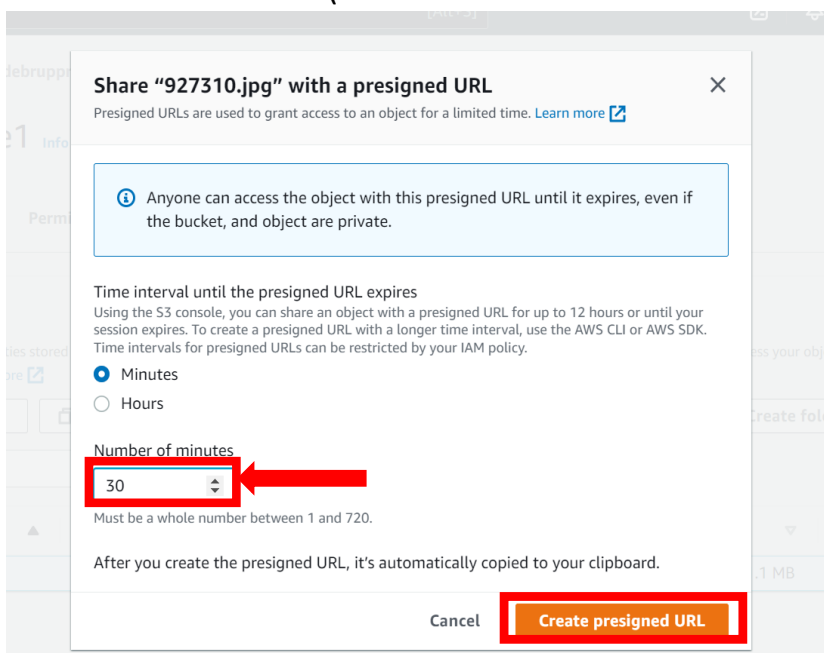
19. Next, **Click** on the **Actions** button as shown above.

20. Select the “Share with presigned URL” option.

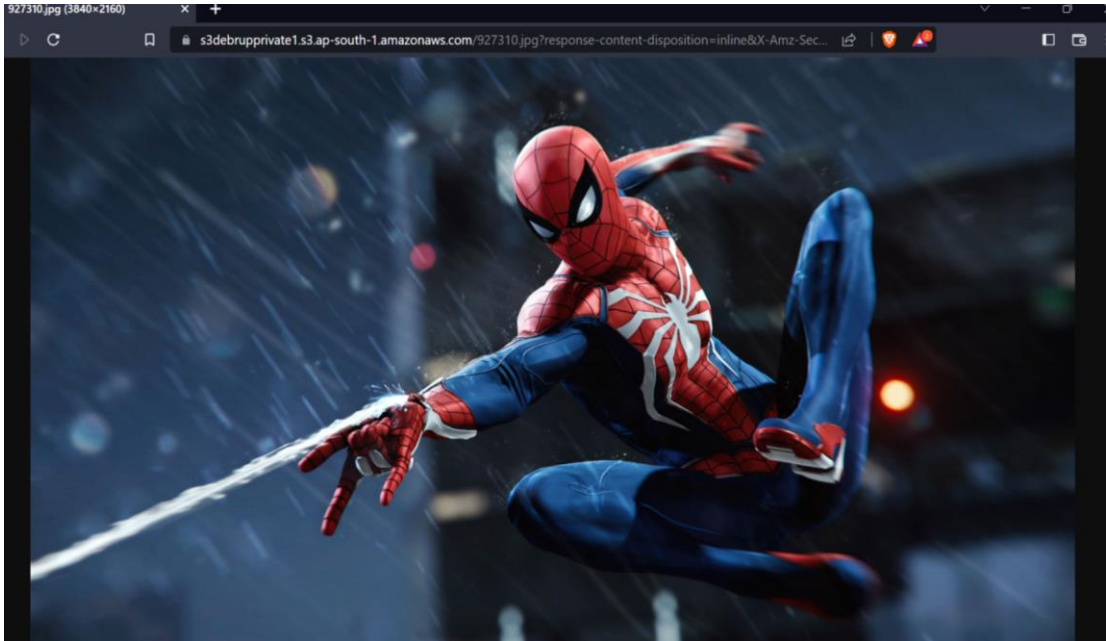


21. Now a pop-up will appear as shown below. You have to specify the duration for which the link remains active. Next click on Create presigned URL.

Note that after creation the URL link automatically gets copied (in your clipboard). So you do not have to manually copy it. Just right click and paste it in another browser(Or use Ctrl+V shortcut in the browser search box)



22. **After pasting the link in the bar, press Enter key. Now we can access our file using the presigned URL.**



So, our file is private and can only be accessed by those with the pre-signed URL link for a limited duration.