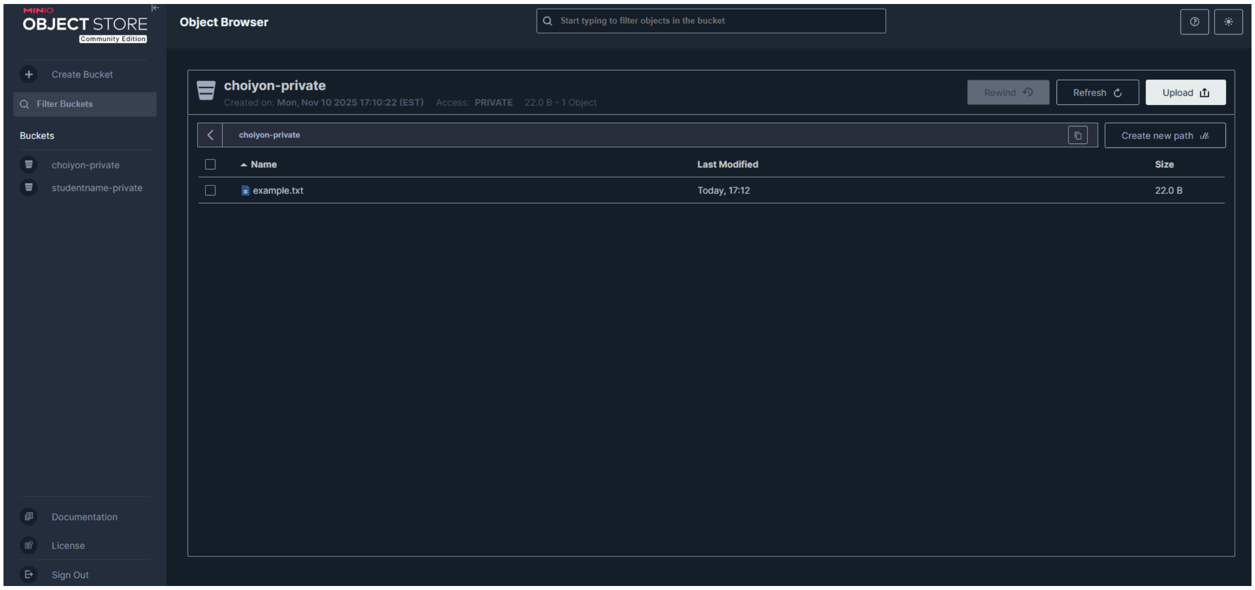

choiyon-private
Created on: Mon, Nov 10 2025 17:10:22 (EST) Access: PRIVATE 22.0 B - 1 Object

choiyon-private

□	Name	Last Modified	Size
□	example.txt	Today, 17:12	22.0 B

1. Setup Summary

- **Platform Used:** Option 3: MinIO Local Deployment. I downloaded the MinIO server executable and ran it on my local Windows machine to create a cloud storage environment that emulates S3.

2. Bucket Configurations

- `choiyon-private`: This bucket's purpose was to simulate storing sensitive files. Its access policy was kept as the default `private` setting, making it accessible only to authenticated users.
- `studentname-public`: This bucket's purpose was to simulate storing public-facing files. Its access policy was manually changed to `public`, allowing anyone on the internet to read its contents. An `example.txt` file was uploaded to both buckets.

3. Access Results

- Private Bucket Test: When the URL for the `example.txt` file in the `choiyon-private` bucket was opened in an incognito browser window, the system correctly returned an "Access Denied" error.
- Public Bucket Test: When the URL for the `example.txt` file in the `studentname-public` bucket was opened in an incognito browser window, the file's contents "This is a test file." were successfully displayed. This confirms that the bucket was open to unauthorized public access as intended.

4. Real-World Example

- **Incident:** The 2019 Capital One data breach.
- **Summary:** An attacker exploited a misconfigured web application firewall to gain access to Capital One's Amazon S3 buckets. These buckets, which were improperly secured and contained excessive permissions, held the personal information of over 100 million individuals. This breach was a direct result of a cloud configuration error on Capital One's part, not a failure of AWS security itself.

5. Reflection

What lessons does this lab teach about cloud responsibility and access control?

This lab demonstrates the critical importance of the Shared Responsibility Model in cloud security. The cloud provider like AWS, or MinIO in this simulation is responsible for securing the underlying infrastructure, but I, the user, am entirely responsible for securing my own data. This lab showed how easy it is to make a simple mistake, like setting an access policy to "public" instead of "private", and the immediate consequence is that the data is exposed. It proves that proper access control is not a set it and forget it task and that misconfigurations are a primary cause of major data breaches.