

AWS S3 Bucket Attack & Defense Lab Report

Created By:

Rituraj Singh

1. Title

AWS S3 Public Bucket Misconfiguration & Remediation using Static Website Hosting

2. Objective

The objective of this lab is to understand how misconfigured AWS S3 buckets can lead to **public data exposure**, and how to identify, exploit, and fix such vulnerabilities using AWS security controls.

3. Overview

In this lab, we performed a practical demonstration of:

- Creating an S3 bucket with public access enabled
 - Uploading a file and exposing it using Static Website Hosting
 - Attempting public access via browser
 - Encountering an **AccessDenied (403 Forbidden)** error
 - Fixing the issue by applying a **Bucket Policy**
 - Successfully accessing the file publicly
 - Securing the bucket again using **Block Public Access**
-

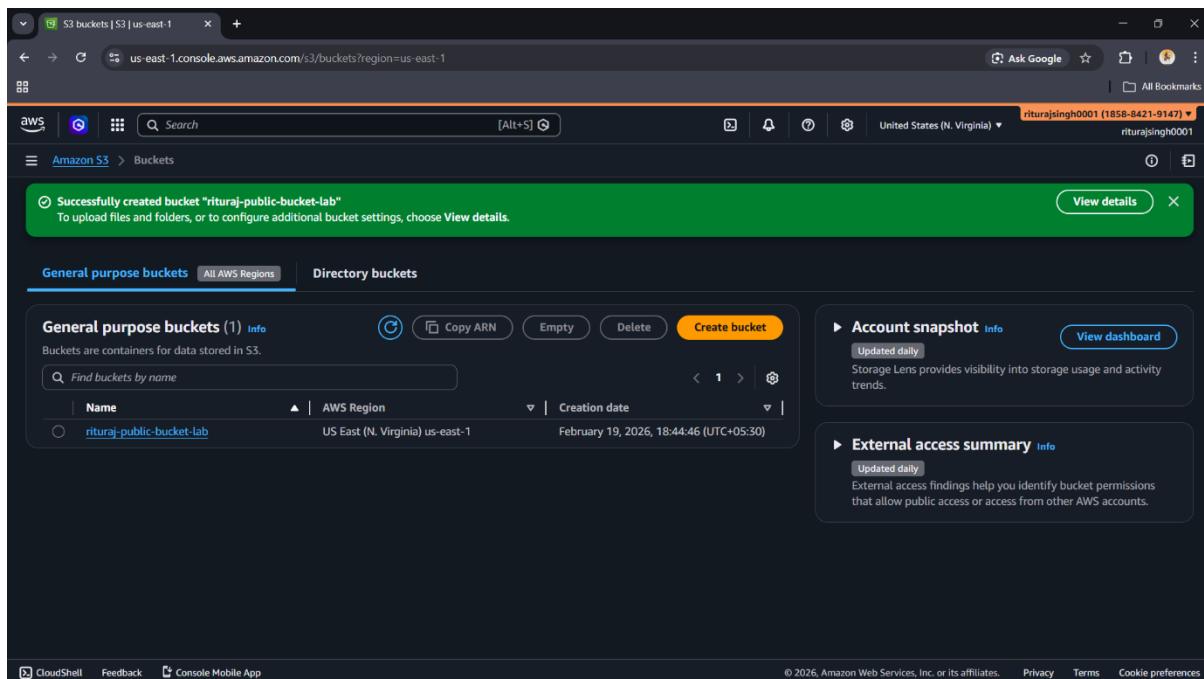
4. Prerequisites

- AWS Account
 - Basic knowledge of Amazon S3
 - Internet browser (Incognito mode for testing)
-

5. Lab Implementation

Step 1 – Create Test Bucket

- Open AWS Console → Amazon S3
- Click **Create Bucket**
- Bucket name: lab-public-bucket-<random>
- Region: us-east-1
- Disabled **Block All Public Access**
- Created the bucket



This configuration makes the bucket **potentially vulnerable** to public exposure.

Step 2 – Upload a File

- Open bucket → **Objects** tab
- Click **Upload**
- Uploaded file: hello.txt

File Content:

Hello,

This is demo lab

The screenshot shows the AWS S3 console interface. At the top, a green success message states: "Upload succeeded. For more information, see the Files and folders table." Below this, the "Upload: status" section indicates "Succeeded" with "1 file, 28.0 B (100.00%)" and "Failed" with "0 files, 0 B (0%)". The "Files and folders" tab is selected, showing a table with one item: "Hello.txt" (text/plain, 28.0 B, Status: Succeeded). The table has columns for Name, Folder, Type, Size, Status, and Error.

Step 3 – Enable Static Website Hosting (Attack Simulation)

- Go to **Properties tab**
- Enable **Static Website Hosting**
- Hosting type: Bucket hosting
- Index document: hello.txt

The screenshot shows the "Edit static website hosting" configuration page. Under "Static website hosting", "Enable" is selected. Under "Hosting type", "Host a static website" is selected. A note states: "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." In the "Index document" section, "Hello.txt" is specified. In the "Error document - optional" section, "error.html" is specified. At the bottom, "Redirection rules - optional" is mentioned with a link to "Learn more".

- Saved changes

Successfully edited static website hosting.

Requester pays
When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

Requester pays
Disabled

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

We recommend using AWS Amplify Hosting for static website hosting. Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [View your existing Amplify apps](#)

S3 static website hosting
Enabled

Hosting type
Bucket hosting

Bucket website endpoint
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)

<http://rituraj-public-bucket-lab.s3-website-us-east-1.amazonaws.com>

- Copied website endpoint:

<http://lab-public-bucket-xxxx.s3-website-us-east-1.amazonaws.com>

Opened in Incognito Mode

✖ Issue Encountered: 403 Forbidden Error

Instead of accessing the file, the following error was observed:

403 Forbidden

Code: AccessDenied

403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: R3QDVCK6VXNHA7TH
- HostId: iHHHaHO56WbfFqkQleOsZrhvVd-WH10YdSolv4CrSpN2JFB4OpCZKb1hBS7osPv3klxtKe60YgiFfDVbzdz9AvNkwbs+

Message: Access Denied

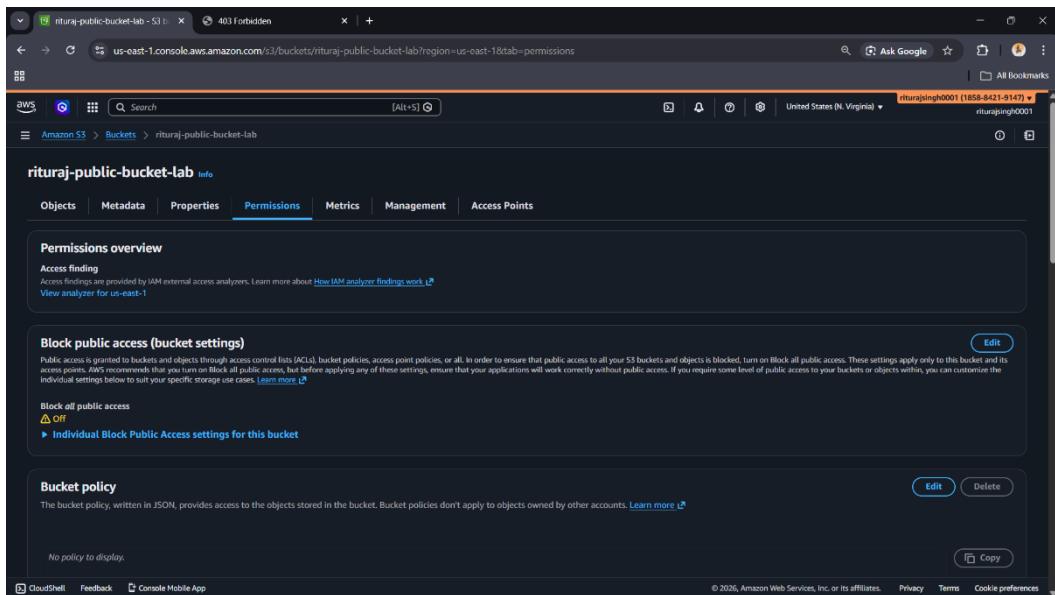
6. Root Cause Analysis

The error occurred because:

- Static Website Hosting was enabled ✓
- BUT **public read permissions were NOT granted** ✗

☞ AWS S3 requires explicit permission using:

- Bucket Policy



Without this, anonymous users cannot access data.

7. Fix – Applying Bucket Policy (Critical Step)

To resolve the issue, a **Bucket Policy** was added:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "PublicReadAccess",
```

```

    "Effect": "Allow",
    "Principal": "*",
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::your_bucket_name_/*"
}
]
}

```

The screenshot shows the AWS S3 Bucket Policy editor for the bucket 'rituraj-public-bucket-lab'. A green success message at the top states 'Successfully edited bucket policy.' Below it, the 'Bucket policy' section displays a JSON policy document:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::rituraj-public-bucket-lab/*"
    }
  ]
}

```

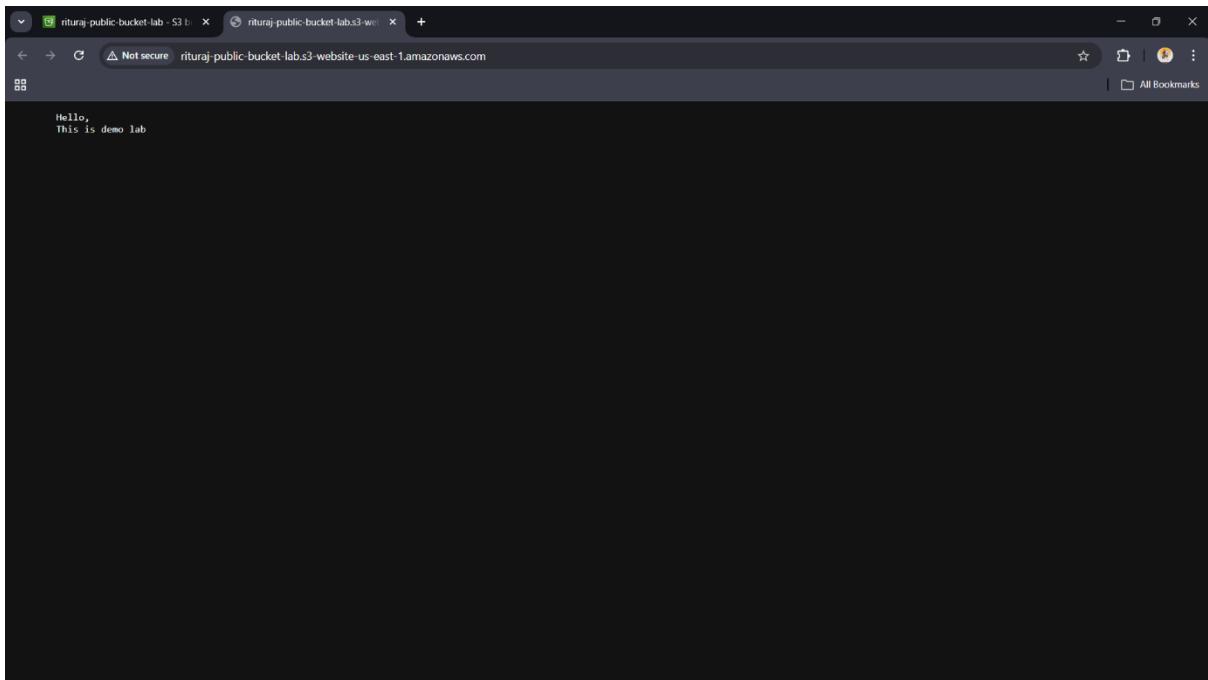
At the bottom right of the editor, there are 'Edit' and 'Delete' buttons, and a 'Copy' button above them. The browser's address bar shows the URL 'us-east-1.console.aws.amazon.com/s3/buckets/rituraj-public-bucket-lab?region=us-east-1&tab=permissions'.

✓ This policy allows:

- Public users (*)
- To perform s3:GetObject
- On all objects inside the bucket

✓ Result After Fix

- Opened website endpoint again in incognito
- Successfully accessed content:



8. Security Risk (Attack Perspective)

This configuration demonstrates a **real-world vulnerability**:

- Sensitive data can be exposed publicly
- No authentication required
- Anyone with the URL can access data

☞ This is a common **cloud misconfiguration vulnerability**

9. Defense – Securing the Bucket

To mitigate the issue:

- Enabled **Block Public Access**
 - Removed public access permissions
 - Ensured no public bucket policy exists
-

🔒 Verification

- Opened website endpoint again
- Received:



403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: R2QJYC6MEXNBAT7H
- HostId: lfHHaBO56WfaErjkQldOwZrvVdzWH0JYd9oIvkCrSpN2FB4OpCZKb1hBSf7osPv3kLxLKeI60YgilEdDV9zd59AwNkwcbn+

10. Cleanup

- Deleted hello.txt
 - Deleted S3 bucket
-

11. Conclusion

This lab demonstrated that:

- Enabling Static Website Hosting alone does NOT make content public
- Improper configurations can lead to **data exposure risks**
- Bucket Policies play a critical role in access control
- Security best practice is to **block public access unless absolutely required**