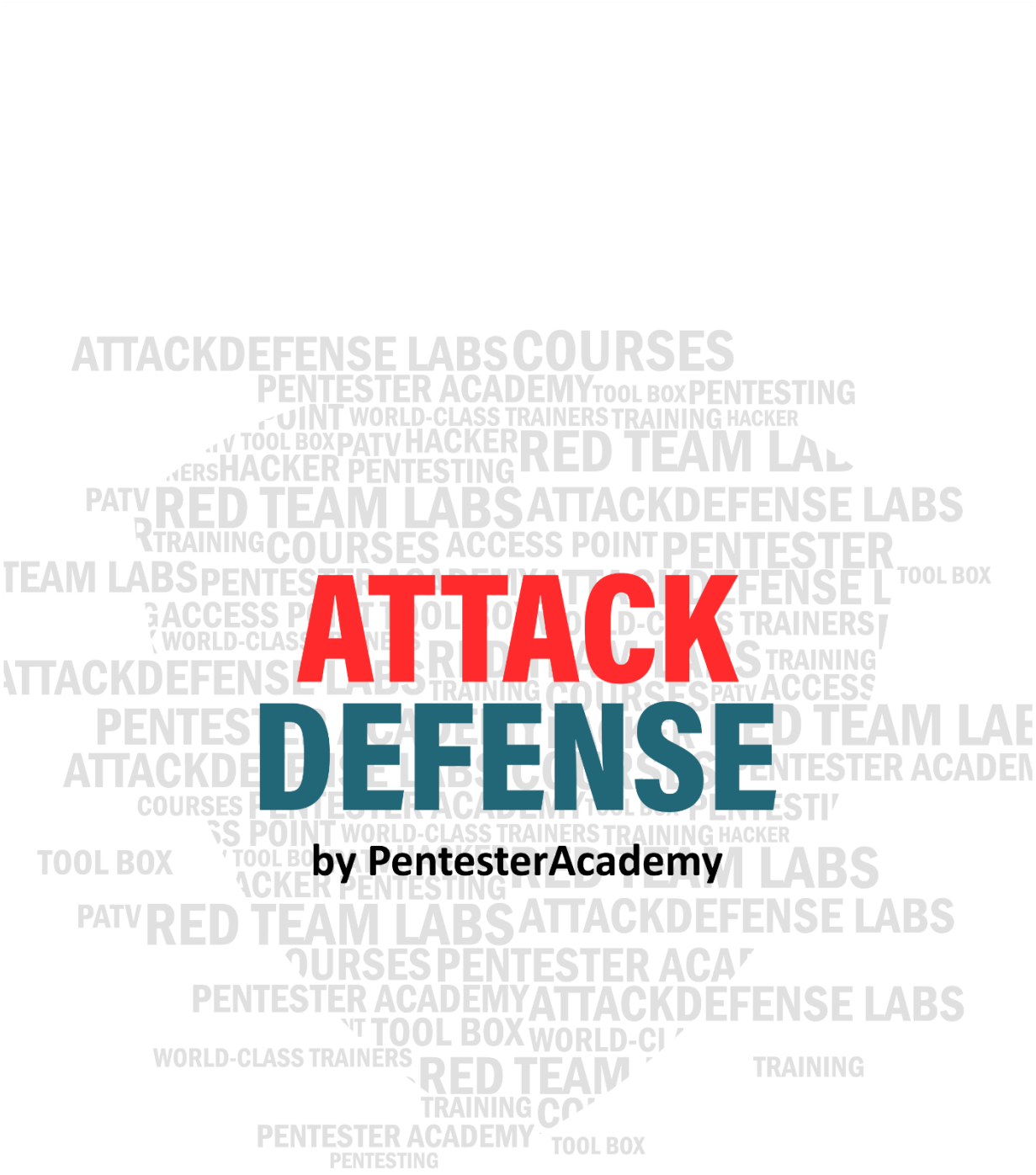

ATTACK
DEFENSE
by PentesterAcademy

Name	S3 Enumeration
URL	https://attackdefense.com/challengedetails?cid=2298
Type	AWS Cloud Security : S3

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

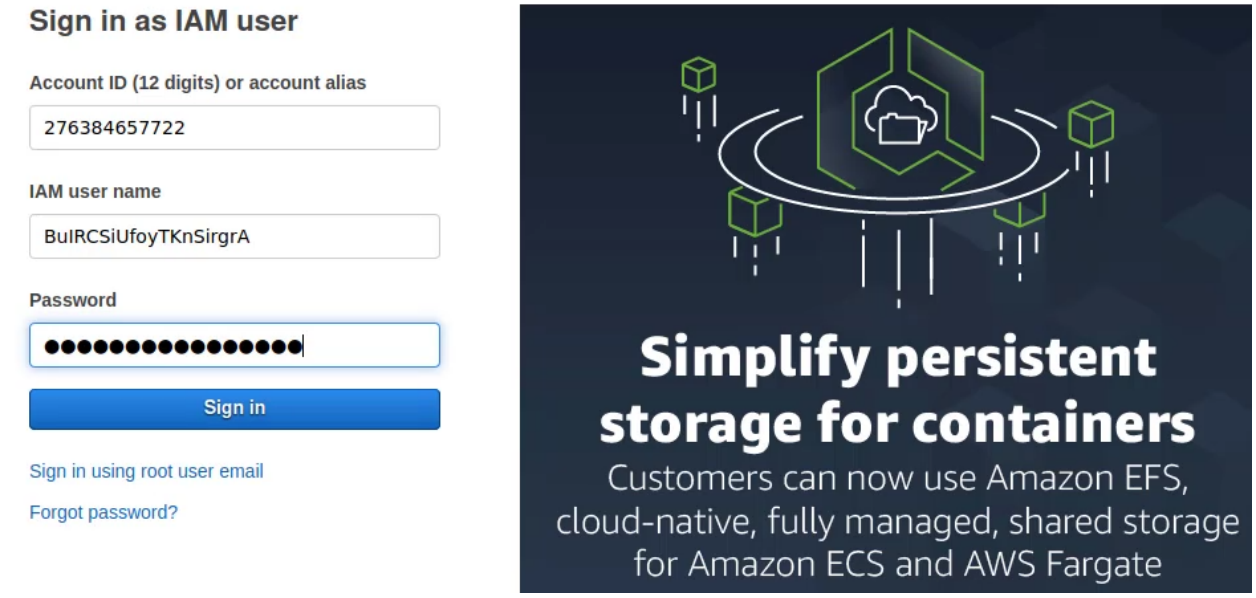
Solution:

Console Based Enumeration

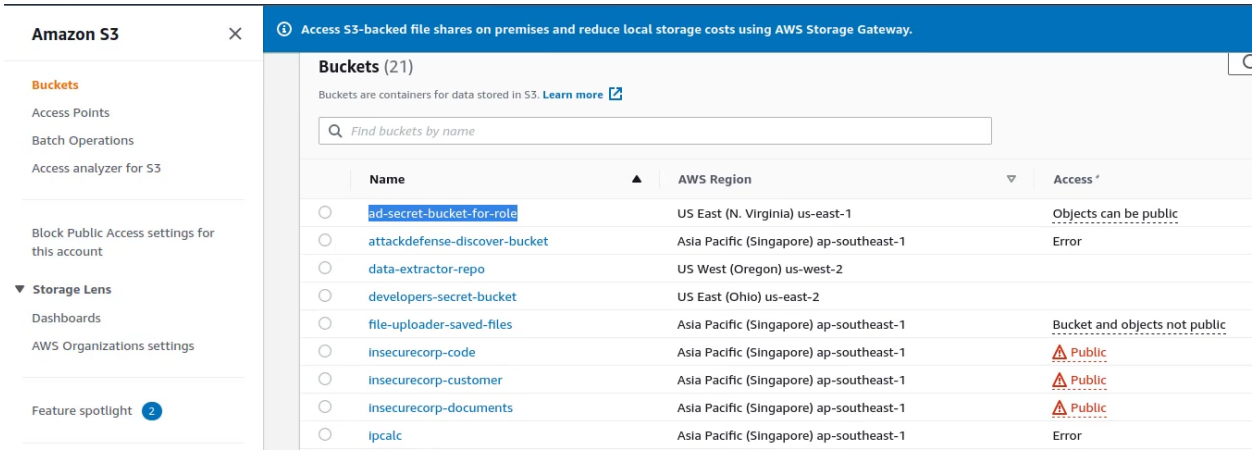
Step 1: Sign in into AWS console using AWS access credentials.

Access Credentials to your AWS lab Account

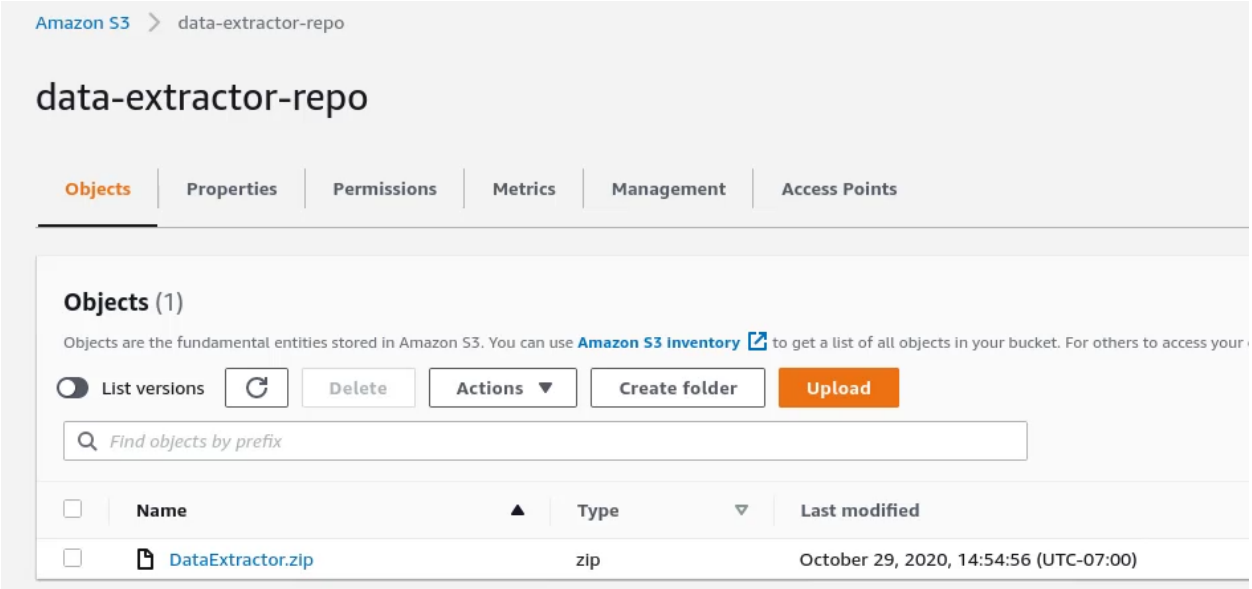
Login URL	https://276384657722.signin.aws.amazon.com/console
Region	Asia Pacific (Singapore) ap-southeast-1
Username	BuIRCSiUfoyTKnSirgrA
Password	Ty9yi1O1VNWdKy7W
Access Key ID	AKIAUAWOPGE5BNVRX7UJ
Secret Access Key	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



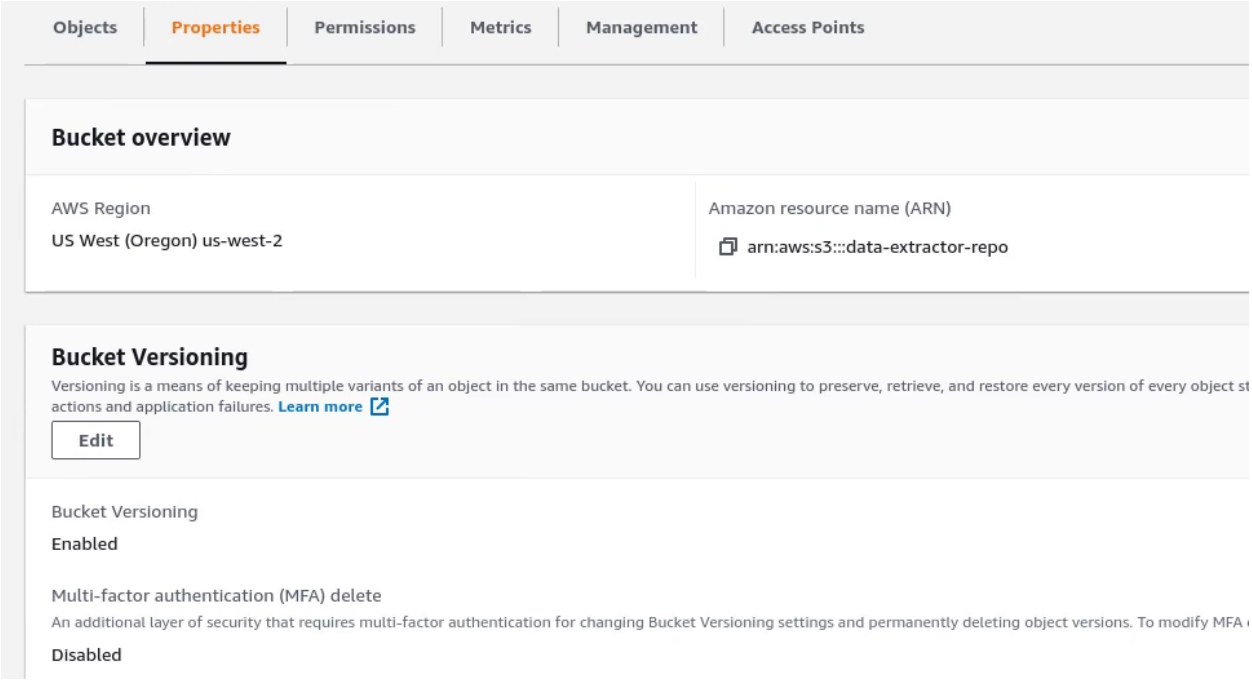
Step 2: Navigate to S3 dashboard.



Step 3: Click on bucket name to check bucket objects.

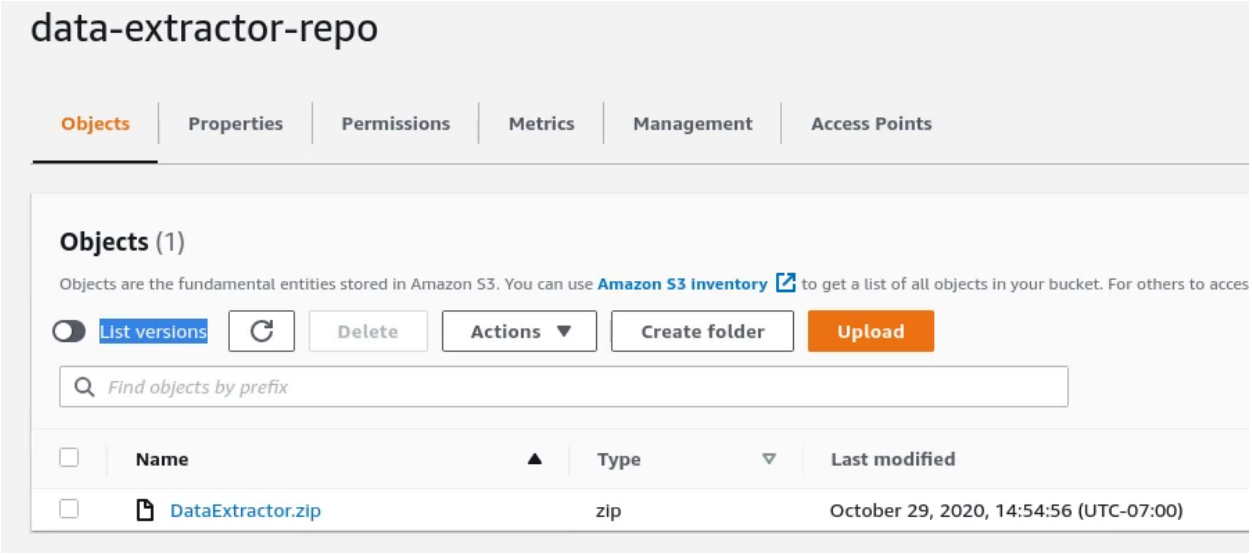


Step 4: Click on the properties tab to view bucket properties.

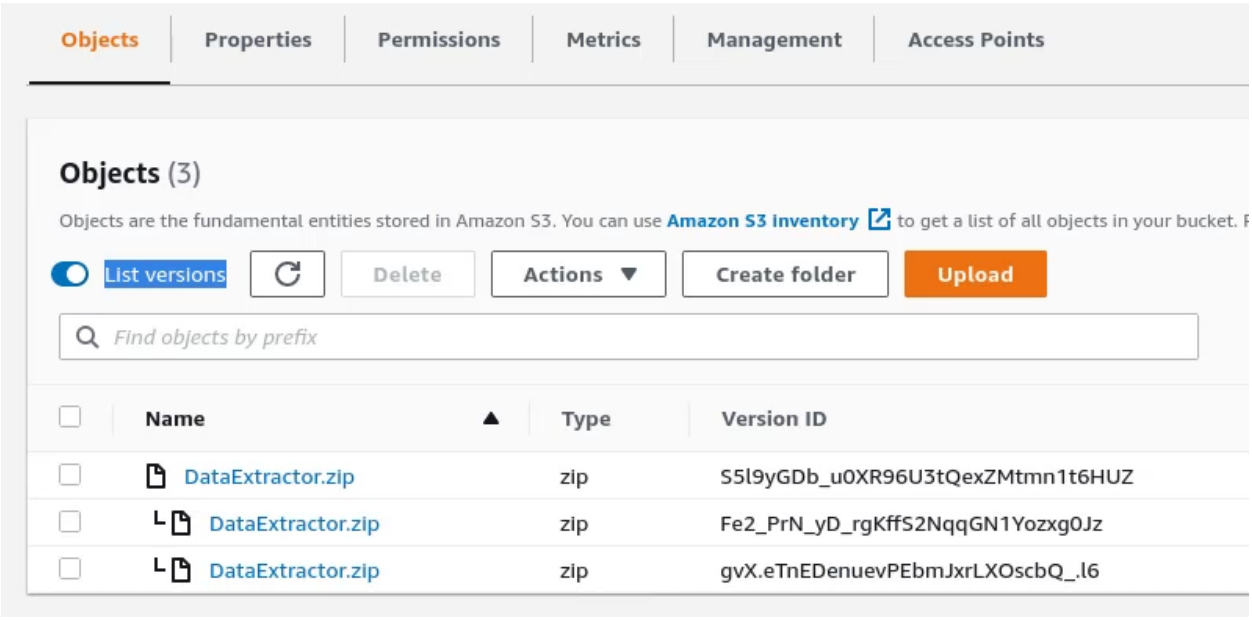


Bucket versioning is enabled !

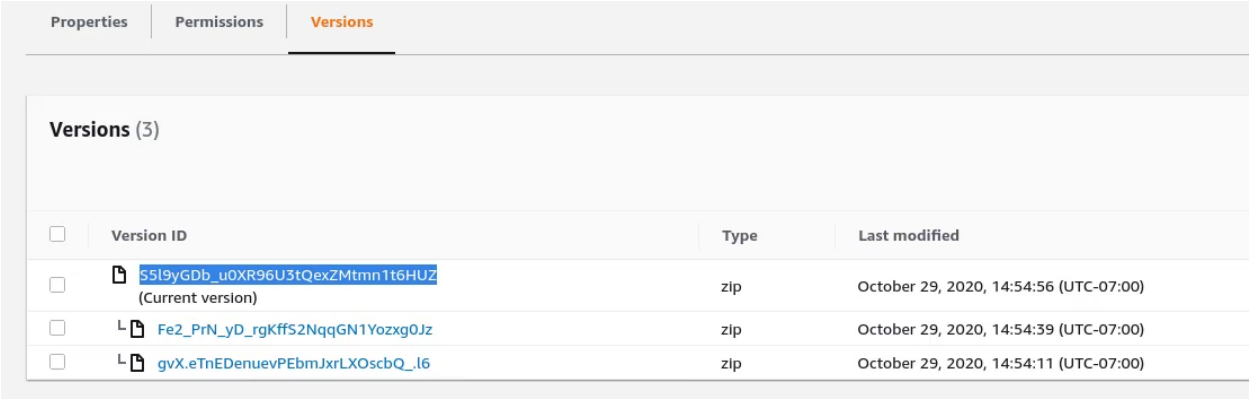
Step 5: Check the object versions for the bucket on the objects tab.



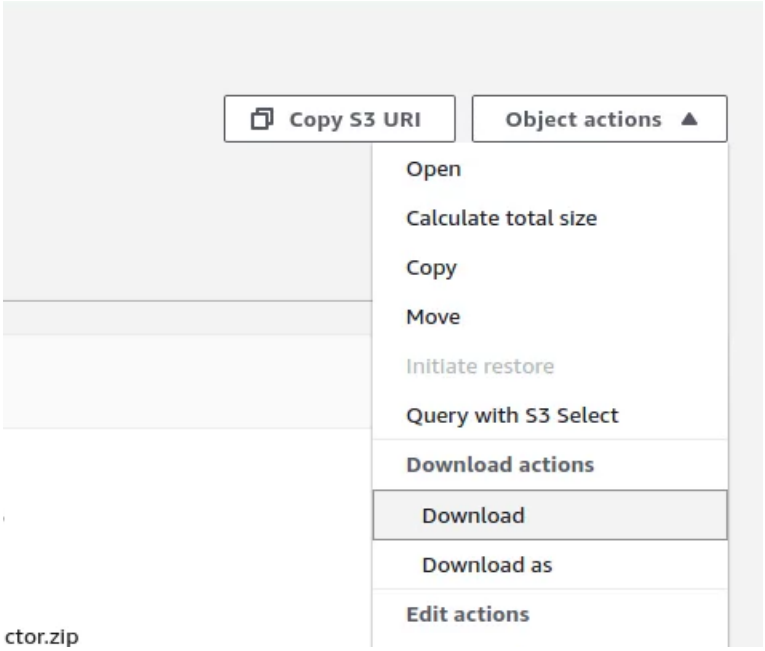
Turn on “List versions”

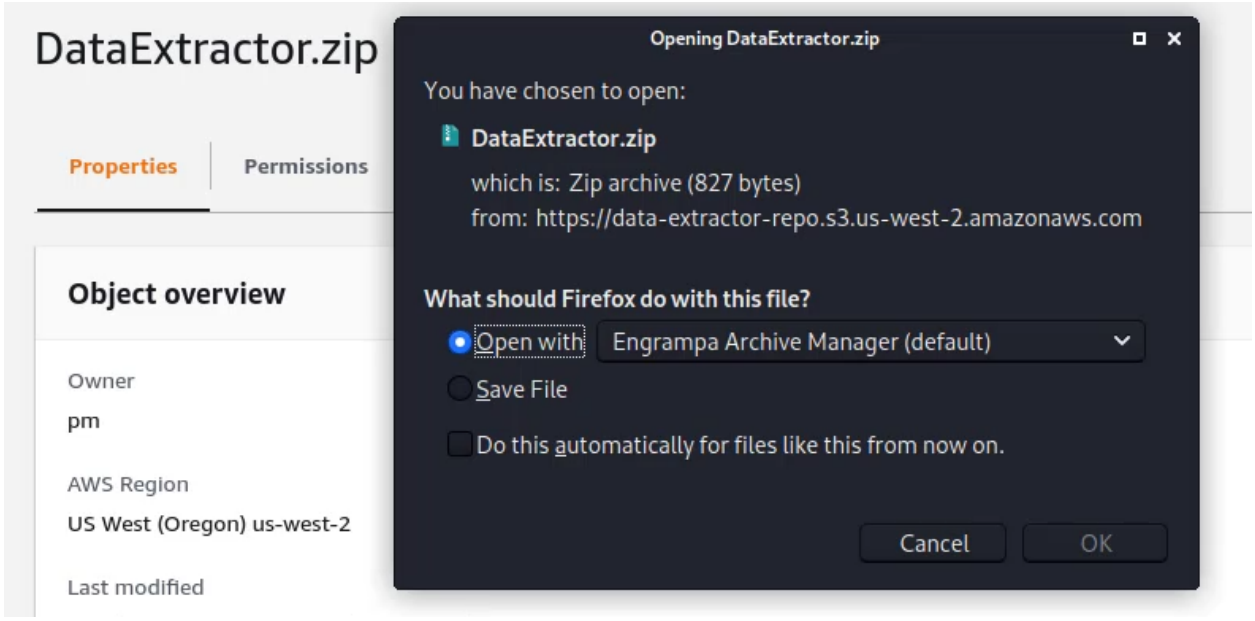


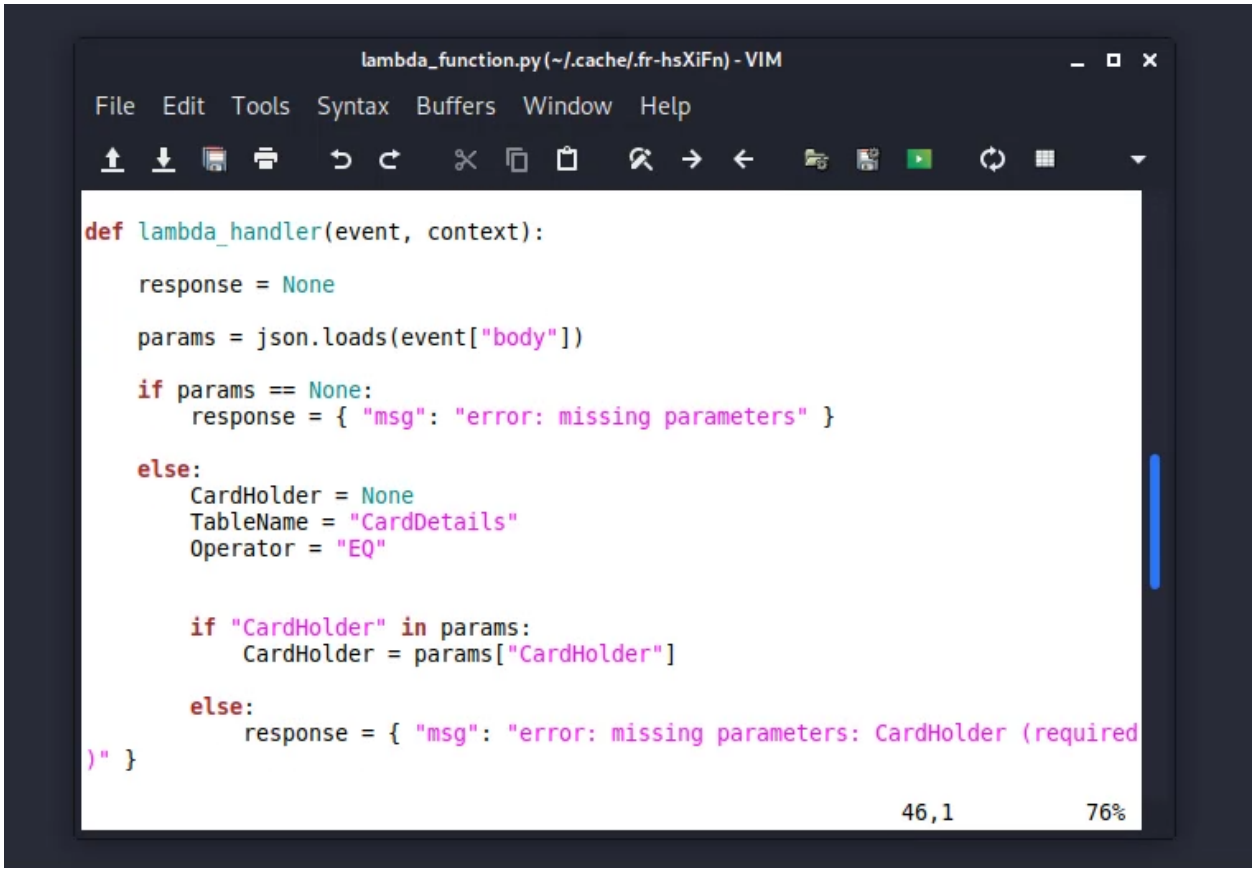
Step 6: Click on the object and navigate to the versions tab to check version details.



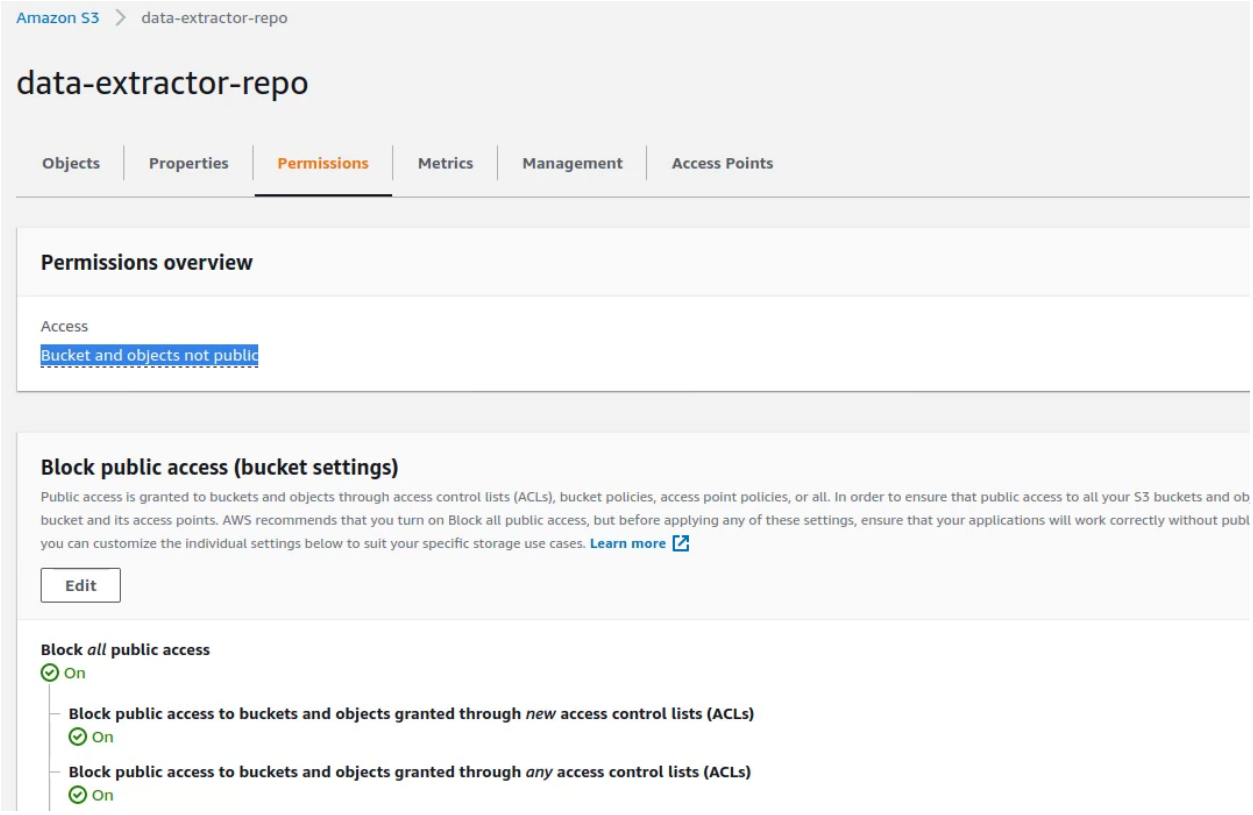
Step 7: Navigate to properties tab and download object to enumerate contents.



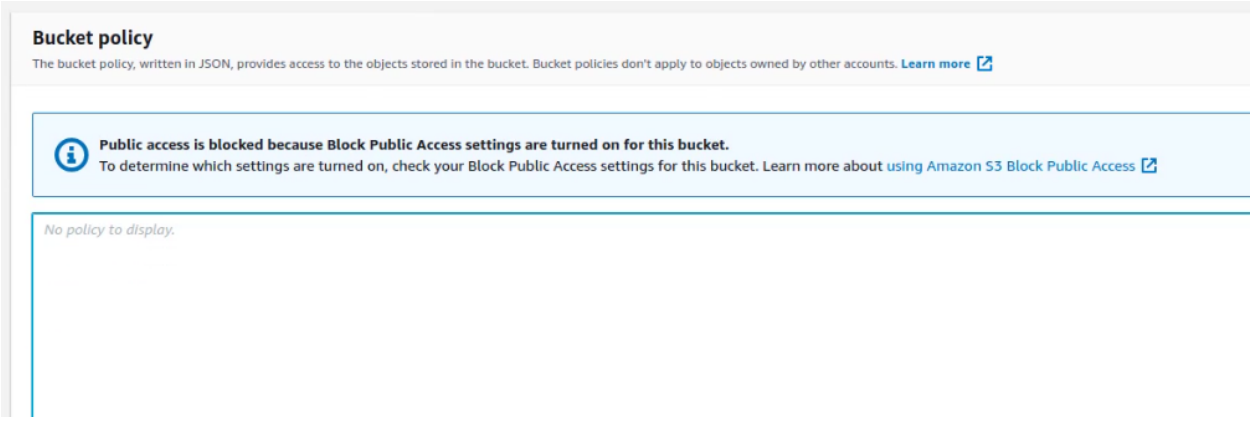

DataExtractor.zip
Properties
Permissions
Object overview
Owner
pm
AWS Region
US West (Oregon) us-west-2
Last modified
Opening DataExtractor.zip
You have chosen to open:
DataExtractor.zip
which is: Zip archive (827 bytes)
from: https://data-extractor-repo.s3.us-west-2.amazonaws.com
What should Firefox do with this file?
Open with
Engrampa Archive Manager (default)
Save File
Do this automatically for files like this from now on.
Cancel
OK


lambda_function.py (~/.cache/.fr-hsXiFn) - VIM
File Edit Tools Syntax Buffers Window Help
def lambda_handler(event, context):
response = None
params = json.loads(event["body"])
if params == None:
response = { "msg": "error: missing parameters" }
else:
CardHolder = None
TableName = "CardDetails"
Operator = "EQ"
if "CardHolder" in params:
CardHolder = params["CardHolder"]
else:
response = { "msg": "error: missing parameters: CardHolder (required
)" }
46,1 76%

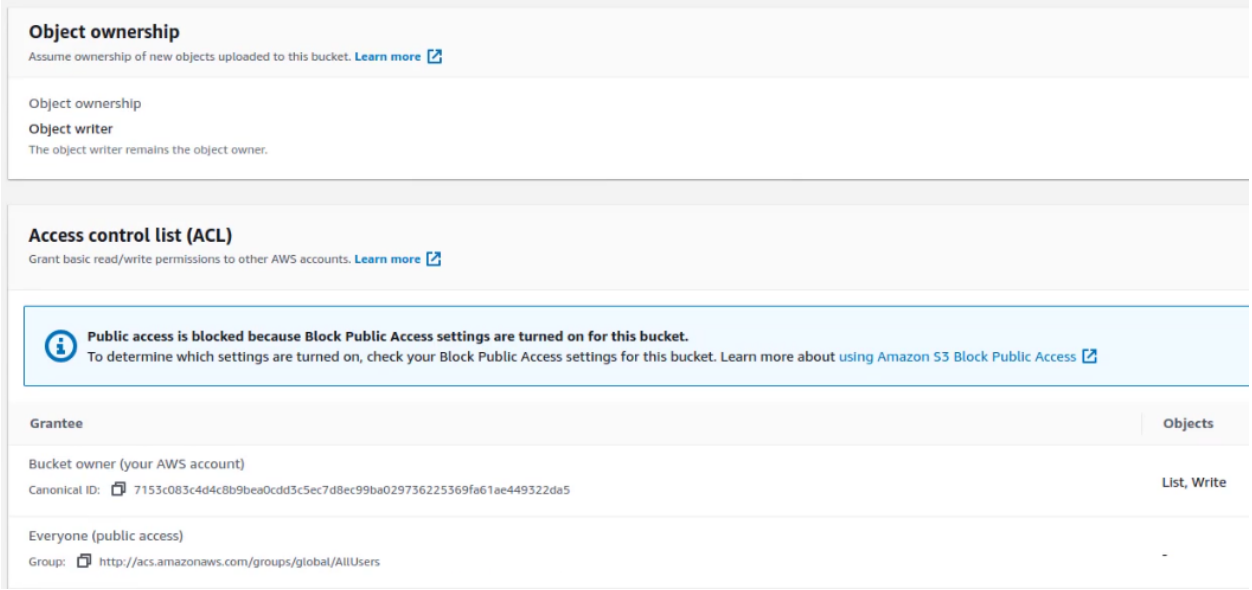
Step 8: Go back to S3 bucket object list and click on the permissions tab to check bucket permissions.



Bucket is not public.

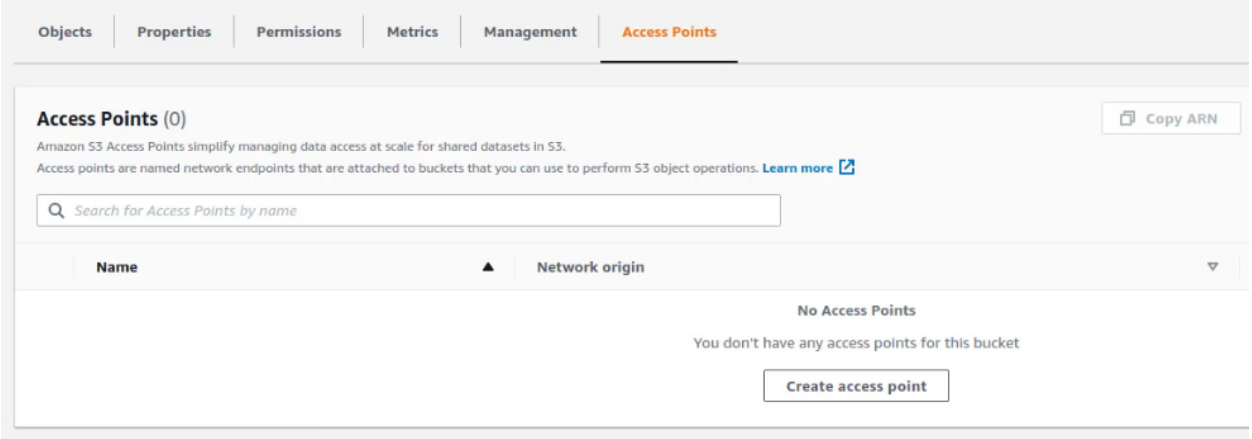


Bucket policy.

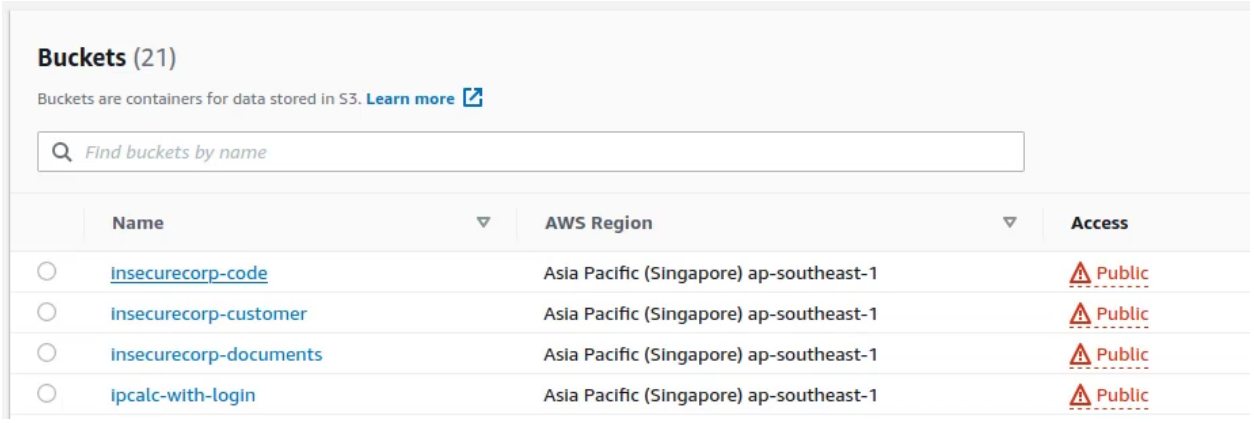


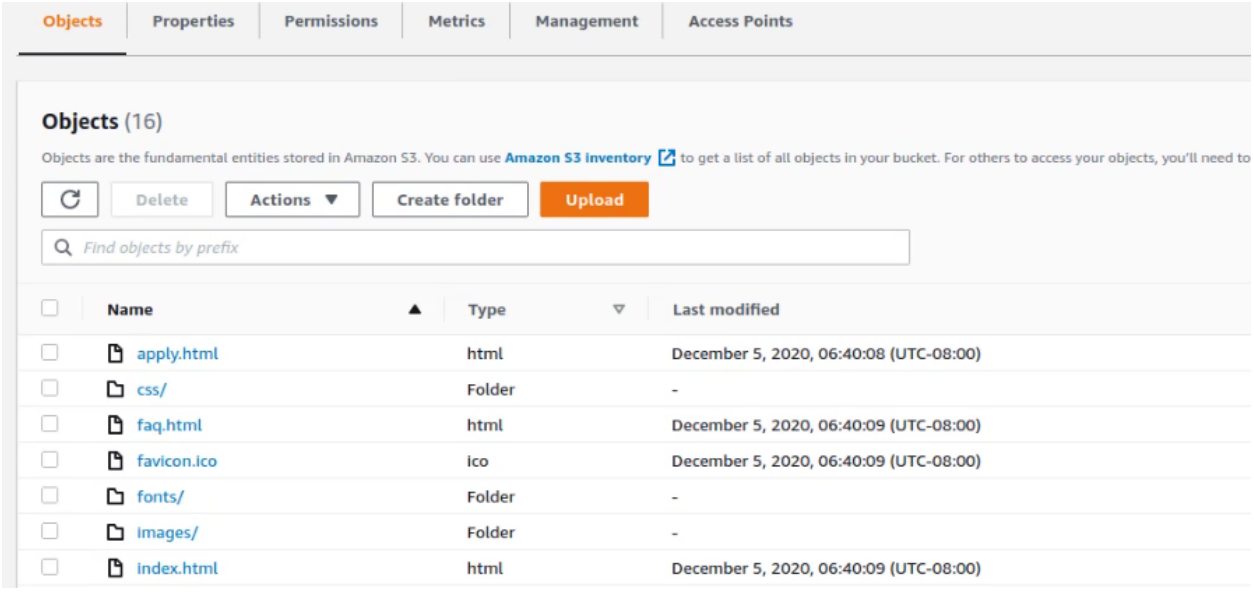
Bucket ownership and ACL.

Go to ‘Access Points’ tab to check the named network endpoints attached to the bucket.

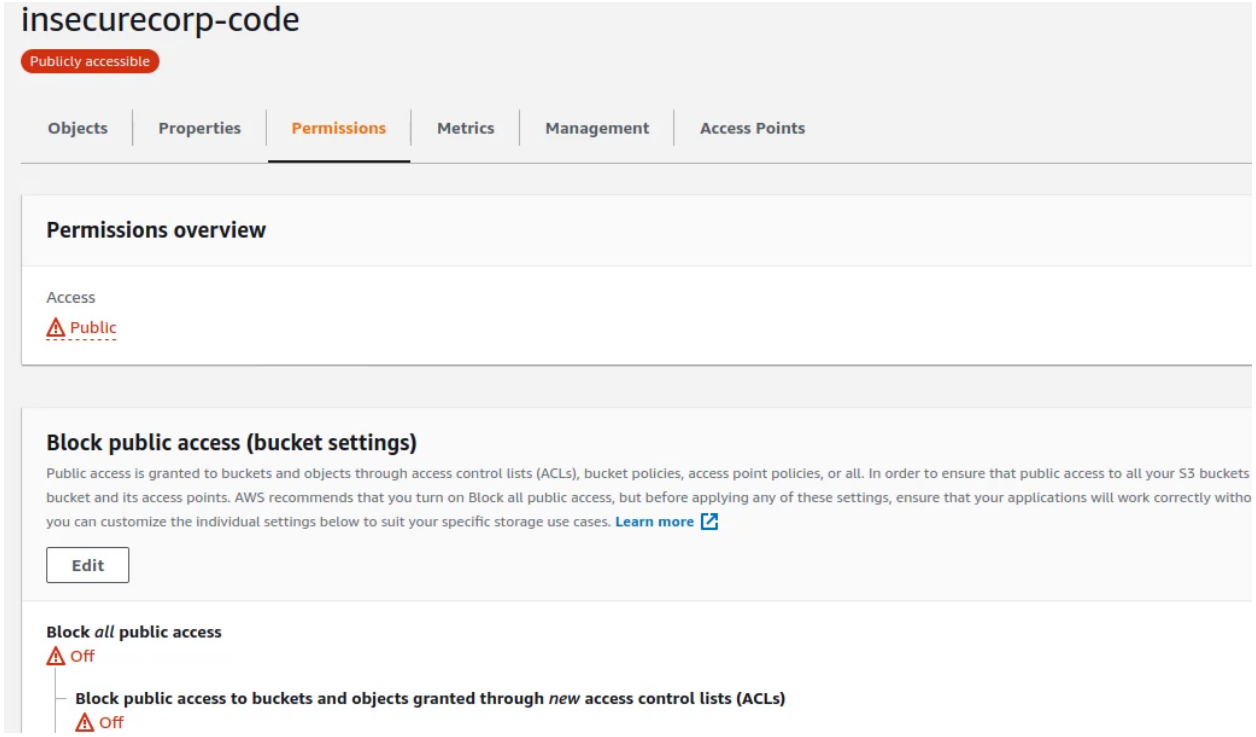


Step 9: Similarly enumerate other buckets.

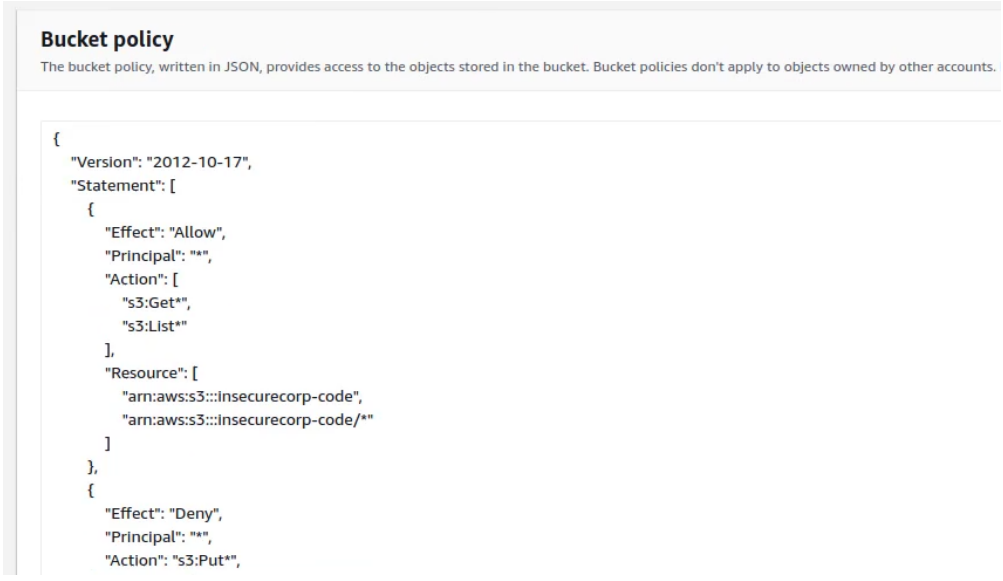




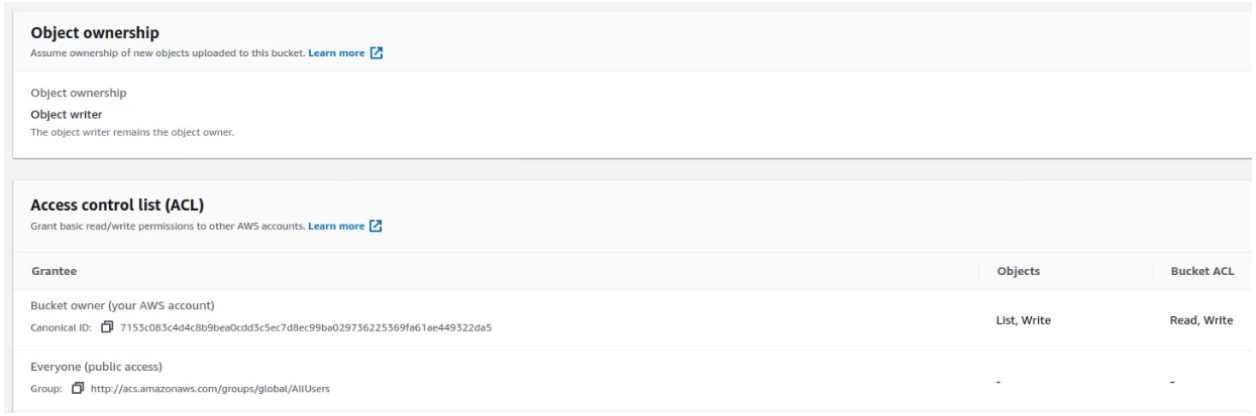
Bucket objects.



Bucket is publicly accessible !

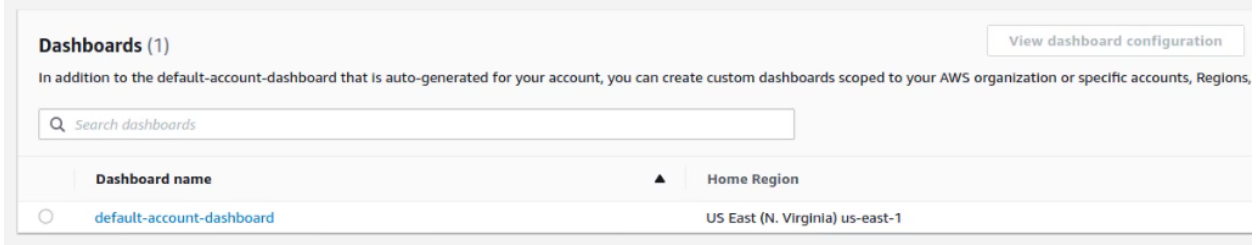


Bucket policy.

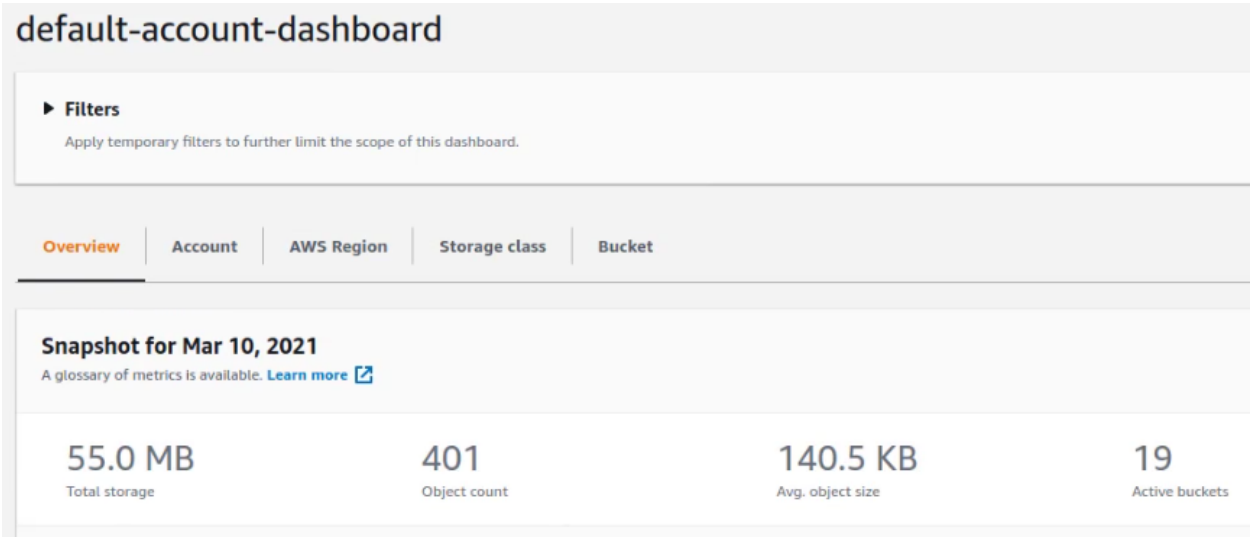


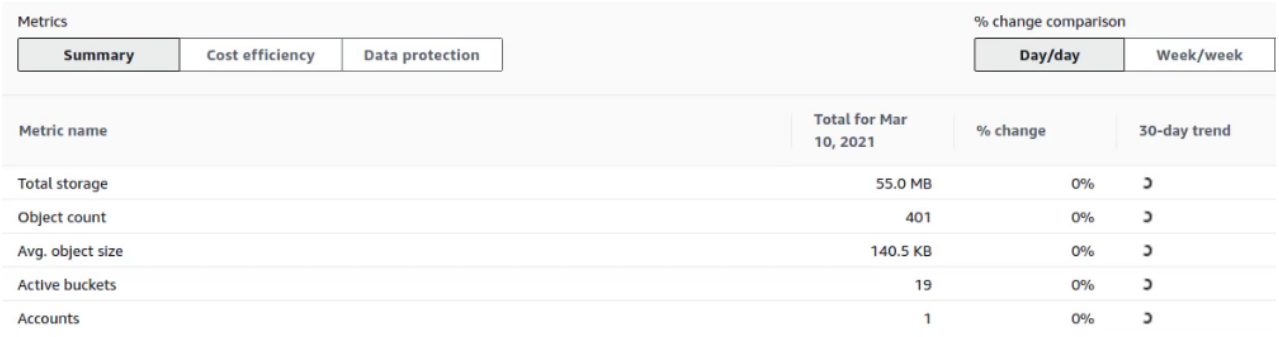
Ownership and ACL.

Step 10: Navigate to S3 storage lens dashboard from the left panel.



Step 11: Click on the dashboard name to view details.





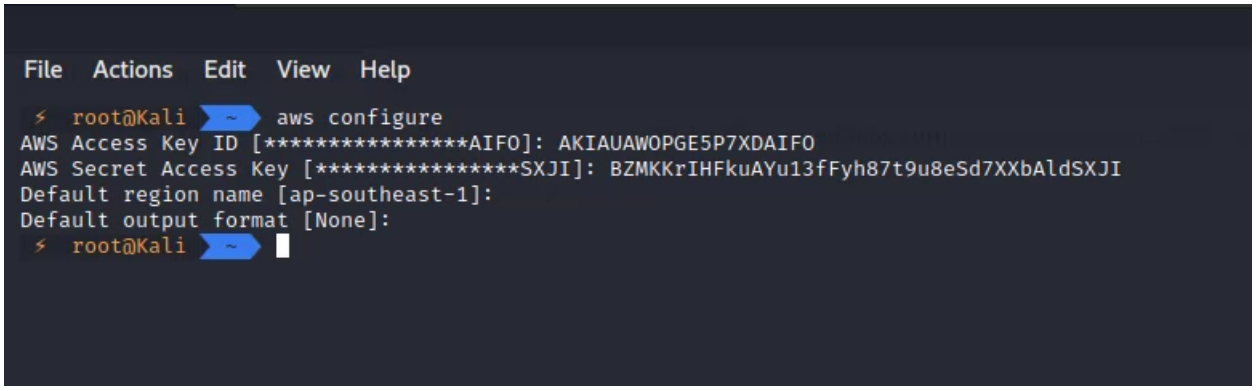
CLI Based Enumeration

Step 1: Configure AWS CLI with AWS access keys

Command: aws configure

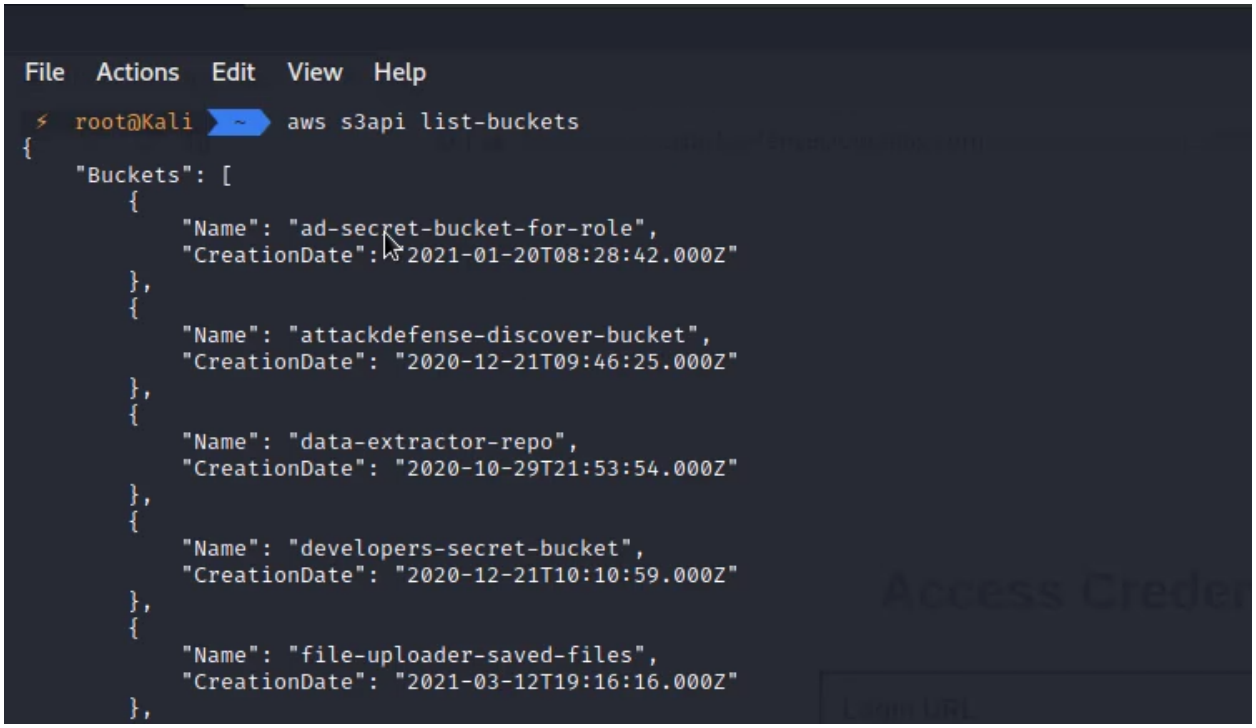
Access Credentials to your AWS lab Account

Login URL	https://276384657722.signin.aws.amazon.com/console
Region	**Asia Pacific (Singapore) ap-southeast-1**
Username	**grLFsxUlNbOQxwlXbNoS**
Password	**uJll1tZw4DElhya4**
Access Key ID	**AKIAUAWOPGE5P7XDAIFO**
Secret Access Key	**BZMKKrlHFkuAYu13fFyh87t9u8eSd7XXbAldSXJl**



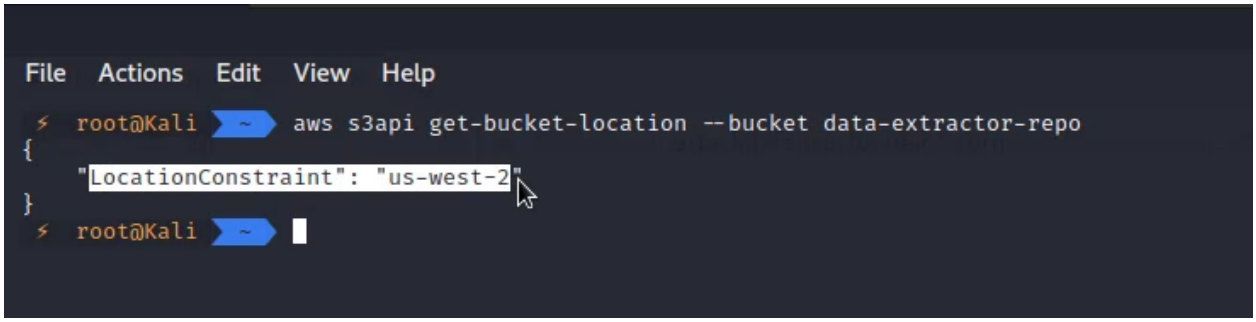
Step 2: List S3 buckets.

Command: aws s3api list-buckets



Step 3: Check bucket location.

Command: aws s3api get-bucket-location --bucket data-extractor-repo



Step 4: Enumerate bucket objects

Commands:
aws s3api list-objects-v2 --bucket data-extractor-repo
aws s3api list-objects --bucket file-uploader-saved-files

```
File  Actions  Edit  View  Help
 ⚡ root@Kali ~ aws s3api list-objects-v2 --bucket data-extractor-repo
{
    "Contents": [
        {
            "Key": "DataExtractor.zip",
            "LastModified": "2020-10-29T21:54:56.000Z",
            "ETag": "\"014458aab6fe8320f7c6a5e86563427b\"",
            "Size": 827,
            "StorageClass": "STANDARD"
        }
    ]
}
 ⚡ root@Kali ~
```

```
File  Actions  Edit  View  Help
 ⚡ root@Kali ~ aws s3api list-objects --bucket file-uploader-saved-files
{
    "Contents": [
        {
            "Key": "flag",
            "LastModified": "2021-03-12T19:17:18.000Z",
            "ETag": "\"4d0569150897d2ec346e9b0ae5399dd5\"",
            "Size": 32,
            "StorageClass": "STANDARD",
            "Owner": {
                "DisplayName": "pm",
                "ID": "7153c083c4d4c8b9bea0cdd3c5ec7d8ec99ba029736225369fa61ae449322da5"
            }
        }
    ]
}
 ⚡ root@Kali ~
```

Step 5: Check object versions.

Command: aws s3api list-object-versions --bucket data-extractor-repo

```
File  Actions  Edit  View  Help
root@Kali ~ aws s3api list-object-versions --bucket data-extractor-repo
{
    "Versions": [
        {
            "ETag": "\"014458aab6fe8320f7c6a5e86563427b\"",
            "Size": 827,
            "StorageClass": "STANDARD",
            "Key": "DataExtractor.zip",
            "VersionId": "S5l9yGDb_u0XR96U3tQexZMtmn1t6HUZ",
            "IsLatest": true,
            "LastModified": "2020-10-29T21:54:56.000Z",
            "Owner": {
                "DisplayName": "pm",
                "ID": "7153c083c4d4c8b9bea0cdd3c5ec7d8ec99ba029736225369fa61ae449322da5"
            }
        },
        {
            "ETag": "\"7c437b026a869f8d51a2d2ddae25d874\"",
            "Size": 844,
            "StorageClass": "STANDARD",
            "Key": "DataExtractor.zip",
```

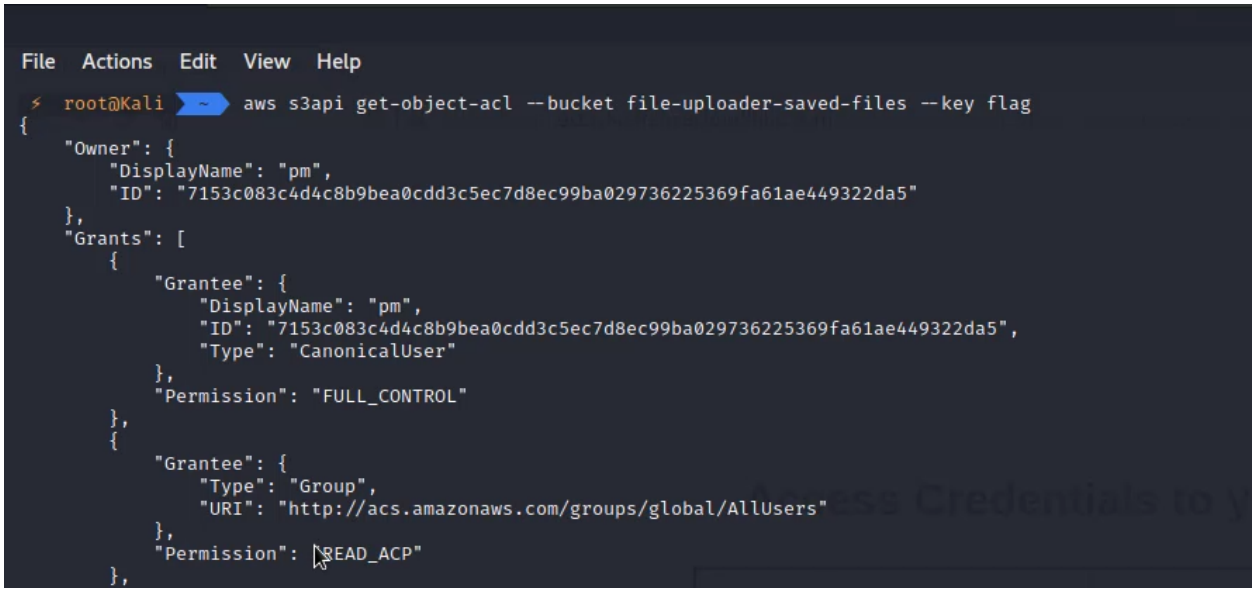
Step 6: Check bucket ACLs and objects ACLs.

Commands:

aws s3api get-bucket-acl --bucket file-uploader-saved-files

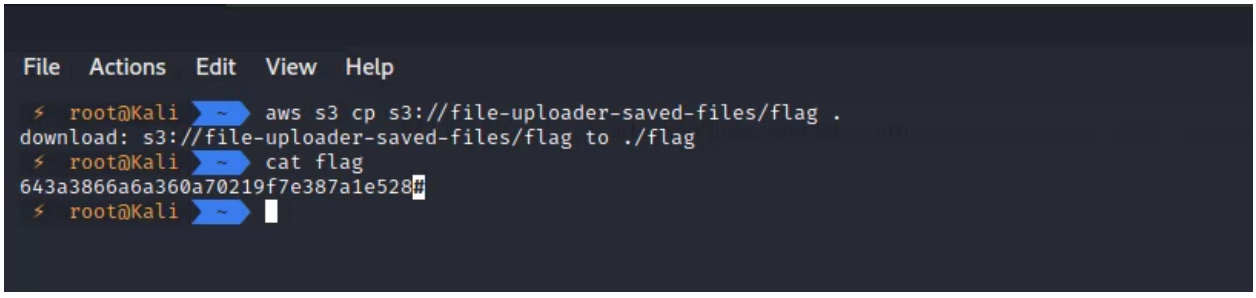
aws s3api get-object-acl --bucket file-uploader-saved-files --key flag

```
File  Actions  Edit  View  Help
root@Kali ~ aws s3api get-bucket-acl --bucket file-uploader-saved-files
{
    "Owner": {
        "DisplayName": "pm",
        "ID": "7153c083c4d4c8b9bea0cdd3c5ec7d8ec99ba029736225369fa61ae449322da5"
    },
    "Grants": [
        {
            "Grantee": {
                "DisplayName": "pm",
                "ID": "7153c083c4d4c8b9bea0cdd3c5ec7d8ec99ba029736225369fa61ae449322da5",
                "Type": "CanonicalUser"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "READ"
        },
        {
```



Step 7: Download objects from the S3 bucket.

Commands:
aws s3 cp s3://file-uploader-saved-files/flag .
cat flag



Step 8: Check bucket policy status.

Command: aws s3api get-bucket-policy-status --bucket insecurecorp-code

```
root@Kali ~ aws s3api get-bucket-policy-status --bucket insecurecorp-code
{
    "PolicyStatus": {
        "IsPublic": true
    }
}
root@Kali ~
```

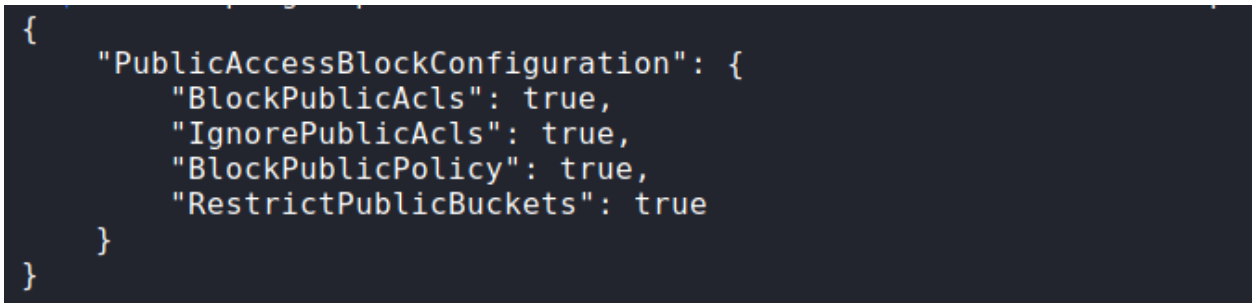
Step 9: Get bucket policy and beautify the output.

Command: aws s3api get-bucket-policy --bucket insecurecorp-code --output text | python -m json.tool

```
root@Kali ~ aws s3api get-bucket-policy --bucket insecurecorp-code --output text | python -m json.tool
{
    "Statement": [
        {
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Effect": "Allow",
            "Principal": "*",
            "Resource": [
                "arn:aws:s3:::insecurecorp-code",
                "arn:aws:s3:::insecurecorp-code/*"
            ]
        },
        {
            "Action": "s3:Put*",
            "Effect": "Deny",
            "Principal": "*",
            "Resource": [
                "arn:aws:s3:::insecurecorp-code",
                "arn:aws:s3:::insecurecorp-code/*"
            ]
        }
    ],
    "Version": "2012-10-17"
}
root@Kali ~
```

Step 9: Check the public access block for a bucket.

Command: aws s3api get-public-access-block --bucket data-extractor-repo



References:

1. AWS CLI (https://docs.aws.amazon.com/cli/latest/reference/)